LEONHARDI EULERI OPERA OMNIA
SUB AUSPICIIS SOCIETATIS SCIENTIARUM NATURALIUM HELVETICAE
EDENDA CURAVERUNT
ANDREAS SPEISER · LOUIS GUSTAVE DU PASQUIER · HEINRICH BRANDT
SERIES PRIMA · OPERA MATHEMATICA · VOLUMEN QUARTUM

LEONHARDI EULERI

COMMENTATIONES ARITHMETICAE

VOLUMEN TERTIUM

EDIDIT

RUDOLF FUETER

AUCTORIATATE ET IMPENSIS
SOCIETATIS SCIENTIARUM NATURALIUM HELVETICAE

GENEVAE MCMXLI

STEREOTYPICE EXCUSSIT
BIRKHAEUSER BASILEAE

LEONHARDI EULERI

OPERA OMNIA

LEONHARDI EULERI
OPERA OMNIA

SUB AUSPICIIS
SOCIETATIS SCIENTIARUM NATURALIUM
HELVETICAE

EDENDA CURAVERUNT

ANDREAS SPEISER
LOUIS GUSTAVE DU PASQUIER
HEINRICH BRANDT

SERIES PRIMA

OPERA MATHEMATICA

VOLUMEN QUARTUM

AUCTORITATE ET IMPENSIS
SOCIETATIS SCIENTIARUM NATURALIUM HELVETICAE

GENEVAE MCMXLI

STEREOTYPICE EXCUSSIT
BIRKHAEUSER BASILEAE

LEONHARDI EULERI

COMMENTATIONES ARITHMETICAE

VOLUMEN TERTIUM

EDIDIT

RUDOLF FUETER

AUCTORITATE ET IMPENSIS
SOCIETATIS SCIENTIARUM NATURALIUM HELVETICAE

GENEVAE MCMXLI

STEREOTYPICE EXCUSSIT
BIRKHAEUSER BASILEAE

Reprint of the first edition published by Orell Füssli, Zürich & Leipzig, and B.G. Teubner, Leipzig & Berlin 1941

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in other ways, and storage in data banks. For any kind of use, permission of the copyright owner must be obtained.

© 2009 Birkhäuser Verlag AG, P.O. Box 133, CH-4010 Basel, Switzerland
Part of Springer Science+Business Media
Printed on acid-free paper produced from chlorine-free pulp. TCF ∞

Printed in Germany

ISBN: 978-3-7643-1403-3

9 8 7 6 5 4 3 2

VORWORT DES HERAUSGEBERS

Der vorliegende Band ist der dritte, der zahlentheoretische Abhandlungen EULERS enthält. Der nächste Band I 5 wird den Abschluß der *Commentationes arithmeticae* bringen. Beim Durchlesen von EULERS Veröffentlichungen bestrickt immer wieder der reiche Ideengehalt. Seine überraschenden Ansätze, sein genialer Spürsinn, um in einfachen Beispielen tiefe Zusammenhänge zu sehen, haben die Forschung in ungeahnter Weise befruchtet und werden sie auch in Zukunft fördern. Gerade dieser Band mit seinen zahlentheoretischen Untersuchungen bringt eine große Zahl von Belegen hierzu. Denn die Zahlentheorie entwickelt sich an „Zahlenexperimenten" und bedarf derselben, um neue Wege zu finden. Man geht wohl nicht fehl, wenn man behauptet, daß alle großen Resultate der Zahlentheorie früher und heute an Beispielen gefunden und erst nachher bewiesen wurden.

Indem ich es im folgenden unternehme, die Abhandlungen dieses Bandes zu charakterisieren, fasse ich alle diejenigen zusammen, die das gleiche Ziel verfolgen, ohne Rücksicht zu nehmen auf die chronologische Reihenfolge. Es ist bekanntlich eine typische Eigenschaft EULERS, daß er fast niemals ein einmal behandeltes Problem fallen läßt; sondern er nimmt es immer wieder auf, wobei es stets reifer und reichhaltiger gelöst wird.

Alle Arbeiten dieses Bandes sind von dem *alten* EULER verfaßt. Man tut gut, sich dies zu vergegenwärtigen. Der größte Teil der Mathematik im Momente der Abfassung war von EULER selbst geschaffen, so daß er souverän auf seine Wissenschaft blicken konnte. Die erste Abhandlung des Bandes ist 1772 der Petersburger Akademie vorgelegt worden. Sie ist nach ENESTRÖM auch in diesem Jahre, in dem EULER fünfundsechzig wurde, geschrieben worden. Die letzten Abhandlungen sind wenige Jahre vor EULERS Tod abgefaßt worden. Alle Abhandlungen von dem ENESTRÖMSCHEN Index 564 an, d. h. nach dem 1. Bande der *Opuscula analytica*, sind erst nach seinem Tode gedruckt worden. Noch bemerkenswerter ist, daß die Abhandlungen mit einem größern ENESTRÖMSCHEN Index als 708 erst nach 1800 erschienen sind. Bekanntlich ist im Jahre 1801 das GAUSSSCHE Werk *Disquisitiones arithmeticae* erschienen. Alle diese EULERSCHEN Abhandlungen konnten daher GAUSS nicht bekannt sein, insbesondere die Abhandlung 708 selbst über

die „numeri idonei“ (siehe unten). Bedenkt man, daß die *disquisitiones arithmeticae* von 1801 an für alle jüngern Mathematiker (wie z. B. LEJEUNE DIRICHLET) das Buch über Zahlentheorie war, so versteht man, daß verschiedene Abhandlungen dieses Bandes nicht den ihnen zukommenden Erfolg hatten.

Wir ordnen die Abhandlungen dieses Bandes in 6 Abschnitte:

I. NIEDERE ZAHLENTHEORIE.

Unter diesem Sammelnamen sollen die Arbeiten zusammengefaßt werden, denen ENESTRÖM die Nummern 560 (erster Abschnitt), 564 und 591 gegeben hat.

Die Abhandlung 560: „*Miscellanea analytica*“ bringt als erstes Problem den WILSONSCHEN Satz, für den EULER einen neuen Beweis führt, nachdem bekanntlich LAGRANGE den Satz zum ersten Male bewiesen hatte. Er nennt ihn „seinen“ Beweis, da dieser, wie er hübsch sagt, „more mihi familiari“ ist. Es ist der klassische Beweis des WILSONSCHEN Satzes mit Hilfe der Existenz der Primitivwurzel (mod. der Primzahl p), wie er heute überall geführt wird, ein Muster EULERSCHER Eleganz.

Die Abhandlung 564: „*Speculationes circa quasdam insignes proprietates numerorum*“ bringt eine neue Herleitung der Formel für die Funktion πD, oder wie wir heute nach GAUSS schreiben: $\varphi(D)$, d. h. der Anzahl der zu D teilerfremden Zahlen zwischen 0 und D. Mit den gleichen Betrachtungen hat er schon in Abhandlung 271[1]) die bekannte Formel berechnet. Neu ist, daß er hier entgegen der frühern Abhandlung das Funktionszeichen πD einführt. Der Beweis selbst beruht auf der grundlegenden Beziehung:

$$\varphi(PQR\ldots) = \varphi(P)\,\varphi(Q)\,\varphi(R)\ldots,$$

wobei $P, Q, R, \ldots$ paarweise zueinander teilerfremd sind. Sehr beachtenswert ist der Ansatz, den EULER macht, um am Schlusse das Wachstum der Funktion $\varphi(D)$ zu bestimmen. Er setzt:

$$s = \sum_{n=1}^{\infty} \varphi(n) x^n, \qquad \int \frac{s}{x}\,dx = \sum_{n=1}^{\infty} \frac{\varphi(n)}{n}\,x^n\,,$$

In der zweiten Reihe haben alle x^n, für die n nur durch die gleichen festen, von einander verschiedenen Primzahlen $p_1, p_2, p_3, \ldots, p_r$ teilbar ist, denselben Koeffizienten. Somit treten in ihr alle Teilsummen auf:

$$\sum_{k_1=1}^{\infty}\ \sum_{k_2=1}^{\infty}\ \sum_{k_3=1}^{\infty} \cdots \sum_{k_r=1}^{\infty} x^{p_1^{k_1} p_2^{k_2} p_3^{k_3} \ldots p_r^{k_r}}$$

auf. Meines Wissens ist dieser Ansatz nirgends weiter verfolgt worden.

1) *LEONHARDI EULERI Opera omnia*, series I, vol. 2, p. 531.

In einen elementaren Teil der Arithmetik führt die Abhandlung 591: „*De relatione inter ternas pluresve quantitates instituenda.*" Es handelt sich um die Aufgabe, zu drei gegebenen reellen Zahlen A, B, C die Gleichung:

$$Ax + By + Cz = 0$$

in ganzen rationalen Zahlen zu lösen, wobei die Zahlen A, B, C möglichst genau durch endliche Dezimalbrüche anzunähern sind. Wird die Gleichung mit einer Potenz von 10 erweitert, so liegt ein Problem für ganze rationale Zahlen vor. EULER gibt einen elementaren Algorithmus als Lösung an. Auf die Frage wurde er durch das Problem geführt, zwischen der ihn sehr beschäftigenden Summe[1]):

$$1 - \frac{1}{2^3} + \frac{1}{3^3} - \frac{1}{4^3} + \cdots$$

und den Größen $\frac{\pi^3}{6} l2$ und $(l2)^3$ eine einfache lineare Relation mit rationalen Koeffizienten zu finden, deren Existenz er vermutet. Der Algorithmus führt aber zu keinem Resultat. Seine Vermutung stützt sich auf die Beobachtung, daß wegen:

$$l2 = 1 - \frac{1}{2} + \frac{1}{3} - \cdots \quad \text{und} \quad \frac{\pi^2}{6} = 1 + \frac{1}{2^2} + \frac{1}{3^2} + \cdots$$

die obige Summe in der Reihenentwicklung für $\frac{\pi^2}{6} l2$ und $(l2)^3$ als Teilsumme auftritt. Ein Mißerfolg ist diese Arbeit auch deshalb, weil in keiner Weise auf die Vieldeutigkeit der Lösung eingegangen wird. Dagegen findet sich S. 141 dieses Bandes der Hinweis darauf, daß die Zahlen e und π weder rational, noch quadratisch irrational sind, indem sie eine Darstellung als unendliche nicht-periodische Kettenbrüche zulassen. Vgl. dazu Bd. I, 14, S. 194 und 203, wo der Kettenbruch für e angegeben ist. Derjenige für π scheint nicht bekannt zu sein.

II. QUADRATISCHE RESTE UND FORMEN

Unter die Rubrik „quadratische Reste" fallen die Abhandlungen 556 und 557 des ENESTRÖMSCHEN Verzeichnisses; Nr. 610 und Nr. 744 enthalten sowohl Ausführungen über quadratische Reste wie über quadratische Formen, während die Nummern 598 und 683 quadratische Formen allein betreffen.

Alle diese Abhandlungen sind gekennzeichnet durch das Ringen EULERS mit dem quadratischen Reziprozitätsgesetze und dessen Folgerungen. Die Abhandlung 556: „*De criteriis aequationis $fxx + gyy = hzz$ utrum ea resolutionem admittat necne?*" fragt nach den Lösungen der diophantischen Gleichung:

1) Siehe etwa die Ausführungen in der Vorrede zu Band I, 16 sectio altera, p. LXXXIV u. ff.

$$ax^2 + by^2 + cz^2 = 0,\ abc \neq 0,$$

einer Gleichung, die bekanntlich GAUSS zur Grundlage seiner Theorie der Geschlechter, in die die binären quadratischen Formen gegebener Determinante eingeteilt werden können, gemacht hat[1]). Der Existenzsatz über die Lösungen der Gleichung gab ihm die Existenz der Hälfte der möglichen Geschlechter. Der Existenzsatz selbst ist drei Jahre nach dem Erscheinen der *Opuscula analytica*, dem die Abhandlung angehörte, also im Jahre 1785 von LEGENDRE bewiesen worden[2]). LEGENDRE, offenbar zu seiner Untersuchung durch die EULERSCHE Abhandlung angeregt, setzt sich in seiner Arbeit mit ihr auseinander und beweist aus seinem Existenzbeweis heraus verschiedene Vermutungen EULERS. Eine Hauptforderung EULERS allerdings, nämlich daß aus der Lösung für a, b, c auch diejenige für $a, b, c + 4nab$ folge, insofern $c + 4nab$ eine Primzahl ist, konnte auch LEGENDRE nicht erhärten, da ihm eben der Beweis des Reziprozitätsgesetzes fehlte. Es ist dies um so merkwürdiger, als ja letzteres im wesentlichen durch die Existenz der Geschlechter gegeben ist[3]).

In den EULERSCHEN Überlegungen ist bemerkenswert, daß sie sofort die notwendigen Bedingungen für die Lösbarkeit bringen, nämlich daß je zwei der Zahlen $-ab, -ac, -bc$ nach jedem in der dritten Zahl enthaltenen Primteiler quadratische Reste sein müssen. Daß sie hinreichend sind, beweist EULER nicht. Das Kriterium für die Lösbarkeit veranlaßt EULER dagegen, in *Propositio 2* (p. 16 dieses Bandes) mit aller Schärfe den bekannten Satz auszusprechen, daß für eine ungerade Primzahl p als Modul r quadratischer Rest oder Nichtrest ist, je nachdem:

$$r^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$$

ist. Damit wird endgültig die Ausführung von RUDIO in der Vorrede zum Band I, 2 der *Opera omnia*, p. XXXI/II und speziell die Anmerkung auf p. XXXII in dem Sinne bestätigt, daß für diesen Satz zweifellos die EULERSCHE Priorität zu Recht besteht.

---

1) GAUSS behandelt die Gleichung in den Art. 294/5 der *disquisitiones arithmeticae, C. F. GAUSS: Werke*, Bd. 1, Göttingen, 1870, p. 349. In den folgenden Artikeln setzt er sich mit dem LEGENDRESCHEN Beweise auseinander (Art. 296/7). Der Beweis der Existenz der Geschlechter wird in Art. 287 erbracht (*Werke*, 1, p. 336). GAUSS hat allerdings beide Resultate aus seiner Theorie der ternären Formen hergeleitet; erst DIRICHLET hat ausgesprochen, daß die Lösung der Gleichung:

$$ax^2 + by^2 + cz^2 = 0$$

schon für die Existenz der Geschlechter hinreicht. Siehe *LEJEUNE DIRICHLET: Vorlesungen über Zahlentheorie*, Braunschweig, 1894, p. 432.

2) *LEGENDRE: Recherches d'analyse indéterminée.* Insbesondere ist hier article III: *Théorème sur la possibilité des équations indéterminées du second degré* für uns wichtig; Histoire de l'acad. roy. des sc., Paris, 1785 (1788), p. 507.

3) Siehe LEGENDRES Ausführungen in der unter 2) zitierten Abhandlung p. 523. Über den Zusammenhang des Reziprozitätsgesetzes mit dem Satz über die Existenz der Geschlechter siehe etwa *HILBERT: Theorie der algebraischen Zahlkörper*, Berlin, 1897, p. 286 u. ff.

