LEONHARDI EULERI OPERA OMNIA
SUB AUSPICIIS SOCIETATIS SCIENTIARUM NATURALIUM HELVETICAE
EDENDA CURAVERUNT
FERDINAND RUDIO · ADOLF KRAZER · PAUL STÄCKEL

SERIES I · OPERA MATHEMATICA · VOLUMEN III

LEONHARDI EULERI

COMMENTATIONES ARITHMETICAE

VOLUMEN SECUNDUM

EDIDIT

FERDINAND RUDIO

LIPSIAE ET BEROLINI
TYPIS ET IN AEDIBUS B. G. TEUBNERI
MCMXVII

LEONHARDI EULERI

OPERA OMNIA

LEONHARDI EULERI
OPERA OMNIA

SUB AUSPICIIS
SOCIETATIS SCIENTIARUM NATURALIUM
HELVETICAE

EDENDA CURAVERUNT

FERDINAND RUDIO
ADOLF KRAZER PAUL STÄCKEL

SERIES PRIMA
OPERA MATHEMATICA
VOLUMEN TERTIUM

LIPSIAE ET BEROLINI
TYPIS ET IN AEDIBUS B. G. TEUBNERI
MCMXVII

LEONHARDI EULERI

COMMENTATIONES ARITHMETICAE

VOLUMEN SECUNDUM

EDIDIT

FERDINAND RUDIO

LIPSIAE ET BEROLINI
TYPIS ET IN AEDIBUS B. G. TEUBNERI
MCMXVII

EDITIO STEREOTYPICA 1978
ORELL FÜSSLI TURICI

VORWORT DES HERAUSGEBERS

Der vorliegende zweite Band der *Commentationes arithmeticae*[1]) EULERS, der mit Abhandlung 283 des ENESTRÖMSCHEN Verzeichnisses beginnt und mit Abhandlung 554 schließt, umfaßt mit 26 Abhandlungen die Druckjahre 1764—1783. EULER ist 1766 von Berlin nach Petersburg zurückgekehrt und ist dort am 18. September 1783 gestorben. Es handelt sich also in unserem Bande um die beiden letzten Jahre seines Aufenthaltes in Berlin und um seinen ganzen zweiten Aufenthalt in Petersburg. Die Drucklegung des ersten Bandes der *Opuscula analytica*, dem die beiden letzten Abhandlungen 552 und 554 des vorliegenden Bandes angehören und der im Todesjahre 1783 erschien, hat EULER noch selbst vorbereitet. Man wird sich überdies erinnern, daß er seit 1766 völlig erblindet war, nachdem er schon 1735 das rechte Auge verloren hatte.

Nach dem Einteilungsplane der Gesamtausgabe von EULERS Werken, wie er im Jahresbericht der Deutschen Mathematiker-Vereinigung **19**, 1910, abgedruckt ist, hätten im vorliegenden Bande I_3 auch die beiden Abhandlungen 395 *De inventione quotcunque mediarum proportionalium citra radicum extractionem* und 530 *Recherches sur une nouvelle espèce de quarrés magiques* Aufnahme finden sollen. Bei genauerer Prüfung hat sich aber gezeigt, daß die erste besser den algebraischen Abhandlungen und die zweite besser den kombinatorischen zuzuweisen ist. So wird denn 395 in I_6 und 530 in I_7 erscheinen. Umgekehrt sind in unsern Band I_3 nachträglich noch zwei Abhandlungen aufgenommen worden, die ursprünglich nicht dafür bestimmt waren, nämlich die Abhandlungen 708a und 541. Davon wird noch ausführlicher zu reden zu sein.[2])

Von den 26 Abhandlungen unseres Bandes gehören nur 23 LEONHARD EULER an. Eine, nämlich die soeben erwähnte Abhandlung 708a, stammt von NICOLAUS FUSS (1755—1826) und zwei, nämlich A_9 und A_{31}, sind von LEONHARDS Sohne JOHANN

---

1) Siehe das Vorwort zum vorhergehenden Bande.

2) Siehe p. XIV—XV und XXXI.

ALBRECHT EULER (1734—1800) verfaßt, dessen Schriften, unserm Redaktionsplane gemäß, in die Gesamtausgabe der Werke des Vaters mit aufgenommen werden sollen.[1])

Die große Mehrzahl der Abhandlungen des vorliegenden Bandes ist in den Denkschriften der Petersburger Akademie erschienen, nämlich 14 in den Novi Commentarii (1764—1776) und 6 in den Acta (1780—1783); 3, in Briefform gehaltene, sind in den Berliner Nouveaux mémoires (1774—1779) veröffentlicht und je eine in den Abhandlungen der churfürstlich-baierischen Akademie (1764) und den Nova acta eruditorum (1773; diese Abhandlung 445 erschien nachher[2]) auch noch 1780 in den Petersburger Acta); endlich sind, wie schon bemerkt, die beiden Abhandlungen 552 und 554 im Jahre 1783 im ersten Bande der *Opuscula analytica* veröffentlicht. Mit Ausnahme der drei Abhandlungen A_9 (J. A. EULER), 708a (N. FUSS) und 541 sind alle Abhandlungen unseres Bandes auch in der bekannten von P. H. und N. FUSS 1849 unter dem Titel *Commentationes arithmeticae collectae* herausgegebenen Sammlung[3]) enthalten. Über das Fehlen von 541 wird noch gesprochen werden.[4]) Umgekehrt haben die Brüder FUSS die beiden Abhandlungen 395 und 530 in ihre Sammlung aufgenommen, die, wie schon bemerkt, in unserer Ausgabe in den Bänden I_6 und I_7 erscheinen werden.

Die Grundsätze, nach denen der vorliegende zweite Band der *Commentationes arithmeticae* bearbeitet wurde, sind dieselben, die auch für den ersten maßgebend waren. Sie sind im Vorworte zu jenem Bande ausführlich dargelegt worden und ich kann mich daher darauf beschränken, auf dieses Vorwort zu verweisen.

Unser Band wird eröffnet durch die große Abhandlung 283 *De numeris primis valde magnis*, die EULER nach den Akten schon am 1. Dezember 1760 der Petersburger Akademie vorgelegt hatte.[5]) Es sei gleich hier bemerkt, daß die Frage nach der Ermittelung großer Primzahlen in unserem Bande I_3 eine nicht unbeträchtliche Rolle spielt. Außer 283 sind

1) Siehe P. STÄCKEL, *JOHANN ALBRECHT EULER*, Vierteljahrsschrift der Naturforschenden Gesellschaft in Zürich 55, 1910, p. 63. Siehe auch ENESTRÖMS *Verzeichnis*, p. 218—222.

2) Siehe p. XXVII.

3) Siehe hierüber das Vorwort zum vorhergehenden Bande. Was dort insbesondere p. XI—XII gesagt worden ist, gilt in gleicher Weise auch für den Abdruck der im vorliegenden Bande enthaltenen Abhandlungen.

4) Siehe p. XXXI.

5) Das Summarium der Abhandlung 283 findet sich auch abgedruckt in den Nova acta eruditorum 1764/5, p. 250. Weitere Bemerkungen sind dort nicht hinzugefügt. Siehe hierzu auch die Anmerkung p. XXVIII des Vorwortes zum vorhergehenden Bande.

auch die Abhandlungen 369, 461, 467, 498, 708a dieser Frage gewidmet und diese 6 Abhandlungen beanspruchen zusammen fast ein Viertel des ganzen Bandes. Im vorhergehenden Bande I_2 war diese Frage nur gestreift worden. Nachdem EULER dort in der kleinen Abhandlung 26 (I_2, p. 1) die Behauptung FERMATS, alle Zahlen $2^{2^m}+1$ seien Primzahlen, widerlegt hatte, hat er sich nur noch gelegentlich, nämlich in den Abhandlungen 228 und 256 (I_2, p. 295 und 459), die den Aggregaten a^2+b^2 und $2a^2+b^2$ gewidmet sind, mit der Untersuchung beschäftigt, ob eine vorgelegte Zahl prim sei oder nicht. An die Abhandlung 228 knüpft nun 283 direkt an. Zunächst zeigt EULER, daß es keine algebraische Progression

$$X = \alpha + \beta x + \gamma x^2 + \delta x^3 + \cdots$$

gibt, die nur Primzahlen darstellt,[1]) und dann beschäftigt er sich speziell mit den Zahlen der Form a^2+1. Von diesen hatte er in 228 bewiesen, daß sie keine anderen Divisoren als solche von der Form p^2+q^2 zulassen. Aus den dort gewonnenen Ergebnissen läßt sich auch leicht ermitteln, von welcher Beschaffenheit a sein muß, damit a^2+1 durch eine bestimmte Primzahl $4n+1$ oder auch durch eine Potenz davon teilbar sei. Die Tabellen, die EULER hierfür gewinnt, können aber auch umgekehrt dazu benutzt werden, für alle Zahlen a die Divisoren von a^2+1 anzugeben, wobei sich dann von selbst zugleich die Primzahlen der Form a^2+1 einstellen. Die große Tabelle, die den Schluß der Abhandlung bildet, steigt bis $a=1500$ an und liefert als größte darin enthaltene Primzahl die Zahl

$$1494^2+1 = 2232037.$$

Auch in der Abhandlung 369 *Quomodo numeri praemagni sint explorandi, utrum sint primi necne*, die nach den Akten am 19. Dezember 1765 der Petersburger Akademie vorgelegt worden ist,[2]) beschränkt sich EULER auf Zahlen der Form $4n+1$. Von diesen hatte er, im Anschluß an FERMAT und DIOPHANT, in der Abhandlung 228 bewiesen, daß sie prim sind, falls sie sich nur auf eine einzige Weise in der Form a^2+b^2 darstellen lassen. Um also eine vorgelegte Zahl $N=4n+1$ daraufhin zu prüfen, ob sie prim sei oder nicht, ist im Grunde genommen nur erforderlich, von ihr der Reihe nach alle Quadrate, die kleiner sind als sie, abzuziehen und zuzusehen, ob sich unter den auftretenden Resten nur ein einziges Quadrat befindet oder aber keines oder deren mehrere. Nun hatte zwar EULER

1) Diesen Satz hatte ihm einst CHR. GOLDBACH mitgeteilt. Siehe hierzu außer dem p. 4, Anmerkung 3, erwähnten Briefe auch noch GOLDBACHS Brief an EULER vom 18. November 1752, *Correspondance math. et phys. publiée par P. H. Fuss*, St.-Pétersbourg 1843, t. I, p. 592, insbesondere 594 (infolge eines Druckfehlers mit 595 bezeichnet); *LEONHARDI EULERI Opera omnia*, series III.

2) Das Summarium der Abhandlung 369 findet sich auch abgedruckt in den Nova acta eruditorum 1770, p. 292. Weitere Bemerkungen sind dort nicht hinzugefügt. Siehe hierzu auch die Anmerkung p. XXVIII des Vorwortes zum vorhergehenden Bande.

schon in 228 zweckmäßige Vorschriften gegeben, durch die diese Rechnungen sehr vereinfacht und abgekürzt werden können und die Subtraktionen sich sogar in Additionen verwandeln, indessen blieb bei einigermaßen großen Zahlen $4n + 1$ die Anzahl der vorzunehmenden Operationen immerhin noch sehr groß, sodaß es wünschenswert erscheinen mußte, womöglich von Anfang an diese Anzahl tunlichst zu verringern. Diesem Gedanken ist die vorliegende Abhandlung 369 gewidmet. EULER zeigt darin, daß je nach der besonderen Form der vorgelegten Zahl $N = 4n + 1$ auch immer nur Quadrate von besonderer Form zur Subtraktion zuzulassen sind. Ist z. B. N von der Form $480n + 77$, so braucht man nur die Quadrate von Zahlen der Form $240p \pm (19, 29, 61, 109)$ in Betracht zu ziehen, wodurch die Rechnung bedeutend abgekürzt wird. Auf diese Weise konnte EULER feststellen, daß

$$3861317 = 8044 \cdot 480 + 197 \quad \text{und} \quad 10091401 = 700 \cdot 14400 + 11401$$

Primzahlen sind.

Zu EULERS Zeit reichten die Faktoren- und Primzahltafeln nur wenig über 100000 hinaus.[1]) J. H. RAHN hatte seiner *Teutschen Algebra*, Zürich 1659, eine Faktorentafel für die ungeraden und durch 5 nicht teilbaren Zahlen bis 24000 hinzugefügt, in der allemal die kleinsten Divisoren angegeben sind. In der von TH. BRANCKER unter Mitwirkung von J. PELL herausgegebenen Übersetzung, London 1668, hatte PELL die RAHNSCHE Tafel unter Beibehaltung ihrer Einrichtung bis zu 100000 fortgeführt und J. WALLIS hatte in der kleinen Schrift *A discourse of combinations, alternations, and aliquot parts*, die seinem *Treatise of Algebra*, London 1685, als vierte Zugabe angehängt ist, 30 Fehler der PELLSCHEN Tafel verbessert. Sodann hatte 1746 J. G. KRÜGER in Halle seine *Gedancken von der Algebra* herausgegeben, worin sich eine bis zu 100999 reichende Primzahltafel befindet, die aber, wie KRÜGER in § 84 seines Buches mitteilt, nicht von ihm selbst, sondern von einem gewissen PETER JÄGER in Nürnberg zusammengestellt worden war. Endlich hatte J. H. LAMBERT die PELLSCHE Tafel in seine *Zusätze zu den logarithmischen und trigonometrischen Tabellen (Supplementa)*, Berlin 1770, aufgenommen, den von WALLIS gegebenen Verbesserungen noch weitere hinzugefügt und die Tafel überdies bis 102000 ausgedehnt.[2]) Aber LAMBERT hatte sich damit nicht begnügt. Der wesentlichste Unterschied seiner Tafel gegenüber der PELLSCHEN besteht darin, daß nicht nur die durch 2 und 5, sondern auch die durch 3 teilbaren Zahlen als überflüssig weggelassen sind. Dadurch aber war LAMBERT gezwungen, die alte RAHN-PELLSCHE Tafeleinrichtung zu verlassen und durch eine neue zu ersetzen, in der die Zahlen, entsprechend den Divisoren 2, 3, 5 und den Forderungen der Dezimalrechnung, nach dem

1) Siehe die Anmerkung 3 p. 104 des vorhergehenden Bandes.

2) Siehe die Einleitung zu LAMBERTS *Zusätzen*, wo auch noch weitere Litteratur mitgeteilt ist, jedoch keine von besonderer Bedeutung.

Modul 300 fortschreiten und demgemäß in drei Gruppen zerfallen, eine Einrichtung, die auch für die Zukunft maßgebend geblieben ist.[1]) Der LAMBERTSCHEN Faktorentafel folgt dann noch eine Primzahltafel bis zu 101999, deren bis 100999 reichenden Teil LAMBERT der JÄGERSCHEN Tafel entnommen hatte.

Das waren im wesentlichen die Hülfsmittel, die EULER zu Gebote standen. Ihre Unzulänglichkeit hatte er von jeher sehr empfunden. Schon gleich in der aus dem Jahre 1732 stammenden Abhandlung 26 (I_2, p. 1) findet sich eine Bemerkung darüber und in der Abhandlung 152 *De numeris amicabilibus* (I_2, p. 86) hatte EULER es in § 95 unentschieden lassen müssen, ob 129503 (weil von der Form $4n + 3$) prim sei oder nicht. So unternahm er es denn selber, die Grundlagen für eine bis zu einer Million ansteigende Faktorentafel zu schaffen und die dazu erforderlichen Rechnungen auszuführen. Am 22. August 1774 legte er seine Arbeit der Petersburger Akademie vor; es ist die Abhandlung 467 *De tabula numerorum primorum usque ad millionem et ultra continuanda, in qua simul omnium numerorum non primorum minimi divisores exprimantur.* Unter Ausscheidung der durch 2, 3, 5 teilbaren Zahlen ordnet EULER nach dem Modul 30, so daß sich jede Zahl in der Form $30q + r$ ($r = 1, 7, 11, 13, 17, 19, 23, 29$) darstellt. Die Hauptarbeit ist dann in der Lösung der folgenden acht Probleme enthalten: Nach Annahme eines Primteilers $30a \pm b$ ($b = 1, 7, 11, 13$) sollen für die einzelnen Reste r die Quoten q gefunden werden, für die die Formel $30q + r$ durch $30a \pm b$ teilbar ist. Die acht Tabellen, zu denen diese Lösungen führen, vereinigt EULER zunächst zu einer großen *Tabula auxiliaris universalis,* aus der man für jede Primzahl p von 7 bis 1009 den kleinsten Quotus q entnehmen kann, für den $30q + r$ durch p teilbar ist, und er zeigt sodann, wie man mit Hülfe dieser Tafel leicht die gewünschte Faktorentafel herstellen kann. Verschiedene zweckmäßige Anweisungen für die Drucklegung einer solchen Tafel bilden den Schluß der Abhandlung. Als Format ist Quart vorgesehen und jede Seite soll 50 Werte von q aufnehmen. Bis zu $q = 33399$ ausgedehnt würde die Tafel also 668 Seiten umfassen. Von diesen hat EULER die beiden letzten selbst hergestellt und sie als Muster folgen lassen.

Für die Benutzung einer solchen nach EULER eingerichteten Tafel hätte man also die zu untersuchende Zahl zunächst durch Division mit 30 auf die Form $30q + r$ zu bringen. Die nach den Werten von q und r geordnete Tafel würde dann allemal den kleinsten Divisor liefern. Die Notwendigkeit dieser jedesmaligen Division würde aber die Brauchbarkeit der Tafel stark beeinträchtigen und so haben sich denn die Tafeln, die in der Folgezeit ent-

1) LAMBERT hatte sich hierüber schon in dem kurz zuvor erschienenen zweiten Bande seiner *Beyträge zum Gebrauche der Mathematik und deren Anwendung*, Berlin 1770, ausführlicher ausgesprochen und als Muster eine bis 10200 reichende Faktorentafel beigefügt. Auch hatte er schon damals die Wünschbarkeit einer Ausdehnung bis zu einer Million betont.

standen sind, unter Benutzung des Moduls 300 im wesentlichen an die von LAMBERT gewählte Einrichtung angeschlossen. Die von EULER gegebene kräftige Anregung hat aber darum doch ihre Früchte gezeitigt und so sei es daher gestattet, das wichtigste darüber noch kurz anzuschließen.

Schon 1776 erschien in Wien der erste bis 144000 reichende Teil des groß angelegten Werkes von A. FELKEL, das eine Faktorentafel bis 10000000 zu liefern versprach. Dieses Werk, von dem der zweite Teil bis 336000 reichte und das mit dem dritten, bis 408000 ansteigenden Teile[1]) sein Ende fand (FELKEL hatte zwar das Manuskript bereits bis 2016000 fertiggestellt[2])), ist indessen mehr unter dem Einfluß LAMBERTS als unter dem EULERS ins Leben gerufen worden, obwohl auch dieser im Vorworte erwähnt wird. Im Jahre 1811 erschien in Deventer die bis zu einer Million ansteigende Tafel von L. CHERNAC, die aber schon nach kurzer Zeit durch die bis 3035999 reichende Tafel von J.-CH. BURCKHARDT[3]), Paris 1814—1817, überholt wurde. Nach langer Pause folgte dann, Hamburg 1862—1865, die Faktorentafel des Rechenkünstlers Z. DASE, den GAUSS zu dieser Arbeit veranlaßt hatte. Die Tafel umfaßt die Zahlen 6000001—9000000 und enthält im Vorworte einen Brief von GAUSS an DASE vom 7. Dezember 1850 mit wertvollen historischen Mitteilungen.[4]) Die Lücke zwischen BURCKHARDT und DASE wurde in den Jahren 1879—1883 durch J. GLAISHER ausgefüllt, der in drei in London veröffentlichten Bänden die Faktorentafeln für die Zahlen 3000000—6000000 lieferte.

Endlich ist in unseren Tagen, Washington 1909, die große Tafel von D. N. LEHMER[5]) erschienen, die in einem einzigen Bande für alle nicht durch 2, 3, 5 oder 7 teilbaren Zahlen bis 10017000 den kleinsten Divisor angibt. Der Umstand, daß auch die durch 7 teilbaren Zahlen ausgeschlossen sind, hat natürlich wieder eine andere Einrichtung der Tafel erfordert, als sie den früheren zugrunde lag. LEHMER ist zunächst zu der EULERSCHEN Einrichtung zurückgekehrt, indem er alle Zahlen, entsprechend den Divisoren 2, 3, 5, 7, auf die Form $210q + r$ bringt und die Tafel, wie EULER, nach den Werten von q und r ordnet, wobei r

1) Siehe J. H. LAMBERT, *Supplementa tabularum logarithmicarum et trigonometricarum*, curante A. FELKEL, Olisipone 1798, p. VII. Der zweite und dritte Teil der FELKELSCHEN Tafel sind äußerst selten, da 1788 bei Anlaß des Türkenkrieges fast die ganze Auflage vernichtet und zu Patronenpapier verwendet wurde.

2) Im Jahre 1785 hatte FELKEL sogar zum zweiten Male eine Faktorentafel berechnet, die bis 2856000 reichte. Siehe die in der vorhergehenden Anmerkung erwähnte FELKELSCHE Ausgabe von LAMBERTS *Supplementa*, p. VII.

3) Siehe die Anmerkung p. 398.

4) Die Angabe von GAUSS, die Tafel von LAMBERT sei nur ein Abdruck der PELLSCHEN, bedarf aber, wie wir gesehen haben, der Berichtigung.

alle durch 2, 3, 5, 7 nicht teilbaren Zahlen durchläuft, die kleiner sind als 210. Um aber die lästige Division mit 210 zu ersparen, ist dann noch eine besondere Hülfstafel beigefügt, die das direkte Aufschlagen ermöglicht. Die LEHMERSCHE Tafel scheint sehr korrekt zu sein; sie enthält überdies Zusammenstellungen von zahlreichen Verbesserungen zu den früheren Tafeln, insbesondere zu denen von BURCKHARDT und DASE (die GLAISHERSCHEN Tafeln enthalten verhältnismäßig wenig Fehler). In der Einleitung gibt LEHMER eine Übersicht über die geschichtliche Entwickelung der Faktorentafeln, die im wesentlichen der Einleitung zum ersten Bande der GLAISHERSCHEN Tafeln entnommen ist.[1])

Schließlich sei noch erwähnt, daß LEHMER, Washington 1914, seiner Faktorentafel auch noch eine Primzahltafel hat folgen lassen unter dem Titel *List of prime numbers from 1 to 10006721.*

Doch kehren wir nach dieser Abschweifung zu EULER und zu unserem Bande I$_3$ zurück. Wie schon bemerkt, enthält dieser noch drei Nummern, nämlich 461, 498 und 708a, die sich speziell auf Primzahlen beziehen. Sie sind in Briefform gehalten, in französischer Sprache geschrieben und in den Berliner Memoiren veröffentlicht. Der erste Brief, 461, aus dem Jahre 1772, gedruckt 1774, ist an JOHANN III BERNOULLI[2]) gerichtet und knüpft an eine Abhandlung an, die dieser ein Jahr zuvor ebenfalls in den Berliner Memoiren veröffentlicht hatte. Es handelt sich in dem Briefe zunächst um Kriterien für die Teilbarkeit der Zahlen von der Form $10^p \pm 1$ durch die Primzahl $2p+1$, d. h. um die Ermittelung der Primzahlen $2p+1$, für welche die Zahl 10 quadratischer Rest ist. Daran schließen sich zwei weitere Mitteilungen, von denen die eine auf Grund eines Satzes von FERMAT den Beweis enthält, daß $2^{31}-1 = 2147483647$ eine Primzahl ist. Den Beweis hatte EULER lange vergeblich gesucht. So schrieb er am 16. Dezember 1752 an CHR. GOLDBACH: „Der folgende [Ausdruck, der eine vollkommene Zahl liefern könnte,] wäre $2^{30}(2^{31}-1)$, wenn nur $2^{31}-1$ ein numerus primus wäre, welches aber weder behauptet noch untersucht werden kann. So viel ist gewiß, daß diese Zahl $2^{31}-1$ keine andere divisores haben kann, als welche in

1) In dieser Übersicht bespricht LEHMER auch das Riesenwerk von J. PH. KULIK, eine Faktorentafel bis 100000000, von der die Handschrift seit 1867 bei der Wiener Akademie liegt. Weitere Litteratur über die Geschichte der Faktorentafeln findet man in der *Encyclopédie d. sc. mathém.*, t. I, vol. 4, p. 224—226, insbesondere in den Zusätzen und Anmerkungen G. ENESTRÖMS.

2) JOHANN III BERNOULLI (1744—1807), Enkel von JOHANN I, war seit 1764, also seit seinem zwanzigsten Jahre, Mitglied der Berliner Akademie und später Direktor ihrer mathematischen Klasse. Im Jahre 1767 wurde er als königlicher Astronom mit der Leitung der Berliner Sternwarte betraut. Mit EULER stand er schon zu dessen Berliner Zeit in freundschaftlicher Beziehung, die er 1778 bei seinem Besuche in Petersburg erneuerte. Er veranstaltete von EULERS *Algebra* die bekannte französische Übersetzung, die mit den Zusätzen von LAGRANGE 1774 in Lyon in zwei Bänden erschien. Siehe *LEONHARDI EULERI Opera omnia*, series I, vol. 1.

dieser Formul $62n + 1$ enthalten sind, woraus ich so viel gefunden, daß kein divisor unter 2000 Statt findet" (*Correspondance math. et phys. publiée par P. H. Fuss*, St.-Pétersbourg 1843, t. I, p. 595; *Leonhardi Euleri Opera omnia*, series III).

Die andere Mitteilung bezieht sich auf die quadratische Form

$$41 - x + x^2,$$

die die Eigenschaft hat, für $x = 1, 2, 3, \ldots 40$ stets Primzahlen darzustellen. Auf Formen solcher Art, in denen viele Primzahlen enthalten sind, war Euler schon früh durch Chr. Goldbach aufmerksam gemacht worden. In dem p. 4, Anmerkung 3, erwähnten Briefe vom 28. September 1743 hatte ihm dieser geschrieben: „Ob es zwar sehr leicht ist zu demonstriren, daß eine formula algebraica huiusmodi $a + bx + cxx + dx^3 +$ etc. [nicht] lauter numeros primos geben kann, . . ., so gibt es doch formulas, welche vor vielen andern eine Menge numerorum primorum in sich halten; dergleichen ist die series $xx + 19x - 19$, so in den ersten 47 terminis nur vier numeros non primos hat [nämlich für $x = 19, 25, 36, 38$]". In seiner Antwort vom 15. Oktober 1743 fand Euler dies in der Tat sehr merkwürdig, fügte aber hinzu: „Inzwischen finden sich doch die numeri compositi um so viel häufiger ein, je weiter man die seriem continuirt" (*Correspondance math. et phys. publiée par P. H. Fuss*, St.-Pétersbourg 1843, t. I, p. 255 und 258; *Leonhardi Euleri Opera omnia*, series III).

Der zweite Brief, 498, den Euler im Mai 1778 an den Berliner Akademiker Nicolas de Beguelin im Anschluß an eine von diesem in den Berliner Memoiren veröffentlichte Abhandlung über Primzahlen gerichtet hat, ist besonders beachtenswert, weil Euler darin zum ersten Male von den merkwürdigen Zahlen spricht, die er *nombres convenables* oder *numeri idonei* nennt. Euler hatte in der Abhandlung 228 bewiesen, daß alle Zahlen, die sich nur auf eine einzige Weise in der Form $x^2 + y^2$ darstellen lassen, Primzahlen oder das Doppelte davon sein müssen. Nun fand er, daß es Zahlen n gibt, für welche die Form $nx^2 + y^2$ dieselbe Eigenschaft besitzt. Solcher Zahlen, für die er ein einfaches Kennzeichen mitteilt, hat er 65 gefunden; die größte ist 1848, und es ist bisher nicht gelungen, weitere numeri idonei ausfindig zu machen. Euler teilt noch eine Reihe großer Primzahlen mit, die er mit Hülfe der Form $1848x^2 + y^2$ gefunden hat, darunter 18518809. Den Beweis hat er später in der Abhandlung 719 (I4) gegeben, die erst nach seinem Tode erschienen ist.

Es ist begreiflich, daß Beguelin nach diesem Briefe Verlangen trug, genaueres über diese nombres convenables zu erfahren und die Prinzipien kennen zu lernen, die zu ihnen führen. So beauftragte denn Euler seinen Gehülfen Nicolaus Fuss, der seit 1773 sein Sekretär oder besser gesagt seine rechte Hand war, für Beguelin einen Auszug aus den Abhandlungen anzufertigen, die er über diesen Gegenstand verfaßt hatte. Dieses Auftrages entledigte sich Fuss am $\frac{19}{30}$ Juni 1778. Der Umstand, daß dieser Brief, 708a, nicht nur

durch EULER veranlaßt worden war, sondern daß er auch dem Inhalte nach ganz und gar EULER angehört, hat das Redaktionskomitee bestimmt, ihn in die Eulerausgabe aufzunehmen und ihm auch die Stelle anzuweisen, die durch das Datum des Druckes vorgeschrieben ist.[1]) Die Abhandlung 708 selbst und die damit zusammenhängenden Abhandlungen 715, 718, 719, 725, die EULER alle im März und April 1778 der Petersburger Akademie vorgelegt hatte, die aber erst in den Jahren 1801—1806 gedruckt wurden, werden im nächsten Bande unserer Ausgabe erscheinen.

Wie schon bemerkt,[2]) befinden sich in unserem Bande I_3 außer 708a noch zwei weitere Abhandlungen, die nicht von LEONHARD EULER herrühren. Es sind die Abhandlungen A_9 und A_{31} JOHANN ALBRECHT EULERS. Die Abhandlung A_{31} wird im Zusammenhange mit 523 zu besprechen sein, hier mögen einige Bemerkungen zu A_9 *Beantwortung einiger arithmetischen Fragen* Platz finden. Die Arbeit ist 1764 in den Abhandlungen der Churfürstlich-baierischen Akademie der Wissenschaften erschienen, deren auswärtiges Mitglied J. A. EULER 1762 geworden war.[3]) Sie ist höchst wahrscheinlich identisch mit der Abhandlung, die J. A. EULER nach C. G. J. JACOBI[4]) am 30. Juni 1763 in der Berliner Akademie, in die er schon 1754, also mit 20 Jahren, als ordentliches Mitglied aufgenommen worden war, gelesen hat. Die Abhandlung A_9 enthält die Lösung von vier arithmetischen Aufgaben, die sich auf die Abzählung von Ziffern beziehen, und hat einen ganz elementaren Charakter, wie schon aus der ersten Aufgabe hervorgeht: „Wenn von einer Billion die Zahl hundert nach der gemeinen Weise der Subtraktion und zu widerholtenmalen so oft abgezogen wird, bis nichts (0) übrig bleibt, wieviel Ziffern zu schreiben hierzu erfordert werden?“

Wir gelangen nun zu der Abhandlung 323 *De usu novi algorithmi in problemate Pelliano solvendo*, die EULER nach den Akten schon am 15. Oktober 1759 und dann noch einmal am 23. Mai 1763 der Petersburger Akademie vorgelegt hatte. Sie ist aber erst 1767 herausgegeben[5]) worden. Es handelt sich darin um die Auflösung der FERMATSCHEN Gleichung

$$lq^2 + 1 = p^2,$$

von der schon im vorhergehenden Bande[6]) gesagt worden war, daß sie von EULER nur

1) Siehe p. VII. 2) Siehe p. VII.

3) Siehe die in der Anmerkung 1 p. VIII erwähnte Biographie J. A. EULERS von P. STÄCKEL.

4) Siehe P. STÄCKEL und W. AHRENS, *Der Briefwechsel zwischen C. G. J. JACOBI und P. H. VON FUSS über die Herausgabe der Werke LEONHARD EULERS*, Leipzig 1908, p. 38.

5) Genaueres über die eigentümliche Geschichte des Druckes dieser Abhandlung 323 (die erste Auflage von 1763 wurde makuliert) findet man in ENESTRÖMS *Verzeichnis*, p. 214.

6) Siehe daselbst die Anmerkungen p. 11 und 12.

irrtümlicher Weise mit dem Namen PELL, mit dem sie auch nicht das geringste zu tun hat, in Verbindung gebracht worden ist. Man darf wohl hoffen, daß die sinnlose Bezeichnung *PELLSCHE Gleichung* endlich einmal aus der mathematischen Litteratur verschwinde.

Es ist bekannt, daß die in der FERMATSCHEN Gleichung enthaltene Aufgabe nicht nur zu den wichtigsten, sondern auch zu den ältesten Problemen der ganzen Zahlentheorie gehört; reichen doch die Anfänge bis auf die alten Griechen zurück. Und so existiert denn auch eine sehr ausgedehnte Litteratur[1]) über diesen Gegenstand.

In der Abhandlung 323 bespricht EULER zunächst die Bedeutung der Gleichung $lq^2 + 1 = p^2$ für die Auflösung der allgemeineren Gleichung

$$lx^2 + mx + n = y^2$$

und der noch allgemeineren

$$Ax^2 + 2Bxy + Cy^2 + 2Dx + 2Ey + F = 0$$

und wendet sich dann zu der Auflösung von $lq^2 + 1 = p^2$ selbst. Den Ausgangspunkt hierfür bildet die Bemerkung, daß $\frac{p}{q}$ ein Näherungswert von $\sqrt{l}$ sein müsse. Um solche Näherungswerte zu gewinnen, benutzt EULER die Kettenbruchentwickelung von $\sqrt{l}$, die er erst an Beispielen und dann allgemein beschreibt. Er setzt

$$\sqrt{z} = v + \cfrac{1}{a + \cfrac{1}{b + \cfrac{1}{c + \text{etc.}}}}$$

und knüpft daran eine einfache Rechnungsvorschrift für die Bildung der von ihm als *Indizes* bezeichneten Zahlen

$$v,\ a,\ b,\ c\ \ldots$$

aus zwei rekurrierenden Zahlenreihen

$$A,\ B,\ C,\ \ldots$$

und

$$\alpha,\ \beta,\ \gamma,\ \ldots$$

Hierauf folgt eine Tafel, enthaltend die Kettenbruchentwickelungen aller quadratischen Irrationalitäten von $\sqrt{2}$ bis $\sqrt{120}$, dargestellt allemal durch die Indizes $v, a, b, c, \ldots$, denen die zugehörigen Zahlen $1, \alpha, \beta, \gamma, \ldots$ untergeschrieben sind. Alle diese Entwickelungen zeigen periodisches Verhalten, insofern dieselben Indizes in derselben Reihenfolge wiederkehren, sobald man zum Index $2v$ gekommen ist. Außerdem besteht innerhalb einer Periode Symmetrie, so daß jede Periode ein Mittelglied oder deren zwei aufweist. Einen allgemeinen Beweis für dieses periodische Verhalten, insbesondere also dafür, daß in

1) Siehe H. KONEN, *Geschichte der Gleichung* $t^2 - Du^2 = 1$, Leipzig 1901; vgl. auch G. WERTHEIMS Besprechung dieses Buches, Biblioth. Mathem. 3_3, 1902, p. 248.

jedem Falle der Index $2v$ wirklich auftreten müsse, gibt EULER nicht, dagegen fügt er seiner Tafel noch einige zusammenfassende Fälle hinzu, in denen er für besondere Formen von z, wie z. B. $z = n^2 + n$, die Werte der Indizes und der zugehörigen $\alpha, \beta, \gamma, \ldots$ allgemein angibt.

Aus den Indizes $v, a, b, c, \ldots$ von $\sqrt{z}$ hat man nach bekannten Vorschriften die Reihe der Näherungsbrüche $\frac{x}{y}$ zu bilden. Dabei bedient sich EULER des in der Überschrift erwähnten abkürzenden Algorithmus, den er in der Abhandlung 281 *Specimen algorithmi singularis* (I_{14}) auseinandergesetzt hatte. Für die Näherungsbrüche ergibt sich nun, daß $x^2 - zy^2$ der Reihe nach die Werte

$$+1, \; -\alpha, \; +\beta, \; -\gamma, \; +\delta, \ldots$$

durchläuft. Sobald also in der Reihe der Zahlen $\alpha, \beta, \gamma, \ldots$ die Einheit auftritt, hat man eine Lösung der Gleichung

$$x^2 - zy^2 = \pm 1.$$

Die Einheit tritt aber allemal auf, sobald der zugehörige Index gleich $2v$ geworden ist. Man hat also x und y aus den Indizes der ersten Periode zu bestimmen. Ist dann $x^2 - zy^2 = +1$, so hat man in $p = x$ und $q = y$ sofort eine Lösung der FERMATSCHEN Gleichung; ist aber $x^2 - zy^2 = -1$, so muß man entweder bis zum Anfange der dritten Periode fortschreiten oder aber $p = 2x^2 + 1$ und $q = 2xy$ setzen. Zur näheren Erläuterung schließt EULER noch die Besprechung von acht besonderen Fällen an, die sich auf die einfachsten Zusammensetzungen einer Periode von $\sqrt{z}$ beziehen. Er zeigt überdies, daß auf Grund gewisser Transformationsformeln, die sich aus dem neuen Algorithmus jener Abhandlung 281 ergeben, die Rechnung insofern auf die Hälfte reduziert werden kann, als man bei der Bildung der Näherungsbrüche die Indizes der ersten Periode immer nur um ein Glied über die Mitte hinaus zu verfolgen braucht. Zahlenbeispiele und eine Tafel der kleinsten Zahlen p, q, für welche $lq^2 + 1 = p^2$ ist, für alle Zahlen l bis 100 und außerdem noch für $l = 103, 109, 113, 157, 367$ bilden den Schluß der Abhandlung. Die Tafel bis $l = 100$ ist auch in EULERS Algebra (I_1, p. 387) abgedruckt; bis $l = 68$ hatte sie EULER schon in der Abhandlung 29 (I_{2_1}, p. 14) mitgeteilt.

Einen strengen Beweis dafür, daß die FERMATSCHE Gleichung $lq^2 + 1 = p^2$, abgesehen von der selbstverständlichen Lösung $p = 1$, $q = 0$, immer wirklich lösbar sei, enthält die Abhandlung 323 nicht.[1]) Den hat erst, 1768, LAGRANGE gegeben. Dagegen gebührt EULER das Verdienst, nicht nur „die tiefe Bedeutung der PELLSCHEN Gleichung für die allgemeine

1) Siehe hierzu p. 56 des Buches von H. KONEN und sodann insbesondere Art. 202 der *Disquisitiones arithmeticae* von C. F. GAUSS, sowie § 83 der vierten Auflage der von R. DEDEKIND herausgegebenen *Vorlesungen über Zahlentheorie von P. G. LEJEUNE DIRICHLET.*

Auflösung der unbestimmten Gleichungen zweiten Grades zuerst dargetan zu haben" (DEDEKIND), sondern auch alles vorbereitet und sorgfältig entwickelt zu haben, was in jedem einzelnen Falle zur wirklichen Lösung erforderlich ist. Man kann also wohl sagen, EULER habe einen Beweis für die Auflösbarkeit der FERMATSCHEN Gleichung nicht gegeben, — aber er hat die Auflösung selbst gegeben.

Auf die Auflösung der unbestimmten Gleichungen zweiten Grades beziehen sich auch die Abhandlungen 452 und 454 unseres Bandes, die daher gleich hier kurz besprochen werden sollen. Die Abhandlung 452 *Resolutio aequationis*

$$Ax^2 + 2Bxy + Cy^2 + 2Dx + 2Ey + F = 0$$

per numeros tam rationales quam integros, die EULER am 19. November 1772 der Petersburger Akademie vorgelegt hat, schließt nach Inhalt und Methode an die Abhandlungen 29 und 279 des vorhergehenden Bandes an (I_2, p. 6 und 576). Hier wie dort setzt EULER voraus, daß eine Lösung $x = a$, $y = b$ bereits bekannt sei, um aus dieser dann beliebig viele neue herzuleiten. Hierfür gibt er zwei Methoden an. Das Resultat der zweiten, das unter Benutzung der FERMATSCHEN Gleichung gewonnen wird, hatte EULER ohne Beweis schon in der soeben besprochenen Abhandlung 323 mitgeteilt.

Als EULER die Abhandlung 452 niederschrieb, hatte er keine Kenntnis davon, daß die vollständige Lösung der allgemeinen Gleichung zweiten Grades schon mehrere Jahre zuvor, 1767 und 1768, von LAGRANGE gegeben worden war.[1])

Wenige Tage, nachdem EULER die Abhandlung 452 der Petersburger Akademie vorgelegt hatte, übergab er ihr, am 3. Dezember 1772, die damit zusammenhängende Abhandlung 454 *De resolutione irrationalium per fractiones continuas, ubi simul nova quaedam et singularis species minimi exponitur.* Bei der Auflösung der allgemeinen Gleichung zweiten Grades war er zu der Aufgabe geführt worden, für x und y solche ganzzahligen Werte zu finden, für welche die Formel $Ax^2 + 2Bxy + Cy^2$ ein Minimum wird. Der Lösung dieser Aufgabe ist die Abhandlung 454 gewidmet. EULER behandelt zunächst die Form $mx^2 - ny^2$, die ein Minimum wird, wenn $\frac{x}{y}$ möglichst nahe an $\frac{\sqrt{mn}}{m}$ herankommt. Dies führt wieder, wie bei der Auflösung der FERMATSCHEN Gleichung, zur Kettenbruchentwickelung von $\frac{\sqrt{mn}}{m}$, aus der sich dann die gesuchten Werte von x und y ergeben. Vorher hatte EULER noch gezeigt, daß, wenn man einen Fall kennt, für den $mx^2 - ny^2$ gleich einer gegebenen Zahl ist, man mit Hülfe der FERMATSCHEN Gleichung sofort unendlich viele Werte für x und y finden kann, die zu derselben Zahl führen. Der Beweis ist der zweiten Methode der vorher-

1) Vergl. Art. 222 der *Disquisitiones arithmeticae* von C. F. GAUSS. Siehe aber auch den p. XX, Anmerkung 2, erwähnten Brief EULERS an LAGRANGE vom $\frac{9}{20}$ März 1770, von dem ein Auszug p. XXX mitgeteilt ist.

gehenden Abhandlung 452 nachgebildet. Ganz ähnlich zeigt EULER sodann, wie man x und y zu bestimmen habe, damit die Form $Ax^2 - 2Bxy + Cy^2$ ein Minimum werde, unter der Voraussetzung, daß $B^2 - AC$ eine positive nicht quadratische Zahl ist. Setzt man diese gleich k, so führt jetzt die Kettenbruchentwickelung von $\frac{B \pm \sqrt{k}}{A}$ zu der gewünschten Lösung, aus der man dann wieder, ähnlich wie bei der Form $mx^2 - ny^2$, unendlich viele andere gewinnen kann. Für beide Formen werden verschiedene erläuternde Zahlenbeispiele entwickelt.

Im vorhergehenden Bande I_2 sind zwei Abhandlungen über die *Partitio numerorum* enthalten, durch die diese Lehre eigentlich erst begründet worden ist. Es sind die Abhandlungen 158 *Observationes analyticae variae de combinationibus* (I_2, p. 163) und 191 *De partitione numerorum* (I_2, p. 254), von denen EULER die erste 1741, die zweite 1750[1]) der Petersburger Akademie vorgelegt hatte. Dazwischen hatte er 1748 seine *Introductio in analysin infinitorum* herausgegeben, deren 16. Kapitel ebenfalls der *Partitio numerorum* gewidmet ist. An diese Arbeiten knüpft im vorliegenden Bande I_3 die Abhandlung 394 *De partitione numerorum in partes tam numero quam specie datas* an, die nach den Akten am 18. August 1768 der Petersburger Akademie eingereicht worden ist. Schon in der *Introductio* und dann auch in der Abhandlung 191 hatte EULER Aufgaben behandelt, bei denen von den Summanden, in die eine gegebene Zahl zerlegt werden soll, eine besondere Beschaffenheit verlangt wird, z. B. ungerade zu sein oder der geometrischen Reihe 1, 2, 4, 8, 16 etc. anzugehören. Aufgaben der letzteren Art hatte EULER bereits bei M. STIFEL und FR. v. SCHOOTEN vorgefunden, aber auch schon LEONARDO PISANO hatte sich damit beschäftigt und war zu bemerkenswerten Ergebnissen gelangt.[2]) In der Abhandlung 394 löst nun EULER zunächst die Aufgabe anzugeben, auf wieviele Arten eine Zahl N mit n gewöhnlichen Würfeln geworfen werden kann. Er bezeichnet diese Anzahl mit $(N)^{(n)}$ und zeigt, daß die Zahlen $(N)^{(n)}$ durch die Entwickelungskoeffizienten des Ausdrucks

$$(x + x^2 + x^3 + x^4 + x^5 + x^6)^n$$

geliefert werden. Für diese Koeffizienten leitet EULER zunächst einfache Rekursionsformeln ab und stellt sodann die Zahlen $(N)^{(n)}$ auch in independenter Form dar. Nun wird die Aufgabe verallgemeinert. Statt gewöhnlicher Würfel von sechs Seiten werden solche von m Seiten, die mit den Zahlen 1, 2, 3, ... m bezeichnet sind, vorausgesetzt. Dabei kann die Zahl m für alle Würfel dieselbe sein, sie kann aber auch von Würfel zu Würfel wechseln. Hat man z. B. drei Würfel, von denen der erste sechs, der zweite acht, der dritte

1) Siehe indessen hierüber die Anmerkung p. XIX des Vorwortes zum vorhergehenden Bande.

2) Siehe die Anmerkungen 1—3 p. 258 des vorhergehenden Bandes, insbesondere die dort erwähnte Notiz von G. ENESTRÖM.

zwölf Seiten hat, und fragt man, auf wieviele Arten mit diesen drei Würfeln die Zahl N geworfen werden kann, so hat man nur das Produkt

$$(x + x^2 + x^3 + \cdots + x^6)(x + x^2 + x^3 + \cdots + x^8)(x + x^2 + x^3 + \cdots + x^{12})$$

zu entwickeln und der Koeffizient von x^N wird die Zahl der Fälle angeben.

Zum Schlusse bringt EULER die *Partitio numerorum* mit dem von FERMAT ohne Beweis ausgesprochenen Satze in Verbindung, wonach jede Zahl als Summe von drei Trigonalzahlen, als Summe von vier Quadratzahlen, als Summe von fünf Pentagonalzahlen usw. dargestellt werden kann. Er gibt analytische Ausdrücke, aus deren Entwickelung der Beweis hervorgehen würde, muß sich aber mit Andeutungen begnügen. Der Beweis selbst ist für die Quadratzahlen erst von LAGRANGE, für die Trigonalzahlen von GAUSS und allgemein für beliebige Polygonalzahlen von CAUCHY geleistet worden. Daß sich jede Zahl als Summe von vier Quadratzahlen darstellen läßt, ein Satz, der übrigens schon vor FERMAT von BACHET ausgesprochen worden war, hat EULER dann aber auch noch selbst bewiesen, und zwar in der Abhandlung 445 des vorliegenden Bandes; allerdings nicht auf dem Wege, den er am Schlusse von 394 angedeutet hatte.

Unser Band I$_3$ enthält neun Abhandlungen, die sich mit DIOPHANTISCHEN Aufgaben im engeren Sinne beschäftigen. Sie tragen im ENESTRÖMSCHEN Verzeichnis die Nummern 405, 427, 428, 451, 466, 474, 515, 523, A$_{31}$ und nehmen zusammen fast ein Drittel des ganzen Bandes ein. Die Abhandlung 405 *Solutio problematis, quo duo quaeruntur numeri, quorum productum tam summa quam differentia eorum sive auctum sive minutum fiat quadratum*, hatte EULER nach den Akten am 5. März 1770 der Petersburger Akademie eingereicht. Die Aufgabe, die in einfacherer Form schon bei DIOPHANT vorkommt,[1]) war ihm noch in Berlin von einem preußischen Offizier[2]) gestellt worden und hatte durch ihre Eleganz sofort sein lebhaftes Interesse erregt. Nach einigen Versuchen fand er, daß

$$A = \frac{13 \cdot 29^2}{8 \cdot 9^2} = \frac{10933}{648}, \quad B = \frac{5 \cdot 29^2}{32 \cdot 11^2} = \frac{4205}{3872}$$

eine Lösung[3]) sei, allerdings auf einem Wege, der ihm nicht erlaubt hätte, weitere Lösungen

1) Vergleiche damit die Aufgabe, die in der Abhandlung 466 behandelt wird

2) Hauptmann v. KAPPE. Dieser hatte die Aufgabe von einem Freunde in Leipzig erhalten, dem es trotz langem und eifrigem Bemühen nicht gelungen war, eine Lösung zu finden. Siehe EULERS Brief an LAGRANGE vom $\frac{9}{20}$ März 1770, *LEONHARDI EULERI Opera postuma*, t. I, p. 574; *Oeuvres de LAGRANGE*, t. XIV, p. 219; *LEONHARDI EULERI Opera omnia*, series III. Der Brief gibt in gekürzter Form den wesentlichsten Inhalt der Abhandlung 405 wieder.

3) Diese Lösung mit einer kurzen Andeutung des Weges, der zu ihr führt — EULER gibt für die gesuchten Zahlen die Formen $\frac{(p^2+q^2)(r^2+s^2)}{2pq(r^2-s^2)}$ und $\frac{(p^2+q^2)(r^2+s^2)}{2rs(p^2-q^2)}$ —, findet sich auch in einem Briefe EULERS an LAGRANGE vom $\frac{16}{27}$ Januar 1770, *LEONHARDI EULERI Opera postuma*, t. I, p. 571; *Oeuvres de LAGRANGE*, t. XIV, p. 214; *LEONHARDI EULERI Opera omnia*, series III.

zu ermitteln, obwohl er nicht daran zweifelte, daß es deren unendlich viele gäbe. Erst später wurde er durch einen Zufall, wie er selbst sagt, auf den richtigen Weg geführt. Er setzte $A = \frac{z}{x}$ und $B = \frac{z}{y}$, so daß also die vier Ausdrücke

$$\frac{z}{xy}(z \pm y \pm x)$$

zu Quadraten zu machen waren. Für die vier Faktoren $z \pm y \pm x$ war dies durch eine einfache Transformation leicht zu bewerkstelligen, größere Mühe aber verursachte es, dann auch $\frac{z}{xy}$ zu einem Quadrate zu machen. Durch geeignete Substitutionen, die darauf abzielten, für die im Nenner von $\frac{z}{xy}$ nach jener Transformation auftretenden Faktoren gemeinsame Divisoren zu gewinnen und dadurch den Bruch für den vorliegenden Zweck zu vereinfachen, gelang schließlich auch dieses. Es kam zuletzt nur noch darauf an, den Ausdruck

$$16m^4 - 44m^3l + 58m^2l^2 - 28ml^3 + 4l^4$$

zu einem Quadrate zu machen, eine Aufgabe, die nach den Methoden von EULERS *Algebra* leicht zu lösen war. Zum Schlusse fügte EULER noch andere Substitutionen hinzu, die sich besonders für die numerische Berechnung eignen.

In der großen Abhandlung 427 *Problematis cuiusdam DIOPHANTEI evolutio*, die nach den Akten am 13. Januar 1772 der Petersburger Akademie vorgelegt worden ist, behandelt EULER zunächst die Aufgabe, vier Zahlen zu finden, für die sich die Summe, die Summe der Produkte zu zweien, die Summe der Produkte zu dreien und das Produkt von allen vieren als Quadrate darstellen. Die entsprechende Aufgabe für nur drei Zahlen, für welche die elementaren symmetrischen Funktionen zu Quadraten werden sollen, hatte EULER in der Abhandlung 270 des vorhergehenden Bandes (I_2, p. 519) behandelt und war dabei auf nicht unbeträchtliche Schwierigkeiten gestoßen. Ähnlich wie dort setzt daher EULER auch hier für die gesuchten Zahlen gleich von Anfang an besondere Formen voraus, nämlich

$$Mab,\ Mbc,\ Mcd,\ Mda,$$

wodurch die vierte Bedingung von selbst erfüllt wird und die dritte sich darauf zurückführen läßt, daß $abcd$ ein Quadrat werden muß. Da es sich um allgemeine Lösungen überhaupt nicht handeln kann, so wird auch noch mit Rücksicht auf die erste Bedingung

$$M = \frac{ab + bc + cd + da}{f^2}$$

gesetzt, so daß jetzt nur noch zwei Bedingungen übrig bleiben, wobei es sich bloß um die Verhältnisse von a und c einerseits und b und d andererseits handelt. Hieran schließt sich die Herleitung spezieller Lösungen.

In derselben Abhandlung 427 werden noch zwei andere DIOPHANTISCHE Probleme behandelt, nämlich: *Es sollen beliebig viele Zahlen gefunden werden, von denen jede mit der*

Summe der übrigen multipliziert ein Quadrat erzeugt, und *Es sollen beliebig viele Quadratzahlen gefunden werden, so daß die Summe aller vermindert um irgend eine von ihnen jedesmal ein Quadrat sei.* Auch hierfür werden nur spezielle Lösungen abgeleitet.

Mit der Abhandlung 427 hängen enge zusammen die schon erwähnten Abhandlungen 523 und A 31. Die Abhandlung 523 *De tribus numeris quadratis, quorum tam summa quam summa productorum ex binis sit quadratum*, ist nach den Akten am 7. September 1780 der Petersburger Akademie vorgelegt worden. Die darin behandelte Aufgabe kann insofern als Spezialfall des in der Abhandlung 270 des vorhergehenden Bandes enthaltenen Problems betrachtet werden, als nunmehr von den Zahlen, deren elementare symmetrische Funktionen Quadrate werden sollen, gefordert wird, daß sie selber Quadrate seien. Dadurch aber wird die Zahl der Bedingungen von drei auf zwei zurückgeführt. EULER setzt

$$x = p^2 + q^2 - r^2, \quad y = 2pr, \quad z = 2qr,$$

wodurch der ersten Bedingung Genüge geleistet wird. Um auch die zweite zu befriedigen, setzt er $r = p - nq$ und wird dadurch zu einem biquadratischen Ausdrucke geführt, den er auf doppelte Weise zu einem Quadrate machen kann. Die kleinsten Quadratzahlen, die er schließlich findet, nämlich

$$x^2 = 784, \quad y^2 = 186624, \quad z^2 = 81,$$

sind aber immer noch beträchtlich größer als die in dem Summarium der Abhandlung 270 mitgeteilten Lösungen.[1])

Unmittelbar an diese Abhandlung schließt sich in den Acta der Petersburger Akademie eine Abhandlung von JOHANN ALBRECHT EULER[2]) an *Ad dissertationem patris de tribus numeris, quorum tam summa quam summa productorum ex binis sit quadratum, commentatio.* Sie ist in ENESTRÖMS Verzeichnis mit A 31 bezeichnet und nach den Akten am 5. Oktober 1780, also vier Wochen nach der Abhandlung des Vaters, der Petersburger Akademie vorgelegt worden. Der Verfasser geht zunächst von einer ganz speziellen Lösungsform aus, indem er die gesuchten Zahlen durch

$$5(p^2 - 1), \quad 8p, \quad 6p$$

ausdrückt, deren Quadrate die Summe $25(p^2 + 1)^2$ ergeben und die daher der ersten Bedingung genügen. Die zweite Bedingung führt ihn zu einem einfachen biquadratischen Ausdrucke, der ein Quadrat werden muß. Sehr bald erhält er hieraus die Lösung

$$35, \quad 96, \quad 72,$$

1) Siehe auch die Besprechung der Abhandlung 270 p. XXVIII des Vorwortes zum vorhergehenden Bande, insbesondere die dazu gehörige Anmerkung.

2) Siehe p. VII.

die beträchtlich einfacher ist als die von dem Vater gefundene Lösung 9, 28, 432. Zu einer Verallgemeinerung gelangt er durch die Bemerkung, daß auch die Summe der Quadrate von

$$(q^2-1)(p^2+1), \quad 2q(p^2-1), \quad 4pq$$

ein Quadrat ist, so daß also auch diese Zahlen bereits die erste Bedingung befriedigen. Fügt man die zweite Bedingung hinzu, so gelangt man wieder zu einem biquadratischen Ausdrucke, der ein Quadrat werden muß. Man findet $q = \frac{2p}{p^2-1}$, wodurch jene drei Zahlen übergehen in

$$x = (6p^2 - p^4 - 1)(p^2+1), \quad y = 4p(p^2-1)^2, \quad z = 8p^2(p^2-1),$$

wo p beliebig gewählt werden kann. Sind a, b, c die Seiten eines rechtwinkligen Dreiecks, so daß $a^2 + b^2 = c^2$ ist, so kann man die Lösung in der eleganteren Form darstellen

$$x = c(a^2 - b^2), \quad y = 2a^2b, \quad z = 2ab^2$$

und es ist dann

$$x^2 + y^2 + z^2 = c^6 \quad \text{und} \quad x^2y^2 + x^2z^2 + y^2z^2 = 4a^2b^2(a^4 + b^4)^2.$$

Diese letzte Form der Lösung leitet JOHANN ALBRECHT noch auf einem ganz direkten Wege ab und zeigt sodann, daß auch die Lösung des Vaters in der seinigen enthalten ist.

Wir wenden uns zu der Abhandlung 428 *Observationes circa bina biquadrata, quorum summam in duo alia biquadrata resolvere liceat*, die EULER nach den Akten am 13. Januar 1772 der Petersburger Akademie eingereicht hat. Die Aufgabe, die Gleichung

$$A^4 + B^4 = C^4 + D^4 \quad \text{oder} \quad A^4 - D^4 = C^4 - B^4$$

zu befriedigen, hat einige Ähnlichkeit mit dem in der Abhandlung 255 des vorhergehenden Bandes (I_2, p. 428) gelösten Probleme, wo es sich darum handelte, drei Kuben zu finden, deren Summe wieder ein Kubus ist, oder der Gleichung

$$A^3 + B^3 = D^3 - C^3$$

zu genügen. Auch die Ansätze zur Lösung stimmen überein, indem EULER auch hier, ähnlich wie bei 255, von der Substitution

$$A = p + q, \quad D = p - q, \quad C = r + s, \quad B = r - s$$

ausgeht. Er begnügt sich dann aber schließlich damit, zwei spezielle Lösungen zu entwickeln, von denen freilich die zweite infolge eines Rechenfehlers arg entstellt ist.[1]) Dies veranlaßte ihn später, in der Abhandlung 776 (I_5), nochmals auf die Aufgabe zurückzukommen, und dabei fand er dann die verhältnismäßig einfache Lösung

$$A = 542, \quad B = 103, \quad C = 359, \quad D = 514.$$

1) Siehe die Anmerkungen p. 216 und 217.

Die Abhandlung 451 *Resolutio problematis de inveniendo triangulo, in quo rectae ex singulis angulis latera opposita bisecantes sint rationales,* die nach den Akten am 24. August 1772 der Petersburger Akademie vorgelegt worden ist, gehört zu der Gruppe der Abhandlungen, in denen DIOPHANTISCHE Probleme in geometrischem Gewande behandelt werden und für die sich seiner Zeit JACOBI so sehr interessiert hatte.[1]) Speziell mit den Seitenhalbierenden eines Dreiecks beschäftigen sich unter diesen auch noch die Abhandlungen 713, 732, 754. In der Abhandlung 451 zeigt EULER zunächst, daß, wenn man ein Dreieck gefunden hat, das der Aufgabe entspricht, man sofort noch ein zweites mit derselben Eigenschaft erhalten kann, indem man das Dreieck konstruiert, dessen Seiten die Seitenhalbierenden des ersten sind. Um nun ein Dreieck der gewünschten Art zu erhalten, hat man drei DIOPHANTISCHE Gleichungen mit sechs Unbekannten aufzulösen. Nach Einführung von zwei neuen Unbekannten und nach geschickten Umformungen wird die Lösung schließlich darauf zurückgeführt, einen biquadratischen Ausdruck in ein Quadrat zu verwandeln. Diese Aufgabe wird von EULER in mehreren speziellen Fällen gelöst, woraus sich dann verhältnismäßig einfache Dreiecke ergeben. Er ist übrigens mit seiner Methode insofern selbst nicht ganz zufrieden, als sie nicht erkennen läßt, ob nicht noch einfachere Lösungen existieren, und so gibt er denn zum Schlusse noch Andeutungen, wie man auf Grund der Eigenschaften der Zahlen $x^2 + 3y^2$ die Aufgabe von einem höheren zahlentheoretischen Standpunkte aus angreifen könne.[2])

In der Abhandlung 466 *Problema DIOPHANTEUM singulare,* die EULER nach den Akten am 21. März 1774 der Petersburger Akademie eingereicht hat, wird eine Aufgabe behandelt, für die schon DIOPHANT unter Hinzufügung noch einer weiteren Bedingung eine spezielle Zahlenlösung gegeben hatte. Es handelt sich darum, zwei Zahlen zu finden, deren Produkt vermehrt oder vermindert um jede einzelne von ihnen ein Quadrat bildet. Die Aufgabe hat also große Ähnlichkeit mit der in Abhandlung 405 gelösten. Hier wie dort geht EULER von der Bemerkung aus, daß die gesuchten Zahlen nicht ganz sein können, und er gibt ihnen daher die Form $\frac{x}{z}$ und $\frac{y}{z}$, so daß also, nach Multiplikation mit z^2, die vier Ausdrücke

$$xy \pm xz \quad \text{und} \quad xy \pm yz$$

zu Quadraten zu machen sind. Den Schlüssel für die Lösung findet er in der Gleichung

1) Siehe die Besprechung der Abhandlung 167 p. XXI—XXII des Vorwortes zum vorhergehenden Bande, insbesondere auch die dazu gehörigen Anmerkungen. Siehe ferner die Anmerkung p. 282 des vorliegenden Bandes. Natürlich ist zu sagen, daß vorübergehend EULER sich noch in vielen andern zahlentheoretischen Abhandlungen geometrischer Einkleidung bedient hat (siehe z. B. die Abhandlungen 466 und 515 dieses Bandes).

2) Insbesondere auf Grund der Eigenschaft, daß die Divisoren der Zahlen $x^2 + 3y^2$ wieder von derselben Form sein müssen, was EULER in der Abhandlung 272 (I_2, p. 556) bewiesen hatte.

$$a^2 + b^2 \pm 2ab = \square$$

und er setzt daher

$$xy = a^2 + b^2 = c^2 + d^2 \quad \text{und} \quad xz = 2ab, \quad yz = 2cd,$$

woraus sich ergibt, daß $\frac{abcd}{a^2+b^2}$ ein Quadrat sein muß. Durch geeignete Substitutionen wird diese Forderung darauf zurückgeführt, daß ein gewisser biquadratischer Ausdruck zu einem Quadrate gemacht werden muß, worauf sich dann die Lösungen für $\frac{x}{z}$ und $\frac{y}{z}$ leicht gewinnen lassen. Da diese aber schon im einfachsten Falle zu außerordentlich großen Zahlen führen, so entwickelt EULER noch verschiedene Abänderungen seines Verfahrens, die ihn freilich zunächst nicht zu einfacheren Lösungen gelangen lassen. Die Abhandlung bietet ein typisches Beispiel für die Offenheit, mit der EULER dem Leser gegenübertritt. Weit davon entfernt, Fehlversuche verheimlichen zu wollen, gewährt er ihm mit größter Liebenswürdigkeit genauen Einblick in seine Werkstatt und läßt ihn in gleicher Weise an seinen Enttäuschungen teilnehmen wie an seiner Freude bei der Entdeckung des richtigen Weges.[1]) So führten ihn auch hier anfänglich vergebliche Versuche zu einer *Solutio plana problematis propositi*. Die Lösung kommt darauf hinaus, zwei rechtwinklige Dreiecke[2]) in ganzen Zahlen zu ermitteln, deren Flächeninhalte gleich sind, eine Aufgabe, die EULER dann noch dahin verallgemeinert, daß er für die Flächeninhalte der beiden Dreiecke ein gegebenes Verhältnis vorschreibt.

Schon vor den Abhandlungen 427, 428, 451, 466 hatte EULER die Abhandlung 474 *Solutio quorundam problematum* DIOPHANTEORUM der Petersburger Akademie vorgelegt, nach den Akten am 4. Juli 1771. Sie ist aber erst 1776 im Drucke erschienen. Es werden darin drei Probleme gelöst. Das erste verlangt, daß die beiden Ausdrücke

$$(x^2 + y^2)(t^2x^2 + u^2y^2) \quad \text{und} \quad (x^2 + y^2)(u^2x^2 + t^2y^2)$$

1) Ich kann mir nicht versagen, eine Stelle aus der Rede zu wiederholen, die FROBENIUS bei dem Festakte der Universität Basel zur Feier des zweihundertsten Geburtstages LEONHARD EULERS als Vertreter der Berliner Akademie gehalten hat (Festbericht, Basel 1907; siehe p. XIX—XX des Vorwortes zur Gesamtausgabe der Werke LEONHARD EULERS, Band I_1). Sie lautet: „Eine Eigenschaft allerdings fehlte EULER, die dem modernen Genie unerläßlich scheint, die Unklarheit, die Dunkelheit. Davor bewahrte ihn sein gerader Verstand, sein ehrlicher Sinn. Während GAUSS bei seiner Darstellung alle Brücken hinter sich abzubrechen pflegt, berichtet EULER getreulich über alle Wege und Umwege, die er gegangen ist. Nicht selten aber gibt er zum Schluß als genialen Einfall eine einfachere Methode, zu dem gewünschten Ziele zu gelangen. Und ein Widerschein der leidenschaftlichen Freude, die ihn beim Aufspüren der Wahrheit durchglühte, erwärmt noch heute den Leser beim Studium seiner Werke. So war EULER unser aller Lehrer, nicht nur in den Ergebnissen der Wissenschaft, sondern auch in der Methode ihrer Darstellung."

2) Siehe die Anmerkung 1 p. XXIV.

gleichzeitig Quadrate werden sollen, wobei man sowohl x und y als auch t und u als teilerfremd voraussetzen kann. Die Lösung führt auf einen biquadratischen Ausdruck, der zu einem Quadrate gemacht werden muß, und liefert dann unendlich viele Paare x, y und t, u. Der ersten Lösung fügt EULER aber auch noch andere hinzu und erhält schließlich für die gesuchten Zahlen sehr einfache Werte, so z. B.

$$x = 3, \quad y = 5, \quad t = 45, \quad u = 11.$$

Im zweiten Probleme wird gefordert, daß

$$(t^2x^2 + u^2y^2)(u^2x^2 + t^2y^2)$$

ein Quadrat werde. Hierfür entwickelt EULER zwei Lösungen, von denen die eine identisch ist mit der Lösung des ersten Problems. Das dritte Problem endlich verlangt, daß

$$t^2x^2 + u^2y^2 \quad \text{und} \quad t^2y^2 + u^2x^2$$

gleichzeitig Quadrate werden. Die Lösung ergibt sich aus den Lösungen der beiden vorhergehenden Aufgaben. Zum Schlusse fügt EULER den beiden Bedingungen noch weitere hinzu, die ihn zu der Gleichung

$$x^4 - x^3y + 2x^2y^2 - xy^3 + y^4 = \square$$

führen, und er bemerkt, daß er zu diesen Untersuchungen durch eine geometrische Aufgabe geführt worden sei, die er bei FR. V. SCHOOTEN gefunden habe.

Die Abhandlung 515 *De casibus quibusdam maxime memorabilibus in analysi indeterminata, ubi imprimis insignis usus calculi angulorum in analysi* DIOPHANTEA *ostenditur*, die nach den Akten am 1. Mai 1780 der Petersburger Akademie vorgelegt worden ist, kann als eine Fortsetzung der Abhandlung 253 *De problematibus indeterminatis, quae videntur plus quam determinata*, gelten, die sich im vorhergehenden Bande (I_2, p. 399) befindet.[1]) In dieser früheren Abhandlung hatte EULER gezeigt, wie man mit leichter Mühe eine Reihe von DIOPHANTISCHEN Problemen gleichzeitig lösen kann, wenn die unbestimmten Größen durch eine einzige Gleichung miteinander verbunden sind. Obwohl solche Aufgaben scheinbar mehr als bestimmt sind, insofern die Zahl der Bedingungen die Zahl der Unbekannten übersteigt, liefern sie doch noch unendlich viele Lösungen. Während er sich aber damals auf Gleichungen beschränkte, die den zweiten Grad nicht übersteigen, legt er jetzt in der Abhandlung 515 Gleichungen zugrunde, in denen die Unbekannten sogar bis zur vierten Dimension ansteigen. Ist beispielsweise die Gleichung

$$x^4 + y^4 + z^4 + v^4 - 2x^2y^2 - 2x^2z^2 - 2y^2z^2 + 2x^2v^2 + 2y^2v^2 + 2z^2v^2 = 0$$

1) Siehe auch die dort (I_2, p. 399) hinzugefügte Anmerkung, in der auf EULERS *Algebra* verwiesen ist.

durch rationale Zahlen x, y, z, v zu befriedigen, so werden durch die Lösungen zugleich sieben Formeln, wie

$$x^2y^2 - z^2v^2, \quad x^2z^2 - y^2v^2 \quad \text{etc.},$$

von selbst in Quadrate übergehen. EULER zeigt nun, daß sich die ganze Lösung darauf zurückführen läßt, nur die beiden ersten Formeln in Quadrate zu verwandeln. Dies führt er auf zwei Arten durch, wobei er sich das zweite Mal auf Grund der Substitutionen

$$xy \sin \alpha = vz \quad \text{und} \quad xz \sin \beta = vy$$

der Hülfsmittel der Trigonometrie[1]) bedient. In ähnlicher Weise wird auch die Lösung der Gleichung

$$x^4 + y^4 + z^4 + v^4 - 2x^2y^2 - 2x^2z^2 - 2y^2z^2 - 2x^2v^2 - 2y^2v^2 - 2z^2v^2 = 0$$

gewonnen.

Nach der Besprechung der neun Abhandlungen, die der Lösung DIOPHANTISCHER Probleme gewidmet sind, wenden wir uns zu der Abhandlung 445 *Novae demonstrationes circa resolutionem numerorum in quadrata.* EULER hatte diese Abhandlung nach den Akten am 21. September 1772 der Petersburger Akademie eingereicht, sie aber 1773 wieder zurückgezogen und im selben Jahre in den Leipziger Nova acta eruditorum veröffentlicht; am 24. März 1774 legte er sie ein zweites Mal der Akademie vor, in deren Acta sie 1780 neuerdings im Drucke erschien.[2]) Die beiden Fassungen weichen nur unbedeutend voneinander ab; unserer Ausgabe liegt die zweite zugrunde. EULER nimmt in dieser Abhandlung 445 ein Problem wieder auf, das er mehr als zwanzig Jahre früher behandelt, aber nicht ganz zu dem gewünschten Ziele geführt hatte. Am Schlusse der Abhandlung 242 *Demonstratio theorematis FERMATIANI omnem numerum sive integrum sive fractum esse summam quatuor pauciorumve quadratorum* (I_2, p. 338), deren Titel — er ist erst nachträglich von JACOBI vorgeschlagen worden — insofern irreleitet, als diese Abhandlung ihrem Hauptinhalte nach den Grundlagen der Theorie der quadratischen Reste gewidmet ist,[3]) hatte EULER als Anwendung seiner Theorie den Satz zu beweisen versucht, daß sich jede Zahl als Summe von vier oder weniger Quadraten darstellen lasse, ein Theorem, um das er sich schon seit 1730 bemüht hatte. Der Satz war, wie bereits früher bemerkt, schon vor FERMAT von BACHET[4]) aufgestellt und durch eine weitgehende Induktion gestützt worden, und zwar in der berühmten Ausgabe der *Arithmetik* DIOPHANTS vom Jahre 1621. EULER war, wie er auch selbst zugab, in jener Abhandlung mit dem Beweise insofern nicht ganz

1) Siehe die Anmerkung 1 p. XXIV.
2) Siehe p. VIII.
3) Siehe p. XXVI—XXVII des Vorwortes zum vorhergehenden Bande.
4) Siehe die Anmerkung 4 p. 358 des vorhergehenden Bandes.

zustande gekommen, als er die Richtigkeit des Satzes nur hatte dartun können, falls auch Brüche zugelassen werden. Daß der Satz von BACHET auch in ganzen Zahlen Geltung hat, ist zuerst von LAGRANGE bewiesen worden in der Abhandlung *Démonstration d'un théorème d'arithmétique*, die 1772 in den Berliner Memoiren erschien.[1]) Diese Abhandlung scheint auf EULER großen Eindruck gemacht zu haben. Noch in demselben Jahre reichte er, wie wir gesehen haben, der Petersburger Akademie seine *Novae demonstrationes* ein, und wenn er das Manuskript bald darauf wieder zurückzog, so war für ihn ohne Zweifel der Wunsch bestimmend, die Arbeit in den Nova acta eruditorum früher veröffentlichen zu können.

EULER beginnt seine Entwickelungen, indem er zunächst den von LAGRANGE gegebenen Beweis in seinen Grundzügen kurz wiederholt und die Stellen bezeichnet, die ihm verbesserungsbedürftig erscheinen. Dann geht er zu seinem eigenen Beweise über. Dieser stützt sich im wesentlichen auf den Satz, daß eine Summe von vier Quadraten keine anderen Teiler zuläßt als solche, die selbst Summen von vier Quadraten sind, daß also eine derartige Summe ähnliche Eigenschaften hat wie die Formen p^2+q^2, p^2+2q^2, p^2+3q^2. Da sich nun zeigen läßt, daß für jede Primzahl N stets vier Quadrate ermittelt werden können, deren Summe durch N teilbar ist, — das hatte zwar auch schon LAGRANGE bewiesen, aber gerade diesen Beweis hatte EULER als *abstrusus et prolixus* bezeichnet, — so war damit festgestellt, daß jede Primzahl als Summe von vier Quadraten darstellbar ist, und da EULER schon in der Abhandlung 242 zu der berühmten Identität gelangt war, nach der das Produkt zweier Summen von vier Quadraten wieder eine Summe von vier Quadraten ist, so war der Satz von BACHET nun ganz allgemein bewiesen.[2])

Die Abhandlung 449 *Demonstrationes circa residua ex divisione potestatum per numeros primos resultantia,* die von EULER nach den Akten am 18. Mai 1772 der Petersburger Akademie vorgelegt worden ist und die 1774 im Drucke erschien, verdient um so mehr unsere Beachtung, als sie die Zahlentheorie um den wichtigen Begriff der *primitiven Wurzeln* bereichert hat. Sie knüpft an die Abhandlungen 262 *Theoremata circa residua ex divisione potestatum relicta* und 271 *Theoremata arithmetica nova methodo demonstrata* des vorhergehenden Bandes an (I_2, p. 493 und 531), von denen die erste die Grundlagen für die Theorie der Potenzreste geschaffen und die zweite die Funktion $\varphi(m)$ in die Zahlentheorie

1) Siehe die Anmerkung 2 p. 370 des vorhergehenden Bandes.

2) Die Anmerkung 2 p. 239 bedarf noch einer Ergänzung. Daß das in den Nova acta eruditorum vorgelegte Problem der Integralrechnung wirklich von EULER herrührt, was auch schon ENESTRÖM in seinem *Verzeichnis*, p. 135, als sicher angenommen hat, ergibt sich aus EULERS Briefwechsel mit LAGRANGE: Die kurze briefliche Mitteilung EULERS, die LAGRANGE mit der Bemerkung „Reçu le 26 janvier 1775, répondu le 10 février" versehen hat, ist identisch mit jenem Eingesandt in den Nova acta eruditorum. Siehe *LEONHARDI EULERI Opera postuma*, t. I, p. 585; *Oeuvres de LAGRANGE*, t. XIV, p. 240; *LEONHARDI EULERI Opera omnia*, series III.

eingeführt hatte. In der Abhandlung 449 kommt EULER nach einigen einleitenden Betrachtungen sehr bald auf den tiefgehenden Unterschied zwischen *vollständigen* und *unvollständigen* Reihen von Potenzresten zu sprechen. Erzeugt eine geometrische Progression

$$1,\ a,\ a^2,\ a^3 \text{ etc.}$$

bei der Division durch die Primzahl P eine vollständige Reihe von Resten, d. h. eine Reihe, in der alle Zahlen, die kleiner sind als P, vorkommen, so nennt er a eine *primitive* Wurzel. EULER beweist nun, daß es für jede Primzahl P immer solche primitiven Wurzeln gibt, und er bestimmt auch ihre Anzahl, die wir heute in der Form $\varphi(P-1)$ schreiben.

Bekanntlich hat GAUSS gegen EULERS Beweisführung zwei Einwände erhoben, von denen sich der erste gegen die Paragraphen 31 und 32 richtet. Dort freilich ist der Einwand auch berechtigt (siehe die Anmerkung p. 250) und EULER hätte in § 32 besser gesagt, die Anzahl aller casus proprii könne nicht größer sein als n. Aber GAUSS scheint übersehen zu haben, daß der gerügte Mangel (der leicht gehoben werden kann) nicht bis zu dem entscheidenden § 35, wo $n = P - 1$ gesetzt wird, hinübergreift. Denn dort hat die Kongruenz

$$x^{P-1} \equiv 1 \pmod{P}$$

nach dem FERMATSCHEN Satze tatsächlich genau $P-1$ reelle Wurzeln. Wenn also auch EULERS Beweis als nicht ganz abgeklärt bezeichnet werden kann, so läßt sich doch nicht behaupten, EULER habe die Existenz primitiver Wurzeln nicht bewiesen. Er hat vielmehr alles beigebracht, was zur Durchführung eines strengen Beweises erforderlich ist, eines Beweises überdies, der sich vor den späteren Beweisen von GAUSS durch größere Einfachheit auszeichnet. Übrigens hat in unseren Tagen E. CAHEN in seinen *Eléments de la théorie des nombres*, Paris 1900, für die Existenz primitiver Wurzeln einen Beweis gegeben, der dem EULERSCHEN sehr ähnlich ist. Auch der zweite von GAUSS erhobene Einwand ist nicht von großem Gewichte. Denn wenn auch EULER die Formel des § 34 nur durch Induktion hergeleitet hat, so könnte er sich doch mit gutem Rechte auf die oben erwähnte Abhandlung 271 berufen, wo er die analoge Herleitung mit aller Gründlichkeit durchgeführt hatte.

Dagegen erfordert die Gerechtigkeit, noch zu sagen, daß der Satz, den EULER in § 28 beweist und wonach eine Kongruenz vom Grade n für einen Primzahlmodul nie mehr als n inkongruente Wurzeln haben kann, schon zwei Jahre vorher von LAGRANGE[1]) bewiesen worden war, wovon EULER aber keine Kenntnis gehabt hat. Seit 1766 völlig erblindet und darauf angewiesen, daß man ihm vorlas, war er nicht mehr imstande, sich eingehend mit den Arbeiten anderer Mathematiker zu beschäftigen. In dem p. XX, Anmerkung 2, erwähnten Briefe

1) J. L. LAGRANGE, *Nouvelle méthode pour résoudre les problèmes indéterminés en nombres entiers*, Mém. de l'acad. d. sc. de Berlin **24** (1768), 1770; *Oeuvres de* LAGRANGE, t. II, p. 655.

an LAGRANGE vom $\frac{9}{20}$ März 1770 schrieb er: „Je me suis fait lire toutes les opérations que vous avez faites sur la formule $101 = p^2 - 13q^2$ et je suis entièrement convaincu de leur solidité; mais étant hors d'état de lire ou d'écrire moi-même, je dois vous avouer que mon imagination n'a pas été capable de saisir le fondement de toutes les déductions que vous avez été obligé de faire et encore moins de fixer dans mon esprit la signification de toutes les lettres que vous y avez introduites. Il est bien vrai que de semblables recherches ont fait autrefois mes délices et m'ont coûté bien du temps; mais à présent je ne saurais plus entreprendre que celles que je suis capable de développer dans ma tête et souvent je suis obligé de recourir à un ami pour exécuter les calculs que mon imagination projette."

Unter den Anwendungen, die EULER in der Abhandlung 449 von den primitiven Wurzeln macht, verdient eine noch ganz besonders hervorgehoben zu werden. Denn in § 85 beweist er mit ihrer Hülfe, daß alle Primzahlen der Form $8m + 1$ zugleich in der Form $x^2 + 2y^2$ enthalten sind. Damit war es ihm gelungen, zunächst einmal die eine Hälfte jenes berühmten von FERMAT ohne Beweis aufgestellten Satzes[1]) als richtig nachzuweisen, was er in der Abhandlung 256 *Specimen de usu observationum in mathesi pura* (I_2, p. 459) vergeblich angestrebt hatte.[2]) Die andere Hälfte des FERMATSCHEN Satzes, daß nämlich auch alle Primzahlen der Form $8m + 3$ zugleich in der Form $x^2 + 2y^2$ enthalten seien, konnte EULER zwar aus denselben Überlegungen nicht gewinnen, der Beweis gelang indessen auf Grund der Ausführungen, die er einem Freunde[3]) zu verdanken hatte. Durch diese in den Paragraphen 85—90 enthaltenen Untersuchungen war aber der quadratische *Charakter* der Zahlen $+2$ und -2 festgestellt, und zwar auf Grund gesicherter Beweise, so wie früher in den Abhandlungen 241 *Demonstratio theorematis Fermatiani omnem numerum primum formae* $4n + 1$ *esse summam duorum quadratorum* und 272 *Supplementum quorundam theorematum arithmeticorum, quae in nonnullis demonstrationibus supponuntur*, des vorhergehenden Bandes (I_2, p. 328 und 556) der Charakter der Zahlen -1 und ± 3 ermittelt worden war.

Es hat den Anschein, als ob diese wichtige Tatsache bisher ganz unbeachtet geblieben sei. GAUSS sagt in Art. 116 seiner *Disquisitiones arithmeticae*, EULER habe stets vergeblich nach einem Beweise gesucht, und in Art. 120 wundert er sich, daß EULER zwar die auf die Reste ± 3 bezüglichen Sätze bewiesen habe, daß aber die Beweise für ± 2 seinem Scharfsinne entgangen seien. Der in der Abhandlung 449 enthaltenen Beweise wird, so weit ich sehe, weder von GAUSS noch von Späteren irgendwie gedacht. Die Abhandlung

1) Siehe die Anmerkung p. 466 des vorhergehenden Bandes.

2) Siehe p. 485 des vorhergehenden Bandes.

3) Vermutlich A. J. LEXELL, dessen Hülfe sich EULER zu jener Zeit besonders bediente. N. FUSS kam erst 1773 nach Petersburg.

Recherches d'arithmétique von LAGRANGE[1]), dem seit GAUSS allgemein die Priorität zugesprochen wird, erschien aber erst 1775—1777 im Drucke, während EULERS Abhandlung, die schon im Mai 1772 eingereicht worden war, 1774 veröffentlicht wurde.

Mit der Abhandlung 541 *Evolutio producti infiniti*

$$(1-x)(1-xx)(1-x^3)(1-x^4)(1-x^5)(1-x^6) \text{ etc.}$$

in seriem simplicem, die nach den Akten am 14. August 1775 der Petersburger Akademie vorgelegt worden war, aber erst 1783 gedruckt wurde, kehrte EULER zu Untersuchungen zurück, die er in den Abhandlungen 158, 175, 191, 243, 244 des vorhergehenden Bandes (I_2, p. 163, 241, 254, 373, 390) und auch in der *Introductio* angestellt hatte.[2]) Die beiden Entwickelungen, die in 541 enthalten sind, unterscheiden sich nicht wesentlich von der, die in Abhandlung 244 *Demonstratio theorematis circa ordinem in summis divisorum observatum* (I_2, p. 390) gegeben worden war. Es ist daher nicht recht zu verstehen, warum die Brüder FUSS die Abhandlung 541 aus ihrer Sammlung ausgeschlossen haben, obwohl JACOBI[3]) ihre Aufnahme befürwortet hatte. In der Tat hat EULER diese Entwickelungen nur vom Standpunkte der Zahlentheorie unternommen und so hielt sich das Redaktionskomitee für verpflichtet, die Abhandlung 541 dem Wunsche JACOBIS entsprechend unter die *Commentationes arithmeticae* einzureihen.[4])

Die Aufnahme der Abhandlung 541 in unsern Band I_3 schien um so mehr geboten, als diese Dissertation geradezu als Einleitung zu der folgenden Abhandlung 542 *De mirabilibus proprietatibus numerorum pentagonalium* gelten kann. EULER hatte diese nach den Akten am 4. September 1775 der Petersburger Akademie vorgelegt, also gleich nach 541, und auch im Drucke folgten beide Abhandlungen hinter einander im selben Bande der Petersburger Acta. Nach einigen einleitenden Bemerkungen über die Pentagonalzahlen knüpft EULER sofort an die eben erwähnten Abhandlungen 175, 243, 244 an, in denen er den engen Zusammenhang zwischen der Reihe der Pentagonalzahlen und der Darstellung der Divisorensummen auseinandergesetzt hatte. Dieser Zusammenhang ist aber gerade in der Entwickelung des unendlichen Produktes

$$(1-x)(1-x^2)(1-x^3)(1-x^4) \text{ etc.}$$

1) Siehe die Anmerkung p. 194 des vorhergehenden Bandes. Ich muß übrigens gestehen daß bei der Herausgabe dieses Bandes I_2 auch mir selbst der EULERSCHE Beweis nicht genügend bekannt war. Danach sind also dort die Stellen p. XXX und p. 485 (Anmerkung) im Sinne der Priorität EULERS zu ändern.

2) Siehe die Anmerkung p. 191 des vorhergehenden Bandes.

3) Siehe P. STÄCKEL und W. AHRENS, *Der Briefwechsel zwischen C. G. J. JACOBI und P. H. VON FUSS über die Herausgabe der Werke LEONHARD EULERS*, Leipzig 1908, p. 65.

4) Siehe p. VII und VIII.

begründet, die er in der vorhergehenden Abhandlung 541 und in jener früheren 244 gegeben hatte, denn die resultierende Reihe

$$S = 1 - x^1 - x^2 + x^5 + x^7 - x^{12} - x^{15} + x^{22} + x^{26} - \text{etc.}$$

ist so beschaffen, daß ihre Exponenten die Reihe der Pentagonalzahlen darstellen. Aus dieser Entwickelung folgt z. B., daß die Gleichung $S = 0$ allemal befriedigt wird, sobald einer der unendlich vielen Faktoren $1 - x^n$ des ihr äquivalenten Produktes verschwindet, daß also alle Einheitswurzeln zugleich Wurzeln der Gleichung $S = 0$ sind. Dies wird für die einzelnen Einheitswurzeln genauer durchgeführt, wobei insbesondere das jedesmalige Zerfallen der Reihe in Perioden besprochen wird. Da ferner jede Einheitswurzel α nicht nur einmal, sondern unendlich oft unter den Wurzeln von $S = 0$ auftritt, so wird nach der Theorie der Gleichungen α auch noch Wurzel von unendlich vielen Gleichungen sein, die aus $S = 0$ abgeleitet werden und die sich in der Form

$$- 1^\lambda x - 2^\lambda x^2 + 5^\lambda x^5 + 7^\lambda x^7 - 12^\lambda x^{12} - 15^\lambda x^{15} + \text{etc.}$$

darstellen.

Wir gelangen schließlich zu den beiden letzten, in engem Zusammenhange stehenden Abhandlungen 552 und 554, die beide im Todesjahre 1783 im ersten Bande der von EULER selbst noch vorbereiteten *Opuscula analytica* erschienen sind. Beide waren nach den Akten schon am 18. Mai 1772 gleichzeitig mit 449 der Petersburger Akademie vorgelegt worden. In der Abhandlung 552 *Observationes circa divisionem quadratorum per numeros primos* entwickelt EULER zunächst von neuem die Grundlagen der Theorie der quadratischen Reste, ähnlich wie in der oft erwähnten Abhandlung 242 des vorhergehenden Bandes, nur daß er sich jetzt von Anfang an auf Primzahlmoduln beschränkt. Dann aber gelangt er im Theorema 3 zu einer sehr wichtigen Erweiterung der Theorie durch Einführung des Begriffes der *reziproken Reste*. Diesem Begriffe, von dem EULER selbst sagt, er sei maximi momenti, war er im Theorema 7 der Abhandlung 242, insbesondere in § 41, bereits sehr nahe gekommen, doch hatte er damals nicht erkannt, daß die paarweise Zuordnung, die er im Sinne hatte, tatsächlich allemal herstellbar ist, und so war es ihm versagt geblieben, den letzten entscheidenden Schritt zu tun. Jetzt aber konnte er ohne Mühe direkt beweisen, daß -1 quadratischer Rest aller Primzahlen $P = 4q + 1$ ist, woraus sich dann sofort ergab, daß auch das *Komplement* eines jeden Restes von P stets wieder ein Rest ist. Damit hatte er den direkten Beweis gewonnen, nach dem er in § 84 von 242 vergeblich verlangt hatte.

Ein besonders heller Glanz aber strahlt von dem Schlusse der Abhandlung aus. Denn hier stellt EULER als einen Satz, dessen Beweis noch ausstehe, „in ganz entwickelter und vollendeter Form" sein berühmtes Reziprozitätsgesetz auf, das in noch unentwickelter

Form schon in der aus dem Jahre 1747 stammenden Abhandlung 164 des vorhergehenden Bandes (I_2, p. 194) enthalten war.[1])

Die Abhandlung 554 *Disquisitio accuratior circa residua ex divisione quadratorum altiorumque potestatum per numeros primos relicta* bringt ihrem Titel entsprechend zunächst eine etwas eingehendere Untersuchung der quadratischen Reste je nach dem Modul $4m + 1$ oder $4m + 3$. Ist α ein Rest von $p = 2q + 1$, so sind auch die einzelnen Glieder der geometrischen Progression

$$1, \alpha, \alpha^2, \alpha^3, \ldots \alpha^{q-1}$$

Reste und es sind darin entweder alle Reste enthalten oder nur ein aliquoter Teil. Ausführlicher werden dann auch wieder die reziproken Reste behandelt, die EULER jetzt *residua sociata* nennt, und es werden für verschiedene Primzahlen der Form $p = 4m + 1$ jedesmal die m Paare komplementärer Reste mit den zugehörigen Quadraten zusammengestellt. Würde sich dabei immer ein Paar zusammengehöriger Quadrate einstellen, deren Summe gleich p ist, so hätte man damit eine direkte Bestätigung des bekannten FERMATSCHEN Satzes. Indessen genügt es auf Grund der in der Abhandlung 228 bewiesenen Eigenschaften der Formen $x^2 + y^2$, daß man für jede Primzahl $p = 4m + 1$ stets Summen von zwei Quadraten angeben kann, die durch p teilbar sind.

EULER kehrt sodann wieder zu den geometrischen Progressionen zurück, die man für $p = 2q + 1$ aus den einzelnen quadratischen Resten $1, \alpha, \beta, \gamma, \ldots \lambda$, deren Anzahl gleich q ist, bilden kann. Ist q prim, so umfaßt jede dieser Progressionen alle q Reste und man kann dann aus einer jeden von ihnen durch gleichmäßiges Überspringen von je zwei oder mehr Gliedern leicht alle übrigen herstellen. Ist aber q zusammengesetzt, so sind von jenen Progressionen die einen vollständig, die anderen unvollständig und in Perioden zerfallend. Aus einer jeden vollständigen Progression kann man aber wiederum durch gleichmäßiges Überspringen alle übrigen, die vollständigen wie die periodischen, ableiten.

Die Untersuchung einer solchen vollständigen Progression für $q = mn$, also $p = 2mn + 1$, führt dazu, nicht nur Reste von Quadraten, sondern auch von höheren Potenzen, zunächst von geraden, dann aber auch von beliebigen, zu betrachten. Ist jetzt $p = mn + 1$ und dividiert man die Potenzen

$$1, 2^m, 3^m, 4^m, 5^m, 6^m, \ldots (p-1)^m$$

durch p, so kommen unter den Resten nur n verschiedene vor, die sich m mal wiederholen, während die andern $(m-1)n$ Zahlen ausgeschlossen sind. Dies wird durch eine große Zahl von Beispielen erläutert. Mit solchen höheren Resten hatte sich EULER zum ersten

1) Siehe hierzu die Ausführungen von L. KRONECKER, die in der Anmerkung p. 217 des vorhergehenden Bandes mitgeteilt sind.

Male in der Abhandlung 134 und dann wieder in der Abhandlung 262 des vorhergehenden Bandes (I_2, p. 62 und 493) beschäftigt und er hatte dort als Kriterium für den Restcharakter einer Zahl D (nach heutiger Schreibweise) die Kongruenz[1])

$$D^{\frac{p-1}{m}} \equiv +1 \,(\text{mod. } p = mn+1) \quad \text{oder} \quad D^n \equiv +1 \,(\text{mod. } p = mn+1)$$

aufgestellt, die eben dann jene n Reste bestimmt.

Zum Schlusse bringt EULER diese Untersuchungen über die quadratischen und höheren Reste in Zusammenhang mit der Theorie der primitiven Wurzeln, die er in der Abhandlung 449 eingeführt hatte. Ist a eine solche primitive Wurzel von $p = 2q+1$, d. h. so beschaffen, daß die geometrische Reihe

$$1,\ a,\ a^2,\ a^3,\ \ldots\ a^{p-2}$$

bei der Division durch p alle Zahlen, die kleiner sind als p, als Reste zurückläßt, so liefert a^q den Rest -1 und die folgenden Potenzen a^{q+1}, a^{q+2}, a^{q+3} etc. geben dann die Reste $-a$, $-a^2$, $-a^3$ etc. und liefern daher mit den vorhergehenden Potenzen a^{q-1}, a^{q-2}, a^{q-3} etc. allemal ein Paar solcher *residua sociata*, deren Produkt der Einheit äquivalent ist. Aus der Reihe 1, a, a^2, a^3 etc. ergeben sich überdies sofort die quadratischen, kubischen, biquadratischen und höheren Reste von p. Die Anzahl der primitiven Wurzeln war schon früher in den Abhandlungen 449 und 271 als gleich $\varphi(p-1)$ ermittelt worden. Kennt man eine von ihnen, so lassen sich die andern leicht daraus ableiten.

Auch bei der Herstellung des vorliegenden Bandes bin ich von meinen beiden Mitredaktoren aufs beste unterstützt worden und so ist es mir ein Bedürfnis, ihnen für ihre nie versagende selbstlose Hülfe auch öffentlich zu danken. Herzlichen Dank schulde ich sodann wiederum Herrn G. ENESTRÖM für so manchen Rat in historischen Fragen, sowie der Verlagsfirma B. G. TEUBNER, die es auch diesmal an freundlichem Entgegenkommen trotz den schwierigen Zeitverhältnissen nicht hat fehlen lassen.

1) Siehe auch p. XXXI—XXXII der Vorrede zum vorhergehenden Bande.

Zürich, den 6. Januar 1917.

FERDINAND RUDIO.

INDEX

Insunt in hoc volumine indicis Enestroemiani commentationes
283, A9, 323, 369, 394, 405, 427, 428, 445, 449, 451, 452, 454, 461, 466, 467, 474, 498, 708a, 515, 523, A31, 541, 542, 552, 554

pag.

283. De numeris primis valde magnis 1

Novi commentarii academiae scientiarum Petropolitanae 9 (1762/3), 1764, p. 99—153

A9. Albrecht Eulers Beantwortung einiger arithmetischen Fragen . . . 46

Abhandlungen der Churfürstlich-baierischen Akademie der Wissenschaften 2, II, 1764, p. 3—36

323. De usu novi algorithmi in problemate Pelliano solvendo 73

Novi commentarii academiae scientiarum Petropolitanae 11 (1765), 1767, p. 28—66

369. Quomodo numeri praemagni sint explorandi, utrum sint primi necne 112

Novi commentarii academiae scientiarum Petropolitanae 13 (1768), 1769, p. 67—88

394. De partitione numerorum in partes tam numero quam specie datas 131

Novi commentarii academiae scientiarum Petropolitanae 14 (1769): I, 1770, p. 168—187

405. Solutio problematis, quo duo quaeruntur numeri, quorum productum tam summa quam differentia eorum sive auctum sive minutum fiat quadratum 148

Novi commentarii academiae scientiarum Petropolitanae 15 (1770), 1771, p. 29—50

427. Problematis cuiusdam Diophantei evolutio 172

Novi commentarii academiae scientiarum Petropolitanae 17 (1772), 1773, p. 24—63

pag.

'428. Observationes circa bina biquadrata, quorum summam in duo alia biquadrata resolvere liceat 211

Novi commentarii academiae scientiarum Petropolitanae 17 (1772), 1773, p. 64—69

'445. Novae demonstrationes circa resolutionem numerorum in quadrata . 218

Nova acta eruditorum 1773, p. 193—211
Acta academiae scientiarum Petropolitanae 1777: II, 1780, p. 48—69

'449. Demonstrationes circa residua ex divisione potestatum per numeros primos resultantia 240

Novi commentarii academiae scientiarum Petropolitanae 18 (1773), 1774, p. 85—135

'451. Solutio problematis de inveniendo triangulo, in quo rectae ex singulis angulis latera opposita bisecantes sint rationales 282

Novi commentarii academiae scientiarum Petropolitanae 18 (1773), 1774, p. 171—184

'452. Resolutio aequationis $Ax^2 + 2Bxy + Cy^2 + 2Dx + 2Ey + F = 0$ per numeros tam rationales quam integros 297

Novi commentarii academiae scientiarum Petropolitanae 18 (1773), 1774, p. 185—197

'454. De resolutione irrationalium per fractiones continuas, ubi simul nova quaedam et singularis species minimi exponitur 310

Novi commentarii academiae scientiarum Petropolitanae 18 (1773), 1774, p. 218—244

'461. Extrait d'une lettre de M. Euler le père à M. Bernoulli concernant le mémoire imprimé parmi ceux de 1771 p. 318 335

Nouveaux mémoires de l'académie des sciences de Berlin 1772, 1774, Histoire, p. 35—36

'466. Problema Diophanteum singulare 338

Novi commentarii academiae scientiarum Petropolitanae 19 (1774), 1775, p. 112—131

'467. De tabula numerorum primorum usque ad millionem et ultra continuanda, in qua simul omnium numerorum non primorum minimi divisores exprimantur 359

Novi commentarii academiae scientiarum Petropolitanae 19 (1774), 1775, p. 132—183

pag.
474. Solutio quorundam problematum DIOPHANTEORUM 405
Novi commentarii academiae scientiarum Petropolitanae 20 (1775), 1776, p. 48—58

498. Extrait d'une lettre de M. EULER à M. BEGUELIN en mai 1778 418
Nouveaux mémoires de l'académie des sciences de Berlin 1776, 1779, p. 337—339

708a. Extrait d'une lettre de M. FUSS à M. BEGUELIN écrite de Pétersbourg le $\frac{19}{30}$ juin 1778 421
Nouveaux mémoires de l'académie des sciences de Berlin 1776, 1779, p. 340—346

515. De casibus quibusdam maxime memorabilibus in analysi indeterminata, ubi imprimis insignis usus calculi angulorum in analysi DIOPHANTEA ostenditur 429
Acta academiae scientiarum Petropolitanae 1778: II, 1781, p. 85—110

523. De tribus numeris quadratis, quorum tam summa quam summa productorum ex binis sit quadratum 453
Acta academiae scientiarum Petropolitanae 1779: I, 1782, p. 30—39

A31. Ad dissertationem patris de tribus numeris, quorum tam summa quam summa productorum ex binis sit quadratum, commentatio. Auctore I. A. EULERO 463
Acta academiae scientiarum Petropolitanae 1779: I, 1782, p. 40—48

541. Evolutio producti infiniti $(1-x)(1-xx)(1-x^3)(1-x^4)(1-x^5)(1-x^6)$ etc. in seriem simplicem 472
Acta academiae scientiarum Petropolitanae 1780: I, 1783, p. 47—55

542. De mirabilibus proprietatibus numerorum pentagonalium 480
Acta academiae scientiarum Petropolitanae 1780: I, 1783, p. 56—75

552. Observationes circa divisionem quadratorum per numeros primos . . 497
Opuscula analytica 1, 1783, p. 64—84

554. Disquisitio accuratior circa residua ex divisione quadratorum altiorumque potestatum per numeros primos relicta 513
Opuscula analytica 1, 1783, p. 121—156

Druck von B. G. Teubner in Leipzig.

DE NUMERIS PRIMIS VALDE MAGNIS[1])

Commentatio 283 indicis Enestroemiani
Novi commentarii academiae scientiarum Petropolitanae 9 (1762/3), 1764, p. 99—153
Summarium ibidem p. 16—18

SUMMARIUM

Cum primum a Pellio[2]) ac deinceps ab aliis tabula numerorum primorum ad centena millia usque sit constructa, nunc quidem proposito quocunque numero hunc limitem non superante facillime iudicare licet, utrum is sit primus necne. Atque adeo ex ista tabula pro lubitu numeri primi excerpi possunt, si forte usus exigat, qui quidem centena millia non excedant. Verum si quis desideret numeros primos hoc termino maiores, nonnisi exantlato immenso fere labore voti sui compos reddi poterit, quandoquidem alia methodus numeros primos investigandi vix patet, nisi ut successive omnes numeri per alios minores divisibiles expungantur, quippe quo facto numeri primi soli relinquentur. Quin etiam proposito numero praegrandi, utrum is sit primus necne, ante pronunciare non licet, quam eius divisio per omnes numeros primos eius radice quadrata minores fuerit tentata. Ita si quis quaerat, utrum hic numerus 2237791 primus sit necne, divisionem per omnes numeros primos usque ad 1496 tentare cogitur hocque labore maxime taedioso suscepto tandem divisionem per 1481 succedere deprehendet. Ex quo patet problema olim inter Fermatium[3]) et Wallisium tractatum, quo methodus certa requiritur numeros primos dato quovis maiores investigandi, maxime esse arduum atque adeo vires ingenii humani superare, postquam solutio a Fermatio tradita iam olim ab Auctore huius dissertationis est profligata.[4]) Quin etiam quaestio iam maxime difficilis est reputanda, si numeri primi centenis millibus

1) Vide etiam Commentationes 369, 461, 467, 498, 708a huius voluminis. F. R.
2) Vide notam 3 p. 104 voluminis praecedentis. F. R.
3) Vide notam 1 p. 3. F. R. 4) Vide notam 2 p. 3. F. R.

vel adeo uno millione maiores desiderentur. Interim tamen in hac dissertatione methodus satis expedita traditur hoc praestandi, dum Auctor alios numeros non contemplatur, nisi qui unitate superent quadratos seu in hac forma $aa + 1$ sint contenti. Cum enim huiusmodi numeri alios divisores non recipiant, nisi qui ipsi sint duorum quadratorum aggregata atque adeo in hac forma $4m + 1$ contineantur, ex serie numerorum formae $aa + 1$ quamvis longe continuata, quae quidem series mox ad maximos numeros excrescit, facili negotio numeri compositi expunguntur, ita ut de relictis certi simus eos esse primos. Huius igitur artificii beneficio labore non nimis operoso omnes numeros primos formae $aa + 1$ ultra binos milliones est adeptus, quos in tabula peculiari complexus est; unde iam certo constat hunc verbi gratia numerum praegrandem 2232037 esse primum, quae veritas si more consueto esset exploranda, divisionem per omnes numeros primos usque ad 1494 tentari oporteret. Quo autem multitudo huiusmodi grandium numerorum primorum magis augeatur, etiam eos casus indicat, quibus formulae $\frac{aa+1}{2}$ et $\frac{aa+1}{5}$ praebent numeros primos.

Vix ullus reperietur Geometra, qui non ordinem numerorum primorum investigando haud parum temporis inutiliter consumserit; videtur enim lex, qua numeri primi progrediuntur, in Arithmetica aeque abstrusae esse indaginis atque in Geometria circuli quadratura; ac si huius indagatio pro desperata est habenda, non leviores adsunt rationes, quae et ordinis, quo numeri primi se invicem sequuntur, cognitionem nos in perpetuum fugere persuadent. Cum deinde etiam circuli quadratura, quamvis innotesceret, vix quicquam utilitatis allatura perhibeatur, eodem iure negare licebit ex ordine numerorum primorum perspecto ullum usum esse redundaturum. Verumtamen nemo facile dubitabit, quin methodus ipsa, quae nos vel ad circuli quadraturam vel ad legem progressionis numerorum primorum manuduceret, quoniam hae res tam diu frustra sunt anquisitae, eximium usum sit praestatura, propterea quod maxima impedimenta, quibus hae investigationes adhuc fuerunt implicatae, feliciter superaverit, ita ut inde omni iure summa subsidia per totam Mathesin nobis polliceri possemus. Haec ideo monenda duxi, ne quis eos, qui forte in hoc studio desudaverint, etiamsi operam perdiderint, reprehendendos censeat. Ac profecto natura numerorum primorum, cum ex iis modo tam admirabili omnes numeri componantur, per se praeclarissima videtur, et quo magis adhuc in proprietates, quibus sunt praeditae, penetrare licuit, eo magis haec doctrina digna censeri debet, cui excolendae plus operae tribuatur, quam nunc quidem plerumque fieri solet.

In hoc autem studii genere imprimis excelluit acutissimus quondam FERMATIUS, cui plurimae insignes numerorum proprietates acceptae sunt referendae; neque parum est dolendum, quod eius scripta post mortem ita interciderint, ut plurimorum theorematum demonstrationes, quas se adinvenisse asseveraverat, adhuc nobis sint ignotae. Hic perspicacissimus vir in doctrina numerorum primorum etiam non mediocriter laboravit atque problema se dignissimum olim WALLISIO proposuerat, quo modum requirebat numerum primum dato quovis numero maiorem assignandi.[1]) Credebat quidem FERMATIUS se huius problematis solutionem in potestate habere, dum affirmaverat omnes numeros in hac forma $2^n + 1$ contentos, siquidem exponens n ipse fuerit potestas binarii, esse numeros primos. Verumtamen eo erat candore, ut negaret se huius asserti demonstrationem habere, etiamsi de eius veritate minime dubitaret. Perspicuum autem est, si haec forma $2^n + 1$ sumendo pro n quasvis binarii potestates semper numeros primos exhiberet, problema propositum perfecte fore solutum. Quocunque enim numero proposito non solum una, sed innumerabiles potestates binarii assignari poterunt, quae loco exponentis n positae praebiturae sint potestates 2^n dato illo numero maiores; ad quas si unitas adiiceretur, haberentur utique totidem numeri primi dato illo numero maiores. Hanc autem regulam a FERMATIO prolatam veritati non esse consentaneam iam ante plures annos animadverti.[2]) Cum enim pro omnibus casibus inter centena millia subsistentibus satisfaceret, qui sunt

$$2^1 + 1 = 3, \quad 2^2 + 1 = 5, \quad 2^4 + 1 = 17, \quad 2^8 + 1 = 257, \quad 2^{16} + 1 = 65537,$$

statim sequentem casum $2^{32} + 1 = 4294967297$ non esse primum inveni, sed divisibilem per numerum 641. Quare cum etiam de sequentibus maioribus numeris ex hac formula natis incerti simus, utrum sint primi necne, hinc nihil plane adiumenti consequimur ad problema memoratum solvendum. Ac primo quidem nullum est dubium, quin proposito numero quantumvis magno infiniti adeo existant numeri primi illo maiores, postquam iam ab EUCLIDE[3]) est demonstratum omnium numerorum primorum multitudinem esse infinitam,

1) Vide EULERI Commentationem 26 (indicis ENESTROEMIANI): *Observationes de theoremate quodam FERMATIANO aliisque ad numeros primos spectantibus*, Comment. acad. sc. Petrop. 6 (1732/3), 1738, p. 103; *LEONHARDI EULERI Opera omnia*, series I, vol. 2, p. 1, imprimis notas p. 2. F. R.

2) Scilicet in Commentatione 26 nota praecedente laudata. F. R.

3) EUCLIDIS *Elementa* (ed. I. L. HEIBERG), vol. II, lib. IX prop. 20. F. R.

etiamsi, ut ego ostendi[1]), haec numerorum primorum multitudo se habeat ad multitudinem omnium prorsus numerorum, ut unitas ad infinitum seu potius ut logarithmus numeri infiniti ad ipsum hunc numerum infinitum, quod posterius infinitum maius est quam potestas quantumvis magna illius infiniti.[2])

Solutionis quidem huius problematis compotes fieremus, si loco formulae $2^n + 1$ aliam formulam indefinitam detegere liceret, quae nonnisi numeros primos complecteretur; sed etiamsi fortasse talis reperiatur, quae vel centum numeros primos suppeditaret, tamen ei aeque parum confidere possemus pro sequentibus, nisi forte, quod autem vix est expectandum, firma demonstratio exhiberi queat. Nulla certe progressio algebraica datur, cuius omnes plane termini in infinitum crescentes futuri sint numeri primi. Sumto enim termino quocunque inter sequentes semper infiniti termini eiusdem seriei assignari poterunt, quae omnes per illum dividi queant, quod Theorema[3]) ita demonstro.

THEOREMA

Nulla datur progressio algebraica, cuius omnes termini sint numeri primi.

DEMONSTRATIO

Cum progressio sit algebraica, posito eius termino indici x respondente $= X$ erit

$$X = \alpha + \beta x + \gamma x^2 + \delta x^3 + \varepsilon x^4 + \zeta x^5 + \eta x^6 + \text{etc.}$$

---

1) Vide EULERI Commentationem 72 (indicis ENESTROEMIANI): *Variae observationes circa series infinitas*, Comment. acad. sc. Petrop. 9 (1737), 1744, p. 160, imprimis p. 174; *LEONHARDI EULERI Opera omnia*, series I, vol. 14. Vide etiam observationes Celeb. G. ENESTROEM, Biblioth. Mathem. 13_3, 1912/3, p. 81. F. R.

2) EULERUS credidisse videtur multitudinem numerorum primorum minorum numero permagno n aequari logarithmo numeri n, cum revera haec multitudo crescente n expressione $n:ln$ exhibeatur. Vide etiam epistolam ab EULERO d. 28. Oct. 1752 ad CHR. GOLDBACH scriptam, *Correspondance math. et phys. publiée par P. H. FUSS*, St.-Pétersbourg 1843, t. I, p. 586; *LEONHARDI EULERI Opera omnia*, series III. F. R.

3) Hoc theorema CHR. GOLDBACH anno 1743 cum EULERO communicaverat; vide *Correspondance math. et phys. publiée par P. H. FUSS*, St.-Pétersbourg 1843, t. I, p. 257. Quod EULERI memoriae excidisse videtur, cum anno 1752 idem theorema GOLDBACHIO proposuerit (vide etiam eodem loco p. 589 nec non p. 595); *LEONHARDI EULERI Opera omnia*, series III. F. R.

Posito ergo termino indici a respondente $= A$, ut sit

$$A = \alpha + \beta a + \gamma a^2 + \delta a^3 + \varepsilon a^4 + \zeta a^5 + \eta a^6 + \text{etc.},$$

si capiatur $x = nA + a$, fiet terminus isti indici respondens X utique per A divisibilis. Omnes ergo progressionis propositae termini, qui indicibus in hac forma $nA + a$ contentis respondent, non erunt numeri primi[1]) neque ergo ulla huiusmodi progressio meros numeros primos complectetur. Q. E. D.

Verum etiamsi non omnes termini huiusmodi progressionis sint numeri primi, problemati tamen satisfieri possit, si modo inter eos infiniti dentur numeri primi, quorum indices certo quodam modo dignoscere liceret; veluti si eiusmodi daretur progressio, cuius omnes termini, quorum indices sunt numeri primi, ipsi essent numeri primi. Sed hoc modo quaerenda esset eiusmodi functio ipsius x, quae, quoties x fuerit numerus primus, ipsa quoque foret numerus primus, vel, quod eodem redit, regula desideraretur, cuius ope ex quovis numero primo proposito inveniri posset novus numerus primus. At huiusmodi regulam profundissimae esse indaginis quilibet in huiusmodi investigationibus vel leviter versatus facile agnoscet, ita ut hinc nulla plane spes affulgeat unquam ad solutionem allati problematis FERMATIANI perveniendi.

Certum igitur est in hoc problemate nihil adhuc esse praestitum, postquam ipsius FERMATII conatus successu sint destituti. Atque adeo, cum tabula numerorum primorum nondum ultra centena millia habeatur extensa, problema sane iam non parum foret difficile, si modo numeri primi quaerantur, qui sint centenis millibus maiores, vel, cum nuper prodierit tabula numerorum primorum usque ad 101000 excurrens[2]), si numeri primi quaerantur hunc terminum superantes. Neque enim ad hoc saltem problema solvendum alia via patere videtur, nisi ut more sólito ex numeris ultra 101000 notatis omnes compositi expungantur, hoc est, omnes, qui per ullum numerum primum radice quadrata minorem divisibiles deprehendentur; qui numeri enim his expunctis relinquentur, erunt numeri primi. Haec autem operatio instituenda plane foret eadem ratione, ac si ipsam tabulam numerorum primorum ad ulteriores limites continuare vellemus; quod opus propterea esset immensi laboris. Quodsi autem quis forte hunc laborem susciperet, certe non esset

1) Fieri quidem potest, ut sit $X = A$, quo casu haec EULERI assertio non valet. Ita si sit $X = 7 - 5x + x^2$, posito $a = 1$ erit $A = 3$, posito autem $x = 1 \cdot 3 + 1 = 4$ fiet etiam $X = 3$ numero primo. F. R.

2) Scilicet tabula, quam J. G. KRÜGER communicavit in libro *Gedancken von der Algebra*, Halle 1746. Vide notam 3 p. 104 voluminis praecedentis. F. R.

expectandum, ut ultra millionem a quoquam produceretur, eoque exantlato omnino impossibile videretur ullum numerum primum exhibere, qui esset millione maior.

Occurrit autem mihi methodus peculiaris, ex qua per calculum non admodum taediosum plures sum adeptus numeros non solum centies millibus, sed etiam millione maiores, quos esse primos certo asseverare possum. Quoniam igitur in tam ardua investigatione leviores successus non sunt contemnendi, haud inutile fore spero, si isthanc methodum meam exposuero, praesertim cum ipsa ex proprietatibus numerorum non spernendis sit derivata, quae etiam in aliis investigationibus usum insignem habere posse videntur.

Deductus autem sum ad hanc methodum per considerationem numerorum quadratorum unitate auctorum seu in hac formula $aa + 1$ contentorum, in quibus, siquidem a sit numerus par, plures numeros primos occurrere manifestum est; sin autem a sit numerus impar, semissis illius formulae $\frac{1}{2}(aa + 1)$ plurimos quoque suppeditat numeros primos. Quaesivi ergo omnes divisores numerorum in hac forma $aa + 1$ contentorum, qui labor non adeo erat taediosus, cum non opus esset divisionem per omnes numeros primos radice a minores tentare, propterea quod demonstravi, atque id quidem post FERMATIUM, cuius autem demonstratio pro deperdita est habenda, huiusmodi numeros $aa + 1$ alios divisores non admittere, nisi qui ipsi sint summae duorum quadratorum.[1]) Quare si numerus in hac forma $aa + 1$ contentus habeat divisores, certo scio hos divisores singulos in forma $pp + qq$ esse contentos. Cum deinde omnes numeri primi formae $4n + 1$ sint summae duorum quadratorum,[2]) numerorum autem primorum formae $4n - 1$ nullus sit duorum quadratorum summa, nullus certe numerus formae $4n - 1$ erit divisor formae $aa + 1$, sed si ea habeat divisores primos, eos in hac forma $4n + 1$ contineri necesse est.[3]) Consideravi itaque omnes numeros primos formae $4n + 1$ et ea quadrata primum investigavi, quae unitate aucta essent per quemvis horum numerorum

1) Vide EULERI Commentationem 228 (indicis ENESTROEMIANI): *De numeris, qui sunt aggregata duorum quadratorum,* Novi comment. acad. sc. Petrop. 4 (1752/3), 1758, p. 3, imprimis § 22; *LEONHARDI EULERI Opera omnia*, series I, vol. 2, p. 295. F. R.

2) Vide EULERI Commentationem 241 (indicis ENESTROEMIANI): *Demonstratio theorematis FERMATIANI omnem numerum primum formae $4n + 1$ esse summam duorum quadratorum*, Novi Comment. acad. sc. Petrop. 5 (1754/5), 1760, p. 3; *LEONHARDI EULERI Opera omnia*, series I, vol. 2, p. 328. F. R.

3) Vide EULERI Commentationem 134 (indicis ENESTROEMIANI): *Theoremata circa divisores numerorum*, Novi comment. acad. sc. Petrop. 1 (1747/8), 1750, p. 20, imprimis § 16—20; *LEONHARDI EULERI Opera omnia*, series I, vol. 2, p. 62. F. R.

primorum divisibilia, quo pacto omnes numeros formae $aa+1$ sum adeptus, qui non sunt numeri primi; reliquos ergo necessario primos esse oportet. Primum autem manifestum est per binarium, qui est etiam summa duorum quadratorum, formam $aa+1$ esse divisibilem, quoties a fuerit numerus impar. Superest ergo, ut ii ipsius a valores indagentur, qui reddant formam $aa+1$ divisibilem per quemquam horum numerorum primorum 5, 13, 17, 29, 37, 41 etc., qui ipsi sint duorum quadratorum summae; quem in finem praemitto sequens problema.

PROBLEMA 1

Proposito numero primo formae $4n+1$ *invenire omnia quadrata, quae unitate aucta per illum sunt divisibilia.*[1])

SOLUTIO

Cum iste numerus primus sit summa duorum quadratorum, sit $4n+1=p^2+q^2$, quadratum vero unitate auctum per illum divisibile sit $aa+1$. Demonstravi[2]) autem, quando summa duorum quadratorum, veluti $aa+bb$, divisibilis est per numerum primum $pp+qq$, semper dari duos huiusmodi numeros r et s, ut sit $a=pr+qs$ et $b=ps-qr$. Nostro casu ergo cum sit $bb=1$, necesse est, ut sit $ps-qr=\pm 1$, unde perspicitur fractiones $\frac{p}{q}$ et $\frac{r}{s}$ proxime inter se convenire, ita ut earum differentia $\frac{ps-qr}{qs}$ minorem numeratorem, unitate quippe aequalem, habere nequeat. Quare cum numeri p et q ex aequalitate $4n+1=pp+qq$ sint cogniti, formetur fractio $\frac{p}{q}$ quaeraturque in numeris minoribus fractio $\frac{r}{s}$ illi proxime aequalis, ut partibus per crucem multiplicatis productorum ps et qr differentia sit $=1$, id quod methodo a me alibi[3]) exposita facile fiet; tum ad fractionem $\frac{p}{q}$ in-

1) Hoc problema EULERUS iam in epistola d. 9. Iulii 1743 ad CHR. GOLDBACH scripta pertractavit, *Correspondance math. et phys. publiée par P. H. Fuss*, St.-Pétersbourg 1843, t. I, p. 237 (vide etiam eodem loco p. 299, 305, 587); *LEONHARDI EULERI Opera omnia*, series III. F. R.

2) Vide § 8 Commentationis 228 supra, p. 6, laudatae. F. R.

3) Vide Commentationem 71 (indicis ENESTROEMIANI): *De fractionibus continuis*, Comment. acad. sc. Petrop. 9 (1737), 1744, p. 98, imprimis § 14; *LEONHARDI EULERI Opera omnia*, series I, vol. 14. Vide etiam EULERI *Introductionem in analysin infinitorum*, Lausannae 1748, t. I cap. XVII, imprimis § 382; *LEONHARDI EULERI Opera omnia*, series I, vol. 8.

Problema, de quo hic agitur, WALLISIUS olim proposuit atque „magno studio pertractavit, solutionem vero dedit vehementer operosam atque difficilem“ (Commentatio 71, § 14). Vide J. WALLIS, *A Treatise of Algebra*, London 1685, chap. X; *Opera* t. II, Oxoniae 1693, p. 40. F. R.

venta hac fractione $\frac{r}{s}$ erit quadrati unius quaesiti radix $a = pr + qs$ vel etiam $a = -pr - qs$. Tum vero si multiplum quodcunque divisoris $4n + 1$ addatur, habebitur quoque valor idoneus pro a. Generatim ergo erit

$$a = m(4n + 1) \pm (pr + qs),$$

in qua forma continentur radices omnium quadratorum, quae unitate aucta per numerum primum propositum $4n + 1$ sunt divisibilia. Q. E. I.

SCHOLION 1

Quemadmodum autem data fractione $\frac{p}{q}$ aliam fractionem $\frac{r}{s}$ inveniri conveniat, quae ab illa tam parum discrepet, ut producta per crucem orta ps et qr unitate tantum differant, alio loco ostendi. Scilicet pro numeris p et q eadem operatio institui debet, quae vulgo ad eorum maximum communem divisorem inveniendum institui solet, tum ex quotis ordine scriptis formentur fractiones, quales ex fractionibus continuis prodeunt, earumque ultima erit ipsa fractio $\frac{p}{q}$, penultima autem pro $\frac{r}{s}$ assumi poterit eritque differentia inter producta ps et qr unitati aequalis, propterea quod numeri p et q erunt inter se primi, quoniam alias numerus $4n + 1 = pp + qq$ non foret primus. Inventa autem fractione $\frac{r}{s}$ manifestum est eius loco quoque assumi posse has fractiones $\frac{p+r}{q+s}$, $\frac{2p+r}{2q+s}$ et in genere $\frac{mp+r}{mq+s}$; nam et haec fractio cum fractione $\frac{p}{q}$ comparata dat producta per crucem $mpq + qr$ et $mpq + ps$ unitate differentia. Quodsi autem fractioni $\frac{p}{q}$ haec $\frac{mp+r}{mq+s}$ adiungatur, ex iis pro radice quadrati quaesiti obtinetur $a = mpp + pr + mqq + qs = m(4n + 1) + pr + qs$ ob $pp + qq = 4n + 1$ seu, cum numeri r et s quoque negative accipi queant, $a = m(4n + 1) \pm (pr + qs)$, quae est ipsa forma generalis in solutione inventa. Verum haec operatio commodissime per exempla docebitur.

EXEMPLUM 1

Invenire omnia quadrata, quae unitate aucta sint per numerum primum 29 *divisibilia.*

Sit a radix quadrata ex quadratis quaesitis, et cum 29 sit numerus primus formae $4n + 1$, erit certe summa duorum quadratorum, quae sunt 25 et 4, ita ut ob $29 = pp + qq = 5^2 + 2^2$ sit $p = 5$ et $q = 2$, unde formatur ista

fractio $\frac{p}{q} = \frac{5}{2}$. Nunc inter numeros 5 et 2 instituatur operatio ad maximum communem divisorem investigandum, quae ita se habebit:

$$\begin{array}{l} 2)\ 5\ (2 \\ \quad\ \underline{4} \\ 1)\ 2\ (2 \\ \quad\ \underline{2} \\ \quad\ 0 \end{array}$$

Sunt ergo quoti 2 et 2, ex quibus formantur fractiones sequenti modo

$$\begin{array}{cccc} 2, & 2 & & \\ \frac{1}{0}, & \frac{2}{1}, & \frac{5}{2}, & \end{array}$$

eritque penultima $\frac{2}{1} = \frac{r}{s}$; ex his autem duabus ultimis fractionibus $\frac{2}{1}$ et $\frac{5}{2}$ valor idoneus pro a erit productum numeratorum $2 \cdot 5 = 10$ auctum producto denominatorum $1 \cdot 2 = 2$, unde erit $a = 10 + 2 = 12$ et in genere

$$a = 29m \pm 12;$$

omniumque horum numerorum quadrata unitate aucta per 29 erunt divisibilia. Quare omnes valores ipsius a in his duabus progressionibus arithmeticis continebuntur:

12, 41, 70, 99, 128, 157, 186, 215, 244, 273 etc.,

17, 46, 75, 104, 133, 162, 191, 220, 249, 278 etc.

EXEMPLUM 2

Invenire omnia quadrata, quae unitate aucta fiant per numerum primum 617 *divisibilia.*

Cum sit $617 = 16^2 + 19^2$, statuatur $p = 19$ et $q = 16$ fiatque inter numeros 16 et 19 haec operatio:

$$\begin{array}{l} 16)\ 19\ (1 \\ \quad\ \underline{16} \\ 3)\ 16\ (5 \\ \quad\ \underline{15} \\ 1)\ 3\ (3 \\ \quad\ \underline{3} \\ \quad\ 0 \end{array}$$

Ex quotis 1, 5, 3 sequentes formentur fractiones

$$1,\quad 5,\quad 3$$

$$\frac{1}{0}',\quad \frac{1}{1}',\quad \frac{6}{5}',\quad \frac{19}{16}',$$

quarum binae postremae dant numeratorum productum = 114, at denominatorum productum = 80, unde idoneus isque minimus valor ipsius a erit = 194 et generatim

$$a = 617m \pm 194.$$

Omnes ergo ipsius a valores in duabus sequentibus progressionibus arithmeticis comprehenduntur:

194, 811, 1428, 2045, 2662, 3279 etc.,

423, 1040, 1657, 2274, 2891, 3508 etc.

EXEMPLUM 3

Invenire omnia quadrata, quae unitate aucta sint per numerum primum 1709 *divisibilia.*

Cum sit $1709 = 22^2 + 35^2$, inter numeros 22 et 35 sequens instituatur operatio

$$\begin{array}{l} 22)\ 35\ (1 \\ \underline{22} \\ 13)\ 22\ (1 \\ \underline{13} \\ 9)\ 13\ (1 \\ \underline{9} \\ 4)\ 9\ (2 \\ \underline{8} \\ 1)\ 4\ (4 \\ \underline{4} \\ 0 \end{array}$$

et ex quotis 1, 1, 1, 2, 4 formentur sequentes fractiones

$$\begin{array}{cccccc} 1, & 1, & 1, & 2, & 4 & \\ \frac{1}{0}, & \frac{1}{1}, & \frac{2}{1}, & \frac{3}{2}, & \frac{8}{5}, & \frac{35}{22}, \end{array}$$

quarum duae ultimae dabunt pro uno ipsius a valore $a = 8 \cdot 35 + 5 \cdot 22 = 390$, ita ut omnes ipsius a valores satisfacientes sint

$$a = 1709m \pm 390.$$

COROLLARIUM 1

Si numerus primus $4n + 1$ fuerit ipse quadratum unitate auctum, veluti $4n + 1 = p^2 + 1$, tum ob $q = 1$ sequens operatio erit instituenda:

$$\begin{array}{l} 1)\ p\ (p \\ \underline{p} \\ 0 \end{array}$$

Unicus ergo habetur quotus p, ex quo nascentur fractiones

$$\begin{array}{cc} & p \\ \frac{1}{0}, & \frac{p}{1}, \end{array}$$

unde fit $a = 1 \cdot p + 0 \cdot 1 = p$ et generatim

$$a = m(4n + 1) \pm p.$$

COROLLARIUM 2

Si amborum quadratorum, quorum summae numerus primus $4n + 1$ aequatur, radices unitate differant, ut sit $4n + 1 = pp + (p - 1)^2$, tum ob $q = p - 1$ sequens habebitur operatio:

$$\begin{array}{l} p-1)\ p\quad (1 \\ \quad \underline{p-1} \\ \qquad 1)\ p-1\ (p-1 \\ \qquad\quad \underline{p-1} \\ \qquad\qquad 0 \end{array}$$

Quoti ergo 1 et $p-1$ has dabunt fractiones

$$\begin{matrix} 1, & p-1 \\ \frac{1}{0}, & \frac{1}{1}, \quad \frac{p}{p-1}, \end{matrix}$$

unde fit $a = 1 \cdot p + 1 \cdot (p-1) = 2p-1$ et in genere

$$a = (4n+1)m \pm (2p-1).$$

COROLLARIUM 3

Si quaerantur omnia quadrata, quae unitate aucta sint per numerum primum $2 = 1+1$ divisibilia, etsi 2 non est formae $4n+1$, tamen, quia $p = 1$ et $q = 1$, erit primo $a = 1$ per Corollarium 1 hincque in genere

$$a = 2m \pm 1.$$

Unde sequitur, quod per se est manifestum, omnia quadrata numerorum imparium, si unitas addatur, fore per 2 divisibilia.

SCHOLION 2

Secundum hanc ergo regulam omnes numeros primos formae $4n+1$ tractavi, et postquam singulos in summam duorum quadratorum converti, quod semper et quidem unico modo fieri potest, cuique formam generalem ipsius a, in qua radices omnium quadratorum, quae unitate aucta per quemque numerum primum sint divisibilia, [continentur,] adscripsi; unde sequens nata est tabula.

Tabula omnium numerorum a,

quorum quadrata unitate aucta $aa + 1$ sunt per quemlibet numerum primum formae $4n + 1$ divisibilia[1])

Numeri primi	Valor ipsius a
$2 = 1^2 + 1^2$	$a = 2m \pm 1$
$5 = 1^2 + 2^2$	$a = 5m \pm 2$
$13 = 2^2 + 3^2$	$a = 13m \pm 5$
$17 = 1^2 + 4^2$	$a = 17m \pm 4$
$29 = 2^2 + 5^2$	$a = 29m \pm 12$
$37 = 1^2 + 6^2$	$a = 37m \pm 6$
$41 = 4^2 + 5^2$	$a = 41m \pm 9$
$53 = 2^2 + 7^2$	$a = 53m \pm 23$
$61 = 5^2 + 6^2$	$a = 61m \pm 11$
$73 = 3^2 + 8^2$	$a = 73m \pm 27$
$89 = 5^2 + 8^2$	$a = 89m \pm 34$
$97 = 4^2 + 9^2$	$a = 97m \pm 22$
$101 = 1^2 + 10^2$	$a = 101m \pm 10$
$109 = 3^2 + 10^2$	$a = 109m \pm 33$
$113 = 7^2 + 8^2$	$a = 113m \pm 15$
$137 = 4^2 + 11^2$	$a = 137m \pm 37$
$149 = 7^2 + 10^2$	$a = 149m \pm 44$
$157 = 6^2 + 11^2$	$a = 157m \pm 28$
$173 = 2^2 + 13^2$	$a = 173m \pm 80$
$181 = 9^2 + 10^2$	$a = 181m \pm 19$
$193 = 7^2 + 12^2$	$a = 193m \pm 81$
$197 = 1^2 + 14^2$	$a = 197m \pm 14$
$229 = 2^2 + 15^2$	$a = 229m \pm 107$
$233 = 8^2 + 13^2$	$a = 233m \pm 89$

1) In editione principe haec tabula nonnullos errores continet, qui omnes fere etiam in *Comment. arithm.* (ed. P. H. et N. Fuss; vide *Proocmium* voluminis praecedentis, p. VIII) inveniuntur, hac in editione autem correcti sunt. Quae correctiones pertinent ad valores ipsius a numeris primis 641, 653, 1021, 1033 correspondentes atque ad compositionem numerorum 1381 et 1861. F. R.

Numeri primi	Valor ipsius a
$241 = 4^2 + 15^2$	$a = 241m \pm 64$
$257 = 1^2 + 16^2$	$a = 257m \pm 16$
$269 = 10^2 + 13^2$	$a = 269m \pm 82$
$277 = 9^2 + 14^2$	$a = 277m \pm 60$
$281 = 5^2 + 16^2$	$a = 281m \pm 53$
$293 = 2^2 + 17^2$	$a = 293m \pm 138$
$313 = 12^2 + 13^2$	$a = 313m \pm 25$
$317 = 11^2 + 14^2$	$a = 317m \pm 114$
$337 = 9^2 + 16^2$	$a = 337m \pm 148$
$349 = 5^2 + 18^2$	$a = 349m \pm 136$
$353 = 8^2 + 17^2$	$a = 353m \pm 42$
$373 = 7^2 + 18^2$	$a = 373m \pm 104$
$389 = 10^2 + 17^2$	$a = 389m \pm 115$
$397 = 6^2 + 19^2$	$a = 397m \pm 63$
$401 = 1^2 + 20^2$	$a = 401m \pm 20$
$409 = 3^2 + 20^2$	$a = 409m \pm 143$
$421 = 14^2 + 15^2$	$a = 421m \pm 29$
$433 = 12^2 + 17^2$	$a = 433m \pm 179$
$449 = 7^2 + 20^2$	$a = 449m \pm 67$
$457 = 4^2 + 21^2$	$a = 457m \pm 109$
$461 = 10^2 + 19^2$	$a = 461m \pm 48$
$509 = 5^2 + 22^2$	$a = 509m \pm 208$
$521 = 11^2 + 20^2$	$a = 521m \pm 235$
$541 = 10^2 + 21^2$	$a = 541m \pm 52$
$557 = 14^2 + 19^2$	$a = 557m \pm 118$
$569 = 13^2 + 20^2$	$a = 569m \pm 86$
$577 = 1^2 + 24^2$	$a = 577m \pm 24$
$593 = 8^2 + 23^2$	$a = 593m \pm 77$
$601 = 5^2 + 24^2$	$a = 601m \pm 125$
$613 = 17^2 + 18^2$	$a = 613m \pm 35$
$617 = 16^2 + 19^2$	$a = 617m \pm 194$
$641 = 4^2 + 25^2$	$a = 641m \pm 154$
$653 = 13^2 + 22^2$	$a = 653m \pm 149$

Numeri primi	Valor ipsius a
$661 = 6^2 + 25^2$	$a = 661m \pm 106$
$673 = 12^2 + 23^2$	$a = 673m \pm 58$
$677 = 1^2 + 26^2$	$a = 677m \pm 26$
$701 = 5^2 + 26^2$	$a = 701m \pm 135$
$709 = 15^2 + 22^2$	$a = 709m \pm 96$
$733 = 2^2 + 27^2$	$a = 733m \pm 353$
$757 = 9^2 + 26^2$	$a = 757m \pm 87$
$761 = 19^2 + 20^2$	$a = 761m \pm 39$
$769 = 12^2 + 25^2$	$a = 769m \pm 62$
$773 = 17^2 + 22^2$	$a = 773m \pm 317$
$797 = 11^2 + 26^2$	$a = 797m \pm 215$
$809 = 5^2 + 28^2$	$a = 809m \pm 318$
$821 = 14^2 + 25^2$	$a = 821m \pm 295$
$829 = 10^2 + 27^2$	$a = 829m \pm 246$
$853 = 18^2 + 23^2$	$a = 853m \pm 333$
$857 = 4^2 + 29^2$	$a = 857m \pm 207$
$877 = 6^2 + 29^2$	$a = 877m \pm 151$
$881 = 16^2 + 25^2$	$a = 881m \pm 387$
$929 = 20^2 + 23^2$	$a = 929m \pm 324$
$937 = 19^2 + 24^2$	$a = 937m \pm 196$
$941 = 10^2 + 29^2$	$a = 941m \pm 97$
$953 = 13^2 + 28^2$	$a = 953m \pm 442$
$977 = 4^2 + 31^2$	$a = 977m \pm 252$
$997 = 6^2 + 31^2$	$a = 997m \pm 161$
$1009 = 15^2 + 28^3$	$a = 1009m \pm 469$
$1013 = 22^2 + 23^2$	$a = 1013m \pm 45$
$1021 = 11^2 + 30^2$	$a = 1021m \pm 374$
$1033 = 3^2 + 32^2$	$a = 1033m \pm 355$
$1049 = 5^2 + 32^2$	$a = 1049m \pm 426$
$1061 = 10^2 + 31^2$	$a = 1061m \pm 103$
$1069 = 13^2 + 30^2$	$a = 1069m \pm 249$
$1093 = 2^2 + 33^2$	$a = 1093m \pm 530$
$1097 = 16^2 + 29^2$	$a = 1097m \pm 341$

Numeri primi	Valor ipsius a
$1109 = 22^2 + 25^2$	$a = 1109m \pm 354$
$1117 = 21^2 + 26^2$	$a = 1117m \pm 214$
$1129 = 20^2 + 27^2$	$a = 1129m \pm 168$
$1153 = 8^2 + 33^2$	$a = 1153m \pm 140$
$1181 = 5^2 + 34^2$	$a = 1181m \pm 243$
$1193 = 13^2 + 32^2$	$a = 1193m \pm 186$
$1201 = 24^2 + 25^2$	$a = 1201m \pm 49$
$1213 = 22^2 + 27^2$	$a = 1213m \pm 495$
$1217 = 16^2 + 31^2$	$a = 1217m \pm 78$
$1229 = 2^2 + 35^2$	$a = 1229m \pm 597$
$1237 = 9^2 + 34^2$	$a = 1237m \pm 546$
$1249 = 15^2 + 32^2$	$a = 1249m \pm 585$
$1277 = 11^2 + 34^2$	$a = 1277m \pm 113$
$1289 = 8^2 + 35^2$	$a = 1289m \pm 479$
$1297 = 1^2 + 36^2$	$a = 1297m \pm 36$
$1301 = 25^2 + 26^2$	$a = 1301m \pm 51$
$1321 = 5^2 + 36^2$	$a = 1321m \pm 257$
$1361 = 20^2 + 31^2$	$a = 1361m \pm 614$
$1373 = 2^2 + 37^2$	$a = 1373m \pm 668$
$1381 = 15^2 + 34^2$	$a = 1381m \pm 366$ [1]
$1409 = 25^2 + 28^2$	$a = 1409m \pm 452$
$1429 = 23^2 + 30^2$	$a = 1429m \pm 620$
$1433 = 8^2 + 37^2$	$a = 1433m \pm 542$
$1453 = 3^2 + 38^2$	$a = 1453m \pm 497$
$1481 = 16^2 + 35^2$	$a = 1481m \pm 465$
$1489 = 20^2 + 33^2$	$a = 1489m \pm 225$
$1493 = 7^2 + 38^2$	$a = 1493m \pm 432$
$1549 = 18^2 + 35^2$	$a = 1549m \pm 88$
$1553 = 23^2 + 32^2$	$a = 1553m \pm 339$
$1597 = 21^2 + 34^2$	$a = 1597m \pm 610$

1) Omnes numeros, quorum quadrata unitate aucta per 1381 divisibilia sunt, in hac forma $1381m \pm 366$ contineri EULERUS uti exemplum iam in epistola ad Chr. GOLDBACH exposuit, quae nota 1 p. 7 laudata est. F. R.

Numeri primi	Valor ipsius a
$1601 = 1^2 + 40^2$	$a = 1601m \pm 40$
$1609 = 3^2 + 40^2$	$a = 1609m \pm 523$
$1613 = 13^2 + 38^2$	$a = 1613m \pm 127$
$1621 = 10^2 + 39^2$	$a = 1621m \pm 166$
$1637 = 26^2 + 31^2$	$a = 1637m \pm 316$
$1657 = 19^2 + 36^2$	$a = 1657m \pm 783$
$1669 = 15^2 + 38^2$	$a = 1669m \pm 220$
$1693 = 18^2 + 37^2$	$a = 1693m \pm 92$
$1697 = 4^2 + 41^2$	$a = 1697m \pm 414$
$1709 = 22^2 + 35^2$	$a = 1709m \pm 390$
$1721 = 11^2 + 40^2$	$a = 1721m \pm 473$
$1733 = 17^2 + 38^2$	$a = 1733m \pm 410$
$1741 = 29^2 + 30^2$	$a = 1741m \pm 59$
$1753 = 27^2 + 32^2$	$a = 1753m \pm 713$
$1777 = 16^2 + 39^2$	$a = 1777m \pm 775$
$1789 = 5^2 + 42^2$	$a = 1789m \pm 724$
$1801 = 24^2 + 35^2$	$a = 1801m \pm 824$
$1861 = 30^2 + 31^2$	$a = 1861m \pm 61$
$1873 = 28^2 + 33^2$	$a = 1873m \pm 737$
$1877 = 14^2 + 41^2$	$a = 1877m \pm 137$
$1889 = 17^2 + 40^2$	$a = 1889m \pm 331$
$1901 = 26^2 + 35^2$	$a = 1901m \pm 218$
$1913 = 8^2 + 43^2$	$a = 1913m \pm 712$
$1933 = 13^2 + 42^2$	$a = 1933m \pm 598$
$1949 = 10^2 + 43^2$	$a = 1949m \pm 589$
$1973 = 23^2 + 38^2$	$a = 1973m \pm 259$
$1993 = 12^2 + 43^2$	$a = 1993m \pm 834$
$1997 = 29^2 + 34^2$	$a = 1997m \pm 412$

Tabula ergo haec in se complectitur omnes numeros primos formae $4n + 1$ infra 2000 existentes eiusque ergo ope omnes numeri inveniri possunt, quorum quadrata unitate aucta per ullum horum numerorum primorum sint divisibilia. Eius ergo beneficio sequens solvi poterit problema.

PROBLEMA 2

Omnium numerorum, qui unitate excedunt numeros quadratos, assignare omnes divisores radicibus ipsorum quadratis minores.

SOLUTIO

Scribantur ordine omnes numeri ab unitate ad 2000, quandoquidem praecedens tabula ad hunc terminum est producta, qui littera a designentur, ita [ut] pro quovis numero inde nato $aa + 1$ divisores sint assignandi. Constat autem hos numeros alios non esse habituros divisores primos nisi formae $4n + 1$; praecedens vero tabula omnes numeros a exhibet, quorum quadrata unitate aucta sint per quemque numerum primum huius formae divisibilia. Verum pro quolibet numero $aa + 1$ sufficit notasse divisores primos radice a minores, quoniam his cognitis etiam divisores radice a maiores sponte innotescunt. Quamobrem singulis numeris a formae $2m \pm 1$ adscribatur binarius, quia eorum quadrata unitate aucta sunt per 2 divisibilia; tum numeris $a = 5m \pm 2$ adscribatur 5, numeris $a = 13m \pm 5$ adscribatur 13, numeris $a = 17m \pm 4$ adscribatur 17, et ita porro; ubi quidem valores ipsius a minores ipso numero primo proposito omittuntur, quia tantum de divisoribus ipso numero a minoribus quaeritur. Hoc ergo modo si ope tabulae praecedentis cuique numero a divisores convenientes adscribantur, obtinebuntur omnes divisores numeri $aa + 1$ ipsa radice a minores. Q. E. I.

COROLLARIUM 1

Si ergo hoc modo numeri a relinquentur, quibus nullus divisor fuerit adscriptus, hoc indicio erit numeros $aa + 1$ inde natos esse primos, nullos quippe divisores admittentes praeter unitatem et se ipsos. Quibus igitur numeris a in tabula hoc modo condita nullus divisor fuerit adscriptus, de iis certo affirmare poterimus eorum quadrata unitate aucta esse numeros primos.[1])

1) Vide tabulam p. 26—45. Ubi quidem notandum est EULERUM ipsum numeris $a = 1, 2, 4, 6, 10$ usque ad 66 integros valores $a^2 + 1 = 2, 5, 17, 37, 101, \ldots 4357$ adscripsisse, quamquam sunt numeri primi. Vide etiam notam 2 p. 21. F. R.

COROLLARIUM 2

Quoniam igitur haec tabula pro numeris a facile ad 2000 extenditur, numeri inde nati $aa+1$ ad 4000000 exsurgent; unde ista tabula omnes numeros primos formae $aa+1$ exhibebit, qui 4 milliones non superant, sicque ex ea numeri primi non solum centenis millibus, sed etiam uno millione maiores depromi poterunt.

COROLLARIUM 3

Quibus autem numeris a unicus divisor α fuerit adscriptus, numeri inde nati $aa+1$ praeter unitatem unicum habebunt hunc divisorem α radice a minorem; ideoque $\frac{aa+1}{\alpha}$ erit numerus primus. Ita quibus numeris a solus binarius fuerit adscriptus, ex iis certo hos obtinemus numeros primos $\frac{aa+1}{2}$; atque adeo ex ista tabula omnes numeri primi formae $\frac{aa+1}{2}$ limite 2000000 non maiores assignari poterunt.

COROLLARIUM 4

Simili modo omnes numeri a, quibus solus quinarius est adscriptus, praebebunt omnes numeros primos formae $\frac{aa+1}{5}$, qui infra limitem 800000 continentur. Atque omnes numeri a, qui tantum divisorem 13 habebunt adscriptum, praebebunt omnes numeros primos formae $\frac{aa+1}{13}$ infra limitem 307692 contentos.

COROLLARIUM 5

Qui autem numeri a duos tantum divisores α et β habebunt adscriptos, id indicio erit numeros $\frac{aa+1}{\alpha\beta}$ fore primos. Hinc quibus numeris a tantum duo divisores 2 et 5 fuerint adscripti, ex iis reperientur omnes numeri primi formae $\frac{aa+1}{10}$, qui quidem limitem 400000 non superabunt.

SCHOLION 1

Verum ut hae conclusiones sint certae, probe notandum est inter numeros $aa+1$, qui sunt per numerum primum $4n+1$ divisibiles, etiam eiusmodi numeros contineri, qui sint per quadratum $(4n+1)^2$ vel etiam per cubum

$(4n+1)^3$ altioresve potestates $(4n+1)^4$, $(4n+1)^5$ etc. divisibiles. Quod quoties accidit, numero a non solum divisor $4n+1$, sed eius summa potestas, per quam numerus $aa+1$ fuerit divisibilis, adscribi debebit, ut hoc modo omnes divisores primi numerorum $aa+1$ ipsa radice a minores obtineantur. Si quidem divisor fuerit $=2$, nulla eius altior potestas, veluti 4, 8, 16 etc., unquam numeri $aa+1$ divisor esse poterit, id quod per se est manifestum, cum existente a numero impari forma $aa+1$ sit numerus impariter par. At de numeris primis formae $4n+1$ dantur utique eiusmodi quadrata, quae unitate aucta sint per quamvis eorum potestatem divisibilia, quos idcirco investigari conveniet.

SCHOLION 2

Cum autem sit $4n+1=pp+qq$, erunt omnes quoque ipsius $4n+1$ potestates summae duorum quadratorum, et quidem pluribus modis, ex quibus vero id quadratorum par sumi conveniet, quorum radices sunt numeri primi inter se. Sic cum sit in genere $(pp+qq)(rr+ss)=(pr+qs)^2+(ps-qr)^2$, erit

$$(4n+1)^2=(pp+qq)^2=4ppqq+(pp-qq)^2,$$
$$(4n+1)^3=(pp+qq)^3=(p^3-3pqq)^2+(3ppq-q^3)^2,$$
$$(4n+1)^4=(pp+qq)^4=(p^4-6ppqq+q^4)^2+(4p^3q-4pq^3)^2.$$

Si simili modo quo ante valores ipsius a investigentur, conficietur pro potestatibus numerorum primorum, quae infra terminum 2000 continentur, sequens tabula.

Tabula omnium numerorum a,
quorum quadrata unitate aucta $aa+1$ sint per potestates numerorum primorum $4n+1$ divisibilia

Potestates numerorum primorum	Valor ipsius a
$5^2 = 3^2 + 4^2$	$a = 25\,m \pm 7$
$5^3 = 2^2 + 11^2$	$a = 125\,m \pm 57$
$5^4 = 7^2 + 24^2$	$a = 625\,m \pm 182$
$5^5 = 38^2 + 41^2$	$a = 3125\,m \pm 1068$
$13^2 = 5^2 + 12^2$	$a = 169\,m \pm 70$
$13^3 = 9^2 + 46^2$	$a = 2197\,m \pm 239$
$13^4 = 119^2 + 120^2$	$a = 13^4 m \pm 239$
$17^2 = 8^2 + 15^2$	$a = 289\,m \pm 38$
$17^3 = 47^2 + 52^2$	$a = 17^3 m \pm 1985$
$29^2 = 20^2 + 21^2$	$a = 841\,m \pm 41$
$37^2 = 12^2 + 35^2$	$a = 1369\,m \pm 117$
$41^2 = 9^2 + 40^2$	$a = 1681\,m \pm 378$
$53^2 = 28^2 + 45^2$	$a = 53^2 m \pm 500$
$61^2 = 11^2 + 60^2$	$a = 61^2 m \pm 682$
$73^2 = 48^2 + 55^2$	$a = 73^2 m \pm 776$
$89^2 = 39^2 + 80^2$	$a = 89^2 m \pm 3861$
$97^2 = 65^2 + 72^2$	$a = 97^2 m \pm 4052$
$101^2 = 20^2 + 99^2$	$a = 101^2 m \pm 515$
$109^2 = 60^2 + 91^2$	$a = 109^2 m \pm 5744$
$113^2 = 15^2 + 112^2$	$a = 113^2 m \pm 1710$
$137^2 = 88^2 + 105^2$	$a = 137^2 m \pm 6613$
$149^2 = 51^2 + 140^2$	$a = 149^2 m \pm 1744$
$197^2 = 28^2 + 195^2$ [1])	$a = 197^2 m \pm 1393$
$257^2 = 32^2 + 255^2$	$a = 257^2 m \pm 2072$

His itaque subsidiis hic subiunctam [2]) construxi tabulam, ex qua statim pro singulis numeris a omnes divisores formae $aa+1$ habentur. Hanc quidem

1) Editio princeps (nec non *Comment. arithm.*): $197^2 = 28^2 + 95^2$. Correxit F. R.

2) Vide p. 26. In editione principe haec quoque tabula permultos errores continet, qui omnes etiam in *Comment. arithm.* inveniuntur, hac in editione autem correcti sunt. Quae correctiones pertinent ad numeros $a = 457, 507, 553, 560, 693, 733, 737, 914, 1090, 1234, 1292, 1318, 1388, 1395$. F. R.

tabulam non ultra 1500 in radicibus continuavi, sed ope harum formularum facile ad 2000 usque progredi licebit.

Ex hac autem tabula iam plures numeri primi formae $aa+1$ desumi poterunt, qui non solum centenis millibus, sed etiam uno millione sint maiores; deinde etiam numeri primi formae $\frac{aa+1}{2}$ et $\frac{aa+1}{5}$ item $\frac{aa+1}{10}$, quos in sequentibus tabellis exhibebo.

Numeri primi formae $aa+1$[1])

Radices a	Numeri primi $aa+1$	Radices a	Numeri primi $aa+1$	Radices a	Numeri primi $aa+1$
1	2	146	21317	340	115601
2	5	150	22501	350	122501
4	17	156	24337	384	147457
6	37	160	25601	386	148997
10	101	170	28901	396	156817
14	197	176	30977	400	160001
16	257	180	32401	406	164837
20	401	184	33857	420	176401
24	577	204	41617	430	184901
26	677	206	42437	436	190097
36	1297	210	44101	440	193601
40	1601	224	50177	444	197137
54	2917	230	52901	464	215297
56	3137	236	55697	466	217157
66	4357	240	57601	470	220901
74	5477	250	62501	474	224677
84	7057	256	65537	490	240101
90	8101	260	67601	496	246017
94	8837	264	69697	536	287297
110	12101	270	72901	544	295937
116	13457	280	78401	556	309137
120	14401	284	80657	570	324901
124	15377	300	90001	576	331777
126	15877	306	93637	584	341057
130	16901	314	98597	594	352837
134	17957	326	106277	634	401957

1) Radices a huius tabulae EULERUS iam in epistola d. 28. Oct. 1752 scripta cum CHR. GOLDBACH communicavit, *Correspondance math. et phys. publiée par P. H Fuss*, St.-Pétersbourg, 1843, t. I, p. 586; *LEONHARDI EULERI Opera omnia*, series III. F. R.

Radices a	Numeri primi $aa+1$	Radices a	Numeri primi $aa+1$	Radices a	Numeri primi $aa+1$
636	404497	936	876097	1274	1623077
644	414737	946	894917	1276	1628177
646	417317	950	902501	1290	1664101
654	427717	960	921601	1294	1674437
674	454277	966	933157	1306	1705637
680	462401	986	972197	1314	1726597
686	470597	1004	1008017	1316	1731857
690	476101	1010	1020101	1320	1742401
696	484417	1036	1073297	1324	1752977
700	490001	1054	1110917	1340	1795601
704	495617	1060	1123601	1350	1822501
714	509797	1066	1136357	1354	1833317
716	512657	1070	1144901	1366	1865957
740	547601	1094	1196837	1374	1887877
750	562501	1096	1201217 [1])	1376	1893377
760	577601	1106	1223237	1394	1943237
764	583697	1124	1263377	1406	1976837
780	608401	1140	1299601	1410	1988101
784	614657	1144	1308737	1416	2005057
816	665857	1146	1313317	1420	2016401
826	682277	1150	1322501	1430	2044901
860	739601	1156	1336337	1434	2056357
864	746497	1174	1378277	1440	2073601
890	792101	1176	1382977	1456	2119937
906	820837	1184	1401857	1460	2131601
910	828101	1210	1464101 [2])	1494	2232037
920	846401	1244	1547537		
930	864901	1246	1552517		

Habentur ergo hic 109 numeri primi maiores quam 100000 et 48 numeri primi millionem superantes.

---

1) Numeros primos 1008017, 1020101, 1073297, 1110917, 1123601, 1136357, 1144901, 1196837, 1201217 uti millionem superantes EULERUS iam in epistola nota 1 p. 7 laudata cum CHR. GOLDBACH communicavit. F. R.

2) In editione principe (atque etiam in *Comment. arithm.*) hic sequitur numerus 1522757 ($= 1234^2 + 1$). Quem numerum utpote compositum delevi. Vide notam p. 42. F. R.

Praeterea autem plures numeri primi formarum $\frac{aa+1}{2}$, $\frac{aa+1}{5}$, $\frac{aa+1}{10}$ assignari possunt, qui etiam centena millia superant, ut ex sequentibus perspicere licet.