In der Abhandlung 557: „*De quibusdam eximiis proprietatibus circa divisores potestatum occurrentibus*" fragt EULER nach dem kleinsten Exponenten x einer zu N teilerfremden Zahl a, für den a^x (mod. N) den Rest 1 besitzt, oder wie man heute sagt, zu dem a (mod. N) gehört, ein Problem, das ihn lange beschäftigt hat[1]). Er formuliert es in der allgemeinern Gestalt: Welches ist die kleinste positive Zahl x, für die:

$$fa^x + g \equiv 0 \text{ (mod. } N)$$

wird? Damit ist die Grundfrage gestellt, auf der die Indizesrechnung beruht, die GAUSS später für Primzahlmoduln entwickelt hat[2]), die aber EULER schon im Keime besaß. Er gibt eine praktische rechnerische Methode an, wie man allgemein das gesuchte x findet, wendet dieselbe dann auf den Fall $a = 2$, $f = 1$, $g = \pm 1$ an und berechnet für alle Primzahlen $p < 401$ die kleinsten x, für die somit $2^x \pm 1$ durch p teilbar ist. Diese Art der Forschung, in die uns EULER hier hineinsehen läßt, ist typisch für alle EULERSCHEN zahlentheoretischen Untersuchungen. Denn jetzt entnimmt er dem berechneten Zahlenmaterial das Gesetz des Restcharakters der Zahl 2 (mod. p), den er übrigens schon früher bestimmt hat[3]), den er aber kaum je so klar wie hier formuliert hat. Entsprechend wird für $a = 3, 5, 6, 7, 8, 10$, wenn N eine Primzahl p ist, der Restcharakter berechnet. Für allgemeines a stellt er durch Induktion das Theorem auf, daß für zwei Primzahlen p und q, für die:

$$p \equiv \pm q \text{ (mod. } 4a)$$

ist, das LEGENDRESCHE Restsymbol stets die Relation erfüllt:

$$\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right).$$

Man sieht, daß EULER eine wichtige Folgerung des quadratischen Reziprozitätsgesetzes damit gefunden hat, offenbar in der Absicht, dem erstern damit näher zu kommen. Alle Theoreme werden rein empirisch an Zahlenbeispielen erhalten und ausgesprochen.

Diese Vermutungen führen EULER im *Additamentum* der Abhandlung 557 dazu, den Beweis des Hauptfalles des quadratischen Reziprozitätsgesetzes zu versuchen. Ist $p \equiv 1$ (mod. 4) eine Primzahl, n eine beliebige Zahl, so ist $\pm a$ in $p = 4a + (2n + 1)^2$ quadratischer Rest (mod. p):

$$\left(\frac{\pm a}{p}\right) = 1.$$

---

1) Siehe die Abhandlung: *Theoremata circa residua ex divisione potestatum relicta*, *LEONHARDI EULERI Opera omnia*, ser. I, vol. 2, p. 493.

2) In den Art. 58 und 59 der *disquisitiones arithmeticae*, *Werke*, Bd. I, p. 47/8.

3) Siehe die Anmerkung 1) von F. RUDIO auf p. 276 des Bandes 3, serie I der *Werke* von EULER.

Rechnet man a aus:

$$a = \frac{p-1}{4} - n - n^2,$$

so sind somit alle diese Zahlen für $n = 0, 1, 2, \ldots, p-1$ stets quadratische Reste (mod. p). EULER behauptet aber noch mehr: *Auch jeder Teiler von a ist quadratischer Rest (mod. p).* Ist diese Behauptung richtig, so folgt für jede ungerade Primzahl q, für die:

$$\left(\frac{p}{q}\right) = 1$$

ist, auch

$$\left(\frac{q}{p}\right) = 1.$$

Denn aus der ersten Bedingung folgt, daß es ein n geben muß, für das:

$$(2n+1)^2 + 4qs = p$$

ist, und q ist dann Teiler von $a = qs$. Dieses Resultat spricht EULER im § 22 seiner Abhandlung als *Theorema generale* aus. Seine Vermutung, daß alle Teiler von a quadratische Reste sein müssen, wird durch die Gruppeneigenschaft der quadratischen Reste (mod. p) in bezug auf die Multiplikation als Operation gestützt und an einem sehr umfangreichen Zahlenmaterial erhärtet.

Die drei Abhandlungen 598: „*De insigni promotione scientiae numerorum*", 610: „*Novae demonstrationes circa divisores numerorum formae xx + nyy*", und 744: „*De divisoribus numerorum in forma mxx + nyy contentorum*" sind dadurch ausgezeichnet, daß vor ihrer Abfassung EULER die berühmte Abhandlung von LAGRANGE über die binären quadratischen Formen studiert hat[1]). Die LAGRANGESCHEN Entdeckungen gaben ihm neuen Impuls. Zugleich mußte er sie in seinen Ideenkreis einordnen. Letzterer fußt auf folgendem Problem: Läßt man in $x^2 + ny^2$ die Größen x, y alle zueinander teilerfremden Paare von ganzen Zahlen durchlaufen, wobei x auch noch zu n teilerfremd ist, welches sind dann alle Primteiler p, durch die $x^2 + ny^2$ teilbar wird? Er sieht, daß jedenfalls $-n$ quadratischer Rest (mod. p) sein muß, was ihn veranlaßt, zu Beginn der Abhandlung 610 nochmals einen Exkurs über quadratische Reste einzuschalten. Allein es gilt auch die

1) *LAGRANGE: Recherches d'arithmétique. Oeuvres* de LAGRANGE, Paris, 1869, t. 3, p. 695. Es ist übrigens bemerkenswert, daß GAUSS die beiden Abhandlungen 598 und 610 nicht gekannt zu haben scheint, ebenso wie alle spätern Arbeiten EULERS über diesen Gegenstand. Wenigstens sagt er in Art. 222 der *disquisitiones arithmeticae*, daß EULER die LAGRANGESCHE Lösung nicht gekannt zu haben scheine. Auch zitiert er nirgends diese Abhandlungen, während die frühern bis zu der 1774 erschienenen Abhandlung 452 genannt werden. Dies ist verwunderlich, da ja die beiden hier besprochenen Abhandlungen 598 und 610 schon 1785/87 erschienen sind. Siehe *GAUSS, Werke*, Bd. 1, p. 222/23.

Umkehrung des Satzes: Wenn $-n$ quadratischer Rest (mod. p) ist, so ist p auch Teiler von $x^2 + ny^2$. Damit ist die Aufgabe gelöst, zu einem gegebenen p alle diejenigen n anzugeben, für die p Teiler der Form $x^2 + ny^2$ ist. Viel schwieriger ist die umgekehrte Problemstellung: welches sind alle p, die bei gegebenem n Teiler von $x^2 + ny^2$ sind? Erst das quadratische Reziprozitätsgesetz gibt hierauf eine erschöpfende Antwort; aber EULER hat dasselbe nicht bewiesen. So kann er nur an unzähligen Beispielen den Satz erhärten, daß auch jede Primzahl $q \equiv p$ (mod. $4n$) Teiler von $x^2 + ny^2$ ist, falls es p selbst ist. Er sieht sogar noch mehr; nämlich nur *die Hälfte der möglichen Restklassen (mod. $4n$), die zu $4n$ teilerfremd sind, können Primteiler der Form $x^2 + ny^2$ liefern.* Dies ist aber nichts anderes wie der Satz, daß nur *die Hälfte der möglichen Geschlechter der binären quadratischen Formen der Determinante $-n$ existieren.* Es ist überraschend, zu sehen, wie weit EULERS große Divinationsgabe ihn führte. Man kann sagen, daß eigentlich alle Bausteine der Zahlentheorie dieses Gebietes in den EULERSCHEN Abhandlungen schon bereitgestellt wurden, und es nur der Meisterhand eines GAUSS bedurfte, um sie zu dem Gebäude der Theorie der quadratischen Formen zusammenzufügen. EULER nennt die Restklassen (mod. $4n$), in denen Teiler der Form liegen, $a, b, c, \ldots$; diejenigen, in denen keine solchen Teiler liegen, $\alpha, \beta, \gamma, \ldots$

In der Abhandlung 744 berechnet EULER mittels einer praktischen Methode die Klassen $a, b, \ldots$ bis zu $n = 25$, und folgert daraus eine größere Zahl von Sätzen, die sich heute aus dem quadratischen Reziprozitätsgesetze einfach ergeben. Die Methode besteht im wesentlichen darin, daß EULER alle in $y^2 + n$ für $y = 1, 2, \ldots \frac{1}{2} n$ aufgehenden Primzahlen berechnet. Diese, sowie ihre Produkte ergeben Klassen $a, b, \ldots$ Die Produkte der nicht unter ihnen auftretenden Primzahlen, kleiner als n, ergeben nur bei gerader Faktorenzahl Klassen.

Nun wußte EULER längst, daß im Falle $n = 1, \pm 2, \pm 3$ jeder Primteiler der Form $x^2 + ny^2$ selbst durch die Form darstellbar ist. Allein dies hört schon für $n = 5$ auf wahr zu sein. Hier setzen nun LAGRANGES Untersuchungen ein. EULER gibt von ihnen zu Beginn der Abhandlung 598 ein größeres Referat mit den nötigsten Beweisen. Welchen Nutzen bringen sie für die oben angegebene EULERSCHE Fragestellung? Es ergibt sich sehr einfach, daß jeder Teiler von $x^2 + ny^2$ durch eine Form derselben Determinante n (Determinante stets im GAUSSSCHEN Sinne gebraucht) darstellbar ist, also durch eine der LAGRANGESCHEN reduzierten Formen.

EULER vermutet jetzt fälschlich, daß man die oben definierten Restklassen $a, b, c, \ldots$ (mod. $4n$) eindeutig auf die reduzierten Formen aufteilen kann. Die ersten von ihm berechneten Beispiele bestätigen diese Ansicht. Bekanntlich können aber die Restklassen (mod. $4n$) nur auf die Geschlechter, in die die Formen der Determinante $-n$ zerfallen, verteilt werden. Jedes Geschlecht ist durch bestimmte Restklassen (mod. $4n$) gegeben.

Wenn also die Zahl der reduzierten Formen in einem Geschlecht eins ist, wie dies bei den ersten Beispielen EULERS der Fall ist ($n = 1, 2, 3, 5, \ldots$), so ist auch jeder Restklasse (mod. $4n$) eine feste reduzierte Form zugeteilt. Schon bei $n = 39$ stimmt die Aussage nicht mehr, weil hier je zwei Formenklassen in den beiden Geschlechtern vorliegen. EULER verbessert daher seine Aussage dadurch, daß er, im Falle nicht alle Primzahlen p einer Restklasse (mod. $4n$) durch dieselbe reduzierte Form darstellbar sind, annimmt, wenigstens t^2p sei stets darstellbar, wo t eine natürliche Zahl ist. Diese Behauptung kommt auf dasselbe hinaus, wie wenn man bei den Darstellungen einer Zahl durch eine quadratische Form auch gebrochene rationale Zahlen für die Variablen zuläßt. Hier bewährt sich wieder EULERS unglaublicher Blick; denn diese Behauptung ist doch nichts anderes wie die Erkenntnis, daß jede Form des Hauptgeschlechtes durch Duplikation einer Form entsteht. Man erhält nämlich alle Klassen eines Geschlechtes, indem man eine Klasse des Geschlechtes mit allen Klassen des Hauptgeschlechtes multipliziert. Das Quadrat einer Form ist übrigens EULER bekannt[1]). Er bringt diese Formel gerade, um seine Vermutung, daß alle Primzahlen einer Restklasse (mod. $4n$) wenigstens in gebrochenen Zahlen durch dieselbe reduzierte Form darstellbar sind, zu stützen. Für unsere heutigen Begriffe sagt die Formel aus, daß zu jeder Klasse eine reziproke Klasse gehört.

Man sagt somit nicht zu viel, wenn man behauptet, daß in den Abhandlungen 598 und 610 die wesentlichen Ansätze der Einteilung der binären quadratischen Formen in Geschlechter enthalten sind. GAUSS war es vorbehalten, durch den Begriff der Formenklasse, der bei EULER nirgends vorkommt, Klarheit zu schaffen und die nötigen Beweise zu leisten. Wenn EULER von „classis" spricht, so meint er verschiedene Dinge, z. B. eben auch die in einem Geschlecht vereinigten Formen. Er sieht darin aber nicht die Menge aller äquivalenten Formen.

In der Abhandlung 683: „*De singulari genere quaestionum Diophantearum et methodo maxime recondita eas resolvendi*" wird folgendes Problem behandelt: Es sei N durch die Form $x^2 + ny^2$ darstellbar,

$$N = a^2 + nb^2,\ n > 0;$$

man bestimme den kleinsten Exponent l, für den:

$$N^l = A^2 + n$$

wird. Setzt man

$$a + b\sqrt{-n} = N^{\frac{1}{2}} e^{i\varphi},$$

so muß:

$$N^{\frac{l}{2}} \sin(l\varphi) = \sqrt{n}$$

1) Siehe diesen Band p. 195, ferner I, 2, p. XIV, 600 und 607.

sein. Man hat daher l so zu berechnen, daß $\sin(l\varphi)$ möglichst klein, d. h. $l\varphi$ möglichst genau ein Vielfaches von π wird. Entwickelt man π/φ in einen Kettenbruch, und ist P/Q ein Näherungsbruch, so wird für $l = P$ ziemlich genau $l\varphi = Q\pi$.

III. GROSSE PRIMZAHLEN

F. Rudio hat die Geschichte der Primzahltafeln in seiner Vorrede zum Band 3, Serie I ausführlich behandelt[1]). Anlaß dazu gab ihm die Abhandlung 283: *De numeris primis valde magnis*, sowie die spätern Abhandlungen 369, 461, 467, 498 und 708a. Über den Inhalt dieser Abhandlungen referiert jene Vorrede, auf die verwiesen sei. Für uns kommen die drei letzten der genannten Abhandlungen in Betracht. In 467 gibt Euler eine Tafel aller Primzahlen zwischen 999000 und 1 002000. Diese enthält verschiedene Zahlen, die keine Primzahlen sind. Eine solche ist $1\,000009$[2]), von der Euler selbst vermutet, daß ein Irrtum vorliege. Er untersucht daher in der Abhandlung 699 dieses Bandes: „*Utrum hic numerus* 1 000009 *sit primus necne inquiritur*", ob die Aufnahme der Zahl unter die Primzahlen zu Recht erfolgt ist oder nicht. Dabei verwendet er eine schon in Abhandlung 369 skizzierte Methode. Ist nämlich eine Zahl nur auf eine Weise als Summe von zwei Quadraten darstellbar, so muß sie Primzahl sein. Nun ist in der Tat:

$$1\,000009 = 1\,000^2 + 3^2;$$

man muß somit nur untersuchen, ob noch eine zweite Zerfällung in zwei Quadrate existiert. Die Theorie der quadratischen Reste (mod. 5) ergibt, daß die Basis des einen der beiden Quadrate, in die $1\,000009$ zerfällt, stets durch 5 teilbar sein muß, und daß man die andere in der Form $3 + 25a$ annehmen darf. Durch diese Bemerkung wird die Rechnung außerordentlich abgekürzt. Euler findet rasch die zweite Zerlegung:

$$1\,000009 = 972^2 + 235^2.$$

Die Zahl ist daher keine Primzahl. Eine einfache Regel läßt aus den beiden Darstellungen als Summe von zwei Quadraten die Teiler der Zahl berechnen.

Viel wichtiger ist die Ausdehnung dieser Methode, wie sie von Euler schon in dem Brief 498 an Béguelin angezeigt wurde[3]). Eine eingehende Darstellung derselben findet sich in den Abhandlungen 708, 715, 718, 719 und 725 dieses Bandes. Nummer 708: „*De formulis speciei* $mxx + nyy$ *ad numeros primos explorandos idoneis, earumque mirabilibus*

1) Siehe *Leonhardi Euleri Opera omnia*, series I, vol. 3, p. X u. ff.
2) Siehe *Leonhardi Euleri Opera omnia*, series I, vol. 3, p. 403.
3) Siehe *Leonhardi Euleri Opera omnia*, series I, vol. 3, p. 418 und 421.

proprietatibus" wirft die Frage auf: wie muß $m > 0$ in $x^2 + my^2$ beschaffen sein, damit eine durch diese Form dargestellte Zahl N dann und nur dann Primzahl ist, wenn sie nur auf eine Weise durch $x^2 + my^2$ dargestellt werden kann? EULER nennt alle die dieser Bedingung genügenden m zuerst „numeri congrui", dann aber stets „numeri idonei". Aus seinen frühern Arbeiten weiß er, daß $m = 1, 2, 3$ „taugliche" Zahlen sind. Sehen wir zuerst, was die Fragestellung im Sinne der modernen Zahlentheorie bedeutet. $m > 0$ darf auch quadratische Faktoren besitzen. Wir legen den Ring $r(m)$ mit der Basis $(1, \sqrt{-m})$ der ganzen Ringzahlen zugrunde. Sind $\mathfrak{p}$ und $\mathfrak{q}$ zwei verschiedene reguläre Primideale 1. Ordnung des Rings, die wir nicht nur zum Führer, sondern zu $4m$ teilerfremd voraussetzen, ist ferner das Produkt $\mathfrak{pq}$ Hauptideal in $r(m)$:

$$\mathfrak{pq} = (\alpha),\ \alpha = a + b\sqrt{-m}\,,$$

so ist $n(\mathfrak{pq}) = n(\mathfrak{p})n(\mathfrak{q}) = n(\alpha)$ keine Primzahl, muß also, falls m „tauglich" ist, auf zwei Weisen als Norm einer ganzen Ringzahl dargestellt werden können. Diese zweite ganze Zahl sei β:

$$n(\alpha) = n(\beta),\ \text{wo}\ \alpha \neq \beta\ \text{ist.}$$

Sehen wir von dem schon erledigten Falle $m = 1$ ab, so kann β sich nicht nur um einen Einheitsfaktor von α unterscheiden. Da $\mathfrak{p}$ und $\mathfrak{q}$ Primideale sind, bleibt nur eine Möglichkeit, nämlich daß β (oder seine Konjugierte $\bar{\beta}$) die Primidealzerlegung besitzt:

$$(\beta) = \bar{\mathfrak{p}}\mathfrak{q},$$

wo wir durch den Querstrich die konjugierten Ideale bezeichnen. Daraus folgt, daß in $r(m)$ sowohl $\mathfrak{pq} \sim (1)$ wie $\bar{\mathfrak{p}}\mathfrak{q} \sim (1)$ ist; d. h. es muß:

$$\mathfrak{p} \sim \bar{\mathfrak{p}},\ \text{im Ringe}\ r(m),$$

sein. *Die Klasse von* $\mathfrak{p}$ *ist ambig.* Da $\mathfrak{p}$ in irgend einer Klasse des Rings liegen kann, müssen daher *alle Klassen des Rings ambig sein.* Die Frage EULERS heißt also: *welches sind alle quadratisch-imaginären Zahlkörper, die nur ambige Klassen besitzen?* Die Zahl der ambigen Klassen ist bekanntlich gleich der Zahl der Geschlechter im Ring $r(m)$. Man kann daher auch nach denjenigen Ringen fragen, in denen *jedes Geschlecht genau eine Klasse enthält.* In diesem Sinne hat GAUSS das Problem in den *disquisitiones* gestellt. GAUSS wußte, daß seine Fragestellung mit derjenigen EULERS übereinstimmte[1]). Er hat auch das Problem

1) Siehe den Art. 303 der *disquisitiones arithmeticae*, *GAUSS, Werke*, Bd. 1, p. 367/68. GAUSS zitiert nur die Arbeit 498 von EULER, da die Abhandlungen 708 und folgende erst nach 1800 erschienen sind. Immerhin darf man annehmen, daß GAUSS durch EULER angeregt wurde, die Frage der Endlichkeit der Zahl der numeri idonei aufzuwerfen.

gleich allgemeiner gefaßt, indem er nach allen Ringen fragte, in denen die Anzahl der Klassen in einem Geschlechte eine bestimmte Zahl ist.

Die erste Sorge EULERS ist, ein Rechnungsverfahren zu finden, das erlaubt, alle numeri idonei anzugeben. Wie schon oben hervorgehoben wurde, ist ein typischer Zug seiner Forschungsmethode, sich ein riesiges Zahlenmaterial zu verschaffen, aus dem er vermöge seiner genialen Divinationsgabe die weitgehendsten Schlüsse zu ziehen vermochte. Heute verfährt man zuweilen umgekehrt, indem man große Theorien entwickelt und kaum oder erst später nach den Möglichkeiten der Realisierung fragt. Welche Methode die fruchtbarere ist und die Forschung weiterführt, ist für den Leser EULERSCHER Abhandlungen leicht zu beantworten.

Die Abhandlung 708 bringt dieses Rechnungsverfahren, und die folgende Abhandlung 715: „*De variis modis numeros praegrandes examinandi utrum sint primi necne?*" setzt die Untersuchung fort. Das Hauptresultat, das gefunden wird, besteht in dem Satz, daß im Falle eines untauglichen m stets eine Zahl kleiner als $4m$ existieren muß, die zusammengesetzt ist, und die sich nur auf eine Weise durch $x^2 + my^2$ darstellen läßt. Damit ist die Betrachtung zurückgeführt auf die Untersuchung der endlich vielen darstellbaren Zahlen kleiner als $4m$. Für alle diese Zahlen ist aber $y = 1$ zu setzen; daher bleibt nur übrig zu sehen, ob es unter den Zahlen $x^2 + m < 4m$ solche gibt, die durch zwei verschiedene (ungerade) Primzahlen teilbar sind. Der Beweis des Satzes ist nicht zwingend. Er ist später von GRUBE kritisch untersucht worden[1]). In der modernen Sprache sagt er aus, daß es in jeder Idealklasse ein Ideal geben muß, dessen Norm kleiner als $|\sqrt{4m}|$ ist. Das Produkt der Normen von zwei Idealen ist also kleiner als $4m$. Übrigens hat EULER das Problem etwas allgemeiner formuliert, indem er die Form $ax^2 + by^2$, $ab = m$, zugrunde legt. Er zeigt leicht, daß diese Form dann und nur dann die Eigenschaft hat, nur die Primzahlen ein einziges Mal darzustellen, wenn m tauglich ist.

Nach diesem Verfahren berechnet EULER die numeri idonei. Er findet 65 solche Zahlen. Trotzdem er seine Rechnungen über 10000 fortsetzt, erhält er keine neuen mehr. Diese Tatsache hat EULER außerordentlich überrascht. Er sagt, daß bisher noch nie Zahlenreihen in der Analysis auftraten, die nach endlich vielen Gliedern abbrechen. Ja, in der Abhandlung 725: „*Illustratio paradoxi circa progressionem numerorum idoneorum sive congruorum*" nennt er dies direkt ein Paradoxon. Bekanntlich hat GAUSS dieselben 65 Zahlen gefunden (siehe Anmerkung p. XVI), wobei für ihn das zugehörige $r(m)$ nur eine Klasse in jedem Geschlecht haben darf. Er spricht dort die weitergehende Vermutung aus, daß es nur endlich viele quadratisch-imaginäre Ringe $r(m)$ gebe, in denen die Anzahl der Klassen eines Geschlechts eine bestimmte Zahl sei. Erst im Jahre 1934 hat HEILBRONN

1) *F. GRUBE: Über einige EULERSCHE Sätze aus der Theorie der quadratischen Formen.* Ztschr. f. Math. u. Phy. 19, 1874, p. 492, insbesondere p. 497 u. ff.

den Satz bewiesen, daß es zu einer gegebenen Klassenzahl nur endlich viele $r(m)$ gibt, und CHOWLA hat durch Erweiterung des Beweises gezeigt, daß die Anzahl der Klassen im Geschlecht nur für endlich viele Ringe eine bestimmte Zahl sein darf[1]). Dabei wird keine obere Schranke dieser Anzahlen angegeben, was zur Bescheidenheit gegenüber den Entdeckungen eines EULERS mahnt.

Die Vermutung über die Endlichkeit der Anzahl tauglicher Zahlen stützt EULER durch eine Reihe von Sätzen. Zum Beispiel ist $m = t^2$ nur für die endlich vielen Fälle $t = 1, 2, 3, 4, 5$ tauglich. Ist ferner ein taugliches m von der Form $4n - 1$ oder $4n + 2$, so muß auch $4m$ tauglich sein. Ist m ungerade und $4m$ tauglich, so ist auch $16m$ tauglich. Hat ein taugliches m die Form $3n - 1$, so ist auch $9m$ tauglich. Dagegen ist $4m$ niemals tauglich, wenn m tauglich und von der Form $4n + 1$ ist. Ist m ungerade und $8m$ resp. $16m$ tauglich, so ist $32m$ resp. $64m$ sicherlich nicht tauglich. Dadurch ist gezeigt, daß man nicht durch fortlaufendes Multiplizieren mit 2 zu beliebig vielen tauglichen Zahlen kommen kann. Umgekehrt folgt aus der Tauglichkeit von t^2m stets diejenige von m. Alle diese Sätze können heute leicht aus der Formel für die Ringklassenzahl abgelesen werden.

Zum Schlusse der Abhandlung 715 wird in den Paragraphen 41 u. ff. unter dem Titel: „*Additamentum de numeris idoneis investigandis*" ein praktisches Verfahren entwickelt, wie man rasch die numeri idonei erhalten kann. Statt nämlich jede Zahl daraufhin zu untersuchen, ob sie tauglich ist oder nicht, kann man durch ein Auswischverfahren alle untauglichen wegschaffen. Es sind nur alle Zahlen m auszuschließen, für die nicht alle $x^2 + m < 4m$ Primzahlen, oder Quadrate von Primzahlen, oder das doppelte einer Primzahl, oder 4 oder 8 oder 16 sind[2]). Daher sind z. B. alle Zahlen der Form $m = 4n + 3$ auszuwischen, da $1^2 + 4n + 3 = 4(n + 1) < 4(4n + 3)$ zerlegbar ist, mit Ausnahme der Fälle $n = 0, 1, 3$, für die $m = 3, 7, 15$ wird. Ebenso sind alle Zahlen der Form $3n + 2$ auszuschließen, da $1^2 + 3n + 2 = 3(n + 1)$ ist, außer für $n = 0, 1, 2$, für welche Werte $m = 2, 5, 8$ wird. So geht EULER weiter bis zu den Zahlen $29n + a$, für die $-a$ quadratischer Rest (mod. 29) ist. Alle Resultate werden in einer Tabelle zusammengefaßt. Will man dieselbe zur Lösung der Frage, ob m tauglich ist, benutzen, so sieht man, ob m in einer der in der Tabelle auftretenden Restklassen auftritt. In letzterm Falle muß man nur kontrollieren, ob m nicht einer der Ausnahmefälle ist.

In den beiden Abhandlungen 718 und 719 wird die Theorie der numeri idonei benutzt, um große Primzahlen zu bestimmen. In 718: „*Facillima methodus plurimos numeros primos*

---

1) *HEILBRONN: On the class-number in imaginary quadratic fields.* The Quarterly Journ. of Math. Oxford ser. t. 5, p. 150 (1934). *CHOWLA: An extension of Heilbronn's class-number Theorem.* Ibid. p. 304.

2) Diese Ausnahmefälle sind bisher nicht besonders hervorgehoben worden. Der Ausnahmefall des Quadrates einer Primzahl ist ohne weiteres gegeben. Ferner ist 2 stets Faktor des Führers des Ringes; daher muß es eine Ausnahmerolle spielen.

praemagnos inveniendi" wird mit Hilfe der tauglichen Zahl 232 gezeigt, wann $232a^2 + 1$ eine Primzahl darstellt. In 719: „*Methodus generalior numeros quosvis satis grandes perscrutandi utrum sint primi necne?* wird mit Hilfe von $m = 30$, einer tauglichen Zahl, bewiesen, daß $100003 = 10 \cdot 100^2 + 3 \cdot 1^2$ eine Primzahl ist. Ebenso ergibt die taugliche Zahl $m = 57$, daß $1000003 = 3.577^2 + 19.8^2$ eine Primzahl ist, und schließlich muß auch $18518809 = 1848.100^2 + 197^2$ wegen der Tauglichkeit von 1848, der größten aller tauglichen Zahlen, Primzahl sein. Im übrigen bringt diese Abhandlung nochmals die Darstellung der Eulerschen Methode.

IV. DIOPHANTISCHE GLEICHUNGEN

In den unter diesen Sammelnamen fallenden Abhandlungen zeigt sich EULERS ganze Meisterschaft. Es sind diejenigen Forschungen, die heute noch die größten Entwicklungsmöglichkeiten bieten. Diese von EULER mit so großem Erfolge durchgeführten Untersuchungen sollten von den heutigen Mathematikern wieder in viel stärkerm Maße aufgenommen und verfolgt werden. Wenn man bedenkt, daß die ganze Idealtheorie ihren Ursprung der von FERMAT aufgestellten DIOPHANTISCHEN Gleichung $x^n + y^n = z^n$ verdankt, kann man ermessen, was alles von einer Durchforschung der EULERSCHEN Ansätze zu erwarten ist. Zum Beispiel fragt EULER in der Regel nur nach rationalen Lösungen, ohne das Problem aufzuwerfen, ob sein Verfahren auch a l l e rationalen Lösungen ergibt. Daran schließt sich die Frage, wie weit seine Verfahren Gültigkeit haben, wenn andere Bereiche als derjenige der rationalen Zahlen zugrunde gelegt werden. Gerade die Abhandlungen dieses Bandes über DIOPHANTISCHE Gleichungen seien lebhaft der Aufmerksamkeit der jungen Mathematiker empfohlen.

Lösungen von DIOPHANTISCHEN Gleichungen werden im vorliegenden Bande in den Abhandlungen 559, 560, 696, 702, 713, 716, 732 und 739 durchgeführt. Die meisten bringen Spezialfälle des folgenden allgemeinen Problems:

Gegeben sei ein System von (ganzen) r a t i o n a l e n Funktionen der Variablen $x, y, z, \ldots$ mit (ganzen) r a t i o n a l e n Zahlkoeffizienten:

$$F_n(x, y, z, \ldots) = 0, \; n = 1, 2, 3, \ldots$$

Man uniformisiere diese Gleichungen durch r a t i o n a l e Funktionen:

$$x = f(p, q, r, \ldots), \; y = g(p, q, r, \ldots), \; z = h(p, q, r, \ldots), \ldots,$$

mit r a t i o n a l e n Zahlkoeffizienten, wobei die Zahl der Variablen $p, q, r, \ldots$ möglichst groß sei.

In der Kunst der Auffindung solcher Funktionen $f, g, h, \ldots$ für ein gegebenes System F_n ist EULER unerreicht.

Nehmen wir das 3. Problem der Abhandlung 560: „*Miscellanea analytica*", so lautet die Aufgabe:

$$\left(\frac{x^3+1}{x}\right)^2 + \left(\frac{y^3+1}{y}\right)^2 = z^2$$

in rationalen Zahlen zu lösen. EULER findet:

$$x = \frac{4p}{p^3-1}, \quad y = \frac{3p^3+1}{p(p^3+3)}, \quad z = \frac{(p^4+14p^3+1)(5p^4+6p^3+5)}{4p(p^3-1)(3p^3+1)(p^3+3)}.$$

Die Kunst besteht in dem Ansatze:

$$y = \frac{px-1}{x+p}.$$

In der Abhandlung 702: „*De novo genere quaestionum arithmeticarum, pro quibus solvendis certa methodus adhuc desideratur*" wird nach denjenigen N gefragt, für die

$$x^2 + y^2 = z^2,$$
$$x^2 + Ny^2 = t^2,$$

in ganzen rationalen Zahlen lösbar ist. Man darf setzen:

$$x = u^2 - v^2,\ y = 2uv,\ z = u^2 + v^2,\ u \neq v,\ uv \neq 0.$$

Dann wird:

$$N = \frac{t^2 - (u^2-v^2)^2}{4u^2v^2}.$$

Nimmt man hier $t = u^2 \pm 2wu^2v^2 \pm v^2$, so erhält man für N die beiden Darstellungen:

$$N = (wu^2 \pm 1)(wv^2 \pm 1) \text{ und } N = (wu^2 \pm 1)(wv^2 \mp 1) + 1.$$

Damit sind x, y, z, t, N durch die Parameter u, v, w rational mit rationalen Koeffizienten ausgedrückt.