Valores numeri a, quibus forma $\frac{aa+1}{2}$ fit numerus primus

1, 3, 5, 9, 11, 15, 19, 25, 29, 35, 39, 45, 49, 51, 59, 61, 65, 69, 71, 79, 85, 95,
101, 121, 131, 139, 141, 145, 159, 165, 169, 171, 175, 181, 195, 199,
201, 205, 209, 219, 221, 231, 245, 261, 271, 275, 279, 289, 299,
309, 315, 321, 325, 329, 335, 345, 349, 371, 375, 379, 391, 399,
405, 409, 415, 425, 435, 441, 445, 449, 451, 459, 461, 471,
519, 521, 529, 535, 545, 559, 569, 571, 575, 579, 581, 595,
609, 631, 639, 641, 649, 661, 669, 685, 689, 695, 699,
711, 715, 739, 745, 751, 779, 781, 791, 799,
815, 819, 821, 841, 855, 861, 869, 875, 881, 885,
901, 909, 921, 925, 929, 935, 949, 951, 955, 959, 979, 981, 985, 989, 991,
1001, 1011, 1025, 1029, 1031, 1039, 1051, 1055, 1069, 1081, 1091, 1095, 1099,
1111, 1125, 1129, 1151, 1155, 1161, 1171, 1179, 1181, 1185, 1199,
1205, 1219, 1225, 1241, 1251, 1255, 1265, 1281, 1285, 1299,
1311, 1315, 1329, 1345, 1349, 1359, 1361, 1389, 1391,
1405, 1411, 1419, 1421, 1439, 1459, 1465, 1469, 1489, 1495, 1499.

Valores numeri a, quibus forma $\frac{aa+1}{5}$ fit numerus primus

2, 8, 12, 22, 28, 42, 48, 52, 58, 62, 78, 88, 92,
102, 108, 152, 158, 178, 188, 198,
202, 222, 238, 248, 258, 262, 272, 292, 298,
308, 312, 328, 352, 358, 362, 388,
402, 422, 428, 458, 462, 478, 488, 492,
508, 522, 558, 572, 588,
602, 622, 628, 638, 652, 662, 692, 698,
702, 728, 738, 758, 792,
828, 838, 842, 848, 862, 872, 898,

908, 912, 942, 962, 972, 978, 988,
1008, 1062, 1072, 1078, 1088,
1108, 1112, 1138, 1192,
1208, 1238, 1272, 1278, 1298,
1312, 1342, 1358, 1372, 1378,
1402, 1442, 1452, 1472, 1488, 1498.

Valores numeri a, quibus forma $\frac{aa+1}{10}$ fit numerus primus

3, 7, 13, 17, 23, 27, 33, 37, 53, 63, 67, 77, 87, 97,
103, 113, 127, 137, 147, 153, 163, 167, 197,
223, 227, 247, 263, 267, 277, 283, 287, 297,
303, 323, 347, 363, 367, 373, 383, 397,
417, 427, 433, 453,
503, 513, 517, 527, 533, 537, 547,[1]) 573, 587,
617, 627, 637, 653, 673, 677, 683,
753, 763, 773, 777, 797,
817, 823, 833, 847, 867, 873, 877, 883,
913, 917, 923, 927, 933, 937, 947, 953, 963, 997,
1047, 1053, 1063, 1073,
1103, 1117, 1137, 1147, 1163, 1167, 1173, 1187, 1197,
1213, 1233, 1247, 1273,
1337, 1367, 1377, 1387, 1397,
1413, 1417, 1423, 1447, 1473, 1497.

Hinc autem iterum 9 numeri primi supra 1000000 obtinentur, ex forma scilicet $\frac{aa+1}{2}$, quando $a > 1414$.

1) In editione principe (atque etiam in *Comment. arithm.*) hic sequitur numerus 553, quem numerum delevi, quia $\frac{553^2+1}{10}$ non est numerus primus. Vide notam p. 33. F. R.

a	Divisores ipsius $aa+1$	a	Divisores ipsius $aa+1$
1	2	39	$2 \cdot 761$
2	5	40	1601
3	$2 \cdot 5$	41	$2 \cdot 29^2$
4	17	42	$5 \cdot 353$
5	$2 \cdot 13$	43	$2 \cdot 5^2 \cdot 37$
6	37	44	$13 \cdot 149$
7	$2 \cdot 5^2$	45	$2 \cdot 1013$
8	$5 \cdot 13$	46	$29 \cdot 73$
9	$2 \cdot 41$	47	$2 \cdot 5 \cdot 13 \cdot 17$
10	101	48	$5 \cdot 461$
11	$2 \cdot 61$	49	$2 \cdot 1201$
12	$5 \cdot 29$	50	$41 \cdot 61$
13	$2 \cdot 5 \cdot 17$	51	$2 \cdot 1301$
14	197	52	$5 \cdot 541$
15	$2 \cdot 113$	53	$2 \cdot 5 \cdot 281$
16	257	54	2917
17	$2 \cdot 5 \cdot 29$	55	$2 \cdot 17 \cdot 89$
18	$5^3 \cdot 13$	56	3137
19	$2 \cdot 181$	57	$2 \cdot 5^3 \cdot 13$
20	401	58	$5 \cdot 673$
21	$2 \cdot 13 \cdot 17$	59	$2 \cdot 1714$
22	$5 \cdot 97$	60	$13 \cdot 277$
23	$2 \cdot 5 \cdot 53$	61	$2 \cdot 1861$
24	577	62	$5 \cdot 769$
25	$2 \cdot 313$	63	$2 \cdot 5 \cdot 397$
26	677	64	$17 \cdot 241$
27	$2 \cdot 5 \cdot 73$	65	$2 \cdot 2113$
28	$5 \cdot 157$	66	4357
29	$2 \cdot 421$	67	$2 \cdot 5 \cdot 449$
30	$17 \cdot 53$	68	$5^3 \cdot 37$
31	$2 \cdot 13 \cdot 37$	69	$2 \cdot 2381$
32	$5^2 \cdot 41$	70	$13^2 \cdot 29$
33	$2 \cdot 5 \cdot 109$	71	$2 \cdot 2521$
34	$13 \cdot 89$	72	$5 \cdot 17 \cdot 61$
35	$2 \cdot 613$	73	$2 \cdot 5 \cdot 13 \cdot 41$
36	1297	74	
37	$2 \cdot 5 \cdot 137$	75	$2 \cdot 29 \cdot 97$
38	$5 \cdot 17^2$	76	$53 \cdot 109$

a	Divisores ipsius $aa+1$	a	Divisores ipsius $aa+1$
77	$2\cdot5\cdot593$	115	$2\cdot17$
78	5	116	
79	2	117	$2\cdot5\cdot37^2$
80	$37\cdot173$	118	5^2
81	$2\cdot17$	119	$2\cdot73\cdot97$
82	$5^2\cdot193\cdot269$	120	
83	$2\cdot5\cdot13\cdot53$	121	2
84		122	$5\cdot13$
85	2	123	$2\cdot5\cdot17\cdot89$
86	$13\cdot569$	124	
87	$2\cdot5$	125	$2\cdot13$
88	5	126	
89	$2\cdot17\cdot233$	127	$2\cdot5$
90		128	$5\cdot29\cdot113$
91	$2\cdot41\cdot101$	129	$2\cdot53$
92	5	130	
93	$2\cdot5^2\cdot173$	131	2
94		132	$5^2\cdot17\cdot41$
95	2	133	$2\cdot5\cdot29\cdot61$
96	$13\cdot709$	134	
97	$2\cdot5$	135	$2\cdot13$
98	$5\cdot17\cdot113$	136	53
99	$2\cdot13^2\cdot29$	137	$2\cdot5$
100	$73\cdot137$	138	$5\cdot13$
101	2	139	2
102	5	140	17
103	$2\cdot5$	141	2
104	29	142	$5\cdot37\cdot109$
105	$2\cdot37$	143	$2\cdot5^2$
106	17	144	89
107	$2\cdot5^2$	145	2
108	5	146	
109	$2\cdot13$	147	$2\cdot5$
110		148	$5\cdot13$
111	$2\cdot61\cdot101$	149	$2\cdot17$
112	$5\cdot13$	150	
113	$2\cdot5$	151	$2\cdot13$
114	41	152	5

a	Divisores ipsius $aa+1$	a	Divisores ipsius $aa+1$
153	$2\cdot 5$	191	$2\cdot 17\cdot 29\cdot 37$
154	37	192	$5\cdot 73\cdot 101$
155	$2\cdot 41$	193	$2\cdot 5^3\cdot 149$
156		194	61
157	$2\cdot 5^2\cdot 17\cdot 29$	195	2
158	5	196	41
159	2	197	$2\cdot 5$
160		198	5
161	$2\cdot 13$	199	2
162	$5\cdot 29$	200	$13\cdot 17\cdot 181$
163	$2\cdot 5$	201	2
164	13	202	5
165	2	203	$2\cdot 5\cdot 13$
166	17	204	
167	$2\cdot 5$	205	2
168	5^2	206	
169	2	207	$2\cdot 5^2$
170		208	$5\cdot 17$
171	2	209	2
172	$5\cdot 61\cdot 97$	210	
173	$2\cdot 5\cdot 41\cdot 73$	211	$2\cdot 113\cdot 197$
174	$13\cdot 17\cdot 137$	212	$5\cdot 89\cdot 101$
175	2	213	$2\cdot 5\cdot 13$
176		214	41
177	$2\cdot 5\cdot 13$	215	$2\cdot 29$
178	5	216	$13\cdot 37\cdot 97$
179	$2\cdot 37$	217	$2\cdot 5\cdot 17$
180		218	5^2
181	2	219	2
182	$5^4\cdot 53$	220	29
183	$2\cdot 5\cdot 17$	221	2
184		222	5
185	$2\cdot 109\cdot 157$	223	$2\cdot 5$
186	29	224	
187	$2\cdot 5\cdot 13$	225	$2\cdot 17$
188	5	226	13
189	$2\cdot 53$	227	$2\cdot 5$
190	13	228	$5\cdot 37$

a	Divisores ipsius $aa+1$	a	Divisores ipsius $aa+1$
229	$2\cdot 13$	267	$2\cdot 5$
230		268	$5^2\cdot 13^2\cdot 17$
231	2	269	$2\cdot 97$
232	5^2	270	
233	$2\cdot 5\cdot 61\cdot 89$	271	2
234	17	272	5
235	$2\cdot 53$	273	$2\cdot 5\cdot 29\cdot 257$
236		274	193
237	$2\cdot 5\cdot 41\cdot 137$	275	2
238	5	276	17
239	$2\cdot 13^4$	277	$2\cdot 5$
240		278	$5\cdot 13\cdot 29\cdot 41$
241	$2\cdot 113$	279	2
242	$5\cdot 13\cdot 17\cdot 53$	280	
243	$2\cdot 5^2$	281	$2\cdot 13$
244	29	282	5^2
245	2	283	$2\cdot 5$
246	73	284	
247	$2\cdot 5$	285	$2\cdot 17$
248	5	286	157
249	$2\cdot 29$	287	$2\cdot 5$
250		288	$5\cdot 53$
251	$2\cdot 17^2\cdot 109$	289	2
252	$5\cdot 13$	290	37
253	$2\cdot 5\cdot 37\cdot 173$	291	$2\cdot 13$
254	149	292	5
255	$2\cdot 13\cdot 41\cdot 61$	293	$2\cdot 5^2\cdot 17\cdot 101$
256		294	$13\cdot 61\cdot 109$
257	$2\cdot 5^2$	295	$2\cdot 53$
258	5	296	41
259	$2\cdot 17$	297	$2\cdot 5$
260		298	5
261	2	299	2
262	5	300	
263	$2\cdot 5$	301	$2\cdot 89$
264		302	$5\cdot 17\cdot 29\cdot 37$
265	$2\cdot 13\cdot 37\cdot 73$	303	$2\cdot 5$
266	173	304	13

a	Divisores ipsius $aa+1$	a	Divisores ipsius $aa+1$
305	$2\cdot193\cdot241$	343	$2\cdot5^2\cdot13\cdot181$
306		344	17
307	$2\cdot5^3\cdot13\cdot29$	345	2
308	5	346	13
309	2	347	$2\cdot5$
310	17	348	$5\cdot53$
311	$2\cdot137$	349	2
312	5	350	
313	$2\cdot5\cdot97\cdot101$	351	$2\cdot229\cdot269$
314		352	5
315	2	353	$2\cdot5\cdot17$
316	61	354	113
317	$2\cdot5\cdot13$	355	$2\cdot61$
318	5^3	356	13
319	$2\cdot17\cdot41\cdot73$	357	$2\cdot5^2$
320	13	358	5
321	2	359	$2\cdot13$
322	$5\cdot89\cdot233$	360	$29\cdot41\cdot109$
323	$2\cdot5$	361	$2\cdot17$
324	113	362	5
325	2	363	$2\cdot5$
326		364	37
327	$2\cdot5\cdot17^2\cdot37$	365	$2\cdot29$
328	5	366	97
329	2	367	$2\cdot5$
330	13	368	5^2
331	$2\cdot29$	369	$2\cdot13$
332	5^2	370	17
333	$2\cdot5\cdot13$	371	2
334	281	372	$5\cdot13$
335	2	373	$2\cdot5$
336	$17\cdot229\cdot29$	374	137
337	$2\cdot5\cdot41\cdot277$	375	2
338	$5\cdot73\cdot313$	376	37
339	$2\cdot37$	377	$2\cdot5\cdot61\cdot233$
340		378	$5\cdot17\cdot41^2$
341	$2\cdot53$	379	2
342	$5\cdot149\cdot157$	380	197

a	Divisores ipsius $aa+1$	a	Divisores ipsius $aa+1$
381	$2\cdot181$	419	$2\cdot41$
382	$5^2\cdot13$	420	
383	$2\cdot5$	421	$2\cdot13\cdot17\cdot401$
384		422	5
385	$2\cdot13$	423	$2\cdot5\cdot29$
386		424	13
387	$2\cdot5\cdot17$	425	2
388	5	426	173
389	$2\cdot29$	427	$2\cdot5$
390	89	428	5
391	2	429	$2\cdot17$
392	$5\cdot73$	430	
393	$2\cdot5^2$	431	$2\cdot293\cdot317$
394	$29\cdot53\cdot101$	432	5^3
395	$2\cdot13\cdot17\cdot353$	433	$2\cdot5$
396		434	13
397	$2\cdot5$	435	2
398	$5\cdot13$	436	
399	2	437	$2\cdot5\cdot13^2\cdot113$
400		438	$5\cdot17\cdot37\cdot61$
401	$2\cdot37\cdot41\cdot53$	439	$2\cdot173$
402	5	440	
403	$2\cdot5\cdot109\cdot149$	441	2
404	17	442	$5\cdot41$
405	2	443	$2\cdot5^4\cdot157$
406		444	
407	$2\cdot5^2$	445	2
408	$5\cdot13^2\cdot197$	446	17
409	2	447	$2\cdot5\cdot13\cdot29\cdot53$
410	97	448	$5\cdot137\cdot293$
411	$2\cdot13\cdot73\cdot89$	449	2
412	$5\cdot17$	450	$13\cdot37\cdot421$
413	$2\cdot5\cdot37$	451	2
414	101	452	$5\cdot29$
415	2	453	$2\cdot5$
416	61	454	53
417	$2\cdot5$	455	$2\cdot17$
418	$5^2\cdot29\cdot241$	456	269

a	Divisores ipsius $aa+1$	a	Divisores ipsius $aa+1$
457	$2\cdot 5^2$	495	$2\cdot 101$
458	5	496	
459	2	497	$2\cdot 5\cdot 17$
460	$13\cdot 41\cdot 397$	498	$5\cdot 193\cdot 257$
461	2	499	$2\cdot 13\cdot 61\cdot 157$
462	5	500	$53^2\cdot 89$
463	$2\cdot 5\cdot 13\cdot 17\cdot 97$	501	$2\cdot 41$
464		502	$5\cdot 13$
465	$2\cdot 73$	503	$2\cdot 5$
466		504	389
467	$2\cdot 5\cdot 118\cdot 193$	505	$2\cdot 29$
468	5^3	506	17
469	$2\cdot 109$	507	$2\cdot 5^2\cdot 53\cdot 97$
470		508	5
471	2	509	$2\cdot 281\cdot 461$
472	$5\cdot 17$	510	29
473	$2\cdot 5\cdot 13$	511	$2\cdot 137$
474		512	$5\cdot 13\cdot 47\cdot 109$
475	$2\cdot 37$	513	$2\cdot 5$
476	$13\cdot 29$	514	17
477	$2\cdot 5\cdot 61\cdot 373$	515	$2\cdot 13\cdot 101^2$
478	5	516	449
479	$2\cdot 89$	517	$2\cdot 5$
480	17	518	5^2
481	$2\cdot 29$	519	2
482	5^3	520	317
483	$2\cdot 5\cdot 41$	521	2
484	73	522	5
485	$2\cdot 337\cdot 349$	523	$2\cdot 5\cdot 17$
486	13	524	$37\cdot 41\cdot 181$
487	$2\cdot 5\cdot 37$	525	$2\cdot 13$
488	5	526	337
489	$2\cdot 13\cdot 17$	527	$2\cdot 5$
490		528	$5\cdot 13$
491	$2\cdot 149$	529	2
492	5	530	257
493	$2\cdot 5^2$	531	$2\cdot 17$
494	277	532	5^2

a	Divisores ipsius $aa+1$	a	Divisores ipsius $aa+1$
533	$2\cdot 5$	568	$5^3\cdot 29\cdot 89$
534	29	569	2
535	2	570	
536		571	2
537	$2\cdot 5$	572	5
538	$5\cdot 13\cdot 61\cdot 73$	573	$2\cdot 5$
539	$2\cdot 29$	574	17
540	17^2	575	2
541	$2\cdot 13$	576	
542	$5\cdot 41$	577	$2\cdot 5\cdot 13^2\cdot 197$
543	$2\cdot 5^2$	578	$5\cdot 109$
544		579	2
545	2	580	$13\cdot 113\cdot 229$
546	241	581	2
547	$2\cdot 5$	582	$5^2\cdot 17$
548	$5\cdot 17$	583	$2\cdot 5\cdot 41$
549	$2\cdot 37$	584	
550	113	585	$2\cdot 137$
551	$2\cdot 13$	586	37
552	$5\cdot 149\cdot 409$	587	$2\cdot 5$
553	$2\cdot 5\cdot 53$ [1])	588	5
554	13	589	$2\cdot 89$
555	$2\cdot 233$	590	13
556		591	$2\cdot 17$
557	$2\cdot 5^3\cdot 17\cdot 73$	592	$5\cdot 29$
558	5	593	$2\cdot 5^2\cdot 13\cdot 541$
559	2	594	
560	$53\cdot 61\cdot 97$	595	2
561	$2\cdot 37$	596	101
562	$5\cdot 181\cdot 349$	597	$2\cdot 5\cdot 29$
563	$2\cdot 5\cdot 29$	598	$5\cdot 37$
564	13	599	$2\cdot 17\cdot 61\cdot 173$
565	$2\cdot 17\cdot 41\cdot 229$	600	157
566	457	601	$2\cdot 313\cdot 577$
567	$2\cdot 5\cdot 13$	602	5

1) In editione principe (nec non in *Comment. arithm.*) factor 53 omissus est, ita ut numerus $\frac{5\,13^2+1}{10} = 30581 = 53\cdot 577$ inter primos numeratus sit. Correxit F. R.

a	Divisores ipsius $aa+1$	a	Divisores ipsius $aa+1$
603	$2\cdot5\cdot13$	641	2
604	97	642	$5\cdot13\cdot17\cdot373$
605	$2\cdot197$	643	$2\cdot5^2$
606	$13^2\cdot41\cdot53$	644	
607	$2\cdot5^2$	645	$2\cdot13$
608	$5\cdot17$	646	
609	2	647	$2\cdot5\cdot41$
610	233	648	$5\cdot137\cdot613$
611	$2\cdot73$	649	2
612	$5\cdot173\cdot433$	650	$17\cdot29$
613	$2\cdot5\cdot53$	651	$2\cdot313$
614	277	652	5
615	$2\cdot281$	653	$2\cdot5$
616	$13\cdot17^2\cdot101$	654	
617	$2\cdot5$	655	$2\cdot13\cdot29\cdot569$
618	5^2	656	157
619	$2\cdot13$	657	$2\cdot5^2\cdot89\cdot97$
620	269	658	$5\cdot13$
621	$2\cdot29\cdot61\cdot109$	659	$2\cdot17\cdot53\cdot241$
622	5	660	$37\cdot61\cdot193$
623	$2\cdot5\cdot37$	661	2
624	41	662	5
625	$2\cdot17$	663	$2\cdot5\cdot113\cdot389$
626	29	664	353
627	$2\cdot5$	665	$2\cdot41$
628	5	666	53
629	$2\cdot13$	667	$2\cdot5\cdot17$
630	73	668	$5^2\cdot13$
631	2	669	2
632	$5^2\cdot13$	670	593
633	$2\cdot5\cdot17$	671	$2\cdot13$
634		672	$5\cdot37$
635	$2\cdot37$	673	$2\cdot5$
636		674	
637	$2\cdot5$	675	$2\cdot409\cdot557$
638	5	676	17
639	2	677	$2\cdot5$
640	149	678	$5\cdot89$

a	Divisores ipsius $aa+1$	a	Divisores ipsius $aa+1$
679	$2\cdot 29$	717	$2\cdot 5\cdot 101\cdot 509$
680		718	$5^2\cdot 17$
681	$2\cdot 13$	719	$2\cdot 53$
682	$5^3\cdot 61^2$	720	13
683	$2\cdot 5$	721	$2\cdot 61$
684	$13\cdot 17\cdot 29\cdot 73$	722	$5\cdot 137$
685	2	723	$2\cdot 5\cdot 13$
686		724	293
687	$2\cdot 5\cdot 109\cdot 433$	725	$2\cdot 269$
688	$5\cdot 41$	726	601
689	2	727	$2\cdot 5\cdot 17$
690		728	5
691	$2\cdot 193$	729	$2\cdot 41$
692	5	730	109
693	$2\cdot 5^3\cdot 17\cdot 113$	731	$2\cdot 397\cdot 673$
694	13	732	5^2
695	2	733	$2\cdot 5\cdot 13$
696		734	37
697	$2\cdot 5\cdot 13\cdot 37\cdot 101$	735	$2\cdot 17$
698	5	736	13
699	2	737	$2\cdot 5\cdot 29$
700		738	5
701	$2\cdot 17\cdot 97\cdot 149$	739	2
702	5	740	
703	$2\cdot 5\cdot 73\cdot 677$	741	$2\cdot 293$
704		742	$5\cdot 29$
705	$2\cdot 181$	743	$2\cdot 5^2\cdot 61\cdot 181$
706	41	744	17
707	$2\cdot 5^2\cdot 13$	745	2
708	$5\cdot 29$	746	$13^2\cdot 37\cdot 89$
709	$2\cdot 37$	747	$2\cdot 5\cdot 41$
710	$13\cdot 17$	748	$5\cdot 317\cdot 353$
711	2	749	$2\cdot 13$
712	$5\cdot 53$	750	
713	$2\cdot 5\cdot 29$	751	2
714		752	$5\cdot 17$
715	2	753	$2\cdot 5$
716		754	97

a	Divisores ipsius $aa+1$	a	Divisores ipsius $aa+1$
755	$2\cdot257$	793	$2\cdot5^2$
756	521	794	229
757	$2\cdot5^2\cdot73\cdot157$	795	$2\cdot17\cdot29\cdot641$
758	5	796	109
759	$2\cdot13$	797	$2\cdot5$
760		798	$5\cdot13\cdot97\cdot101$
761	$2\cdot17$	799	2
762	$5\cdot13$	800	$29^2\cdot761$
763	$2\cdot5$	801	$2\cdot13$
764		802	$5\cdot197\cdot653$
765	$2\cdot53$	803	$2\cdot5\cdot17$
766	29	804	61
767	$2\cdot5\cdot89\cdot661$	805	$2\cdot457\cdot709$
768	5^2	806	113
769	$2\cdot17$	807	$2\cdot5^4\cdot521$
770	41	808	$5\cdot37$
771	$2\cdot29\cdot37\cdot277$	809	$2\cdot229$
772	$5\cdot13\cdot53\cdot173$	810	509
773	$2\cdot5$	811	$2\cdot13\cdot41\cdot617$
774	197	812	$5\cdot17$
775	$2\cdot13^2$	813	$2\cdot5\cdot157\cdot421$
776	$73^2\cdot113$	814	13
777	$2\cdot5$	815	2
778	$5\cdot17$	816	
779	2	817	$2\cdot5$
780		818	$5^3\cdot53\cdot101$
781	2	819	2
782	$5^2\cdot61\cdot401$	820	$17\cdot37$
783	$2\cdot5\cdot37$	821	2
784		822	$5\cdot337\cdot401$
785	$2\cdot13\cdot137\cdot173$	823	$2\cdot5$
786	17	824	$13\cdot29$
787	$2\cdot5\cdot241\cdot257$	825	$2\cdot53$
788	$5\cdot13\cdot41\cdot233$	826	
789	$2\cdot149$	827	$2\cdot5\cdot13$
790	281	828	5
791	2	829	$2\cdot17^2\cdot29\cdot41$
792	5	830	73

a	Divisores ipsius $aa+1$	a	Divisores ipsius $aa+1$
831	$2\cdot 449\cdot 769$	869	2
832	5^2	870	41
833	$2\cdot 5$	871	$2\cdot 17\cdot 53\cdot 421$
834	349	872	5
835	$2\cdot 89$	873	$2\cdot 5$
836	701	874	461
837	$2\cdot 5\cdot 13\cdot 17\cdot 317$	875	2
838	5	876	13
839	$2\cdot 109$	877	$2\cdot 5$
840	13	878	$5\cdot 53$
841	2	879	$2\cdot 13$
842	5	880	17
843	$2\cdot 5^2\cdot 61\cdot 233$	881	2
844	757	882	$5^2\cdot 29^2\cdot 37$
845	$2\cdot 37$	883	$2\cdot 5$
846	17	884	193
847	$2\cdot 5$	885	2
848	5	886	181
849	$2\cdot 73$	887	$2\cdot 5\cdot 29$
850	$13\cdot 149\cdot 373$	888	$5\cdot 17$
851	$2\cdot 97$	889	$2\cdot 13\cdot 113\cdot 269$
852	$5\cdot 41$	890	
853	$2\cdot 5\cdot 13\cdot 29\cdot 193$	891	$2\cdot 277$
854	17	892	$5\cdot 13$
855	2	893	$2\cdot 5^2\cdot 41\cdot 389$
856	89	894	37
857	$2\cdot 5^2\cdot 37\cdot 397$	895	$2\cdot 97$
858	$5\cdot 29$	896	281
859	$2\cdot 137$	897	$2\cdot 5\cdot 17$
860		898	5
861	2	899	$2\cdot 101$
862	5	900	241
863	$2\cdot 5\cdot 13\cdot 17\cdot 337$	901	2
864		902	$5\cdot 13$
865	$2\cdot 61$	903	$2\cdot 5\cdot 73$
866	13	904	61
867	$2\cdot 5$	905	$2\cdot 13\cdot 17^2\cdot 109$
868	5^2	906	

a	Divisores ipsius $aa+1$	a	Divisores ipsius $aa+1$
907	$2\cdot 5^2$	945	$2\cdot 29\cdot 89\cdot 173$
908	5	946	
909	2	947	$2\cdot 5$
910		948	$5\cdot 17\cdot 97\cdot 109$
911	$2\cdot 29\cdot 41\cdot 349$	949	2
912	5	950	
913	$2\cdot 5$	951	2
914	$17\cdot 157\cdot 313$	952	$5\cdot 41$
915	$2\cdot 13^2$	953	$2\cdot 5$
916	29	954	13
917	$2\cdot 5$	955	2
918	$5^2\cdot 13$	956	$17\cdot 37$
919	$2\cdot 37\cdot 101\cdot 113$	957	$2\cdot 5^2\cdot 13$
920		958	$5\cdot 173$
921	2	959	2
922	$5\cdot 17\cdot 73.137$	960	
923	$2\cdot 5$	961	$2\cdot 409$
924	$53\cdot 89\cdot 181$	962	5
925	2	963	$2\cdot 5$
926	61	964	313
927	$2\cdot 5$	965	$2\cdot 17\cdot 61\cdot 449$
928	$5\cdot 13$	966	
929	2	967	$2\cdot 5\cdot 13$
930		968	$5^2\cdot 37$
931	$2\cdot 13\cdot 17\cdot 37\cdot 53$	969	$2\cdot 29$
932	5^3	970	$13\cdot 157\cdot 461$
933	$2\cdot 5$	971	$2\cdot 197$
934	41	972	5
935	2	973	$2\cdot 5\cdot 17$
936		974	29
937	$2\cdot 5$	975	$2\cdot 41$
938	$5\cdot 149$	976	73
939	$2\cdot 17$	977	$2\cdot 5\cdot 53$
940	29	978	5
941	$2\cdot 13$	979	2
942	5	980	13
943	$2\cdot 5^3$	981	2
944	13^2	982	$5^2\cdot 17$

a	Divisores ipsius $aa+1$	a	Divisores ipsius $aa+1$
983	$2\cdot5\cdot13$	1021	$2\cdot233$
984	53	1022	$5\cdot13$
985	2	1023	$2\cdot5\cdot229\cdot457$
986		1024	17
987	$2\cdot5\cdot61$	1025	2
988	5	1026	61
989	2	1027	$2\cdot5\cdot29$
990	17	1028	$5\cdot241\cdot877$
991	2	1029	2
992	$5\cdot97$	1030	$37\cdot53\cdot541$
993	$2\cdot5^2\cdot13\cdot37\cdot41$	1031	2
994	269	1032	$5^2\cdot13\cdot29\cdot113$
995	$2\cdot73$	1033	$2\cdot5\cdot17$
996	$13\cdot137\cdot557$	1034	$41\cdot89\cdot293$
997	$2\cdot5$	1035	$2\cdot13$
998	$5\cdot29$	1036	
999	$2\cdot17\cdot149\cdot197$	1037	$2\cdot5\cdot53$
1000	101	1038	$5\cdot229\cdot941$
1001	2	1039	2
1002	$5\cdot113$	1040	617
1003	$2\cdot5\cdot29$	1041	$2\cdot17$
1004		1042	$5\cdot37$
1005	$2\cdot37$	1043	$2\cdot5^2$
1006	13	1044	257
1007	$2\cdot5^2\cdot17$	1045	$2\cdot13\cdot97\cdot433$
1008	5	1046	193
1009	$2\cdot13$	1047	$2\cdot5$
1010		1048	$5\cdot13\cdot61\cdot277$
1011	2	1049	$2\cdot73$
1012	$5\cdot257\cdot797$	1050	17
1013	$2\cdot5\cdot89$	1051	2
1014	109	1052	$5\cdot389\cdot569$
1015	$2\cdot373$	1053	$2\cdot5$
1016	$17\cdot41$	1054	
1017	$2\cdot5\cdot293\cdot353$	1055	2
1018	5^2	1056	29
1019	$2\cdot13$	1057	$2\cdot5^3\cdot41\cdot109$
1020	101	1058	$5\cdot13\cdot17\cdot1013$

a	Divisores ipsius $aa+1$	a	Divisores ipsius $aa+1$
1059	$2\cdot137$	1097	$2\cdot5\cdot13$
1060		1098	$5\cdot41$
1061	$2\cdot13\cdot29$	1099	2
1062	5	1100	13
1063	$2\cdot5$	1101	$2\cdot17\cdot101\cdot353$
1064	857	1102	$5\cdot89$
1065	$2\cdot317$	1103	$2\cdot5$
1066		1104	37
1067	$2\cdot5\cdot17\cdot37\cdot181$	1105	$2\cdot181$
1068	$5^5\cdot73$	1106	
1069	2	1107	$2\cdot5^2$
1070		1108	5
1071	$2\cdot13\cdot157\cdot281$	1109	$2\cdot17\cdot61\cdot593$
1072	5	1110	13
1073	$2\cdot5$	1111	2
1074	13	1112	5
1075	$2\cdot17\cdot41\cdot829$	1113	$2\cdot5\cdot13^2\cdot733$
1076	233	1114	29
1077	$2\cdot5\cdot193\cdot601$	1115	$2\cdot113$
1078	5	1116	$37\cdot41\cdot821$
1079	$2\cdot37$	1117	$2\cdot5$
1080	773	1118	$5^2\cdot17^2\cdot173$
1081	2	1119	$2\cdot29$
1082	5^2	1120	433
1083	$2\cdot5\cdot53$	1121	$2\cdot101$
1084	$13^2\cdot17\cdot409$	1122	$5\cdot73$
1085	$2\cdot29$	1123	$2\cdot5\cdot13\cdot89\cdot109$
1086	733	1124	
1087	$2\cdot5\cdot13\cdot61\cdot149$	1125	2
1088	5	1126	$13\cdot17$
1089	$2\cdot97$	1127	$2\cdot5\cdot157\cdot809$
1090	$29\cdot53\cdot773$	1128	$5\cdot397\cdot641$
1091	2	1129	2
1092	$5\cdot17$	1130	577
1093	$2\cdot5^2$	1131	$2\cdot173$
1094		1132	5^2
1095	2	1133	$2\cdot5\cdot137\cdot937$
1096		1134	541

a	Divisores ipsius $aa+1$	a	Divisores ipsius $aa+1$
1135	$2\cdot 17$	1173	$2\cdot 5$
1136	$13\cdot 53$	1174	
1137	$2\cdot 5$	1175	$2\cdot 13$
1138	5	1176	
1139	$2\cdot 13\cdot 41$	1177	$2\cdot 5\cdot 17\cdot 29\cdot 281$
1140		1178	$5\cdot 13\cdot 37\cdot 577$
1141	$2\cdot 37\cdot 73\cdot 241$	1179	2
1142	$5\cdot 97$	1180	41
1143	$2\cdot 5^2\cdot 17\cdot 29\cdot 53$	1181	2
1144		1182	5^3
1145	$2\cdot 113$	1183	$2\cdot 5\cdot 349\cdot 401$
1146		1184	
1147	$2\cdot 5$	1185	2
1148	$5\cdot 29\cdot 61\cdot 149$	1186	$17\cdot 97\cdot 853$
1149	$2\cdot 13$	1187	$2\cdot 5$
1150		1188	$5\cdot 13$
1151	2	1189	$2\cdot 53$
1152	$5\cdot 13\cdot 17$	1190	37
1153	$2\cdot 5\cdot 37$	1191	$2\cdot 13\cdot 89\cdot 613$
1154	317	1192	5
1155	2	1193	$2\cdot 5^3$
1156		1194	17^2
1157	$2\cdot 5^2\cdot 41\cdot 653$	1195	$2\cdot 73$
1158	$5\cdot 269\cdot 997$	1196	$53\cdot 137\cdot 197$
1159	$2\cdot 337$	1197	$2\cdot 5$
1160	17	1198	$5\cdot 41$
1161	2	1199	2
1162	$5\cdot 13$	1200	337
1163	$2\cdot 5$	1201	$2\cdot 13\cdot 29$
1164	1061	1202	$5\cdot 101$
1165	$2\cdot 13$	1203	$2\cdot 5\cdot 17$
1166	109	1204	13
1167	$2\cdot 5$	1205	2
1168	$5^2\cdot 197\cdot 277$	1206	29
1169	$2\cdot 17$	1207	$2\cdot 5^2$
1170	61	1208	5
1171	2	1209	2.61
1172	$5\cdot 29$	1210	

a	Divisores ipsius $aa+1$	a	Divisores ipsius $aa+1$
1211	$2\cdot17$	1246	
1212	$5\cdot89$	1247	$2\cdot5$
1213	$2\cdot5$	1248	$5\cdot181$
1214	$13\cdot73$	1249	$2\cdot53$
1215	$2\cdot37$	1250	1201
1216	661	1251	2
1217	$2\cdot5\cdot13$	1252	$5\cdot37^2\cdot229$
1218	5^2	1253	$2\cdot5.13^2\cdot929$
1219	2	1254	$17\cdot233\cdot397$
1220	17	1255	2
1221	$2\cdot41$	1256	13
1222	$5\cdot101$	1257	$2\cdot5^2$
1223	$2\cdot5\cdot373\cdot401$	1258	$5\cdot113$
1224	569	1259	$2\cdot29$
1225	2	1260	349
1226	509	1261	$2\cdot613$
1227	$2\cdot5\cdot13\cdot37\cdot313$	1262	$5\cdot17\cdot41\cdot457$
1228	$5\cdot17\cdot113\cdot157$	1263	$2\cdot5\cdot269\cdot593$
1229	$2\cdot773\cdot977$	1264	$29\cdot37$
1230	$13\cdot29$	1265	2
1231	$2\cdot61$	1266	13
1232	$5^2\cdot109\cdot557$	1267	$2\cdot5\cdot229\cdot701$
1233	$2\cdot5$	1268	$5^2\cdot73\cdot881$
1234	421 [1]	1269	$2\cdot13\cdot241\cdot257$
1235	$2\cdot29$	1270	$61\cdot137\cdot193$
1236	149	1271	$2\cdot17$
1237	$2\cdot5\cdot17$	1272	5
1238	5	1273	$2\cdot5$
1239	$2\cdot41\cdot97\cdot193$	1274	
1240	13	1275	$2\cdot109$
1241	2	1276	
1242	$5\cdot53$	1277	$2\cdot5\cdot313\cdot521$
1243	$2\cdot5^2\cdot13$	1278	5
1244		1279	$2\cdot13\cdot17$
1245	$2\cdot17$	1280	$41\cdot89\cdot449$

1) In editione principe (nec non in *Comment. arithm.*) hic numerus 421 omissus est, ita ut numerus $1234^2+1 = 1522757 = 421\cdot3617$ inter primos numeratus sit. Correxit F. R.

a	Divisores ipsius $aa+1$	a	Divisores ipsius $aa+1$
1281	2	1319	$2 \cdot 509$
1282	$5^2 \cdot 13^2 \cdot 389$	1320	
1283	$2 \cdot 5 \cdot 97$	1321	$2 \cdot 13 \cdot 41$
1284	157	1322	$5 \cdot 17 \cdot 29 \cdot 709$
1285	2	1323	$2 \cdot 5 \cdot 101$
1286	181	1324	
1287	$2 \cdot 5 \cdot 73$	1325	$2 \cdot 277$
1288	$5 \cdot 17 \cdot 29 \cdot 673 \cdot 1033$	1326	37
1289	$2 \cdot 37$	1327	$2 \cdot 5 \cdot 293 \cdot 601$
1290		1328	$5 \cdot 521 \cdot 677$
1291	$2 \cdot 173$	1329	2
1292	$5 \cdot 13 \cdot 61 \cdot 421$	1330	17
1293	$2 \cdot 5^2 \cdot 29 \cdot 1153$	1331	$2 \cdot 13 \cdot 61 \cdot 1117$
1294		1332	5^2
1295	$2 \cdot 13 \cdot 53 \cdot 1217$	1333	$2 \cdot 5 \cdot 137 \cdot 1297$
1296	17	1334	13
1297	$2 \cdot 5 \cdot 149 \cdot 1129$	1335	$2 \cdot 461$
1298	5	1336	97
1299	2	1337	$2 \cdot 5$
1300	809	1338	$5 \cdot 37$
1301	$2 \cdot 37 \cdot 89 \cdot 257$	1339	$2 \cdot 17$
1302	$5 \cdot 53$	1340	
1303	$2 \cdot 5 \cdot 41^2 \cdot 101$	1341	$2 \cdot 73 \cdot 109 \cdot 113$
1304	173	1342	5
1305	$2 \cdot 13 \cdot 17$	1343	$2 \cdot 5^2$
1306		1344	$13 \cdot 41$
1307	$2 \cdot 5^3$	1345	2
1308	$5 \cdot 13$	1346	29
1309	$2 \cdot 233$	1347	$2 \cdot 5 \cdot 13 \cdot 17 \cdot 821$
1310	293	1348	$5 \cdot 53$
1311	2	1349	2
1312	5	1350	
1313	$2 \cdot 5 \cdot 17$	1351	$2 \cdot 29$
1314		1352	$5 \cdot 281 \cdot 1301$
1315	2	1353	$2 \cdot 5 \cdot 61$
1316		1354	
1317	$2 \cdot 5 \cdot 29$	1355	$2 \cdot 53$
1318	$5^3 \cdot 13 \cdot 1069$	1356	17

a	Divisores ipsius $aa+1$	a	Divisores ipsius $aa+1$
1357	$2\cdot5^2\cdot13$	1395	$2\cdot953\cdot1021$
1358	5	1396	13
1359	2	1397	$2\cdot5$
1360	$13\cdot73$	1398	$5\cdot17$
1361	2	1399	$2\cdot13$
1362	$5\cdot41$	1400	37
1363	$2\cdot5\cdot37$	1401	$2\cdot53$
1364	17	1402	5
1365	$2\cdot197$	1403	$2\cdot5\cdot41$
1366		1404	$29\cdot101\cdot673$
1367	$2\cdot5$	1405	2
1368	5^2	1406	
1369	$2\cdot89$	1407	$2\cdot5^2\cdot17^2\cdot137$
1370	$13\cdot353\cdot409$	1408	$5\cdot53$
1371	$2\cdot113$	1409	$2\cdot13\cdot29$
1372	5	1410	
1373	$2\cdot5\cdot13\cdot17\cdot853$	1411	2
1374		1412	$5\cdot13.37\cdot829$
1375	$2\cdot29\cdot37\cdot881$	1413	$2\cdot5$
1376		1414	$61\cdot73\cdot449$
1377	$2\cdot5$	1415	$2\cdot17$
1378	5	1416	
1379	$2\cdot797\cdot1193$	1417	$2\cdot5$
1380	$29\cdot97\cdot677$	1418	5^2
1381	$2\cdot17$	1419	2
1382	$5^2\cdot241\cdot317$	1420	
1383	$2\cdot5\cdot13$	1421	2
1384	109	1422	$5\cdot13^2$
1385	$2\cdot41\cdot149\cdot157$	1423	$2\cdot5$
1386	13	1424	$17\cdot101\cdot1181$
1387	$2\cdot5$	1425	$2\cdot13$
1388	$5\cdot373\cdot1033$	1426	41
1389	2	1427	$2\cdot5\cdot269\cdot757$
1390	$17\cdot89\cdot1277$	1428	$5\cdot617\cdot661$
1391	2	1429	$2\cdot181$
1392	$5\cdot61$	1430	
1393	$2\cdot5^2\cdot197^2$	1431	$2\cdot461$
1394		1432	$5^4\cdot17\cdot193$

a	Divisores ipsius $aa+1$	a	Divisores ipsius $aa+1$
1433	$2\cdot5\cdot29\cdot73\cdot97$	1467	$2\cdot5\cdot29\cdot41\cdot181$
1434		1468	5^2
1435	$2\cdot13$	1469	2
1436	641	1470	137
1437	$2\cdot5\cdot37$	1471	$2\cdot317$
1438	$5\cdot13\cdot29\cdot1097$	1472	5
1439	2	1473	$2\cdot5$
1440		1474	$13\cdot37$
1441	$2\cdot17\cdot157\cdot389$	1475	$2\cdot17\cdot61\cdot1049$
1442	5	1476	769
1443	$2\cdot5^3$	1477	$2\cdot5\cdot13\cdot97\cdot173$
1444	41	1478	$5\cdot433\cdot1009$
1445	$2\cdot277$	1479	$2\cdot89$
1446	149	1480	457
1447	$2\cdot5$	1481	$2\cdot229$
1448	$5\cdot13$	1482	5^2
1449	$2\cdot17\cdot37$	1483	$2\cdot5\cdot17^2\cdot761$
1450	109	1484	113
1451	$2\cdot13^2$	1485	$2\cdot41$
1452	5	1486	37^2
1453	$2\cdot5\cdot61$	1487	$2\cdot5\cdot13\cdot73\cdot233$
1454	$53\cdot113\cdot353$	1488	5
1455	$2\cdot653$	1489	2
1456		1490	$13\cdot313$
1457	$2\cdot5^2$	1491	$2\cdot29$
1458	$5\cdot17\cdot89\cdot281$	1492	$5\cdot17$
1459	2	1493	$2\cdot5^2\cdot109\cdot409$
1460		1494	
1461	$2\cdot13\cdot53$	1495	2
1462	$5\cdot29$	1496	$29\cdot229\cdot337$
1463	$2\cdot5\cdot193\cdot1109$	1497	$2\cdot5$
1464	$13\cdot173\cdot953$	1498	5
1465	2	1499	2
1466	17	1500	$13\cdot17$

ALBRECHT EULERS BEANTWORTUNG EINIGER ARITHMETISCHEN FRAGEN[1])

Commentatio A 9 indicis Enestroemiani
Abhandlungen der Churfürstlich-baierischen Akademie der Wissenschaften **2**, 1764, II, p. 3—36

I.

Man fraget: Wenn von einer Billion die Zahl hundert nach der gemeinen Weise der Subtraktion und zu widerholtenmalen so oft abgezogen wird, bis nichts (0) *übrig bleibt, wieviel Ziffern zu schreiben hierzu erfordert werden?*

1. Diese Frage ist von wenig Erheblichkeit und ihre Beantwortung erfordert weder Scharfsinn noch Kunstgriffe: sobald dieselbe aber in einem weiteren Verstande genommen wird, so daß die beyden gegebenen Zahlen, welche von einander beständig abgezogen werden sollen, nicht bestimmt, sondern nur durch allgemeine Buchstaben angedeutet werden: so setzet uns eine analytische Auflösung dieser Frage schon in eine größere Verlegenheit. Man sieht sich gezwungen, auf gewisse Hülfsmittel zu denken, auf welche man durch andere Untersuchungen nicht so leicht gefallen wäre. Ein Satz folget dem andern, und wir gerathen durch die Auflösung dieser einzigen Aufgabe auf mehrere, welche unsere Aufmerksamkeit nicht weniger verdienen. Neue Schwierigkeiten hemmen bey der Auflösung jeder dieser Aufgaben unsern Fortgang: die Begierde wird größer, und, indem der Verstand alle

---

1) Die Editio princeps enthält ungewöhnlich viele Fehler, die nur zum Teil als Druckfehler betrachtet werden können. Ich habe mich aber auf die notwendigsten Anmerkungen beschränkt und die übrigen Fehler stillschweigend verbessert. F. R.

Mühe anwendet, diese Schwierigkeiten zu heben, so wird derselbe je länger je geschickter, auch in nützlichen Untersuchungen mit erwünschtem Fortgange arbeiten zu können. Ob ich also gleich nicht läugnen kann, daß gegenwärtige Schrift ohne Nutzen sey, wenn anderst etwas, das den Verstand allein schärft, unter die unnützen Dinge gerechnet werden kann: so schmeichle ich mir dannoch, daß die sonderbare Untersuchungen, auf welche ich bey der Betrachtung eben dieser Frage gefallen bin, der Aufmerksamkeit der Mathematiker nicht gänzlich unwürdig seyn werden. Ich werde mit der Beantwortung der Frage, so wie dieselbe hier vorgelegt worden, den Anfang machen.

2. Da eine Billion 1000000000000 aus 13 Ziffern, und die Zahl 100 aus 3 Ziffern besteht, so müssen gleich vor der ersten Subtraction $13 + 3$, das ist 16 Ziffern geschrieben werden.

Da nun ferner der durch die erste Subtraction entstandene Rest 1 Billion $- 100 = 999999999900$ nur noch aus 12 Ziffern besteht: so wird man bis zur zweyten Subtraction $12 + 3$, das ist 15 Ziffern zu schreiben haben. Und weil der daher entstandene zweyte Rest 999999999800 sowohl als alle folgende, bis man nämlich zu der Zahl 99999999900, das ist 100000 Millionen $-$ 100 gekommen, gleichfalls aus 12 Ziffern bestehen: so wird man so oft $12 + 3$ oder 15 Ziffern schreiben müssen, als Subtractionen zwischen 1 Billion und 100000 Millionen enthalten sind: das ist, man wird so oft 15 Ziffern zu schreiben haben, als

$$\frac{1 \text{ Billion} - 100000 \text{ Millionen}}{100}$$

Einheiten enthält; folglich 9000 Millionen 15 mal oder 135000 Millionen Ziffer.

Auf eine ähnliche Art wird man leicht begreifen, daß man von dem Rest 100000 Millionen $-$ 100 oder 99999999900 bis zum Rest 10000 Millionen $-$ 100 oder 9999999900

$$\frac{100000 \text{ Millionen} - 10000 \text{ Millionen}}{100}(11 + 3)$$

Ziffern, das ist, 900 Millionen 14 mal oder 12600 Millionen Ziffern zu schreiben habe.

Ferner wird von dem Rest 10000 Millionen $-$ 100 bis zu dem Rest 1000 Millionen $-$ 100 die Anzahl der zu schreibenden Ziffern seyn

$$90 \text{ Millionen} \cdot (10 + 3),$$

das ist 1170 Millionen. Und so weiter.

Also wird die verlangte Anzahl aller zu schreibenden Ziffern durch die Addition folgender Zahlen gefunden:

1.	$1 \cdot (13 + 3)$	Ziffern	16
2.	9000 Millionen $\cdot (12 + 3)$	Ziffern	135000000000
3.	900 Millionen $\cdot (11 + 3)$	Ziffern	12600000000
4.	90 Millionen $\cdot (10 + 3)$	Ziffern	1170000000
5.	9 Millionen $\cdot (9 + 3)$	Ziffern	108000000
6.	$900000 \cdot (8 + 3)$	Ziffern	9900000
7.	$90000 \cdot (7 + 3)$	Ziffern	900000
8.	$9000 \cdot (6 + 3)$	Ziffern	81000
9.	$900 \cdot (5 + 3)$	Ziffern	7200
10.	$90 \cdot (4 + 3)$	Ziffern	630
11.	$9 \cdot (3 + 3)$	Ziffern	54
		Also in allem	148888888900 Ziffern.

Wie nun diese Frage beantwortet worden, so können auch alle übrige Fragen von gleicher Art aufgelöset werden. Man wird nämlich durch ähnliche Schlüsse die Anzahl aller deren Ziffern herausbringen, welche geschrieben werden müssen, wenn eine jegliche gegebene Zahl von einer andern gegebenen größern Zahl nach der gemeinen Weise der Subtraction so oft abgezogen würde, bis entweder, wie in diesem Falle, nichts (0) oder eine Zahl, so kleiner als die zu subtrahirende ist, übrig bleibt. Ich werde nun zeigen, wie auch diese Anzahl der Ziffern könne gefunden werden, wenn die beyden gegebenen Zahlen nicht eigentlich bestimmet, sondern bloß auf eine allgemeine Art durch Buchstaben angedeutet werden.

II.

Es werden zwey Zahlen a und b gegeben: wenn die kleinere derselben b von der größeren a nach der gewöhnlichen Art so oft abgezogen wird, bis eine Zahl, die kleiner ist als b, übrig bleibt, so soll die Anzahl aller hierzu erforderlichen Ziffern durch eine analytische Formul ausgedrückt werden.

3. Man setze zu diesem Ende, die Zahl a bestehe aus n Ziffern, und die zu subtrahirende Zahl b aus m Ziffern. Nun merke ich überhaupt an, daß, weil die größte Zahl von einer bestimmten Menge Ziffern, z. E. von n Ziffern,

aus n neben einander gesetzten Neunern (9) besteht, dieselbe ganz bequem durch $10^n - 1$ angedeutet werden könne. Also wird die allergrößte Zahl von $n-1$ Ziffern $= 10^{n-1} - 1$, von $n-2$ Ziffern $= 10^{n-2} - 1$, von $n-3$ Ziffern $= 10^{n-3} - 1$, und so weiter seyn. Hernach ist aus dem vorhergehenden offenbar, daß man so oft werde $n+m$ Ziffern zu schreiben haben, bis eine Zahl von $n-1$ Ziffern übrig bleibt; imgleichen wird man so oft $n+m-1$, $n+m-2$, $n+m-3$ u. s. w. Ziffern schreiben müssen, bis man auf Reste von $n-2$, $n-3$, $n-4$ u. s. w. Ziffern kömmt.

Ferner wird es nicht schwer seyn einzusehen, daß die Anzahl aller Subtractionen bis zum ersten Rest von $n-1$ Ziffern durch den nächst größten Quotienten von $\frac{a-10^{n-1}+1}{b}$ ausgedrückt werde. Deuten wir nun diesen nächst größten Quotienten von $\frac{a-10^{n-1}+1}{b}$ durch

$$Q\frac{a+1-10^{n-1}}{b}$$

an, so werden bis zu dem ersten Rest von $n-1$ Ziffern

$$(n+m)\,Q\frac{a+1-10^{n-1}}{b}$$

Zahlen geschrieben werden müssen.

Da auf eine gleiche Weise die Anzahl aller Subtractionen vom Anfang an bis zu dem ersten Rest von $n-2$ Ziffern durch den nächst größten Quotienten von $\frac{a-10^{n-2}+1}{b}$ oder durch

$$Q\frac{a+1-10^{n-2}}{b}$$

angedeutet wird: so muss die Anzahl aller Subtractionen von dem ersten Rest von $n-1$ Ziffern bis zu dem ersten Rest von $n-2$ Ziffern seyn

$$= Q\frac{a+1-10^{n-2}}{b} - Q\frac{a+1-10^{n-1}}{b}.$$

Und da man auch eben so oft $n+m-1$ Ziffern zu schreiben hat, so werden in allem bis zu dem ersten Rest von $n-2$ Ziffern

$$(n+m)\,Q\frac{a+1-10^{n-1}}{b}$$
$$+(n+m-1)\,Q\frac{a+1-10^{n-2}}{b} - (n+m-1)\,Q\frac{a+1-10^{n-1}}{b}$$

Zahlen erfordert werden.

Auf eine ähnliche Art wird man leicht gewahr werden, daß die Anzahl aller Subtractionen von dem ersten Rest von $n-2$ Ziffern bis zu dem ersten Rest von $n-3$ Ziffern seyn werde

$$Q\frac{a+1-10^{n-3}}{b} - Q\frac{a+1-10^{n-2}}{b}.$$

Und da man auch wiederum eben so oft $n+m-2$ Ziffern zu schreiben hat, so wird vom Anfang an bis zu dem ersten Rest von $n-3$ Ziffern die Anzahl der zu schreibenden Ziffern also ausgedrückt werden:

$$\begin{aligned}&(n+m)\,Q\frac{a+1-10^{n-1}}{b}\\ &+(n+m-1)\,Q\frac{a+1-10^{n-2}}{b} - (n+m-1)\,Q\frac{a+1-10^{n-1}}{b}\\ &+(n+m-2)\,Q\frac{a+1-10^{n-3}}{b} - (n+m-2)\,Q\frac{a+1-10^{n-2}}{b}\end{aligned}$$

Wann man nun diese Schlüsse weiter fort setzet, so wird man sich leicht überführen, daß die verlangte Anzahl aller zu schreibenden Ziffern, nämlich von Anfang an, bis daß man zu einem Rest kömmt, so weniger als m Ziffern hat, seyn werde

$$\begin{aligned}&(n+m)\,Q\frac{a+1-10^{n-1}}{b} - (n+m-1)\,Q\frac{a+1-10^{n-1}}{b}\\ &+(n+m-1)\,Q\frac{a+1-10^{n-2}}{b} - (n+m-2)\,Q\frac{a+1-10^{n-2}}{b}\\ &+(n+m-2)\,Q\frac{a+1-10^{n-3}}{b} - (n+m-3)\,Q\frac{a+1-10^{n-3}}{b}\\ &+(n+m-3)\,Q\frac{a+1-10^{n-4}}{b} - (n+m-4)\,Q\frac{a+1-10^{n-4}}{b}\end{aligned}$$

und so weiter bis zum Gliede

$$+(n+m+m-n)\,Q\frac{a+1-10^{n-n+m-1}}{b}.$$

Oder da man, außer dem letzten, allezeit je zwey und zwey Glieder bequem zusammen bringen kann, so wird die begehrte Anzahl aller zu schreibenden Ziffern also ausgedrückt werden:

$$\begin{aligned}&Q\frac{a+1-10^{n-1}}{b} + Q\frac{a+1-10^{n-2}}{b} + Q\frac{a+1-10^{n-3}}{b} + Q\frac{a+1-10^{n-4}}{b}\\ &+\cdots+ Q\frac{a+1-10^{m}}{b} + 2m\,Q\frac{a+1-10^{m-1}}{b}.\end{aligned}$$

Oder besser, wann diese Reihe umgekehrt geschrieben wird,

$$2m\,Q\frac{a+1-10^{m-1}}{b}+Q\frac{a+1-10^{m}}{b}+Q\frac{a+1-10^{m+1}}{b}$$
$$+Q\frac{a+1-10^{m+2}}{b}+Q\frac{a+1-10^{m+3}}{b}+\cdots+Q\frac{a+1-10^{n-1}}{b}.$$

Und die Anzahl aller Glieder dieser Reihe belauft sich auf $n-m+1$.

4. Da in der Aufgabe eigentlich vorausgesetzt worden, daß b von a so oft abgezogen wird, als es die Zahl a zulassen will, und wir in der Auflösung nur gesetzt haben, daß b so oft unter den Resten geschrieben werde, bis eine Zahl heraus kömmt, die aus weniger Ziffern besteht, als die zu subtrahirende Zahl b hat: so wird unsere gefundene Formul, wenn sie den Bedingungen der Aufgabe gänzlich ein Genügen leisten soll, noch einige Zusätze und Veränderungen nöthig haben. Man wird zu diesem Ende auf den letzten Rest Achtung geben müssen, und wenn befunden wird, daß derselbe so wie die zu subtrahirende Zahl b noch aus m Ziffern besteht, so wird man von der angezeigten Anzahl aller zu schreibenden Ziffern die Zahl m abziehen müssen. Und wenn dieser letzte Rest aus weniger als m Ziffern besteht, so wird man zu der gefundenen Formul die Anzahl der Ziffern eben dieses Rests noch hinzu zu thun haben. Der letzte Rest aber wird, wie bekannt, durch die wirkliche Theilung der Zahl a durch b gefunden.

Da nun aus der Natur der Division erhellt, daß der Rest von $\frac{a}{b}$ der zu theilenden Zahl a weniger dem Theiler b mit dem nächst kleinsten Quotient von $\frac{a}{b}$ vermehrt gleich sey, wenn wir diesen nächst kleinsten Quotienten von $\frac{a}{b}$ durch $q\frac{a}{b}$ andeuten, so werden wir auch die eben erwähnte Bedingungen mit in der analytischen Formul folgender Weise eintragen können.

Wenn nämlich der letzte Rest $a-b\cdot q\frac{a}{b}$ aus m Ziffern besteht, so wird die verlangte Anzahl aller zu schreibenden Ziffern also ausgedrückt werden:

$$2m\,Q\frac{a+1-10^{m-1}}{b}+Q\frac{a+1-10^{m}}{b}+Q\frac{a+1-10^{m+1}}{b}$$
$$+Q\frac{a+1-10^{m+2}}{b}+\cdots+Q\frac{a+1-10^{n-1}}{b}-m,$$

und wenn $a-b\cdot q\frac{a}{b}$ aus weniger als m Ziffern, zum Exempel aus r Ziffern besteht, so wird die verlangte Anzahl aller zu schreibenden Ziffern seyn:

$$2mQ\frac{a+1-10^{m-1}}{b}+Q\frac{a+1-10^{m}}{b}+Q\frac{a+1-10^{m+1}}{b}$$
$$+Q\frac{a+1-10^{m+2}}{b}+\cdots+Q\frac{a+1-10^{n-1}}{b}+r.$$

5. Einige Exempel sollen dieses noch deutlicher machen.

I. Die Zahl 12 wird von der Zahl 1763[1]) so oft abgezogen, bis eine Zahl, die kleiner ist als 12, übrig bleibt; man verlangt zu wissen, wieviel Ziffern zu schreiben hierzu erfordert werden?

Hier ist also $a=1763$, $n=4$, $b=12$, $m=2$,

$a+1 \quad\quad =1764,$

$a+1-\ 10=1754, \quad Q\frac{1754}{12}=147, \quad 4Q\frac{1754}{12}=588$

$a+1-\ 100=1664, \quad Q\frac{1664}{12}=139$

$a+1-1000=\ 764, \quad Q\frac{764}{12}=\ 64$

b	a	$q\frac{a}{b}$
12)	1763	(146
	12	
	56	
	48	
	83	
	72	
	11	

Summa 791 Ziffern, Rest $11=a-b\cdot q\frac{a}{b}$.

Ziehen wir nun ferner den in dem vorhergehenden § gedachten Umstand in Erwägung: weil der letzte Rest $a-b\cdot q\frac{a}{b}=11$ aus 2, das ist aus eben soviel Ziffern besteht, als die Zahl $b=12$ hat, so werden von der eben gefundenen Zahl 791 noch diese 2 abgezogen werden müssen. Also ist die verlangte Anzahl aller zu schreibenden Ziffern $791-2$, das ist 789.

II. Man setze die Zahl 12 werde von 1765 so oft abgezogen, bis eine Zahl, die kleiner ist als 12, übrig bleibt, und es wird gefragt: wieviel Ziffern hierzu zu schreiben erfordert werden?

---

1) Nach C. G. J. Jacobi wurde die vorliegende Abhandlung am 30. Juni 1763 in der Berliner Akademie gelesen. Auch Leonhard Euler hatte die Gewohnheit, bei Zahlenbeispielen das Jahr der Abfassung zu benutzen. Siehe die Anmerkungen p. XIX und 289 des vorhergehenden Bandes. F. R.

Da also $a = 1765$, $n = 4$, $b = 12$, $m = 2$, so wird

$$a + 1 \qquad = 1766,$$
$$a + 1 - \quad 10 = 1756, \quad 4\,Q\frac{1756}{12} = 588$$
$$a + 1 - \quad 100 = 1666, \quad Q\frac{1666}{12} = 139$$
$$a + 1 - 1000 = \quad 766, \quad Q\frac{766}{12} = \quad 64$$

$b \quad a \quad q\frac{a}{b}$

12) 1765 (147
12
56
48
85
84
1

Summa 791 Ziffern, Rest $1 = a - b \cdot q\frac{a}{b}$.

Nun zeigt uns die wirkliche Theilung, daß der letzte Rest nur aus einer Ziffer besteht, folglich muß zu der gefundenen Anzahl der Ziffern 791 noch 1 hinzu gethan werden. Also wird die verlangte Anzahl aller zu schreibenden Ziffern in diesem Falle seyn $791 + 1$, das ist 792.

III. Wann die Zahl 10^q von der Zahl 10^p so oft abgezogen wird, bis nichts übrig bleibt, so fragt man: wieviel Ziffern zu schreiben hierzu erfordert werden?

Weil hier $q < p$ und also 10^p durch 10^q theilbar ist, so kann der im 4. § erwähnte Umstand nicht Statt finden, und die im 3. § gegebene Formul wird uns die verlangte Anzahl aller zu schreibenden Ziffern folgendermaßen geben.

Es sey also $a = 10^p$, $n = p + 1$, $b = 10^q$, $m = q + 1$; so wird

$$Q\frac{a + 1 - 10^{m-1}}{b} = Q\frac{10^p - 10^q + 1}{10^q} = 10^{p-q} - 1 + 1 = 10^{p-q},$$

$$Q\frac{a + 1 - 10^m}{b} = 10^{p-q} - 10 + 1,$$

$$Q\frac{a + 1 - 10^{m+1}}{b} = 10^{p-q} - 10^2 + 1,$$

$$Q\frac{a + 1 - 10^{m+2}}{b} = 10^{p-q} - 10^3 + 1$$

etc.

Da nun die Anzahl aller dieser Glieder $n - m + 1 = p - q + 1$ ist, so wird, wenn das erste Glied $2m = 2q + 2$ mal genommen wird, die Summe aller Glieder seyn

$$(2 + p + q)10^{p-q} + p - q - 10 - 10^2 - 10^3 - 10^4 - \cdots - 10^{p-q}.$$

Folglich weil

$$10 + 10^2 + 10^3 + 10^4 + 10^5 + \cdots 10^{p-q} = 10\frac{10^{p-q} - 1}{10 - 1},$$

so wird die Anzahl aller zu schreibenden Ziffern seyn

$$(2 + p + q)10^{p-q} - 10\frac{10^{p-q} - 1}{10 - 1} + p - q.$$

Wann demnach, wie in der vorgelegten Frage, $a = 1$ Billion und $b = 100$, so wird $a = 10^{12}$, $b = 10^2$, $p = 12$, $q = 2$, folglich die verlangte Anzahl aller zu schreibenden Ziffern seyn

$$16 \cdot 10^{10} - 10\frac{10^{10} - 1}{9} + 10 = 148888888900,$$

so wie dieselbe oben gefunden worden.

6. Man erlaube mir hier einige Sätze, den nächst größten und nächst kleinsten Quotienten der Brüche betreffend, anzuführen; da ich zumalen inskünftige öfter werde Gelegenheit haben, dieselben mit Vortheile zu gebrauchen.[1])

I. Wenn $a - b \cdot q\frac{a}{b} = 0$ oder wenn a durch b theilbar ist, so wird

$$Q\frac{a}{b} = q\frac{a}{b} = \frac{a}{b}.$$

II. Wenn $a - b \cdot q\frac{a}{b} \neq 0$ oder wenn a durch b nicht theilbar ist, so wird

$$Q\frac{a}{b} = q\frac{a}{b} + 1.$$

---

1) In der Editio princeps sind die Sätze IV—VII durch Druckfehler arg entstellt. Ich habe sie so formuliert, wie sie sich der Autor wohl gedacht hatte, doch schien es mir nicht nötig, die Fehler einzeln namhaft zu machen. F. R.

III. $$Q\frac{bc+a}{b} = c + Q\frac{a}{b} = c + 1 + q\frac{a}{b}.$$

IV. $$q\frac{bc+a}{b} = c + q\frac{a}{b} = c - 1 + Q\frac{a}{b}.$$

V. $$Q\frac{bc-a}{b} = c - q\frac{a}{b} = c + 1 - Q\frac{a}{b}.$$

VI. $$q\frac{bc-a}{b} = c - Q\frac{a}{b} = c - 1 - q\frac{a}{b}.$$

VII. Also

$$Q\frac{bc+a}{b} = 2c - q\frac{bc-a}{b} \quad \text{und} \quad q\frac{bc+a}{b} = 2c - Q\frac{bc-a}{b}.$$

VIII. Wenn $a + c - b\left(q\frac{a}{b} + q\frac{c}{b}\right) > b$, so ist

$$Q\frac{a+c}{b} = Q\frac{a}{b} + Q\frac{c}{b} = q\frac{a}{b} + q\frac{c}{b} + 2.$$

IX. Wenn $a + c - b\left(q\frac{a}{b} + q\frac{c}{b}\right) < b$, so ist

$$Q\frac{a+c}{b} = Q\frac{a}{b} + Q\frac{c}{b} - 1 = q\frac{a}{b} + Q\frac{c}{b}.$$

X. Wenn $a - c - b\left(q\frac{a}{b} - q\frac{c}{b}\right) > b$, so ist

$$Q\frac{a-c}{b} = Q\frac{a}{b} - Q\frac{c}{b} + 2 = Q\frac{a}{b} - q\frac{c}{b} + 1.$$

XI. Wenn $a - c - b\left(q\frac{a}{b} - q\frac{c}{b}\right) < b$, so ist

$$Q\frac{a-c}{b} = Q\frac{a}{b} - Q\frac{c}{b} + 1 = Q\frac{a}{b} - q\frac{c}{b}.$$

Ich hätte können noch mehrere dergleichen Sätze anführen, da aber diese wenige zu meinem Vorhaben schon überflüssig sind, so will ich es nur immer hierbey bewenden lassen. Ich glaube auch nicht, daß es nöthig seyn möchte, die Beweise dieser Sätze beyzulegen, weil dieselben mit leichter Mühe aus der Natur der Theilung heraus gebracht werden können. Ich fahre fort, meinen Untersuchungen freyen Lauf zu lassen.

7. Durch Hülfe des zweyten Satzes $Q\frac{a}{b} = q\frac{a}{b} + 1$ können wir sogleich die in dem 3. § gefundene Formul in eine andere verwandeln, worinnen, anstatt der nächst größten, die nächst kleinsten Quotienten der Brüche vorkommen.

$$2mq\frac{a+1-10^{m-1}}{b} + q\frac{a+1-10^{m}}{b} + q\frac{a+1-10^{m+1}}{b}$$
$$+ q\frac{a+1-10^{m+2}}{b} + \cdots + q\frac{a+1-10^{n-1}}{b} + m + n^{1})$$

wird nämlich die Anzahl aller Ziffern andeuten, welche geschrieben werden müssen, wenn die Zahl b von m Ziffern von der Zahl a von n Ziffern so oft subtrahiret würde, bis nichts übrig bleibt. Hier setzen wir nämlich zum voraus, daß die Zahl a durch b theilbar sey.

Wenn aber die Zahl a durch b nicht theilbar ist, und der letzte Rest $a - b \cdot q\frac{a}{b}$ noch aus m, das ist, aus eben soviel Ziffern besteht, als die zu subtrahirende Zahl b hat, so wird die Anzahl dieser Ziffern seyn:

$$2mq\frac{a+1-10^{m-1}}{b} + q\frac{a+1-10^{m}}{b} + q\frac{a+1-10^{m+1}}{b}$$
$$+ q\frac{a+1-10^{m+2}}{b} + \cdots + q\frac{a+1-10^{n-1}}{b} + n$$

und wenn der letzte Rest $a - b \cdot q\frac{a}{b}$ nur aus r, das ist, aus weniger Ziffern, als die zu subtrahirende Zahl b hat, besteht, so wird die verlangte Anzahl aller zu schreibenden Ziffern seyn:

$$2mq\frac{a+1-10^{m-1}}{b} + q\frac{a+1-10^{m}}{b} + q\frac{a+1-10^{m+1}}{b}$$
$$+ q\frac{a+1-10^{m+2}}{b} + \cdots + q\frac{a+1-10^{n-1}}{b} + m + n + r.$$

III.

Wenn einer von der Zahl c bis zur Zahl a mit eingeschlossen alle mittlere Zahlen, ihrer natürlichen Reihe nach, schreiben wollte, so wird gefragt, wie viel Ziffern hierzu erfordert werden?

---

1) In der Editio princeps steht in dieser wie auch in den beiden folgenden Formeln unrichtiger Weise überall Q statt q, während doch ausdrücklich gefordert ist, alles in den nächst kleinsten Quotienten darzustellen. F. R.

8. Meine Absicht ist hier eigentlich, die vorgelegte Frage durch Hülfe der im 3. § gegebenen Formul zu beantworten, und dieses wird auf folgende Art sehr leicht geschehen können. Wir wollen erstlich suchen, wieviel Ziffern erfordert werden, alle Zahlen der natürlichen Ordnung nach von 1 bis a mit eingeschlossen zu schreiben: und da eben dieser Ausdruck uns auch dienen wird, die Anzahl aller zu schreibenden Ziffern von 1 bis $c-1$ mit eingeschlossen anzugeben, so wird uns die Differenz dieser beyden Ausdrücke die verlangte Anzahl aller Ziffern von c bis a mit eingeschlossen darreichen.

Wenn wir nun in der Formul des 3. § $b=1$ setzen, so wird auch $m=1$, und wenn die Zahl a aus n Ziffern besteht, so wird uns diese Formul

$$2Q\frac{a+1-1}{1}+Q\frac{a+1-10}{1}+Q\frac{a+1-10^2}{1}$$
$$+Q\frac{a+1-10^3}{1}+\cdots+Q\frac{a+1-10^{n-1}}{1}$$

die Anzahl aller Ziffern andeuten, welche geschrieben werden müssen, wenn von der Zahl a die Zahl 1 so oft abgezogen werden würde, bis nichts (0) übrig bleibt. Nun sieht man leicht ein, daß hierzu nicht nur alle Zahlen von 1 bis a zu schreiben erfordert werden, sondern man wird auch über das die Zahl 1 so oft schreiben müssen, als Subtractionen zwischen a und 1 enthalten sind. Das ist, unsere eben jetzt gegebene Formul wird die Anzahl aller Ziffern, welche zwischen 1 und a mit eingeschlossen enthalten sind, andeuten, und noch über das a Ziffern: folglich wird diese Anzahl aller Ziffern von 1 bis zu einer Zahl a von n Ziffern mit eingeschlossen seyn

$$2Q\frac{a+1-1}{1}+Q\frac{a+1-10}{1}+Q\frac{a+1-10^2}{1}$$
$$+Q\frac{a+1-10^3}{1}+\cdots+Q\frac{a+1-10^{n-1}}{1}-a.$$

Da nun jederzeit $Q\frac{M}{1}=M$ ist, so wird eben diese Anzahl also ausgedrückt werden

$$(n+1)a+n-1(1+10+10^2+10^3+\cdots+10^{n-1})-a$$

oder kürzer

$$n(a+1)-\frac{10^n-1}{10-1}.$$

Setzen wir nun, die Zahl $c-1$ bestehe aus m Ziffern, so wird auf eine ähnliche Weise die Anzahl aller Ziffern, welche von 1 bis $c-1$ mit eingeschlossen enthalten sind, folgendermaßen ausgedrückt werden

$$mc - \frac{10^m - 1}{10 - 1},$$

folglich wird die verlangte Anzahl aller Ziffern, welche erfordert werden, um von der Zahl c bis a mit eingeschlossen alle Zahlen ihrer natürlichen Reihe nach zu schreiben, seyn

$$n(a+1) - \frac{10^n - 1}{10 - 1} - mc + \frac{10^m - 1}{10 - 1} \quad \text{oder} \quad n(a+1) - mc - \frac{10^n - 10^m}{10 - 1}.$$

9. Wenn wir also $a = 1$ Billion, und folglich $n = 13$ setzen, so wird die Anzahl aller Ziffern von 1 bis einer Billion mit eingeschlossen seyn

$$13\,(1\text{ Billion} + 1) - \frac{10^{13} - 1}{10 - 1},$$

das ist

$$13000000000013 - 1111111111111 \quad \text{oder} \quad 11888888888902.$$

Und die Anzahl aller Ziffern von 1700 bis 1763 mit eingeschlossen ist

$$4 \times 1764 - \frac{10^4 - 1}{10 - 1} - 4 \times 1700 + \frac{10^4 - 1}{10 - 1}$$

oder

$$4 \times 1764 - 4 \times 1700, \quad \text{das ist} \quad 4 \times 64 = 256.$$

Und die Anzahl aller Ziffern von 12 bis 1763 mit eingeschlossen wird seyn

$$4 \times 1764 - 2 \times 12 - \frac{10^4 - 10^2}{10 - 1}, \quad \text{das ist} \quad 7056 - 24 - 1100 \quad \text{oder} \quad 5932.$$

IV.

Man soll zwey Zahlen finden, eine größere a von n Ziffern, und eine kleinere b von m Ziffern, dergestalt, daß wenn die kleinere b von der größeren a so oft abgezogen wird, bis entweder nichts oder eine Zahl, die kleiner ist als b, übrig bleibt: die Anzahl aller hierzu erforderlichen Ziffern der größeren Zahl a gleich sey.

10. Laßt uns erstlich zwey solche Zahlen a und b suchen, da zugleich a durch b theilbar ist, und weil solchergestalt bey dem beständigen subtrahiren zuletzt nichts übrig bleibt, so erfordert unsere Aufgabe, daß da sey

$$2mQ\frac{a+1-10^{m-1}}{b}+Q\frac{a+1-10^{m}}{b}+Q\frac{a+1-10^{m+1}}{b}$$
$$+Q\frac{a+1-10^{m+2}}{b}+\cdots+Q\frac{a+1-10^{n-1}}{b}=a.$$

Um nun in dieser Gleichung die nächst größten Quotienten von der Größe a zu befreyen, als welche man hauptsächlich zu suchen hat, so nehme man den V. Satz des 6. § zu Hülf, und setze für

$$Q\frac{a+1-10^{m-1}}{b}=Q\frac{a-(10^{m-1}-1)}{b}=\frac{a}{b}-q\frac{10^{m-1}-1}{b},$$

imgleichen

$$Q\frac{a+1-10^{m}}{b}=\frac{a}{b}-q\frac{10^{m}-1}{b}$$
$$Q\frac{a+1-10^{m+1}}{b}=\frac{a}{b}-q\frac{10^{m+1}-1}{b}$$

und so weiter für alle übrige nächst größte Quotienten.

Hierdurch wird nun unsere Gleichung in die folgende verwandelt

$$(m+n)\frac{a}{b}-2mq\frac{10^{m-1}-1}{b}-q\frac{10^{m}-1}{b}-q\frac{10^{m+1}-1}{b}$$
$$-q\frac{10^{m+2}-1}{b}-\cdots-q\frac{10^{n-1}-1}{b}=a.$$

Man setze der Kürze halber

$$2mq\frac{10^{m-1}-1}{b}+q\frac{10^{m}-1}{b}+q\frac{10^{m+1}-1}{b}+\cdots+q\frac{10^{n-1}-1}{b}=R,$$

so wird

$$(m+n)\frac{a}{b}-R=a,$$

folglich

$$a=\frac{Rb}{m+n-b}.$$

Wobey folgende Stücke zu beobachten sind: erstlich $b<m+n$, zweytens Rb muß durch $m+n-b$ theilbar seyn, drittens a muß aus n Ziffern, so wie viertens b aus m Ziffern bestehen.

Der ersten und zweyten Bedingung wird am leichtesten ein Genüge geleistet, wenn $b = m + n - 1$ gesetzt wird: es wird aber in diesem Falle

$$R = 2mq\frac{10^{m-1}-1}{m+n-1} + q\frac{10^{m}-1}{m+n-1} + q\frac{10^{m+1}-1}{m+n-1} + \cdots + q\frac{10^{n-1}-1}{m+n-1}$$

und die verlangte Zahl

$$a = Rb,$$

welche aber aus n Ziffern bestehen muß. Da nun $b < m + n$, so kann die Zahl b nicht wohl aus mehr als einer Ziffer bestehen, die Zahl a bestünde dann aus 9 oder mehrern Ziffern; wenn wir also keine allzu große Zahlen für a verlangen, so können wir immer setzen, b bestehe aus einer Ziffer, das ist m wäre $= 1$; folglich in unserm Fall $b = m + n - 1 = 1 + n - 1 = n$,

$$R = 2q\frac{10^{0}-1}{n} + q\frac{10-1}{n} + q\frac{10^{2}-1}{n} + \cdots + q\frac{10^{n-1}-1}{n},$$

oder weil $2q\frac{10^{0}-1}{n} = 2q\frac{0}{n} = 0$, so wird

$$R = q\frac{10-1}{n} + q\frac{10^{2}-1}{n} + q\frac{10^{3}-1}{n} + \cdots + q\frac{10^{n-1}-1}{n}$$

und die beyden verlangten Zahlen

$$a = nR \quad \text{und} \quad b = n,$$

wo also $n < 9$ und a aus n Ziffern besteht.

Laßt uns also für n alle Zahlen von 2 bis 9 setzen, und wir werden folgende Zahlen für a und b erhalten, welche alle der Aufgabe ein Genügen leisten.

Wenn	$n =$	2	3	4	5	6	7	8	9
so wird	$R =$	4	36	275	2218	18515	158727	1388883	12345678
und	$a =$	8	108	1100	11090	111090	1111089	11111064	111111102
	$b =$	2	3	4	5	6	7	8	9

Wo alle Zahlen für a aus n Ziffern bestehen, die allererste 8 ausgenommen, welche aber nichts destoweniger der Aufgabe ein Genügen leistet. Überdem

so ist hier allenthalben die kleinere Zahl b der Anzahl der Ziffern der größeren a gleich, und diese a hinwiederum durch jene b theilbar.

Wir können nun auch, um der 1ten Bedingung $b < m + n$ ein Genügen zu leisten, setzen $b = m + n - 2$, oder $b = m + n - 3$, oder noch $b = m + n - 4$ und so weiter; aber man wird sich leichte überführen können, daß wenn alsdann auch Rb durch $m + n - b$ theilbar wird, die für a gefundene Zahl allemal aus weniger als n Ziffern, wider die 3te Bedingung, bestehen würde.

11. Nun laßt uns solche Zahlen für a und b suchen, daß $a + 1$ durch b theilbar werde. Weil alsdann vermöge des V. Satzes (§ 6)

$$Q\frac{a+1-10^{m-1}}{b} = \frac{a+1}{b} - q\frac{10^{m-1}}{b},$$

so wird man folgende Gleichung aufzulösen haben

$$(n+m)\frac{a+1}{b} - 2mq\frac{10^{m-1}}{b} - q\frac{10^m}{b} - q\frac{10^{m+1}}{b} - \cdots - q\frac{10^{n-1}}{b} \pm 1 = a,$$

wo nämlich das Zeichen + gilt, wenn b aus mehr als einer Ziffer besteht, und das Zeichen — wird allemal Statt haben, wenn b nur eine Ziffer ist.[1]) Nun setze man wiederum der Kürze halber

$$2mq\frac{10^{m-1}}{b} + q\frac{10^m}{b} + q\frac{10^{m+1}}{b} + \cdots + q\frac{10^{n-1}}{b} = R,$$

so wird

$$\frac{(n+m)(a+1)}{b} - R \pm 1 = a$$

und folglich der gesuchte Werth von a

$$= \frac{b(R \mp 1) - n - m}{n + m - b},$$

wo nunmehro aber das Zeichen -1 gilt, wenn b aus mehr als einer Ziffer, und +, wenn b nur aus einer Ziffer besteht.

---

1) Der letzte Rest von $\frac{a}{b}$ ist nicht, wie ALBRECHT EULER zu glauben scheint, gleich 1, sondern gleich $b - 1$. Da sich der Verfasser aber in der Folge auf $m = 1$ beschränkt, so ist der Fehler ohne Bedeutung. F. R.

Da nun hier wiederum $b < m + n$ seyn muss, so laßt uns setzen, b bestehe nur aus einer Figur, das ist, m sey $= 1$,

$$R = 2q\frac{1}{b} + q\frac{10}{b} + q\frac{10^2}{b} + q\frac{10^3}{b} + \cdots + q\frac{10^{n-1}}{b},$$

oder weil $q\frac{1}{b} = 0$,

$$R = q\frac{10}{b} + q\frac{10^2}{b} + q\frac{10^3}{b} + q\frac{10^4}{b} + \cdots + q\frac{10^{n-1}}{b},$$

da wir dann erhalten

$$a = \frac{b(R+1) - n - 1}{n + 1 - b}.$$

Wobey wohl zu merken, daß 1lich b aus einer und a aus n Ziffern bestehen muß, 2tens $b < n + 1$, folglich $n < 10$, 3tens muß $b(R+1) - n - 1$ durch $n + 1 - b$ theilbar seyn.

Wir wollen also sogleich den Nenner $n + 1 - b = 1$ setzen, oder es sey wie in dem vorhergehenden § $b = n$, so wird

$$R = q\frac{10}{n} + q\frac{10^2}{n} + q\frac{10^3}{n} + \cdots + q\frac{10^{n-1}}{n}$$

und die gesuchte Zahl

$$a = nR - 1.$$

Wenn wir also für n alle Zahlen unter 10 setzen, so werden wir aus dieser Quelle folgende Zahlen für a und b finden, die der Aufgabe in so fern ein Genügen leisten, als die Zahl a wirklich aus n Ziffern besteht.

Wenn	$n =$	2	3	4	5	6	7	8	9
so wird	$R =$	5	36	277	2222	18515	158727	1388888	12345678
und	$a =$	9	107	1107	11109	111089	1111088	11111103	111111101
	$b =$	2	3	4	5	6	7	8	9

Wo die Zahlen 9 und 2 nichts destoweniger der Aufgabe ein Genügen leisten, ob gleich hier 9 nicht aus 2 Ziffern, wie es seyn sollte, besteht.

Endlich so würde es uns hier eben so wenig, als in dem vorhergehenden § helfen, wenn wir nun ferner $b = n + m - 2 = n - 1$, oder $b = n + m - 3 = n - 2$

und so weiter setzen wollten; wir würden dadurch keine Werthe für a und b erlangen, so der Aufgabe ein Genügen leisten könnten, weil die Zahl a allezeit aus weniger als n Ziffern bestehen würde.

12. Nun sey drittens $a+2$ durch b theilbar, und die Zahlen, welche in dieser Hypothese der Aufgabe ein Genügen leisten, werden folgender Gestalt gefunden. Da wir immer voraussetzen können, daß die Zahl b nicht wohl aus mehr als einer Ziffer bestehen kann, es sey dann, daß die Zahl a sehr groß seyn soll, so lasst uns setzen $m=1$; und weil der letzte Rest von $\frac{a}{b}$ hier 2[1]) ist, und folglich so, wie die Zahl b, aus einer Ziffer besteht, so wird man folgende Gleichung aufzulösen haben:

$$2Q\frac{a+1-1}{b}+Q\frac{a+1-10}{b}+Q\frac{a+1-10^2}{b}+\cdots+Q\frac{a+1-10^{n-1}}{b}-1=a$$

oder, weil

$$Q\frac{a+1-10^m}{b}=Q\frac{a+2-(10^m+1)}{b}=\frac{a+2}{b}-q\frac{10^m+1}{b}$$

und $q\frac{2}{b}=0$ (wenn nämlich $b>2$),

$$\frac{(n+1)(a+2)}{b}-q\frac{10+1}{b}-q\frac{10^2+1}{b}-q\frac{10^3+1}{b}-\cdots-q\frac{10^{n-1}+1}{b}-1=a.$$

Es sey wiederum

$$q\frac{10+1}{b}+q\frac{10^2+1}{b}+q\frac{10^3+1}{b}+q\frac{10^4+1}{b}+\cdots+q\frac{10^{n-1}+1}{b}=R,$$

so wird

$$\frac{(n+1)(a+2)}{b}-R-1=a$$

und folglich die gesuchte Zahl

$$a=\frac{b(R+1)-2n-2}{n+1-b}.$$

Damit nun der Zehler $b(R+1)-2n-2$ gewiss durch den Nenner $n+1-b$ theilbar werde, und dabey die Zahl a aus n Ziffern bestehe, so laßt uns, wie

1) Er ist eigentlich $b-2$, was aber für das Folgende ohne Bedeutung ist. Siehe die Anmerkung p. 61. F. R.

bey den vorhergehenden Hypothesen, setzen $n+1-b=1$ oder $b=n$; und wir werden bekommen:

$$R = q^{\frac{10+1}{n}} + q^{\frac{10^2+1}{n}} + q^{\frac{10^3+1}{n}} + \cdots + q^{\frac{10^{n-1}+1}{n}},$$

$$a = n(R-1)-2 \quad \text{und} \quad b = n;$$

folglich [1])

wenn	$n=$	3	4	5	6	7	8	9
so wird	$R=$	36	277	2222	18515	158728	1388888	12345678
und	$a=$	103	1102	11103	111082	1111087	11111094	111111091
	$b=$	3	4	5	6	7	8	9

13. Die Zahl b bestehe noch immer aus einer einzigen Ziffer, oder es sey $m=1$. Man setze aber jetzo auf eine allgemeinere Art, daß $a+f$ durch b theilbar sey. Da nun der letzte Rest f [2]) in diesem Fall auch nur aus einer einzigen Ziffer bestehen kann, so wird man folgender Gleichung ein Genügen zu leisten haben:

$$2Q^{\frac{a+f-10^0-f+1}{b}} + Q^{\frac{a+f-10-f+1}{b}} + Q^{\frac{a+f-10^2-f+1}{b}}$$

$$+ \cdots + Q^{\frac{a+f-10^{n-1}-f+1}{b}} - 1 = a,$$

oder weil

$$Q^{\frac{a+f-10^m-f+1}{b}} = \frac{a+f}{b} - q^{\frac{10^m+f-1}{b}},$$

$$\frac{(n+1)(a+f)}{b} - 2q^{\frac{f}{b}} - q^{\frac{10+f-1}{b}} - q^{\frac{10^2+f-1}{b}} - q^{\frac{10^3+f-1}{b}}$$

$$- \cdots - q^{\frac{10^{n-1}+f-1}{b}} - 1 = a.$$

---

1) Die Spalte für $n=4$ ist in der Editio princeps, augenscheinlich aus Versehen, ausgefallen. F. R.

2) Soll heißen $b-f$. Siehe die Anmerkungen p. 61 und 63. F. R.

Man setze nun der Kürze willen

$$2q\frac{f}{b}+q\frac{10+f-1}{b}+q\frac{10^2-f+1}{b}+\cdots+q\frac{10^{n-1}+f-1}{b}=R,$$

so wird

$$\frac{(n+1)(a+f)}{b}-R-1=a,$$

folglich

$$a=\frac{b(R+1)-nf-f}{n+1-b}.$$

Wo wiederum a aus n Ziffern bestehen und $b(R+1)-nf-f$ durch $n+1-b$ theilbar seyn muß. Nun setze man zu diesem Ende wie in den vorhergehenden § $b=n$; so wird

$$R=2q\frac{f}{n}+q\frac{10+f-1}{n}+q\frac{10^2+f-1}{n}+\cdots+q\frac{10^{n-1}+f-1}{n},$$

oder weil f allezeit kleiner als b und $q\frac{f}{b}=0$,

$$R=q\frac{10+f-1}{n}+q\frac{10^2+f-1}{n}+q\frac{10^3+f-1}{n}+\cdots+q\frac{10^{n-1}+f-1}{n}$$

und die verlangten beyden Zahlen a und b werden seyn

$$a=n(R+1)-nf-f=n(R+1-f)-f \quad \text{und} \quad b=n,$$

wo a aus n Ziffern, b aber nur aus einer Ziffer bestehen muss.

14. Wenn aber b aus mehr als aus einer Ziffer besteht, und $a+f$ durch b theilbar ist, so wird man vor allen Dingen auf die Anzahl der Ziffern des letzten Rests f[1]) Achtung zu geben haben, ob derselbe nämlich aus m oder aus weniger als m, z. E. aus μ Ziffern[2]) bestehe. Im ersten Fall wird man dieser Gleichung

1) Soll heißen $b-f$. Dieser Fehler kehrt nun immer wieder; da er aber in der Folge ohne Bedeutung ist, so habe ich darauf verzichtet, ihn immer von neuem hervorzuheben. F. R.

2) Im Original steht ungeschickter Weise *aus n Ziffern.* Erst nachher wird dieses n durch μ ersetzt. F. R.

$$2mQ\frac{a+f-10^{m-1}-f+1}{b}+Q\frac{a+f-10^{m}-f+1}{b}+Q\frac{a+f-10^{m+1}-f+1}{b}$$
$$+\cdots+Q\frac{a+f-10^{n-1}-f+1}{b}-m=a$$

und im andern Fall folgender Gleichung

$$2mQ\frac{a+f-10^{m-1}-f+1}{b}+Q\frac{a+f-10^{m}-f+1}{b}+Q\frac{a+f-10^{m+1}-f+1}{b}$$
$$+\cdots+Q\frac{a+f-10^{n-1}-f+1}{b}+\mu=a$$

ein Genügen leisten müssen.

Wir wollen diese beyden Gleichungen zusammen durch die folgende vorstellen:

$$2mQ\frac{a+f-10^{m-1}-f+1}{b}+Q\frac{a+f-10^{m}-f+1}{b}+Q\frac{a+f-10^{m+1}-f+1}{b}$$
$$+\cdots+Q\frac{a+f-10^{n-1}-f+1}{b}\left\{\begin{matrix}-m\\+\mu\end{matrix}\right\}=a,$$

oder weil $a+f$ durch b theilbar und

$$Q\frac{a+f-10^{m}-f+1}{b}=\frac{a+f}{b}-q\frac{10^{m}+f-1}{b},$$

so wird

$$\frac{(n+m)(a+f)}{b}-2mq\frac{10^{m-1}+f-1}{b}-q\frac{10^{m}+f-1}{b}-q\frac{10^{m+1}+f-1}{b}$$
$$-\cdots-q\frac{10^{n-1}+f-1}{b}\left\{\begin{matrix}-m\\+\mu\end{matrix}\right\}=a.$$

Man setze nun

$$2mq\frac{10^{m-1}+f-1}{b}+q\frac{10^{m}+f-1}{b}+q\frac{10^{m+1}+f-1}{b}+\cdots+q\frac{10^{n-1}+f-1}{b}=R,$$

so wird

$$a=\frac{(n+m)(a+f)}{b}-R\left\{\begin{matrix}-m\\+\mu\end{matrix}\right\},$$

folglich die verlangte Zahl

$$a=\frac{\left\{\begin{matrix}R+m\\R-\mu\end{matrix}\right\}b-(n+m)f}{n+m-b},$$

welche mit der Zahl b, so nach Belieben genommen worden, der Aufgabe ein völliges Genügen leisten müssen.

Wo aber a aus n Ziffern bestehen, und $\left\{\begin{matrix} R+m \\ R-\mu \end{matrix}\right\} b-(n+m)f$ durch $n+m-b$ theilbar seyn, und noch über dem $b<n+m$ seyn muss, so wird, wie aus dem vorhergehenden erhellet, erfordert, daß man setze $n+m-b=1$ oder $b=n+m-1$. Es ist also

$$R=2mq\frac{10^{m-1}+f-1}{n+m-1}+q\frac{10^{m}+f-1}{n+m-1}+q\frac{10^{m+1}+f-1}{n+m-1}+\cdots+q\frac{10^{n-1}+f-1}{n+m-1}$$

und die beyden gesuchten Zahlen

$$a=\left\{\begin{matrix} R+m \\ R-\mu \end{matrix}\right\}(n+m-1)-(n+m)f \quad \text{und} \quad b=n+m-1.$$

Wo der Factor $R+m$ gilt, wenn der letzte Rest f aus m Ziffern, und der Factor $R-\mu$, wenn der letzte Rest f aus μ, das ist, aus weniger als m Ziffern, besteht.

Endlich so sind bey dieser letzten Auflösung, welche mit allem Recht eine allgemeine genannt werden kann, noch folgende Stücke, die Wahl der Zahlen m, n, f und μ betreffend, zu beobachten.

Erstlich weil $b=n+m-1$ aus m Ziffern bestehen muß, so wird, wenn wir die Anzahl der Ziffern der Zahl b zu 2 annehmen, n, das ist, die Anzahl der Ziffern der Zahl a, zum wenigsten 9 seyn; imgleichen wenn wir setzen wollen, daß die Zahl b aus 3 Ziffern bestehen soll, so muß die Zahl a nothwendig aus 98 oder mehrern Ziffern bestehen, und so weiter. Oder kürzer, wenn wir annehmen $m=2$, so muss $n>8$, und wenn wir setzen $m=3$, so muss $n>97$, und wenn $m=4$, so muss $n>996$, also überhaupt, wenn wir setzen, daß die Zahl b aus m Ziffern bestehet, so muss $n\geqq 10^{m-1}+1-m$, oder die Zahl a muss alsdann nothwendiger Weise aus mindestens $10^{m-1}+1-m$ Ziffern bestehen.

Zweytens muss $f<$ seyn als b; und der Buchstaben μ deutet uns die Anzahl der Ziffern dieses letzten Rests f an: wenn aber $\mu=m$, so wird

$$a=(R+m)(n+m-1)-(n+m)f,$$

und wenn $\mu<m$, so ist

$$a=(R-\mu)(n+m-1)-(n+m)f.$$

Ich will diese Auflösung mit einem Exempel beschließen.

Es sey $m = 2$, und weil alsdann $n > 8$, so laßt uns setzen $n = 9$; ferner so sey $f = 5$ und also $\mu = 1$; folglich, weil in diesem Fall $\mu < m$, so werden die gesuchten Zahlen seyn

$$a = (R - \mu)(n + m - 1) - (n + m)f \quad \text{und} \quad b = n + m - 1 = 10.$$

Es ist aber

$$R = 4q\frac{14}{10} + q\frac{104}{10} + q\frac{1004}{10} + \cdots + q\frac{100000004}{10},$$

folglich

$$R = 11111114, \quad R - \mu = 11111113$$

und die beyden Zahlen

$$a = 111111075 \quad \text{und} \quad b = 10,$$

welche der Aufgabe ein völliges Genügen leisten.

15. Ich kann nicht umhin noch eine besondere Auflösung der vorgelegten Aufgabe beyzufügen, welche, ob sie gleich nicht so allgemein als die kurz vorhergehende ist, dennoch mit leichter Mühe unendlich viel Zahlen für a und b giebt, so der Aufgabe ein Genügen leisten. Es sei $m = 1$, oder die Zahl b bestehe allezeit nur aus einer Ziffer, die Zahl a aber aus n Ziffern. Nun wird entweder a durch b theilbar seyn, oder nicht.

I. Es sey a durch b nicht theilbar. Wenn man sich demnach vorstellt, daß die Zahl b von der Zahl a so oft abgezogen wird, bis eine Zahl, die kleiner ist als b, übrig bleibt, so erhellet aus dem 4. §, daß die Anzahl aller zu schreibenden Ziffern, welche wir der Kürze halber durch den Buchstaben N andeuten wollen, seyn werde

$$N = 2Q\frac{a}{b} + Q\frac{a+1-10}{b} + Q\frac{a+1-10^2}{b} + Q\frac{a+1-10^3}{b} + \cdots + Q\frac{a+1-10^{n-1}}{b} - 1.$$

Man setze nun, daß $a + ib$ auch noch eine Zahl von n Ziffern sey, und die Anzahl aller zu schreibenden Ziffern (wenn nämlich b von $a + ib$ so oft abgezogen werden soll, bis eine Zahl, die kleiner ist als b, übrig bleibt) wird auf eine ähnliche Weise also ausgedrückt werden

$$2Q\frac{a+ib}{b}+Q\frac{a+1-10+ib}{b}+Q\frac{a+1-10^2+ib}{b}+Q\frac{a+1-10^3+ib}{b}$$
$$+\cdots+Q\frac{a+1-10^{n-1}+ib}{b}-1.$$

Es ist aber vermöge des im 6. § angeführten III. Satzes

$$Q\frac{a+ib}{b}=i+Q\frac{a}{b},\quad Q\frac{a+1-10+ib}{b}=i+Q\frac{a+1-10}{b}\quad\text{und so weiter,}$$

folglich wird diese letztere Anzahl aller zu schreibenden Ziffern seyn

$$(n+1)i+2Q\frac{a}{b}+Q\frac{a+1-10}{b}+Q\frac{a+1-10^2}{b}+Q\frac{a+1-10^3}{b}$$
$$+\cdots+Q\frac{a+1-10^{n-1}}{b}-1$$

oder kürzer

$$(n+1)i+N.$$

Damit nun solche Zahlen gefunden werden, welche der Aufgabe ein Genügen leisten, so darf für i nur ein solcher Werth gesucht werden, daß da sey

$$(n+1)i+N=a+ib,$$

daraus man dann erhält

$$i=\frac{a-N}{n+1-b}.$$

Man nehme also 2 Zahlen a von n Ziffern und b von einer Ziffer nach Belieben an; man suche hernach die Anzahl aller zu schreibenden Ziffern in Ansehung eben dieser Zahlen a und b, oder man berechne den Werth von N, so da ist

$$N=2Q\frac{a}{b}+Q\frac{a+1-10}{b}+Q\frac{a+1-10^2}{b}+Q\frac{a+1-10^3}{b}$$
$$+\cdots+Q\frac{a+1-10^{n-1}}{b}-1,$$

darauf werde gesucht eine Zahl i, welche ist

$$i=\frac{a-N}{n+1-b},$$

und dann werden die verlangten Zahlen, welche der Aufgabe ein Genügen leisten, seyn

$$a + ib \quad \text{und} \quad b.$$

Hierbey aber wird nothwendiger Weise erfordert: erstlich, daß i eine ganze Zahl sey; zweytens, daß $a + ib$ aus n Ziffern (so wie a) bestehe; drittens, daß a durch b nicht theilbar sey; und endlich, daß die Zahl b nur aus einer Ziffer bestehe.

Um nun der ersten Bedingniß am leichtesten ein Genügen zu leisten, so sey beständig $b = n$, also daß da sey

$$N = 2Q\frac{a}{n} + Q\frac{a+1-10}{n} + Q\frac{a+1-10^2}{n} + Q\frac{a+1-10^3}{n} + \cdots + Q\frac{a+1-10^{n-1}}{n} - 1,$$

$= a - N$ und die beyden verlangten Zahlen

$$a + ni \quad \text{oder} \quad (n+1)a - nN \quad \text{und} \quad n.$$

II. Wenn aber a durch b theilbar ist, so ist aus dem vorhergehenden offenbar, daß man für N nur zu schreiben habe

$$N = 2Q\frac{a}{n} + Q\frac{a+1-10}{n} + Q\frac{a+1-10^2}{n} + Q\frac{a+1-10^3}{n} + \cdots + Q\frac{a+1-10^{n-1}}{n},$$

und alsdann wird man wie kurz vorher erhalten $i = a - N$ und die beyden verlangten Zahlen

$$a + ni \quad \text{oder} \quad (n+1)a - nN \quad \text{und} \quad n.$$

Einige Exempel dieser letzten Auflösung sollen diese Abhandlung beschließen.

I. Es sey $a = 100$, $n = 3$; so wird

$$N = 2Q\frac{100}{3} + Q\frac{91}{3} + Q\frac{1}{3} - 1 = 100 - 1 = 99,$$

$i = 100 - 99 = 1$, $ni = 3$ und die gesuchten Zahlen 103 und 3.

Es sey $a = 200$, $n = 3$; so wird $N = 232 - 1 = 231$, $i = -31$, $ni = -93$ und folglich die beyden verlangten Zahlen 107 und 3 seyn.

Es sey $a = 120$, $n = 3$; und weil hier a durch b theilbar ist, so wird nach der letzten Formul $N = 124$, folglich $i = -4$, $ni = -12$ und die beyden gesuchten Zahlen sind 108 und 3; welche drey paar Zahlen wir auch schon in den 10ten, 11ten und 12ten § gefunden haben.

Überhaupt, so lange $n = 3$ ist, und für a auch alle mögliche Zahlen von 3 Ziffern gesetzt werden, so wird man dannoch nicht mehr als 3 paar Zahlen, nämlich 103 und 3, 107 und 3, 108 und 3 erhalten, welche der Aufgabe ein Genügen leisten. Dieses ist schon aus der vorhergehenden Auflösung deutlich, und wird durch folgende Tafel noch weiter bekräftiget.

Wenn	$a =$	200	201	202	203	204	205	206	207	208
so wird	$N =$	231	232	235	235	236	239	239	240	243
und	$i =$	— 31	— 31	— 33	— 32	— 32	— 34	— 33	— 33	— 35
folglich	$a + in =$	107	108	103	107	108	103	107	108	103
und	$n =$	3	3	3	3	3	3	3	3	3

II. Nun sey $n = 4$; und man schreibe für a lauter Zahlen von 4 Ziffern, so wird man viererley paar Zahlen erhalten, welche der Aufgabe ein Genügen leisten.

Man setze	$a =$	1000	1001	1002	1003	1004
so wird	$N =$	975	976	977	977	980
und	$i =$	25	25	25	26	24
folglich	$a + in =$	1100	1101	1102	1107	1100
und	$n =$	4	4	4	4	4

III. Es sey $n = 7$; und folglich soll die Zahl a aus 7 Ziffern bestehen; und wir werden hier auch sieben paar Zahlen erhalten, welche der Aufgabe ein Genügen leisten. Nämlich

wenn $a =$	so wird $N =$	$i =$	und die beyden gesuchten Zahlen
1111111	1111115	— 4	1111083 und 7
1111112	1111116	— 4	1111084 und 7
1111113	1111117	— 4	1111085 und 7
1111114	1111118	— 4	1111086 und 7
1111115	1111119	— 4	1111087 und 7
1111116	1111120	— 4	1111088 und 7
1111117	1111121	— 4	1111089 und 7
1111118	1111123	— 5	1111083 und 7
1111119	1111124	— 5	1111084 und 7

DE USU NOVI ALGORITHMI IN PROBLEMATE PELLIANO SOLVENDO[1])

Commentatio 323 indicis ENESTROEMIANI
Novi commentarii academiae scientiarum Petropolitanae 11 (1765), 1767, p. 28—66
Summarium ibidem p. 7—9

SUMMARIUM

In Arithmetica indefinita, quae DIOPHANTEA adpellari solet, saepenumero problematum resolutio eo nititur, ut expressiones sub hac forma $lxx + mx + n$ contentae quadrata sint efficiendae; quod, simulac unus ipsius x valor quaesito satisfaciens fuerit cognitus, infinite multis modis etiam in integris ipsius x valoribus praestari potest, quicunque etiam pro l, m et n numeri integri ponantur, modo l sit numerus positivus non quadratus. Atque solutionum harum innumerabilium insigne compendium ex eo petitur, quod constet omnes istos ipsius x valores idoneos secundum seriem recurrentem progredi, cuius singuli termini ex binis praecedentibus certa et constante lege determinantur.

Semper autem huius generis resolutiones ad hoc redeunt, ut proposito numero quocunque l inveniatur numerus quadratus qq, qui per illum multiplicatus adscita unitate iterum fiat quadratus, sive ut $lqq + 1$ fiat $= pp$; quod quidem in fractis atque paucis quibusdam casibus obviis facile expeditur, verum si pro quovis valore ipsius l valores ipsius q integri desiderentur, multum difficultatis habet adeoque dignum omnino est, in quo Geo-

1) Vide ad hanc dissertationem praeter Commentationes 29 et 279 p. 75 laudatas etiam EULERI epistolas d. 10. Aug. 1730, 4. Aug. 1753, 23. Aug. 1755 ad CHR. GOLDBACH scriptas, *Correspondance math. et phys. publiée par P. H. Fuss*, St.-Pétersbourg 1843, t. I, p. 35, 614, 627; *LEONHARDI EULERI Opera omnia*, series III. Vide porro L. EULER, *Vollständige Anleitung zur Algebra*, St. Petersburg 1770, Zweyter Theil, zweyter Abschnitt, Cap. 7; *LEONHARDI EULERI Opera omnia*, series I, vol. 1, nec non Commentationes 452, 454, 559 in hoc vol. 3 et in vol. 4 contentas.

Ceterum vide H. KONEN, *Geschichte der Gleichung* $t^2 - Du^2 = 1$, Leipzig 1901. F. R.

metrarum se exerceat industria. Quam PELLIUS[1]) olim dedit, in se ingeniosissima est solutio; ad quam taediosos autem et molestos calculos, cum continuis radicum extractionibus absolvatur, ea deducat, tentanti mox patebit. Hic igitur Ill. Auctor novum quoddam Algorithmi genus, cuius vim et naturam iam pridem[2]) in his Commentariis demonstravit, huic problemati adplicuit atque pro omnibus valoribus ipsius l centenarium non superantibus idoneos valores q methodo maxime concinna et facili actu computavit. Scilicet ut sit $lqq+1=pp$, evidens est esse proxime $\sqrt{l}=\frac{p}{q}$, quae fractio valorem irrationalem $\sqrt{l}$ tam prope exprimit, ut id nisi adhibendo maiores numeros adcuratius fieri nequeat. Ante omnia igitur Ill. Auctor methodum exposuit ope fractionum continuarum radices quadratas evolvendi; atque tum adhibitis novi Algorithmi subsidiis pro quolibet casu p et q ita definire docuit, ut $lqq+1$ quadratum fieret, ipsamque methodum evolutis multis exemplis stabilivit atque illustravit, idque potissimum in numeris admodum magnis; si enim verbi gratia assumatur $l=61$, reperitur valor ipsius $q=226153980$ atque ipsius $p=1766319049$, ubi simul certum est non dari numeros minores casui satisfacientes; ad quos numeros cum methodo PELLIANA nonnisi per taediosissimos calculos pervenire licuisset, non solum huius solutionis praestantia inde demonstratur, sed vix etiam aliud dari potest praeclarius specimen, quo Algorithmi istius novi ab Ill. Auctore inventi egregius usus Geometris possit commendari.

1. Quicunque numeri integri pro litteris l, m et n assumantur, innumerabiles quoque numeri integri pro x inveniri possunt, quibus haec formula

$$lxx+mx+n$$

reddatur quadratum, siquidem sequentes conditiones habeant locum:

I. ut l sit numerus positivus non quadratus,

II. ut pro x unus saltem valor sit cognitus.

Nam si l est numerus vel negativus vel quadratus, manifestum est infinitas solutiones in numeris integris exhiberi non posse, etiamsi una innotuerit. Tum vero etiam evenire potest, ut formula $lxx+mx+n$ naturae quadrati prorsus adversetur, uti fit hoc casu $3xx+2$. Verum statim atque unica solutio habetur, semper innumerabiles invenire licet.

2. Quare si statuamus

$$lxx+mx+n=yy$$

1) Sed vide notam 1 p. 77. F. R. 2) Vide notam 3 p. 77. F. R.

unusque casus constet, quo huic conditioni satisfiat, ita ut posito $x = a$ prodeat

$$laa + ma + n = bb$$

sicque sumto $x = a$ obtineatur $y = b$, regula[1]), cuius ope plures, imo infinitae solutiones elici possunt, ita se habet:

Primo ex dato numero l duo huiusmodi numeri p et q investigentur, ut sit

$$pp = lqq + 1 \quad \text{seu} \quad p = \sqrt{(lqq + 1)},$$

quibus inventis ex solutione prima cognita statim eruitur haec nova

$$x = pa + qb + \frac{m}{2l}(p - 1),$$

unde fit

$$y = pb + lqa + \frac{1}{2}mq,$$

ex qua deinceps simili modo aliae derivantur. Si enim hos valores loco a et b substituamus, nascitur tertia solutio ista

$$x = (2pp - 1)a + 2pqb + mqq$$

et

$$y = (2pp - 1)b + 2lpqa + mpq,$$

quae certe est in numeris integris, si forte praecedentes adhuc fuerint fracti.

3. Cum igitur hoc modo continuo novae solutiones inveniri queant, ad calculi compendium plurimum iuvat notasse continuos istos valores, tam ipsius x quam ipsius y, secundum seriem recurrentem progredi, cuius singuli termini per binos praecedentes certa et constante lege determinentur. Scilicet si fuerint valores hi continuo progredientes

ipsius x $a, \ldots P, Q, R, S$ etc.,

ipsius y $b, \ldots \mathfrak{P}, \mathfrak{Q}, \mathfrak{R}, \mathfrak{S}$ etc.,

1) Vide EULERI Commentationes 29 et 279 (indicis ENESTROEMIANI): *De solutione problematum DIOPHANTEORUM per numeros integros*, Comment. acad. sc. Petrop. 6 (1732/3), 1738, p. 175, imprimis § 5—7, et *De resolutione formularum quadraticarum indeterminatarum per numeros integros*, Novi comment. acad. sc. Petrop. 9 (1762/3), 1764, p. 3, imprimis § 13; *LEONHARDI EULERI Opera omnia*, series I, vol. 2, p. 6 et 576. F. R.

erit per legem seriei recurrentis

$$R = 2pQ - P + \frac{m(p-1)}{l}, \quad \mathfrak{R} = 2p\mathfrak{Q} - \mathfrak{P},$$

$$S = 2pR - Q + \frac{m(p-1)}{l}, \quad \mathfrak{S} = 2p\mathfrak{R} - \mathfrak{Q}.$$

Atque hinc isti valores expressionibus generalibus comprehendi possunt, quae ita se habent

$$x = \frac{2la + m + 2b\sqrt{l}}{4l}(p + q\sqrt{l})^\mu + \frac{2la + m - 2b\sqrt{l}}{4l}(p - q\sqrt{l})^\mu - \frac{m}{2l},$$

$$y = \frac{2la + m + 2b\sqrt{l}}{4\sqrt{l}}(p + q\sqrt{l})^\mu - \frac{2la + m - 2b\sqrt{l}}{4\sqrt{l}}(p - q\sqrt{l})^\mu,$$

unde, quicunque numeri integri exponenti μ tribuantur, semper valores rationales pro x et y resultant.[1])

4. Haec autem investigatio multo latius ita potest extendi, ut proposita inter binos numeros x et y huiusmodi aequatione

$$Axx + 2Bxy + Cyy + 2Dx + 2Ey + F = 0$$

omnes solutiones in numeris rationalibus et integris sint eruendae. Hic quidem pariter necesse est unam solutionem esse cognitam, quae sit $x = a$ et $y = b$, ita ut sit

$$Aaa + 2Bab + Cbb + 2Da + 2Eb + F = 0.$$

Tum vero quaerantur bini numeri p et q, ut sit

$$pp = (BB - AC)qq + 1,$$

quod quidem fieri nequit, nisi sit $BB > AC$. Atque nova solutio[2]) ita erit comparata

$$x = a(p + Bq) + bCq + Eq + \frac{BE - CD}{BB - AC}(p - 1),$$

$$y = b(p - Bq) - aAq - Dq + \frac{BD - AE}{BB - AC}(p - 1),$$

unde per eandem legem continuo plures elicere licet.

1) Vide paragraphos 12 et 18 Commentationis 279 supra, p. 75, laudatae. F. R.

2) Demonstrationem huius solutionis EULERUS postea dedit in Commentatione 452 (§ 14) huius voluminis. F. R.

5. Haec ideo in medium afferre est visum, ut intelligatur ad omnes huius generis resolutiones id omnino requiri, ut proposito quocunque numero integro positivo non quadrato l eiusmodi binos numeros pariter integros p et q inveniri oporteat, ut sit

$$pp = lqq + 1 \quad \text{seu} \quad p = \sqrt{(lqq + 1)}.$$

Atque hoc est illud problema olim quidem maxime celebratum a solutionis ingeniosissimae auctore PELLIANUM[1]) vocatum, quo pro quovis huiusmodi numero l numerus quadratus qq requiritur, qui per l multiplicatus adiuncta unitate fiat quadratus. In fractis quidem haec quaestio nullam haberet difficultatem, cum sumto $q = \frac{2rs}{lss - rr}$ fiat $p = \frac{lss + rr}{lss - rr}$; verum quia numeri integri desiderantur, negotium iterum eo revocatur, ut denominator $lss - rr$ in unitatem abeat.

6. Etiamsi autem solutio PELLIANA[2]) huius problematis sit elegantissima, tamen saepenumero tam operosis calculis implicatur, qui non minus taedii quam laboris creare solent. Cum igitur observassem Algorithmum illum novum, cuius nuper[3]) indolem exposui, ad hos calculos, quibus hic est opus, contrahendos insignia subsidia suppeditare, praeclarius certe specimen exhibere vix licebit, quo usus istius Algorithmi illustretur et commendetur. Ubi id imprimis notatu dignum occurrit, quod totum compendium inde subministratum potissimum idoneorum signorum usu contineatur.

7. Operationes, quibus PELLIUS[4]) est usus, aliunde quidem satis sunt notae egoque iam eas alia occasione fusius descripsi[5]); ex quo eo minus

1) Hoc vero tempore evictum est illud problema, quod recte FERMATIANUM, non PELLIANUM vocari debet, ab EULERO per errorem tantum PELLIO attributum esse. Vide H. KONEN, *Geschichte der Gleichung* $t^2 - Du^2 = 1$, Leipzig 1901, p. 29—49, et G. ENESTROEM, *Über den Ursprung der Benennung „PELLSCHE Gleichung"*, Biblioth. Mathem. 3_3, 1902, p. 204.

Problematis FERMATIANI solutio ab EULERO hic laudata a BROUNCKERO et WALLISIO exposita est. Vide J. WALLIS, *A Treatise of Algebra,* London 1685, chap. 98—99; *Opera*, t. II, Oxoniae 1693, p. 418—429. F. R.

2) Sed vide notam 1. F. R.

3) Vide Commentationem 281 (indicis ENESTROEMIANI): *Specimen algorithmi singularis,* Novi Comment acad. sc. Petrop. 9 (1762/3), 1764, p. 53; *LEONHARDI EULERI Opera omnia*, series I, vol. 14. F. R.

4) Sed vide notam 1. F. R.

5) Vide Commentationem 29 supra, p. 75, laudatam, imprimis § 16. F. R.

opus est, ut iis denuo explicandis hic immorer, cum totam Analysin hic longe alia ratione sim instituturus. Eius scilicet principium ex hoc fonte haurio, quod, cum sit $pp = lqq + 1$, proxime fiat $\frac{p}{q} = \sqrt{l}$, ex quo manifestum est $\frac{p}{q}$ eiusmodi esse fractionem, quae valorem irrationalem $\sqrt{l}$ tam prope exprimat seu eum tam parum excedat, ut id nisi maioribus numeris adhibendis accuratius fieri nequeat. Quod problema olim feliciter a WALLISIO[1]) solutum equidem quoque iam dudum per fractiones continuas multo commodius expedivi.[2])

8. Quo ergo hoc argumentum luculentius et ordine pertractem, primum radicem quadratam ex quovis numero in fractionem continuam evolvere docebo, idque methodo quam minime molesta. Deinde ostendam, quomodo inde fractiones $\frac{p}{q}$ valorem irrationalem $\sqrt{l}$ proxime exprimentes formari debeant in subsidium vocato Algorithmo novo supra explicato. Tum vero facile patebit, quomodo hinc numeros p et q definiri oporteat, ut fiat $pp = lqq + 1$. Denique tabulam subiungam, in qua pro omnibus numeris l centenarium non superantibus numeri bini p et q exhibentur.

DE EVOLUTIONE RADICUM QUADRATARUM PER FRACTIONES CONTINUAS

9. Operationes in hunc finem constituendae in exemplo facillime explicabuntur. Sit igitur proposita radix quadrata ex numero 13, et cum radix rationalis proxime minor sit 3, statuo

$$\sqrt{13} = 3 + \frac{1}{a}.$$

Hinc colligitur

$$a = \frac{1}{\sqrt{13} - 3} = \frac{\sqrt{13} + 3}{4},$$

cuius valor in integris proxime minor est 1, quod inde patet, si 3 loco $\sqrt{13}$ scribatur. Pono itaque

---

1) Vide notam 1 p. 77. F. R.

2) Vide Commentationem 71 nota 3 p. 7 laudatam. F. R.

$$a = \frac{\sqrt{13}+3}{4} = 1 + \frac{1}{b}$$

hincque

$$b = \frac{4}{\sqrt{13}-1} = \frac{4(\sqrt{13}+1)}{12} = \frac{\sqrt{13}+1}{3} = 1 + \frac{1}{c},$$

ergo

$$c = \frac{3}{\sqrt{13}-2} = \frac{3(\sqrt{13}+2)}{9} = \frac{\sqrt{13}+2}{3} = 1 + \frac{1}{d},$$

ergo

$$d = \frac{3}{\sqrt{13}-1} = \frac{3(\sqrt{13}+1)}{12} = \frac{\sqrt{13}+1}{4} = 1 + \frac{1}{e},$$

ergo

$$e = \frac{4}{\sqrt{13}-3} = \frac{4(\sqrt{13}+3)}{4} = \sqrt{13}+3 = 6 + \frac{1}{f},$$

ergo

$$f = \frac{1}{\sqrt{13}-3} = \frac{\sqrt{13}+3}{4} = 1 + \frac{1}{g};$$

atque hic operationem abrumpere licet, quia valor f ipsi a aequalis prodiit ideoque sequentes eodem ordine repetuntur. Sicque invenimus esse

$$\sqrt{13} = 3 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{6 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{6 + \text{etc.}}}}}}}}}}}$$

10. Quo indoles harum operationum melius perspiciatur, aliud exemplum prolixiorem calculum postulans adiungam. Proposita scilicet sit $\sqrt{61}$; cuius valor proxime minor cum sit 7, pono

$$\sqrt{61} = 7 + \frac{1}{a}$$

et operationes sequenti modo erunt instituendae:

$$\text{I.}\quad a = \frac{1}{\sqrt{61}-7} = \frac{\sqrt{61}+7}{12} = 1 + \frac{1}{b},$$

$$\text{II.}\quad b = \frac{12}{\sqrt{61}-5} = \frac{12(\sqrt{61}+5)}{36} = \frac{\sqrt{61}+5}{3} = 4 + \frac{1}{c},$$

$$\text{III.}\quad c = \frac{3}{\sqrt{61}-7} = \frac{3(\sqrt{61}+7)}{12} = \frac{\sqrt{61}+7}{4} = 3 + \frac{1}{d},$$

$$\text{IV.}\quad d = \frac{4}{\sqrt{61}-5} = \frac{4(\sqrt{61}+5)}{36} = \frac{\sqrt{61}+5}{9} = 1 + \frac{1}{e},$$

$$\text{V.}\quad e = \frac{9}{\sqrt{61}-4} = \frac{9(\sqrt{61}+4)}{45} = \frac{\sqrt{61}+4}{5} = 2 + \frac{1}{f},$$

$$\text{VI.}\quad f = \frac{5}{\sqrt{61}-6} = \frac{5(\sqrt{61}+6)}{25} = \frac{\sqrt{61}+6}{5} = 2 + \frac{1}{g},$$

$$\text{VII.}\quad g = \frac{5}{\sqrt{61}-4} = \frac{5(\sqrt{61}+4)}{45} = \frac{\sqrt{61}+4}{9} = 1 + \frac{1}{h},$$

$$\text{VIII.}\quad h = \frac{9}{\sqrt{61}-5} = \frac{9(\sqrt{61}+5)}{36} = \frac{\sqrt{61}+5}{4} = 3 + \frac{1}{i},$$

$$\text{IX.}\quad i = \frac{4}{\sqrt{61}-7} = \frac{4(\sqrt{61}+7)}{12} = \frac{\sqrt{61}+7}{3} = 4 + \frac{1}{k},$$

$$\text{X.}\quad k = \frac{3}{\sqrt{61}-5} = \frac{3\sqrt{(61}+5)}{36} = \frac{\sqrt{61}+5}{12} = 1 + \frac{1}{l},$$

$$\text{XI.}\quad l = \frac{12}{\sqrt{61}-7} = \frac{12(\sqrt{61}+7)}{12} = \sqrt{61}+7 = 14 + \frac{1}{m},$$

$$\text{XII.}\quad m = \frac{1}{\sqrt{61}-7},$$

ergo $m = a$ hincque porro $n = b$, $o = c$ etc. Ex quo indices pro fractione continua erunt

7, 1, 4, 3, 1, 2, 2, 1, 3, 4, 1, 14, 1, 4, 3, 1, 2 etc.

neque opus est ipsam fractionem continuam hic exhibere.

11. Adhuc aliud exemplum adiecisse iuvabit, ubi indicum numerus, antequam iidem recurrunt, fit impar. Esto hoc exemplum

$$\sqrt{67} = 8 + \frac{1}{a}$$

et operationes sequentes institui oportebit:

I. $a = \dfrac{1}{\sqrt{67}-8} = \dfrac{\sqrt{67}+8}{3} = 5 + \dfrac{1}{b}$,

II. $b = \dfrac{3}{\sqrt{67}-7} = \dfrac{3(\sqrt{67}+7)}{18} = \dfrac{\sqrt{67}+7}{6} = 2 + \dfrac{1}{c}$,

III. $c = \dfrac{6}{\sqrt{67}-5} = \dfrac{6(\sqrt{67}+5)}{42} = \dfrac{\sqrt{67}+5}{7} = 1 + \dfrac{1}{d}$,

IV. $d = \dfrac{7}{\sqrt{67}-2} = \dfrac{7(\sqrt{67}+2)}{63} = \dfrac{\sqrt{67}+2}{9} = 1 + \dfrac{1}{e}$,

V. $e = \dfrac{9}{\sqrt{67}-7} = \dfrac{9(\sqrt{67}+7)}{18} = \dfrac{\sqrt{67}+7}{2} = 7 + \dfrac{1}{f}$,

VI. $f = \dfrac{2}{\sqrt{67}-7} = \dfrac{2(\sqrt{67}+7)}{18} = \dfrac{\sqrt{67}+7}{9} = 1 + \dfrac{1}{g}$,

VII. $g = \dfrac{9}{\sqrt{67}-2} = \dfrac{9(\sqrt{67}+2)}{63} = \dfrac{\sqrt{67}+2}{7} = 1 + \dfrac{1}{h}$,

VIII. $h = \dfrac{7}{\sqrt{67}-5} = \dfrac{7(\sqrt{67}+5)}{42} = \dfrac{\sqrt{67}+5}{6} = 2 + \dfrac{1}{i}$,

IX. $i = \dfrac{6}{\sqrt{67}-7} = \dfrac{6(\sqrt{67}+7)}{18} = \dfrac{\sqrt{67}+7}{3} = 5 + \dfrac{1}{k}$,

X. $k = \dfrac{3}{\sqrt{67}-8} = \dfrac{3(\sqrt{67}+8)}{3} = \sqrt{67}+8 = 16 + \dfrac{1}{l}$,

XI. $l = \dfrac{1}{\sqrt{67}-8}$,

ergo $l = a$ indeque indices b, c, d etc. ordine recurrunt; quare indices fractionis continuae quaesitae sunt

8, 5, 2, 1, 1, 7, 1, 1, 2, 5, 16, 5, 2, 1, 1, 7, 1, 1, 2, 5, 16 etc.

12. His exemplis probe perpensis poterimus iam in genere operationes describere, quibus pro cuiusvis numeri radice quadrata fractio continua ipsi aequalis seu indices eam constituentes inveniuntur. Sit scilicet numerus propositus $= z$ eiusque radix integra proxime minor $= v$, vera autem hac fractione continua exprimatur

$$\sqrt{z} = v + \cfrac{1}{a + \cfrac{1}{b + \cfrac{1}{c + \cfrac{1}{d + \text{ etc.}}}}}$$

cuius indices a, b, c, d etc. post primum v per se cognitum sequentibus operationibus reperiuntur:

Capiatur	tum vero	eritque
I. $A = v$,	$\alpha = z - AA = z - vv$	$a < \frac{v + A}{\alpha}$,
II. $B = \alpha a - A$,	$\beta = \frac{z - BB}{\alpha} = 1 + a(A - B)$	$b < \frac{v + B}{\beta}$,
III. $C = \beta b - B$,	$\gamma = \frac{z - CC}{\beta} = \alpha + b(B - C)$	$c < \frac{v + C}{\gamma}$,
IV. $D = \gamma c - C$,	$\delta = \frac{z - DD}{\gamma} = \beta + c(C - D)$	$d < \frac{v + D}{\delta}$,
V. $E = \delta d - D$,	$\varepsilon = \frac{z - EE}{\delta} = \gamma + d(D - E)$	$e < \frac{v + E}{\varepsilon}$
	etc.,	

ubi in postrema columna signum $<$ indicat pro litteris a, b, c, d etc. sumi debere numeros integros proxime minores fractionibus adiectis, nisi hae fractiones ipsae in numeros integros abeant, quo casu hi ipsi erunt indices.

13. Pro indicibus igitur a, b, c, d etc. eliciendis binas alias numerorum series investigari oportet, quarum priorem litteris maiusculis

$$A, \quad B, \quad C, \quad D \text{ etc.},$$

posteriorem vero graecis

$$\alpha, \quad \beta, \quad \gamma, \quad \delta \text{ etc.}$$

designavi. Circa priores numeros observo eos numerum v nunquam superare posse. Eorum quidem primus est $A = v$, at cum sit $a < \frac{v+A}{\alpha}$, erit $\alpha a - A < v$ ideoque $B < v$ vel ad summum $B = v$, quo casu fit $\beta = 1$ et $b = 2v$. Deinde ob $b < \frac{v+B}{\beta}$ est $\beta b - B = C < v$ similique modo $D < v$, $E < v$ etc., ita ut horum numerorum nullus ipso v maior prodire possit. Deinde patet praeter casus, quibus graecarum litterarum quaepiam fit unitas, indices a, b, c etc. omnes ipso v maiores esse non posse, quandoquidem in fractionibus $\frac{v+B}{\beta}$, $\frac{v+C}{\gamma}$ etc. numeratores non excedere possunt $2v$, denominatores vero ad minimum sint $= 2$. Denique cum fuerit perventum ad indicem $= 2v$, sequentes iterum prodeunt a, b, c, d etc.

14. Illustremus etiam has operationes nonnullis exemplis.

I. Sit $z = 31$; erit $v = 5$.

$A = 5,$	$\alpha = 6,$	$a < \frac{10}{6} = 1,$
$B = 6 - 5 = 1,$	$\beta = 1 + 1 \cdot 4 = 5,$	$b < \frac{6}{5} = 1,$
$C = 5 - 1 = 4,$	$\gamma = 6 - 1 \cdot 3 = 3,$	$c < \frac{9}{3} = 3,$
$D = 9 - 4 = 5,$	$\delta = 5 - 3 \cdot 1 = 2,$	$d < \frac{10}{2} = 5,$
$E = 10 - 5 = 5,$	$\varepsilon = 3 + 5 \cdot 0 = 3,$	$e < \frac{10}{3} = 3,$
$F = 9 - 5 = 4,$	$\zeta = 2 + 3 \cdot 1 = 5,$	$f < \frac{9}{5} = 1,$
$G = 5 - 4 = 1,$	$\eta = 3 + 1 \cdot 3 = 6,$	$g < \frac{6}{6} = 1,$
$H = 6 - 1 = 5,$	$\theta = 5 - 1 \cdot 4 = 1,$	$h < \frac{10}{1} = 10.$

II. Sit $z = 46$; erit $v = 6$.

$A = 6$, $\alpha = 10$, $a < \frac{12}{10} = 1$,

$B = 10 - 6 = 4$, $\beta = 1 + 1 \cdot 2 = 3$, $b < \frac{10}{3} = 3$,

$C = 9 - 4 = 5$, $\gamma = 10 - 3 \cdot 1 = 7$, $c < \frac{11}{7} = 1$,

$D = 7 - 5 = 2$, $\delta = 3 + 1 \cdot 3 = 6$, $d < \frac{8}{6} = 1$,

$E = 6 - 2 = 4$, $\varepsilon = 7 - 1 \cdot 2 = 5$, $e < \frac{10}{5} = 2$,

$F = 10 - 4 = 6$, $\zeta = 6 - 2 \cdot 2 = 2$, $f < \frac{12}{2} = 6$,

$G = 12 - 6 = 6$, $\eta = 5 + 6 \cdot 0 = 5$, $g < \frac{12}{5} = 2$,

$H = 10 - 6 = 4$, $\theta = 2 + 2 \cdot 2 = 6$, $h < \frac{10}{6} = 1$,

$I = 6 - 4 = 2$, $\iota = 5 + 1 \cdot 2 = 7$, $i < \frac{8}{7} = 1$,

$K = 7 - 2 = 5$, $\varkappa = 6 - 1 \cdot 3 = 3$, $k < \frac{11}{3} = 3$,

$L = 9 - 5 = 4$, $\lambda = 7 + 3 \cdot 1 = 10$, $l < \frac{10}{10} = 1$,

$M = 10 - 4 = 6$, $\mu = 3 - 1 \cdot 2 = 1$, $m < \frac{12}{1} = 12$.

III. Sit $z = 54$; erit $v = 7$.

$A = 7$, $\alpha = 5$, $a < \frac{14}{5} = 2$,

$B = 10 - 7 = 3$, $\beta = 1 + 2 \cdot 4 = 9$, $b < \frac{10}{9} = 1$,

$C = 9 - 3 = 6$, $\gamma = 5 - 1 \cdot 3 = 2$, $c < \frac{13}{2} = 6$,

$D = 12 - 6 = 6$, $\delta = 9 + 6 \cdot 0 = 9$, $d < \frac{13}{9} = 1$,

$E = 9 - 6 = 3$, $\varepsilon = 2 + 1 \cdot 3 = 5$, $e < \frac{10}{5} = 2$,

$F = 10 - 3 = 7$, $\zeta = 9 - 2 \cdot 4 = 1$, $f < \frac{14}{1} = 14$.

15. Tabulam ergo hic subiungam pro singulorum numerorum radicibus quadratis indices continentem, ex quibus fractiones continuae ipsis aequales formari queant. Simul vero litterarum graecarum singulis convenientium valores subscripti reperiuntur.

Numeri surdi	Indices
$\sqrt{2}$	1, 2, 2, 2 etc. 1 1 1 1
$\sqrt{3}$	1, 1, 2, 1, 2, 1, 2 etc. 1 2 1 2 1 2 1
$\sqrt{5}$	2, 4, 4, 4 etc. 1 1 1 1
$\sqrt{6}$	2, 2, 4, 2, 4, 2, 4 etc. 1 2 1 2 1 2 1
$\sqrt{7}$	2, 1, 1, 1, 4, 1, 1, 1, 4 etc. 1 3 2 3 1 3 2 3 1
$\sqrt{8}$	2, 1, 4, 1, 4, 1, 4 etc. 1 4 1 4 1 4 1
$\sqrt{10}$	3, 6, 6, 6 etc. 1 1 1 1
$\sqrt{11}$	3, 3, 6, 3, 6, 3, 6 etc. 1 2 1 2 1 2 1
$\sqrt{12}$	3, 2, 6, 2, 6, 2, 6 etc. 1 3 1 3 1 3 1
$\sqrt{13}$	3, 1, 1, 1, 1, 6, 1, 1, 1, 1, 6 etc. 1 4 3 3 4 1 4 3 3 4 1
$\sqrt{14}$	3, 1, 2, 1, 6, 1, 2, 1, 6 etc. 1 5 2 5 1 5 2 5 1
$\sqrt{15}$	3, 1, 6, 1, 6, 1, 6 etc. 1 6 1 6 1 6 1
$\sqrt{17}$	4, 8, 8, 8, 8 etc. 1 1 1 1 1
$\sqrt{18}$	4, 4, 8, 4, 8, 4, 8, 4, 8 etc. 1 2 1 2 1 2 1 2 1
$\sqrt{19}$	4, 2, 1, 3, 1, 2, 8, 2, 1, 3, 1, 2, 8 etc. 1 3 5 2 5 3 1 3 5 2 5 3 1
$\sqrt{20}$	4, 2, 8, 2, 8, 2, 8, 2, 8 etc. 1 4 1 4 1 4 1 4 1
$\sqrt{21}$	4, 1, 1, 2, 1, 1, 8, 1, 1, 2, 1, 1, 8 etc. 1 5 4 3 4 5 1 5 4 3 4 5 1

Numeri surdi	Indices
$\sqrt{22}$	4, 1, 2, 4, 2, 1, 8, 1, 2, 4, 2, 1, 8 etc. 1 6 3 2 3 6 1 6 3 2 3 6 1
$\sqrt{23}$	4, 1, 3, 1, 8, 1, 3, 1, 8 etc. 1 7 2 7 1 7 2 7 1
$\sqrt{24}$	4, 1, 8, 1, 8, 1, 8 etc. 1 8 1 8 1 8 1
$\sqrt{26}$	5, 10, 10, 10 etc. 1 1 1 1
$\sqrt{27}$	5, 5, 10, 5, 10, 5, 10 etc. 1 2 1 2 1 2 1
$\sqrt{28}$	5, 3, 2, 3, 10, 3, 2, 3, 10 etc. 1 3 4 3 1 3 4 3 1
$\sqrt{29}$	5, 2, 1, 1, 2, 10, 2, 1, 1, 2, 10 etc. 1 4 5 5 4 1 4 5 5 4 1
$\sqrt{30}$	5, 2, 10, 2, 10, 2, 10, 2, 10 etc. 1 5 1 5 1 5 1 5 1
$\sqrt{31}$	5, 1, 1, 3, 5, 3, 1, 1, 10 etc. 1 6 5 3 2 3 5 6 1
$\sqrt{32}$	5, 1, 1, 1, 10, 1, 1, 1, 10 etc. 1 7 4 7 1 7 4 7 1
$\sqrt{33}$	5, 1, 2, 1, 10, 1, 2, 1, 10 etc. 1 8 3 8 1 8 3 8 1
$\sqrt{34}$	5, 1, 4, 1, 10, 1, 4, 1, 10 etc. 1 9 2 9 1 9 2 9 1
$\sqrt{35}$	5, 1, 10, 1, 10, 1, 10 etc. 1 10 1 10 1 10 1
$\sqrt{37}$	6, 12, 12, 12 etc. 1 1 1 1
$\sqrt{38}$	6, 6, 12, 6, 12, 6, 12 etc. 1 2 1 2 1 2 1
$\sqrt{39}$	6, 4, 12, 4, 12, 4, 12 etc. 1 3 1 3 1 3 1
$\sqrt{40}$	6, 3, 12, 3, 12, 3, 12 etc. 1 4 1 4 1 4 1
$\sqrt{41}$	6, 2, 2, 12, 2, 2, 12 etc. 1 5 5 1 5 5 1
$\sqrt{42}$	6, 2, 12, 2, 12, 2, 12 etc. 1 6 1 6 1 6 1
$\sqrt{43}$	6, 1, 1, 3, 1, 5, 1, 3, 1, 1, 12 etc. 1 7 6 3 9 2 9 3 6 7 1

Numeri surdi	Indices
$\sqrt{44}$	6, 1, 1, 1, 2, 1, 1, 1, 12 etc. 1 8 5 7 4 7 5 8 1
$\sqrt{45}$	6, 1, 2, 2, 2, 1, 12, 1, 2, 2, 2, 1, 12 etc. 1 9 4 5 4 9 1 9 4 5 4 9 1
$\sqrt{46}$	6, 1, 3, 1, 1, 2, 6, 2, 1, 1, 3, 1, 12 etc. 1 10 3 7 6 5 2 5 6 7 3 10 1
$\sqrt{47}$	6, 1, 5, 1, 12, 1, 5, 1, 12 etc. 1 11 2 11 1 11 2 11 1
$\sqrt{48}$	6, 1, 12, 1, 12, 1, 12 etc. 1 12 1 12 1 12 1
$\sqrt{50}$	7, 14, 14, 14 etc. 1 1 1 1
$\sqrt{51}$	7, 7, 14, 7, 14, 7, 14 etc. 1 2 1 2 1 2 1
$\sqrt{52}$	7, 4, 1, 2, 1, 4, 14, 4, 1, 2, 1, 4, 14 etc. 1 3 9 4 9 3 1 3 9 4 9 3 1
$\sqrt{53}$	7, 3, 1, 1, 3, 14, 3, 1, 1, 3, 14 etc. 1 4 7 7 4 1 4 7 7 4 1
$\sqrt{54}$	7, 2, 1, 6, 1, 2, 14, 2, 1, 6, 1, 2, 14 etc. 1 5 9 2 9 5 1 5 9 2 9 5 1
$\sqrt{55}$	7, 2, 2, 2, 14, 2, 2, 2, 14, 2, 2, 2, 14 etc. 1 6 5 6 1 6 5 6 1 6 5 6 1
$\sqrt{56}$	7, 2, 14, 2, 14, 2, 14 etc. 1 7 1 7 1 7 1
$\sqrt{57}$	7, 1, 1, 4, 1, 1, 14 etc. 1 8 7 3 7 8 1
$\sqrt{58}$	7, 1, 1, 1, 1, 1, 1, 14 etc. 1 9 6 7 7 6 9 1
$\sqrt{59}$	7, 1, 2, 7, 2, 1, 14 etc. 1 10 5 2 5 10 1
$\sqrt{60}$	7, 1, 2, 1, 14 etc. 1 11 4 11 1
$\sqrt{61}$	7, 1, 4, 3, 1, 2, 2, 1, 3, 4, 1, 14 etc. 1 12 3 4 9 5 5 9 4 3 12 1
$\sqrt{62}$	7, 1, 6, 1, 14 etc. 1 13 2 13 1
$\sqrt{63}$	7, 1, 14, 1, 14 etc. 1 14 1 14 1
$\sqrt{65}$	8, 16, 16 etc. 1 1 1

Numeri surdi	Indices
$\sqrt{66}$	8, 8, 16, 8, 16 etc. 1 2 1 2 1
$\sqrt{67}$	8, 5, 2, 1, 1, 7, 1, 1, 2, 5, 16 etc. 1 3 6 7 9 2 9 7 6 3 1
$\sqrt{68}$	8, 4, 16, 4, 16 etc. 1 4 1 4 1
$\sqrt{69}$	8, 3, 3, 1, 4, 1, 3, 3, 16 etc. 1 5 4 11 3 11 4 5 1
$\sqrt{70}$	8, 2, 1, 2, 1, 2, 16 etc. 1 6 9 5 9 6 1
$\sqrt{71}$	8, 2, 2, 1, 7, 1, 2, 2, 16 etc. 1 7 5 11 2 11 5 7 1
$\sqrt{72}$	8, 2, 16, 2, 16 etc. 1 8 1 8 1
$\sqrt{73}$	8, 1, 1, 5, 5, 1, 1, 16 etc. 1 9 8 3 3 8 9 1
$\sqrt{74}$	8, 1, 1, 1, 1, 16 etc. 1 10 7 7 10 1
$\sqrt{75}$	8, 1, 1, 1, 16 etc. 1 11 6 11 1
$\sqrt{76}$	8, 1, 2, 1, 1, 5, 4, 5, 1, 1, 2, 1, 16 etc. 1 12 5 8 9 3 4 3 9 8 5 12 1
$\sqrt{77}$	8, 1, 3, 2, 3, 1, 16 etc. 1 13 4 7 4 13 1
$\sqrt{78}$	8, 1, 4, 1, 16 etc. 1 14 3 14 1
$\sqrt{79}$	8, 1, 7, 1, 16 etc. 1 15 2 15 1
$\sqrt{80}$	8, 1, 16, 1, 16 etc. 1 16 1 16 1
$\sqrt{82}$	9, 18, 18, 18 etc. 1 1 1 1
$\sqrt{83}$	9, 9, 18, 9, 18 etc. 1 2 1 2 1
$\sqrt{84}$	9, 6, 18, 6, 18 etc. 1 3 1 3 1
$\sqrt{85}$	9, 4, 1, 1, 4, 18 etc. 1 4 9 9 4 1
$\sqrt{86}$	9, 3, 1, 1, 1, 8, 1, 1, 1, 3, 18 etc. 1 5 10 7 11 2 11 7 10 5 1

Numeri surdi	Indices
$\sqrt{87}$	9, 3, 18, 3, 18 etc. 1 6 1 6 1
$\sqrt{88}$	9, 2, 1, 1, 1, 2, 18 etc. 1 7 9 8 9 7 1
$\sqrt{89}$	9, 2, 3, 3, 2, 18 etc. 1 8 5 5 8 1
$\sqrt{90}$	9, 2, 18, 2, 18 etc. 1 9 1 9 1
$\sqrt{91}$	9, 1, 1, 5, 1, 5, 1, 1, 18 etc. 1 10 9 3 14 3 9 10 1
$\sqrt{92}$	9, 1, 1, 2, 4, 2, 1, 1, 18 etc. 1 11 8 7 4 7 8 11 1
$\sqrt{93}$	9, 1, 1, 1, 4, 6, 4, 1, 1, 1, 18 etc. 1 12 7 11 4 3 4 11 7 12 1
$\sqrt{94}$	9, 1, 2, 3, 1, 1, 5, 1, 8, 1, 5, 1, 1, 3, 2, 1, 18 etc. 1 13 6 5 9 10 3 15 2 15 3 10 9 5 6 13 1
$\sqrt{95}$	9, 1, 2, 1, 18 etc. 1 14 5 14 1
$\sqrt{96}$	9, 1, 3, 1, 18 etc. 1 15 4 15 1
$\sqrt{97}$	9, 1, 5, 1, 1, 1, 1, 1, 1, 5, 1, 18 etc. 1 16 3 11 8 9 9 8 11 3 16 1
$\sqrt{98}$	9, 1, 8, 1, 18 etc. 1 17 2 17 1
$\sqrt{99}$	9, 1, 18, 1, 18 etc. 1 18 1 18 1
$\sqrt{101}$	10, 20, 20 etc. 1 1 1
$\sqrt{102}$	10, 10, 20, 10, 20 etc. 1 2 1 2 1
$\sqrt{103}$	10, 6, 1, 2, 1, 1, 9, 1, 1, 2, 1, 6, 20 etc. 1 3 13 6 9 11 2 11 9 6 13 3 1
$\sqrt{104}$	10, 5, 20, 5, 20 etc. 1 4 1 4 1
$\sqrt{105}$	10, 4, 20, 4, 20 etc. 1 5 1 5 1
$\sqrt{106}$	10, 3, 2, 1, 1, 1, 1, 2, 3, 20 etc. 1 6 7 10 9 9 10 7 6 1
$\sqrt{107}$	10, 2, 1, 9, 1, 2, 20 etc. 1 7 13 2 13 7 1

Numeri surdi	Indices
$\sqrt{108}$	10, 2, 1, 1, 4, 1, 1, 2, 20 etc. 1 8 9 11 4 11 9 8 1
$\sqrt{109}$	10, 2, 3, 1, 2, 4, 1, 6, 6, 1, 4, 2, 1, 3, 2, 20 etc. 1 9 5 12 7 4 15 3 3 15 4 7 12 5 9 1
$\sqrt{110}$	10, 2, 20, 2, 20 etc. 1 10 1 10 1
$\sqrt{111}$	10, 1, 1, 6, 1, 1, 20 etc. 1 11 10 3 10 11 1
$\sqrt{112}$	10, 1, 1, 2, 1, 1, 20 etc. 1 12 9 7 9 12 1
$\sqrt{113}$	10, 1, 1, 1, 2, 2, 1, 1, 1, 20 etc. 1 13 8 11 7 7 11 8 13 1
$\sqrt{114}$	10, 1, 2, 10, 2, 1, 20 etc. 1 14 7 2 7 14 1
$\sqrt{115}$	10, 1, 2, 1, 1, 1, 1, 1, 2, 1, 20 etc. 1 15 6 11 9 10 9 11 6 15 1
$\sqrt{116}$	10, 1, 3, 2, 1, 4, 1, 2, 3, 1, 20 etc. 1 16 5 7 13 4 13 7 5 16 1
$\sqrt{117}$	10, 1, 4, 2, 4, 1, 20 etc. 1 17 4 9 4 17 1
$\sqrt{118}$	10, 1, 6, 3, 2, 10, 2, 3, 6, 1, 20 etc. 1 18 3 6 9 2 9 6 3 18 1
$\sqrt{119}$	10, 1, 9, 1, 20 etc. 1 19 2 19 1
$\sqrt{120}$	10, 1, 20, 1, 20 etc. 1 20 1 20 1

16. In omnibus his indicum seriebus periodi[1]) deprehenduntur modo strictiores modo largiores, quae indicibus iis, qui primo duplo sunt maiores, includuntur, atque hae periodi eo clarius in oculos incidunt, si primi indices cuiusque seriei duplicantur. Deinde in qualibet periodo idem indicum ordo, sive antrorsum sive retrorsum, observatur; ex quo in qualibet periodo vel unus datur index medius vel duo, prout terminorum numerus fuerit par vel impar. In litteris vero etiam graecis similes periodi observantur, ubi imprimis animadvertendum pro omnibus indicibus $2v$ litteram graecam in uni-

1) Qua cum observatione conferas § 18—20 Commentationis 71 nota 3 p. 7 laudatae, ubi exemplis demonstratur vicissim omnem fractionem continuam periodicam radicem esse aequationis secundi gradus, cuius coefficientes sunt numeri integri. F. R.

tatem abire. Hanc proprietatem insignem, quae in ipsis operationibus facilius perspicitur quam verborum ambage demonstratur, probe notasse in sequentibus plurimum interierit.

17. Ex his autem exemplis formas quasdam generales colligere licet, quae ita se habent:

I. Si $z = nn + 1$, erunt indices $\underset{1}{n}, \underset{1}{2n}, \underset{1}{2n}, \underset{1}{2n}$ etc.,

II. si $z = nn + 2$, erunt indices $\underset{1}{n}\ \underset{2}{n}\ \underset{1}{2n}\ \underset{2}{n}\ \underset{1}{2n}$ etc.,

III. si $z = nn + n$, erunt indices $\underset{1}{n}, \underset{n}{2}, \underset{1}{2n}, \underset{n}{2}, \underset{1}{2n}$ etc.,

IV. si $z = nn + 2n - 1$, erunt indices $\underset{1}{n}, \underset{2n-1}{1}, \underset{2}{n-1}, \underset{2n-1}{1}, \underset{1}{2n}$ etc.,

V. si $z = nn + 2n$, erunt indices $\underset{1}{n}, \underset{2n}{1}, \underset{1}{2n}, \underset{2n}{1}, \underset{1}{2n}$ etc.

Ac fractionum quidem continuarum ex his indicibus formatarum valor in genere facile definitur idemque, quem hic assignavimus, deprehenditur. Tum vero etiam patet,

VI. si sit $z = 4nn + 4$, fore indices $\underset{1}{2n}, \underset{4}{n}, \underset{1}{4n}, \underset{4}{n}, \underset{1}{4n}$ etc.,

VII. si sit $z = 9nn + 3$, fore indices $\underset{1}{3n}, \underset{3}{2n}, \underset{1}{6n}, \underset{3}{2n}, \underset{1}{6n}$ etc.,

VIII. si sit $z = 9nn + 6$, fore indices $\underset{1}{3n}, \underset{6}{n}, \underset{1}{6n}, \underset{6}{n}, \underset{1}{6n}$ etc.

DE RESOLUTIONE FORMULAE $p = \sqrt{(lqq + 1)}$ IN NUMERIS INTEGRIS

18. Inventis indicibus pro radice quadrata numeri cuiusvis z ea hoc modo per fractionem continuam exprimitur:

$$\sqrt{z} = v + \cfrac{1}{a + \cfrac{1}{b + \cfrac{1}{c + \cfrac{1}{d + \text{etc.}}}}}$$

atque ex his indicibus v, a, b, c, d etc. fractiones $\frac{x}{y}$ formari possunt, quae tam prope ad $\sqrt{z}$ accedunt, ut nonnisi maioribus numeris adhibendis eius valor accuratius exhiberi possit. Hae fractiones autem ita formantur:

$$\begin{array}{lllllll} \text{Indices} & v, & a, & b, & c, & \cdots\ m, & n, \\ \frac{x}{y} & \frac{1}{0}, & \frac{v}{1}, & \frac{av+1}{a}, & \frac{(ab+1)v+b}{ab+1}, & \cdots\ \frac{M}{P}, & \frac{N}{Q}, \quad \frac{nN+M}{nQ+P}, \end{array}$$

quae continuo propius valorem irrationalem $\sqrt{z}$ exprimunt.

19. Novus autem Algorithmus[1]) succinctum modum suppeditat has fractiones commode per indices repraesentandi, quae ita se habent:

$$\frac{1}{0}, \frac{(v)}{1}, \frac{(v,a)}{(a)}, \frac{(v,a,b)}{(a,b)}, \frac{(v,a,b,c)}{(a,b,c)}, \frac{(v,a,b,c,d)}{(a,b,c,d)} \text{ etc.;}$$

ubi cum ex natura progressionis sit

$$(v,a) = a(v) + 1, \quad (v,a,b) = b(v,a) + (v), \quad (v,a,b,c) = c(v,a,b) + (v,a),$$
$$(a) = a1 + 0, \qquad (a,b) = b(a) + 1, \qquad (a,b,c) = c(a,b) + (a),$$

erit etiam ex natura harum formularum

$$(v,a) = v(a) + 1, \quad (v,a,b) = v(a,b) + b, \quad (v,a,b,c) = v(a,b,c) + (b,c);$$

deinde etiam sequentes transformationes demonstravi[2])

$$(v,a,b,c,d,e) = v(a,b,c,d,e) + (b,c,d,e),$$
$$(v,a,b,c,d,e) = (v,a)(b,c,d,e) + v(c,d,e),$$
$$(v,a,b,c,d,e) = (v,a,b)(c,d,e) + (v,a)(d,e),$$
$$(v,a,b,c,d,e) = (v,a,b,c)(d,e) + (v,a,b)(e),$$

quas probe notasse in sequentibus plurimum iuvabit.

20. Videamus iam, quam prope singulae istae fractiones ad valorem $\sqrt{z}$ accedant, quod pro instituto nostro luculentissime inde patebit, si ex quaque

1) Vide Commentationem 281 nota 3 p. 77 laudatam. F. R.

2) Vide § 32 illius Commentationis 281. F. R.

fractione $\frac{x}{y}$ valorem $xx - zyy$ colligamus; quippe qui quo minor fuerit prae ipsis numeris x et y, eo exactius fractio $\frac{x}{y}$ valori $\sqrt{z}$ aequabitur. Ac primo quidem si $\frac{x}{y} = \frac{1}{0}$, erit $xx - zyy = 1$. Deinde sumto $\frac{x}{y} = \frac{v}{1}$ fit

$$xx - zyy = vv - z,$$

quae differentia per operationes supra (§ 12) expositas prima littera graeca negative sumta $-\alpha$ designatur. Porro posito $\frac{x}{y} = \frac{(v, a)}{(a)} = \frac{va+1}{a}$ colligitur

$$xx - zyy = (vv - z)aa + 2va + 1 = -\alpha aa + 2va + 1,$$

ergo

$$xx - zyy = 1 + a(2v - \alpha a) = 1 + a(A - B) = \beta$$

ob $v = A$ et $\alpha a = A + B$. Quocirca hoc casu fit $xx - zyy = \beta$.

21. Cum igitur nacti simus

$$vv - z = -\alpha \quad \text{et} \quad (v, a)^2 - z(a)^2 = \beta,$$

hinc ulterius progredi poterimus. Sit igitur

$$\frac{x}{y} = \frac{(v, a, b)}{(a, b)} = \frac{b(v, a) + v}{b(a) + 1}$$

atque adhibitis illis reductionibus obtinebimus

$$xx - zyy = \beta bb + 2vb(v, a) - 2zb(a) - \alpha,$$

ergo ob $(v, a) = v(a) + 1$ erit

$$xx - zyy = \beta bb - 2\alpha ab + 2vb - \alpha = -\alpha - b(2\alpha a - \beta b - 2v);$$

at est $v = A$, $\alpha a = A + B$ et $\beta b = B + C$ ideoque

$$xx - zyy = -\alpha - b(B - C) = -\gamma,$$

ita ut sit

$$(v, a, b)^2 - z(a, b)^2 = -\gamma.$$

22. Consideremus nunc fractionem sequentem

$$\frac{x}{y} = \frac{(v, a, b, c)}{(a, b, c)} = \frac{c(v, a, b) + (v, a)}{c(a, b) + a},$$

ex qua colligitur

$$xx - zyy = -\gamma cc + 2c(v, a, b)(v, a) + \beta - 2zca(a, b),$$

cuius pars media reducitur ad $2c(\beta b - \alpha a + v)$, unde ob $v = A$, $\alpha a = A + B$, $\beta b = B + C$, $\gamma c = C + D$ resultat

$$xx - zyy = \beta + c(C - D) = \delta,$$

ita ut sit

$$(v, a, b, c)^2 - z(a, b, c)^2 = \delta,$$

unde per inductionem sequentes valores facile colliguntur.