In den Abhandlungen 713: „*Investigatio trianguli, in quo distantiae angulorum ab eius centro gravitatis rationaliter exprimantur*" und 732: „*Solutio facilior problematis Diophantei circa triangulum, in quo rectae ex angulis latera opposita bisecantes rationaliter exprimantur*" wird eine in Abhandlung 451 behandelte Aufgabe wieder aufgegriffen: Man soll alle Dreiecke mit rationalen Seiten und Schwerpunktslinien angeben. Über die

Bedeutung und die Geschichte des Problems hat RUDIO in der Vorrede zu Band I, 3[1]) und in den Anmerkungen zu Abhandlung 451 ausführlich berichtet. Die vorliegenden Abhandlungen sind bedeutend reifer als die frühern. Die zweite bringt gegenüber der ersten nur unwesentliche Vereinfachungen.

Es handelt sich um die Lösung der Gleichungen:

$$u^2 = 2y^2 + 2z^2 - x^2,$$
$$v^2 = 2z^2 + 2x^2 - y^2,$$
$$w^2 = 2x^2 + 2y^2 - z^2,$$

wo x, y, z die halben Dreiecksseiten, und u, v, w die Längen der Schwerpunktslinien sind. Die Gleichungen können umgekehrt werden:

$$(3x)^2 = 2v^2 + 2w^2 - u^2,$$
$$(3y)^2 = 2w^2 + 2u^2 - v^2,$$
$$(3z)^2 = 2u^2 + 2v^2 - w^2,$$

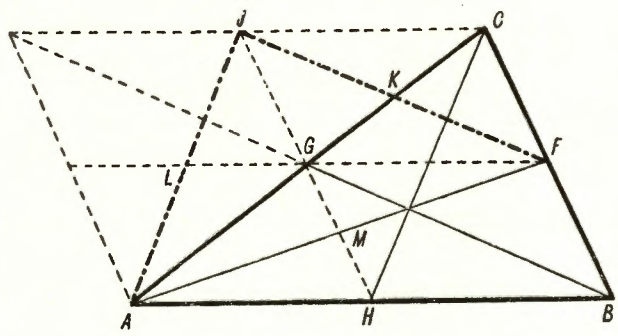
was EULER den eleganten Satz aussprechen läßt, daß das Dreieck mit den halben Seiten u, v, w die Schwerpunktslinien $3x, 3y, 3z$ besitzt[2]).

Die Idee EULERS besteht darin, daß er für y, z, v, w vier Größen p, q, r, s durch die Relationen einführt:

$$y + z = p(r + s), \quad w + v = 3q(r + s),$$
$$y - z = q(r - s), \quad w - v = p(r - s).$$

1) Siehe *LEONHARDI EULERI Opera omnia*, series I, vol. 3, p. XXIV.

2) Das Resultat ergibt sich sofort aus der Figur:



Die Dreieckseiten sind: $BC = 2a$, $CA = 2b$, $AB = 2c$ und die Schwerpunktslinien: $AF = f$, $BG = g$, $CH = h$. Das Dreieck JAF hat offenbar die Seitenlängen f, g, h, und seine Seiten sind parallel zu den entsprechenden Schwerpunktslinien von ABC. Die Längen der Schwerpunktslinien von JAF sind: $JM = \frac{3}{2}a$, $AK = \frac{3}{2}b$, $FL = \frac{3}{2}c$.

Dadurch wird erreicht, daß die Lösung der ersten und zweiten Gleichung auch diejenige der dritten nach sich zieht. Setzt man schließlich:

$$x = q(r + ts),$$
$$u = p(r - ts),$$

so werden durch:

$$t = \frac{9q^4 - p^4}{8p^2q^2}, \quad r = (p^2 + q^2)(p^2 + 9q^2), \quad s = -16p^2q^2$$

alle drei Gleichungen gelöst. Damit sind alle sechs Größen x, y, z, u, v, w als rationale Funktionen mit rationalen Koeffizienten der beiden Parameter p, q gegeben. Jedes rationale Zahlenpaar p, q ergibt eine Lösung.

Auch die Abhandlung 716: „*Resolutio formulae Diophanteae* $ab(maa + nbb) = cd(mcc + ndd)$ *per numeros rationales*“ greift auf ein früher in Abhandlung 428 schon bearbeitetes Problem zurück[1]): Kann die Summe zweier Biquadrate wieder Summe zweier anderer Biquadrate werden? Es soll daher:

$$x^4 + y^4 = z^4 + t^4$$

rational gelöst werden. EULER setzt wie früher:

$$x = a + b, \qquad y = c - d,$$
$$z = a - b, \qquad t = c + d.$$

Die Gleichung geht dann in:

$$ab(a^2 + b^2) = cd(c^2 + d^2)$$

über, die aber EULER gegenüber der Abhandlung 428 in der allgemeinern Form:

$$ab(ma^2 + nb^2) = cd(mc^2 + nd^2)$$

schreibt. Für $m = n = 1$ geht sie in den ersten Fall über. EULER setzt genau wie früher:

$$b = cp, \qquad d = aq,$$

führt also statt b, d die neuen Größen p, q ein. Dann wird:

$$\left(\frac{a}{c}\right)^2 = \frac{np^2 - mq}{nq^2 - mp}.$$

1) Siehe auch hierzu die Ausführungen von RUDIO in der Vorrede des Bandes I, 3. *LEONHARDI EULERI Opera omnia*, series I, vol. 3, p. XXII.

Die rechte Seite ist zu einem Quadrat zu machen. Hier wird ein neuer Ansatz verwendet:

$$p = q(1+z), \quad \frac{a}{c} = 1 + zs.$$

Man erhält eine in z quadratische Gleichung. Setzt man das konstante Glied null, so muß:

$$s = \frac{3nq^2 + m}{2(nq^2 - m)}$$

sein. Für z ergibt sich dann ebenfalls ein rationaler Wert:

$$z = -\frac{3(nq^2 - m)^3}{4nq^2(nq^2 - m)^2 + m(3nq^2 + m)^2}.$$

Damit sind a/c und p, d. h. auch d/b als rationale Funktionen von q dargestellt. Die Koeffizienten sind überall rational. Bis auf einen Homogenitätsfaktor erhält man eine einparametrige Schar von Lösungen. Für $m = n = 1$, $q = 3$ ergibt sich die einfachste bekannte Lösung:

$$158^4 + 59^4 = 133^4 + 134^4,$$

deren Zahlen viel kleiner sind als die in der früheren Abhandlung gefundenen Werte[1]).

Zuweilen kann Euler die Uniformisierung des Gleichungssystemes nicht vollständig durchführen, sondern die Parameter $p, q, r, \ldots$ müssen ihrerseits wieder einer einfachen Diophantischen Gleichung

$$\Phi(p, q, r, \ldots) = 0$$

genügen, die ebenfalls ganz und rational ist. Im zweiten Problem der oben zitierten Abhandlung 560 werden vier Zahlen verlangt, deren Produkte zu je zweien, um eins vermehrt, ein Quadrat ergeben. Nimmt man p, q, l als Lösungen der Gleichung:

$$\Phi(p, q, l) = pq - l^2 + 1 = 0$$

an, so lautet die Lösung für die vier Zahlen x, y, z, t:

$$x = p,\ y = q,\ z = p + q + 2l,\ t = 4l(l + p)(l + q).$$

Im 6. Problem derselben Abhandlung wird zu diesen vier Zahlen noch eine fünfte u verlangt, die mit ihnen dieselben verlangten Eigenschaften besitzt. Sind:

$$m = x + y + z + t, n = xy + xz + \ldots, r = xyz + xyt + \ldots, s = xyzt,$$

1) Siehe *Leonhardi Euleri Opera omnia*, series I, vol. 3, p. 216.

die elementarsymmetrischen Funktionen der vier Zahlen, so wird:

$$u = \frac{4r + 2m(s+1)}{(s-1)^2}$$

die gesuchte fünfte Zahl sein.

In der Abhandlung 696: „*De casibus quibus hanc formulam* $x^4 + kx^2y^2 + y^4$ *ad quadratum reducere licet*" fragt EULER, wie k beschaffen sein muß, damit:

$$x^4 + kx^2y^2 + y^4 = z^2, \quad xy \neq 0,$$

rational lösbar ist. Dies ist sicherlich der Fall für $k = \pm 2$ und für $k = -n^2$ oder $n^2 - 2$, $n = 1, 2, 3, \ldots$ Um weitere Werte k zu finden, macht EULER den überaus reizvollen Ansatz:

$$k = P + \sqrt{Q},$$

wo P, Q ganze rationale Funktionen von x, y mit rationalen Koeffizienten sein sollen. Die Rechnung ergibt:

$$P = fx^2, \quad Q = 4fy^2 + 4,$$

wo f eine beliebige ganze rationale Zahl bedeutet. k wird somit nur dann rational, wenn $fy^2 + 1 = u^2$ ist, d. h. wenn u, y Lösungen der zu f gehörigen PELLSCHEN Gleichung sind. k hat dann den Wert:

$$k = fx^2 + 2u,$$

und f darf kein Quadrat sein.

EULER ist offenbar auf die Gleichung des Titels geführt worden durch die Aufgabe, zwei Formen $x^2 + my^2$ und $x^2 + ny^2$ zugleich zu einem Quadrate zu machen. In der im Bande I, 5 erscheinenden Abhandlung 758 wird dieses Problem auf die vorliegende Gleichung reduziert. Auch hat EULER umgekehrt in der Abhandlung 98 für $k = \pm 6$ die Unmöglichkeit der Auflösung mit Hilfe von Sätzen des letztern Problems gezeigt[1]). Im Summarium der vorliegenden Abhandlung wird behauptet, daß für $k = 7$ keine rationale Lösung existiere, was wegen:

$$1^4 + 7 \cdot 1^2 \cdot 1^2 + 1^4 = 3^2$$

nicht richtig ist, und auf eine Flüchtigkeit der redigierenden Sekretäre zurückzuführen ist, um so mehr, da im Text selbst die Unmöglichkeit nur für $k = 1, 3, 4, 5, 6$ behauptet wird. Dagegen wird in Abhandlung 755, die ebenfalls erst im Band I, 5 erscheinen wird,

1) Siehe *LEONHARDI EULERI Opera omnia*, series I, vol. 2, p. 48/49.

von EULER selbst behauptet, daß die eine Lösung für $k = 7$ nicht auf die Existenz von unendlich vielen Lösungen schließen lasse. Es handelt sich also offenbar auch hier um drei Fragen, ob es keine, endlich viele oder unendlich viele Lösungen gebe. Wir werden in der Vorrede des Bandes I, 5 ausführlich auf diese Fragen zurückkommen.

Ebenfalls auf die PELLSCHE Gleichung führt die in der Abhandlung 739: „*Regula facilis problemata Diophantea per numeros integros expedite resolvendi*" behandelte Aufgabe, die Gleichung:

$$\alpha x^2 + \beta x + \gamma = \zeta y^2 + \eta y + \theta$$

in ganzen rationalen Zahlen x, y zu lösen, wobei vorausgesetzt wird, daß die Koeffizienten ebenfalls ganz und rational sind, eine Grundlösung bekannt, und $\alpha\zeta$ kein Quadrat ist. Auf eine solche Gleichung wird man durch die Frage geführt, wann zwei Polygonalzahlen in bestimmter Weise linear von einander abhängen; z. B. wann eine Trigonalzahl einer Pentagonalzahl gleich wird. Schreibt man die Bedingungsgleichung so:

$$\zeta u^2 - \alpha v^2 = A\,, \quad \text{wo} \quad \begin{cases} u = \alpha x + \frac{\beta}{2}\,, \\ v = \zeta y + \frac{\eta}{2}\,, \\ A = \alpha\zeta(\theta - \gamma) + \zeta\frac{\beta^2}{4} - \alpha\frac{\eta^2}{4}\,, \end{cases}$$

ist, und setzt man voraus, daß $x = a$, $y = b$ die bekannte Lösung ist, so erhält man unendlich viele Lösungen, indem man den irrationalen Faktor der linken Seite:

$$\sqrt{\zeta}u + \sqrt{\alpha}v$$

mit

$$(s + r\sqrt{\alpha\zeta})^n\,, \quad n = 0\,, \pm 1\,, \pm 2\,, \pm 3\,, \ldots$$

multipliziert, wo s, r die Grundlösung der PELLSCHEN Gleichung $s^2 - r^2\alpha\zeta = 1$ ist. Man findet so zur Berechnung von x, y sofort die beiden Gleichungen:

$$2\sqrt{\zeta}u = (\sqrt{\zeta}u_0 + \sqrt{\alpha}v_0)(s + r\sqrt{\alpha\zeta})^n + (\sqrt{\zeta}u_0 - \sqrt{\alpha}v_0)(s - r\sqrt{\alpha\zeta})^n\,,$$
$$2\sqrt{\alpha}v = (\sqrt{\zeta}u_0 + \sqrt{\alpha}v_0)(s + r\sqrt{\alpha\zeta})^n - (\sqrt{\zeta}u_0 - \sqrt{\alpha}v_0)(s - r\sqrt{\alpha\zeta})^n\,,$$

wo $u_0 = \alpha a + \frac{\beta}{2}\,, \quad v_0 = \zeta b + \frac{\eta}{2}$ ist.

Dies ist die EULERSCHE Lösung, die etwas umständlicher gefunden wird. Die Formel wird an den drei Beispielen:

$$x^2 = \frac{y(y+1)}{2}, \qquad x^2 - 1 = \frac{y(y+1)}{2}, \qquad 3\frac{x(x+1)}{2} = \frac{y(y+1)}{2}$$

erläutert.

Schließlich behandelt EULER in Abhandlung 559: „*Nova subsidia pro resolutione formulae axx + 1 = yy*" die PELLSCHE Gleichung selbst, die man nach dem Vorschlage RUDIOS die FERMATSCHE Gleichung nennen sollte[1]). Diese hat er häufig untersucht[2]). Schon bei $a = 61$ werden die Werte von x, y ungeheuer groß. EULER sucht nach einem einfachern und schnellern Rechnungsverfahren als dem bisherigen. Allerdings handelt es sich nicht darum, für ein bestimmtes a die Lösungen x, y zu finden, sondern es soll mit einfacher Rechnung für möglichst viele a die Lösung gefunden und tabellarisch zusammengestellt werden.

Man nehme eine beliebige Lösung

$$p^2 = b^2 + c^2$$

in natürlichen Zahlen an und bestimme f, g so, daß:

$$bg - cf = \pm 1$$

wird. Dann löst:

$$x = bf + cg, \quad y = p$$

die Gleichung $x^2 - ay^2 = -1$, für

$$a = f^2 + g^2 .$$

Durch Quadrieren wird die Lösung der PELLSCHEN Gleichung selbst hieraus sofort berechnet. Ebenso kann man $x^2 - ay^2 = 2$ oder 4 lösen, wenn man von einer beliebigen Lösung

$$p^2 = b^2 - 2c^2, \text{ resp. } p^2 = b^2 - c^2$$

ausgeht. Es wird dann $a = f^2 - 2g^2$, resp. $f^2 - g^2$.

In dem 4. Problem der schon öfters genannten Abhandlung 560 wird von EULER die so oft von ihm benutzte „*descente indéfinie*" zur Lösung folgender Aufgabe verwandt: Es seien die positiven Zahlen x, y gesucht, für die:

---

1) Siehe die Ausführungen von RUDIO in der Vorrede zu Band I, 3 der *Opera omnia LEONHARDI EULERI*, p. XV/VI.

2) EULER befaßte sich mit der PELLSCHEN Gleichung schon in der Abhandlung 29; siehe *LEONHARDI EULERI Opera omnia*, series I, vol. 2, p. 6. Dann in der Abhandlung 323, series I, vol. 3, p. 73.

$$x + y = z^2, \text{ und } x^2 + y^2 = t^4, \; x > 0, \; y > 0,$$

ist. Es muß somit:

$$(x - y)^2 = 2t^4 - z^4, \; t < z,$$

werden. Diese Gleichung wird gelöst durch $x = 2uv$, $y = u^2 - v^2$, falls:

$$t^2 = u^2 + v^2, \; z^2 = u^2 + 2uv - v^2.$$

Die Frage ist somit auf die Lösung dieser beiden diophantischen Gleichungen zurückgeführt. Setzt man in denselben:

$$t = p^2q^2 + r^2s^2, \; z = p^2r^2 - 2q^2s^2, \; u = p^2q^2 - r^2s^2, \; v = 2pqrs,$$

so erhält man:

$$\frac{p}{s} = \frac{qr + \sqrt{2q^4 - r^4}}{r^2 - q^2}.$$

Man hat also wiederum $2q^4 - r^4$ zu einem Quadrat zu machen, und da q, r offenbar kleiner als z, t sind, erhält man sukzessive kleinere Lösungen. Nun ist $t = 1$, $z = 1$ eine Lösung. Man kann also durch Umkehrung des Verfahrens zu weiteren Lösungen kommen. Zum Beispiel ist $t = 13$, $z = 1$ die nächste Lösung nach der Grundlösung. Allerdings wird y nicht mehr positiv.

V. ADDITIVE ZAHLENTHEORIE

In der Abhandlung 566: „*De inductione ad plenam certitudinem evehenda*" nimmt EULER das Problem der Zerfällung einer Zahl in vier Quadrate wieder auf. Da man weiß, daß jede Primzahl der Form $4n + 1$ die Summe von zwei Quadraten ist, so kann man jede Zahl der Form $4n + 2$, die Summe zweier Primzahlen der Form $4n + 1$ ist, als Summe von vier Quadraten darstellen. EULER sieht empirisch, ob alle Zahlen der Form $4n + 2$ bis 110 Summe zweier Primzahlen der Form $4n + 1$ sind, was in der Tat stimmt. Statt Primzahlen kann man auch zwei Zahlen nehmen, die nur durch Primzahlen der Form $4n + 1$ teilbar sind. Interessant ist, daß EULER dabei als selbstverständlich den Satz ausspricht, daß es unendlich viele Primzahlen der Form $4n + 1$ gibt[1]).

Entsprechend kann man versuchen, den FERMATSCHEN Satz, daß alle Zahlen der Form $8n + 3$ Summe von drei Quadraten sind, zu beweisen. Man braucht nur zu zeigen,

1) Siehe p. 118 dieses Bandes.

daß jede Zahl der Form $8n + 3$ Summe einer Quadratzahl und einer Primzahl der Form $4n + 1$ ist.

Man darf sich wohl bei dieser Abhandlung vorstellen, daß sie aus Gesprächen von EULER mit seinen Schülern hervorgegangen ist, die letztere nachher aufschrieben, daß aber keine Beweise dabei zur Sprache kamen.

In der Abhandlung 586: „*Considerationes super theoremate Fermatiano de resolutione numerorum in numeros polygonales*" wird das berühmte EULERSCHE Verfahren, Zerlegungssätze durch Reihenentwicklungen zu beweisen, auseinandergesetzt. Dasselbe ist in der Folge so häufig angewandt worden, daß es sich erübrigt, alle die Fälle anzuführen. Hier handelt es sich um die Frage, wie oft jede natürliche Zahl als Summe von p Zahlen der vorgegebenen Reihe:

$$n_1, n_2, n_3, \ldots$$

dargestellt werden kann. EULER entwickelt die $p$te Potenz der Reihe:

$$s = \sum_{k=1}^{\infty} x^{n_k}$$

wieder in eine Potenzreihe. Der Koeffizient von x^n gibt dann die Zahl an, wie oft n durch p Zahlen der gegebenen Reihe darstellbar ist. Ist insbesondere jeder Koeffizient von null verschieden, so ist jede Zahl durch p Zahlen der Reihe darstellbar. EULER wendet dieses Verfahren für die Reihen der Trigonalzahlen, Tetragonalzahlen, allgemein der Polygonalzahlen an. Er gibt für die Berechnung der Koeffizienten der Reihen s^p eine Rekursionsformel an. Für die Reihe n^2 der Tetragonalzahlen ist s im wesentlichen eine Thetareihe, für die JACOBI erst den EULERSCHEN Ansatz zu Ende führte, indem er aus seiner Theorie der elliptischen Thetafunktionen die Zahl der Darstellungen für $p = 4$ berechnete[1]).

Ein entsprechendes Problem hat EULER in der Abhandlung 558: „*Proposita quacunque progressione ab unitate incipiente, quaeritur, quot eius terminos ad minimum addi oporteat, ut omnes numeri producantur*" im Anschluß an eine Behauptung von BÉGUELIN behandelt. Der letztere hatte arithmetische Reihen höherer Ordnung zugrunde gelegt. Wesentlich ist, daß das erste Glied eins ist. EULER gibt zunächst für eine allgemeine Reihe natürlicher Zahlen:

$$1, A, B, C, \ldots$$

ein Verfahren an, um die kleinste Zahl N zu finden, so daß jede natürliche Zahl Summe von N Zahlen der Reihe ist. Das Verfahren führt aber zu keinem Ziele, wenn nicht ein Gesetz über das Fortschreiten der Zahlen der Reihe bekannt ist. Im Falle arithmetischer

1) *JACOBIS Gesammelte Werke*, Bd. I, 1881, p. 239.

Reihen ergibt das Verfahren, daß die Vermutung BEGUELINS nur in besondern Fällen stimmt, im allgemeinen aber unrichtig ist. Ist die Reihe geometrisch, so wächst N ins Unendliche.

VI. ANALYTISCHE ZAHLENTHEORIE

Über dieses Gebiet enthält der vorliegende Band nur die eine Abhandlung 596: „*De summa seriei ex numeris primis formatae*

$$\frac{1}{3}-\frac{1}{5}+\frac{1}{7}+\frac{1}{11}-\frac{1}{13}-\frac{1}{17}+\frac{1}{19}+\frac{1}{23}-\frac{1}{29}+\frac{1}{31}-\text{etc.}$$

ubi numeri primi formae $4n-1$ *habent signum positivum, formae autem* $4n+1$ *signum negativum*", in der verschiedene Versuche gemacht werden, die Summe der im Titel genannten Reihe zu berechnen. Geht man von

$$\frac{\pi}{4}=1-\frac{1}{3}+\frac{1}{5}-\frac{1}{7}+\cdots$$

aus, so kann man zuerst alle Glieder mit echten Vielfachen von 3 im Nenner auswischen; dann von 5 usf. Dieses Verfahren konvergiert aber sehr langsam und ergibt nach langer Rechnung nur die Annäherung 0,331 für die Summe.

Besser geht man von der Formel:

$$2=\frac{3+1}{3-1}\times\frac{5-1}{5+1}\times\frac{7+1}{7-1}\times\frac{11+1}{11-1}\cdots$$

aus, von der man den Logarithmus nach der Formel:

$$\frac{1}{2}\,l\frac{a+1}{a-1}=\frac{1}{a}+\frac{1}{3a^3}+\frac{1}{5a^5}+\cdots$$

entwickelt. Setzt man:

$$P_k=\sum_{(p)}(-1)^{\frac{p+1}{2}}\frac{1}{p^{2k-1}},$$

wobei über alle ungeraden Primzahlen zu summieren ist, so wird:

$$\frac{1}{2}\,l\,2=\sum_{k=1}^{\infty}\frac{1}{2k-1}P_k.$$

P_1 ist die gesuchte Summe. P_k kann man aber für $k > 1$ ziemlich rasch auf 7 Dezimalstellen berechnen. Daraus folgt dann für P_1:

$$P_1 = 0{,}3349816\,.$$

Vergleiche zu dieser Abhandlung die Abhandlung 819 und die Vorrede zum Band I, 16 sectio altera[1]).

Die Abhandlungen EULERS lassen den modernen Leser nicht nur den Reichtum der Ideen bewundern, der im Gegensatz zur Dürre mancher moderner Theorien steht. Er führt ihn auch zur Bescheidenheit. Unsere Erkenntnisse sind ja wohl gewachsen, wir verstehen vieles besser. Aber manche tiefe Probleme stehen immer noch da, wo EULER sie verlassen hat.

Die ersten zwei Abhandlungen dieses Bandes sollten ursprünglich zum Bande I, 3 kommen. Sie sind dementsprechend noch von F. RUDIO einer ersten Durchsicht unterzogen worden. Seine Anmerkungen tragen die Initialen F. R. Nachher hat A. MARKOFF die Manuskripte des ganzen Bandes durchgearbeitet. Leider hat der Tod ihn an der Vollendung verhindert. Seine Anmerkungen sind mit A. M. gekennzeichnet, während die Anmerkungen des heutigen Herausgebers die Initialen R. F. tragen.

Zürich, den 2. März 1941. RUDOLF FUETER.

---

1) *LEONHARDI EULERI Opera omnia*, series I, vol. 16, sectio altera, p. 312: *Continuatio fragmentorum ex adversariis mathematicis depromptorum*. Siehe insbesondere die Vorrede zu jenem Bande, p. XCVI.

INDEX

Insunt in hoc volumine indicis ENESTROEMIANI commentationes
556, 557, 558, 559, 560, 564, 566, 586, 591, 596, 598, 610, 683, 696, 699, 702, 708, 713, 715, 716, 718, 719, 725, 732, 739, 744

pag.

556. De Criteriis aequationis $fxx + gyy = hzz$, utrum ea resolutionem admittat necne? 1
Opuscula analytica 1, 1783, p. 211—241

557. De quibusdam eximiis proprietatibus circa divisores potestatum occurrentibus 25
Opuscula analytica 1, 1783, p. 242—295

558. Proposita quacunque progressione ab unitate incipiente, quaeritur, quot eius terminos ad minimum addi oporteat, ut omnes numeri producantur 65
Opuscula analytica 1, 1783, p. 296—309

559. Nova subsidia pro resolutione formulae $axx + 1 = yy$ 76
Opuscula analytica 1, 1783, p. 310—328

560. Miscellanea analytica 91
Opuscula analytica 1, 1783, p. 329—344

564. Speculationes circa quasdam insignes proprietates numerorum . . 105
Acta academiae scientiarum Petropolitanae 4 II (1780: II), 1784, p. 18—30

566. De inductione ad plenam certitudinem evehenda 116
Acta academiae scientiarum Petropolitanae 4 II (1780: II), 1784, p. 38—48

pag.

586. Considerationes super theoremate Fermatiano de resolutione numerorum in numeros polygonales 125
Opuscula analytica 2, 1785, p. 3—15

591. De relatione inter ternas pluresve quantitates instituenda . . . 136
Opuscula analytica 2, 1785, p. 91—101

596. De summa seriei ex numeris primis formatae
$$\frac{1}{3} - \frac{1}{5} + \frac{1}{7} + \frac{1}{11} - \frac{1}{13} - \frac{1}{17} + \frac{1}{19} + \frac{1}{23} - \frac{1}{29} + \frac{1}{31} - \text{etc.}$$
ubi numeri primi formae $4n - 1$ habent signum positivum, formae autem $4n + 1$ signum negativum 146
Opuscula analytica 2, 1785, p. 240—256

598. De insigni promotione scientiae numerorum 163
Opuscula analytica 2, 1785, p. 275—314

610. Novae demonstrationes circa divisores numerorum formae $xx + nyy$ 197
Nova acta academiae scientiarum Petropolitanae 1 (1783), 1787, p. 47—74

683. De singulari genere quaestionum Diophantearum et methodo maxime recondita eas resolvendi 221
Nova acta academiae scientiarum Petropolitanae 9 (1791), 1795, p. 3—18

696. De casibus quibus hanc formulam $x^4 + kxxyy + y^4$ ad quadratum reducere licet. 235
Nova acta academiae scientiarum Petropolitanae 10 (1792), 1797, p. 27—40

699. Utrum hic numerus 1000009 sit primus necne inquiritur . . . 245
Nova acta academiae scientiarum Petropolitanae 10 (1792), 1797, p. 63—73

702. De novo genere quaestionum arithmeticarum pro quibus solvendis certa methodus adhuc desideratur 255
Nova acta academiae scientiarum Petropolitanae 11 (1793), 1798, p. 78—93

708. De formulis speciei $mxx + nyy$ ad numeros primos explorandos idoneis earumque mirabilibus proprietatibus 269
Nova acta academiae scientiarum Petropolitanae 12 (1794), 1801, p. 22—46

pag.

713. Investigatio trianguli in quo distantiae angulorum ab eius centro gravitatis rationaliter exprimantur 290
Nova acta academiae scientiarum Petropolitanae 12 (1794), 1801, p. 101—113

715. De variis modis numeros praegrandes examinandi, utrum sint primi necne? 303
Nova acta academiae scientiarum Petropolitanae 13 (1795/6), 1802, p. 14—44

716. Resolutio formulae diophanteae $ab(maa+nbb) = cd(mcc+ndd)$ per numeros rationales. 329
Nova acta academiae scientiarum Petropolitanae 13 (1795/6), 1802, p. 45—63

718. Facillima methodus plurimos numeros primos praemagnos inveniendi 352
Nova acta academiae scientiarum Petropolitanae 14 (1797/8), 1805, p. 3—10

719. Methodus generalior numeros quosvis satis grandes perscrutandi utrum sint primi necne? 360
Nova acta academiae scientiarum Petropolitanae 14 (1797/8), 1805, p. 11—51

725. Illustratio paradoxi circa progressionem numerorum idoneorum sive congruorum 395
Nova acta academiae scientiarum Petropolitanae 15 (1799/1802), 1806, p. 29—32

732. Solutio facilior problematis Diophantei circa triangulum, in quo rectae ex angulis latera opposita bisecantes rationaliter exprimantur. 399
Mémoires de l'académie des sciences de St-Pétersbourg 2 (1807/8), 1810, p. 10—16

739. Regula facilis problemata Diophantea per numeros integros expedite resolvendi 406
Mémoires de l'académie des sciences de St-Pétersbourg 4 (1811), 1813, p. 3—17

744. De divisoribus numerorum in forma $mxx + nyy$ contentorum 418
Mémoires de l'académie des sciences de St-Pétersbourg 5 (1812), 1815, p. 3—23

DE CRITERIIS AEQUATIONIS $fxx+gyy=hzz$ UTRUM EA RESOLUTIONEM ADMITTAT NECNE

Commentatio 556 indicis Enestroemiani
Opuscula analytica 1, 1783, p. 211—241
[Conventui exhibita die 7. decembris 1772]

1. Notum est huiusmodi aequationem pro varia relatione, quae inter numeros f, g et h intercedit, modo esse possibilem modo impossibilem, siquidem pro x, y et z numeros rationales accipi oportet, atque adeo integros, quia fracti facillime ad integros revocarentur. Ita notum est hanc aequationem: $xx + yy = 2zz$ esse possibilem, hanc vero: $xx + yy = 3zz$ impossibilem. Quando autem litterae f, g et h maiores tenent valores, iudicium, utrum aequatio sit possibilis necne, difficulter instituitur; in maximis vero numeris vix suscipiendum videtur. Hic igitur constitui in certa criteria inquirere, ex quibus iudicare liceat, utrum haec aequatio sit possibilis necne, quantumvis magni fuerint numeri f, g et h.

2. Ante omnia autem sequentia notasse iuvabit:

I. Numeros f, g et h non solum integros assumo, sed etiam non-quadratos, neque etiam per quadratum divisibiles; si enim numerus f haberet factorem quadratum, is in quadrato xx involvi posset, quod etiam de reliquis tenendum.

II. Praeterea hos numeros aeque negativos ac positivos assumere licet; et quia aequatio ita semper disponi potest, ut membra fxx et hzz obtineant valores positivos, solum membrum gyy relinquitur, quod vel positivum vel negativum esse poterit.

III. Numeros f et g tamquam primos inter se spectamus; si enim haberent communem divisorem d, vel numerus h eundem habere deberet, quo casu ille per divisionem tolleretur, vel quantitas z per d esset divisibilis[1]). Unde si loco z scribamus dv, nostra aequatio ad hanc formam reduceretur: $fxx + gyy = dhvv$, ita ut nunc f et g futuri sint primi inter se.