23. Ne autem hic inductioni nimium videar tribuisse, sequenti modo haec investigatio institui potest. Sit

$$\begin{aligned}
&(v)^2 && - z1^2 && = \mathfrak{A},\\
&(v, a)^2 && - z(a)^2 && = \mathfrak{B},\\
&(v, a, b)^2 && - z(a, b)^2 && = \mathfrak{C},\\
&(v, a, b, c)^2 && - z(a, b, c)^2 && = \mathfrak{D},\\
&(v, a, b, c, d)^2 && - z(a, b, c, d)^2 && = \mathfrak{E}
\end{aligned}$$

etc.,

ubi quidem iam vidimus esse $\mathfrak{A} = -\alpha$, $\mathfrak{B} = \beta$, $\mathfrak{C} = -\gamma$ etc. Cum vero sit

$$\begin{aligned}
&(v, a) && = a(v) && + 1, && (a) && = a, &&\\
&(v, a, b) && = b(v, a) && + (v), && (a, b) && = b(a) && + 1,\\
&(v, a, b, c) && = c(v, a, b) && + (v, a), && (a, b, c) && = c(a, b) && + (a),\\
&(v, a, b, c, d) && = d(v, a, b, c) && + (v, a, b), && (a, b, c, d) && = d(a, b, c) && + (a, b)
\end{aligned}$$

etc.,

habebimus

$$\begin{aligned}
\mathfrak{B} &= \mathfrak{A}aa + 1 + 2a(v),\\
\mathfrak{C} &= \mathfrak{B}bb + \mathfrak{A} + 2b((v, a)(v) - z(a)),\\
\mathfrak{D} &= \mathfrak{C}cc + \mathfrak{B} + 2c((v, a, b)(v, a) - z(a, b)(a)),\\
\mathfrak{E} &= \mathfrak{D}dd + \mathfrak{C} + 2d((v, a, b, c)(v, a, b) - z(a, b, c)(a, b)),\\
\mathfrak{F} &= \mathfrak{E}ee + \mathfrak{D} + 2e((v, a, b, c, d)(v, a, b, c) - z(a, b, c, d)(a, b, c))
\end{aligned}$$

etc.

24. Statuamus iam brevitatis gratia

$$\begin{aligned}
\mathfrak{B} &= 1 + \mathfrak{A}ab + 2a\cdot O,\\
\mathfrak{C} &= \mathfrak{A} + \mathfrak{B}bb + 2b\cdot P,\\
\mathfrak{D} &= \mathfrak{B} + \mathfrak{C}cc + 2c\cdot Q,\\
\mathfrak{E} &= \mathfrak{C} + \mathfrak{D}dd + 2d\cdot R,\\
\mathfrak{F} &= \mathfrak{D} + \mathfrak{E}ee + 2e\cdot S\\
&\text{etc.}
\end{aligned}$$

et ex superioribus reductionibus colligemus

$$\begin{aligned}
P - O &= a(v)^2 - za = \mathfrak{A}a,\\
Q - P &= b(v, a)^2 - zb(a)^2 = \mathfrak{B}b,\\
R - Q &= c(v, a, b)^2 - cz(a, b)^2 = \mathfrak{C}c,\\
S - R &= d(v, a, b, c)^2 - dz(a, b, c)^2 = \mathfrak{D}d\\
&\text{etc.}
\end{aligned}$$

sicque fiet

$$\begin{aligned}
O &= v,\\
P &= v + \mathfrak{A}a,\\
Q &= v + \mathfrak{A}a + \mathfrak{B}b,\\
R &= v + \mathfrak{A}a + \mathfrak{B}b + \mathfrak{C}c,\\
S &= v + \mathfrak{A}a + \mathfrak{B}b + \mathfrak{C}c + \mathfrak{D}d\\
&\text{etc.}
\end{aligned}$$

25. Formulae autem supra usurpatae praebent

$$\begin{aligned}
A &= v,\\
B &= -v + \alpha a,\\
C &= v - \alpha a + \beta b,\\
D &= -v + \alpha a - \beta b + \gamma c,\\
E &= v - \alpha a + \beta b - \gamma c + \delta d\\
&\text{etc.,}
\end{aligned}$$

unde patet esse

$$O = A \quad \text{et} \quad P = -B \quad \text{ob} \quad \mathfrak{A} = -\alpha.$$

Cum iam sit $\mathfrak{B} = 1 - \alpha aa + 2av = 1 + a(A - B)$, erit utique

$$\mathfrak{B} = \beta \quad \text{hincque} \quad Q = C,$$

ex quo porro colligitur

$$\mathfrak{C} = -\alpha + \beta bb - 2bB = -\alpha - b(2B - \beta b) = -\alpha - b(B - C),$$

sicque est

$$\mathfrak{C} = -\gamma \quad \text{et} \quad R = -D;$$

simili modo

$$\mathfrak{D} = \beta - \gamma cc + 2cC = \beta + c(2C - \gamma c) = \beta + c(C - D)$$

ideoque est

$$\mathfrak{D} = \delta \quad \text{et} \quad S = E.$$

Tum vero porro

$$\mathfrak{E} = -\gamma + \delta dd - 2dD = -\gamma - d(2D - \delta d) = -\gamma - d(D - E)$$

ac propterea

$$\mathfrak{E} = -\varepsilon,$$

unde superior inductio satis confirmatur.

26. Pro fractionibus ergo $\frac{x}{y}$ formulae radicali $\sqrt{z}$ proxime aequalibus sequentes adipiscimur relationes:

Si sumatur		erit
$x = 1,$	$y = 0,$	$xx = zyy + 1,$
$x = (v),$	$y = 1,$	$xx = zyy - \alpha,$
$x = (v, a),$	$y = (a),$	$xx = zyy + \beta,$
$x = (v, a, b),$	$y = (a, b),$	$xx = zyy - \gamma,$
$x = (v, a, b, c),$	$y = (a, b, c),$	$xx = zyy + \delta,$
$x = (v, a, b, c, d),$	$y = (a, b, c, d),$	$xx = zyy - \varepsilon$

etc.,

unde problema PELLIANUM solvetur, quoties litterarum graecarum per saltum excerptarum β, δ, ζ etc. quaepiam in unitatem abit.

27. Vidimus autem supra nonnisi iis indicibus, qui sunt $2v$, respondere litteram graecam in unitatem abeuntem; cum igitur quaelibet periodorum, quas in indicum ordine observavimus, indice $2v$ inchoetur, perspicuum est, si numeros x et y per indices primae periodi definiamus, fore vel

$$xx = zyy - 1$$

vel

$$xx = zyy + 1;$$

ac prius quidem evenit, si indicum singulas periodos constituentium numerus fuerit impar, posterius vero, si is fuerit par. Hoc igitur casu statim habetur solutio problematis PELLIANI, quo requiritur, ut sit

$$pp = zqq + 1,$$

quandoquidem capi oportet $p = x$ et $q = y$.

28. At si ex prima periodo prodeat $xx = zyy - 1$, quod evenit, si indicum numerus est impar, tum indices usque ad initium tertiae periodi ad definiendos numeros x et y capi possent; quorum numerus cum sit par, hoc modo idonei numeri pro p et q obtinerentur. Verum casu invento, quo fit $xx = zyy - 1$, multo facilius inde numeri p et q reperiri possunt, ut sit $pp = zqq + 1$. Sumatur enim

$$p = 2xx + 1 \quad \text{et} \quad q = 2xy$$

eritque

$$pp - zqq = 4x^4 + 4xx + 1 - 4zxxyy = 1 + 4xx(xx - zyy + 1);$$

at $xx - zyy + 1 = 0$ ideoque

$$pp - zqq = 1 \quad \text{seu} \quad pp = zqq + 1,$$

quemadmodum problema PELLIANUM postulat.

Videamus igitur, quomodo pro quovis numero z ex indicibus inde natis numeri p et q sint definiendi, ut fiat $pp = zqq + 1$, ubi quidem casus secundum periodos percurramus.

I. CASUS QUO PRO NUMERO z INDICES SUNT v, $2v$, $2v$ etc.

29. Hic singulae periodi unicum indicem continent; sumto ergo

$$x = (v) \quad \text{et} \quad y = 1$$

erit

$$xx = zyy - 1.$$

Quamobrem ut fiat $pp = zqq + 1$, capiatur

$$p = 2xx + 1 = 2vv + 1 \quad \text{et} \quad q = 2xy = 2v.$$

Hic casus, ut supra vidimus, locum habet, si sit

$$z = vv + 1,$$

seu quo numerus z unitate superat quadratum; tum igitur capi debet

$$p = 2vv + 1 \quad \text{seu} \quad p = 2z - 1 \quad \text{et} \quad q = 2v,$$

quo pacto problemati Pelliano satisfit, ut sit $p = \sqrt{(zqq + 1)}$.

Ita si sit	erit	sicque
$z = 2$,	$p = 3$ et $q = 2$	$p = \sqrt{(2qq + 1)}$,
$z = 5$,	$p = 9$ et $q = 4$	$p = \sqrt{(5qq + 1)}$,
$z = 10$,	$p = 19$ et $q = 6$	$p = \sqrt{(10qq + 1)}$,
$z = 17$,	$p = 33$ et $q = 8$	$p = \sqrt{(17qq + 1)}$

etc.

II. CASUS QUO PRO NUMERO z INDICES SUNT v, a, $2v$, a, $2v$ etc.

30. Prima periodus constat binis numeris v, a, unde sumtis

$$x = (v, a) = va + 1 \quad \text{et} \quad y = (a) = a$$

habebitur

$$xx = zyy + 1.$$

Ut igitur pro problemate PELLIANO fiat $pp = zqq + 1$, capi oportet

$$p = va + 1 \quad \text{et} \quad q = a.$$

Ex indicibus autem patet hunc casum locum habere, quoties fuerit numerus

$$z = vv + \frac{2v}{a},$$

unde intelligitur hunc casum in integris, de quibus hic agitur, existere non posse, nisi sit a divisor ipsius $2v$, ubi duo casus sunt considerandi:

1. Si $a = 2n$, erit $v = mn$ et $\frac{2v}{a} = m$;
2. si $a = 2n + 1$, erit $v = m(2n + 1)$ et $\frac{2v}{a} = 2m$.

III. CASUS QUO PRO NUMERO z INDICES SUNT $v, a, a, 2v, a, a, 2v$ etc.

31. Ex prima periodo sumtis numeris x et y, ita ut sit

$$x = (v, a, a) \quad \text{et} \quad y = (a, a),$$

erit

$$xx = zyy - 1;$$

unde ut fiat $pp = zqq + 1$, sumi debet

$$p = 2xx + 1 \quad \text{et} \quad q = 2xy.$$

Hic vero est

$$y = aa + 1 \quad \text{et} \quad x = vy + a,$$

unde numeri p et q facillime definiuntur. Ex indicibus autem numerus z eiusmodi habebit formam

$$z = vv + u$$

existente

$$u = \frac{2av + 1}{aa + 1},$$

unde patet numerum a esse debere parem. Si ergo statuatur $a = 2n$, necesse est sit

$$v = n + m(4nn + 1),$$

tumque fit

$$u = 1 + 4mn.$$

IV. CASUS QUO PRO NUMERO z INDICES SUNT

$v,\ a,\ b,\ a,\ 2v,\ a,\ b,\ a,\ 2v$ etc.

32. Quia numerus indicum in quaque periodo est par, si sumatur

$$x = (v, a, b, a) \quad \text{et} \quad y = (a, b, a),$$

erit

$$xx = zyy + 1$$

ideoque

$$p = x \quad \text{et} \quad q = y.$$

Per transformationes autem supra ostensas duplicatio indicum tolli potest hoc modo

$$x = (a)(v, a, b) + (v, a) \quad \text{et} \quad y = (a)(a, b) + (a).$$

Hinc si ex indicibus $v,\ a,\ b$ sequentes fractiones formentur

$$\text{indices} \qquad v, \quad a, \quad b$$

$$\text{fractiones} \quad \frac{1}{0}, \ \frac{\mathfrak{A}}{\mathfrak{a}}, \ \frac{\mathfrak{B}}{\mathfrak{b}}, \ \frac{\mathfrak{C}}{\mathfrak{c}},$$

ob

$$\mathfrak{A} = (v), \quad \mathfrak{B} = (v, a), \quad \mathfrak{C} = (v, a, b)$$

et

$$\mathfrak{a} = 1, \qquad \mathfrak{b} = (a), \qquad \mathfrak{c} = (a, b)$$

erit

$$x = \mathfrak{b}\mathfrak{C} + \mathfrak{a}\mathfrak{B} \quad \text{et} \quad y = \mathfrak{b}\mathfrak{c} + \mathfrak{a}\mathfrak{b}.$$

Ex indicibus autem fit

$$z = vv + u$$

existente

$$2v = m(a, b, a) - b(a, b)$$

et

$$u = m(a, b) - b(b).$$

V. CASUS QUO PRO NUMERO z INDICES SUNT

$v,\ a,\ b,\ b,\ a,\ 2v$ etc

33. Ob indicum cuiusque periodi numerum imparem, si capiamus

$$x = (v, a, b, b, a) \quad \text{et} \quad y = (a, b, b, a),$$

erit

$$xx = zyy - 1;$$

hinc pro problemate PELLIANO ut fiat $pp = zqq + 1$, statui oportet

$$p = 2xx + 1 \quad \text{et} \quad q = 2xy.$$

Quo autem numeri x et y facilius inveniri queant, sequentes transformationes instituantur[1])

$$x = (a, b)(v, a, b) + (a)(v, a) \quad \text{et} \quad y = (a, b)(a, b) + (a)(a),$$

qui ergo per solos indices v, a, b fractionibus inde formandis definientur:

$$\text{indices} \qquad v, \quad a, \quad b$$

$$\text{fractiones} \quad \frac{1}{0}, \quad \frac{\mathfrak{A}}{\mathfrak{a}}, \quad \frac{\mathfrak{B}}{\mathfrak{b}}, \quad \frac{\mathfrak{C}}{\mathfrak{c}},$$

ubi

$$\mathfrak{A} = v, \quad \mathfrak{B} = a\mathfrak{A} + 1, \quad \mathfrak{C} = b\mathfrak{B} + \mathfrak{A}$$

et

$$\mathfrak{a} = 1, \quad \mathfrak{b} = a\mathfrak{a} + 0, \quad \mathfrak{c} = b\mathfrak{b} + \mathfrak{a};$$

tum enim capi oportet

$$x = \mathfrak{c}\mathfrak{C} + \mathfrak{b}\mathfrak{B} \quad \text{et} \quad y = \mathfrak{c}\mathfrak{c} + \mathfrak{b}\mathfrak{b}.$$

Hic autem casus locum habet, quoties posito

$$z = vv + u$$

fuerit

$$2v = m(a, b, b, a) + (b, b)(a, b, b)$$

et

$$u = m(a, b, b) + (b, b)(b, b).$$

VI. CASUS QUO PRO NUMERO z INDICES SUNT v, a, b, c, b, a, $2v$ etc.

34. Quoniam hic numerus indicum in qualibet periodo est par, si sumamus

$$x = (v, a, b, c, b, a) \quad \text{et} \quad y = (a, b, c, b, a),$$

erit

$$xx = zyy + 1$$

---

1) Vide § 32 Commentationis 281 nota 3 p. 77 laudatae. F. R.

ideoque pro PELLIANO problemate statim habetur

$$p = x \quad \text{et} \quad q = y.$$

Facilius autem numeri x et y his transformationibus adhibitis invenientur

$$x = (a, b)(v, a, b, c) + (a)(v, a, b) \quad \text{et} \quad y = (a, b)(a, b, c) + (a)(a, b);$$

unde si ex indicibus v, a, b, c more exposito fractiones formentur

$$\text{indices} \quad v, \quad a, \quad b, \quad c$$

$$\text{fractiones} \quad \frac{1}{0}, \quad \frac{\mathfrak{A}}{\mathfrak{a}}, \quad \frac{\mathfrak{B}}{\mathfrak{b}}, \quad \frac{\mathfrak{C}}{\mathfrak{c}}, \quad \frac{\mathfrak{D}}{\mathfrak{d}},$$

sumi oportet

$$x = \mathfrak{c}\mathfrak{D} + \mathfrak{b}\mathfrak{C} \quad \text{et} \quad y = \mathfrak{c}\mathfrak{d} + \mathfrak{b}\mathfrak{c}.$$

At hic casus locum habet, quoties posito

$$z = vv + u$$

fuerit

$$2v = m(a, b, c, b, a) - (b, c, b)(a, b, c, b)$$

et

$$u = m(a, b, c, b) - (b, c, b)(b, c, b).$$

VII. CASUS QUO PRO NUMERO z INDICES SUNT $v, a, b, c, c, b, a, 2v$ etc.

35. Hic iterum indicum numerus in qualibet periodo est impar; ideoque si ponamus

$$x = (v, a, b, c, c, b, a) \quad \text{et} \quad y = (a, b, c, c, b, a),$$

erit

$$xx = zyy - 1;$$

ex quo ut fiat $pp = zqq + 1$, sumi oportet

$$p = 2xx + 1 \quad \text{et} \quad q = 2xy.$$

Pro faciliori autem numerorum x et y inventione ex indicibus v, a, b, c formentur fractiones

$$\text{indices} \quad v, \quad a, \quad b, \quad c$$

$$\text{fractiones} \quad \frac{1}{0}, \quad \frac{\mathfrak{A}}{\mathfrak{a}}, \quad \frac{\mathfrak{B}}{\mathfrak{b}}, \quad \frac{\mathfrak{C}}{\mathfrak{c}}, \quad \frac{\mathfrak{D}}{\mathfrak{d}}$$

hincque erit

$$x = \mathfrak{b}\mathfrak{D} + \mathfrak{c}\mathfrak{C} \quad \text{et} \quad y = \mathfrak{b}\mathfrak{d} + \mathfrak{c}\mathfrak{c}.$$

At hic casus locum habebit, quoties posito

$$z = vv + u$$

fuerit

$$2v = m(a, b, c, c, b, a) + (b, c, c, b)(a, b, c, c, b)$$

et

$$u = m(a, b, c, c, b) + (b, c, c, b)(b, c, c, b).$$

VIII. CASUS QUO PRO NUMERO z INDICES SUNT $v, a, b, c, d, c, b, a, 2v$ etc.

36. Hic quaelibet periodus octo continet indices; ideoque si ponamus

$$x = (v, a, b, c, d, c, b, a) \quad \text{et} \quad y = (a, b, c, d, c, b, a),$$

erit

$$xx = zyy + 1$$

et pro problemate Pelliano capi oportet

$$p = x \quad \text{et} \quad q = y,$$

ut fiat $pp = zqq + 1$. Transformationibus autem adhibitis numeros x et y per solos indices v, a, b, c, d definire licet. Formatis enim inde fractionibus

indices	$v,$	$a,$	$b,$	$c,$	d	
fractiones	$\frac{1}{0},$	$\frac{\mathfrak{A}}{\mathfrak{a}},$	$\frac{\mathfrak{B}}{\mathfrak{b}},$	$\frac{\mathfrak{C}}{\mathfrak{c}},$	$\frac{\mathfrak{D}}{\mathfrak{d}},$	$\frac{\mathfrak{E}}{\mathfrak{e}}$

fiet

$$x = \mathfrak{d}\mathfrak{E} + \mathfrak{c}\mathfrak{D} \quad \text{et} \quad y = \mathfrak{d}\mathfrak{e} + \mathfrak{c}\mathfrak{d}.$$

Hic vero casus locum habet, quoties posito

$$z = vv + u$$

fuerit

$$2v = m(a, b, c, d, c, b, a) - (b, c, d, c, b)(a, b, c, d, c, b)$$

et

$$u = m(a, b, c, d, c, b) - (b, c, d, c, b)(b, c, d, c, b).$$

EXPOSITIO CALCULI PRO QUOLIBET NUMERO z UT FIAT $pp = zqq + 1$

37. Primum igitur methodo supra exposita pro numero z ex eius radice quadrata indices investigari oportet; quam operationem autem ulterius continuari non est opus, quam donec indices ordine retrogrado prodire incipiant, quo pacto semissi laboris supra explicati supersedere poterimus. Cum autem in prima periodo vel unus index medius occurrat vel bini, hi casus probe sunt distinguendi, cum, si unicus medius affuerit, inventio numerorum p et q modo in casibus II, IV, VI et VIII tradito institui debeat, sin autem bini fuerint medii, eo modo, qui in casibus I, III, V et VII est descriptus. Scilicet si prius eveniat, numeri p et q numeris x et y aequales sumuntur, sin autem posterius, uti vidimus, statui oportet $p = 2xx + 1$ et $q = 2xy$, ita ut his casibus numeri p et q caeteris paribus multo grandiores reperiantur.

38. En igitur exempla prioris generis, quo in qualibet periodo unus datur index medius.

I. Si $z = 6$, sunt indices 2, 2, 4; hinc operatio:

$$2,\ 2$$

$$\frac{1}{0},\ \frac{2}{1},\ \frac{5}{2};$$

$$\begin{aligned} x &= 1\cdot 5 + 0\cdot 2, \\ y &= 1\cdot 2 + 0\cdot 1, \end{aligned} \quad \text{ergo} \quad \begin{aligned} p &= 5, \\ q &= 2. \end{aligned}$$

II. Si $z = 14$, sunt indices 3, 1, 2, 1, 6:

$$3,\ 1,\ 2$$

$$\frac{1}{0},\ \frac{3}{1},\ \frac{4}{1},\ \frac{11}{3};$$

$$\begin{aligned} x &= 1\cdot 11 + 1\cdot 4, \\ y &= 1\cdot\ 3 + 1\cdot 1, \end{aligned} \quad \text{ergo} \quad \begin{aligned} p &= 15, \\ q &=\ 4. \end{aligned}$$

III. Si $z = 19$, sunt indices 4, 2, 1, 3, 1, 2, 8:

$$4,\ 2,\ 1,\ 3$$
$$\frac{1}{0},\ \frac{4}{1},\ \frac{9}{2},\ \frac{13}{3},\ \frac{48}{11};$$

$$\begin{aligned} x &= 3\cdot 48 + 2\cdot 13, \\ y &= 3\cdot 11 + 2\cdot\ 3, \end{aligned} \quad \text{ergo} \quad \begin{aligned} p &= 170, \\ q &= \ 39. \end{aligned}$$

IV. Si $z = 31$, sunt indices 5, 1, 1, 3, 5, 3, 1, 1, 10:

$$5,\ 1,\ 1,\ 3,\ 5$$
$$\frac{1}{0},\ \frac{5}{1},\ \frac{6}{1},\ \frac{11}{2},\ \frac{39}{7},\ \frac{206}{37};$$

hinc

$$\begin{aligned} x &= 7\cdot 206 + 2\cdot 39, \\ y &= 7\cdot\ 37 + 2\cdot\ 7, \end{aligned} \quad \text{ergo} \quad \begin{aligned} p &= 1520, \\ q &= \ 273. \end{aligned}$$

V. Si $z = 44$, sunt indices 6, 1, 1, 1, 2, 1, 1, 1, 12:

$$6,\ 1,\ 1,\ 1,\ 2$$
$$\frac{1}{0},\ \frac{6}{1},\ \frac{7}{1},\ \frac{13}{2},\ \frac{20}{3},\ \frac{53}{8};$$

hinc

$$\begin{aligned} x &= 3\cdot 53 + 2\cdot 20, \\ y &= 3\cdot\ 8 + 2\cdot\ 3, \end{aligned} \quad \text{ergo} \quad \begin{aligned} p &= 199, \\ q &= \ 30. \end{aligned}$$

VI. Si $z = 55$, sunt indices 7, 2, 2, 2, 14:

$$7,\ 2,\ 2$$
$$\frac{1}{0},\ \frac{7}{1},\ \frac{15}{2},\ \frac{37}{5};$$

hinc

$$\begin{aligned} x &= 2\cdot 37 + 1\cdot 15, \\ y &= 2\cdot\ 5 + 1\cdot\ 2, \end{aligned} \quad \text{ergo} \quad \begin{aligned} p &= 89, \\ q &= 12. \end{aligned}$$

39. Alterius vero generis, quo bini dantur indices medii in qualibet periodo, haec adiungo exempla.

I. Si $z = 13$, sunt indices 3, 1, 1, 1, 1, 6:

$$3,\ 1,\ 1$$
$$\frac{1}{0},\ \frac{3}{1},\ \frac{4}{1},\ \frac{7}{2};$$

hinc

$$x = 2 \cdot 7 + 1 \cdot 4 = 18,$$
$$y = 2 \cdot 2 + 1 \cdot 1 = 5.$$

Ergo

$$p = 2xx + 1 = 649,$$
$$q = 2xy \quad = 180.$$

II. Si $z = 29$, sunt indices 5, 2, 1, 1, 2, 10:

$$5,\ 2,\ 1$$
$$\frac{1}{0},\ \frac{5}{1},\ \frac{11}{2},\ \frac{16}{3};$$

hinc

$$x = 3 \cdot 16 + 2 \cdot 11 = 70,$$
$$y = 3 \cdot\ 3 + 2 \cdot\ 2 = 13.$$

Ergo

$$p = 2xx + 1 = 9801,$$
$$q = 2xy \quad = 1820.$$

III. Si $z = 58$, sunt indices 7, 1, 1, 1, 1, 1, 1, 14:

$$7,\ 1,\ 1,\ 1$$
$$\frac{1}{0},\ \frac{7}{1},\ \frac{8}{1},\ \frac{15}{2},\ \frac{23}{3};$$

hinc

$$x = 3 \cdot 23 + 2 \cdot 15 = 99,$$
$$y = 3 \cdot\ 3 + 2 \cdot\ 2 = 13.$$

Ergo

$$p = 2xx + 1 = 19603,$$
$$q = 2xy \quad = 2574.$$

IV. Si $z = 61$, indices sunt 7, 1, 4, 3, 1, 2, 2, 1, 3, 4, 1, 14:

$$7,\ 1,\ 4,\ 3,\ 1,\ 2$$
$$\frac{1}{0},\ \frac{7}{1},\ \frac{8}{1},\ \frac{39}{5},\ \frac{125}{16},\ \frac{164}{21},\ \frac{453}{58};$$

hinc fit

$$x = 58 \cdot 453 + 21 \cdot 164 = 29718,$$
$$y = 58 \cdot 58 + 21 \cdot 21 = 3805.$$

Ergo

$$p = 2xx + 1 = 1766319049,$$
$$q = 2xy = 226153980.$$

40. Quodsi pro maioribus numeris z, quam ante sunt evoluti, quaeri debeant numeri p et q, ut sit $pp = zqq + 1$, primum methodo supra exposita (§ 12) indices v, a, b, c, d etc. quaeri oportet, quos autem ulterius continuari non est opus, quam donec ad indicem medium vel binos medios primae periodi perveniatur; tum vero ex iis per operationes hic descriptas primo numeri x et y, tum vero ipsi quaesiti p et q determinabuntur. Id quod aliquibus exemplis illustrari conveniet.

I. Quaerantur numeri p et q, ut sit $pp = 157qq + 1$

41. Cum hic sit $z = 157$, erit $v = 12$ et $\alpha = 13$, unde indicum inventio ita se habebit:

$$\begin{array}{lll} A = 12, & \alpha = 13, & a = 1, \\ B = 1, & \beta = 12, & b = 1, \\ C = 11, & \gamma = 3, & c = 7, \\ D = 10, & \delta = 19, & d = 1, \\ E = 9, & \varepsilon = 4, & e = 5, \\ F = 11, & \zeta = 9, & f = 2, \\ G = 7, & \eta = 12, & g = 1, \\ H = 5, & \theta = 11, & h = 1 \\ I = 6, & \iota = 11, & i = 1 \end{array} \Big\} \text{ medii.}$$

Hinc ob binos medios exemplum ad genus secundum pertinet et operationes ita sunt instituendae:

$$12,\ 1,\ 1,\ 7,\ 1,\ 5,\ 2,\ 1,\ 1$$
$$\frac{1}{0},\ \frac{12}{1},\ \frac{13}{1},\ \frac{25}{2},\ \frac{188}{15},\ \frac{213}{17},\ \frac{1253}{100},\ \frac{2719}{217},\ \frac{3972}{317},\ \frac{6691}{534}$$

Hinc erit

$$x = 534 \cdot 6691 + 317 \cdot 3972 = 4832118$$

et

$$y = 534 \cdot\ 534 + 317 \cdot\ 317 = \ 385645.$$

Quocirca

$$p = 2xx + 1 = 46698728731849$$

et

$$q = 2xy \quad = \ 3726964292220$$

atque hi adeo sunt minimi numeri integri formulae $p = \sqrt{(157qq + 1)}$ satisfacientes.

II. Quaerantur numeri p et q, ut sit $pp = 367qq + 1$

42. Hic ergo est $z = 367$, $v = 19$ hincque

$A = 19,$	$\alpha = \ 6,$	$a = \ 6,$
$B = 17,$	$\beta = 13,$	$b = \ 2,$
$C = \ 9,$	$\gamma = 22,$	$c = \ 1,$
$D = 13,$	$\delta = \ 9,$	$d = \ 3$[1]),
$E = 14,$	$\varepsilon = 19,$	$e = \ 1,$
$F = \ 5,$	$\zeta = 18,$	$f = \ 1,$
$G = 13,$	$\eta = 11,$	$g = \ 2,$
$H = \ 9,$	$\theta = 26,$	$h = \ 1,$
$I = 17,$	$\iota = \ 3,$	$i = 12,$
$K = 19,$	$\varkappa = \ 2,$	$k = 19$ medius,
$L = 19,$	$\lambda = \ 3,$	$l = 12.$

Hoc ergo exemplum ad genus primum pertinet.

19, 6, 2, 1, 3[2]), 1, 1, 2, 1, 12, 19

$\frac{1}{0}$, $\frac{19}{1}$, $\frac{115}{6}$, $\frac{249}{13}$, $\frac{364}{19}$, $\frac{1341}{70}$, $\frac{1705}{89}$, $\frac{3046}{159}$, $\frac{7797}{407}$, $\frac{10843}{566}$, $\frac{137913}{7199}$, $\frac{2631190}{137347}$,

1) Editio princeps (atque etiam *Comment. arithm.*): $d = 9$. Sequentes autem numeros E et ε EULERUS ope valoris $d = 3$ recte computavit. F. R.

2) Ob falsum indicem $d = 9$ (vide notam praecedentem) fractiones sequentes ideoque etiam solutiones, quae in editione principe (atque in *Comment. arithm.*) continentur, corrigendae erant.

Hinc erit

$$x = 7199 \cdot 2631190 + 566 \cdot 137913$$

et

$$y = 7199 \cdot 137347 + 566 \cdot 7199,$$

ex quo minimi numeri satisfacientes sunt

$$p = 19019995568,$$
$$q = 992835687.$$

Tabula numerorum p et q,
quibus fit $pp = lqq + 1$ pro omnibus valoribus numeri l usque ad 100

l	q	p	l	q	p
2	2	3	26	10	51
3	1	2	27	5	26
			28	24	127
5	4	9	29	1820	9801
6	2	5	30	2	11
7	3	8	31	273	1520
8	1	3	32	3	17
			33	4	23
10	6	19	34	6	35
11	3	10	35	1	6
12	2	7			
13	180	649	37	12	73
14	4	15	38	6	37
15	1	4	39	4	25
			40	3	19
17	8	33	41	320	2049
18	4	17	42	2	13
19	39	170	43	531	3482
20	2	9	44	30	199
21	12	55	45	24	161
22	42	197	46	3588	24335
23	5	24	47	7	48
24	1	5	48	1	7

Ceterum manifestum est numeros $p = 110413985786$ et $q = 5763448635$ ab EULERO computatos non posse satisfacere aequationi $pp = 367qq + 1$. Substitutis enim his numeris et computatis ultimis tantum figuris statim invenitur esse $p^2 = \cdots 96$, at $367q^2 + 1 = \cdots 76$. Rectae solutiones $v = 19019995568$ et $q = 992835687$ inveniuntur iam in prima editione libri, qui inscribitur *Essai sur la théorie des nombres par A. M. LEGENDRE*, Paris 1798, table XII. F. R.

l	q	p	l	q	p
50	14	99	75	3	26
51	7	50	76	6630	57799
52	90	649	77	40	351
53	9100	66249[1])	78	6	53
54	66	485	79	9	80
55	12	89	80	1	9
56	2	15	82	18	163
57	20	151	83	9	82[2])
58	2574	19603	84	6	55
59	69	530	85	30996[3])	285769
60	4	31	86	1122	10405
61	226153980	1766319049	87	3	28
62	8	63	88	21	197
63	1	8	89	53000	500001[4])
65	16	129	90	2	19
66	8	65	91	165	1574
67	5967	48842	92	120	1151
68	4	33	93	1260	12151
69	936	7775	94	221064	2143295
70	30	251	95	4	39
71	413	3480	96	5	49
72	2	17	97	6377352	62809633
73	267000	2281249	98	10	99
74	430	3699	99	1	10

Exempla denique quaedam numerorum maiorum pro l assumtorum adiungam:

$$\text{Si} \quad l = 103, \quad \text{erit} \quad \begin{cases} p = 227528, \\ q = \ 22419; \end{cases}$$

$$\text{si} \quad l = 109, \quad \text{erit} \quad \begin{cases} p = 158070671986249, \\ q = \ 15140424455100; \end{cases}$$

1) Editio princeps (atque etiam *Comment. arithm.*): $p = 33125$, qui falsus numerus ex formula manca $p = x^2 + 1 = 182^2 + 1$ loco $p = 2x^2 + 1 = 2 \cdot 182^2 + 1$ ortus est. Rectus valor $p = 66249$ iam invenitur in tabula Commentationis 29 nota p. 75 laudatae. F. R.

2) Editio princeps (atque etiam *Comment. arithm.*): $p = 32$. F. R.

3) Editio princeps (atque etiam *Comment. arithm.*): $q = 30906$. F. R.

4) Editio princeps (atque etiam *Comment. arithm.*): $p = 500901$.

Recti valores $p = 82$ ($l = 83$), $p = 500001$ ($l = 89$), $q = 30996$ ($l = 85$) inveniuntur etiam in tabula, quae continetur in L. Euleri *Vollständige Anleitung zur Algebra.* Vide notam p. 73. F. R.

$$\text{si } l = 113, \text{ erit } \begin{cases} p = 1204353, \\ q = 113296; \end{cases}$$

$$\text{si } l = 157, \text{ erit } \begin{cases} p = 46698728731849, \\ q = 3726964292220; \end{cases}$$

$$\text{si } l = 367, \text{ erit } \begin{cases} p = 19019995568, \\ q = 992835687.^{1}) \end{cases}$$

1) Vide notam 2 p. 108. F. R.

QUOMODO NUMERI PRAEMAGNI SINT EXPLORANDI UTRUM SINT PRIMI NECNE[1])

Commentatio 369 indicis ENESTROEMIANI
Novi commentarii academiae scientiarum Petropolitanae 13 (1768), 1769, p. 67—88
Summarium ibidem p. 8—11

SUMMARIUM

Inter maximi momenti quaestiones arithmeticas praecipuum omnino locum tenet illa, qua quaeritur de methodo explorandi naturam numerorum, utrum primi sint necne. Quamvis autem hoc ipsum vix alia ratione generaliter perfici posse videatur quam operatione vulgari, qua divisio per omnes numeros primos radice quadrata numeri propositi minores est tentanda, quum tamen haec operatio pro numeris mediocriter magnis iam operosior sit, quam ut suscipi queat, hinc operae omnino pretium erat eiusmodi methodum tradere, quae, etiamsi pro certo tantum numerorum genere valeat, ad numeros tamen quantumvis magnos sub eo comprehensos explorandos applicari possit. Quum itaque Illustr. Auctor post FERMATIUM observaverit[2]) omnes numeros primos in hac forma $4n+1$ contentos nonnisi unico modo in duos numeros quadratos resolvi posse, exinde vicissim colligit numeros huius formae $4n+1$, qui unico modo in duo quadrata resolvuntur, fore numeros primos, illis tamen numeris exceptis, qui ipsi sunt quadrati. Examen igitur hoc ita instituendum est, ut a numero proposito omnes numeri quadrati ipso minores subtrahantur eaque residua notentur, quae etiam numeri sunt quadrati; ubi si fiat, ut vel nullum vel plura talia dentur residua, tum tuto colligere licet numerum esse compositum; sin autem unicum detur, erit numerus propositus vel primus vel ipse quadratus, qui duo casus facile ab invicem digno-

1) Vide etiam Commentationes 283, 461, 467, 498, 708a huius voluminis. F. R.

2) Vide notam 1 p. 114. F. R.

scuntur. Liquet autem pro hoc fine obtinendo sufficere, si a numero proposito tantum quadrata semissi maiora subtrahantur, quo ipso numerus subtractionum ad trientem fere redigitur.

Quum vero etiam haec operandi ratio pro numeris praemagnis nimis sit molesta, eae subtractiones heic excludendae sunt, quae ad talia residua perducant, quae cum quadratorum natura consistere nequeunt, qualia sunt, quae his formis continentur $3m+2$, $5m+2$, $5m+3$ etc. Si igitur numerus propositus $N=4n+1$ simul contineatur in his formis $3m+2$ et $5m+2$ vel $3m+2$ et $5m+3$, inde perspicitur, quales esse debeant numeri, quorum quadrata subtrahenda sunt. Scilicet pro prima specie, qua $N=4n+1$ per has formas $3m+2$, $5m+2$ exprimitur, continebitur N in hac formula $60n+17$; unde si $N=xx+yy$, erit x vel y huius formae $15p\pm(1, 4)$, nempe vel $15p\pm1$ vel $15p\pm4$. Pro altera deinceps specie, qua $N=4n+1$ duplici forma $3m+2$ et $5m+3$ exprimi potest, erit quoque idem N huius formae $60n+53$, unde ab eo ista solum quadrata subtrahenda sunt, quorum radices in forma $15p\pm(2, 7)$ continentur.

Omnes vero numeri formae $4n+1$ quum sub his quatuor speciebus comprehendantur $16n+1$, $16n+5$, $16n+9$, $16n+13$, si hae quatuor species cum binis praecedentibus combinentur, orientur inde octo novae species, pro quibus formae radicum numerorum subtrahendorum facile exhibentur, atque tum demum totidem novae species orientur, si formae $32n+5$, $32n+13$, $32n+21$, $32n+29$ cum binis principalibus combinentur. Quae autem et quales sint pro quovis casu formae radicum numerorum subtrahendorum, ex ipsa Dissertatione addiscendum est, ad quam studiose evolvendam Lectores ablegamus id tantum observantes, quod numeri primi hac ratione explorati 3861317 atque 10091401 tam magni sint, ut non sine labore taediosissimo methodo vulgari eorum indoles investigari possit; quamobrem liquet examen heic allatum eo maioris esse habendum, quod ad numeros maximos sine ulla calculi prolixitate applicari possit.

1. Ante omnia monendum est me hic non eiusmodi methodum polliceri, cuius ope omnes omnino numeri, cuiuscunque sint generis, examinari queant, utrum sint primi necne. Huiusmodi enim methodum vix aliam dari posse existimo, nisi quae ad regulam redeat vulgarem, qua divisio per omnes numeros primos radice quadrata numeri propositi minores est tentanda, quae operatio sane, si numeri saltem mediocriter magni proponantur, nimis est molesta, quam ut suscipi queat. Quae igitur hic in medium afferre constitui, ad certum tantum numerorum genus sunt restringenda, pro quo scilicet hoc

examen, utrum sint primi necne, citra laborem tam operosum institui queat. Cum enim numerorum primorum natura adhuc maxime sit abscondita, quicquid in hoc negotio praestare licuerit, etiamsi alias arctissimis limitibus sit circumscriptum, usu neutiquam destitui est censendum.

2. Numeros ergo tantum in hac forma $4n+1$ contentos sum contemplaturus, de quibus equidem post FERMATIUM demonstravi, si huiusmodi numerus fuerit primus, tum eum semper esse summam duorum quadratorum idque unico modo.[1]) Unde proposito numero quocunque huius formae $4n+1$ examen, utrum sit primus necne, hoc modo instituetur. Ab eo successive omnes numeri quadrati ipso minores auferantur eaque notentur residua, quae pariter sint numeri quadrati; atque si unico modo numerus propositus $4n+1$ in forma $aa+bb$ contineri deprehendatur, id certum erit criterium numerum propositum esse primum. Sin autem vel prorsus non in ea forma contineatur vel plus uno modo, tum certe non erit primus; priori quidem casu, quo numerus $4n+1$ non est summa duorum quadratorum, plus concludere non licet quam eum non esse primum neque inde eius divisores innotescunt; sin autem plus uno modo fuerit duorum quadratorum summa, veluti

$$4n+1 = aa+bb = cc+dd,$$

tum hinc quaerantur eiusmodi bini numeri p et q, ut sit $\frac{p}{q} = \frac{a \pm c}{b \pm d}$ vel $\frac{p}{q} = \frac{a \pm d}{b \pm c}$, ac numeri $4n+1$ et $pp+qq$ certo habebunt divisorem communem, qui ergo facile assignatur.[2])

3. Proposito itaque huiusmodi numero $4n+1$ operationem ita institui convenit, ut ab eo continuo numeri quadrati subtrahantur eaque residua tantum notentur, quae etiam sint numeri quadrati; ubi quidem statim apparet

---

1) Vide EULERI Commentationes 228 et 241 (indicis ENESTROEMIANI): *De numeris, qui sunt aggregata duorum quadratorum*, Novi comment. acad. sc. Petrop. 4 (1752/3), 1758, p. 3, et *Demonstratio theorematis FERMATIANI omnem numerum primum formae* $4n+1$ *esse summam duorum quadratorum*, Novi comment. acad. sc. Petrop. 5 (1754/5), 1760, p. 3; *LEONHARDI EULERI Opera omnia*, series I, vol. 2, p. 295 et 328. F. R.

2) Vide § 42 et 43 Commentationis 228 nota praecedente laudatae. F. R.

hanc subtractionem non ultra quadrata semissi minora continuari opus esse.[1]) Si enim fuerit $4n+1 = aa+bb$, horum quadratorum alterum certe erit minus semissi $\frac{4n+1}{2}$. Vel cum horum binorum quadratorum alterum necessario sit par, alterum impar, sufficiet vel paria tantum vel imparia quadrata ipso numero proposito minora subtrahi, quo pacto multitudo quadratorum subtrahendorum haud mediocriter imminuitur. Cum autem numerus omnium quadratorum ipso numero proposito minorum sit $= \sqrt{(4n+1)}$, eorum autem, quae eius semissi sunt minora, $= \sqrt{\frac{4n+1}{2}}$, erit quadratorum semissi maiorum numerus

$$= \left(1 - \frac{1}{\sqrt{2}}\right)\sqrt{(4n+1)} = \frac{5}{17}\sqrt{(4n+1)}$$

proxime; quae quoniam etiam subtrahi sufficit, hoc modo numerus subtractionum ad trientem fere redigitur.

4. Maxime ergo expedire videtur hanc operationem ita institui, ut a quadrato maximo infra numerum propositum $4n+1$ initium capiatur indeque quadrata continuo minora subtrahantur, donec ad quadrata semissi minora perveniatur. Veluti si numerus propositus sit 101, sufficiet inde haec tria quadrata 100, 81, 64 subtraxisse, quia sequens 49 iam foret semissi $50\frac{1}{2}$ minus; hoc modo cum inter tria residua 1, 20, 37 unicum occurrat quadratum 1, hoc certum est signum numerum 101 esse primum. Verumtamen si numerus propositus $4n+1$ fuerit praemagnus, etiam hae operationes nimis multiplicantur; ex quo in id potissimum erit incumbendum, ut harum subtractionum numerus imminuatur, quod fiet, si eae excludantur, quae ad talia residua perducunt, quae a quadratorum natura abhorreant, cuiusmodi sunt residua in his formis contenta $3m+2$, $5m+2$, $5m+3$, $8m+5$ etc.; formae enim $8m+3$ et $8m+7$ ob indolem numeri propositi $4n+1$ nunquam occurrunt.

5. Dantur autem certae numerorum formae $4n+1$ species, unde plurima quadrata inde subtrahenda excluduntur. Veluti si sit $4n+1 = 3m+2$ ac ponatur hic numerus $= xx+yy$, uterque numerus x et y in forma $3p \pm 1$

1) Vide § 44—52 Commentationis 228 supra laudatae. Confer etiam § 57—63 Commentationis 256 (indicis Enestroemiani): *Specimen de usu observationum in mathesi pura*, Novi Comment. acad. sc. Petrop. 6 (1756/7), 1761, p. 185; *Leonhardi Euleri Opera omnia*, series I, vol. 2, p. 459. F. R.

contineatur necesse est, ita ut numeri formae $3p$ excludantur; simili modo si sit $4n+1=5m+2$, utrumque numerum x et y in forma $5p \pm 1$ contineri oportet, et si $4n+1=5m+3$, in forma $5p \pm 2$. Denique si $8m+5=xx+yy$, numerorum quidem x et y alter est impar, alter par, hic vero adeo impariter par seu formae $4p+2$. Quodsi ergo simul fuerit

$$xx+yy=3m+2, \quad =5m+2,$$

numeros x et y simul in his duabus formis $3p \pm 1$ et $5p \pm 1$ contineri oportet, unde eorum forma concluditur

$$x \text{ vel } y = 15p \pm (1, 4).$$

At si fuerit

$$xx+yy=3m+2, \quad =5m+3,$$

forma numerorum x et y est et $3p \pm 1$ et $5p \pm 2$, quae duplex forma in hanc unam contrahitur

$$x \text{ vel } y = 15p \pm (2, 7).$$

6. Quoniam hoc modo duae tertiae partes omnium numerorum, quos tentari oporteret, excluduntur, hi casus imprimis sunt apti, quibus examen satis expedite instituere licebit. Quare numerorum $N=4n+1$ eas species potissimum contemplemur, quae vel in his duabus formis $3m+2$ et $5m+2$ vel in his $3m+2$ et $5m+3$ contineantur. Numeri autem prioris speciei ad hanc formam $15m+2$ reducuntur; qui cum insuper in forma $4n+1$ contineri debeant, haec species sequenti formula exprimetur:

$$\text{Species prima} \quad N=60n+17,$$

qui numerus alio modo summa duorum quadratorum esse nequit, nisi utriusque quadrati radix sit numerus formae $15p \pm (1, 4)$, scilicet vel $15p \pm 1$ vel $15p \pm 4$, unde numeri tentandi ex his quatuor progressionibus sunt capiendi

1, 16, 31, 46, 61, 76, 91, 106, 121, 136 etc.,
4, 19, 34, 49, 64, 79, 94, 109, 124, 139 etc.,
11, 26, 41, 56, 71, 86, 101, 116, 131, 146 etc.,
14, 29, 44, 59, 74, 89, 104, 119, 134, 149 etc.

et reliquos omnes in hoc negotio praetermittere licet.

7. Simili modo alteram speciem evolvamus, quae duplici forma $3m + 2$ et $5m + 3$ continetur et propterea ad hanc unam $15m + 8$ revocatur. Hinc autem tantum illi numeri sunt usui, qui simul sunt formae $4n + 1$, ex quo haec species sequenti formula exprimetur:

$$\text{Species secunda} \quad N = 60n + 53.$$

Huius ergo formae si fuerit numerus explorandus, utrum sit primus necne, ab eo alia quadrata subtrahi non est opus, nisi quorum radices in hac forma $15p \pm (2, 7)$ contineantur, quas ergo ex sequentibus quaternis progressionibus arithmeticis sumi oportet

2, 17, 32, 47, 62, 77, 92, 107, 122, 137, 152 etc.,
7, 22, 37, 52, 67, 82, 97, 112, 127, 142, 157 etc.,
8, 23, 38, 53, 68, 83, 98, 113, 128, 143, 158 etc.,
13, 28, 43, 58, 73, 88, 103, 118, 133, 148, 163 etc.;

hoc ergo modo multitudo quadratorum subtrahendorum fere ad trientem reducitur.

8. Neque vero his omnibus quadratis tentamen institui opus est; prout enim numerus propositus N insuper fuerit comparatus, inde praeterea multa excluduntur. Cum enim omnes numeri formae $N = 4n + 1$ in has quatuor resolvantur

$$16n + 1, \quad 16n + 5, \quad 16n + 9, \quad 16n + 13,$$

si statuatur $N = xx + yy$ et x denotet numerum parem, y vero imparem, pro his speciebus numeri x et y sequenti modo comparati reperiuntur:

Si sit	erit	et
$N = 16n + 1$	$x = 4m$	$y = 8p \pm 1$
$N = 16n + 5$	$x = 4m \pm 2$	$y = 8p \pm 1$
$N = 16n + 9$	$x = 4m$	$y = 8p \pm 3$
$N = 16n + 13$	$x = 4m \pm 2$	$y = 8p \pm 3.$

9. Combinemus has quaternas species cum binis praecedentibus et obtinebimus sequentes octo species, pro quibus formas tam radicis paris x quam imparis y exhibeamus:

Si fuerit N	erit x	et y
$240n + 17$	$60m \pm (4, 16)$	$120p \pm (1, 31, 41, 49)$
$240n + 77$	$60m \pm (14, 26)$	$120p \pm (11, 19, 29, 59)$
$240n + 137$	$60m \pm (4, 16)$	$120p \pm (11, 19, 29, 59)$
$240n + 197$	$60m \pm (14, 26)$	$120p \pm (1, 31, 41, 49)$
$240n + 53$	$60m \pm (2, 22)$	$120p \pm (7, 17, 23, 47)$
$240n + 113$	$60m \pm (8, 28)$	$120p \pm (7, 17, 23, 47)$
$240n + 173$	$60m \pm (2, 22)$	$120p \pm (13, 37, 43, 53)$
$240n + 233$	$60m \pm (8, 28)$	$120p \pm (13, 37, 43, 53)$.

10. Dantur autem in his numeris species, quibus adhuc plures numeri tentandi excluduntur, quae ita se habent:

Si sit	erit	et
$N = 32n + 5$	$x = 4m \pm 2$	$y = 16p \pm 1$
$N = 32n + 13$	$x = 4m \pm 2$	$y = 16p \pm 3$
$N = 32n + 21$	$x = 4m \pm 2$	$y = 16p \pm 7$
$N = 32n + 29$	$x = 4m \pm 2$	$y = 16p \pm 5$;

quae cum binis principalibus combinatae praebent:

Si sit N	erit x	et y
$480n + 77$	$60m \pm (14, 26)$	$240p \pm (19, 29, 61, 109)$
$480n + 197$	$60m \pm (14, 26)$	$240p \pm (1, 31, 49, 79)$
$480n + 317$	$60m \pm (14, 26)$	$240p \pm (11, 59, 91, 101)$
$480n + 437$	$60m \pm (14, 26)$	$240p \pm (41, 71, 89, 119)$
$480n + 53$	$60m \pm (2, 22)$	$240p \pm (7, 23, 73, 103)$
$480n + 173$	$60m \pm (2, 22)$	$240p \pm (13, 67, 77, 83)$
$480n + 293$	$60m \pm (2, 22)$	$240p \pm (17, 47, 97, 113)$
$480n + 413$	$60m \pm (2, 22)$	$240p \pm (37, 43, 53, 107)$.

Hic ergo ex valoribus ipsius y, quos praecedentes species admittunt, denuo semissis excluditur.

11. Quoniam hic valores radicis imparis y multo magis imminuuntur quam radicis paris x, calculus multo evadet facilior et brevior, si a numero proposito N, siquidem in una postremarum specierum contineatur, successive omnia quadrata imparia ipso minora subtrahantur residuaque examinentur, an sint quadrata necne; harum operationum numerus satis erit modicus, etiamsi numerus propositus fuerit praemagnus, et quoniam radices per differentiam 240 increscunt, insignia compendia in calculo usurpari poterunt. Scilicet si quaecunque quatuor minimarum radicum dicatur $= a$, quia a numero proposito N, si modo in aliqua octo postremarum specierum contineatur vel, quod eodem redit, si fuerit vel huius formae $120n + 77$ vel huius $120n + 53$, successive subtrahi debent quadrata aa, $(240 \pm a)^2$, $(480 \pm a)^2$ etc., notetur differentias esse primas $57600 \pm 480a$, $3 \cdot 57600 \pm 480a$ etc., secundas vero esse constantes $= 115200$, quo pacto totum negotium ad meras additiones et subtractiones reducitur; et quia quaelibet radix simplex a tam positive quam negative accipi potest, utraque pari calculo expedietur.

PROBLEMA

12. *Proposito numero quantumvis magno N, qui vel in hac forma $120n + 77$ vel in hac $120n + 53$ contineatur, explorare, utrum is sit primus necne.*

SOLUTIO

Statuatur $N = aa + zz$ et pro octonis formis ipsius N littera a quatuor habebit valores sequentes:

Si sit	erunt quaterni valores ipsius a
$N = 480n + 77$	19, 29, 61, 109
$N = 480n + 197$	1, 31, 49, 79
$N = 480n + 317$	11, 59, 91, 101
$N = 480n + 437$	41, 71, 89, 119
$N = 480n + 53$	7, 23, 73, 103
$N = 480n + 173$	13, 67, 77, 83
$N = 480n + 293$	17, 47, 97, 113
$N = 480n + 413$	37, 43, 53, 107.

Pro quolibet ergo numero N habebimus quatuor valores ipsius a, quorum singuli dabunt binas numerorum series descendentes

$$N - aa, \quad N - (240 + a)^2, \quad N - (480 + a)^2, \quad N - (720 + a)^2 \quad \text{etc.},$$

$$N - aa, \quad N - (240 - a)^2, \quad N - (480 - a)^2, \quad N - (720 - a)^2 \quad \text{etc.},$$

quarum illius differentia prima est $57600 + 480a$, huius vero $57600 - 480a$, utriusque vero differentia secunda constans $= 115200$. Ambae hae progressiones continuentur, donec ad terminos negativos perveniatur, ex iisque ii notentur, qui sunt numeri quadrati. Quodsi tum eveniat, ut unicus occurrat numerus quadratus, hoc erit signum indubium propositum numerum N esse primum; sin autem vel nullus numerus quadratus occurrat vel plures uno, certo hinc erit concludendum numerum propositum N non esse primum, sed ex factoribus componi.

COROLLARIUM 1

13. Quodsi ergo numerus propositus N in altera harum formarum $120n + 77$ et $120n + 53$ contineatur, tum satis expedite examen institui poterit, utrum is numerus sit primus necne, cum quadrata, quae successive subtrahi oportet, scilicet $(240\lambda \pm a)^2$, mox ipsum numerum N sint superatura.

COROLLARIUM 2

14. Si enim numerus propositus N unum millionem non superet, quadrata subtrahenda infra $(1200 \pm a)^2$ subsistent eorumque ergo numerus pro quolibet numero a non ad 9 usque ascendet; et quoniam quaterni huiusmodi numeri a habentur, paucioribus quam 36 operationibus totum negotium conficietur.

COROLLARIUM 3

15. Si numerus N adeo decuplo fuerit maior, operationum numerus ad triplum tantum increscet, et quoniam pro quovis numero a quadrata subtrahenda eiusmodi progressionem constituunt, quarum differentiae secundae sunt constantes, hinc ingentia calculi compendia nascuntur.

SCHOLION

16. Etsi haec methodus ad nonnullas tantum numerorum species patet, quippe quae in altera harum formarum $120n + 77$ et $120n + 53$ sint contentae, ea tamen neutiquam attentione indigna videtur. Cum enim eiusmodi methodum, quae se prorsus ad omnes numeros extendat, ne sperare quidem liceat, quae scilicet a vulgari regula, qua divisionem per omnes numeros primos radice quadrata numeri propositi minores tentari oportet, discrepet eaque sit multo expeditior, omnia compendia, quae quidem in hoc negotio invenire licet, neutiquam sunt contemnenda, etiamsi ea ad paucissimas numerorum species extendantur, dummodo numeros quantumvis magnos in se complectantur. Cum enim problema iam olim propositum, quo numerus primus dato numero maior desideratur, adhuc vires ingenii humani superare videatur, non parum praestitisse censendus est, qui numeros valde magnos, qui certo sint primi, in medium afferre valuerit. Usum igitur methodi hic expositae aliquot exemplis declarabo.

EXEMPLUM 1

17. *Explorare, utrum hic numerus* 481037 *sit primus necne.*

Cum hic numerus sit $= 1002 \cdot 480 + 77$, in prima forma continetur, ubi quatuor valores ipsius a sunt 19, 29, 61, 109; calculus ergo sequenti modo instituatur:

$a = \pm 19$		$a = \pm 29$	
481037	57600	481037	57600
361	9120	841	13920
−480676	480676−	−480196	480196−
66720	48480	71520	43680
1152	1152	1152	1152
−413956	432196−	−408676	436516−
181920	163680	186720	158880
1152	1152	1152	1152
−232036	268516−	−221956	277636−
			274080
			3556−

$a = \pm 61$		$a = \pm 109$	
481037	57600	481038	57600
3721	29280	11881	52320
−477316	477316−	−469156	469156−
86880	28320	109920	5280
1152	1152	1152	1152
−390436	448996−	−359236	463876−
202080	143520	225120	120480
1152	1152	1152	1152
□ 188356	305476−	−134116	343396 □
	258720		235680
	46756−		107716−

In his residuis duo occurrunt quadrata signo □ notata, dum reliqua non quadrata lineola — notavi; ex quo concludo numerum propositum non esse primum. Cum autem sit duplici modo duorum quadratorum summa, scilicet

$$481037 = 434^2 + 541^2 = 586^2 + 371^2,$$

eius divisores, quos quoque summas esse duorum quadratorum necesse est, assignare licebit; sit enim $pp + qq$ divisor; erit

$$\frac{p}{q} = \frac{434 \pm 586}{541 \pm 371} \text{ vel } \frac{p}{q} = \frac{586 \pm 541}{434 \pm 371},$$

hinc

$$\frac{p}{q} = \frac{6}{1} \text{ vel } \frac{p}{q} = \frac{85}{76},$$

ergo divisores sunt 37 et 13001.

EXEMPLUM 2

18. *Explorare, utrum hic numerus* 829853 *sit primus necne.*

Cum hic numerus sit $= 1728 \cdot 480 + 413$, ad ultimam speciem pertinet, ubi valores ipsius a sunt 37, 43, 53, 107; calculus ergo sequenti modo instituatur:

$a = \pm 37$		$a = \pm 43$	
829853	57600	829853	57600
1369	17760	1849	20640
−828484	828484−	−828004	828004−
75360	39840	78240	36960
1152	1152	1152	1152
−753124	788644−	−749764	791044−
190560	155040	193440	152160
1152	1152	1152	1152
−562564	633604−	−556324	638884−
305760	270240	308640	267360
1152	1152	1152	1152
−256804	363364−	−247684	371524−

$a = \pm 53$		$a = \pm 107$	
829853	57600	829853	57600
2809	25440	11449	51360
−827044	827044−	−818404	818404−
83040	32160	108960	6240
1152	1152	1152	1152
−744004	794884−	−709444	812164−
198240	147360	224160	121440
1152	1152	1152	1152
−545764	647524−	−485284	690724−
313440	262560	339360	236640
1152	1152	1152	1152
□ 232324	384964−	□ 145924	454084−
	377760		351840
	7204−		102244−

Quoniam hic duo occurrunt quadrata, unde fit

$$829853 = 482^2 + 773^2 = 382^2 + 827^2,$$

hic numerus non est primus, sed factores habet 257 et 3229.

EXEMPLUM 3

19. *Explorare, utrum hic numerus* 2400317 *sit primus necne.*

Ex huius numeri forma $= 5000 \cdot 480 + 317$ intelligitur eum ad speciem tertiam pertinere, pro qua valores ipsius a sunt 11, 59, 91, 101, unde calculus ita se habebit:

$a = \pm 11$		$a = \pm 59$	
2400317	57600	2400317	57600
121	5280	3481	28320
−2400196	2400196−	−2396836	2396836−
62880	52320	85920	29280
1152	1152	1152	1152
−2337316	2347876−	−2310916	2367556−
178080	167520	201120	144480
1152	1152	1152	1152
−2159236	2180356−	−2109796	2223076−
293280	282720	316320	259680
1152	1152	1152	1152
□ 1865956	1897636−	−1793476	1963396−
408480	397920	431520	374880
1152	1152	1152	1152
−1457476	1499716−	−1361956	1588516−
523680	513120	546720	490080
1152	1152	1152	1152
−933796	986596−	−815236	1098436−
638880	628320	661920	605280
−294916	358276−	−153316	493156−

$a = \pm 91$		$a = \pm 101$	
2400317	57600	2400317	57600
8281	43680	10201	48480
−2392036	2392036−	−2390116	2390116□
101280	13920	106080	9120
1152	1152	1152	1152
−2290756	2378116−	−2284036	2380996−
216480	129120	221280	124320
1152	1152	1152	1152
−2074276	2248996−	−2062756	2256676−
331680	244320	336480	239520
1152	1152	1152	1152
−1742596	2004676−	−1726276	2017156−
446880	359520	451680	354720
1152	1152	1152	1152
−1295716	1645156−	−1274596	1662436−
562080	474720	566880	469920
1152	1152	1152	1152
−733636	1170436−	−707716	1192516−
677280	589920	682080	585120
1152	1152	1152	1152
−56356	580516−	−25636	607396−

Ex duobus quadratis, quae hic occurrunt, numerus propositus concluditur habere factores 53 et 45289.

EXEMPLUM 4

20. *Explorare, utrum hic numerus* 3861317 *sit primus necne.*

Cum hic numerus sit $= 8044 \cdot 480 + 197$, ad secundam speciem pertinet et calculus ita se habebit:

$a = \pm 1$		$a = \pm 31$	
3861317	57600	3861317	57600
1	480	961	14880
−3861316	3861316−	−3860356	3860356−
58080	57120	72480	42720
1152	1152	1152	1152
−3803236	3804196−	−3787876	3817636−
173280	172320	187680	157920
1152	1152	1152	1152
−3629956	3631876−	−3600196	3659716−
288480	287520	302880	273120
1152	1152	1152	1152
−3341476	3344356−	−3297316	3386596−
403680	402720	418080	388320
1152	1152	1152	1152
□ 2937796	2941636−	−2879236	2998276−
518880	517920	533280	503520
1152	1152	1152	1152
−2418916	2423716−	−2345956	2494756−
634080	633120	648480	618720
1152	1152	1152	1152
−1784836	1790596−	−1697476	1876036−
749280	748320	763680	733920
1152	1152	1152	1152
−1035556	1042276−	−933796	1142116−
864480	863520	878880	849120
−171076	178756−	−54916	292996−

$a = \pm 49$		$a = \pm 79$	
3861317	57600	3861317	57600
2401	23520	6241	37920
−3858916	3858916−	−3855076	3855076−
81120	34080	95520	19680
1152	1152	1152	1152
−3777796	3824836−	−3759556	3835396−
196320	149280	210720	134880
1152	1152	1152	1152
−3581476	3675556−	−3548836	3700516−
311520	264480	325920	250080
1152	1152	1152	1152
−3269956	3411076−	−3222916	3450436−
426720	379680	441120	365280
1152	1152	1152	1152
−2843236	3031396−	−2781796	3085156−
541920	494880	556320	480480
1152	1152	1152	1152
−2301316	2536516−	−2225476	2604676−
657120	610080	671520	595680
1152	1152	1152	1152
−1644196	1926436−	−1553956	2008996−
772320	725280	786720	710880
1152	1152	1152	1152
−871876	1201156−	−767236	1298116−
	840480		826080
	360676−		472036−

Quoniam igitur in his residuis unicum quadratum reperitur, numerus propositus certe est primus; aequatur autem summae horum duorum quadratorum $1714^2 + 961^2$.

SCHOLION

21. Cum igitur iam certi simus numerum 3861317 esse primum, hic fortasse maximus est numerus primus, quem novimus; ac si quis hunc numerum secundum regulam vulgarem explorare voluerit, divisionem per

omnes numeros primos usque ad 1965 tentare deberet, qui labor certe non solum maxime foret prolixus, sed etiam summopere taediosus, cum tamen hoc modo totum negotium brevi temporis spatio facillime expediri possit. Simili modo tentavi numerum $3862997 = 8047 \cdot 480 + 437$ ad quartam speciem referendum, quem pariter primum esse deprehendi.

Nisi autem numerus propositus in octo memoratis speciebus contineatur, etiamsi sit formae $4n + 1$, examen laborem magis operosum postulat, quamvis negotium ita dirigi queat, ut non pluribus subtractionibus sit opus. Verum cum universa haec investigatio plerisque omni usu destituta videatur, hoc argumentum fusius non prosequar, sed Theoremata tantum, quibus haec methodus innititur, breviter subiungo.

THEOREMA 1

Si sit $xx + yy = 9n + 1$, *erit vel* $x = 3p$ *vel* $x = 9p \pm 1$.

THEOREMA 2

Si sit $xx + yy = 9n + 4$, *erit vel* $x = 3p$ *vel* $x = 9p \pm 2$.

THEOREMA 3

Si sit $xx + yy = 9n + 7$, *erit vel* $x = 3p$ *vel* $x = 9p \pm 4$.

THEOREMA 4

Si sit $xx + yy = 3n + 2$, *erit* $x = 3p \pm 1$.

THEOREMA 5

Si sit $xx + yy = 5n + 2$, *erit* $x = 5p \pm 1$.

THEOREMA 6

Si sit $xx + yy = 5n + 3$, *erit* $x = 5p \pm 2$.

THEOREMA 7

Si sit $xx + yy = 25n + 1$, *erit vel* $x = 5p$ *vel* $x = 25p \pm 1$.

THEOREMA 8

Si sit $xx + yy = 25n + 4$, *erit vel* $x = 5p$ *vel* $x = 25p \pm 2$.

THEOREMA 9

Si sit $xx + yy = 25n + 6$, *erit vel* $x = 5p$ *vel* $x = 25p \pm 9$.

THEOREMA 10

Si sit $xx + yy = 25n + 9$, *erit vel* $x = 5p$ *vel* $x = 25p \pm 3$.

THEOREMA 11

Si sit $xx + yy = 25n + 11$, *erit vel* $x = 5p$ *vel* $x = 25p \pm 6$.

THEOREMA 12

Si sit $xx + yy = 25n + 14$, *erit vel* $x = 5p$ *vel* $x = 25p \pm 8$.

THEOREMA 13

Si sit $xx + yy = 25n + 16$, *erit vel* $x = 5p$ *vel* $x = 25p \pm 4$.

THEOREMA 14

Si sit $xx + yy = 25n + 19$, *erit vel* $x = 5p$ *vel* $x = 25p \pm 12$.

THEOREMA 15

Si sit $xx + yy = 25n + 21$, *erit vel* $x = 5p$ *vel* $x = 25p \pm 11$.

THEOREMA 16

Si sit $xx + yy = 25n + 24$, *erit vel* $x = 5p$ *vel* $x = 25p \pm 7$.

CONCLUSIO

Ex his theorematis sequitur, si summa duorum quadratorum habuerit hanc formam

$$xx + yy = 14400n + 11401,$$

tum quadrati imparis xx radicem fore

vel $x = 480m \pm (75, 105)$
vel $x = 1440m \pm (85, 355, 445, 715)$
vel $x = 2400m \pm (99, 501, 651, 1149)$
vel $x = 7200m \pm (149, 949, 1301, 1949, 2101, 2749, 3101, 3299)$.

Ex hoc numerorum ordine sumto $n = 700$ exploravi hunc numerum 10091401, cuius resolutionem in duo quadrata unico modo succedere deprehendi, scilicet $1251^2 + 2920^2$, quod certum est indicium hunc numerum esse primum.[1]) Habemus ergo numerum decem millionibus maiorem 10091401, quem certo novimus esse primum; si quis autem alia quacunque methodo uti voluerit, nunquam profecto tantum numerum primum exhibebit.

1) Hunc numerum 10091401 esse primum postea etiam ab A. M. LEGENDRE alia quidem methodo demonstratum est in libro, qui inscribitur *Essai sur la théorie des nombres*, Paris 1798, p. 317—320. F. R.

DE PARTITIONE NUMERORUM IN PARTES TAM NUMERO QUAM SPECIE DATAS

Commentatio 394 indicis ENESTROEMIANI
Novi commentarii academiae scientiarum Petropolitanae 14 (1769): I, 1770, p. 168—187
Summarium ibidem p. 20—22

SUMMARIUM

Methodus, qua Illustr. huius dissertationis Auctor problema de partitione numerorum olim[1]) tractavit, quum ita sit comparata, ut etiam ad alia problemata solvenda adhiberi possit, hac occasione eam ad solutionem vulgatissimi problematis, quo quaeritur, quot modis datus numerus dato tesserarum numero proiici possit, applicare constituit. Haec autem quaestio generaliter concepta eo redit, ut investigandum sit, quot modis datus numerus in datum partium numerum dispertiri queat, quarum singulae specie dentur data quoque multitudine omnium harum partium. Si nimirum concipiantur eiusmodi tesserae, quae non sex ut vulgo habent hedras, sed in quibus hedrarum numerus ad m numerum utcunque magnum ascendat, tum vero faciebus harum hedrarum inscripti sint numeri α, β, γ, δ etc., quaestio in eo versatur, ut determinetur, quot modis proiiciendo n eiusmodi tesseras numerus N produci possit. Ut vero ad huius problematis tractationem eo facilior aditus pateret, Illustr. Auctor casum primo vulgarem, quo tesserae numeris naturalibus ab 1 usque ad 6 notantur, consideravit, circa quem ostendit, si huiusmodi expressionis $(x^1+x^2+x^3+x^4+x^5+x^6)^n$ fiat evolutio, tum quamvis potestatem x^N in ea toties occurrere, quot modis proiiciendo n tesseras numerus N cadere possit. Deinde, quomodo haec evolutio aptissime sit instituenda, docet, et quaenam inde oriatur determinatio coefficientium, quae ita comparata est, ut semper quilibet coefficiens per tres praecedentes exprimatur, ubi id tamen notatu dignum evenit, ut, licet hi coefficientes tandem in nihilum abeant et postremi primis sint pares, id tamen ex ipsa earundem relatione inventa nequaquam perspicere liceat.

1) Vide notam p. 132. F. R.

Porro faciliorem exponit modum, quo hi coefficientes investigari possunt pro quovis tesserarum numero, si iidem pro numero unitate minore iam fuerint inventi, ubi etiam tabulam subiungit ostendentem, quot modis omnes numeri ab 1 ad 36 tesseris vulgaribus, quarum numerus usque ad 8 ascendit, cadere possint. At vero quum evolutio formulae primum propositae alia ratione institui possit, ut quilibet coefficiens absolute assignetur neque praecedentibus ad hoc opus sit, isthaec evolutio tanto magis expositionem meruit, quo facilius eadem ad ipsum problema generale applicari queat. Neque maiorem quidem molestiam hac evolutione adhibita facessit problema adhuc generalius propositum, quo singulae tesserae inaequali hedrarum numero praeditae supponuntur. Si enim exempli causa proponantur tres tesserae, quarum prima hexaedra, secunda octaedra, tertia vero dodecaedra est, quarum faciebus numeri naturales ab unitate incipiendo inscripti sint, atque quaeratur, quot modis tribus his tesseris numerus N cadere possit, resolutio eius quaestionis pendebit ab evolutione huius producti

$$(x+x^2+\cdots+x^6)(x+x^2+x^3+\cdots+x^8)(x+x^2+x^3+\cdots+x^{12});$$

coefficiens nimirum potestatis x^N ostendet casuum numerum.

Denique mentio instituitur quorundam elegantium Theorematum FERMATII, quorum demonstrationes ope huius methodi aptissime investigari posse videntur, licet nondum constet, quomodo id perficere liceat. Horum prius est, quod omnes numeri in tres numeros trigonales resolubiles sint, posterius vero, quod omnes numeri ex additione quaternorum quadratorum oriantur, quibus etiam hoc adiici potest, quod omnis numerus sit aggregatum m numerorum polygonalium, laterum numero existente $= m$, vel pauciorum.

1. Cum olim[1]) tractavissem problema de partitione numerorum, quo quaerebatur, quot variis modis datus numerus in duas vel tres vel quatuor vel generatim in tot partes, quot quis voluerit, discerpi possit, id potissimum curavi, ut in eius solutione nihil quicquam inductioni, cuius usus plerumque in huiusmodi problematibus solvendis solet esse frequentissimus, tribuerem. Atque methodus, qua sum usus, ita videtur comparata, ut etiam ad alia

1) Vide Commentationes 158 et 191 (indicis ENESTROEMIANI): *Observationes analyticae variae de combinationibus*, Comment. acad. sc. Petrop. **13** (1741/3), 1751, p. 64, et *De partitione numerorum*, Novi Comment. acad. sc. Petrop. **3** (1750/1), 1753, p. 125; *LEONHARDI EULERI Opera omnia*, series I, vol. 2, p. 163 et 254. Vide etiam L. EULERI *Introductionem in analysin infinitorum*, Lausannae 1748, t. I cap. XVI; *LEONHARDI EULERI Opera omnia*, series I, vol. 8. F. R.

problemata aequo successu adhiberi possit, id quod vulgatissimo illo problemate, quo quaeri solet, quot modis datus numerus dato tesserarum numero proiici possit, eo quidem amplissime extenso hic ostendere constitui.

2. Quando autem quaeritur, quot modis datus numerus N datum tesserarum numerum n proiiciendo cadere possit, quaestio huc redit, quot variis modis datus numerus N in n partes resolvi possit, quarum singulae sint vel 1 vel 2 vel 3 vel 4 vel 5 vel 6, siquidem facies tesserarum his numeris sint insignitae. Ex quo nascitur haec quaestio latius patens, quot variis modis datus numerus N dividi possit in n partes, quarum singulae sint vel α vel β vel γ vel δ etc., quorum numerorum α, β, γ, δ etc. multitudo sit pariter data, puta $= m$, ita ut partes, in quas datus numerus sit resolvendus, tam numero quam specie dentur.

3. Concipiantur scilicet eiusmodi tesserae, quae non ut vulgo sex, sed m habeant facies seu hedras, ita ut in singulis hae facies notatae sint numeris α, β, γ, δ etc., atque iam quaeritur, si habeantur n huiusmodi tesserae, quot modis iis proiiciendis datus numerus N produci possit. Possent etiam tesserae inter se dispares assumi, ita ut singulae peculiarem haberent hedrarum numerum, quae etiam in singulis peculiaribus numeris sint inscriptae; verum ex iis, quae de tesseris vulgaribus sum allaturus, etiam solutio huius quaestionis latissime patentis haud difficulter colligetur.

4. Numeros autem, quibus facies tesserarum sunt notatae, tanquam exponentes quantitatis cuiusdam x considero, ita ut pro tessera vulgari hanc habeamus expressionem

$$x^1 + x^2 + x^3 + x^4 + x^5 + x^6,$$

ubi cuique potestati unitatem pro coefficiente tribuo, quandoquidem quilibet numerus exponente designatus aeque facile cadere potest. Quodsi iam huius expressionis quadratum sumatur, quaevis potestas ipsius x tantum recipiet coefficientem, qui indicet, quot modis ea potestas ex multiplicatione binorum terminorum istius expressionis resultare, hoc est, quot modis eius exponens ex additione binorum numerorum ex ordine 1, 2, 3, 4, 5, 6 produci possit. Evoluto ergo nostrae expressionis quadrato, si in eo occurrat terminus Mx^N, inde colligitur numerum N binis tesseris iaciendis tot modis prodire, quot coefficiens M contineat unitates.

5. Simili modo evidens est, si istius expressionis sumatur cubus $(x + x^2 + x^3 + x^4 + x^5 + x^6)^3$, in eius evolutione quamvis potestatem x^N toties occurrere, quot modis eius exponens N oriri potest addendis tribus numeris ex ordine 1, 2, 3, 4, 5, 6; unde si huius potestatis coefficiens sit M totusque terminus Mx^N, ex eo concludimus numerum N tribus tesseris iaciendis tot modis produci posse, quot coefficiens M contineat unitates. Generatim ergo si sumatur exponentis n dignitas nostrae expressionis $(x+x^2+x^3+x^4+x^5+x^6)^n$, ea evoluta secundum potestates ipsius x quilibet terminus Mx^N docebit, si numerus tesserarum fuerit $= n$, iis iaciendis numerum N tot modis cadere posse, quot coefficiens M contineat unitates.

6. Si ergo tesserarum numerus fuerit $= n$ quaeraturque, quot modis datus numerus N iis proiiciendis cadere possit, quaestio resolvetur per evolutionem huius formulae

$$(x + x^2 + x^3 + x^4 + x^5 + x^6)^n;$$

cuius cum primus terminus futurus sit x^n, ultimus vero x^{6n}, prodibit huiusmodi terminorum progressio

$$x^n + Ax^{n+1} + Bx^{n+2} + Cx^{n+3} + \cdots + Mx^N + \cdots + x^{6n},$$

cuius quilibet terminus Mx^N ostendet numerum N exponenti aequalem tot modis cadere posse, quot coefficiens M contineat unitates; ex quo statim elucet quaestionem locum habere non posse, nisi numerus propositus N contineatur intra limites n et $6n$. Totum ergo negotium huc redit, ut ista progressio seu singulorum terminorum coefficientes assignentur.

7. Ad hos igitur inveniendos ponatur formula evolvenda hoc modo repraesentata

$$x^n(1 + x + x^2 + x^3 + x^4 + x^5)^n = V,$$

tum vero pro eiusdem evolutione statuatur

$$V = x^n(1 + Ax + Bx^2 + Cx^3 + Dx^4 + Ex^5 + Fx^6 + \text{etc.}).$$

Ac posito $\frac{V}{x^n} = Z$ erit ex priori differentiale logarithmicum

$$\frac{x\,dZ}{Z\,dx} = \frac{nx + 2nx^2 + 3nx^3 + 4nx^4 + 5nx^5}{1 + x + x^2 + x^3 + x^4 + x^5}.$$

Eiusdem autem valor ex posteriori prodit

$$\frac{xdZ}{Zdx} = \frac{Ax + 2Bx^2 + 3Cx^3 + 4Dx^4 + 5Ex^5 + 6Fx^6 + \text{etc.}}{1 + Ax + Bx^2 + Cx^3 + Dx^4 + Ex^5 + Fx^6 + \text{etc.}},$$

quae duae expressiones inter se debent esse aequales, unde coefficientium valores determinabuntur.

8. Constituta autem harum duarum expressionum aequalitate oritur ista aequatio

$$\begin{aligned}
&nx + nAx^2 + nBx^3 + nCx^4 + nDx^5 + nEx^6 + nFx^7 + nGx^8 + \text{etc.}\\
&\quad + 2n + 2nA + 2nB + 2nC + 2nD + 2nE + 2nF\\
&\qquad + 3n + 3nA + 3nB + 3nC + 3nD + 3nE\\
&\qquad\quad + 4n + 4nA + 4nB + 4nC + 4nD\\
&\qquad\qquad + 5n + 5nA + 5nB + 5nC\\
&= Ax + 2Bx^2 + 3Cx^3 + 4Dx^4 + 5Ex^5 + 6Fx^6 + 7Gx^7 + 8Hx^8 + \text{etc.},\\
&\quad + A + 2B + 3C + 4D + 5E + 6F + 7G\\
&\qquad + A + 2B + 3C + 4D + 5E + 6F\\
&\qquad\quad + A + 2B + 3C + 4D + 5E\\
&\qquad\qquad + A + 2B + 3C + 4D\\
&\qquad\qquad\quad + A + 2B + 3C
\end{aligned}$$

quae binae expressiones, cum secundum singulos terminos inter se debeant esse aequales, valores singulorum coefficientium suppeditabunt.

9. Hinc autem sequentes determinationes impetrantur:

$$\begin{aligned}
A &= n,\\
2B &= (n-1)A + 2n,\\
3C &= (n-2)B + (2n-1)A + 3n,\\
4D &= (n-3)C + (2n-2)B + (3n-1)A + 4n,\\
5E &= (n-4)D + (2n-3)C + (3n-2)B + (4n-1)A + 5n,\\
6F &= (n-5)E + (2n-4)D + (3n-3)C + (4n-2)B + (5n-1)A,\\
7G &= (n-6)F + (2n-5)E + (3n-4)D + (4n-3)C + (5n-2)B,\\
8H &= (n-7)G + (2n-6)F + (3n-5)E + (4n-4)D + (5n-3)C\\
&\text{etc.}
\end{aligned}$$

Quilibet ergo coefficiens determinatur per quinos praecedentium, quibus inventis erit

$$V = x^n + Ax^{n+1} + Bx^{n+2} + Cx^{n+3} + Dx^{n+4} + Ex^{n+5} + \text{etc.},$$

sicque problema de n tesseris in genere est solutum.

10. Si a qualibet superiorum aequationum praecedens subtrahatur, obtinebuntur sequentes determinationes multo simpliciores:

$$\begin{aligned}
A &= n,\\
2B &= nA + n,\\
3C &= nB + nA + n,\\
4D &= nC + nB + nA + n,\\
5E &= nD + nC + nB + nA + n,\\
6F &= nE + nD + nC + nB + nA - 5n,\\
7G &= nF + nE + nD + nC + nB - (5n-1)A,\\
8H &= nG + nF + nE + nD + nC - (5n-2)B\\
&\text{etc.}
\end{aligned}$$

Si denuo differentiae caperentur, relationes istae adhuc simpliciores essent prodituraе hoc modo:

$$\begin{aligned}
2B &= (n+1)A,\\
3C &= (n+2)B,\\
4D &= (n+3)C,\\
5E &= (n+4)D,\\
6F &= (n+5)E - 6n,\\
7G &= (n+6)F - (6n-1)A + 5n,\\
8H &= (n+7)G - (6n-2)B + (5n-1)A,\\
9I &= (n+8)H - (6n-3)C + (5n-2)B,\\
10K &= (n+9)I - (6n-4)D + (5n-3)C\\
&\text{etc.}
\end{aligned}$$

11. Hinc, prout tesserarum numerus fuerit vel 2 vel 3 vel 4, lex progressionis coefficientium erit, ut sequitur,

pro duabus	pro tribus	pro quatuor
$A = 2$	3	4
$2B = 3A$	$4A$	$5A$
$3C = 4B$	$5B$	$6B$
$4D = 5C$	$6C$	$7C$
$5E = 6D$	$7D$	$8D$
$6F = 7E - 12$	$8E - 18$	$9E - 24$
$7G = 8F - 11A + 10$	$9F - 17A + 15$	$10F - 23A + 20$
$8H = 9G - 10B + 9A$	$10G - 16B + 14A$	$11G - 22B + 19A$
$9I = 10H - 9C + 8B$	$11H - 15C + 13B$	$12H - 21C + 18B$
$10K = 11I - 8D + 7C$	$12I - 14D + 12C$	$13I - 20D + 17C$
$11L = 12K - 7E + 6D$	$13K - 13E + 11D$	$14K - 19E + 16D$
$12M = 13L - 6F + 5E$	$14L - 12F + 10E$	$15L - 18F + 15E$
etc.	etc.	etc.

Quilibet ergo coefficiens per tres praecedentes determinatur, ubi hoc imprimis est notatu dignum, quod tandem in nihilum abeant et postremi primis evadant pares, id quod ex hac lege minus perspicere licet.

12. Quo autem hanc legem clarius intelligamus, denotet haec formula

$$(N)^{(n)}$$

numerum casuum, quibus numerus N per n tesseras produci potest, ita ut sit

$$(n)^{(n)} = 1, \quad (n+1)^{(n)} = A, \quad (n+2)^{(n)} = B, \quad (n+3)^{(n)} = C,$$
$$(n+4)^{(n)} = D, \ \ldots \ (n+9)^{(n)} = I \quad \text{et} \quad (n+10)^{(n)} = K.$$

Hinc ergo fiet

$$10(n+10)^{(n)} = (n+9)(n+9)^{(n)} - (6n-4)(n+4)^{(n)} + (5n-3)(n+3)^{(n)},$$

unde concluditur fore in genere

$$\lambda(n+\lambda)^{(n)} = (n+\lambda-1)(n+\lambda-1)^{(n)} - (6n+6-\lambda)(n+\lambda-6)^{(n)} + (5n+7-\lambda)(n+\lambda-7)^{(n)}.$$

Ponamus iam $n + \lambda = N$, ut sit $\lambda = N - n$, eritque

$$(N)^{(n)} = \frac{(N-1)(N-1)^{(n)} - (7n+6-N)(N-6)^{(n)} + (6n+7-N)(N-7)^{(n)}}{N-n},$$

ubi notandum est semper fore $(P)^{(n)} = 0$, si fuerit $P < n$.

13. Facilius autem hi coefficientes definiri possunt pro quovis tesserarum numero, si iidem pro tesserarum numero unitate minore iam fuerint reperti. Si enim sit

$$(x + x^2 + x^3 + x^4 + x^5 + x^6)^n = x^n + Ax^{n+1} + Bx^{n+2} + Cx^{n+3} + Dx^{n+4} + \text{etc.}$$

ponaturque

$$(x + x^2 + x^3 + x^4 + x^5 + x^6)^{n+1} = x^{n+1} + A'x^{n+2} + B'x^{n+3} + C'x^{n+4} + D'x^{n+5} + \text{etc.},$$

erit, quia haec expressio illi per $x + x^2 + x^3 + x^4 + x^5 + x^6$ multiplicatae est aequalis,

	hinc differentiis sumendis
$A' = A + 1$	
$B' = B + A + 1$	$B' = A' + B$
$C' = C + B + A + 1$	$C' = B' + C$
$D' = D + C + B + A + 1$	$D' = C' + D$
$E' = E + D + C + B + A + 1$	$E' = D' + E$
$F' = F + E + D + C + B + A$	$F' = E' + F - 1$
$G' = G + F + E + D + C + B$	$G' = F' + G - A$
etc.,	etc.

14. Quare si modo denotandi ante introducto utamur, ex aequatione $G' = F' + G - A$ nascitur haec

$$(n+8)^{(n+1)} = (n+7)^{(n+1)} + (n+7)^{(n)} - (n+1)^{(n)},$$

quae in genere ita repraesentabitur

$$(n+1+\lambda)^{(n+1)} = (n+\lambda)^{(n+1)} + (n+\lambda)^{(n)} - (n+\lambda-6)^{(n)}.$$

Quodsi iam pro $n + \lambda$ scribatur N, erit

$$(N+1)^{(n+1)} = (N)^{(n+1)} + (N)^{(n)} - (N-6)^{(n)},$$

ubi notandum est, quamdiu fuerit $N - 6 < n$, fore $(N-6)^{(n)} = 0$. Hinc simul patet omnes hos numeros fore integros, quod ex priori lege minus apparet.

Tabula

ostendens, quot modis quilibet numerus N per n tesseras cadere possit

N	$n=1$	$n=2$	$n=3$	$n=4$	$n=5$	$n=6$	$n=7$	$n=8$
1	1	0	0	0	0	0	0	0
2	1	1	0	0	0	0	0	0
3	1	2	1	0	0	0	0	0
4	1	3	3	1	0	0	0	0
5	1	4	6	4	1	0	0	0
6	1	5	10	10	5	1	0	0
7	0	6	15	20	15	6	1	0
8	0	5	21	35	35	21	7	1
9	0	4	25	56	70	56	28	8
10	0	3	27	80	126	126	84	36
11	0	2	27	104	205	252	210	120
12	0	1	25	125	305	456	462	330
13	0	0	21	140	420	756	917	792
14	0	0	15	146	540	1161	1667	1708
15	0	0	10	140	651	1666	2807	3368
16	0	0	6	125	735	2247	4417	6147
17	0	0	3	104	780	2856	6538	10480
18	0	0	1	80	780	3431	9142	16808
19	0	0	0	56	735	3906	12117	25488
20	0	0	0	35	651	4221	15267	36688
21	0	0	0	20	540	4332	18327	50288
22	0	0	0	10	420	4221	20993	65808
23	0	0	0	4	305	3906	22967	82384
24	0	0	0	1	205	3431	24017	98813
25	0	0	0	0	126	2856	24017	113688
26	0	0	0	0	70	2247	22967	125588
27	0	0	0	0	35	1666	20993	133288
28	0	0	0	0	15	1161	18327	135954
29	0	0	0	0	5	756	15267	133288
30	0	0	0	0	1	456	12117	125588
31	0	0	0	0	0	252	9142	113688
32	0	0	0	0	0	126	6538	98813
33	0	0	0	0	0	56	4417	82384
34	0	0	0	0	0	21	2807	65808
35	0	0	0	0	0	6	1667	50288
36	0	0	0	0	0	1	917	36688

15. In his ergo seriebus etiam proprietas § 12 inventa locum habet; ita si fuerit $n = 6$, erit

$$(N)^{(6)} = \frac{(N-1)(N-1)^{(6)} - (48-N)(N-6)^{(6)} + (43-N)(N-7)^{(6)}}{N-6},$$

unde, si exempli gratia $N = 25$, erit

$$(25)^{(6)} = \frac{24\cdot(24)^{(6)} - 23\cdot(19)^{(6)} + 18\cdot(18)^{(6)}}{19};$$

at est $(24)^{(6)} = 3431$, $(19)^{(6)} = 3906$, $(18)^{(6)} = 3431$ ideoque

$$(25)^{(6)} = \frac{24\cdot 3431 - 23\cdot 3906 + 18\cdot 3431}{19} = \frac{54264}{19} = 2856,$$

uti tabula habet. Similiter si sit $N = 29$, erit

$$(29)^{(6)} = \frac{28\cdot(28)^{(6)} - 19\cdot(23)^{(6)} + 14\cdot(22)^{(6)}}{23};$$

hinc ob $(28)^{(6)} = 1161$, $(23)^{(6)} = 3906$ et $22^{(6)} = 4221$ erit

$$(29)^{(6)} = \frac{32508 - 74214 + 59094}{23} = \frac{17388}{23} = 756.$$

16. Verum evolutio formulae V (§ 7) alio modo institui potest, ut quilibet terminus absolute assignetur neque ad hoc praecedentibus sit opus. Cum enim sit

$$1 + x + x^2 + x^3 + x^4 + x^5 = \frac{1-x^6}{1-x},$$

erit

$$V = \frac{x^n(1-x^6)^n}{(1-x)^n}$$

atque evolutione facta ob

$$(1-x^6)^n = 1 - \frac{n}{1}x^6 + \frac{n(n-1)}{1\cdot 2}x^{12} - \frac{n(n-1)(n-2)}{1\cdot 2\cdot 3}x^{18} + \frac{n(n-1)(n-2)(n-3)}{1\cdot 2\cdot 3\cdot 4}x^{24} - \text{etc.},$$

$$\frac{x^n}{(1-x)^n} = x^n + \frac{n}{1}x^{n+1} + \frac{n(n+1)}{1\cdot 2}x^{n+2} + \frac{n(n+1)(n+2)}{1\cdot 2\cdot 3}x^{n+3} + \frac{n(n+1)(n+2)(n+3)}{1\cdot 2\cdot 3\cdot 4}x^{n+4} + \text{etc.}$$

inde colligitur fore

$$(n)^{(n)} = 1,$$

$$(n+1)^{(n)} = \frac{n}{1},$$

$$(n+2)^{(n)} = \frac{n(n+1)}{1\cdot 2},$$

$$(n+3)^{(n)} = \frac{n(n+1)(n+2)}{1\cdot 2\cdot 3},$$

$$(n+4)^{(n)} = \frac{n(n+1)\cdots(n+3)}{1\cdot 2\cdot 3\cdot 4},$$

$$(n+5)^{(n)} = \frac{n(n+1)\cdots(n+4)}{1\cdot 2\cdot 3\cdot 4\cdot 5},$$

$$(n+6)^{(n)} = \frac{n(n+1)\cdots(n+5)}{1\cdot 2\cdot 3\cdots 6} - \frac{n}{1}1,$$

$$(n+7)^{(n)} = \frac{n(n+1)\cdots(n+6)}{1\cdot 2\cdot 3\cdots 7} - \frac{n}{1}\cdot\frac{n}{1},$$

$$(n+8)^{(n)} = \frac{n(n+1)\cdots(n+7)}{1\cdot 2\cdot 3\cdots 8} - \frac{n}{1}\cdot\frac{n(n+1)}{1\cdot 2},$$

$$(n+9)^{(n)} = \frac{n(n+1)\cdots(n+8)}{1\cdot 2\cdot 3\cdots 9} - \frac{n}{1}\cdot\frac{n(n+1)(n+2)}{1\cdot 2\cdot 3},$$

$$(n+10)^{(n)} = \frac{n(n+1)\cdots(n+9)}{1\cdot 2\cdot 3\cdots 10} - \frac{n}{1}\cdot\frac{n(n+1)\cdots(n+3)}{1\cdot 2\cdot 3\cdot 4},$$

$$(n+11)^{(n)} = \frac{n(n+1)\cdots(n+10)}{1\cdot 2\cdot 3\cdots 11} - \frac{n}{1}\cdot\frac{n(n+1)\cdots(n+4)}{1\cdot 2\cdot 3\cdot 4\cdot 5},$$

$$(n+12)^{(n)} = \frac{n(n+1)\cdots(n+11)}{1\cdot 2\cdot 3\cdots 12} - \frac{n}{1}\cdot\frac{n(n+1)\cdots(n+5)}{1\cdot 2\cdot 3\cdots 6} + \frac{n(n-1)}{1\cdot 2}\cdot 1,$$

$$(n+13)^{(n)} = \frac{n(n+1)\cdots(n+12)}{1\cdot 2\cdot 3\cdots 13} - \frac{n}{1}\cdot\frac{n(n+1)\cdots(n+6)}{1\cdot 2\cdot 3\cdots 7} + \frac{n(n-1)}{1\cdot 2}\cdot\frac{n}{1}$$

etc.,

unde in genere concluditur

$$(n+\lambda)^{(n)}$$
$$= \frac{n(n+1)\cdots(n+\lambda-1)}{1\cdot 2\cdot 3\cdots\lambda} - \frac{n}{1}\cdot\frac{n(n+1)\cdots(n+\lambda-7)}{1\cdot 2\cdot 3\cdots(\lambda-6)} + \frac{n(n-1)}{1\cdot 2}\cdot\frac{n(n+1)\cdots(n+\lambda-13)}{1\cdot 2\cdot 3\cdots(\lambda-12)}$$
$$- \frac{n(n-1)(n-2)}{1\cdot 2\cdot 3}\cdot\frac{n(n+1)\cdots(n+\lambda-19)}{1\cdot 2\cdot 3\cdots(\lambda-18)} + \frac{n(n-1)(n-2)(n-3)}{1\cdot 2\cdot 3\cdot 4}\cdot\frac{n(n+1)\cdots(n+\lambda-25)}{1\cdot 2\cdot 3\cdots(\lambda-24)}$$
$$- \text{etc.}$$

17. Hinc solutio ad tesseras quocunque alio facierum numero praeditas accommodari potest. Sit enim m numerus facierum in singulis tesseris, quae notatae sint numeris 1, 2, 3, . . . m, talium autem tesserarum numerus sit $= n$, quibus proiectis quaeritur, quot modis datus numerus N cadere possit. Seu, quod eodem redit, quaeritur, quot modis numerus N in n partes resolvi possit, quae singulae in hoc ordine numerorum 1, 2, 3, . . . m sint contentae; ubi quidem notandum est non solum diversas partitiones, sed etiam diversos ordines earundem partium numerari, uti in tesseris fieri solet, ubi exempli gratia iactus 3, 4 et 4, 3 pro duobus diversis casibus habentur.

18. Quodsi ergo haec scriptio $(N)^{(n)}$ denotet casuum numerum, quibus numerus N proiiciendis n tesseris, quarum singulae habeant m facies numeris 1, 2, 3, . . . m notatas, produci possit, primo notandum est fore $(n)^{(n)} = 1$, et si $N < n$, esse $(N)^{(n)} = 0$. Deinde si $N = mn$, est quoque $(mn)^{(n)} = 1$, et si $N > mn$, erit $(N)^{(n)} = 0$. Denique sive sit $N = n + \lambda$ sive $N = mn - \lambda$, numerus casuum est idem seu

$$(n + \lambda)^{(n)} = (mn - \lambda)^{(n)}.$$

Postrema autem formula praebet

$$(n + \lambda)^{(n)} = \frac{n(n+1)\cdots(n+\lambda-1)}{1\cdot 2\cdot 3\cdots\lambda} - \frac{n}{1}\cdot\frac{n(n+1)\cdots(n+\lambda-m-1)}{1\cdot 2\cdot 3\cdots(\lambda-m)}$$
$$+\frac{n(n-1)}{1\cdot 2}\cdot\frac{n(n+1)\cdots(n+\lambda-2m-1)}{1\cdot 2\cdot 3\cdots(\lambda-2m)} - \frac{n(n-1)(n-2)}{1\cdot 2\cdot 3}\cdot\frac{n(n+1)\cdots(n+\lambda-3m-1)}{1\cdot 2\cdot 3\cdots(\lambda-3m)} + \text{etc.}$$

19. Facillime autem hi numeri cum ex praecedentibus tum ex casibus, ubi tesserarum numerus est unitate minor, determinabuntur. Erit enim generaliter, si singularum tesserarum numerus facierum fuerit $= m$ eaeque numeris 1, 2, 3, . . . m sint insignitae,

$$(N+1)^{(n+1)} = (N)^{(n+1)} + (N)^{(n)} - (N-m)^{(n)}$$

seu

$$(N+1)^{(n)} = (N)^{(n)} + (N)^{(n-1)} - (N-m)^{(n-1)}.$$

Hinc, si pro $N+1$ scribatur $n + \lambda$, habebitur

$$(n + \lambda)^{(n)} = (n + \lambda - 1)^{(n)} + (n + \lambda - 1)^{(n-1)} - (n + \lambda - m - 1)^{(n-1)}.$$

Denique pro eodem tesserarum numero n isti numeri ita a praecedentibus pendent, ut sit

$$\lambda(n+\lambda)^{(n)} = (n+\lambda-1)(n+\lambda-1)^{(n)} - (mn+m-\lambda)(n+\lambda-m)^{(n} + (mn-n+m+1-\lambda)(n+\lambda-m-1)^{(n)}.$$

Ceterum notum est summam omnium horum numerorum esse $= m^n$.

20. Simili modo haec quaestio resolvi potest, si non omnes tesserae pari hedrarum numero fuerint praeditae. Ponamus tres dari tesseras, primam hexaedram numeros 1, 2, 3, 4, 5, 6, secundam octaedram numeros 1, 2, 3, . . . 8 et tertiam dodecaedram numeros 1, 2, 3, . . . 12 gerentem; quodsi iam quaeratur, quot modis datus numerus N cadere possit, evolvatur hoc productum

$$(x+x^2+x^3+\cdots+x^6)(x+x^2+x^3+\cdots+x^8)(x+x^2+x^3+\cdots+x^{12}) = V$$

et coefficiens potestatis x^N ostendet casuum numerum. Cum iam sit

$$V = \frac{x^3(1-x^6)(1-x^8)(1-x^{12})}{(1-x)^3},$$

erit numeratorem evolvendo

$$V = \frac{x^3-x^9-x^{11}-x^{15}+x^{17}+x^{21}+x^{23}-x^{29}}{(1-x)^3}.$$

21. Hic numerator multiplicetur per $\frac{1}{(1-x)^3}$ seu hanc seriem

$$1+3x+6x^2+10x^3+15x^4+21x^5+28x^6+36x^7+\text{etc.},$$

cuius coefficientes sunt numeri trigonales; unde, cum numeri n trigonalis [sit] $\frac{n(n+1)}{2}$, quivis huius seriei terminus erit

$$\frac{n(n+1)}{2}x^{n-1} \quad \text{seu} \quad \frac{(n-1)(n-2)}{2}x^{n-3}.$$

Iam per numeratorem multiplicando potestatis x^n coefficiens reperitur

$$\frac{(n-1)(n-2)}{2} - \frac{(n-7)(n-8)}{2} - \frac{(n-9)(n-10)}{2} - \frac{(n-13)(n-14)}{2} + \frac{(n-15)(n-16)}{2} + \frac{(n-19)(n-20)}{2} + \frac{(n-21)(n-22)}{2} + \frac{(n-27)(n-28)}{2},$$

quae expressio autem quovis casu non ulterius continuari debet, quam donec ad factores negativos perveniatur.

22. Relicto autem denominatore $(1-x)^3 = 1 - 3x + 3x^2 - x^3$ series quaesita erit recurrens ex scala relationis 3, -3, $+1$ nata, dummodo terminorum numeratoris ratio habeatur. Hinc pro quovis exponente sequentes coefficientes inveniuntur:

Exponentes	Coefficientes	Exponentes	Coefficientes
3	1	15	47
4	3	16	45
5	6	17	42
6	10	18	38
7	15	19	33
8	21	20	27
9	27	21	21
10	33	22	15
11	38	23	10
12	42	24	6
13	45	25	3
14	47	26	1

Numeri hic maiores quam 26 produci nequeunt, cum sit $26 = 6 + 8 + 12$, et omnium casuum summa est $576 = 6 \cdot 8 \cdot 12$.

23. Cum hoc modo resolutio numerorum in partes numero et specie datas sine inductionis subsidio absolvi possit, in mentem mihi incidunt quaedam FERMATII elegantia Theoremata; quae cum nondum sint demonstrata, fortasse haec methodus ad demonstrationes eorum perductura videtur. Cum enim FERMATIUS asseverasset[1]) omnes numeros vel esse trigonales vel duorum vel trium trigonalium aggregata, quia cyphra etiam in ordine trigonalium reperitur, theorema ita enunciari potest, ut omnes numeri in tres trigonales

1) In observationibus marginalibus ad *DIOPHANTUM* BACHETI primum editis a filio S. FERMATIO, Tolosae 1670. Vide notam 4 p. 358 voluminis praecedentis. Vide etiam EULERI epistolam d. 4. Maii 1748 ad CHR. GOLDBACH datam, *Correspondance math. et phys. publiée par P. H. Fuss*, St.-Pétersbourg 1843, t. I, p. 450; *LEONHARDI EULERI Opera omnia*, series III. F. R.

resolubiles dicantur. Quare si numeris trigonalibus pro exponentibus sumtis formetur haec series

$$1 + x^1 + x^3 + x^6 + x^{10} + x^{15} + x^{21} + x^{28} + \text{etc.} = S,$$

demonstrari oportet, si huius seriei cubus evolvatur, tum omnes plane potestates ipsius x esse occursuras nullamque omissum iri; quod si demonstrari posset, haberetur demonstratio istius Theorematis FERMATIANI.[1])

24. Simili modo si huius seriei

$$1 + x^1 + x^4 + x^9 + x^{16} + x^{25} + x^{36} + \text{etc.} = S$$

sumatur potestas quarta ostendique queat in ea omnes plane potestates ipsius x reperiri, habebitur demonstratio huius Theorematis FERMATIANI[2]), quo omnes numeri ex additione quaternorum quadratorum resultare statuuntur.

In genere autem si ponatur

$$S = 1 + x^1 + x^m + x^{3m-3} + x^{6m-8} + x^{10m-15} + x^{15m-24} + x^{21m-35} + \text{etc.}$$

huiusque seriei sumatur potestas exponentis m, demonstrandum est in ea omnes potestates ipsius x esse produturas, ita ut omnis numerus sit aggregatum m numerorum polygonalium, laterum numero existente $= m$, vel pauciorum.[3])

25. Ex iisdem principiis alia se offert via ad has demonstrationes investigandas, quae a praecedente hoc differt, quod, uti ibi non solum diversitas

---

1) Quae demonstratio primum data est a C. F. GAUSS, *Disquisitiones arithmeticae,* Lipsiae 1801, art. 293; *C. F. Gauss Werke*, I, p. 348. F. R.

2) Hoc theorema primum demonstratum ab I. L. LAGRANGE recte BACHETIANUM, non FERMATIANUM appellari debet. Vide EULERI Commentationem 242 (indicis ENESTROEMIANI): *Demonstratio theorematis FERMATIANI omnem numerum sive integrum sive fractum esse summam quatuor pauciorumve quadratorum*, Novi comment. acad. sc. Petrop. 5 (1754/5), 1760, p. 13; *LEONHARDI EULERI Opera omnia*, series I, vol. 2, p. 338 (vide imprimis notam 4 p. 358 et notam 2 p. 370). Vide etiam EULERI epistolam nota p. 144 laudatam. F. R.

3) Hoc theorema generale primum demonstratum est ab A. CAUCHY, *Démonstration générale du théorème de FERMAT sur les nombres polygones*, Mémoires de l'Institut, t. XIV, 1re série (années 1813, 1814, 1815), p. 177; *Oeuvres complètes*, IIe série, t. 6, p. 320. F. R.

partium, sed etiam ordo spectatur, hic ordinis ratio omittitur. Pro resolutione scilicet in triangulares numeros constituatur haec formula

$$\frac{1}{(1-z)(1-xz)(1-x^3z)(1-x^6z)(1-x^{10}z)(1-x^{15}z)\text{ etc.}},$$

quae evoluta hanc praebeat seriem

$$1 + Pz + Qz^2 + Rz^3 + Sz^4 + Tz^5 + \text{etc.},$$

ita ut P, Q, R, S etc. sint functiones ipsius x tantum. Manifestum autem est fore

$$P = 1 + x + x^3 + x^6 + x^{10} + x^{15} + x^{21} + \text{etc.};$$

at Q praeterea eas potestates ipsius x continebit, quarum exponentes sunt aggregata duorum trigonalium. Demonstrari ergo debet in functione R omnes plane potestates ipsius x esse occursuras.

26. Simili modo pro resolutione numerorum in quaterna quadrata evolvatur haec fractio

$$\frac{1}{(1-z)(1-xz)(1-x^4z)(1-x^9z)(1-x^{16}z)(1-x^{25}z)\text{ etc.}};$$

quae si abeat in hanc formam

$$1 + Pz + Qz^2 + Rz^3 + Sz^4 + \text{etc.},$$

demonstrandum est functionem S omnes potestates ipsius x complecti. Nam P aequatur seriei $1 + x + x^4 + x^9 + x^{16} + \text{etc.}$ et Q praeterea eas continet potestates ipsius x, quarum exponentes sunt aggregata duorum quadratorum, in qua ergo serie multae adhuc potestates desunt. In R autem insuper eae potestates, quarum exponentes sunt aggregata ternorum quadratorum, aderunt atque in S quoque eae, quarum exponentes sunt summae quaternorum, ita ut in S omnes numeri in exponentibus occurrere debeant.

27. Ex hoc principio definiri potest, quot solutiones problemata, quae ab Arithmeticis ad *Regulam Virginum*[1]) referri solent, admittant. Huiusmodi

1) De hac *Regula Virginum* (*Regula Coeci*, *Regula Potatorum*) vide L. Euler, *Vollständige Anleitung zur Algebra*, St. Petersburg 1770, Zweyter Theil, zweyter Abschnitt, Cap. 2; *Leonhardi*

problemata huc redeunt, ut inveniri debeant numeri p, q, r, s, t etc., ita ut his duabus conditionibus satisfiat

$$ap + bq + cr + ds + \text{etc.} = n$$

et

$$\alpha p + \beta q + \gamma r + \delta s + \text{etc.} = \nu,$$

et iam quaestio est, quot solutiones in numeris integris positivis locum sint habiturae; ubi quidem tenendum est numeros a, b, c, d etc., n et α, β, γ, δ etc., ν esse integros, quia, nisi tales essent, facile eo reducerentur. Statim quidem apparet, si duo tantum numeri inveniendi p et q proponantur, plus una solutione non dari, quae adeo, nisi pro p et q numeri integri positivi prodeant, pro nulla haberi solet.

28. Iam ad numerum omnium solutionum quovis casu definiendum, ne inductioni seu tentationi quicquam tribuatur, consideretur haec expressio

$$\frac{1}{(1-x^a y^\alpha)(1-x^b y^\beta)(1-x^c y^\gamma)(1-x^d y^\delta)\text{ etc.}}$$

eaque evolvatur, unde prodibit huiusmodi series

$$1 + Ax^{\cdot\cdot}y^{\cdot\cdot} + Bx^{\cdot\cdot}y^{\cdot\cdot} + Cx^{\cdot\cdot}y^{\cdot\cdot} \text{ etc.};$$

in qua si occurrat terminus $Nx^n y^\nu$, coefficiens N numerum solutionum indicabit; ac si eveniat, ut hic terminus non occurrat, id indicio erit nullam dari solutionem. Totum ergo negotium in hoc versatur, ut coefficiens huius termini $x^n y^\nu$ investigetur.

Euleri Opera omnia, series I, vol. 1. Vide porro M. Cantor, *Vorlesungen über Geschichte der Mathematik*, II, 2. Aufl., Leipzig 1900, p. 428—429, praecipue autem observationes, quas G. Enestroem sub titulo *Kleine Bemerkungen zur zweiten Auflage von Cantors „Vorlesungen über Geschichte der Mathematik"* huc adiecit, Biblioth. Mathem. 5_3, 1904, p. 201—202, et 8_3, 1907/8, p. 208—209. F. R.

SOLUTIO PROBLEMATIS QUO DUO QUAERUNTUR NUMERI QUORUM PRODUCTUM TAM SUMMA QUAM DIFFERENTIA EORUM SIVE AUCTUM SIVE MINUTUM FIAT QUADRATUM[1])

Commentatio 405 indicis ENESTROEMIANI
Novi commentarii academiae scientiarum Petropolitanae 15 (1770), 1771, p. 29—50
Summarium ibidem p. 8—11

SUMMARIUM

Problema, quod Ill. Auctor in hac dissertatione evolvit, ad Analysin DIOPHANTEAM pertinet seque non sua solum elegantia, sed et eo commendat, quod ad eius solutionem singularia requirantur calculi artificia. Quamquam perspecta problematis natura pateat id innumerabiles solutiones admittere, tamen Ill. Auctor post plura demum tentamina binos numeros problemati idoneos invenire potuit idque methodo indirecta, quae ad inventionem plurium eiusmodi numerorum nihil praestaret subsidii. Idem tamen argumentum cum Ill. Auctor postea iterum meditationi suae subiiceret, casu fortuito et singulari in solutionem generalem incidit; quam igitur in praesenti dissertatione evolvit uberius et artificia exponit, quorum ope superatis problematis difficultatibus ad istam solutionem pervenit. Problema in eo consistit, ut satisfiat his quatuor aequationibus

$$\text{I. } AB + A + B = \square, \qquad \text{II. } AB + A - B = \square,$$
$$\text{III. } AB - A + B = \square, \qquad \text{IV. } AB - A - B = \square.$$

---

1) Simplicius problema, quo tantum duo quaeruntur numeri, quorum productum sive auctum sive minutum summa eorum fiat quadratum, iam in quaestione XXX libri II DIOPHANTI *Arithmeticorum* (ed. P. TANNERY; quae quaestio est quaestio XXXI editionis BACHETI; vide notam p. 404 voluminis praecedentis) pertractatum est. F. R.

Haud ita difficulter statim iudicari potest istos numeros integros esse non posse; unde posito $A = \frac{z}{x}$ et $B = \frac{z}{y}$ et admissa signi ambiguitate aequationes quatuor adimplendae his duabus formulis repraesentari possunt

$$\frac{z}{xy}(z + y \mp x) = \square \quad \text{et} \quad \frac{z}{xy}(z - y \mp x) = \square;$$

in quibus ut factor posterior evadat quadratus, facile efficitur ponendo

$$z = \frac{(pp + ss)(qq + rr)}{2}, \quad [x = 2pqrs] \quad \text{et} \quad y = \frac{(pp - ss)(qq - rr)}{2};$$

praecipua vero difficultas in eo versatur, ut pro p, q, r, s eiusmodi assumantur valores, quibus et alter ille factor communis $\frac{z}{xy}$ quadratum reddatur. Quodsi igitur modo memorati ipsorum $[z]$, x, y valores in hoc factore substituantur, formula, quae quadrata est efficienda, inde resultans

$$2pqrs(pp - ss)(qq - rr)(pp + ss)(qq + rr) = \square$$

non quatuor solum quantitates diversas continet, sed singulae etiam illae quantitates ad quintam usque dimensionem assurgunt; ex quo facile liquet problematis huius solutionem longe transcendere communia illa artificia, quae pro resolutione eiusmodi quaestionum in Analyseos DIOPHANTEAE institutionibus tradi sunt solita. Ad superandam hanc difficultatem Ill. Auctor eo utitur artificio, ut aliquot ingeniosis positionibus factoribus denominatoris fractionis memoratae $\frac{z}{xy}$ tot, quot fieri potest, communes divisores concilientur; quorum multiplicatio cum factores efficiat quadraticos, iis omissis quaestio ad formulam multo simpliciorem

$$\frac{5mm - 6mn - 2nn}{2n(2m + n)}$$

quadratam efficiendam revocatur, cui adeo, statim ac unicus casus idoneus innotuit, innumerabilibus modis satisfieri potest; cum scilicet tam numerator quam denominator quadratum esse debeat, eorum quoque productum tale sit necesse est; ex hac vero multiplicatione formula resultat, quae generaliter ita repraesentari potest

$$\alpha\alpha z^4 - 2\beta z^3 + \gamma z^2 - 2\delta z + \varepsilon\varepsilon = \square,$$

cuius quidem aequationis resolutionem et quatuor ipsius z idoneos valores etiam per consuetas[1]) methodos invenire licet; quemadmodum vero infinite multae solutiones erui queant, Ill. Auctor hic uberius exponit. Sub finem dissertationis, quamquam problema iam fuerit resolutum, aliae superadduntur transformationes formulae resolvendae; indeque casus complures speciales actu evolvuntur, inter quos bini sequentes in numeris non nimis magnis notatu imprimis digni videntur

$$A = \frac{10933}{648} \quad \text{et} \quad B = \frac{4205}{3872}.$$

1) Vide notam p. 157. F. R.

1. Problema hoc mihi ante complures annos Berolini a Centurione quodam Prussico erat propositum, quod se Lipsiae ab amico accepisse aiebat; neque vero se neque istum amicum solutionem ullo modo invenire potuisse. Quaerebat igitur ex me, utrum hoc problema possibile iudicarem necne. Statim quidem hoc problema mihi ob elegantiam mirifice placebat, et quum facile summam solutionis difficultatem perspexissem, id omnino dignum iudicavi, in quo vires meas exercerem. Tandem vero post plura tentamina solutionem sum adeptus, quae ita se habebat. Positis duobus numeris quaesitis A et B inveni

$$A = \frac{13 \cdot 29^2}{8 \cdot 9^2} = \frac{10933}{648} \quad \text{et} \quad B = \frac{5 \cdot 29^2}{32 \cdot 11^2} = \frac{4205}{3872}.$$

2. Via autem, qua ad hanc solutionem perveni, ita erat comparata, ut nullo modo mihi liceret alias solutiones inde eruere, etiamsi nullus dubitandi locus relinqueretur, quin hoc problema innumerabiles admitteret solutiones. Nuper autem cum in hoc idem argumentum incidissem, casu prorsus fortuito methodus mihi se obtulit infinitas solutiones huius problematis eliciendi. Quod quum casui prorsus singulari sit acceptum referendum, quaestio haec omnino digna mihi est visa, quam accuratius perscrutarer. Quare primo quidem solutionem generalem proponam, deinde vero artificium illud, quod mihi infinitas solutiones suppeditavit, uberius evolvam.

SOLUTIO PROBLEMATIS GENERALIS

3. Si litterae A et B denotent ambos numeros quaesitos, necesse est, ut sequentes quatuor formulae quadrata efficiantur

$$\text{I. } AB + A + B = \square, \qquad \text{II. } AB + A - B = \square,$$

$$\text{III. } AB - A + B = \square, \qquad \text{IV. } AB - A - B = \square.$$

Quum autem statim pateat hos numeros integros esse non posse ob rationes mox perspiciendas, eos ita expressos assumo, ut sit

$$A = \frac{z}{x} \quad \text{et} \quad B = \frac{z}{y},$$

ita ut quatuor sequentes formulae ad quadrata reducendae habeantur

$$\text{I. } \frac{z}{xy}(z+y+x) = \square, \qquad \text{II. } \frac{z}{xy}(z+y-x) = \square,$$

$$\text{III. } \frac{z}{xy}(z-y+x) = \square, \qquad \text{IV. } \frac{z}{xy}(z-y-x) = \square.$$

4. Quodsi ergo factor communis fuerit quadratum, quatuor sequentes formulas quadrata effici oportet, quas quidem per ambiguitatem signorum ita duabus formulis comprehendere licet

$$\text{I. et II. } z+y \pm x = \square, \qquad \text{III. et IV. } z-y \pm x = \square.$$

Quare, quum in genere sit $aa + bb \pm 2ab = \square$ similique modo $cc + dd \pm 2cd = \square$, statuamus, ut sequitur,

$$z + y = aa + bb, \quad x = 2ab,$$
$$z - y = cc + dd, \quad x = 2cd.$$

Ut autem fiat $2ab = 2cd$, statuatur utrumque

$$= 2pqrs = x$$

sumaturque

$$a = pq, \quad b = rs, \quad c = pr \quad \text{et} \quad d = qs$$

eritque

$$z + y = aa + bb = ppqq + rrss$$

et

$$z - y = cc + dd = pprr + qqss,$$

unde colligitur

$$z = \frac{(pp+ss)(qq+rr)}{2} \quad \text{et} \quad y = \frac{(pp-ss)(qq-rr)}{2};$$

tum vero erit

$$\text{I. } z + y + x = (a+b)^2 = (pq+rs)^2,$$
$$\text{II. } z + y - x = (a-b)^2 = (pq-rs)^2,$$
$$\text{III. } z - y + x = (c+d)^2 = (pr+qs)^2,$$
$$\text{IV. } z - y - x = (c-d)^2 = (pr-qs)^2.$$

5. Superest igitur, ut etiam factor communis $\frac{z}{xy}$ quadratum reddatur, qui evolutus praebet hanc formulam

$$\frac{z}{xy} = \frac{(pp+ss)(qq+rr)}{2pqrs(pp-ss)(qq-rr)};$$

at vero in hoc efficiendo summa consistit difficultas; quodsi enim numerator in denominatorem ducatur, ut haec formula quadratum fieri debeat

$$2pqrs(pp-ss)(qq-rr)(pp+ss)(qq+rr) = \square,$$

singulae litterae ad quinque dimensiones assurgunt, cuiusmodi quaestiones in Analysi DIOPHANTEA adhuc non sunt tractari solitae; ceterum iam olim post plura tentamina repperi huic conditioni satisfieri sumendo $p = 13$, $s = 11$, $q = 16$ et $r = 11$, uti periculum facienti mox patebit.[1])

6. Quodsi autem quocumque modo huiusmodi valores idonei pro litteris p, q, r, s fuerint inventi, solutio problematis inde ita adstruitur. Posita formula

$$\frac{(pp+ss)(qq+rr)}{2pqrs(pp-ss)(qq-rr)} = \frac{M^2}{N^2}$$

primo ambo numeri quaesiti ita erunt expressi

$$A = \frac{(pp+ss)(qq+rr)}{4pqrs} \quad \text{et} \quad B = \frac{(pp+ss)(qq+rr)}{(pp-ss)(qq-rr)},$$

tum vero conditionibus problematis ita satisfiet, ut sit

$$\text{I.} \quad \sqrt{(AB+A+B)} = \frac{M}{N}(pq+rs),$$

$$\text{II.} \quad \sqrt{(AB+A-B)} = \frac{M}{N}(pq-rs),$$

$$\text{III.} \quad \sqrt{(AB-A+B)} = \frac{M}{N}(pr+qs),$$

$$\text{IV.} \quad \sqrt{(AB-A-B)} = \frac{M}{N}(pr-qs).$$

1) Quibus valoribus substitutis formula ista revera abit in 5971680^2. F. R.

SINGULARIS EVOLUTIO NOSTRAE FORMULAE QUAE AD QUADRATUM EST REVOCANDA

7. Quum omnis opera in hac formula reducenda frustra consumatur, quamdiu in ea tot diversae quantitates occurrunt earumque singulae ad tot dimensiones assurgunt, ante omnia elaborandum est, ut diversis factoribus denominatoris communes divisores concilientur; hunc in finem usus sum sequentibus positionibus

$$p + s = \alpha\beta, \quad p - s = \varepsilon\zeta, \quad q + r = \alpha\gamma \quad \text{et} \quad q - r = \varepsilon\eta,$$

ita ut fiat

$$p = \frac{\alpha\beta + \varepsilon\zeta}{2}, \quad s = \frac{\alpha\beta - \varepsilon\zeta}{2}, \quad q = \frac{\alpha\gamma + \varepsilon\eta}{2} \quad \text{et} \quad r = \frac{\alpha\gamma - \varepsilon\eta}{2};$$

tum vero nostra conditio principalis postulat, ut sit

$$\frac{(pp + ss)(qq + rr)}{2pqrs \cdot \beta\gamma\zeta\eta \cdot \alpha^2\varepsilon^2} = \frac{M^2}{N^2} \quad \text{sive} \quad \frac{(pp + ss)(qq + rr)}{2pqrs \cdot \beta\gamma\zeta\eta} = \frac{M^2}{N^2}\alpha^2\varepsilon^2.$$

8. Secundo constituatur ratio inter litteras r et s, quae sit ut $f : g$, eritque

$$f : g :: \alpha\gamma - \varepsilon\eta : \alpha\beta - \varepsilon\zeta \quad \text{sive} \quad g(\alpha\gamma - \varepsilon\eta) = f(\alpha\beta - \varepsilon\zeta),$$

unde colligitur

$$\alpha(f\beta - g\gamma) = \varepsilon(f\zeta - g\eta),$$

quocirca ponamus

$$\alpha = f\zeta - g\eta, \quad \varepsilon = f\beta - g\gamma;$$

tum vero habebitur

$$p = \frac{2f\beta\zeta - g\beta\eta - g\gamma\zeta}{2}, \quad q = \frac{f\beta\eta + f\zeta\gamma - 2g\gamma\eta}{2},$$

$$r = \frac{f(\gamma\zeta - \beta\eta)}{2} \quad \text{et} \quad s = \frac{g(\gamma\zeta - \beta\eta)}{2}.$$

9. Ut adhuc plures factores in denominatore communes reddamus, faciamus insuper $q = h\beta\zeta$, unde haec aequatio emergit

$$2h\beta\zeta = f\beta\eta + f\zeta\gamma - 2g\gamma\eta \quad \text{sive} \quad \beta(2h\zeta - f\eta) = \gamma(f\zeta - 2g\eta),$$

quamobrem ponamus

$$\beta = f\zeta - 2g\eta \quad \text{et} \quad \gamma = 2h\zeta - f\eta.$$

Ex his autem valoribus porro colligimus

$$\alpha = f\zeta - g\eta, \quad \varepsilon = (ff - 2gh)\zeta - fg\eta,$$
$$p + s = (f\zeta - g\eta)(f\zeta - 2g\eta) = ff\zeta\zeta - 3fg\zeta\eta + 2gg\eta\eta,$$
$$p - s = \zeta((ff - 2gh)\zeta - fg\eta) = (ff - 2gh)\zeta\zeta - fg\zeta\eta,$$
$$q + r = (f\zeta - g\eta)(2h\zeta - f\eta) = 2fh\zeta\zeta - (ff + 2gh)\zeta\eta + fg\eta\eta,$$
$$q - r = \eta((ff - 2gh)\zeta - fg\eta) = (ff - 2gh)\zeta\eta - fg\eta\eta$$

hincque porro

$$p = (ff - gh)\zeta\zeta - 2fg\zeta\eta + gg\eta\eta,$$
$$s = gh\zeta\zeta - fg\zeta\eta + gg\eta\eta = g(h\zeta\zeta - f\zeta\eta + g\eta\eta),$$
$$q = fh\zeta\zeta - 2gh\zeta\eta = h\zeta(f\zeta - 2g\eta),$$
$$r = fh\zeta\zeta - ff\zeta\eta + fg\eta\eta = f(h\zeta\zeta - f\zeta\eta + g\eta\eta).$$

10. Denique hos valores ita determinemus, ut numerus p divisor evadat formulae $qq + rr$; iam vero invenitur

$$qq + rr = ffgg\eta^4 - 2f^3g\eta^3\zeta + (f^4 + 2ffgh + 4gghh)\eta\eta\zeta\zeta - 2fh(ff + 2gh)\eta\zeta^3 + 2ffhh\zeta^4;$$

quare, quum sit $p = gg\eta\eta - 2fg\eta\zeta + (ff - gh)\zeta\zeta$, ut p fiat factor illius formulae, statuatur alter factor $ff\eta\eta + t\eta\zeta + u\zeta\zeta$ eritque productum

$$\begin{array}{llll} ffgg\eta^4 - 2f^3g\eta^3\zeta + (f^4 - ffgh)\eta\eta\zeta\zeta + t(ff - gh)\eta\zeta^3 + u(ff - gh)\zeta^4, \\ \quad + tgg & \quad - 2tfg & \quad - 2ufg \\ & \quad + ugg & \end{array}$$

ubi primi termini iam congruunt, secundi vero dant $t = 0$, tertii

$$3ffgh + 4gghh = ugg,$$

unde

$$u = \frac{3ffh}{g} + 4hh;$$

quarti porro praebent

$$u = \frac{h(ff + 2gh)}{g},$$

quinti vero tandem dant

$$u = \frac{2ffhh}{ff - gh}.$$

Necesse igitur est, ut hi tres valores ipsius u inter se congruant; primus vero cum secundo collatus dat $3ffh + 4ghh = hff + 2ghh$ seu $2ffh + 2ghh = 0$ ideoque

$$ff + gh = 0,$$

at secundus tertio aequatus dat $f^4 - ffgh - 2gghh = 0$ sive

$$(ff + gh)(ff - 2gh) = 0;$$

utrique ergo conditioni satisfit uno eodemque valore

$$h = -\frac{ff}{g}.$$

11. Quoniam igitur invenimus $h = -\frac{ff}{g}$, reliqui valores sequenti modo exprimentur

$$p = 2ff\zeta\zeta - 2fg\zeta\eta + gg\eta\eta,$$

$$q = -\frac{ff}{g}\zeta(f\zeta - 2g\eta) = 2ff\zeta\eta - \frac{f^3}{g}\zeta\zeta,$$

$$r = -\frac{f^3}{g}\zeta\zeta - ff\zeta\eta + fg\eta\eta,$$

$$s = -ff\zeta\zeta - fg\zeta\eta + gg\eta\eta,$$

ubi notatu dignum evenit, ut in valoribus p et s producta $f\zeta$ et $g\eta$ tamquam simplices quantitates occurrant, quod quidem in litteris q et r non accidit. Verum quia totum negotium tantum in ratione q ad r versatur, hi ambo valores multiplicentur per $-\frac{g}{f}$, ut sit

$$q = ff\zeta\zeta - 2fg\zeta\eta \quad \text{et} \quad r = ff\zeta\zeta + fg\zeta\eta - gg\eta\eta;$$

hanc ob rem, ut formulas nostras in compendium redigamus atque adeo ad duas quantitates revocemus, statuamus

$$f\zeta = m \quad \text{et} \quad g\eta = n,$$

quo facto nostrae quatuor litterae ita se habebunt

$$p = 2mm - 2mn + nn, \quad q = mm - 2mn = m(m - 2n),$$
$$s = -mm - mn + nn, \quad r = mm + mn - nn.$$

12. Quoniam vero res eodem redit, sive quaepiam littera positive sive negative accipiatur, ponamus

$$p = 2mm - 2mn + nn, \quad q = mm - 2mn = m(m - 2n),$$
$$s = r = mm + mn - nn,$$

unde fit

$$p + s = 3mm - mn = m(3m - n),$$
$$p - s = mm - 3mn + 2nn = (m - n)(m - 2n),$$
$$q + r = 2mm - mn - nn = (m - n)(2m + n),$$
$$q - r = -3mn + nn = -n(3m - n).$$

Hic signum negationis in valore $q - r$ nihil plane turbat; tantum enim opus est litteras q et r inter se permutari, ita ut sit

$$p = 2mm - 2mn + nn, \quad q = mm + mn - nn,$$
$$s = mm + mn - nn, \quad r = mm - 2mn = m(m - 2n),$$

unde fit

$$p + s = 3mm - mn = m(3m - n),$$
$$p - s = mm - 3mn + 2nn = (m - n)(m - 2n),$$
$$q + r = 2mm - mn - nn = (2m + n)(m - n),$$
$$q - r = 3mn - nn = n(3m - n),$$

quibus valoribus in sequenti calculo utemur.

13. His constitutis valoribus pro numeratore nostrae fractionis habebimus

$$pp + ss = 5m^4 - 6m^3n + 7mmnn - 6mn^3 + 2n^4$$

seu

$$pp + ss = (mm + nn)(5mm - 6mn + 2nn)$$

et

$$qq + rr = 2m^4 - 2m^3n + 3mmnn - 2mn^3 + n^4$$

sive

$$qq + rr = (mm + nn)(2mm - 2mn + nn),$$

unde fractio nostra ad quadratum reducenda erit

$$\frac{MM}{NN} = \frac{(5mm - 6mn + 2nn)(mm + nn)^2}{2n(2m+n)m^2(m-n)^2(m-2n)^2(3m-n)^2(mm+mn-nn)^2},$$

hincque colligimus

$$\frac{M}{N} = \frac{mm + nn}{m(m-n)(m-2n)(3m-n)(mm+mn-nn)} \sqrt{\frac{5mm - 6mn + 2nn}{2n(2m+n)}};$$

totum ergo negotium huc est reductum, ut formula

$$\frac{5mm - 6mn + 2nn}{2n(2m+n)}$$

quadratum efficiatur, id quod infinitis modis praestari posse manifestum est, statim atque unicus casus innotuerit.

14. Quo haec forma tractabilior reddatur, ponamus $2m - n = l$, ut sit $n = 2m - l$, et formula ad quadratum reducenda erit

$$\frac{mm - 2ml + 2ll}{(4m-2l)(4m-l)},$$

ubi productum ex numeratore in denominatorem evolutum, quippe quod etiam quadratum esse debet, perducit ad hanc conditionem

$$16m^4 - 44m^3l + 58mmll - 28ml^3 + 4l^4 = \square;$$

cuius quum ambo termini extremi iam sint quadrati, per methodos satis cognitas[1]) facile est innumerabiles solutiones investigare; quem in finem ponamus $\frac{m}{l} = z$, ut habeamus hanc formulam

$$16z^4 - 44z^3 + 58zz - 28z + 4 = \square,$$

quae ponendo $z = y - 2$ transit in hanc

$$16y^4 - 172y^3 + 706yy - 1300y + 900 = \square,$$

ubi iterum ambo extremi termini sunt quadrata.

1) Vide L. Euler, *Vollständige Anleitung zur Algebra*, St. Petersburg 1770, Zweyter Theil, zweyter Abschnitt, Cap. 9; *Leonhardi Euleri Opera omnia*, series I, vol. 1, p. 396 F. R.

15. Ad hoc negotium expediendum praestabit resolutionem nostrae aequationis sive prioris sive posterioris in genere docere. Sit igitur proposita haec aequatio generalis

$$\alpha\alpha z^4 - 2\beta z^3 + \gamma zz - 2\delta z + \varepsilon\varepsilon = \square$$

atque pro idoneis valoribus ipsius z sequentes quatuor formulae per methodos consuetas[1]) reperiuntur

$$\text{I.}\quad z = \frac{2\alpha(\beta\varepsilon - \alpha\delta)}{2\alpha^3\varepsilon + \beta\beta - \alpha\alpha\gamma},$$

$$\text{II.}\quad z = \frac{2\alpha\varepsilon^3 + \delta\delta - \gamma\varepsilon\varepsilon}{2\varepsilon(\alpha\delta - \beta\varepsilon)},$$

$$\text{III.}\quad z = \frac{(2\alpha^3\varepsilon + \alpha\alpha\gamma - \beta\beta)(2\alpha^3\varepsilon - \alpha\alpha\gamma + \beta\beta)}{4\alpha\alpha(2\alpha^4\delta - \alpha\alpha\beta\gamma + \beta^3)},$$

$$\text{IV.}\quad z = \frac{4\varepsilon\varepsilon(2\beta\varepsilon^4 - \gamma\delta\varepsilon\varepsilon + \delta^3)}{(2\alpha\varepsilon^3 + \gamma\varepsilon\varepsilon - \delta\delta)(2\alpha\varepsilon^3 - \gamma\varepsilon\varepsilon + \delta\delta)};$$

ubi quum litterae α et ε pro lubitu tam positive quam negative accipi queant, binae priores formulae geminos valores suppeditant.

16. Quemadmodum autem innumerabiles huius aequationis solutiones inveniri oporteat, sequenti modo calculus instituatur. Sit f valor quicumque per praecedentes formulas inventus, ita ut nostra expressio

$$\alpha\alpha z^4 - 2\beta z^3 + \gamma zz - 2\delta z + \varepsilon\varepsilon$$

posito $z = f$ fiat quadratum, sitque propterea

$$\alpha\alpha f^4 - 2\beta f^3 + \gamma ff - 2\delta f + \varepsilon\varepsilon = gg;$$

nunc igitur ponatur $z = x + f$ et nostra aequatio induet hanc formam

$$\begin{array}{rrrrrrrrr} \alpha\alpha x^4 & + & 4\alpha\alpha x^3 & + & 6\alpha\alpha ff x^2 & + & 4\alpha\alpha f^3 x & + & gg = \square, \\ - & 2\beta & - & 6\beta f & - & 6\beta ff & & & \\ & & + & \gamma & + & 2\gamma f & & & \\ & & & & - & 2\delta & & & \end{array}$$

1) Vide notam praecedentem. Sequentes quatuor formulae alia quidem significatione adhibita loco ibi citato eliciuntur. F. R.

quae aequatio brevitatis gratia ita repraesentetur

$$aax^4 - 2bx^3 + cxx - 2dx + ee = \square,$$

ita ut sit

$$aa = \alpha\alpha, \quad b = \beta - 2\alpha\alpha, \quad c = \gamma - 6\beta f + 6\alpha\alpha ff,$$

$$d = \delta - \gamma f + 3\beta ff - 2\alpha\alpha f^3 \text{ ac denique } ee = gg,$$

ubi sumi potest $a = \pm\alpha$ et $e = \pm g$. Tum vero quatuor novi valores pro z inveniuntur sequentes

$$\text{I.} \quad z = f + \frac{2a(be - ad)}{2a^3e + bb - aac},$$

$$\text{II.} \quad z = f + \frac{2ae^3 + dd - cee}{2e(ad - be)},$$

$$\text{III.} \quad z = f + \frac{(2a^3e + aac - bb)(2a^3e - aac + bb)}{4aa(2a^4d - aabc + b^3)},$$

$$\text{IV.} \quad z = f + \frac{4ee(2be^4 - cdee + d^3)}{(2ae^3 + cee - dd)(2ae^3 - cee + dd)};$$

quoniam igitur quemcumque valorem pro z hoc modo inventum assumere licet, hinc numerus solutionum in infinitum augeri poterit.

17. Postquam autem pro z valor quicumque idoneus fuerit inventus, qui sit $z = \frac{h}{k}$, ob $z = \frac{m}{l} = \frac{m}{2m - n}$ habebimus

$$m = h \quad \text{et} \quad n = 2h - k,$$

ex quibus duobus numeris m et n reliquae quantitates sequenti modo determinantur

$$p = 2mm - 2mn + nn, \quad q = mm + mn - nn,$$

$$s = mm + mn - nn, \quad r = mm - 2mn = m(m - 2n),$$

ubi notasse iuvabit esse

$$pp + ss = (mm + nn)(5mm - 6mn + 2nn)$$

et

$$qq + rr = (mm + nn)(2mm - 2mn + nn) = (mm + nn)p,$$

atque hinc denique ambo nostri numeri quaesiti erunt

$$A = \frac{(mm+nn)^2(5mm-6mn+2nn)}{4m(m-2n)(mm+mn-nn)^2}$$

et

$$B = \frac{(mm+nn)^2(5mm-6mn+2nn)(2mm-2mn+nn)}{(3m-n)^2(m-n)^2mn(m-2n)(2m+n)}.$$

18. Ut autem etiam innotescat, quemadmodum huiusmodi valores inventi satisfaciant, ex binis numeris idoneis m et n prodeat formula radicalis

$$\sqrt{\frac{5mm-6mn+2nn}{2n(2m+n)}} = \frac{\mu}{\nu},$$

unde colligitur

$$\frac{M}{N} = \frac{(mm+nn)\mu}{\nu m(m-n)(m-2n)(3m-n)(mm+mn-nn)};$$

tum vero, quoniam supra [§ 12] litteras q et r permutavimus, quaternae formulae propositae sequenti modo ad quadrata reducentur:

I. $\sqrt{(AB+A+B)} = \frac{M}{N}(pr+qs) = \frac{\mu}{\nu}\cdot\frac{(mm+nn)^2}{m(m-2n)(mm+mn-nn)}$,

II. $\sqrt{(AB+A-B)} = \frac{M}{N}(pr-qs) = \frac{\mu}{\nu}\cdot\frac{(mm+nn)(m^4-8m^3n+6mmnn-n^4)}{m(m-n)(m-2n)(3m-n)(mm+mn-nn)}$,

III. $\sqrt{(AB-A+B)} = \frac{M}{N}(pq+rs) = \frac{\mu}{\nu}\cdot\frac{mm+nn}{m(m-2n)}$,

IV. $\sqrt{(AB-A-B)} = \frac{M}{N}(pq-rs) = \frac{\mu}{\nu}\cdot\frac{(mm+nn)^2}{m(m-n)(m-2n)(3m-n)}$.[1])

ALIAE TRANSFORMATIONES FORMULAE RESOLVENDAE

19. Quum tota quaestio huc sit perducta, ut ista formula (§ 13)

$$\frac{5mm-6mn+2nn}{2n(2m+n)} \quad \text{sive} \quad \frac{(2m-n)^2+(m-n)^2}{2n(2m+n)}$$

1) Editio princeps (atque etiam *Comment. arithm.*):

III. $\sqrt{(AB-A+B)} = \frac{M}{N}(pq+rs) = \frac{\mu}{\nu}\cdot\frac{(mm+nn)}{(m-n)(m-2n)}$

IV. $\sqrt{(AB-A-B)} = \frac{M}{N}(pq-rs) = \frac{\mu}{\nu}\cdot\frac{(mm+nn)}{m(3m-n)}$.

Correxit F. R.

ad quadratum revocetur, ponamus

$$2m - n = t \quad \text{et} \quad m - n = u,$$

ita ut sit

$$m = t - u \quad \text{et} \quad n = t - 2u$$

hincque $2m + n = 3t - 4u$ atque nunc quadratum esse debeat

$$\frac{tt + uu}{(2t - 4u)(3t - 4u)} = \square \quad \text{sive} \quad \frac{tt + uu}{(4u - 2t)(4u - 3t)} = \square,$$

circa quam formulam observo numeratorem cum denominatore alios factores communes habere non posse praeter 2 et 5. Hinc igitur sequitur numeratorem $tt + uu$ vel ipsum quadratum esse debere vel duplum vel quintuplum vel decuplum quadratum. Unde quatuor casus resultant, quos singulos sequenti modo evolvamus.

20. Denotent litterae a et b binos cathetos trianguli rectanguli numerici cuius hypotenusa sit $= c$, ita ut sit $aa + bb = cc$. Nunc igitur pro primo casu faciamus $tt + uu = cc$, quod fit sumendo

$$t = a \quad \text{et} \quad u = b,$$

atque hoc casu necesse est, ut fiat

$$(4b - 2a)(4b - 3a) = \square.$$

Pro secundo casu faciamus $tt + uu = 2cc$, quod fit sumendo

$$t = a - b \quad \text{et} \quad u = a + b,$$

atque nunc necesse est, ut sit

$$(a + 3b)(a + 7b) = \square.$$

Pro tertio casu faciamus $tt + uu = 5cc$, quod fit sumendo

$$t = a + 2b \quad \text{et} \quad u = 2a - b;$$

tum enim ob $4u - 2t = 6a - 8b$ et $4u - 3t = 5a - 10b$ formula ad quadratum reducenda erit $(6a - 8b)(a - 2b) = \square$, hoc est

$$(4b - 2a)(4b - 3a) = \square,$$

quae cum casu primo perfecte congruit.

Pro casu denique quarto faciamus $tt + uu = 10cc$, quod fit sumendo

$$t = 3a + b \quad \text{et} \quad u = a - 3b;$$

tum enim ob $4u - 2t = -14b - 2a$ et $4u - 3t = -5a - 15b$ formula ad quadratum reducenda erit

$$(3b + a)(7b + a) = \square,$$

prorsus uti in casu secundo.

Verum hic notandum est casum tertium et quartum adhuc alio modo expediri posse. Si enim pro tertio ponamus

$$t = a + 2b \quad \text{et} \quad u = b - 2a,$$

ob $4u - 2t = -10a$ et $4u - 3t = -2b - 11a$ formula ad quadratum reducenda erit

$$2a(11a + 2b) = \square.$$

Pro casu quarto autem si ponamus

$$t = 3a + b \quad \text{et} \quad u = 3b - a,$$

ob $4u - 2t = 10b - 10a$ et $4u - 3t = 9b - 13a$ formula ad quadratum reducenda est

$$(a - b)(13a - 9b) = \square.$$

Verum plerumque, quoties his duobus casibus satisfieri potest, toties numeri t et u communi factore 5 praediti reperiuntur ideoque ad novas solutiones non perducunt.

21. His igitur duobus casibus postremis relictis circa quatuor praecedentes omnino memoratu dignum est, quod primus et tertius, tum vero etiam secundus et quartus ad eandem formulam perduxerit. Quare pro primo et tertio si numeri a et b ita fuerint comparati, ut formula

$$(4b - 2a)(4b - 3a)$$

fiat quadratum, tum duplici modo inde idonei valores pro t et u obtinentur; priori enim modo habebimus $t = a$ et $u = b$, altero vero modo $t = a + 2b$ et $u = 2a - b$. Simili modo pro casibus secundo et quarto si fuerit formula

$$(3b + a)(7b + a)$$

quadratum, tum etiam duo casus oriuntur, alter $t = a - b$ et $u = a + b$, alter vero $t = 3a + b$ et $n = a - 3b$. Operae igitur pretium erit has geminas resolutiones accuratius exponere.

I. SI FUERIT $(4b - 2a)(4b - 3a) = \square$ EXISTENTE $aa + bb = cc$

22. Hinc igitur primo statim deducimus fractionem supra (§ 18) introductam

$$\frac{\mu}{\nu} = \sqrt{\frac{cc}{(4b - 2a)(4b - 3a)}};$$

deinde pro priori resolutione habebimus

$$t = a, \quad u = b,$$

$$m = a - b, \quad n = a - 2b,$$

$$p = aa - 2ab + 2bb, \quad q = aa - ab - bb,$$

$$s = aa - ab - bb, \quad r = (a - b)(3b - a),$$

$$\frac{p}{s} = \frac{aa - 2ab + 2bb}{aa - ab - bb}, \quad \frac{q}{r} = \frac{aa - ab - bb}{(a - b)(3b - a)},$$

$$mm + nn = 2aa - 6ab + 5bb;$$

pro altera vero solutione

$$t = a + 2b, \quad u = 2a - b,$$

$$m = 3b - a, \quad n = 4b - 3a,$$

$$p = 5(aa - 2ab + 2bb), \quad q = -5(aa - ab - bb),$$

$$s = -5(aa - ab - bb), \quad r = 5(a - b)(3b - a),$$

$$\frac{p}{s} = -\frac{aa - 2ab + 2bb}{aa - ab - bb}, \quad \frac{q}{r} = -\frac{aa - ab - bb}{(a - b)(3b - a)},$$

unde manifestum est has duas solutiones a se invicem non differre.

23. Speciales autem solutiones, quae ex hac formula primo intuitu derivantur, sunt sequentes:

a	b	m	n	$\frac{p}{s}$	$\frac{q}{r}$
0	1	-1	-2	$\frac{2}{1}$	$\frac{1}{3}$
4	3	1	-2	$\frac{2}{1}$	$\frac{1}{1}$
12	5	7	2	$\frac{74}{59}$	$\frac{59}{21}$

quarum binae priores scopo nostro non conveniunt, tertia vero idoneam praebet solutionem atque adeo ab illa, quam olim iam inveni, diversam; quum enim sit $pp + ss = 8957 = 53 \cdot 169$ et $qq + rr = 3922 = 53 \cdot 74$, erunt ambo quaesiti numeri

$$A = \frac{169 \cdot 53^2 \cdot 74}{4 \cdot 74 \cdot 59^2 \cdot 21} = \frac{169 \cdot 53^2}{4 \cdot 21 \cdot 59^2}, \quad B = \frac{169 \cdot 74 \cdot 53^2}{2 \cdot 16 \cdot 3 \cdot 5^2 \cdot 7 \cdot 19^2} = \frac{169 \cdot 37 \cdot 53^2}{16 \cdot 3 \cdot 5^2 \cdot 7 \cdot 19^2}.$$ [1])

24. Consideremus autem attentius hanc formulam $(4b - 2a)(4b - 3a) = \square$, et quia numeri a et b sunt catheti trianguli rectanguli atque evidens est pro a sumi debere parem, pro b vero imparem, statuamus

$$a = 2de \quad \text{et} \quad b = dd - ee,$$

ut sit hypotenusa $c = dd + ee$; tum vero erit $4b - 2a = 4(dd - de - ee)$ et $4b - 3a = 4dd - 6de - 4ee$; quorum productum quum quadratum esse debeat, necesse est, ut utriusque quadrans fiat quadratum, hoc est

$$\text{I.} \quad dd - de - ee = \square,$$

$$\text{II.} \quad dd - \tfrac{3}{2} de - ee = \square;$$

ubi quum numerorum d et e alter debeat esse par, alter impar, etiam posterior numeris integris constat. Quod autem ad priorem attinet, quum sit $dd - de - ee = \left(d - \frac{1}{2}e\right)^2 - 5\frac{e^2}{4}$, ponamus

$$d - \tfrac{1}{2}e = rr + 5ss \quad \text{et} \quad \tfrac{1}{2}e = 2rs;$$

tum enim fiet

$$dd - de - ee = (rr - 5ss)^2;$$

1) Vide p. 171. F. R.

at vero habebimus

$$e = 4rs \quad \text{et} \quad d = rr + 2rs + 5ss$$

hincque

$$dd - ee = r^4 + 4r^3s - 2rrss + 20rs^3 + 25s^4 \quad \text{et} \quad de = 4r^3s + 8rrss + 20rs^3,$$

unde altera conditio postulat

$$r^4 - 2r^3s - 14rrss - 10rs^3 + 25s^4 = \square .$$

25. Statuamus hic $\frac{r}{s} = z$, ut habeamus hanc formulam

$$z^4 - 2z^3 - 14zz - 10z + 25 = \square,$$

quae cum formula supra data (§ 15) comparata praebet

$$\alpha = \pm 1, \quad \beta = 1, \quad \gamma = -14, \quad \delta = 5, \quad \varepsilon = \pm 5,$$

unde pro z quatuor sequentes expressiones elicimus:

$$\text{I.} \quad z = \frac{2\alpha(\varepsilon - 5\alpha)}{2\alpha^3\varepsilon + 1 + 14} = \frac{2\alpha(\varepsilon - 5\alpha)}{2\alpha^3\varepsilon + 15} = \frac{2(\alpha\varepsilon - 5)}{2\alpha\varepsilon + 15},$$

hinc vel $z = 0$ vel $z = -4$;

$$\text{II.} \quad z = \frac{50\alpha\varepsilon + 375}{2(5\alpha\varepsilon - 25)} = \frac{10\alpha\varepsilon + 75}{2(\alpha\varepsilon - 5)}$$

hincque vel $z = \infty$ vel $z = -\frac{5}{4}$;

$$\text{III.} \quad z = \frac{(2\alpha\varepsilon - 14 - 1)(2\alpha\varepsilon + 14 + 1)}{4(10 + 14 + 1)} = -\frac{125}{100} = -\frac{5}{4};$$

$$\text{IV.} \quad z = \frac{100(1250 + 70 \cdot 25 + 5 \cdot 25)}{(50\alpha\varepsilon - 15 \cdot 25)(50\alpha\varepsilon + 15 \cdot 25)} = \frac{4 \cdot 25^2 \cdot 125}{25^2(2\alpha\varepsilon + 15)(2\alpha\varepsilon - 15)} = -4.$$

Ex valore $z = -4$ oriuntur valores $r = 4$, $s = -1$, $d = 13$, $e = -16$ hincque $a = -416$ et $b = -87$, unde oritur

$$\frac{p}{s} = \frac{23162}{25859}^{1)} \quad \text{et} \quad \frac{q}{r} = \frac{25859}{10199};$$

1) Editio princeps (atque etiam *Comment. arithm.*): $\frac{p}{s} = \frac{23362}{25859}$. Correxit F. R.

at ex valore $z = -\frac{5}{4}$ habemus $r = 5$, $s = -4$, $d = 65$, $e = -80$, qui per quinarium ad terminos minores reducti praebent ut ante $d = 13$ et $e = -16$, ubi notasse iuvabit ex his valoribus a et b praegrandes numeros pro p, q, r, s esse prodituros.

26. At circa binas illas formulas notasse iuvabit utramque etiam quadrato negativo aequari posse; verum tum solutio eadem exsurgit, nisi quod valores pro a et b fiant negativi. Ceterum hic notari convenit ultimae aequationi etiam valorem $z = -3$ satisfacere, etiamsi eum non per methodum consuetam detexerimus; inde autem fit $r = 3$ et $s = -1$ hincque porro $d = 2$ et $e = -3$, unde fit $a = -12$ et $b = -5$, quem casum iam supra [§ 23] evolvimus.

II. SI FUERIT $(3b + a)(7b + a) = \square$

27. Hic statim apparet sumi debere

$$a = dd - ee \quad \text{et} \quad b = 2de,$$

ut fiat $c = dd + ee$; tum ergo sequentes duae formulae quadrata esse debent

$$dd + 6de - ee = \square \quad \text{et} \quad dd + 14de - ee = \square.$$

Quum prior sit $= (d + 3e)^2 - 10ee$, si ponamus $\zeta\eta = 10$ ac statuamus $d + 3e = \zeta rr + \eta ss$ et $e = 2rs$, fiet illa formula

$$= (\zeta rr - \eta ss)^2;$$

tum autem erit $d = \zeta rr - 6rs + \eta ss$ et $e = 2rs$; hinc ergo pro altera formula, quae est $(d + 7e)^2 - 50ee$, erit $d + 7e = \zeta rr + 8rs + \eta ss$ ideoque haec formula abit in

$$\zeta\zeta r^4 + 16\zeta r^3 s - 116rrss + 16\eta rs^3 + \eta\eta s^4 = \square,$$

unde per methodum supra [§ 16] indicatam infinitae solutiones inveniri possunt; ubi notasse iuvabit esse vel $\zeta = 1$ et $\eta = 10$, vel $\zeta = 2$ et $\eta = 5$.

28. Quum autem idonei valores pro a et b fuerint inventi, duplici modo inde litterae t et u definiri poterunt. Priore modo fit

$$t = a - b \quad \text{et} \quad u = a + b,$$

hinc

$$m = t - u = -2b \quad \text{et} \quad n = -a - 3b$$

ideoque

$$p = mm + (m-n)^2 = aa + 2ab + 5bb,$$

$$q = s = mm + n(m-n) = -aa - 4ab + bb$$

et

$$r = m(m-2n) = -4b(a+2b),$$

ita ut sit

$$\frac{p}{s} = -\frac{aa+2ab+5bb}{aa+4ab-bb} \quad \text{et} \quad \frac{q}{r} = \frac{aa+4ab-bb}{4b(a+2b)}.$$

Posteriore vero modo fit

$$t = 3a + b \quad \text{et} \quad u = a - 3b,$$

unde

$$m = 2a + 4b \quad \text{et} \quad n = a + 7b,$$

hincque porro ob $m - n = a - 3b$ fit

$$p = 5(aa + 2ab + 5bb),$$

$$q = s = 5(aa + 4ab - bb) \quad \text{et} \quad r = -5 \cdot 4b(a+2b)$$

sicque patet hunc posteriorem casum ad priorem redire.

29. Simpliciores autem solutiones, quas facili negotio divinando elicere licet, sunt sequentes:

a	b	m	n	$\frac{p}{s}$	$\frac{q}{r}$
1	0	— 0	— 1	$\frac{1}{1}$	$\frac{1}{0}$
— 3	4	— 8	— 9	$\frac{13}{11}$	$\frac{11}{16}$
— 35	12	— 24	— 1	$\frac{1105}{599}$	$\frac{599}{528}$

Hic secundus casus praebet illam ipsam solutionem, quam iam olim dederam.

His autem duabus formulis pertractatis adiungamus insuper binas postremas supra (§ 20) inventas.

III. SI FUERIT $2a(11a + 2b) = \square$

30. Casus simpliciores, qui statim se offerunt, sunt:

a	b	m	n	$\frac{p}{s}$	$\frac{q}{r}$
0	1	1, 1	0, 0	$\frac{2}{1}$	$\frac{1}{1}$
4	3	15, 3	20, 4	$\frac{2}{1}$	$\frac{1}{3}$
16	-63	$-15, -3$	80, 16	$\frac{74}{59}$	$\frac{59}{21}$

ubi ex datis a et b fit

$$t = a + 2b \quad \text{et} \quad u = b - 2a$$

hincque ut ante

$$m = t - u = 3a + b \quad \text{et} \quad n = t - 2u = 5a.$$

Hae solutiones autem iam in superioribus [§ 23] continentur.