IV. Denique notandi sunt casus maxime obvii, quibus aequatio nostra sit possibilis. Primo scilicet hoc evenit, si fuerit vel $h = f$ vel $h = g$; illo enim casu foret $y = 0$ et $z = x$, hoc vero $x = 0$ et $z = y$. Tum vero etiam casus satis obvius erit, si fuerit $h = f + g$, quia ei satisfieret sumendo $z = x = y$. Minus obvii autem erunt casus, quibus $h = faa + gbb$; foret enim tum $x = a$, $y = b$ et $z = 1$.

3. Primum autem investigabo, datis numeris f et g, cuiusmodi numeri pro h locum habere queant, ut aequatio fiat possibilis. Quare quum hic h ut numerum incognitum spectemus, aequationem nostram hac forma referamus[2]): $fxx + gyy = szz$, ut iam idoneos valores pro littera s investigari oporteat, quibus aequatio fiat possibilis, et quidem omnes, qui hoc praestent; quem in finem sequentia Theoremata adiungo.

THEOREMA 1

Si casu $s = h$ possibilis fuerit aequatio $fxx + gyy = hzz$, ita ut litterae x, y, z iam sint cognitae, si vero insuper habeatur haec aequatio $pp + fgqq = krr$, tum nostra aequatio quoque erit possibilis casu $s = hk$.

DEMONSTRATIO

Multiplicentur enim hae duae aequationes in se et prodibit haec nova aequatio

$$hkrrzz = (fxx + gyy)(pp + fgqq) = f(px \pm gqy)^2 + g(py \mp fqx)^2 .$$

Quare si statuamus

1) [, d non continente quadratum, vide I.] R. F.

2) Editio princeps (atque etiam Comment. arithm. ed. P. H. et N. Fuss) $fxx + gyy = hzz$. Correxit F. R.

$$rz = Z\,,\ px \pm gqy = X \text{ et } py \mp fqx = Y\,,$$

nascitur haec aequatio propositae omnino similis

$$fX^2 + gY^2 = hkZ^2\,.$$

COROLLARIUM 1

4. Quodsi ergo litterae p et q ita assumere liceat, ut k obtineat factorem h, scilicet $k = hl$, tum ob $s = hhl$ novus valor idoneus erit $s = l$, quoniam quadratum hh omittere licet.

COROLLARIUM 2

5. Quemadmodum igitur ex illo valore idoneo $s = h$ erutus est alius $s = hk$ sive $s = l$, ita ex hoc simili modo alius novus valor, puta $s = m$, hincque denuo novus $s = n$ erui poterit; atque hanc determinationem in infinitum continuare licebit. Ita ex casu quocunque cognito innumerabiles alii derivari poterunt.

COROLLARIUM 3

6. Si eveniat, ut numeri h et k communem habeant divisorem d, tum novus valor hk[1]) factorem habebit dd, qui ergo expungi poterit. Hoc modo continuo ad minores numeros idoneos pro s pervenire licebit, donec tandem ad casum obvium perducamur.

COROLLARIUM 4

7. Hinc si adhuc fuerimus incerti, utrum h sit valor idoneus ipsius s, hoc autem modo procedendo perveniamus tandem ad casum obvium, tuto concludere poterimus etiam casum $s = h^2$) esse possibilem. Sin autem hoc nullo modo succedat, vel tandem in minoribus numeris ad eiusmodi casum perveniatur, cuius impossibilitas patescat, etiam valor ipse $s = h^2$) pro impossibili erit habendus.

---

1) Editio princeps: fk. Correxit R. F.
2) Editio princeps: $h = k$. Correxit R. F.

THEOREMA 2

8. *Si pro nostra aequatione tres innotescant casus possibiles* $s = h$, $s = h'$ *et* $s = h''$, *tum etiam valor idoneus erit* $s = hh'h''$.

DEMONSTRATIO

Quum igitur habeantur tres huiusmodi aequationes, quae sint

$$\begin{aligned} &\text{I.} \quad faa + gbb &&= hcc\,, \\ &\text{II.} \quad fAA + gBB &&= h'CC\,, \\ &\text{III.} \quad f\alpha\alpha + g\beta\beta &&= h''\gamma\gamma\,; \end{aligned}$$

ducatur prima in secundam et productum erit

$$hh'ccCC = (faa + gbb)(fAA + gBB) = (faA \pm gbB)^2 + fg(aB \mp bA)^2\,.$$

Faciamus nunc

$$cC = r \text{ et } faA \pm gbB = p \text{ et } aB \mp bA = q\,,$$

ut hoc productum fiat

$$pp + fgqq = hh'rr\,,$$

quod denuo multiplicatum in tertiam aequationem dabit tale productum

$$hh'h''rr\gamma\gamma = (f\alpha\alpha + g\beta\beta)(pp + fgqq) = f(p\alpha \pm gq\beta)^2 + g(p\beta \mp fq\alpha)^2\,;$$

quae forma cum plane conveniat cum proposita, veritas Theorematis est manifesta et casus $s = hh'h''$ erit possibilis.

COROLLARIUM 1

9. Ex cognitis ergo tribus valoribus idoneis h, h', h'' quartus facile invenitur. Ac si forte illi terni habeant divisores communes, hoc modo ad novos valores continuo minores pertingere licebit.

COROLLARIUM 2

10. Si ergo hunc novum valorem indicemus littera h''', tum etiam valores idonei erunt $s = hh'h'''$, $s = hh''h'''$, $s = h'h''h'''$; ex quibus porro simili modo plures alii deduci possunt.

COROLLARIUM 3

11. Quando autem hi novi valores per quadrata, uti praecepimus, deprimuntur, continuo iidem casus cogniti recurrent. Quum enim sit $h''' = hh'h''$, forma $hh'h'''$ reducitur ad h'', haec vero $hh''h'''$ ad h' et $h'h''h'''$ ad h, ita ut revera unus tantum casus novus hoc modo reperiatur.

THEOREMA 3

12. *Si aequationi nostrae* $fxx + gyy = szz$ *satisfaciat casus* $s = h$, *tum quoque omnes isti valores satisfacient*

$$s = 4fg + h,\ s = 8fg + h,\ s = 12fg + h,\ s = 16fg + h \text{ etc.},$$

quin etiam, si h *fuerit numerus satis magnus, isti*

$$s = h - 4fg,\ s = h - 8fg,\ s = h - 12fg \text{ etc.},$$

et in genere $s = h \pm 4nfg$, *dummodo hi numeri fuerint primi.*

Huius elegantissimi Theorematis demonstratio adhuc desideratur, postquam a pluribus iam dudum frustra est investigata; cuius rei difficultas manifesto in hoc est sita, quod omnes hi numeri tum demum quaesito satisfaciant, quando sunt numeri primi. Quando enim sunt compositi, evenire potest, ut non satisfaciant, etiamsi non semper a scopo aberrent. Quum autem hic tantum valeant numeri primi, probe notandum est numeros negativos, qui ex formula $s = h - 4fg$ resultare possunt, non pro primis esse habendos. Quocirca plurimum is praestitisse erit censendus, cui successerit demonstrationem huius Theorematis invenire.

COROLLARIUM 1

13. Quum hoc modo saltem ascendendo in infinitum progredi liceat, etiam multitudo valorum idoneorum pro s eo usque augeri poterit, quo usque Tabula numerorum primorum fuerit constructa[1]).

COROLLARIUM 2

14. Ita quum haec aequatio $xx + yy = zz$ sit possibilis, ubi est $f = 1$, $g = 1$ et $s = h = 1$, haec forma $4n + 1$, quatenus scilicet praebet numeros primos, etiam totidem valores idoneos pro s suppeditabit, qui numeri sunt

1, 5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97 etc.

Hos autem numeros omnes ipsos aequari summae duorum quadratorum iam dudum rigorosissime a me est demonstratum[2]), unde eo minus de demonstratione reliquorum casuum desperare fas est. His igitur omnibus casibus licebit sumere $z = 1$. Interim tamen hinc etiam numeros compositos pro s invenire licet, dum per Theorema primum producta ex binis vel pluribus horum ipsorum numerorum etiam pro s valebunt, quoniam binae illae formulae $fxx + gyy$ et $pp + fgqq$ hoc casu congruunt.

COROLLARIUM 3

15. Quia aequationi $2xx + 3yy = szz$ satisfieri potest casu $s = 341$, alios casus idem praestantes dabit formula $341 \pm 24n$, quoties scilicet prodierint numeri primi. Hinc ergo descendendo oriuntur sequentes valores

341, 317, 293, 269, 197, 173, 149, 101, 53, 29, 5.

Hi autem omnes numeri ipsi iam in forma $2xx + 3yy$ continentur, ita ut possit esse $z = 1$.

---

1) Vide EULERI Commentationem 467 (indicis ENESTROEMIANI): *De tabula numerorum primorum usque ad millionem et ultra continuanda in qua simul omnium numerorum non primorum minimi divisores exprimantur*, Novi comment. acad. sc. Petrop. 19 (1774), 1775, p. 132—183; *LEONHARDI EULERI Opera omnia*, series I, vol. 3, p. 359—404. Vide etiam in eodem volumine 3 praefationem editoris, p. X—XIII. 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—13; *LEONHARDI EULERI Opera omnia*, series I, vol. 2, p. 328—337. Vide etiam in eodem volumine 2 praefationem editoris, p. XXV—XXVI. F. R.

SCHOLION

16. Hoc Theoremate, quasi demonstratum esset, praemisso, pro quovis casu numerorum f et g omnes plane valores idonei litterae s facile inveniri poterunt. Ad hoc autem ostendendum, duos casus separatim tractari oportet: priorem, quo $f = 1$ atque idcirco primi termini primi Theorematis inter se conveniunt; alterum vero, quo f non est unitas. Unde primo aequationem $xx + gyy = szz$ evolvemus.

PROBLEMA 1

17. *Proposita aequatione* $xx + gyy = szz$, *invenire omnes valores idoneos pro* s, *quibus haec aequatio evadit possibilis.*

SOLUTIO

Hic statim evidens est valorem idoneum fore $s = g$; tum enim fit $x = 0$ et $y = z$. Etsi enim $4g$, $9g$, $16g$ etc. aeque satisfaciant, tamen omnes per quadratum depressi redeunt ad g. Verum sumto $y = 0$, omnes numeri quadrati pro s prodeunt, quos igitur omnes ad unitatem reducere liceret. Sed quia praeter hos ipsos numeros etiam iidem numeris $4ng$ sive aucti sive minuti satisfaciunt, quatenus scilicet prodeunt numeri primi, haec quadrata hic negligere non licet. Iis autem tantum quadratis indigemus, quae ad numerum $4g$ fuerint primi, quia aliter nulli numeri primi inde emergerent; quamobrem statim omnia quadrata paria hinc excluduntur et iis tantum imparibus locus conceditur, quorum radices ad numerum g fuerint primi. Semper ergo hic occurrit unitas, tum vero etiam novem, nisi g sit per 3 divisibilis, porro etiam 25, nisi g divisorem habeat 5, etc. Quando autem haec quadrata excedunt numerum $4g$, eorum loco scribantur residua ex divisione per $4g$ remanentia. Ponamus ergo hinc prodire formulas:

$$4ng + 1,\ 4ng + a,\ 4ng + b,\ 4ng + c,\ 4ng + d \text{ etc.},$$

ubi scilicet a, b, c, d [etc. sunt] ea residua, quae ex quadratis per $4g$ divisis resultant. Verum praeter hos casus alius est obvius $s = 1 + g$, siquidem g fuerit numerus par; sin autem fuerit impar, sumatur $s = 4 + g$, ut scilicet habeatur numerus ad $4g$ primus. Tum vero quia per Theorema primum

producta ex binis numeris satisfacientibus etiam satisfaciunt, habebimus insuper istas formulas loco $1 + g$ vel $4 + g$ scribendo h

$$s = 4ng + h,\ 4ng + ah,\ 4ng + bh,\ 4ng + ch,\ 4ng + dh \text{ etc.},$$

quos omnes valores coniunctim ita ob oculos constituamus:

$$s = 4ng + \begin{pmatrix} 1, & a, & b, & c, & d & \text{etc.} \\ h, & ah, & bh, & ch, & dh & \text{etc.} \end{pmatrix}.$$

Quae omnes formulae eatenus valent, quatenus numeros primos producunt, hocque modo omnes plane numeri primi idonei reperientur; compositi autem nulla plane laborant difficultate, quum nascantur ex duobus pluribusve numeris primis idoneis. Quin etiam ipsum numerum g eiusque producta per numeros iam inventos annumerari oportet.

COROLLARIUM 1

18. Quia veritas huius solutionis nondum plane est evicta, casus aliquos obvios consideremus, quos semper in aliqua superiorum formularum contineri deprehendemus. Ita casus $s = 1 + 4g$ continetur in formula $4ng + 1$ et $s = 1 + 9g$ continetur in formula $4ng + h$, si fuerit $h = 1 + g$; at si $h = 4 + g$, in ea continebitur $s = 4 + 9g$. Similique modo res se habet in formulis $1 + 16g$, $1 + 25g$, $1 + 36g$ vel $4 + g$, $4 + 9g$, $4 + 25g$ etc., ubi eos casus, qui numeros primos producere nequeunt, excludimus.

COROLLARIUM 2

19. Haec solutio aeque locum habet, sive g sit numerus positivus, sive negativus. At quia hoc posteriori casu in formulis inventis littera h obtinet valorem negativum, loco terminorum h, ah, bh, ch etc. eorum complementa ad numerum $4g$ scribantur.

COROLLARIUM 3

20. Casu, quo g est numerus negativus, si iam fuerint inventae formulae superiores, quae valent pro formula $xx - gyy$, si ibi signa mutentur, sive loco numerorum 1, a, b, c, d etc. scribantur eorum complementa ad $4g$, tum illae inservient huic aequationi $gyy - xx = szz$.

SCHOLION

21. Haec autem maxime illustrabuntur et facilius in usum vocari poterunt, si plura exempla adiungamus, quibus etiam natura numerorum aliaeque abstrusae proprietates clarius perspicientur.

EXEMPLUM 1

Sit $g = 1$ et aequatio proposita $xx + yy = szz$, atque hic pro valoribus ipsius s unica habetur formula $4n + 1$. Casus autem $1 + g = 2$, quia ad $4g$ non est primus, generali formulae innecti nequit; interim tamen seorsim praebet numerum idoneum $= 2$. Pro numeris igitur primis satisfacientibus praeter 2 habemus superiorem seriem

1, 5, 13, 17, 29, 37, 41 etc.

et producta ex quocunque horum praebebunt omnes numeros compositos satisfacientes.

At pro casu $g = -1$ seu aequatione $xx - yy = szz$ praeter formam $4n + 1$ ex quadratis ortam formula $4 + g = 3$ dabit insuper hanc $4n + 3$. Sicque omnes numeri primi in alterutra harum duarum formularum $4n + 1$ et $4n + 3$ erunt contenti, ideoque omnes plane numeri primi hoc casu sunt idonei, quippe quos omnes in differentiam duorum quadratorum resolvere licet. Hinc quidem 2 excluditur, quoniam differentia duorum quadratorum esse nequit; attamen valorem pro s dari potest, siquidem pro z sumatur numerus par. Nam $2 \cdot 4$ utique est $9 - 1$.

EXEMPLUM 2

22. Sit nunc $g = 2$ et proposita haec forma $xx + 2yy = szz$, ubi quum sit $4g = 8$, quadrata imparia 1, 9, 25 etc. omnia reducuntur ad eandem formam $8n + 1$; at casus $1 + g = h = 3$ insuper dat hanc formam $8n + 3$, sicque omnes numeri primi hac specie referentur: $8n + (1, 3)$, quibus accedit insuper $s = g = 2$, sicque omnes hi numeri primi sunt

1, 3, 11, 17, 19, 41, 43, 59, 67, 73, 83, 89, 97 etc.

At si sit $g = -2$, pro formula $xx - 2yy = szz$ reperitur $s = 8n + (1, 7)$, quibus annumerari debet -2, atque hinc vicissim pro

aequatione $2yy - xx = szz$ erit $s = 8n + (7, 1)$. Iidem ergo numeri pro his duobus posterioribus casibus valent.

EXEMPLUM 3

23. Pro formula $xx + 3yy = szz$ secundum praecepta data prodit $s = 12n + (1, 7)$, et insuper numerus solitarius 3. Pro formula autem $xx - 3yy = szz$ reperitur $s = 12n + (1)$.

EXEMPLUM 4

Pro formula $xx + 5yy = szz$ reperitur $s = 20n + (1, 9)$, cum numero 5; at pro formula $xx - 5yy = szz$ reperitur $s = 20n + (1, 19)$, cum numero -5.

EXEMPLUM 5

Pro formula $xx + 6yy = szz$ reperitur $s = 24n + (1, 7)$, una cum numero 6; pro formula autem $xx - 6yy = szz$ colligitur $s = 24 + (1, 19)$, una cum numero -6, ubi numeri ± 6 tamquam primi sunt spectandi, etiamsi in se sint compositi.

SCHOLION

24. Plura huiusmodi exempla non evolvimus, quum calculus satis sit perspicuus, sed potius Tabulam sequentem adiungimus, in qua pro quavis formula $xx + gyy = szz$ primo formam numerorum primorum pro s exhibebimus, deinde vero ipsos numeros primos usque ad centum; quibus cognitis omnia producta, tam ex binis quam pluribus numeris primis, pro valore litterae s satisfaciunt:

$xx + yy = szz$	$s = 4n + 1$ cum 2
Num. primi	1, 2, 5, 13, 17, 29, 37, 41 etc.
$xx - yy = szz$	$s = 4n + (1, 3)$
Num. primi	1, 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37 etc.
$xx + 2yy = szz$	$s = 8n + (1, 3)$ cum 2
Num. primi	2; 1, 3, 11, 17, 19, 41, 43, 59, 67, 73, 83, 89, 97
$xx - 2yy = szz$	$s = 8n + (1, 7)$ cum -2
Num. primi	-2; 1, 7, 17, 23, 31, 41, 47, 71, 73, 79, 89, 97

$xx + 3yy = szz$	$s = 12n + (1, 7)$ cum 3
Num. primi	3; 1, 7, 13, 19, 31, 37, 43, 61, 67, 73, 79, 97
$xx - 3yy = szz$	$s = 12n + 1$ cum solitario -3
Num. primi	-3; 1, 13, 37, 61, 73, 97
$xx + 5yy = szz$	$s = 20n + (1, 9)$ cum numero 5
Num. primi	5; 1, 29, 41, 61, 89
$xx - 5yy = szz$	$s = 20n + (1, 9, 11, 19)$ cum numero -5
Num. primi	-5; 1, 11, 19, 29, 31, 41, 59, 61, 71, 79, 89
$xx + 6yy = szz$	$s = 24n + (1, 7)$ cum numero 6
Num. primi	6; 1, 7, 31, 73, 79, 97
$xx - 6yy = szz$	$s = 24n + (1, 19)$ cum -6
Num. primi	-6; 1, 19, 43, 67, 73, 97
$xx + 7yy = szz$	$s = 28n + (1, 11, 23, 9, 25, 15)$ cum numero 7
Num. primi	7; 1, 11, 23, 29, 37, 43, 53, 67, 71, 79
$xx - 7yy = szz$	$s = 28n + (1, 9, 25)$ cum -7
Num. primi	-7; 1, 29, 37, 53[1])
$xx + 10yy = szz$	$s = 40n + (1, 9, 11, 19)$ cum 10
Num. primi	10; 1, 11, 19, 41, 59, 89
$xx - 10yy = szz$	$s = 40n + (1, 9, 31, 39)$ cum -10
Num. primi	-10; 1, 31, 41, 71, 79, 89
$xx + 11yy = szz$	$s = 44n + \left(\begin{smallmatrix} 1, & 9, & 25, & 5, & 37, \\ 15, & 3, & 23, & 31, & 27 \end{smallmatrix}\right)$ cum 11
Num. primi	$+11$; 1, 3, 5, 23, 31, 37, 47, 53, 59, 67, 71, 89, 97
$xx - 11yy = szz$	$s = 44n + (1, 9, 25, 5, 37)$ cum -11
Num. primi	-11; 1, 5, 37, 53, 89, 97

PROBLEMA 2

25. *Proposita aequatione* $fxx + gyy = szz$, *invenire omnes numeros primos, qui pro* s *valores idoneos praebent, quibus haec aequatio evadit possibilis.*

SOLUTIO

Sit h valor quicunque idoneus pro s et per Theorema nondum demonstratum patet omnes numeros primos in hac formula contentos $4nfg + h$,

1) Editio princeps: 43, 83. Correxit R. F.

pariter pro s valere; ex quo manifestum est istum valorem h ad $4fg$ primum esse debere. Talis autem valor facile invenitur. Si enim ambo numeri f et g fuerint impares, capi poterit $h = 4f + g$ sive $h = f + 4g$; sin autem numerorum f et g alter fuerit par, alter impar, valor idoneus habetur $h = f + g$. Quo autem alii insuper numeri primi, atque adeo omnes, pro s obtineantur, consideretur formula $pp + fgqq = krr$ atque in Problemate praecedente iam assignavimus omnes primos pro k valentes, qui sint $4nfg + (1, a, b, c, d$ etc.); nunc hae duae aequationes ducantur in se et iam ostendimus prodire huiusmodi formam $hkrrzz$ sive $hkZ^2 = fX^2 + gY^2$, quocirca productum hk etiam dabit valorem idoneum pro s; unde perspicuum est omnes numeros primos pro s idoneos contineri debere in hac forma generali

$$s = 4nfg + (h, ah, bh, ch, dh \text{ etc.})^1).$$

Cognitis autem numeris primis pro s valentibus, qui nostrae aequationi $fxx + gyy = szz$ satisfaciunt, si insuper omnes numeri primi pro k adhibendi innotescant, qui sint A, B, C, D etc., tum producta priorum pro s inventorum in singulos vel binos vel ternos etc. horum posteriorum praebebunt etiam valores idoneos pro s, hocque adeo modo facile erit infinitos valores litterae x exhibere.

COROLLARIUM 1

26. Si eveniat, ut primus valor pro h inventus sit quadratus, tum, quia is iam in ordine numerorum $1, a, b, c, d$ etc. continetur, iidem valores pro s locum habebunt, qui pro k sunt assignati.

COROLLARIUM 2

27. Sin autem numerus h in ordine $1, a, b, c, d$ etc. non contineatur, tum nullo modo fieri poterit, ut valores pro s et k inter se conveniant, sed omnes a se invicem discrepabunt.

EXEMPLUM 1

28. Proposita sit aequatio $2xx + 3yy = szz$, ubi $f = 2$ et $g = 3$, primus autem valor $h = 5$. Tum ergo consideretur aequatio $pp + 6qq = krr$,

1) Editio princeps: $s = 4nfk + (h, ah, bh, ch, dh$ etc.). Correxit R. F.

et vidimus valores primos pro k contineri in hac formula $24n + (1, 7)$. His igitur numeris 1, 7 in $h = 5$ ductis omnes numeri primi pro s in hac formula continentur $24n + (5, 11)$, qui sunt 5, 11, 29, 53, 59, 83 etc.

Pro aequatione $2xx - 3yy = szz$, ubi $f = 2$ et $g = -3$, valor cognitus habetur $h = -1$ sive $h = 23$; at aequationi $pp - 6qq = krr$ pro k inventa est formula $24n + (1, 19)$, unde omnes numeri primi pro s fiunt: $24n + (5, 23)$, quae formula praebet hos numeros primos: 5, 23, 29, 47, 53, 71 etc.

Verum pro hac aequatione $3xx - 2yy = szz$, ubi $f = 3$ et $g = -2$, valor h fit $= 1$; et quia formula $pp - 6qq = krr$ eadem est quae ante, iidem etiam numeri primi pro s in formula $24n + (1, 19)$ continentur hincque ipsi numeri primi $24n + (1, 19)$[1]), qui igitur fient: 19, 43, 67, 73 etc.[2])

EXEMPLUM 2

29. Proposita aequatione $2xx + 5yy = szz$, ubi $f = 2$ et $g = 5$, primus valor h fit $= 7$, et quia aequationi $pp + 10qq = krr$ convenit formula

$$40n + (1, 9, 11, 19),$$

pro valoribus primis ipsius s habebimus

$$s = 40n + (7, 23, 37, 13),$$

ergo ipsi numeri primi erunt 7, 13, 23, 37, 47, 53 etc.

At proposita aequatione $2xx - 5yy = szz$ fit statim $h = -3$; et quia pro aequatione $pp - 10qq = krr$ invenimus formulam $40n + (1, 9, 31, 39)$, numeri primi quaesiti continebuntur in hac formula

$$40n + (37, 13, 27, 3);$$

ergo ipsi numeri primi erunt 3, 13, 37, 43, 53, 67, 83 etc.

Denique pro formula $5xx - 2yy = szz$ ob $h = 3$ ex iisdem numeris k numeri quaesiti pro s sunt:

$$40n + (37, 13, 27, 3).$$

1) Editio princeps: (5, 23). Correxit R. F.
2) Editio princeps: 5, 23, 29, 47, 53, 71 etc. Correxit R. F.

SCHOLION 1

30. Quae hactenus iam tradita hisque exemplis illustrata sunt, omnes numeros primos pro s satisfacientes suppeditant, qui in se invicem multiplicati, uti praecepimus, dant numeros compositos aeque satisfacientes. Neque vero hinc semper omnes plane numeri compositi pro s idonei obtinentur, sed dantur casus, quibus praeterea alii numeri primi in valores compositos ipsius s ingrediuntur. Caussa huius rei in eo consistit, quod in investigatione superiori numeros pares statim exclusimus, qui tamen cum aliis numeris primis iuncti quaesito satisfacere possunt. Ad hos ergo eruendos ponamus statim $s = 2h$, ut sit

$$\frac{fxx + gyy}{2} = hzz .$$

Quodsi iam haec formula $\frac{fxx + gyy}{2}$ praebeat numerum imparem sive productum ex impari in quadratum par, ex eo statim infinitos alios valores pro h elicere licet. Sit enim α eiusmodi numerus impar, et quum pro forma $xx + fgyy = szz$ omnes valores primi ipsius s in hac forma contineantur $4fg + (1, a, b, c, d$ etc.), omnes numeri primi idonei pro nostra littera h in hac forma continebuntur

$$4fg + (\alpha, \alpha a, \alpha b, \alpha c, \alpha d \text{ etc.}) ,$$

qui si fuerint diversi ab iis, quos ante sumus assecuti, etiam infiniti alii habebuntur numeri primi, qui in compositionem numeri s ingredi possunt. Singuli enim isti numeri, quos litteris A, B, C, D etc. designemus, per 2 multiplicati, idoneos praebent valores pro s, qui ergo erunt $2A$, $2B$, $2C$, $2D$ etc.[1]). Et quia producta ex binis eorum etiam satisfaciunt, hinc nascentur numeri impares, AB, AC, AD, BC, BD, CD etc.[1]). Ita in exemplo $xx - 3yy = szz$ formula $\frac{xx - 3yy}{2}$ statim dat -1. Quum ergo pro hoc casu inventa sit formula $s = 12n + 1$, pro valoribus ipsius h habebimus formulam $12n - 1$ sive $12n + 11$, quae praebet hos numeros primos

$$11, 23, 47, 59, 71, 83,$$

qui duplicati omnes etiam satisfaciunt, atque etiam producta ex eorum binis, tum vero etiam producta ex his in singulos eorum, quos ante iam assigna-

1) Editio princeps (atque etiam Comment. arithm. ed. P. H. et N. Fuss) loco $A, B, C, \ldots$ habet $a, b, c, \ldots$ Correxit F. R.

vimus; hocque pacto multitudo valorum compositorum vehementer augetur. Hoc praecipue iis casibus usu venit, ubi formulae supra inventae ex paucioribus membris constabant. Pro formula autem $xx + 7yy = szz$ eius dimidium $\frac{xx+7yy}{2}$ praebet 4, sive $1 = \alpha$, qui valor quum iam in formula supra data contineatur, hinc novi valores non oriuntur. At vero formula $\frac{xx-7yy}{2}$ praebet $\alpha = -3$ ideoque valores pro h erunt $28n + (1, 9, 25)$, qui numeri iam antea occurrunt. Hoc ergo probe observare oportet eum, qui etiam omnes numeros compositos pro s satisfacientes investigare voluerit, unde huic negotio immorari superfluum foret.

SCHOLION 2

31. Quamtumvis autem haec egregia videantur, utique hic erit dolendum, quod nondum firmis demonstrationibus sunt munita, cuius rei ratio potissimum in eo sita videtur, quod formulae pro s inventae eatenus tantum valent, quatenus numeros primos suppeditant. Quamquam autem omnes labores a me suscepti spem meam fefellerunt, tamen spero conatus meos iis, qui huiusmodi speculationibus delectantur, non fore ingratos, praecipue quia iam memoratam illam difficultatem circa numeros primos de medio sustuli, ita ut nunc sine dubio aditus ad ista numerorum mysteria non mediocriter facilior reddi videatur.

PROPOSITIO 1

32. *Si fuerit* $fxx + gyy = szz$, *existente* s *numero primo, tum si omnia quadrata per hunc numerum* s *dividantur et residua ex singulis enata notentur, inter ea semper occurret* $-fg$ *sive sublata negatione* $s - fg$.

DEMONSTRATIO

Sint residua illa ex divisione per s orta $1, a, b, c, d$ etc. ac praebeat quadratum xx residuum a, quadratum vero yy residuum b, atque evidens est numerum $fa + gb$ per s fore divisibilem. Sit ergo $fa + gb = \lambda s$ eritque $gb = \lambda s - fa$ ideoque $bg^2 = \lambda gs - fga$. Quum iam omne residuum, in quadratum ductum, iterum inter residua occurrat, siquidem infra s deprimatur, prodeat inde residuum c, ita ut sit $c = \lambda gs - fga$, et multiplo ipsius s sublato $c = -fga$ sive $c = s - fga$, et quia hoc aeque valet de omnibus residuis, loco a sumentes unitatem habebimus $c = -fg$ sive $c = s - fg$.

COROLLARIUM 1

33. Si ergo satisfaciat valor $s = h$, quia formula $4nfg + h$, si fuerit numerus primus, etiam satisfaciat pro s, si per hunc numerum omnia quadrata dividantur, inter residua certo occurret $-fg$.

COROLLARIUM 2

34. Sit ille divisor $= D$, et quia datur quadratum, quod sit pp, unde nascitur residuum $-fg$, manifestum est formulam $pp + fg$ divisibilem fore per divisorem D.

COROLLARIUM 3

35. Hic autem iam manifesto involvitur difficilis illa conditio numeri primi, quia ordo residuorum hic memoratus locum non habet, nisi D sit numerus primus. Fieri enim utique posset, ut $-fg$ non inter residua occurreret, si divisor non esset primus.

PROPOSITIO 2

36. *Si quadrata dividendo per quemcunque numerum primum* $D = 2P + 1$ *inter residua occurrat numerus* r, *tunc eius potestas* r^P *per* D *divisa unitatem relinquet; et vicissim, si* $r^P - 1$ *divisorem habeat* D, *numerum* r *inter residua reperiri necesse est*[1]).