IV. SI FUERIT $(a - b)(13a - 9b) = \square$

31. Inventis idoneis valoribus pro a et b erit

$$t = 3a + b \quad \text{et} \quad u = 3b - a,$$

hinc

$$m = 4a - 2b = 2(2a - b) \quad \text{et} \quad n = 5(a - b)$$

atque ob $m - n = 3b - a$ atque $m - 2n = 2(4b - 3a)$ habebimus

$$\frac{p}{s} = \frac{17aa - 22ab + 13bb}{11aa + 4ab - 11bb} \quad \text{et} \quad \frac{q}{r} = \frac{11aa + 4ab - 11bb}{4(6aa - 11ab + 4bb)}.$$

Solutiones autem simpliciores hinc oriundae sunt:

a	b	m	n	$\frac{p}{s}$	$\frac{q}{r}$
0	1	-2	-5	$\frac{13}{11}$	$\frac{11}{16}$
4	3	10, 2	5, 1	$\frac{1}{1}$	$\frac{1}{0}$

ubi memoratu dignum evenit, quod statim primum tentamen, quo $a = 0$ et $b = 1$, praebeat solutionem iam dudum inventam.

32. Quodsi pro ulteriore huius formulae evolutione ponamus $a = 2de$ et $b = dd - ee$, fiet $a - b = ee + 2de - dd$; sive mutandis signis ut

$$(b - a)(9b - 13a) = \square,$$

erit

$$b - a = dd - 2de - ee \quad \text{et} \quad 9b - 13a = 9dd - 26de - 9ee.$$

Reddamus nunc priorem quadratum; quae quum sit $(d - e)^2 - 2ee$, statuamus $d - e = rr + 2ss$ et $e = 2rs$; tum enim fiet

$$dd - 2de - ee = (rr - 2ss)^2;$$

tum vero alter factor ob $dd - ee = r^4 + 4r^3s + 4rrss + 8rs^3 + 4s^4$ erit

$$9r^4 - 16r^3s - 68rrss - 32rs^3 + 36s^4,$$

ubi casus primo intuitu se offerentes sunt:

$$1.\ r = 1,\ s = 0; \quad 2.\ r = 0,\ s = 1; \quad 3.\ r = 1,\ s = -1;$$
$$4.\ r = 2,\ s = -1; \quad 5.\ r = 1,\ s = 2.$$

33. Pro horum casuum primo habemus $d = 1$ et $e = 0$; hinc $a = 0$ et $b = 1$, qui iam occurrit. Pro secundo habemus $d = 2$ et $e = 0$; hinc $a = 0$ et $b = 4$[1]), qui a praecedente non differt. At pro tertio habemus $d = 1$ et $e = -2$; hinc $a = -4$ et $b = -3$, qui supra iam est tractatus. Pro quarto habemus $d = 2$ et $e = -4$ sive $d = 1$ et $e = -2$, unde fit $a = -4$ et $b = -3$ ut praecedens. Pro quinto denique habemus $d = 13$ et $e = 4$; hinc $a = 104$ et $b = 153$, ex quibus numeri praegrandes pro quaesitis A et B resultant, quibus non immoramur.

34. Imprimis autem quoque notatu dignus est casus, quo invenimus $\frac{p}{s} = \frac{2}{1}$ et $\frac{q}{r} = \frac{1}{3}$ sive $\frac{q}{r} = \frac{3}{1}$, unde deducuntur numeri quaesiti

1) Editio princeps (atque etiam *Comment. arithm.*): $b = 1$. Cum autem sit $a = 0$, valores pro $\frac{p}{s}$ et $\frac{q}{r}$ inventi in his duobus casibus non differunt. F. R.

$$A = \frac{25}{12} \quad \text{et} \quad B = \frac{25}{12},$$

ita ut ambo numeri quaesiti hoc casu fiant aequales, quod quidem scopo problematis minus convenit. Si enim numeri aequales desiderentur, ob eorum differentiam evanescentem quaestio huc rediret, ut inveniatur numerus A, ita ut tam $AA + 2A$ quam $AA - 2A$ fiat quadratum, quod quidem est facillimum. Statuatur enim

$$AA = \frac{aa + bb}{nn} \quad \text{et} \quad 2A = \frac{2ab}{nn};$$

fiet utique

$$\sqrt{(AA + 2A)} = \frac{a + b}{nn} \quad \text{et} \quad \sqrt{(AA - 2A)} = \frac{a - b}{n};$$

verum nunc requiritur, ut $aa + bb$ sit quadratum, quem in finem ponamus $a = pp - qq$ et $b = 2pq$, ut fiat

$$A = \frac{pp + qq}{n};$$

est vero etiam

$$A = \frac{2pq(pp - qq)}{nn},$$

unde fit $n(pp + qq) = 2pq(pp - qq)$ et

$$n = \frac{2pq(pp - qq)}{pp + qq},$$

ita ut numerus quaesitus in genere sit

$$A = \frac{(pp + qq)^2}{2pq(pp - qq)}.$$

Tales ergo numeri sunt sequentes:

$$1.\ A = \frac{25}{12}, \quad 2.\ A = \frac{169}{60}, \quad 3.\ A = \frac{289}{120}, \quad 4.\ A = \frac{625}{168} \quad \text{etc.}$$

35. Pro solutionibus autem ad quaestionem propositam accommodatis duae in numeris non nimis magnis notatu dignae videntur, quarum prior est ea ipsa, quam iam dudum inveni, qua erat

$$A = \frac{13 \cdot 29^2}{8 \cdot 9^2} \quad \text{et} \quad B = \frac{5 \cdot 29^2}{32 \cdot 11^2} \quad \text{sive} \quad A = \frac{10933}{648} \quad \text{et} \quad B = \frac{4205}{3872},$$

unde

$$V(AB + A + B) = \frac{7 \cdot 29 \cdot 47}{16 \cdot 9 \cdot 11}\,^{1}),$$

$$V(AB + A - B) = \frac{29^2}{16 \cdot 3 \cdot 11},$$

$$V(AB - A + B) = \frac{29^2}{16 \cdot 9},$$

$$V(AB - A - B) = \frac{29}{48}.$$

Pro altera vero solutione orta ex valoribus $\frac{p}{s} = \frac{74}{59}$ et $\frac{q}{r} = \frac{59}{21}$ obtinemus

$$A = \frac{13^2 \cdot 53^2}{4 \cdot 21 \cdot 59^2} \quad \text{et} \quad B = \frac{13^2 \cdot 37 \cdot 53^2}{16 \cdot 3 \cdot 5^2 \cdot 7 \cdot 19^2},$$

unde

$$V(AB + A + B) = \frac{13 \cdot 53}{8 \cdot 3 \cdot 7},$$

$$V(AB + A - B) = \frac{13 \cdot 53^2}{8 \cdot 3 \cdot 5 \cdot 7 \cdot 19},$$

$$V(AB - A + B) = \frac{13 \cdot 53^2}{8 \cdot 3 \cdot 7 \cdot 59},$$

$$V(AB - A - B) = \frac{13 \cdot 41 \cdot 47 \cdot 53}{8 \cdot 3 \cdot 5 \cdot 7 \cdot 19 \cdot 59}.$$

---

1) Editio princeps (atque etiam *Comment. arithm.*): $V(AB + A + B) = \frac{7 \cdot 29 \cdot 37}{16 \cdot 9 \cdot 11}$.
Correxit F. R.

PROBLEMATIS CUIUSDAM DIOPHANTEI EVOLUTIO

Commentatio 427 indicis ENESTROEMIANI
Novi commentarii academiae scientiarum Petropolitanae 17 (1772), 1773, p. 24—63
Summarium ibidem p. 7—8

SUMMARIUM

Methodus DIOPHANTEA quanta Ill. EULERO et quam praeclara debeat incrementa, inter Geometras constat et sane, qui, quantum Analysis sublimior ex ea ipsa lucri sit adepta, perpenderit, eam minime esse repudiandam haud aegre fatebitur; adde, quod eiusmodi investigationes suis non careant deliciis animoque gravioribus studiis defesso haud ingratam recreationem afferant. Problema, quod Ill. Vir hic pertractat, difficillimum utique ita se habet:

Invenire quatuor numeros eius indolis, ut 1. *summa singulorum,* 2. *summa factorum ex binis,* 3. *summa factorum ex ternis et* 4. *productum omnium sint numeri quadrati.*

Vel, quod eodem redit:

Invenire aequationem biquadraticam huius formae

$$x^4 - Ax^3 + Bx^2 - Cx + D = 0,$$

quae omnes suas radices habeat rationales et cuius singuli coefficientes A, B, C, D *sint numeri quadrati.*

Huius vero problematis solutionem generalem frustra tentari Cel. Auctor statim observat, unde animum nonnisi ad solutiones particulares intendit, inter quas, quae numeros minimos est largita, ita se habet, ut quatuor isti numeri quaesiti sint

I. $21 \cdot 20$, II. $21 \cdot 25$, III. $21 \cdot 64$ et IV. $21 \cdot 80$;

ex qua solutione unica quamquam innumerae aliae possunt derivari, tamen, quia prima

fortuito quasi sese obtulit, methodum certam eiusmodi problemata resolvendi adhuc desiderari infitias ire non licet; multum tamen hic profecisse is videretur, cui naturam huius formae

$$ac(xx + yy) + (a + c)^2xy$$

ad quadratum reducendae penitus evolvere contingeret; quamobrem Cel. Auctor etiam hanc formulam calculis suis prosequitur.

His accedunt considerationes de aliis duobus problematibus DIOPHANTEIS, quae ita se habent:

I. *Invenire quotcumque numeros, quorum quilibet in summam reliquorum ductus producat numerum quadratum.*

II. *Invenire quotcumque numeros quadratos, ut summa omnium quolibet imminuta fiat numerus quadratus.*

1. Cum olim[1]) istud problema DIOPHANTEUM tractassem, quo quaerebantur tres numeri, quo 1. summa, 2. summa productorum ex binis et 3. productum omnium sint numeri quadrati, solutio tantis difficultatibus implicata videbatur, ut huius generis problemata adhuc difficiliora vix aggredi essem ausus. Multo autem difficilius esse problema, cuius enodationem hic suscipio, nemo dubitabit, qui eius solutionem tentare voluerit. Problema autem hoc ita se habet:

Invenire quatuor numeros eius indolis, ut 1. *summa singulorum*, 2. *summa factorum ex binis*, 3. *summa factorum ex ternis et* 4. *productum omnium sint numeri quadrati.*

Vel, quod eodem redit:

Invenire aequationem biquadraticam huius formae

$$x^4 - Ax^3 + Bx^2 - Cx + D = 0,$$

quae omnes suas radices habeat rationales et cuius insuper singuli coefficientes A, B, C, D sint numeri quadrati.

---

1) Vide Commentationem 270 (indicis ENESTROEMIANI): *Solutio problematis de investigatione trium numerorum, quorum tam summa, quam productum, nec non summa productorum ex binis, sint numeri quadrati*, Novi comment. acad. sc. Petrop. 8 (1760/1), 1763, p. 64; *LEONHARDI EULERI Opera omnia*, series I, vol. 2, p. 519; vide ibidem imprimis notas p. XXVIII et 520. Confer etiam Commentationes 523 et A 31 huius voluminis. F. R.

2. Non dubito fore plerosque, qui mirabuntur me in huiusmodi quaestionibus evolvendis, quas nunc quidem summi Geometrae aversari videntur, operam consumere; verum equidem fateri cogor me ex huiusmodi investigationibus tantundem fere voluptatis capere quam ex profundissimis Geometriae sublimioris speculationibus. Ac si plurimum studii et laboris impendi in quaestionibus gravioribus evolvendis, huiusmodi variatio argumenti quandam mihi haud ingratam recreationem afferre solet. Ceterum Analysis sublimior tantum debet Methodo DIOPHANTEAE, ut nefas videatur eam penitus repudiare.

3. Problema igitur propositum aggressurus primum observo solutionem eius generalem frustra tentari; postquam enim pluribus modis calculum instituissem ac semper in formulas nullo pacto extricabiles incidissem, agnovi vix quicquam praestari posse, nisi vires nostras in solutionem quandam particularem intendamus. Sequenti ergo modo quatuor numeros quaesitos constituo

$$Mab,\quad Mbc,\quad Mcd,\quad Mda,$$

ubi, etsi quinque litterae sunt inductae, tamen haec positio ista limitatione restringitur, ut productum primi in tertium aequale sit producto secundi in quartum; quae restrictio utique in se non est necessaria vixque dubitare licet, quin etiam eiusmodi quaterni numeri quaesito satisfaciant, in quibus haec conditio locum non habeat; verum equidem nullam adhuc viam detegere valui, qua huiusmodi solutiones elicere liceret.

4. Hac igitur numerorum quaesitorum forma constituta quatuor conditiones praescriptae sequentes aequationes suppeditant

I. $M(ab + bc + cd + da) =$ quadrato,

II. $M^2(abbc + bccd + cdda + daab + 2abcd) =$ quadrato,

III. $M^3(abbccd + abccdd + aabcdd + aabbcd) =$ quadrato,

IV. $M^4 aabbccdd =$ quadrato,

ubi postrema conditio iam sponte impletur; neque vero hinc concludere licet limitationem supra inductam esse necessariam, cum eadem conditio aeque obtineretur, si quis quatuor numerorum insuper per numerum quadratum quemcumque multiplicaretur, quo pacto solutio ab omni restrictione liberaretur; sed tum reliquae aequationes nullo modo resolvi possent.

5. Restrictio autem adhibita hoc commodi nobis largitur, ut tertia aequatio hanc formam induat

$$Mabcd(ab + bc + cd + da) = \text{quadrato},$$

unde, cum ob primam iam quadratum esse debeat haec forma

$$M(ab + bc + cd + da),$$

necesse est, ut hoc productum $abcd$ quadrato aequetur. Praeterea autem ut tam primae quam tertiae conditioni satisfiat, capi oportet

$$M = ab + bc + cd + da;$$

vel si haec summa factorem habeat quadratum, puta ff, sufficiet sumi

$$M = \frac{ab + bc + cd + da}{ff},$$

siquidem per se manifestum est solutionem semper ad numeros integros reduci posse.

6. Hinc iam ratio est perspicua, cur initio quatuor quaesitis numeris factorem communem M tribuerim; eo igitur rite definito, ut sit

$$M = ab + bc + cd + da \quad \text{vel} \quad M = \frac{ab + bc + cd + da}{ff},$$

duae tantum supersunt conditiones, quas impleri oportet; alteram scilicet modo elicui, qua esse debet

$$abcd = \text{quadrato},$$

alteram aequatio secunda suppeditat, quae postulat ob factorem M^2 iam quadratum, ut sit

$$abbc + bccd + acdd + aabd + 2abcd = \text{quadrato},$$

quae in hanc formam redigitur

$$(aa + cc)bd + ac(bb + dd) + 2abcd = \text{quadrato}$$

seu

$$bd(aa + cc) + (b + d)^2 ac = \text{quadrato}.$$

7. Tota ergo quaestio ad inventionem huiusmodi quatuor numerorum a, b, c, d est perducta, ut binis modo memoratis conditionibus satisfiat; ubi notari convenit inter binos numeros a et c similem rationem intercedere atque inter binos b et d atque totum negotium a sola ratione tam inter a et c quam inter b et d pendere. Quare ut pro quavis solutione minimos numeros obtineamus, tam numeros a et c quam b et d primos inter se statui oportet. Si enim communem haberent divisorem, eo sublato conditioni utrique aeque satisfieret.

8. Quia evolutio posterioris aequationis praecipuas difficultates involvit, ab ea inchoandum esse arbitror ac primo quidem observo, etiamsi ea duas rationes $a:c$ et $b:d$ contineat, neutram tamen arbitrio nostro relinqui; unde imprimis inquirendum est, cuiusmodi rationes pro alterutra accipi debeant, ut forma nostra quadratum reddi possit. Quod quo facilius perspiciatur, consideremus casum, quo loco alterius rationis ratio dupla poneretur; sit ergo $b:d = 2:1$ et haec forma

$$2aa + 2cc + 9ac$$

quadratum reddi deberet, quod autem numquam fieri posse facile intelligitur. Posito enim $a = p + q$ et $c = p - q$ prodit haec forma $13pp - 5qq$, quae nullo modo umquam quadratum exhibere potest; idem evenit, si poneretur $b:d = 3:1$; unde patet nonnisi certas rationum species pro alterutra rationum $a:c$ et $b:d$ assumi posse, reliquas vero omnes ab hac investigatione excludi.

9. Statim autem patet inter rationes huic scopo accommodatas primum locum obtinere rationes quadraticas; sit igitur $b:d = pp:qq$ et formula nostra

$$ppqq(aa + cc) + ac(pp + qq)^2$$

aequetur huic quadrato

$$ppqqaa + \frac{2m}{n}pqac + \frac{mm}{nn}cc,$$

unde fit

$$nn(pp + qq)^2a + nnppqqc = 2mnpqa + mmc$$

ideoque

$$\frac{a}{c} = \frac{mm - nnppqq}{nn(pp+qq)^2 - 2mnpq}.$$

vel sit $m = \pm kpq$, ut habeamus has formulas satisfacientes

$$\frac{b}{d} = \frac{pp}{qq} \quad \text{et} \quad \frac{a}{c} = \frac{(kk-nn)ppqq}{nn(pp+qq)^2 \pm 2knppqq}$$

existente $k > n$.

10. Evolvamus casus simpliciores numerorum k et n et habebimus aequationis nostrae sequentes resolutiones: Si fuerit $\frac{b}{d} = \frac{pp}{qq}$, erit

I. $\frac{a}{c} = \frac{3ppqq}{(pp+qq)^2 \pm 4ppqq}$, II. $\frac{a}{c} = \frac{8ppqq}{(pp+qq)^2 \pm 6ppqq}$,

III. $\frac{a}{c} = \frac{5ppqq}{4(pp+qq)^2 \pm 12ppqq}$, IV. $\frac{a}{c} = \frac{15ppqq}{(pp+qq)^2 \pm 8ppqq}$,

V. $\frac{a}{c} = \frac{7ppqq}{9(pp+qq)^2 \pm 24ppqq}$, VI. $\frac{a}{c} = \frac{24ppqq}{(pp+qq)^2 \pm 10ppqq}$,

VII. $\frac{a}{c} = \frac{21ppqq}{4(pp+qq)^2 \pm 20ppqq}$, VIII. $\frac{a}{c} = \frac{16ppqq}{9(pp+qq)^2 \pm 30ppqq}$,

IX. $\frac{a}{c} = \frac{9ppqq}{16(pp+qq)^2 \pm 40ppqq}$ etc.

11. Si iam pro litteris k, n, p, q eiusmodi valores inveniri possent, ut productum ac seu haec expressio

$$n(kk-nn)(n(pp+qq)^2 \pm 2kppqq)$$

fieret numerus quadratus, haberetur solutio problematis propositi, siquidem tum ob $bd = ppqq$ etiam formula $abcd$ foret quadratum. Verum haec investigatio nimis est molesta, quam ut eam suscipi conveniat; ac si forte succederet, ad maximos numeros certe perduceret. Quare consultum erit etiam alias rationes pro $\frac{b}{d}$ contemplari, quae quidem alteri conditioni, scilicet

$$bd(aa+cc) + ac(b+d)^2 = \text{quadrato},$$

convenire queant. At ob similem rationem fractionum $\frac{b}{d}$ et $\frac{a}{c}$ omnes valores hic pro $\frac{a}{c}$ eruti etiam vicissim pro $\frac{b}{d}$ assumi poterunt, unde denuo novae huius generis fractiones elicientur.

12. In genere quidem hic labor nimis foret taediosus, unde casus primo simpliciores evolvam:

Si $\frac{b}{d} = \frac{1}{1}$, erit $\frac{a}{c} = \frac{3}{8}, -\frac{4}{1}, \frac{4}{5}, \frac{5}{28}, -\frac{15}{4}, \frac{7}{12}, \frac{7}{60}, \frac{8}{33}$;

si $\frac{b}{d} = \frac{4}{1}$, erit $\frac{a}{c} = \frac{4}{3}, \frac{12}{41}, \frac{32}{1}, \frac{32}{49}, \frac{5}{13}, \frac{5}{37}, -\frac{60}{7}, \frac{20}{19}$;

si $\frac{b}{d} = \frac{9}{1}$, erit $\frac{a}{c} = \frac{27}{64}, \frac{27}{136}, \frac{36}{23}, \frac{36}{77}, \frac{45}{292}, \frac{108}{5}$;

si $\frac{b}{d} = \frac{9}{4}$, erit $\frac{a}{c} = \frac{108}{25}, \frac{45}{61}, \frac{28}{73}, \frac{64}{49}, \frac{64}{289}$.

En ergo hic praeter expectationem duos casus, quibus pro a et c numeri quadrati prodierunt, unde, cum etiam b et d sint numeri quadrati, duas iam sumus adepti problematis nostri solutiones.

13. En ergo duas problematis nostri solutiones. Quarum prima ob $a = 64$, $b = 9$, $c = 49$ et $d = 4$ praebet

$$M = 576 + 441 + 196 + 256 = 1469$$

sicque quatuor numeri quaesiti sunt

I. $1469 \cdot 196$, II. $1469 \cdot 256$, III. $1469 \cdot 441$, IV. $1469 \cdot 576$.

Altera ob $a = 64$, $b = 9$, $c = 289$, $d = 4$ dat

$$M = 576 + 2601 + 1156 + 256 = 4589,$$

unde alii quatuor numeri problemati satisfacientes sunt

I. $4589 \cdot 256$, II. $4589 \cdot 576$, III. $4589 \cdot 1156$, IV. $4589 \cdot 2601$.

Has autem solutiones haud facile ex formula § 11 data derivare licuisset, etiamsi in ea contineantur.

14. Cum autem singulae fractiones pro $\frac{a}{c}$ inventae etiam pro $\frac{b}{d}$ usurpari queant, evolvamus simpliciores, quae sunt

$$\frac{4}{3}, \frac{5}{4}, \frac{8}{3}, \frac{12}{7}, \frac{13}{5}, \frac{20}{19}, \frac{28}{5}, \frac{32}{1}, \frac{33}{8} \text{ etc.}$$

Sit igitur primo $\frac{b}{d} = \frac{4}{3}$ et habebitur

$$12aa + 12cc + 49ac = \text{quadrato},$$

cui satisfacit $\frac{a}{c} = 4$; ponatur ergo $\frac{a}{c} = 4 + x$:

$$\begin{array}{l} 192 + 96x + 12xx \\ 12 \\ 196 + 49x \\ \hline 400 + 145x + 12xx = \square = (20 + xy)^2, \end{array}$$

ergo

$$145 + 12x = 40y + xyy \quad \text{et} \quad x = \frac{145 - 40y}{yy - 12}$$

hincque

$$\frac{a}{c} = \frac{4yy - 40y + 97}{yy - 12}$$

seu posito $y = \frac{m}{n}$

$$\frac{a}{c} = \frac{4mm - 40mn + 97nn}{mm - 12nn},$$

unde sequentes novae fractiones idoneae simpliciores colliguntur

$$\frac{a}{c} = \frac{24}{1}, \frac{37}{13}, \frac{121}{24}.$$

15. Statuatur simili modo $\frac{b}{d} = \frac{5}{4}$ fietque

$$20aa + 20cc + 81ac = \square,$$

cui satisfacit $\frac{a}{c} = 1$; sit ergo $\frac{a}{c} = 1 + x$:

$$\begin{array}{l} 20 + 40x + 20xx \\ 20 \\ 81 + 81x \\ \hline 121 + 121x + 20xx = \square = (11 + xy)^2, \end{array}$$

ergo

$$121 + 20x = 22y + xyy \quad \text{et} \quad x = \frac{121 - 22y}{yy - 20}$$

et

$$\frac{a}{c} = \frac{yy - 22y + 101}{yy - 20} = \frac{mm \pm 22mn + 101nn}{mm - 20nn},$$

unde elicitur $\frac{a}{c} = \frac{16}{5}$, ita ut sit $abcd$ quadratum.

16. Haec solutio nobis largitur quatuor numeros multo minores problemati satisfacientes. Cum enim habeamus

$$a = 16, \quad b = 5, \quad c = 5, \quad d = 4,$$

erit factor communis

$$M = \frac{80 + 25 + 20 + 64}{ff} = \frac{189}{ff},$$

unde sumto $f = 3$ erit $M = 21$ et quatuor numeri problema solventes erunt

I. $21 \cdot 20$, II. $21 \cdot 25$, III. $21 \cdot 64$ et IV. $21 \cdot 80$,

quorum summa singulorum est $= 9 \cdot 21^2$,

summa productorum ex binis $= 110^2 \cdot 21^2$,

summa productorum ex ternis[1]) $= 120^2 \cdot 21^4$,

productum omnium $= 1600^2 \cdot 21^4$,

ita ut huius aequationis biquadraticae

$$x^4 - 9 \cdot 21^2 \cdot x^3 + 110^2 \cdot 21^2 \cdot xx - 120^2 \cdot 21^4 \cdot x + 1600^2 \cdot 21^4 = 0$$

radices sint

$$21 \cdot 20, \quad 21 \cdot 25, \quad 21 \cdot 64, \quad 21 \cdot 80.$$

---

1) Editio princeps (atque etiam *Comment. arithm.*):

$$\text{summa productorum ex ternis} = 4800^2 \cdot 21^4.$$

Qui error iam correctus est a T. L. HEATH in libro, qui inscribitur *DIOPHANTUS of Alexandria. A study in the history of greek algebra.* Second edition. With a supplement containing an account of FERMATS theorems and problems connected with DIOPHANTINE analysis and some solutions of DIOPHANTINE problems by EULER. Cambridge 1910, p. 357. F. R.

17. Ex cognita autem una solutione certa methodo aliae, immo infinitae elici possunt; quod quo facilius ostendam, hac postrema solutione utar, qua posito $\frac{b}{d} = \frac{5}{4}$ invenimus in genere $\frac{a}{c} = \frac{yy - 22y + 101}{yy - 20}$; unde ut $abcd$ fiat quadratum, reddi oportet hanc formam

$$5(yy - 20)(yy - 22y + 101) = \text{quadrato},$$

id quod evenit sumto $y = 5$. Statuatur ergo $y = z + 5$ et habebitur

$$5(zz + 10z + 5)(zz - 12z + 16) = \square$$

seu

$$400 + 500z - 495zz - 10z^3 + 5z^4 = \square,$$

cui etiam satisfacit $z = 1$ et $y = 6$, unde autem eadem solutio resultat.

18. Ut aliam solutionem eliciamus, fingamus radicem quadratam huius formae $20 + \frac{25}{2}z - \frac{521}{32}zz$, cuius quadratum

$$400 + 500z - 495zz - \frac{25 \cdot 521}{32}z^3 + \frac{521^2}{32^2}z^4$$

illi formae aequatum praebet

$$\left(\frac{521^2}{32^2} - 5\right)z = \frac{25 \cdot 521}{32} - 10$$

seu

$$z = \frac{32 \cdot 12705}{266321} = \frac{32 \cdot 1155}{24211} = \frac{32 \cdot 105}{2201} \quad \text{ideoque} \quad z = \frac{3360}{2201} \quad \text{et} \quad y = \frac{14365}{2201},$$

unde pro a et c numeri enormes resultant, quos evolvere operae non est pretium.

19. Ut autem plures solutiones derivare liceat, ob casum cognitum $z = 1$ ponamus $z = \frac{1}{1+v}$ et prodibit haec forma ad quadratum redigenda

$$\begin{array}{r} 400 + 1600v + 2400vv + 1600v^3 + 400v^4 \\ + 500 + 1500v + 1500vv + 500v^3 \\ - 495 - 990v - 495vv \\ - 10 - 10v \\ + 5 \\ \hline \text{seu } 400 + 2100v + 3405vv + 2100v^3 + 400v^4 = \square, \end{array}$$

cuius radix posita $= 20 + \frac{105}{2}v - 20vv$ dat

$$4205 - \frac{105^2}{4} + 4200v = 0$$

seu

$$v = -\frac{1159}{3360} \quad \text{et} \quad 1 + v = \frac{2201}{3360}$$

ut ante. Ob formam reciprocam erit etiam

$$v = -\frac{3360}{1159} \quad \text{et} \quad 1 + v = -\frac{2201}{1159} \quad \text{et} \quad z = -\frac{1159}{2201} \quad \text{hincque} \quad y = \frac{9846}{2201},$$

unde autem non alia solutio obtinetur.

20. Quamquam autem hoc modo ex qualibet solutione aliae innumerae deduci possunt, tamen, quia in primas casu quasi fortuito incidimus, methodus adhuc certa desideratur, quae ad huius problematis solutionem perducat; cuius inventio in Analysi DIOPHANTEA utique maximi foret momenti. Verum antequam talem methodum expectare liceat, necesse videtur, ut natura huius formae

$$ac(xx + yy) + (a + c)^2xy$$

ad quadratum reducendae accuratius investigetur et rationes pro $a:c$ assumendae, quibus resolutio succedit, explorentur, unde hanc quaestionem perscrutandam propono:

Invenire omnes valores idoneos pro ratione $a:c$ substituendos, ut haec expressio

$$ac(xx + yy) + xy(aa + cc) + 2acxy$$

quadrato aequalis reddi possit.

21. Ex superioribus iam satis liquet rationem $a:c$ neutiquam pro lubitu accipi posse, sed eam certis conditionibus esse adstrictam, quas potissimum determinari oportet. Ad has conditiones explorandas statuamus

$$ac(xx + yy) + xy(aa + cc) + 2acxy = zz,$$

quam aequationem in sequentes formas transfundere licet:

I. $(aa + cc)(xx + yy) = (a + c)^2(x + y)^2 - 2zz,$

II. $(aa + 4ac + cc)(xx + 4xy + yy) = 6zz + (a - c)^2(x - y)^2,$

III. $(aa + cc)(xx + 4xy + yy) = 2zz + (a - c)^2(x + y)^2,$

IV. $(aa + 4ac + cc)(xx + yy) = 2zz + (a + c)^2(x - y)^2.$

22. Cum iam ex prima forma intelligamus formulam $aa + cc$ factorem esse numeri huius formae $tt - 2zz$, qui, uti constat[1]), alios non admittit divisores, nisi qui ipsi sint vel huius formae $AA - 2BB$ vel huius $2AA - BB$, sequitur numerum $aa + cc$ in alterutra harum formarum contineri debere. Ex tertia autem forma intelligitur eundem numerum $aa + cc$, cum sit divisor formae $2zz + tt$, etiam in forma $2AA + BB$ contineri debere. Iam vero numeri formae $2AA - BB$ vel $AA - 2BB$ praeter binarium alios non habent divisores primos, nisi qui in forma $8n \pm 1$ contineantur, et numeri formae $2AA + BB$ alios non habent divisores primos praeter binarium, nisi qui vel in hac forma $8n + 1$ vel $8n + 3$ contineantur. Ex quo concluditur haec conditio, ut numerus $aa + cc$ alios praeter binarium non habeat divisores primos, nisi qui sint formae $8n + 1$.

23. Simili modo cum altera formula $aa + 4ac + cc$ sit divisor formae $6zz + tt$, quae alios divisores praeter 2 et 3 non admittit primos, nisi qui in aliqua harum formularum

$$24n + 1, \quad 24n + 5, \quad 24n + 7, \quad 24n + 11$$

contineantur, tum vero, quia eadem formula $aa + 4ac + cc$ etiam est divisor formae $2zz + tt$, ea praeter 2 alios non admittit divisores primos, nisi qui in alterutra harum formarum $8n + 1$ vel $8n + 3$ contineantur; ex quibus coniunctis sequitur numerum $aa + 4ac + cc$ praeter 2 et 3 alios divisores primos habere non posse, nisi qui contineantur vel in hac formula $24n + 1$ vel hac $24n + 11$.

---

1) Vide ad hoc et ad sequentia Commentationes 164 et 256 (indicis ENESTROEMIANI): *Theoremata circa divisores numerorum in hac forma* $paa \pm qbb$ *contentorum*, Comment. acad. sc. Petrop. 14 (1744/6), 1751, p. 151, et *Specimen de usu observationum in mathesi pura*, Novi comment. acad. sc. Petrop. 6 (1756/7), 1761, p. 185; *LEONHARDI EULERI Opera omnia*, series I, vol. 2, p. 194 et 459. F. R.

24. Hinc e valoribus rationis $a:c$ primum omnes ii excluduntur, quibus numerus $aa+cc$ haberet divisorem primum formae $8n+5$, siquidem reliquae formae ineptae $8n+3$ et $8n+7$ sponte excluduntur, propterea quod summa duorum quadratorum $aa+cc$ per tales numeros numquam divisibilis existit.[1]) Deinde etiam ii valores rationis $a:c$ excluduntur, quibus numerus $aa+4ac+cc$, qui per se praeter 2 et 3 alios habere nequit divisores, nisi qui sint huius formae $12n+1$ vel huius formae $12n+11$, haberet divisorem vel huius formae $24n+13$ vel huius $24n+23$. Quocirca ex rationibus pro $a:c$ adhibendis primo expungi debent omnes eae, quibus numerus $aa+cc$ dividi potest per numerum primum formae $8n+5$, deinde etiam eae, quibus numerus $aa+4ac+cc$ admitteret divisorem formae $24n+13$ vel $24n+23$.

25. Quando autem ratio $a:c$ ita est comparata, ut numerus $aa+cc$ nullum habeat divisorem formae $8n+5$, tum vicissim certum est eundem numerum tam in hac forma $2AA-BB$ quam hac $2AA+BB$ contineri. Ac si quoque numerus $aa+4ac+cc$ nullum habet divisorem formae $24n+13$ vel $24n+23$, tum perinde certum est eundem numerum tam in hac forma $2AA+BB$ quam ista $6AA+BB$ contineri. Hac duplici regula observata facili negotio omnes rationes, quas loco $a:c$ assumi non licet, excluduntur.

26. Facta autem hac exclusione pro fractione $\frac{a}{c}$ sequentes valores sunt relicti

$$\frac{1}{1},\ \frac{4}{1},\ \frac{4}{3},\ \frac{5}{4},\ \frac{8}{3},\ \frac{8}{7},\ \frac{9}{1},\ \frac{9}{4},\ \frac{11}{4},\ \frac{12}{5},\ \frac{12}{7},\ \frac{13}{5},\ \frac{13}{12},\ \frac{15}{7},\ \frac{15}{8},\ \frac{16}{1},\ \frac{16}{5},\ \frac{16}{9},\ \frac{16}{13},$$

$$\frac{17}{12},\ \frac{19}{8},\ \frac{19}{11},\ \frac{20}{1},\ \frac{20}{3},\ \frac{20}{7},\ \frac{20}{11},\ \frac{20}{13},\ \frac{20}{19},\ \frac{21}{5},\ \frac{21}{20},\ \frac{23}{8},\ \frac{24}{1},\ \frac{24}{5},\ \frac{24}{7},\ \frac{24}{11},\ \frac{24}{19},\ \frac{25}{1},\ \frac{25}{4},$$

$$\frac{25}{9},\ \frac{25}{12},\ \frac{25}{16},\ \frac{25}{17},\ \frac{27}{11},\ \frac{27}{20},\ \frac{28}{5},\ \frac{28}{13},\ \frac{28}{15},\ \frac{28}{25},\ \frac{29}{3},$$

ubi observari convenit reliquas rationes omnes frustra adhibitum iri; num autem hae omnes post exclusiones expositas relictae succedant, quaestio est maximi momenti, quae vix decidi posse videtur.

---

1) Vide Commentationem 134 (indicis Enestroemiani): *Theoremata circa divisores numerorum*, Novi comment. acad sc. Petrop. 1 (1747/8), 1750, p. 20, imprimis § 16—20; *Leonhardi Euleri Opera omnia*, series I, vol. 2, p. 62. F. R.

27. Hic prima ratio in praecedentibus nondum inventa est $\frac{8}{7}$; quae igitur an solutionem quaestionis admittat, videamus. Fieri nempe oportet

$$56(xx + yy) + 225xy = \square.$$

Ponatur $x = p + q$ et $y = p - q$, ut prodeat haec forma

$$337pp - 113qq = \square;$$

quod an fieri possit, facilius exploratur quam ex forma praecedente; satisfaciunt autem hi valores minimi $p = 3$ et $q = 4$, unde colligitur $x = 7$ et $y = -1$ seu $\frac{x}{y} = -7$; statuatur ergo $\frac{x}{y} = \frac{-7+v}{1}$ et prodit

$$1225 - 559v + 56vv = \square,$$

unde colligitur[1])

$$v = \frac{70t - 559}{tt - 56}$$

et

$$\frac{x}{y} = \frac{-7tt + 70t - 167}{tt - 56}$$

seu

$$\frac{x}{y} = \frac{7tt \pm 70t + 167}{56 - tt} = \frac{7mm - 14mn - nn}{20nn + 12mn - mm}.$$

28. Cum deinde etiam alios plures casus examinassem, inveni negotium semper succedere; ex quo asseverare vix dubito omnes istas fractiones post binas exclusiones ante memoratas relictas semper ita esse comparatas, ut loco rationis $a : c$ positae aequationem

$$ac(xx + yy) + (a + c)^2xy = \square$$

resolubilem reddant. Nunc igitur omnino operae foret pretium in indolem harum fractionum accuratius inquirere earumque verum characterem indagare, quo eae ab omnibus reliquis fractionibus distinguuntur. Primo quidem patet in iis omnes fractiones huius formae $\frac{pp}{qq}$ occurrere; quomodo autem reliquarum indoles sit comparata, altioris videtur indaginis.

1) Vide L. Euler, *Vollständige Anleitung zur Algebra*, St. Petersburg 1770, Zweyter Theil, zweyter Abschnitt, Cap. 4; *Leonhardi Euleri Opera omnia*, series I, vol. 1, p. 349, imprimis p. 353. F. R.

29. Videamus autem, quomodo in genere numeri a et c comparati esse debeant, ut $aa + cc$ obtineat formam $AA - 2BB$. Posito autem

$$aa + cc = AA - 2BB$$

erit

$$AA - aa = cc + 2BB$$

ideoque tam $A + a$ quam $A - a$, utpote divisores formae $cc + 2BB$, eiusdem formae numeri esse debent; unde posito

$$A + a = pp + 2qq$$

et

$$A - a = rr + 2ss$$

fit

$$A = \frac{pp + 2qq + rr + 2ss}{2} \quad \text{et} \quad a = \frac{pp + 2qq - rr - 2ss}{2}$$

et ob

$$cc + 2BB = (pp + 2qq)(rr + 2ss)$$

erit

$$c = 2qs + pr \quad \text{et} \quad B = ps - qr.$$

Quocirca conditio praescripta impletur sumendo

$$a = pp - rr + 2qq - 2ss \quad \text{et} \quad c = 2pr + 4qs,$$

unde fit

$$aa + cc = (pp + rr)^2 + 4(qq + ss)^2 + 4(pp - rr)(qq - ss) + 16pqrs,$$

quae forma non solum est

$$= (pp + rr + 2qq + 2ss)^2 - 2(2ps - 2qr)^2,$$

sed etiam

$$= (pp + rr - 2qq - 2ss)^2 + 2(2pq + 2rs)^2.$$

Unde tam in hac forma $AA - 2BB$ quam ista $AA + 2BB$ continetur.

30. Evolvamus simili modo alteram conditionem, quae postulat

$$aa + 4ac + cc = AA + 2BB,$$

et cum fiat

$$(a + 2c)^2 - 3cc = AA + 2BB \quad \text{seu} \quad (a + 2c)^2 - AA = 2BB + 3cc,$$

debet esse

$$a + 2c + A = 2tt + 3uu \quad \text{et} \quad a + 2c - A = xx + 6yy,$$

ergo

$$a + 2c = \frac{2tt + 3uu + xx + 6yy}{2};$$

tum vero ob

$$2BB + 3cc = (2tt + 3uu)(xx + 6yy)$$

fit

$$B = tx - 3uy \quad \text{et} \quad c = ux + 2ty$$

ideoque

$$a = 2tt - 8ty + 6yy + 3uu - 4ux + xx$$

seu

$$a = 2(t - y)(t - 3y) + (u - x)(3u - x) \quad \text{et} \quad c = 2ux + 4ty.$$

Vel sit

$$t = y + v \quad \text{et} \quad x = u - z,$$

ut fiat

$$a = 2v(y - 2v) + z(z + 2u),$$

$$c = 4y(y + v) + 2u(u - z);$$

hocque modo simul alteri conditioni, qua esse debet

$$aa + 4ac + cc = 6AA + BB,$$

satisfit.

31. Quo igitur utrique conditioni satisfiat, necesse est, ut ambo numeri a et c simul in sequentibus binis formulis contineantur

$$a = (p - r)(p + r) + 2(q - s)(q + s), \qquad c = 2pr + 4qs,$$

$$a = (u - x)(3u - x) + 2(t - y)(t - 3y), \quad c = 2ux + 4ty.$$

Nova ergo hinc nascitur quaestio, quomodo hae binae geminae formulae ad eundem valorem sint reducendae; ad quod necesse est, ut huic aequalitati satisfiat

$$(ux + 2ty)(pp - rr + 2qq - 2ss) = (pr + 2qs)(3uu - 4ux + xx + 2tt - 8ty + 6yy),$$

quoniam totum negotium in ratione $a : c$ versatur.

ALIUD PROBLEMA DIOPHANTEUM

Invenire quotcumque numeros, quorum quilibet in summam reliquorum multiplicatus producat numerum quadratum.

32. Sint numeri quaesiti p, q, r, s etc. eorumque summa $= S$; requiritur ergo, ut omnes hae formulae

$$p(S-p), \quad q(S-q), \quad r(S-r), \quad s(S-s) \quad \text{etc.}$$

sint quadrata; quae cum sint similes, sufficit pro una posuisse $p(S-p) = ffpp$, unde fit $p = \frac{S}{1+ff}$. Quare numeri quaesiti erunt

$$\frac{S}{1+ff}, \quad \frac{S}{1+gg}, \quad \frac{S}{1+hh}, \quad \frac{S}{1+kk} \quad \text{etc.},$$

dummodo eorum summa fiat $= S$; sicque problema huc redit, ut quaerantur numeri quotcumque f, g, h, k etc. ita comparati, ut fiat

$$\frac{1}{1+ff} + \frac{1}{1+gg} + \frac{1}{1+hh} + \frac{1}{1+kk} + \text{etc.} = 1.$$

33. Statuamus, quoniam hi numeri plerumque sunt fracti,

$$f = \frac{a}{\alpha}, \quad g = \frac{b}{\beta}, \quad h = \frac{c}{\gamma}, \quad k = \frac{d}{\delta} \quad \text{etc.}$$

et quaestio huc redit, ut aliquot fractiones huiusmodi

$$\frac{\alpha\alpha}{aa+\alpha\alpha}, \quad \frac{\beta\beta}{bb+\beta\beta}, \quad \frac{\gamma\gamma}{cc+\gamma\gamma} \quad \text{etc.}$$

inveniantur, quorum summa unitati aequetur; ubi observo quemlibet denominatorem esse summam duorum quadratorum. Quodsi ergo talis denominator sit numerus primus, ex eo duae tantum eiusmodi nascuntur fractiones, scilicet

$$\frac{\alpha\alpha}{aa+\alpha\alpha} \quad \text{et} \quad \frac{aa}{aa+\alpha\alpha};$$

quarum summa cum unitati aequetur, evidens est ambas simul capi non

posse, nisi quaestio de duobus numeris instituatur, quorum alter in alterum ductus praebeat quadratum. Tum enim ob

$$\frac{aa}{aa+\alpha\alpha}+\frac{\alpha\alpha}{aa+\alpha\alpha}=1$$

sumto S pro lubitu numeri satisfacientes erunt Maa et $M\alpha\alpha$, qui propterea casus nullam habet difficultatem.

34. Quando autem plures duobus numeri sunt investigandi, qui problemati conveniant, necesse est, ut etiam casus, quibus denominatores sunt numeri compositi[1]), evolvantur, siquidem inde plures fractiones huius indolis formari possunt; quarum cum binae itidem unitati aequentur, sequente modo eas repraesentabo:

Denominator $D=(aa+\alpha\alpha)(bb+\beta\beta)$

$$\frac{(ab-\alpha\beta)^2}{D} \quad \frac{(a\beta+\alpha b)^2}{D}$$
$$\frac{(a\beta-\alpha b)^2}{D} \quad \frac{(ab+\alpha\beta)^2}{D}$$

Denominator $D=(aa+\alpha\alpha)(bb+\beta\beta)(cc+\gamma\gamma)$

$$\frac{(a\beta c+\alpha bc-ab\gamma+\alpha\beta\gamma)^2}{D} \quad \frac{(a\beta\gamma+\alpha b\gamma+abc-\alpha\beta c)^2}{D}$$
$$\frac{(a\beta\gamma+\alpha b\gamma-abc+\alpha\beta c)^2}{D} \quad \frac{(a\beta c+\alpha bc+ab\gamma-\alpha\beta\gamma)^2}{D}$$
$$\frac{(abc+\alpha\beta c-\alpha\beta\gamma+\alpha b\gamma)^2}{D} \quad \frac{(ab\gamma+\alpha\beta\gamma+a\beta c-\alpha bc)^2}{D}$$
$$\frac{(ab\gamma+\alpha\beta\gamma-a\beta c+\alpha bc)^2}{D} \quad \frac{(abc+\alpha\beta c+a\beta\gamma-\alpha b\gamma)^2}{D}.$$

1) Ad sequentes denominatorum decompositiones vide Commentationem 228 (indicis Enestroemiani): *De numeris, qui sunt aggregata duorum quadratorum*, Novi comment. acad. sc. Petrop. 4 (1752/3), 1758, p. 3, imprimis § 5; *Leonhardi Euleri Opera omnia*, series I, vol. 2, p. 295. F. R.

35. Circa ordinem secundum annotasse iuvabit esse

$$\frac{(ab-\alpha\beta)^2}{D}+\frac{(a\beta-\alpha b)^2}{D}=1-\frac{4ab\alpha\beta}{D}$$

et

$$\frac{(ab-\alpha\beta)^2}{D}+\frac{(ab+\alpha\beta)^2}{D}=1+\frac{aabb+\alpha\alpha\beta\beta-aa\beta\beta-\alpha\alpha bb}{D}.$$

Deinde in ordine tertio si quatuor partes prioris columnae invicem addantur, summa erit

$$2-\frac{8(aa-\alpha\alpha)b\beta c\gamma}{(aa+\alpha\alpha)(bb+\beta\beta)(cc+\gamma\gamma)}.$$

Hinc non contemnenda subsidia peti poterunt pro quavis numerorum quaesitorum multitudine, dum, si solutio in genere tentaretur, insignes difficultates occurrerent. Quoniam igitur casus duorum numerorum per se est perspicuus, a casu trium exordiar inde ad quatuor progressurus.

CASUS TRIUM NUMERORUM

36. Ponamus pro tribus numeris quaesitis has fractiones

$$\frac{aa}{aa+\alpha\alpha},\quad\frac{(ab-\alpha\beta)^2}{(aa+\alpha\alpha)(bb+\beta\beta)},\quad\frac{(a\beta-\alpha b)^2}{(aa+\alpha\alpha)(bb+\beta\beta)},$$

quarum summa est

$$\frac{aa}{aa+\alpha\alpha}+1-\frac{4a\alpha b\beta}{(aa+\alpha\alpha)(bb+\beta\beta)}$$

unitati aequanda, unde fit

$$aa(bb+\beta\beta)=4a\alpha b\beta$$

hincque

$$\frac{a}{\alpha}=\frac{4b\beta}{bb+\beta\beta}.$$

Quare sumtis $a=4b\beta$ et $\alpha=bb+\beta\beta$ numeri quaesiti ad integros perducti erunt

$$aa(bb+\beta\beta),\quad(ab-\alpha\beta)^2,\quad(a\beta-\alpha b)^2.$$

Iam vero est

$$ab-\alpha\beta=3bb\beta-\beta^3=\beta(3bb-\beta\beta)$$

et

$$a\beta-\alpha b=3b\beta\beta-b^3=b(3\beta\beta-bb).$$

Consequenter habebimus has formulas

$$16bb\beta\beta(bb+\beta\beta),\quad \beta\beta(3bb-\beta\beta)^2,\quad bb(3\beta\beta-bb)^2,$$

quarum quaelibet in summam reliquarum ducta producit quadratum.

37. Evolvamus hinc solutiones simpliciores ponendo numeros minores loco b et β, quorum tantum ratio spectatur, ac si ambo sint impares, numeri quaesiti per 4 deprimantur.

Numeri quaesiti

I. $\frac{b}{\beta}=\frac{1}{1}$, $p=8$, $q=1$, $r=1$;

II. $\frac{b}{\beta}=\frac{2}{1}$, $p=320$, $q=121$, $r=4$;

III. $\frac{b}{\beta}=\frac{3}{1}$, $p=360$, $q=169$, $r=81$;

IV. $\frac{b}{\beta}=\frac{3}{2}$, $p=7488$, $q=2116$, $r=81$;

V. $\frac{b}{\beta}=\frac{4}{1}$, $p=4352$, $q=2209$, $r=2704$;

VI. $\frac{b}{\beta}=\frac{4}{3}$, $p=57600$, $q=13689$, $r=1936$;

VII. $\frac{b}{\beta}=\frac{5}{1}$, $p=2600$, $q=1369$, $r=3025$.[1])

38. Aliae solutiones reperientur ex his formulis

$$\frac{aa}{aa+\alpha\alpha},\quad \frac{(ab-\alpha\beta)^2}{(aa+\alpha\alpha)(bb+\beta\beta)},\quad \frac{(ab+\alpha\beta)^2}{(aa+\alpha\alpha)(bb+\beta\beta)},$$

quarum summa est

$$\frac{aa}{aa+\alpha\alpha}+1+\frac{aabb+\alpha\alpha\beta\beta-aa\beta\beta-\alpha\alpha bb}{(aa+\alpha\alpha)(bb+\beta\beta)};$$

quae cum unitati aequari debeat, fiet

$$2aabb+\alpha\alpha\beta\beta-\alpha\alpha bb=0,$$

1) Editio princeps (atque etiam *Comment. arithm.*): $r=12100$. EULERUS hunc numerum 12100 per 4 dividere neglexit. F. R.

hinc

$$\frac{aa}{\alpha\alpha} = \frac{bb - \beta\beta}{2bb} \quad \text{seu} \quad \frac{bb}{\beta\beta} = \frac{\alpha\alpha}{\alpha\alpha - 2aa},$$

unde

$$b = \alpha \quad \text{et} \quad \beta = \sqrt{(\alpha\alpha - 2aa)}.$$

Capiatur ergo

$$a = 2mn, \quad \alpha = mm + 2nn, \quad b = mm + 2nn, \quad \beta = mm - 2nn$$

eruntque tres numeri quaesiti

$$p = 8mmnn(m^4 + 4n^4),$$
$$q = (mm + 2mn - 2nn)^2(mm + 2nn)^2,$$
$$r = (mm - 2mn - 2nn)^2(mm + 2nn)^2,$$

unde sequentes solutiones deducuntur:

I.	$p = 40,$	$q = 9,$	$r = 81;$
II.	$p = 8 \cdot 9 \cdot 85,$	$q = 121 \cdot 169,$	$r = 121;$
III.	$p = 8 \cdot 4 \cdot 65,$	$q = 81 \cdot 9,$	$r = 81 \cdot 121;$
IV.	$p = 8 \cdot 36 \cdot 145,$	$q = 289 \cdot 169,$	$r = 289 \cdot 121;$
V.	$p = 8 \cdot 9 \cdot 325,$	$q = 361 \cdot 121,$	$r = 361 \cdot 529;$
VI.	$p = 8 \cdot 100 \cdot 689,$	$q = 1089 \cdot 1369,$	$r = 1089 \cdot 9;$
VII.	$p = 8 \cdot 16 \cdot 1025,$	$q = 1089 \cdot 529,$	$r = 1089 \cdot 1521;$
VIII.	$p = 8 \cdot 144 \cdot 1105,$	$q = 1681 \cdot 1,$	$r = 1681 \cdot 2209;$
IX.	$p = 8 \cdot 225 \cdot 949,$	$q = 1849 \cdot 1369,$	$r = 1849 \cdot 529.$

39. Neque vero haec solutio generalis est putanda, sed potius innumerabiles aliae locum habent, quae in his geminis formulis non continentur. Pro generali enim solutione hanc aequationem resolvi oporteret

$$\frac{1}{1+xx} + \frac{1}{1+yy} + \frac{1}{1+zz} = 1,$$

unde oritur

$$xxyyzz - xx - yy - zz - 2 = 0$$

hincque

$$zz = \frac{xx + yy + 2}{xxyy - 1},$$

ita ut haec formula

$$(xxyy - 1)(xx + yy + 2)$$

in genere ad quadratum reduci debeat; quod quomodo sit efficiendum, non patet.

40. Interim ex solutione iam aliunde cognita ope huius formulae infinitae aliae elici possunt. Dividantur enim terni numeri inventi, veluti 40, 9, 81, per eorum summam 130, ut hae fractiones obtineantur

$$\frac{4}{13}, \quad \frac{9}{130}, \quad \frac{81}{130},$$

quae cum generalibus comparatae praebent

$$x = \frac{3}{2}, \quad y = \frac{11}{3}, \quad z = \frac{7}{9};$$

quarum una tantum $x = \frac{3}{2}$ pro cognita sumatur, pro binis reliquis vero haec aequatio resolvatur

$$\frac{9}{4}yyzz - yy - zz - \frac{17}{4} = 0 \quad \text{seu} \quad zz = \frac{4yy + 17}{9yy - 4},$$

unde fit

$$(9yy - 4)z = \sqrt{(9yy - 4)(4yy + 17)}:$$

Quia autem novimus satisfacere valorem $y = \frac{11}{3}$, statuamus $y = \frac{11 + u}{3}$ fitque

$$3(9yy - 4)z = \sqrt{(9 \cdot 13 + 22u + uu)(49 \cdot 13 + 88u + 4uu)},$$

ita ut haec formula ad quadratum sit reducenda

$$273^2 + 22 \cdot 1105u + 3041uu + 176u^3 + 4u^4;$$

cuius radix si statuatur $273 + \frac{85 \cdot 11}{21}u \pm 2uu$, fit

$$\left(\frac{8 \cdot 13 \cdot 4489}{21^2} \mp 4 \cdot 13 \cdot 21\right)uu + 44\left(4 \mp \frac{85}{21}\right)u^3 = 0$$

et

$$u = -\frac{13(8978 \mp 9261)}{11 \cdot 21(84 \mp 85)}$$

sicque pro signo superiori

$$u = -\frac{13 \cdot 283}{11 \cdot 21} \quad \text{et} \quad y = -\frac{1138}{693},$$

pro signo inferiori

$$u = -\frac{1403}{231} \quad \text{et} \quad y = +\frac{1138}{693},$$

qui duo valores conveniunt; et ob $y = \frac{1138}{693}$ fit

$$z = \sqrt{\frac{4 \cdot 1138^2 + 17 \cdot 693^2}{9 \cdot 1138^2 - 4 \cdot 693^2}} = \frac{3653}{8 \cdot 13 \cdot 30} = \frac{281}{240},$$

unde ternae fractiones prodeunt

$$\frac{4}{13}, \quad \frac{480249}{13 \cdot 136561}, \quad \frac{57600}{136561},$$

quae in integris dant hos numeros

$$p = 4 \cdot 136561 = 4 \cdot 17 \cdot 29 \cdot 277 = 546244,$$

$$q = 480249 \quad = 693^2 \quad = 480249,$$

$$r = 13 \cdot 57600 = 13 \cdot 240^2 \quad = 748800$$

hincque

$$p + q + r = 13 \cdot 17 \cdot 29 \cdot 277 = 1775293.$$

Hac ergo methodo solutiones particulares datae ad maiorem generalitatem evehuntur.

CASUS QUATUOR NUMERORUM

41. Statuamus quatuor fractiones

$$\frac{aa}{aa+\alpha\alpha}, \quad \frac{bb}{bb+\beta\beta}, \quad \frac{(ab-\alpha\beta)^2}{(aa+\alpha\alpha)(bb+\beta\beta)}, \quad \frac{(a\beta-\alpha b)^2}{(aa+\alpha\alpha)(bb+\beta\beta)},$$

quarum summa est

$$\frac{aa}{aa+\alpha\alpha} + \frac{bb}{bb+\beta\beta} + 1 - \frac{4aa\alpha b\beta}{(aa+\alpha\alpha)(bb+\beta\beta)}$$

unitati aequanda; unde fit

$$2aabb + aa\beta\beta + \alpha\alpha bb = 4aab\beta$$

ideoque

$$\frac{b}{\beta} = \frac{2a\alpha \pm \sqrt{(4aa\alpha\alpha - 2a^4 - aa\alpha\alpha)}}{2aa + \alpha\alpha}$$

seu

$$\frac{b}{\beta} = \frac{2a\alpha \pm a\sqrt{(3\alpha\alpha - 2aa)}}{2aa + \alpha\alpha}.$$

Quare litteras a et α ita accipi oportet, ut formula $3\alpha\alpha - 2aa$ quadratum evadat.

42. Hunc in finem ponamus

$$\sqrt{(3\alpha\alpha - 2aa)} = \alpha + \frac{m}{n}(\alpha - a)$$

fietque

$$2nn\alpha + 2nna = 2mn\alpha + mm\alpha - mma.$$

Ergo

$$a = mm + 2mn - 2nn \quad \text{et} \quad \alpha = mm + 2nn,$$

hinc

$$\alpha - a = -2mn + 4nn$$

et

$$\sqrt{(3\alpha\alpha - 2aa)} = -mm + 4mn + 2nn.$$

Quocirca habebimus

$$\text{vel } \frac{b}{\beta} = \frac{(mm + 2mn - 2nn)(3mm - 4mn + 2nn)}{2(mm + 2mn - nn)^2 + (mm + 2nn)^2} = \frac{mm + 2mn - 2nn}{mm + 4mn + 6nn}$$

$$\text{vel } \frac{b}{\beta} = \frac{(mm + 2mn - 2nn)(mm + 4mn + 6nn)}{2(mm + 2mn - 2nn)^2 + (mm + 2nn)^2} = \frac{mm + 2mn - 2nn}{3mm - 4mn + 2nn}.$$

Tandem numeri quaesiti habebuntur

$$p = aa(bb + \beta\beta), \quad q = bb(aa + \alpha\alpha), \quad r = (ab - \alpha\beta)^2, \quad s = (a\beta - \alpha b)^2.$$

43. Cum sit $\alpha = mm + 2nn$, loco α alii numeri assumi nequeunt, nisi qui sint vel primi huius formae $8m + 1$ seu $8m + 3$ vel ex huiusmodi primis compositi. Simpliciores cum numeris a et $[\gamma =] \sqrt{(3\alpha\alpha - 2aa)}$ ipsis respon-

dentibus in sequenti tabella exhibeo:

$\alpha = 1$	3	9	11	11	17	17	19	19
$a = 1$	1	11	1	13	11	13	11	23
$\gamma = 1$	5	1	19	5	25	23	29	5
$\beta = 3$	11	323	123	459	531	627	603	1419
$b = 3$	1	187	3	221	99	143	99	759
vel $b = 1$	11	209	41	351	649	741	737	989
vel $\beta = 1$	1	19	3	17	9	11	9	33
vel $b = 1$	1	11	1	13	11	13	11	23
vel $\beta = 3$	11	17	41	27	59	57	67	43
vel $b = 1$	1	11	1	13	11	13	11	23

44. Cum ergo in genere sit

$$a = mm + 2mn - 2nn, \quad b = mm + 2mn - 2nn,$$

$$\alpha = mm + 2nn, \quad \beta = mm + 4mn + 6nn$$

vel

$$\beta = 3mm - 4mn + 2nn,$$

erit

$$ab - \alpha\beta = -8nn(m+n)^2$$

vel

$$= -2mm(m-2n)^2,$$

$$a\beta - \alpha b = 4n(m+n)(mm + 2mn - 2nn)$$

vel

$$= 2m(m-2n)(mm + 2mn - 2nn).$$

Item

$$aa + \alpha\alpha = 2mm(m+n)^2 + 2nn(m-2n)^2$$

et

$$bb + \beta\beta = 2(m+n)^2(m+2n)^2 + 2nn(m+4n)^2$$

vel

$$= 2mm(2m-n)^2 + 2(m-n)^2(m-2n)^2,$$

unde in numeris sequentes nanciscimur solutiones:

I.	$p = 1,$	$q = 1,$	$r = 0,$	$s = 0,$
II.	$p = 5,$	$q = 1,$	$r = 2,$	$s = 2,$
III.	$p = 61,$	$q = 5,$	$r = 512,$	$s = 32,$
IV.	$p = 841,$	$q = 61,$	$r = 225 \cdot 450,$	$s = 450,$
V.	$p = 121 \cdot 205,$	$q = 121 \cdot 101,$	$r = 16 \cdot 32,$	$s = 121 \cdot 32,$
VI.	$p = 121 \cdot 241$[1]),	$q = 121 \cdot 101,$	$r = 25 \cdot 50,$	$s = 121 \cdot 50,$
VII.	$p = 121 \cdot 2305,$	$q = 121 \cdot 241,$	$r = 576 \cdot 1152,$	$s = 121 \cdot 1152,$
VIII.	$p = 169 \cdot 229,$	$q = 169 \cdot 145,$	$r = 9 \cdot 18,$	$s = 169 \cdot 18,$
IX.	$p = 169 \cdot 449,$	$q = 169 \cdot 145,$	$r = 64 \cdot 128,$	$s = 169 \cdot 128.$

45. Formulae generales autem ita se habebunt:

vel

$$p = (mm(m+n)^2 + nn(m-2n)^2)(mm+2mn-2nn)^2,$$
$$q = ((m+n)^2(m+2n)^2 + nn(m+4n)^2)(mm+2mn-2nn)^2,$$
$$r = 8nn(m+n)^2(mm+2mn-2nn)^2,$$
$$s = 8nn(m+n)^2 4nn(m+n)^2$$

vel

$$p = (mm(m+n)^2 + nn(m-2n)^2)(mm+2mn-nn)^2,$$
$$q = (mm(2m-n)^2 + (m-n)^2(m-2n)^2)(mm+2mn-2nn)^2,$$
$$r = 2mm(m-2n)^2(mm+2mn-2nn)^2,$$
$$s = 2mm(m-2n)^2 mm(m-2n)^2.$$

Utroque casu quatuor numeri p, q, r, s ita sunt comparati, ut quilibet in summam trium reliquorum ductus producat numerum quadratum. Quamquam autem hinc innumerabiles solutiones derivare licet, haec solutio nonnisi pro maxime particulari est habenda.

---

1) Editio princeps (atque etiam *Comment. arithm.*): $p = 121 \cdot 289$, qui autem numerus problemati proposito non satisfacit. Correxit F. R.

46. Solutio autem generaliter instruitur ponendo in genere pro quaternis fractionibus

$$\frac{1}{1+zz}, \quad \frac{1}{1+yy}, \quad \frac{1}{1+xx}, \quad \frac{1}{1+vv};$$

quarum summa cum unitati esse debeat aequalis, orietur haec aequatio

$$vvxxyyzz = vvxx + vvyy + vvzz + xxyy + xxzz + yyzz + 2vv + 2xx + 2yy + 2zz + 3,$$

cuius autem resolutio maximis difficultatibus est implicata. Verum si ex iam inventis solutionibus pro binis litteris x et v idonei valores accipiuntur, praeter valores reliquarum y et z cognitos innumerabiles alii assignari poterunt.

47. Ut hoc exemplo ostendam, assumam solutionem secundam his fractionibus $\frac{1}{2}, \frac{1}{10}, \frac{1}{5}, \frac{1}{5}$ contentam indeque statuo $v = 2$ et $x = 3$, reliquas autem, quae hoc exemplo sunt $y = 1$ et $z = 2$, ut incognitas specto. Habebimus ergo hanc aequationem

$$36yyzz = yyzz + 15yy + 15zz + 65$$

seu

$$7yyzz = 3yy + 3zz + 13,$$

ex qua prodit

$$zz = \frac{3yy + 13}{7yy - 3},$$

ita ut haec formula $\frac{3yy+13}{7yy-3}$ quadrato aequari debeat, quod duobus casibus $y = 1$ et $y = 2$ evenire novimus. Iam $7yy - 3$ in genere fit quadratum ponendo [1])

$$y = \frac{mm + 3}{mm + 4m - 3},$$

qui in $3yy + 13$ substitutus dat

$$16m^4 + 104m^3 + 148mm - 312m + 144 = \square,$$

1) Vide L. Euler, *Vollständige Anleitung zur Algebra*, St. Petersburg 1770, Zweyter Theil, zweyter Abschnitt, Cap. 4; *Leonhardi Euleri Opera omnia*, series I, vol. 1, p. 349, imprimis p. 359. F. R.

cuius radix posita $4mm + 13m + 12$ dat

$$m = -\frac{16}{3};$$

at radix posita $4mm - 13m + 12$ dat

$$m = \frac{9}{16};$$

utrimque reperitur

$$y = \frac{283}{37} \quad \text{et} \quad z = \frac{254}{373}\ ^{1}).$$

48. Quamquam autem hoc modo ex inventa quavis solutione continuo alias novas elicere licet, tamen sic mox ad numeros praegrandes pervenitur, quod eo maius est incommodum, cum aliunde solutiones multo simpliciores obtineri queant; id quod quidem nulla certa methodo, sed mero tentamine praestatur. Considerentur scilicet plures fractiones huius formae $\frac{\alpha\alpha}{\alpha\alpha + \alpha\alpha}$, ex quibus quippe quatuor eligi oportet, quarum summa unitati aequetur. Ita sumtis fractionibus, quarum denominatores in 130 continentur,

$$\frac{1}{2},\ \frac{1}{5},\ \frac{1}{10},\ \frac{4}{13},\ \frac{1}{26},\ \frac{1}{65},\ \frac{16}{65},\ \frac{9}{130},\ \frac{49}{130},$$
$$\frac{4}{5},\ \frac{9}{10},\ \frac{9}{13},\ \frac{25}{26},\ \frac{64}{65},\ \frac{49}{65},\ \frac{121}{130},\ \frac{81}{130}$$

binarum $\frac{9}{130}$ et $\frac{49}{130}$ summa est $\frac{29}{65}$; huic addatur $\frac{16}{65}$ proditque $\frac{45}{65} = \frac{9}{13}$, quae cum $\frac{4}{13}$ producit unitatem. Ita quatuor fractiones

$$\frac{4}{13},\ \frac{16}{65},\ \frac{9}{130},\ \frac{49}{130}$$

praebent hos numeros

$$p = 40, \quad q = 32, \quad r = 9, \quad s = 49.$$

Alio modo fit $\frac{9}{130} + \frac{1}{5} = \frac{35}{130} = \frac{7}{26}$, porro $\frac{7}{26} + \frac{1}{26} = \frac{4}{13}$, quae cum $\frac{9}{13}$ dat unitatem, unde ex fractionibus

$$\frac{9}{130},\ \frac{1}{5},\ \frac{1}{26},\ \frac{9}{13}$$

---

1) Editio princeps (atque etiam *Comment. arithm.*): $z = \frac{254}{273}$. Correxit F. R.

nascuntur hi numeri

$$p = 9, \quad q = 26, \quad r = 5, \quad s = 90,$$

qui utique multo sunt minores quam superiores certa ratione inventi, primis quidem ibi exceptis, qui ob aequales numeros excludendi videntur.

49. Simili modo posita summa $p + q + r + s = 170$ reperiuntur duae solutiones

$$\text{I.} \quad p = 1, \quad q = 10, \quad r = 34, \quad s = 125;$$
$$\text{II.} \quad p = 10, \quad q = 17, \quad r = 45, \quad s = 98.$$

Summa numerorum 290 dat

$$p = 1, \quad q = 40, \quad r = 121, \quad s = 128.$$

Hinc itaque patet casu quasi fortuito multo simpliciores numeros problemati satisfacientes reperiri atque adeo hac ratione non difficulter quinque numeri assignari possunt, ut quilibet per reliquorum summam multiplicatus praebeat numerum quadratum, cuiusmodi sunt

$$2, \quad 40, \quad 45, \quad 58, \quad 145$$

et

$$32, \quad 61, \quad 98, \quad 169, \quad 250.$$

Hocque modo etiam plures numeros huius indolis detegere licet, ad quos inveniendos nulla certa methodus adhuc est explorata.

APPENDIX

50. Si problemati modo tractato haec conditio adiungatur, ut singuli numeri esse debeant quadrati, quaestionis quasi natura immutatur, quae ita enunciabitur:

Invenire quotcumque numeros quadratos, ut summa omnium quolibet imminuta fiat numerus quadratus.[1])

1) Confer hanc quaestionem cum quaestionibus XXVII et XXVIII libri V DIOPHANTI *Arithmeticorum* (ed. P. TANNERY; quae quaestiones sunt quaestiones XXX et XXXI editionis BACHETI; vide notam p. 404 voluminis praecedentis). F. R.

Sint numeri quadrati quaesiti

$$A^2,\ B^2,\ C^2,\ D^2 \text{ etc.},$$

quorum summa ponatur $= S$, fierique debet

$$S - A^2 = P^2,\quad S - B^2 = Q^2,\quad S - C^2 = R^2 \text{ etc.},$$

unde patet S esse summam eiusmodi binorum quadratorum, quae pluribus modis in bina quadrata se distribui patiantur; seu posito $S = xx + yy$ hanc duorum quadratorum summam indefinite in alia bina quadrata secari oportet, quod in genere ita praestatur

$$S = \left(\frac{2fx + (ff-1)y}{ff+1}\right)^2 + \left(\frac{(ff-1)x - 2fy}{ff+1}\right)^2 = xx + yy.$$

51. Pro casu ergo trium quadratorum poni debet

$$A = x,\quad B = \frac{2fx - (ff-1)y}{ff+1} \quad \text{et} \quad C = \frac{2gx - (gg-1)y}{gg+1}$$

et summa quadratorum tum ipsi $xx + yy$ aequari. Quod cum in genere difficulter praestetur, in solutionem particularem inquiramus ponendo $g = \frac{f+1}{f-1}$, unde fit

$$C = \frac{(ff-1)x - 2fy}{ff+1}$$

et haec oritur aequatio

$$xx + xx + yy - \frac{8f(ff-1)}{(ff+1)^2}xy = xx + yy,$$

ex qua sequitur

$$x = \frac{8f(ff-1)}{(ff+1)^2}y \quad \text{seu} \quad x = 8f(ff-1) \quad \text{et} \quad y = (ff+1)^2,$$

hincque quadratorum quaesitorum radices in integris

$$A = 8f(ff-1)(ff+1),$$
$$B = 2f(3f^4 - 10ff + 3) = 2f(3ff-1)(ff-3),$$
$$C = (ff-1)(f^4 - 14ff + 1) = (ff-1)(ff+4f+1)(ff-4f+1),$$

unde, si $f = 2$, sequuntur hi numeri

$$A = 16 \cdot 3 \cdot 5, \quad B = 4 \cdot 11 \cdot 1, \quad C = 3 \cdot 13 \cdot 3$$

seu

$$A = 240, \qquad B = 44, \qquad C = 117.$$

52. Ad casum autem quatuor quadratorum progrediamur, quandoquidem tum problema fit difficillimum, ut solutio adeo simplicissima iam ad maximos numeros exsurgat. Faciamus ergo

$$A = x, \quad B = \frac{2fx-(ff-1)y}{ff+1}, \quad C = \frac{(ff-1)x-2fy}{ff+1}, \quad D = \frac{2px-(pp-1)y}{pp+1},$$

et cum sit

$$BB + CC = xx + yy - \frac{8f(ff-1)}{(ff+1)^2}xy,$$

posito brevitatis ergo

$$\frac{4f(ff-1)}{(ff+1)^2} = g$$

prodit haec aequatio

$$xx + \frac{4ppxx-4p(pp-1)xy+(pp-1)^2yy}{(pp+1)^2} - 2gxy = 0$$

seu

$$(pp-1)^2yy = 2g(pp+1)^2xy - 4ppxx + 4p(pp-1)xy - (pp+1)^2xx$$

hincque

$$\frac{(pp-1)^2y}{x} = g(pp+1)^2 + 2p(pp-1)$$

$$\pm\sqrt{(gg(pp+1)^4+4gp(pp-1)(pp+1)^2+4pp(pp-1)^2-(pp-1)^2(pp+1)^2-4pp(pp-1)^2)}$$

$$= g(pp+1)^2 + 2p(pp-1) \pm (pp+1)\sqrt{(gg(pp+1)^2+4gp(pp-1)-(pp-1)^2)}.$$

53. Haec formula rationalis reddenda insigni molestia premi videtur, quam autem ponendo $p = \frac{q+1}{q-1}$ tollere licet. Facilior vero redditur solutio, si pro primo numero sumatur $A = y$, unde fit

$$4ppxx = 2g(pp+1)^2xy - (pp-1)^2yy + 4p(pp-1)\,xy - (pp+1)^2yy,$$

hincque

$$\frac{4ppx}{y} = g(pp+1)^2 + 2p(pp-1) \pm (pp+1)\sqrt{(gg(pp+1)^2+4gp(pp-1)-4pp)},$$

ubi quantitas rationalis reddenda est

$$ggp^4 + 4gp^3 + (2gg - 4)pp - 4gp + gg,$$

cuius radix posita $gpp + 2p + g$ dat $p = -g$, ita ut sit

$$\frac{4ggx}{y} = g(gg+1)^2 - 2g(gg-1) \pm (gg+1)(g^3 - g)$$

seu

$$\frac{4gx}{y} = (gg+1)^2 - 2(gg-1) \pm (gg+1)(gg-1).$$

Ergo

$$\text{vel } \frac{4gx}{y} = 2(g^4+1) \quad \text{vel } \frac{4gx}{y} = 4.$$

54. Evolvamus primo posteriorem solutionem utpote simpliciorem et ob $\frac{y}{x} = \frac{g}{1}$ et $p = -g$ habebitur

$$A = g, \quad B = \frac{2f - g(ff-1)}{ff+1}, \quad C = \frac{ff - 1 - 2fg}{ff+1}, \quad D = \frac{-2g - g(gg-1)}{gg+1} \text{ seu } D = -g;$$

forent ergo duo quadrata A^2 et D^2 inter se aequalia, scilicet

$$A = D = g = \frac{4f(ff-1)}{(ff+1)^2},$$

et pro rèliquis

$$B = \frac{2f(f^4 - 6ff + 1)}{(ff+1)^3} \quad \text{et} \quad C = \frac{(ff-1)(f^4 - 6ff + 1)}{(ff+1)^3},$$

quae radices per $(ff+1)^3$ multiplicando ad numeros integros revocatae fient

$$A = D = 4f(ff-1)(ff+1),$$

$$B = 2f(f^4 - 6ff + 1), \quad C = (ff-1)(f^4 - 6ff + 1),$$

unde sumto $f = 2$ oritur haec solutio

$$A = 8 \cdot 3 \cdot 5, \quad D = 8 \cdot 3 \cdot 5, \quad B = 4 \cdot 7, \quad C = 3 \cdot 7$$

seu

$$A = 120, \quad D = 120, \quad B = 28, \quad C = 21.$$

55. Si aequalitas duorum numerorum minus placet, evolvamus alteram solutionem $\frac{x}{y} = \frac{g^4+1}{2g}$, unde fit $x = g^4 + 1$, $y = 2g$, et ob $p = -g$ erit

$$A = 2g, \quad B = \frac{2f(g^4+1) - 2g(ff-1)}{ff+1}, \quad C = \frac{(ff-1)(g^4+1) - 4fg}{ff+1}$$

et

$$D = \frac{-2g(g^4+1) - 2g(gg-1)}{gg+1} = -2g^3$$

seu

$$A = 2g(ff+1), \quad B = 2f(g^4+1) - 2g(ff-1),$$
$$C = (ff-1)(g^4+1) - 4fg, \quad D = 2g^3(ff+1),$$

ubi

$$g = \frac{4f(ff-1)}{(ff+1)^2};$$

seu ponatur $g = \frac{m}{n}$ et omnibus ad integros reductis fiet

$$A = 2mn^3(ff+1), \quad B = 2f(m^4+n^4) - 2mn^3(ff-1),$$
$$C = (ff-1)(m^4+n^4) - 4fmn^3, \quad D = 2m^3n(ff+1).$$

Hinc sumto $f = 2$, ut sit $g = \frac{24}{25} = \frac{m}{n}$, erunt quatuor quadratorum radices

$$A = 2^4 \cdot 3 \cdot 5^7 = 3750000, \qquad B = 2^3 \cdot 7 \cdot 22843 = 639604,$$
$$C = 3^2 \cdot 7 \cdot 13219 = 832797, \qquad D = 2^{10} \cdot 3^3 \cdot 5^3 = 3456000.$$

56. Ob hos numeros tam grandes problema eo magis est attentione dignum, quamobrem operae pretium videtur adhuc aliam eius solutionem etsi particularem proponere. Positis igitur quatuor quadratis quaesitis vv, xx, yy, zz primo has duas tantum conditiones considero

$$vv + yy + zz = \square \quad \text{et} \quad xx + yy + zz = \square;$$

quibus ut satisfaciam, assumo binos numeros a et α, ut sit $aa + \alpha\alpha = AA$, ac statuo[1])

$$vv + yy + zz = \left(\frac{Av + \alpha x}{a}\right)^2$$

et

$$xx + yy + zz = \left(\frac{Ax + \alpha v}{a}\right)^2,$$

1) Editio princeps (atque etiam *Comment. arithm.*): . . . *statuo*

$$vv + yy + zz = \frac{Av + \alpha x}{a} \quad et \quad xx + yy + zz = \frac{Ax + \alpha v}{a}.$$

Correxit F. R.

ut utrimque eadem prodeat aequatio

$$aa(yy + zz) = \alpha\alpha(vv + xx) + 2\alpha Avx.$$

Simili modo pro binis reliquis conditionibus pono[1])

$$yy + vv + xx = \left(\frac{Ay - az}{\alpha}\right)^2,$$

$$zz + vv + xx = \left(\frac{Az - ay}{\alpha}\right)^2$$

prodibitque hinc

$$\alpha\alpha(vv + xx) = aa(yy + zz) - 2Aayz,$$

quae duae aequationes additae dant

$$\alpha vx = ayz \quad \text{hincque} \quad z = \frac{\alpha vx}{ay};$$

qui valor in priori substituatur fietque

$$aayy + \frac{\alpha\alpha vvxx}{yy} - \alpha\alpha vv - \alpha\alpha xx - 2\alpha Avx = 0$$

seu

$$\alpha\alpha xx(vv - yy) = 2\alpha Avxyy + \alpha\alpha vvyy - aay^4$$

et

$$\alpha x = \frac{Avyy \pm y\sqrt{(AAvvyy + \alpha\alpha v^4 - \alpha\alpha vvyy - aavvyy + aay^4)}}{vv - yy},$$

quae ob $AA = \alpha\alpha + aa$ abit in

$$\frac{\alpha x}{y} = \frac{Avy \pm \sqrt{(\alpha\alpha v^4 + aay^4)}}{vv - yy}.$$

57. Ponatur $v = y(1 + s)$, et cum fiat

$$\sqrt{(\alpha\alpha v^4 + aay^4)} = yy\sqrt{(AA + 4\alpha\alpha s + 6\alpha\alpha ss + 4\alpha\alpha s^3 + \alpha\alpha s^4)},$$

---

1) Editio princeps (atque etiam *Comment. arithm.*): . . . *pono*

$$yy + vv + xx = \frac{Ay - az}{\alpha}, \quad zz + vv + xx = \frac{Az - ay}{\alpha}.$$

Correxit F. R.

statuatur haec radix $= A + \frac{2\alpha\alpha}{A}s + \alpha ss$ eritque

$$6\alpha\alpha ss + 4\alpha\alpha s^3 = \left(\frac{4\alpha^4}{AA} + 2\alpha A\right)ss + \frac{4\alpha^3}{A}s^3$$

hincque

$$s = \frac{A^3 - 3\alpha AA + 2\alpha^3}{2\alpha A(A-\alpha)} = \frac{AA - 2\alpha A - 2\alpha\alpha}{2\alpha A},$$

quare

$$\frac{v}{y} = \frac{AA - 2\alpha\alpha}{2\alpha A}$$

et radix illa

$$= A + \frac{\alpha(AA - 2\alpha A - 2\alpha\alpha)}{AA} + \frac{(AA - 2\alpha A - 2\alpha\alpha)^2}{4\alpha AA}$$

$$= A + \frac{(AA - 2\alpha A + 2\alpha\alpha)(AA - 2\alpha A - 2\alpha\alpha)}{4\alpha AA} = \frac{A^4 + 4\alpha\alpha AA - 4\alpha^4}{4\alpha AA}.$$

Porro est

$$vv - yy = \frac{(AA + 2\alpha A - 2\alpha\alpha)(AA - 2\alpha A - 2\alpha\alpha)}{4\alpha\alpha AA}yy$$

hincque

$$\frac{(AA + 2\alpha A - 2\alpha\alpha)(AA - 2\alpha A - 2\alpha\alpha)}{4\alpha AA} \cdot \frac{x}{y} = \frac{AA - 2\alpha\alpha}{2\alpha} \pm \frac{A^4 + 4\alpha\alpha AA - 4\alpha^4}{4\alpha AA}$$

$$= \text{vel } \frac{A^4 - 8\alpha\alpha AA + 4\alpha^4}{4\alpha AA} = \frac{(AA + 2\alpha A - 2\alpha\alpha)(AA - 2\alpha A - 2\alpha\alpha)}{4\alpha AA} \quad \text{vel } \frac{3A^4 - 4\alpha^4}{4\alpha AA}.$$

Consequenter habebimus

$$\text{vel } \frac{x}{y} = 1 \quad \text{vel } \frac{x}{y} = \frac{3A^4 - 4\alpha^4}{(AA - 2\alpha\alpha)^2 - 4\alpha\alpha AA};$$

denique est

$$\frac{z}{y} = \frac{AA - 2\alpha\alpha}{2\alpha A} \cdot \frac{x}{y} \quad \text{ob } \frac{v}{y} = \frac{AA - 2\alpha\alpha}{2\alpha A}.$$

58. Duas igitur adepti sumus solutiones, quarum prior ita se habet sumto $y = 2\alpha aA$:

$$v = a(AA - 2\alpha\alpha),$$

$$x = 2\alpha aA,$$

$$y = 2\alpha aA,$$

$$z = \alpha(AA - 2\alpha\alpha).$$

Unde sumendo $\alpha = 3$, $a = 4$ et $A = 5$ prodit solutio simplicissima

$$v = 28, \quad x = 120, \quad y = 120, \quad z = 21.$$

Altera autem solutio in numeris integris dat

$$v = a(AA - 2\alpha\alpha)(AA + 2\alpha A - 2\alpha\alpha)(AA - 2\alpha A - 2\alpha\alpha),$$
$$x = 2a\alpha A(3A^4 - 4\alpha^4),$$
$$y = 2a\alpha A(AA + 2\alpha A - 2\alpha\alpha)(AA - 2\alpha A - 2\alpha\alpha),$$
$$z = \alpha(AA - 2\alpha\alpha)(3A^4 - 4\alpha^4).$$

Unde sumtis $\alpha = 3$, $a = 4$, $A = 5$ solutio simplicissima emergit

$$v = 4 \cdot 7 \cdot 37 \cdot 23 \quad = 23828,$$
$$x = 8 \cdot 3 \cdot 5 \cdot 1551 \quad = 186120,$$
$$y = 8 \cdot 3 \cdot 5 \cdot 37 \cdot 23 = 102120,$$
$$z = 3 \cdot 7 \cdot 1551 \quad = 32571,$$

quorum numerorum quadrata sunt

$$vv = \quad 567773584,$$
$$xx = 34640654400,$$
$$yy = 10428494400,$$
$$zz = \quad 1060870041,$$

reperiturque

$$xx + yy + zz = 214779^2, \qquad vv + yy + zz = 109805^2,$$
$$vv + xx + zz = 190445^2, \qquad vv + xx + yy = 213628^2,$$

at

$$vv + xx + yy + zz = 25 \cdot 1201 \cdot 1555297.$$

59. Quo ratio harum formularum clarius perspiciatur, notari convenit esse

$$3A^4 - 4\alpha^4 = -(AA + 2aA - 2aa)(AA - 2aA - 2aa),$$

unde erit

$$v = a(AA - 2aa)(AA + 2\alpha A - 2\alpha\alpha)(AA - 2\alpha A - 2\alpha\alpha),$$
$$z = \alpha(AA - 2\alpha\alpha)(AA + 2aA - 2aa)(AA - 2aA - 2aa),$$
$$x = 2a\alpha A(AA + 2aA - 2aa)(AA - 2aA - 2aa),$$
$$y = 2a\alpha A(AA + 2\alpha A - 2\alpha\alpha)(AA - 2\alpha A - 2\alpha\alpha);$$

sicque patet numeros a et α inter se permutari, ut natura rei postulat. Quod facilius ex his formulis perspicietur

$$v = a(aa - \alpha\alpha)(3\alpha^4 + 6aa\alpha\alpha - a^4),$$
$$z = \alpha(aa - \alpha\alpha)(3\alpha^4 + 6aa\alpha\alpha - \alpha^4),$$
$$x = 2a\alpha A(3\alpha^4 + 6aa\alpha\alpha - \alpha^4),$$
$$y = 2a\alpha A(3\alpha^4 + 6aa\alpha\alpha - a^4).$$

Hinc est in genere

$$vv + xx + yy = a^2(a^6 + 13a^4\alpha\alpha + 11aa\alpha^4 + 7\alpha^6)^2,$$
$$xx + yy + zz = \alpha^2(\alpha^6 + 13\alpha^4 aa + 11\alpha\alpha a^4 + 7a^6)^2,$$
$$vv + yy + zz = A^2(a^6 - a^4\alpha\alpha + 15aa\alpha^4 + \alpha^6)^2,$$
$$vv + xx + zz = A^2(\alpha^6 - \alpha^4 aa + 15\alpha\alpha a^4 + a^6)^2$$

et summa omnium

$$xx + yy + zz + vv = A^2(a^{12} + 34a^{10}\alpha^2 + 175a^8\alpha^4 + 92a^6\alpha^6 + 175a^4\alpha^8 + 34a^2\alpha^{10} + \alpha^{12}),$$

quae in hos factores resolvitur

$$A^2(a^4 + 6a^2\alpha^2 + \alpha^4)(a^8 + 28a^6\alpha^2 + 6a^4\alpha^4 + 28a^2\alpha^6 + \alpha^8).$$

60. Neque tamen hae formulae minimos numeros suppeditant; sequenti enim modo minores reperiuntur. Ut formula [§ 56]

$$\alpha\alpha v^4 + aay^4$$

fiat quadratum, sumtis similibus numeris b et β, ut sit

$$bb + \beta\beta = BB,$$

statuatur

$$\alpha vv = \beta M \quad \text{et} \quad ayy = bM \quad \text{seu} \quad \frac{vv}{yy} = \frac{a\beta}{\alpha b},$$

ut fiat

$$\sqrt{(\alpha\alpha v^4 + aay^4)} = BM = \frac{aB}{b}yy,$$

ubi necesse est, ut $\frac{a}{\alpha}\cdot\frac{\beta}{b}$ sit quadratum. Sit ergo

$$\frac{a}{\alpha}\cdot\frac{\beta}{b} = \frac{mm}{nn}$$

eritque

$$\frac{v}{y} = \frac{m}{n};$$

tum

$$\frac{x}{y} = \frac{\frac{Am}{n} \pm \frac{aB}{b}}{\alpha\left(\frac{a\beta}{\alpha b} - 1\right)} = \frac{Abm \pm aBn}{a\beta n - \alpha bn}$$

et

$$\frac{z}{y} = \frac{\alpha m}{an}\cdot\frac{x}{y} = \frac{\beta(Abm \pm aBn)}{bm(a\beta - \alpha b)}.$$

Iam ponatur

$$a = 21, \quad \alpha = 20, \quad A = 29, \quad b = 35, \quad \beta = 12 \quad \text{et} \quad B = 37$$

eritque

$$\frac{mm}{nn} = \frac{21}{20}\cdot\frac{12}{35} = \frac{9}{25},$$

ut sit $m = 3$ et $n = 5$, unde colligitur

$$\frac{v}{y} = \frac{3}{5}, \quad \frac{x}{y} = \frac{29\cdot 35\cdot 3 \pm 37\cdot 21\cdot 5}{-5\cdot 4\cdot 7\cdot 16} = \frac{3(29 \pm 37)}{64} \quad \text{et} \quad \frac{z}{y} = \frac{3(29 \pm 37)}{16\cdot 7}.$$

Pro signo inferiori ergo erit

$$\frac{v}{y} = \frac{3}{5}, \quad \frac{x}{y} = \frac{3}{8} \quad \text{et} \quad \frac{z}{y} = \frac{3}{14},$$

unde in integris

$$\begin{aligned} v &= 8\cdot 3\cdot 7 = 168, & \sqrt{(xx + yy + zz)} &= 305,\\ x &= 3\cdot 5\cdot 7 = 105, & \sqrt{(vv + yy + zz)} &= 332,\\ y &= 8\cdot 5\cdot 7 = 280, & \sqrt{(vv + xx + zz)} &= 207,\\ z &= 4\cdot 3\cdot 5 = 60, & \sqrt{(vv + xx + yy)} &= 343, \end{aligned}$$

$$vv + xx + yy + zz = 121249 = 29\cdot 37\cdot 113.$$

Huiusmodi autem formulae generales sunt

$$v = 4fg(f+g)(3f-g)(3ff+gg),$$
$$y = 4fg(f-g)(3f+g)(3ff+gg),$$
$$x = (ff-gg)(9ff-gg)(3ff+gg),$$
$$z = 2fg(ff-gg)(9ff-gg).^{1})$$

1) Fit enim

$$vv+yy+xx = (3f^2+g^2)^6,$$
$$vv+yy+zz = 4f^2g^2(27f^4+2f^2g^2+3g^4)^2,$$
$$yy+xx+zz = (f-g)^2(3f+g)^2(9f^4+6f^3g+10f^2g^2-2fg^3+g^4)^2,$$
$$zz+xx+vv = (f+g)^2(3f-g)^2(9f^4-6f^3g+10f^2g^2+2fg^3+g^4)^2.$$

Numeri speciales $v = 168$, $y = 280$, $x = 105$, $z = 60$ inveniuntur ponendo $f = 1$, $g = 2$. F. R.

OBSERVATIONES CIRCA BINA BIQUADRATA QUORUM SUMMAM IN DUO ALIA BIQUADRATA RESOLVERE LICEAT

Commentatio 428 indicis ENESTROEMIANI
Novi commentarii academiae scientiarum Petropolitanae 17 (1772), 1773, p. 64—69
Summarium ibidem p. 8—9

SUMMARIUM

Inter theoremata, quae circa proprietates numerorum versantur, id quidem demonstrari solet trium biquadratorum summam nullo modo posse quoque esse biquadratum sive

$$a^4 + b^4 + c^4 = d^4$$

aequationem esse impossibilem; neque vero id eodem modo etiam de differentiis valet, quandoquidem hanc aequationem

$$A^4 + B^4 - C^4 = D^4$$

sive

$$A^4 + B^4 = C^4 + D^4$$

sive etiam

$$A^4 - D^4 = C^4 - B^4$$

infinitis adeo modis resolvere licet; quod etsi fortasse etiam ab aliis Geometris est praestitum, methodus tamen, qua Cel. Auctor hic utitur, plus uno titulo omnem Analystarum attentionem mereri est censenda. Quatuor numeri minimi propositae quaestioni satisfacientes ita sunt ab Ill. Viro inventi:

$$A = 477069, \quad B = 8497, \quad C = 310319 \quad \text{et} \quad D = 428397.^{1})$$

1) Hos quidem numeros quaestioni propositae non satisfacere notis p. 216 et 217 expositum est. F. R.

1. Quum demonstratum sit neque summam neque differentiam duorum biquadratorum quadratum esse posse, multo minus biquadratum esse poterit[1]); haud minori autem fiducia negari solet summam trium adeo biquadratorum umquam biquadratum esse posse, etiamsi hoc nusquam demonstratum reperiatur. Utrum autem quatuor biquadrata reperire liceat, quorum summa sit biquadratum, merito dubitamus, quum a nemine adhuc talia biquadrata sint exhibita.

2. Quamvis autem demonstrari posset non dari terna biquadrata, quorum summa quoque sit biquadratum, id tamen neutiquam ad differentias extendere liceret neque enim propterea affirmari posset talem aequationem

$$A^4 + B^4 - C^4 = D^4$$

esse impossibilem; observavi enim hanc aequationem adeo infinitis modis resolvi posse. Neque tamen asseverare ausim hoc a nemine adhuc esse praestitum et nunc quidem minime vacat omnia monumenta in hoc Analysis genere evolvere; quicquid autem sit, spero methodum, qua sum usurus, non omni attentione fore indignam. Manifestum autem est hanc quaestionem versari circa bina biquadratorum paria, quorum sive summae sive differentiae inter se sint aequales; si enim fuerit $A^4 + B^4 = C^4 + D^4$, utique etiam erit $A^4 - D^4 = C^4 - B^4$, unde hoc Problema nobis sit propositum.

PROBLEMA

Invenire bina biquadrata A^4 et B^4, quorum summam in alia duo biquadrata resolvere liceat, ita ut habeatur talis aequalitas

$$A^4 + B^4 = C^4 + D^4.$$

SOLUTIO

3. Quum igitur hinc esse debeat

$$A^4 - D^4 = C^4 - B^4,$$

1) Id quod primum anno 1676 a B. Frénicle de Bessy demonstratum est. Vide Euleri Commentationem 98 (indicis Enestroemiani): *Theorematum quorumdam arithmeticorum demonstrationes*, Comment. acad. sc. Petrop. **10** (1738), 1747, p. 125; *Leonhardi Euleri Opera omnia*, series I, vol. 2, p. 38. F. R.

ponamus

$$A = p + q, \quad D = p - q, \quad C = r + s \quad \text{et} \quad B = r - s,$$

ut prodeat ista aequatio concinnior

$$pq(pp + qq) = rs(rr + ss),$$

cui quidem satisfieri liquet sumendo $r = p$ et $s = q$; verum inde nihil plane lucraremur, quum oriatur casus per se obvius $C = A$ et $B = D$; interim tamen hic ipse casus ad alias solutiones manuducere valet.

4. Iam statuamus

$$p = ax, \quad q = by, \quad r = kx \quad \text{et} \quad s = y,$$

ut obtineatur ista aequatio resolvenda

$$ab(aaxx + bbyy) = k(kkxx + yy),$$

unde statim deducimus

$$\frac{yy}{xx} = \frac{k^3 - a^3b}{ab^3 - k},$$

quam ergo fractionem quadratum reddi oportet. Hic autem statim in oculos incurrit casus, quo hoc usu venit, scilicet sumendo $k = ab$; tum enim fit

$$\frac{yy}{xx} = \frac{a^3b(bb-1)}{ab(bb-1)} = aa,$$

unde fieret $y = a$, $x = 1$ hincque $p = a$, $q = ab$, $r = ab$, $s = a$, qui valores producunt ipsum illum casum per se obvium.

5. Hunc igitur casum prosequentes statuamus $k = ab(1 + z)$ et aequatio nostra transfundetur in hanc formam

$$\frac{yy}{xx} = \frac{a^3b(bb - 1 + 3bbz + 3bbz^2 + bbz^3)}{ab(bb - 1 - z)} = aa\,\frac{bb - 1 + 3bbz + 3bbz^2 + bbz^3}{bb - 1 - z}$$

atque ex hac aequatione elicimus

$$\frac{y}{x} = \frac{a\sqrt{((bb-1)^3 + (bb-1)(3bb-1)z + 3bb(bb-2)zz + bb(bb-4)z^3 - bbz^4)}}{bb - 1 - z}.$$

Quo igitur formulam

$$(bb-1)^2+(bb-1)(3bb-1)z+3bb(bb-2)zz+bb(bb-4)z^3-bbz^4$$

ad quadratum perducamus, statuamus eius radicem

$$=bb-1+fz+gzz$$

et litteras f et g ita assumamus, ut terni termini priores destruantur; quare quum huius formae quadratum sit

$$(bb-1)^2+2(bb-1)fz+2(bb-1)gzz+2fgz^3+ggz^4,\\ +ffzz$$

primi quidem termini se sponte destruunt; ut autem idem in secundis eveniat, sumi debet

$$f=\frac{3bb-1}{2}$$

atque pro tertiis habebimus

$$3bb(bb-2)=2(bb-1)g+\frac{9b^4-6bb+1}{4},$$

unde colligitur

$$g=\frac{3b^4-18bb-1}{8(bb-1)},$$

quibus valoribus definitis aequatio resolvenda fit

$$(gg+bb)z=bb(bb-4)-2fg,$$

unde colligimus

$$z=\frac{bb(bb-4)-2fg}{bb+gg}.$$

6. Hinc igitur littera b adhuc arbitrio nostro permittitur; ea igitur pro lubitu assumta, simulatque hinc quantitatem z determinaverimus, statim habebimus

$$x=bb-1-z \quad \text{et} \quad y=a(bb-1+fz+gzz)$$

hincque porro

$$p=a(bb-1-z), \quad q=ab(bb-1+fz+gzz),$$
$$r=ab(1+z)(bb-1-z), \quad s=a(bb-1+fz+gzz);$$

quae formulae quum omnes sint per a divisibiles, eam divisione tollere licebit, ita ut sit

$$p = bb - 1 - z, \quad q = b(bb - 1 + fz + gzz),$$
$$r = b(1 + z)(bb - 1 - z), \quad s = bb - 1 + fz + gzz,$$

ubi notandum, si numeri x et y communem habuerint factorem, eum divisione ante tolli posse, quam litterae p, q, r, s inde definiuntur.

Operae igitur pretium erit solutiones quasdam speciales evolvere; at vero statim apparet sumi non posse $b = 1$, quia fieret $g = \infty$; multo vero minus ponere licet $b = 0$, quia fieret $q = 0$. Ex quo casus expediamus duos tantum, primo scilicet $b = 2$, tum vero $b = 3$.

PRIMA SOLUTIO SPECIALIS

7. Sit $b = 2$ ac superiores valores colliguntur, ut sequitur,

$$f = \frac{11}{2}, \quad g = -\frac{25}{24}, \quad z = \frac{6600}{2929};$$

deinde quia littera a plane non in computum ingreditur, eius loco unitas scribatur; tum vero erit

$$x = 3 - \frac{6600}{2929} = \frac{2187}{2929},$$

$$y = 3 + \frac{11}{2}\cdot\frac{6600}{2929} - \frac{25}{24}\cdot\frac{6600^2}{2929^2} = 3 + \frac{55407\cdot 1100}{2929^2} = \frac{3\cdot 28894941}{2929^2}.$$

Totum autem negotium redit ad rationem inter x et y; quae quum sit

$$\frac{y}{x} = \frac{3\cdot 28894941}{2187\cdot 2929} = \frac{28894941}{2929\cdot 729} = \frac{3210549}{2929\cdot 81} = \frac{1070183}{27\cdot 2929},$$

habebimus

$$x = 79083 \quad \text{et} \quad y = 1070183;$$

tum igitur ob

$$k = 2(1 + z) = \frac{2\cdot 9529}{2929} = \frac{19058}{2929}$$

concludimus fore

$$p = 79083, \quad q = 2\cdot 1070183 = 2140366,$$
$$r = 27\cdot 19058 = 514566, \quad s = 1070183.$$

Consequenter pro ipsis radicibus biquadratorum nanciscimur

$$A = p + q = 2219449, \qquad C = [r + s =] 1584749,$$
$$B = r - s = -555617, \qquad D = [p - q = -] 2061283$$

eritque propterea

$$A^4 + B^4 = C^4 + D^4.$$

SECUNDA SOLUTIO SPECIALIS

8. Sit $b = 3$ eritque

$$f = 13, \quad g = \frac{5}{4}, \quad \text{hinc} \quad z = \frac{200}{169}$$

ideoque

$$k = \frac{3 \cdot 369}{169} = \frac{1107}{169} = \frac{9 \cdot 123}{169} = \frac{27 \cdot 41}{169},$$

porro

$$x = \frac{8 \cdot 144}{169} = \frac{128 \cdot 9}{169}$$

et

$$y = 8 + \frac{200}{169}\left(13 + \frac{5}{4} \cdot \frac{200}{169}\right) = 8 + \frac{200}{169} \cdot \frac{2447}{169} = \frac{8 \cdot 89736}{169^2}\ ^{1})$$

sicque erit

$$x : y = 8 \cdot 144 \cdot 169 : 8 \cdot 89736 = 6 \cdot 169 : 3739$$

ideoque

$$x = 6 \cdot 169 = 1014 \quad \text{et} \quad y = 3739,$$

ex quibus valoribus consequimur

$$p = 1014, \qquad r = 6642 = 6 \cdot 1107,$$
$$q = 11217, \qquad s = 3739.$$

Atque hinc ipsae litterae A, B, C, D colliguntur

$$A = 12231, \qquad C = 10381,$$
$$B = 2903, \qquad D = -10203$$

---

1) Editio princeps (atque etiam *Comment. arithm.*): $y = \cdots = \frac{8\ 150911}{169^2}$, qui valor e computatione falsa $8 + \frac{200}{169} \cdot \frac{2447}{169} = 8\left(1 + \frac{50 \cdot 2447}{169^2}\right)$ ortus est. Quem ob errorem etiam omnes numeri sequentes contextu quidem servato corrigendi erant. Vide notam 2 p. 217. F. R.

eritque iterum

$$A^4 + B^4 = C^4 + D^4$$ [1])

atque hi numeri videntur minimi quaestioni nostrae satisfacientes.[2])

---

1) Scilicet:

$$A^4 = 22379370418164321,$$
$$B^4 = \quad 71021222453281$$

et

$$C^4 = 11613329925355921,$$
$$D^4 = 10837061715261681,$$

ita ut sit

$$A^4 + B^4 = 22450391640617602 = C^4 + D^4.$$ F. R.

2) EULERUS computatione falsa (vide notam p. 216) ad sequentes valores valde magnos perductus est

$$A = 477069, \quad B = 8497, \quad C = 310319, \quad D = 428397.$$

Hos quidem numeros problemati proposito satisfacere non posse facile perspicitur ultimas tantum eorum figuras respiciendo. Statim enim invenitur $A^4 + B^4 = \cdots 302$, at $C^4 + D^4 = \cdots 002$.

Ad istos falsos numeros A, B, C, D pertinent illa EULERI verba „atque hi numeri videntur minimi quaestioni nostrae satisfacientes." Iam vero vidimus rectos numeros supra inventos multo minores esse.

Ceterum EULERUS ipse postea errorem istum correxit, scilicet in Commentatione 776 (indicis ENESTROEMIANI): *Dilucidationes circa binas summas duorum biquadratorum inter se aequales*, Mém. de l'acad. d. sc. de St.-Pétersbourg **11**, 1830, p. 49, *LEONHARDI EULERI Opera omnia*, series I, vol. 5. Qua in Commentatione Illustr. Auctor insuper sequentes solutiones simplicissimas adiecit

$$A = 542, \quad B = 103, \quad C = 359, \quad D = 514,$$

pro quibus revera invenitur

$$A^4 = 86297287696,$$
$$B^4 = \quad 112550881$$

et

$$C^4 = 16610312161,$$
$$D^4 = 69799526416,$$

ita ut sit

$$A^4 + B^4 = 86409838577 = C^4 + D^4.$$ F. R.

NOVAE DEMONSTRATIONES CIRCA RESOLUTIONEM NUMERORUM IN QUADRATA[1])

Commentatio 445 indicis ENESTROEMIANI
Nova acta eruditorum 1773, p. 193—211
Acta academiae scientiarum Petropolitanae 1777: II, 1780, p. 48—69

1. Quum saepe et multum in hoc argumento fuissem occupatus neque tamen ea demonstratio, quam olim[2]) dederam circa resolutionem omnium numerorum in quatuor vel pauciora quadrata, mihi ipsi penitus satisfecisset, eo maiore ardore evolvi demonstrationem, quam Celeb. D. LAGRANGE[3]) nuper in primo volumine Novorum Actorum Acad. sc. Boruss. huius theorematis tradidit, quam utique negotium perfecisse sum admiratus, etiamsi eius momenta nimis longe repetita et vehementer operosa viderentur.

---

1) Haec dissertatio primum Novis actis eruditorum, deinde vero Actis academiae scientiarum Petropolitanae inserta est. Editioni nostrae subest editio posterior, quae a priore nonnullis locis paulo discrepat (vide *Redaktionsplan für die Eulerausgabe*, Jahresber. d. Deutschen Mathem.-Verein. 19, 1910, Zweite Abt., p. 94). F. R.

2) Vide Commentationem 242 (indicis ENESTROEMIANI): *Demonstratio theorematis FERMATIANI omnem numerum sive integrum sive fractum esse summam quatuor pauciorumve quadratorum*, Novi comment. acad. sc. Petrop. 5 (1754/5), 1760, p. 13; *LEONHARDI EULERI Opera omnia*, series I, vol. 2, p. 338. F. R.

3) I. L. LAGRANGE, *Démonstration d'un théorème d'arithmétique*, Nouv. mém. de l'acad. d. sc. de Berlin (1770), 1772, p. 123; *Oeuvres de LAGRANGE*, publiées par les soins de M. I.-A. SERRET t. III, p. 189. F. R.

2. Lectoribus autem haud ingratum fore arbitror, si praecipua momenta, quibus haec demonstratio innititur, hic breviter et concinne proposuero. Postquam Celeb. Auctor hoc lemma praemisit, quodsi duae summae binorum quadratorum $pp+qq$ et $rr+ss$ communem habeant divisorem ϱ neque tamen singula quadrata per eum dividi queant, tum non solum ipsum hunc divisorem ϱ, sed etiam ambos quotos $\frac{pp+qq}{\varrho}$ et $\frac{rr+ss}{\varrho}$ fore summas duorum quadratorum, progreditur ad theorema demonstrandum, *quodsi summa quatuor quadratorum* $P^2+Q^2+R^2+S^2$ *divisibilis fuerit per numerum quemcumque* A *neque tamen singula quadrata per eum sint divisibilia, tum ipsum hunc numerum* A *fore summam quatuor quadratorum,* cuius demonstratio sequentibus continetur ratiociniis.

I. Posito quoto ex illa divisione oriundo $=a$, ut sit

$$Aa = P^2+Q^2+R^2+S^2,$$

si forte eveniat, ut binae formulae P^2+Q^2 et R^2+S^2 habeant communem divisorem ϱ, quem ergo etiam numerus a continebit, ponit $a=b\varrho$, ut fiat

$$Ab = \frac{P^2+Q^2}{\varrho}+\frac{R^2+S^2}{\varrho};$$

quae formulae quum per lemma praemissum sint summae duorum quadratorum, habebitur huiusmodi aequatio

$$Ab = pp+qq+rr+ss,$$

ubi formulae $pp+qq$ et $rr+ss$ non amplius habebunt factorem communem.

II. Tum vero ponit $pp+qq=t$ et $rr+ss=u$, ut sit $Ab=t+u$, quam aequationem ducit in t faciendo $Abt=tt+tu$; et quia tu etiam est summa duorum quadratorum, puta $xx+yy$, sumendo scilicet $x=pr+qs$ et $y=ps-qr$, fiet

$$Abt = tt+xx+yy.$$

III. Nunc per numeros t et b, quippe qui inter se sunt primi, ambos x et y ita exprimi posse observat, ut sit $x=\alpha t+\gamma b$ et $y=\beta t+\delta b$; ubi quum litterae $\alpha, \beta, \gamma, \delta$ infinitis modis accipi queant sive negative sive positive, inter earum valores tales certe dabuntur, ut sit $\alpha<\frac{1}{2}b$ et $\beta<\frac{1}{2}b$.

IV. His iam valoribus pro x et y substitutis resultabit ista aequatio

$$Abt = tt(1 + \alpha\alpha + \beta\beta) + 2bt(\alpha\gamma + \beta\delta) + bb(\gamma\gamma + \delta\delta).$$

Quae expressio quum divisibilis esse debeat per b neque tamen in primo membro tt hanc divisionem admittat, necesse est, ut ibi formula $1 + \alpha\alpha + \beta\beta$ factorem habeat b; eodem modo etiam in ultimo membro factorem $\gamma\gamma + \delta\delta$ divisibilem per t esse necesse est. Ponatur ergo $1 + \alpha\alpha + \beta\beta = ba'$, et quia uterque numerus α et β minor est quam $\frac{1}{2}b$, manifestum est fore $a' < \frac{1}{2}b + \frac{1}{b}$; facta ergo divisione per b erit

$$At = a'tt + 2t(\alpha\gamma + \beta\delta) + b(\gamma\gamma + \delta\delta).$$

V. Multiplicetur nunc haec aequatio per a', ut prodeat

$$Aa't = a'^2tt + 2a't(\alpha\gamma + \beta\delta) + a'b(\gamma\gamma + \delta\delta),$$

et in ultimo membro loco $a'b$ scribendo $1 + \alpha\alpha + \beta\beta$ fiet

$$Aa't = a'^2tt + 2a't(\alpha\gamma + \beta\delta) + (\alpha\alpha + \beta\beta)(\gamma\gamma + \delta\delta) + \gamma\gamma + \delta\delta,$$

quae expressio in sequentia quatuor quadrata resolvetur

$$Aa't = (a't + \alpha\gamma + \beta\delta)^2 + (\beta\gamma - \alpha\delta)^2 + \gamma^2 + \delta^2;$$

ubi quum summa binorum postremorum quadratorum $\gamma^2 + \delta^2$ divisibilis sit per numerum t, necesse est, ut summa duorum priorum quoque divisibilis sit per t, ita ut hic duae binorum quadratorum summae occurrant communem divisorem t habentes; quare si per t dividatur, ambo illi quoti itidem erunt summae binorum quadratorum.

VI. Quodsi ergo ponamus

$$\frac{(a't + \alpha\gamma + \beta\delta)^2 + (\beta\gamma - \alpha\delta)^2}{t} = p'^2 + q'^2 \quad \text{et} \quad \frac{\gamma^2 + \delta^2}{t} = r'^2 + s'^2,$$

habebimus

$$Aa' = p'^2 + q'^2 + r'^2 + s'^2.$$

In hac autem formula Aa', si cum prima Aa comparetur, numerus a' multo minor erit quam a, quandoquidem $b < a$ et $a' < \frac{1}{2}b$. Simili modo ergo per-

venire licebit ad formulam Aa'', ubi a'' multo minor erit quam a', sicque tandem perveniri necesse est ad formulam $A \cdot 1$, ita ut iam ipse numerus A reperiatur aequalis summae quatuor quadratorum.

3. Demonstrato hoc theoremate insuper ostendi oportet proposito quocumque numero primo semper exhiberi posse summam quatuor quadratorum per eum divisibilem, quorum tamen singula quadrata divisionem non admittant. Atque hoc etiam Cel. LAGRANGE modo maxime ingenioso demonstrat, qui autem tantopere est abstrusus et prolixus, ut eius momenta breviter et dilucide nequaquam exhiberi possint. Nunc igitur famosum illud theorema sive BACHETI[1]) sive FERMATII, *quod omnis numerus in quadrata quatuor vel pauciora resolvi possit*, pro perfecte demonstrato est habendum. Quia enim pro numero primo quocumque semper dari potest summa quatuor quadratorum per illum divisibilis, omnes numeri primi summae erunt quatuor pauciorumve quadratorum, et quia iam dudum[2]) demonstratum est producta ex duobus pluribusve numeris, qui singuli sunt summae quatuor pauciorumve quadratorum, quoque in quatuor quadrata dispertiri posse, solidissime iam est evictum omnes plane numeros esse summas quatuor quadratorum pauciorumve.

4. Quamvis omnino nefas esset quicquam contra soliditatem et rigorem harum demonstrationum excipere, tamen nemo negabit eas nimis longe esse repetitas neque ipsa fundamenta et rationes singulorum ratiociniorum, quibus hae demonstrationes sint compositae, haud levi obscuritate esse involutas, ita ut etiamnunc merito clariores et perceptu faciliores demonstrationes desiderare liceat. Quo quidem desiderio summae laudi, quam istae demonstrationes merentur, nihil detrahi est censendum.

5. Quum igitur, postquam hoc argumentum de novo perpendissem, in novas et satis planas eorundem theorematum demonstrationes mihi incidere contigerit, iis, qui hoc studio delectantur, communicatio harum novarum demonstrationum certe gratissima fore videtur; quocirca eas hoc loco, quantum potero, breviter et dilucide sum propositurus. Ac primo quidem a theoremate illo notissimo simulque plenissime demonstrato, quo omnes divi-

1) Vide notam 4 p. 358 voluminis praecedentis. F. R.

2) Vide § 93 Commentationis 242 nota 2 p. 218 laudatae. F. R.

sores cuiusque summae duorum quadratorum inter se primorum ipsi summae duorum quadratorum aequales affirmantur, incipiam, cum quod haec nova[1]) demonstratio simplicitate se maxime commendat, tum vero quod iisdem vestigiis insistendo demonstratio facile ad quatuor quadrata extendi potest.

LEMMA 1

6. *Productum ex duabus summis binorum quadratorum itidem est summa duorum quadratorum.*

Nam si illud productum fuerit $(aa+bb)(\alpha\alpha+\beta\beta)$ et capiatur

$$A = a\alpha + b\beta \quad \text{et} \quad B = a\beta - b\alpha,$$

utique erit

$$(aa+bb)(\alpha\alpha+\beta\beta) = AA + BB.$$

THEOREMA 1

Si numerus N fuerit divisor summae duorum quadratorum P^2+Q^2 inter se primorum, tum ipse ille numerus N erit summa duorum quadratorum.

DEMONSTRATIO

Quo hanc demonstrationem facilius etiam in numeris exsequi liceat, cui forte libuerit, observo, quantumvis magni fuerint numeri P et Q, ex iis semper aliam summam duorum quadratorum $pp+qq$ formari posse, quorum radices p et q semissem numeri propositi N non superent. Nam si ponatur

$$P = fN \pm p \quad \text{et} \quad Q = gN \pm q,$$

notissimum est numeros p et q ita sumi posse, ut semissem $\frac{1}{2}N$ non superent. Quum igitur iam sit

$$PP + QQ = NN(ff+gg) + 2N(\pm fp \pm gq) + pp + qq$$

1) Confer illius theorematis demonstrationem priorem, quae continetur in Commentatione 228 (indicis Enestroemiani): *De numeris, qui sunt aggregata duorum quadratorum*, Novi comment. acad. sc. Petrop. 4 (1752/3), 1758, p. 3; *Leonhardi Euleri Opera omnia*, series I, vol. 2, p. 295. F. R.

haecque expressio per N sit divisibilis, evidens est etiam hanc binorum quadratorum summam per N divisibilem fore. Hoc praemisso ipsam demonstrationem sequentibus momentis complectar.

I. Quum igitur ista formula $pp + qq$ divisorem habeat N, ponendo quotum $= n$ habebimus

$$Nn = pp + qq,$$

ubi ergo n minor erit quam $\frac{1}{2}N$, quia $p < \frac{1}{2}N$ et $q < \frac{1}{2}N$.

II. Iam istos numeros p et q per numerum n ita exprimere licebit, ut sit

$$p = a + \alpha n \quad \text{et} \quad q = b + \beta n,$$

ubi admissis etiam numeris negativis pro a et b eos infra $\frac{1}{2}n$ deprimere licebit, uti iam initio observavimus. Tum vero erit

$$Nn = aa + bb + 2n(a\alpha + b\beta) + nn(\alpha\alpha + \beta\beta),$$

et quia in lemmate praemisso erat $a\alpha + b\beta = A$, fiet

$$Nn = aa + bb + 2nA + nn(\alpha\alpha + \beta\beta).$$

III. Huius ergo expressionis primum membrum $aa + bb$ factorem habeat necesse est n, quia reliqua membra iam per se divisorem n admittunt. Statuamus ergo

$$aa + bb = nn',$$

et quia $a < \frac{1}{2}n$ et $b < \frac{1}{2}n$ ideoque $nn' < \frac{1}{2}nn$, erit utique $n' < \frac{1}{2}n$. Hoc autem valore substituto et divisione per n facta prodit

$$N = n' + 2A + n(\alpha\alpha + \beta\beta).$$

IV. Hanc aequationem ducamus in n', et quia $nn' = aa + bb$, postremum membrum per lemma praemissum reducitur ad

$$nn'(\alpha\alpha + \beta\beta) = (aa + bb)(\alpha\alpha + \beta\beta) = AA + BB,$$

ita ut nunc habeamus

$$Nn' = n'n' + 2n'A + AA + BB,$$

quae expressio manifesto est summa duorum quadratorum, scilicet

$$Nn' = (n' + A)^2 + B^2.$$

V. Quum ergo initio fuisset productum Nn summa duorum quadratorum indeque hic elicuerimus productum minus Nn' etiam aequale summae duorum quadratorum, eodem modo ad talia producta continuo minora pertingere licebit, scilicet Nn'', Nn''' etc. Necesse igitur est, ut tandem ad productum minimum, scilicet $N \cdot 1$, perveniatur, sicque ipse numerus propositus N quoque erit summa duorum quadratorum.

COROLLARIUM

Mirum forsitan videbitur, quum perventum fuerit ad huiusmodi numerum $n' = 1$, quomodo sequentes operationes similes se sint habiturae; id quod facile patebit sumendo statim $n = 1$; tum enim habebitur $p = a + \alpha \cdot 1$ et $q = b + \beta \cdot 1$, ubi manifesto sumere licet $a = 0$ et $b = 0$, quippe quo pacto fiunt $< \frac{1}{2}$; tum vero ob $aa + bb = 0$ utique erit $n' = 0$ atque hic progressio ulterior nostri ratiocinii sponte sistitur.

SCHOLION

Eodem modo demonstrari potest omnes numeros vel huius formae $pp + 2qq$ vel $pp + 3qq$ alios non admittere divisores, nisi qui ipsi sint eiusdem formae, siquidem numeri p et q fuerint primi inter se.[1]) Neque vero hoc ratiocinium ad formas altiores, veluti $pp + 5qq$, $pp + 6qq$, extendi potest, quia tum non amplius sequeretur numerum n' necessario minorem esse quam n. Priorum igitur illorum casuum demonstrationes hic apponamus.

LEMMA 2

7. *Productum ex duobus numeris huius formae $pp + 2qq$ semper est numerus eiusdem formae.*

Si enim tale productum proponatur $(aa + 2bb)(\alpha\alpha + 2\beta\beta)$ et sumatur

$$A = a\alpha + 2b\beta \quad \text{et} \quad B = a\beta - b\alpha,$$

tum utique erit

$$AA + 2BB = (aa + 2bb)(\alpha\alpha + 2\beta\beta).$$

1) Vide ad has formas $pp + 2qq$ et $pp + 3qq$ Commentationes 256 et 272 (indicis Enestroemiani): *Specimen de usu observationum in mathesi pura*, Novi comment. acad. sc. Petrop. 6 (1756/7), 1761, p. 185, et *Supplementum quorundam theorematum arithmeticorum, quae in nonnullis demonstrationibus supponuntur*, Novi comment. acad. sc. Petrop. 8 (1760/1), 1763, p. 105; *Leonhardi Euleri Opera omnia*, series I, vol. 2, p. 459 et 556. F. R.

THEOREMA 2

Si N fuerit divisor numeri $pp + 2qq$ et p et q sint primi inter se, tum etiam ipse numerus N in tali forma continebitur.

DEMONSTRATIO

Hic iterum numeros p et q infra semissem numeri N deprimere licebit et nostra demonstratio sequenti modo procedet.

I. Sit

$$Nn = pp + 2qq,$$

et quia $p < \frac{1}{2}N$ et $q < \frac{1}{2}N$, erit $n < \frac{3}{4}N$. Iam ponatur ut ante

$$p = a + \alpha n \quad \text{et} \quad q = b + \beta n,$$

ubi a et b capi poterunt minores quam $\frac{1}{2}n$, hincque habebitur

$$Nn = aa + 2bb + 2n(a\alpha + 2b\beta) + nn(\alpha\alpha + 2\beta\beta),$$

quae forma per lemma praemissum reducitur ad

$$Nn = aa + 2bb + 2nA + nn(\alpha\alpha + 2\beta\beta).$$

II. Hic igitur primum membrum $aa + 2bb$ factorem habebit n, unde posito

$$aa + 2bb = nn'$$

erit utique $n' < \frac{3}{4}n$. Hoc iam valore substituto et per n diviso fiet

$$N = n' + 2A + n(\alpha\alpha + 2\beta\beta).$$

III. Multiplicetur per n' atque per lemma praemissum habebitur

$$nn'(\alpha\alpha + 2\beta\beta) = (aa + 2bb)(\alpha\alpha + 2\beta\beta) = AA + 2BB,$$

ita ut nunc habeatur

$$Nn' = n'n' + 2n'A + AA + 2BB,$$

quae forma manifesto reducitur ad hanc

$$Nn' = (n' + A)^2 + 2BB,$$

ideoque itidem numerus formae $pp + 2qq$.

IV. Quum ergo sit $n' < n$, simili modo ad producta sequentia pervenire licebit Nn'', Nn''' etc., ita ut numeri n, n', n'', n''' etc. continuo decrescant. Tandem ergo perveniatur necesse est ad formam $N \cdot 1$, ita ut ipse numerus N quoque in eadem forma $pp + 2qq$ contineatur.

LEMMA 3

8. *Productum ex duobus numeris formae* $pp + 3qq$ *semper ad similem formam reduci potest.*

Sit enim tale productum $(aa + 3bb)(\alpha\alpha + 3\beta\beta)$ et capiatur

$$A = a\alpha + 3b\beta \quad \text{et} \quad B = a\beta - b\alpha;$$

manifesto habebitur

$$AA + 3BB = (aa + 3bb)(\alpha\alpha + 3\beta\beta).$$

THEOREMA 3

Si N *fuerit divisor numeri* $pp + 3qq$, *ubi* p *et* q *sint numeri primi inter se, tum ipse numerus* N *ad eandem formam reduci poterit.*

DEMONSTRATIO

Quum iterum spectare liceat $p < \frac{1}{2}N$ et $q < \frac{1}{2}N$, ipsa forma $pp + 3qq$ minor erit quam N^2. Posito ergo

$$pp + 3qq = Nn$$

factor n minor erit quam N, quae quidem reductio ad demonstrationem non est necessaria; ea enim aeque procedet, etiamsi fuerit $n > N$, uti sequitur.

I. Posito iam

$$p = a + \alpha n \quad \text{et} \quad q = b + \beta n$$

hic numeros a et b minores statuere licet quam $\frac{1}{2}n$, saltem non maiores; tum autem erit

$$Nn = aa + 3bb + 2n(a\alpha + 3b\beta) + nn(\alpha\alpha + 3\beta\beta),$$

quae per lemma praemissum fit

$$Nn = aa + 3bb + 2nA + nn(\alpha\alpha + 3\beta\beta).$$

II. Necesse igitur est, ut primum membrum $aa + 3bb$ factorem habeat n; quare posito

$$aa + 3bb = nn'$$

hic numerus n' certe minor erit quam n, saltem non maior; tum vero facta divisione per n prodibit

$$N = n' + 2A + n(\alpha\alpha + 3\beta\beta).$$

III. Multiplicemus iam per n' et postremum membrum

$$nn'(\alpha\alpha + 3\beta\beta) = (aa + 3bb)(\alpha\alpha + 3\beta\beta)$$

per lemma praemissum fit $AA + 3BB$ sicque habebimus

$$Nn' = n'n' + 2n'A + AA + 3BB,$$

quae expressio manifesto reducitur ad hanc

$$Nn' = (n' + A)^2 + 3BB.$$

IV. Quum igitur Nn' iterum sit formae $pp + 3qq$ et $n' < n$, eodem modo continuo progredi licebit ad continuo minora producta Nn'', Nn''' etc., donec tandem ad ultimum $N \cdot 1$ perveniatur; atque adeo demonstratum est fore ipsum numerum N formae $pp + 3qq$.

COROLLARIUM 1

Fundamentum huius demonstrationis ut et praecedentium in hoc consistit, quod a quolibet numero n perveniatur ad alium n' multo minorem, id quod

iis casibus, quibus n est numerus satis magnus, per se est perspicuum. Quin etiam haec ratio eo casu valet, quo $n = 1$; quia enim tum sumi poterit $a = 0$ et $b = 0$, ob $nn' = 0$ utique fiet $n' = 0$.

Interim tamen pro hoc theoremate singularis plane casus occurrit, quando in progressione numerorum n, n', n'' etc. tandem ad binarium pervenitur; qui casus eo maiorem attentionem meretur, quod nusquam alibi occurrat.[1])

COROLLARIUM 2

Pro hoc ergo casu statuamus statim $n = 2$ et manifestum est in formula $pp + 3qq$ utrumque numerum p et q esse debere imparem; utrumque enim parem assumere non licet, quia p et q inter se primi statuuntur. Quare quum hic fieri debeat $p = a + 2\alpha$ et $q = b + 2\beta$, fiet $a = 1$ et $b = 1$ ideoque $aa + 3bb = 4 = nn'$, unde patet etiam n' fore $= 2$, ita ut nulla ulterior diminutio locum habere possit. Quoties ergo hoc evenit, tum non ipse numerus N, sed eius duplum $2N$ erit numerus formae $pp + 3qq$.

COROLLARIUM 3

Hoc eo magis clarum reddetur, si perpendamus formulam $pp + 3qq$, quando ambo numeri p et q sunt impares, non solum esse parem, sed etiam per 4 divisibilem, neque adeo impariter parem umquam esse posse formam $pp + 3qq$. Quoties ergo, uti his casibus usu venit, numerus $2N$ in forma $pp + 3qq$ contineatur, tum N semper erit numerus par eiusque semissis $\frac{1}{2}N$ seu pars quarta ipsius $2N$ in hac forma $pp + 3qq$ continebitur. Quoties enim uterque numerus p et q est impar, tum etiam $\frac{pp+3qq}{4}$ semper est numerus eiusdem formae, idque adeo in integris, quod quidem non tam facile perspicitur. Posito enim $p = 2r + 1$ et $q = 2s + 1$ prodit forma

$$\frac{pp+3qq}{4} = 1 + r + rr + 3s + 3ss,$$

quam generatim neutiquam in integris ad quadratum cum triplo quadrato reducere licet. Sequenti autem modo haec resolutio in genere institui poterit. Observo enim omnia quadrata imparia in hac forma $(4m + 1)^2$ contineri, siquidem pro m etiam numeri negativi admittantur; namque si m sit positivum, quadrata numerorum 1, 5, 9, 13 etc., quorum forma est $4i + 1$, resultant;

1) Confer propositiones 5—7 Commentationis 272 nota p. 224 laudatae. F. R.

sin autem m sit numerus negativus, tum quadrata numerorum 3, 7, 11, 15 etc., quorum forma est $4i - 1$, oriuntur. Iam ponamus

$$pp = (4r+1)^2 \text{ et } qq = (4s+1)^2$$

eritque

$$\frac{pp+3qq}{4} = 1 + 2r + 4rr + 6s + 12ss,$$

quae manifesto ad hanc formam redigitur

$$(1 + r + 3s)^2 + 3(r - s)^2.$$

SCHOLION

His theorematibus praemissis id, quod nobis maxime est propositum, aggrediamur demonstraturi, *quod summae quatuor quadratorum nullos alios divisores admittant, nisi qui ipsi quoque sint summae quatuor quadratorum.* Ad similitudinem autem praecedentium theorematum lemma quoque praemitti oportet.

LEMMA 4

9. *Productum ex duobus pluribusve numeris, qui singuli sunt summae quatuor quadratorum, semper quoque per summam quatuor quadratorum exprimi potest.*

Sit tale productum

$$(aa + bb + cc + dd)(\alpha\alpha + \beta\beta + \gamma\gamma + \delta\delta)$$

et capiatur

$$A = a\alpha + b\beta + c\gamma + d\delta,$$
$$B = a\beta - b\alpha - c\delta + d\gamma,$$
$$C = a\gamma + b\delta - c\alpha - d\beta,$$
$$D = a\delta - b\gamma + c\beta - d\alpha$$

horumque quadratorum summa erit

$$A^2 + B^2 + C^2 + D^2 = (a^2 + b^2 + c^2 + d^2)(\alpha^2 + \beta^2 + \gamma^2 + \delta^2);$$

manifestum enim est singula producta ex binis partibus se mutuo destruere et singula quadrata litterarum latinarum in singula graecarum duci.[1])

1) Vide § 93 Commentationis 242 nota 2 p. 218 laudatae, imprimis notam ibi adiectam. F. R.

THEOREMA 4

Si N fuerit divisor cuiuspiam summae quatuor quadratorum seu formae $pp + qq + rr + ss$, quae quidem singula per N non sint divisibilia, tum N certe erit summa quatuor quadratorum.

DEMONSTRATIO

Non parum iuvabit hic quoque notasse quatuor illas radices p, q, r, s infra semissem numeri propositi N deprimi posse; demonstratio autem sequenti modo procedet.

I. Denotante n quotum ex illa divisione resultantem, ut sit

$$Nn = pp + qq + rr + ss,$$

ubi litterae p, q, r, s ita ad n referantur, ut sit

$$p = a + n\alpha, \quad q = b + n\beta, \quad r = c + n\gamma, \quad s = d + n\delta,$$

evidens omnino est litteras a, b, c, d ita sumi posse, ut $\frac{1}{2}n$ non superent, quandoquidem valores negativi hinc non excluduntur. Sicque formula $aa + bb + cc + dd$ certe minor erit quam nn.

II. His autem valoribus substitutis aequatio nostra erit

$$Nn = aa + bb + cc + dd + 2n(a\alpha + b\beta + c\gamma + d\delta) + nn(\alpha\alpha + \beta\beta + \gamma\gamma + \delta\delta),$$

quae ex lemmate praemisso, ubi posuimus

$$A = a\alpha + b\beta + c\gamma + d\delta,$$

ita contrahitur

$$Nn = aa + bb + cc + dd + 2nA + nn(\alpha\alpha + \beta\beta + \gamma\gamma + \delta\delta).$$

Quia ergo hic pars prima $aa + bb + cc + dd$ factorem habere debet n, statuatur

$$aa + bb + cc + dd = nn'$$

eritque omnino $n' < n$, uti modo ostendimus. Facta ergo divisione per n obtinebimus

$$N = n' + 2A + n(\alpha\alpha + \beta\beta + \gamma\gamma + \delta\delta).$$

III. Multiplicemus nunc per n', et quia $nn' = aa + bb + cc + dd$, habebimus ex lemmate praemisso

$$nn'(\alpha\alpha + \beta\beta + \gamma\gamma + \delta\delta) = A^2 + B^2 + C^2 + D^2,$$

qua forma introducta nostra aequatio erit

$$Nn' = n'n' + 2n'A + A^2 + B^2 + C^2 + D^2,$$

quae manifesto ad haec quatuor quadrata reducitur

$$Nn' = (n' + A)^2 + B^2 + C^2 + D^2.$$

IV. Quatenus igitur hic $n' < n$, eodem modo ad formas continuo minores Nn'', Nn''' etc. pertingere licebit, donec tandem ad formam $N \cdot 1$ perveniatur ideoque numerus propositus N quatuor quadratis aequetur.

COROLLARIUM 1

Hoc ratiocinium iterum levi exceptioni est obnoxium, quando scilicet fuerit $n = 2$ omnesque numeri p, q, r, s impares; tum enim fiet $a = 1$, $b = 1$, $c = 1$ et $d = 1$ hincque $nn' = 4$, ita ut quoque fiat $n' = 2$ sicque non minor quam n. Verum quum hinc numerus $2N$ aequetur summae quatuor quadratorum, aliunde perspicuum est etiam semissem N fore summam quatuor quadratorum, ita ut haec exceptio nihil plane turbare sit censenda.

COROLLARIUM 2

Quo hoc clarius perspiciatur, sint numeri p, q, r, s impares et n numerus par; tum, quia $Nn = pp + qq + rr + ss$, erit

$$\frac{1}{2}Nn = \left(\frac{p+q}{2}\right)^2 + \left(\frac{p-q}{2}\right)^2 + \left(\frac{r+s}{2}\right)^2 + \left(\frac{r-s}{2}\right)^2,$$

quae quatuor quadrata itidem erunt integra; qua reductione uti licebit, quamdiu omnes radices quatuor quadratorum fuerint impares; tum autem exceptio ante memorata sponte concidit.

SCHOLION

Hac demonstratione potissimum theorema illud FERMATIANUM conficitur, quandoquidem altera pars, quae adhuc superest, quod scilicet proposito quo-

cumque numero primo semper summae quatuor quadratorum exhiberi queant per illum divisibiles, a me iam dudum[1]) satis clare est expedita atque adeo nuper a Celeb. LAGRANGE[2]) subtilissima demonstratione est firmata. Ut tamen hoc argumentum penitus conficiam, sequentem demonstrationem admodum facilem hic subiungam.

THEOREMA 5

10. *Proposito quocumque numero primo N non solum quaterna quadrata, verum adeo terna quadrata infinitis modis exhiberi possunt, quorum summa sit divisibilis per istum numerum N neque tamen singula per eum dividi queant.*

DEMONSTRATIO

Respectu numeri N omnes plane numeri in aliqua sequentium formarum continentur

$$\lambda N,\ \lambda N+1,\ \lambda N+2,\ \lambda N+3,\ \ldots\ \lambda N+N-1,$$

quarum numerus est N. Seposita autem prima forma, quae multipla ipsius N continet, circa reliquas, quarum numerus est $N-1$, notandum est quadrata primae formae $\lambda N+1$ et ultimae $\lambda N+N-1$ ad eandem formam $\lambda N+1$ redire, quadrata vero secundae formae $\lambda N+2$ et penultimae $\lambda N+N-2$ ad formam $\lambda N+4$, tertiae vero et antepenultimae ad $\lambda N+9$ redigi, et ita porro, ita ut hae tantum formae

$$\lambda N+1,\quad \lambda N+4,\quad \lambda N+9\quad \text{etc.},$$

quarum numerus est $\frac{1}{2}(N-1)$, quadrata in se complecti queant, quas formas primae classis appellemus et ita designemus

$$\lambda N+a,\quad \lambda N+b,\quad \lambda N+c,\quad \lambda N+d\quad \text{etc.},$$

ita ut litterae a, b, c, d etc. vel ipsa quadrata 1, 4, 9, 16 etc. denotent vel, si numerum N excedant, residua ex divisione restantia. Reliquae vero formae, quarum numerus itidem erit $\frac{1}{2}(N-1)$, hoc modo designentur

$$\lambda N+\alpha,\quad \lambda N+\beta,\quad \lambda N+\gamma,\quad \lambda N+\delta\quad \text{etc.},$$

1) Vide paragraphos 90 et 91 Commentationis 242 nota 2 p. 218 laudatae. F. R.

2) Vide notam 3 p. 218. F. R.

quas formas posterioris classis vocabimus. De his autem geminis classibus tres sequentes proprietates notentur, quas quidem facile demonstrare licet.[1])

I. Productum ex binis numeris primae classis itidem in prima classe continetur, scilicet forma $\lambda N + ab$ in prima classe reperietur; si enim ab maius fuerit quam N, eius loco residuum ex divisione per N facta relictum capi est intelligendum.

II. Numeri primae classis a, b, c, d etc. in quemcumque numerum posterioris classis α, β, γ, δ etc. ducti in classem posteriorem incident.

III. Denique producta ex binis numeris posterioris classis, veluti $\alpha\beta$, in classem primam transferuntur.

His praemissis demonstrabo: Si non darentur terna quadrata, quorum summa divisibilis esset per N, tum maximum absurdum inde esse secuturum. Ad hoc concedamus tantisper adversario nulla dari terna quadrata, quorum summa sit divisibilis per N; multo minus ergo duo talia quadrata dabuntur. Hinc statim sequitur formam $\lambda N - a$ sive, quod eodem redit, $\lambda N + (N - a)$ non in prima classe occurrere; si enim daretur quadratum formae $\lambda N - a$, hoc ad quadratum formae $\lambda N + a$ praeberet summam per N divisibilem, contra hypothesin. Forma igitur $\lambda N - a$ in posteriore classe contineatur necesse est sicque inter litteras α, β, γ, δ etc. reperientur numeri -1, -4, -9 etc. Sit f numerus quicumque primae classis, ita ut dentur quadrata formae $\lambda N + f$; ad quae si addantur quadrata formae $\lambda N + 1$, summa binorum habebit formam $\lambda N + f + 1$. Iam si daretur quadratum formae $\lambda N - f - 1$, haberetur summa trium quadratorum per N divisibilis; quod quum negetur, forma $\lambda N - f - 1$ non in prima classe ideoque in posteriori continebitur; in qua ergo quum reperiantur numeri -1 et $-f-1$, eorum productum $+f+1$ in priori classe occurrat necesse est. Simili modo ostendetur in prima classe quoque occurrere debere numeros

$$f + 2, \quad f + 3, \quad f + 4 \quad \text{etc.};$$

quare sumto $f = 1$ in prima classe occurrerent omnes plane formae

$$\lambda N + 1, \quad \lambda N + 2, \quad \lambda N + 3 \quad \text{etc.}$$

1) Demonstrationes inveniuntur in Commentatione 242 nota 2 p. 218 laudata. F. R.

nullaeque penitus pro classe posteriore relinquerentur. Interim tamen eodem ratiocinio vidimus in classe posteriore occurrere numeros

$$-1, \quad -f-1, \quad -f-2 \quad \text{etc.}$$

ideoque etiam omnes plane formas; quod quum sit maxime absurdum, sequitur falsum esse non dari terna quadrata, quorum summa sit divisibilis per numerum propositum N. Dantur ergo omnino terna multoque magis quaterna huiusmodi quadrata, quorum summa per N erit divisibilis.[1])

COROLLARIUM

Ex hoc theoremate cum praecedente coniuncto manifesto sequitur omnes plane numeros primos esse summas quatuor vel pauciorum quadratorum. Et quum producta ex binis pluribusve huiusmodi numeris eandem naturam sequantur, solidissime evictum est *omnes plane numeros esse summas quatuor quadratorum vel adeo pauciorum.*

SCHOLION

Loco huius propositionis Cel. LAGRANGE theorema multo latius patens in medium attulit et demonstratione munivit ingeniosissima quidem, sed tantopere abstrusa et intellectu difficili, ut nonnisi summa adhibita attentione percipi posset. Demonstravit scilicet proposito quocumque numero primo A semper bina quadrata pp et qq ad illum prima dari posse, ita ut formula $pp - Bqq - C$ per eum numerum primum A fiat divisibilis, quicumque numeri pro litteris B et C accipiantur, dummodo fuerint primi respectu ipsius A. Idem igitur theorema aliquanto latius extensum cum demonstratione longe faciliori et planiori hic subiungam.

THEOREMA 6

11. *Proposito quocumque numero primo N semper terna quadrata xx, yy et zz ad eum prima exhibere licet, ut formula*

$$\lambda xx + \mu yy + \nu zz$$

per numerum illum primum N fiat divisibilis, dummodo isti coefficientes λ, μ et ν ad ipsum N fuerint primi, hoc est, nullus eorum neque evanescat neque ipsi N neque eius multiplo cuipiam fuerit aequalis.

1) Confer § 90 Commentationis 242 nota 2 p. 218 laudatae. F. R.

DEMONSTRATIO

Denotent litterae

$$a,\ b,\ c,\ d \text{ etc.}$$

omnia residua, quae ex divisione quadratorum per numerum primum propositum N facta relinquuntur, quos numeros ante ad classem priorem rettulimus, quorum multitudo est $\frac{1}{2}(N-1)$; in iis scilicet omnes occurrunt numeri quadrati 1, 4, 9, 16 etc. minores quam N, maiorum autem residua illa ex divisione per N resultantia accedunt. Ad eandem vero classem etiam iidem numeri a, b, c, d etc. quovis multiplo numeri N aucti sunt referendi. Omnes autem reliqui numeri minores quam N, quorum numerus itidem est $\frac{1}{2}(N-1)$ quosque *non-residua*[1]) appellare licet, ad classem posteriorem sunt relati et litteris graecis

$$\alpha,\ \beta,\ \gamma,\ \delta \text{ etc.}$$

designentur. Circa hos numeros duplicis generis iam ante [§ 10] notavimus producta ex binis residuis seu classis prioris iterum in eandem classem cadere, veluti ab, ac, bc etc., quatenus scilicet per divisionem infra N deprimuntur, at productum ex residuo in non-residuum in classe posteriore non-residuorum reperiri ac denique producta ex binis non-residuis iterum fore residua. His notatis demonstrationem ita adornabimus, ut ostendamus ingens absurdum esse secuturum, si nulla daretur formula $\lambda xx + \mu yy + \nu zz$ per numerum N divisibilis. Demonstratio autem sequenti modo procedet.

I. Quum omnia quadrata aequentur cuipiam residuo a vel b vel c multiplo quodam numeri N aucto, si daretur talis formula $\lambda xx + \mu yy + \nu zz$ per numerum N divisibilis, ob $xx = \zeta N + a$, $yy = \eta N + b$ et $zz = \vartheta N + c$ foret utique formula $\lambda a + \mu b + \nu c$ per N divisibilis. Quare qui nostrum theorema negaverit, statuere debet nullam dari huiusmodi formulam $\lambda a + \mu b + \nu c$ per N divisibilem.

II. Quum igitur nulla detur huiusmodi formula per N divisibilis, multo minus fieri poterit $= 0$ ideoque ista aequatio $\lambda a = -\mu b - \nu c$ erit impossibilis pariter ac talis aequatio

$$\lambda a = (\zeta N - \mu) b + (\eta N - \nu) c.$$

1) Vide § 16 Commentationis 242 nota 2 p. 218 laudatae. F. R.

Verum quia λ, μ et ν sunt primi ad N, semper coefficientes ζ et η ita accipere licet, ut formulae $\zeta N - \mu$ et $\eta N - \nu$ fiant per λ divisibiles. Ponamus ergo

$$\zeta N - \mu = \lambda m \quad \text{et} \quad \eta N - \nu = \lambda n$$

atque impossibilis quoque erit ista aequatio

$$a = mb + nc.$$

III. Quum igitur ista formula $mb + nc$ non sit aequalis a ideoque in classe resíduorum non reperiatur (secundum mentem scilicet adversarii, qui nostrum theorema negat), necessario in altera classe non-residuorum reperietur; ibidem ergo etiam (quia c unitatem denotare potest) occurret $mb + n$ hincque adeo omnes istae formulae

$$ma + n, \quad mb + n, \quad mc + n, \quad md + n \quad \text{etc.};$$

quae quum omnes a se invicem diversae et numero sint $\frac{1}{2}(N-1)$, his tota classis non-residuorum exhaurietur, quatenus scilicet divisae per N infra N deprimuntur.

IV. In eadem vero etiam classe occurrere debent omnia producta horum numerorum in quemlibet numerum primae classis, veluti d, ducta, quae ergo erunt

$$mad + nd, \quad mbd + nd, \quad mcd + nd \quad \text{etc.}$$

Verum producta ad, bd, cd etc. in priorem classem cadunt ac reperientur inter ipsos numeros a, b, c, d etc.; sicque in altera classe inter non-residua occurrent quoque omnes hae formulae

$$ma + nd, \quad mb + nd, \quad mc + nd \quad \text{etc.},$$

quae praecedentes singulas superant quantitate $n(d-1)$. Hoc discrimen ponatur brevitatis gratia $= \omega$, quod utique ad ipsum divisorem N erit primum, si modo pro d non assumatur unitas, quia $d - 1$ est $< N$ atque etiam numerus n primus ad N.

V. Quodsi igitur in classe non-residuorum contineatur numerus α, ibidem quoque occurret $\alpha + \omega$ atque ob eandem rationem hic numerus iterum incrementum ω accipiens, scilicet $\alpha + 2\omega$, ibi reperiatur necesse est atque ob

eandem rationem etiam numeri $\alpha + 3\omega$, $\alpha + 4\omega$ etc. Omnes igitur termini huius progressionis arithmeticae

$$\alpha, \quad \alpha + \omega, \quad \alpha + 2\omega, \quad \alpha + 3\omega \quad \text{etc.},$$

quatenus scilicet per N divisae infra N deprimuntur, inter non-residua occurrere debebunt.

VI. Quia differentia huius progressionis est ω, numerus scilicet ad N primus, in hac progressione occurrunt termini non solum per N divisibiles, sed etiam insuper omnes, qui per N divisi pro residuis praebent omnes plane numeros 1, 2, 3, 4 etc, nullo excluso.[1]) Quocirca secundum mentem adversarii in classe non-residuorum omnes plane occurrerent numeri 1, 2, 3, 4 etc.; quod quum sit absurdum, opinio adversarii certe est falsa. Scilicet falsum est nullos dari numeros formae

$$\lambda xx + \mu yy + \nu zz,$$

qui sint per N divisibiles. Utique igitur tales numeri dabuntur; atque hoc ipsum est, quod praestare suscepimus.

COROLLARIUM 1

Non solum autem semper tria huiusmodi quadrata xx, yy et zz reperire licet, sed etiam unum eorum, veluti zz, pro lubitu assumere licet, dumne sit per N divisibile. Ita si f denotet numerum pro lubitu datum non divisibilem per N, semper assignare licebit bina quadrata xx et yy, ut formula

$$\lambda xx + \mu yy + \nu ff$$

fiat per N divisibilis. Ad hoc demonstrandum, quicumque fuerit numerus z, semper dabitur eiusmodi numerus v, ut productum vz per N divisum relinquat datum residuum f. Sit enim $vz = \vartheta N + f$ et formula nostra per vv multiplicata, quae utique adhuc divisibilis erit per N, fiet

$$\lambda vvxx + \mu vvyy + \nu(\vartheta\vartheta NN + 2\vartheta Nf + ff),$$

---

1) Vide theorema 1 Commentationis 271 (indicis Enestroemiani): *Theoremata arithmetica nova methodo demonstrata*, Novi comment. acad. sc. Petrop. 8 (1760/1), 1763, p. 74; *Leonhardi Euleri Opera omnia*, series I, vol. 2, p. 531. F. R.

ubi, quia membra $\vartheta\vartheta NN + 2\vartheta Nf$ per N sponte sunt divisibilia, etiam reliqua forma

$$\lambda\nu\nu xx + \mu\nu\nu yy + \nu ff$$

per N divisibilis erit.

COROLLARIUM 2

Quicumque fuerint numeri λ, μ, ν, pro uno eorum semper unitatem aliumve numerum pro lubitu assumere licet. Quia enim per ϑ multiplicando haec formula

$$\vartheta\lambda xx + \vartheta\mu yy + \vartheta\nu zz$$

divisionem per N admittit, loco ϑ eiusmodi numerum assumere licebit, ut productum $\vartheta\lambda$ per N divisum relinquat unitatem; tum autem haec formula

$$xx + \vartheta\mu yy + \vartheta\nu zz$$

etiamnunc per N erit divisibilis. Quin etiam hic loco $\vartheta\mu$ et $\vartheta\nu$ residua ex divisione per N facta oriunda scribere licet hocque modo formulam illi, quam Celeb. LAGRANGE est contemplatus, omnino similem assequimur.

SCHOLION

Ecce ergo demonstrationem omnibus numeris absolutam tandem sumus assecuti theorematis illius notissimi, quod omnes plane numeri sint summae quatuor vel pauciorum quadratorum, quam quidem iam olim FERMATIUS se invenisse est professus, iniuria autem temporum intercidisse etiamnunc maxime est dolendum. Nullum enim plane est dubium, quin FERMATII demonstratio multo simplicior et generalior fuerit, quam istae, quae nunc demum lucem aspexerunt. Quantum enim ex eius monimentis suspicari licet, ex principiis longe diversis demonstrationem suam petiisse videtur, quandoquidem asseverat se ex eodem fonte demonstrasse, quod omnes plane numeri sint summae numerorum vel trium trigonalium vel pauciorum, tum etiam summae quinque pentagonalium aut pauciorum nec non summae sex hexagonalium, et ita porro, a qua generalitate nostra determinatio longissime abest. Atque etiamnunc demonstrationem ignoramus, quod omnis numerus sit summa trium vel pauciorum trigonalium.[1]) Interim tamen circa hoc theorema ob-

1) Id quod primum a C. F. GAUSS demonstratum est. Vide notam 1 p. 145. Vide ibidem notas 2 et 3 atque etiam notam 4 p. 358 voluminis praecedentis. F. R.

servari convenit id tantum in numeris integris esse verum, dum alterum, quod hic demonstravimus, etiam numeros fractos complectitur;[1]) omnes enim istae fractiones $\frac{1}{2}, \frac{3}{2}, \frac{5}{2}, \frac{7}{2}, \frac{9}{2}$ etc. nullo modo in ternos numeros trigonales resolvi se patiuntur sive nullos valores rationales loco x, y, z invenire licet, ut fiat

$$\frac{1}{2} = \frac{xx+x}{2} + \frac{yy+y}{2} + \frac{zz+z}{2};$$

quare, quod maxime mirandum videtur, haec aequatio

$$1 = xx + x + yy + y + zz + z$$

est impossibilis, quicumque etiam numeri fracti pro x, y, z accipiantur.[2])

---

1) Vide Commentationem 242 nota 2 p. 218 laudatam, imprimis theorema 20. F. R.

2) In Novis actis eruditorum hic statim sequitur:

Sequens Theorema attentione Geometrarum haud indignum, et Analysin prorsus singularem postulare videtur:

THEOREMA DEMONSTRANDUM

Si formula differentialis $\frac{(x-1)dx}{lx}$ *ita integretur, ut facto* $x = 0$ *integrale evanescat, tum vero statuatur* $x = 1$, *eius valor aequalis est logarithmo binarii, ubi quidem logarithmi hyperbolici sunt intelligendi.*

Non dubitari potest, quin ab EULERO ipso inserta sit haec propositio, quippe cuius demonstratio inveniatur in EULERI Commentatione 464 (indicis ENESTROEMIANI): *Nova methodus quantitates integrales determinandi,* Novi comment acad. sc. Petrop. **19** (1774), 1775, p. 66; *LEONHARDI EULERI Opera omnia,* series I, vol. 17, p. 421. Vide etiam EULERI Commentationem 475 (indicis ENESTROEMIANI): *Speculationes analyticae*, Novi comment. acad. sc. Petrop. **20** (1775), 1776, p. 59; *LEONHARDI EULERI Opera omnia,* series I, vol. 18, p. 1. F. R.

DEMONSTRATIONES CIRCA RESIDUA EX DIVISIONE POTESTATUM PER NUMEROS PRIMOS RESULTANTIA [1])

Commentatio 449 indicis ENESTROEMIANI
Novi commentarii academiae scientiarum Petropolitanae 18 (1773), 1774, p. 85—135
Summarium ibidem p. 15—17

SUMMARIUM

Continet haec dissertatio varia theoremata, in quibus plures novae veritates ex principiis prorsus singularibus demonstrantur, ad quas per methodos adhuc usitatas vix ullus patere aditus videtur. Placet istorum theorematum praecipua hic ante oculos ponere, quorum uberior evolutio in ipsa dissertatione traditur.

Primum theorema ita se habet. Si P designet numerum primum sitque $x < P$, forma $x^n - 1$ nonnisi n modis per P divisibilis reddi potest; unde problema resultat, quo pro omnibus exponentibus n numerus casuum propriorum quaeritur, quibus formula $x^n - 1$ per P divisibilis reddi queat alios pro x valores non admittendo, nisi qui divisore sint minores. Haec etsi omni fere usu videntur destituta, ideo tamen erant praemittenda, quod viam muniunt demonstrationibus sequentium theorematum; verbi causa si divisor primus sit $P = 2n + 1$ et a radix primitiva, tum progressionis geometricae

$$1, \quad a, \quad a^2, \quad a^3 \quad \text{etc.}$$

terminus a^n residuum praebet $2n$ seu -1. Porro si divisor fuerit numerus quicumque

1) Confer hac cum dissertatione Commentationes 262 et 271 (indicis ENESTROEMIANI): *Theoremata circa residua ex divisione potestatum relicta*, Novi comment. acad. sc. Petrop. 7 (1758/9), 1761, p. 49, et *Theoremata arithmetica nova methodo demonstrata*, Novi comment. acad. sc. Petrop. 8 (1760/1), 1763, p. 74; *LEONHARDI EULERI Opera omnia*, series I, vol. 2, p. 493 et 531. F. R.

primus P, tot dantur radices primitivae, quot reperiuntur numeri ad $P-1$ primi eoque minores, quandoquidem tantum radices divisore minores considerantur. Elegantia imprimis sunt sequentia: Proposito numero primo formae $4n+1$ semper summa duorum quadratorum ad eum primorum exhiberi potest, quae sit per eum divisibilis, atque alterum quidem quadratum pro lubitu accipere licet. Nulla vero summa duorum quadratorum inter se primorum per ullum numerum primum formae $4n-1$ divisibilis existit.

Hisce expeditis Ill. Auctor etiam ad potestates cubicas progreditur, atque si omnes numeri cubici

$$1,\quad 2^3,\quad 3^3,\quad 4^3 \text{ etc.}$$

per numerum quemcumque primum P dividantur, residuorum inde nascentium indolem investigat; et hoc ipsum problema etiam pro potestatibus quartis resolvit; tandem in fine dissertationis sequens subiungitur theorema: Si omnium numerorum potestates exponentis λ, scilicet

$$1,\quad 2^\lambda,\quad 3^\lambda,\quad 4^\lambda,\quad 5^\lambda \text{ etc.},$$

per numerum primum formae $\lambda n+1$ dividantur, multitudo residuorum diversorum erit n ideoque multitudo non-residuorum $=(\lambda-1)n$.

HYPOTHESIS

1. *Si termini progressionis geometricae ab unitate incipientis per numerum primum P dividantur, residua inde nata litteris* $1, \alpha, \beta, \gamma, \delta$ *etc. denotabo hoc modo:*

Progressio geometrica $1,\ a,\ a^2,\ a^3,\ a^4,\ a^5,\ a^6$ etc.

Residua $1,\ \alpha,\ \beta,\ \gamma,\ \delta,\ \varepsilon,\ \zeta$ etc.

CONCLUSIONES

2. Omnia haec residua sunt minora divisore P; quamdiu enim termini progressionis geometricae divisore P sunt minores, residua ipsis sunt aequalia; cum autem divisorem P superant, auferendo ab iis divisorem P, quoties fieri potest, residua tandem ipso P minora relinqui necesse est.

3. Si numerus a sit primus ad divisorem P, hoc est, si neque ipsi sit aequalis neque eius multiplo cuipiam, nulla quoque eius potestas per P erit divisibilis, neque ergo in residuis cyphra umquam occurret.

4. Cum omnia residua sint divisore P minora, multitudo autem numerorum divisore P minorum sit $= P-1$, plura residua diversa occurrere nequeunt quam $P-1$. Quare, cum series residuorum sit infinita, eadem residua in ea saepius recurrere debent.

5. Ex quolibet residuo, veluti ε, sequens ζ facile definitur. Cum enim sit $\varepsilon = a^5 - mP$ et $\zeta = a^6 - nP$, erit $\zeta - a\varepsilon = (ma-n)P$ hincque

$$\zeta = a\varepsilon - (n - ma)P.$$

Quare a producto $a\varepsilon$ auferatur divisor P, quoties fieri potest, ac relinquetur residuum sequens ζ.

6. Respectu numeri primi P omnes numeri in certos ordines distribui possunt ad eundem ordinem referendo omnes eos numeros, qui per P divisi idem relinquunt residuum; hi ergo ordines erunt:

I. $0, P, 2P, 3P, 4P, \ldots mP,$

II. $1, P+1, 2P+1, 3P+1, 4P+1, \ldots mP+1,$

III. $2, P+2, 2P+2, 3P+2, 4P+2, \ldots mP+2,$

IV. $3, P+3, 2P+3, 3P+3, 4P+3, \ldots mP+3$

etc.

7. Pro quolibet ergo numero primo P tot habentur numerorum ordines, quot unitates in numero P continentur, et quilibet ordo determinatur residuo, quod omnibus numeris eius ordinis est commune, hocque residuum in quovis ordine locum occupat primum.

8. Cum cuiusque ordinis natura residuo ipsi proprio determinetur, quilibet cuiusque ordinis numerus eius naturam perinde declarat ac primus, qui ipsum residuum exhibet. Hinc nihil impedit, quominus idem residuum ε per quemlibet alium numerum eiusdem ordinis $mP + \varepsilon$ denotetur.

9. Ita idem residuum ε non solum per numeros positivos $\varepsilon + P$, $\varepsilon + 2P$ etc. indicare licebit, sed etiam per negativos $\varepsilon - P$, $\varepsilon - 2P$ etc. Cum igitur, si ε

sit divisoris P semisse maius, $\varepsilon - P$ eodem sit minus, patet numeros negativos admittendo omnia residua numeris, qui divisoris P semissem non superent, exprimi posse.

OBSERVATIONES

10. Proposito divisore primo P, prout progressionis geometricae radix a constituatur, fieri potest, ut in residuis vel omnes numeri ipso P minores occurrant vel non omnes. Si enim sumatur radix $a = 1$, omnia residua in unitatem abeunt, ac si sumatur $a = P - 1$, series residuorum prodit

$$1,\ P-1,\quad 1,\ P-1,\quad 1,\ P-1 \text{ etc.}$$

vel (§ 9)

$$+1,\quad -1,\ +1,\quad -1,\ +1,\quad -1 \text{ etc.}$$

11. Quod autem interdum omnes numeri divisore P minores in residuis occurrunt, unico exemplo declarasse sufficiat. Sit scilicet $P = 7$ et sumatur radix $a = 3$; habebitur:

Progressio geometrica	1,	3,	3^2,	3^3,	3^4,	3^5,	3^6,	3^7,	3^8,	3^9 etc.
Residua	1,	3,	2,	6,	4,	5,	1,	3,	2,	6 etc.

12. Si pro eodem divisore $P = 7$ radici a alii valores tribuantur, series residuorum se habebunt, ut sequitur:

Progressio geometrica	1,	2,	2^2,	2^3,	2^4,	2^5,	2^6,	2^7,	2^8,	2^9 etc.
Residua	1,	2,	4,	1,	2,	4,	1,	2,	4,	1 etc.
Progressio geometrica	1,	4,	4^2,	4^3,	4^4,	4^5,	4^6,	4^7,	4^8,	4^9 etc.
Residua	1,	4,	2,	1,	4,	2,	1,	4,	2,	1 etc.
Progressio geometrica	1,	5,	5^2,	5^3,	5^4,	5^5,	5^6,	5^7,	5^8,	5^9 etc.
Residua	1,	5,	4,	6,	2,	3,	1,	5,	4,	6 etc.

13. Ut omnes variationes, quae in serie residuorum locum habere possunt, obtineantur, sufficit radici a omnes valores divisore P minores tribuisse;

si enim loco a sumatur $a + P$, ex progressione geometrica

$$1, \quad a + P, \quad (a + P)^2, \quad (a + P)^3, \quad (a + P)^4 \quad \text{etc.}$$

eadem residuorum series recurrit, quae ex progressione geometrica 1, a, a^2, a^3, a^4 etc.

14. Quemadmodum in residuis etiam numeros negativos admittimus (§ 9), ut ea infra semissem divisoris P deprimamus, ita etiam pro radice progressionis geometricae a numeros negativos assumere licet ac tum habebitur:

Progressio geometrica	1,	$-a$,	$+a^2$,	$-a^3$,	$+a^4$,	$-a^5$,	$+a^6$,	$-a^7$ etc.
Residua	1,	$-\alpha$,	β,	$-\gamma$,	δ,	$-\varepsilon$,	ζ,	$-\eta$ etc.

15. Sumta autem radice $-a$ eadem residua oriuntur, ac si radix poneretur $P - a$; unde patet pro casibus, quibus radix a semissem divisoris P superat, residua ex casibus, quibus est $a < \frac{1}{2}P$, facile colligi.

16. Quodsi loco radicis a successive omnes numeri divisore P minores substituantur, series residuorum inde natae vel erunt completae vel incompletae; *completas* scilicet appello, in quibus omnes numeri divisore P minores occurrunt, *incompletas* vero, ubi quidam horum numerorum ex serie residuorum excluduntur.

17. Quoniam vidimus pro quovis divisore P dari eiusmodi valores radicis a, veluti si $a = 1$ et $a = P - 1$, ex quibus series residuorum incompletae resultant, hinc nascitur quaestio, *an semper eiusmodi progressiones geometricae exhiberi queant, unde series residuorum completae oriantur.*

18. Huiusmodi radices progressionis geometricae, quae series residuorum completas producunt, *primitivas* appellabo. Ita supra [§ 11 et 12] vidimus pro divisore $P = 7$ radices primitivas esse 3 et 5. Num autem pro omnibus divisoribus primis dentur radices primitivae, quaestio est altioris indaginis infra decidenda.

LEMMATA

19. *Cum in serie residuorum termini praecedentes tandem recurrere debeant, primus, qui recurrit, semper est unitas.*

DEMONSTRATIO

Ponamus enim aliud quodvis residuum ε ex potestate a^μ natum recurrere, antequam unitas recurrat, idque secunda vice ex potestate $a^{\mu+\nu}$ prodire. Cum igitur sit $\varepsilon = a^\mu - mP$ et $\varepsilon = a^{\mu+\nu} - nP$, erit $a^{\mu+\nu} - a^\mu = (n-m)P$ ideoque $a^\mu(a^\nu - 1)$ multiplum ipsius P; at quia a^μ per numerum primum P dividi nequit (radix enim a divisore P minor ideoque ad eum prima statuitur), necessario alter factor $a^\nu - 1$ per P divisionem admittet hincque potestas a^ν per P divisa unitatem relinquet; quae potestas cum inferior sit quam $a^{\mu+\nu}$, evidens est residuum ε ante recurrere non posse, quam unitas recurrerit.

20. *Statim atque in serie residuorum*

$$1,\ \alpha,\ \beta,\ \gamma,\ \delta \text{ etc.}$$

unitas iterum occurrit, deinceps eadem residua eodem ordine uti ab initio iterum recurrent.

DEMONSTRATIO

Oriatur enim unitas secunda vice ex potestate a^ν ac sequens residuum erit (§ 5) $a \cdot 1 = a$, idem, quod ex secundo termino a nascebatur, ideoque α, post quod denuo sequentur residua β, γ, δ etc. eodem ordine uti ab initio.

21. *Si a sit radix primitiva, eius potestas a^{P-1} per divisorem primum P divisa unitatem relinquet.*

DEMONSTRATIO

Quia a est radix primitiva, in serie residuorum omnes numeri divisore P minores occurrunt, quorum multitudo est $P-1$; ex totidem ergo progressionis geometricae terminis 1, a^1, a^2, a^3 etc., quorum ultimus erit a^{P-2}, oriantur necesse est; sequens ergo terminus a^{P-1} aliquod ex residuis praecedentibus reproducet, quod autem necessario est unitas (§ 19).

22. *Si progressio geometrica*

$$1, \quad a, \quad a^2, \quad a^3, \quad a^4 \quad etc.$$

seriem residuorum incompletam producat, numerus residuorum diversorum erit pars aliquota numeri $P-1$, *hoc est divisoris primi* P *unitate minuti.*

DEMONSTRATIO

Sit numerus residuorum diversorum

$$1, \quad \alpha, \quad \beta, \quad \gamma, \quad \delta \quad \text{etc.}$$

ex hac progressione geometrica natorum $= r$, qui ergo per hypothesin minor est quam $P-1$, ita ut quidam numeri, qui sint

$$\mathfrak{A}, \quad \mathfrak{B}, \quad \mathfrak{C}, \quad \mathfrak{D} \quad \text{etc.}$$

eorumque multitudo $= P-1-r$, ex serie residuorum excludantur. Iam dico, quia $\mathfrak{A}$ in serie residuorum non reperitur, ibidem quoque nec $\alpha\mathfrak{A}$ nec $\beta\mathfrak{A}$ nec $\gamma\mathfrak{A}$ etc. occurrere posse. Si enim $\varepsilon\mathfrak{A}$ esset residuum, quia ε ex certa potestate radicis a, quae sit a^ν, nascitur, loco $\varepsilon\mathfrak{A}$ spectare licet $a^\nu\mathfrak{A}$, unde sequentia residua forent [§ 5] $a^{\nu+1}\mathfrak{A}$, $a^{\nu+2}\mathfrak{A}$, $a^{\nu+3}\mathfrak{A}$ etc. et in genere $a^n\mathfrak{A}$; quia autem datur potestas a^n unitatem relinquens, hoc residuum foret $\mathfrak{A}$ contra hypothesin. Hinc dato uno non-residuo $\mathfrak{A}$ simul dantur r non-residua; quae si nondum multitudinem numerorum $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D}$ etc., quorum numerus est $P-1-r$, exhauriant, de novo r non-residua accedunt, sicque porro, unde numerus $P-1-r$ necessario erit multiplus ipsius r. Sit ergo

$$P-1-r = nr;$$

fiet

$$r = \frac{P-1}{n+1}$$

ac propterea numerus residuorum r semper est pars aliquota numeri $P-1$.

23. *Quicumque valor divisore primo* P *minor radici* a *tribuatur, potestas* a^{P-1} *per* P *divisa unitatem relinquit seu formula* $a^{P-1}-1$ *per* P *erit divisibilis.*[1])

1) Quod est celebre theorema FERMATIANUM. Vide Commentationes 54, 134, 262, 271 voluminis praecedentis. F. R.

DEMONSTRATIO

Sit r numerus omnium residuorum diversorum

$$1, \quad \alpha, \quad \beta, \quad \gamma, \quad \delta \text{ etc.},$$

quae ergo nascuntur ex progressione geometrica

$$1, \quad a, \quad a^2, \quad a^3, \quad a^4, \ldots a^{r-1};$$

sequens igitur potestas a^r unitatem pro residuo habebit eritque forma $a^r - 1$ per divisorem P divisibilis. Quia vero r est pars aliquota numeri $P-1$, illa forma $a^{P-1} - 1$ per hanc $a^r - 1$ erit divisibilis ideoque etiam per ipsum divisorem P.

24. *In serie residuorum*

$$1, \quad \alpha, \quad \beta, \quad \gamma, \quad \delta \text{ etc.},$$

sive fuerit completa sive incompleta, simul producta ex binis, ternis, quaternis etc. hincque etiam singulorum potestates quaecumque, siquidem per divisorem P deprimantur, occurrunt.

DEMONSTRATIO

Si enim potestas a^m residuum relinquat μ et potestas a^n residuum ν, erit $a^m = \cdot\cdot P + \mu$ et $a^n = \cdot\cdot P + \nu$, ubi duo puncta $\cdot\cdot$ loco cuiusvis indicis integri scribo; hincque $a^{m+n} = \cdot\cdot P + \mu\nu$, ita ut potestas a^{m+n} residuum $\mu\nu$ sit relictura. Quare cum productum binorum quorumcumque residuorum in serie residuorum occurrat, propositum est manifestum.

25. *Datis duobus residuis μ et ν in serie residuorum etiam aliquod reperietur ω, ut sit $\nu = \mu\omega$ vel $\nu = \mu\omega - \cdot\cdot P$.*

DEMONSTRATIO

Oriantur enim residua μ et ν a potestatibus a^m et a^n ac sit ω residuum a potestate a^{n-m} vel hac $a^{P-1+n-m}$, si forte fuerit $n < m$, eritque potestatis $a^n = a^m \cdot a^{n-m}$ residuum $= \mu\omega - \cdot\cdot P$ ideoque $\nu = \mu\omega - \cdot\cdot P$.

26. Cum unitas semper in serie residuorum contineatur, cuique residuo μ respondebit ibidem aliud quoddam ω, ut sit $\mu\omega = 1$ seu $\mu\omega = 1 + \cdot\cdot P$. Huiusmodi bina residua *socia* appellabo. Unde patet in omni serie residuorum terminos ita sociatim exhiberi posse, ut bina quaeque sibi sint socia. Hoc tantum notetur unitatem sibi ipsi esse sociam, ac si -1 occurrat, socium quoque ipsi esse aequalem.

27. His praemissis, quae alibi[1]) fusius pertractavi, ad sequentia theoremata progredior, in quibus plures novae veritates ex principiis prorsus singularibus demonstrabuntur, ad quas per methodos adhuc usurpatas accessus nimis difficilis videtur.

THEOREMA

28. *Ut forma* $x^n - 1$ *per numerum primum* P *divisibilis evadat sumendo* $x < P$, *id pluribus quam* n *modis fieri nequit.*

DEMONSTRATIO

A casibus simplicissimis inchoemus ac primo statim manifestum est formam $x^1 - 1$ per numerum primum P unico modo divisibilem esse posse sumendo $x = 1$, cum valores ipsius x divisore P maiores excludantur.

Ut forma $x^2 - 1$ divisionem per numerum primum P admittat, vel $x - 1$ vel $x + 1$ divisionem admittere debet; priori casu fit $x = 1$, posteriori $x = P - 1$; neque ullo alio modo id evenire potest, siquidem casus $x > P$ excluduntur.

Forma $x^3 - 1 = (x - 1)(xx + x + 1)$ per P divisibilis est, primo si $x = 1$, tum vero si $xx + x + 1 = mP$. Quod si eveniat casu $x = a$, etiam casu $x = a^2$ succedet; altiores enim potestates ob $a^3 - 1$ divisibilem per P ideoque residuum ipsius $a^3 = 1$ ad praecedentes reducuntur. Iam vero dico praeter hos tres casus alios dari nullos. Si enim divisio succederet quoque casu $x = b$, ob $aa + a + 1$ et $bb + b + 1$ per P divisibiles differentia $(a - b)(a + b + 1)$ etiam esset divisibilis, hoc est, vel $a - b$ vel $a + b + 1$; prius daret $b = a$, posterius ab $aa + a + 1$ ablatum praeberet $aa - b = mP$, hoc est, $b = aa$, qui sunt casus iam enumerati. Unde pluribus quam tribus modis divisio non succedit.

---

1) Scilicet in Commentatione 262 nota p. 240 laudata. F. R.

Iam pro forma $x^n - 1$ in genere observo, si ea per numerum primum P fuerit divisibilis casu $x = a$, ut sit $x - a$ divisor formae $x^n - 1 - mP$, tum facta divisione oriri formam uno gradu inferiorem per P divisibilem reddendam; quod si praestet valor $x = b$, denuo ad formam inferiorem pervenietur, ex quo perinde atque in resolutione aequationum concluditur pluribus quam n modis quaesitum obtineri non posse; qui, si $x = a$ fuerit unus valor idoneus, erunt

$$x = 1, \quad x = a, \quad x = a^2, \quad x = a^3, \quad x = a^4, \ldots x = a^{n-1},$$

quandoquidem a^n iterum unitati aequivalet.

SCHOLION

29. Theorema hoc ita accipi debet, ut forma $x^n - 1$ certe non pluribus quam n modis per numerum primum P divisibilis reddi queat aliis pro x valoribus non admittendis, nisi qui ipso P sint minores. Cum enim, si quispiam valor $x = a$ id praestet, omnes in hac formula $x = a + mP$ idem sint praestaturi, hos omnes pro unico casu haberi convenit. Hac lege constituta saepius evenire potest, ut numerus casuum sit minor quam exponens n; veluti si quaestio sit, quot casibus forma $x^5 - 1$ per 7 divisibilis exìstat, hoc non quinque, sed unico modo $x = 1$ fieri posse deprehenditur, dum reliqui quatuor casus quasi fiunt imaginarii. Ex sequentibus autem patebit semper quasdam solutiones fieri impossibiles, quoties exponens n non fuerit pars aliquota ipsius $P - 1$, dum contra, quoties n est pars aliquota ipsius $P - 1$, omnes solutiones sunt reales. Ac si $n = P - 1$, tum manifesto totidem habentur solutiones, quia omnes numeri ipso P minores, quorum multitudo est $P - 1$, loco x positi formulam $x^n - 1$ per numerum primum P divisibilem reddunt (§ 23). Quando autem exponens n maior est quam $P - 1$, veluti $n = P - 1 + k$, tum forma $x^{P-1+k} - 1$ reducitur ad $x^k - 1$, quoniam potestas x^{P-1} ratione residuorum unitati aequivalere est censenda.

DEFINITIO

30. *Casus proprii, quibus formula* $x^n - 1$ *per quempiam numerum primum divisibilis esse potest, sunt ii, qui ipsi cum nulla forma inferiori, ubi exponens* n *est minor, sunt communes.*

COROLLARIUM 1

31. Quia casus $x = 1$ formulae $x^n - 1$ cum omnibus inferioribus est communis, hunc semper a casibus formulae isti propriis excludi oportet; unde, cum numerus omnium casuum sit n[1]), numerus casuum propriorum saltem unitate est minor.

COROLLARIUM 2

32. Si exponens n fuerit numerus primus, formula $x^n - 1$ per nullam inferiorem eiusdem formae divisibilis est praeter $x^1 - 1$; unde numerus casuum propriorum est $n - 1$.[1])

COROLLARIUM 3

33. Sin autem exponens n fuerit numerus compositus, puta $n = \mu\nu$, tum formula $x^n - 1$ iisdem casibus est divisibilis, quibus formulae $x^\mu - 1$ et $x^\nu - 1$, quandoquidem ipsa per has divisibilis existit; unde casus harum formularum a casibus propriis formulae $x^n - 1$ sunt segregandi.

PROBLEMA

34. *Pro omnibus exponentibus n numerum casuum propriorum definire, quibus formula* $x^n - 1$ *per quempiam numerum primum P divisibilis reddi potest, alios pro x valores non admittendo, nisi qui divisore sint minores.*

SOLUTIO

A numero omnium casuum, qui est $= n$, excludantur casus, quibus formulae inferiores in proposita contentae simul fiunt divisibiles; aliae autem formulae inferiores, veluti $x^\nu - 1$, in proposita $x^n - 1$ non continentur, nisi quarum exponens ν est pars aliquota exponentis n. Verum si plures huiusmodi formulae inferiores dentur, ne iidem casus bis vel pluries excludantur, tantum casus cuique proprii excludi debent, quo facto remanebunt casus formulae propositae $x^n - 1$ proprii; hoc modo ab exponentibus minoribus ad continuo maiores facile progredi licet:

---

1) Observandum quidem est hoc tantum demonstratum esse numerum omnium casuum non esse maiorem quam n. Vide C. F. Gauss, *Disquisitiones arithmeticae*, Lipsiae 1801, art. 56; *C. F. Gauss Werke*, I, p. 46. F. R.

Formula	Numerus casuum propriorum
$x^1 - 1$	1
$x^2 - 1$	$2 - 1 = 1$
$x^3 - 1$	$3 - 1 = 2$
$x^4 - 1$	$4 - 1 - 1 = 2$
$x^5 - 1$	$5 - 1 = 4$
$x^6 - 1$	$6 - 2 - 1 - 1 = 2$
$x^7 - 1$	$7 - 1 = 6$
$x^8 - 1$	$8 - 2 - 1 - 1 = 4$
$x^9 - 1$	$9 - 2 - 1 = 6$

etc.

Hinc in genere si α, β, γ, δ etc. sint numeri primi, res ita se habebit:

Formula	Numerus casuum propriorum
$x^1 - 1$	1
$x^\alpha - 1$	$\alpha - 1$
$x^\beta - 1$	$\beta - 1$
$x^\gamma - 1$	$\gamma - 1$
$x^{\alpha\alpha} - 1$	$\alpha\alpha - \alpha = \alpha(\alpha - 1)$
$x^{\alpha\beta} - 1$	$\alpha\beta - \alpha - \beta + 1 = (\alpha - 1)(\beta - 1)$
$x^{\beta\beta} - 1$	$\beta\beta - \beta = \beta(\beta - 1)$
$x^{\alpha\gamma} - 1$	$\alpha\gamma - \alpha - \gamma + 1 = (\alpha - 1)(\gamma - 1)$
$x^{\beta\gamma} - 1$	$\beta\gamma - \beta - \gamma + 1 = (\beta - 1)(\gamma - 1)$
$x^{\gamma\gamma} - 1$	$\gamma\gamma - \gamma = \gamma(\gamma - 1)$
$x^{\alpha\alpha\alpha} - 1$	$\alpha^3 - \alpha\alpha + \alpha - \alpha + 1 - 1 = \alpha\alpha(\alpha - 1)$
$x^{\alpha\alpha\beta} - 1$	$\alpha\alpha\beta - \alpha\alpha + \alpha - (\alpha - 1)(\beta - 1) - \alpha - \beta + 1 = \alpha(\alpha - 1)(\beta - 1)$

Unde colligimus, si fuerit

$$n = \alpha^\lambda \beta^\mu \gamma^\nu,$$

pro formula $x^n - 1$ fore numerum casuum propriorum

$$\alpha^{\lambda-1}(\alpha - 1) \cdot \beta^{\mu-1}(\beta - 1) \cdot \gamma^{\nu-1}(\gamma - 1).$$

Quae si attentius contemplemur, mox deprehendemus pro qualibet formula $x^n - 1$ tot dari casus proprios, quot infra exponentem n dantur numeri ad ipsum primi.[1])

COROLLARIUM 1

35. Divisore primo existente $= P$ si exponens n sumatur $= P - 1$, quia formula $x^{P-1} - 1$ certo habet $P - 1$ casus eosque omnes reales, cum x omnes valores ipso P minores recipere queat [§ 23], si inde expungantur ii, qui huic formulae cum simplicioribus sunt communes, casus proprii, qui relinquuntur, omnes certo erunt reales.[2])

COROLLARIUM 2

36. Hinc semper eiusmodi dantur numeri divisore P minores, qui casus formulae $x^{P-1} - 1$ proprios exhibent, ita ut iidem casus nulli formulae inferiori conveniant.

SCHOLION

37. Quamvis haec nimis abstracta et omni usu destituta videantur, tamen equidem iis supersedere non potui in sequentibus demonstrationibus adornandis, ubi imprimis ante omnia est ostendendum, quicumque numerus primus pro divisore P accipiatur, semper eiusmodi progressiones geometricas 1, a, a^2, a^3, a^4 etc. exhiberi posse, unde series residuorum completae resultent, in quibus scilicet omnes numeri divisore P minores occurrant, antequam idem residuorum ordo revertatur. Plerisque[3]) forte haec res ita manifesta videbitur, ut demonstratione non egeat, cum pro minoribus divisoribus primis huiusmodi progressiones geometricae series residuorum completas praebentes actu exhiberi queant, pro maioribus autem ratio dubitandi continuo decrescere videatur. Verum quoniam hoc secus evenit pro divisoribus non-primis, haec numerorum primorum proprietas utique demonstrationem postulare est visa.

---

1) Vide Commentationem 271 nota p. 240 laudatam. F. R.

2) Ubi notasse iuvabit ea, quae C. F. Gauss paragrapho 31 opposuit (vide notam p. 250), ob theorema Fermatianum pro formula x^{P-1} non valere. F. R.

3) Vide exempli gratia I. H. Lambert, *Adnotata quaedam de numeris eorumque Anatomia,* Nova acta eruditorum, 1769, p. 107, imprimis p. 127—128. F. R.

THEOREMA

38. *Quicumque numerus primus pro divisore P accipiatur, semper eiusmodi progressio geometrica*

$$1,\ a,\ a^2,\ a^3,\ a^4 \text{ etc.}$$

exhiberi potest, ex qua series residuorum completa oriatur.

DEMONSTRATIO

Cum posita in genere progressionis geometricae radice x minore semper quam divisor P terminus x^{P-1} per P divisus unitatem relinquat indeque residua eodem ordine uti ab initio revertantur, ostendi oportet pro x eiusmodi numerum a assumi posse, ut a^{P-1} sit eius infima potestas, quae per P divisa unitatem relinquat; quia enim tum in serie residuorum unitas ante hunc terminum non occurrit, omnia antecedentia residua inter se diversa sint necesse est; quorum numerus cum sit $= P-1$, omnes numeri divisore P minores in serie residuorum reperientur eaque propterea erit completa. Res itaque huc redit, ut ostendatur non omnes numeros divisore P minores ita esse comparatos, ut eorum inferior quaepiam potestas per P divisa unitatem relinquat. Verum si hoc eveniat in potestate x^n existente $n < P-1$, iam ostendimus (§ 22) eius exponentem n esse necessario partem aliquotam ipsius $P-1$; cum iam § 34—36 docuerim formam $x^{P-1}-1$ semper habere casus sibi proprios, puta $x = a$, ut nulla inferior divisionem per P admittat, perspicuum est potestatem a^{P-1} fore infimam, quae per P divisa unitatem relinquat; unde sumto tali numero a pro radice progressionis geometricae ex ea series residuorum completa oriatur necesse est.

SCHOLION

39. Quo haec clarius intelligantur, conveniet pro simplicioribus divisoribus primis tales series residuorum completas conspectui exponi, ubi quidem progressiones geometricas, unde nascuntur, non opus est exponi, quia radix semper secundo termino seriei residuorum est aequalis, sed sufficiet generalem progressionem in capite posuisse, ut inde exponentes, quibus singuli termini in seriebus residuorum respondent, perspiciantur:

Divisor primus	$a^0, a^1, a^2, a^3, a^4, a^5, a^6, a^7, a^8, a^9, a^{10}, a^{11}, a^{12}, a^{13}, a^{14}, a^{15}, a^{16}, a^{17}, a^{18}, a^{19}, a^{20}, a^{21}$ etc.
3	1, 2 | 1, 2 | 1, 2 | 1, 2 | 1, 2 | 1, 2 | 1, 2 | 1, 2 | 1, 2 | 1, 2 | 1, 2 etc.
5	1, 2, 4, 3 | 1, 2, 4, 3 | 1, 2, 4, 3 | 1, 2, 4, 3 | 1, 2, 4, 3 | 1, 2 etc.
7	1, 3, 2, 6, 4, 5 | 1, 3, 2, 6, 4, 5 | 1, 3, 2, 6, 4, 5 | 1, 3, 2, 6 etc.
11	1, 2, 4, 8, 5, 10, 9, 7, 3, 6 | 1, 2, 4, 8, 5, 10, 9, 7, 3, 6 | 1, 2 etc.
13	1, 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7 | 1, 2, 4, 8, 3, 6, 12, 11, 9, 5 etc.
17	1, 3, 9, 10, 13, 5, 15, 11, 16, 14, 8, 7, 4, 12, 2, 6 | 1, 3, 9, 10, 13, 5 etc.
19	1, 2, 4, 8, 16, 13, 7, 14, 9, 18, 17, 15, 11, 3, 6, 12, 5, 10 | 1, 2, 4, 8 etc.
23	1, 5, 2, 10, 4, 20, 8, 17, 16, 11, 9, 22, 18, 21, 13, 19, 3, 15, 6, 7, 12, 14 | etc.

Radices igitur, quibus hic pro istis divisoribus primis sumus usi, sunt primitivae, quia earum potestates omnia diversa residua divisore minora suppeditant, quibus exhaustis demum unitas recurrit et series eodem ordine uti ab initio progrediuntur. Via quidem adhuc non patet tales radices primitivas pro quovis divisore primo inveniendi neque etiam demonstratio, qua tales radices primitivas semper dari evici, methodum eas inveniendi declarat. Pro quovis autem divisore primo radix huiusmodi primitiva tentando non difficulter elicitur. Veluti pro divisore 23 primum radicem $a = 2$ assumo, unde haec series residuorum nascitur

$$1,\ 2,\ 4,\ 8,\ 16,\ 9,\ 18,\ 13,\ 3,\ 6,\ 12,\ 1;$$

quae cum sit incompleta, iam inde patet radicem primitivam inter numeros exclusos quaeri debere, quorum minimus 5 negotium conficere deprehenditur; nisi hoc accidisset, denuo inter numeros exclusos radicem primitivam quaesivissem.

THEOREMA

40. *Si divisor primus sit* $P = 2n + 1$ *et* a *radix primitiva, tum progressionis geometricae*

$$1,\ a,\ a^2,\ a^3 \text{ etc.}$$

terminus a^n *residuum praebet* $2n$ *seu* -1.

DEMONSTRATIO

Cum a sit radix primitiva, eius potestas a^{2n} per divisorem $2n+1$ divisa unitatem relinquit neque ulla datur potestas inferior idem praestans; formula ergo $a^{2n}-1$ per eundem divisorem erit divisibilis neque ulla alia inferior. Cum igitur sit $a^{2n}-1=(a^n-1)(a^n+1)$ et factor a^n-1 non sit per divisorem $2n+1$ divisibilis, alterum factorem a^n+1 divisibilem esse necesse est seu erit $a^n+1=m(2n+1)$ hincque

$$a^n=m(2n+1)-1 \quad \text{vel} \quad a^n=(m-1)(2n+1)+2n;$$

unde manifestum est potestatem a^n per divisorem $2n+1$ divisam relinquere -1 seu $2n$.

COROLLARIUM 1

41. Si ergo residua ex initio progressionis geometricae $1, a, a^2, a^3$ etc. nata sint

$$1,\ \alpha,\ \beta,\ \gamma \text{ etc.},$$

residua ex terminis $a^n, a^{n+1}, a^{n+2}, a^{n+3}$ etc. nata erunt

$$-1,\ -\alpha,\ -\beta,\ -\gamma \text{ etc.}$$

seu

$$2n,\ 2n+1-\alpha,\ 2n+1-\beta,\ 2n+1-\gamma \text{ etc.},$$

cum sit [§ 5] $\alpha=a$, $\beta=a\alpha$, $\gamma=a\beta$ etc. semperque sequens terminus oriatur ex praecedente per radicem a multiplicato.

COROLLARIUM 2

42. Series ergo residuorum completa, cuius terminorum numerus est $=2n$, antequam iidem termini recurrant, in duas partes dispescitur

$$1,\ \alpha,\ \beta,\ \gamma,\ \delta \text{ etc.}$$

et

$$-1,\ -\alpha,\ -\beta,\ -\gamma,\ -\delta \text{ etc.},$$

cuius posterioris termini sunt complementa[1]) terminorum prioris; seu residua ex terminis a^λ et $a^{n+\lambda}$ nata simul sumta sunt $=0$ sive divisorem $2n+1$ praebent.

1) Confer § 55 Commentationis 242 nota 2 p. 218 laudatae. F. R.

SCHOLION

43. Quae de binis residuis sociis supra [§ 26] sunt observata, quorum productum unitate superat multiplum divisoris, ea hic ita sunt disposita, ut a medio, quod est -1 vel $2n$, aequidistent. Si enim r et s sint residua ex potestatibus $a^{n+\nu}$ et $a^{n-\nu}$ nata, productum rs erit residuum ex potestate a^{2n} natum; quod cum sit unitas, erit $rs = 1$ vel $1 + m(2n+1)$. Ipsum autem residuum medium -1 seu $2n$ sibi ipsum est socium, omnino uti primum $+1$ se ipsum habet pro socio. Reliqua residua sociata omnia sunt inaequalia et quocumque proposito r alterum sibi socium s erit $= \frac{1+m(2n+1)}{r}$; semper enim m ita definire licet, ut $m(2n+1)+1$ per r divisionem admittat, siquidem, uti assumimus, $2n+1$ fuerit numerus primus et r numerus ipso minor vel saltem ad eum primus. Quemadmodum autem in nostra serie residua sunt disposita, cuiusque socium expedite reperitur, cum ambo a medio -1 aequidistent.

THEOREMA

44. *Si divisor fuerit numerus quicumque primus P, tot dantur radices primitivae, quot reperiuntur numeri ad $P-1$ primi eoque minores, quandoquidem tantum radices divisore minores consideramus.*

DEMONSTRATIO

Ponamus $P-1 = Q$, et cum certe detur radix primitiva [§ 38], sit ea $= a$, ita ut a^Q sit minima potestas ipsius a per P divisa unitatem relinquens. Tum vero sit n numerus quicumque primus ad Q ac potestas a^n per divisorem P divisa relinquat residuum b, quod utique ab a erit diversum; eritque b itidem radix primitiva seu, quod eodem redit, ipsa potestas a^n uti radix primitiva spectari potest. Ad quod demonstrandum ostendi debet in progressione geometrica

$$1,\ a^n,\ a^{2n},\ a^{3n},\ \ldots\ a^{Qn}$$

ante terminum a^{Qn} nullum occurrere, qui per P divisus unitatem relinquat. Iam quia a est radix primitiva, nullae aliae eius potestates per P divisae unitatem relinquunt, nisi quarum exponentes sint vel Q vel $2Q$ vel $3Q$ vel multiplum quodcumque ipsius Q, unde quidem manifestum est potestatem a^{Qn}

unitatem relinquere. Simul vero patet, quia numerus n ad Q est primus, nullum multiplum ipsius n minus quam Qn simul esse multiplum ipsius Q; si enim mn existente $m < Q$ esset multiplum ipsius Q, puta $= kQ$, ob $mn = kQ$ foret $n : Q = k : m$ ideoque numeri n et Q non forent inter se primi. Quare cum in superiori progressione geometrica ante terminum a^{Qn} nullus alius occurrat, qui per divisorem P divisus unitatem relinquat, series residuorum inde nata Q terminos diversos complectetur eritque propterea completa et a^n seu residuum inde natum b erit radix primitiva. Cum igitur ex quolibet numero n ad Q seu $P-1$ primo obtineatur radix primitiva, admissa una saltem primitiva a manifestum est semper tot dari radices primitivas, quot dantur numeri ad numerum $Q = P-1$ primi eoque minores, quandoquidem radices maiores ab hac consideratione excludimus.

COROLLARIUM 1

45. Pro divisore ergo $P = 3$ et $Q = 2$ unica datur radix primitiva 2 ex potestate a^1 nata; pro divisore $P = 5$ et $Q = 4$ duae dantur 2 et 3 ex potestatibus a^1 et a^3 natae. Pro divisore $P = 7$ et $Q = 6$ iterum duae dantur 3 et 5 ex potestatibus a^1 et a^5 natae. Pro divisore $P = 11$ et $Q = 10$, ad quem numerum Q primi sunt 1, 3, 7, 9, radices primitivae sunt 2, 8, 7, 6 ex potestatibus a^1, a^3, a^7, a^9 natae, uti ex seriebus residuorum completis § 39 allatis perspicitur.

COROLLARIUM 2

46. Pro quovis ergo divisore primo P multitudo radicum primitivarum multitudini numerorum ad numerum $Q = P-1$ primorum eoque minorum est aequalis ideoque ex compositione numeri Q est iudicanda. Ita si fuerit

$$Q = \alpha^\lambda \beta^\mu \gamma^\nu \text{ etc.}$$

existentibus α, β, γ etc. numeris primis, constat numerum radicum primitivarum fore

$$= \alpha^{\lambda-1}(\alpha-1) \cdot \beta^{\mu-1}(\beta-1) \cdot \gamma^{\nu-1}(\gamma-1) \cdot \text{etc.}$$

COROLLARIUM 3

47. Ipsi autem numeri ad Q primi facile reperiuntur, dum ex numeris omnibus ipso Q minoribus expunguntur ii, qui ad Q sunt compositi; qui enim restant, inter quos semper unitas reperitur, erunt ad Q primi.

SCHOLION

48. Ex data theorematis demonstratione autem simul intelligitur plures non dari radices primitivas, quam assignavimus. Sumta enim quacumque alia potestate radicis primitivae iam cognitae a, puta a^m, cuius exponens m non sit primus ad Q, sed cum Q communem habeat divisorem, qui sit d, ut tam $\frac{Q}{d}$ quam $\frac{m}{d}$ sit numerus integer, in progressione geometrica $1, a^m, a^{2m}, a^{3m}, a^{4m}$ etc. occurret potestas, cuius scilicet exponens $= \frac{Q}{d} m$, antequam ad a^{Qm} perveniatur; qui cum sit quoque $= \frac{m}{d} Q$ ideoque multiplum ipsius Q, ex ea potestate iam orietur residuum 1 ac propterea series residuorum prodibit incompleta. Talis ergo potestas a^m seu residuum inde resultans certe non erit radix primitiva.

COROLLARIUM 4

49. Si residuum r praebeat radicem primitivam, etiam eius socium s dabit radicem primitivam. Posito enim divisore primo $P = 2n + 1$, ut sit $Q = 2n$, sit $a^{n-\lambda}$ potestas praebens residuum r et socium s resultat ex potestate $a^{n+\lambda}$. Evidens autem est, si $n - \lambda$ fuerit ad $Q = 2n$ primus, tum etiam exponentem alterum $n + \lambda$ fore ad Q primum.

SCHOLION

50. Haud abs re fore arbitror, si pro simplicioribus divisoribus primis P tam numeros ad $Q = P - 1$ primos quam radices primitivas iis respondentes conspectui exposuero:

Divisor primus	
3	1 ad 2 primus 2 radix primitiva
5	1, 3 primi ad 4 2, 3 radices primitivae
7	1, 5 primi ad 6 3, 5 radices primitivae
11	1, 3, 7, 9 primi ad 10 2, 8, 7, 6 radices primitivae
13	1, 5, 7, 11 primi ad 12 2, 6, 11, 7 radices primitivae
17	1, 3, 5, 7, 9, 11, 13, 15 primi ad 16 3, 10, 5, 11, 14, 7, 12, 6 radices primitivae
19	1, 5, 7, 11, 13, 17 primi ad 18 2, 13, 14, 15, 3, 10 radices primitivae
23	1, 3, 5, 7, 9, 13, 15, 17, 19, 21 primi ad 22 5, 10, 20, 17, 11, 21, 19, 15, 7, 14 radices primitivae[1])
29	1, 3, 5, 9, 11, 13, 15, 17, 19, 23, 25, 27 primi ad 28 2, 8, 3, 19, 18, 14, 27, 21, 26, 10, 11, 15 radices primitivae
31	1, 7, 11, 13, 17, 19, 23, 29 primi ad 30 3, 17, 13, 24, 22, 12, 11, 21 radices primitivae
37	1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35 primi ad 36 2, 32, 17, 13, 15, 18, 35, 5, 20, 24, 22, 19 radices primitivae

Nullam autem hic inter quemque numerum primum et radices primitivas ipsi convenientes relationem deprehendere licet, ex qua pro quovis divisore primo saltem unica radix primitiva colligi posset; atque adeo ordo inter istas radices aeque absconditus videtur ac inter ipsos numeros primos.

1) Editio princeps (atque etiam *Comment. arithm.*): *13* (loco 19). Correxit F. R.

THEOREMA

51. *Si numeri quadrati per quempiam divisorem primum P dividantur, residua inde orta, nisi sint* 0, *in serie residuorum completa potestatibus parium exponentium respondent.*

DEMONSTRATIO

Sit pro divisore primo P radix quaedam primitiva a, ut haec progressio geometrica

$$1,\ a,\ a^2,\ a^3,\ a^4,\ a^5,\ a^6,\ a^7 \text{ etc.}$$

seriem residuorum completam praebeat, in qua omnes numeri divisore minores occurrant. Sit iam xx quadratum quodcumque per P dividendum et r residuum ex divisione radicis x ortum, ut sit $x = mP + r$; ac si $r = 0$ seu x multiplum divisoris P, etiam residuum ex quadrato xx natum erit $= 0$, quos casus, cum per se sint perspicui, hic non consideramus. At si r sit numerus quicumque divisore P minor, quia in serie residuorum completa certe continetur, ex certa quadam potestate ipsius a, quae sit a^λ, nascatur necesse est; tum autem residuum ex divisione quadrati xx oriundum conveniet cum eo, quod ex divisione potestatis $a^{2\lambda}$ nascitur, sicque ex divisione quadratorum alia residua resultare nequeunt, nisi quae ex potestatibus formae $a^{2\lambda}$, hoc est, quarum exponentes sunt numeri pares, oriuntur.

COROLLARIUM 1

52. Residua ergo, quae ex divisione quadratorum per divisorem primum P nascuntur, convenient cum iis residuis, quae ex hac progressione geometrica nascuntur

$$1,\ a^2,\ a^4,\ a^6,\ a^8,\ a^{10},\ a^{12} \text{ etc.}$$

existente a radice primitiva.

COROLLARIUM 2

53. Si ergo divisor primus sit $P = 2n + 1$, quam formam omnes numeri primi praeter binarium habent, quia 2 non est numerus primus ad $P - 1 = 2n$, etiam a^2 non erit radix primitiva ideoque series residuorum ex quadratis oriunda non erit completa.

COROLLARIUM 3

54. Quia autem a^{2n} est minima potestas radicis a unitatem relinquens, multitudo residuorum, quae ex numeris quadratis resultare possunt, certo est $= n$ cyphra exclusa totidemque numeri numquam possunt esse residua quadratorum, quos proinde *non-residua* appellavi.[1])

SCHOLION 1

55. Hoc etiam ex serie residuorum completa facillime perspicitur; quae si progressioni geometricae subscripta fuerint

$$1,\ a,\ a^2,\ a^3,\ a^4,\ a^5,\ a^6,\ a^7,\ \ldots\ a^{2n}$$

$$1,\ \alpha,\ \beta,\ \gamma,\ \delta,\ \varepsilon,\ \zeta,\ \eta,\ \ldots\ 1,$$

ex divisione quadratorum nascitur haec series residuorum

$$1,\ \beta,\ \delta,\ \zeta,\ \ldots\ 1,$$

quorum multitudo manifesto est semissis illorum, quoniam serie etiam continuata eadem eodem ordine recurrunt.

Hinc uti residua quadratorum sunt 1, β, δ, ζ etc., ita non-residua erunt α, γ, ε, η etc. numero totidem, nisi scilicet binarius pro divisore primo accipiatur. Quare cum ex serie quadratorum 1, 4, 9, 16 usque ad $4nn$ continuata omnia residua diversa oriri debeant horumque quadratorum numerus sit $2n$, residuorum vero numerus tantum $= n$, necesse est ex binis horum quadratorum aequalia residua nasci, quod adeo per se est perspicuum, cum quadrata bb et $(2n + 1 - b)^2$ per divisorem $2n + 1$ divisa idem residuum relinquant.

SCHOLION 2

56. Simili modo ostendi potest residua, quae ex divisione cuborum nascuntur, non discrepare ab iis, quae progressioni geometricae

$$1,\ a^3,\ a^6,\ a^9,\ a^{12}\ \text{etc.}$$

1) Vide § 16 Commentationis 242 nota 2 p. 218 laudatae. F. R.

conveniunt denotante a semper radicem primitivam. Atque in genere si potestates numerorum quaecumque

$$1,\ 2^\lambda,\ 3^\lambda,\ 4^\lambda,\ 5^\lambda,\ 6^\lambda,\ 7^\lambda \text{ etc.}$$

per numerum primum P dividantur, residua inde oriunda eadem erunt atque ea, quae ex hac progressione geometrica nascuntur

$$1,\ a^\lambda,\ a^{2\lambda},\ a^{3\lambda},\ a^{4\lambda},\ a^{5\lambda},\ a^{6\lambda} \text{ etc.}$$

existente a radice primitiva pro divisore primo P; unde patet, si exponens λ fuerit numerus ad $P-1$ primus, seriem residuorum fore completam; at si exponens λ ad $P-1$ non sit primus ac maximus eorum communis divisor fuerit $=d$, tum utique in residuis non omnes numeri occurrent, sed tot tantum, ut eorum multitudo sit $=\frac{P-1}{d}$, cuius ratio ex hactenus allatis satis est manifesta. Sed antequam altiores potestates accuratius scrutemur, quasdam insignes proprietates circa residua quadratorum explicasse iuvabit.

THEOREMA

57. *Divisore primo posito* $P=2n+1$ *in residuis quadratorum occurret numerus* -1 *seu* $2n$, *quoties* n *fuerit numerus par; sin autem* n *sit numerus impar, tum* -1 *seu* $2n$ *certe non reperietur in residuis, sed erit non-residuum.*[1])

DEMONSTRATIO

Cum progressio geometrica $1,\ a^2,\ a^4,\ a^6,\ a^8$ etc. omnia producat residua quadratorum, evidens est in ea occurrere terminum a^n, siquidem n sit numerus par; at supra [§ 40] vidimus potestatem a^n semper dare residuum -1 seu $2n$, ex quo manifestum est, quoties n fuerit numerus par, toties in residuis quadratorum reperiri -1 seu $2n$; contra vero, si n fuerit impar, $2n$ seu -1 erit non-residuum.

---

1) Vide ad hoc theorema § 55—65 atque imprimis § 84 Commentationis 242 nota 2 p. 218 laudatae. Sed vide etiam theoremata 4 et 5 Commentationis 552 huius voluminis. F. R.

COROLLARIUM 1

58. Pro omnibus ergo divisoribus primis formae $4n+1$ in residuis quadratorum certe occurrit -1 seu $4n$, et cum productum ex binis residuis iterum sit residuum, si residuum quodcumque fuerit α, etiam $-\alpha$ in residuis reperietur; scilicet cuiusque residui complementum quoque est residuum.

COROLLARIUM 2

59. Pro divisoribus autem primis formae $4n-1$ in residuis quadratorum certe non occurrit -1, sed erit non-residuum; hinc, cum productum ex residuo et non-residuo semper sit non-residuum, omnium residuorum complementa erunt non-residua.

THEOREMA

60. *Proposito numero primo formae* $4n+1$ *semper summa duorum quadratorum ad eum primorum exhiberi potest, quae sit per eum divisibilis, atque alterum quidem quadratum pro lubitu accipere licet.*[1])

DEMONSTRATIO

Sumto enim quadrato quocumque bb, quod per $4n+1$ divisum relinquat residuum β, dabitur semper aliud quadratum xx, quod per $4n+1$ divisum relinquet residuum $-\beta$ seu $4n+1-\beta$, ex quo summa horum duorum quadratorum $bb+xx$ per numerum primum $4n+1$ divisibilis sit necesse est; et cum neutrum per se divisionem admittat, ea utique ad $4n+1$ erunt prima.

COROLLARIUM 1

61. Evidens quoque est quadratum xx infinitis modis accipi posse, cum omnia quadrata in hac forma $(m(4n+1)\pm x)^2$ [contenta] idem residuum, quod xx, praebeant; unde pro x dabitur valor non solum minor quam $4n+1$, sed etiam minor eius semisse $\frac{4n+1}{2}$ seu minor quam $2n+1$.

---

1) Confer theorema 16 atque iterum § 84 Commentationis 242 nota 2 p. 218 laudatae. F. R.

COROLLARIUM 2

62. Semper ergo tales summae binorum quadratorum

$$1 + pp, \quad 4 + qq, \quad 9 + rr, \quad 16 + ss, \quad 25 + tt \quad \text{etc.}$$

exhiberi possunt, quae omnes sint per numerum primum $4n + 1$ divisibiles, atque ita, ut singulorum [quadratorum pp, qq, rr etc.] radices sint minores quam $2n + 1$.

COROLLARIUM 3

63. Cum multitudo numerorum minorum quam $2n + 1$ sit $= 2n$ ac semper bina quadrata disparia iungantur, multitudo harum formularum erit n; et quia talis summa binorum quadratorum minor est quam

$$2(2n + 1)^2 = 8nn + 8n + 2,$$

quotus erit minor quam $2n + \frac{3}{2}$ seu $2n + 2$.

SCHOLION

64. Quo has summas binorum quadratorum pro quovis numero primo formae $4n + 1$ facilius elicere queamus, residua ex quadratis orta pro simplicioribus apponamus:

Num. primi formae $4n+1$	Quadrata 1, 4, 9, 16, 25, 36, 49, 64, 81, 100, 121, 144, 169, 196, 225, 256 etc.
	Residua
5	1, −1, |−1, 1, 0
13	1, 4, −4, 3, −1, −3, |−3, −1, 3, −4, 4, 1, 0
17	1, 4, −8, −1, 8, 2, −2, −4, |−4, −2, 2, 8, −1, −8, 4, 1
29	1, 4, 9, −13, −4, 7, −9, 6, −6, 13, 5, −1, −5, −7, |−7, −5
37	1, 4, 9, 16, −12, −1, 12, −10, 7, −11, 10, −4, −16, 11, 3, −3, −7, −9, |−9

Hinc pro his divisoribus formae $4n + 1$ sequentes habebimus binorum quadratorum summas per eos divisibiles:

Divisor 5:	1								
	4								
summa	5								
quotus	1								
Divisor 13:	1	4	16						
	25	9	36						
summae	26	13	52						
quoti	2	1	4						
Divisor 17:	1	4	9	36					
	16	64	25	49					
summae	17	68	34	85					
quoti	1	4	2	5					
Divisor 29:	1	4	9	16	36	64	121		
	144	25	49	100	196	81	169		
summae	145	29	58	116	232	145	290		
quoti	5	1	2	4	8	5	10		
Divisor 37:	1	4	9	16	25	64	81	100	225
	36	144	324	169	49	121	289	196	256
summae	37	148	333	185	74	185	370	296	481
quoti	1	4	9	5	2	5	10	8	13

Si igitur demonstrari posset in his quotis semper unitatem reperiri, haberetur demonstratio completa theorematis FERMATIANI, quod omnis numerus primus formae $4n+1$ sit summa duorum quadratorum. Quoniam vero alibi[1]) demonstravi summam duorum quadratorum inter se primorum

1) Vide Commentationem 228 nota p. 222 laudatam. Vide praeterea Commentationem 445 huius voluminis, theorema 1. F. R.

alios divisores non admittere, nisi qui ipsi sint summae duorum quadratorum, demonstratio iam pro absoluta est habenda, quae multo concinnior est ea, quam olim[1]) per plures ambages elicueram. Sin autem simul perpendamus in quotis illis nullos numeros primos formae $4n - 1$ occurrere posse, uti mox demonstrabitur, haec demonstratio forte multo magis contrahi poterit.

THEOREMA

65. *Nulla summa duorum quadratorum inter se primorum per ullum numerum primum formae* $4n - 1$ *divisibilis existit.*[2])

DEMONSTRATIO

Quia sumto quocumque quadrato bb, quod per $4n - 1$ divisum praebeat residuum β, numerus $-\beta$ seu $4n - 1 - \beta$ ex residuis quadratorum prorsus excluditur (§ 59), nullum datur quadratum, quod ipsi bb additum summam producat per numerum primum $4n - 1$ divisibilem.

COROLLARIUM 1

66. Summa ergo duorum quadratorum nullum divisorem admittit formae $4n - 1$, etiamsi hic divisor non sit primus, quoniam tum inter eius factores semper unus saltem primus formae $4n - 1$ contineretur, nisi forte ambo quadrata seorsim per eum fuerint divisibilia.

COROLLARIUM 2

67. Quando ergo summa duorum quadratorum per numerum primum formae $4n + 1$ est divisibilis, quotus inde resultans neque erit formae $4n - 1$

1) Vide Commentationem 241 (indicis Enestroemiani): *Demonstratio theorematis Fermatiani omnem numerum primum formae* $4n + 1$ *esse summam duorum quadratorum,* Novi comment. acad. sc. Petrop. 5 (1754/5), 1760, p. 3; *Leonhardi Euleri Opera omnia*, series I, vol. 2, p. 328. F. R.

2) Quod theorema ab Eulero primum demonstratum est in Commentatione 134 (indicis Enestroemiani): *Theoremata circa divisores numerorum*, Novi comment. acad. sc. Petrop. 1 (1747/8), 1750, p. 20; *Leonhardi Euleri Opera omnia*, series I, vol. 2, p. 62. Demonstratio hac in paragrapho 65 data iam invenitur in § 70 Commentationis 242 nota 2 p. 218 laudatae. F. R.

neque ullum habebit factorem primum huius formae, nisi forte ambo quadrata huiusmodi habuerint communem divisorem, quo casu quotus adeo quadratum talis numeri contineret.

COROLLARIUM 3

68. Ex ordine quotorum ergo, qui supra ex divisione summae binorum quadratorum per numerum primum formae $4n+1$ sunt orti, excluduntur h, numeri

3, 6, 7, 11, 12, 14, 15, 19, 21, 22, 23, 24, 27, 28, 30, 31 etc.

ac propterea relinquuntur isti tantum

1, 2, 4, 5, 8, 9, 10, 13, 16, 17, 18, 20, 25, 26, 29, 32 etc.

PROBLEMA

69. *Si omnes numeri cubici*

$$1,\ 2^3,\ 3^3,\ 4^3 \text{ etc.}$$

per numerum quemcumque primum P dividantur, investigare indolem residuorum, quae inde nascentur.

SOLUTIO

Sit a radix primitiva respectu divisoris primi P, et cum progressio geometrica $1, a, a^2, a^3, a^4$ etc. seriem residuorum completam exhibeat, quilibet numerus x per P divisus idem dabit residuum, quod quaepiam potestas ipsius a, quae sit a^λ. Hinc eius numeri cubus x^3 idem dabit residuum, quod potestas $a^{3\lambda}$, unde ex cubis eadem nascentur residua atque ex progressione geometrica

$$1,\ a^3,\ a^6,\ a^9,\ a^{12},\ a^{15} \text{ etc.},$$

ac sumto λ ita, ut 3λ sit vel $P-1$ vel eius multiplum, potestas $a^{3\lambda}$ unitatem relinquet. Quare si pro λ minimus numerus accipiatur, cuius triplum sit per $P-1$ divisibile, numerus λ simul multitudinem omnium residuorum diversorum, quae ex divisione cuborum resultare possunt, indicabit.

Cum iam omnis numerus primus sit vel formae $3n+1$ vel $3n+2$, pro utraque forma iudicium seorsim est instituendum.

I. Sit ergo $P = 3n + 1$, et quia $P - 1 = 3n$, fiet $\lambda = n$ et residua cuborum omnia ex hac progressione geometrica nascentur

$$1,\ a^3,\ a^6,\ a^9,\ \ldots\ a^{3n-3},$$

quia sequens terminus a^{3n} iterum unitatem producit. Hinc non plures quam n numeri in residuis occurrent ac reliqui duplo plures excluduntur eruntque non-residua.

II. Si divisor primus sit $P = 3n + 2$ ideoque $P - 1 = 3n + 1$, minor numerus pro λ accipi nequit quam $\lambda = 3n + 1$, ut 3λ per $P - 1$ fiat divisibile, unde omnia residua diversa ex hac progressione geometrica nascentur

$$1,\ a^3,\ a^6,\ a^9,\ \ldots\ a^{9n};$$

quorum numerus cum sit $= 3n + 1$, in residuis omnes plane numeri divisore P minores occurrent nullique excluduntur seu nulla dabuntur non-residua.

COROLLARIUM 1

70. Si ergo divisor primus P fuerit formae $3n + 1$, cuiusmodi numeri sunt

7, 13, 19, 31, 37, 43, 61, 67, 73, 79, 97 etc.,

in residuis cuborum tantum n numeri diversi occurrunt indeque $2n$ numeri excluduntur.

COROLLARIUM 2

71. Quare si haec cuborum progressio

$$1,\ 2^3,\ 3^3,\ 4^3,\ \ldots\ (3n)^3,$$

unde omnia residua diversa prodire debent, per numerum primum $3n + 1$ dividatur, quia terminorum numerus est $= 3n$, quodlibet residuum ter occurrat necesse est seu semper terni cubi minores quam $(3n)^3$ exhiberi possunt, qui idem residuum producant.

SCHOLION 1

72. Respectu ergo cuborum numeri primi formae $3n + 1$ praecipue notari merentur operaeque pretium erit residua in casibus simplicioribus notasse:

Divisor primus $3n+1$	1, 2^3, 3^3, 4^3, 5^3, 6^3, 7^3, 8^3, 9^3, 10^3, 11^3, 12^3, 13^3, 14^3, 15^3, 16^3, 17^3, 18^3
	Residua
7	1, 1, −1, 1, −1, −1, 0
13	1, −5, 1, −1, −5, −5, 5, 5, 1, −1, 5, −1, 0
19	1, 8, 8, 7, −8, 7, 1, −1, 7, −7, 1, −1, −7, 8, −7, −8, −8, −1, 0

Ubi manifesto quodvis residuum ter occurrit totiesque idem signo — affectum; cuius ratio inde est perspicua, quod postremus cuiusque ordinis cubus $(3n)^3$ pro residuo dat -1 et producta ex binis residuis semper quoque inter residua reperiantur. Cum igitur praeter cubum $(3n)^3$ semper dentur duo minores pariter residuum -1 habentes, qui sint f^3 et g^3, erunt formulae $1+f^3$ et $1+g^3$ per $3n+1$ divisibiles, et quia neque $1+f$ neque $1+g$ divisionem admittit, necesse est, ut hae $1-f+ff$ et $1-g+gg$ sint divisibiles; ubi quidem observare licet semper esse debere $g=-ff$ vel $g=m(3n+1)-ff$, quia tum fit $1+g^3=1-f^6$, quae aeque ac $1+f^3$ est divisibilis.

SCHOLION 2

73. Sint f^3, g^3, h^3 terni cubi minores quam $(3n+1)^3$, qui per numerum primum $3n+1$ divisi idem relinquant residuum, et quia binorum differentiae g^3-f^3, h^3-f^3 et h^3-g^3 divisionem admittunt, dum factores $g-f$, $h-f$, $h-g$ divisore sunt minores, hae tres formae

$$ff+fg+gg, \quad ff+fh+hh, \quad gg+gh+hh$$

singulae per $3n+1$ divisibiles sint necesse est hincque etiam binarum differentiae

$$hh-gg+fh-fg=(h-g)(f+g+h).$$

Unde patet quoque summam radicum

$$f+g+h$$

per divisorem $3n+1$ esse divisibilem; quae proprietas illi est analoga, qua invenimus [§ 55], si bina quadrata ff et gg per numerum quempiam primum P divisa idem residuum relinquant, dum ambo sunt minora quam P^2, tum

summam radicum $f+g$ per P esse divisibilem. Pro casu nostro trium cuborum erit quoque

$$h(ff+fg+gg)-g(ff+fh+hh)=ff(h-g)-gh(h-g)$$

ideoque formula $ff-gh$ per $3n+1$ divisibilis similique modo $gg-fh$ et $hh-fg$; hinc istas duas formulas ab illa $gg+gh+hh$ auferendo relinquitur haec

$$fg+fh+gh$$

pariter per $3n+1$ divisibilis; et haec combinatio $(ff+fg+gg)+(hh-fg)$ praebet hanc

$$ff+gg+hh$$

itidem per $3n+1$ divisibilem. Quocirca hoc habebimus theorema satis memorabile:

THEOREMA

74. *Si* f^3, g^3, h^3 *fuerint terni cubi minores quam* $(3n+1)^3$, *qui per numerum primum* $3n+1$ *divisi idem relinquant residuum, tum sequentes formulae*

$$f+g+h,\quad fg+fh+gh,\quad ff+gg+hh$$

singulae divisionem per $3n+1$ *admittent.*

COROLLARIUM

75. Ita pro divisore 19 videmus hos tres cubos 4^3, 6^3 et 9^3 idem residuum 7 dare; unde ob $f=4$, $g=6$, $h=9$ fit

$$f+g+h=19,\ fg+fh+gh=114=6\cdot 19\quad\text{et}\quad ff+gg+hh=133=7\cdot 19.$$

THEOREMA

76. *Semper numeri huius formae* $pp+3qq$ *exhiberi possunt per numerum primum huius formae* $3n+1$ *divisibiles. At vero nulla eiusmodi datur formula* $pp+3qq$, *quae per ullum numerum primum huius formae* $3n-1$ *sit divisibilis.*

DEMONSTRATIO

Si $3n+1$ est numerus primus, tum tres adeo cubi f^3, g^3, h^3, quorum radices ipso sunt minores, exhiberi possunt, qui per $3n+1$ divisi idem residuum relinquant; unde g^3-f^3 per $3n+1$ divisionem admittet hincque etiam $ff+fg+gg$. At haec forma est vel $\left(f+\frac{1}{2}g\right)^2+3\left(\frac{1}{2}g\right)^2$, si g sit numerus par, vel $\left(\frac{1}{2}f+g\right)^2+3\left(\frac{1}{2}f\right)^2$, si f sit par, vel $\left(\frac{f-g}{2}\right)^2+3\left(\frac{f+g}{2}\right)^2$, si ambo sint impares, unde forma $ff+fg+gg$ semper ad hanc $pp+3qq$ reducitur.[1])

At si $3n-1$ sit divisor primus, omnes cubi, quorum radices ipso sunt minores, diversa praebent residua neque ergo binorum differentia vel numerus huius formae $ff+fg+gg$ exhiberi potest, qui per $3n-1$ dividi posset; quod proinde etiam de numeris huius formae $pp+3qq$ locum habet. Atque hoc adeo de omnibus numeris formae $3n-1$ valet, quoniam, si non fuerint primi, factorem saltem primum istius formae involvunt.

COROLLARIUM 1

77. Si igitur forma $pp+3qq$ per numerum primum $3n+1$ sit divisibilis et quadratum qq per eundem divisum relinquat residuum γ, alterum quadratum pp relinquet residuum -3γ. Unde si omnes numeri quadrati per numerum primum $3n+1$ dividantur, in residuis certe reperitur -3 vel $3n-2$.

COROLLARIUM 2

78. Sin autem omnes numeri quadrati per numerum primum formae $3n-1$ dividantur, in serie residuorum certe non erit numerus -3; ideoque -3 vel $3n-4$ erit non-residuum.

SCHOLION

79. Hinc si numeri quadrati per numerum quemcumque primum dividantur, de binis numeris $+3$ et -3 iudicari poterit, utrum in ordine residuorum an non-residuorum occurrant. Omnes enim numeri primi praeter

1) Vide Commentationem 272 nota p. 224 laudatam, imprimis § 37. F. R.

2 et 3, qui hic non spectantur, in aliqua harum quatuor formarum continentur

$$12m + 1, \quad 12m + 5, \quad 12m + 7, \quad 12m + 11,$$

quas singulas contemplemur.

I. Si divisor primus sit formae $12m + 1$, quatenus haec forma est $4n + 1$, tam $+1$ quam -1 erit residuum; quatenus vero est $3n + 1$, residuum quoque erit -3 hincque etiam $+3$. Hoc ergo in ordine residuorum occurrent $+3$ et -3.[1])

II. Si divisor primus sit formae $12m + 5$, quatenus haec forma est $4n + 1$, in residuis erunt $+1$ et -1; quatenus vero est $3n - 1$, in residuis non reperitur -3 seu -3 erit non-residuum hincque etiam $+3$. Quare hoc casu neuter numerorum $+3$ et -3 inter residua reperietur.

III. Si divisor primus sit formae $12m + 7$, quatenus haec forma est $4n - 1$, erit -1 non-residuum; quatenus vero est $3n + 1$, erit -3 residuum ideoque $+3$ non-residuum. Unde hoc casu erit -3 residuum, at $+3$ non-residuum.[1])

IV. Si divisor primus sit formae $12m + 11$, quatenus haec forma est $4n - 1$, erit -1 non-residuum; quatenus vero est formae $3n - 1$, erit quoque -3 non-residuum, unde $+3$ utpote productum ex duobus non-residuis inter residua occurret. Quare hoc casu erit $+3$ residuum, at -3 non-residuum

Ad hanc ergo egregiam proprietatem consideratio cuborum nos perduxit; quae via cum satis sit obliqua, alia magis naturalis maxime desideratur.

PROBLEMA

80. *Si omnes potestates quartae per numerum quemcumque primum P dividantur, investigare indolem residuorum, quae inde nascentur.*

---

1) Numerum -3 residuum esse omnium numerorum primorum formae $6n + 1$ vel, quod eodem redit, omnem numerum primum formae $6n + 1$ simul in hac forma $pp + 3qq$ contineri ab EULERO iam demonstratum erat in Commentatione nota 272 p. 224 laudata. F. R.

SOLUTIO

Posita a radice primitiva respectu divisoris P, ut a^{P-1} sit infima potestas unitatem relinquens, residua quaesita orientur quoque ex hac progressione geometrica

$$1,\ a^4,\ a^8,\ a^{12},\ a^{16} \text{ etc.}$$

eousque continuanda, donec exponens per $P-1$ fiat divisibilis; quod si eveniat in exponente 4λ, erit λ multitudo residuorum.

I. Sit divisor primus $P = 4n+1$, ut sit $P-1 = 4n$; unde ut 4λ per $4n$ dividi queat, erit $\lambda = n$ hocque casu residua quaesita omnia ex hac progressione geometrica nascentur

$$1,\ a^4,\ a^8,\ a^{12},\ \ldots\ a^{4n-4},$$

quorum multitudo est n.

II. Sit divisor primus $P = 4n+3$, ut sit $P-1 = 4n+2$; unde sumi debet $\lambda = 2n+1$ et haec progressio geometrica

$$1,\ a^4,\ a^8,\ a^{12},\ \ldots\ a^{8n}$$

dabit omnia residua quaesita; cum autem a^{4n+2} unitatem relinquat uti a^0, termini

$$a^{4n+4},\ a^{4n+8},\ a^{4n+12} \text{ etc.}$$

eadem residua praebent atque a^2, a^6, a^{10} etc., unde his interpolatis oritur progressio

$$1,\ a^2,\ a^4,\ a^6,\ a^8,\ \ldots\ a^{4n},$$

quae eadem residua dat ac progressio numerorum quadratorum. Ex biquadratis ergo hoc casu eadem plane residua omnia nascuntur atque ex ipsis quadratis.

COROLLARIUM 1

81. Si ergo numeri biquadrati per numerum primum formae $4n+1$ dividantur, tantum n residua diversa oriuntur, unde semper quaterna biquadrata dantur p^4, q^4, r^4, s^4, quorum radices divisore sunt minores, quae per $4n+1$ divisa idem praebeant residuum; ubi quidem perspicuum est fore

$s = -p$ et $r = -q$ seu, quod eodem redit, $s = 4n + 1 - p$ et $r = 4n + 1 - q$. Hinc istae formulae

$$p + q + r + s, \quad p^2 + q^2 + r^2 + s^2 \quad \text{et} \quad p^3 + q^3 + r^3 + s^3$$

per $4n + 1$ erunt divisibiles.

COROLLARIUM 2

82. Quaterna ergo biquadrata, quae per numerum primum $4n + 1$ divisa unitatem relinquent, erunt valores ipsius x, quibus formula $x^4 - 1$ per $4n + 1$ fit divisibilis, unde primo est $x = 1$, tum, si alius valor sit $x = b$, erit quoque $x = b^2$ et $x = b^3$; neque ultra progredi opus est, quia b^4 unitati aequivalet.

COROLLARIUM 3

83. Cum potestas a^{2n} per $4n + 1$ [divisa] residuum det -1, patet, si n sit numerus par, in residuis biquadratorum semper reperiri -1 et quodvis residuum quoque signo $-$ affectum occurrere; quod ergo evenit, si divisor primus sit formae $8m + 1$; sin autem sit formae $8m + 5$, tum -1 erit non-residuum.

COROLLARIUM 4

84. Si ergo divisor primus sit formae $8m + 1$, pro quovis biquadrato b^4 semper dabitur aliud p^4, ut summa $b^4 + p^4$ sit per $8m + 1$ divisibilis, atque adeo quaterna huiusmodi biquadrata p^4 assignari poterunt, quorum radices divisore sint minores; sin autem divisor sit formae $8m + 5$, tum nulla summa binorum biquadratorum per eum divisibilis exhiberi potest.

SCHOLION

85. Cum summa binorum biquadratorum sit

$$b^4 + p^4 = (bb - pp)^2 + 2(bp)^2 \quad \text{itemque} \quad b^4 + p^4 = (bb + pp)^2 - 2(bp)^2,$$

pro quovis divisore primo formae $8m + 1$ numeri tam huius formae $xx + 2yy$ quam huius $xx - 2yy$ exhiberi possunt per $8m + 1$ divisibiles; unde si numeri quadrati per talem numerum primum $8m + 1$ dividantur, in residuis occurrent numeri $+2$ et -2. Cum igitur demonstrari possit, numeros huius formae $xx + 2yy$ alios divisores non admittere, nisi qui ipsi sint eiusdem formae[1]),

1) Id quod EULERUS demonstravit in Commentatione 256 (§ 42) nota p. 224 laudata. Vide etiam theorema 2 Commentationis 445 huius voluminis. F. R.

hinc sequitur omnes numeros primos formae $8m + 1$ simul in forma $xx + 2yy$ contineri. Quod est insigne theorema FERMATII [1]), cuius demonstrationem nunc primum mihi eruere contigit. Huic autem aliud affine FERMATIUS proposuit, quod etiam omnes numeri primi huius formae $8m + 3$ in eadem forma $xx + 2yy$ contineantur, cuius demonstrationem ex hac speculatione petere non licet; sequentem ergo ab amico mecum communicatam hic apponam.

THEOREMA

86. *Nullus numerus huius formae* $2pp - qq$, *siquidem* p *et* q *sint numeri inter se primi, ullum admittit divisorem sive huius formae* $8m + 3$ *sive huius* $8m - 3$.

DEMONSTRATIO

Si numerorum p et q ambo sint impares, numerus $2pp - qq$ habebit formam $8n + 1$; sin p sit par et q impar, formam habebit $8n - 1$; sin autem p sit impar et q par $= 2r$, forma erit $2(pp - 2rr)$ ideoque vel $2(8n + 1)$ vel $2(8n - 1)$; semissis vero $pp - 2rr$ iterum in forma $2pp - qq$ continetur, cum sit $pp - 2rr = 2(p + r)^2 - (p + 2r)^2$. Hoc praemisso si forma $2pp - qq$ divisorem haberet $8m \pm 3$, per eundem divisibilis esset numerus formae $8n \pm 1$ quotusque ergo foret iterum formae $8m \pm 3$ atque minor divisore, quoniam p et q non solum divisore, sed etiam eius semisse minores statuere licet. Cum igitur forma $2pp - qq$ per quotum ideoque numerum minorem formae $8m \pm 3$ esset divisibilis, ubi iterum p et q infra eius semissem deprimere licet, quotus denuo minor divisore oriretur et numeri p et q semper primi inter se manerent [2]), ita ut neuter umquam ad nihilum redigeretur. Tandem ergo ad numerum minimum formae $2pp - qq$ perveniretur, qui foret per numerum formae $8m \pm 3$, hoc est, vel 3 vel 5 divisibilis, quod autem fieri non posse per se est perspicuum.

---

1) Vide notam p. 466 voluminis praecedentis. F. R.

2) Numeros p et q per se semper primos manere inter se neque asseverari potest neque omnino necesse est. Initio quidem inter se primi sunt. Cum autem per divisorem primum $d = 8m \pm 3$ infra eius semissem deprimuntur, fieri potest, ut factorem communem praebeant. Talis vero factor certe primus erit ad divisorem d ideoque omitti potest. Ubi notandum est omnes divisores $d = 8m \pm 3$ primos supponi posse. Si enim divisor $d = 8m \pm 3$ non esset primus, factorem saltem primum eiusdem formae habere deberet, quem tum uti divisorem accipere liceret. F. R.

COROLLARIUM 1

87. Quodsi ergo omnes numeri quadrati per divisores primos formae $8m \pm 3$ dividantur, in residuis certe non occurret $+2$, quia alioquin eiusmodi forma $2pp - qq$ divisibilis exhiberi posset; ideoque pro talibus divisoribus erit $+2$ non-residuum.

COROLLARIUM 2

88. Pro divisoribus autem primis formae $8m + 3$ etiam -1 est non-residuum; unde, cum producta ex binis non-residuis quadratorum transeant in residua, inter residua certe reperietur -2; hincque semper numeri formae $2pp + qq$ exhiberi poterunt per numerum primum $8m + 3$ divisibiles, ex quo numerus primus $8m + 3$ ipse eiusdem formae $2pp + qq$ sit necesse est; quod est alterum theorema FERMATII.

COROLLARIUM 3

89. Pro divisoribus autem primis formae $8m - 3$ in residuis quadratorum reperitur -1; unde, cum productum ex residuo in non-residuum sit non-residuum, tam $+2$ quam -2 erunt non-residua; ideoque neutra harum formarum $2pp + qq$ et $2pp - qq$ umquam erit divisibilis per ullum numerum primum formae $8m - 3$.

SCHOLION 1

90. Eodem modo demonstrari potest nullum numerum formae $2pp + qq$, quoniam huiusmodi numeri omnes sunt vel $8n + 1$ vel $8n + 3$, per ullos numeros formae vel $8m - 1$ vel $8m - 3$ esse divisibiles, quoniam quoti eiusdem forent formae et, cum sint divisore minores, perveniendum esset ad minores numeros $2pp + qq$, qui forent per $8m - 1$ vel $8m - 3$, hoc est, per 7 vel 5 divisibiles, quod autem evenire nequit. Hinc porro sequitur pro divisoribus primis formae $8m - 1$ vel $8m - 3$ necessario esse -2 non-residuum; ideoque pro divisoribus $8m - 1$ erit $+2$ residuum et pro divisoribus $8m - 3$ non-residuum. Quod autem pro divisoribus primis formae $8m + 1$ tam $+2$ quam -2 in residuis quadratorum occurrant [§ 85], simili ratiocinio vix ostendi posse videtur.[1])

1) Ex paragraphis 85—90 satis elucet revera iam EULERUM characterem quadraticum numerorum $+2$ et -2 rectis demonstrationibus determinasse neque igitur I. L. LAGRANGE, ut affirmavit C. F. GAUSS, *Disquisitiones arithmeticae*, art. 116 et 120, primum fuisse, qui hoc praestiterit. F. R.

SCHOLION 2

91. Quae hactenus de residuis quadratorum sunt eruta, utrum numeri ± 2 ac supra etiam ± 3 in iis occurrant necne, ita conspectui exposuisse iuvabit:

Divisor primus

$4n+1$ $\begin{cases} +1 \text{ residuum} \\ -1 \text{ residuum} \end{cases}$

$4n-1$ $\begin{cases} +1 \text{ residuum} \\ -1 \text{ non-residuum} \end{cases}$

$8n+1$ $\begin{cases} +2 \text{ residuum} \\ -2 \text{ residuum} \end{cases}$

$8n-1$ $\begin{cases} +2 \text{ residuum} \\ -2 \text{ non-residuum} \end{cases}$

$8n+3$ $\begin{cases} +2 \text{ non-residuum} \\ -2 \text{ residuum} \end{cases}$

$8n-3$ $\begin{cases} +2 \text{ non-residuum} \\ -2 \text{ non-residuum} \end{cases}$

$12n+1$ $\begin{cases} +3 \text{ residuum} \\ -3 \text{ residuum} \end{cases}$

$12n-1$ $\begin{cases} +3 \text{ residuum} \\ -3 \text{ non-residuum} \end{cases}$

$12n+5$ $\begin{cases} +3 \text{ non-residuum} \\ -3 \text{ non-residuum} \end{cases}$

$12n-5$ $\begin{cases} +3 \text{ non-residuum} \\ -3 \text{ residuum.} \end{cases}$

Hinc per inductionem[1]) ulterius progredi licet hoc modo:

1) Vide Commentationem 164 (indicis Enestroemiani): *Theoremata circa divisores numerorum in hac forma $paa \pm qbb$ contentorum*, Comment. acad. sc. Petrop. **14** (1744/6), 1751, p. 151; *Leonhardi Euleri Opera omnia*, series I, vol. 2, p. 194 (vide imprimis notam p. 194). F. R.

Erit	si divisor primus sit
$+5$ residuum -5 residuum	$20n+1,\ 20n+9$
$+5$ residuum -5 non-residuum	$20n-1,\ 20n-9$
$+5$ non-residuum -5 residuum	$20n+3,\ 20n+7$
$+5$ non-residuum -5 non-residuum	$20n-3,\ 20n-7$
$+7$ residuum -7 residuum	$28n+1,\ -3,\ +9$
$+7$ residuum -7 non-residuum	$28n-1,\ +3,\ -9$
$+7$ non-residuum -7 residuum	$28n+11,\ +15,\ +23$
$+7$ non-residuum -7 non-residuum	$28n+5,\ +13,\ +17$
$+11$ residuum -11 residuum	$44n+1,\ +9,\ +25,\ +5,\ +37$
$+11$ residuum -11 non-residuum	$44n-1,\ -9,\ -25,\ -5,\ -37$
$+11$ non-residuum -11 residuum	$44n+3,\ +15,\ +23,\ +27,\ +31$
$+11$ non-residuum -11 non-residuum	$44n+13,\ +17,\ +21,\ +29,\ +41.$

Quorum theorematum demonstrationes scientiam numerorum haud mediocriter promoverent.

THEOREMA

92. *Si omnium numerorum potestates exponentis λ, scilicet*

$$1,\ 2^\lambda,\ 3^\lambda,\ 4^\lambda,\ 5^\lambda,\ 6^\lambda \text{ etc.},$$

per numerum primum formae $\lambda n + 1$ dividantur, multitudo residuorum diversorum erit $= n$ ideoque multitudo non-residuorum $= (\lambda - 1)n$.

DEMONSTRATIO

Sit a radix primitiva pro divisore primo $\lambda n + 1$, cuius ergo potestates omnia plane suppeditant residua, et quilibet numerus divisore minor x erit residuum certae potestatis a^m, unde eius potestas x^λ idem praebebit residuum, quod $a^{\lambda m}$; quare omnia residua quaesita oriuntur ex hac progressione geometrica

$$1,\ a^\lambda,\ a^{2\lambda},\ a^{3\lambda},\ a^{4\lambda},\ \ldots\ a^{(n-1)\lambda},$$

quoniam potestas sequens $a^{\lambda n}$ per numerum primum $\lambda n + 1$ divisa iterum unitatem relinquit eaque est minima hoc praestans; ex quo multitudo residuorum inde resultantium est $= n$, et cum multitudo omnium numerorum divisore minorum sit $= \lambda n$, reliquorum ex serie residuorum exclusorum multitudo erit $= (\lambda - 1)n$.

COROLLARIUM 1

93. Quare si series potestatum $1, 2^\lambda, 3^\lambda, 4^\lambda$ etc. usque ad $(\lambda n)^\lambda$ continuetur, in ea semper totidem termini, quot exponens λ continet unitates, reperientur, qui per numerum primum $\lambda n + 1$ divisi idem residuum relinquant. Totidem ergo erunt, qui unitatem relinquunt, ac si unius radix sit $= r$, reliquorum radices erunt $r^2, r^3, r^4, \ldots r^{\lambda-1}$.

COROLLARIUM 2

94. Semper ergo plures huiusmodi numerorum formae $p^\lambda - q^\lambda$ exhiberi possunt per numerum primum $\lambda n + 1$ divisibiles, ita ut factor $p - q$ non sit divisibilis; atque adeo alterum numerorum p et q pro lubitu accipere licet.

COROLLARIUM 3

95. Si n sit numerus par, in progressione geometrica 1, a^λ, $a^{2\lambda}$ etc. occurret terminus $a^{\frac{1}{2}n\lambda}$, cui residuum -1 respondet; quare si divisor primus sit $2m\lambda+1$, in residuis reperietur -1, sin autem sit $(2m+1)\lambda+1$, tum -1 erit non-residuum; evidens autem est, si λ sit numerus impar, posteriorem formam locum habere non posse.

SCHOLION 1

96. Si omnium numerorum potestates quintae

$$1,\ 2^5,\ 3^5,\ 4^5 \text{ etc.}$$

per numeros primos formae $5n+1$, qui sunt

$$11,\ 31,\ 41,\ 61,\ 71 \text{ etc.},$$

dividantur, tantum n residua diversa resultabunt, inter quae utique reperietur -1. Huiusmodi ergo numerorum formae $p^5 \pm q^5$ dabuntur per numerum primum $5n+1$ divisibiles, ita [ut] factor $p \pm q$ divisionem non admittat. Hinc alter factor, qui est

$$p^4 \mp p^3q + p^2q^2 \mp pq^3 + q^4,$$

per eundem erit divisibilis; qui cum sit

$$\left(pp \mp \tfrac{1}{2}pq + qq\right)^2 - 5\left(\tfrac{1}{2}pq\right)^2,$$

dabitur huiusmodi forma $ff - 5gg$ per $5n+1$ divisibilis; unde sequitur, si [omnia] quadrata dividantur per numerum primum formae $5n+1$, tum inter residua certe reperiri $+5$, quod cum coniectura ante [§ 91] allata congruit.

SCHOLION 2

97. Simili modo si potestates septimae per numerum primum $7n+1$ dividantur, dabuntur huiusmodi formae $p^7 - q^7$ seu

$$p^6 + p^5q + p^4q^2 + p^3q^3 + p^2q^4 + pq^5 + q^6$$

per eum divisibiles; haec vero expressio reducitur ad hanc formam

$$\left(p^3+\tfrac{1}{2}ppq-\tfrac{1}{2}pqq-q^3\right)^2+7\left(\tfrac{1}{2}ppq+\tfrac{1}{2}pqq\right)^2.$$

Unde semper numeri huius formae $ff+7gg$ exhiberi possunt per numerum primum $7n+1$ divisibiles. Ex quo sequitur, si omnia quadrata per numerum primum formae $7n+1$ dividantur, inter residua certe repertum iri -7, quo etiam coniectura supra [§ 91] data confirmatur.

SOLUTIO PROBLEMATIS DE INVENIENDO TRIANGULO IN QUO RECTAE EX SINGULIS ANGULIS LATERA OPPOSITA BISECANTES SINT RATIONALES[1])

Commentatio 451 indicis ENESTROEMIANI
Novi commentarii academiae scientiarum Petropolitanae 18 (1773), 1774, p. 171—184
Summarium ibidem p. 20—21

SUMMARIUM

Problematis huius evolutio ad resolutionem trium sequentium formularum reducitur

$$2b^2+2c^2-a^2=f^2,$$

$$2c^2+2a^2-b^2=g^2$$

et

$$2a^2+2b^2-c^2=h^2,$$

si scilicet $2a$, $2b$ et $2c$ sint latera trianguli a rectis f, g et h bisecta. Ex hisce tribus formulis ternae aliae resultant

---

1) Alia problemata DIOPHANTEA ad triangula pertinentia pertractata sunt in L. EULERI Commentationibus 167, 713, 732, 748, 754, 799, inter quas hic imprimis Commentationum 713, 732, 754 ratio est habenda; *LEONHARDI EULERI Opera omnia,* series I, vol. 2, 4, 5. Vide etiam Prooemium voluminis praecedentis, p. XXI—XXII. Confer porro commentarium a BACHETO adiectum ad quaestionem XVIII libri VI DIOPHANTI *Arithmeticorum* (Lutetiae Parisiorum 1621; vide notam p. 404 voluminis praecedentis). Vide praeterea P. v. SCHAEWEN, *Dreiecke mit rationalen Seiten und rationalen Seitenhalbierenden*, Zeitschr. f. d. Realschulwesen, **40**, 1915, p. 145. F. R.

$$2g^2+2h^2-f^2=9a^2,$$
$$2h^2+2f^2-g^2=9b^2$$
et
$$2f^2+2g^2-h^2=9c^2,$$

ex quarum cum prioribus similitudine concludit Illustr. Auctor pro lateribus $2f$, $2g$ et $2h$ fore rectas bisecantes $3a$, $3b$ et $3c$ adeoque pro f, g et h istas fore $\frac{3}{2}a$, $\frac{3}{2}b$ et $\frac{3}{2}c$, unde colligitur invento uno huiusmodi triangulo, si rectae bisecantes pro lateribus novi trianguli accipiantur, id eadem praeditum fore proprietate.

His praemissis Ill. Auctor ipsum problema adgreditur; cuius resolutio cum meris absolvatur artificiis analyticis, nihil hic in epitome de ea adferre licet, nisi quod pendeat ab huiusmodi forma

$$Ax^4+Bx^3+Cx^2+Dx+E$$

ad quadratum revocanda, pro cuius resolutione naturalis et simplex methodus adhuc desideratur.

1. Vocatis ternis lateribus $2a$, $2b$, $2c$ et rectis haec latera bisecantibus f, g, h quaestio reducitur ad resolutionem trium sequentium formularum

$$2bb+2cc-aa=ff,$$
$$2cc+2aa-bb=gg,$$
$$2aa+2bb-cc=hh.$$

2. Hinc differentiis sumendis sequitur fore

$$3(bb-aa)=ff-gg,\quad 3(cc-bb)=gg-hh,\quad 3(cc-aa)=ff-hh$$
seu
$$ff+3aa=gg+3bb=hh+3cc.$$

Cum autem sit $ff=2bb+2cc-aa$, habebimus

$$ff+3aa=gg+3bb=hh+3cc=2(aa+bb+cc).$$

3. Summa porro nostrarum trium formularum praebet

$$2(ff+gg+hh)=3ff+9aa=3gg+9bb=3hh+9cc,$$

ita ut hinc istae ternae formulae resultent

$$2gg + 2hh - ff = 9aa,$$
$$2hh + 2ff - gg = 9bb,$$
$$2ff + 2gg - hh = 9cc.$$

4. Quae cum similes sint ipsis propositis, concludimus, si pro lateribus $2a$, $2b$, $2c$ sint rectae bisecantes f, g, h, tum pro lateribus $2f$, $2g$, $2h$ fore rectas bisecantes $3a$, $3b$, $3c$ ideoque pro lateribus f, g, h rectas bisecantes $\frac{3}{2}a$, $\frac{3}{2}b$, $\frac{3}{2}c$. Quare invento uno huiusmodi triangulo, si rectae bisecantes pro lateribus novi trianguli accipiantur, hoc eadem gaudebit proprietate, quia in hoc rectae bisecantes sunt tres quadrantes laterum praecedentis.

5. His observatis solutionem quaestionis sequenti modo aggredior. Primo binis tantum formulis satisfacturus eas ita exhibeo

$$(b-c)^2 + (b+c)^2 - aa = (b-c)^2 + (b+c+a)(b+c-a) = ff,$$
$$(a-c)^2 + (a+c)^2 - bb = (a-c)^2 + (a+c+b)(a+c-b) = gg.$$

Statuo igitur

$$f = b - c + (b+c+a)p \quad \text{et} \quad g = a - c + (a+c+b)q,$$

ut facta substitutione divisio per $a+b+c$ succedat; hoc modo obtinetur

$$b + c - a = 2(b-c)p + (b+c+a)pp,$$
$$a + c - b = 2(a-c)q + (a+c+b)qq.$$

6. Ex utraque aequatione definiatur valor ipsius c:

$$c = \frac{a(1+pp) - b(1-2p-pp)}{1+2p-pp} = \frac{b(1+qq) - a(1-2q-qq)}{1+2q-qq},$$

unde fit

$$a + b + c = \frac{2a(1+p) + 4bp}{1+2p-pp} = \frac{2b(1+q) + 4aq}{1+2q-qq},$$

ex quo duplici valore ratio inter numeros a et b colligitur

$$a(1+p)(1+2q-qq) - 2aq(1+2p-pp)$$
$$= b(1+q)(1+2p-pp) - 2bp(1+2q-qq);$$

quamobrem statuo

$$a = 1 + q - pp - 2pq - ppq + 2pqq,$$
$$b = 1 + p - qq - 2pq - pqq + 2ppq$$

hincque fit

$$\frac{a+b+c}{2} = \frac{1+3p+q+pp-pq-7ppq-p^3+3p^3q}{1+2p-pp}$$

seu

$$a + b + c = 2 + 2p + 2q - 6pq.$$

7. Cum igitur sit

$$a + b = 2 + p + q - pp - qq - 4pq + ppq + pqq,$$

erit

$$c = p + q + pp + qq - 2pq - ppq - pqq$$

sicque binis formulis satisfit numeris a, b, c sequentes valores tribuendo

$$a = 1 + q - pp - 2pq - ppq + 2pqq,$$
$$b = 1 + p - qq - 2pq - pqq + 2ppq,$$
$$c = p + q + pp + qq - 2pq - ppq - pqq;$$

unde cum fiat

$$a + b + c = 2 + 2p + 2q - 6pq,$$
$$b - c = 1 - q - pp - 2qq + 3ppq,$$
$$a - c = 1 - p - qq - 2pp + 3pqq,$$

habebimus

$$f = 1 + 2p - q + pp - 2qq + 2pq - 3ppq,$$
$$g = 1 + 2q - p + qq - 2pp + 2pq - 3pqq$$

et

$$b - c + f = 2(1 + q)(1 + p - 2q),$$
$$a - c + g = 2(1 + p)(1 + q - 2p).$$

8. Iuvabit hinc etiam sequentes valores elicuisse

$$a + b - c = 2 - 2pp - 2qq - 2pq + 2ppq + 2pqq = 2(1-p)(1-q)(1+p+q),$$
$$b + c - a = 2p + 2pp - 2pq - 4pqq + 2ppq = 2p(1+q)(1+p-2q),$$
$$a + c - b = 2q + 2qq - 2pq - 4ppq + 2pqq = 2q(1+p)(1+q-2p),$$

ubi cavendum est, ne harum ulla evanescat, quia alioquin triangulum periret; excluduntur ergo sequentes valores

$$p = 0, \quad q = 0, \quad p = \pm 1, \quad q = \pm 1, \quad p + q = -1, \quad q = \frac{p+1}{2}, \quad p = \frac{q+1}{2}.$$

Praeterea vero etiam excludi oportet $1 + p + q = 3pq$, ne summa laterum evanescat. Tum vero etiam notetur esse

$$a - b = q - p + qq - pp + 3pqq - 3ppq = (q - p)(1 + p + q + 3pq),$$
$$g - f = 3q - 3p + 3qq - 3pp - 3pqq + 3ppq = 3(q - p)(1 + p + q - pq);$$

tandem vero est

$$aa + bb + cc = 2(1 - p - q + pp - pq + qq)(1 + 2(p + q) + (p + q)^2 + 3ppqq)$$

seu

$$aa + bb + cc = \tfrac{1}{2}\left((2 - p - q)^2 + 3(p - q)^2\right)\left((1 + p + q)^2 + 3ppqq\right).$$

9. Superest igitur, ut tertia conditio impleatur, quae in hac formula continetur

$$hh = (a + b)^2 + (a - b)^2 - cc = (a - b)^2 + (a + b + c)(a + b - c);$$

ubi si valores modo indicati substituantur, colligitur

$$hh = (q - p)^2(1 + p + q + 3pq)^2 + 4(1 - p)(1 - q)(1 + p + q)(1 + p + q - 3pq),$$

quae evolvitur in hanc formam

$$hh = 9ppqq(q - p)^2 + 6pq(p + q)(pp - 4pq + qq) + p^4 + 22p^3q$$
$$+ 6ppqq + 22pq^3 + q^4 - 2(p + q)^3 - 3(pp + 6pq + qq) + 4(p + q) + 4,$$

quae secundum potestates ipsius q disposita fit

$$hh = (1 + 3p)^2q^4 - 2(1 - 11p + 9pp + 9p^3)q^3 - 3(1 + 2p - 2pp + 6p^3 - 3p^4)q^2$$
$$+ 2(2 - 9p - 3pp + 11p^3 + 3p^4)q + (2 + p - pp)^2.$$

10. Alia methodus hanc aequationem resolvendi non patet, nisi ut more solito pro h eiusmodi expressio assumatur, qua substituta valor ipsius q per aequationem simplicem determinetur. Tum vero constat, quomodo uno valore

invento ex eo continuo plures elici queant. Ad minores autem valores eruendos generatim notetur, si fuerit

$$hh = AAq^4 + 2Bq^3 + Cqq + 2Dq + EE,$$

sequentibus positionibus[1]) negotium confectum iri:

1. Si $h = Aqq + \frac{B}{A}q \pm E$, fit $q = \frac{2A(AD \mp BE)}{BB - AA(C \mp 2AE)}$;
2. si $h = \pm Aqq + \frac{D}{E}q + E$, fit $q = \frac{DD - EE(C \mp 2AE)}{2E(BE \mp AD)}$;
3. si $h = Aqq + \frac{B}{A}q + \frac{C}{2A} - \frac{BB}{2A^3}$, fit $q = \frac{(BB - AAC)^2 - 4A^6EE}{4AA(B(BB - AAC) + 2A^4D)}$;
4. si $h = \frac{CEE - DD}{2E^3}qq + \frac{D}{E}q + E$, erit $q = \frac{4EE(D(DD - CEE) + 2BE^4)}{(DD - CEE)^2 - 4AAE^6}$.

11. Cum autem casus supra exclusi nostrae aequationi sponte satisfaciant et pro hh quadratum producant, ex iis novas formas similes elicere licet, unde deinceps novi valores idonei pro q erui queant.

Sit ergo primo

$$q = 1 + x$$

eritque

$$hh = (1 - p + x)^2\big(2 + 4p + (1 + 3p)x\big)^2 - 4x(1 - p)(2 + p + x)\big(2 - 2p + (1 - 3p)x\big),$$

quae evoluta praebet hanc formam

$$hh = (1 + 3p)^2x^4 + 2(1 + 23p + 9pp - 9p^3)x^3 + (-3 + 96p + 6pp - 72p^3 + 9p^4)xx + 4(1 - p)(-1 + 14p + 11pp - 6p^3)x + 4(1 - p)^2(1 + 2p)^2;$$

tum vero est

$$a + b - c = -2x(1 - p)(2 + p + x),$$
$$b + c - a = -2p(2 + x)(1 - p + 2x),$$
$$a + c - b = 2(1 + p)(1 + x)(2 - 2p + x).$$

Praestabit autem quovis casu, quo loco p determinatus valor assumitur, substitutionem in priori forma facere ac tum denique evolutionem instituere.

1) Vide L. Euler, *Vollständige Anleitung zur Algebra*, St. Petersburg 1770, Zweyter Theil, zweyter Abschnitt, Cap. 9; *Leonhardi Euleri Opera omnia*, series I, vol. 1, p. 396. F. R.

12. Sit igitur secundo

$$q = -1 - p + x$$

eritque

$$hh = (1+2p-x)^2(3p(1+p)-(1+3p)x)^2+4x(1-p)(2+p-x)(3p(1+p)+(1-3p)x)$$

atque

$$a + b - c = 2x(1-p)(2+p-x),$$
$$b + c - a = -2p(p-x)(3+3p-2x),$$
$$a + c - b = 2(1+p)(1+p-x)(3p-x).$$

Sit tertio

$$q = -1 + x$$

eritque

$$hh = (1+p-x)^2(2p-(1+3p)x)^2+4(1-p)(2-x)(p+x)(4p+(1-3p)x)$$

atque

$$a + b - c = 2(1-p)(2-x)(p+x),$$
$$b + c - a = 2px(3+p-2x),$$
$$a + c - b = 2(1+p)(1-x)(2p-x).$$

Sit quarto

$$q = \frac{1+p+x}{2}$$

eritque

$$16hh = (1-p+x)^2(3(1+p)^2+(1+3p)x)^2$$
$$+ 8(1-p)(1-p-x)(3+3p+x)(3(1-pp)+(1-3p)x)$$

atque

$$a + b - c = \tfrac{1}{2}(1-p)(1-p-x)(3(1+p)+x),$$
$$b + c - a = -px(3+p+x),$$
$$a + c - b = \tfrac{1}{2}(1+p)(1+p+x)(3(1-p)+x).$$

Sit denique quinto

$$q = \frac{1+p+x}{3p-1};$$

erit

$$(3p-1)^4hh = ((1-p)(1+3p)+x)^2(6p(1+p)+(1+3p)x)^2$$
$$+ 4(3p-1)^2x(1-p)(2(1-p)+x)(3p(1+p)+x)$$

atque

$$a+b-c=\frac{-2(1-p)(2(1-p)+x)(3p(1+p)+x)}{(3p-1)^2},$$

$$b+c-a=\frac{-2p(4p+x)(3(1-pp)+2x)}{(3p-1)^2},$$

$$a+c-b=\frac{2(1+p)(1+p+x)(6p(1-p)+x)}{(3p-1)^2}.$$

Semper autem est

$$f=b-c+(a+b+c)p \quad \text{et} \quad g=a-c+(a+b+c)q.$$

13. Hinc ergo satis patet innumerabiles solutiones nostri problematis inveniri posse. Invento enim pro q valore quocumque $q=n$ statuatur $q=n+x$ et aequatio resultans iterum huiusmodi formam habebit

$$hh=AAx^4+2Bx^3+Cxx+2Dx+EE,$$

unde novos valores pro x et h eruere licet methodo ante indicata. Cum autem hic potissimum solutiones in minoribus numeris desiderentur, litterae p valores simpliciores tribuamus, unde quidem valores 0 et ± 1 excludi conveniet.

CASUS I $p=-2$

14. Ob $p=-2$ habemus

$$a=-3+q-4qq, \quad b=-1+12q+qq, \quad c=2+q+3qq,$$

$$a+b+c=-2+14q,$$

$$f=1-17q-2qq, \quad g=-5-2q+7qq,$$

unde fieri oportet

$$hh=(q+2)^2(5q+1)^2-12(q-1)^2(7q-1),$$

quae evoluta abit in hanc formam

$$25q^4+26q^3+321qq-64q+16=hh.$$

Hic igitur est

$$A=5, \quad B=13, \quad C=321, \quad D=-32 \quad \text{et} \quad E=4$$

ideoque sequentes solutiones nascuntur:

1. Si $h = 5qq + \frac{13}{5}q \pm 4$, fit $q = \frac{10(40 \pm 13)}{1964 \mp 250}$;

2. si $h = \pm 5qq - 8q + 4$, fit $q = \frac{-257 \pm 40}{26 \pm 80}$;

ubi tertiam et quartam, quia numeros nimis magnos praebent, omitto.

15. Prioris solutionis signum superius praebet

$$q = \frac{10 \cdot 53}{1714} = \frac{5 \cdot 53}{857},$$

unde nascuntur numeri nimis magni, signum vero inferius

$$q = \frac{10 \cdot 27}{2214} = \frac{15}{123} = \frac{5}{41}, \quad \text{ergo} \quad h = -\frac{6066}{1681}.$$

Posterioris vero solutionis signum superius dat

$$q = -\frac{217}{106},$$

signum vero inferius

$$q = \frac{-297}{-54} = \frac{11}{2}, \quad \text{ergo} \quad h = -\frac{765}{4},$$

unde etiam reliquas litteras definiamus

$$a = -\frac{237}{2}, \quad b = \frac{381}{4}, \quad c = \frac{393}{4},$$

$$f = -153, \quad g = \frac{783}{4}, \quad h = -\frac{765}{4}.$$

Hos numeros multiplicemus per 4 ac dividamus per 3, ut obtineamus hanc solutionem satis simplicem

$$a = 158, \quad b = 127, \quad c = 131,$$

$$f = 204, \quad g = 261, \quad h = 255,$$

et quia litterae f, g, h, quae communem habent divisorem 3, in locum litterarum a, b, c substitui possunt, prodibit haec solutio multo simplicior

$$a = 68, \quad b = 87, \quad c = 85,$$

$$f = 158, \quad g = 127, \quad h = 131,$$

unde fit

$$aa + bb + cc = 2 \cdot 7 \cdot 19 \cdot 73,$$

qui factores utique sunt numeri formae $xx + 3yy$, uti natura rei postulat.

16. Cum loco q satisfaciat tam $+1$ quam -1, utamur hac substitutione

$$q = \frac{y+1}{y-1}$$

fietque

$$\tfrac{1}{4}(y-1)^4 hh = 81y^4 + 54y^3 - 99yy - 36y + 100,$$

unde ob

$$A = 9, \quad B = 27, \quad C = -99, \quad D = -18, \quad E = 10$$

habebimus has resolutiones:

1. Si $\frac{1}{2}(y-1)^2 h = 9yy + 3y \pm 10$, erit $y = \frac{-9(3 \pm 5)}{27(3 \pm 5)} = -\frac{1}{3}$;

2. si $\frac{1}{2}(y-1)^2 h = \pm 9yy - \frac{9}{5}y + 10$, erit $y = \frac{9 + 25(11 \pm 20)}{30(5 \pm 3)}$;

quarum prior dat $q = -\frac{1}{2}$, qui est casus exclusus formae $q = \frac{p+1}{2}$; altera vero suppeditat sub signo superiori

$$y = \frac{784}{240} = \frac{49}{15} \quad \text{et} \quad q = \frac{32}{17},$$

sub signo inferiori

$$y = -\frac{24 \cdot 9}{60} = -\frac{18}{5} \quad \text{et} \quad q = \frac{13}{23}.$$

17. Sit ergo $y = \frac{49}{15}$ et $q = \frac{32}{17}$ eritque

$$\frac{2 \cdot 17^2}{15^2} h = \frac{2504}{25}, \quad \text{hinc} \quad h = \frac{9 \cdot 1252}{289},$$

porro

$$a = -3 + \frac{32}{17} - \frac{4096}{289} = -\frac{4419}{289},$$

$$b = -1 + \frac{12\cdot 32}{17} + \frac{1024}{289} = \frac{7263}{289},$$

$$c = 2 + \frac{32}{17} + \frac{3072}{289} = \frac{4194}{289},$$

$$f = 1 - \frac{17\cdot 32}{17} - \frac{2048}{289} = -\frac{11007}{289},$$

$$g = -5 - \frac{2\cdot 32}{17} + \frac{7\cdot 1024}{289} = \frac{4635}{289}.$$

Omnes hi valores per 289 multiplicati per 9 deprimantur et habebitur ista solutio

$$a = 491, \quad b = 807, \quad c = 466,$$
$$f = 1223, \quad g = 515, \quad h = 1252,$$

quae eadem resultat ex altero casu invento $q = \frac{13}{23}$; unde est

$$aa + bb + cc = 2\cdot 7\cdot 19\cdot 43\cdot 97.$$

CASUS II $p = 2$

18. Pro hoc ergo casu primo habemus

$$a + b - c = -2(1-q)(3+q),$$
$$b + c - a = 4(1+q)(3-2q),$$
$$a + c - b = -6q(3-q),$$

$$b - c + f = \frac{b+c-a}{2}, \quad a - c + g = \frac{a+c-b}{q},$$

unde fit

$$hh = (q-2)^2(7q+3)^2 - 4(1-q)(3+q)(3-5q),$$

quae evoluta praebet hanc formam

$$hh = 49q^4 - 174q^3 + 9qq + 216q,$$

haecque facto $q = 3r$ transit in hanc simpliciorem

$$\frac{1}{81}hh = 49r^4 - 58r^3 + rr + 8r;$$

casus autem excludendi sunt $q = \pm 1$, $q = -3$, $q = \frac{3}{2}$, $q = 3$ et $q = \frac{3}{5}$.

19. Cum hic sit

$$A = 7, \quad B = -29, \quad C = 1, \quad D = 4, \quad E = 0,$$

ex solutione prima sumto

$$\frac{1}{9}h = 7rr - \frac{29}{7}r$$

erit

$$r = \frac{14 \cdot 28}{841 - 49} = \frac{49}{99} \quad \text{et} \quad q = \frac{49}{33} \quad \text{hincque} \quad h = -\frac{7 \cdot 470}{11 \cdot 99},$$

tum vero porro

$$a + b - c = \frac{2 \cdot 16 \cdot 148}{33 \cdot 33},$$

$$b + c - a = \frac{4 \cdot 82 \cdot 1}{33 \cdot 33},$$

$$a + c - b = -\frac{6 \cdot 49 \cdot 50}{33 \cdot 33},$$

$$b - c + f = \frac{4 \cdot 41}{33 \cdot 33}, \quad a - c + g = -\frac{6 \cdot 50}{33};$$

multiplicentur hi valores omnes per $\frac{33 \cdot 33}{4}$; erit

$$\begin{aligned} a + b - c &= 1184, & 2c &= -3593, & 2f &= -4777, \\ b + c - a &= 82, & 2a &= -2491, & 2g &= -6052^{1}), \\ a + c - b &= -3675, & 2b &= +1266, & 2h &= -1645. \\ a + b + c &= -2409, \end{aligned}$$

Duplicatis ergo valoribus prodit haec solutio

$$a = 2491, \quad b = 1266, \quad c = 3593,$$
$$f = 4777, \quad g = 6052^{1}), \quad h = 1645,$$

hinc vero est

$$aa + bb + cc = 2 \cdot 19 \cdot 31 \cdot 43 \cdot 409.$$

20. Transformemus aequationem nostram ponendo

$$r = \frac{y+1}{y-1}$$

orieturque

$$\frac{1}{324}hh(y-1)^4 = 25 + 82y + 73yy + 16y^3;$$

1) Editio princeps (atque etiam *Comment. arithm.*): $2g = -6092$. Correxit F. R.

statuatur

$$\frac{1}{18}h(y-1)^2 = 5 + \frac{41}{5}y$$

fitque

$$y = -\frac{9}{25}, \quad \text{hinc} \quad r = -\frac{8}{17} \quad \text{et} \quad q = -\frac{24}{17} \quad \text{ideoque} \quad h = \frac{45 \cdot 128}{289}.$$

Porro

$$a+b-c = -\frac{2 \cdot 41 \cdot 27}{289}, \qquad b-c+f = -\frac{2 \cdot 7 \cdot 99}{289},$$

$$b+c-a = -\frac{4 \cdot 7 \cdot 99}{289}, \qquad a-c+g = -\frac{6 \cdot 17 \cdot 75}{289}.$$

$$a+c-b = \frac{6 \cdot 24 \cdot 75}{289},$$

Multiplicentur omnes hi valores per $\frac{289}{9}$ et habebitur

$$a+b-c = -246, \quad 2c = 892, \quad h = 640,$$
$$b+c-a = -308, \quad 2a = 954, \quad b-c+f = -154, \quad f = 569,$$
$$a+c-b = 1200, \quad 2b = -554, \quad a-c+g = -850, \quad g = -881,$$
$$a+b+c = 646,$$

unde colligitur haec solutio

$$a = 477, \quad b = 277, \quad c = 446,$$
$$f = 569, \quad g = 881, \quad h = 640.$$

21. In aequatione per q expressa [§ 18] statuatur

$$q = \frac{y+1}{y-1}$$

ac reperietur

$$\frac{1}{4}hh(y-1)^4 = 25y^4 - 146y^3 + 69yy + 244y + 4,$$

ubi

$$A = 5, \quad B = -73, \quad C = 69, \quad D = 122, \quad E = 2.$$

Ergo:

1. Si $\frac{1}{2}h(y-1)^2 = 5yy - \frac{73}{5}y \pm 2$, fit

$$y = \frac{10(610 \pm 146)}{73^2 - 25(69 \mp 20)} = \frac{5(305 \pm 73)}{901 \pm 125};$$

2. si $\frac{1}{2}h(y-1)^2 = \pm 5yy + 61y + 2$, fit

$$y = \frac{4\cdot 61^2 - 4(69 \mp 20)}{4(-146 \mp 610)} = \frac{1826 \pm 10}{-73 \mp 305}.$$

Ex priori dat signum superius

$$y = \frac{5\cdot 378}{1026} = \frac{35}{19} \quad \text{et} \quad q = \frac{27}{8},$$

at signum inferius

$$y = \frac{5\cdot 232}{776} = \frac{145}{97} \quad \text{et} \quad q = \frac{121}{24}.$$

Ex secunda dat signum superius

$$y = -\frac{1836}{378} = -\frac{34}{7} \quad \text{et} \quad q = \frac{27}{41},$$

at signum inferius

$$y = \frac{1816}{232} = \frac{227}{29} \quad \text{et} \quad q = \frac{128}{99}.$$

Ex valore $q = \frac{27}{8}$ colligimus hanc solutionem

$$a = 404, \quad b = 377, \quad c = 619,$$
$$f = 3\cdot 314, \quad g = 3\cdot 325, \quad h = 3\cdot 159,$$

ubi fit

$$aa + bb + cc = 2\cdot 3\cdot 7\cdot 13^2\cdot 97.$$

Ex valore autem $q = \frac{27}{41}$ nascitur ista solutio

$$a = 823, \quad b = 607, \quad c = 134,$$
$$f = 3\cdot 103, \quad g = 3\cdot 337, \quad h = 3\cdot 480^{1}),$$

ubi est

$$aa + bb + cc = 2\cdot 3\cdot 7\cdot 19\cdot 31\cdot 43;$$

notandumque est hic bina latera tertio non esse maiora.

22. Pluribus casibus involvendis hic non immoror, sed potius animadverto methodum, qua hic sum usus, non satis videri naturalem et ad scopum

1) In editione principe (atque etiam in *Comment. arithm.*) litterae a, b, c atque f, g, h inter se permutatae sunt. F. R.

accommodatam, propterea quod nulla suppeditat criteria solutiones simpliciores distinguendi. Desideratur ergo [adhuc naturalis et simplex methodus] tam pro hoc problemate quam pro aliis similibus, quarum solutio ad huiusmodi formam

$$Ax^4 + Bx^3 + Cx^2 + Dx + E$$

ad quadratum reducendam revocatur. Atque in hoc quidem problemate solutio a quantitate $aa + bb + cc$ inchoanda videtur, quae huiusmodi numero $2(xx + 3yy)$ certe est aequalis; et cum debeat esse

$$4(xx + 3yy) = ff + 3aa = gg + 3bb = hh + 3cc,$$

evidens est numerum $xx + 3yy$ factores habere debere, quos constat eiusdem esse formae. Statui igitur poterit

$$xx + 3yy = (mm + 3nn)(pp + 3qq)(rr + 3ss)$$

et $4(xx + 3yy)$ octo modis ad formam $AA + 3BB$ referri potest, unde ternas illas eligi oportet. Foret nempe

$$a = 2m(ps + qr) + 2n(3qs - pr),$$
$$b = m((3q + p)s \pm (q - p)r) \pm n(3(q - p)s \mp (3q + p)r),$$
$$c = m((3q - p)s \pm (q + p)r) \pm n(3(q + p)s \mp (3q - p)r)$$

et effici restat

$$aa + bb + cc = 4(xx + 3yy).$$

Verum hoc modo calculus fit satis prolixus, nisi forte certis artificiis tractabilior reddi potest.

RESOLUTIO AEQUATIONIS
$Ax^2 + 2Bxy + Cy^2 + 2Dx + 2Ey + F = 0$
PER NUMEROS TAM RATIONALES QUAM INTEGROS[1])

Commentatio 452 indicis ENESTROEMIANI
Novi commentarii academiae scientiarum Petropolitanae 18 (1773), 1774, p. 185—197
Summarium ibidem p. 21—22

SUMMARIUM

Forma huius aequationis tam late patet, ut insignem Analyseos DIOPHANTEAE partem complecti censenda sit. Prouti coefficientibus A, B, C etc. varii diversae indolis valores tribuuntur, plures quoque inde resultant casus diversis vulgo methodis pertractati. In hac dissertatione Ill. Auctor singularem explicat modum istam aequationem resolvendi, atque ita quidem, ut solutio non ad rationales modo, sed integros quoque numeros possit adplicari et ab omni radicis extractione sit libera. Casus dantur haud pauci, quibus haec aequatio fit impossibilis, unde Ill. Auctor unicum saltem casum, quo illi satisfiat, supponit esse cognitum; ex quo qua ratione alii sive numero finiti sive infiniti erui queant, deinceps explicat. Peculiari autem iudicio opus est, utrum aequatio proposita solutionem admittat in numeris integris necne. Consideretur hunc in finem formula $B^2 - AC$; quae si fuerit numerus positivus non quadratus, semper impetrari possunt bini numeri integri aequationi satisfacientes, idque adeo infinitis modis. Duplicem Ill. Auctor resolutionem tradit aequationis propositae, quarum posterior ideo potissimum peculiari attentione digna est, quod ex doctrina irrationalium est petita; quae quomodo in Analysi indeterminata seu DIOPHANTEA

1) Confer hac cum dissertatione L. EULERI Commentationes 29 et 279 nota p. 75 laudatas, porro Commentationes 323 et 454 huius voluminis atque Commentationem 559 voluminis sequentis. F. R.

in usum possit vocari, minime obvium est. Eximiam vero eius in eiusmodi problematibus adplicationem iam pridem uberius docuit Ill. Auctor in *Algebra*[1]) sua ruthenice et germanice apud nos typis impressa. Casibus particularibus aequationis datae evolvendis Ill. Auctor non censuit esse immorandum, utpote qui iam passim satis superque sunt pertractati.

Haec forma latissime patens, quae insignem partem Analyseos DIOPHANTEAE complectitur, pro varia indole numerorum A, B, C, D, E, F plures in se continet casus, qui vulgo diversis methodis tractari solent. Hic autem singulari modo eius resolutionem sine radicis extractione ita docebo, ut solutio non solum ad numeros rationales, sed etiam integros accommodari possit.

1. In genere quidem resolutionem huius aequationis tradere non licet, quia saepe usu venire potest, ut ea sit impossibilis; certissimum autem criterium possibilitatis solutionis sine dubio est, si unicus saltem casus, quo huic aequationi satisfiat, fuerit cognitus. Ponamus igitur hoc contingere casu, quo $x=a$ et $y=b$, ita ut revera sit

$$Aa^2+2Bab+Cb^2+2Da+2Eb+F=0,$$

et quemadmodum ex hoc casu cognito alii sive numero finiti sive infiniti erui queant, hic sum ostensurus.

2. Subtrahatur ista aequatio ab ipsa proposita generali, ut obtineatur haec

$$A(x^2-a^2)+2B(xy-ab)+C(y^2-b^2)+2D(x-a)+2E(y-b)=0,$$

cuius singula membra praeter secundum factorem habent vel $x-a$ vel $y-b$; at membrum secundum pluribus modis in duas partes resolvi potest, quarum altera habeat factorem $x-a$, altera $y-b$:

$$xy-ab=x(y-b)+b(x-a)=y(x-a)+a(y-b);$$

ut autem ambae litterae x et y parem rationem ineant, hac resolutione utamur

$$2(xy-ab)=(x-a)(y+b)+(x+a)(y-b);$$

1) Vide notam 1 p. 309. F. R.

quo facto aequatio nostra sequentem induet formam

$$A(x-a)(x+a)+B(x-a)(y+b)+B(x+a)(y-b)+C(y-b)(y+b)$$
$$+2D(x-a)+2E(y-b)=0.$$

3. Consideretur nunc ratio quantitatum $x-a$ et $y-b$ tamquam data ac statuatur

$$\frac{x-a}{y-b}=\frac{p}{q},$$

ita ut sit $qx-aq=py-bp$, qua ratione introducta nostra aequatio evadet

$$Ap(x+a)+Bp(y+b)+Bq(x+a)+Cq(y+b)+2Dp+2Eq=0,$$

ex quibus binis aequationibus utramque quantitatem quaesitam x et y definire licebit. Quum enim posterior sit

$$(x+a)(Ap+Bq)+(y+b)(Bp+Cq)+2Dp+2Eq=0,$$

prior vero praebeat

$$y=\frac{qx-aq+bp}{p},$$

hic valor in illa substitutus dat

$$(Ap^2+2Bpq+Cq^2)x+Aap^2+2Bbp^2+2Cbpq-Caq^2+2Dp^2+2Epq=0,$$

unde colligitur

$$x=\frac{-a(Ap^2-Cq^2)-2b(Bpp+Cpq)-2Dp^2-2Epq}{Ap^2+2Bpq+Cq^2}$$

hincque

$$y=\frac{+b(Ap^2-Cq^2)-2a(Bqq+Apq)-2Dpq-2Eq^2}{Ap^2+2Bpq+Cq^2}.$$

4. Ecce ergo iam sumus assecuti solutionem generalissimam aequationis propositae in numeris rationalibus; quia enim ambos numeros p et q pro arbitrio assumere licet, evidens est omnes plane solutiones in his formulis contineri debere. Quod autem solutiones in numeris integris attinet, manifestum est tales exhiberi non posse, nisi ambo numeratores illarum fractionum divisionem admittant per communem denominatorem $Ap^2+2Bpq+Cq^2$, id

quod fieri nequit, nisi hic denominator ad numerum satis exiguum se reduci patiatur. Statim ergo hinc excludi oportet casus, quibus $B^2 < AC$ sive quibus $AC-B^2$ est numerus positivus; tum enim, quicumque valores loco p et q accipiantur, formulam $Ap^2+2Bpq+Cq^2$ non infra certum valorem deprimere licebit.

5. Quodsi ergo numeri A, B et C ita fuerint comparati, ut per certos numeros p et q formula $Ap^2+2Bpq+Cq^2$ ad exiguum numerum, sive unitatem sive binarium tam positive quam negative sumtum, redigi queat, omnes partes binarum formularum pro x et y inventarum abibunt in numeros integros. Posito autem isto numero $=\omega$, ita ut his casibus sit ω vel ± 1 vel ± 2, ob $Ap^2+2Bpq+Cq^2=\omega$ reperitur

$$p=\frac{-Bq\pm\sqrt{((BB-AC)q^2+A\omega)}}{A};$$

sic formula

$$(BB-AC)q^2+A\omega$$

debebit esse quadratum, quod quidem plerumque fieri poterit, quia pro ω sumi potest vel $+1$ vel -1 vel $+2$ vel -2, dummodo $BB-AC$ fuerit numerus positivus non quadratus, etiamsi sine dubio dantur casus, quibus ω maiorem sortitur valorem. Tum vero habebitur

$$x=\frac{a}{\omega}(Cq^2-Ap^2)-\frac{2b}{\omega}(Bpp+Cpq)-\frac{2D}{\omega}p^2-\frac{2E}{\omega}pq,$$

$$y=\frac{b}{\omega}(Ap^2-Cq^2)-\frac{2a}{\omega}(Bqq+Apq)-\frac{2D}{\omega}pq-\frac{2E}{\omega}q^2.$$

6. Utrum igitur nostra aequatio admittat solutiones in numeris integris necne, iudicium facillime instituitur. Consideretur enim formula $BB-AC$; quae si fuerit numerus positivus non quadratus, semper adeo infinitis modis numerum q assignare licebit, ut formula illa radicalis abeat in numerum rationalem, indeque definietur alter numerus p, quibus adhibitis impetrabimus binos numeros satisfacientes x et y. Sufficiet autem pro q unicum valorem idoneum invenisse, dum ex eo pro x et y successive innumerabiles valores satisfacientes deduci possunt, id quod operae pretium erit clarius ostendisse.

Ponamus scilicet ex numeris primo satisfacientibus a et b hoc modo prodiisse sequentes

$$x = \zeta a + \eta b + \theta \quad \text{et} \quad y = \lambda a + \mu b + \nu,$$

atque si iam hi pro a et b adhibeantur, per easdem formulas novos deducemus valores pro x et y, qui denuo loco a et b assumti praebebunt iterum alios idoneos valores pro x et y, et ita porro.

7. Sint numeri, qui hoc modo successive pro x reperiuntur,

$$a,\ a',\ a'',\ a''',\ a'''' \text{ etc.},$$

numeri autem pro y respondentes sint

$$b,\ b',\ b'',\ b''',\ b'''' \text{ etc.}$$

atque habebimus sequentes aequationes

$$\begin{aligned} a' &= \zeta a + \eta b + \theta, & b' &= \lambda a + \mu b + \nu, \\ a'' &= \zeta a' + \eta b' + \theta, & b'' &= \lambda a' + \mu b' + \nu, \\ a''' &= \zeta a'' + \eta b'' + \theta, & b''' &= \lambda a'' + \mu b'' + \nu \\ &\text{etc.} & &\text{etc.} \end{aligned}$$

Ex his relationibus eliminando litteras b, b' satis simplex relatio concluditur inter valores continuos a, a', a'', quae ita se habet

$$a'' = (\zeta + \mu)a' + (\eta\lambda - \zeta\mu)a + \theta(1 - \mu) + \eta\nu;$$

simili modo eliminando litteras a, a'

$$b'' = (\zeta + \mu)b' + (\eta\lambda - \zeta\mu)b + \theta\lambda + \nu(1 - \zeta),$$

unde patet utramque seriem esse recurrentem secundi ordinis secundum eandem scalam relationis

$$\zeta + \mu, \quad \eta\lambda - \zeta\mu;$$

utrimque autem insuper numerum quemdam absolutum addi oportet.

8. Cognita hac scala relationis formetur haec aequatio quadratica

$$z^2=(\zeta+\mu)z+(\eta\lambda-\zeta\mu),$$

cuius binae radices sunt

$$z=\frac{\zeta+\mu}{2}\pm\sqrt{\left(\left(\frac{\zeta-\mu}{2}\right)^2+\eta\lambda\right)},$$

quarum potestatibus exprimi possunt termini generales utriusque seriei. Quo hoc clarius reddatur, sit prioris seriei

$$a,\ a',\ a'',\ a'''\ \text{etc.}$$

terminus quotuscumque $=x$, alterius vero seriei

$$b,\ b',\ b'',\ b'''\ \text{etc.}$$

terminus generalis y, et posito brevitatis gratia

$$\frac{\zeta+\mu}{2}=r\quad\text{et}\quad\sqrt{\left(\left(\frac{\zeta-\mu}{2}\right)^2+\eta\lambda\right)}=\sqrt{s}$$

pro priori serie statuatur[1])

$$x=f(r+\sqrt{s})^n+g(r-\sqrt{s})^n+h$$

eritque valor sequens

$$x'=f(r+\sqrt{s})\,(r+\sqrt{s})^n+g(r-\sqrt{s})\,(r-\sqrt{s})^n+h$$

huncque sequens

$$x''=f(r+\sqrt{s})^2(r+\sqrt{s})^n+g(r-\sqrt{s})^2(r-\sqrt{s})^n+h.$$

Quare cum ex lege progressionis esse debeat

$$x''=(\zeta+\mu)x'+(\eta\lambda-\zeta\mu)x+\theta(1-\mu)+\eta\nu,$$

si illi valores substituantur, potestates sponte se destruunt ac resultat

$$h=\frac{\theta(1-\mu)+\eta\nu}{(1-\mu)(1-\zeta)-\eta\lambda}.$$

---

1) Vide L. Euleri *Introductionem in analysin infinitorum*, Lausannae 1748, t. I cap. XIII; *Leonhardi Euleri Opera omnia*, series I, vol. 8. Vide etiam notas p. 584 voluminis praecedentis. F. R.

Pro coefficientibus autem f et g considerentur termini initiales ante definiti et facto quidem $n = 0$ prodeat $x = a$ hincque erit

$$a = f + g + h;$$

tum vero ponatur $n = 1$, ut prodeat

$$x = a' = \zeta a + \eta b + \theta$$

fiatque ea

$$= f(r + \sqrt{s}) + g(r - \sqrt{s}) + h,$$

et quia $f + g = a - h$, erit

$$a' = (a - h)r + (f - g)\sqrt{s} + h$$

hincque

$$f - g = \frac{a'}{\sqrt{s}} - \frac{(a-h)r}{\sqrt{s}} - \frac{h}{\sqrt{s}} = \frac{a' - ar - h(1-r)}{\sqrt{s}}.$$

Eodem modo pro altera serie recurrente terminus generalis y reperietur, ita ut in genere nihil amplius desiderari possit.

9. Ceterum, uti iam innuimus, dantur casus, quibus formula

$$App + 2Bpq + Cqq$$

neque ad unitatem neque ad binarium deprimi potest; conveniet igitur litteras p et q ita assumi, ut huic formulae minimus valor concilietur, unde non parum egregium nascitur problema, quo datis numeris A, B, C quaeruntur valores litterarum p et q in integris, ut formula $App + 2Bpq + Cqq$ minimum omnium accipiat valorem.

ALIA RESOLUTIO EIUSDEM AEQUATIONIS

10. Quum tres termini initiales per A multiplicati factores habeant

$$(Ax + By + y\sqrt{(B^2 - AC)}), \quad (Ax + By - y\sqrt{(B^2 - AC)}),$$

totam aequationem sub tali forma repraesentare licebit

$$\big(Ax + By + M + (y + N)\sqrt{(B^2 - AC)}\big)\big(Ax + By + M - (y + N)\sqrt{(B^2 - AC)}\big) = 0,$$

quae evoluta praebet

$$A^2x^2+2ABxy+ACy^2+2AMx+(2MB-2NB^2+2ACN)y \\ +M^2-B^2N^2+ACN^2-O=0,$$

qua cum forma proposita comparata assequimur

$$2AD=2AM, \quad D=M,$$

$$2AE=2MB-2N(B^2-AC),$$

$$AF=M^2-N^2(B^2-AC)-O$$

hincque

$$M=D, \quad N=\frac{BD-AE}{B^2-AC}, \quad O=D^2-AF-\frac{(BD-AE)^2}{B^2-AC}.$$

11. Inventis igitur valoribus M, N et O ponatur brevitatis gratia

$$BB-AC=k,$$

ut aequatio nostra per factores irrationales expressa sit

$$(Ax+By+D+(y+N)\sqrt{k})\,(Ax+By+D-(y+N)\sqrt{k})=O.$$

Et quia assumimus unam solutionem iam esse cognitam, quae sit $x=a$ et $y=b$, habebimus quoque

$$(Aa+Bb+D+(b+N)\sqrt{k})(Aa+Bb+D-(b+N)\sqrt{k})=O,$$

quocirca bina haec producta inter se aequalia esse debebunt; statuamus hinc brevitatis gratia

$$Ax+By+M=P, \quad y+N=Q,$$

$$Aa+Bb+M=G, \quad b+N=H,$$

ita ut nostra binorum productorum aequalitas fiat

$$(P+Q\sqrt{k})(P-Q\sqrt{k})=O=(G+H\sqrt{k})(G-H\sqrt{k}),$$

ubi notandum, si prior factor illius producti alterutri factori istius aequalis ponatur, tum quoque posteriorem factorem illius sponte alteri huius aequalem esse futurum, quoniam discrimen tantum in signo quantitatis radicalis $\sqrt{k}$

est situm. Manifestum autem est, si factores priores inter se aequales statuantur et partes tam rationales quam irrationales seorsim aequentur, scilicet $P = G$ et $Q = H$, inde ipsum casum cognitum esse proditurum, nempe $x = a$ et $y = b$.

12. Sin autem hoc modo prior factor illius producti posteriori huius aequetur, ut sit

$$P + Q\sqrt{k} = G - H\sqrt{k},$$

nova solutio hinc elicietur; aequalitas enim $Q = -H$ dabit

$$y + N = -b - N$$

sive

$$y = -b - 2N,$$

unde altera conditio $P = G$ dabit

$$Ax - Bb - 2NB + M = Aa + Bb + M$$

seu

$$Ax = Aa + 2Bb + 2NB$$

hincque

$$x = a + \frac{2B(b+N)}{A}.$$

Ergo ex qualibet solutione iam inventa, puta $x = a$ et $y = b$, alia quasi sociata ex ea facillime concluditur, quippe quae, si loco M et N valores assumti restituantur, praebebit

$$x = a + \frac{2B}{A}\left(b + \frac{BD - AE}{B^2 - AC}\right), \quad y = -b - \frac{2(BD - AE)}{B^2 - AC}.$$

Quae quidem solutio numeris fractis continetur, nisi forte numeratores fuerint per denominatores suos divisibiles.

13. Quo autem hinc plures atque adeo infinitas solutiones eliciamus, in subsidium vocemus formulam

$$s = \sqrt{(kr^2 + 1)},$$

quippe quae methodo PELLIANA[1]) semper infinitis modis resolvi potest, dummodo k non fuerit vel numerus negativus vel numerus quadratus. Quum enim hinc fiat

$$ss - kr^2 = 1,$$

nostram aequationem hac forma repraesentare poterimus

$$P^2 - kQ^2 = (G^2 - kH^2)(ss - kr^2).$$

Hincque per factores irrationales statuamus

$$P + Q\sqrt{k} = (G + H\sqrt{k})(s + r\sqrt{k}) = Gs + kHr + (Gr + Hs)\sqrt{k};$$

sic enim simul toti aequationi satisfiet, siquidem partes rationales et irrationales seorsim aequantur. At irrationales praebent $Q = Gr + Hs$,

$$y + N = Aar + Bbr + Mr + bs + Ns,$$
$$y = Aar + Bbr + Mr + bs + Ns - N.$$

At partes rationales dant $P = Gs + kHr$ seu

$$Ax + By + D = Aas + Bbs + Ds + kbr + kNr,$$

unde

$$x = s\left(a + \frac{D - BN}{A}\right) + r\left(\frac{kb + kN - B^2b - BD}{A} - Ba\right) + \frac{BN - D}{A}.$$

14. Nunc igitur loco litterarum M et N restituantur valores supra inventi atque pro nostris quantitatibus quaesitis x et y sequentes reperiuntur formulae[2]), si scilicet loco k scribatur $B^2 - AC$,

$$x = \left(a + \frac{BE - CD}{B^2 - AC}\right)s + (Ba + Cb + E)(-r) + \frac{CD - BE}{B^2 - AC},$$

$$y = \left(b + \frac{BD - AE}{B^2 - AC}\right)s + (Bb + Aa + D)r \quad + \frac{AE - BD}{B^2 - AC},$$

ubi permutatio, quae inter litteras x et y locum habet, manifesto elucet.

---

1) Sed vide de hac falsa nominatione notam 1 p. 77. F. R.

2) Ponendo $s = p$ et $-r = q$ hae formulae transeunt in illas, quas EULERUS in paragrapho 4 Commentationis 323 huius voluminis sine demonstratione exposuit. F. R.

15. Quodsi hi valores pro x et y inventi loco a et b substituantur in istis formulis, pro x et y inde novi valores eruentur, qui denuo loco a et b sumti alios novos pro x et y praebebunt, et ita porro in infinitum. Verum omnes istos valores simul in formulis generalibus complecti licebit, uti iam supra fecimus. Sequenti autem modo idem negotium multo commodius et succinctius conficietur.

16. Quoniam $ss - krr = 1$ atque adeo omnes potestates ipsius $ss - krr$ etiam unitati aequantur, ponere poterimus

$$P^2 - kQ^2 = (G^2 - kH^2)(ss - krr)^n$$

hincque per factores irrationales

$$P + Q\sqrt{k} = (G + H\sqrt{k})(s + r\sqrt{k})^n;$$

quia autem huius potestatis aliae partes sunt rationales, aliae irrationales per $\sqrt{k}$ affectae, statuamus

$$(s + r\sqrt{k})^n = S + R\sqrt{k}$$

atque ut ante hinc sequentes valores pro x et y eliciemus

$$x = \left(a + \frac{BE - CD}{B^2 - AC}\right)S + (Ba + Cb + E)(-R) + \frac{CD - BE}{B^2 - AC},$$

$$y = \left(b + \frac{BD - AE}{B^2 - AC}\right)S + (Bb + Aa + D)R \qquad + \frac{AE - BD}{B^2 - AC}.$$

17. Quum autem sit

$$S + R\sqrt{k} = (s + r\sqrt{k})^n,$$

erit eodem modo

$$S - R\sqrt{k} = (s - r\sqrt{k})^n,$$

unde deducimus

$$S = \frac{1}{2}(s + r\sqrt{k})^n + \frac{1}{2}(s - r\sqrt{k})^n$$

et

$$R = \frac{1}{2\sqrt{k}}(s + r\sqrt{k})^n - \frac{1}{2\sqrt{k}}(s - r\sqrt{k})^n,$$

quibus valoribus substitutis obtinebimus

$$x=\left(\frac{BE-CD}{2(B^2-AC)}+\frac{a\sqrt{k}-Ba-Cb-E}{2\sqrt{k}}\right)(s+r\sqrt{k})^n$$
$$+\left(\frac{BE-CD}{2(B^2-AC)}+\frac{a\sqrt{k}+Ba+Cb+E}{2\sqrt{k}}\right)(s-r\sqrt{k})^n+\frac{CD-BE}{B^2-AC},$$
$$y=\left(\frac{BD-AE}{2(B^2-AC)}+\frac{b\sqrt{k}+Bb+Aa+D}{2\sqrt{k}}\right)(s+r\sqrt{k})^n$$
$$+\left(\frac{BD-AE}{2(B^2-AC)}+\frac{b\sqrt{k}-Bb-Aa-D}{2\sqrt{k}}\right)(s-r\sqrt{k})^n+\frac{AE-BD}{B^2-AC},$$

et quia $k=B^2-AC$, hae formulae ita simpliciores evadent

$$x=\frac{1}{2k}(BE-CD+ak-(Ba+Cb+E)\sqrt{k})(s+r\sqrt{k})^n$$
$$+\frac{1}{2k}(BE-CD+ak+(Ba+Cb+E)\sqrt{k})(s-r\sqrt{k})^n+\frac{1}{k}(CD-BE),$$
$$y=\frac{1}{2k}(BD-AE+bk+(Bb+Aa+D)\sqrt{k})(s+r\sqrt{k})^n$$
$$+\frac{1}{2k}(BD-AE+bk-(Bb+Aa+D)\sqrt{k})(s-r\sqrt{k})^n+\frac{1}{k}(AE-BD).$$

18. Ante [§ 12] iam vidimus quamlibet solutionem $x=a$ et $y=b$ suppeditare aliam sibi quasi sociam

$$x=a+\frac{2B}{A}\left(b+\frac{BD-AE}{B^2-AC}\right) \quad \text{et} \quad y=-b-\frac{2(BD-AE)}{B^2-AC};$$

quia autem ex ipsa indole nostrae aequationis litterae x et y inter se permutari possunt, dummodo

1. litterae a et b,
2. litterae A et C

et

3. litterae D et E

inter se permutentur, haec consideratio nobis adhuc aliam solutionem suppeditabit, scilicet

$$x = -a - \frac{2(BE-CD)}{B^2-AC}, \quad y = +b + \frac{2B}{C}\left(a + \frac{BE-CD}{B^2-AC}\right).$$

Sicque ex eadem solutione duae novae sociae obtinentur.

19. Haec methodus posterior aequationem nostram resolvendi eo magis est notatu digna, quod ex doctrina irrationalium est petita, cuius alioquin nullus videtur esse usus in Analysi DIOPHANTEA. Eximium autem huius doctrinae usum iam pridem in *Algebra*[1]) mea Ruthenice et Germanice edita fusius ostendi. Ceterum ad casus particulares nostrae aequationis propositae hic descendere non opus videtur, quum huiusmodi casus iam passim[2]) satis superque sint pertractati.

---

1) Vide L. EULER, *Vollständige Anleitung zur Algebra*, St. Petersburg 1770, Zweyter Theil, zweyter Abschnitt; *LEONHARDI EULERI Opera omnia*, series I, vol. 1 (vide etiam ibidem notam p. 3). F. R.

2) Vide exempli gratia L. EULERI Commentationes 29 et 279 nota p. 75 laudatas atque Commentationem 323 huius voluminis. F. R.

DE RESOLUTIONE IRRATIONALIUM PER FRACTIONES CONTINUAS UBI SIMUL NOVA QUAEDAM ET SINGULARIS SPECIES MINIMI EXPONITUR[1])

Commentatio 454 indicis ENESTROEMIANI
Novi commentarii academiae scientiarum Petropolitanae 18 (1773), 1774, p. 218—244
Summarium ibidem p. 24—27

SUMMARIUM

Cohaeret dissertationis huius argumentum cum resolutione aequationis

$$Ax^2 + 2Bxy + Cy^2 + 2Dx + 2Ey + F = 0,$$

quam Ill. Auctor in antecedentium dissertationum una[2]) pertractavit. Totum istud negotium eo rediit, ut eiusmodi pro x et y investigarentur valores in numeris integris, quibus formulae

$$Ax^2 + 2Bxy + Cy^2$$

minimus valor induceretur. Tres autem hic casus occurrunt distinguendi; aut enim formae istius factores sunt reales et diversi inter se, id est, $B^2 - AC$ positivum; aut reales, sed inter se aequales, quod fit, si $B^2 - AC = 0$; aut denique imaginarii, si $B^2 - AC$ fuerit negativum. Secundus et tertius casus ab Ill. Auctore est praetermissus, quandoquidem quaestio minimi in utroque nulla plane difficultate laborat. Solus ergo relinquitur ille casus, ubi factores sunt reales et inter se diversi, ubi quidem haec superaddenda est conditio, ut $B^2 - AC$ non sit numerus quadratus; quod si acciderit, factores evaderent rationales et nulla de minimo quaestio locum haberet, cum formulae propositae

---

1) Confer hac cum dissertatione Commentationem 323 huius voluminis. F. R.

2) Vide notam p. 312. F. R.

valor adeo ad nihilum possit redigi. Numerus itaque $B^2 - AC$ debet esse formae $mx^2 - ny^2$ denotantibus litteris m et n numeros integros; atque hic iam quaestio notatu digna occurrit, quinam valores integri litteris x et y sint tribuendi, ut ipsa formula minimum omnium adipiscatur valorem. Notum est, si vel m vel n ponatur $= 1$, istam formulam adeo ad unitatem usque posse deprimi; ex theoremate enim celebri PELLIANO[1]) constat semper effici posse $x^2 - ny^2 = 1$, dummodo n non fuerit numerus quadratus. Dantur insuper praeter hos duos et alii casus, quibus formulae propositae valor in unitatem abit, veluti $3x^2 - 2y^2 = 1$ positis $x = 1$ et $y = 1$, uti et $9x^2 - 5y^2 = 1$ posito $x = 3$ et $y = 4$. Evenire autem utique potest, ut formulae valor minimus unitatem superet; ac tum difficillima plerumque est determinatio minimi quaesiti, veluti fit in formula $7x^2 - 13y^2$, quae deprimitur ad binarium posito $x = 15$ et $y = 11$; quod quidem de minimo iudicium calculos eo operosiores postulat, quo maiores fuerint numeri m et n. Ex hactenus allatis abunde perspicitur expositionem methodi in his casibus minimum investigandi haud exiguum Analysi incrementum adferre; atque id ipsum est, in quo explicando Ill. Auctor hic versatur.

Antequam ipsius methodi explicationem traderet, e re fore censuit ostendere semper infinitis modis idem minimum posse obtineri; ipsa vero methodus ex eo est petita, quod casu minimi valor formulae $mx^2 - ny^2$ propius ad nihilum quam ullo alio accedat; quocirca negotium eo iam est perductum, ut valores quaerantur, quibus proxime fiat $\frac{x}{y} = \sqrt{\frac{n}{m}}$, sive ut quaerantur fractiones rationales $\frac{x}{y}$, quae tam prope aequentur formae irrationali $\sqrt{\frac{n}{m}}$, quam quidem fieri potest non maioribus pro x et y numeris adhibendis. Hunc in finem Ill. Auctor formulam $\frac{\sqrt{nm}}{m}$ in fractiones continuas convertit; omnes enim fractiones hoc modo formatae hac gaudent proprietate, ut quaelibet valorem $\frac{\sqrt{mn}}{m}$ propius exhauriat, quam ullo alio modo fieri posset numeris non maioribus adhibendis, ubi quidem notum est inter has fractiones eas quam maxime adpropinquare, quae maximos indices habent. Ill. Auctor hic methodum explicat, qua operationes, quibus isti quoti continui reperiuntur, haud mediocriter contrahi possunt, et quam exemplo dilucidat.

His explicatis ad ipsum problema progreditur et primo quidem, si formula

$$Ax^2 - 2Bxy + Cy^2$$

casu $x = a$ et $y = b$ praebeat valorem c, infinitos alios valores pro x et y substituendos investigare docet, qui eundem formulae valorem c sint praebiturae; et tum porro, quod erat principale, in eos inquirit valores, quibus ipsa formula evadat minimum; quam autem facilis et concinna sit Ill. Auctoris regula, ex subiunctis exemplis abunde perspicitur, quae desumuntur a formulis sequentibus

$$5x^2 - 6xy - 7y^2, \quad 7x^2 - 20xy + 14y^2, \quad 25x^2 - 70xy + 46y^2.$$

1) Sed vide notam 1 p. 313. F. R.

Regula quoque proposita felicissime adhiberi potest in solvendo celebri illo problemate PELLIANO, in quo notum est quaeri duos numeros x et y tales, ut sit $y = \sqrt{(kx^2 + 1)}$; tum enim oportet utique, ut sit proxime $\frac{y}{x} = \sqrt{k}$.

1. In superiore dissertatione[1]) de resolutione aequationis

$$Ax^2 + 2Bxy + Cy^2 + 2Dx + 2Ey + F = 0$$

totum negotium praecipue ad hanc quaestionem erat deductum, ut pro litteris x et y valores in numeris integris investigentur, quibus formulae

$$Ax^2 + 2Bxy + Cy^2$$

minimus valor inducatur. Tres autem hic potissimum considerandi sunt casus, prouti haec formula vel duos factores habet imaginarios, quod fit, si $BB - AC$ fuerit numerus negativus, vel factores inter se aequales, quod fit, si $BB - AC = 0$, vel denique, si eius factores fuerint reales, quod fit, si $BB - AC$ numerus positivus. Primo autem casu haec quaestio minimi nullam attentionem meretur, quoniam solutio nulla plane difficultate laborat. Secundus vero casus multo minus negotium facessit, quum formula abeat in quadratum, cuius radicem facillime minimam reddere licet. Solus ergo tertius casus superest, qui accuratiorem investigationem postulat, unde quidem insuper excludi convenit casus, quibus formula $BB - AC$ est numerus quadratus et ambo factores adeo rationales evadunt; tum enim valor formulae propositae adeo ad nihilum redigi poterit, ita ut quaestio minimi hic ne locum quidem habeat.

2. Soli ergo nobis relinquuntur casus, quibus numerus $BB - AC$ est numerus positivus, sed non quadratus, cuiusmodi est ista formula

$$mxx - nyy$$

denotantibus litteris m et n numeros integros positivos, eiusmodi tamen, ut non uterque sit quadratus; tum enim evidens est istam formulam ad nihilum reduci non posse, nisi tam x quam y evanescat, quem casum tamen utpote

1) Scilicet in Commentatione 452 huius voluminis. F. R.

obvium excludi oportet. Cum ergo haec formula $mxx - nyy$ ad nihilum redigi se non patiatur, quaestio sine dubio notatu digna est censenda, qua litterarum x et y ii valores in integris quaeruntur, quibus ipsa formula $mx^2 - ny^2$ minimum omnium adipiscatur valorem. Si alter numerorum m et n unitati aequetur, semper formulam ad unitatem usque deprimere licebit, qui certe est minimus valor cyphra excepta. Si enim fuerit $m = 1$, ex Theoremate PELLIANO[1]) notissimo constat semper effici posse $xx - nyy = 1$ sive $x = \sqrt{(nyy + 1)}$, dummodo n non fuerit numerus quadratus, atque adeo hoc non solum unico modo praestari potest, sed etiam infinitis, quemadmodum iam ab ipso PELLIO[1]) est demonstratum. Sin autem alter numerus n unitati aequetur, formula $mxx - yy$ hac methodo ad -1 deprimitur, qui casus aeque pro minimo est habendus ac $+1$, dum in ea investigatione, quae ad hanc quaestionem ansam dedit, discrimen signi non spectatur.

3. His ergo casibus remotis, quo alter numerus m vel n unitati aequatur, quaestio nostra potissimum versatur circa formulam

$$mxx - nyy,$$

quippe ad quam semper formulam generalem $Axx - 2Bxy + Cyy$ revocare licet. Si enim in genere statuatur

$$x = t + Bu \quad \text{et} \quad y = Au,$$

facta substitutione formula generalis abit in hanc formam

$$Att - A(B^2 - AC)uu$$

sicque formula nostra assumta $mxx - nyy$ aeque late patere est censenda atque ipsa proposita trinomialis.[2]) Etiamsi autem neque m neque n unitati aequetur, saepenumero usu venire potest, ut formulam nostram quoque ad unitatem usque deprimere liceat; idque vel statim manifesto occurrit, veluti in hac forma $3xx - 2yy$, quae ad unitatem redigitur sumtis $x = 1$ et $y = 1$, vel non statim se offert, uti fit in $9xx - 5yy$, quae posito $x = 3$ et $y = 4$

1) Sed vide de hac falsa nominatione notam 1 p. 77. F. R.

2) Sed vide § 17. Revera haec reductio non succedit, quia forma $Att - A(B^2 - AC)uu$ formae $Axx - 2Bxy + Cyy$ sensu a C. F. GAUSS usurpato non aequivalet. F. R.

ad unitatem redit. Quicquid autem sit, utique evenire potest, ut minimus valor nostrae formulae unitatem excedat, ac tum iudicium de minimo plerumque summis difficultatibus involutum deprehenditur, ceu fit in hac formula $7xx - 13yy$, quam usque ad binarium deprimi posse non facile perspicitur, si scilicet ponatur $x = 15$ et $y = 11$. At si m et n fuerint numeri praegrandes, iudicium multo operosiores calculos requirit, quamobrem methodus certa etiam in his casibus minimum investigandi analysin haud contemnendo incremento locupletare videtur.

4. Antequam autem hanc ipsam methodum explicare adgrediar, plurimum ostendisse iuvabit semper infinitis modis idem minimum obtineri posse. Atque hoc adeo generalius ita demonstrari potest. Quodsi unicus casus constet, quo formula $mxx - nyy$ aequalis fiat dato numero k, tum semper infiniti valores pro x et y reperiri possunt, qui ad eundem numerum k deducant. Sit enim casu illo cognito $x = a$ et $y = b$, ita ut sit

$$maa - nbb = k,$$

et nunc numeros x et y ita definiri oportet, ut fiat

$$mxx - nyy = maa - nbb,$$

id quod sequenti modo commodissime praestabitur. Ante omnia quaerantur numeri p et q, ut fiat

$$pp - mnqq = 1,$$

id quod infinitis modis semper fieri posse constat, dummodo mn non fuerit numerus quadratus, uti hic assumimus; atque nunc quaesito satisfieri manifestum est, si statuatur

$$mxx - nyy = (maa - nbb)(pp - mnqq)^2;$$

quod quo facilius fieri possit, sumamus factores etsi irrationales et ponamus

$$x\sqrt{m} + y\sqrt{n} = (a\sqrt{m} + b\sqrt{n})(p + q\sqrt{mn})^2;$$

tum enim mutato signo radicalis $\sqrt{n}$ sponte fiet

$$x\sqrt{m} - y\sqrt{n} = (a\sqrt{m} - b\sqrt{n})(p - q\sqrt{mn})^2$$

sicque alteri tantum harum duarum aequationum satisfecisse sufficiet. Quia autem evolutio formulae $(p+q\sqrt{mn})^\lambda$ alternatim terminos rationales et irrationales radicali $\sqrt{mn}$ affectos praebet, sit P summa terminorum rationalium et $Q\sqrt{mn}$ summa irrationalium, ita ut sit

$$(p+q\sqrt{mn})^\lambda = P + Q\sqrt{mn}$$

similique modo

$$(p-q\sqrt{mn})^\lambda = P - Q\sqrt{mn}.$$

Nunc igitur aequatio nostra erit

$$x\sqrt{m} + y\sqrt{n} = (a\sqrt{m} + b\sqrt{n})(P + Q\sqrt{mn})$$

sive

$$x\sqrt{m} + y\sqrt{n} = (aP + nbQ)\sqrt{m} + (bP + maQ)\sqrt{n},$$

ubi tam partes signo $\sqrt{n}$ quam partes signo $\sqrt{m}$ affectae seorsim sunt inter se aequandae, atque hinc statim elicimus sequentes valores

$$x = aP + nbQ, \quad y = bP + maQ$$

simulque patet multitudinem harum solutionum revera esse infinitam.

5. His praemissis ipsam nostram quaestionem adgrediamur quaesituri valores litterarum x et y, quibus formula

$$mxx - nyy$$

minimum sortiatur valorem, qui sit $= k$; ac statim quidem evidens est his casibus formulam $mxx - nyy$ propius ad nihilum redigi quam ullis aliis casibus sicque pro x et y eiusmodi investigandi sunt valores, quibus proxime fiat

$$\frac{x}{y} = \sqrt{\frac{n}{m}} = \frac{\sqrt{mn}}{m},$$

quocirca negotium iam huc est perductum, ut quaerantur fractiones rationales $\frac{x}{y}$, quae tam prope aequentur formae irrationali $\frac{\sqrt{mn}}{m}$, quam quidem fieri potest non maioribus numeris pro x et y adhibendis.

6. Hoc autem Problema iam olim a WALLISIO[1]) propositum expeditissime resolvitur, si formula $\frac{\sqrt{mn}}{m}$ in fractionem continuam convertatur, simili scilicet operatione, qua vulgo maximus communis divisor duorum numerorum quaeri solet. Si enim hoc modo perventum fuerit ad hanc fractionem continuam

$$\frac{\sqrt{mn}}{m} = \alpha + \cfrac{1}{\beta + \cfrac{1}{\gamma + \cfrac{1}{\delta + \cfrac{1}{\varepsilon + \text{etc.}}}}}$$

continui hi quoti in seriem disponantur ac primo quidem ipsi α subscribatur fractio $\frac{1}{0}$, ipsi β vero $\frac{\alpha}{1}$; ac deinceps ex binis fractionibus continuo sequens formatur, dum ultimae tam nominator quam denominator per indicem supra scriptum multiplicetur hisque productis tam numerator quam denominator penultimae fractionis respective addantur, sequenti scilicet modo

$$\begin{array}{cccccc} \alpha, & \beta, & \gamma, & \delta, & \varepsilon & \\ \frac{1}{0}, & \frac{\alpha}{1}, & \frac{\alpha\beta+1}{\beta}, & \frac{\alpha\beta\gamma+\gamma+\alpha}{\beta\gamma+1}, & \frac{\alpha\beta\gamma\delta+\gamma\delta+\alpha\delta+\alpha\beta+1}{\beta\gamma\delta+\delta+\beta} & \text{etc.} \end{array}$$

7. Omnes istae fractiones hac gaudent proprietate, ut quaelibet valorem formulae $\frac{\sqrt{mn}}{m}$ propius exhauriat, quam fieri poterit numeris non maioribus adhibendis. Verum etiam inter has ipsas fractiones ingens intercedit discrimen, quod aliae aliis, ceteris quidem paribus, magis appropinquent. Eae autem maxime appropinquare sunt compertae, quae maximos indices sibi habent inscriptos; si ergo illae pro $\frac{x}{y}$ accipiantur, iam certi sumus istis numeris pro x et y assumtis formulae nostrae $mxx - nyy$ minimum valorem induci. Simul vero notari oportet inter hos quotos successivos $\alpha, \beta, \gamma, \delta, \varepsilon$ etc. semper dari periodos, in quibus idem quotorum ordo recurrit; omnes ergo fractiones iisdem maximis quotis subscriptae omnes quoque valores idoneos pro x et y suppeditabunt, quibus formula nostra $mxx - nyy$ eundem minimum valorem nanciscitur.

---

1) Vide notam 1 p. 77. F. R.

8. Quo autem operationes, quibus isti quoti facillime eruuntur, clarius explicare valeam, exemplum primo determinatum expediamus, quo formula proposita sit

$$7xx - 13yy,$$

ita ut iam proxime fieri debeat

$$\frac{x}{y} = \frac{\sqrt{91}}{7},$$

ubi tantum notetur esse $\sqrt{91} > 9$ et < 10. Nunc ergo operatio uti pro maximo divisore instituatur. Ac primo dividi oportet $\sqrt{91}$ per 7, unde primus quotus prodit $= 1$, residuum vero $= \sqrt{91} - 7$, per quod praecedens divisor 7 debet dividi; multiplicetur uterque numerus per $\sqrt{91} + 7$ ac divisor iam erit 42, dividendus autem $7(\sqrt{91} + 7)$, qui per septenarium depressi praebent divisorem $= 6$ et dividendum $= \sqrt{91} + 7 > 16$, unde secundus quotus colligitur 2 ac residuum fiet $\sqrt{91} - 5$, per quod 6 debet dividi. Multiplicando per $\sqrt{91} + 5$ divisor erit 66 et dividendus $6(\sqrt{91} + 5)$ ac per 6 deprimendo iam per 11 dividi debet $\sqrt{91} + 5$, unde tertius quotus fit 1 residuo manente $\sqrt{91} - 6$, per quod praecedens divisor 11 debet dividi. Quae operatio ulterius hic repraesentatur:

$\frac{11}{\sqrt{91} - 6}$ multipl. per $\sqrt{91} + 6$ fit $\frac{11(\sqrt{91} + 6)}{55}$, divid. per 11 fit $\frac{\sqrt{91} + 6}{5}$, quot. 3 (*N.* 4),

$\frac{5}{\sqrt{91} - 9}$ „ „ $\sqrt{91} + 9$ „ $\frac{5(\sqrt{91} + 9)}{10}$, „ „ 5 „ $\frac{\sqrt{91} + 9}{2}$, „ 9 (*N.* 5),

$\frac{2}{\sqrt{91} - 9}$ „ „ $\sqrt{91} + 9$ „ $\frac{2(\sqrt{91} + 9)}{10}$, „ „ 2 „ $\frac{\sqrt{91} + 9}{5}$, „ 3 (*N.* 6),

$\frac{5}{\sqrt{91} - 6}$ „ „ $\sqrt{91} + 6$ „ $\frac{5(\sqrt{91} + 6)}{55}$, „ „ 5 „ $\frac{\sqrt{91} + 6}{11}$, „ 1 (*N.* 7),

$\frac{11}{\sqrt{91} - 5}$ „ „ $\sqrt{91} + 5$ „ $\frac{11(\sqrt{91} + 5)}{66}$, „ „ 11 „ $\frac{\sqrt{91} + 5}{6}$, „ 2 (*N.* 8),

$\frac{6}{\sqrt{91} - 7}$ „ „ $\sqrt{91} + 7$ „ $\frac{6(\sqrt{91} + 7)}{42}$, „ „ 6 „ $\frac{\sqrt{91} + 7}{7}$, „ 2 (*N.* 9),

$\frac{7}{\sqrt{91} - 7}$ „ „ $\sqrt{91} + 7$ „ $\frac{7(\sqrt{91} + 7)}{42}$, „ „ 7 „ $\frac{\sqrt{91} + 7}{6}$, „ 2 (*N.* 10).

Ulterius calculum producere non est opus, quia haec postrema divisio cum secunda convenit et iam periodus secunda incipit, ubi notandum loco primi quoti 1 hic eius duplum occurrere, id quod in huiusmodi divisionibus semper usu venit.

9. Quoti ergo ordine inventi sequenti modo progrediuntur

$$1, 2, 1, 3, 9, 3, 1, 2 \quad 2, 2, 1, 3, 9, 3, 1, 2,$$

inter quos maxime eminent 9; ideoque nullum amplius est dubium, quin illae fractiones, quae his quotis subiiciuntur, formulae $7xx - 13yy$ omnium valorum minimum concilient. Apponamus igitur has fractiones sequenti modo

$$\begin{matrix} 1, & 2, & 1, & 3, & 9 \\ \frac{1}{0}, & \frac{1}{1}, & \frac{3}{2}, & \frac{4}{3}, & \frac{15}{11}, \end{matrix}$$

unde patet fractionem nobis satisfacientem fore $\frac{x}{y} = \frac{15}{11}$ sive $x = 15$ et $y = 11$. Hinc autem $7xx = 1575$ et $13yy = 1573$, unde minimus valor sine ullo dubio est binarius, quem divinando non tam facile quisquam detexerit.

10. Si has operationes, quibus illi quoti continui reperiuntur, attentius perpendamus, calculum non mediocriter contrahi posse facile perspicere licet. Sit enim $\sqrt{k}$ quantitas illa irrationalis, quam formula in fractionem continuam convertenda involvit, numerus autem integer proxime minor quam $\sqrt{k}$ sit $= e$ et ponamus perventum iam esse ad divisionem, qua formula $\sqrt{k} + r$ dividi debet per numerum p, ita ut quotus hinc oriundus sit $q < \frac{e+r}{p}$, eritque residuum $= \sqrt{k} + r - pq$, et quia $pq > r$ (saltem quando operationes iam ordine progrediuntur), vocemus $pq - r = r'$, ita ut iam residuum sit $\sqrt{k} - r'$, unde pro sequente divisione habebimus divisorem $= \sqrt{k} - r'$ et dividendum $= p$; multiplicetur uterque per $\sqrt{k} + r'$ et fiat $\frac{k - r'r'}{p} = p'$ (vidimus enim semper in decursu operationum formulam $k - r'r'$ divisibilem fore per p) et iam sequens divisio ita erit comparata, ut sit divisor $= p'$ et dividendus $\sqrt{k} + r'$, unde nascetur quotus $q' < \frac{e+r'}{p'}$, atque hinc simili modo tertia et sequentes divisiones conficientur.

11. Ex prima igitur illa operatione, qua formulam $\sqrt{k} + r$ dividi oportet per numerum p, notentur tantum numeri r et p, unde deducitur quotus $q < \frac{e+r}{p}$; deinde sumatur

$$r' = pq - r \quad \text{et} \quad p' = \frac{k - r'r'}{p}$$

hincque fiet $q' < \frac{e+r'}{p'}$; simili modo capiatur porro

$$r'' = p'q' - r' \quad \text{et} \quad p'' = \frac{k - r''r''}{p}$$

hincque $q'' < \frac{e+r''}{p''}$. Quas operationes sequente schemate[1]) repraesentamus:

$r,$	$p,$	$q < \frac{e+r}{p},$
$r' = pq - r,$	$p' = \frac{k-r'r'}{p},$	$q' < \frac{e+r'}{p'},$
$r'' = p'q' - r',$	$p'' = \frac{k-r''r''}{p'},$	$q'' < \frac{e+r''}{p''},$
$r''' = p''q'' - r''$	$p''' = \frac{k-r'''r'''}{p''}$	$q''' < \frac{e+r'''}{p'''}$
etc.	etc.	etc.

Hocque modo progressio quotorum q, q', q'', q''' etc. facillime inveniri posse videtur.

12. Dilucidemus hanc regulam exemplo, quo formula

$$5xx - 38yy$$

minimum sit reddenda seu fractio

$$\frac{x}{y} = \frac{\sqrt{38}}{\sqrt{5}} = \frac{\sqrt{190}}{5}$$

per fractionem infinitam evolvenda. Hic igitur erit

$$k = 190, \quad e = 13, \quad p = 5 \quad \text{et} \quad r = 0,$$

1) Quod schema aliis quidem significationibus adhibitis iam invenitur in Commentatione 323 huius voluminis, p. 82. F. R.

unde totus calculus sequenti modo instituetur:

$$\begin{array}{llll}
r = 0, & p = 5, & & q = 2 < \frac{13+0}{5}, \\
r^{\mathrm{I}} = 10, & p^{\mathrm{I}} = \frac{190-100}{5} = 18, & & q^{\mathrm{I}} = 1 < \frac{13+10}{18}, \\
r^{\mathrm{II}} = 8, & p^{\mathrm{II}} = \frac{190-64}{18} = 7, & & q^{\mathrm{II}} = 3 < \frac{13+8}{7}, \\
r^{\mathrm{III}} = 13, & p^{\mathrm{III}} = \frac{190-169}{7} = 3, & & q^{\mathrm{III}} = 8 < \frac{13+13}{3}, \\
r^{\mathrm{IV}} = 11, & p^{\mathrm{IV}} = \frac{190-121}{3} = 23, & & q^{\mathrm{IV}} = 1 < \frac{13+11}{23}, \\
r^{\mathrm{V}} = 12, & p^{\mathrm{V}} = \frac{190-144}{23} = 2, & & q^{\mathrm{V}} = 12 < \frac{13+12}{2}, \\
r^{\mathrm{VI}} = 12, & p^{\mathrm{VI}} = \frac{190-144}{2} = 23, & & q^{\mathrm{VI}} = 1 < \frac{13+12}{23}, \\
r^{\mathrm{VII}} = 11, & p^{\mathrm{VII}} = \frac{190-121}{23} = 3, & & q^{\mathrm{VII}} = 8 < \frac{13+11}{3}, \\
r^{\mathrm{VIII}} = 13, & p^{\mathrm{VIII}} = \frac{190-169}{3} = 7, & & q^{\mathrm{VIII}} = 3 < \frac{13+13}{7}, \\
r^{\mathrm{IX}} = 8, & p^{\mathrm{IX}} = \frac{190-64}{7} = 18, & & q^{\mathrm{IX}} = 1 < \frac{13+8}{18}, \\
r^{\mathrm{X}} = 10 & p^{\mathrm{X}} = \frac{190-100}{18} = 5 & & q^{\mathrm{X}} = 4 < \frac{13+10}{5} \\
\text{etc.} & \text{etc.} & & \text{etc.}
\end{array}$$

Calculum ulterius prosequi non est opus, quum iam patescat quotorum ordo

2, 1, 3, 8, 1, 12, 1, 8, 3, 1 | 4, 1, 3, 8, 1, 12, 1, 8 etc.,

unde fractio continua oritur

$$\frac{x}{y} = \sqrt{\frac{38}{5}} = 2 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{8 + \cfrac{1}{1 + \cfrac{1}{12 + \cfrac{1}{1 + \cfrac{1}{8 + \text{etc.}}}}}}}}$$

Tum vero quum maximus horum quotorum sit 12, ei respondebit valor minimus formulae propositae $5xx - 38yy$; at fractio $\frac{x}{y}$ ita definietur

$$\begin{array}{cccccc} 2, & 1, & 3, & 8, & 1, & 12 \\ \frac{1}{0}, & \frac{2}{1}, & \frac{3}{1}, & \frac{11}{4}, & \frac{91}{33}, & \frac{102}{37} \end{array}$$

sicque pro casu minimi habemus $x = 102$ et $y = 37$, unde $5xx = 52020$ et $38yy = 52022$, ergo differentia $= -2$; quia autem inter quotos etiam eminet 8 eique subiacet fractio $\frac{11}{4}$, sumendo $x = 11$ et $y = 4$ colligitur valor formulae $5xx - 38yy = 605 - 608 = -3$, qui valor post illum sine dubio est minimus.

13. Plura huius generis exempla non afferimus, sed quo haec methodus succincta ad usum ampliorem accommodetur, investigemus fractiones continuas pro singulis multiplis ipsius $\sqrt{2}$; plurimum enim iuvabit relationem inter hos valores perpendisse, siquidem hoc argumentum de fractionibus continuis neutiquam adhuc satis est exploratum. Quotos autem tantum pro singulis his multiplis apposuisse sufficiet:

Pro $\sqrt{2}$ quoti 1, 2, 2, 2, 2, 2 etc.

Pro $2\sqrt{2}$ quoti 2, 1, 4, 1, 4, 1, 4 etc.

Pro $3\sqrt{3}$ quoti 4, 4, 8, 4, 8, 4, 8 etc.

Pro $4\sqrt{2}$ quoti 5, 1, 1, 1, 10, 1, 1 etc.

Pro $5\sqrt{2}$ quoti 7, 14, 14, 14, 14, 14, 14 etc.

Pro $6\sqrt{2}$ quoti 8, 2, 16, 2, 16, 2, 16 etc.

Pro $7\sqrt{2}$ quoti 9, 1, 8, 1, 18, 1, 8 etc.

14. Hae progressiones eo magis sunt notatu dignae, quod tantopere a se invicem discrepant, etiamsi ipsae quantitates iis expressae tam simplicem rationem inter se teneant. Neque vero tantum multipla tantam gignunt differentiam in fractionibus continuis, sed etiam ipsa additio adhuc maius discrimen parit, si scilicet ad $\sqrt{2}$ quaepiam fractio rationalis addatur; id quod exemplo formulae $\frac{1}{2} + \sqrt{2}$ illustremus, ubi adeo usu venit, ut primae opera-

tiones peculiarem evolutionem requirant, dum quotos a sequentibus periodis diversos praebent. Ponatur ergo

$$\frac{x}{y} = \frac{1+2\sqrt{2}}{2} = \frac{1+\sqrt{8}}{2}.$$

Primo igitur per 2 dividatur $1+\sqrt{8}$ et quotus erit 1, residuum vero $\sqrt{8}-1$, per quod dividi debet 2; multiplicetur utrimque per $\sqrt{8}+1$, ut per 7 dividi debeat $2\sqrt{8}+2 = \sqrt{32}+2$, et nunc operatio in ordinem subit; hic scilicet est

$$k = 32, \quad e = 5, \quad r = 2 \quad \text{et} \quad p = 7$$

et operationes ita se habebunt:

$r = 2,$	$p = 7,$	$q = 1,$
$r = 5,$	$p = 1,$	$q = 10,$
$r = 5,$	$p = 7,$	$q = 1,$
$r = 2,$	$p = 4,$	$q = 1,$
$r = 2,$	$p = 7,$	$q = 1,$
$r = 5,$	$p = 1,$	$q = 10,$
$r = 5$	$p = 7$	$q = 1$
etc.	etc.	etc.

Quum igitur primus quotus fuerit 1 a prioribus prorsus separandus, series quotorum erit

$$1 \quad 1, 10, 1, 1, 1, 10, 1 \quad 1, 10 \text{ etc.},$$

quae series eo maiorem attentionem meretur, quod a praecedentibus toto coelo discrepat.

15. Sumamus aliud exemplum

$$\frac{x}{y} = \frac{1}{3} + \sqrt{2} = \frac{1+\sqrt{18}}{3},$$

unde resultat primus quotus $= 1$, et residuum est $\sqrt{18}-2$, per quod dividi oportet 3; sive multiplicando per $\sqrt{18}+2$ divisor fit 14, dividendus autem $3\sqrt{18}+6 = \sqrt{162}+6$, cuius evolutio sequenti modo repraesentatur:

$$k = 162, \quad e = 12,$$

$r = 6,$	$p = 14,$	$q = 1,$
$r = 8,$	$p = 7,$	$q = 2,$
$r = 6,$	$p = 18,$	$q = 1,$
$r = 12,$	$p = 1,$	$q = 24,$
$r = 12,$	$p = 18,$	$q = 1,$
$r = 6,$	$p = 7,$	$q = 2,$
$r = 8,$	$p = 14,$	$q = 1,$
$r = 6,$	$p = 9,$	$q = 2,$
$r = 12,$	$p = 2,$	$q = 12,$
$r = 12,$	$p = 9,$	$q = 2,$
$r = 6,$	$p = 14,$	$q = 1,$
$r = 8,$	$p = 7,$	$q = 2,$
$r = 6,$	$p = 18,$	$q = 1,$
$r = 12,$	$p = 1,$	$q = 24,$
$r = 12,$	$p = 18,$	$q = 1,$
$r = 6,$	$p = 7,$	$q = 2,$
$r = 8,$	$p = 14,$	$q = 1,$
$r = 6,$	$p = 9,$	$q = 2,$
$r = 12$	$p = 2$	$q = 12$
etc.	etc.	etc.

Series igitur quotorum est

$$1 \quad 1, 2, 1, 24, 1, 2, 1, 2, 12, 2 \quad 1, 2, 1, 24, 1, 2 \text{ etc.},$$

ubi excluso primo reliqui secundum denos periodum constituunt.

16. Quum hic sit $\frac{x}{y} = \frac{1+\sqrt{18}}{3}$, habebimus $3x - y = y\sqrt{18}$; reddamus hanc aequationem rationalem et prodibit

$$9xx - 6xy = 17yy \quad \text{sive} \quad 9xx - 6xy - 17yy = 0.$$

Hinc ergo discimus, si proposita fuerit haec formula trinomialis

$$9xx - 6xy - 17yy,$$

cuiusmodi valores litteris x et y tribui debeant, ut haec formula minimum nanciscatur valorem. Scilicet quotis modo inventis subscribantur fractiones more solito atque ea, cui maximus quotus est inscriptus, dabit valores ipsarum x et y; quocirca has fractiones hic subiiciamus

$$\begin{matrix} 1, & 1, & 2, & 1, & 24 \\ \frac{1}{0}, & \frac{1}{1}, & \frac{2}{1}, & \frac{5}{3}, & \frac{7}{4}. \end{matrix}$$

Pro casu ergo minimi habemus $\frac{x}{y} = \frac{7}{4}$ sive $x = 7$ et $y = 4$, unde fit

$$9xx = 441, \quad 6xy = 168, \quad 17yy = 272,$$

ergo ipsa formula abit in $+1$, qui valor utique est omnium minimus.

17. Quodsi autem hanc formulam modo supra [§ 3] exposito tractare et ad duos terminos redigere vellemus, ob $A = 9$, $B = 3$, $C = -17$ ponendo

$$x = t + 3u \quad \text{et} \quad y = 9u$$

prodiret haec formula

$$9tt - 1458uu = 9(tt - 162uu),$$

quae formula certe numquam minor evadere potest quam 9, ex quo intelligimus, si huiusmodi formularum valores minimos investigare voluerimus, neutiquam licere eas ad duos terminos reducere, quandoquidem hoc modo earum natura penitus mutaretur[1]), quocirca necesse est tales formulas data opera evolvere, id quod in sequentibus problematibus sumus expedituri.

PROBLEMA 1

18. *Si formula* $Ax^2 - 2Bxy + Cy^2$ *casu, quo* $x = a$ *et* $y = b$, *praebeat valorem* $= c$, *invenire infinitos alios valores pro* x *et* y, *qui eundem valorem* c *producant, siquidem quantitas* $B^2 - AC$ *fuerit numerus positivus non quadratus.*[2])

SOLUTIO

Quum igitur sit

$$Aa^2 - 2Bab + Bb^2 = c,$$

1) Vide notam 2 p. 313. F. R.

2) Confer secundam partem Commentationis praecedentis. F. R.

requiritur, ut fiat

$$Ax^2 - 2Bxy + Cy^2 = Aa^2 - 2Bab + Cb^2.$$

Iam quaerantur ante omnia numeri p et q, ut fiat

$$pp - 2Bpq + ACqq = 1,$$

id quod semper fieri licet, quum hinc sit

$$p = Bq + \sqrt{((B^2 - AC)qq + 1)},$$

cuius resolutio a Problemate PELLIANO pendet, dummodo $B^2 - AC$ fuerit numerus positivus non quadratus. Statuamus ergo

$$B^2 - AC = k,$$

ut fieri debeat

$$p = Bq + \sqrt{(kq^2 + 1)},$$

ita ut quaeri oporteat numerum q, ut formula $kq^2 + 1$ fiat quadratum. Hoc ergo facto statuamus

$$Ax^2 - 2Bxy + Cy^2 = (Aa^2 - 2Bab + Cbb)(pp - 2Bpq + ACqq),$$

quod productum cum ipsa forma proposita convenire ita per factores irrationales ostendimus. Quum enim sit

$$Ax^2 - 2Bxy + Cy^2 = \frac{1}{A}(Ax - By + y\sqrt{k})(Ax - By - y\sqrt{k})$$

et

$$Aa^2 - 2Bab + Cb^2 = \frac{1}{A}(Aa - Bb + b\sqrt{k})(Aa - Bb - b\sqrt{k})$$

et

$$pp - 2Bpq + ACq^2 = (p - Bq + q\sqrt{k})(p - Bq - q\sqrt{k}),$$

statuamus

$$Ax - By + y\sqrt{k} = (Aa - Bb + b\sqrt{k})(p - Bq + q\sqrt{k}):$$

tum enim sponte fiet sumendo $\sqrt{k}$ negative

$$Ax - By - y\sqrt{k} = (Aa - Bb - b\sqrt{k})(p - Bq - q\sqrt{k}),$$

unde sufficiet alteram aequationem tantum evolvisse, si modo partes rationales et irrationales seorsim inter se aequentur. Prodibit igitur

$$Ax - By = (Aa - Bb)(p - Bq) + bq(B^2 - AC),$$

$$y = q(Aa - Bb) + b(p - Bq),$$

qui valor in priori aequatione substitutus praebet $x = ap - Cbq$, ita ut valores quaesiti sint

$$x = ap - Cbq, \quad y = bp + Aaq - 2Bbq.$$

Atque hinc adhuc alia solutio formari potest, quoniam permutatis litteris A et C tam litterae x et y quam a et b inter se permutantur, litterae vero p et q eaedem manent, scilicet

$$x = ap + Cbq - 2Baq, \quad y = bp - Aaq.$$

Inventa autem unica solutione valores pro x et y reperti scribentur in locum litterarum a et b sicque denuo nova solutio eruitur atque hinc simili modo infinitas alias successive elicere licebit.

COROLLARIUM 1

19. Quin etiam adhuc alias solutiones impetrare licet, si alii factores inter se combinentur; veluti si ponamus

$$Ax - By + y\sqrt{k} = (Aa - Bb - b\sqrt{k})(p - Bq + q\sqrt{k}),$$

hinc orientur istae aequationes

$$Ax - By = (Aa - Bb)(p - Bq) - kbq,$$

$$y = q(Aa - Bb) - b(p - Bq) = Aaq - bp$$

hincque

$$Ax = Aap - 2Bbp + ACbq$$

seu

$$x = ap + Cbq - \frac{2B}{A}bp,$$

quae autem solutio non est integra, nisi $2Bbp$ per A sit divisibile. Permutatio autem porro hanc suppeditat solutionem

$$x = Cbq - ap, \quad y = bp + Aaq - \frac{2B}{C}ap.$$

COROLLARIUM 2

20. Utemur nunc etiam hac combinatione

$$Ax - By + y\sqrt{k} = (Aa - Bb + b\sqrt{k})(p - Bq - q\sqrt{k})$$

hincque obtinebimus

$$Ax - By = (Aa - Bb)(p - Bq) - kbq,$$

$$y = -(Aa - Bb)q + b(p - Bq) = bp - Aaq,$$

$$x = ap - 2Baq + Cbq.$$

Quae solutio iam permutatione in problematis solutione est eruta.

COROLLARIUM 3

21. Eodem modo si hos factores adhibeamus

$$Ax - By + y\sqrt{k} = (Aa - Bb - b\sqrt{k})(p - Bq - q\sqrt{k}),$$

easdem solutiones reperimus, quas in primo Corollario iam invenimus, permutatione scilicet adhibita.

COROLLARIUM 4

22. Verum adeo infinitas solutiones simul exhibere poterimus, si loco factorum $p - Bq \pm q\sqrt{k}$ eorum potestates[1]) quascumque usurpamus, quarum quidem exponentes sunt numeri integri. Si enim evoluta formula $(p - Bq + q\sqrt{k})^n$ terminos irrationales ponamus $= Q\sqrt{k}$, rationales vero $P - BQ$, ita ut iam P et Q infinitos valores in se involvant, omnes praecedentes solutiones generales reddentur, si modo litterarum p et q loco scribantur litterae P et Q.

1) Confer secundam partem Commentationis praecedentis, imprimis § 16 et seq. F. R.

PROBLEMA 2

23. *Proposita formula* $Ax^2 - 2Bxy + Cy^2$, *in qua* $BB - AC$ *sit numerus positivus non quadratus, invenire eos valores pro litteris* x *et* y, *quibus ipsa formula ad minimum valorem perducatur.*

SOLUTIO

Hoc problema simili modo solvetur, quo supra [§ 5] formulam binomialem tractavimus, scilicet ipsa nostra formula aequetur nihilo ex eiusque resolutione quaeratur fractio $\frac{x}{y}$, quae posito ut ante $B^2 - AC = k$ reperitur

$$\frac{x}{y} = \frac{B \pm \sqrt{k}}{A};$$

quocirca istam formulam irrationalem in fractionem continuam resolvi oportet, quaerendo scilicet seriem quotorum continuorum; quibus si more solito fractiones subscribantur, eae, quae maximis quotis respondent, loco $\frac{x}{y}$ sumtae formulae propositae minimum valorem inducent, et quia hic $\sqrt{k}$ tam negative quam positive accipere licet, geminas solutiones assignare licebit, quae quidem plerumque inter se convenient. Id quod clarissime exemplis ostendetur.

EXEMPLUM 1

24. Sit proposita ista formula

$$5xx - 6xy - 7yy,$$

unde fit

$$\frac{x}{y} = \frac{3 \pm \sqrt{44}}{5}.$$

Valeat primo signum superius et formula $\frac{3+\sqrt{44}}{5}$ dabit primum quotum $= 1$, ex quo oritur residuum $\sqrt{44} - 2$, per quod dividi oportet 5. Multiplicetur utrimque per $\sqrt{44} + 2$, ut prodeat divisor 40 et dividendus $5(\sqrt{44} + 2)$, qui deprimuntur ad 8 et $\sqrt{44} + 2$; nunc iam regula supra data uti poterimus, uti hic videre licet:

$$k = 44, \quad e = 6,$$

$r = 2,$	$p = 8,$	$q = 1,$
$r = 6,$	$p = 1,$	$q = 12,$
$r = 6,$	$p = 8,$	$q = 1,$
$r = 2,$	$p = 5,$	$q = 1,$
$r = 3,$	$p = 7,$	$q = 1,$
$r = 4,$	$p = 4,$	$q = 2,$
$r = 4,$	$p = 7,$	$q = 1,$
$r = 3,$	$p = 5,$	$q = 1,$
$r = 2,$	$p = 8,$	$q = 1,$
$r = 6$	$p = 1$	$q = 12$
etc.	etc.	etc.

Qui quoti cum ante invento hanc seriem constituunt

$$1, 1, 12, 1, 1, 1, 2, 1 \mid 1, 1, 12 \text{ etc.},$$

unde fractiones quotis 12 subscriptae quaesito satisfacient, quarum prima est $\frac{2}{1}$, ita ut sit $x = 2$ et $y = 1$, unde formula proposita acquirit valorem $+1$.

At si sumamus

$$\frac{x}{y} = \frac{3 - \sqrt{44}}{5} \quad \text{sive} \quad \frac{-y}{x} = \frac{5}{\sqrt{44} - 3} = \frac{5(\sqrt{44} + 3)}{35} = \frac{\sqrt{44} + 3}{7},$$

inde posito ut ante

$$k = 44 \quad \text{et} \quad e = 6$$

habemus

$r = 3,$	$p = 7,$	$q = 1,$
$r = 4,$	$p = 4,$	$q = 2$

atque hic subsistimus, quia eaedem divisiones iam supra occurrerunt, et nunc series quotorum erit

$$1, 2, 1, 1, 1, 12, 1, 1 \mid 1, 2, 1 \text{ etc.};$$

prima autem fractio quoto 12 respondens hic fit $\frac{11}{8}$; sumatur ergo $x = 8$ et $y = -11$ atque nostrae formulae valor evadit $+1$.

EXEMPLUM 2

25. Proposita [sit] formula

$$7xx - 20xy + 14yy$$

minimum reddenda, cuius valor casu $x = 1$ et $y = 1$ statim fit $+1$, certe minimum. Hic ergo fractio $\frac{x}{y}$ proxime debet esse aequalis formulae

$$\frac{10 + \sqrt{2}}{7},$$

unde statim primus quotus oritur $= 1$, et residuum erit $3 + \sqrt{2}$; unde pro secundo quoto habemus $\frac{7}{3+\sqrt{2}} = \frac{7(3-\sqrt{2})}{7} = \frac{3-\sqrt{2}}{1}$, sicque quotus $= 1$ et residuum $= 2 - \sqrt{2}$. Pro tertio quoto habemus $\frac{1}{2-\sqrt{2}} = \frac{2+\sqrt{2}}{2}$ sicque quotus $= 1$ et residuum $\sqrt{2}$, quare pro quarto habemus $\frac{2}{\sqrt{2}} = \frac{\sqrt{2}}{1}$, unde sequentes quoti sunt, uti supra [§ 13] invenimus,

$$1,\ 2,\ 2,\ 2 \text{ etc.};$$

integra ergo series quotorum erit

$$1,\ 1,\ 1\quad 1,\ 2,\ 2,\ 2,\ 2 \text{ etc.}$$

Quamquam hae operationes initio irregulares videntur, eas tamen secundum regulam praescriptam evolvere licet; hic enim est statim

$$k = 2,\quad e = 1,\quad r = 10 \quad \text{et} \quad p = 7,$$

unde calculus ita procedet:

$r = +10,$	$p = +7,$	$q = 1,$
$r = -3,$	$p = -1,$	$q = 1,$
$r = +2,$	$p = +2,$	$q = 1,$
$r = +0,$	$p = +1,$	$q = 1,$
$r = +1,$	$p = +1,$	$q = 2,$
$r = +1$	$p = +1$	$q = 2$
etc.	etc.	etc.

hincque superior series quotorum oritur, unde valores fractionis $\frac{x}{y}$ sequenti modo procedent

$$\begin{array}{cccccccc} 1, & 1, & 1, & 1, & 2, & 2, & 2, & 2 \\ \frac{1}{0}, & \frac{1}{1}, & \frac{2}{1}, & \frac{3}{2}, & \frac{5}{3}, & \frac{13}{8}, & \frac{31}{19}, & \frac{75}{46}, \end{array}$$

quarum secunda statim dat casum minimi ante memoratum. Tertia dat $+2$, quarta -1, quinta dat $+1$, sexta -1 etc.

Iidem valores sine dubio prodire debent, si in fractione pro $\frac{x}{y}$ capiatur $\sqrt{2}$ negative, ut habeatur

$$\frac{10-\sqrt{2}}{7},$$

quam etiam per regulam nostram evolvere licebit, dummodo ita repraesentetur $\frac{\sqrt{2}-10}{-7}$, ita ut sit

$$r=-10 \quad \text{et} \quad p=-7,$$

unde calculus erit

$$k=2, \quad e=1,$$

$$\begin{array}{lll} r=-10, & p=-7, & q=1, \\ r=+3, & p=+1, & q=4, \\ r=+1, & p=+1, & q=2, \\ r=+1 & p=+1 & q=2 \\ \text{etc.} & \text{etc.} & \text{etc.} \end{array}$$

Ex quibus quotis sequentes fractiones formantur

$$\begin{array}{ccccc} 1, & 4, & 2, & 2, & 2 \\ 1 & 1 & 5 & 11 & 27 \\ 0', & 1', & 4', & 9', & 22', \end{array}$$

quarum secunda formulam reducit ad $+1$, tertia ad -1, quarta ad $+1$ etc. Notatu dignum hic occurrit, quod hae fractiones a praecedentibus tantopere discrepent atque nihilo secius eadem minima producant. Sed supra [§ 18] iam ostendimus huiusmodi formulam eosdem valores recipere posse, dum loco x et y diversi valores substituuntur.

EXEMPLUM 3

26. Sit proposita formula

$$25xx - 70xy + 46yy$$

minimum reddenda; hic ergo proxime esse oportet

$$\frac{x}{y} = \frac{7+\sqrt{3}}{5},$$

unde primus quotus fit $= 1$ et residuum $= 2 + \sqrt{3}$, ergo pro secundo quoto habetur fractio $\frac{5}{2+\sqrt{3}} = \frac{5(2-\sqrt{3})}{1} = \frac{10-\sqrt{75}}{1}$ hincque quotus $= 1$. Tota autem operatio per regulam nostram expediri potest, si fractio nostra per 5 multiplicando ad hanc formam reducatur $\frac{35+\sqrt{75}}{25}$, ubi est

$$k = 75, \quad e = 8, \quad r = 35 \quad \text{et} \quad p = 25,$$

unde calculus sequitur:

$r = +35,$	$p = +25,$	$q = 1,$
$r = -10,$	$p = -1,$	$q = 1,$
$r = +9,$	$p = +6,$	$q = 2,$
$r = +3,$	$p = +11,$	$q = 1,$
$r = +8,$	$p = +1,$	$q = 16,$
$r = +8,$	$p = +11,$	$q = 1,$
$r = +3,$	$p = +6,$	$q = 1,$
$r = +3,$	$p = +11,$	$q = 1,$
$r = +8$	$p = +1$	$q = 16$
etc.	etc.	etc.

Quoti ergo cum fractionibus[1]) ita se habebunt:

$$1,\ 1,\ 2,\ |\ 1,\ 16,\ 1,\ 1,\ |\ 1,\ 16$$

$$\frac{1}{0},\ \frac{1}{1},\ \frac{2}{1},\ \frac{5}{3},\ \frac{7}{4},\ \frac{117}{67},\ \frac{124}{71},\ \frac{241}{138},\ \frac{365}{209}.$$

1) In editione principe (atque etiam in *Comment. arithm.*) quotis hae fractiones falsae subscriptae sunt:

$$\frac{1}{0},\ \frac{1}{1},\ \frac{2}{1},\ \frac{5}{3},\ \frac{7}{4},\ \frac{117}{35},\ \frac{124}{39},\ \frac{241}{74},\ \frac{365}{113}$$

Correxit F. R.

evidens est ergo fractiones indicibus 16 subscriptas quaesito satisfacere debere, quod fit, si $x = 7$ et $y = 4$; tum autem formula nostra abit in $+1$.

Si in prima formula radicali tribuatur signum -1, ut prodeat

$$\frac{x}{y} = \frac{\sqrt{75 - 35}}{-25},$$

haec per regulam evoluta praebet ob

$k = 75$ et $e = 8$, $r = -35$, $p = -25$, $q = 1$:

$r = -35,$	$p = -25,$	$q = 1,$
$r = +10,$	$p = +1,$	$q = 18,$
$r = +8,$	$p = +11,$	$q = 1,$
$r = +3,$	$p = +6,$	$q = 1,$
$r = +3,$	$p = +11,$	$q = 1,$
$r = +8,$	$p = +1,$	$q = 16,$
$r = +8,$	$p = +11,$	$q = 1,$
$r = +3,$	$p = +6,$	$q = 1,$
$r = +3$	$p = +11$	$q = 1$
etc.	etc.	etc.

Hinc autem quoti cum fractionibus[1]) ita procedent:

$$\begin{array}{cccccccc} 1, & 18, & 1, & 1, & 1, & 16, & 1, & 1 \\ \frac{1}{0}, & \frac{1}{1}, & \frac{19}{18}, & \frac{20}{19}, & \frac{39}{37}, & \frac{59}{56}, & \frac{983}{933}, & \frac{1042}{989}. \end{array}$$

Secunda fractio indici 18 respondens sine dubio producit valorem minimum, scilicet $+1$, quod ex priori casu concludi nequit, quum ibi haec fractio $\frac{1}{1}$ exiguo quoto sit subscripta; verum hoc neutiquam est mirandum, propterea quod hi valores litterarum x et y sunt valde exigui, principium autem supra stabilitum, quo fractiones maximis quotis respondentes accipere iubemur, proprie numeris maioribus convenit atque utique evenire potest, ut valores minimis numeris expressi ab hac regula recedant.

1) In editione principe ultimis quotis hae falsae fractiones $\frac{98}{93}, \frac{157}{149}$ subscriptae sunt, qui errores iam in *Comment. arithm.* correcti sunt. F. R.

27. Ex his exemplis abunde perspicitur, quomodo regula nostra aeque facili ac concinna in omnibus casibus uti conveniat; imprimis autem ea optimo successu adhiberi poterit in Problemate illo PELLIANO famosissimo solvendo, ubi quaeruntur numeri x et y, ut sit $y = \sqrt{(kxx + 1)}$; tum enim utique oportebit esse proxime $\frac{y}{x} = \sqrt{k}$, quandoquidem formula $yy - kxx$ minima fieri debet, minimum autem iam sponte constat esse $= 1$ prodiens, si $x = 0$ et $y = 1$. Veluti si fuerit $k = 13$, cui convenit $e = 3$; ac primo fit $r = 0$, $p = 1$ sicque calculus ita progredietur:

$r = 0,$	$p = 1,$	$q = 3,$
$r = 3,$	$p = 4,$	$q = 1,$
$r = 1,$	$p = 3,$	$q = 1,$
$r = 2,$	$p = 3,$	$q = 1,$
$r = 1,$	$p = 4,$	$q = 1,$
$r = 3,$	$p = 1,$	$q = 6,$
$r = 3$	$p = 4$	$q = 1$
etc.	etc.	etc.

Unde quoti cum fractionibus $\frac{y}{x}$ erunt

$$3,\ 1,\ 1,\ 1,\ 1,\ 6,\ 1,\ 1,\ 1,\ 1\ \ 6$$
$$\frac{1}{0}',\ \frac{3}{1}',\ \frac{4}{1}',\ \frac{7}{2}',\ \frac{11}{3}',\ \frac{18}{5}',\ \frac{119}{33}',\ \frac{137}{38}',\ \frac{256}{71}',\ \frac{393}{109}',\ \frac{649}{180}',$$

ubi maximi quoti sunt sex; quia autem $\frac{y}{x}$ maius esse debet quam $\sqrt{k}$, fractiones autem hic resultantes alternatim superant et deficiunt ab isto valore, pro casu nostro eas accipi oportet, quae locis imparibus consistunt, ergo undecima harum fractionum, quae dat $y = 649$ et $x = 180$, quaesito satisfacit; fractio autem priori 6 subscripta[1]) resolvit aequationem $y = \sqrt{(13xx - 1)}$.

1) Vide Commentationem 323 huius voluminis, § 26 et seq., imprimis § 39. F. R.

EXTRAIT D'UNE LETTRE DE M. EULER LE PERE A M. BERNOULLI CONCERNANT LE MEMOIRE IMPRIME PARMI CEUX DE 1771 p. 318[1])

Commentatio 461 indicis Enestroemiani
Nouveaux mémoires de l'académie des sciences de Berlin 1772, 1774, Histoire, p. 35—36

Ayant lu avec bien du plaisir vos recherches sur les nombres de la forme $10^p \pm 1$, j'ai l'honneur de vous communiquer les critères par lesquels on peut juger, pour chaque nombre premier $2p+1$, laquelle de ces deux formules $10^p - 1$ ou $10^p + 1$ sera divisible par $2p+1$.

Pour cet effet, il faut distinguer les deux cas suivans.

PREMIER CAS

Si $2p+1 = 4n+1$, on n'a qu'à considérer les diviseurs de ces trois nombres n, $n-2$ et $n-6$, et si parmi eux on trouve ou les deux nombres 2 et 5 ou aucun d'eux, c'est une marque que la formule $10^p - 1$ sera divisible; mais si parmi les dits diviseurs ne se trouve qu'un des nombres 2 ou 5, alors la formule $10^p + 1$ sera divisible. Ainsi, pour le nombre premier $2p+1 = 53 = 4n+1$, on aura $n = 13$, et nos trois nombres seront 13, 11, 7, donc ni 2 ni 5 n'est diviseur, et partant la formule $10^{26} - 1$ sera divisible par 53.

1) Le mémoire de M. Bernoulli — c'est Jean III Bernoulli (1744—1807), fils de Jean II (1710—1790) et petit-fils de Jean I (1667—1748) — est intitulé: *Recherches sur les diviseurs de quelques nombres très grands compris dans la somme de la progression géométrique* $1 + 10^1 + 10^2 + 10^3 + \cdots + 10^T = S$, Nouv. mém. de l'acad. d. sc. de Berlin 1771, 1773, p. 318—337. F. R.

SECOND CAS

Si $2p + 1 = 4n - 1$, on doit considérer ces trois nombres n, $n + 2$ et $n + 6$, et si parmi leurs diviseurs se rencontrent ou tous les deux nombres 2 et 5 ou aucun d'eux, alors la formule $10^p - 1$ sera divisible; mais si seulement l'un des nombres 2 ou 5 s'y trouve, alors la formule $10^p + 1$ sera divisible. Comme si $2p + 1 = 59 = 4n - 1$, et partant $n = 15$, nos trois nombres sont 15, 17, 21, ou 5 est parmi les diviseurs et non pas 2, donc la formule $10^{29} + 1$ sera divisible par 59.

Ces règles sont fondées sur un principe dont la démonstration n'est pas encore connue.

Le plus grand nombre premier que nous connoissions, est sans doute $2^{31} - 1 = 2147483647$ que FERMAT[1]) a déjà assuré être premier, et moi, je l'ai

---

1) Il faut remarquer cependant que ni dans les *Oeuvres de FERMAT* ni ailleurs ne se trouvent des documents qui pourraient appuyer l'assertion d'EULER — EULER cite presque toujours de mémoire. On sait seulement que FERMAT s'était occupé de découvrir dès nombres premiers de la forme $2^x - 1$ à l'occasion de ses recherches sur les nombres parfaits. Voir surtout les lettres de FERMAT à MERSENNE, (mai?) 1640 et (juin?) 1640, et la lettre à FRÉNICLE du 18 oct. 1640, P. DE FERMAT, *Varia opera mathematica*, Tolosae 1679, p. 176 et 162; *Oeuvres de FERMAT*, publiées par les soins de MM. P. TANNERY et CH. HENRY, t. II, p. 194, 195 et 206. Dans la seconde lettre à MERSENNE FERMAT énonce, entre autres, sans démonstration, le théorème suivant: Lorsque l'exposant $[x]$ est nombre premier, je dis que son radical $[2^x - 1]$ ne peut être mesuré par aucun nombre premier que par ceux qui sont plus grands de l'unité qu'un multiple du double de l'exposant ou que le double de l'exposant. (Comparez le théorème trouvé plus tard par EULER, selon lequel les nombres $2^{2^m} + 1$ ne peuvent être mesurés par aucun nombre qui ne soit pas de la forme $2^{m+1}k + 1$. Voir le mémoire 134 (suivant l'Index d'ENESTRÖM): *Theoremata circa divisores numerorum*, Novi comment. acad. sc. Petrop. 1 (1747/8), 1750, p. 20; *LEONHARDI EULERI Opera omnia*, series I, vol. 2, p. 62). Dans la lettre à FRÉNICLE FERMAT énonce, entre autres, que $2^{37} - 1$ est divisible par 223. Voir aussi le mémoire 26 (suivant l'Index d'ENESTRÖM): *Observationes de theoremate quodam FERMATIANO aliisque ad numeros primos spectantibus*, Comment. acad. sc. Petrop. 6 (1732/3), 1738, p. 103; *LEONHARDI EULERI Opera omnia*, series I, vol. 2, p. 1.

En citant FERMAT, EULER peut avoir confondu les noms FERMAT et MERSENNE. Voir *M. MERSENNI Cogitata physico-mathematica*, Parisiis 1644, Praefatio gener. num. XIX. En effet, on y trouve parmi les nombres parfaits énumérés par MERSENNE, comme huitième, le nombre $2^{30}(2^{31} - 1)$, ce qui prouve que MERSENNE a reconnu le nombre $2^{31} - 1$ comme premier. Voir aussi E. LUCAS, *Théorie des fonctions numériques simplement périodiques*, American journal of Mathem., 1878, p. 184 et 289, surtout p. 235—236 et 292—293. Mais il se peut aussi qu' EULER ait été d'avis, que les théorèmes de MERSENNE appartenaient au fond à FERMAT. Voir encore *Encyclopédie d. sc. mathém.*, t. I, vol. 3, p. 53—56, surtout les notes 291 et 292. F. R.

aussi prouvé; car, puisque cette formule ne sauroit admettre d'autres diviseurs[1]) que de l'une ou de l'autre de ces deux formes $248n + 1$ et $248n + 63$, j'ai examiné tous les nombres premiers contenus dans ces deux formules jusqu'à 46339, dont aucun ne s'est trouvé diviseur.

Cette progression

$$41,\ 43,\ 47,\ 53,\ 61,\ 71,\ 83,\ 97,\ 113,\ 131 \text{ etc.}$$

dont le terme général est

$$41 - x + xx,$$

est d'autant plus remarquable que les quarante premiers termes sont tous des nombres premiers.[2])

---

1) D'après le théorème de FERMAT mentionné dans la note précédente, les diviseurs de $2^{31} - 1$ doivent être de la forme $62n + 1$; d'autre part, les diviseurs impairs de $2(2^{31} - 1) = 2^{32} - 2 = x^2 - 2$ ne pourront être que de la forme $8n \pm 1$ (voir le théorème 42 du mémoire 164 cité p. 277, ou aussi le scholion 2 qui s'y trouve à la même page 277). En combinant, on trouve que tout diviseur de $2^{31} - 1$ est nécessairement de l'une des formes $248n + 1$, $248n + 63$. Voir aussi A. M. LEGENDRE, *Théorie des nombres*, 3e éd., Paris 1830, t. I, p. 228—229. F. R.

2) Cet énoncé est contenu dans un théorème plus général concernant les formes quadratiques qui a été démontré par G. FROBENIUS dans le mémoire *Über quadratische Formen, die viele Primzahlen darstellen*, Sitzungsber. d. preuß. Akad. d. Wissensch., 1912, p. 966. F. R.

PROBLEMA DIOPHANTEUM SINGULARE

Commentatio 466 indicis ENESTROEMIANI
Novi commentarii academiae scientiarum Petropolitanae 19 (1774), 1775, p. 112—131
Summarium ibidem p. 20—21

SUMMARIUM

Problema, cuius resolutionem heic tradit Illustr. EULERUS, illud est, quo duo quaeruntur numeri, quorum productum utrovis sive auctum sive minutum evadat quadratum. Quum igitur hos numeros fractos esse oporteat, statuantur $\frac{x}{z}$, $\frac{y}{z}$, ex quo colligitur utramque hanc expressionem

$$xy \pm xz \quad \text{et} \quad xy \pm yz$$

quadrato aequari, unde utraque huius erit formae $a^2 + b^2 \pm 2ab$, ideoque xy fit

$$= aa + bb = cc + dd;$$

tum vero remanet, ut $\frac{abcd}{aa+bb}$ fiat quadratum. Si pro m, n tales accipiantur numeri, ut sit $mm + nn = 1$, erit

$$c = ma + nb \quad \text{et} \quad d = na - mb;$$

tum vero si ponatur

$$m = \frac{pp - qq}{pp + qq}, \; n = \frac{2pq}{pp + qq},$$

quaestio eo reducitur, ut expressio[1])

$$aabbp^4 - 2ab(aa - bb)p^3q - 6aabbppqq + 2ab(aa - bb)pq^3 + aabbq^4$$

evadat quadratum, modo $aa + bb$ fuerit quadratum, quod facile obtinetur ponendo

$$p = 4ab(aa - bb) \quad \text{et} \quad q = a^4 + 6aabb + b^4.$$

---

1) Editio princeps: ... *eo reducitur, ut expressio*

$$aabbp^4 - 2ab(aa - bb)p^3q + 2aabbppqq - 2ab(aa - bb)pq^3 + aabbq^4 + (aa - bb)^2ppqq$$

evadat quadratum ... Haec autem expressio iam ipsa per se est quadratum; confer paragraphos 5 et 6. F. R.

Verum quum ex simplicissimis valoribus ipsorum a et b valde magni prodeant pro fractionibus $\frac{x}{z}$, $\frac{y}{z}$, inquirendum iudicavit Illustr. EULERUS, an non solutiones in numeris minoribus invenire liceat. Et licet prima quidem tentamina, quibus superiorem solutionem contrahi posse existimaverit, non successerint, aliam tamen deinde invenit solutionem valde planam et facilem. Scilicet ponendo numeros quaesitos A, B respective aequales fractionibus $\frac{aa+bb}{2ab}$ et $\frac{cc+dd}{2cd}$ quaestio eo reducitur, ut hae fractiones $\frac{aa+bb}{abcd}$, $\frac{cc+dd}{abcd}$ evadant quadrata. Si igitur supponantur numeratores quadratis aequari, remanet tantum, ut productum $abcd$ fiat quadratum. Conditione, qua $aa+bb$, $cc+dd$ supponuntur quadrata, solutio quidem limitatur, at haec conditio simul ad simplicissimos valores deducere videtur. Positis iam

$$a=pp-qq, \quad b=2pq, \quad c=rr-ss, \quad d=2rs$$

fieri debet

$$abcd=2pq(pp-qq)2rs(rr-ss),$$

ita ut quaestio reducatur ad problema iam notum, quo duo triangula rectangula in numeris quaeruntur, quorum areae inter se sint aequales.

PROBLEMA

1. *Invenire duos numeros, quorum productum utrovis sive auctum sive minutum fiat quadratum.*[1])

SOLUTIO

Cum ambo numeri quaesiti necessario sint fracti, ponatur unus $\frac{x}{z}$ et alter $\frac{y}{z}$ et conditiones problematis postulant, ut sit

$$1. \ \frac{xy}{zz} \pm \frac{x}{z} = \square, \quad 2. \ \frac{xy}{zz} \pm \frac{y}{z} = \square,$$

quae ergo formulae etiam per zz multiplicatae debent esse quadrata, unde hae conditiones sunt adimplendae

$$1. \ xy \pm xz = \square, \quad 2. \ xy \pm yz = \square.$$

---

1) Confer quaestiones XXVI et XXVII libri II DIOPHANTI *Arithmeticorum* (ed. P. TANNERY; quae quaestiones sunt quaestiones XXVII et XXVIII editionis BACHETI; vide notam p. 404 voluminis praecedentis). F. R.

2. Cum iam sit $aa + bb \pm 2ab = \square$, ex hoc fonte solutionem peti conveniet; quia autem duae huiusmodi conditiones proponuntur, ponamus duplici modo esse tam

$$xy = aa + bb$$

quam

$$xy = cc + dd,$$

ita ut sit

$$aa + bb = cc + dd,$$

id quod infinitis modis evenire potest; unde pro priore conditione faciamus $xz = 2ab$ et [pro posteriore] $yz = 2cd$, quo pacto ambae conditiones adimplentur; quare cum inde habeamus

$$x = \frac{2ab}{z} \quad \text{et} \quad y = \frac{2cd}{z},$$

erit nunc

$$xy = \frac{4abcd}{zz} = aa + bb = cc + dd,$$

unde deducimus

$$zz = \frac{4abcd}{aa + bb} \quad \text{sive} \quad \frac{zz}{4} = \frac{abcd}{aa + bb},$$

ita ut haec formula $\frac{abcd}{aa + bb}$ reddi debeat quadratum; praeterea vero etiam necesse est, ut sit

$$cc + dd = aa + bb.$$

3. Incipiamus ab hac postrema conditione ac denotent litterae m et n eiusmodi numeros, ut sit $mm + nn = 1$, id quod facile praestatur, ac capiatur

$$c = ma + nb \quad \text{et} \quad d = na - mb;$$

tum enim erit

$$cc + dd = (aa + bb)(mm + nn) = aa + bb;$$

hinc igitur altera conditio postulat, ut sit

$$\frac{zz}{4} = \frac{ab(ma + nb)(na - mb)}{aa + bb} = \square$$

vel etiam

$$\frac{zz}{4} = \frac{ab(am + bn)(bm - an)}{aa + bb},$$

quandoquidem postremus factor $bm - an$ idem dat quadratum ac praecedens $na - mb$.

4. Notum autem est litteris m et n hos valores tribui debere

$$m = \frac{pp-qq}{pp+qq} \quad \text{et} \quad n = \frac{2pq}{pp+qq};$$

tum enim fit $mm + nn = 1$; hinc autem erit

$$am + bn = \frac{a(pp-qq)+2bpq}{pp+qq} \quad \text{et} \quad bm - an = \frac{b(pp-qq)-2apq}{pp+qq},$$

quae formulae in se invicem multiplicatae praebent

$$\frac{ab(pp-qq)^2 + 2(bb-aa)pq(pp-qq) - 4abppqq}{(pp+qq)^2},$$

cuius fractionis numeratorem brevitatis gratia designemus littera S, ita ut sit

$$S = abp^4 + 2(bb-aa)p^3q - 6abppqq - 2(bb-aa)pq^3 + abq^4,$$

quo valore notato erit

$$\frac{zz}{4} = \frac{abS}{(aa+bb)(pp+qq)^2}$$

sive

$$\frac{1}{4}(aa+bb)(pp+qq)^2zz = abS.$$

5. Hinc igitur facta substitutione erit

$$abS = aabbp^4 - 2ab(aa-bb)p^3q - 6aabbppqq + 2ab(aa-bb)pq^3 + aabbq^4,$$

quae formula, cum tam primum quam postremum membrum sint quadrata, commode ad quadratum reduci poterit, ita ut litteris a et b pro lubitu assumtis valores idonei pro p et q erui possint; tum vero ut etiam formula

$$\frac{1}{4}(aa+bb)(pp+qq)^2zz$$

fiat quadratum, necesse est litteras a et b ita assumi, ut $aa+bb$ fiat quadratum, quo facto radicem quadratam extrahendo habebitur

$$\frac{1}{2}(pp+qq)z\sqrt{(aa+bb)} = \sqrt{abS}.$$

6. Statuamus igitur secundum praecepta cognita[1])

$$\sqrt{abS} = abpp - (aa - bb)pq + abqq;$$

tum autem erit

$$abS = aabbp^4 - 2ab(aa - bb)p^3q + 2aabbppqq - 2ab(aa - bb)pq^3 + aabbq^4;$$
$$+ (aa - bb)^2ppqq$$

quod quadratum[2]) si cum formula superiori comparetur, membra prima, secunda et ultima se mutuo tollunt, reliqua vero per pqq divisa hanc suppeditant aequationem

$$-6aabbp + 2ab(aa - bb)q = 2aabbp - 2ab(aa - bb)q,$$
$$+ (aa - bb)^2p$$

quae reducitur ad hanc formam

$$4ab(aa - bb)q = (a^4 + 6aabb + b^4)p,$$

unde concluditur

$$\frac{q}{p} = \frac{a^4 + 6aabb + b^4}{4ab(aa - bb)};$$

quae fractio si deprimi nequeat, quod quidem numquam evenire potest, ponatur

$$p = 4ab(aa - bb) \quad \text{et} \quad q = a^4 + 6aabb + b^4.$$

7. Sumtis igitur numeris a et b ita, ut $aa + bb$ fiat quadratum, hae formulae nobis praebent idoneos valores pro litteris p et q, quibus inventis erit

$$\frac{1}{2}(pp + qq)z\sqrt{aa + bb} = \sqrt{abS} = abpp - (aa - bb)pq + abqq$$

hincque

$$z = \frac{2\sqrt{abS}}{(pp + qq)\sqrt{aa + bb}};$$

tum vero ipsi numeri quaesiti erunt

$$\frac{x}{z} = \frac{2ab}{zz} \quad \text{et} \quad \frac{y}{z} = \frac{2cd}{zz} = \frac{2(ma + nb)(na - mb)}{zz},$$

---

1) Vide L. Euler, *Vollständige Anleitung zur Algebra*, St. Petersburg 1770, Zweyter Theil, zweyter Abschnitt, Cap. 9; *Leonhardi Euleri Opera omnia*, series I, vol. 1. F. R.

2) Vide notam p. 338. F. R.

ubi litteris m et n hi tributi sunt valores

$$m = \frac{pp-qq}{pp+qq} \quad \text{et} \quad n = \frac{2pq}{pp+qq}.$$

Hic perinde est, sive valor posterior prodeat negativus sive positivus; semper enim positivus locum habebit valor, quandoquidem terminus yz producto xy tam addi quam subtrahi debet.

8. Quia $aa+bb$ debet esse quadratum, casus simplicissimus, quo hoc contingit, est $a=4$ et $b=3$; tum enim erit

$$\sqrt{aa+bb} = 5, \quad ab = 12 \quad \text{et} \quad aa-bb = 7;$$

ex his igitur porro deducimus $p=336$, $q=1201$, deinde

$$\sqrt{abS} = 12(pp+qq) - 7pq$$

hincque

$$z = \frac{24(pp+qq)-14pq}{5(pp+qq)} = \frac{24}{5} - \frac{14pq}{5(pp+qq)},$$

denique vero pro y inveniendo erit

$$ma+nb = \frac{4(pp-qq)+6pq}{pp+qq} \quad \text{et} \quad mb-na = \frac{3(pp-qq)-8pq}{pp+qq},$$

quibus valoribus substitutis erit

$$\frac{x}{z} = \frac{24}{zz} \quad \text{et} \quad \frac{y}{z} = \frac{2(4m+3n)(4n-3m)}{zz}.$$

Pro his formulis autem evolvendis notetur esse

$$pp = 112896, \quad qq = 1442401, \quad pq = 403536,$$

unde elicitur

$$pp+qq = 1555297, \quad \frac{5z}{2} = \frac{15838812}{1555297}, \quad \text{hinc} \quad z = \frac{2 \cdot 15838812}{5 \cdot 1555297},$$

porro

$$m = -\frac{1329505}{1555297}, \quad n = \frac{807072}{1555297},$$

unde fit

$$4m+3n = -\frac{2896804}{1555297} \quad \text{et} \quad 4n-3m = \frac{7216803}{1555297};$$

hinc ergo colligimus

$$\frac{x}{z} = \frac{6 \cdot 25 \cdot 1555297^2}{15838812^2} \quad \text{et} \quad \frac{y}{z} = \frac{2896804 \cdot 25 \cdot 7216803}{2 \cdot 15838812^2}.$$

9. Cum hi numeri sint tam immensi, accuratius inquiramus, an non solutionem in numeris minoribus eruere liceat, et quo calculum paulisper contrahamus, incipiamus ab aequatione [§ 3]

$$\frac{zz}{4} = \frac{ab(am+bn)(bm-an)}{aa+bb},$$

ubi est

$$m = \frac{pp-qq}{pp+qq} \quad \text{et} \quad n = \frac{2pq}{pp+qq},$$

haecque formula quadratum efficienda tam negative quam positive accipi potest; statuamus iam

$$a = nb \quad \text{et} \quad p = qr,$$

ut primo sit

$$m = \frac{rr-1}{rr+1} \quad \text{et} \quad n = \frac{2r}{rr+1},$$

tum vero haec formula ad quadratum reduci debeat

$$\frac{zz}{4} = \pm \frac{nbb(n(rr-1)+2r)(rr-1-2nr)}{(nn+1)(rr+1)^2}$$

sive

$$\frac{zz(rr+1)^2}{4bb} = \pm \frac{n(n(rr-1)+2r)(rr-1-2nr)}{nn+1} = \square.$$

Hic autem primo observamus casu $r = 1$ hanc formulam evadere

$$= -\frac{4nn}{nn+1} \quad \text{sive etiam} \quad +\frac{4nn}{nn+1},$$

quae ergo erit quadratum, dummodo $nn+1$ fuerit quadratum; praeterea vero notasse iuvabit sumto $r = n$ hanc formulam fieri

$$= -nn(nn+1),$$

cuius negativum iterum fit quadratum, si modo $nn+1$ sit quadratum.

Cum igitur duos iam habeamus casus, quibus haec formula fit quadratum, ex iis alios casus secundum praecepta cognita eliciamus.

EVOLUTIO PRIMA

10. Cum utroque casu $nn + 1$ debeat esse quadratum, ponamus

$$\frac{zz(rr+1)^2(nn+1)}{4bb} = TT,$$

ut sit

$$TT = n(2r + n(rr-1))(2nr - (rr-1));$$

quae formula quia evadit quadratum posito $r = 1$, statuamus

$$r = 1 + v$$

eritque $rr - 1 = 2v + vv$, unde oritur[1])

$$TT = n(2 + 2(n+1)v + nvv)(2n + 2(n-1)v - vv),$$

quae formula evoluta praebet

$$TT = 4nn + 4n(nn + 2n - 1)v + 6n(nn-1)vv + 2n(nn - 2n - 1)v^3 - nnv^4.$$

Statuatur ergo[2])

$$T = 2n + (nn + 2n - 1)v + fvv$$

ideoque

$$TT = 4nn + 4n(nn + 2n - 1)v + (nn + 2n - 1)^2vv + 2f(nn + 2n - 1)v^3 + ffv^4, \\ + 4nfvv$$

ubi duo membra priora mutuo se tollunt; capiamus igitur f ita, ut etiam tertia membra se destruant, unde fieri debet

$$6n(nn-1) = (nn + 2n - 1)^2 + 4nf$$

ideoque

$$f = -\frac{n^2(n-1)^2 + (n+1)^2}{4n}.$$

1) Editio princeps (atque etiam *Comment. arithm.*): ... *unde oritur*

$$TT = n(2 + 2(n+1)v + nvv)(2n(n-1)v - vv)$$

quae formula evoluta praebet

$$TT = 4nn + 4n(nn + 2n - 1)v + 4n(nn-1)vv + \cdots$$

Quem ob errorem etiam computatio ipsius f $\left(\text{editio princeps: } f = -\frac{(nn+1)^2}{4n}\right)$ corrigenda erat. F. R.

2) Vidè notam 1 p. 342. F. R.

Iam cognito valore f reliqua membra per v^3 divisa dant

$$2n(nn-2n-1)-nnv = 2f(nn+2n-1)+ffv,$$

unde colligitur

$$v = \frac{2n(nn-2n-1)-2f(nn+2n-1)}{ff+nn};$$

hinc autem valor ipsius v multo magis fieret complicatus, quia in hac formula numerus n ad octavam potestatem exsurgit.

EVOLUTIO SECUNDA

11. Ponamus nunc

$$r = n+v$$

eritque

$$TT = n(n(nn+1)+2(nn+1)v+nvv)(nn+1-vv)$$

ideoque evolvendo

$$TT = nn(nn+1)^2+2n(nn+1)^2v-2n(nn+1)v^3-nnv^4.$$

Ponatur igitur[1])

$$T = n(nn+1)+(nn+1)v+fv^2,$$

cuius quadratum dat

$$TT = nn(nn+1)^2+2n(nn+1)^2v+2n(nn+1)fvv+2(nn+1)fv^3+ffv^4, \\ +(nn+1)^2vv$$

ubi duo membra priora iam se destruunt; ut igitur etiam termini vv se destruant, sumi debet

$$f = -\frac{(nn+1)}{2n};$$

tum vero bina membra posteriora per v^3 divisa praebent

$$-2n(nn+1)-nnv = 2(nn+1)f+ffv,$$

unde fit

$$v = \frac{-2n(nn+1)-2(nn+1)f}{ff+nn},$$

1) Vide notam 1 p. 342. F. R.

quae formula loco f valorem substituendo praebet

$$v = \frac{-4n(nn+1)(nn-1)}{5n^4+2nn+1},$$

unde fit

$$r = \frac{n(n^4+2nn+5)}{5n^4+2nn+1} = \frac{p}{q};$$

hinc, cum sit [§ 9] $n = \frac{a}{b}$, erit[1])

$$p = a(a^4+2aabb+5b^4) \quad \text{et} \quad q = b(5a^4+2aabb+b^4).$$

12. Quodsi ergo hic ut supra sumatur $a = 4$ et $b = 3$, reperietur

$$p = 4 \cdot 949 = 4 \cdot 13 \cdot 73 \quad \text{et} \quad q = 3 \cdot 1649 = 3 \cdot 97 \cdot 17,$$

qui numeri, cum sint maiores iis, quos supra invenimus, videntur maiores numeros quaesitos producere; quia autem uterque est impar[2]), reductio quaepiam locum inveniet; interim tamen ad numeros minores non pervenitur.

13. Si formulae hic pro TT inventae signa invertamus, ut prodeat

$$TT = nnv^4 + 2n(nn+1)v^3 - 2n(nn+1)^2v - nn(nn+1)^2,$$

ac ponamus

$$T = nvv + (nn+1)v + f,$$

erit sumto quadrato

$$TT = nnv^4 + 2n(nn+1)v^3 + 2nfvv + 2(nn+1)fv + ff, \\ + (nn+1)^2vv$$

ubi prima et secunda membra se destruunt, ac pro tertiis fiat

$$f = -\frac{(nn+1)^2}{2n};$$

iam invento hoc valore fiat etiam

$$v = \frac{ff + nn(nn+1)^2}{-2n(nn+1)^2 - 2f(nn+1)}$$

---

1) Editio princeps (atque etiam *Comment. arithm.*): ... *erit*

$$p = a^4 + 2aabb + 5b^4 \quad \text{et} \quad q = 5a^4 + 2aabb + b^4.$$

Quem ob errorem etiam in exemplo sequente factores 4 et 3 omissi erant. F. R.

2) Sed vide notam praecedentem. F. R.

et substituto pro f valore invento $-\frac{(nn+1)^2}{2n}$ reperitur

$$v = \frac{5n^4 + 2nn + 1}{4n(1-nn)}$$

hincque porro

$$r = \frac{n^4 + 6nn + 1}{4n(1-nn)} = \frac{p}{q};$$

quia igitur $n = \frac{a}{b}$, erit

$$\frac{p}{q} = \frac{a^4 + 6aabb + b^4}{4ab(bb - aa)}.$$

Quae solutio eosdem praebet valores, quos per primam evolutionem eruimus, ex quo concludi posse videtur simpliciores solutiones huius problematis vix expectari posse.

14. Imprimis autem hic casus omni attentione dignus occurrit, quo $v = 0$, ubi formula TT sponte fit quadratum, scilicet $nn(nn+1)^2$, ita ut hoc casu prodeat

$$\frac{zz(rr+1)^2(nn+1)}{4bb} = nn(nn+1)^2$$

seu radice quadrata extracta

$$\frac{z(rr+1)\sqrt{nn+1}}{2b} = n(nn+1);$$

cum autem sit $v = 0$, ob $r = n + v$ erit $r = n$, unde colligitur

$$z = \frac{2bn(nn+1)}{(nn+1)^{\frac{3}{2}}} = \frac{2bn}{\sqrt{nn+1}} = \frac{2ab}{\sqrt{aa+bb}};$$

porro ob $r = n = \frac{a}{b}$ erit

$$p = a \quad \text{et} \quad q = b, \quad c = ma + nb \quad \text{et} \quad d = na - mb$$

existente

$$m = \frac{aa - bb}{aa + bb} \quad \text{et} \quad n = \frac{2ab}{aa + bb},$$

quocirca erit

$$c = a \quad \text{et} \quad d = b,$$

unde bini numeri quaesiti erunt

$$\text{unus} \quad \frac{x}{z} = \frac{2ab}{zz} = \frac{aa+bb}{2ab}, \quad \text{alter} \quad \frac{y}{z} = \frac{2cd}{zz} = \frac{aa+bb}{2ab},$$

ita ut ambo nostri numeri sint inter se aequales; meminisse autem oportet formulam $aa + bb$ quadratum esse debere.

15. Quamquam autem haec solutio satis est simplex, tamen indoli quaestionis propositae minus satisfacere est censenda, propterea quod duos numeros aequales exhibet, cum nostrum problema manifesto duos numeros inaequales postulet. Interim tamen deducimur ad solutionem huius quaestionis:

Invenire numerum quadratum, qui radice sua sive auctus sive minutus producat quadratum.

Quodsi ergo radix huius quadrati vocetur $= z$, erit, uti modo invenimus,

$$z = \frac{aa+bb}{2ab},$$

dummodo $aa + bb$ fuerit quadratum; capiatur ergo

$$a = pp - qq \quad \text{et} \quad b = 2pq,$$

ut fiat $aa + bb = (pp + qq)^2$, hincque solutio nostra praebet

$$z = \frac{(pp+qq)^2}{4pq(pp-qq)},$$

unde pro z sequentes valores simpliciores eruuntur

$$\frac{25}{24}, \ \frac{169}{120}, \ \frac{289}{240}, \ \frac{625}{336}, \ \frac{841}{840}, \ \frac{1681}{720} \quad \text{etc.}$$

16. Etsi autem hic casus parum ad propositum nostrum conferre videtur, tamen eius consideratio attenta mox eiusmodi binos numeros suppeditabit ipsi problemati proposito satisfacientes, cuiusmodi sunt hi duo numeri

$$A = \frac{841}{840} \quad \text{et} \quad B = \frac{1369}{840};$$

tum enim erit

$$AB \pm A = A(B \pm 1),$$

ubi $B + 1 = \frac{2209}{840} = \frac{47^2}{840}$ et $B - 1 = \frac{529}{840} = \frac{23^2}{840}$; uterque autem valor in $A = \frac{29^2}{840}$ ductus manifesto praebet quadrata. Eodem modo reliquae conditiones

$$AB \pm B = B(A \pm 1)$$

ob $A + 1 = \frac{1681}{840} = \frac{41^2}{840}$ et $A - 1 = \frac{1}{840}$ utraque in $B = \frac{37^2}{840}$ ducta pariter quadrata exhibent.

17. Nunc igitur multo magis mirari oportet, cur istam solutionem satis simplicem ex analysi supra allata nullo modo elicere licuerit; quin etiam hi duo numeri ne quidem in formulis nostris supra usurpatis, scilicet $\frac{x}{z} = \frac{2ab}{zz}$ et $\frac{y}{z} = \frac{2cd}{zz}$, contineri videntur, cum nostri numeratores in factores resolvi nequeant, denominatores autem non sint quadrata. Hac autem circumstantia probe perpensa facile agnoscimus solutionem problematis nostri longe alio modo esse aggrediendam, ut huiusmodi solutiones simpliciores eliciamus, atque hinc clare perspicimus, quanti sit momenti huiusmodi problemata idoneo modo ad calculum revocare, hancque ob rem sequentem solutionem satis planam hic subiungamus.

SOLUTIO PLANA PROBLEMATIS PROPOSITI

18. Denotent litterae A et B binos numeros quaesitos, ita ut hae formulae

$$AB \pm A = A(B \pm 1) \quad \text{et} \quad AB \pm B = B(A \pm 1)$$

debeant esse quadrata. Hunc in finem tribuamus his numeris sequentes formas

$$A = \frac{aa + bb}{2ab} \quad \text{et} \quad B = \frac{cc + dd}{2cd};$$

sic enim prodibit

$$A \pm 1 = \frac{(a \pm b)^2}{2ab} \quad \text{et} \quad B \pm 1 = \frac{(c \pm d)^2}{2cd},$$

quare, ut ambae illae formulae fiant quadrata, pro priore necesse est, ut sit $\frac{aa + bb}{4abcd}$ quadratum, pro altera autem, ut haec forma $\frac{cc + dd}{4abcd}$ sit quadratum.

19. Quo igitur his conditionibus satisfaciamus, statuamus tam

$$aa + bb = \square$$

quam

$$cc + dd = \square;$$

tum vero necesse est, ut etiam productum $abcd$ fiat quadratum, quae quidem positio iam est limitata, dum istis conditionibus etiam aliis modis satisfieri posset; at vero simplicissimas solutiones suppeditare videtur. Hunc igitur in finem ponamus

$$a = pp - qq, \quad b = 2pq, \quad c = rr - ss \quad \text{et} \quad d = 2rs,$$

ut fiat

$$aa + bb = (pp + qq)^2 \quad \text{et} \quad cc + dd = (rr + ss)^2,$$

ita ut sit

$$A = \frac{(pp+qq)^2}{4pq(pp-qq)} \quad \text{et} \quad B = \frac{(rr+ss)^2}{4rs(rr-ss)};$$

tum vero superest, ut

$$abcd = 2pq(pp - qq) \cdot 2rs(rr - ss)$$

sive haec formula

$$pq(pp - qq) \cdot rs(rr - ss)$$

fiat quadratum. Hic vero casus manifesto ad problema satis notum deducitur, quo duo triangula rectangula in numeris quaeruntur, quorum areae sint inter se aequales[1]); quaeruntur igitur duo numeri, uterque formae $xy(xx - yy)$, quorum productum sit quadratum, unde in sequenti tabella simpliciores numeros huius formae exhibeamus per factores expressos, ubi quidem factores quadratos omittamus.

---

1) Vide § 3 Commentationis 167 (indicis Enestroemiani): *Solutio problematis difficillimi a Fermatio propositi*, Novi comment. acad. sc. Petrop. 2 (1749), 1751, p. 49; *Leonhardi Euleri Opera omnia*, series I, vol. 2, p. 223. Vide porro quaestionem VI libri V Diophanti *Arithmeticorum* (ed. P. Tannery; quae quaestio est quaestio VIII editionis Bacheti), imprimis autem Fermatii observationes ad hanc quaestionem adiectas primum a filio S. Fermatio editas in libro, qui inscribitur *Diophanti Alexandrini Arithmeticorum libri sex, et de numeris multangulis liber unus. Cum Commentariis C. G. Bacheti V. C. et observationibus D. P. de Fermat Senatoris Tolosani. Accessit Doctrinae Analyticae inventum novum, collectum ex variis eiusdem D. de Fermat Epistolis.* Tolosae 1670, p. 220; *Oeuvres de Fermat*, t. I, p. 309. F. R.

x	y	$xy(x+y)(x-y)$
2	1	$2\cdot3$
3	2	$2\cdot3\cdot5$
4	1	$3\cdot5$
4	3	$3\cdot7$
5	2	$2\cdot3\cdot5\cdot7$
5	4	5
6	1	$2\cdot3\cdot5\cdot7$
6	5	$2\cdot3\cdot5\cdot11$
7	2	$2\cdot5\cdot7$
7	4	$3\cdot7\cdot11$
7	6	$2\cdot3\cdot7\cdot13$
8	1	$2\cdot7$
8	3	$2\cdot3\cdot5\cdot11$
8	5	$2\cdot3\cdot5\cdot13$
8	7	$2\cdot3\cdot5\cdot7$
9	2	$2\cdot7\cdot11$
9	4	$5\cdot13$
10	1	$2\cdot5\cdot11$
10	3	$2\cdot3\cdot5\cdot7\cdot13$
11	2	$2\cdot11\cdot13$
11	4	$3\cdot5\cdot7\cdot11$
11	10	$2\cdot3\cdot5\cdot7\cdot11$
12	1	$3\cdot11\cdot13$
13	2	$2\cdot3\cdot5\cdot11\cdot13$
13	8	$2\cdot3\cdot5\cdot7\cdot13$
13	12	$3\cdot13$
14	1	$2\cdot3\cdot5\cdot7\cdot13$
14	11	$2\cdot3\cdot7\cdot11$
14	13	$2\cdot3\cdot7\cdot13$

20. Haec tabula nobis iam aliquot solutiones suppeditat, quarum prima et simplicissima oritur sumendo $p=5$, $q=2$ et $r=6$, $s=1$, unde oritur

$$A=\frac{29^2}{840}=\frac{841}{840} \quad \text{et} \quad B=\frac{37^2}{840}=\frac{1369}{840},$$

qui sunt ipsi numeri supra memorati. In nostra autem tabella occurrunt quoque isti numeri $x = 8$ et $y = 7$ eosdem factores $2 \cdot 3 \cdot 5 \cdot 7$ continentes; hinc igitur formemus numerum

$$C = \frac{(xx + yy)^2}{4xy(xx - yy)};$$

erit

$$C = \frac{113^2}{3360},$$

ubi $3360 = 4 \cdot 840$. Quemadmodum igitur ambo numeri A et B quaesito satisfecerunt, ita etiam hi duo numeri A et C eodemque modo etiam isti B et C seorsim satisfacient.

21. Porro etiam iidem factores $2 \cdot 3 \cdot 5 \cdot 11$ reperiuntur casibus $x = 6$ et $y = 5$, item $x = 8$ et $y = 3$; sumtis ergo $p = 6$, $q = 5$, $r = 8$ et $s = 3$ nascuntur isti numeri satisfacientes

$$A = \frac{61^2}{1320} \quad \text{et} \quad B = \frac{73^2}{5280},$$

ubi $5280 = 4 \cdot 1320$. Simili modo insuper plures alias solutiones ex tabula ista peti licet.

22. Quo autem plures huiusmodi solutiones exhibere queamus, faciamus

$$pq(pp - qq) = rs(rr - ss);$$

quod cum in genere nonnisi operose effici queat, casum magis particularem accipiamus et statuamus $r = p$, ut fieri debeat

$$q(pp - qq) = s(pp - ss),$$

unde elicimus

$$pp = qq + qs + ss;$$

quare statuamus $p = q + \frac{m}{n} s$, ut fiat

$$q + s = \frac{2mq}{n} + \frac{mms}{nn} \quad \text{sive} \quad nnq + nns = 2mnq + mms,$$

unde colligitur

$$\frac{q}{s} = \frac{mm-nn}{nn-2mm}.$$

Sumamus igitur

$$q = mm - nn \quad \text{et} \quad s = nn - 2mn$$

eritque

$$p = r = mm - nn + mn - 2mm = -mm - nn + mn,$$

ubi litteras m et n pro lubitu tam negativas quam positivas accipere licet. Haec ergo solutio ita se habebit. Sumto numero n negativo habebimus

$$p = mm + mn + nn, \quad r = mm + mn + nn,$$
$$q = mm - nn, \qquad s = nn + 2mn,$$

unde iam innumerabiles solutiones nascuntur; inde vero habebitur

$$a = pp - qq, \quad b = 2pq, \quad c = rr - ss \quad \text{et} \quad d = 2rs,$$

unde numeri quaesiti reperientur

$$A = \frac{(pp+qq)^2}{4pq(pp-qq)} = \frac{aa+bb}{2ab} \quad \text{et} \quad B = \frac{cc+dd}{2cd} = \frac{(rr+ss)^2}{4rs(rr-ss)}.$$

23. Cum haec solutio tantopere discrepet a prima, quam dedimus, operae pretium erit investigare, quomodo haec etiam in illa contineatur. Posueramus autem ipsos numeros quaesitos $\frac{x}{z}$ et $\frac{y}{z}$, tum vero statuimus

$$xy = aa + bb = cc + dd,$$

hinc vero deduximus

$$\frac{zz}{4} = \frac{abcd}{aa+bb},$$

ita ut esse debeat primo

$$aa + bb = cc + dd,$$

tum vero

$$\frac{abcd}{aa+bb} = \square.$$

Iam tribuamus tam litteris a et b quam c et d communem factorem et statuamus $a = fp$ et $b = fq$, tum vero $c = gr$ et $d = gs$ eritque

$$aa + bb = ff(pp + qq) \quad \text{et} \quad cc + dd = gg(rr + ss):$$

quae formulae cum sibi debeant aequari, fiat

$$pp + qq = gg \quad \text{et} \quad rr + ss = ff;$$

sic enim fiet $xy = ffgg$, praeterea vero esse debebit

$$\frac{zz}{4} = \frac{ffpq \cdot ggrs}{ffgg} \quad \text{sive} \quad \frac{zz}{4} = pqrs = \square.$$

Quamobrem statuamus

$$p = \alpha\alpha - \beta\beta, \quad q = 2\alpha\beta \quad \text{atque} \quad r = \gamma\gamma - \delta\delta \quad \text{et} \quad s = 2\gamma\delta,$$

ut fiat

$$pp + qq = (\alpha\alpha + \beta\beta)^2 = gg \quad \text{et} \quad rr + ss = (\gamma\gamma + \delta\delta)^2 = ff,$$

unde erit

$$f = \gamma\gamma + \delta\delta \quad \text{et} \quad g = \alpha\alpha + \beta\beta,$$

et nunc habebitur

$$\frac{zz}{4} = 4\alpha\beta(\alpha\alpha - \beta\beta) \cdot \gamma\delta(\gamma\gamma - \delta\delta),$$

ita ut hoc productum

$$\alpha\beta(\alpha\alpha - \beta\beta) \cdot \gamma\delta(\gamma\gamma - \delta\delta)$$

debeat esse quadratum, quae est eadem formula, quam in solutione posteriore quadratum efficere debuimus. Cui conditioni quando erit satisfactum, numeri quaesiti ita se habebunt

$$\frac{x}{z} = \frac{2ab}{zz} = \frac{aa+bb}{2cd} = \frac{cc+dd}{2cd},$$

$$\frac{y}{z} = \frac{2cd}{zz} = \frac{aa+bb}{2ab},$$

quae sunt eaedem formulae, quibus solutio posterior est superstructa.

24. Hic etiam generalius potuissemus statuere

$$pp + qq = Ngg \quad \text{et} \quad rr + ss = Nff,$$

unde fit

$$xy = aa + bb = cc + dd = Nffgg;$$

tum vero ut ante debet esse

$$\frac{zz}{4} = \frac{ffgg \cdot pqrs}{Nffgg} = \frac{pqrs}{N},$$

ita ut debeat esse

$$\frac{pqrs}{N} \text{ sive } Npqrs = \square.$$

Sumamus exempli gratia $N = 5$, et cum esse debeat

$$5(pp + qq) = 25gg = (2p - q)^2 + (p + 2q)^2,$$

sumamus

$$2p - q = \alpha\alpha - \beta\beta \quad \text{et} \quad p + 2q = 2\alpha\beta$$

ac reperietur

$$p = \frac{2(\alpha\alpha + \alpha\beta - \beta\beta)}{5}, \quad q = \frac{4\alpha\beta - \alpha\alpha + \beta\beta}{5};$$

simili modo quia debet esse

$$5(rr + ss) = 25ff,$$

habebitur

$$r = \frac{2(\gamma\gamma + \gamma\delta - \delta\delta)}{5} \quad \text{et} \quad s = \frac{4\gamma\delta - \gamma\gamma + \delta\delta}{5}$$

et iam superest, ut $5pqrs$ reddatur quadratum, similique modo solutionem generaliorem reddere licebit.

25. Quoniam autem solutio nostri problematis perducta est ad inventionem duorum triangulorum rectangulorum, quorum areae inter se teneant rationem quadraticam, adiungamus hic aliquot solutiones quaestionis latius patentis[1]), qua scilicet quaeruntur duo triangula rectangula, quorum areae datam inter se teneant rationem, puta ut α et β, ita ut esse debeat

$$pq(pp - qq) : rs(rr - ss) = \alpha : \beta.$$

1) Vide quaestionem XXI libri V DIOPHANTI *Arithmeticorum* (ed. P. TANNERY; quae quaestio est quaestio XXIV editionis BACHETI), imprimis autem FERMATII observationes ad hanc quaestionem adiectas, quae inveniuntur p. 249 editionis tolosanae nota p. 351 laudatae; *Oeuvres de FERMAT*, t. I, p. 318. F. R.

Cui conditioni satisfiet sequentibus octo formulis[1])

	p	q	r	s
I.	$\alpha+\beta$	$2\alpha-\beta$	$\alpha+\beta$	$2\beta-\alpha$
II.	3α	$2\beta-\alpha$	3β	$2\alpha-\beta$
III.	$2\alpha+\beta$	$\beta-\alpha$	$\alpha+2\beta$	$\beta-\alpha$
IV.	$\alpha+2\beta$	3α	3β	$\beta+2\alpha$
V.	$\beta-2\alpha$	6α	$2\beta-4\alpha$	$\beta+4\alpha$
VI.	$\beta+4\alpha$	$\beta-8\alpha$	3β	$8\alpha-\beta$
VII.	$\beta+2\alpha$	6α	$2\beta+4\alpha$	$\beta-4\alpha$
VIII.	$\beta+8\alpha$	$\beta-4\alpha$	3β	$8\alpha+\beta$

Ubi notasse iuvabit, si qui horum numerorum prodeant negativi, eos tuto in positivos verti posse, tum vero pro utroque triangulo maiores numeros litteris p et r, minores vero litteris q et s tribui oportere.

26. Pro nostro igitur problemate tantum opus est, ut loco α et β numeri quadrati accipiantur, id quod exemplo illustrasse sufficiet. Sumamus igitur $\alpha = 9$ et $\beta = 4$ ac sequentes octo solutiones[2]) obtinebuntur

I. $p = 14$, $q = 13$, $r = 13$ et $s = 1$;
II. $p = 27$, $q = 1$, $r = 14$ et $s = 12$;
III. $p = 22$, $q = 5$, $r = 17$ et $s = 5$;

1) In editione principe (atque etiam in *Comment. arithm.*) inter sequentes formulas hae falsae inveniuntur

IV. $\alpha+2\beta$, 3β, 3β, $\beta+2\alpha$.
V. $\beta-2\alpha$, 6α, $2\beta+4\alpha$, $\beta+4\alpha$.

In exemplo quidem sequente numeri correspondentes

V. $p = 54$, $q = 14$, $r = 40$ et $s = 28$

recte computati sunt. Correxit F. R.

2) In editione principe (atque etiam in *Comment. arithm.*) tabulae sequentes hos falsos valores continent

III. $p = 22$, $q = 1$, $r = 17$ et $s = 5$;
IV. $p = 23$, $q = 21$, $r = 22$ et $s = 12$.

Correxit F. R.

IV. $p = 27$, $q = 17$, $r = 22$ et $s = 12$;
V. $p = 54$, $q = 14$, $r = 40$ et $s = 28$;
VI. $p = 68$, $q = 40$, $r = 68$ et $s = 12$;
VII. $p = 54$, $q = 22$, $r = 44$ et $s = 32$;
VIII. $p = 76$, $q = 32$, $r = 76$ et $s = 12$.

Quae solutiones ob communes divisores reducuntur ad sequentes simpliciores

I. $p = 14$, $q = 13$, $r = 13$ et $s = 1$;
II. $p = 27$, $q = 1$, $r = 14$ et $s = 12$;
III. $p = 22$, $q = 5$, $r = 17$ et $s = 5$;
IV. $p = 27$, $q = 17$, $r = 22$ et $s = 12$;
V. $p = 27$, $q = 7$, $r = 20$ et $s = 14$;
VI. $p = 17$, $q = 10$, $r = 17$ et $s = 3$;
VII. $p = 27$, $q = 11$, $r = 22$ et $s = 16$;
VIII. $p = 19$, $q = 8$, $r = 19$ et $s = 3$;

hinc igitur facile, quotcumque solutiones desiderentur, deducere licet.

DE TABULA NUMERORUM PRIMORUM USQUE AD MILLIONEM ET ULTRA CONTINUANDA IN QUA SIMUL OMNIUM NUMERORUM NON PRIMORUM MINIMI DIVISORES EXPRIMANTUR[1])

Commentatio 467 indicis Enestroemiani
Novi commentarii academiae scientiarum Petropolitanae 19 (1774), 1775, p. 132—183
Summarium ibidem p. 22—26

SUMMARIUM

Continet haec Dissertatio expositionem modi, quo tabula numerorum primorum usque ad millies mille vel ultra, si placuerit, labore haud ita operoso construi queat. Si enim in huiusmodi tabula omnes numeri ordine recenserentur, non solum eius constructio nimis evaderet operosa, sed etiam in volumen valde magnum excresceret; hoc vero incommodum ut evitetur, omnes numeri ex hac tabula excludendi sunt, quorum divisores sponte innotescunt, quales sunt praeter numeros pares, qui per 3 vel 5 divisibiles sunt. In hanc igitur tabulam alii non referuntur numeri, nisi quorum divisores sint vel 7 vel 11 vel 13 vel alii numeri primi maiores, cuiusmodi usque ad triginta numerantur septem. Numeri igitur hac tabula comprehensi hac forma generali exhiberi possunt

$$30q + r,$$

ubi q designat numerum quemcumque, r vero nonnisi octo valores recipere potest

$$1, 7, 11, 13, 17, 19, 23, 29.$$

Quodsi nunc in forma quarta huiusmodi tabula sit construenda, in qualibet pagina quin-

1) Vide etiam Commentationes 283, 369, 461, 498, 708a huius voluminis. Vide praeterea notam 3 p. 104 voluminis praecedentis. F. R.

quaginta valores litterae q in prima columna verticali locum invenire poterunt huicque columnae adiungi debent octo a latere, quae respondent octo valoribus litterae r. Quoniam itaque quaelibet pagina continet quinquaginta valores litterae q, unaquaeque autem q valeat 30, censendum est quamlibet paginam continere 1500 numeros illis etiam comprehensis, qui in tabula non comparent. Hinc si tabula usque ad millies mille sit construenda, 666 paginis absolvetur, quod volumen pro nimis magno haberi non debet.

Si in genere quaerendi sint numeri formae $30q + r$, qui per numerum primum quemcumque datum P sint divisibiles, notandum est, quodsi unus quispiam innotuerit valor ipsius q satisfaciens, omnes alios hinc derivari posse, pro dato nimirum valore ipsius r. Nam si posito $q = a$ fiat $30a + r$ divisibilis per P, erit quoque $30q + r$ divisibilis per P, si pro q assumatur aliquis valorum $a + P$, $a + 2P$, $a + 3P$ etc. vel $a - P$, $a - 2P$, $a - 3P$ etc. Si itaque pro qualibet columna verticali prima constet areola, cui numerum P tamquam divisorem inscribi oportet, tum per omnes paginas sequentes areolae, quibus idem numerus inscribendus est, facillime definientur. In eo igitur praecipuus labor versatur, ut proposito numero P pro singulis residuis r definiantur minimi numeri q, qui formulam $30q + r$ divisibilem producant per P; nam his numeris inventis reliqui valores ipsorum q continua additione numeri P invenientur. Quomodo vero investigatio ista minimorum numerorum q propositis divisoribus septem istis numeris

$$7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29$$

pro singulis residuis r sit instituenda, id Illustr. Auctor septem Problematibus ostendit, quibus tamen recensendis non est ut immoremur, quia deinceps totam hanc investigationem octo Problematibus generalibus comprehendit. Haec autem Problemata ita enunciantur.

Proposito divisore primo

$$30a \pm 1,\quad 30a \pm 7,\quad 30a \pm 11,\quad 30a \pm 13$$

pro singulis residuis r omnes invenire quotos q, ut formula $30q + r$ fiat divisibilis per aliquem divisorum propositorum.

Ut idea solutionis horum Problematum constet, seligamus illud, quo ponitur divisor primus huius formae $30a + 11$. Quum itaque minimus numerus hoc divisore signandus sit

$$30 \cdot 30aa + 30 \cdot 22a + 121,$$

pro hoc numero erit $q = 30aa + 22a + 4$ et $r = 1$. Iam pro reliquis numeris per $30a + 11$ divisibilibus, quia tantum numeri desiderantur impares, ad numerum supra inventum continuo addatur

$$60 \cdot a + 22 = 2a^{(q)} + 22^{(r)} \quad \text{sive} \quad (2a + 1)^{(q)} - 8^{(r)}$$

hocque modo ista conficietur tabella:

q	r
$30aa+22a+4$	1
$30aa+24a+4$	23
$30aa+26a+5$	15
$30aa+28a+6$	7
$30aa+30a+6$	29
$30aa+32a+7$	21
$30aa+34a+8$	13
etc.	etc.

Hinc vero seligantur illi quoti q, qui respondent octo residuis assumtis $1, 7, 11, 13, 17, 19, 23, 29$; residua enim eiusmodi ut 15, 21, 5, 27, 3, 25 sponte liquet numeros exhibere per 5 aut 3 divisibiles, qui ex tabula exclusi sunt. Singulis his octo Problematibus Illustr. EULERUS tabulas subiunxit, quae minimos exhibent quotos pro divisoribus formae propositae millionario minoribus ad singula octo residua relatos. Tum vero ex octo his tabulis tabulam generalem subsidiariam confecit, qua pro omnibus divisoribus primis a 7 usque ad 1000 minimi quoti singulis octo residuis respondentes exhibentur. Hoc autem praestito opera ipsa tabulas conficiendi in eo consistet, ut procedendo a numeris primis minoribus ad maiores pro quovis ex tabula subsidiaria exquiratur quotus q, qui pro residuo r exhibet numerum minimum formae $30q+r$ per propositum divisibilem. Quodsi hic divisor dicatur D, in columna verticali quaeratur valor ipsius q tumque in eadem linea horizontali sub residuo r illa invenietur areola, cui inscribi debet divisor propositus D. Reliquae autem areolae eodem divisore implendae invenientur, si pro q successive adhibeantur $q+D$, $q+2D$, $q+3D$ etc. Areolae, quae divisore non impletae sunt, signentur littera p, quae significabit numerum huic areolae respondentem esse primum. Usus autem huiusmodi tabulae facilis est, nam proposito numero quocumque, quem examinare quis voluerit, utrum primus sit necne et quosnam habeat divisores, dividet istum numerum per 30 quotusque dabit valorem litterae q, residuum vero erit r. In prima igitur columna verticali quaeratur numerus q et a latere invenietur areola sub residuo r, quae ostendet, utrum numerus sit primus vel quemnam habeat minimum divisorem. Ut constructio ipsius tabulae eo facilius procedat, totus labor inter plures personas distribui posset, in septem exempli causa pensa, ita ut primum a 0 ad 5000, secundum hinc ad 10000, tertium ab hoc termino ad 15000, quartum ab hoc ad 20000, quintum ad 25000, sextum ad 30000 et denique septimum ad finem porrigeretur. Quo autem melius perspiceretur idea huius laboris, tabulam adnectendam iudicavit Illustr. EULERUS, qua valores ipsius q a 33300 ad 33400 comprehenduntur ideoque illi numeri, qui millies mille proxime sunt minores.

1. Si omnes numeros ab unitate usque ad millies mille ordine recensere et unicuique [minimum] suum divisorem vel notam numeri primi adscribere vellemus, tam labor quam volumen huiusmodi tabulas continens in immensum excresceret; quamobrem conveniet omnes eos numeros, quorum divisores minimi sponte patent, prorsus praetermittere, unde non solum omnes numeros pares, sed etiam eos, qui vel per 3 vel per 5 sunt divisibiles, excludemus, quippe quorum minimi divisores sponte se produnt. Alios igitur numeros in nostram tabulam non referemus praeter primos, nisi quorum minimi divisores sint vel 7 vel 11 vel 13 vel alii numeri primi maiores; cuiusmodi numeri usque ad triginta sunt tantum octo isti

$$1,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23 \text{ et } 29.$$

2. Omnes ergo numeri, quos in nostram tabulam referemus, in hac forma generali

$$30q + r$$

erunt contenti, ubi r denotat octo illos numeros modo memoratos; pro q vero successive scribamus omnes plane numeros naturales 0, 1, 2, 3, 4, etc., donec valor formulae $30q$ usque ad unum millionem excrescat, quod fit sumendo $q = 33333$ vel etiam ultra, si limitem unius millionis transgredi voluerimus.

3. Quodsi iam talem tabulam in quarto expedire voluerimus, in qualibet pagina commode poterimus quinquaginta valores litterae q in prima cuiusque columna a summo ad imum descendendo exprimere, cui dextrorsum octo columnas adiungemus pro octo valoribus litterae r, sicque tantum opus erit singulis areolis in octo istis columnis, quae cuilibet valori litterae q respondent, vel minimos divisores numeri $30q + r$ vel notam numeri primi, quae nobis erit littera p, inscribere; sic enim proposito quocumque numero N dividatur ille per 30 et quotus ex divisione resultans sit $= q$, residuum vero restans $= r$, tum hi numeri q et r in nostris tabulis quaerantur et areola utrique conveniens ostendet minimum divisorem huius numeri N vel characterem p, si fuerit numerus primus.

4. Si singulae igitur paginae contineant quinquaginta valores litterae q, quibus octo memoratae columnae sint adiunctae, quaelibet pagina extendetur ad $30 \cdot 50 = 1500$ numeros sicque usque ad unum millionem opus erit 666 paginis;

quare cum una scheda in quarto praebeat octo paginas, numerus schedarum erit 83 circiter, unde nascitur volumen non nimis magnum, et aliquot calculatores sufficient ad totum opus brevi temporis spatio exsequendum.

5. Singulae igitur paginae huius operis ita erunt dispositae, uti specimen annexum ostendit, in quo primam paginam repraesentamus, cuius prima columna litterae q subiacens eius valores a 0 usque ad 49 exhibet, cui ad dextram adiunctae sunt octo illae columnae in fronte gerentes totidem residua 1, 7, 11, 13, 17, 19, 23, 29; tum vero simili modo sequens pagina in prima columna continebit numeros 50, 51, ... 99, tertia vero a 100 usque ad 149 etc., ubi semper octo columnae sequentes eadem octo residua referunt sicque totum negotium huc redit, ut in singulas areolas, quarum quaelibet pagina continet 400, vel divisores debitos vel litteram p utpote notam numeri primi inseramus, quem in finem sequentia subsidia explicare necesse erit.

q	1	7	11	13	17	19	23	29
0		p	p	p	p	p	p	p
1	p	p	p	p	p	7	p	p
2	p	p	p	p	7	p	p	p
3	7	p	p	p	p	p	p	7
4	11	p	p	7	p	p	11	p
5	p	p	7	p	p	13	p	p
6	p	11	p	p	p	p	7	11
7	p	7	13	p	p	p	p	p
8	p	13	p	11	p	7	p	p
9	p	p	p	p	7	17	p	13
10	7	p	p	p	p	11	17	7
11	p	p	11	7	p	p	p	p
12	19	p	7	p	13	p	p	p
13	17	p	p	13	11	p	7	p
14	p	7	p	p	19	p	p	p
15	11	p	p	p	p	7	11	p
16	13	p	p	17	7	p	p	p

q	1	7	11	13	17	19	23	29
17	7	11	p	p	17	23	13	7
18	p	p	19	7	p	13	p	p
19	p	p	7	11	p	19	p	p
20	p	p	13	p	p	p	7	17
21	p	7	p	p	p	11	p	p
22	p	23	11	p	p	7	p	13
23	p	17	p	19	7	p	23	p
24	7	p	17	p	11	p	p	7
25	p	p	p	7	13	p	p	19
26	11	p	7	13	p	17	11	p
27	p	19	p	p	p	p	7	p
28	29	7	23	p	p	p	p	11
29	13	p	p	p	p	7	19	29
30	17	p	p	11	7	p	13	p
31	7	p	p	23	p	13	p	7
32	31	p	p	7	p	11	p	23
33	p	p	7	17	19	p	p	p
34	p	13	p	p	17	p	7	p
35	p	7	p	p	11	p	29	13
36	23	p	p	p	p	7	p	p
37	11	p	19	p	7	p	11	17
38	7	31	p	p	13	19	p	7
39	p	11	p	7	p	29	p	11
40	p	17	7	p	p	23	p	p
41	p	p	17	11	29	p	7	p
42	13	7	31	19	p	p	p	p
43	p	p	p	p	p	7	13	p
44	p	p	11	31	7	13	17	19
45	7	23	p	29	p	37	p	7
46	1	19	13	7	11	p	23	p
47	17	13	7	p	p	p	p	p
48	11	p	p	p	31	p	7	13
49	p	7	p	p	p	p	p	p

6. Ponamus igitur in genere quaerendos esse omnes numeros formae $30q + r$, qui per datum numerum primum P sint divisibiles, ita ut in areolas his numeris respondentes ipse numerus P inscribi debeat, nisi forte eidem areolae iam numerus minor fuerit inscriptus. Sumamus autem pro residuo $r = \alpha$ formulam $30q + \alpha$ divisibilem fieri per propositum numerum primum P casu, quo $q = a$, ita ut numerus $30a + \alpha$ divisionem per P admittat; tum igitur manifestum est formulam $30q + \alpha$ etiam divisibilem fore sumendo $q = a + nP$, unde hoc commodum nanciscimur, ut, si in quapiam columna pro residuo α numerus $30q + \alpha$ divisibilis fuerit per P casu $q = a$, tum omnes valores ipsius q eadem indole gaudentes futuri sint

$$a + P, \quad a + 2P, \quad a + 3P, \quad a + 4P, \quad a + 5P \text{ etc.},$$

iuxta quos igitur areolis respondentibus sub residuo α divisor iste primus P inscribi debebit, quod ergo negotium per omnes paginas sequentes facillime absolvetur. Dummodo igitur pro qualibet columna prima areola constet, cui numerum primum P inscribi oportet, tum per omnes paginas sequentes areolae, quibus idem numerus inscribi debet, facillime definiuntur.

7. Sumto autem numero primo quocumque P minimus numerus, cuius minimus divisor est $= P$, est semper PP, in cuius igitur areola omnium prima numerus P inscribendus erit. Ita si proponatur divisor 7, is in nostra tabula primum occurret apud numerum $49 = 30 \cdot 1 + 19$, ubi est $q = 1$ et $r = 19$; at si divisor proponatur 11, minimus numerus, cui is in nostra tabula respondebit, erit $11^2 = 121$, pro quo erit $q = 4$ et $r = 1$, sicque in prima columna, ubi $r = 1$, apud $q = 4$ occurret numerus 11, qui deinceps pro eadem columna conveniet omnibus valoribus, qui sunt $4 + 11 = 15, 26, 37, 48, 59$ etc. usque ad finem totius tabulae.

8. Praecipuus igitur labor in hoc consistet, ut proposito numero quocumque P pro singulis residuis r definiantur minimi numeri q, qui formulam $30q + r$ divisibilem producant per P; haec autem investigatio eo modo est instituenda, quemadmodum in sequenti Problemate docebimus, ubi pro divisore P sumemus 7, quippe qui est minimus divisor, qui in nostra tabula occurrere potest, propterea quod numeri primi minores 2, 3 et 5 sunt exclusi.

PROBLEMA 1

9.[1]) *Pro singulis octo valoribus litterae r invenire minimos valores litterae q, quibus formula $30q + r$ per 7 fiat divisibilis.*

SOLUTIO

Sit primo $r = 1$ et formula $30q + 1$ divisibilis esse debet per 7; ponatur ergo $30q + 1 = 7A$ eritque $A = 4q + \frac{2q+1}{7}$; ita $2q + 1$ divisibilis esse debet per 7, quod manifesto fit, si $q = 3$; omnes ergo valores ipsius q erunt

3, 10, 17, 24, 31, 38, 45, 52, 59, 66 etc.

Sit secundo $r = 7$ et formula $30q + 7$ divisibilis manifesto fit, si $q = 0$; eius ergo sequentes valores sunt

7, 14, 21, 28, 35, 42, 49, 56 etc.;

unde singulis areolis in nostra tabula numerum 7 inscribamus praeterquam primae areolae, quae continet notam p.

Sit tertio $r = 11$ et fiat $30q + 11 = 7A$ eritque $A = 4q + 1 + \frac{2q+4}{7}$, ubi ergo est $q = 5$ eiusque sequentes valores

12, 19, 26, 33, 40, 47 etc.

Sit quarto $r = 13$ et fiat $30q + 13 = 7A$ eritque $A = 4q + 1 + \frac{2q+6}{7}$, ubi ergo $q = 4$ et sequentes eius valores

11, 18, 25, 32, 39, 46, 53 etc.

Sit quinto $r = 17$, ut formula $30q + 17$ divisibilis esse debeat per 7; ideoque ponamus eam $= 7A$ fietque $A = 4q + 2 + \frac{2q+3}{7}$, quocirca q esse debet $= 2$ et valores sequentes erunt

9, 16, 23, 30, 37, 44, 51 etc.

---

1) Abhinc paragraphorum numeri in editione principe desunt. F. R.

Sit sexto $r = 19$ et fiat $30q + 19 = 7A$ ideoque $A = 4q + 2 + \frac{2q+5}{7}$; manifesto hinc fit $q = 1$, sequentes autem valores erunt

8, 15, 22, 29, 36, 43, 50 etc.

Sit septimo $r = 23$ fietque $30q + 23 = 7A$, hinc $A = 4q + 3 + \frac{2q+2}{7}$; debet ergo esse $q = 6$ et sequentes valores

13, 20, 27, 34, 41, 48 etc.

Sit octavo $r = 29$ et $30q + 29 = 7A$, ita ut $A = 4q + 4 + \frac{2q+1}{7}$; hincque manifesto $q = 3$ et sequentes valores

10, 17, 24, 31, 38, 45 etc.

COROLLARIUM 1

10. Quia areola, quae respondet numeris $q = 1$, $r = 19$, prima est, cui divisor 7 est inscribendus, omnes praecedentes numeri in nostra tabula relati erunt primi ideoque eorum areolas charactere p impleri oportet.

COROLLARIUM 2

11. Quia igitur pro omnibus octo residuis r minimos quotos q assignavimus, quibus formula $30q + r$ per 7 divisibilis evadit, unde simul omnes sequentes valores ipsius q facillime innotescunt, eos sequenti modo conspectui exponamus, quo facilius omnes areolae numero 7 implendae per omnes tabulas sequentes agnoscantur:

$r =$	1	7	11	13	17	19	23	29
$q =$	3	7	5	4	2	1	6	3
sequentes $q =$	10	14	12	11	9	8	13	10
sequentes $q =$	17	21	19	18	16	15	20	17
sequentes $q =$	24	28	26	25	23	22	27	24
generaliter $q =$	$3 + 7n$	$7 + 7n$	$5 + 7n$	$4 + 7n$	$2 + 7n$	$1 + 7n$	$6 + 7n$	$3 + 7n$

PROBLEMA 2

12. *Proposito divisore* 11 *pro singulis residuis* r *invenire minimos quotos* q, *quibus formula* $30q + r$ *per* 11 *fit divisibilis.*

SOLUTIO

Cum minimus numerus hunc divisorem gerens sit $121 = 30 \cdot 4 + 1$, prima areola, in qua iste divisor 11 occurret, erit $q = 4$, $r = 1$, omnes praecedentes areolae adhuc vacuae charactere p sunt replendae; nunc igitur pro singulis residuis r quotos minimos q quaeramus.

1. Si $r = 1$, modo vidimus fore $q = 4$ ideoque in genere $q = 4 + 11n$.

2. Sit $r = 7$ et ponatur $30q + 7 = 11A$; erit

$$A = 2q + \frac{8q+7}{11} = 3q - \frac{3q-7}{11},$$

unde fit $q = 6$ et in genere $q = 6 + 11n$.

3. Si $r = 11$, ponatur $30q + 11 = 11A$, unde $q = 0$; minimus autem erit $0 + 11$.

4. Si $r = 13$, ponatur $30q + 13 = 11A$, unde erit

$$A = 2q + 1 + \frac{8q+2}{11};$$

esse igitur debet $q = 8$ et in genere $q = 8 + 11n$.

5. Si $r = 17$, ponatur $30q + 17 = 11A$, unde erit

$$A = 2q + 1 + \frac{8q+6}{11},$$

quod divisibile fit per 11 ponendo $q = 2$; vel cum hic non sit minimus[1]), erit $q = 13$ et in genere $q = 13 + 11n$.

1) Quod significat pro numero $30 \cdot 2 + 17 = 77$ non 11, sed 7 esse divisorem minimum. Ad hoc autem observandum est in sequentibus schematibus permultos numeros $30q + r$ occurrere, pro quibus propositus divisor non est minimus, neque necessarium esse hanc ob rem correctiones ad hibere. F. R.

6. Si $r = 19$, ponatur $30q + 19 = 11A$, unde fit

$$A = 2q + 1 + \frac{8q+8}{11},$$

unde esse debet $q = 10$ et in genere $q = 10 + 11n$.

7. Si $r = 23$, ponatur $30q + 23 = 11A$, unde fit

$$A = 2q + 2 + \frac{8q+1}{11},$$

ubi esse debet $q = 4$ et in genere $q = 4 + 11n$.

8. Si $r = 29$, ponatur $30q + 29 = 11A$ hincque fit

$$A = 2q + 2 + \frac{8q+7}{11},$$

quocirca esse debet $q = 6$ et in genere $q = 6 + 11n$.

Hos igitur valores ita conspectui exponamus[1]) pro divisore 11:

$r =$	1	7	11	13	17	19	23	29
$q =$	4	6	11	8	13	10	4	6
sequentes $q =$	15	17	22	19	24	21	15	17
sequentes $q =$	26	28	33	30	35	32	26	28
sequentes $q =$	37	39	44	41	46	43	37	39

etc.

PROBLEMA 3

13. *Proposito divisore* 13 *pro singulis residuis r invenire quotos q, ut formula* $30q + r$ *divisibilis fiat per* 13.

SOLUTIO

Cum minimus numerus in nostra tabula, qui divisorem 13 adscriptum habebit, sit $13^2 = 169 = 30 \cdot 5 + 19$, omnia [praecedentia] loca [adhuc] vacua

1) In editione principe tabula sequens nonnullos errores continet, qui iam in *Comment arithm.* correcti sunt. F. R.

charactere p sunt replenda. Pro reliquis residuis aliam viam ineamus. Cum enim $30 \cdot 5 + 19$ minimus sit numerus divisore 13 signandus, omnes maiores continebuntur in hac forma $30 \cdot 5 + 19 + 13n$; quia autem numeri pares excluduntur, pro n sumi debent tantum numeri pares, ita ut tantum multipla 26 addi debeant, ubi notandum, si numeri prodeant maiores quam 30, tum unitatem accedere ad primum membrum $30q$, quod hic est $30 \cdot 5$; habebimus scilicet duas columnas, priorem pro q, alteram vero pro r, quae quasi monetas diversae speciei referunt, quarum triginta sub specie r contentae faciunt unitatem pro altera specie q.

Hoc notato, quia pro primo casu habuimus $q = 5$ et $r = 19$, continuo hic 26 addamus, uti sequens schema declarabit:

q	r	q	r	q	r	q	r
5	19	9	3	12	17	16	1
	26		26		26		26
6	15	9	29	13	13	16	27
	26		26		26		26
7	11	10	25	14	9	17	23
	26		26		26		
8	7	11	21	15	5		
	26		26		26		

Hae operationes scilicet eousque sunt continuandae, donec sub columna r omnia residua occurrant; tum igitur unicuique valor respondens q habebitur; hinc igitur sequens schema constituatur pro divisore 13:

$r =$	1	7	11	13	17	19	23	29
$q =$	16	8	7	13	12	5	17	9
sequentes $q =$	29	21	20	26	25	18	30	22
sequentes $q =$	42	34	33	39	38	31	43	35

etc.

SCHOLION

14. Non autem opus est superiores operationes eousque continuare, donec octo nostra residua omnia occurrant, sed sufficit quatuor tantum nosse; ex quolibet enim casu $q = a$ et $r = \alpha$ etiam casus, quo $r = 30 - \alpha$, facile deducitur. Cum enim sit $30a + \alpha$ divisibile per 13, erit $30(a+1) - 30 + \alpha$ etiam divisibile hincque etiam eius negativum $-30(a+1) + 30 - \alpha$; addatur $30 \cdot 13$, ut habeatur $30(12 - a) + 30 - \alpha$ divisibile per 13; ergo si fuerit $r = 30 - \alpha$, erit $q = 12 - a$. Hinc igitur, quia primo erat $a = 5$ et $\alpha = 19$, nunc pro $r = 30 - 19 = 11$ erit $q = 7$. Deinde erat $\alpha = 7$ et $a = 8$, hinc pro casu $r = 30 - 7 = 23$ erit $q = 4$ sive $q = 17$. Porro ubi $\alpha = 29$, erat $a = 9$, hinc, si $r = 1$, fit $q = 3$ sive $q = 16$. Eodem modo ubi $\alpha = 17$, erat $a = 12$, hinc, si $r = 13$, fiet $q = 0$, hoc est $q = 13$.

PROBLEMA 4

15. *Proposito divisore* 17 *pro singulis residuis* r *invenire quotos* q, *ut formula* $30q + r$ *divisibilis fiat per* 17.

SOLUTIO

Cum minimus numerus hoc divisore signandus sit $17^2 = 289 = 30 \cdot 9 + 19$, pro eo erit $q = 9$ et $r = 19$ atque omnes praecedentes areolae adhuc vacuae littera p erunt replendae. Nunc igitur si q et r ut nomina duarum specierum spectemus, quarum prior continet triginta posterioris, primus noster numerus per 17 divisibilis erit $9^{(q)} + 19^{(r)}$; cui si continuo addamus $2 \cdot 17 = 34$, hoc est $1^{(q)} + 4^{(r)}$, operationes sequentes praebebunt valores:

q	r	q	r
9	19	17	17
10	23	18	21
11	27	19	25
13	1	20	29
14	5	22	3
15	9	23	7
16	13	24	11

Unde sequens schema perficitur pro divisore 17:

r	1	7	11	13	17	19	23	29
q	13	23	24	16	17	9	10	20
q	30	40	41	33	34	26	27	37
q	47	57	58	50	51	43	44	54

etc.

PROBLEMA 5

16. *Proposito divisore* 19 *pro singulis residuis* r *invenire quotos* q, *ut formula* $30q + r$ *divisibilis fiat per* 19.

SOLUTIO

Minimus numerus hoc divisore signandus erit $361 = 30 \cdot 12 + 1$, ita ut sit $q = 12$ et $r = 1$; hinc formulae $12^{(q)} + 1^{(r)}$ continuo addatur numerus $2 \cdot 19 = 38 = 1^{(q)} + 8^{(r)}$ sive $2^{(q)} - 22^{(r)}$, unde sequentes nascuntur operationes:

q	r	q	r
12	1	22	5
13	9	23	13
14	17	24	21
15	25	25	29
17	3	27	7
18	11	28	15
19	19	29	23
20	27	31	1

Unde sequens schema conficitur pro divisore 19:

$r =$	1	7	11	13	17	19	23	29
$q =$	12	27	18	23	14	19	29	25
$q =$	31	46	37	42	33	38	48	44
$q =$	50	65	56	61	52	57	67	63

etc.

PROBLEMA 6

17. *Proposito divisore* 23 *pro singulis residuis* r *invenire quotos* q, *ut formula* $30q + r$ *divisibilis fiat per* 23.

SOLUTIO

Cum minimus numerus hoc divisore 23 signandus sit $23^2 = 529 = 30 \cdot 17 + 19$, erit $q = 17$ et $r = 19$. Nunc igitur formulae $17^{(q)} + 19^{(r)}$ continuo addamus numerum $46 = 1^{(q)} + 16^{(r)}$ sive $2^{(q)} - 14^{(r)}$, ut sequitur:

q	r	q	r
17	19	29	27
19	5	31	13
20	21	32	29
22	7	34	15
23	23	36	1
25	9	37	17
26	25	39	3
28	11	40	19

Unde hoc schema conficitur pro divisore 23:

$r =$	1	7	11	13	17	19	23	29
$q =$	36	22	28	31	37	17	23	32
$q =$	59	45	51	54	60	40	46	55

etc.

PROBLEMA 7

18. *Proposito divisore* 29 *pro singulis residuis* r *invenire quotos* q, *ut formula* $30q + r$ *divisibilis fiat per* 29.

SOLUTIO

Cum minimus numerus hoc divisore signandus sit $29^2 = 841 = 30 \cdot 28 + 1$, erit $q = 28$ et $r = 1$. Nunc igitur ad $28^{(q)} + 1^{(r)}$ continuo addamus $58 = 1^{(q)} + 28^{(r)}$ sive $2^{(q)} - 2^{(r)}$, uti sequitur:

q	r	q	r
28	1	43	15
29	29	45	13
31	27	47	11
33	25	49	9
35	23	51	7
37	21	53	5
39	19	55	3
41	17	57	1

Unde sequens schema pro divisore 29 conficitur:

$r =$	1	7	11	13	17	19	23	29
$q =$	28	51	47	45	41	39	35	29
$q =$	57	80	76	74	70.	68	64	58

etc.

SCHOLION

19. Pro sequentibus divisoribus talia Problemata generalius tractari possunt sicque totum negotium nostrum conficietur, quando sequentia octo Problemata solvemus.

PROBLEMA GENERALE I

20. *Proposito divisore primo* $30a + 1$ *pro singulis residuis* r *omnes quotos* q *invenire, ut formula* $30q + r$ *divisibilis fiat per numerum* $30a + 1$.

SOLUTIO

Cum minimus numerus hoc divisore signandus sit

$$900aa + 60a + 1,$$

erit $q = 30aa + 2a$ et $r = 1$. Nunc igitur ad hunc numerum

$$(30aa + 2a)^{(q)} + 1^{(r)}$$

continuo addamus duplum divisorem

$$60a + 2 = 2a^{(q)} + 2^{(r)} \quad \text{sive} \quad (2a + 1)^{(q)} - 28^{(r)},$$

uti sequitur:

q	r	q	r
$30aa + 2a$	1	$30aa + 18a$	17
$30aa + 4a$	3	$30aa + 20a$	19
$30aa + 6a$	5	$30aa + 22a$	21
$30aa + 8a$	7	$30aa + 24a$	23
$30aa + 10a$	9	$30aa + 26a$	25
$30aa + 12a$	11	$30aa + 28a$	27
$30aa + 14a$	13	$30aa + 30a$	29
$30aa + 16a$	15	$30aa + 32a + 1$	1

Nunc igitur singula nostra residua in linea verticali exponamus et singulis quotos respondentes q adscribamus:

r	q
1	$30aa + 2a + n(30a + 1)$
7	$30aa + 8a + n(30a + 1)$
11	$30aa + 12a + n(30a + 1)$
13	$30aa + 14a + n(30a + 1)$
17	$30aa + 18a + n(30a + 1)$
19	$30aa + 20a + n(30a + 1)$
23	$30aa + 24a + n(30a + 1)$
29	$30aa + 30a + n(30a + 1)$

SCHOLION

21. Quodsi tabulam numerorum primorum usque ad unum millionem continuare velimus, maiores divisores primi in ea occurrere non possunt quam 1000, unde tantum opus est nostra schemata pro omnibus numeris primis millenario non maioribus extendere; hinc divisores primi in formula $30a + 1$ contenti in adiuncta tabula referuntur:

Numeri primi formae $30a + 1$	Numeri a	Numeri primi formae $30a + 1$	Numeri a
31	1	541	18
61	2	571	19
151	5	601	20
181	6	631	21
211	7	661	22
241	8	691	23
271	9	751	25
331	11	811	27
421	14	991	33
		1021	34

Nunc igitur pro singulis his divisoribus schemata nostra, uti incepimus, adiungere poterimus.

Tabula exhibens minimos quotos q
pro divisoribus primis formae $30a + 1$ ad singula octo residua relatos

Tabula generalis

a	Divisor	1	7	11	13	17	19	23	29
1	31	32	38	42	44	48	50	54	60
2	61	124	136	144	148	156	160	168	180
5	151	760	790	810	820	840	850	870	900
6	181	1092	1128	1152	1164	1188	1200	1224	1260
7	211	1484	1526	1554	1568	1596	1610	1638	1680
8	241	1936	1984	2016	2032	2064	2080	2112[1]	2160
9	271	2448	2502	2538	2556	2592	2610	2646	2700
11	331	3652	3718	3762	3784	3828	3850	3894	3960
14	421	5908	5992	6048	6076	6132	6160	6216	6300
18	541	9756	9864	9936	9972	10044	10080	10152	10260
19	571	10868	10982	11058	11096	11172	11210	11286	11400
20	601	12040	12160	12240	12280	12360	12400	12480	12600
21	631	13272	13398	13482	13524	13608	13650	13734	13860
22	661	14564	14696	14784	14828	14916	14960	15048	15180
23	691	15916	16054	16146	16192	16284	16330	16422	16560
25	751	18800	18950	19050	19100	19200	19250	19350	19500
27	811	21924	22086	22194[2]	22248	22356	22410	22518	22680
33	991	32736	32934	33066	33132	33264	33330	33462	33660

PROBLEMA GENERALE II

22. *Proposito divisore primo* $30a - 1$ *pro omnibus residuis* r *invenire quotos* q, *ut formula* $30q + r$ *divisibilis sit per* $30a - 1$.

SOLUTIO

Cum minimus numerus hoc divisore signandus sit

$$30 \cdot 30aa - 2 \cdot 30a + 1,$$

1) Editio princeps: 2110, qui error iam in *Comment. arithm.* correctus est. F. R.

2) Editio princeps (atque etiam *Comment. arithm.*): 22904. Correxit F. R.

erit $q = 30aa - 2a$ et $r = 1$; nunc igitur ad hanc formulam

$$(30aa - 2a)^{(q)} + 1^{(r)}$$

continuo addatur numerus

$$60a - 2 = 2a^{(q)} - 2^{(r)} \quad \text{sive} \quad (2a - 1)^{(q)} + 28^{(r)},$$

unde sequitur:

q	r	q	r
$30aa - 2a$	1	$30aa + 12a - 1$	17
$30aa + 0a - 1$	29	$30aa + 14a - 1$	15
$30aa + 2a - 1$	27	$30aa + 16a - 1$	13
$30aa + 4a - 1$	25	$30aa + 18a - 1$	11
$30aa + 6a - 1$	23	$30aa + 20a - 1$	9
$30aa + 8a - 1$	21	$30aa + 22a - 1$	7
$30aa + 10a - 1$	19		

Hinc igitur quoti q singulis residuis r respondentes erunt:

r	q
1	$30aa - 2a + n(30a - 1)$
7	$30aa + 22a - 1 + n(30a - 1)$
11	$30aa + 18a - 1 + n(30a - 1)$
13	$30aa + 16a - 1 + n(30a - 1)$
17	$30aa + 12a - 1 + n(30a - 1)$
19	$30aa + 10a - 1 + n(30a - 1)$
23	$30aa + 6a - 1 + n(30a - 1)$
29	$30aa + 0a - 1 + n(30a - 1)$

Cum igitur divisor noster $30a - 1$ contineatur in forma $30q + 29$ existente $a = q + 1$, ex nostra tabula [§ 5] excerpantur ordine omnes numeri primi formae $30q + 29$ et pro singulis capiatur $a = q + 1$ hincque sequens prodit

Tabula generalis

a	Divisor	1	7	11	13	17	19	23	29
1	29	28	51	47	45	41	39	35	29
2	59	116	163	155	151	143	139	131	119
3	89	264	335	323	317	305	299	287	269
5	149	740	859	839	829	809	799	779	749
6	179	1068	1211	1187	1175	1151	1139	1115	1079
8	239	1904	2095	2063	2047	2015	1999	1967	1919
9	269	2412	2627	2591	2573	2537	2519	2483	2429
12	359	4296	4583	4535	4511	4463	4439	4391	4319
13	389	5044	5355	5303	5277	5225	5199	5147	5069
14	419	5852	6187	6131	6103	6047	6019	5963	5879
15	449	6720	7079	7019	6989	6929	6899	6839	6749
16	479	7648	8031	7967	7935	7871	7839	7775	7679
17	509	8636	9043	8975	8941	8873	8839	8771	8669
19	569	10792	11247	11171	11133	11057	11019	10943	10829
20	599	11960	12439	12359	12319	12239	12199	12119	11999
22	659	14476	15003	14915	14871	14783	14739	14651	14519
24	719	17232	17807	17711	17663	17567	17519	17423	17279
27	809	21816	22463	22355	22301	22193	22139	22031	21869
28	839	23464	24135	24023	23967	23855	23799	23687	23519
31	929	28768	29511	29387	29325	29201	29139	29015	28829

PROBLEMA GENERALE III

23. *Proposito divisore primo* $30a + 7$ *pro singulis residuis* r *invenire quotos* q, *ut formula* $30q + r$ *divisibilis fiat per* $30a + 7$.

SOLUTIO

Cum minimus numerus hoc divisore signandus sit

$$30 \cdot 30aa + 30 \cdot 14a + 49,$$

pro eo erit $q = 30aa + 14a + 1$ et $r = 19$. Nunc igitur ad formulam

$$(30aa + 14a + 1)^{(q)} + 19^{(r)}$$

continuo addatur numerus

$$60a + 14 = 2a^{(q)} + 14^{(r)} \quad \text{sive} \quad (2a + 1)^{(q)} - 16^{(r)},$$

unde sequitur:

q	r	q	r
$30aa + 14a + 1$	19	$30aa + 28a + 4$	27
$30aa + 16a + 2$	3	$30aa + 30a + 5$	11
$30aa + 18a + 2$	17	$30aa + 32a + 5$	25
$30aa + 20a + 3$	1	$30aa + 34a + 6$	9
$30aa + 22a + 3$	15	$30aa + 36a + 6$	23
$30aa + 24a + 3$	29	$30aa + 38a + 7$	7
$30aa + 26a + 4$	13		

Et hinc pro singulis residuis r quoti q ita colliguntur:

r	q
1	$30aa + 20a + 3 + n(30a + 7)$
7	$30aa + 38a + 7 + n(30a + 7)$
11	$30aa + 30a + 5 + n(30a + 7)$
13	$30aa + 26a + 4 + n(30a + 7)$
17	$30aa + 18a + 2 + n(30a + 7)$
19	$30aa + 14a + 1 + n(30a + 7)$
23	$30aa + 36a + 6 + n(30a + 7)$
29	$30aa + 24a + 3 + n(30a + 7)$

Cum divisor noster in forma $30q + 7$ contineatur, excerpantur ex tabula nostra [§ 5] ordine omnes numeri primi huius formae ac pro singulis erit $a = q$ hincque sequens construatur

Tabula generalis

a	Divisor	1	7	11	13	17	19	23	29
0	7	3	7	5	4	2	1	6	3
1	37	53	75	65	60	50	45	72	57
2	67	163	203	185	176	158	149	198	171
3	97	333	391	365	352	326[1])	313	384	345
4	127	563	639	605	588	554	537	630	579
5	157	853	947	905	884	842	821	936	873
9	277	2613	2779	2705	2668	2594	2557	2760	2649
10	307	3203	3387	3305	3264	3182	3141	3366	3243
11	337	3853	4055	3965	3920	3830	3785	4032	3897
12	367	4563	4783	4685	4636	4538	4489	4758	4611
13	397	5333	5571	5465	5412	5306	5253	5544	5385
15	457	7053	7327	7205	7144	7022	6961	7296	7113
16	487	8003	8295	8165	8100	7970	7905	8262	8067
18	547	10083	10411	10265	10192	10046	9973	10374	10155
19	577	11213	11559	11405	11328	11174	11097	11520	11289
20	607	12403	12767	12605	12524	12362	12281	12726	12483
24	727	17763	18199	18005	17908	17714	17617	18150	17859
25	757	19253	19707	19505	19404	19202	19101	19656	18353
26	787	20803	21275	21065	20960	20750	20645	21222	20907
29	877	25813	26339	26105	25988	25754	25637	26280	25929
30	907	27603	28147	27905	27784	27542	27421	28086	27723
31	937	29453	30015	29765	29640	29390	29265	29952	29577
32	967	31363	31943	31685	31556	31298	31169	31878	31491
33	997	33333	33931	33665	33532	33266	33133	33864	33465

PROBLEMA GENERALE IV

24. *Proposito divisore primo* $30a - 7$ *pro singulis residuis* r *invenire quotos* q, *ut formula* $30q + r$ *fiat divisibilis per* $30a - 7$.

1) Editio princeps (atque etiam *Comment. arithm.*): 308. Correxit F. R.

SOLUTIO

Cum minimus numerus hoc divisore signandus sit

$$30 \cdot 30aa - 30 \cdot 14a + 49,$$

erit $q = 30aa - 14a + 1$ et $r = 19$; hinc ad numerum

$$(30aa - 14a + 1)^{(q)} + 19^{(r)}$$

continuo addatur forma

$$60a - 14 = 2a^{(q)} - 14^{(r)} \quad \text{seu} \quad (2a - 1)^{(q)} + 16^{(r)},$$

unde calculus iste oritur:

q	r	r	r
$30aa - 14a + 1$	19	$30aa + 2a - 3$	27
$30aa - 12a + 1$	5	$30aa + 4a - 3$	13
$30aa - 10a$	21	$30aa + 6a - 4$	29
$30aa - 8a$	7	$30aa + 8a - 4$	15
$30aa - 6a - 1$	23	$30aa + 10a - 4$	1
$30aa - 4a - 1$	9	$30aa + 12a - 5$	17
$30aa - 2a - 2$	25	$30aa + 14a - 5$	3
$30aa + 0a - 2$	11	$30aa + 16a - 6$	19

Hinc igitur quoti ordine disponantur pro singulis nostris residuis r, uti sequitur:

r	q
1	$30aa + 10a - 4 + n(30a - 7)$
7	$30aa - 8a - 0 + n(30a - 7)$
11	$30aa + 0a - 2 + n(30a - 7)$
13	$30aa + 4a - 3 + n(30a - 7)$
17	$30aa + 12a - 5 + n(30a - 7)$
19	$30aa - 14a + 1 + n(30a - 7)$
23	$30aa - 6a - 1 + n(30a - 7)$
29	$30aa + 6a - 4 + n(30a - 7)$

Cum igitur divisor noster $30a - 7$ pertineat ad formam $30q + 23$, ex tabula nostra [§ 5] ordine excerpantur omnes numeri primi formae $30q + 23$ eritque pro singulis $a = q + 1$ hincque sequens tabula generalis conficiatur.

Tabula generalis

a	Divisor	1	7	11	13	17	19	23	29
1	23	36	22	28	31	37	17	23	32
2	53	136	104	118[1])	125	139	93	107	128
3	83	296	246	268	279	301	229	251	284
4	113	516	448	478	493	523	425	455	500[2])
6	173	1136	1032	1078	1101	1147	997	1043	1112
8	233	1996	1856	1918	1949	2011	1809	1871	1964[3])
9	263	2516	2358	2428	2463	2533	2305	2375	2480
10	293	3096	2920	2998	3037	3115	2861	2939	3056
12	353	4436	4224	4318	4365	4459[4])	4153	4247	4388
13	383	5196[5])	4966[6])	5068	5119	5221	4889	4991	5144
15	443	6896	6630	6748	6807[7])	6925[8])	6541	6659	6836
17	503	8836	8534	8668	8735[9])	8869	8433	8567	8768
19	563	11016	10678	10828	10903	11053	10565	10715	10940
20	593	12196	11840	11998	12077	12235	11721	11879	12116
22	653	14736	14344	14518	14605	14779	14213	14387	14648
23	683	16096	15686	15868	15959	16141	15549	15731	16004
25	743	18996	18550	18748	18847	19045	18401	18599	18896
26	773	20536	20072	20278	20381	20587	19917	20123	20432[10])
29	863	25516	24998	25228	25343	25573	24825	25055	25400
32	953	31036	30464	30718	30845	31099	30273	30527	30908
33	983	32996	32406	32668	32799	33061	32209	32471	32864

PROBLEMA GENERALE V

25. *Proposito divisore primo* $30a + 11$ *invenire pro singulis residuis* r *quotos* q, *ut formula* $30q + r$ *fiat divisibilis per* $30a + 11$.

1) Editio princeps: 108. 2) Ed. pr.: 460. 3) Ed. pr.: 1876. 4) Ed. pr.: 4181. 5) Ed. pr.: 5206. 6) Ed. pr.: 4996. 7) Ed. pr.: 6693. 8) Ed. pr.: 6575. 9) Ed. pr.: 8734. 10) Ed. pr.: 20430. Qui errores omnes etiam in *Comment. arithm.* inveniuntur. Correxit F. R.

SOLUTIO

Cum minimus hoc divisore signandus numerus sit

$$30 \cdot 30aa + 30 \cdot 22a + 121,$$

pro eo erit $q = 30aa + 22a + 4$ et $r = 1$. Nunc igitur ad formulam

$$(30aa + 22a + 4)^{(q)} + 1^{(r)}$$

continuo numerum

$$60a + 22 = 2a^{(q)} + 22^{(r)} \quad \text{sive} \quad (2a + 1)^{(q)} - 8^{(r)}$$

addamus, uti sequitur:

q	r	q	r
$30aa + 22a + 4$	1	$30aa + 36a + 9$	5
$30aa + 24a + 4$	23	$30aa + 38a + 9$	27
$30aa + 26a + 5$	15	$30aa + 40a + 10$	19
$30aa + 28a + 6$	7	$30aa + 42a + 11$	11
$30aa + 30a + 6$	29	$30aa + 44a + 12$	3
$30aa + 32a + 7$	21	$30aa + 46a + 12$	25
$30aa + 34a + 8$	13	$30aa + 48a + 13$	17

Et hinc pro singulis residuis r quoti q colliguntur sequenti modo:

r	q
1	$30aa + 22a + 4 + n(30a + 11)$
7	$30aa + 28a + 6 + n(30a + 11)$
11	$30aa + 42a + 11 + n(30a + 11)$
13	$30aa + 34a + 8 + n(30a + 11)$
17	$30aa + 48a + 13 + n(30a + 11)$
19	$30aa + 40a + 10 + n(30a + 11)$
23	$30aa + 24a + 4 + n(30a + 11)$
29	$30aa + 30a + 6 + n(30a + 11)$

Cum nunc divisor ille $30a + 11$ in forma $30q + 11$ contineatur, excerpantur ordine ex tabula nostra [§ 5] omnes numeri [primi huius formae] ac pro singulis erit $a = q$.

Tabula generalis

a	Divisor	1	7	11	13	17	19	23	29
0	11	4	6	11	8	13	10	4	6
1	41	56	64	83	72	91	80	58	66
2	71	168	182	215	196	229	210	172	186
3	101	340	360	407	380	427	400	346	366
4	131	572	598	659	624	685	650	580	606
6	191	1216	1254	1343	1292	1381	1330	1228	1266
8	251	2100	2150	2267	2200	2317	2250	2116	2166
9	281	2632	2688	2819	2744	2875	2800	2650	2706
10	311	3224	3286	3431	3348	3493	3410	3244	3306
13	401	5360	5440	5627	5520	5707	5600	5386	5466
14	431	6192	6278	6479	6364	6565	6450	6220	6306
15	461	7084	7176	7391	7268 [1])	7483	7360	7114	7206
16	491	8036	8134	8363	8232	8461	8330	8068	8166
17	521	9048	9152	9395	9256	9499	9360	9082	9186
21	641	13696	13824	14123	13952	14251	14080	13738	13866
23	701	16380	16520	16847	16660	16987	16800	16426	16566
25	761	19304	19456	19811	19608	19963	19760	19354	19506
27	821	22468	22632	23015	22796	23179	22960	22522	22686
29	881	25872	26048	26459	26224	26635	26400	25930	26106
30	911	27664	27846	28271	28028	28453	28210	27724	27906
31	941	29516 [2])	29704	30143	29892	30331	30080	29578	29766
32	971	31428	31622	32075	31816	32269	32010	31492	31686

PROBLEMA GENERALE VI

26. *Proposito divisore primo* $30a - 11$ *pro singulis residuis* r *invenire quotos* q, *ut formula* $30q + r$ *divisibilis fiat per* $30a - 11$.

1) Editio princeps: 7238. 2) Ed. pr.: 29716. Qui errores etiam in *Comment. arithm.* inveniuntur. Correxit F. R.

SOLUTIO

Cum minimus numerus hoc divisore signandus sit

$$30 \cdot 30aa - 30 \cdot 22a + 121,$$

erit $q = 30aa - 22a + 4$ et $r = 1$, unde ad numerum

$$(30aa - 22a + 4)^{(q)} + 1^{(r)}$$

continuo addere debemus formulam

$$60a - 22 = 2a^{(q)} - 22^{(r)} \quad \text{seu} \quad (2a - 1)^{(q)} + 8^{(r)},$$

uti ex sequente calculo constat:

q	r	q	r
$30aa - 22a + 4$	1	$30aa - 6a - 2$	5
$30aa - 20a + 3$	9	$30aa - 4a - 3$	13
$30aa - 18a + 2$	17	$30aa - 2a - 4$	21
$30aa - 16a + 1$	25	$30aa - 0a - 5$	29
$30aa - 14a + 1$	3	$30aa + 2a - 5$	7
$30aa - 12a - 0$	11	$30aa + 4a - 6$	15
$30aa - 10a - 1$	19	$30aa + 6a - 7$	23
$30aa - 8a - 2$	27	$30aa + 8a - 7$	1

Quotos autem hinc pro singulis nostris residuis ordine hic disponamus:

r	q
1	$30aa - 22a + 4 + n(30a - 11)$
7	$30aa + 2a - 5 + n(30a - 11)$
11	$30aa - 12a - 0 + n(30a - 11)$
13	$30aa - 4a - 3 + n(30a - 11)$
17	$30aa - 18a + 2 + n(30a - 11)$
19	$30aa - 10a - 1 + n(30a - 11)$
23	$30aa + 6a - 7 + n(30a - 11)$
29	$30aa - 0a - 5 + n(30a - 11)$

Cum nunc divisor noster $30a - 11$ sit formae $30q + 19$, ex tabula nostra [§ 5] excerpantur omnes numeri primi huius formae et pro singulis erit $a = q + 1$, unde construitur sequens tabula.

Tabula generalis

a	Divisor	1	7	11	13	17	19	23	29
1	19	12	27	18	23	14	19	29	25
3	79	208	271	234	255	218	239	281	265
4	109	396	483	432	461	410	439	497	475
5	139	644	755	690	727	662	699	773	745
7	199	1320	1479	1386	1439	1346	1399	1505	1465
8	229	1748	1931	1824	1885	1778	1839	1961	1915
12	349	4060	4339	4176	4269	4106	4199	4385	4315
13	379	4788	5091	4914	5015	4838	4939	5141	5065
14	409	5576	5903	5712	5821	5630	5739	5957	5875
15	439	6424	6775	6570	6687	6482	6599	6833	6745
17	499	8300	8699	8466	8599	8366	8499	8765 [1]	8665
21	619	12772	13267	12978	13143	12854	13019	13349	13225
24	709	16756	17323	16992	17181	16850	17039	17417	17275
25	739	18204	18795	18450	18647	18302	18499	18893	18745
26	769	19712	20327	19968	20173	19814	20019	20429	20275
28	829	22908	23571	23184	23405	23018	23239	23681	23515
29	859	24596	25283	24882	25111 [2]	24710	24939	25397	25225
31	919	28152	28887	28458	28703	28274	28519	29009	28825
34	1009	33936	34743	34272	34541	34070	34339	34877	34675

PROBLEMA GENERALE VII

27. *Proposito divisore primo* $30a + 13$ *pro singulis residuis* r *invenire quotos* q, *ut formula* $30q + r$ *divisibilis fiat per* $30a + 13$.

---

1) Editio princeps: 8867. 2) Ed. pr.: 25101. Qui errores etiam in *Comment. arithm.* inveniuntur. Correxit F. R.

SOLUTIO

Cum minimus numerus hoc divisore signandus sit

$$30 \cdot 30aa + 30 \cdot 26a + 169,$$

pro quo erit $q = 30aa + 26a + 5$ et $r = 19$, nunc igitur ad formulam

$$(30aa + 26a + 5)^{(q)} + 19^{(r)}$$

continuo addatur numerus

$$60a + 26 = 2a^{(q)} + 26^{(r)} \quad \text{sive} \quad (2a + 1)^{(q)} - 4^{(r)},$$

unde iste nascitur calculus:

q	r	q	r
$30aa + 26a + 5$	19	$30aa + 42a + 12$	17
$30aa + 28a + 6$	15	$30aa + 44a + 13$	13
$30aa + 30a + 7$	11	$30aa + 46a + 14$	9
$30aa + 32a + 8$	7	$30aa + 48a + 15$	5
$30aa + 34a + 9$	3	$30aa + 50a + 16$	1
$30aa + 36a + 9$	29	$30aa + 52a + 16$	27
$30aa + 38a + 10$	25	$30aa + 54a + 17$	23
$30aa + 40a + 11$	21	$30aa + 56a + 18$	19

Nunc autem pro singulis residuis r quoti q ita colliguntur, uti sequitur:

r	q
1	$30aa + 50a + 16 + n(30a + 13)$
7	$30aa + 32a + 8 + n(30a + 13)$
11	$30aa + 30a + 7 + n(30a + 13)$
13	$30aa + 44a + 13 + n(30a + 13)$
17	$30aa + 42a + 12 + n(30a + 13)$
19	$30aa + 26a + 5 + n(30a + 13)$
23	$30aa + 54a + 17 + n(30a + 13)$
29	$30aa + 36a + 9 + n(30a + 13)$

Cum nunc divisor $30a + 13$ sit formae $30q + 13$, ex tabula nostra [§ 5] excerpantur ordine numeri primi illic expositi eritque $a = q$, unde sequens tabula generalis construitur.

Tabula generalis

a	Divisor	1	7	11	13	17	19	23	29
0	13	16	8	7	13	12	5	17	9
1	43	96	70	67	87	84	61	101	75
2	73	236	192	187	221	216	177	245	201
3	103	436	374	367	415	408	353	449	387
5	163	1016	918	907	983	972	885	1037	939
6	193	1396	1280	1267	1357	1344	1241	1421	1305
7	223	1836	1702	1687	1791	1776	1657	1865	1731
9	283	2896	2726	2707	2839	2820	2669	2933	2763
10	313	3516	3328	3307	3453	3432	3265	3557	3369
12	373	4936	4712	4687	4861	4836	4637	4985	4761
14	433	6596	6336	6307	6509	6480	6249	6653	6393
15	463	7516	7238	7207	7423	7392	7145	7577	7299
17	523	9536	9222	9187	9431	9396	9117	9605	9291
20	613	13016	12648	12607	12893	12852	12525	13097	12729
21	643	14296	13910	13867	14167	14124	13781	14381	13995
22	673	15636	15232	15187	15501	15456	15097	15725	15321
24	733	18496	18056	18007	18349	18300	17909	18593	18153
27	823	23236	22742	22687	23071	23016	22577	23345	22851
28	853	24936	24424	24367	24765	24708	24253	25049	24537
29	883	26696	26166	26107	26519	26460	25989	26813	26283

PROBLEMA GENERALE VIII

28. *Proposito divisore primo* $30a - 13$ *pro singulis residuis* r *invenire quotos* q *formulam* $30q + r$ *divisibilem reddentes per* $30a - 13$.

SOLUTIO

Cum minimus numerus hoc divisore signandus sit

$$30 \cdot 30aa - 30 \cdot 26a + 169,$$

erit $q = 30aa - 26a + 5$ et $r = 19$, unde ad numerum

$$(30aa - 26a + 5)^{(q)} + 19^{(r)}$$

continuo addi debet formula

$$60a - 26 = 2a^{(q)} - 26^{(r)} \quad \text{seu} \quad (2a - 1)^{(q)} + 4^{(r)},$$

uti sequens calculus declarat:

q	r	q	r
$30aa - 26a + 5$	19	$30aa - 10a - 2$	21
$30aa - 24a + 4$	23	$30aa - 8a - 3$	25
$30aa - 22a + 3$	27	$30aa - 6a - 4$	29
$30aa - 20a + 3$	1	$30aa - 4a - 4$	3
$30aa - 18a + 2$	5	$30aa - 2a - 5$	7
$30aa - 16a + 1$	9	$30aa + 0a - 6$	11
$30aa - 14a + 0$	13	$30aa + 2a - 7$	15
$30aa - 12a - 1$	17	$30aa + 4a - 8$	19

Quotos autem hinc pro singulis nostris residuis r ordine hic exponamus:

r	q
1	$30aa - 20a + 3 + n(30a - 13)$
7	$30aa - 2a - 5 + n(30a - 13)$
11	$30aa + 0a - 6 + n(30a - 13)$
13	$30aa - 14a + 0 + n(30a - 13)$
17	$30aa - 12a - 1 + n(30a - 13)$
19	$30aa - 26a + 5 + n(30a - 13)$
23	$30aa - 24a + 4 + n(30a - 13)$
29	$30aa - 6a - 4 + n(30a - 13)$

Cum divisor ille $30a - 13$ in forma $30q + 17$ sit contentus, ex tabula prima [§ 5] excerpantur ordine numeri primi formulae $30q + 17$ eritque pro singulis $a = q + 1$ hincque sequens tabula generalis construatur.

Tabula generalis

a	Divisor	1	7	11	13	17	19	23	29
1	17	13	23	24	16	17	9	10	20
2	47	83	111	114	92	95	73	76	104
4	107	403	467	474	424	431	381	388	452
5	137	653	735	744	680	689	625	634	716
6	167	963	1063	1074	996	1007	929	940	1040
7	197	1333	1451	1464	1372	1385	1293	1306	1424[1])
8	227	1763	1899	1914	1808	1823	1717[2])	1732	1868
9	257	2253	2407	2424	2304	2321	2201	2218	2372
11	317	3413[3])	3603	3624[4])	3476	3497	3349	3370	3560
12	347	4083	4291	4314	4152	4175	4013	4036	4244
16	467	7363	7643	7674	7456	7487	7269[5])	7300	7580
19	557	10453	10787	10824	10564	10601	10341	10378	10712
20	587	11603	11955	11994	11720	11759	11485	11524	11876
21	617	12813	13183	13224	12936	12977	12689	12730	13100
22	647	14083	14471	14514	14212	14255	13953	13996	14384
23	677	15413[6])	15819	15864	15548	15593	15277	15322	15728
27	797	21333	21811	21864	21492	21545	21173	21226	21704
28	827	22963	23459	23514	23128	23183	22797	22852	23348
29	857	24653	25167	25224	24824	24881	24481	24538	25052
30	887	26403	26935	26994	26580	26639	26225	26284	26816
32	947	30083	30651	30714	30272	30335	29893	29956	30524
33	977	32013	32599	32664	32208	32273	31817	31882	32468

SCHOLION GENERALE

29. Quoniam divisores primos maiores in tabulam numerorum primorum introduci non convenit, nisi omnes minores iam fuerint expediti, omnino necesse est, ut ex octo tabulis praecedentibus una tabula maxime generalis conficiatur, in qua pro omnibus divisoribus primis ordine dispositis minimi quoti q exhibeantur singulis nostris octo residuis respondentes, quorum areolae singulis illis divisoribus signari debent.

1) Editio princeps: 1224. 2) Ed. pr.: 1817. 3) Ed. pr.: 2413. 4) Ed. pr.: 2624. 5) Ed. pr.: 7279. 6) Ed. pr.: 15513. Quorum errorum tertius et quartus iam in *Comment. arithm.* correcti sunt. F. R.

Tabula auxiliaris universalis

pro omnibus divisoribus primis a 7 usque ad 1000 continuatis minimos quotos q exhibens singulis octo residuis respondentes[1])

Divisores	1	7	11	13	17	19	23	29
7	3	7	5	4	2	1	6	3
11	4	6	11	8	13	10	4	6
13	16	8	7	13	12	5	17	9
17	13	23	24	16	17	9	10	20
19	12	27	18	23	14	19	29	25
23	36	22	28	31	37	17	23	32
29	28	51	47	45	41	39	35	29
31	32	38	42	44	48	50	54	60
37	53	75	65	60	50	45	72	57
41	56	64	83	72	91	80	58	66
43	96	70	67	87	84	61	101	75
47	83	111	114	92	95	73	76	104
53	136	104	118	125	139	93	107	128
59	116	163	155	151	143	139	131	119
61	124	136	144	148	156	160	168	180
67	163	203	185	176	158	149	198	171
71	168	182	215	196	229	210	172	186
73	236	192	187	221	216	177	245	201
79	208	271	234	255	218	239	281	265
83	296	246	268	279	301	229	251	284
89	264	335	323	317	305	299	287	269
97	333	391	365	352	326	313	384	345
101	340	360	407	380	427	400	346	366
103	436	374	367	415	408	353	449	387
107	403	467	474	424	431	381	388	452
109	396	483	432	461	410	439	497	475
113	516	448	478	493	523	425	455	500
127	563	639	605	588	554	537	630	579
131	572	598	659	624	685	650	580	606
137	653	735	744	680	689	625	634	716

1) In editione principe (atque etiam in *Comment. arithm.*) omnes fere errores, quos iam in octo tabulis praecedentibus correximus, etiam hac in tabula inveniuntur. F. R.

Divisores	1	7	11	13	17	19	23	29
139	644	755	690	727	662	699	773	745
149	740	859	839	829	809	799	779	749
151	760	790	810	820	840	850	870	900
157	853	947	905	884	842	821	936	873
163	1016	918	907	983	972	885	1037	939
167	963	1063	1074	996	1007	929	940	1040
173	1136	1032	1078	1101	1147	997	1043	1112
179	1068	1211	1187	1175	1151	1139	1115	1079
181	1092	1128	1152	1164	1188	1200	1224	1260
191	1216	1254	1343	1292	1381	1330	1228	1266
193	1396	1280	1267	1357	1344	1241	1421	1305
197	1333	1451	1464	1372	1385	1293	1306	1424
199	1320	1479	1386	1439	1346	1399	1505	1465
211	1484	1526	1554	1568	1596	1610	1638	1680
223	1836	1702	1687	1791	1776	1657	1865	1731
227	1763	1899	1914	1808	1823	1717	1732	1868
229	1748	1931	1824	1885	1778	1839	1961	1915
233	1996	1856	1918	1949	2011	1809	1871	1964
239	1904	2095	2063	2047	2015	1999	1967	1919
241	1936	1984	2016	2032	2064	2080	2112	2160
251	2100	2150	2267	2200	2317	2250	2116	2166
257	2253	2407	2424	2304	2321	2201	2218	2372
263	2516	2358	2428	2463	2533	2305	2375	2480
269	2412	2627	2591	2573	2537	2519	2483	2429
271	2448	2502	2538	2556	2592	2610	2646	2700
277	2613	2779	2705	2668	2594	2557	2760	2649
281	2632	2688	2819	2744	2875	2800	2650	2706
283	2896	2726	2707	2839	2820	2669	2933	2763
293	3096	2920	2998	3037	3115	2861	2939	3056
307	3203	3387	3305	3264	3182	3141	3366	3243
311	3224	3286	3431	3348	3493	3410	3244	3306
313	3516	3328	3307	3453	3432	3265	3557	3369
317	3413	3603	3624	3476	3497	3349	3370	3560
331	3652	3718	3762	3784	3828	3850	3894	3960
337	3853	4055	3965	3920	3830	3785	4032	3897
347	4083	4291	4314	4152	4175	4013	4036	4244
349	4060	4339	4176	4269	4106	4199	4385	4315
353	4436	4224	4318	4365	4459	4153	4247	4388

Divisores	1	7	11	13	17	19	23	29
359	4296	4583	4535	4511	4463	4439	4391	4319
367	4563	4783	4685	4636	4538	4489	4758	4611
373	4936	4712	4687	4861	4836	4637	4985	4761
379	4788	5091	4914	5015	4838	4939	5141	5065
383	5196	4966	5068	5119	5221	4889	4991	5144
389	5044	5355	5303	5277	5225	5199	5147	5069
397	5333	5571	5465	5412	5306	5253	5544	5385
401	5360	5440	5627	5520	5707	5600	5386	5466
409	5576	5903	5712	5821	5630	5739	5957	5875
419	5852	6187	6131	6103	6047	6019	5963	5879
421	5908	5992	6048	6076	6132	6160	6216	6300
431	6192	6278	6479	6364	6565	6450	6220	6306
433	6596	6336	6307	6509	6480	6249	6653	6393
439	6424	6775	6570	6687	6482	6599	6833	6745
443	6896	6630	6748	6807	6925	6541	6659	6836
449	6720	7079	7019	6989	6929	6899	6839	6749
457	7053	7327	7205	7144	7022	6961	7296	7113
461	7084	7176	7391	7268	7483	7360	7114	7206
463	7516	7238	7207	7423	7392	7145	7577	7299
467	7363	7643	7674	7456	7487	7269	7300	7580
479	7648	8031	7967	7935	7871	7839	7775	7679
487	8003	8295	8165	8100	7970	7905	8262	8067
491	8036	8134	8363	8232	8461	8330	8068	8166
499	8300	8699	8466	8599	8366	8499	8765	8665
503	8836	8534	8668	8735	8869	8433	8567	8768
509	8636	9043	8975	8941	8873	8839	8771	8669
521	9048	9152	9395	9256	9499	9360	9082	9186
523	9536	9222	9187	9431	9396	9117	9605	9291
541	9756	9864	9936	9972	10044	10080	10152	10260
547	10083	10411	10265	10192	10046	9973	10374	10155
557	10453	10787	10824	10564	10601	10341	10378	10712
563	11016	10678	10828	10903	11053	10565	10715	10940
569	10792	11247	11171	11133	11057	11019	10943	10829
571	10868	10982	11058	11096	11172	11210	11286	11400
577	11213	11559	11405	11328	11174	11097	11520	11289
587	11603	11955	11994	11720	11759	11485	11524	11876
593	12196	11840	11998	12077	12235	11721	11879	12116
599	11960	12439	12359	12319	12239	12199	12119	11999

Divisores	1	7	11	13	17	19	23	29
601	12040	12160	12240	12280	12360	12400	12480	12600
607	12403	12767	12605	12524	12362	12281	12726	12483
613	13016	12648	12607	12893	12852	12525	13097	12729
617	12813	13183	13224	12936	12977	12689	12730	13100
619	12772	13267	12978	13143	12854	13019	13349	13225
631	13272	13398	13482	13524	13608	13650	13734	13860
641	13696	13824	14123	13952	14251	14080	13738	13866
643	14296	13910	13867	14167	14124	13781	14381	13995
647	14083	14471	14514	14212	14255	13953	13996	14384
653	14736	14344	14518	14605	14779	14213	14387	14648
659	14476	15003	14915	14871	14783	14739	14651	14519
661	14564	14696	14784	14828	14916	14960	15048	15180
673	15636	15232	15187	15501	15456	15097	15725	15321
677	15413	15819	15864	15548	15593	15277	15322	15728
683	16096	15686	15868	15959	16141	15549	15731	16004
691	15916	16054	16146	16192	16284	16330	16422	16560
701	16380	16520	16847	16660	16987	16800	16426	16566
709	16756	17323	16992	17181	16850	17039	17417	17275
719	17232	17807	17711	17663	17567	17519	17423	17279
727	17763	18199	18005	17908	17714	17617	18150	17859
733	18496	18056	18007	18349	18300	17909	18593	18153
739	18204	18795	18450	18647	18302	18499	18893	18745
743	18996	18550	18748	18847	19045	18401	18599	18896
751	18800	18950	19050	19100	19200	19250	19350	19500
757	19253	19707	19505	19404	19202	19101	19656	19353
761	19304	19456	19811	19608	19963	19760	19354	19506
769	19712	20327	19968	20173	19814	20019	20429	20275
773	20536	20072	20278	20381	20587	19917	20123	20432
787	20803	21275	21065	20960	20750	20645	21222	20907
797	21333	21811	21864	21492	21545	21173	21226	21704
809	21816	22463	22355	22301	22193	22139	22031	21869
811	21924	22086	22194	22248	22356	22410	22518	22680
821	22468	22632	23015	22796	23179	22960	22522	22686
823	23236	22742	22687	23071	23016	22577	23345	22851
827	22963	23459	23514	23128	23183	22797	22852	23348
829	22908	23571	23184	23405	23018	23239	23681	23515
839	23464	24135	24023	23967	23855	23799	23687	23519
853	24936	24424	24367	24765	24708	24253	25049	24537

Divisores	1	7	11	13	17	19	23	29
857	24653	25167	25224	24824	24881	24481	24538	25052
859	24596	25283	24882	25111	24710	24939	25397	25225
863	25516	24998	25228	25343	25573	24825	25055	25400
877	25813	26339	26105	25988	25754	25637	26280	25929
881	25872	26048	26459	26224	26635	26400	25930	26106
883	26696	26166	26107	26519	26460	25989	26813	26283
887	26403	26935	26994	26580	26639	26225	26284	26816
907	27603	28147	27905	27784	27542	27421	28086	27723
911	27664	27846	28271	28028	28453	28210	27724	27906
919	28152	28887	28458	28703	28274	28519	29009	28825
929	28768	29511	29387	29325	29201	29139	29015	28829
937	29453	30015	29765	29640	29390	29265	29952	29577
941	29516	29704	30143	29892	30331	30080	29578	29766
947	30083	30651	30714	30272	30335	29893	29956	30524
953	31036	30464	30718	30845	31099	30273	30527	30908
967	31363	31943	31685	31556	31298	31169	31878	31491
971	31428	31622	32075	31816	32269	32010	31492	31686
977	32013	32599	32664	32208	32273	31817	31882	32468
983	32996	32406	32668	32799	33061	32209	32471	32864
991	32736	32934	33066	33132	33264	33330	33462	33660
997	33333	33931	33665	33532	33266	33133	33864	33465
1009	33936	34743	34272	34541	34070	34339	34877	34675

PROBLEMA

30. *Tabulam numerorum primorum, quousque libuerit, continuare, quae simul omnium numerorum non primorum divisores minimos exhibeat.*

SOLUTIO

Ante omnia in singulis paginis, quotquot erit opus, lineae illae tam verticales quam horizontales, quae in pagina hic annexa[1]) cernuntur, erunt ducendae. Qui labor cum per se esset immensus, eum commodissime in typographia exsequi licebit, ubi omnes paginae talibus retibus signatae brevi temporis spatio excudi poterunt. Quin etiam, cum singulae paginae in suprema linea

1) Vide p. 399—400. F. R.

horizontali octo nostra residua 1, 7, 11, 13, 17, 19, 23, 29 referant, ea statim in omnibus paginis simul typo exprimi conveniet. Deinde quia primae columnae verticales quotos q ordine numerorum naturali procedentes complectuntur eorumque quinquaginta singulis paginis inseri debent, horum numerorum binae postremae notae etiam in typographia adiungi poterunt, dum alternatim numeri 00, 01, 02, 03, 04, 05 usque ad 49, tum vero 50, 51, 52, 53 etc. usque ad 99 in his primis columnis repraesentantur, quibus deinceps centuriae seu notae praecedentes facili negotio calamo praefiguntur; ubi quidem sufficiet hoc in solo supremo loco notasse. Quibus praeparatis singuli divisores primi 7, 11, 13, 17 etc. ordine areolis suis per omnes paginas inscribantur. A septenario igitur erit incipiendum; qui cum in prima columna residuum referente primum quoto $q = 3$ adscribi debeat, sequentes quoti continuo septenario augendi pariter numero 7 designari debebunt, qui labor facile per omnes sequentes tabulas continuabitur; similique modo pro reliquis [residuis 7,] 11, 13, 17 etc. hoc opus absolvetur. Deinde eodem modo divisor 11 per omnes paginas pro singulis residuis areolis debitis inscribatur, siquidem adhuc erunt vacuae; tum vero pari modo negotium pro omnibus sequentibus divisoribus primis instituatur. Scilicet si ad divisorem quemcumque primum, qui sit D, fuerit perventum, pro eo tabula praecedens generalis minimos praebet quotos q singulis octo residuis r respondentes, quibus notatis in singulis columnis eae areolae hoc divisore D signentur, quae respondebunt quotis $q + D$, $q + 2D$, $q + 3D$, $q + 4D$ etc., donec ad finem perveniatur; ubi autem iste divisor D primum in his tabulis occurret, omnes areolae praecedentes [adhuc vacuae] signo numerorum primorum p impleantur; ita si hae tabulae non ultra unum millionem extendi debeant, ultimus divisor primus erit 997 et ultimus quotus $q = 33333$; sicque totum hoc negotium ad finem erit perductum. Tum igitur si numerus quicumque M millionem non superans examinandus proponatur, is per 30 divisus praebeat quotum $= q$ et residuum $= r$; quibus binis valoribus in tabula quaeratur areola respondens et numerus ibi signatus ostendet minimum divisorem istius numeri; sin autem in ea areola reperiatur littera p, id erit signum propositum numerum M esse primum.

Quo autem hoc opus, quod utique multum temporis postularet, si ab una persona absolvi deberet, facilius exsequi liceat, totum laborem plures personae commode inter se partiri poterunt, dum quilibet certum pensum absolvendum suscipiet. Ita cum hae tabulae, siquidem ad unum millionem sint extendendae, usque ad quotum $q = 33400$ continuari debeant, totus labor in septem pensa distribui poterit, quorum primum a $q = 0$ usque ad 5000, secun-

dum ab hoc termino usque ad $q = 10000$, tertium ab hoc usque ad $q = 15000$, quartum ab hoc termino usque ad $q = 20000$, quintum ab hoc usque ad $q = 25000$, sextum ab hoc termino usque ad $q = 30000$ et septimum ab hoc termino usque ad finem porrigetur. Hoc pacto, quia singulae paginae quinquaginta valores ipsius q complectuntur, in quolibet penso habebuntur centum paginae adimplendae.

Posteriora quidem pensa continuo plus laboris requirent, quia in iis plures divisores occurrunt. Quo hoc clarius appareat, ponamus pensum aliquod incipere a valore $q = A$, et quia semper a divisoribus minimis ordine procedi oportet, pro quolibet divisore D ante omnia quaeratur eius multiplum proxime minus quam A, quod sit mD; tum istud multiplum mD addatur ad valores omnes ipsius q in nostra tabula divisori D respondentes. Sicque habebuntur totidem areolae, quibus iste divisor primus D erit inscribendus; sequentes autem areolae facillime obtinentur, dum illi primi valores ipsius q continuo ipso divisore D augentur. Harum regularum ope duas ultimas paginas huiusmodi tabularum expedivimus, quae valores ipsius q a termino 33300 usque ad 33400 complectuntur.[1])

1) In editione principe tabula sequens permultos errores continet, qui praeter unum omnes etiam in *Comment. arithm.* inveniuntur, hac autem in editione ope tabulae divisorum satis cognitae, quae inscribitur *Table des diviseurs pour tous les nombres du 1—3 million par J. Ch. Burckhardt*, Paris 1814—17, revisione quidem instituta correcti sunt. (Quae quidem tabula ipsa permultos errores continet, hoc vero tempore correctos in tabula, quae inscribitur *Factor table for the first ten millions containing the smallest factor of every number not divisible by 2, 3, 5, or 7, between the limits 0 and 10017000 by D. N. Lehmer*, Washington 1909.)

Editionis principis errores sunt hi (confer tabulam sequentem):

1) *p.* 2) 127. 3) *p.* 4) *p.* 5) *p.* 6) 499. 7) 599. 8) *p.* 9) 31. 10) *p.* 11) *p.* 12) 47. 13) 233. 14) *p.* 15) 197. 16) *p.* 17) *p.* 18) *p.* 19) 277. 20) *p.* 21) *p.* 22) 127. 23) *p.* 24) *p.* 25) *p.* 26) 101. 27) 79. 28) 127. 29) *p.*

Vide etiam notas sequentes. F. R.

q	1	7	11	13	17	19	23	29
33300	19	p	13	347	859 [1])	7	p	p
01	11	13	71	p	7	p [2])	11	107
02	7	p	83	17	19	29	p	7
03	p	11	p	7	17	127 [3])	79	11
04	191	229	7	p	29	277 [4])	23	p
05	73	821	31	11	13	p	7	199
06	p	7	19	13	97 [5])	p	89	17
07	41	p	p	31	541	7	p	p
08	61	383	11	29	7	37	223	p
09	7	17	23	59	p	331	41	7
10	181	p	17	7	11	641	13	p
11	p	233	7	19	31	13	163	p
12	11	911	p	23	p	17	7	p
13	97	7	13	83	37	31	17	19
14	53	11	p	p	p	7	73	11
15	p	19	503	601	7	151	257	13
16	7	107	p	11	499	p	191	7
17	23	281	p	7	53	p	19	41
18	p	193	7	p	13	11	p [6])	83
19	19	199	11	13	79	73	7	p
20	29	7	p	p	17	157	p	37
21	p	59	149	47	11	7	p	29
22	13	p	p	479	7	163	p	137
23	7	953	107	37	43	223	11	7
24	p	p [7])	599 [8])	7	47	13	653	p
25	71 [9])	11	7	p	173	p	p	11
26	31 [10])	17	13	43	433	19	7	p
27	487	7	17	11	139	167	23	283
28	67	467	37	p	109	7	p	13
29	127 [11])	691	73	p	7	11	71	307
30	7	p [12])	11	19	p	991	17	7
31	p	113	577	7	13	29	p	p [13])
32	p	31	7	13	11	p	p	19
33	17	757	101	p	29	293 [14])	7	47
34	11	7	41	p	p	p	11	353
35	13	53	79	23	83	7	37	281 [15])
36	p	11	31	17	7	p	13	11
37	7	p	p	29	17	13	p	7
38	19	37	p	7	617	p	53	197 [16])
39	p	71	7	p	p	263	p	p
40	23	13	p	p	19	11	7	17
41	p	7	11	67	23	p	p	13
42	271 [17])	191	89	p	31	7	941	p
43	p	17	47	p	7	43	p	71
44	7	701	17	p	13	23	107	7
45	11	p	97	7	p	19	11	127 [18])
46	p	181	7	p	p	17	p	p
47	269	11	907	p	p	p	7	11
48	13	7	563	p	p	173	31	769
49	29	23	43	11	311	7	13	523

q	1	7	11	13	17	19	23	29
33350	17	p	67	307	7	13	23	29
51	7	p	p	463	p	11	337	7
52	157	43	11	7	p	p	47	p
53	37	13	7	17	101	p	331 [19])	p
54	p	89	479	127 [20])	11	p	7	13
55	p	7	23	433	p	p	19	p
56	11	41	p	53	p	7	11	131
57	19	421	p	p	7	109	809	17
58	7	11	673	13	73	373	p	7
59	47	p	467	7	19	179	p	23
60	277 [21])	17	7	11	59	29	409	p
61	13	397	17	227	p	p	7	p
62	p	7	569	241	29	11	13	p
63	23	31	11	73	p	7	67	p
64	p	839	p	41	7	19	17	61
65	7	197	13	571	11	p	p	7
66	p	13	419	7	43	p	p	79
67	11	p	7	p	p	23	11	13
68	p	67	29	19	103	137	7	p
69	61	7	p [22])	31	p	p	p	11
70	971	p	181	17	13	7	p	19
71	149	97	127 [23])	11	7	491	p	p
72	7	19	59	p	p	41	37	7
73	p	p	233	7	31	11	23	p
74	13	337	7	131	p	251	19	17
75	359	37	41	103	p	31	7	p
76	19	7	p	113	11	13	p	163
77	p	17	p	p	p	7	137	89
78	11	p	13	p	7	439	11	p
79	7	13	p	109	p	p	31	7
80	p	11	p	7	229	17	887	11
81	p	61	7	23	p	67	17	p
82	353	p	19	11	193	37	7	23
83	p	7	p	157	13	19	43	113 [24])
84	17	p	p	13	283	7	367	p
85	p	547	11	p	7	p	29	31
86	7	p	823 [25])	p	71	43	953	7
87	13	47 [26])	p	7	11	p	73	p
88	31 [27])	53	7	937	17	p	13	p
89	11	983	61	p	p	13	7	19
90	37	7	47	p	67	23	p	701
91	311	11	13	p	29	7	41	11
92	59	13	43	139	7	73	p	347
93	7	p	p	11	p	p	19	7
94	p	17	p	7	241	p	173 [28])	37
95	19	23	7	29	601	11	89	59
96	71	271	11	83	13	47	7	277 [20])
97	p	7	29	13	19	17	p	223
98	p	p	31	p	11	7	17	359
99	113	p	p	p	7	p	47	41

SCHOLION 1

31. Quamquam ope tabulae nostrae auxiliaris omnes divisores primi haud difficulter in tabulam numerorum primorum inseruntur, tamen, quando iam ad divisores primos maiores fuerit perventum, etiam alio modo eorum insertio in hanc tabulam perfici poterit; id quod imprimis pro divisoribus maximis laborem mirifice diminuit. Sit enim A divisor quicumque primus maior quam 100; qui quia primum inscribitur areolae numero AA respondenti, deinceps tantum pro huiusmodi productis AB locum inveniet, ubi alter factor B, dum ipse maior quam A, nullum habet divisorem ipso numero A minorem. Quare, cum $A > 100$, numerus B non maior erit quam 10000; unde, nisi is fuerit primus, divisorem habebit centenario minorem, qui ergo tabulae inscribi deberet, non autem numerus A; quamobrem iste divisor A tum tantum erit inscribendus, quando factor B fuerit numerus primus. Hinc igitur proposito huiusmodi divisore primo A pro B excerpantur ex nostra tabula [§ 5] omnes numeri primi maiores quam A eousque, donec productum AB superet unum millionem; hisque omnibus productis in tabula nostra inscribi debebit numerus A utpote minimus eorum divisor primus. Quo autem haec operatio facilius ad formam nostram numerorum generalem $30q + r$ revocari possit, ponamus esse

$$A = 30a + \alpha \quad \text{et} \quad B = 30b + \beta,$$

et quia productum erit

$$30^2ab + 30a\beta + 30b\alpha + \alpha\beta,$$

ubi sit $\alpha\beta = 30x + y$, hoc productum in forma $30q + r$ continebitur sumendo

$$q = 30ab + a\beta + b\alpha + x \quad \text{et} \quad r = y;$$

consequenter areolae huic formae respondenti inscribi debebit divisor primus A. Quod quo exemplo illustremus, proponatur numerus $A = 907$ et excerpantur ex nostra tabula prima [§ 5] pro B sequentes numeri primi

B		B		B	
$30^{(b)}$	$11^{(\beta)}$	$33^{(b)}$	$1^{(\beta)}$	$35^{(b)}$	$1^{(\beta)}$
30	19	33	7	35	11
30	29	33	19	35	13
31	7	33	23	35	19
31	11	33	29	36	7
31	17	34	1	36	11
31	23	34	11	36	13
32	7	34	13	36	17
32	11	34	19	36	23
32	17	34	29	36	29
32	23				

Pro singulis igitur productis hinc natis divisor 907 areolis inscribi debet.

SCHOLION 2

32. Ex binis postremis tabulis iam omnes numeri inter limites 999000 et 1002000 examinari possunt, utrum sint primi necne, et casu posteriore simul eorum divisores minimi innotescunt. Patet igitur intra hoc intervallum omnino 217[1]) numeros primos contineri, ex quibus eos, qui unum millionem superant, operae pretium erit hic exhibere, quandoquidem alia via nondum patet tam ingentes numeros primos assignandi.

1) Editio princeps: 228. Vide notam praecedentem. F. R.

Numeri primi uno millione maiores[1])

1000003	1000333	1000669	1001027	1001353	1001683
1000033	1000357	1000679	1001041	1001369	1001687
1000037	1000367	1000691	1001069	1001381	1001713
1000039	1000381	1000697	1001081	1001387	1001723
1000081	1000393	1000721	1001087	1001389	1001743
1000099	1000397	1000723	1001089	1001401	1001783
1000117	1000403	1000763	1001093	1001411	1001797
1000121	1000409	1000777	1001107	1001431	1001801
1000133	1000423	1000793	1001123	1001447	1001807
1000151	1000427	1000829	1001153	1001459	1001809
1000159	1000429	1000847	1001159	1001467	1001821
1000171	1000453	1000849	1001173	1001491	1001831
1000183	1000457	1000859	1001177	1001501	1001839
1000187	1000507	1000861	1001191	1001527	1001911
1000193	1000537	1000889	1001197	1001531	1001933
1000199	1000541	1000907	1001219	1001549	1001941
1000211	1000547	1000919	1001237	1001551	1001947
1000213	1000577	1000921	1001267	1001563	1001953
1000231	1000579	1000931	1001279	1001569	1001977
1000249	1000589	1000969	1001291	1001587	1001981
1000253	1000609	1000973	1001303	1001593	1001983
1000273	1000619	1000981	1001311	1001621	1001989
1000289	1000621	1000999	1001321	1001629	
1000291	1000639	1001003	1001323	1001639	
1000303	1000651	1001017	1001327	1001659	
1000313	1000667	1001023	1001347	1001669	

1) In editione principe haec tabula etiam numeros 1000009, 1000169, 1000261, 1000379, 1000633, 1000801, 1001141, 1001519, 1001591, 1001909 continet. Quos numeros utpote divisoribus 293, 197, 271, 127, 127, 277, 127, 113, 823, 277 praeditos delevi. Vicissim numerus primus 1001081 in editione principe deest (vide notam 22 p. 398).

Numerum 1000009 compositum esse, scilicet $= 293 \cdot 3413$, EULERUS ipse postea demonstravit in Commentatione 699 (indicis ENESTROEMIANI): *Utrum hic numerus 1000009 sit primus necne, inquiritur,* Nova acta acad. sc. Petrop. **10** (1792), 1797, p. 63, *LEONHARDI EULERI Opera omnia*, series I, vol. 4, postquam iam antea nota Actis acad. sc. Petrop. sub titulo *Monitum* (vide infra) inserta atque etiam in Commentatione 498 huius voluminis breviter notaverat in computatione binarum illarum postremarum tabularum divisorem 293 praetermissum esse. F. R.

MONITUM

Acta academiae scientiarum Petropolitanae 1777: I, 1778, p. X

Circa dissertationem Ill. EULERI *De tabula numerorum primorum ad millionem usque et ultra continuanda*, quae extat in Tomo Commentariorum XIX praecedentis collectionis, notandum est numerum 10000009 in tabula annexa numerorum primorum millione maiorum occurrentem non esse primum, sed divisore gaudere 293, quippe qui divisor Schemati praemisso pro valore $q = 33333$ sub residuo 19 loco signi primorum p inserendus tum temporis pro unica[1]) hac areola fuerat praetermissus, uti deinceps facta revisione calculorum pro construenda hac tabula institutorum compertum est; qua de re huiusmodi disquisitionum curiosos hoc loco certiores facere haud abs re fore duximus.

1) Sed vide notam p. 398. F. R.

SOLUTIO QUORUNDAM PROBLEMATUM DIOPHANTEORUM

Commentatio 474 indicis ENESTROEMIANI
Novi commentarii academiae scientiarum Petropolitanae 20 (1775), 1776, p. 48—58
Summarium ibidem p. 12—14

SUMMARIUM

Analysis sublimior quantum methodo DIOPHANTEAE quantaque haec Ill. EULERO incrementa debeat, eos haud latet, qui hoc speculationum genus non adversantur. Tria potissimum in praesenti dissertatione soluta traduntur problemata DIOPHANTEA, quae ita denunciari possunt. Invenire duo quadratorum paria xx, yy et tt, uu, ut fiat

1) $(xx+yy)(ttxx+uuyy)$, $(xx+yy)(uuxx+ttyy)$,

2) $(ttxx+uuyy)(uuxx+ttyy)$,

3) $ttxx+uuyy$ et $uuxx+ttyy$

quadratum. Quod ad prius horum problematum attinet, id ita restringitur, ut tam x et y quam t et u sint numeri primi inter se, quoniam, quicumque bini numeri pro iis fuerint inventi, eorum aeque multipla, veluti αx, αy et βt, βu, quaesito, uti statim patet, aeque satisfaciunt.

Quodsi iam formula prior $(xx+yy)(ttxx+uuyy)$ quadrato

$$(xx+yy)^2xxyy(pp+qq)^2$$

aequetur, inde statim binae litterae t et u sequenti modo expressae prodeunt

$$t=xy(pp-qq)+2pqyy$$

et

$$u=xy(pp-qq)-2pqxx,$$

ex quibus pro altera formula fit

$$ty = xyy(pp-qq) + 2pqy^3$$

et

$$ux = xxy(pp-qq) - 2pqx^3.$$

Cum igitur productum $(xx+yy)(ttyy+uuxx)$ quadratum fieri debeat, omnibus debite in usum vocatis sequens prodit expressio ad quadratum reducenda

$$4ppqqx^4 - 4pq(pp-qq)x^3y + (p^4 - 6ppqq + q^4)xxyy + 4pq(pp-qq)xy^3 + 4ppqqy^4,$$

ubi quidem Ill. Auctor casum se quasi sponte offerentem $x=y$ excludendum iudicavit, quia formula quadratum efficienda hoc casu foret $2(tt+uu)$, quod nulla plane difficultate laboraret. At si formula illa huic quadrato

$$(2pqxx - (pp-qq)xy + 2pqyy)^2$$

aequetur, inde sequens colligitur solutio problematis (ubi scilicet numeri t et u ad minimos terminos sunt reducti)

$$x = 2(pp-qq), \quad y = 3pq,$$
$$t = 3(p^4 + ppqq + q^4), \quad u = (pp-qq)^2.$$

Huic vero solutioni Vir Ill. alias adhuc pariter infinite patentes adiecit, veluti

$$x = p(p+2q), \quad y = q(q+2p),$$
$$t = p(q+2p)(pp+2pq+3qq), \quad u = q(p+2q)(qq+2pq+3pp)$$

et

$$x = p(p-2q), \quad y = q(2p-q),$$
$$t = p(2p-q)(pp-2pq+3qq), \quad u = q(p-2q)(qq-2pq+3pp);$$

quae vero solutio cum a praecedente non discrepet, Ill. Auctor ex duabus prioribus solutiones particulares, quomodo facili negotio deducendae sint, breviter ostendit pluresque simpliciores subiungit.

En ergo specimen methodi, qua Ill. EULERUS usus est, ad solutionem problematum supra denunciatorum perveniendi; eandem enim solutionem sortiuntur problemata sequentia, ita ut non opus sit recensioni huius dissertationis diutius immorari. Tantum enim circa problema secundum observandum erit, quod infinitas solutiones admittere videatur, quae praecedenti non conveniant, quia formula

$$(ttxx + uuyy)(uuxx + ttyy)$$

quadratum fieri potest, etiamsi neutra praecedentium fuerit quadratum, ad cuius rei confirmationem Cel. Auctor hoc adfert exemplum[1])

$$x = 973, \quad y = 263, \quad t = 973, \quad u = 1841.$$

1) Sed vide notam p. 414. F. R.

Solutio autem huius problematis latius patens ita se habet:

$$x = 3n^4 + 6mmnn - m^4, \quad t = mx,$$
$$y = 3m^4 + 6mmnn - n^4, \quad u = ny.$$

PROBLEMA 1

Invenire duo quadratorum paria xx, yy *et* tt, uu, *ita ut tam*

$$(xx + yy)(ttxx + uuyy)$$

quam

$$(xx + yy)(uuxx + ttyy)$$

fiat numerus quadratus.

ANALYSIS

1. Primo patet, quicumque bini numeri tam pro x, y quam pro t, u fuerint inventi, eorum aeque multipla, veluti αx, αy et βt, βu, quaesito aeque satisfacere; sicque problema ita restringi conveniet, ut tam x et y quam t et u sint numeri primi inter se.

2. Incipiamus a formula priori $(xx + yy)(ttxx + uuyy)$, quae posita huic quadrato

$$(xx + yy)^2 xxyy(pp + qq)^2$$

aequalis fit

$$ttxx + uuyy = xxyy(xx + yy)((pp - qq)^2 + (2pq)^2),$$

unde concluditur

$$tx = xy(x(pp - qq) + 2pqy), \quad uy = xy(y(pp - qq) - 2pqx),$$

sicque erit

$$t = xy(pp - qq) + 2pqyy, \quad u = xy(pp - qq) - 2pqxx.$$

3. Iam pro altera formula, cum sit

$$ty = xyy(pp - qq) + 2pqy^3, \quad ux = xxy(pp - qq) - 2pqx^3,$$

fiet

$$ttyy + uuxx = xxy^4(pp - qq)^2 + 4pqxy^5(pp - qq) + 4ppqqy^6$$
$$+ x^4yy(pp - qq)^2 - 4pqx^5y(pp - qq) + 4ppqqx^6,$$

quae forma, quia manifesto per $xx+yy$ est divisibilis, abit in

$$(xx+yy)(xxyy(pp-qq)^2-4pqxy(xx-yy)(pp-qq)+4ppqq(x^4-xxyy+y^4)).$$

4. Cum nunc haec forma per $xx+yy$ multiplicata numerum quadratum praebere debeat, habebimus sequentem expressionem ad quadratum reducendam

$$4ppqqx^4-4pq(pp-qq)x^3y+(p^4-6p^2q^2+q^4)x^2y^2+4pq(pp-qq)xy^3+4ppqqy^4,$$

quae quidem manifesto fit quadratum, si $x=y$; verum hunc casum utpote facillimum hinc merito excludimus, siquidem tota quaestio huc rediret, ut $2(tt+uu)$ quadratum efficeretur.

5. At ponendo illam formulam aequalem huic quadrato[1])

$$(2pqxx-(pp-qq)xy+2pqyy)^2$$

deletis terminis paribus fit

$$p^4-6ppqq+q^4)x^2y^2+4pq(pp-qq)xy^3=(p^4+6ppqq+q^4)x^2y^2-4pq(pp-qq)xy^3$$

hincque

$$8pq(pp-qq)y=12ppqqx,$$

unde colligitur haec solutio problematis

$$x=2(pp-qq), \quad y=3pq,$$

hincque porro

$$t=6pq(p^4+ppqq+q^4) \quad \text{et} \quad u=-2pq(pp-qq)^2.$$

6. En ergo solutionem primam infinite patentem, quoniam numeros p et q ad arbitrium capere licet. Reductis scilicet numeris t et u ad minimos terminos, et quia perinde est, sive sint positivi sive negativi, habebimus

$$x=2(pp-qq), \quad y=3pq,$$

$$t=3(p^4+ppqq+q^4)=\tfrac{3}{4}xx+yy, \quad u=(pp-qq)^2=\tfrac{1}{4}xx$$

1) Vide L. Euler, *Vollständige Anleitung zur Algebra*, St. Petersburg 1770, Zweyter Theil, zweyter Abschnitt, Cap. 9; *Leonhardi Euleri Opera omnia*, series I, vol. 1, p. 396. F. R.

hincque reperitur[1])

$$xx + yy = 4p^4 + ppqq + 4q^4,$$

$$ttxx + uuyy = \tfrac{9}{4}xx(xx + yy)(pp + qq)^2 = xx\,(xx + yy)\left(\tfrac{9}{16}xx + yy\right),$$

$$uuxx + ttyy = (xx + yy)(p^4 + 7ppqq + q^4)^2 = (xx + yy)\left(\tfrac{1}{4}xx + yy\right)^2.$$

7. Ut alias solutiones inveniamus, ponamus superioris formae [§ 4] radicem quadratam

$$2pqxx - (pp - qq)xy - 2pqyy + Ayy;$$

cuius quadrato illi aequali posito prodibit aequatio

$$(AA - 4Apq)yy - 2A(pp - qq)xy + (4Apq - 4ppqq)xx = 0.$$

Hic si $A = 4pq$, prodit solutio praecedens; at posito $A = pq$ fit

$$3pqy + 2(pp - qq)x = 0,$$

quae cum illa pariter congruit.

8. Ponamus $A = -2pp$ prodibitque haec aequatio

$$(pp + 2pq)yy + (pp - qq)xy - (2pq + qq)xx = 0,$$

quae per $x + y$ divisa dat

$$(pp + 2pq)y - (2pq + qq)x = 0,$$

unde fit

$$x = p(p + 2q) \quad \text{et} \quad y = q(q + 2p),$$

tum vero

$$t = ppq(q + 2p)(pp + 2pq + 3qq) \quad \text{et} \quad u = pqq(p + 2q)(qq + 2pq + 3pp).$$

1) Editio princeps (atque etiam *Comment. arithm.*): ... *hincque reperitur*

$$xx + yy = 4p^4 + ppqq + 4q^4$$

$$ttxx + uuyy = xxyy(xx + yy)(pp + qq)^2 = xx(xx + yy)\left(\tfrac{9}{16}xx + yy\right)$$

$$uuxx + ttyy = 4ppqq(xx + yy)(p^4 + 7ppqq + q^4)^2 = (xx + yy)\left(\tfrac{1}{4}xx + yy\right)^2.$$

Correxit F. R.

9. En ergo aliam solutionem a praecedente diversam et infinite patentem, qua numeris t et u ad minimos terminos reductis fit

$$x = p(p + 2q), \quad y = q(q + 2p),$$
$$t = p(q + 2p)(pp + 2pq + 3qq), \quad u = q(p + 2q)(qq + 2pq + 3pp),$$

hincque reperitur

$$xx + yy = p^4 + 4p^3q + 8ppqq + 4pq^3 + q^4,$$
$$ttxx + uuyy = (p + 2q)^2(q + 2p)^2(pp + qq)^2(xx + yy),$$
$$uuxx + ttyy = ppqq(5pp + 8pq + 5qq)^2(xx + yy).$$

10. Posito $A = 2pp$ prodit

$$(pp - 2pq)yy - (pp - qq)xy + (2pq - qq)xx = 0,$$

quae per $y - x$ divisa dat

$$(pp - 2pq)y - (2pq - qq)x = 0$$

ideoque

$$x = p(p - 2q), \quad y = q(2p - q),$$
$$t = p(2p - q)(pp - 2pq + 3qq), \quad u = q(p - 2q)(qq - 2pq + 3pp),$$
$$xx + yy = p^4 - 4p^3q + 8ppqq - 4pq^3 + q^4,$$
$$ttxx + uuyy = (p - 2q)^2(2p - q)^2(pp + qq)^2(xx + yy),$$
$$uuxx + ttyy = ppqq(5pp - 8pq + 5qq)^2(xx + yy).$$

Haec autem solutio a praecedente non differt; neque positiones $A = 2qq$ et $A = -2qq$ solutiones diversas praebent.

11. Constant methodi, quarum beneficio ex una solutione inventa aliae erui possunt; verum eae ad calculos nimium intricatos deducunt. Ita reperire licet

$$x = q(pp - qq)(3pp - qq),$$
$$y = (pp + qq)(p(pp + qq) \pm q(3pp + qq));$$

convenientes vero valores pro t et u paragraphus 2 suppeditat.

SOLUTIO 1

12.[1]) In hac solutione ratio numerorum x et y est

$$\frac{x}{y} = \frac{4}{3} \cdot \frac{pp-qq}{2pq},$$

unde [ipsi] ex cathetis trianguli rectanguli inveniuntur; tum vero ratio

$$\frac{t}{u} = \frac{3xx+4yy}{xx},$$

unde solutiones simpliciores sunt:

1. $x = 5, \quad y = 2, \quad t = 91, \quad u = 25;$
2. $x = 7, \quad y = 5, \quad t = 247, \quad u = 49;$
3. $x = 5, \quad y = 9, \quad t = 399, \quad u = 25;$
4. $x = 3, \quad y = 10, \quad t = 427, \quad u = 9;$
5. $x = 11, \quad y = 14, \quad t = 1147, \quad u = 121;$
6. $x = 15, \quad y = 7, \quad t = 871, \quad u = 225;$
7. $x = 16, \quad y = 5, \quad t = 217, \quad u = 64;$
8. $x = 16, \quad y = 9, \quad t = 273, \quad u = 64;$
9. $x = 7, \quad y = 18, \quad t = 1443, \quad u = 49;$
10. $x = 13, \quad y = 20, \quad t = 2107, \quad u = 169.$

SOLUTIO 2

13. Hic ratio numerorum x et y est

$$\frac{x}{y} = \frac{p(p+2q)}{q(q+2p)},$$

numerorum t et u vero

$$\frac{t}{u} = \frac{p(q+2p)(pp+2pq+3qq)}{q(p+2q)(qq+2pq+3pp)}.$$

1) Abhinc paragraphorum numeri in editione principe (atque etiam in *Comment. arithm.*) desunt. F. R.

Si numeros x et y ut datos spectemus, ob

$$ppy + 2pqy = qqx + 2pqx$$

reperitur

$$\frac{p}{q} = \frac{x-y+\sqrt{(xx-xy+yy)}}{y},$$

unde numerorum x et y character in hoc consistit, ut $xx - xy + yy$ sit quadratum; cuiusmodi numeri cum facile inveniantur, sit

$$xx - xy + yy = zz$$

eritque

$$\frac{p}{q} = \frac{x-y+z}{y} = \frac{x}{y-x+z} \quad \text{seu} \quad \frac{p}{q} = \frac{z-y}{x-z};$$

hinc fit

$$\frac{p+2q}{q+2p} = \frac{2x-y-z}{z-2y+x} = \frac{z+y}{z+x} \quad \text{et} \quad \frac{p(q+2p)}{q(p+2q)} = \frac{(z-y)(z+x-2y)}{(z-x)(z+y-2x)},$$

at

$$(z-y)(z+x-2y) = (z+x-y)(2z-x-y),$$

$$(z-x)(z+y-2x) = (z+y-x)(2z-x-y),$$

unde

$$\frac{p(q+2p)}{q(p+2q)} = \frac{z+x-y}{z+y-x}.$$

Deinde est

$$\frac{pp+2pq+3qq}{qq+2pq+3pp} = \frac{(x-y)^2+2(x-z)^2}{(x-y)^2+2(z-y)^2} = \frac{2z+y-x}{2z+x-y}$$

hincque tandem elicitur

$$\frac{t}{u} = \frac{(z+x-y)(2z-x+y)}{(z+y-x)(2z-y+x)}.$$

Sicque pro x et y eiusmodi numeris inventis, ut sit rationaliter

$$\sqrt{(xx-xy+yy)} = z,$$

capiatur

$$t = (z+x-y)(2z-x+y) = xx+yy+(x-y)z,$$

$$u = (z+y-x)(2z-y+x) = xx+yy-(x-y)z;$$

hinc obtinetur

$$ttxx + uuyy = (xx+yy)(xx-2xy+yy+(x+y)z)^2,$$

$$uuxx + ttyy = (xx+yy)(xx-2xy+yy-(x+y)z)^2$$

vel etiam hoc modo

$$ttxx + uuyy = \tfrac{1}{9}(xx + yy)(x + y + z)^2(4z - x - y)^2,$$

$$uuxx + ttyy = \tfrac{1}{9}(xx + yy)(x + y - z)^2(4z + x + y)^2.$$

Nunc autem quo facilius valores pro x et y idoneos reperiamus, spectemus x ut datum ac ponamus $z = y - v$ eritque

$$xx - xy = -2yv + vv \quad \text{et} \quad y = \frac{xx - vv}{-2v + x} = \frac{vv - xx}{2v - x},$$

ubi pro quovis valore ipsius x assumto casus integri pro y sunt eruendi; notandum vero est pro x numerum impariter parem assumi non posse, quia y quoque fieret par.

x	y	z	t	u
3	− 5	7	45	11
3	+ 8	7	19	54
5	+ 8	7	34	55
5	− 16	19	340	59
5	+ 21	19	81	385
7	− 8	13	154	41
7	+ 15	13	85	189
7	− 33	37	1309	171
7	+ 40	37	214	1435
8	+ 15	13	99	190
9	− 56	61	3591	374
9	+ 65	61	445	3861
11	− 24	31	891	194
11	+ 35	31	301	1045
11	− 85	91	8041	695
11	+ 96	91	801	8536
13	− 35	43	1729	335
13	+ 48	43	484	1989
13	− 120	127	15730	1161
13	+ 133	127	1309	16549

PROBLEMA 2

14. *Invenire duo quadratorum paria* xx, yy *et* tt, uu, *ut*

$$(ttxx + uuyy)(uuxx + ttyy)$$

sit numerus quadratus.

SOLUTIO

Hoc problema eandem sortitur solutionem, quam praecedens, iidemque quaterni numeri pro x, y, t, u inventi satisfaciunt. Inde ergo solutio simplicissima est

$$x = 3, \quad y = 5, \quad t = 11, \quad u = 45,$$

ex qua fit

$$ttxx + uuyy = 34 \cdot 9 \cdot 169, \quad uuxx + ttyy = 34 \cdot 625$$

ideoque

$$(ttxx + uuyy)(uuxx + ttyy) = 34^2 \cdot 39^2 \cdot 25^2.$$

Ceterum haec solutio non solum ob eam causam tantum est particularis, ob quam talis erat, sed etiam hoc problema infinitas solutiones admittere videtur, quae praecedenti non conveniant. Fieri enim potest, ut haec formula

$$(ttxx + uuyy)(uuxx + ttyy)$$

sit quadratum, etiamsi neutra praecedentium

$$(xx + yy)(ttxx + uuyy) \quad \text{et} \quad (xx + yy)(uuxx + ttyy)$$

fuerit quadratum, cuius rei unicum exemplum dedisse sufficiat:

$$x = 973, \quad y = 263, \quad t = 973, \quad u = 1841;$$

est enim

$uuxx + ttyy = 2 \cdot 25 \cdot 263^2 \cdot 973^2$ quadratum duplicatum,

$ttxx + uuyy = 2 \cdot 25 \cdot 141793^2$ quadratum duplicatum.[1])

1) Hoc exemplum non valet. Est enim revera $ttxx + uuyy = 2 \cdot 7^2 \cdot 11538050785$ neque ergo quadratum duplicatum. F. R.

En adhuc aliam solutionem latius patentem

$$x = 3n^4 + 6mmnn - m^4, \quad t = mx,$$
$$y = 3m^4 + 6mmnn - n^4, \quad u = ny,$$

cuius inventionis ratio facile intelligitur. Posito enim $t = mx$ et $u = ny$ fit

$$ttxx + uuyy = mmx^4 + nny^4 \quad \text{et} \quad uuxx + ttyy = xxyy(mm + nn)$$

sicque ad quadratum reducenda est haec formula

$$(mm + nn)(mmx^4 + nny^4),$$

quae facto $x = v + z$ et $y = v - z$ ad istam solutionem perducit; hinc autem praecedentes solutiones non obtinentur.

PROBLEMA 3

15. *Invenire duo quadratorum paria* xx, yy *et* tt, uu, *ut tam hic numerus*

$$ttxx + uuyy$$

quam iste

$$ttyy + uuxx$$

fiat quadratus.

SOLUTIO

Ex modo tradita solutione problematis praecedentis solutio huius facile adornatur pro m et n eiusmodi numeris sumendis, ut $mm + nn$ fiat quadratum. Sic si fiat $m = 4$ et $n = 3$, reperitur

$$x = 851, \quad t = 3404,$$
$$y = 1551, \quad u = 4653.$$

At ex problemate primo multo concinniores solutiones impetrantur, quibus adeo praeter binas praescriptas conditiones et haec tertia adimpletur, ut $xx + yy$ fiat etiam quadratum. At solutio secunda primi problematis unum praebet casum, quo $xx + yy$ fit quadratum, scilicet

$$x = 8, \quad y = 15, \quad t = 99, \quad u = 190,$$

unde fit

$$xx + yy = 17^2,$$
$$ttxx + uuyy = 2^2 \cdot 3^2 \cdot 17^2 \cdot 29^2,$$
$$ttyy + uuxx = 5^2 \cdot 5^2 \cdot 5^2 \cdot 17^2.$$

Si insuper addita fuisset haec conditio, ut etiam $xx - xy + yy$ foret quadratum, eadem solutio negotium conficeret. Huiusmodi autem solutiones elicientur quaerendis numeris x et y, ut haec expressio

$$x^4 - x^3y + 2xxyy - xy^3 + y^4$$

fiat quadratum, ad quos porro ut ante numeros t et u investigare oportet.

Occasionem hoc problema DIOPHANTEUM tractandi praebuit problema geometricum a SCHOTENIO[1]) propositum, quo datis in triangulo basi, perpendiculo et ratione laterum ipsa latera quaeruntur. Problema hoc geminam admittit solutionem; quarum utraque ut praebeat latera rationaliter expressa, negotium ad problema istud DIOPHANTEUM perducitur. Si enim basis trianguli ponatur $= a$, perpendiculum $= b$ et laterum ratio $m : n$ vocatis ipsis lateribus mz et nz, primo necesse est a et b ita exprimi

$$a = (mm - nn)(xx + yy) \quad \text{et} \quad b = 2mnxy;$$

tum vero pro z haec duplex expressio reperitur

$$z = \sqrt{(xx + yy)((m - n)^2xx + (m + n)^2yy)}$$

et

$$z = \sqrt{(xx + yy)((m + n)^2xx + (m - n)^2yy)};$$

quae ut ambae fiant rationales facto $m + n = t$, $m - n = u$, nascitur nostrum problema DIOPHANTEUM. Cuius ergo casus simplicissimus erit sumto

$$x = 3, \quad y = 5, \quad t = 45 \quad \text{et} \quad u = 11,$$

unde haec nascuntur data

ratio laterum $m : n = 28 : 17$,
basis trianguli $a = 33$
et perpendiculum $b = 28$,

1) Fr. v. SCHOOTEN (1615—1660), *Exercitationum mathematicarum libri quinque*, Lugduni Batavorum 1657, p. 68. F. R.

unde reperiuntur ipsa latera

$$\text{vel } mz = \frac{140}{3} \text{ et } nz = \frac{85}{3}$$

$$\text{vel } mz = \frac{364}{5} \text{ et } nz = \frac{221}{5},$$

sive in integris sumta basi $a = 495$ et perpendiculo $b = 420$ obtinebuntur latera rationem $28 : 17$ tenentia

$$\text{vel } mz = 700 \text{ et } nz = 425$$

$$\text{vel } mz = 1092 \text{ et } nz = 663.$$

EXTRAIT D'UNE LETTRE DE M. EULER A M. BEGUELIN

EN MAI 1778[1])

Commentatio 498 indicis Enestroemiani
Nouveaux mémoires de l'académie des sciences de Berlin 1776, 1779, p. 337—339

J'ai entendu[2]) avec plaisir la lecture du mémoire de M. Beguelin[3]) sur les nombres premiers, inséré dans le dernier volume des Mémoires de l'Académie Royale de Berlin*); et comme j'ai travaillé, depuis quelque tems, sur le même sujet, je crois qu'il recevra, avec autant de satisfaction, quelques observations que j'ai eu occasion de faire relativement au problème qu'il a traité dans le mémoire mentionné.

Ses recherches sont fondées sur cette belle propriété, que tous les nombres qui ne sont contenus qu'une seule fois dans la formule $xx + yy$, sont ou premiers, ou doubles de premiers, en prenant les nombres x et y premiers entr'eux.[4]) Or j'ai remarqué que plusieurs autres formules semblables de la forme $nxx + yy$ sont douées de la même propriété, et que, pourvu qu'on donne à la lettre n des valeurs *convenables*, telles que, par

*) Pour l'année 1775.

1) Voir les mémoires 283, 369, 461, 467, 708a de ce volume. F. R.

2) On se souviendra qu' Euler était aveugle depuis 1766. F. R.

3) N. de Beguelin (1714—1789), *Solution particulière du problème sur les nombres premiers,* Nouv. mém. de l'acad. d. sc. de Berlin 1775, 1777, p. 300—322. F. R.

4) Voir outre les mémoires déjà cités surtout le mémoire 228: *De numeris, qui sunt aggregata duorum quadratorum,* Novi comment. acad. sc. Petrop. 4 (1752/3), 1758, p. 3, en particulier § 35; *Leonhardi Euleri Opera omnia*, series I, vol. 2, p. 295. F. R.

exemple

2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13 etc.

on en tire toujours des nombres premiers; ou bien, qu'à l'exclusion des valeurs suivantes de n, savoir

11, 14, 17, 19, 20, 23, 26, 27 etc.,

la formule $nxx + yy$ donne toujours des nombres premiers; car le nombre 15, par exemple, quoique contenu d'une seule façon dans la formule $11xx + yy$, est un nombre composé. Il en est ainsi des autres nombres que je viens d'exclure; au lieu que ceux que j'ai nommés valeurs convenables, donnent sûrement pour premier tout nombre qui est contenu d'une seule façon dans la forme $nxx + yy$. Il est donc de la dernière importance de bien distinguer les valeurs convenables de la lettre n de celles qu'il faut exclure dans ces recherches.

Pour cet effet, j'ai trouvé et démontré cette règle: que si tous les nombres contenus dans la forme $n + yy$ et moindres que $4n$ (en prenant pour y des nombres premiers à n) sont ou premiers p, ou doubles de premiers $2p$, ou quarrés de premiers pp, ou enfin quelque puissance de 2, alors la valeur de n, qui satisfait à ces conditions, pourra être admise comme convenable à l'examen de tel nombre qu'on se propose. Ainsi, par exemple, j'ai trouvé que le nombre 60 est dans la série des valeurs convenables; car il y a

$$60 + 1^2 = 61 = p,\quad 60 + 7^2 = 109 = p,\quad 60 + 11^2 = 181 = p,\quad 60 + 13^2 = 229 = p,$$

où il faut s'arrêter, les suivans surpassant la limite $4 \cdot 60$. Il en est de même du nombre 15, puisque

$$15 + 1^2 = 16 = 2^4,\quad [15 + 2^2 = 19 = p,]\quad 15 + 4^2 = 31 = p.$$

Moyennant cette règle, j'ai été en état de trouver avec assez de facilité toutes les valeurs qu'on peut donner à la lettre n, pour que tout nombre contenu d'une seule façon dans la forme $nxx + yy$ puisse être censé premier. Voici ces valeurs:

1,	6,	12,	21,	30,	44,	70,	93,	130,	190,	273,	357,	760,
2,	7,	13,	22,	33,	48,	72,	102,	133,	210,	280,	385,	840,
3,	8,	15,	24,	37,	57,	78,	105,	165,	232,	312,	408,	1320,
4,	9,	16,	25,	40,	58,	85,	112,	168,	240,	330,	462,	1365,
5,	10,	18,	28,	42,	60,	88,	120,	177,	253,	345,	520,	1848.

Ces nombres, qui, loin d'être semés au hazard, ont une loi de progression, qui est assez évidente lorsqu'on parcourt toutes les exclusions successives par lesquelles il faut passer pour trouver les valeurs convenables, semblent devoir aller à l'infini; j'ai donc été bien surpris de me voir arrêté au dernier 1848, au delà duquel je n'ai plus trouvé que des valeurs incongrues.[1]) Cependant, moyennant la dernière valeur 1848, on est en état de découvrir des nombres premiers extrêmement grands, vu que rien n'est plus facile que d'examiner, si quelque nombre proposé est contenu une seule fois dans la forme $1848xx+yy$, ou non, et dans le premier cas on pourra prononcer hardiment, que ce nombre est premier. Par le moyen de cette forme j'ai trouvé premiers, entr'autres, les nombres suivans:

1016401, 1103257, 1288057, 1487641, 1702009, 2995609, 4658809, 9094009, 11866009, 18518809.[2])

Dans l'autre cas, où le nombre proposé est contenu de plus d'une façon dans la forme $1848xx + yy$, il seroit superflu de remarquer qu'on pourra assigner très facilement les diviseurs de ce nombre.

Mais je juge à propos d'ajouter, que dans la table des nombres premiers insérée dans le volume XIX des Commentaires de notre Académie, il s'est glissé une erreur provenue de ce qu'on a négligé le diviseur 293, qui au reste n'influe que sur le nombre 1000009, qui doit être effacé de cette liste, étant $= 293 \cdot 3413$.[3])

---

1) Euler avait poussé l'examen au delà de 10000; voir le mémoire 725 cité p. 421, note 3. A. Cunningham et J. Cullen ont continué ces recherches jusqu'à 101220 sans avoir trouvé des valeurs convenables plus grandes que 1848. Voir A. Cunningham and J. Cullen, *On idoneal numbers*, Report of the British Association for the advancement of science, 1901, p. 552. F. R.

2) Pour la démonstration voir le mémoire 719 cité p. 421, note 3. F. R.

3) Voir la note p. 403. F. R.

EXTRAIT D'UNE LETTRE DE M. FUSS A M. BEGUELIN

ECRITE DE PETERSBOURG LE $\frac{19}{30}$ JUIN 1778[1])

Commentatio 708a indicis Enestroemiani
Nouveaux mémoires de l'académie des sciences de Berlin 1776, 1779, p. 340—346

Mr. Euler a été flatté de l'attention dont vous et Mr. de la Grange avez honoré les observations que j'ai eu l'honneur de vous envoyer, il y a quelque tems, de sa part, par rapport au sujet de votre Mémoire, inséré dans le dernier volume de l'Histoire de l'Académie Royale des Sciences et Belles-Lettres[2]); et comme il a appris que vous désirez savoir plus en détail l'essentiel de la méthode qu'il propose pour examiner des grands nombres, s'ils sont premiers ou non, il m'a chargé de vous en faire le petit Extrait que vous recevrez ci-joint, considérant que la publication des Mémoires[3]) qu'il a composés depuis peu de tems sur ce sujet, pourroit bien être différée trop longtems.

---

1) Voir les mémoires 283, 369, 461, 467, 498 de ce volume et en particulier le mémoire 708: *De formulis speciei mxx + nyy ad numeros primos explorandos ideoneis earumque mirabilibus proprietatibus*, Nova acta acad. sc. Petrop. **12** (1794), 1801, p. 22; *Leonhardi Euleri Opera omnia*, series I, vol. 4. F. R.

2) Voir p. 418, note 3. F. R.

3) Voir outre le mémoire 708 déjà cité surtout les mémoires 715, 718, 719, 725: *De variis modis numeros praegrandes examinandi, utrum sint primi necne*, Nova acta acad. sc. Petrop. **13** (1795/6), 1802, p. 14, *Facillima methodus plurimos numeros primos praemagnos inveniendi* Nova acta acad. sc. Petrop. **14** (1797/8), 1805, p. 3, *Methodus generalior numeros quosvis satis grandes perscrutandi, utrum sint primi necne*, ibidem p. 11, *Illustratio paradoxi circa progressionem numerorum idoneorum sive congruorum*, Nova acta acad. sc. Petrop. **15** (1799/1802), 1806, p. 29; *Leonhardi Euleri Opera omnia*, series I, vol. 4. F. R.

La nouvelle méthode de Mr. EULER, pour examiner des grands nombres, s'ils sont premiers ou non, est fondée sur les principes suivans:

1. Tout nombre N, contenu de double façon dans la forme $\alpha xx + \beta yy$, ou bien, ce qui revient au même, dans la forme $\alpha\beta xx + yy$, est composé.[1])

Car, s'il y a

$$N = \alpha aa + \beta bb,$$

aussi bien que

$$N = \alpha AA + \beta BB,$$

il y aura

$$N(BB - bb) = N(B + b)(B - b) = \alpha(aB + Ab)(aB - Ab);$$

par conséquent le nombre proposé N aura dans ce cas-ci toujours un facteur commun tant avec $aB + Ab$ qu' avec $aB - Ab$, parce que ces formules sont tout différentes des formules $B + b$ et $B - b$; et il sera même aisé d'assigner ce facteur, car:

2. Pour cet effet on n'a qu'à construire des deux formules $\alpha aa + \beta bb$ et $\alpha AA + \beta BB$ la fraction

$$\frac{p}{q} = \frac{a \pm A}{b \pm B},$$

et la formule $\alpha pp + \beta qq$ contiendra toujours les facteurs du nombre proposé N, division faite par α, ou β, ou $\alpha\beta$, ou enfin par 2 ou une de ses puissances.

Car, parce que $\alpha aa + \beta bb = \alpha AA + \beta BB$, nous aurons

$$\alpha(a^2 - A^2) = \beta(B^2 - b^2)$$

ou bien

$$\frac{a + A}{B + b} = \frac{\beta(B - b)}{\alpha(a - A)}.$$

Soit donc $\frac{p}{q}$ la fraction la plus simple équivalente à ces deux formules, ou bien soit

$$a + A = mp, \quad B + b = mq, \quad B - b = \alpha np, \quad a - A = \beta nq,$$

1) Voir aussi le mémoire 228 cité p. 418, note 4, en particulier § 40. F. R.

et il y aura

$$a = \frac{mp + \beta nq}{2} \quad \text{et} \quad b = \frac{mq - \alpha np}{2},$$

ce qui donnera

$$N = \alpha aa + \beta bb = \frac{\alpha}{4}(mmpp + \beta\beta nnqq) + \frac{\beta}{4}(mmqq + \alpha\alpha nnpp)$$

$$= \frac{1}{4}(mm + \alpha\beta nn)(\alpha pp + \beta qq),$$

d'où il s'ensuit que $\alpha pp + \beta qq$ sera un diviseur du nombre proposé N, le quotient étant de la forme $mm + \alpha\beta nn$.

3. Il y a des formules de cette forme, par exemple $xx + yy$, $2xx + yy$, $3xx + yy$, $3xx + 2yy$, $5xx + yy$, $5xx + 2yy$ etc. dont il est démontré que tout nombre qui n'y est contenu que d'une seule façon, est premier, excepté quelques cas qui sont évidens par eux-mêmes; mais il y a aussi d'autres formules semblables qui n'ont pas cette propriété: telle est $7xx + 2yy$, dans laquelle le nombre 15 n'est contenu que d'une seule manière, quoiqu'il soit composé. Il est donc de la dernière importance de bien distinguer ces deux classes de formules, pour être en état de rejeter toutes celles qui contiennent d'une seule façon des nombres composés. Pour cet effet on établit les vérités suivantes:

4. Que si un nombre composé mp (où $m > 2$) est contenu d'une seule manière dans la forme $\alpha xx + \beta yy$, il est aisé d'assigner un grand nombre d'autres composés qui y sont contenus de même d'une seule façon (où il faut remarquer que α et β, de même que x et y, sont premiers entr'eux, aussi bien que x à β et y à α, et enfin m et p à α, β, x et y).

Car, si $mp = \alpha aa + \beta bb$, il sera aisé de trouver un autre produit mq contenu d'une seule façon dans la forme $\alpha xx + \beta yy$ (ou bien dans $\alpha\beta xx + yy$ qui est la même que la forme précédente et s'y réduit en mettant $y = \beta z$, ce qui donne $\beta(\alpha xx + \beta zz)$; d'où l'on voit l'affinité de ces deux formes, qui dans tout cet examen peuvent être traitées de la même manière). Soit donc $mq = \alpha\beta dd + cc$ et il y aura

$$\beta ddmp - aamq = (\beta bd + ac)(\beta bd - ac).$$

En prenant donc pour c et d des valeurs telles que l'un ou l'autre des deux facteurs $\beta bd + ac$ ou $\beta bd - ac$ devient divisible par m, il en résultera pour q une valeur telle que le produit mq sera contenu d'une seule façon dans la forme $\alpha xx + \beta yy$. Ainsi si $\beta bd + ac = \delta m$, il y aura

$$\beta ddp - aaq = \delta(\beta bd - ac)$$

et partant

$$q = \frac{\beta ddp - \delta(\beta bd - ac)}{aa},$$

où il suffit de donner à q la moindre valeur possible, pour être certain que le produit mq sera contenu d'une seule façon dans la forme proposée. Si, par exemple, $a = 1$ et $d = 1$ et partant $mp = \alpha + \beta bb$ et qu'on prenne q en sorte que $mq < 4\alpha\beta$, il est évident que mq ne peut être contenu que d'une seule manière dans la forme $\alpha xx + \beta yy$, parce que le cas $x = 2$ donneroit déjà une plus grande valeur.

De là on pourra aisément tirer d'autres produits qui sont aussi contenus d'une seule façon dans la forme proposée. Ainsi, en multipliant les deux produits mp et mq on obtient

$$mmpq = \alpha(aacc + \beta\beta bbdd) + \beta(bbcc + \alpha\alpha add)$$

et partant

$$pq = \alpha\left(\frac{ac \pm \beta bd}{m}\right)^2 + \beta\left(\frac{bc \mp \alpha ad}{m}\right)^2,$$

où l'ambiguïté des signes paroît conduire à une double résolution; mais on se convaincra facilement qu'il n'y a jamais plus d'une résolution en nombres entiers, excepté les cas $m = 1$ et $m = 2$ que nous avons d'abord exclus par la condition $m > 2$. Observons encore que de ce produit pq on pourra de la même manière déduire d'autres produits plus grands qui seront toujours contenus d'une seule façon dans la forme $\alpha xx + \beta yy$.

5. De même si un produit, quelque grand qu'il soit, pq, est contenu d'une seule manière dans la forme $\alpha xx + \beta yy$, il est facile d'assigner des produits moindres qui y sont contenus pareillement une seule fois.

Car parce que le produit pq est d'une seule façon de la forme $\alpha xx + \beta yy$, soit $pq = \alpha ff + \beta gg$, et il est sûr, que ni p ni q n'y peuvent être contenus,

parce qu' autrement le produit devroit admettre une double résolution (par exemple, si $p = \alpha pp + \beta qq$ et $q = \alpha rr + \beta ss$, il y auroit

$$pq = \alpha\beta(ps \pm qr)^2 + (\alpha pr \mp \beta qs)^2,$$

où chaque signe donne une résolution). Considérant donc le mineur facteur q, qui peut être de plusieurs manières un facteur de $\alpha xx + \beta yy$, en prenant $x = nf \pm \mu q$ et $y = ng \pm \nu q$, la forme se convertira en celle-ci

$$\alpha(nnff \pm 2\mu nfq + \mu\mu qq) + \beta(nngg \pm 2\nu ngq + \nu\nu qq),$$

qui à cause de $\alpha ff + \beta gg = pq$ se réduit à

$$q\big(nnp \pm \alpha(2\mu nf \pm \mu\mu q) \pm \beta(2\nu ng \pm \nu\nu q)\big) = qr,$$

où il est aisé de prendre les lettres μ, ν et n, en sorte que le facteur

$$nnp \pm \alpha(2\mu nf \pm \mu\mu q) \pm \beta(2\nu ng \pm \nu\nu q) = r$$

devienne moindre que q et partant le produit qr moindre que pq, et de là on pourra parvenir à un autre rs où $s < r$ et ainsi de suite, jusqu'à ce qu'on parvienne à des nombres composés moindres que le terme $4\alpha\beta$.

6. Le même raisonnement vaut aussi pour l'autre forme $\alpha\beta xx + yy$, de laquelle on peut dire pareillement, que dès qu'on a trouvé un produit ou nombre composé qui y est contenu d'une seule façon, on en peut tirer d'autres produits moindres qui y sont contenus de même, jusqu' à ce qu'on ait obtenu des nombres composés moindres que $4\alpha\beta$. Car si dans les grands nombres un nombre composé de la forme $\alpha\beta xx + yy$ est contenu d'une seule façon dans cette forme et qu'on en puisse déduire des moindres jusqu' aux plus petits, qui n'y sont contenus que d'une seule manière, quoiqu'ils soient composés, il sera permis d'en conclure que si, en deçà de cette limite, on ne rencontre point de ces produits, il n'y en aura pas non plus dans les plus grands,[1]) et tous les nombres composés de la forme $\alpha\beta xx + yy$ seront sûrement contenus de plus d'une façon dans la forme proposée, et tout nombre qui n'y est contenu que d'une façon sera premier.

1) Concernant cette méthode de conclure, appelée par FERMAT *la descente infinie* ou *indéfinie*, voir la préface du volume précédent, p. XV. F. R.

7. Pour distinguer donc des formules qui contiennent d'une seule façon des nombres composés, celles qui contiennent véritablement des nombres premiers, et pour être en état d'assigner les valeurs de $\alpha\beta$ qui donnent cette propriété à la forme $\alpha\beta xx + yy$, on n'a qu'à examiner, s'il y a des nombres composés de la forme $\alpha\beta xx + yy$ et moindres que $4\alpha\beta$ qui soient contenus dans cette forme, ou non. Dans le premier cas, la formule proposée doit être rangée dans la classe des incongrues; dans le second, elle peut être employée avec sûreté dans l'examen de tout nombre qui y est contenu d'une seule façon. Or, pour faciliter cet examen, on met $x = 1$, parce qu'on ne va pas au delà du terme marqué $4\alpha\beta$, et dans la forme $\alpha\beta + yy$ on donne à y successivement toutes les valeurs premières à $\alpha\beta$, et si parmi tous les nombres qui en résultent jusqu' au terme mentionné il ne se rencontre aucun composé, la valeur de $\alpha\beta$ sera telle que tout nombre contenu une seule fois dans la forme $\alpha\beta xx + yy$ ou $\alpha xx + \beta yy$ sera premier. Où il est à remarquer que parmi les nombres de la forme $\alpha\beta + yy$ on regarde comme premiers:

a) Tout nombre quarré; parce que, si $\alpha\beta + yy = kk$, ce quarré est contenu encore d'une autre façon dans la forme $\alpha\beta xx + yy$, savoir si $x = 0$ et $y = k$; ou bien parce que si $\alpha\beta + yy = kk$, il y aura

$$\alpha\beta ff + ffyy = ffkk.$$

Qu' on en soustraie $2\nu fky - \nu\nu kk$ pour avoir

$$\alpha\beta ff + (fy - \nu k)^2 = ffkk - 2\nu fky + \nu\nu kk,$$

ou bien, à cause de $\nu\nu kk = \nu\nu(\alpha\beta + yy)$ il y aura

$$\alpha\beta ff + (fy - \nu k)^2 = \alpha\beta\nu\nu + (fk - \nu y)^2.$$

b) Tous les premiers doubles, ou nombres pairs, parce que nous avons vu ci-dessus que pour qu'il n'y ait pas deux résolutions pour les produits pq, il faut exclure des valeurs de la lettre m tant l'unité que le binaire.

c) Toutes les puissances de 2 en certains cas, puisqu'elles sont aussi contenues d'une seule façon dans certaines formules; par exemple, dans celle-ci: $5xx + 3yy$, qui néanmoins appartient à la classe des formes convenables, vu que tous les nombres impairs premiers à 15 et contenus d'une seule façon dans cette forme sont véritablement premiers.

Suivant cette règle fondée sur les principes précédens on peut examiner tous les nombres $\alpha\beta$ qui rendent la formule $\alpha\beta xx + yy$ ou $\alpha xx + \beta yy$ propre à l'examen des nombres premiers; par exemple, pour la formule $7xx + 2y$ il y a

$14 + 1^2$,	$+ 3^2$,	$+ 5^2$
15,	23,	39
c,	p,	c

qui par conséquent doit être rejetée, aussi bien que $14xx + yy$.

Pour la formule $43xx + yy$ il y a

$43 + 1^2$,	$+ 2^2$,	$+ 3^2$,	$+ 4^2$,	$+ 5^2$,	$+ 6^2$,	$+ 7^2$,	$+ 8^2$,	$+ 9^2$,	$+ 10^2$,	$+ 11^2$
44,	47,	52,	59,	68,	79,	92,	107,	124,	143,	164
c,	p,	c,	p,	c,	p,	c,	p,	c,	c,	c

par conséquent la forme $43xx + yy$ doit être exclue.

Pour la formule $210xx + yy$ il y a

$210 + 1^2$,	$+ 11^2$,	$+ 13^2$,	$+ 17^2$,	$+ 23^2$
211,	331,	379,	499,	739
p,	p,	p,	p,	p

Ici on doit donc admettre non seulement la forme $210xx + yy$, mais encore (à cause de l'affinité souvent remarquée des formes $\alpha\beta xx + yy$ et $\alpha xx + \beta yy$) les suivantes: $105xx + 2yy$, $70xx + 3yy$, $42xx + 5yy$, $30xx + 7yy$, $35xx + 6yy$, $21xx + 10yy$, $14xx + 15yy$.

Toute la doctrine des valeurs convenables, qui a été exposée ici, se réduit au reste aux principes suivans:

1. Que tout nombre de la forme $mxx + yy$ est censé être premier, non seulement lorsqu'il est premier lui-même, mais encore s'il est un produit d'un nombre premier dans un facteur quelconque de $2m$.

2. Que tout nombre de la forme $mxx + yy$ n'est censé être composé que lorsque outre le facteur de $2m$ il contient encore deux ou plusieurs autres facteurs premiers entr'eux.

3. Que si un nombre composé de la forme $mxx + yy$, quelque grand qu'il soit, n'est contenu que d'une seule façon dans cette forme, on pourra toujours assigner d'autres nombres composés moindres, qui pareillement ne sont contenus que d'une façon dans la forme proposée.

4. Que, par conséquent, si dans les petits nombres de cette forme il ne se rencontre point de composés contenus d'une seule manière dans la forme $mxx + yy$, il n'y en aura pas non plus dans les plus grands; et en ce cas le nombre m sera dans la classe des valeurs convenables (*idoneus*).

5. Tant que $m + bb < 4m$, tous les nombres de cette forme seront certainement contenus d'une seule façon dans la forme $mxx + yy$, excepté le cas où $m + bb = pp = \square$. Or si parmi les nombres $m + bb$ moindres que $4m$ il ne se trouve point de composés, m sera un nombre convenable.

DE CASIBUS QUIBUSDAM MAXIME MEMORABILIBUS IN ANALYSI INDETERMINATA UBI IMPRIMIS INSIGNIS USUS CALCULI ANGULORUM IN ANALYSI DIOPHANTEA OSTENDITUR

Commentatio 515 indicis ENESTROEMIANI
Acta academiae scientiarum Petropolitanae 1778: II, 1781, p. 85—110

1. Quaestionum, quas hic sum tractaturus, iam olim mentionem feci in Dissertatione Tomo VI Novorum Commentariorum inserta sub titulo: *De Problematibus indeterminatis, quae videntur plus quam determinata*[1]), ubi ostendi, quomodo unica aequatione inter quantitates indeterminatas constituta plurima Problemata DIOPHANTEA facili calculo simul resolvi queant; id quod utique maxime paradoxon videbatur, cum vulgo numerus conditionum propositarum numerum quantitatum incognitarum superare non soleat. Quam ob causam argumentum ibi tractatum utique in Analysi maximi momenti est censendum. Tum temporis autem in eiusmodi aequationibus subsistere fui coactus, in quibus quantitates indeterminatae non ultra secundam dimensionem ascendant. Nunc autem tales aequationes sum contemplaturus, ubi indeterminatae adeo ad quartam dimensionem assurgunt, quarum resolutio fines Analyseos transcendere videatur, quandoquidem hic tantum de solutionibus per numeros rationales agitur.

2. Prima igitur aequatio quarti gradus, quam hic tractabo, hoc Problemate continetur.

---

1) Quae dissertatio est Commentatio 253 (indicis ENESTROEMIANI): Novi comment. acad. sc. Petrop. 6 (1756/7), 1761, p. 85; *LEONHARDI EULERI Opera omnia*, series I, vol. 2, p. 399. F. R.

PROBLEMA 1

Invenire quatuor numeros rationales x, y, z, v, ut huic aequationi satisfiat

$$x^4 + y^4 + z^4 - 2xxyy - 2xxzz - 2yyzz + 2xxvv + 2yyvv + 2zzvv + v^4 = 0,$$

cuius formulae satis prolixae loco hic brevitatis gratia in sequentibus scribam litteram V.

3. Pro his autem litteris x, y, z, v inventis idoneis valoribus simul sequentes septem formulae sponte evadent numeri quadrati, quae sunt

$$\begin{aligned}
&\text{I.} && xxyy - zzvv && = \tfrac{1}{4}(xx + yy - zz + vv)^2,\\
&\text{II.} && xxzz - yyvv && = \tfrac{1}{4}(xx + zz - yy + vv)^2,\\
&\text{III.} && yyzz - xxvv && = \tfrac{1}{4}(yy + zz - xx + vv)^2,\\
&\text{IV.} && xxyy - vv(xx + yy) && = \tfrac{1}{4}(xx + yy - zz - vv)^2,\\
&\text{V.} && xxzz - vv(xx + zz) && = \tfrac{1}{4}(xx + zz - yy - vv)^2,\\
&\text{VI.} && yyzz - vv(yy + zz) && = \tfrac{1}{4}(yy + zz - xx - vv)^2,\\
&\text{VII.} && xxyy + xxzz + yyzz && = \tfrac{1}{4}(xx + yy + zz + vv)^2.
\end{aligned}$$

Ratio per se est manifesta, cum quarta pars formulae nostrae V, cuius valor per hypothesin $= 0$, singulis his septem formulis addita producat revera quadrata, quorum radices hic assignavimus.

4. Quodsi autem duae tantum huiusmodi formulae vel adeo tres proponantur, quae quadrata reddi debeant, per praecepta communia methodi DIOPHANTEAE negotium difficillime confici poterit, etiamsi quis maxime prolixos calculos expediverit; unde intelligitur, si quatuor pluresve tales formulae ad quadrata reducendae proponantur, solutionem ne tentari quidem posse. Tanto magis igitur erit mirandum, quando omnium harum septem formarum reductionem ad quadrata unico quasi labore assignabimus.

SOLUTIO PROBLEMATIS PROPOSITI

5. Totam autem solutionem ex duabus tantum prioribus formulis deduci posse observavi, quemadmodum ex sequente analysi intelligetur. Facile autem apparet primam formulam $xxyy - zzvv$ quadratum reddi, si sumatur

$$xy = \frac{zv(pp+rr)}{2pr};$$

tum enim huius formulae radix erit

$$= \frac{zv(pp-rr)}{2pr},$$

quae igitur aequalis erit quantitati

$$\frac{1}{2}(xx + yy - zz + vv).$$

Simili modo secunda formula evadit quadratum, si sumatur

$$xz = \frac{yv(qq+ss)}{2qs};$$

tum enim eius radix erit

$$\frac{yv(qq-ss)}{2qs} = \frac{1}{2}(xx + zz - yy + vv),$$

ex quibus conditionibus iam liquet omnes quatuor quantitates x, y, z, v determinari posse, ita ut non opus sit ad reliquas formulas respicere.

6. Cum igitur sit

$$\frac{xy}{zv} = \frac{pp+rr}{2pr} \quad \text{et} \quad \frac{xz}{yv} = \frac{qq+ss}{2qs},$$

prior per posteriorem multiplicata dabit hanc aequationem

$$\frac{xx}{vv} = \frac{(pp+rr)(qq+ss)}{4prqs}.$$

Prior autem per posteriorem divisa dat

$$\frac{yy}{zz} = \frac{qs(pp+rr)}{pr(qq+ss)},$$

unde patet istam solutionem absolvi non posse, nisi pro litteris p, r, q, s tales numeri exhiberi queant, ut ista formula $\frac{(pp+rr)(qq+ss)}{4prqs}$ evadat quadratum. Hoc autem praestito quoque altera expressio pro $\frac{yy}{zz}$ inventa fiet quadratum. Infra [§ 21 et seq.] autem fusius ostendemus, quomodo tales numeri p, r, q, s, quotcumque libuerit, investigari queant.

7. Hic igitur assumemus tales numeros nobis iam esse cognitos indeque reperiri

$$\frac{xx}{vv} = \frac{aa}{bb} \quad \text{et} \quad \frac{yy}{zz} = \frac{cc}{dd};$$

inde ergo statuatur

$$x = at, \quad v = bt, \quad y = cu \quad \text{et} \quad z = du$$

et iam has duas litteras t et u ex radicibus ante exhibitis sequenti modo facile eruere licebit. His enim valoribus substitutis prior radix praebebit

$$\frac{bdtu(pp-rr)}{pr} = (aa+bb)tt + (cc-dd)uu.$$

Simili modo ex altera radice nanciscimur

$$\frac{bctu(qq-ss)}{qs} = (aa+bb)tt - (cc-dd)uu.$$

Sufficeret autem unica harum duarum aequationum, quandoquidem per extractionem radicis quadratae ambae quantitates t et u atque adeo duplici modo definiri possent, nisi forte ad irrationalia delaberemur. Hoc autem fieri non posse ex sequenti analysi patescet.

8. Statuamus hic brevitatis gratia

$$\frac{pp-rr}{2pr} = m \quad \text{et} \quad \frac{qq-ss}{2qs} = n,$$

ubi notetur pro radicibus quadratis etiam sumi potuisse

$$\frac{rr-pp}{2pr} \quad \text{et} \quad \frac{ss-qq}{2qs},$$

unde patet ambas litteras m et n tam positive quam negative accipi posse. Hoc modo habebimus has aequationes

$$2mbdtu = (aa + bb)tt + (cc - dd)uu,$$
$$2nbctu = (aa + bb)tt - (cc - dd)uu,$$

quae duae aequationes additae dabunt hanc

$$b(md + nc)tu = (aa + bb)tt,$$

quae praebet

$$\frac{t}{u} = \frac{b(md+nc)}{aa+bb}.$$

Eodem modo, si posterior a priore subtrahatur, prodibit ista aequalitas

$$b(md - nc)tu = (cc - dd)uu,$$

unde iterum deducitur

$$\frac{t}{u} = \frac{cc-dd}{b(md-nc)},$$

qui duo valores certe inter se convenire debent. Utamur igitur posteriore forma, et quia litteras m et n pro lubitu sive positive sive negative accipere licet, statuamus

$$t = cc - dd \quad \text{et} \quad u = b(md \pm nc),$$

ubi iam duplex solutio involvitur.

9. Substituamus igitur hos valores atque omnes nostrae quatuor quantitates incognitae x, y, z, v sequenti modo prodibunt determinatae

$$x = a(cc - dd), \qquad v = b(cc - dd),$$
$$y = bc(md \pm nc), \quad z = bd(md \pm nc),$$

ubi vel signa superiora vel inferiora ubique capi debebunt. Atque nunc certo asseverare possumus his valoribus litterarum x, y, z, v omnes septem formulas supra memoratas quadrata reddi, quamvis tantum duas priores hic in computum duxerimus.

10. Ante autem quam methodum sumus traditurus numeros idoneos pro litteris p, r, q, s investigandi, conveniet hanc solutionem per aliquot exempla illustrare, in quo negotio quidem necesse erit ex iis, quae deinceps tradentur, valores idoneos pro litteris p, r, q, s depromere.

EXEMPLUM 1

UBI $p = 5$, $r = 1$, $q = 8$, $s = 1$

11. Ex his igitur valoribus habebimus statim

$$\frac{xy}{zv} = \frac{13}{5} \quad \text{et} \quad \frac{xz}{yv} = \frac{65}{16};$$

hinc iam sequitur fore

$$\frac{xx}{vv} = \frac{13^2}{4^2} \quad \text{et} \quad \frac{yy}{zz} = \frac{4^2}{5^2},$$

quamobrem statuamus

$$x = 13t, \quad v = 4t, \quad y = 4u, \quad z = 5u,$$

ita ut sit

$$a = 13, \quad b = 4, \quad c = 4, \quad d = 5.$$

Iam porro quia est $m = \frac{12}{5}$ et $n = \frac{63}{16}$, ex his iam valoribus nanciscemur

$$x = 39, \quad v = 12,$$

$$y = 16\left(4 \pm \frac{21}{4}\right), \quad z = 20\left(4 \pm \frac{21}{4}\right).$$

Prouti igitur vel inferiora signa vel superiora valent, obtinebimus duas sequentes solutiones ad minimos terminos reductas, si forte habuerint inter se communem factorem,

I. $x = 39$, $v = 12$, $y = 20$, $z = 25$,

II. $x = 39$, $v = 12$, $y = 148$, $z = 185$,

quarum solutionum prior sine dubio simplices satis numeros Problemati satisfacientes suppeditat.

12. Videamus, quomodo prior solutio omnibus septem formulis supra allatis satisfaciat:

$$\text{I.}\quad \sqrt{(xxyy - zzvv)} = \tfrac{1}{2}(xx + yy - zz + vv) = 720,$$

$$\text{II.}\quad \sqrt{(xxzz - yyvv)} = \tfrac{1}{2}(xx + zz - yy + vv) = 945,$$

$$\text{III.}\quad \sqrt{(yyzz - xxvv)} = \tfrac{1}{2}(yy + zz - xx + vv) = 176,$$

$$\text{IV.}\quad \sqrt{(xxyy - vv(xx + yy))} = \tfrac{1}{2}(xx + yy - zz - vv) = 576,$$

$$\text{V.}\quad \sqrt{(xxzz - vv(xx + zz))} = \tfrac{1}{2}(xx + zz - yy - vv) = 801,$$

$$\text{VI.}\quad \sqrt{(yyzz - vv(yy + zz))} = \tfrac{1}{2}(yy + zz - xx - vv) = 320,$$

$$\text{VII.}\quad \sqrt{(xxyy + xxzz + yyzz)} = \tfrac{1}{2}(xx + yy + zz + vv) = 1345.$$

EXEMPLUM 2
QUO $p = 5$, $r = 1$, $q = 13$, $s = 9$

13. Hic igitur erit

$$\frac{xy}{zv} = \frac{13}{5} \quad \text{et} \quad \frac{xz}{yv} = \frac{125}{117},$$

hinc

$$\frac{xx}{vv} = \frac{5^2}{3^2} \quad \text{et} \quad \frac{yy}{zz} = \frac{39^2}{25^2} \quad \text{ideoque} \quad \frac{x}{v} = \frac{5}{3} \quad \text{et} \quad \frac{y}{z} = \frac{39}{25}.$$

Fiat ergo

$$x = 5t, \quad v = 3t, \quad y = 39u, \quad z = 25u,$$

ita ut sit

$$a = 5, \quad b = 3, \quad c = 39, \quad d = 25.$$

Porro autem erit $m = \frac{12}{5}$ et $n = \frac{44}{117}$, ex quibus valoribus fiet

$$x = 5 \cdot 896, \quad v = 3 \cdot 896,$$
$$y = 3 \cdot 39 \cdot 60 \pm 39 \cdot 44, \quad z = 3 \cdot 25 \cdot 60 \pm 25 \cdot 44.$$

Hinc ergo sequentes duae solutiones deducuntur[1])

1) Editio princeps (atque etiam *Comment. arithm.*): . . . *solutiones deducuntur*

$$\text{I.}\quad x = 112, \quad v = 672, \quad y = 39, \quad z = 25,$$
$$\text{II.}\quad x = 112, \quad v = 672, \quad y = 39 \cdot 89, \quad z = 25 \cdot 89.$$

Correxit F. R.

I. $x = 20, \quad v = 12, \quad y = 39, \quad z = 25,$

II. $x = 560, \quad v = 336, \quad y = 17 \cdot 39, \quad z = 17 \cdot 25.$

EXEMPLUM 3

QUO $p = 8, \ r = 1, \ q = 13, \ s = 9$

14. Hoc casu erit

$$\frac{xy}{zv} = \frac{65}{16} \quad \text{et} \quad \frac{xz}{yv} = \frac{125}{117}$$

hincque

$$\frac{xx}{vv} = \frac{25^2}{12^2} \quad \text{et} \quad \frac{yy}{zz} = \frac{39^2}{20^2}.$$

Sumto igitur

$$x = 25t, \quad v = 12t, \quad y = 39u, \quad z = 20u$$

erit

$$a = 25, \quad b = 12, \quad c = 39, \quad d = 20.$$

Porro fit $m = \frac{63}{16}$ et $n = \frac{44}{117}$. Hinc iam colligitur

$$x = 25 \cdot 1121, \quad v = 12 \cdot 1121,$$

$$y = 39(945 \pm 176), \quad z = 20(945 \pm 176).$$

Has ergo nanciscimur solutiones

I. $x = 25 \cdot 1121, \quad v = 12 \cdot 1121, \quad y = 39 \cdot 769, \quad z = 20 \cdot 769,$

II. $x = 25, \quad v = 12, \quad y = 39, \quad z = 20.$

EXEMPLUM 4

QUO $p = 3, \ r = 1, \ q = 15, \ s = 8$

15. Fiet igitur

$$\frac{xy}{zv} = \frac{5}{3} \quad \text{et} \quad \frac{xz}{yv} = \frac{289}{240}$$

ideoque

$$\frac{xx}{vv} = \frac{17^2}{12^2} \quad \text{et} \quad \frac{yy}{zz} = \frac{20^2}{17^2}.$$

Hinc sumto

$$x = 17t, \quad v = 12t, \quad y = 20u, \quad z = 17u$$

erit

$$a = 17, \quad b = 12, \quad c = 20, \quad d = 17.$$

Deinde fiet $m = \frac{4}{3}$ et $n = \frac{161}{240}$, unde colligitur

$$x = 17 \cdot 111, \quad v = 12 \cdot 111,$$

$$y = 20(272 \pm 161), \quad z = 17(272 \pm 161).$$

Hinc sequentes solutiones

I. $x = 17 \cdot 111, \quad v = 12 \cdot 111, \quad y = 20 \cdot 433, \quad z = 17 \cdot 433,$

II. $x = 17, \quad v = 12, \quad y = 20, \quad z = 17,$

quae solutio posterior sine dubio omnium est simplicissima.

EXEMPLUM 5

QUO $p = 5, \ r = 2, \ q = 9, \ s = 8$

16. Hic erit

$$\frac{xy}{zv} = \frac{29}{20} \quad \text{et} \quad \frac{xz}{yv} = \frac{145}{144},$$

hinc

$$\frac{xx}{vv} = \frac{29^2}{24^2} \quad \text{et} \quad \frac{yy}{zz} = \frac{6^2}{5^2}.$$

Sumatur ergo

$$a = 29, \quad b = 24, \quad c = 6, \quad d = 5,$$

et cum sit $m = \frac{21}{20}$ et $n = \frac{17}{144}$, valores quaesiti erunt

$$x = 29 \cdot 11, \quad v = 24 \cdot 11,$$

$$y = 6(126 \pm 17), \quad z = 5(126 \pm 17).$$

Ambae ergo solutiones erunt

I. $x = 29 \cdot 11, \quad v = 24 \cdot 11, \quad y = 6 \cdot 109, \quad z = 5 \cdot 109,$

II. $x = 29, \quad v = 24, \quad y = 78, \quad z = 65.$

ALIA SOLUTIO EIUSDEM PROBLEMATIS PER CALCULUM ANGULORUM DEDUCTA

17. Cum formula $xxyy - zzvv$ debeat esse quadratum, hoc eveniet, si sumatur

$$xy \sin. \alpha = vz;$$

tum enim erit

$$\sqrt{(xxyy - zzvv)} = xy \cos. \alpha,$$

quae ergo quantitas aequalis est huic formulae

$$\tfrac{1}{2}(xx + yy - zz + vv).$$

Simili modo posito

$$yv = xz \sin. \beta$$

fiet

$$\sqrt{(xxzz - yyvv)} = xz \cos. \beta = \tfrac{1}{2}(xx + zz - yy + vv).$$

18. Cum igitur sit

$$\frac{xy}{zv} = \frac{1}{\sin. \alpha} \quad \text{et} \quad \frac{xz}{yv} = \frac{1}{\sin. \beta},$$

productum dabit

$$\frac{xx}{vv} = \frac{1}{\sin. \alpha \sin. \beta};$$

quamobrem statuamus

$$x = t \quad \text{et} \quad v = t\sqrt{\sin. \alpha \sin. \beta}.$$

Prior vero per posteriorem divisa dat

$$\frac{yy}{zz} = \frac{\sin. \beta}{\sin. \alpha},$$

unde statuamus

$$y = u\sqrt{\sin. \beta} \quad \text{et} \quad z = u\sqrt{\sin. \alpha}.$$

Substituantur nunc hi valores in superiore radice extracta sive in hac aequatione

$$2xy \cos. \alpha = xx + yy - zz + vv$$

orieturque ista

$$2tu \cos. \alpha \sqrt{\sin. \beta} = tt(1 + \sin. \alpha \sin. \beta) + uu(\sin. \beta - \sin. \alpha),$$

ex qua aequatione quadratica quaeratur u fietque

$$u = \frac{t \cos.\alpha \sqrt{\sin.\beta} \pm t \cos.\beta \sqrt{\sin.\alpha}}{\sin.\beta - \sin.\alpha};$$

quamobrem sumi poterit

$$t = \sin.\beta - \sin.\alpha \quad \text{et} \quad u = \cos.\alpha \sqrt{\sin.\beta} \pm \cos.\beta \sqrt{\sin.\alpha}.$$

19. Substitutis igitur his valoribus loco t et u quatuor quantitates quaesitae x, y, z, v ita determinabuntur, ut sit

$$x = \sin.\beta - \sin.\alpha, \quad v = (\sin.\beta - \sin.\alpha)\sqrt{\sin.\alpha \sin.\beta},$$

$$y = \cos.\alpha \sin.\beta \pm \cos.\beta \sqrt{\sin.\alpha \sin.\beta}, \quad z = \cos.\beta \sin.\alpha \pm \cos.\alpha \sqrt{\sin.\alpha \sin.\beta}.$$

Cum igitur hoc modo aequationi

$$2\sqrt{(xxyy - zzvv)} = xx + yy - zz + vv$$

satisfiat, sumtis utrimque quadratis ipsa aequatio biquadratica proposita V oritur, cui ergo etiam his valoribus satisfiet; consequenter etiam omnes septem formulae supra allatae simul fient quadrata, etiamsi in hac Analysi binas tantum priores simus contemplati.

20. Ut igitur valores pro x, y, z, v inventi fiant rationales, ante omnia sinus et cosinus angulorum α et β debent esse rationales, id quod fiet, si sumamus

$$\sin.\alpha = \frac{2pr}{pp + rr} \quad \text{et} \quad \sin.\beta = \frac{2qs}{qq + ss};$$

tum enim erit

$$\cos.\alpha = \frac{pp - rr}{pp + rr} \quad \text{et} \quad \cos.\beta = \frac{qq - ss}{qq + ss}.$$

Praeterea vero hic imprimis requiritur, ut productum sinuum, scilicet

$$\sin.\alpha \sin.\beta = \frac{4prqs}{(pp + rr)(qq + ss)} = \square,$$

quae est ea ipsa conditio, quae in solutione praecedente postulabatur, ita ut ista solutio ab illa non aliter nisi modo investigationis discrepet. Hic vero

fundamentum totius solutionis multo clarius perspicitur. Nunc igitur eam investigationem aggrediamur, quam supra sumus polliciti, quemadmodum scilicet binae tales formulae indagari queant, quarum productum quadratum efficiat.

QUAESTIO

Investigare binas huiusmodi formulas

$$\frac{pp+rr}{2pr} \quad et \quad \frac{qq+ss}{2qs},$$

quarum productum fiat quadratum.

SOLUTIO

21. Cum igitur istud productum debeat fieri quadratum, per quadratum $4pprrqqss$ multiplicando etiam hoc productum quadratum reddi debet

$$pr(pp+rr) \asymp qs(qq+ss);$$

ubi id commodum sumus adepti, ut prior factor tantum litteras p et r, posterior vero solas q et s contineat, cui conditioni utique perfectissime satisfieret, si utraque formula $pr(pp+rr)$ et $qs(qq+ss)$ seorsim quadratum effici posset. Verum iam dudum demonstratum est hoc prorsus esse impossibile. Quia enim producti prioris factores p, r, $(pp+rr)$ sunt primi inter se, necesse foret, ut singuli essent quadrata. Posito ergo $p=tt$ er $r=uu$ tertius factor quadratus efficiendus foret t^4+u^4. Demonstratum autem est summam duorum biquadratorum quadratum reddi numquam posse.[1])

22. Cum igitur ambae hae formulae

$$pr(pp+rr) \quad \text{et} \quad qs(qq+ss)$$

ipsae quadrata esse nequeant, necesse est, ut sint *numeri planisimiles*, uti ab

1) Id quod primum anno 1676 demonstratum est a B. Frénicle de Bessy. Vide L. Euleri Commentationem 98 (indicis Enestroemiani): *Theorematum quorundam arithmeticorum demonstrationes*, Comment. acad. sc. Petrop. 10 (1738), 1747, p. 125; *Leonhardi Euleri Opera omnia*, series I, vol. 2, p. 38. F. R.

EUCLIDE[1]) vocantur. Quamquam autem ad hoc efficiendum quatuor habemus quantitates indeterminatas p, r, q, s, tamen nullo modo solutio generalis adhuc investigari potuit; quam ob causam tantum solutionibus particularibus contenti esse debemus, quae etiam maximas difficultates involvunt, nisi istas formulas in aliam speciem transmutemus, quod commodissime hoc modo fiet. Ponatur

$$p = 2fg \quad \text{et} \quad r = ff - gg$$

similique modo

$$q = 2hk \quad \text{et} \quad s = hh - kk$$

hocque modo ambae nostrae formulae evadent

$$2fg(ff - gg)(ff + gg)^2 \quad \text{et} \quad 2hk(hh - kk)(hh + kk)^2.$$

Quia igitur postremi factores sponte sunt quadrata, superest, ut hoc productum

$$2fg(ff - gg) \times 2hk(hh - kk)$$

reddatur quadratum sive, quod eodem redit, hoc

$$fg(ff - gg) \times hk(hh - kk),$$

et quia hic etiam quatuor litterae insunt, ut eas ad pauciorem numerum reducamus, statuamus

$$h = g \quad \text{et} \quad k = f - g;$$

hoc modo posterior formula erit $fg(f - g)(2g - f)$, quae per priorem multiplicata omissis factoribus quadratis praebet hoc productum

$$(f + g)(2g - f)$$

quadratum efficiendum. Hunc in finem ponatur

$$f = \frac{2mm - nn}{3} \quad \text{et} \quad g = \frac{mm + nn}{3}$$

sive, quia utriusque litterae aeque multipla sumere licet, sumamus

$$f = 2mm - nn \quad \text{et} \quad g = mm + nn,$$

unde fiet

$$h = mm + nn \quad \text{et} \quad k = mm - 2nn.$$

1) EUCLIDIS *Elementa* (ed. I. L. HEIBERG), vol. II, lib. VII defin. 21, lib. IX prop. 1 et 2. F. R.

23. Hinc ergo pro lubitu innumerabilia paria binarum talium formularum

$$fg(ff-gg) \quad \text{et} \quad hk(hh-kk)$$

erui poterunt, quarum productum certe erit quadratum. Veluti si sumamus $m=2$ et $n=1$, habebimus hos valores

$$f=7, \quad g=5, \quad h=5, \quad k=2.$$

Hinc enim fit

$$fg(ff-gg)=840 \quad \text{et} \quad hk(hh-kk)=210,$$

quarum productum est $4\cdot 210^2$.

24. Verum hoc modo valores litterarum p, r, q, s mox prodirent satis enormes, quia posuimus

$$p=2fg, \quad r=ff-gg, \quad q=2hk \quad \text{et} \quad s=hh-kk,$$

qui in exemplo allato fierent

$$p=70, \quad r=24, \quad q=20, \quad s=21,$$

ubi bini p et r per 2 depressi evadent $p=35$ et $r=12$, ita ut nostrum productum utique sit quadratum, scilicet

$$3^2\cdot 4^2\cdot 5^2\cdot 7^2\cdot 29^2\cdot 37^2.$$

Verum quia hi numeri ex casu simplicissimo pro m et n sumto sunt orti, facile intelligitur ex maioribus valoribus pro m et n ortis pro litteris p, r, q, s mox maximos numeros esse prodituros.

25. Cum igitur pro nostro Problemate solutiones potissimum simpliciores intendamus, istae formulae, ad quas sumus perducti, ad hunc scopum neutiquam sunt accommodatae; unde longe aliam viam inire conveniet, quae ita sit comparata, uti non ad numeros nimis magnos pro litteris p, r, q, s perducat, et quae simul simplicissimas solutiones certissime exhibeat, id quod sequenti modo commodissime praestabitur.

Cum $ab(aa+bb)$ sit forma utriusque formulae, qua indigemus, pro a et b successive accipiamus numeros simpliciores et productum revocemus ad hanc formam A^2F, ubi A^2 complectatur omnes factores quadratos, F vero sit productum ex factoribus non quadratis. Pro nostro igitur instituto eiusmodi duae pluresve formulae requiruntur, quae pro F eundem valorem praebeant,

quandoquidem tales pro binis nostris formulis $pr(pp+rr)$ et $qs(qq+ss)$ accipere licebit. Hunc in finem sequentem tabulam adiungimus, quae pro singulis valoribus litterarum a et b numeros littera F indicatos exhibeat, et quoniam consultum est in valoribus simplicioribus subsistere, hinc omittamus omnes numeros primos maiores quam 13.

a	b	F	a	b	F
2	1	2·5	9	7	2·5·7·13
3	1	2·3·5	11	2	2·5·11
3	2	2·3·13	11	3	2·3·5·11·13
4	3	3	12	5	3·5
5	1	2·5·13	13	9	2·5·13
7	1	2·7	15	8	2·3·5
7	4	5·7·13	18	1	2·13
8	1	2·5·13			

26. Hanc autem tabulam ulterius continuare licet statuendo $a=2fg$ et $b=ff-gg$; tum enim tantum formulam $2fg(ff-gg)$ examinare sufficiet. Hinc ergo similem tabulam pro numeris f et g subiungamus adscriptis simul valoribus litterarum a et b et ultima columna valores litterae F indicabit.

f	g	a	b	F	f	g	a	b	F
2	1	4	3	3	8	1	16	63	7
3	2	12	5	3·5	8	3	48	55	3·5·11
4	1	8	15	2·3·5	8	5	80	39	3·5·13
4	3	24	7	2·3·7	8	7	112	15	3·5·7
5	2	20	21	3·5·7	9	2	36	77	7·11
5	4	40	9	2·5	9	4	72	65	2·5·13
6	1	12	35	3·5·7	10	1	20	99	5·11
6	5	60	11	3·5·11	10	3	60	91	3·5·7·13
7	2	28	45	5·7	11	2	44	117	11·13
7	4	56	33	2·3·7·11	11	4	88	105	2·3·5·7·11
7	6	84	13	3·7·13	11	10	220	21	3·5·7·11

27. Iam ex his duabus tabulis coniunctis excerpamus eos casus, quibus eadem littera F convenit.

F	a	b	F	a	b	F	a	b
$2\cdot5$	2	1	$2\cdot5\cdot13$	5	1	$3\cdot5\cdot7$	20	21
	40	9		8	1		12	35
$2\cdot3\cdot5$	3	1		13	9		112	15
	15	8		72	65	$3\cdot5\cdot11$	60	11
							48	55

28. Ex his iam casibus plurimae solutiones nostri Problematis, quo quaeruntur quatuor numeri x, y, z, v, quibus formula biquadratica in Problemate proposito signo V indicata revera ad nihilum redigitur, deduci possunt, quarum iam plures in exemplis allatis sunt datae, quas igitur hic conspectui coniunctim exponamus[1])

x	20	39	185	$17\cdot39$	78	$25\cdot1121$	$20\cdot433$	$6\cdot109$
y	17	25	148	560	65	$12\cdot1121$	$17\cdot433$	$5\cdot109$
z	17	20	39	$17\cdot25$	29	$39\cdot\ 769$	$17\cdot111$	$29\cdot\ 11$
v	12	12	12	336	24	$20\cdot\ 769$	$12\cdot111$	$24\cdot\ 11$

ubi, quia litterae x, y, z inter se permutari possunt, maximos valores ipsi x tribuimus hincque descendentes pro y et z scripsimus. Semper autem minimus valor litterae v competit.

PROBLEMA 2

Proposita formula biquadratica

$$V = x^4 + y^4 + z^4 + v^4 - 2xxyy - 2xxzz - 2xxvv - 2yyzz - 2yyvv - 2zzvv$$

investigare valores quatuor numerorum x, y, z, v, ut ista formula nihilo fiat aequalis.

Quod Problema etiam ita enunciari potest:

Quaerantur quatuor quadrata xx, yy, zz, vv, quorum si ponatur summa $= \Sigma$ et summa factorum ex binis $= \Pi$, ut sit $\Sigma^2 = 4\Pi$.

1) Tabula sequens secundum notam p. 435 correcta est. F. R.

29. Quodsi tales valores pro litteris x, y, z, v fuerint inventi, simul sequentes formulae reddentur quadrata, quorum radices ita se habebunt:

I. $2\sqrt{(xxyy + zzvv)} = xx + yy - zz - vv,$

II. $2\sqrt{(xxzz + yyvv)} = xx + zz - yy - vv,$

III. $2\sqrt{(xxvv + yyzz)} = xx + vv - yy - zz,$

IV. $2\sqrt{(xxyy + xxzz + yyzz)} = xx + yy + zz - vv,$

V. $2\sqrt{(xxyy + xxvv + yyvv)} = xx + yy + vv - zz,$

VI. $2\sqrt{(xxzz + xxvv + zzvv)} = xx + zz + vv - yy,$

VII. $2\sqrt{(yyzz + yyvv + zzvv)} = yy + zz + vv - xx,$

quibus addi potest

VIII. $2\sqrt{\Pi} = xx + yy + zz + vv.$

In hoc igitur Problemate quaterni numeri x, y, z, v aequaliter ingrediuntur, cum in priore Problemate quadrati vv ratio fuisset diversa.

SOLUTIO HUIUS PROBLEMATIS

30. Solae priores formulae hic iterum sufficiunt ad totam solutionem absolvendam. Cum enim formula $xxyy + zzvv$ debeat reddi quadratum, hoc eveniet sumendo

$$xy = \frac{zv(pp - rr)}{2pr};$$

tum enim erit

$$\sqrt{(xxyy + zzvv)} = \frac{zv(pp + rr)}{2pr}$$

ideoque

$$= \frac{1}{2}(xx + yy - zz - vv).$$

Simili modo pro secunda formula si sumatur

$$xz = \frac{yv(qq - ss)}{2qs},$$

erit

$$\sqrt{(xxzz + yyvv)} = \frac{yv(qq + ss)}{2qs} = \frac{1}{2}(xx + zz - yy - vv).$$

31. Cum igitur habeamus has duas aequationes

$$\frac{xy}{zv} = \frac{pp-rr}{2pr} \quad \text{et} \quad \frac{xz}{yv} = \frac{qq-ss}{2qs},$$

earum productum dabit

$$\frac{xx}{vv} = \frac{(pp-rr)(qq-ss)}{4prqs};$$

prior vero per posteriorem divisa dabit

$$\frac{yy}{zz} = \frac{qs(pp-rr)}{pr(qq-ss)}$$

atque nunc utrique conditioni satisfiet, dummodo fuerit

$$\frac{(pp-rr)(qq-ss)}{prqs} = \square.$$

Quomodo igitur hoc effici debeat, in sequentibus [§ 39] fusius docebimus. Interim vero hic assumamus tales valores pro litteris p, r, q, s nobis esse cognitos.

32. Statuere igitur poterimus

$$\frac{xx}{vv} = \frac{aa}{bb} \quad \text{et} \quad \frac{yy}{zz} = \frac{cc}{dd},$$

ubi ergo numeri a, b, c, d ut cogniti spectantur. Quamobrem hinc ponamus

$$x = at, \quad v = bt, \quad y = cu, \quad z = du$$

sicque totum negotium nunc eo est reductum, ut ambo numeri t et u debite assignentur. Pro priore igitur radice quadrata $\frac{zv(pp+rr)}{2pr}$ habebimus $zv = bdtu$; unde si statuamus brevitatis gratia

$$\frac{bd(pp+rr)}{2pr} = m$$

similique modo pro altera radice ob $yv = bctu$

$$\frac{bc(qq+ss)}{2qs} = n,$$

ambo radices erunt mtu et ntu.

33. Pro priore igitur radice habebimus

$$2mtu = xx + yy - zz - vv,$$

pro altera vero

$$2ntu = xx + zz - yy - vv,$$

quarum summa dabit

$$(m+n)tu = xx - vv = (aa - bb)tt,$$

unde statim deducitur

$$\frac{t}{u} = \frac{m+n}{aa-bb}.$$

Simili modo differentia dabit

$$(m-n)tu = yy - zz = (cc - dd)uu,$$

unde etiam deducimus

$$\frac{t}{u} = \frac{cc-dd}{m-n},$$

qui duo valores per ipsam quaestionis naturam inter se congruere debebunt. At vero quia m et n per extractionem radicis sunt natae, eas tam negative quam positive accipere licebit, unde simul gemini valores pro t et u reperientur, quibus inventis tota Problematis solutio ita se habebit:

$$x = a(m+n), \quad v = b(m+n),$$
$$y = c(aa - bb), \quad z = d(aa - bb),$$

unde facile erit exempla quotcumque evolvere.

EXEMPLUM 1
QUO SUMITUR $p = 5$, $r = 2$, $q = 6$ ET $s = 1$

34. Hic igitur erit

$$\frac{xy}{zv} = \frac{21}{20} \quad \text{et} \quad \frac{yz}{yv} = \frac{35}{12},$$

unde oritur

$$\frac{xx}{vv} = \frac{7^2}{4^2}$$

ideoque

$$a = 7 \quad \text{et} \quad b = 4;$$

tum vero erit

$$\frac{yy}{zz} = \frac{3^2}{5^2},$$

ergo

$$c = 3 \quad \text{et} \quad d = 5;$$

unde fiet $m = 29$ et $n = 37$. Cum autem sit $m = \pm 29$, duplex solutio ita se habebit:

$$x = 7\,(37 \pm 29), \quad v = 4(37 \pm 29), \quad y = 99, \quad z = 165.$$

Signa igitur superiora praebent hanc solutionem

$$x = 14, \quad v = 8, \quad y = 3, \quad z = 5,$$

inferiora vero

$$x = 56, \quad v = 32, \quad y = 99, \quad z = 165.$$

EXEMPLUM 2

QUO $p = 5$, $r = 2$, $q = 8$, $s = 7$

35. Hic erit

$$\frac{xy}{zv} = \frac{21}{20} \quad \text{et} \quad \frac{xz}{yv} = \frac{15}{112},$$

unde oritur

$$\frac{xx}{vv} = \frac{3^2}{8^2} \quad \text{et} \quad \frac{yy}{zz} = \frac{14^2}{5^2}.$$

Sumatur ergo

$$a = 3, \quad b = 8, \quad c = 14, \quad d = 5$$

fietque $m = 58$ et $n = 113$. Verum ob $m = \pm 58$ duplex oritur solutio, scilicet

$$x = 3(113 \pm 58), \quad v = 8(113 \pm 58), \quad y = 14 \cdot 55 \quad \text{et} \quad z = 5 \cdot 55.$$

Hinc hae duae solutiones

$$x = 3, \quad v = 8, \quad y = 14, \quad z = 5,$$

$$x = 3 \cdot 171, \quad v = 8 \cdot 171, \quad y = 14 \cdot 55, \quad z = 5 \cdot 55.$$

EXEMPLUM 3

QUO $p = 6$, $r = 1$, $q = 8$, $s = 7$

36. Hoc casu fit

$$\frac{xy}{zv} = \frac{35}{12} \quad \text{et} \quad \frac{xz}{yv} = \frac{15}{112}$$

ideoque

$$\frac{xx}{vv} = \frac{5^2}{8^2} \quad \text{et} \quad \frac{yy}{zz} = \frac{14^2}{3^2}.$$

Sumto igitur

$$a = 5, \quad b = 8, \quad c = 14, \quad d = 3$$

erit $m = \pm 74$ et $n = 113$ hincque

$$x = 5(113 \pm 74) \quad \text{et} \quad v = 8(113 \pm 74),$$

unde hae duae solutiones oriuntur

$$x = 5, \quad v = 8, \quad y = 14, \quad z = 3,$$

$$x = 5 \cdot 187, \quad v = 8 \cdot 187, \quad y = 14 \cdot 39, \quad z = 3 \cdot 39.$$

EXEMPLUM 4

QUO $p = 6$, $r = 5$, $q = 8$, $s = 3$

37. Cum hinc sit

$$\frac{xy}{zv} = \frac{11}{60} \quad \text{et} \quad \frac{xz}{yv} = \frac{55}{48},$$

erit

$$\frac{xx}{vv} = \frac{11^2}{24^2} \quad \text{et} \quad \frac{yy}{zz} = \frac{2^2}{5^2}$$

ideoque

$$a = 11, \quad b = 24, \quad c = 2, \quad d = 5;$$

hinc ob $m = 122$ et $n = 73$ erit

$$x = 11(122 \pm 73) \quad \text{et} \quad v = 24(122 \pm 73),$$

unde sequentes deducuntur solutiones

$$x = 11 \cdot 49, \quad v = 24 \cdot 49, \quad y = 2 \cdot 455, \quad z = 5 \cdot 455,$$

$$x = 33, \quad v = 72, \quad y = 14, \quad z = 35.$$

38. Si quis plura huiusmodi exempla evolvere voluerit, quoniam totum negotium eo redit, ut pro p, r, q, s idonei valores exhiberi queant, ad hoc efficiendum sequentem regulam adiungamus.

REGULA PRO INVENIENDIS NUMERIS IDONEIS PRO p, r, q, s

39. Si f et g denotent numeros quoscumque sive positivos sive negativos, semper accipi poterit

$$p = fg \quad \text{et} \quad r = (2g + f)(3g + 2f);$$

tum vero sumi poterunt duplici modo pro q et s valores debiti, scilicet

$$q = (2g + f)(3g + f) \quad \text{et} \quad s = f(f + g)$$

vel

$$q = (f + g)(3g + 2f) \quad \text{et} \quad s = g(3g + f);$$

ubi notandum, si bini tales numeri habeant factorem communem, eum omitti posse, ac si eveniat, ut tales numeri prodeant negativi, eorum loco semper positivos scribere licebit.[1]) Ita si pro f et g unitas accipiatur, erit $p = 1$ et $r = 15$; tum vero habebitur vel $q = 6$ et $s = 1$ vel $q = 5$ et $s = 2$, ubi insuper notasse iuvabit loco binorum talium numerorum etiam eorum semi-summam et semi-differentiam accipi posse. Ita loco $p = 1$ et $r = 15$ sumi poterit $p = 8$ et $r = 7$, quem casum in exemplis ante allatis expedivimus.

SOLUTIO EX CALCULO ANGULORUM PETITA

40. Pro hoc igitur Problemate statuamus

$$\frac{xy}{zv} = \frac{\cos.\alpha}{\sin.\alpha};$$

tum enim erit

$$\sqrt{(xxyy + zzvv)} = \frac{zv}{\sin.\alpha} = \frac{1}{2}(xx + yy - zz - vv).$$

Tum vero statuatur

$$\frac{xz}{yv} = \frac{\cos.\beta}{\sin.\beta}$$

ac tum habebitur

$$\sqrt{(xxzz + yyvv)} = \frac{yv}{\sin.\beta} = \frac{1}{2}(xx + zz - yy - vv).$$

---

1) Substitutionibus propositis formula $\frac{(p^2 - r^2)(q^2 - s^2)}{prqs}$ transit in $\frac{4^2(3g^2 + 3gf + f^2)^2}{f^2(2g + f)^2}$ vel $\frac{4^2(3g^2 + 3gf + f^2)^2}{g^2(3g + 2f)^2}$. F. R.

41. Iam his duabus formulis combinandis habebimus primo

$$\frac{xx}{vv} = \frac{\cos.\alpha \cos.\beta}{\sin.\alpha \sin.\beta} = \cot.\alpha \cot.\beta,$$

unde ponatur

$$x = t\sqrt{\cot.\alpha \cot.\beta} \quad \text{et} \quad v = t.$$

Simili modo habebitur

$$\frac{yy}{zz} = \frac{\cot.\alpha}{\cot.\beta},$$

unde ponatur

$$y = u\sqrt{\cot.\alpha} \quad \text{et} \quad z = u\sqrt{\cot.\beta}.$$

Substituantur hi valores in priore aequatione radicali fietque

$$\frac{2tu\sqrt{\cot.\beta}}{\sin.\alpha} = tt(\cot.\alpha \cot.\beta - 1) + uu(\cot.\alpha - \cot.\beta),$$

unde colligitur

$$\frac{u}{t} = \frac{\frac{\sqrt{\cot.\beta}}{\sin.\alpha} \pm \frac{\sqrt{\cot.\alpha}}{\sin.\beta}}{\cot.\alpha - \cot.\beta}.$$

Statuatur ergo

$$u = \frac{\sqrt{\cot.\beta}}{\sin.\alpha} \pm \frac{\sqrt{\cot.\alpha}}{\sin.\beta} \quad \text{et} \quad t = \cot.\alpha - \cot.\beta$$

et quatuor valores quaesiti erunt

$$x = \cot.\alpha\sqrt{\cot.\alpha \cot.\beta} - \cot.\beta\sqrt{\cot.\alpha \cot.\beta}, \quad v = \cot.\alpha - \cot.\beta,$$

$$y = \frac{\cot.\alpha}{\sin.\beta} + \sqrt{\frac{\cot.\alpha \cot.\beta}{\sin.\alpha}}, \quad z = \frac{\cot.\beta}{\sin.\alpha} + \frac{\sqrt{\cot.\alpha \cot.\beta}}{\sin.\beta}.$$

42. Ut igitur isti valores fiant rationales, ante omnia necesse est, ut tam sinus quam cosinus angulorum α et β, tum vero etiam, ut $\sqrt{\cot.\alpha \cot.\beta}$ fiant rationales. Priori satisfit ponendo

$$\sin.\alpha = \frac{2pr}{pp+rr} \quad \text{et} \quad \sin.\beta = \frac{2qs}{qq+ss};$$

tum enim fiet

$$\cos.\alpha = \frac{pp-rr}{pp+rr} \quad \text{et} \quad \cos.\beta = \frac{qq-ss}{qq+ss}$$

ideoque

$$\cot.\alpha = \frac{pp-rr}{2pr} \quad \text{et} \quad \cot.\beta = \frac{qq-ss}{2qs}.$$

Quamobrem requiritur, ut productum

$$\frac{(pp-rr)(qq-ss)}{prqs}$$

fiat quadratum, sicque deducimur ad ipsam solutionem ante inventam, et quia hoc modo ipsa aequatio biquadratica adimpletur, simul omnes septem formulae supra memoratae evadent quadrata.

43. Colligamus iam casus in exemplis superioribus evolutos atque simul plures casus habebimus, quibus huic aequationi biquadraticae satisfit, scilicet

$$x^4 + y^4 + z^4 + v^4 - 2xxyy - 2xxzz - 2xxvv - 2yyzz - 2yyvv - 2zzvv = 0,$$

et quia litterae x, y, z, v inter se permutari patiuntur, valores supra inventos secundum ordinem magnitudinis disponamus:

$x = 14$	72	165	8·171	8·187	5·455
$y = 8$	35	99	14· 55	5·187	24· 49
$z = 5$	33	56	3·171	14· 39	2·455
$v = 3$	14	32	5· 55	3· 39	11· 49

DE TRIBUS NUMERIS QUADRATIS QUORUM TAM SUMMA QUAM SUMMA PRODUCTORUM EX BINIS SIT QUADRATUM

Commentatio 523 indicis ENESTROEMIANI
Acta academiae scientiarum Petropolitanae 1779: I, 1782, p. 30—39

1. In Tomo Novorum Commentariorum VIII[1]) tractavi Problema, quo tres numeri quaeruntur, quorum tam summa quam summa productorum ex binis una cum producto omnium fiant quadrata; cuius solutio cum non solum esset difficillima, sed etiam ad immensos numeros[2]) perduxisset, merito videri poterat, si insuper nova conditio adderetur, solutionem vires Analyseos penitus esse superaturam. Hoc tamen evenit in quaestione, quam hic tractabo, ubi praeter tres conditiones memoratas etiam haec postulatur, ut singuli numeri quaesiti sint quadrati. Interim tamen hac conditione adiecta post plures conatus irritos tandem modum inveni istud Problema satis commode resolvendi, ubi adeo numeros satis modicos assignare licet Problemati satisfacientes.

---

1) Commentatio 270 (indicis ENESTROEMIANI): *Solutio problematis de investigatione trium numerorum, quorum tam summa quam productum nec non summa productorum ex binis sint numeri quadrati.* Novi Comment. acad. sc. Petrop. 8 (1760/1), 1763, p. 64; *LEONHARDI EULERI Opera omnia*, series I, vol. 2, p. 519. Vide etiam Commentationes 427 et A 31 huius voluminis.
F. R.

2) Sed vide summarium Commentationis 270 modo laudatae nec non p. XXVIII Prooemii voluminis praecedentis. F. R.

2. Sint xx, yy, zz terni numeri quadrati quaesiti, ita ut esse debeat

$$\text{I. } xx + yy + zz = \square,$$

$$\text{II. } xxyy + xxzz + yyzz = \square,$$

quarum conditionum priori satisfiet sumendo

$$x = pp + qq - rr, \quad y = 2pr \quad \text{et} \quad z = 2qr;$$

tum enim erit

$$xx + yy + zz = (pp + qq + rr)^2;$$

unde si ponamus

$$xx + yy + zz = P^2,$$

sumtis $x = pp + qq - rr$, $y = 2pr$, $z = 2qr$ fiet

$$P = pp + qq + rr.$$

3. Progrediamur nunc ad alteram conditionem, quae postulat, ut sit

$$xx(yy + zz) + zzyy = Q^2;$$

quare, cum sit

$$yy + zz = 4rr(pp + qq),$$

hinc orietur ista aequatio

$$Q^2 = 4rr(pp + qq)(pp + qq - rr)^2 + 16ppqqr^4,$$

quae divisa per factorem quadratum $4rr$ dabit

$$\frac{QQ}{4rr} = (pp + qq)(pp + qq - rr)^2 + 4ppqqrr,$$

quam ergo formulam quadratum reddi oportet. Ea autem evoluta litterae p et q ad sextam potestatem ascendent, littera vero r tantum ad quartam, quae ergo commode investigari posse videtur, siquidem casus sponte patet, scilicet si $rr = pp + qq$, dummodo fuerit $pp + qq$ quadratum. Interim tamen hinc ne unicam quidem aliam solutionem derivare licet, unde negotium prorsus alio modo aggredi oportet, quod sequenti modo egregio successu praestari poterit.

4. Pono autem $r = p - nq$, ita ut hoc modo nulla restrictio inferatur, quoniam loco litterae r nova indeterminata n introducitur; tum autem nostra aequatio hanc induet formam

$$\frac{QQ}{4(p-nq)^2} = (pp+qq)(2npq+(1-nn)qq)^2 + 4ppqq(p-nq)^2,$$

quae iam dividi potest per qq, ita ut

$$\frac{QQ}{4qq(p-nq)^2} = (pp+qq)(2np+(1-nn)q)^2 + 4pp(p-nq)^2,$$

quod quadratum brevitatis gratia designemus per R^2, ita ut sit

$$Q = 2q(p-nq)R.$$

Nunc igitur facta evolutione prodibit haec aequatio

$$\begin{aligned} R^2 = {} & 4(1+nn)p^4 - 4n(1+nn)p^3q + (1+6nn+n^4)ppqq \\ & + 4n(1-nn)pq^3 + (1-nn)^2q^4, \end{aligned}$$

in qua formula postremum membrum evasit quadratum; primum vero membrum reddi posset quadratum faciendo $nn+1 = \square$; at vero ad solutionem sufficere potest, ut postremus tantum terminus sit quadratum.

5. Pro R^2 eiusmodi quadratum statuamus, quo sublato tres ultimi termini e medio tollantur et ex duobus prioribus relictis ratio inter p et q determinetur. Hunc in finem statuatur[1])

$$R = (1-nn)qq + 2npq + \alpha pp$$

et α ita determinetur, ut etiam antepenultimus auferatur, quod fit sumendo $\alpha = \frac{1+2nn+n^4}{2(1-nn)}$, quo facto aequatio relicta erit

$$4p^4 - 4np^3q = \frac{(1+nn)^3}{4(1-nn)^2}p^4 + \frac{2n(1+nn)}{1-nn}p^3q,$$

1) Vide L. Euler, *Vollständige Anleitung zur Algebra*, St. Petersburg 1770, Zweyter Theil, zweyter Abschnitt, Cap. 9; *Leonhardi Euleri Opera omnia*, series I, vol. 1, p. 396. F. R.

sive per $4(1-nn)^2$ multiplicando, per p^3 dividendo et litteras p et q ad eandem partem transferendo fiet

$$(15-35nn+13n^4-n^6)p = 8n(1-nn)(3-nn)q,$$

quae aequatio porro per $3-nn$ dividi potest, quo facto fit

$$(5-10nn+n^4)p = 8n(1-nn)q,$$

unde deducitur

$$\frac{p}{q} = \frac{8n(1-nn)}{5-10nn+n^4}.$$

6. Sumamus igitur, ut huic aequationi satisfiat,

$$q = 5-10nn+n^4 \quad \text{et} \quad p = 8n(1-nn),$$

ex quibus valoribus colligitur

$$r = p-nq = n(3+2nn-n^4).$$

Praeterea vero his valoribus substitutis invenimus[1])

$$R = (1-nn)\left((5-10nn+n^4)^2+16nn(5-10nn+n^4)+32nn(1+nn)^2\right).$$

Inventis autem his valoribus ipsi numeri quaesiti ita formabuntur, ut sit

$$x = pp+qq-rr, \quad y = 2pr, \quad z = 2qr.$$

Ope harum formularum igitur aliquot exempla evolvamus.

EXEMPLUM 1

7. Sit $n = 2$ eritque $p = -48$, $q = -19$, $r = -10$, unde fit $R = 7035$. Erat autem

$$Q = 2qrR = 4 \cdot 5^2 \cdot 19 \cdot 1407.$$

---

1) Editio princeps (atque etiam *Comment. arithm.*): ... *invenimus*

$$R = (1-nn)((5-10nn+n^4)^2+16nn(5-10nn+n^4)+32(1+nn)^2).$$

In exemplis quidem sequentibus valores ipsius R recte computati sunt. F. R.

Hinc vero ipsi numeri quaesiti ita se habebunt

$$x = 2565, \quad y = 2 \cdot 10 \cdot 48, \quad z = 2 \cdot 10 \cdot 19.$$

Quoniam autem hi numeri communem divisorem habent 5, per eius divisionem deprimi poterunt simulque numerus P quinquies evadet minor, at vero Q vicies quinquies minor hocque modo solutio sequentibus valoribus continebitur

$$P = 553, \quad Q = 106932, \quad x = 513, \quad y = 192, \quad z = 76.$$

Quadrata iam numerorum x, y, z eiusmodi erunt numeri, qui Problemati olim tractato satisfacient. Tales igitur numeri erunt

$$x^2 = 263169, \quad y^2 = 36864, \quad z^2 = 5776,$$

qui numeri sunt incomparabiliter minores iis, quos loco citato exhibui; unde intelligitur methodum, qua tum temporis sum usus, non satis esse accommodatam. Summa autem horum trium numerorum est $= 553^2$, summa productorum ex binis[1]) $= 106932^2$ et productum omnium $= 513^2 \cdot 192^2 \cdot 76^2$.

EXEMPLUM 2

8. Sit $n = 3$ eritque $p = -8 \cdot 24 = -192$, $q = -4$, $r = -180$, qui numeri per -4 depressi evadent $p = 48$, $q = 1$, $r = 45$, unde fit

$$R = 14120 \quad \text{hincque} \quad Q = 18 \cdot 25 \cdot 2824.$$

Hinc vero ipsi numeri quaesiti erunt

$$x = 280, \quad y = 90 \cdot 48, \quad z = 90$$

sive deprimendo per 10 fiet

$$x = 28, \quad y = 432, \quad z = 9, \quad P = 433, \quad Q = 12708,$$

qui numeri adhuc praecedentibus sunt minores ideoque minimi omnium esse videntur, qui satisfaciant. Quadrata ergo horum numerorum, quae sunt

$$x^2 = 784, \quad y^2 = 186624, \quad z^2 = 81,$$

1) Editio princeps (atque etiam *Comment. arithm.*): ... *summa productorum ex binis* $= 35948^2$. Valor autem Q^2 huius summae iam supra recte computatus erat. Correxit F. R.

erunt sine dubio minimi[1]) Problemati olim tractato satisfacientes, quippe quorum summa est 433^2, summa productorum ex binis $= 12708^2$ et productum omnium $28^2 \cdot 432^2 \cdot 9^2$.

EXEMPLUM 3

9. Sit $n = \frac{1}{2}$ fietque $p = 3$, $q = \frac{41}{16}$, $r = \frac{55}{32}$ sive ductis his omnibus numeris in 32 fiet $p = 96$, $q = 82$, $r = 55$, unde fit

$$R = 22515 \quad \text{et} \quad Q = 2 \cdot 82 \cdot 55 \cdot 22515.$$

Tum vero erit

$$x = 12915, \quad y = 2 \cdot 55 \cdot 96, \quad z = 2 \cdot 55 \cdot 82,$$

qui numeri per 5 deprimi possunt, quo facto fit

$$x = 2583, \quad y = 2112, \quad z = 1804$$

sive

$$x = 3 \cdot 7 \cdot 123, \quad y = 3 \cdot 11 \cdot 64, \quad z = 4 \cdot 11 \cdot 41.$$

10. Haec omnia ex formulae biquadraticae § 4 allatae prima resolutione sunt deducta. Constat autem methodus, qua ex qualibet resolutione iam inventa plures novae derivari possunt; verum hoc modo ad formulas nimis complicatas perveniretur, quod negotium hic non suscipio; praecipue enim in talibus investigationibus id solet intendi, ut solutiones saltem simpliciores eruantur.

EVOLUTIO CASUUM QUIBUS EST $nn + 1$ QUADRATUM

11. Sit igitur $nn + 1 = mm$, quod evenit, quoties fuerit $n = \frac{aa - bb}{2ab}$; tum enim erit $m = \frac{aa + bb}{2ab}$. Quo observato retineamus in calculo litteras m et n eritque aequatio resolvenda

$$R^2 = 4mmp^4 - 4nmmp^3q + (m^4 + 4nn)ppqq + 4n(1 - nn)pq^3 + (1 - nn)^2q^4,$$

---

1) Sed vide solutiones multo minores 306, 272, 578 expositas in summario Commentationis 270 nota 1 p. 453 laudatae. Vide porro correctas solutiones § 17 nec non solutiones ab I. A. Eulero in Commentatione A 31 huius voluminis inventas. F. R.

ubi iam tam primus quam ultimus terminus sunt quadrata ideoque praeter operationem praecedentem tres[1]) adhuc respectu primi termini institui poterunt, quas ergo ordine prosequemur.

OPERATIO 1

12. Primo igitur ponatur

$$R = 2mpp - nmpq + (1 - nn)qq,$$

ubi notetur numerum m tam positive quam negative accipi posse, unde ergo gemina solutio nascetur. Huius ergo valoris pro R quadrato a superiore expressione pro R^2 sublato orietur sequens aequatio

$$\frac{p}{q} = \frac{4n + 2mn - 2mn^3 - 4n^3}{4m - 4mnn + mmnn - 4nn - m^4}$$

sive ob $nn = mm - 1$ erit

$$\frac{p}{q} = \frac{2n(4 + 2m - 2mm - m^3)}{4 + 8m - 5mm - 4m^3}.$$

13. Quoniam litterae m et n semper sunt fractiones, quo eae facilius tollantur, introducamus multiplicatorem indefinitum $\triangle$ ponamusque

$$p = 2\triangle n(4 + 2m - 2mm - m^3)$$

et

$$q = \triangle(4 + 8m - 5mm - 4m^3),$$

unde ob $r = p - nq$ fiet

$$r = \triangle n(4 - 4m + mm + 2m^3).$$

14. His igitur tribus valoribus inventis numeri quaesiti x, y, z ita ex iis determinantur, ut sit

$$x = pp + qq - rr, \quad y = 2pr, \quad z = 2qr.$$

Praeterea vero erit

$$P = pp + qq + rr, \quad Q = 2qrR$$

existente

$$R = 2mpp - mnpq + (1 - nn)qq.$$

1) Vide notam p. 455. F. R.

15. Unicum exemplum evolvamus, ut pateat, num hinc minores numeri sint prodituri quam ante. Sumamus igitur $a = 2$ et $b = 1$ fietque $n = \frac{3}{4}$ et $m = \pm\frac{5}{4}$ hincque fiet

$$p = \frac{3}{2}\triangle\left(4 \pm \frac{5}{2} - \frac{25}{8} \mp \frac{125}{64}\right), \quad q = \triangle\left(4 \pm 10 - \frac{125}{16} \mp \frac{125}{16}\right)$$

sive

$$p = \frac{3}{2}\triangle\left(\frac{7}{8} \pm \frac{35}{64}\right) \quad \text{et} \quad q = \triangle\left(-\frac{61}{16} \pm \frac{35}{16}\right).$$

Sumamus $\triangle = 128$ fietque

$$p = 3(56 \pm 35), \quad q = 8(-61 \pm 35)$$

hincque

$$r = p - \frac{3}{4}q = 3(178 \mp 35).$$

Valeat signum superius, quoniam hoc casu numeri resultantes per 13 deprimi possunt, quo facto reperitur

$$p = 3 \cdot 7 = 21, \quad q = -2 \cdot 8 = -16, \quad r = 3 \cdot 11 = 33,$$

unde colligimus

$$x = -392, \quad y = 1386, \quad z = -1056,$$

qui denuo reiectis signis per 2 deprimuntur, ita ut

$$x = 196, \quad y = 693, \quad z = 528.$$

Supra autem iam multo minores numeros nacti sumus.

OPERATIO 2

16. Ut praeter primum terminum etiam duo ultimi tollantur, statuamus

$$R = 2mpp + 2npq + (1 - nn)qq,$$

unde orietur sequens aequatio[1])

$$\frac{p}{q} = -\frac{4m - 4mnn - m^4}{4mn(2 + m)} \quad \text{sive} \quad \frac{p}{q} = -\frac{8 - 4mm - m^3}{4n(2 + m)}$$

1) In editione principe (atque etiam in *Comment. arithm.*) signum negativum formularum sequentium pro $\frac{p}{q}$ expositarum praetermissum est. Quem ob errorem omnes fere sequentes formulae corrigendae erant. F. R.

ob $nn = mm - 1$ sive etiam

$$\frac{p}{q} = -\frac{(2+m)(4-2m-mm)}{4n(2+m)} = -\frac{4-2m-mm}{4n}.$$

Fiat[1]) ut supra

$$p = \triangle(4 - 2m - mm) \quad \text{et} \quad q = -4\triangle n$$

hincque erit[2])

$$r = p - nq = \triangle m(3m - 2);$$

denique

$$x = pp + qq - rr, \quad y = 2pr, \quad z = 2qr,$$

$$P = pp + qq + rr \quad \text{et} \quad Q = 2qrR$$

existente

$$R = 2mpp + 2npq + (1 - nn)qq.$$

17. Sumamus iterum, quo res exemplo illustretur, $n = \frac{3}{4}$ ideoque $m = \pm\frac{5}{4}$ fietque

$$p = \triangle\left(\frac{39}{16} \mp \frac{5}{2}\right) \quad \text{et} \quad q = -3\triangle.$$

Sumatur $\triangle = 16$ et signo superiore valente erit $p = -1$ et $q = -48$; hinc fit $r = +35$, unde numeri quaesiti prodeunt

$$x = 1080, \quad y = 70, \quad z = 3360$$

sive deprimendo

$$x = 108, \quad y = 7, \quad z = 336,$$

qui praecedentibus adhuc minores sunt.[3])

---

1) Editio princeps: *Fiat . . . et* $q = 4\triangle n$. Vide notam p. 460. F. R.

2) Editio princeps: . . . *erit* $r = p - nq = \triangle(8 - 2m - 5mm)$. Vide notam p. 460. F. R.

3) Editio princeps (atque etiam *Comment. arithm.*): *Sumatur* $\triangle = 16$ *et . . . erit* $p = -1$ *et* $q = 48$; *hinc fit* $r = -37$, *unde . . . prodeunt*

$$x = 936, \quad y = 74, \quad z = 3552,$$

sive deprimendo

$$x = 468, \quad y = 37, \quad z = 1776,$$

qui praecedentibus adhuc maiores sunt. Vide notam p. 460. Ceterum periculum facienti mox patebit numeros ab EULERO computatos problemati proposito neutiquam satisfacere. F. R.

OPERATIO 3

18. Tollamus nunc tres terminos priores ponendo[1])

$$R = 2mpp - mnpq + \frac{m^4 - mmnn + 4nn}{4m} qq,$$

ex quo haec resultat aequatio

$$q\left(\frac{(m^4 - mmnn + 4nn)^2}{16mm} - (1 - nn)^2\right) = \frac{n}{2}(m^4 - mmnn - 4nn + 8)p.$$

Ex hac autem forma iam satis manifestum est nullos numeros minores Problemati satisfacientes elici posse; quamobrem ulteriore evolutione supersedemus.

---

1) Editio princeps (atque etiam *Comment. arithm.*): ... *ponendo*

$$R = 2mpp - mnpq + \frac{m^4 + 3nn}{4m} qq,$$

ex quo haec resultat aequatio:

$$g\left(\frac{(m^4 + 3nn)^2}{16mm} - (1 - nn)^2\right) = -\frac{n}{2}(m^4 - 5nn + 8)p.$$

Correxit F. R.

AD DISSERTATIONEM PATRIS DE TRIBUS NUMERIS QUORUM TAM SUMMA QUAM SUMMA PRODUCTORUM EX BINIS SIT QUADRATUM COMMENTATIO[1])

AUCTORE I. A. EULERO

Commentatio A 31 indicis ENESTROEMIANI
Acta academiae scientiarum Petropolitanae 1779: I, 1782, p. 40—48

Idem Problema, de quo hic sermo est, aggressus in solutionem incidi, particularem quidem, at ab Patris solutione plane diversam et numeros praebentem, qui nec magni nec in illa solutione contenti sunt. Adeoque non incongruum fore arbitror conatus ac repertus meos hic Academiae communicaturus supplementi instar ad Dissertationem modo indicatam adiicere.

Inchoabo a solutione maxime speciali, quae primo detecta ansam mihi praebuit sequentem generaliorem invenire.

1. Consideremus hos tres numeros

$$5(pp-1), \quad 8p \quad \text{et} \quad 6p,$$

quorum quadrata primae conditioni manifesto satisfaciunt. Est enim

$$25(pp-1)^2+64pp+36pp = 25(pp-1)^2+100pp = 25(pp+1)^2.$$

---

1) Vide dissertationem praecedentem. F. R.

At altera conditio postulat, ut sit

$$64 \cdot 25pp(pp-1)^2 + 36 \cdot 25pp(pp-1)^2 + 36 \cdot 64p^4$$

quadratum vel

$$2500pp(pp-1)^2 + 36 \cdot 64p^4 = \square$$

sive dividendo per quadratum $4pp$

$$625(pp-1)^2 + 576pp = \square$$

et evolvendo

$$625p^4 - 674pp + 625 = \square.$$

Fingamus huius quadrati radicem $= 25pp - v$ et fieri debet

$$625p^4 - 674pp + 625 = 625p^4 - 50ppv + vv,$$

unde eruitur

$$pp = \frac{625 - vv}{674 - 50v}.$$

2. Hic iam succedit sumendo $vv = 49$ et $v = 7$ tam numeratorem fractionis pp quam denominatorem quadrata evadere; fit enim $625 - vv = 576 = 24^2$ et $674 - 50v = 324 = 18^2$, unde $pp = \frac{24^2}{18^2}$ et deprimendo per 6^2

$$pp = \frac{4^2}{3^2} \quad \text{et} \quad p = \frac{4}{3}.$$

Hinc numeri quaesiti

$$5(pp-1) = \frac{5 \cdot 7}{9} = \frac{35}{9}, \quad 8p = \frac{32}{3} \quad \text{et} \quad 6p = \frac{24}{3},$$

qui multiplicati per 9 sequentes dabunt numeros integros Problemati satisfacientes

$$35, \ 96 \text{ et } 72,$$

qui certe satis parvi sunt comparatione facta cum illis minimis, quos Pater invenit, scilicet 9, 28 et 432. Nostri vero numeri 35, 96 et 72 conditiones praescriptas sequenti modo adimplent:

$$35^2 + 96^2 + 72^2 = 125^2$$

$$35^2 \cdot 96^2 + 35^2 \cdot 72^2 + 96^2 \cdot 72^2 = 8088^2.$$

Progrediamur iam ad solutionem generaliorem.

3. Ex Analysi DIOPHANTEA constat esse

$$(pp-1)^2+4pp=(pp+1)^2$$

similique modo

$$(qq-1)^2+4qq=(qq+1)^2.$$

Multiplicetur prima aequatio per $4qq$ et secunda per $(pp+1)^2$ eritque

$$4qq(pp-1)^2+16ppqq=4qq(pp+1)^2,$$

$$(qq-1)^2(pp+1)^2+4qq(pp+1)^2=(pp+1)^2(qq+1)^2.$$

Scribatur in hac postrema aequatione pro $4qq(pp+1)^2$ valor ex prima erutus et obtinebitur summa trium quadratorum numero quadrato aequalis

$$(qq-1)^2(pp+1)^2+4qq(pp-1)^2+16ppqq=(pp+1)^2(qq+1)^2.$$

4. Inventis ergo tribus numeris

$$(qq-1)(pp+1),\quad 2q(pp-1)\quad\text{et}\quad 4pq,$$

quorum quadrata iam primae conditioni satisfaciunt, superest, ut summa productorum ex binis quadratis reddatur quadratum. Oportet ergo sit

$$4qq(qq-1)^2(pp-1)^2(pp+1)^2+16ppqq(qq-1)^2(pp+1)^2 + 64ppq^4(pp-1)^2=\square$$

vel deprimendo per quadratum $4qq$

$$(qq-1)^2(p^4-1)^2+4pp(qq-1)^2(pp+1)^2+16ppqq(pp-1)^2=\square.$$

Est autem

$$(p^4-1)^2+4pp(pp+1)^2=(pp+1)^4.$$

Hinc requiritur quadratum fieri debere

$$(pp+1)^4(qq-1)^2+16ppqq(pp-1)^2=\square.$$

Quae conditio abit in illam solutionis specialis § 1 ponendo $p=2$.

5. Sit brevitatis gratia

$$(pp+1)^4 = AA \quad \text{et} \quad 16pp(pp-1)^2 = BB,$$

ut quadratum fieri debeat haec formula

$$AA(qq-1)^2 + BBqq \quad \text{vel} \quad AAq^4 + (BB-2AA)qq + AA,$$

cuius radix ponatur $= Aqq + v$, ut fiat

$$AAq^4 + (BB-2AA)qq + AA = AAq^4 + 2Aqqv + vv.$$

Unde eruitur

$$qq = \frac{AA-vv}{2AA-BB+2Av}.$$

6. Hic iterum evenit tam numeratorem quam denominatorem fractionis pro qq inventae evadere quadratum ponendo $vv = AA - BB$. Numerator enim $AA - vv$ abit in BB et denominator in

$$2AA - BB + 2A\sqrt{(AA-BB)},$$

qui manifesto est quadratum formulae

$$A + \sqrt{(AA-BB)}.$$

At restitutis pro A et B valoribus supra (§ 5) positis invenietur

$$AA - BB = p^8 - 12p^6 + 38p^4 - 12p^2 + 1,$$

id est

$$AA - BB = (p^4 - 6p^2 + 1)^2,$$

ideoque

$$\sqrt{(AA-BB)} = p^4 - 6p^2 + 1,$$

ita ut irrationalitas prorsus e calculo egrediatur.

7. Facto ergo $vv = AA - BB$ obtinetur

$$qq = \frac{BB}{(A+\sqrt{(AA-BB)})^2}$$

et

$$q = \frac{B}{A+\sqrt{(AA-BB)}} \quad \text{sive} \quad q = \frac{4p(pp-1)}{(pp+1)^2+p^4-6p^2+1} = \frac{4p(pp-1)}{2p^4-4pp+2},$$

hoc est

$$q = \frac{2p}{pp-1}.$$

8. Substituto denique pro q valore modo invento ob $qq - 1 = \frac{6pp - p^4 - 1}{(pp-1)^2}$ tres numeri Problemati satisfacientes erunt

$$\frac{(6pp - p^4 - 1)(pp + 1)}{(pp-1)^2}, \quad 4p \quad \text{et} \quad \frac{8pp}{pp-1}$$

et multiplicando per $(pp-1)^2$

$$(6pp - p^4 - 1)(pp + 1), \quad 4p(pp-1)^2 \quad \text{et} \quad 8pp(pp-1).$$

Summa quadratorum autem horum numerorum fiet

$$(pp+1)^2(qq+1)^2(pp-1)^4,$$

quae ob $qq + 1 = \frac{(pp+1)^2}{(pp-1)^2}$ transformatur in

$$(pp+1)^6,$$

ita ut summa quadratorum numerorum hic inventorum non solum quadratum fiat, sed adeo potestas sexta. Porro cum summa productorum ex binis numerorum quadratis quadratum fiat, cuius radix

$$= 2q(Aqq + v) \times (pp-1)^4,$$

ob

$$qq = \frac{4pp}{(pp-1)^2}, \quad A = (pp+1)^2 \quad \text{et} \quad v = \sqrt{(AA - BB)} = p^4 - 6pp + 1$$

haec radix abibit in hanc formam

$$4p(pp-1)(p^8 - 4p^6 + 22p^4 - 4pp + 1).$$

9. En ergo solutionem Problematis propositi: p pro lubitu assumto tres numeri quaesiti erunt

$$(6pp - p^4 - 1)(pp + 1) = x,$$
$$4p(pp-1)^2 = y,$$
$$8pp(pp-1) = z,$$

qui binas conditiones sequenti modo implebunt:

$$xx + yy + zz = (pp+1)^6,$$
$$xxyy + xxzz + yyzz = 16pp(pp-1)^2(p^8 - 4p^6 + 22p^4 - 4pp + 1)^2;$$

vel sumto

$$x = (pp+1)(4pp-(pp-1)^2),$$
$$y = 4p(pp-1)^2,$$
$$z = 8pp(pp-1)$$

fiet

$$xx+yy+zz = (pp+1)^6,$$
$$xxyy+xxzz+yyzz = 16pp(pp-1)^2((pp-1)^4+16p^4)^2.$$

EXEMPLA

10. Ponatur $p=2$ et invenietur

$$x = 5(16-9) = 35, \quad y = 8\cdot 9 = 72, \quad z = 8\cdot 4\cdot 3 = 96,$$
$$xx+yy+zz = 5^6 = 125^2,$$
$$xxyy+xxzz+yyzz = 16\cdot 4\cdot 9\cdot 337^2 = 8088^2,$$

quos numeros iam § 2 per solutionem specialissimam eruimus.

11. Positio $p=3$ eosdem numeros octies sumtos praebet; at ponendo $p=4$ fit[1])

$$x = 17\cdot 161 = 2737, \quad y = 16\cdot 15^2 = 3600, \quad z = 8\cdot 16\cdot 15 = 1920,$$
$$xx+yy+zz = 17^6 = 4913^2,$$
$$xxyy+xxzz+yyzz = 16^2\cdot 15^2\cdot 54721^2 = 13133040^2.$$

12. Cum $pp-1$, $2p$ et $pp+1$ latera trianguli rectanguli rationalis exprimant, nostra solutio sequenti modo concinnior reddi poterit. Sumantur tres numeri a, b et c, ut sit $aa+bb=cc$; quo facto fiunt numeri Problemati satisfacientes

$$x = c(aa-bb), \quad y = 2aab \quad \text{et} \quad z = 2abb;$$

1) In editione principe (atque etiam in *Comment. arithm.*) ultima sequentium formularum est

$$xxyy+xxzz+yyzz = 16^2\cdot 15^2\cdot 50881^2 = 12211440^2.$$

Correxit F. R.

tum enim erit

$$xx + yy + zz = c^6$$

et

$$xxyy + xxzz + yyzz = 4aabb(a^4 + b^4)^2.$$

Pro casu simplicissimo, quo $a = 4$, $b = 3$ et $c = 5$, inveniemus numeros iam supra erutos

$$x = 35, \quad y = 96 \quad \text{et} \quad z = 72.$$

Ponamus iam $a = 12$, $b = 5$ et $c = 13$ et obtinebimus hanc novam solutionem

$$x = 1547, \quad y = 1440, \quad z = 600,$$

unde fit

$$xx + yy + zz = 2197^2$$

$$xxyy + xxzz + yyzz = 5^3 \cdot 24^2 \cdot 21361^2 = 2563320^2.$$

In genere autem erit

$$a = 2mn, \quad b = mm - nn \quad \text{et} \quad c = mm + nn.$$

13. Formulae pro solutione nostri Problematis modo inventae ad aliam analysin conducunt, quae, cum concinnior sit praecedente, hic utique locum meretur. Sint numeri quaesiti x, y et z, ita ut fieri debeat

$$xx + yy + zz = MM$$

et

$$xxyy + xxzz + yyzz = NN.$$

Sumto iam

$$aa + bb = cc$$

sit

$$x = am \quad \text{et} \quad y = bm;$$

erit

$$xx + yy = ccmm.$$

Posito ergo

$$z = cn$$

erit

$$MM = cc(mm + nn);$$

quare fiat

$$m = 2pq \quad \text{et} \quad n = pp - qq,$$

ut sit

$$MM = cc(pp + qq)^2$$

ideoque

$$M = c(pp + qq).$$

Deinde cum sit

$$xy = abmm, \quad xz = acmn \quad \text{et} \quad yz = bcmn,$$

fit

$$NN = mm(aabbmm + aaccnn + bbccnn)$$

sive

$$NN = mm(aabbmm + c^4nn)$$

seu

$$NN = mm(4aabbppqq + c^4(pp - qq)^2) = \square.$$

Quod evadet manifesto, si fuerit

$$cc(pp - qq) = aapp - bbqq;$$

tum enim erit

$$NN = mm(aapp + bbqq)^2$$

et

$$N = m(aapp + bbqq).$$

Unde p et q ita definiri debent, ut fiat

$$ccpp - ccqq = aapp - bbqq,$$

unde fit

$$\frac{pp}{qq} = \frac{cc - bb}{cc - aa} = \frac{aa}{bb};$$

consequenter erit

$$p = a \quad \text{et} \quad q = b,$$

hinc

$$m = 2ab \quad \text{et} \quad n = aa - bb;$$

ergo numeri quaesiti

$$x = 2aab, \quad y = 2abb \quad \text{et} \quad z = c(aa - bb).$$

Tum autem erit

$$M = c(aa + bb) = c^3 \quad \text{et} \quad N = 2ab(a^4 + b^4).$$

14. Denique comparationem addam meae solutionis cum illa, quam Pater in eius dissertatione tentavit. Posuit autem

$$x = pp + qq - rr, \quad y = 2pr \quad \text{et} \quad z = 2qr,$$

ita ut hanc formulam

$$(pp+qq)(pp+qq-rr)^2+4ppqqrr$$

adhuc quadratum reddere supersit. Praesenti nostro casu erat $p=a$ et $q=b$ existente $aa+bb=cc$. Erit ergo

$$x=cc-rr, \quad y=2ar \quad \text{et} \quad z=2br;$$

quadratum autem esse debet haec formula

$$cc(cc-rr)^2+4aabbrr,$$

quae casibus $r=c$ et $r=0$ manifesto fit quadratum. Neuter autem horum casuum novos valores suppeditat. Interim tamen omnino requiritur, ut praeterea casus innotescat; talis autem casus est $r=\frac{ac}{b}$; tum enim haec formula erit

$$c^6(bb-aa)^2+4a^4b^4cc$$

sive

$$c^4(bb-aa)^2+4a^4b^4.$$

Est vero $cc(bb-aa)=b^4-a^4$, ergo formula

$$c^4(bb-aa)^2+4a^4b^4=(b^4-a^4)^2+4a^4b^4=(b^4+a^4)^2.$$

Potuisset etiam poni $r=\frac{bc}{a}$. At vero nemini certe in mentem venire potuisset hos valores in usum vocare vel divinando reperire. Nunc vero posito $r=\frac{ac}{b}$ numeri quaesiti sunt

$$x=\frac{cc(bb-aa)}{bb}, \quad y=\frac{2aac}{b}, \quad z=2ac$$

sive

$$x=c(bb-aa), \quad y=2aab, \quad z=2abb,$$

quae est ipsa mea solutio. At vero iste casus cognitus deducere potest ad infinitos alios; minimus autem eorum certe numeros enormes pro x, y et z esset daturus, qui forte ad trilliones et quadrilliones adsurgerent.

EVOLUTIO PRODUCTI INFINITI
$(1-x)(1-xx)(1-x^3)(1-x^4)(1-x^5)(1-x^6)$ etc.
IN SERIEM SIMPLICEM[1])

Commentatio 541 indicis Enestroemiani
Acta academiae scientiarum Petropolitanae 1780: I, 1783, p. 47—55

1. Posito

$$s = (1-x)(1-xx)(1-x^3)(1-x^4) \text{ etc.}$$

facile patet fore

$$s = 1 - x - xx(1-x) - x^3(1-x)(1-xx) - x^4(1-x)(1-xx)(1-x^3) - \text{ etc.};$$

quae series cum iam sit infinita, quaeritur, si singuli eius termini evolvantur, qualis series secundum simplices potestates ipsius x sit proditura. Cum igitur duo primi termini $1-x$ iam sint evoluti, loco reliquorum omnium scribatur littera A, ita ut sit

$$s = 1 - x - A$$

ideoque

$$A = xx(1-x) + x^3(1-x)(1-xx) + x^4(1-x)(1-xx)(1-x^3) + \text{ etc.}$$

---

1) Confer hanc dissertationem cum Commentatione 244 (indicis Enestroemiani): *Demonstratio theorematis circa ordinem in summis divisorum observatum*, Novi comment. acad. Petrop. 5 (1754/5), 1760, p. 75; *Leonhardi Euleri Opera omnia* series I, vol. 2, p. 390. Vide etiam, quae C. G. J. Jacobi de his duabus dissertationibus scripsit, apud P. Stäckel und W. Ahrens, *Der Briefwechsel zwischen C. G. J. Jacobi und P. H. von Fuss über die Herausgabe der Werke Leonhard Eulers*, Leipzig 1908, p. 63 et 65. Vide porro notam p. 191 voluminis praecedentis. F. R.

2. Quoniam hi termini omnes factorem habent communem $1-x$, eo evoluto singuli termini discerpentur in binas partes, quas ita repraesentemus

$$A = xx + x^3(1-xx) + x^4(1-xx)(1-x^3) + x^5(1-xx)(1-x^3)(1-x^4) + \text{etc.}$$
$$- x^3 - x^4\ (1-xx) - x^5(1-xx)(1-x^3) - x^6(1-xx)(1-x^3)(1-x^4) - \text{etc.}$$

Hinc iam binae partes eadem potestate ipsius x affectae in unam contrahantur ac resultabit pro A sequens forma

$$A = xx - x^5 - x^7(1-xx) - x^9(1-xx)(1-x^3) - x^{11}(1-x^2)(1-x^3)(1-x^4) - \text{etc.},$$

ubi duo termini primi $xx - x^5$ iam sunt evoluti; sequentes autem procedunt per has potestates $x^7, x^9, x^{11}, x^{13}, x^{15}$, quarum exponentes binario crescunt.

3. Ponamus nunc simili modo ut ante

$$A = xx - x^5 - B,$$

ita ut sit

$$B = x^7(1-xx) + x^9(1-xx)(1-x^3) + x^{11}(1-xx)(1-x^3)(1-x^4) + \text{etc.},$$

cuius omnes termini habent factorem communem $1-xx$, quo evoluto singuli termini in binas partes discerpantur, uti sequitur,

$$B = x^7 + x^9(1-x^3) + x^{11}(1-x^3)(1-x^4) + x^{13}(1-x^3)(1-x^4)(1-x^5) + \text{etc.}$$
$$- x^9 - x^{11}(1-x^3) - x^{13}(1-x^3)(1-x^4) - x^{15}(1-x^3)(1-x^4)(1-x^5) - \text{etc.}$$

Hic iterum bini termini, qui eandem potestatem ipsius x habent praefixam, in unam colligantur et prodibit

$$B = x^7 - x^{12} - x^{15}(1-x^3) - x^{18}(1-x^3)(1-x^4) - x^{21}(1-x^3)(1-x^4)(1-x^5) - \text{etc.}$$

ubi iam potestates ipsius x crescunt ternario.

4. Statuatur nunc porro

$$B = x^7 - x^{12} - C,$$

ita ut sit

$$C = x^{15}(1-x^3) + x^{18}(1-x^3)(1-x^4) + x^{21}(1-x^3)(1-x^4)(1-x^5) + \text{etc.},$$

et iam singuli termini per evolutionem factoris $1-x^3$ in binas partes resolvantur fietque

$$C = x^{15} + x^{18}(1-x^4) + x^{21}(1-x^4)(1-x^5) + x^{24}(1-x^4)(1-x^5)(1-x^6) + \text{etc.}$$
$$- x^{18} - x^{21}(1-x^4) - x^{24}(1-x^4)(1-x^5) - x^{27}(1-x^4)(1-x^5)(1-x^6) - \text{etc.},$$

ubi denuo membra, quibus eadem potestas ipsius x praefixa, in unum contracta praebebunt

$$C = x^{15} - x^{22} - x^{26}(1-x^4) - x^{30}(1-x^4)(1-x^5) - x^{34}(1-x^4)(1-x^5)(1-x^6) - \text{etc.},$$

ubi potestates praefixae quaternario crescunt.

5. Statuatur

$$C = x^{15} - x^{22} - D,$$

ut sit

$$D = x^{26}(1-x^4) + x^{30}(1-x^4)(1-x^5) + x^{34}(1-x^4)(1-x^5)(1-x^6) + \text{etc.},$$

qui termini per evolutionem factoris $1-x^4$ in binos discerpantur hoc modo

$$D = x^{26} + x^{30}(1-x^5) + x^{34}(1-x^5)(1-x^6) + x^{38}(1-x^5)(1-x^6)(1-x^7) + \text{etc.}$$
$$- x^{30} - x^{34}(1-x^5) - x^{38}(1-x^5)(1-x^6) - x^{42}(1-x^5)(1-x^6)(1-x^7) - \text{etc.}$$

Nunc binis [membris] ut hactenus contrahendis colligitur

$$D = x^{26} - x^{35} - x^{40}(1-x^5) - x^{45}(1-x^5)(1-x^6) - x^{50}(1-x^5)(1-x^6)(1-x^7) - \text{etc.}$$

Hic igitur potestates ipsius x quinario crescunt.

6. Statuatur

$$D = x^{26} - x^{35} - E,$$

ita ut sit

$$E = x^{40}(1-x^5) + x^{45}(1-x^5)(1-x^6) + x^{50}(1-x^5)(1-x^6)(1-x^7) + \text{etc.},$$

ac resolutione in binas partes ut hactenus instituta prodit

$$E = x^{40} + x^{45}(1-x^6) + x^{50}(1-x^6)(1-x^7) + x^{55}(1-x^6)(1-x^7)(1-x^8) + \text{etc.}$$
$$- x^{45} - x^{50}(1-x^6) - x^{55}(1-x^6)(1-x^7) - x^{60}(1-x^6)(1-x^7)(1-x^8) - \text{etc.}$$

Contractis vero binis terminis in unum prodibit

$$E = x^{40} - x^{51} - x^{57}(1-x^6) - x^{63}(1-x^6)(1-x^7) - x^{69}(1-x^6)(1-x^7)(1-x^8) - \text{etc.},$$

ubi potestates ipsius x senario crescunt.

7. Cum lex, qua istae operationes ulterius sunt continuandae, satis sit perspicua, si postremi valores pro singulis litteris A, B, C, D, E etc. inventi ordine substituantur, pro serie quaesita reperiemus sequentem formam

$$s = 1 - x, \; -xx + x^5, \; +x^7 - x^{12}, \; -x^{15} + x^{22}, \; +x^{26} - x^{35}, \; -x^{40} + x^{51}, \; + \text{etc.}$$

Hic igitur tota quaestio huc reducitur, ut ordo definiatur, quo exponentes potestatum ipsius x continuo ulterius augentur, quandoquidem ex operationibus institutis iam satis est manifestum signa terminorum $+$ et $-$ ita alternatim se excipere, ut ambo geminentur.

8. Quo igitur in hanc legem inquiramus, videamus, quomodo in singulis litteris isti numeri sint orti. Hunc in finem primos saltem cuiusque litterae terminos in eius forma prima exhibitos ordine disponamus:

$A = xx(1 - x)$	$7 = 3 + 4 = 3 + 1 + 3 = 3 + 1 + 1 + 2$
$B = x^7(1 - xx)$	$15 = 4 + 11 = 4 + 2 + 9 = 4 + 2 + 2 + 7$
$C = x^{15}(1 - x^3)$	$26 = 5 + 21 = 5 + 3 + 18 = 5 + 3 + 3 + 15$
$D = x^{26}(1 - x^4)$	$40 = 6 + 34 = 6 + 4 + 30 = 6 + 4 + 4 + 26$
$E = x^{40}(1 - x^5)$	$57 = 7 + 50 = 7 + 5 + 45 = 7 + 5 + 5 + 40$
etc.	etc.

Hic scilicet ex evolutione litterae A vidimus numerum 7 oriri ex aggregato $3 + 4$, tum vero 4 oriri ex $1 + 3$ ac denique 3 ex $1 + 2$, quae ergo resolutio dabit

$$7 = 3 + 4 = 3 + 1 + 3 = 3 + 1 + 1 + 2.$$

Atque idem ordo in sequentibus litteris est observatus, ubi ultimi numeri procedunt ordine 2, 7, 15, 26, 40.

9. Ex his iam manifestum est numerorum 2, 7, 15, 26, 40, 57 etc. differentias progressionem arithmeticam constituere, unde horum numerorum

terminus generalis erit

$$2+5(n-1)+\frac{3(n-1)(n-2)}{1\cdot 2}=\frac{3nn+n}{2}.$$

Exponentes autem, qui hos antecedunt, erant 1, 5, 12, 22, 35, 51 etc. ab illis numeris 1, 2, 3, 4, 5, 6 etc. et in genere ipso numero n [diversi], ita ut exponens, qui formulam $\frac{3nn+n}{2}$ praecedit, futurus sit

$$\frac{3nn-n}{2}.$$

10. Nunc igitur seriem simplicem inventam, quae aequalis est producto infinito proposito

$$(1-x)(1-xx)(1-x^3)(1-x^4) \text{ etc.},$$

perfecte cognoscimus. Cum enim haec series inventa sit

$$s=1-x^1-x^2+x^5+x^7-x^{12}-x^{15}+x^{22}+x^{26}-x^{35}-x^{40}+x^{51}+\text{etc.},$$

certi nunc sumus in ea alias potestates ipsius x non occurrere, nisi quarum exponentes contineantur in hac formula generali $\frac{3nn\pm n}{2}$, et quidem ita, ut, si n fuerit numerus impar, bini termini inde nati habituri sint signum —, qui autem ex paribus oriuntur, signum +.

ALIA INVESTIGATIO EIUSDEM SERIEI

11. Eadem series secundum potestates ipsius x procedens etiam sequenti modo investigari potest. Cum scilicet sit

$$s=1-x-xx(1-x)-x^3(1-x)(1-xx)-x^4(1-x)(1-x^2)(1-x^3)-\text{etc.},$$

evolvatur statim secundum membrum $-xx(1-x)$, ut fiat

$$s=1-x-xx+x^3-x^3(1-x)(1-xx)-x^4(1-x)(1-xx)(1-x^3)-\text{etc.},$$

ac statuatur

$$s=1-x-xx+A,$$

ut sit

$$A=x^3-x^3(1-x)(1-xx)-x^4(1-x)(1-xx)(1-x^3)-\text{etc.},$$

cuius singula membra per evolutionem factoris $1 - x$ in duas partes discerpantur, ut prodeat

$$A = x^3 - x^3(1 - xx) - x^4(1 - xx)(1 - x^3) - x^5(1 - x^2)(1 - x^3)(1 - x^4) - \text{etc.}$$
$$+ x^4(1 - xx) + x^5(1 - xx)(1 - x^3) + x^6(1 - x^2)(1 - x^3)(1 - x^4) + \text{etc.}$$

Hic iterum bina membra eadem potestate ipsius x affecta contracta praebebunt

$$A = x^5 + x^7(1 - xx) + x^9(1 - xx)(1 - x^3) + x^{11}(1 - x^2)(1 - x^3)(1 - x^4) + \text{etc.}$$

12. Hic nunc iterum secundum membrum evolvatur, ut prodeat

$$A = x^5 + x^7 - x^9 + x^9(1 - xx)(1 - x^3) + x^{11}(1 - x^2)(1 - x^3)(1 - x^4) + \text{etc.}$$

Iam ponatur

$$A = x^5 + x^7 - B,$$

ut sit

$$B = x^9 - x^9(1 - xx)(1 - x^3) - x^{11}(1 - xx)(1 - x^3)(1 - x^4) - \text{etc.};$$

quare si ubique factor $1 - xx$ evolvatur, obtinebitur

$$B = x^9 - x^9\,(1 - x^3) - x^{11}(1 - x^3)(1 - x^4) - x^{13}(1 - x^3)(1 - x^4)(1 - x^5) - \text{etc.}$$
$$+ x^{11}(1 - x^3) + x^{13}(1 - x^3)(1 - x^4) + x^{15}(1 - x^3)(1 - x^4)(1 - x^5) + \text{etc.},$$

tum vero contrahendis binis membris orietur

$$B = x^{12} + x^{15}(1 - x^3) + x^{18}(1 - x^3)(1 - x^4) + x^{21}(1 - x^3)(1 - x^4)(1 - x^5) + \text{etc.}$$

13. Evolvatur pariter secundum membrum ac statuatur

$$B = x^{12} + x^{15} - C$$

eritque

$$C = x^{18} - x^{18}(1 - x^3)(1 - x^4) - x^{21}(1 - x^3)(1 - x^4)(1 - x^5) - \text{etc.}$$

Nunc termini evolvantur secundum factorem $1 - x^3$ fietque

$$C = x^{18} - x^{18}(1 - x^4) - x^{21}(1 - x^4)(1 - x^5) - x^{24}(1 - x^4)(1 - x^5)(1 - x^6) - \text{etc.}$$
$$+ x^{21}(1 - x^4) + x^{24}(1 - x^4)(1 - x^5) + x^{27}(1 - x^4)(1 - x^5)(1 - x^6) + \text{etc.}$$

Hinc binis membris contrahendis fiet

$$C = x^{22} + x^{26}(1 - x^4) + x^{30}(x - x^4)(1 - x^5) + x^{34}(1 - x^4)(1 - x^5)(1 - x^6) + \text{etc.}$$

14. Evoluto nunc hic iterum secundo membro statuatur

$$C = x^{22} + x^{26} - D$$

eritque

$$D = x^{30} - x^{30}(1-x^4)(1-x^5) - x^{34}(1-x^4)(1-x^5)(1-x^6) - \text{etc.},$$

ubi evolutio factoris $1-x^4$ producet

$$\begin{aligned} D = {} & x^{30} - x^{30}(1-x^5) - x^{34}(1-x^5)(1-x^6) - x^{38}(1-x^5)(1-x^6)(1-x^7) - \text{etc.} \\ & + x^{34}(1-x^5) + x^{38}(1-x^5)(1-x^6) - x^{42}(1-x^5)(1-x^6)(1-x^7) + \text{etc.} \end{aligned}$$

Hinc binis membris contractis fiet

$$D = x^{35} + x^{40}(1-x^5) + x^{45}(1-x^5)(1-x^6) + x^{50}(1-x^5)(1-x^6)(1-x^7) + \text{etc.}$$

15. Evoluto secundo membro statuatur denuo

$$D = x^{35} + x^{40} - E$$

eritque

$$E = x^{45} - x^{45}(1-x^5)(1-x^6) - x^{50}(1-x^5)(1-x^6)(1-x^7) - \text{etc.}$$

et evoluto factore secundo $1-x^5$ fiet

$$\begin{aligned} E = {} & x^{45} - x^{45}(1-x^6) - x^{50}(1-x^6)(1-x^7) - x^{55}(1-x^6)(1-x^7)(1-x^8) - \text{etc.} \\ & + x^{50}(1-x^6) + x^{55}(1-x^6)(1-x^7) + x^{60}(1-x^6)(1-x^7)(1-x^8) + \text{etc.} \end{aligned}$$

binisque terminis collectis elicitur

$$E = x^{51} + x^{57}(1-x^6) + x^{63}(1-x^6)(1-x^7) + x^{69}(1-x^6)(1-x^7)(1-x^8) + \text{etc.}$$

16. Inventis igitur his valoribus litterarum A, B, C, D, E etc. si singuli successive substituantur, resultabit ista series

$$1 - x - xx,\ + x^5 + x^7,\ - x^{12} - x^{15},\ + x^{22} + x^{26},\ - x^{35} - x^{40},\ + \text{etc.}$$

Hic autem ordo exponentium facilius perspicitur. Cum enim in valoribus litterarum A, B, C, D, E etc. primo constitutis primi termini simplices essent x^3, x^9, x^{18}, x^{30}, x^{45} etc., exponentes manifesto sunt numeri trigonales triplicati, unde generatim pro numero n erit iste exponens $\frac{3nn+3n}{2}$. Verum hi

termini sequuntur binas potestates ipsius x praecedentes per eandem differentiam n, unde numerum n ab hac formula bis subtrahendo orientur binae potestates in seriem quaesitam ingredientes, quarum exponentes consequenter erunt

$$\frac{3nn+n}{2} \quad \text{et} \quad \frac{3nn-n}{2}.$$

17. Hinc igitur vicissim patet seriem

$$s = 1 - x - xx + x^5 + x^7 - x^{12} - x^{15} + x^{22} + x^{26} - x^{35} - \text{etc.}$$

in infinitum continuatam habere infinitos factores, qui scilicet erunt

$$1 - x, \quad 1 - xx, \quad 1 - x^3, \quad 1 - x^4, \quad 1 - x^5 \quad \text{etc.},$$

ita ut, si primo dividatur per $1 - x$, tum vero quotus per $1 - xx$, iste quotus porro per $1 - x^3$ hocque modo in infinitum divisio continuetur, ultimum quotum resultantem unitati aequalem esse oporteat.

18. Quodsi ergo proposita fuerit ista aequatio in infinitum excurrens

$$1 - x - xx + x^5 + x^7 - x^{12} - x^{15} + x^{22} + x^{26} - x^{35} - \text{etc.} = 0,$$

eius omnes radices facile assignari possunt. Primum enim radix erit $x = 1$, deinde binae radices quadratae ex unitate, tum vero ternae radices cubicae ex unitate, porro quaternae radices biquadratae ex unitate similique modo quinae radices potestatis quintae ex unitate, et ita porro, inter quas igitur ipsa unitas infinities occurrit; at vero -1 ibi reperietur, ubi radix potestatis paris est extrahenda.

DE MIRABILIBUS PROPRIETATIBUS NUMERORUM PENTAGONALIUM

Commentatio 542 indicis Enestroemiani
Acta academiae scientiarum Petropolitanae 1780: I, 1783, p. 56—75

1. Ad classem numerorum pentagonalium non solum eos refero, qui vulgo proprie ita nominari solent et in formula $\frac{3nn-n}{2}$ continentur[1]), sed etiam eos, quos ista formula $\frac{3nn+n}{2}$ suppeditat, ita ut formula generalis omnium horum numerorum sit

$$\frac{3nn \mp n}{2},$$

ex qua igitur nascitur sequens geminata numerorum series, si loco n successive scribantur ordine numeri 0, 1, 2, 3, 4 etc.

n	0,	1,	2,	3,	4,	5,	6
Numeri	0,	1,	5,	12,	22,	35,	51
pentagonales	0,	2,	7,	15,	26,	40,	57

Quilibet scilicet numerus pro n assumtus duos producit numeros, quos hic sibi invicem subscripsi, ita ut series superior contineat numeros pentagonales proprie ita dictos, inferior vero eos, quos hic quoque ad eandem classem refero et qui oriuntur, si superior series retro continuetur. Hic autem binos coniunctim exhibeo, qui ex eodem numero n in formula $\frac{3nn \mp n}{2}$ oriuntur, quoniam in sequentibus eos horum numerorum distinguemus, qui vel ex numeris paribus vel imparibus pro n assumtis nascuntur.

---

1) Vide L. Euler, *Vollständige Anleitung zur Algebra*, St. Petersburg 1770, Erster Theil, dritter Abschnitt, Cap. 5; *Leonhardi Euleri Opera omnia*, series I, vol. 1, p. 159. F. R.

2. Quodsi hos numeros ordine magnitudinis in unam seriem coniiciamus, orietur ista progressio

$$0,\ 1,\ 2,\ 5,\ 7,\ 12,\ 15,\ 22,\ 26,\ 35,\ 40,\ 51,\ 57 \text{ etc.},$$

cuius ordo manifesto est interruptus, quoniam progressio differentiarum hinc fit

$$1,\ 1,\ 3,\ 2,\ 5,\ 3,\ 7,\ 4,\ 9,\ 5,\ 11 \text{ etc.},$$

quae mixta est ex serie numerorum naturalium et imparium. At vero ista series ad continuitatem perduci potest, si post tertium quemque terminum certa fractio interpoletur. Scilicet inter terminos 2 et 5 constituatur $\frac{10}{3}$, tum vero $\frac{28}{3}$ inter 7 et 12, porro $\frac{55}{3}$ inter 15 et 22, ita ut series completa sit

$$1,\ 2,\ \frac{10}{3},\ 5,\ 7,\ \frac{28}{3},\ 12,\ 15,\ \frac{55}{3},\ 22,\ 26 \text{ etc.};$$

sic enim series differentiarum lege continua procedet, dum erit

$$1,\ \frac{4}{3},\ \frac{5}{3},\ 2,\ \frac{7}{3},\ \frac{8}{3},\ 3,\ \frac{10}{3},\ \frac{11}{3},\ 4 \text{ etc.}$$

Manifestum autem est illam seriem oriri, si omnes numeri trigonales per 3 dividantur. Hinc igitur iam pulchra se offert proprietas nostrorum numerorum pentagonalium, quod singuli ter sumti evadant numeri trigonales.

3. Tales autem proprietates, quas immediate ex formulis generalibus derivare licet, etiam in aliis numeris polygonalibus locum habere possunt, ad quas igitur non respicio, cum mihi potius propositum sit quasdam proprietates admirabiles commemorare, quibus numeri pentagonales prae omnibus reliquis polygonalibus sunt praediti. Atque hic occurrit illa insignis horum numerorum proprietas, qua iam olim[1]) ostendi istam numerorum pentagonalium seriem tam arcte cum progressione, quam summae divisorum numerorum

1) Vide imprimis Commentationes 175, 243, 244 (indicis Enestroemiani): *Découverte d'une loi tout extraordinaire des nombres par rapport à la somme de leurs diviseurs*, Bibliothèque impartiale **3**, 1751, p. 10, *Observatio de summis divisorum*, Novi comment. acad. sc. Petrop. **5** (1754/5), 1760, p. 59, *Demonstratio theorematis circa ordinem in summis divisorum observatum*, ibidem p. 75; *Leonhardi Euleri Opera omnia*, series I, vol. 2, p. 241, 373, 390. F. R.

naturalium constituunt, esse connexam, ut eius ope adeo lex istius seriei maxime irregularis assignari possit, id quod breviter repetere operae pretium erit.

4. Quodsi quilibet numerus N cum suis divisoribus in unam summam colligatur, quam summam hoc charactere $\int N$ indicemus, ex numeris naturalibus sequens nascetur series primo intuitu maxime irregularis

N	1,	2,	3,	4,	5,	6,	7,	8,	9,	10,	11
$\int N$	1,	3,	4,	7,	6,	12,	8,	15,	13,	18,	12

ubi termini tam inordinate progrediuntur, dum modo crescunt modo decrescunt, ut vix quisquam eorum legem detegat, quandoquidem ista series ordinem numerorum primorum manifesto in se involvit.

5. Interim tamen demonstravi istam progressionem quantumvis irregularem ad classem serierum recurrentium esse referendam et singulos eius terminos secundum certam legem ex praecedentibus determinari posse. Quodsi enim $\int N$ denotet summam omnium divisorum huius numeri N ipso non excepto, inveni semper fore

$$\int N = \int(N-1) + \int(N-2) - \int(N-5) - \int(N-7) + \int(N-12) + \int(N-15) - \int(N-22) - \int(N-26) + \text{etc.},$$

ubi numeri, qui successive ab N subtrahuntur, constituunt manifesto nostram seriem numerorum pentagonalium

$$1, 2, 5, 7, 12, 15, 22, 26, 35, 40 \text{ etc.},$$

ita ut termini ex numeris imparibus pro n assumtis oriundi habeant signum $+$, qui vero ex paribus nascuntur, signum $-$. Tum vero quovis casu has formulas eousque continuari oportet, quoad numeri post signum $\int$ scripti non evadant negativi; at si occurrat formula $\int(N-N)$, eius loco scribi debet ipse numerus N. Ita si sumamus $N = 12$, erit

$$\int 12 = \int 11 + \int 10 - \int 7 - \int 5 + \int 0$$

ideoque erit

$$\int 12 = 12 + 18 - 8 - 6 + 12 = 28.$$

At vero si sumamus $N = 13$, erit

$$\int 13 = \int 12 + \int 11 - \int 8 - \int 6 + \int 1$$

sive erit

$$\int 13 = 28 + 12 - 15 - 12 + 1 = 14.$$

6. Quoniam igitur ordo, quo summae divisorum progrediuntur, merito maxime irregularis videtur, nemini certe in mentem venire potuit eum per numeros pentagonales explorari potuisse, ex quo ista speculatio utique maxime est admiranda. Afferam autem adhuc aliam eiusmodi proprietatem, quae quidem cum exposita arctissime est connexa, attamen ad plures non minus admirandas proprietates perducit, quae omnes pariter in natura numerorum nostrorum pentagonalium sunt fundatae.

7. Fundamentum autem omnium harum mirabilium proprietatum in evolutione huius producti infiniti

$$S = (1 - x)(1 - xx)(1 - x^3)(1 - x^4)(1 - x^5)(1 - x^6)(1 - x^7) \text{ etc.}$$

continetur. Demonstravi[1]) enim, si singuli hi factores actu in se invicem multiplicentur, tum denique resultare istam seriem

$$S = 1 - x^1 - x^2 + x^5 + x^7 - x^{12} - x^{15} + x^{22} + x^{26} - \text{etc.},$$

ubi exponentes ipsius x constituunt nostram seriem numerorum pentagonalium; ratione signorum autem + et — ambo alternatim geminantur, ita ut, qui exponentes ex numeris paribus pro n assumtis oriuntur, eae potestates habeant signum +, reliqui vero ex imparibus orti signum —. Haec igitur non minus admirationem nostram meretur quam proprietas ante commemorata, cum nulla certe appareat ratio, unde ullus nexus intelligi possit inter evolutionem illius producti et nostros numeros pentagonales.

8. Cum igitur series ista potestatum ipsius x aequalis sit producto illi infinito, si eam nihilo aequalem statuamus, ut habeamus hanc aequationem

$$0 = 1 - x^1 - x^2 + x^5 + x^7 - x^{12} - x^{15} + x^{22} + x^{26} - \text{etc.},$$

1) Vide Commentationem praecedentem atque Commentationem 244 nota p. 481 laudatam.

ea omnes easdem involvet radices, quas productum illud nihilo aequatum includit. Ex primo scilicet factore $1 - x$ erit

$$x = 1;$$

ex secundo factore $1 - xx$ erit

$$\text{vel } x = +1 \text{ vel } x = -1;$$

ex tertio factore $1 - x^3$ nascuntur hae tres radices

$$1)\ x = 1, \quad 2)\ x = \frac{-1+\sqrt{-3}}{2}, \quad 3)\ x = \frac{-1-\sqrt{-3}}{2};$$

ex quarto autem factore $1 - x^4 = 0$ oriuntur hae quatuor radices

$$1)\ x = +1, \quad 2)\ x = -1, \quad 3)\ x = +\sqrt{-1} \text{ et } 4)\ x = -\sqrt{-1};$$

quintus autem factor $1 - x^5 = 0$ suppeditat has quinque radices[1])

$$1)\ x = 1,$$

$$2)\ x = \frac{-1-\sqrt{5}+\sqrt{(-10+2\sqrt{5})}}{4}, \quad 3)\ x = \frac{-1-\sqrt{5}-\sqrt{(-10+2\sqrt{5})}}{4},$$

$$4)\ x = \frac{-1+\sqrt{5}+\sqrt{(-10-2\sqrt{5})}}{4}, \quad 5)\ x = \frac{-1+\sqrt{5}-\sqrt{(-10-2\sqrt{5})}}{4};$$

sextus autem factor $[1 - x^6 = 0]$ praebet has sex radices

$$1)\ x = 1, \quad 2)\ x = -1,$$

$$3)\ x = \frac{+1+\sqrt{-3}}{2}, \quad 4)\ x = \frac{+1-\sqrt{-3}}{2},$$

$$5)\ x = \frac{-1+\sqrt{-3}}{2}, \quad 6)\ x = \frac{-1-\sqrt{-3}}{2};$$

etc.

9. Hinc igitur patet omnes radices cuiuscumque potestatis ex unitate simul esse radices nostrae aequationis. Ac si rem in genere consideremus

1) Vide L. Euler, *Vollständige Anleitung zur Algebra*, St. Petersburg 1770, Zweyter Theil, erster Abschnitt, Cap. 13, § 200; *Leonhardi Euleri Opera omnia*, series I, vol. 1, p. 300. F. R.

ponendo $1 - x^n = 0$, primo patet unam radicem semper esse $x = 1$, ac si n fuerit numerus par, aliam radicem fore $x = -1$. Pro reliquis autem radicibus considerari debent factores trinomiales formulae $1 - x^n$, qui, uti alibi[1]) satis est expositum, in hac forma generali continentur

$$1 - 2x \cos. \frac{2i\pi}{n} + xx$$

sumendo pro i successive omnes numeros integros ipso $\frac{1}{2}n$ non maiores. Hoc autem factore nihilo aequato eruuntur istae duae radices

$$x = \cos. \frac{2i\pi}{n} + \sqrt{-1} \cdot \sin. \frac{2i\pi}{n}$$

et

$$x = \cos. \frac{2i\pi}{n} - \sqrt{-1} \cdot \sin. \frac{2i\pi}{n}$$

Hinc enim vicissim fit

$$x^n = \cos. 2i\pi \pm \sqrt{-1} \cdot \sin. 2i\pi.$$

Est autem $\cos. 2i\pi = 1$ et $\sin. 2i\pi = 0$ ideoque $x^n = 1$; unde si pro n et i successive omnes numeri integri accipiantur, haec forma

$$x = \cos. \frac{2i\pi}{n} \pm \sqrt{-1} \cdot \sin. \frac{2i\pi}{n}$$

praebebit omnes radices nostrae aequationis

$$0 = 1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + x^{22} + x^{26} - \text{etc.},$$

ita ut istius aequationis omnes plane radices assignare valeamus.

10. Quodsi ergo omnes radices istius aequationis litteris α, β, γ, δ, ε etc. indicemus, eius factores erunt

$$1 - \frac{x}{\alpha}, \quad 1 - \frac{x}{\beta}, \quad 1 - \frac{x}{\gamma}, \quad 1 - \frac{x}{\delta} \quad \text{etc.},$$

unde ex natura aequationum colligimus fore summam omnium harum fractionum

$$\frac{1}{\alpha} + \frac{1}{\beta} + \frac{1}{\gamma} + \frac{1}{\delta} + \text{etc.} = 1,$$

1) Vide exempli gratia L. Euleri *Introductionem in analysin infinitorum*, Lausannae 1784, t. I cap. IX; *Leonhardi Euleri Opera omnia*, series I, vol. 8. F. R.

summam vero productorum ex binis $= -1$, tum vero summam productorum ex ternis $= 0$, summam productorum ex quaternis $= 0$, summam productorum ex quinis $= -1$, summam productorum ex senis $= 0$, summam productorum ex septenis $= -1$ etc. Hinc autem porro concludimus[1]) fore summam quadratorum illarum fractionum, scilicet

$$\frac{1}{\alpha^2} + \frac{1}{\beta^2} + \frac{1}{\gamma^2} + \frac{1}{\delta^2} + \text{etc.} = 3,$$

summam cuborum

$$\frac{1}{\alpha^3} + \frac{1}{\beta^3} + \frac{1}{\gamma^3} + \frac{1}{\delta^3} + \text{etc.} = 4,$$

summam biquadratorum

$$\frac{1}{\alpha^4} + \frac{1}{\beta^4} + \frac{1}{\gamma^4} + \frac{1}{\delta^4} + \text{etc.} = 7,$$

et ita porro, ubi quidem nullus ordo perspicitur.

11. Quod autem hic de fractionibus $\frac{1}{\alpha}$, $\frac{1}{\beta}$, $\frac{1}{\gamma}$ etc. diximus, etiam de ipsis radicibus α, β, γ etc. valet. Si enim α fuerit radix nostrae aequationis, per ea, quae ostendimus, haec radix continetur in hac formula

$$\cos.\frac{2i\pi}{n} \pm \sqrt{-1}\cdot\sin.\frac{2i\pi}{n}.$$

Hinc autem fit

$$\frac{1}{\alpha} = \frac{1}{\cos.\frac{2i\pi}{n} \pm \sqrt{-1}\cdot\sin.\frac{2i\pi}{n}} = \cos.\frac{2i\pi}{n} \mp \sqrt{-1}\cdot\sin.\frac{2i\pi}{n},$$

quae itidem est radix nostrae aequationis; unde patet, si $\frac{1}{\alpha}$ fuerit radix nostrae aequationis, etiam α fore radicem.

12. Denotet igitur α radicem quamcumque aequationis $1 - x^n = 0$, quandoquidem tum etiam erit radix nostrae aequationis

$$1 - x - xx + x^5 + x^7 - x^{12} - x^{15} + \text{etc.} = 0;$$

1) Vide L. Euleri Commentationem 153 (indicis Enestroemiani): *Demonstratio gemina theorematis Neutoniani, quo traditur relatio inter coefficientes cuiusvis aequationis algebraicae et summas potestatum radicum eiusdem*, Opuscula varii argumenti 2, 1750, p. 108; *Leonhardi Euleri Opera omnia* series I, vol. 6. F. R.

tum igitur erit $\alpha^n = 1$. Praeterea vero etiam omnes potestates ipsius α radices simul erunt aequationis $1 - x^n = 0$. Si enim loco x scribamus $\alpha\alpha$, fiet

$$1 - x^n = 1 - \alpha^{2n}.$$

Cum autem sit $\alpha^n = 1$, patet etiam fore $\alpha^{2n} = 1$ ideoque $1 - \alpha^{2n} = 0$, quod idem manifestum est de cubo α^3 et omnibus potestatibus altioribus. Hinc igitur sequitur fore

$$\alpha^{n+1} = \alpha \quad \text{et} \quad \alpha^{n+2} = \alpha\alpha \quad \text{et} \quad \alpha^{n+3} = \alpha^3.$$

Sicque in genere erit $\alpha^{in+\lambda} = \alpha^\lambda$.

13. Si igitur α denotet radicem quamcumque nostrae aequationis, ita ut sit $\alpha^n = 1$, si in ea loco x scribamus α, certe evadet haec series

$$1 - \alpha^1 - \alpha^2 + \alpha^5 + \alpha^7 - \alpha^{12} - \alpha^{15} + \alpha^{22} + \text{etc.} = 0.$$

Praeterea vero etiam ponendo $x = \alpha\alpha$ erit

$$1 - \alpha^2 - \alpha^4 + \alpha^{10} + \alpha^{14} - \alpha^{24} - \alpha^{30} + \alpha^{44} + \text{etc.} = 0,$$

et in genere si loco x scribamus α^i denotante i numerum quemcumque integrum, etiam fiet

$$1 - \alpha^i - \alpha^{2i} + \alpha^{5i} + \alpha^{7i} - \alpha^{12i} - \alpha^{15i} + \alpha^{22i} + \text{etc.} = 0.$$

Atque hoc etiam valebit, si pro i numeri negativi accipiantur, siquidem ostendimus radices quoque esse $\frac{1}{\alpha^2}$, $\frac{1}{\alpha^3}$, $\frac{1}{\alpha^4}$, $\frac{1}{\alpha^5}$ etc.

14. Quoniam hic assumsimus α esse radicem aequationis $1 - x^n = 0$, percurramus ordine casus, quibus est n vel 1 vel 2 vel 3 vel 4 etc. Ac primo quidem, si $n = 1$, necessario est $\alpha = 1$, quo valore substituto nostra aequatio generalis induet hanc formam

$$1 - 1 - 1 + 1 + 1 - 1 - 1 + 1 + \text{etc.},$$

quae series manifesto ex infinitis periodis[1]) conflatur, quarum singulae conti-

1) Vide D. Bernoulli, *De summationibus serierum quarundam incongrue veris earumque interpretatione atque usu*, Novi comment. acad. sc. Petrop. 16 (1771), 1772, p. 71. F. R.

nent hos terminos $1-1-1+1$; unde cuiusque periodi valor est $=0$ ideoque etiam infinitae periodi simul sumtae summam habebunt $=0$. Quoniam autem continuata concipi debet, si percursis iam infinitis periodis insuper unus terminus accedat, summa erit [$=1$, si duo accedant, summa erit] $=0$, si tres accedant, summa erit $=-1$, et si quatuor accedant, $=0$, quo casu tota periodus est adiecta; quare, cum numerus infinitus nusquam terminetur, summa seriei infinitae medium tenebit inter quatuor summas modo memoratas 1, 0, -1, 0, quod medium reperitur, si aggregatum harum quatuor summarum per numerum, hoc est per quaternarium, dividatur; tum autem manifesto prodit 0, quae ergo vera censenda est summa nostrae seriei.

15. Simile scilicet ratiocinium hic adhiberi potest, quo vulgo ostendi solet summam seriei LEIBNIZIANAE[1]) $1-1+1-1+1-1+1-1+$ etc. esse $=\frac{1}{2}$; hoc autem concesso veritas praesentis asserti sponte elucet. Cum enim sit

$$1-1+1-1+1-1+\text{etc.}=\frac{1}{2},$$

erit

$$-1+1-1+1-1+1-1+\text{etc.}=-\frac{1}{2};$$

ergo combinandis his duabus seriebus erit

$$1-1-1+1+1-1-1+1+1-1-\text{etc.}=0.$$

16. Consideremus nunc casum, quo $n=2$ et $\alpha\alpha=1$, ubi quidem est α vel $+1$ vel -1. Retineamus autem litteram α pro utravis earum designanda, et cum sit

$$\alpha^3=\alpha,\quad \alpha^4=1,\quad \alpha^5=\alpha,\quad \alpha^6=1\quad \text{etc.},$$

facta substitutione nostra aequatio generalis hanc induet formam

$$1-\alpha-1+\alpha+\alpha-1-\alpha+1\,|+1-\alpha-1+\alpha+\alpha-1-\alpha+1\,|+\text{etc.},$$

quae series pariter per certas periodos progreditur, quae continuo replicantur, atque unaquaeque earum constat ex his octo terminis

$$1-\alpha-1+\alpha+\alpha-1-\alpha+1,$$

1) Vide M. CANTOR, *Vorlesungen über Geschichte der Mathematik*, 3. Bd., 2. Aufl., Leipzig 1901, p. 365–367. F. R.

quorum summa est 0, sicque numerus quantumvis magnus talium integrarum periodorum certe evanescit. At si vero insuper unus vel duo vel tres vel adeo octo termini accedant, summae sequenti modo se habebunt:

Si insuper accedat	summa erit
unus terminus	1
duo termini	$1-\alpha$
tres termini	$-\alpha$
quatuor termini	0
quinque termini	α
sex termini	$\alpha-1$
septem termini	-1
octo termini	0

Quarum octo summarum aggregatum est 0, unde tuto concludimus totius huius seriei, quam invenimus, in infinitum continuatae summam esse $= 0$.

17. Hinc patet summam huius seriei periodicae perinde nihilo aequari, quemcumque valorem habuerit littera α; verus enim valor ipsius α, quo est $\alpha\alpha = 1$, iam in considerationem est ductus, dum ipsae periodi ex eo sunt natae; quamobrem haec series in duas partes dispesci potest, quarum altera contineat solas unitates, altera vero solas litteras α; ac necesse est, ut utriusque summa seorsim nihilo fiat aequalis, ita ut sit

$$1-1-1+1,\ +1-1-1+1,\ +1-1-1+1,\ +\text{etc.} = 0,$$
$$-\alpha+\alpha+\alpha-\alpha,\ -\alpha+\alpha+\alpha-\alpha,\ -\alpha+\alpha+\alpha-\alpha,\ -\text{etc.} = 0;$$

utriusque autem veritas ex positis principiis fit manifesta.

18. Simili modo res se habebit in radicibus cubicis ipsius 1 ponendo $\alpha^3 = 1$, et quoniam periodi ad plures terminos excurrent, seriem generalem per binos terminos sibi subscriptos referamus, ut sit in genere

$$\left.\begin{aligned} 1-\alpha\ &+\alpha^5-\alpha^{12}+\alpha^{22}-\alpha^{35}+\text{etc.} \\ -\alpha^2\ &+\alpha^7-\alpha^{15}+\alpha^{26}-\alpha^{40}+\text{etc.} \end{aligned}\right\} = 0.$$

Quodsi iam sumatur $\alpha^3 = 1$, ut sit

$$\alpha^4 = \alpha, \quad \alpha^5 = \alpha^2, \quad \alpha^6 = 1, \quad \alpha^7 = \alpha \quad \text{etc.},$$

prodibit sequens progressio periodica

$$\begin{array}{l} 1 - \alpha + \alpha^2 - 1 + \alpha - \alpha^2 + 1 \left| - \alpha + \alpha^2 - 1 + \alpha - \alpha^2 + 1 \right| \\ \quad - \alpha^2 + \alpha - 1 + \alpha^2 - \alpha \left| + 1 - \alpha^2 + \alpha - 1 + \alpha^2 - \alpha \right| + 1 \end{array} \text{ etc.}$$

nihilo aequalis, ubi quaelibet periodus constat duodecim terminis triplicis generis, scilicet 1, α, α^2. Ac facile apparet terminos cuiusque generis seorsim sumtos seriem exhibere nihilo aequalem; unitates enim constituunt hanc seriem

$$+1 -1 -1 +1, \quad +1 -1 -1 +1, \quad +1 -1 -1 +1, \quad + \text{etc.} = 0,$$

litterae vero α et $\alpha\alpha$ constituunt sequentes series

$$\begin{array}{l} -\alpha + \alpha + \alpha - \alpha, \quad -\alpha + \alpha + \alpha - \alpha, \quad -\alpha + \alpha + \alpha - \alpha, \quad + \text{etc.} = 0, \\ -\alpha^2 + \alpha^2 + \alpha^2 - \alpha^2, \quad -\alpha^2 + \alpha^2 + \alpha^2 - \alpha^2, \quad -\alpha^2 + \alpha^2 + \alpha^2 - \alpha^2, \quad + \text{etc.} = 0. \end{array}$$

Harum autem singularum summas nihilo aequales esse manifestum est.

19. Consideremus porro etiam radices biquadratas unitatis sitque $\alpha^4 = 1$ ac prodibit sequens series periodica

$$\begin{array}{l} 1 - \alpha + \alpha - 1 + \alpha^2 - \alpha^3 + \alpha^3 - \alpha^2 + 1 \left| - \alpha + \alpha - 1 \right. \\ \quad - \alpha^2 + \alpha^3 - \alpha^3 + \alpha^2 - 1 + \alpha - \alpha \left| + 1 - \alpha^2 + \alpha^3 - \alpha^3 \right. \end{array} \text{ etc.},$$

ubi singulae periodi constant ex sedecim terminis, qui ad quatuor genera relati praebent sequentes quatuor series singulas nihilo aequales

$$\begin{array}{l} +1 -1 -1 +1, \quad +1 -1 -1 +1, \quad +1 -1 -1 +1, \quad + \text{etc.} = 0, \\ -\alpha + \alpha + \alpha - \alpha, \quad -\alpha + \alpha + \alpha - \alpha, \quad -\alpha + \alpha + \alpha - \alpha, \quad + \text{etc.} = 0, \\ -\alpha^2 + \alpha^2 + \alpha^2 - \alpha^2, \quad -\alpha^2 + \alpha^2 + \alpha^2 - \alpha^2, \quad -\alpha^2 + \alpha^2 + \alpha^2 - \alpha^2, \quad + \text{etc.} = 0, \\ +\alpha^3 - \alpha^3 - \alpha^3 + \alpha^3, \quad +\alpha^3 - \alpha^3 - \alpha^3 + \alpha^3, \quad +\alpha^3 - \alpha^3 - \alpha^3 + \alpha^3, \quad + \text{etc.} = 0. \end{array}$$

20. Quamquam hinc nostra conclusio pro radicibus altioribus iam satis est confirmata, tamen necesse est insuper casum, quo $\alpha^5 = 1$, evolvere, quandoquidem hic non omnes potestates quinta inferiores occurrent. Sit igitur $\alpha^5 = 1$

et haec series periodica prodibit

$$\begin{array}{l} 1-\alpha\ +1\ -\alpha^2+\alpha^2-1+\alpha\ -1\ +\alpha^2-\alpha^2+1\ |-\alpha\ +1 \\ \quad -\alpha^2+\alpha^2-1\ +\alpha\ -1+\alpha^2-\alpha^2+1\ -\alpha|+1-\alpha^2+\alpha^2 \end{array} \text{ etc.,}$$

ubi potestates α^3 et α^4 penitus excluduntur. Quare, cum quaelibet periodus viginti constet terminis, reliquae potestates saepius occurrant necesse est; singulis autem seorsim sumtis tres sequentes series periodicae occurrunt

$$+1+1-1-1\ -1-1+1+1,\ +1+1-1-1-1-1+1+1,\ +\text{etc.}=0,$$
$$-\alpha+\alpha+\alpha-\alpha,-\alpha+\alpha+\alpha-\alpha,\ -\alpha+\alpha+\alpha-\alpha,-\alpha+\alpha+\alpha-\alpha,\ -\text{etc.}=0,$$
$$-\alpha^2+\alpha^2-\alpha^2+\alpha^2+\alpha^2-\alpha^2+\alpha^2-\alpha^2,-\alpha^2+\alpha^2-\alpha^2+\alpha^2+\alpha^2-\alpha^2+\alpha^2-\alpha^2,-\text{etc.}=0.$$

Hinc iam veritas seriei ipsarum α ex praecedentibus est manifesta; binae reliquae autem, quarum periodi octo terminis constant, si secundum principia hactenus stabilita examinentur, etiam nihilo aequales deprehendentur, quoniam non solum termini solius periodi se mutuo destruunt, sed etiam termini seriei summatricis inde formatae. Ita ex serie unitatum oritur haec series summatrix

$$1,\ 2,\ 1,\ 0,\ -1,\ -2,\ -1,\ 0,$$

cuius summa itidem evanescit; quod idem usu venit in serie quadratorum.

21. Ex his iam abunde patet eandem proprietatem etiam in radicibus altioribus locum esse habituram, ex quotcumque etiam terminis singulae periodi fuerint compositae; quod certe eo magis est mirandum, cum ista proprietas in nullas alias series potestatum competere possit atque penitus propria sit seriei numerorum pentagonalium.

22. Ut autem rem in genere ob oculos ponamus, sit $\alpha^n = 1$, unde nascuntur periodi ex $4n$ terminis constantes, qui erunt vel 1 vel α vel α^2 vel α^3 etc. Plerumque autem non omnes potestates inferiores quam α^n occurrent, unde periodi singularum potestatum ipsius α plerumque pluribus quam quatuor terminis constabunt. Semper autem non solum ipsi termini cuiusque periodi se mutuo destruent, sed etiam termini seriei summatricis. Ita si consideremus potestates α^r existente r numero minore quam n, ex serie nostra numerorum pentagonalium omnes excerpantur termini, qui per n divisi hoc idem residuum

r relinquant. Ac si cuique horum terminorum suum debitum signum praefigatur, talis prodibit series

$$\pm\alpha^r \pm \alpha^r \pm \alpha^r \pm \alpha^r \pm \alpha^r \pm \alpha^r \pm \alpha^r \pm \alpha^r \pm \text{etc.},$$

quae semper ex certis periodis ratione signorum + et — constabit idque ita, ut cuiusque periodi omnes termini simul sumti se mutuo destruant atque idem etiam in serie summatrice eveniat.

23. Verum hae proprietates hactenus commemoratae insuper innumerabiles alias non minus admirandas post se trahunt. Si enim α fuerit radix cuiusque potestatis n ex unitate, ita ut $1 - \frac{x}{\alpha}$ sit factor formulae $1 - x^n$, evidens est eum etiam fore factorem formularum $1 - x^{2n}$, $1 - x^{3n}$, $1 - x^{4n}$ etc. in infinitum. Quare, cum hae formulae omnes sint factores nostrae progressionis

$$1 - x - xx + x^5 + x^7 - x^{12} - \text{etc.},$$

eadem radix α in hac aequatione non tantum semel, sed adeo infinities occurrit, ita ut ista aequatio infinitas habeat radices ipsi α aequales.

24. Novimus autem ex natura aequationum, si aequatio quaecumque

$$1 + Ax + Bxx + Cx^3 + Dx^4 + \text{etc.} = 0$$

habeat duas radices aequales α, tum etiam α fore radicem aequationis per differentiationem natae, scilicet

$$A + 2Bx + 3Cxx + 4Dx^3 + \text{etc.} = 0,$$

ac si habeat tres radices aequales α, tum insuper α quoque erit radix istius aequationis per differentiationem natae, postquam scilicet illam aequationem differentialem per x multiplicaverimus,

$$1^2A + 2^2Bx + 3^2Cxx + 4^2Dx^3 + \text{etc.} = 0;$$

unde si haec aequatio habuerit λ radices aequales, quae singulae sint $= \alpha$, semper erit

$$1^\lambda A + 2^\lambda B\alpha + 3^\lambda C\alpha\alpha + 4^\lambda D\alpha^3 + \text{etc.} = 0;$$

unde si uniformitatis gratia hanc aequationem per α multiplicemus, erit quoque

$$1^\lambda A\alpha + 2^\lambda B\alpha^2 + 3^\lambda C\alpha^3 + 4^\lambda D\alpha^4 + \text{etc.} = 0.$$

25. Cum igitur posito $\alpha^n = 1$ nostra aequatio ex numeris pentagonalibus formata

$$1 - x^1 - x^2 + x^5 + x^7 - x^{12} - x^{15} + \text{etc.} = 0$$

habeat infinitas radices ipsi α aequales, erit quoque α radix omnium aequationum in hac forma generali contentarum

$$-1^\lambda x - 2^\lambda x^2 + 5^\lambda x^5 + 7^\lambda x^7 - 12^\lambda x^{12} - 15^\lambda x^{15} + \text{etc.} = 0,$$

quicumque numerus integer pro λ accipiatur. Semper igitur erit

$$-1^\lambda \alpha - 2^\lambda \alpha^2 + 5^\lambda \alpha^5 + 7^\lambda \alpha^7 - 12^\lambda \alpha^{12} - 15^\lambda \alpha^{15} + \text{etc.} = 0.$$

26. Ad hoc clarius ostendendum sumamus $\alpha = 1$ eritque semper

$$-1^\lambda - 2^\lambda + 5^\lambda + 7^\lambda - 12^\lambda - 15^\lambda + \text{etc.} = 0;$$

ac pro casu $\lambda = 0$ veritatem istius aequationis iam probavimus. Sit igitur $\lambda = 1$ et monstrandum erit huius seriei divergentis infinitae

$$-1 - 2 + 5 + 7 - 12 - 15 + 22 + 26 - \text{etc.}$$

summam esse $= 0$. Quoniam autem haec series est interrupta seu potius ex duabus seriebus mixta, utramque seorsim contemplemur ponendo

$$s = -1 + 5 - 12 + 22 - 35 + \text{etc.}$$

et

$$t = -2 + 7 - 15 + 26 - 40 + \text{etc.}$$

atque ostendi oportet fore $s + t = 0$.

27. Ex doctrina autem serierum, quae signis alternantibus procedunt, veluti $A - B + C - D + \text{etc.}$, constat huius seriei in infinitum progredientis summam esse

$$= \frac{1}{2}A - \frac{1}{4}(B - A) + \frac{1}{8}(C - 2B + A) - \frac{1}{16}(D - 3C + 3B - A) + \text{etc.},$$

quae regula ita commodius per differentias exponitur, scilicet ratione signorum seposita. Ex serie numerorum A, B, C, D, E etc. formetur series differentiarum, dum quilibet terminus illius seriei a sequente subtrahitur, quae sit a, b, c, d, e etc. Eadem porro lege ex hac serie differentiarum formetur series secundarum differentiarum, quae sit a', b', c', d', e' etc., ex hac porro series tertiarum differentiarum, quae sit a'', b'', c'', d'', e'' etc., atque hoc modo ulterius, donec ad differentias constantes perveniatur. Tum autem ex terminis primis omnium harum serierum summa seriei propositae ita determinatur, ut ea sit

$$\frac{1}{2}A - \frac{1}{4}a + \frac{1}{8}a' - \frac{1}{16}a'' + \frac{1}{32}a''' - \frac{1}{64}a'''' + \text{etc.}$$

28. Hac regula stabilita cum signis mutatis sit

$$-s = 1 - 5 + 12 - 22 + 35 - 51 + 70 - \text{etc.}$$

et

$$-t = 2 - 7 + 15 - 26 + 40 - 57 + 77 - \text{etc.},$$

hi termini sequenti modo disponantur ac differentiae subscribantur:

1, 5, 12, 22, 35, 51, 70 etc.	2, 7, 15, 26, 40, 57, 77 etc.
4, 7, 10, 13, 16, 19	5, 8, 11, 14, 17, 20
3, 3, 3, 3, 3	3, 3, 3, 3, 3
0, 0, 0, 0	0, 0, 0, 0

Hinc igitur colligitur fore

$$-s = \frac{1}{2} - \frac{4}{4} + \frac{3}{8} = -\frac{1}{8} \quad \text{sive} \quad s = +\frac{1}{8},$$

porro

$$-t = \frac{2}{2} - \frac{5}{4} + \frac{3}{8} = +\frac{1}{8} \quad \text{sive} \quad t = -\frac{1}{8},$$

unde manifesto conficitur esse $s + t = 0$.

29. Quamquam ipsae rationes, quibus hae proprietates innituntur, nullum plane dubium relinquunt, tamen haud inutile erit istam veritatem etiam pro casu $\lambda = 2$ ostendisse sive revera esse

$$-1^2 - 2^2 + 5^2 + 7^2 - 12^2 - 15^2 + 22^2 + \text{etc.} = 0.$$

Discerpatur enim haec series itidem in duas, quae sint mutatis signis

$$s = 1^2 - 5^2 + 12^2 - 22^2 + 35^2 - 51^2 + \text{etc.},$$
$$t = 2^2 - 7^2 + 15^2 - 26^2 + 40^2 - 57^2 + \text{etc.},$$

ac pro prioris summa invenienda instituatur sequens operatio:

Series	1,	25,	144,	484,	1225,	2601, 4900
Diff. I.		24,	119,	340,	741,	1376, 2299
Diff. II.			95,	221,	401,	635, 923
Diff. III.				126,	180,	234, 288
Diff. IV.					54,	54, 54
Diff. V.						0, 0

Hinc igitur erit

$$s = \frac{1}{2} - \frac{24}{4} + \frac{95}{8} - \frac{126}{16} + \frac{54}{32} = + \frac{3}{16}.$$

Simili modo pro altera serie:

Series	4,	49,	225,	676,	1600,	3249, 5929
Diff. I.		45,	176,	451,	924,	1649, 2680
Diff. II.			131,	275,	473,	725, 1031
Diff. III.				144,	198,	252, 306
Diff. IV.					54,	54, 54
Diff. V.						0, 0

Hinc concluditur

$$t = \frac{4}{2} - \frac{45}{4} + \frac{131}{8} - \frac{144}{16} + \frac{54}{32} = - \frac{3}{16}.$$

Quamobrem evictum est totam summam fore $s + t = 0$.

30. Consideremus nunc etiam radices quadratas sive sit $\alpha^2 = 1$ hincque orietur ista series

$$-1^\lambda\alpha - 2^\lambda + 5^\lambda\alpha + 7^\lambda\alpha - 12^\lambda - 15^\lambda\alpha + 22^\lambda + 26^\lambda - \text{etc.} = 0,$$

unde, si terminos unitatem et α continentes a se invicem separemus, binas obtinebimus series nihilo aequales, scilicet

$$-2^\lambda - 12^\lambda + 22^\lambda + 26^\lambda - 40^\lambda - 70^\lambda + 92^\lambda + \text{etc.} = 0$$

et

$$-1^\lambda\alpha + 5^\lambda\alpha + 7^\lambda\alpha - 15^\lambda\alpha - 35^\lambda\alpha + 51^\lambda\alpha + 57^\lambda\alpha - \text{etc.} = 0.$$

Quodsi vero harum serierum veritatem eodem modo, quo ante sumus usi, ostendere vellemus, unamquamque in quatuor alias series discerpi oporteret, ut scilicet tandem ad differentias constantes perveniremus. At vero si quis hanc operam suscipere voluerit, certus esse poterit aggregatum omnium summarum partialium fore $= 0$.

31. Nunc generalissime totum negotium complectamur sitque $\alpha^n = 1$ et quaeramus seriem, quae contineat tantum postestates α^r. Hunc in finem ex omnibus nostris numeris pentagonalibus excerpamus eos, qui per n divisi relinquunt idem residuum r. Sint igitur isti numeri pentagonales

$$A,\ B,\ C,\ D,\ E \text{ etc.},$$

omnes scilicet formae $\gamma n + r$, et cuiusque signum $\pm$, quod ipsi convenit, sollicite notetur. Tum autem semper erit

$$\pm A^\lambda \pm B^\lambda \pm C^\lambda \pm D^\lambda \pm E^\lambda \pm \text{etc.} = 0,$$

quicumque valor integer exponenti λ tribuatur. Atque in hac forma generalissima omnes series, quas hactenus eruimus et quarum summas nihilo aequari ostendimus, continentur.

OBSERVATIONES CIRCA DIVISIONEM QUADRATORUM PER NUMEROS PRIMOS[1])

Commentatio 552 indicis ENESTROEMIANI
Opuscula analytica 1, 1783, p. 64—84

HYPOTHESIS

1. *Si numerorum* a, b, c, d *etc. quadrata* a^2, b^2, c^2, d^2 *etc. per numerum quempiam primum* P *dividantur, residua in divisione relicta litteris cognominibus graecis* α, β, γ, δ *etc. indicemus.*

COROLLARIUM 1

2. Cum ergo quadratum aa per numerum P divisum relinquat residuum α, posito quoto $= A$ erit $aa = AP + \alpha$ ideoque $aa - \alpha$ divisibile erit per P; similique modo hae expressiones $bb - \beta$, $cc - \gamma$, $dd - \delta$ etc. divisibiles erunt per eundem divisorem P.

COROLLARIUM 2

3. Quadrata $(a + P)^2$, $(a + 2P)^2$, $(a + 3P)^2$ et in genere $(a + nP)^2$ idem residuum α relinquent, si per numerum propositum P dividantur. Unde patet numerorum divisore P maiorum quadrata eadem praebere residua, quae ex quadratis numerorum divisore P minorum nascuntur.

---

1) Fundamenta theoriae residuorum quadraticorum, quae hac in dissertatione continentur, ab EULERO iam exposita sunt in Commentatione 242 (indicis ENESTROEMIANI): *Demonstratio theorematis FERMATIANI omnem numerum sive integrum sive fractum esse summam quatuor pauciorumve quadratorum,* Novi comment. acad. sc. Petrop. 5 (1754/5), 1760, p. 13; *LEONHARDI EUERI Opera omnia*, series I, vol. 2, p. 338. F. R.

COROLLARIUM 3

4. Cum deinde quadratum $(P-a)^2$ per P divisum idem praebeat residuum, quod quadratum a^2, patet, si fuerit $a > \frac{1}{2}P$, fore $P-a < \frac{1}{2}P$. Unde manifestum est omnia residua diversa ex quadratis numerorum, qui semisse divisoris P sint minores, resultare.

COROLLARIUM 4

5. Quare si omnia residua desiderentur, quae ex divisione quadratorum per datum divisorem P proveniunt, sufficiet ea tantum quadrata considerasse, quorum radices semissem ipsius P non superent.

COROLLARIUM 5

6. Hinc si divisor sit $P = 2p+1$, si per eum omnes numeri quadrati 1, 4, 9, 16, 25 etc. dividantur, plura residua diversa inde prodire nequeunt, quam unitates in numero p continentur, eaque resultant ex quadratis numerorum 1, 2, 3, 4, ... p; sequentium enim numerorum $p+1$, $p+2$, $p+3$ etc. quadrata eadem residua ordine retrogrado reproducunt.

SCHOLION

7. Manifestum hoc inde est, quod haec duo quadrata p^2 et $(p+1)^2$ per numerum $2p+1$ divisa idem praebent residuum, siquidem eorum differentia per $2p+1$ est divisibilis. Generatim enim, quorumcumque numerorum differentia $M-N$ per $2p+1$ est divisibilis, necesse est, ut uterque M et N seorsim divisus idem residuum relinquat. Hinc etiam, cum sit

$$(p+2)^2 - (p-1)^2 = 3(2p+1),$$

utrumque quadratum seorsim, $(p+2)^2$ et $(p-1)^2$, idem residuum praebere debet et in genere quadratum $(p+n+1)^2$ idem residuum dabit, quod quadratum $(p-n)^2$. Hoc igitur ostenso perspicuum est plura residua resultare non posse, quam in numero p unitates continentur; utrum autem haec residua omnia sint diversa an quaepiam inter se conveniant, hinc non definitur; atque adeo, si divisores quicumque admittantur, utrumque evenire potest. Sin autem divisor $2p+1$ fuerit numerus primus, omnia illa residua erunt inter se diversa, quod sequenti modo demonstro.

THEOREMA 1

8. *Si divisor* $P = 2p + 1$ *fuerit numerus primus per eumque omnia quadrata* $1, 4, 9, 16, \ldots$ *usque ad* p^2 *dividantur, omnia residua hinc resultantia inter se erunt diversa eorumque adeo multitudo* $= p$.

DEMONSTRATIO

Sint a et b duo numeri quicumque ipso p minores vel saltem non maiores ac demonstrandum est, si eorum quadrata a^2 et b^2 per numerum primum $2p + 1$ dividantur, residua certe diversa esse proditura. Si enim idem praeberent residuum, eorum differentia $aa - bb$ per $2p + 1$ foret divisibilis ideoque ob $2p + 1$ numerum primum et $aa - bb = (a + b)(a - b)$ alter horum factorum per $2p + 1$ divisibilis esse deberet. Cum autem sit tam $a < p$ quam $b < p$, saltem non $a > p$, summa $a + b$ multoque magis differentia $a - b$ divisore $2p + 1$ est minor; indeque neutra per $2p + 1$ divisibilis esse potest. Ex quo manifesto sequitur omnia quadrata, quorum radices non sint ipso p maiores, per numerum primum $2p + 1$ divisa certe diversa residua esse relictura.

COROLLARIUM 1

9. Quodsi ergo omnia quadrata 1, 4, 9, 16 etc. per numerum primum $2p + 1$ dividantur omniaque residua diversa notentur, eorum numerus neque maior erit neque minor quam p, sed huic numero p praecise aequalis.

COROLLARIUM 2

10. Omnia vero haec residua diversa numero p oriuntur ex totidem quadratis in serie naturali primum occurrentibus, scilicet 1, 4, 9, 16, . . . pp, neque ex sequentibus maioribus ulla nova residua eliciuntur.

COROLLARIUM 3

11. Non omnes ergo numeri ipso divisore $2p + 1$ minores inter residua occurrent, sed tantum tot eorum, quot unitates continentur in divisoris minori semisse p. Quare, cum numerorum divisore $2p + 1$ minorum multitudo sit $= 2p$, horum alter semissis tantum in ordine residuorum reperietur, alter vero inde penitus excluditur.

SCHOLION

12. Numeros hos divisore primo $2p+1$ minores, qui ex ordine residuorum excluduntur, nomine *non-residuorum*[1]) indicabo, quorum ergo multitudo semper numero residuorum est aequalis. Hoc discrimen inter residua et non-residua probe perpendisse iuvabit, quare pro divisoribus aliquot primis minoribus tam residua quam non-residua hic exhibebo.

Divisor 3, $p=1$		Divisor 5, $p=2$		Divisor 7, $p=3$	
Quadratum	1	Quadrata	1, 4	Quadrata	1, 4, 9
Residuum	1	Residua	1, 4	Residua	1, 4, 2
Non-residuum	2	Non-residua	2, 3	Non-residua	3, 5, 6

Divisor 11, $p=5$		Divisor 13, $p=6$	
Quadrata	1, 4, 9, 16, 25	Quadrata	1, 4, 9, 16, 25, 36
Residua	1, 4, 9, 5, 3	Residua	1, 4, 9, 3, 12, 10
Non-residua	2, 6, 7, 8, 10	Non-residua	2, 5, 6, 7, 8, 11

Divisor 17, $p=8$	
Quadrata	1, 4, 9, 16, 25, 36, 49, 64
Residua	1, 4, 9, 16, 8, 2, 15, 13
Non-residua	3, 5, 6, 7, 10, 11, 12, 14

Divisor 19, $p=9$	
Quadrata	1, 4, 9, 16, 25, 36, 49, 64, 81
Residua	1, 4, 9, 16, 6, 17, 11, 7, 5
Non-residua	2, 3, 8, 10, 12, 13, 14, 15, 18

Circa haec residua et non-residua pro quovis divisore primo tam memorabiles proprietates observantur, quas eo maiori studio perpendisse operae est pretium, quod inde non contemnenda incrementa in numerorum Theoriam redundare videntur.

1) Vide § 16 Commentationis 242 nota p. 497 laudatae. F. R.

THEOREMA 2

13. *Si in ordine residuorum ex divisore P ortorum occurrant numeri α et β, ibidem quoque occurret eorum productum $\alpha\beta$, siquidem minus fuerit divisore P; sin autem sit maius, eius loco capi convenit $\alpha\beta - P$ vel $\alpha\beta - 2P$ vel generatim $\alpha\beta - nP$, donec infra P deprimatur.*

DEMONSTRATIO

Oriantur residua α et β ex divisione quadratorum aa et bb per divisorem P facta, ita ut sit

$$aa = AP + \alpha \quad \text{et} \quad bb = BP + \beta.$$

Hinc erit

$$aabb = ABP^2 + (A\beta + B\alpha)P + \alpha\beta.$$

Quare si quadratum $aabb$ per divisorem P dividatur, residuum relinquetur $\alpha\beta$, vel si $\alpha\beta$ superet divisorem P, eius loco sumi debet residuum, quod ex divisione ipsius $\alpha\beta$ per P facta relinquetur, quod proinde erit vel $\alpha\beta - P$ vel $\alpha\beta - 2P$ vel $\alpha\beta - 3P$ vel generatim $\alpha\beta - nP$, ita ut sit $\alpha\beta - nP < P$.

COROLLARIUM 1

14. Si ergo inter residua occurrat numerus α, ibidem quoque occurret $\alpha\alpha$ item α^3, α^4 etc. omnesque adeo eius potestates, siquidem a singulis eiusmodi multiplum divisoris P subtrahâtur, ut residuum minus fiat divisore P.

COROLLARIUM 2

15. Cum igitur existente divisore P numero primo $2p + 1$ residuorum numerus sit $= p$, si unius cuiuspiam residui α omnes potestates α^0, α^1, α^2, α^3, α^4 etc. per eundem divisorem P dividantur, inde non plura quam p residua diversa resultare possunt.

COROLLARIUM 3

16. Hinc sequitur potestatem α^p per $P = 2p + 1$ divisam idem praebere residuum, quod $\alpha^0 = 1$, seu residuum fore unitatem, uti alibi[1]) ostendi, siquidem divisor $2p + 1$ fuerit numerus primus.

1) Vide Commentationem 134 (indicis Enestroemiani): *Theoremata circa divisores numerorum*, Novi comment. acad. sc. Petrop. 1 (1747/8), 1750, p. 20, imprimis theorema 11;

SCHOLION

17. Eximiis proprietatibus, quae hinc deduci possunt, hic uberius evolvendis non immoror, cum hoc iam olim[1]) a me sit factum. Ea hic tantum principia breviter repetere constitui, quibus indigeo ad novas quasdam residuorum affectiones explicandas, unde insignes nonnullas numerorum proprietates multo expeditius demonstrare liceat. Hunc in finem animadverto, quod quidem per se est perspicuum, quemadmodum residuo $\alpha\beta$ aequivalent numeri $\alpha\beta - P$, $\alpha\beta - 2P$ et in genere $\alpha\beta - nP$ existente P divisore, ita etiam omnes numeros per P divisos idem residuum relinquentes in hoc negotio tamquam hoc ipsum residuum spectari posse. Ita in ordine residuorum pro quocumque divisore P omnes plane numeri quadrati ipsi occurrere sunt censendi, cum quilibet aa huiusmodi forma $AP + \alpha$ exhiberi queat ideoque vero residuo α aequivalere sit existimandus. Hinc etiam inter residua numeri negativi admitti poterunt, cum residuo α aequivaleat $\alpha - P$, hocque pacto omnia residua ad numeros semisse divisoris P minores revocare licebit.

THEOREMA 3

18. *Si in ordine residuorum ex divisore P ortorum occurrant bina residua α et β, in eo quoque occurret residuum $\frac{\alpha + nP}{\beta}$ numero n ita assumto, ut $\frac{\alpha + nP}{\beta}$ fiat numerus integer, id quod semper fieri licet.*[2])

DEMONSTRATIO

Sint aa et bb ea quadrata, quae per P divisa relinquunt residua α et β, ut sit

$$aa = AP + \alpha \quad \text{et} \quad bb = BP + \beta.$$

Iam quaeratur c, ut sit $c = \frac{a + mP}{b}$ numerus integer, eritque

$$cc = \frac{aa + 2amP + mmPP}{bb} = \frac{\alpha + (A + 2am + mmP)P}{\beta + BP} = \text{numero integro.}$$

Leonhardi Eulèri Opera omnia, series I, vol. 2, p. 62. Vide etiam, quae in Prooemio (p. XXXI) eiusdem voluminis de Commentationibus 134 (theorema 11) et 262 (theorema 19) exposita sunt. F. R.

1) Vide notam praecedentem atque imprimis notam p. 497. F. R.

2) Confer theorema 7 Commentationis 242 nota p. 497 laudatae. F. R.

Cum nunc numerator tamquam ipsum residuum α, denominator vero tamquam residuum β spectari possit, patet, si cc per P dividatur, residuum ad formam propositam reductum iri. Posito enim brevitatis gratia $A + 2am + mmP = D$, ut sit $cc = \frac{\alpha + DP}{\beta + BP}$, tum vero $\frac{\alpha + nP}{\beta} = \gamma$, ostendi oportet fore $cc = CP + \gamma$, ut residuum ex divisione quadrati cc per numerum P natum prodeat $= \gamma$. Cum autem sit $\alpha = \beta\gamma - nP$, utique fieri poterit

$$cc = \frac{\beta\gamma + (D-n)P}{\beta + BP} = CP + \gamma,$$

quoniam inde sequitur

$$(D-n)P = (\beta C + \gamma B + BCP)P \quad \text{seu} \quad D - n = \beta C + \gamma B + BCP,$$

cuiusmodi relatio inter coefficientes ipsius P omnino necessaria est, ut numeri integri prodeant.

ALITER

Loco residui α aliud aequivalens accipiatur $\alpha + nP$, ut sit $\alpha + nP = \beta\gamma$; et cum omnia quadrata huius formae $(a + mP)^2$ idem praebeant residuum α, quod ex quadrato aa nasci assumitur, sumatur m ita, ut fiat $a + mP = bc$; et quia quadratum $bbcc$ per P divisum relinquit residuum α vel $\beta\gamma$, quadratum vero bb residuum β, necesse est, ut quadratum cc relinquat residuum $\gamma = \frac{\alpha + nP}{\beta}$. Sit enim $bbcc = EP + \beta\gamma$ et $bb = BP + \beta$; tum vero si neges quadratum cc praebiturum esse residuum γ, praebeat diversum x, ut sit $cc = CP + x$; erit ergo

$$bbcc = EP + \beta\gamma = (BP + \beta)(CP + x) = \beta x + (\beta C + Bx + BCP)P.$$

Iam multiplis divisoris P utrimque omissis, quemadmodum in aestimatione residuorum fieri solet, siquidem in minima forma desiderentur, habebitur $\beta x = \beta\gamma$ ideoque $x = \gamma$.

COROLLARIUM 1

19. Cum igitur unitas semper sit residuum, si pro divisore P fuerit aliquod residuum α, tum etiam $\frac{1 + nP}{\alpha}$ inter residua occurret; quod si vocetur β, erit $\alpha\beta = 1 + nP$, seu inter residua productum $\alpha\beta$ unitati aequivalebit.

COROLLARIUM 2

20. Pro quolibet ergo residuo α aliud quasi eius reciprocum β assignari potest, ut $\alpha\beta$ unitati aequivaleat, sumendo scilicet $\beta = \frac{1 + nP}{\alpha}$; atque haec

duo residua reciproca α et β inter se erunt diversa, nisi ambo fuerint vel $+1$ vel -1. Si enim sit $\beta = \alpha$ et

$$\alpha\alpha = 1 + nP = 1 + 2mP + mmPP,$$

erit

$$\alpha = \pm (1 + mP)$$

et multiplum divisoris mP omittendo $\alpha = \pm 1$.

COROLLARIUM 3

21. Dum igitur in ordine residuorum cuilibet residuo suum reciprocum adiungitur, hoc modo bina copulabuntur; semper autem unitas solitaria relinquetur, tum vero etiam residuum -1 seu $P-1$, quoties quidem inter residua occurrit.

SCHOLION

22. Idea haec binorum residuorum reciprocorum maximi est momenti et ad demonstrationem facilem Theorematis pulcerrimi nos manuducet, quod alias per satis multas ambages demonstraveram[1]), scilicet quod numerus primus formae $4q+1$ semper sit summa duorum quadratorum. Ceterum hic meminisse iuvabit, si pro quopiam divisore P residua sint α, β, γ, δ etc., non-residua vero $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D}$ etc., tum residuorum omnia producta mutua $\alpha\beta$, $\alpha\gamma$ etc. etiam inter residua reperiri [§ 13], eorum autem producta per quodpiam non-residuum, veluti $\alpha\mathfrak{A}$, inter non-residua esse referenda. At producta ex binis non-residuis, uti $\mathfrak{A}\mathfrak{B}$, in ordinem residuorum transeunt.[2])

THEOREMA 4

23. *Si divisor P fuerit numerus primus formae $4q+3$, tum -1 seu $P-1$ certe in ordine non-residuorum reperitur.*

---

1) Vide Commentationes 228 et 241 (indicis Enestroemiani): *De numeris, qui sunt aggregata duorum quadratorum*, Novi comment. acad. sc. Petrop. 4 (1752/3), 1758, p. 3, imprimis propositionem 5 (Tentamen demonstrationis), et *Demonstratio theorematis Fermatiani omnem numerum primum formae $4n+1$ esse summam duorum quadratorum*, Novi comment. acad. sc. Petrop. 5 (1754/5), 1760, p. 3; *Leonhardi Euleri Opera omnia*, series I, vol. 2, p. 295 et 328. F. R.

2) Quae theoremata in Commentatione 242 nota p. 497 laudata demonstrata sunt. F. R.

DEMONSTRATIO

Cum posito divisore $P = 2p + 1$ hic sit $p = 2q + 1$ ideoque numerus impar, numerus omnium residuorum erit impar. At si -1 in ordine residuorum occurreret, cuilibet residuo α responderet aliud residuum $-\alpha$, unde ordo residuorum ita se esset habiturus

$$+1, \quad +\alpha, \quad +\beta, \quad +\gamma, \quad +\delta \text{ etc.}$$
$$-1, \quad -\alpha, \quad -\beta, \quad -\gamma, \quad -\delta \text{ etc.}$$

foretque ergo numerus residuorum par. Cum igitur numerus residuorum certo sit impar, fieri nequit, ut in ordine residuorum occurrat -1 seu $P-1$; consequenter in ordine non-residuorum necessario reperiri debet.

COROLLARIUM 1

24. Quodsi ergo pro divisore primo $P = 4q + 3$ inter residua occurrat numerus α, tum numerus $-\alpha$ seu $P - \alpha$ certe inter non-residua reperietur; similique modo, si $-\beta$ fuerit residuum, tum $+\beta$ erit non-residuum.

COROLLARIUM 2

25. Si quadratum aa per divisorem $P = 4q + 3$ divisum relinquat residuum α, quia nullum datur quadratum xx, quod praebeat residuum $-\alpha$, fieri omnino nequit, ut ulla summa duorum quadratorum $aa + xx$ per numerum illum $4q + 3$ divisibilis existat.[1])

COROLLARIUM 3

26. Oriatur praeterea residuum β ex quadrato bb, et quia forma βaa residuum dat $\beta\alpha$, forma vero αbb residuum $\alpha\beta$, haec forma $\beta aa - \alpha bb$ per divisorem $P = 4q + 3$ erit divisibilis.

COROLLARIUM 4

27. Cum autem nullum detur quadratum xx, quod residuum praebeat $-\beta$, nulla datur forma αxx residuum praebens $-\alpha\beta$; nulla [ergo] huiusmodi forma $\beta aa + \alpha xx$ per numerum $P = 4q + 3$ erit divisibilis, siquidem α et β sint residua et α residuum quadrato aa respondens.

1) Vide notam 2 p. 266. F. R.

COROLLARIUM 5

28. Cum autem neque haec forma $\beta aacc + \alpha ccxx$ per divisorem $P = 4q + 3$ sit divisibilis, nisi quadratum cc divisionem admittat, qui casus sponte excluditur, quadrato $aacc$ quodcumque aliud residuum praeter α respondere potest; unde loco $aacc$ et $ccxx$ scribendo dd et yy nulla huiusmodi forma

$$\beta dd + \alpha yy$$

exhiberi potest per numerum $P = 4q + 3$ divisibilis, dum α et β sint residua.

SCHOLION

29. Quo haec clarius perspiciantur, percurramus quosdam numeros primos formae $4q + 3$ ac residua eius semisse maiora subtrahendo inde $4q + 3$ negative repraesentemus, ut infra semissem revocentur indeque pateat nullius residui α negativum $-\alpha$ simul in ordine residuorum occurrere:

Divisor	Residua
3	1
7	1, −3, +2
11	1, +4, −2, + 5, +3
19	1, +4, +9, − 3, +6, − 2, − 8, +7, + 5
23	1, +4, +9, − 7, +2, −10, + 3, −5, −11, +8, +6
31	1, +4, +9, −15, −6, + 5, −13, +2, −12, +7, −3, −11, +14, +10, +8.

Hic evidens est inter residua omnes numeros semisse divisoris non maiores occurrere vel signo + vel − affectos, nullum autem bis utroque signo affectum occurrere. Hinc si singulorum horum residuorum signa mutentur, ordo non-residuorum complebitur. Hinc pro divisore 31 sequentes formae exhiberi possunt numquam per 31 divisibiles:

$$aa + bb,\ aa - 15bb,\ aa - 6bb,\ aa + 5bb,\ aa - 13bb,\ aa + 2bb,\ aa + 7bb,$$
$$aa - 3bb,\ aa - 11bb,\ aa + 14bb,\ aa + 10bb.$$

Atque in genere, si α et β sint duo quaecumque residua, nulla huiusmodi forma

$$\alpha aa + \beta bb$$

per numerum 31 divisionem admittet.

THEOREMA 5

30. *Si divisor P fuerit numerus primus formae $4q+1$, tum numerus -1 seu $P-1$ certe in ordine residuorum reperitur.*

DEMONSTRATIO

Sit α residuum quodcumque eritque etiam eius reciprocum $\frac{1}{\alpha}$ seu $\frac{1+nP}{\alpha}$ residuum (§ 19), quod, nisi sit vel $\alpha=+1$ vel $\alpha=-1$, ab α erit diversum, ita ut exceptis his duobus casibus cuilibet residuo α respondeat suum reciprocum, quod sit α', ab α diversum; ubi notetur ipsius α' reciprocum vicissim esse α. Quare si -1 inter residua non reperiretur, omnia residua ita repraesentari possent binis reciprocis coniungendis

$$1,\ \alpha,\ \beta,\ \gamma,\ \delta \text{ etc.}$$
$$\alpha',\ \beta',\ \gamma',\ \delta' \text{ etc.}$$

sicque, cum omnia sint diversa, numerus omnium residuorum foret impar. Cum autem divisor sit numerus primus formae $4q+1$, numerus omnium residuorum est $2q$ ideoque par; unde necessario sequitur inter residua quoque numerum -1 seu $P-1$ occurrere, quia alioquin numerus residuorum foret impar.

COROLLARIUM 1

31. Cum ergo pro divisore primo $P=4q+1$ numerus -1 certe inter residua reperiatur, si aliud residuum quodcumque fuerit α, inter residua etiam occurret $-\alpha$.[1])

COROLLARIUM 2

32. Si igitur quadratum aa per divisorem primum $4q+1$ divisum relinquat residuum α, aliud dabitur quadratum bb, quod residuum praebebit $-\alpha$, unde horum quadratorum summa $aa+bb$ certe erit per numerum primum $4q+1$ divisibilis.

1) En ergo demonstrationem directam, ab EULERO ipso iam in Commentatione 242 (§ 84) saepenumero laudata desideratam. Confer etiam demonstrationem ope radicum primitivarum expositam, quae invenitur in Commentatione 449 (§ 57—59) huius voluminis. F. R.

COROLLARIUM 3

33. Quoniam omnia residua ex quadratis, quorum radices semissem divisoris non superant, nascuntur, quadrato quocumque proposito aa aliud semper bb non maius quam $4qq$ exhiberi potest, ut summa $aa + bb$ prodeat divisibilis per $4q + 1$.

COROLLARIUM 4

34. Si $1 + aa$ divisionem per $4q + 1$ admittat, tum etiam $bb + aabb$ ac proinde quoque

$$bb + (ab - (4q + 1)n)^2$$

divisionem admittet; sicque altero quadrato bb pro lubitu assumto alterum $(ab - (4q + 1)n)^2$ facile reperitur.

COROLLARIUM 5

35. Si haec duorum quadratorum summa $aa + bb$ per divisorem $4q + 1$ fuerit divisibilis, tum etiam $aaxx + bbxx$ ac proinde quoque haec forma

$$(ax - (4q + 1)m)^2 + (bx - (4q + 1)n)^2$$

divisionem admittet. Semper autem x ita assumere licet, ut alterius radix $ax - (4q + 1)m$ dato numero c aequetur sumendo $x = \frac{c + (4q + 1)m}{a}$, quod semper in integris fieri potest.

SCHOLION 1

36. Pro quovis divisore primo, sive sit formae $4q + 1$ sive $4q + 3$, numerorum reciprocorum consideratio omnem attentionem meretur, cum inde tam facile hanc insignem veritatem elicuerimus, quod proposito numero primo quocumque formae $4q + 1$ semper summae binorum quadratorum exhiberi queant per illum divisibiles. Cum igitur demonstrari praeterea possit summam duorum quadratorum alios non admittere divisores, nisi qui ipsi sint summae duorum quadratorum[1]), hoc modo Theorematis Fermatiani, quod omnes numeri primi formae $4q + 1$ sint duorum quadratorum aggregata, demonstratio multo expeditius absolvitur, quam quidem olim[2]) a me est fac-

1) Id quod ab Eulero demonstratum est propositione 4 Commentationis 228 nota p. 504 laudatae. F. R.

2) Scilicet Commentatione 241 nota p. 504 laudata. Confer autem etiam § 79—84 Commentationis 242 nota p. 497 laudatae. F. R.

tum. Quemadmodum autem numeri reciproci pro quovis divisore P se habeant, dum cuiusvis numeri α reciprocus est $\frac{1+nP}{\alpha}$, ex subiunctis exemplis clarius intelligetur:

Divisor	Reciprocorum paria
3	
5	2 3
7	2, 3 4, 5
11	2, 3, 5, 7 6, 4, 9, 8
13	2, 3, 4, 5, 6 7, 9, 10, 8, 11
17	2, 3, 4, 5, 8, 10, 11 9, 6, 13, 7, 15, 12, 14
19	2, 3, 4, 6, 7, 8, 9, 14 10, 13, 5, 16, 11, 12, 17, 15
23	2, 3, 4, 5, 7, 9, 11, 13, 15, 17 12, 8, 6, 14, 10, 18, 21, 16, 20, 19
29	2, 3, 4, 5, 7, 8, 9, 12, 14, 16, 18, 19, 23 15, 10, 22, 6, 25, 11, 13, 17, 27, 20, 21, 26, 24

Singula haec paria reciproca ita inter se sunt connexa, ut quilibet numerus unicum tantum recipiat reciprocum, divisore scilicet minorem, prorsus uti in Theoremate assumsimus.

SCHOLION 2

37. Quodsi ergo divisor primus fuerit formae $4q + 1$, videamus, quomodo residua secundum hanc legem reciprocorum disposita se sint habitura:

Divisor	Residua
5	1, 4
	1, (— 1)
13	1, 4, 9, 3, 12, 10
	1, 4, 9, 12 10, 3, (— 1)
17	1, 4, 9, 16, 8, 2, 15, 13
	1, 4, 9, 8, 16 13, 2, 15, (— 1)
29	1, 4, 9, 16, 25, 7, 20, 6, 23, 13, 5, 28, 24, 22
	1, 4, 9, 16, 25, 6, 23, 28 22, 13, 20, 7, 5, 24, (— 1)
37	1, 4, 9, 16, 25, 36, 12, 27, 7, 26, 10, 33, 21, 11, 3, 34, 30, 28
	1, 4, 9, 16, 25, 12, 27, 26, 21, 36 28, 33, 7, 3, 34, 11, 10, 30, (— 1)

Ex his exemplis perspicuum est, cum unitas sit solitaria et reliquorum residuorum quodque suum reciprocum habeat adiunctum, numerum residuorum futurum esse imparem, nisi praeter unitatem aliud residuum solitarium accederet, quod sibi ipsi esset reciprocum. Quoniam igitur his casibus, quibus divisor est numerus primus formae $4q + 1$, numerus residuorum certo est par $= 2q$, necesse est, ut praeter unitatem residuum $4q$ vel -1 occurrat, cuius quippe reciprocum ipsi est aequale. Unde veritas insignis istius Theorematis, cuius demonstratio alioquin maxime erat difficilis, admodum fit perspicua, quod scilicet, quoties divisor sit numerus primus formae $4q + 1$, inter residua semper occurrat numerus $4q$ vel -1.

SCHOLION 3

38. Quemadmodum hinc patet numerum -1 inter residua reperiri, quoties divisor fuerit numerus primus formae $4q + 1$, ita pro quovis alio numero primo s divisorum primorum forma assignari, at nondum demon-

strari potest, ut iste numerus s in residuis reperiatur. Cuiusmodi est hoc Theorema:

Si divisor primus fuerit formae $4ns + (2x+1)^2$ *existente* s *numero primo, tum in residuis occurrent numeri* $+s$ *et* $-s$;

alterumque huic simile:

Si divisor primus fuerit formae $4ns - (2x+1)^2$ *existente* s *numero primo, tum in residuis occurret numerus* $+s$, *at* $-s$ *erit in non-residuis.*

Quando autem vicissim $-s$ occurrat in residuis, at $+s$ in non-residuis, ita in genere definiri nequit. Pro casibus autem particularibus res ita se habere deprehenditur:

Ut sit	divisor primus debet esse
$\left\{\begin{matrix} -2 \text{ residuum} \\ +2 \text{ non-residuum} \end{matrix}\right\}$	$P = 8n + 3$
$\left\{\begin{matrix} -3 \text{ residuum} \\ +3 \text{ non-residuum} \end{matrix}\right\}$	$P = 12n + 7$
$\left\{\begin{matrix} -5 \text{ residuum} \\ +5 \text{ non-residuum} \end{matrix}\right\}$	$P = 20n + 3, 7$
$\left\{\begin{matrix} -7 \text{ residuum} \\ +7 \text{ non-residuum} \end{matrix}\right\}$	$P = 28n + 11, 15, 23$
$\left\{\begin{matrix} -11 \text{ residuum} \\ +11 \text{ non-residuum} \end{matrix}\right\}$	$P = 44n + 3, 15, 23, 27, 31$
$\left\{\begin{matrix} -13 \text{ residuum} \\ +13 \text{ non-residuum} \end{matrix}\right\}$	$P = 52n + 7, 11, 19, 15, 31, 47$
$\left\{\begin{matrix} -17 \text{ residuum} \\ +17 \text{ non-residuum} \end{matrix}\right\}$	$P = 68n + 3, 7, 11, 23, 27, 31, 39, 63$
$\left\{\begin{matrix} -19 \text{ residuum} \\ +19 \text{ non-residuum} \end{matrix}\right\}$	$P = 76n + 7, 11, 19, 23, 35, 39, 43, 47, 55, 63$
$\left\{\begin{matrix} -23 \text{ residuum} \\ +23 \text{ non-residuum} \end{matrix}\right\}$	$P = 92n + 3, 23, 27, 31, 35, 39, 47, 55, 59, 71, 75, 87$

Quorum casuum contemplatio hoc suppeditat Theorema:

Si divisor primus fuerit formae $4ns - 4z - 1$ *excludendo omnes valores in forma* $4ns - (2x+1)^2$ *contentos, existente* s *numero primo, tum in residuis occurret* $-s$, *at* $+s$ *erit non-residuum.*

Quibus Theorematibus insuper hoc adiungi potest:

Si divisor primus fuerit formae $4ns + 4z + 1$ *excludendo omnes valores in forma* $4ns + (2x+1)^2$ *contentos, existente* s *numero primo, tum tam* $+s$ *quam* $-s$ *in non-residuis occurret.*

Theoremata haec ideo subiungo, ut, qui huiusmodi speculationibus delectantur, in eorum demonstrationem inquirant, cum nullum sit dubium, quin inde Theoria numerorum insignia incrementa sit adeptura.

CONCLUSIO

39. Quatuor haec Theoremata postrema, quorum demonstratio adhuc desideratur, sequenti modo[1]) concinnius exhiberi possunt:

Existente s *numero quocumque primo dividantur tantum quadrata imparia* 1, 9, 25, 49 *etc. per divisorem* $4s$ *notenturque residua, quae omnia erunt formae* $4q+1$, *quorum quodvis littera* α *indicetur, reliquorum autem numerorum formae* $4q+1$, *qui inter residua non occurrunt, quilibet littera* $\mathfrak{A}$ *indicetur; quo facto si fuerit*

divisor numerus primus formae	*tum est*
$4ns + \alpha$	$+s$ *residuum et* $-s$ *residuum*
$4ns - \alpha$	$+s$ *residuum et* $-s$ *non-residuum*
$4ns + \mathfrak{A}$	$+s$ *non-residuum et* $-s$ *non-residuum*
$4ns - \mathfrak{A}$	$+s$ *non-residuum et* $-s$ *residuum.*

1) En habes celeberrimum illud theorema primum demonstratum a C. F. Gauss, qui ei nomen *theorematis fundamentalis* dedit — „quia omnia fere, quae de residuis quadraticis dici possunt, huic theoremati innituntur". Vide C. F. Gauss, *Disquisitiones arithmeticae*, Lipsiae 1801, art. 125—146; *C. F. Gauss Werke*, I, p. 94—113. In summa quidem illud theorema fundamentale iam continetur in L. Euleri Commentatione 164 (indicis Enestroemiani): *Theoremata circa divisores numerorum in hac forma* $paa \pm qbb$ *contentorum*, Comment. acad. sc. Petrop. 14 (1744/46), 1751, p. 151; *Leonhardi Euleri Opera omnia*, series I, vol. 2, p. 194; vide imprimis ibidem notas p. 194 et 217.

F. R.

DISQUISITIO ACCURATIOR CIRCA RESIDUA EX DIVISIONE QUADRATORUM ALTIORUMQUE POTESTATUM PER NUMEROS PRIMOS RELICTA [1]

Commentatio 554 indicis ENESTROEMIANI
Opuscula analytica 1, 1783, p. 121—156

1. Si numerus quadratus aa per numerum primum p dividatur, residuum relictum littera α indicetur; similique modo litterae β, γ, δ etc. mihi denotabunt residua in divisione quadratorum bb, cc, dd etc. relicta.

2. Erit ergo $\alpha = aa - np$, quia residuum α prodit, si a quadrato aa multiplum numeri p auferatur idque maximum, ut residuum α ipso divisore p minus reddatur. Nihil autem impedit, quominus multiplum np maius accipiatur quadrato aa, unde residuum α prodit negativum, sicque eius valor infra $\frac{1}{2}p$ deprimi potest.

3. Idem igitur residuum α multis modis exhiberi potest, quoniam cunctae hae formae $\alpha \pm mp$ eandem naturam continent. Perinde scilicet est, sive residuum ex divisione quadrati aa per numerum p ortum dicatur esse α sive $\alpha \pm p$ sive $\alpha \pm mp$ denotante littera m numerum integrum quemcumque.

---

1) Confer Commentationem praecedentem. F. R.

4. Innumera autem quadrata aa per numerum p divisa idem relinquunt residuum α, quae omnia ex cognito uno aa facile inveniuntur. Cuncta haec quadrata ista forma $(a \pm mp)^2$ vel $(mp \pm a)^2$ contineri evidens est sicque sufficit residuum ex harum forma minima, cuius radix non excedet $\frac{1}{2}p$, notasse; omnia scilicet haec quadrata $(mp \pm a)^2$ respectu numeri p eiusdem indolis sunt censenda.

5. Quadratis secundum ordinem naturalem dispositis residua per divisorem p orta ita se habebunt:

Quadrata	$1,$	$2^2,$	$3^2,$	$4^2,$	$\ldots$	$(p-4)^2,$	$(p-3)^2,$	$(p-2)^2,$	$(p-1)^2,$
Residua	$1,$	$4,$	$9,$	$16,$	$\ldots$	$16,$	$9,$	$4,$	$1.$

Quadratis ergo ad $(p-1)^2$ continuatis singula residua bis occurrunt; et quia p est numerus primus, eorum numerus est par et bina quadrata media $\left(\frac{p-1}{2}\right)^2$ et $\left(\frac{p+1}{2}\right)^2$ idem dabunt residuum $\frac{pp-2p+1}{4}$

6. Omnia ergo residua, quae quidem ex divisione numerorum quadratorum per numerum primum p resultare possunt, nascuntur ex his quadratis:

Quadrata	$1,$	$2^2,$	$3^2,$	$4^2,$	$\ldots$	$\left(\frac{p-1}{2}\right)^2,$
Residua	$1,$	$4,$	$9,$	$16,$	$\ldots$	$\frac{pp-2p+1}{4},$

quorum numerus est $= \frac{p-1}{2}$. Neque ergo omnes numeri divisore p minores, quorum multitudo est $p-1$, inter residua occurrunt, sed eorum semissis inde certe excluditur.

7. Continuatis autem quadratis ad $\left(\frac{p-1}{2}\right)^2$ residua inde orta omnia sunt diversa; neque enim ullum usque ad hunc terminum bis occurrere potest, siquidem divisor p sit numerus primus. Namque si bina quadrata aa et bb neutro quadratum $\left(\frac{p-1}{2}\right)^2$ excedente idem darent residuum r, differentia eorum $aa-bb$ ideoque vel $a-b$ vel $a+b$ per p dividi posset. Cum autem neque a neque b superet $\frac{p-1}{2}$, etiam summa $a+b$ minor erit quam p ideoque fieri omnino nequit, ut ea summa ac multo minus differentia $a-b$ divisionem per numerum p admittat.

8. Proposito ergo numero primo p omnia residua ex his quadratis

$$1,\ 2^2,\ 3^2,\ 4^2,\ \ldots\ \left(\frac{p-1}{2}\right)^2$$

obtinentur; quorum numerus cum sit $=\frac{p-1}{2}$ et residua omnia inter se differant, numerorum ipso p minorum, quorum multitudo est $p-1$, semissis certe inter residua occurrit; semissis vero inde excluditur et classem *non-residuorum* constituit. Pro quolibet ergo numero primo p residua a non-residuis probe sunt discernenda.

9. Si enim α inter residua occurrat, pronunciare possumus innumerabilia quadrata dari, quae in hac forma $np+\alpha$ contineantur, ac minimi eorum radicem non excedere numerum $\frac{p-1}{2}$. Sin autem numerus $\mathfrak{A}$ inter residua non reperiatur, pronunciabimus nullum numerum quadratum in forma $np+\mathfrak{A}$ contineri. Quovis autem casu tam residuorum α quam non-residuorum $\mathfrak{A}$ multitudo est $=\frac{p-1}{2}$.

10. Quodsi residua ex divisione quadratorum per numerum primum p oriunda secundum hunc ordinem naturalem disponantur, primo occurrent numeri quadrati 1, 4, 9, 16 etc., donec divisione per numerum p ad minores numeros redigi possunt; postremum vero eorum erit $\frac{pp-2p+1}{4}$, unde numerum p, quoties fieri potest, auferri oportet.

11. Ad hoc postremum residuum agnoscendum duos casus contemplari convenit, prout numerus primus p fuerit formae vel $4q+1$ vel $4q+3$.

Sit primo $p=4q+1$ ideoque $\frac{p-1}{2}=2q$ et ultimum residuum $4qq$, quod subtractione multipli $qp=4qq+q$ reducitur ad $-q$ seu ad $3q+1$.

Altero vero casu $p=4q+3$ seu $\frac{p-1}{2}=2q+1$ ultimum residuum $4qq+4q+1$ ablatione multipli $qp=4qq+3q$ reducitur ad $q+1$.

12. Simili modo penultimum residuum ex quadrato $\left(\frac{p-3}{2}\right)^2$ ortum reperitur

pro casu $p=4q+1$: $4qq-4q+1$ seu $-5q+1$ seu $-q+2$,

pro casu $p=4q+3$: $4qq$ seu $-3q$ seu $q+3$.

At antepenultimum ex $\left(\frac{p-5}{2}\right)^2$ ortum ita prodit

pro casu $p = 4q+1$: $4qq - 8q + 4$ seu $-9q+4$ seu $-q+6$,
pro casu $p = 4q+3$: $4qq - 4q + 1$ seu $-7q+1$ seu $q+7$.

Quod vero antepenultimum praecedit, hoc modo

pro casu $p = 4q+1$: $4qq - 12q + 9$ seu $-13q+9$ seu $-q+12$,
pro casu $p = 4q+3$: $4qq - 8q + 4$ seu $-11q+4$ seu $q+13$.

13. Hos igitur binos casus distinguendo residua sequenti modo se habebunt.

Casu $p = 4q+1$:

Quadrata $1, 2^2, 3^2, 4^2, \ldots (2q-3)^2, (2q-2)^2, (2q-1)^2, (2q)^2$,
Residua $1, 4, 9, 16, \ldots -q+12, -q+6, -q+2, -q$
seu $3q+13, 3q+7, 3q+3, 3q+1$.

Casu $p = 4q+3$:

Quadrata $1, 2^2, 3^2, 4^2, \ldots (2q-2)^2, (2q-1)^2, (2q)^2, (2q+1)^2$,
Residua $1, 4, 9, 16, \ldots q+13, q+7, q+3, q+1$.

Priori scilicet casu in genere occurrit residuum $-q+nn+n$ seu $3q+nn+n+1$, posteriori vero $q+nn+n+1$.

14. Quo hic residuorum ordo clarius perspiciatur, exempla spectanda proponam et primo quidem pro numeris primis formae $p = 4q+1$.

$p = 5$ { $1, 2^2$
$q = 1$ { $1, 4$
seu $1, -1$

$p = 13$ { $1, 2^2, 3^2, 4^2, 5^2, 6^2$
$q = 3$ { $1, 4, 9, 3, 12, 10$
seu $1, 4, -4, 3, -1, -3$

$p = 17$ { $1, 2^2, 3^2, 4^2, 5^2, 6^2, 7^2, 8^2$
$q = 4$ { $1, 4, 9, 16, 8, 2, 15, 13$
seu $1, 4, -8, -1, 8, 2, -2, -4$

$p = 29$ { $1, 2^2, 3^2, 4^2, 5^2, 6^2, 7^2, 8^2, 9^2, 10^2, 11^2, 12^2, 13^2, 14^2$
$q = 7$ { $1, 4, 9, 16, 25, 7, 20, 6, 23, 13, 5, 28, 24, 22$
seu $1, 4, 9, -13, -4, 7, -9, 6, -6, 13, 5, -1, -5, -7$

$p = 37$ { $1, 2^2, 3^2, 4^2, 5^2, 6^2, 7^2, 8^2, 9^2, 10^2, 11^2, 12^2, 13^2, 14^2, 15^2, 16^2, 17^2, 18^2$
$q = 9$ { $1, 4, 9, 16, 25, 36, 12, 27, 7, 26, 10, 33, 21, 11, 3, 34, 30, 28$
seu $1, 4, 9, 16, -12, -1, 12, -10, 7, -11, 10, -4, -16, 11, 3, -3, -7, -9$

$p = 41$ { $1, 2^2, 3^2, 4^2, 5^2, 6^2, 7^2, 8^2, 9^2, 10^2, 11^2, 12^2, 13^2, 14^2, 15^2, 16^2, 17^2, 18^2, 19^2, 20^2$
$q = 10$ { $1, 4, 9, 16, 25, 36, 8, 23, 40, 18, 39, 21, 5, 32, 20, 10, 2, 37, 33, 31$
seu $1, 4, 9, 16, -16, -5, 8, -18, -1, 18, -2, -20, 5, -9, 20, 10, 2, -4, -8, -10$

Ubi observare licet in residuis per negativa ad minimam formam reductis singulos numeros bis, positive scilicet et negative, occurrere.[1])

15. Sequentia exempla pertinent ad numeros primos formae $p = 4q + 3$.

$p = 3$ { 1
$q = 0$ { 1

$p = 7$ { $1, 2^2, 3^2$
$q = 1$ { $1, 4, 2$
seu $1, -3, 2$

$p = 11$ { $1, 2^2, 3^2, 4^2, 5^2$
$q = 2$ { $1, 4, 9, 5, 3$
seu $1, 4, -2, 5, 3$

$p = 19$ { $1, 2^2, 3^2, 4^2, 5^2, 6^2, 7^2, 8^2, 9^2$
$q = 4$ { $1, 4, 9, 16, 6, 17, 11, 7, 5$
seu $1, 4, 9, -3, 6, -2, -8, 7, 5$

1) Vide § 31. F. R.

$p = 23$ { 1, 2^2, 3^2, 4^2, 5^2, 6^2, 7^2, 8^2, 9^2, 10^2, 11^2
$q = 5$ { 1, 4, 9, 16, 2, 13, 3, 18, 12, 8, 6
seu 1, 4, 9, -7, 2, -10, 3, -5, -11, 8, 6

$p = 31$ { 1, 2^2, 3^2, 4^2, 5^2, 6^2, 7^2, 8^2, 9^2, 10^2, 11^2, 12^2, 13^2, 14^2, 15^2
$q = 7$ { 1, 4, 9, 16, 25, 5, 18, 2, 19, 7, 28, 20, 14, 10, 8
seu 1, 4, 9, -15, -6, 5, -13, 2, -12, 7, -3, -11, 14, 10, 8

$p = 43$ { 1, 2^2, 3^2, 4^2, 5^2, 6^2, 7^2, 8^2, 9^2, 10^2, 11^2, 12^2, 13^2, 14^2, 15^2, 16^2, 17^2, 18^2, 19^2, 20^2, 21^2
$q = 10$ { 1, 4, 9, 16, 25, 36, 6, 21, 38, 14, 35, 15, 40, 24, 10, 41, 31, 23, 17, 13, 11
seu 1, 4, 9, 16, -18, -7, 6, 21, -5, 14, -8, 15, -3, -19, 10, -2, -12, -20, 17, 13, 11

In istis residuis ad minimam formam reductis omnes plane numeri ab unitate usque ad $2q + 1$ occurrunt, alii signo positionis, alii negationis affecti. Verum has proprietates observatas demonstrari oportet.[1])

16. Iam supra, p. 69[2]), demonstravi, si inter residua ex divisione quadratorum per numerum p orta occurrant numeri α et β, ibidem quoque reperiri productum $\alpha\beta$ ac proinde quoque hanc formam latius patentem $\alpha^m\beta^n$. Oriantur enim haec residua ex quadratis aa et bb, ita ut sit

$$aa = mp + \alpha \quad \text{et} \quad bb = np + \beta,$$

atque manifestum est ex horum quadratorum producto

$$aabb = mnpp + (m\beta + n\alpha)p + \alpha\beta,$$

cuius forma est $Mp + \alpha\beta$, nasci residuum $\alpha\beta$; similique modo ex quadrato $a^{2m}b^{2n}$ provenire residuum $\alpha^m\beta^n$ seu $\alpha^m\beta^n - Mp$, ut ad minimam formam reducatur. Quin etiam notari convenit hoc ipsum residuum $\alpha^m\beta^n$ nasci ex omnibus his quadratis $(a^mb^n \pm Np)^2$ seu $(Np \pm a^mb^n)^2$ ideoque ex quadrato, cuius latus $a^mb^n - Np$ seu $Np - a^mb^n$ minus erit quam $\frac{1}{2}p$.

1) Vide § 31. F. R.

2) Scilicet p. 501 huius voluminis. F. R.

17. Denotent litterae

$$a,\ b,\ c,\ d,\ \ldots\ l$$

omnes numeros divisoris p semisse $\frac{1}{2}p$ minores, quorum ergo multitudo est $= \frac{p-1}{2}$, sintque

$$\alpha,\ \beta,\ \gamma,\ \delta,\ \ldots\ \lambda$$

residua ex eorum quadratorum

$$a^2,\ b^2,\ c^2,\ d^2,\ \ldots\ l^2$$

per numerum p divisione relicta, quorum multitudo itidem est $= \frac{p-1}{2}$, ita ut ex omnibus numeris divisore p minoribus, quorum multitudo est $p-1$, totidem ex residuorum ordine excludantur, quos nomine *non-residuorum* complexos litteris

$$\mathfrak{A},\ \mathfrak{B},\ \mathfrak{C},\ \mathfrak{D},\ \ldots\ \mathfrak{L}$$

indicabo. Notatu ergo maxime dignum est in ordine residuorum α, β, γ, δ, $\ldots$ λ, etiamsi eorum multitudo tantum est $= \frac{p-1}{2}$, tamen omnia eorundem producta ex binis pluribusque atque etiam singulorum potestates omnes occurrere, siquidem auferendo inde, quoties fieri potest, divisorem p ad minimam formam revocentur.

18. Quo magis haec illustrentur, animadverti oportet ratione cuiusque divisoris p omnes numeros in totidem species distribui; scilicet ratione divisoris 2 duae habentur species numerorum parium et imparium formulis $2x$ et $2x+1$ contentorum. Divisor autem 3 tres praebet numerorum species $3x$, $3x+1$ et $3x+2$ et divisor 4 has quatuor $4x$, $4x+1$, $4x+2$ et $4x+3$, quae diversae species in numerorum doctrina sollicite distingui solent. Simili ergo modo ratione divisoris cuiusque p hae diversae numerorum species constituuntur

$$px,\ px+1,\ px+2,\ px+3,\ \ldots\ px+p-1,$$

quarum multitudo est p. Omissa ergo prima specie px multipla divisoris p continente reliquarum multitudo est $p-1$, ac si p fuerit numerus primus, has species in duas classes dividi convenit utraque $\frac{p-1}{2}$ species complectente

$$px+\alpha,\ px+\beta,\ px+\gamma,\ px+\delta,\ \ldots\ px+\lambda,$$
$$px+\mathfrak{A},\ px+\mathfrak{B},\ px+\mathfrak{C},\ px+\mathfrak{D},\ \ldots\ px+\mathfrak{L},$$

ita ut omnes numeri quadrati in priori classe contineantur, posterior vero classis naturae quadratorum prorsus adversetur.

19. Pro quolibet ergo divisore primo p his duabus classibus constitutis, quarum utraque $\frac{p-1}{2}$ species continet et quae ambae coniunctim omnes plane numeros continent exceptis multiplis ipsius p, quippe quorum iudicium est in promtu, omnes numeri in priori classe contenti hac gaudent proprietate, ut producta ex binis in eadem classe contineantur, in qua ergo simul non solum potestates singulorum quaecumque, sed etiam producta ex binis pluribusque harum potestatum occurrunt. Prior igitur classis, quam voco residuorum, numeris α, β, γ, δ, $\ldots$ λ determinatur, dum altera classis, non-residuorum, numeris $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D}$, $\ldots$ $\mathfrak{L}$ definitur.

20. Demonstravi deinde etiam, si in classe residuorum occurrant duo numeri r et rs, quorum ille r huius rs sit factor, tum etiam huius alterum factorem in eadem classe reperiri.[1]) Cum enim dentur duo quadrata aa et bb, ut formae $aa-r$ et $bb-rs$ sint per numerum primum p divisibiles existentibus numeris a et b ipso p minoribus, etiam forma $aas-rs$ per p est divisibilis hincque etiam differentia $bb-aas$ et $(b+np)^2-aas$. Cum autem a et b sint ipso p minores, semper n ita assumere licet, ut fiat $b+np=ma$. Ex quo talis forma $mmaa-aas$ dabitur per p divisibilis adeoque et haec $mm-s$, ita ut sit $s=mm-np$ ac propterea numerus s inter residua reperiatur. Hinc sequitur, si r fuerit residuum, at s non-residuum, tum productum rs certe fore non-residuum; seu producta ex quovis residuo per non-residuum facta, veluti $\alpha\mathfrak{A}$, $\alpha\mathfrak{B}$, $\beta\mathfrak{A}$, inter non-residua reperiuntur.[2])

21. Si igitur $\mathfrak{A}$ fuerit non-residuum, omnia haec producta

$$\alpha\mathfrak{A},\ \beta\mathfrak{A},\ \gamma\mathfrak{A},\ \delta\mathfrak{A},\ \ldots\ \lambda\mathfrak{A}$$

1) Vide theorema 7 Commentationis 242 nota p. 497 laudatae. F. R.

2) Vide eiusdem Commentationis 242 theorema 9. F. R.

erunt non-residua; quae cum sint diversa inter se etiam reductione ad minimam formam facta eorumque numerus $= \frac{p-1}{2}$, in iis adeo omnia non-residua continentur. Ex quo iam perspicuum est producta ex binis non-residuis, veluti $\alpha\beta\mathfrak{A}\mathfrak{A}$, ad classem residuorum esse referenda, quoniam $\alpha\beta$ est residuum et $\mathfrak{A}\mathfrak{A}$ utpote numerus quadratus per se inter residua occurrit. Simul vero patet producta ex ternis non-residuis, uti $\mathfrak{A}\mathfrak{B}\mathfrak{C}$, iterum in classem non-residuorum cadere, producta vero ex quaternis inter ipsa residua reperiri, et ita porro.[1])

22. Praeterea vero etiam observo ex datis binis residuis α et β per divisionem novum residuum oriri et fractionem $\frac{\alpha}{\beta}$ inter residua esse referendam. Etsi enim fractiones ex hac ratione prorsus excluduntur, tamen, quia numerus α aequivalens censetur huic formae generali $\alpha + np$ universam speciem continenti, numerum n utique ita accipere licet, ut $\frac{\alpha+np}{\beta}$ fiat numerus integer, de quo effatum est intelligendum, quod scilicet inter residua reperiatur.[2]) Hinc ergo omnes termini huius progressionis geometricae

$$\alpha,\ \beta,\ \frac{\beta^2}{\alpha},\ \frac{\beta^3}{\alpha^2},\ \frac{\beta^4}{\alpha^3}\ \text{etc.}$$

ex binis residuis α et β continuatae in classe residuorum continentur, si scilicet singuli ad formas integras revocentur. Quodsi enim fractio $\frac{\beta}{\alpha}$ aequivaleat numero integro r, statim sequentes numeri integri obtinentur

$$\alpha,\ \beta,\ \beta r,\ \beta r^2,\ \beta r^3,\ \beta r^4\ \text{etc.},$$

qui ad minimam formam reducti non plures quam $\frac{p-1}{2}$ numeros diversos praebere possunt.

23. Consideremus ergo hanc progressionem geometricam

$$\alpha,\ \beta,\ \beta r,\ \beta r^2,\ \beta r^3,\ \beta r^4\ \text{etc.},$$

et cum omnes termini diversi esse nequeant, praebeant hi termini βr^m et βr^{m+n} per p divisi idem residuum, ita ut differentia $\beta r^{m+n} - \beta r^m$ ac propterea

1) Vide eiusdem Commentationis 242 theorema 10. F. R.

2) Vide Commentationem 552 huius voluminis, theorema 3. F. R.

$r^n - 1$ per p fiat divisibilis. Tum ergo etiam termini β et βr^n atque etiam α et βr^{n-1} ratione residui convenient; ex quo patet plura residua diversa prodire non posse, quam quae oriuntur ex his terminis initialibus

$$\alpha,\ \beta,\ \beta r,\ \beta r^2,\ \ldots\ \beta r^{n-2},$$

quoniam ex sequentibus βr^{n-1}, βr^n, βr^{n+1} etc. eadem residua eodem ordine recurrunt; quorum ergo residuorum, siquidem fuerint diversa, multitudo maior esse nequit quam $\frac{p-1}{2}$, quod evenit, si r^n sit minima potestas ipsius r, quae unitate minuta per p divisionem admittat. Hinc patet numerum n certe non superare $\frac{p-1}{2}$; ac si fuerit $n = \frac{p-1}{2}$, omnia plane residua obtinentur.

24. Sin autem ex terminis α, β, βr, βr^2, $\ldots$ βr^{n-2} non omnia residua prodeant, sed quaedam omittantur, facile ostenditur ad minimum totidem omitti, quot adsunt. Si enim residuum γ inter ea non occurrat, quod etiam per $\alpha\delta$ repraesentare licet, quoniam $\gamma + mp$ semper ad formam $\alpha\delta$ revocari potest, tum etiam neque $\beta\delta$ neque $\beta\delta r$ neque $\beta\delta r^2$ etc. inter ea residua reperietur; quae cum sint diversa, excluso uno simul n excluduntur, unde $2n$ numerum omnium $\frac{p-1}{2}$ superare nequit. Erit ergo vel $2n = \frac{p-1}{2}$ vel $2n < \frac{p-1}{2}$ et posteriori casu adhuc de novo ad minimum n residua excluduntur. Quare cum termini progressionis geometricae α, β, βr, βr^2, $\ldots$ βr^{n-2}, quorum numerus est n, vel omnia residua contineant ex quadratis orta, quorum multitudo est $= \frac{p-1}{2}$, vel inde exclusorum numerus sit $= n$ vel $= 2n$ vel $= 3n$ etc., evidens est numerum n necessario partem aliquotam ipsius $\frac{p-1}{2}$ esse debere ideoque minimum exponentem n, quo potestas r^n unitate minuta per p divisibilis reddatur, vel ipsi numero $\frac{p-1}{2}$ vel eiusdem parti cuipiam aliquotae esse aequalem.[1])

25. Sive autem sit $n = \frac{p-1}{2}$, sive eius parti cuidam aliquotae aequetur, semper forma $r^{\frac{1}{2}(p-1)} - 1$ divisionem admittet per numerum primum p.[2]) Ponamus $p = 2q + 1$, ut sit $\frac{p-1}{2} = q$; ac si ex binis quadratorum residuis quibuscumque α et β sumendo $r = \frac{\beta + np}{\alpha}$ formetur haec progressio geometrica

$$\alpha,\ \beta,\ \beta r,\ \beta r^2,\ \beta r^3,\ \ldots\ \beta r^{q-2}$$

1) Confer theoremata 9—13 Commentationis 262 nota p. 240 laudatae. F. R.

2) Vide notam p. 501. F. R.

terminorum numero existente $= q$, tum hinc vel omnia residua quadratorum $\alpha, \beta, \gamma, \delta, \varepsilon, \ldots \lambda$ resultabunt vel eorum tantum semissis vel pars tertia vel pars quarta aliave aliquota; simulque perspicitur, quot ab initio diversa prodierint, eadem deinceps eodem ordine continuo repetitum iri. Semper autem termini sequentes βr^{q-1}, βr^q, βr^{q+1} etc. eadem residua reproducent $\alpha, \beta, \beta r$ etc., quae initio habentur.

26. Quoties ergo q est numerus primus existente $p = 2q + 1$, tum progressio geometrica ex binis quadratorum residuis quibusque α et β formata et ad q terminos continuata

$$\alpha, \beta, \beta r, \beta r^2, \beta r^3, \ldots \beta r^{q-2}$$

omnium plane quadratorum residua exhibebit nullo neque excluso neque repetito. Omnia ergo reliqua residua $\gamma, \delta, \varepsilon, \ldots \lambda$ cum tali quopiam termino βr^n, ut sit $n < q - 1$, convenient. Sin autem numerus q fuerit compositus, puta $q = mn$ et $p = 2mn + 1$, tum evenire potest, ut non omnia residua quadratorum sic prodeant, sed tantum eiusmodi pars aliquota ipsius q, qualem eius indoles admittit. Quod si usu venit, tota progressio geometrica q terminis constans quasi sponte in duo plurave membra distinguitur, in quibus eadem residua recurrunt.

27. Cum sit $\frac{\beta}{\alpha} = r$ ideoque $\beta = \alpha r$, nostra progressio geometrica hoc modo expressa magis fit perspicua

$$\alpha, \alpha r, \alpha r^2, \alpha r^3, \ldots \alpha r^{q-1};$$

cuius omnes termini quia sunt per α multiplicati, hoc factore communi praetermisso progressio simplicius ita exhiberi potest. Proposito scilicet divisore primo $p = 2q + 1$ si residuum quodcumque fuerit α, singuli termini huius progressionis geometricae

$$1, \alpha, \alpha^2, \alpha^3, \alpha^4, \ldots \alpha^{q-1},$$

quorum numerus est $= q$, inter residua quadratorum reperiuntur, ac si omnes ad diversas species pertineant, etiam universam residuorum classem implent. Fieri autem potest, uti vidimus, ut non omnia residua hoc modo prodeant, sed totius classis tantum pars aliquota, dum eadem post certam periodum iterum repetuntur, reliqua vero hinc prorsus excluduntur.

28. Sive autem omnia quadratorum residua ex hac progressione geometrica nascantur sive quaedam tantum pars aliquota, ea, quae terminis istius progressionis continentur, tam insignibus proprietatibus sunt praedita, ut operae omnino pretium sit eas accuratius evolvere. Primum igitur observo, si haec progressio geometrica ulterius continuetur, terminos sequentes α^q, α^{q+1}, α^{q+2} etc. aequivalere primis 1, α, α^2 etc., propterea quod $\alpha^q - 1$ dividi certe potest per divisorem primum $p = 2q + 1$. Adiecto ergo termino sequente α^q unitati aequivalente, ita ut habeamus

$$1,\ \alpha,\ \alpha^2,\ \alpha^3,\ \ldots\ \alpha^{q-3},\ \alpha^{q-2},\ \alpha^{q-1},\ 1,$$

quia productum ex primo termino in ultimum est $= 1$, ex natura progressionis geometricae sequitur etiam producta ex secundo α in penultimum α^{q-1}, item ex tertio α^2 in antepenultimum α^{q-2} et in genere ex binis ab extremis aequidistantibus α^m et α^{q-m} ad unitatem reduci.

29. Dato ergo quocumque residuo α inter reliqua unum reperietur β, ita ut productum $\alpha\beta$ unitati aequivaleat seu sit $\beta = \frac{1+np}{\alpha}$, unde id facile invenitur. Quia igitur haec duo residua α et β tali vinculo inter se colligantur, ea *sociata*[1]) nominabo; ex quo superioris progressionis geometricae bini termini ab extremis aequidistantes huiusmodi bina residua sociata suppeditant. Terminus scilicet penultimus α^{q-1} aequivalet ipsi β, antepenultimus α^{q-2} ipsi β^2, et ita porro; unde si sociata subscribantur hoc modo

$$1,\ \alpha,\ \alpha^2,\ \alpha^3,\ \ldots\ \alpha^{q-3},\ \alpha^{q-2},\ \alpha^{q-1},\ 1,$$

$$1,\ \beta,\ \beta^2,\ \beta^3,\ \ldots\ \beta^{q-3},\ \beta^{q-2},\ \beta^{q-1},\ 1,$$

inferior series congruit cum superiori retro scripta. Semper autem residuum unitati associatum quoque est unitas.

30. Consideratio horum residuorum sociatorum aperit nobis viam ad insignes proprietates detegendas. Cum enim posito divisore primo $p = 2q + 1$ sit numerus omnium residuorum $= q$, quorum cuilibet praeter unitatem convenit suum sociatum, unitate exclusa reliqua, quorum numerus est $= q - 1$, secundum hanc sociationem in paria distribui possunt binis sociatis invicem

1) Vide § 20 Commentationis praecedentis, ubi talia residua *reciproca* nominantur. F. R.

iungendis. Hinc si $q-1$ fuerit numerus impar ac propterea q par, necesse est, ut in hac distributione idem residuum, puta δ, bis occurrat. Verum idem residuum δ duobus diversis residuis associari nequit; si enim esset $\alpha\delta = 1$ et $\beta\delta = 1$, residua α et β non discreparent. Quare nihil aliud relinquitur, nisi ut idem residuum δ secum ipsum associetur sitque idcirco $\delta\delta = 1$, unde fit vel $\delta = 1$ vel $\delta = -1$; sed quia unitas iam est seposita, necesse est hoc casu, quo q est numerus par, inter residua reperiri -1 vel $p-1$.

31. En ergo egregiam demonstrationem veritatis supra[1]) iam observatae, quod, si divisor primus sit $p = 4m+1$ ideoque $q = 2m$, inter residua necessario occurrat -1 seu semper exhiberi queat quadratum aa, ut $aa+1$ per illum numerum primum $p = 4m+1$ dividi possit. Hinc simul patet, si inter residua sit numerus α, ibidem quoque productum $-1\cdot\alpha$, nempe $-\alpha$, occurrere hincque omnia residua ad minimam formam reducta tam positive quam negative adesse, omnino uti in exemplis § 14 allatis perspicitur. Simul vero etiam patet, si fuerit $p = 4m+3$ ideoque residuorum multitudo impar, ibi -1 locum habere non posse, quia tum singula residua utroque signo $+$ et $-$ occurrerent ideoque eorum numerus impar esse non posset.[2]) Ex quo sequitur per huiusmodi numerum primum $p = 4m+3$ nullam binorum quadratorum summam dividi posse.

32. Pro divisoribus autem primis formae $p = 4m+1$, si quadratum aa det residuum α, aliud semper dabitur quadratum bb praebens residuum $-\alpha$; sicque horum quadratorum summa $aa+bb$ per illum numerum primum erit divisibilis, ita ut nec a nec b superet $2m$. Operae pretium ergo erit his casibus bina residua signo discrepantia iunctim exhibere simulque quadrata, unde nascuntur, adscribere.

$$p = 5 \begin{cases} +1 & 1^2 \\ -1 & 2^2 \end{cases} \qquad p = 13 \begin{cases} +1, +4, +3 & 1^2 \quad 2^2 \quad 4^2 \\ -1, -4, -3 & 5^2 \quad 3^2 \quad 6^2 \end{cases} \qquad p = 17 \begin{cases} +1, +2, +4, +8 & 1^2 \quad 6^2 \quad 2^2 \quad 5^2 \\ -1, -2, -4, -8 & 4^2 \quad 7^2 \quad 8^2 \quad 3^2 \end{cases}$$

1) Scilicet theoremate 5 Commentationis praecedentis. Vide imprimis eiusdem Commentationis § 36 atque notas ibi adiectas.. F. R.

2) Vide theorema 4 Commentationis praecedentis. F. R.

$$1^2 \quad 2^2 \quad 11^2 \quad 8^2 \quad 6^2 \quad 3^2 \quad 10^2$$

$$p = 29 \begin{cases} +1, +4, +5, +6, +7, +9, +13 \\ -1, -4, -5, -6, -7, -9, -13 \end{cases}$$

$$12^2 \quad 5^2 \quad 13^2 \quad 9^2 \quad 14^2 \quad 7^2 \quad 4^2$$

$$1^2 \quad 15^2 \quad 2^2 \quad 9^2 \quad 3^2 \quad 11^2 \quad 14^2 \quad 7^2 \quad 4^2$$

$$p = 37 \begin{cases} +1, +3, +4, +7, +9, +10, +11, +12, +16 \\ -1, -3, -4, -7, -9, -10, -11, -12, -16 \end{cases}$$

$$6^2 \quad 16^2 \quad 12^2 \quad 17^2 \quad 18^2 \quad 8^2 \quad 10^2 \quad 5^2 \quad 13^2$$

$$1^2 \quad 17^2 \quad 2^2 \quad 13^2 \quad 7^2 \quad 3^2 \quad 16^2 \quad 4^2 \quad 10^2 \quad 15^2$$

$$p = 41 \begin{cases} +1, +2, +4, +5, +8, +9, +10, +16, +18, +20 \\ -1, -2, -4, -5, -8, -9, -10, -16, -18, -20 \end{cases}$$

$$9^2 \quad 11^2 \quad 18^2 \quad 6^2 \quad 19^2 \quad 14^2 \quad 20^2 \quad 5^2 \quad 8^2 \quad 12^2$$

33. Hinc evidens est pro divisore primo $p = 4m + 1$ tot modis, quot m continet unitates, bina quadrata radices limitem $2m$ non superantes habentia assignari posse, quorum summa sit divisibilis per numerum p. In his autem binis quadratis nulla lex, qua inter se cohaereant, perspicitur aliorumque summa modo maior reperitur modo minor ac minima quidem ubique ipsi numero p est aequalis. Num autem semper talis binorum quadratorum summa divisori p aequalis detur, hinc non facile demonstrari posse videtur. Cum autem ex alio fonte demonstraverim[1]) binorum quadratorum summam alios non admittere divisores, nisi qui ipsi sint binorum quadratorum summae, quoniam hic evictum est semper dari binorum quadratorum summas, quae sint per numerum primum $p = 4m + 1$ divisibiles, iam certo constat omnes numeros primos formae $4m + 1$ esse summam duorum quadratorum. Praesens autem supplementum demonstrationem huius propositionis mirifice contrahit. Olim[2]) enim nonnisi per multas ambages ostendi dari semper eiusmodi binorum quadratorum summas, quae sint per quemlibet numerum primum formae $4m + 1$ divisibiles, id quod hic in aprico est positum.

1) Vide notam 1 p. 508. F. R.

2) Scilicet Commentationibus 228 et 241 nota 1 p. 504 laudatis. Vide etiam notam 2 p. 508. F. R.

34. Data autem duorum quadratorum summa $aa + bb$ per numerum primum p divisibili alias inde binorum quadratorum summas idem praestantes facile reperire licet.

1. Si numeri a et b communem habeant divisorem, ut sit $a = nc$ et $b = nd$, etiam summa quadratorum $cc + dd$ per p erit divisibilis.

2. Si numeri a et b ambo sint impares ideoque $\frac{a+b}{2}$ et $\frac{a-b}{2}$ numeri integri, etiam horum quadratorum summa per p divisionem admittet; semissis autem ea est praecedentis.

3. Tum vero etiam hae quadratorum summae $(p-a)^2 + (p-b)^2$ vel $a^2 + (p-b)^2$ per p erunt divisibiles; unde si radices communem sortiantur divisorem, eo ad formam minorem redigi possunt.

4. Si ergo sint ambo impares $a = 2c + 1$ et $b = 2d + 1$, ob $p = 4m + 1$ horum quadratorum summa $(2m-c)^2 + (2m-d)^2$ erit [per p] divisibilis; et si alter par $a = 2c$, alter impar $b = 2d + 1$, haec summa $cc + (2m-d)^2$ erit per p divisibilis; hocque modo continuo plures huiusmodi binorum quadratorum summas invenire licet.

35. Exemplo haec fient clariora. Sumto igitur divisore $p = 41$ inventa sit summa duorum quadratorum $17^2 + 11^2$ per eum divisibilis, ut sit $a = 17$ et $b = 11$, atque per has regulas sequentes valores alii pro a et b reperientur

$$p = 41 \begin{cases} a = 17, 24 & 4, 4 & 1, 40 & 5 \\ b = 11, 30 & 5, 36 & 9, 32 & 4 \end{cases}$$

Tum vero porro ex casu, quo alteruter numerorum est $= 1$, alteri valor quicumque tribui alterque ita definiri potest, ut infra $\frac{1}{2}p$ subsistat. Scilicet invento casu $a = 1$ et $b = 9$ satisfacit quoque $a = m$ et $b = 9m$, ubi loco b sumi potest $9m - np$ seu $np - 9m$, ita ut b infra $\frac{1}{2}p$ deprimatur; sicque pro a omnes numeros accipere licebit

$a = 1$	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16 etc.
$b = 9$	18	14	5	4	13	19	10	1	8	17	15	6	3	12	20 etc.

Desideratur ergo methodus inter omnes hos binos valores litterarum a et b

eos inveniendi, quorum quadratorum summa sit minima, ut deinceps demonstretur hanc summam ipsi divisori 41 certe fore aequalem; quod quidem praesenti casu evenit, si litterarum a et b valores sint 4 et 5.

36. Revertor autem ad eam residuorum ex quadratis oriundorum dispositionem, qua ea secundum progressionem geometricam disponi posse observavi. Sit igitur divisor primus $p = 2q + 1$ et residua inde ex quadratis orta ordine quocumque scripta

$$1, \alpha, \beta, \gamma, \delta, \ldots \lambda,$$

quorum multitudo est $= q$, atque sequentes progressiones geometricae omnes in his residuis continebuntur

$$\begin{gathered} 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \ldots \alpha^{q-1}, \\ 1, \beta, \beta^2, \beta^3, \beta^4, \ldots \beta^{q-1}, \\ 1, \gamma, \gamma^2, \gamma^3, \gamma^4, \ldots \gamma^{q-1}, \\ 1, \delta, \delta^2, \delta^3, \delta^4, \ldots \delta^{q-1} \\ \text{etc.,} \end{gathered}$$

in quibus omnibus termini sequentes α^q, β^q, γ^q, δ^q, $\ldots$ λ^q unitati aequivalebunt, quippe qui omnes unitate minuti per divisorem p erunt divisibiles. Huiusmodi ergo progressiones geometricas tot exhibere licet, quot unitates in q continentur, in iisque omnibus nullus terminus occurret, qui non inter residua $1, \alpha, \beta, \gamma, \ldots \lambda$ reperiatur.

37. Evenire autem potest, ut supra [§ 24] est ostensum, ut non omnes istae progressiones geometricae, etiamsi cuiusque terminorum numerus sit $= q$, omnia residua praebeant, sed tantum eorum vel semissem vel trientem vel etiam quampiam partem aliquotam; quod quibus casibus contingat, accuratius est perpendendum.

Primum igitur observo, si q fuerit numerus primus, hoc nullo modo usu venire posse; si enim in huiusmodi progressione geometrica q terminorum non omnia residua occurrant, eorum, quae occurrunt, singula vel bis vel ter vel aliquoties occurrant necesse est. Unde si q est numerus primus, quaelibet progressio geometrica omnia residua diversa numero q complectitur. Ita si

$p = 11$ et $q = 5$, ex quinque residuis

$$1,\ 4,\ -2,\ 5,\ 3$$

ab unitate incipiendo hae quatuor progressiones geometricae formantur

$1,\ 4,\ 4^2,\ 4^3,\ 4^4$	$1,\ -2,\ 2^2,\ -2^3,\ 2^4$
seu $1,\ 4,\ 5,\ -2,\ 3$	seu $1,\ -2,\ 4,\ 3,\ 5$
$1,\ 5,\ 5^2,\ 5^3,\ 5^4$	$1,\ 3,\ 3^2,\ 3^3,\ 3^4$
seu $1,\ 5,\ 3,\ 4,\ -2$	seu $1,\ 3,\ -2,\ 5,\ 4$

Ubi singula residua per omnia loca variantur praeter primum.

38. Hinc evidens est ex qualibet harum progressionum geometricarum reliquas facile formari posse, dum ex illa per saltum transiliendo vel unum vel duos vel plures terminos termini excerpuntur hac numeratione, cum ad finem fuerit perventum, iterum ab initio instituta. Ita si casum sumamus, quo $p = 23$ et $q = 11$ ac residua

$$1,\ 4,\ 9,\ -7,\ 2,\ -10,\ 3,\ -5,\ -11,\ 8,\ 6,$$

una progressione geometrica formata, cuius terminis indices inscribo, quo deinceps reliquae terminis per saltum excerpendis facilius exhiberi queant, decem progressiones geometricae ita se habebunt:

												Seq.
1.	Indices	0,	1,	2,	3,	4,	5,	6,	7,	8,	9,	10	0
	Progressio	1,	4,	−7,	−5,	3,	−11,	2,	8,	9,	−10,	6	1
2.	Indices	0,	2,	4,	6,	8,	10,	1,	3,	5,	7,	9	0
	Progressio	1,	−7,	3,	2,	9,	6,	4,	−5,	−11,	8,	−10	1
3.	Indices	0,	3,	6,	9,	1,	4,	7,	10,	2,	5,	8	0
	Progressio	1	−5,	2,	−10,	4,	3,	8,	6,	−7,	−11,	9	1
4.	Indices	0,	4,	8,	1,	5,	9,	2,	6,	10,	3,	7	0
	Progressio	1,	3,	9,	4,	−11,	−10,	−7,	2,	6,	−5,	8	1
5.	Indices	0,	5,	10,	4,	9,	3,	8,	2,	7,	1,	6	0
	Progressio	1,	−11,	6,	3,	−10,	−5,	9,	−7,	8,	4,	2	1

6.	Indices	0,	6,	1,	7,	2,	8,	3,	9,	4,	10,	5	0
	Progressio	1,	2,	4,	8,	−7,	9,	−5,	−10,	3,	6,	−11	1
7.	Indices	0,	7,	3,	10,	6,	2,	9,	5,	1,	8,	4	0
	Progressio	1,	8,	−5,	6,	2,	−7,	−10,	−11,	4,	9,	3	1
8.	Indices	0,	8,	5,	2,	10,	7,	4,	1,	9,	6,	3	0
	Progressio	1,	9,	−11,	−7,	6,	8,	3,	4,	−10,	2,	−5	1
9.	Indices	0,	9,	7,	5,	3,	1,	10,	8,	6,	4,	2	0
	Progressio	1,	−10,	8,	−11,	−5,	4,	6,	9,	2,	3,	−7	1
10.	Indices	0,	10,	9,	8,	7,	6,	5,	4,	3,	2,	1	0
	Progressio	1,	6,	−10,	9,	8,	2,	−11,	3,	−5,	−7,	4	1

Indices scilicet hic ultra 11 ascensuri subtrahendo 11 sunt depressi. Hic porro observari convenit bina residua, quorum indices iuncti faciunt 11 seu in genere q, esse inter se sociata eorumque productum unitati aequivalere. Hoc nempe casu residua sociata sunt

$$4,\ -7,\ -5,\ 3,\ -11,$$
$$6,\ -10,\ 9,\ 8,\ 2.$$

39. Consideremus nunc quoque casus, quibus q est numerus compositus ac primo quidem duplus cuiuspiam numeri primi. Ab exemplo exordiamur, quo $p = 13$ et $q = 6 = 2 \cdot 3$ ac residua haec

$$1,\ 4,\ -4,\ 3,\ -1,\ -3,$$

unde hae quinque progressiones geometricae formentur

$$\text{I.}\ 1,\ 4,\ 3,\ -1,\ -4,\ -3,$$
$$\text{II.}\ 1,\ -4,\ 3,\ 1,\ -4,\ 3,$$
$$\text{III.}\ 1,\ 3,\ -4,\ 1,\ 3,\ -4,$$
$$\text{IV.}\ 1,\ -1,\ 1,\ -1,\ 1,\ -1,$$
$$\text{V.}\ 1,\ -3,\ -4,\ -1,\ 3,\ 4.$$

Ubi prima et quinta omnia continent residua, secunda vero et tertia eorum tantum semissem 1, −4, 3, quae bis repetuntur reliquis −1, +4, −3 exclusis, quarta vero duo tantum habet +1 et −1 ter repetita.

Similis ratio deprehenditur in casu $p = 29$ et $q = 14 = 2 \cdot 7$, quo residua sunt

$$1,\ -1,\ 4,\ -4,\ 5,\ -5,\ 6,\ -6,\ 7,\ -7,\ 9,\ -9,\ 13,\ -13,$$

unde hae progressiones geometricae formantur

I. 1, −1,| 1, −1,| 1, −1,| 1, −1,| 1, −1,| 1, −1,| 1, −1,

II. 1, 4, −13, 6, −5, 9, 7, −1, −4, 13, −6, 5, −9, −7,

III. 1, −4, −13, 6, −5, −9, 7,| 1, −4, −13, −6, −5, −9, 7,

IV. 1, 5, −4, 9, −13, −7, −6, −1, −5, 4, −9, 13, 7, 6,

V. 1, −5, −4, −9, −13, 7, −6,| 1, −5, −4, −9, −13, 7, −6,

VI. 1, 6, 7, 13, −9, 4, −5, −1, −6, −7, −13, 9, −4, 5,

VII. 1, −6, 7, −13, −9, −4, −5,| 1, −6, 7, −13, −9, −4, −5,

VIII. 1, 7, −9, −5, −6, −13, −4,| 1, 7, −9, −5, −6, −13, −4,

IX. 1, −7, −9, 5, −6, 13, −4, −1, 7, 9, −5, 6, −13, 4,

X. 1, 9, −6, 4, 7, 5, −13, −1, −9, 6, −4, −7, −5, 13,

XI. 1, −9, −6, −4, 7, −5, −13,| 1, −9, −6, −4, 7, −5, −13,

XII. 1, 13, −5, −7, −4, 6, −9, −1, −13, 5, 7, 4, −6, 9,

XIII. 1, −13, −5, 7, −4, −6, −9,| 1, −13, −5, 7, −4, −6, −9.

40. Antequam hinc quicquam concludimus, evolvamus etiam casum, quo q est productum ex aliis binis numeris primis. Sit ergo divisor $p = 31$ et $q = 15 = 3 \cdot 5$, quo casu residua sunt

$$1,\ 4,\ 9,\ -15,\ -6,\ 5,\ -13,\ 2,\ -12,\ 7,\ -3,\ -11,\ 14,\ 10,\ 8,$$

unde sequentes progressiones geometricae formantur, ubi quidem cuique suam sociatam retro dispositam adiungo,

I. 1, 4, −15, 2, 8,| 1, 4, −15, 2, 8,| 1, 4, −15, 2, 8,

II. 1, 8, 2, −15, 4,| 1, 8, 2, −15, 4,| 1, 8, 2, −15, 4,

III. 1, 9, −12, −15, −11, −6, 8, 10, −3, 4, 5, 14, 2, −13, 7

IV. 1, 7, −13, 2, 14, 5, 4, −3, 10, 8, −6, −11, −15, −12, 9,

V. 1, 2, 4, 8, −15,| 1, 2, 4, 8, −15,| 1, 2, 4, 8, −15,

VI. 1, −15, 8, 4, 2,| 1, −15, 8, 4, 2,| 1, −15, 8, 4, 2,

VII.	1,	−3,	9,	4,	−12,	5,	−15,	14,	−11,	2,	−6,	−13,	8,	7,	10,
VIII.	1,	10,	7,	8,	−13,	−6,	2,	−11,	14,	−15,	5,	−12,	4,	9,	−3,
IX.	1,	5,	−6,	1,	5,	−6,	1,	5,	−6,	1,	5,	−6,	1,	5,	−6,
X.	1,	−6,	5,	1,	−6,	5,	1,	−6,	5,	1,	−6,	5,	1,	−6,	5,
XI.	1,	−11,	−3,	2,	9,	−6,	4,	−13,	−12,	8,	5,	7,	−15,	10,	14,
XII.	1,	14,	10,	−15,	7,	5,	8,	−12,	−13,	4,	−6,	9,	2,	−3,	−11,
XIII.	1,	−12,	−11,	8,	−3,	5,	2,	7,	9,	−15,	−6,	10,	4,	14,	−13,
XIV.	1,	−13,	14,	4,	10,	−6,	−15,	9,	7,	2,	5,	−3,	8,	−11,	−12.

41. Has progressiones geometricas intuenti mox patet earum alias esse completas, quarum termini omnia residua exhibeant, alias vero esse periodicas, quae scilicet duabus pluribusve periodis constent, in quibus eadem residua eodem ordine recurrant, quam distinctionem inter progressiones completas et periodicas probe notasse iuvabit. Periodicae scilicet locum inveniunt, quando posito divisore primo $p = 2q + 1$ numerus q in duos factores est resolubilis, ut sit $q = mn$; tum enim eiusmodi progressiones geometricae dabuntur, quae continent m periodos qualibet n residua complectente; ac tales quidem assignari poterunt tot, quot numerus $n - 1$ continet unitates. Cum enim in eadem periodo cuiusque termini omnes potestates occurrant, evidens est quemque pro denominatore sumtum similem progressionem periodicam producere, nisi forte periodorum numerus adeo duplicetur vel multiplicetur, hoc est in duas pluresve periodos subdividatur.

42. Ex progressione autem completa, quaecumque ea sit, facile reliquae omnes, sive sint completae sive periodicae, formantur. Sit enim divisor primus $p = 2q + 1$ haecque progressio completa

$$\begin{aligned} &\text{indices} \quad 0,\ 1,\ 2,\ 3,\ 4,\ 5,\ \ldots\ q-1, \\ &\text{progressio} \quad 1,\ \alpha,\ \alpha^2,\ \alpha^3,\ \alpha^4,\ \alpha^5,\ \ldots\ \alpha^{q-1}; \end{aligned}$$

si hinc excerpantur per saltus aequales termini

$$\begin{aligned} &0,\ n,\ 2n,\ 3n,\ 4n,\ \ldots\ nq-n, \\ &1,\ \alpha^n,\ \alpha^{2n},\ \alpha^{3n},\ \alpha^{4n},\ \ldots\ \alpha^{nq-n}, \end{aligned}$$

haec progressio erit completa, si numerus n ad q fuerit primus; sin autem n et q habeant communem divisorem, puta d, tum haec progressio totidem habebit periodos, in quarum singulis eadem residua numero $\frac{q}{d}$ recurrent, reliqua autem inde prorsus excludentur. Numerus autem harum periodorum maximo communi divisore inter n et q definietur. At vero vicissim ex progressione periodica non licet progressionem completam formare.

43. Imprimis autem hic notari meretur in omnibus his progressionibus summam omnium terminorum semper esse nihilo aequalem seu per divisorem p divisibilem, quod hoc modo demonstratur. Cum $\alpha^q - 1$ per p divisionem admittat, haec autem forma in factores resolvatur

$$\alpha - 1 \quad \text{et} \quad 1 + \alpha + \alpha^2 + \alpha^3 + \cdots + \alpha^{q-1},$$

quorum ille $\alpha - 1$ certe non per p est divisibilis, necesse est hunc alterum, hoc est summam totius nostrae progressionis, per numerum p divisionem admittere. Ac si progressio habeat periodos, termini cuiusque periodi iunctim sumti seu summa omnium residuorum inde oriundorum per p erit divisibilis, id quod in exemplis supra allatis per se est manifestum.

44. Ex eodem autem fonte colligitur, si progressio geometrica fuerit completa et q habeat factorem m, ut sit $q = mn$ et divisor primus $p = 2mn + 1$, tum ob formam $\alpha^{mn} - 1$ divisibilem per $\alpha^m - 1$, quae per p divisibilis non existit, quia progressio alioquin completa non foret, quotum inde ortum

$$1 + \alpha^m + \alpha^{2m} + \alpha^{3m} + \cdots + \alpha^{(n-1)m}$$

per divisorem p fore divisibilem. Quamobrem si tota progressio in membra distribuatur hoc modo

$$1, \alpha, \ldots \alpha^{m-1} \mid \alpha^m, \alpha^{m+1}, \ldots \alpha^{2m-1} \mid \alpha^{2m}, \alpha^{2m+1}, \ldots \alpha^{3m-1} \mid \ldots \mid \alpha^{(n-1)m}, \ldots \alpha^{mn-1},$$

quorum membrorum numerus est n, haecque membra ita sibi subscribantur

$$\begin{array}{llll}
1, & \alpha, & \alpha^2, & \ldots \alpha^{m-1}, \\
\alpha^m, & \alpha^{m+1}, & \alpha^{m+2}, & \ldots \alpha^{2m-1}, \\
\alpha^{2m}, & \alpha^{2m+1}, & \alpha^{2m+2}, & \ldots \alpha^{3m-1}, \\
\vdots & \vdots & \vdots & \vdots \\
\alpha^{(n-1)m}, & \alpha^{(n-1)m+1}, & \alpha^{(n-1)m+2}, & \ldots \alpha^{nm-1},
\end{array}$$

tum summae terminorum in qualibet columna verticali positorum ad nihilum reducentur seu per divisorem primum $p = 2mn + 1$ divisibiles erunt. Tot autem diversis modis progressio completa in huiusmodi membra distribui potest, quot numerus q habuerit divisores.

45. Prima autem columna verticalis simul dabit periodos pro omnibus progressionibus periodicis. De his numeris tenendum est eos non solum esse residua quadratorum, sed etiam altiorum potestatum parium. Scilicet si divisor primus sit huius formae $p = 2mn + 1$, quemadmodum inter numeros ipso minores, quorum multitudo est $= 2mn$, tantum semissis mn in residuis quadratorum occurrit totidemque inde excluduntur, ita potestates exponentis $2m$ per eundem numerum p dividendo tantum n diversa residua inde resultant et reliqui omnes, quorum multitudo est $(2m - 1)n$, ita sunt comparati, ut in forma $a^{2m} - ip$ nullo modo contineantur seu nulla exhiberi possit potestas exponentis $2m$, quae ullo istorum numerorum minuta per numerum primum $p = 2mn + 1$ fiat divisibilis.

46. Neque vero haec proprietas ad potestates exponentium parium est adstricta, sed in genere pronunciare licet, si divisor primus sit formae $p = mn + 1$, qui scilicet unitate minutus in factores m et n resolvi possit, ac potestates exponentis m, nempe

$$1,\ 2^m,\ 3^m,\ 4^m,\ 5^m,\ 6^m,\ \ldots\ (p-1)^m,$$

per eum dividantur, tum inter residua tantum n diversos numeros occurrere, quorum singuli m vicibus repetantur, reliqui autem numeri omnes, quorum multitudo est $(m - 1)n$, hinc excludantur; ex quo insignes proprietates numerorum, qui sunt potestates, ratione divisibilitatis per numeros primos agnoscere licet.[1])

47. Quoniam igitur nullum est dubium, quin hinc multae praeclarae numerorum proprietates erui queant, exempla plurium numerorum primorum hic adiicere visum est pro iisque residua, quae ex divisione potestatum nascuntur, exhibere, ubi quidem sociata iunctim repraesentantur:

1) Confer theorema 13 Commmentationis 134 nota p. 501 laudatae nec non theorema 19 Commentationis 262 nota p. 240 laudatae. Vide etiam Prooemium vnluminis praecedentis, p. XXXI—XXXII. F. R.

1. Divisor $p = 3 = 2 + 1$

Potestates	Residuum
a^2	$\{1$

2. Divisor $p = 5 = 2 \cdot 2 + 1$

Potestates	Residua
a^2	$\{1, -1$
a^4	$\{1$

3. Divisor $p = 7 = 2 \cdot 3 + 1$

Potestates	Residua
a^2	$\begin{cases} 1, & 2 \\ & -3 \end{cases}$
a^3	$\{1, -1$
a^6	$\{1$

4. Divisor $p = 11 = 2 \cdot 5 + 1$

Potestates	Residua
a^2	$\begin{cases} 1, & 4, & 5, \\ & 3, & -2 \end{cases}$
a^5	$\{1, -1$
a^{10}	$\{1$

5. Divisor $p = 13 = 2 \cdot 2 \cdot 3 + 1$

Potestates	Residua
a^2	$\begin{cases} 1, & 4, & 3, & -1 \\ & -3, & -4 \end{cases}$
a^3	$\begin{cases} 1, & -5, & -1 \\ & 5 \end{cases}$
a^4	$\begin{cases} 1, & 3 \\ & -4 \end{cases}$
a^6	$\{1, -1$
a^{12}	$\{1$

6. Divisor $p = 17 = 2^4 + 1$

Potestates	Residua
a^2	$\begin{cases} 1, & 2, & 4, & 8, & -1 \\ & -8, & -4, & -2 \end{cases}$
a^4	$\begin{cases} 1, & 4, & -1 \\ & -4 \end{cases}$
a^8	$\{1, -1$
a^{16}	$\{1$

7. Divisor $p = 19 = 2 \cdot 3 \cdot 3 + 1$

Potestates	Residua
a^2	$\begin{cases} 1, & 4, & -3, & 7, & 9 \\ & 5, & 6, & -8, & -2 \end{cases}$
a^3	$\begin{cases} 1, & 8, & 7, & -1 \\ & -7, & -8 \end{cases}$
a^6	$\begin{cases} 1, & 7 \\ & -8 \end{cases}$
a^9	$\{1, -1$

8. Divisor $p = 23 = 2 \cdot 11 + 1$

Potestates	Residua
a^2	$\begin{cases} 1, & 4, & -7, & -5, & 3, & -11 \\ & 6, & -10, & 9, & 8, & 2 \end{cases}$
a^{11}	$\{1, -1$

9. Divisor $p = 29 = 2 \cdot 2 \cdot 7 + 1$

Potestates	Residua
a^2	$\begin{cases} 1, & 4, -13, & 6, -5, & 9, & 7, -1 \\ & -7, -9, & 5, -6, & 13, & -4 \end{cases}$
a^4	$\begin{cases} 1, & -13, -5, & 7 \\ & -9, -6, & -4 \end{cases}$
a^7	$\begin{cases} 1, & 12, -1 \\ & -12 \end{cases}$
a^{14}	$\{1, -1$

---

10. Divisor $p = 31 = 2 \cdot 3 \cdot 5 + 1$

Potestates	Residua
a^2	$\begin{cases} 1, & 9, -12, -15, -11, -6, 8, & 10 \\ & 7, -13, & 2, & 14, & 5, 4, -3 \end{cases}$
a^3	$\begin{cases} 1, & -4, -15, -2, & 8, -1 \\ & -8, & 2, & 15, & 4 \end{cases}$
a^5	$\begin{cases} 1, & -5, -6, -1 \\ & 6, & 5 \end{cases}$
a^6	$\begin{cases} 1, & 2, & 4 \\ & -15, & 8 \end{cases}$
a^{10}	$\begin{cases} 1, & 5 \\ & -6 \end{cases}$
a^{15}	$\{1, -1$

11. Divisor $p = 37 = 2 \cdot 2 \cdot 3 \cdot 3 + 1$

Potestates	Residua
a^2	$\begin{cases} 1, & 4, & 16, & -10, & -3, & -12, & -11, & -7, & 9, & -1 \\ -9, & 7, & 11, & 12, & 3, & 10, & -16, & -4 \end{cases}$
a^3	$\begin{cases} 1, & 8, & -10, & -6, & -11, & -14, & -1 \\ 14, & 11, & 6, & 10, & -8 \end{cases}$
a^4	$\begin{cases} 1, & 16, & -3, & -11, & 9 \\ 7, & 12, & 10, & -4 \end{cases}$
a^6	$\begin{cases} 1, & -10, & -11, & -1 \\ 11, & 10 \end{cases}$
a^9	$\begin{cases} 1, & -6, & -1 \\ 6 \end{cases}$
a^{12}	$\begin{cases} 1, & -11 \\ 10 \end{cases}$
a^{18}	$\{1, -1$

12. Divisor $p = 41 = 2^3 \cdot 5 + 1$

Potestates	Residua
a^2	$\begin{cases} 1, & -2, & 4, & -8, & 16, & 9, & -18, & -5, & 10, & -20, & -1 \\ 20, & -10, & 5, & 18, & -9, & -16, & 8, & -4, & 2 \end{cases}$
a^4	$\begin{cases} 1, & 4, & 16, & -18, & 10, & -1 \\ -10, & 18, & -16, & -4 \end{cases}$
a^5	$\begin{cases} 1, & -3, & 9, & 14, & -1 \\ -14, & -9, & 3 \end{cases}$
a^8	$\begin{cases} 1, & 16, & 10 \\ 18, & -4 \end{cases}$
a^{10}	$\begin{cases} 1, & 9, & -1 \\ -9 \end{cases}$
a^{20}	$\{1, -1$

13. Divisor $p = 43 = 2 \cdot 3 \cdot 7 + 1$

Potestates	Residua
a^2	1, 9, −5, −2, −18, 10, 4, −7, −20, −8, 14
	−19, 17, 21, −12, 13, 11, 6, 15, 16, −3
a^3	1, 8, 21, −4, 11, 2, 16, −1
	−16, −2, −11, 4, −21, −8
a^6	1, 21, 11, 16
	−2, 4, −8
a^7	1, −6, −7, −1
	7, 6
a^{14}	1, −7
	6
a^{21}	1, −1

14. Divisor $p = 47 = 2 \cdot 23 + 1$

Potestates	Residua
a^2	1, 4, 16, 17, 21, −10, 7, −19, 18, −22, 6, −23
	12, 3, −11, 9, 14, −20, −5, −13, −15, 8, 2
a^{23}	1, −1

15. Divisor $p = 53 = 2 \cdot 2 \cdot 13 + 1$

Potestates	Residua
a^2	1, 4, 16, 11, −9, 17, 15, 7, −25, 6, 24, −10, 13, −1
	−13, 10, −24, −6, 25, −7, −15, −17, 9, −11, −16, −4
a^4	1, 16, −9, 15, −25, 24, 13
	10, −6, −7, −17, −11, −4
a^{13}	1, −23, −1
	23
a^{26}	1, −1

16. Divisor $p = 59 = 2 \cdot 29 + 1$

Potestates	Residua
a^2	1, 4, 16, 5, 20, 21, 25, −18, −13, 7, 28, − 6, −24, 22, 29 15, −11, 12, 3, −14, 26, −23, 9, 17, 19, −10, 27, − 8, − 2
a^{29}	1, −1

17. Divisor $p = 61 = 2 \cdot 2 \cdot 3 \cdot 5 + 1$

Potestates	Residua
a^2	1, 4, 16, 3, 12, −13, 9, −25, 22, 27, −14, 5, 20, 19, 15, −1 −15, −19, −20, − 5, 14, −27, −22, 25, − 9, 13, −12, −3, −16, −4
a^3	1, 8, 3, 24, 9, 11, 27, −28, 20, −23, − 1 23, −20, 28, −27, −11, − 9, −24, −3, − 8
a^4	1, 16, 12, 9, 22, −14, 20, 15 −19, − 5, −27, 25, 13, − 3, − 4
a^5	1, −29, −13, 11, −14, −21, − 1 21, 14, −11, 13, 29
a^6	1, 3, 9, 27, 20, − 1 −20, −27, − 9, − 3
a^{10}	1, −13, −14, − 1 14, 13
a^{12}	1, − 3, 9 20, −27
a^{15}	1, 11, − 1 −11
a^{20}	1, −14 13
a^{30}	1, − 1

CONCLUSIO

DE POTESTATIBUS CUIUSQUE ORDINIS ET RESIDUIS IN EARUM DIVISIONE PER NUMEROS PRIMOS RELICTIS

48. Quemadmodum in his exemplis residua pro singulis potestatibus per progressiones geometricas sunt exhibita, quae simul retro continuatae bina residua sociata iunctim repraesentant, ita idem pro potestatibus primi ordinis fieri potest, ubi quidem omnes plane numeri divisore minores occurrere debent, ita ut, si divisor primus sit $p = 2q + 1$, multitudo residuorum diversorum sit $= 2q$, quae ad minimam formam reducta erunt ± 1, ± 2, ± 3, ± 4 etc. usque ad $\pm q$. Haec vero residua omnia quoque secundum progressionem geometricam disponi possunt ab unitate incipientem, dummodo pro eius denominatore seu secundo termino eiusmodi numerus accipiatur, qui omnes plane numeros producat, quod evenit, si is ita fuerit comparatus, ut nulla eius potestas, cuius exponens minor sit quam $2q$, pro residuo unitatem relinquat. Tales autem numeros[1]) pro quovis divisore dari certum est, etiamsi eos assignare maxime difficile videatur eorumque indoles ad profundissima numerorum mysteria sit referenda.

49. Sit igitur in genere pro divisore primo $p = 2q + 1$ littera a eiusmodi numerus, cuius potestates per p divisae omnes numeros ipso p minores pro residuis relinquant neque in serie geometrica

$$1,\ a,\ a^2,\ a^3,\ a^4 \text{ etc.}$$

unitas ante recurrat, quam ad potestatem a^{2q} fuerit perventum, quippe quae semper per $p = 2q + 1$ divisa unitatem relinquit, sicque omnes potestates hac minores diversa residua producant. Cum igitur potestas a^q non relinquat unitatem et $a^{2q} - 1 = (a^q + 1)(a^q - 1)$ per numerum p divisionem admittat, erit $a^q + 1$ per p divisibilis et potestas a^q residuum dabit -1; tum vero sequentes potestates a^{q+1}, a^{q+2}, a^{q+3} etc. dabunt residua $-a$, $-a^2$, $-a^3$ etc., quae ita sunt comparata, ut cum antecedentibus a^{q-1}, a^{q-2}, a^{q-3} etc. ordine

1) Quos numeros EULERUS antea *radices primitivas* appellaverat. Vide Commentationem 449 huius voluminis, imprimis § 38. F. R.

iuncta bina residua sociata exhibeant, quorum scilicet productum a^{2q} unitati aequivaleat. Sequenti ergo modo haec residua per associationem repraesentare poterimus:

Indices	0,	1,	2,	3,	4,		$q-3$,	$q-2$,	$q-1$,	q
	1,	a^1,	a^2,	a^3,	a^4,	...	a^{q-3},	a^{q-2},	a^{q-1},	-1
		$-a^{q-1}$,	$-a^{q-2}$,	$-a^{q-3}$,	$-a^{q-4}$,	...	$-a^3$,	$-a^2$	$-a$	
indices	$2q$,	$2q-1$,	$2q-2$,	$2q-3$,	$2q-4$,		$q+3$,	$q+2$,	$q+1$,	q

ubi bina residua sibi subscripta sunt inter se sociata, extrema vero $+1$ et -1 solitaria, quippe quae secum ipsa sociantur.

50. Tali progressione geometrica constituta, quae omnia residua ex potestatibus primi ordinis oriunda, hoc est omnes plane numeros, complectitur, ex ea omnia residua pro potestatibus cuiusvis ordinis innotescent, eodem scilicet divisore primo $p = 2q + 1$ retento.

Residua nimirum ex divisione quadratorum orta erunt

$$1,\ a^2,\ a^4,\ a^6,\ a^8,\ \ldots\ a^{2q-2},$$

quae indicibus tantum paribus respondent et ita per associationem exhibentur

1,	a^2,	a^4,	a^6,	a^8	etc.
	$-a^{q-2}$,	$-a^{q-4}$,	$-a^{q-6}$,	$-a^{q-8}$	etc.

in quibus ergo -1 reperietur, si q fuerit numerus par.

Pro cubis autem eos tantum terminos accipi oportet, quorum indices sunt multipla ternarii,

$$1,\ a^3,\ a^6,\ a^9 \text{ etc.}$$

Unde patet, si exponens $2q$ divisionem per 3 admittat, multitudinem residuorum ad trientem redigi, dum reliquis casibus omnia plane residua occurrunt.

Simili modo residua potestatum quartarum obtinentur ex indicibus per 4 divisibilibus seu ex his potestatibus

$$1,\ a^4,\ a^8,\ a^{12} \text{ etc.}$$

et residua potestatum quintarum ex his

$$1,\ a^5,\ a^{10},\ a^{15} \text{ etc.}$$

51. Tantum ergo opus est, ut pro quolibet divisore primo $p = 2q + 1$ idonei numeri pro a habeantur, ex cuius potestatibus omnia plane residua resultent; ad quod autem nullam certam regulam mihi esse cognitam fateri cogor. Hoc saltem observasse iuvabit, si unus huiusmodi numerus a fuerit cognitus, eius socium, qui sit b, ut $ab - 1$ per p fiat divisibile, quoque pari proprietate esse praeditum; vidimus autem hunc socium b vel per a^{2q-1} vel per $-a^{q-1}$ exhiberi posse. Ex quo concludere licet tum etiam pro a quamvis eius potestatem a^n, cuius exponens n sit ad numerum $2q$ primus, accipi posse, ubi quidem sufficit pro n numeros ipso $2q$ minores assumsisse, cum ex altioribus potestatibus eadem residua repetantur. Quoniam vero certa lex adhuc latet, pro divisoribus simplicioribus idoneos numeros pro a assumendos, ex cuius scilicet potestatibus omnia plane residua nascantur, exhibebo:

Divisores primi	Numeri pro a assumendi
$p = 3,\ q = 1$	-1
$p = 5,\ q = 2$	± 2
$p = 7,\ q = 3$	$-2, +3$
$p = 11,\ q = 5$	$+2, -3, -4, -5$
$p = 13,\ q = 6$	$\pm 2, \pm 6$
$p = 17,\ q = 8$	$\pm 3, \pm 5, \pm 6, \pm 7$
$p = 19,\ q = 9$	$+2, +3, -4, -5, -6, -9$
$p = 23,\ q = 11$	$-2, -3, -4, +5, -6, +7, -8, -9, +10, +11$
$p = 29,\ q = 14$	$\pm 2, \pm 3, \pm 8, \pm 10, \pm 11, \pm 14$
$p = 31,\ q = 15$	$+3, -7, -9, -10, +11, +12, +13, -14$
$p = 37,\ q = 18$	$\pm 2, \pm 5, \pm 13, \pm 15, \pm 17, \pm 18$
$p = 41,\ q = 20$	$\pm 6, \pm 7, \pm 11, \pm 12, \pm 13, \pm 15, \pm 17, \pm 19$

52. In casu postremo $p = 41$ ergo patet pro a minorem numerum quam 6 assumi non posse, cum in praecedentibus progressio geometrica ex minoribus numeris formari queat; unde pro hoc divisore $p = 41$ ista progressio geometrica ita se habebit:

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1,	+6,	−5,	+11,	−16,	−14,	− 2,	−12,	+10,	+19,	−9,	−13,	+ 4,	−17,	−20,	+ 3,	+18,	−15,	−8,	−7,	−1
	+7,	+8,	+15,	−18,	− 3,	+20,	+17,	− 4,	+13,	+9,	−19,	−10,	+12,	+ 2,	+14,	+16,	−11,	+5,	−6	

Hinc si ii numeri excerpantur, qui indicibus paribus respondent, habebuntur residua ex quadratis orta; sin autem ii excerpantur, qui indicibus vel per 4 vel 5 vel 8 vel 10 vel 20 [divisibilibus] conveniunt, residua pro eiusdem nominis potestatibus obtinebuntur, eaque ipsa, quae iam supra [§ 47] sunt recensita. Similisque est ratio omnium reliquorum numerorum primorum.

53. Quod autem ad multitudinem horum numerorum a attinet, observo eam quovis casu $p = 2q + 1$ aequalem esse multitudini eorum numerorum ipso p minorum, qui sint ad $2q$ primi; atque alio loco[1]) ostendi ad hanc multitudinem inveniendam numerum $2q$ in factores suos primos resolvi debere, ita ut, si fuerit

$$2q = f^\xi g^\eta h^\theta k^\varkappa,$$

sit ista multitudo

$$= (f-1)f^{\xi-1} \cdot (g-1)g^{\eta-1} \cdot (h-1)h^{\theta-1} \cdot (k-1)k^{\varkappa-1}.$$

Definita autem pro quovis numero $p = 2q + 1$ hac multitudine sint ipsi numeri ad $2q$ primi $1, \alpha, \beta, \gamma, \delta$ etc., atque si datus fuerit unus numerus a quicumque, reliqui ideoque omnes erunt

$$a,\ a^\alpha - np,\ a^\beta - np,\ a^\gamma - np,\ a^\delta - np \text{ etc.}$$

sumendo n ita, ut omnes isti numeri infra p deprimantur. Haec fortasse consideratio viam aperiet pro quovis casu hos numeros investigandi.

1) Vide Commentationem 271 (indicis Enestroemiani): *Theoremata arithmetica nova methodo demonstrata*, Novi comment. acad. sc. Petrop. 8 (1760/1), 1763, p. 74; *Leonhardi Euleri Opera omnia*, series I, vol. 2, p. 531. Vide etiam Commentationem 449 huius voluminis, imprimis § 34. F. R.