DEMONSTRATIO

Quum divisor D ponatur $2P + 1$, omnium numerorum ipso minorum multitudo est $2P$; quorum quia semissis tantum in residua ingreditur, multitudo residuorum erit P. Deinde etiam certum est, si inter residua occurrat numerus r, tum quoque omnes eius potestates ibidem occurrere debere, quemadmodum simplicissima $r^0 = 1$ inest. Quocirca potestas r^P necessario non novum residuum praebere potest. Atque hinc rite concludi-

1) Vide commentationes 134 et 262 (indicis ENESTROEMIANI): *Theoremata circa divisores numerorum*, Novi comment. acad. sc. Petrop, 1 (1747/8), 1750, p. 20—48. *LEONHARDI EULERI Opera omnia*, series I, vol. 2, p. 62—85, et *Theoremata circa residua ex divisione potestatum relicta*, Novi comment. acad. sc. Petrop. 7 (1758/9), 1761, p. 49—82. *LEONHARDI EULERI Opera omnia*, series I, vol. 2, p. 493—518. R. F.

tur inde ipsum primum residuum 1 prodire debere, sicque constat propositam potestatem r^P, per numerum primum D divisam, residuum relinquere $= 1$.

Quod ad inversionem propositionis attinet, perpendamus formulam $r^{2P}-1$ perpetuo divisibilem esse per $2P+1$, ex quo sequitur vel formulam[1]) r^P-1 vel r^P+1 divisibilem esse debere. Omnes ergo numeri pro r sumti, quibus formula posterior r^P+1 fit divisibilis, ex ordine residuorum excluduntur, atque illi tantum, qui formulam r^P-1 divisibilem producunt, relinquuntur; quorum numerus quum sit P, sequitur omnes numeros r fore residua.

COROLLARIUM 1

37. Quum primus divisor fuerit $= h$, ponamus $h = 2p+1$, et quia $r = -fg$, sequitur formulam $(-fg)^p - 1$ per $h = 2p+1$ esse divisibilem seu fore $r^p = 1 + m(2p+1)$. Quum deinde etiam divisor esse possit $h + 4nfg$, dummodo fuerit numerus primus, ob $h = 2p+1$ faciamus

$$D = 2p + 1 + 4nfg = 2P + 1 ,$$

ita ut sit $P = p + 2nfg$, atque etiam haec potestas

$$(-fg)^P = (-fg)^{p+2nfg}$$

unitate minuta per divisorem $2p + 1 + 4nfg$ evadet divisibilis.

COROLLARIUM 2

38. Quocirca totum negotium huc redit, ut ponendo brevitatis gratia $-fg = r$ ostendatur, si formula $r^p - 1$ fuerit divisibilis per $2p+1$, tum etiam hanc formulam $r^{p+2nr} - 1$ fore divisibilem per $2p + 1 + 4nr$, siquidem numerus $2p + 1 + 4nr$ fuerit numerus primus.

COROLLARIUM 3

39. Si ponamus $r = -1$, evidens est formulam $(-1)^p - 1$ dividi non posse per $2p+1$, nisi p sit numerus par. Sit ergo $p = 2q$ et $4q+1$

1) Editio princeps (atque etiam Comment. arithm. ed. P. H. et N. Fuss): *formulam* $r^{2P}-1$. Correxit F. R.

numerus primus, tum certe inter residua reperietur $4q$. Sit quadratum, unde hoc residuum nascitur, $= vv$, et $vv + 1$ divisibile erit per $4q + 1$. Ita ex his rationibus facillime patet semper dari summam duorum quadratorum divisibilem per numerum $4q + 1$, id quod alias per multas demum ambages ostendi solet.

40. Missis autem his, quae principiis nondum satis corroboratis innituntur, per certa principia in indolem huiusmodi aequationum $fxx + gyy = szz$ accuratius inquiramus. Ac primo quidem iam rigorose monstravimus, si haec aequatio possibilis fuerit casu $s = h$, tum sumto numero k, ita ut sit $pp + fgqq = krr$, fore etiam $s = hk$ valorem idoneum pro s. Hoc igitur praemisso ad sequentia progrediamur.

THEOREMA 4

41. *Si aequatio $fxx + gyy = hzz$ fuerit possibilis, tum semper assignari potest talis formula $tt + fg$, per numerum h divisibilis, ita ut numerus t minor sit quam $\frac{1}{2}h$.*

DEMONSTRATIO

Quum formula illa $fxx + gyy$ divisibilis sit per h, si ea ducatur in formulam $fpp + gqq$, etiam productum per h erit divisibile. Sumantur ergo numeri p et q ita, ut sit $py - qx = 1$, id quod semper fieri potest, nisi x et y habeant communem divisorem, qui autem casus hinc sponte excluditur; tum autem productum illud erit

$$(fpx + gqy)^2 + fg\,,$$

unde sumto $t = fpx + gqy$ formula $tt + fg$ divisorem habebit h. Hic autem ponamus $t = t' \pm \lambda h$, acque tum haec formula $t't' + fg$ etiamnunc per h erit divisibilis. Hoc vero modo t' infra semissem numeri h deprimetur; consequenter certo dabitur formula $tt + fg$ divisibilis per h, in qua t non excedit semissem ipsius h.

COROLLARIUM 1

42. Haec eadem proprietas numeri h, quia tantum a producto fg pendet, aeque patet ad hanc aequationem $xx + fgyy = hzz$. Quin etiam, si productum fg in duos alios factores ζ et η resolvi queat, eadem conditio locum habet, ut aequatio $\zeta xx + \eta yy = hzz$ sit possibilis.

COROLLARIUM 2

43. Quoties ergo numerus h fuerit divisor formulae $tt + fg$, inde non semper concludi potest aequationem $fxx + gyy = hzz$ esse possibilem, sed plus inde inferri nequit, quam dari formulam affinem $\zeta xx + \eta yy$ aequalem termino hzz, dummodo fuerit $\zeta\eta = fg$.

COROLLARIUM 3

44. Quia $t < \frac{1}{2}h$, formula $tt + fg$ minor erit quam $\frac{1}{4}hh + fg$, quae ergo si dividatur per h, quotus minor erit quam $\frac{1}{4}h + \frac{fg}{h}$.

COROLLARIUM 4

45. Vicissim ergo etiam patet, si nulla detur huiusmodi formula per h divisibilis, tum etiam neque hanc aequationem: $fxx + gyy = hzz$ neque ullam aliam adfinem $\zeta xx + \eta yy = hzz$ esse possibilem, si scilicet fuerit $\zeta\eta = fg$. Ad hoc ergo examinandum sufficit eos tantum casus evolvisse, quibus $t < \frac{1}{2}h$.

THEOREMA 5

46. *Si aequatio $fxx + gyy = hzz$ fuerit possibilis, tum semper numerum h', minorem quam h*[1]*, exhibere licet, ita ut haec aequatio $fxx + gyy = h'zz$ sit possibilis.*

DEMONSTRATIO

Si ponamus formulam $tt + fg = k$, supra iam demonstravimus etiam hanc formam $fxx + gyy = hkzz$ esse possibilem. Modo autem vidimus pro t dari valorem adeo minorem quam $\frac{1}{2}h$, quo formula $tt + fg$ habeat factorem h. Sit ergo alter factor h' ideoque $k = hh'$ et $hk = h'h^2$, et deleto quadrato hh, utpote in quadrato zz involvendo, orietur aequatio quoque possibilis:

$$fxx + gyy = h'zz, \text{ ubi } h' < \tfrac{1}{4}h + \frac{fg}{h}.$$

1) Vide Corollarium 1. R. F.

COROLLARIUM 1

47. Quantuscunque ergo fuerit numerus h', hoc modo continuo ad minores valores h', h'' etc. pervenire licebit, donec tandem numeri prodeant tam parvi, qui ulteriorem diminutionem non admittunt. Quia enim $h' < \frac{1}{4}h + \frac{fg}{h}$, utique h' excedere debebit $\frac{fg}{h}$; unde manifestum est, quo minor numerus h fuerit redditus, ulteriorem diminutionem retardari atque adeo penitus sisti.

COROLLARIUM 2

48. Si, dum hoc modo pro h continuo minores valores eruuntur, tandem perveniatur ad valorem vel f vel g, hinc certo concludere poterimus aequationem propositam esse possibilem, quandoquidem ista: $fxx + gyy = fzz$ casum maxime obvium involvit, scilicet $y = 0$ et $z = x$. Sin autem nullo modo deducamur ad f vel g, sed ad alium numerum, ζ, divisorem ipsius fg, indicio id erit non ipsam aequationem propositam, sed aliam adfinem, scilicet $\zeta xx + \eta yy = hzz$, esse possibilem; unde si tandem adeo perveniretur ad unitatem, tum aequatio $xx + fgyy = hzz$ foret possibilis.

PROBLEMA 3

49. *Proposita aequatione* $fxx + gyy = hzz$, *investigare, utrum ea sit possibilis necne.*

SOLUTIO

Quia hic tres numeri proponuntur, f, g et h, aequatio ita exhibeatur, ut numerus h eorum sit maximus, quandoquidem hic perinde est, utrum termini aequationis sint positivi, an negativi. Tum sumatur formula $tt + fg$ et examen instituatur, utrum, pro t numeris minoribus quam $\frac{1}{2}h$ sumendis, haec formula fiat divisibilis per h necne. Casu posteriore statim pronunciare poterimus aequationem propositam [non] esse possibilem; priore autem casu loco h nanciscemur alium numerum minorem h' simili modo examini subiiciendum, donec tandem ulterior diminutio non habeat locum. Et si inter hos valores occurrat f vel g, certum hoc erit indicium aequationem propositam esse possibilem; sin autem ad alium numerum ζ, divisorem producti fg, perveniamus, tum concludemus aequationem $\zeta xx + \eta yy = hzz$ esse possibilem existente

$\zeta\eta = fg$. Quodsi autem neutrum usu veniat, tum in valore minimo in locum h succedente acquiescamus, qui sit h', et nunc aequationem $fxx + gyy = h'zz$ ita disponamus, ut litterarum f et g maior, puta g, ad dextram referatur hoc modo: $h'zz - fxx = gyy$, et nunc loco g simili modo quaerantur g', donec perveniatur ad g' sive ipsi h' sive ipsi f aequalem, quo casu propositum nostrum itidem erit evictum. At si ne hoc quidem facile patescat, loco g introducamus valorem exiguum inde ortum g', et nunc aequatio $h'zz - g'yy = fxx$ simili modo tractetur; sicque tandem ad ternos numeros f', g', h' pervenietur, ut iudicium nulla amplius difficultate laborare possit.

COROLLARIUM 1

50. Si numerus h fuerit praegrandis, utique taedioso calculo erit opus antequam formulae $tt + fg$ omnes casus usque ad $t = \frac{1}{2}h$ exigantur; vix autem talem laborem quisquam suscipiet. Admisso autem superiore principio statim valor iste h infra $4fg$ deprimetur.

COROLLARIUM 2

51. Si ingens ille numerus h habeat factores, puta m et n, hic labor non parum sublevabitur, dum primo talis valor pro t investigatur, ut formula $tt + fg$ saltem divisibilis fiat vel per m vel per n; neque enim deinceps difficile erit casum elicere, quo ista formula per ipsum numerum h fiat divisibilis. De caetero tota haec operatio exemplis clarius illustrabitur.

EXEMPLUM 1

52. Examinanda proponatur haec aequatio $3xx + 5yy = 1007zz$. Sumatur ergo formula $tt + 15$ ob $f = 3$ et $g = 5$, et quia $h = 1007 = 19 \cdot 53$, quaeratur t primo ita, ut $tt + 15$ saltem divisorem obtineat 19, quod manifesto fit sumendo $t = 2$; tum enim fit $k = 19$ et sic prodit $h' = 53$, sublato quadrato 19^2. Nunc porro quaeratur t, ut formula $tt + 15$ divisorem nanciscatur 53, quod fit, si $t = 12$, ita ut iam habeamus $k = 159 = 3 \cdot 53$ ideoque $h'k = 3 \cdot 53^2$ sicque $h'' = 3$, qui numerus, quum aequalis sit ipsi f, indicat nostram formulam esse possibilem.

EXEMPLUM 2

53. Proponatur haec aequatio: $2xx + 7yy = 23zz$. Hic $f = 2$, $g = 7$ et $h = 23$. Sumatur $k = tt + 14$, qui numerus fit divisibilis per 23 sumendo $t = 3$. Erit autem $k = 23 = h$ ideoque $hk = 23^2$; unde intelligimus hanc aequationem $xx + 14yy = zz$ esse possibilem; neque vero hinc sequitur propositam esse impossibilem, quum fieri possit, ut utraque simul locum habeat. Videamus ergo, an haec forma: $2xx + 7yy = zz$ sit possibilis, quod quidem manifestum est sumendo $x = 1$, $y = 1$ et $z = 3$. Sed tamen regula nostra utamur, et quia est $h' = 1$, sumendo $t = 2$ erit $k = 18 = 2 \cdot 3^2$, hinc $h'k = 2 \cdot 3^2$ ideoque $h'' = 2$, hoc est $h'' = f$; sicque patet etiam ipsam propositam aequationem esse possibilem.

COROLLARIUM

54. Quum ergo hoc casu utraque forma $fxx + gyy = hzz$ et $xx + fgyy = hzz$ sit possibilis, operae pretium erit in eos casus inquirere, quibus utraque formula $fxx + gyy$ et $xx + fgyy$ eidem termino hzz aequalis esse possit. Hoc autem manifesto eveniet, quando fieri poterit $fxx + gyy = uu + fgvv$; quod si evenire possit, infiniti certe exhiberi poterunt casus, inter quos dabitur unus, quo $v = 0$. Illud igitur evenit, quoties evadere potest $fxx + gyy = uu$, id quod nostro exemplo manifesto fit.

EXEMPLUM 3

55. Proponatur aequatio $xx + 6yy = 145zz = 5 \cdot 29zz$. In formula ergo $k = tt + 6$ sumamus $t = 2$, ut fiat $k = 2 \cdot 5$ ideoque $hk = 2 \cdot 5^2 \cdot 29$ sicque $h' = 2 \cdot 29$. Nunc sumatur t ita, ut k fiat per 29 divisibile, quod evenit sumendo $t = 9$; fiet enim $k = 87 = 3 \cdot 29$, ergo $h'k = 2 \cdot 3 \cdot 29^2$ et $h'' = 6 = g$; consequenter nostra aequatio est utique possibilis.

EXEMPLUM 4

56. Proponatur aequatio $3xx + 7yy = 89zz$. Hic est $f = 3$, $g = 7$ et $h = 89$ ideoque $k = tt + 21$. Quaeratur ergo t, ut illa formula divisibilis fiat per 89. Ponamus in hunc finem $tt + 84 = 89n$. Hic enim loco 21 scribere liceret $21uu$ in genere, atque hic sumpsimus $u = 2$, ut etiam hunc casum

illustramus. Quum autem nullum quadratum sit formae $3n + 2$, pro numero n excluduntur valores 1, 4, 7, 10 etc. et in genere $3\alpha + 1$. Deinde excluduntur omnes numeri impariter pares 2, 6, 10, 14 etc. et, quia omnia quadrata sunt formae vel $5\alpha + 1$ vel $5\alpha + 4$, pro n etiam excluduntur hi numeri: 3, 4, 8, 9, 13, 14 et in genere $5\alpha + 3$ et $5\alpha + 4$. His exclusis pro n remanent examinandi hi numeri: 5, 11, 12, 15, 17, 20, 21, 27, 32, 35, 36, 41, quos ergo successive in aequatione $tt = 89n - 84$ loco n substitui oportet. At vero primus valor $n = 5$ statim praebet quadratum, unde $k = 5 \cdot 89$ et $h' = 5$. Nunc autem k per 5 fiet divisibile sumendo $t = 1$, unde fit $k = 5 \cdot 17$ et $h'' = 17$. Quia ergo neque ad 3 neque ad 7 pervenimus, sumto $h' = 5$ examinemus aequationem $5zz - 3xx = 7yy$ atque iam tota operatio est mutanda, dum habemus $f = 5$, $g = -3$ et $h = 7$; quocirca, posito $k = tt - 15$, sumamus $t = 1$, ut fiat $k = -2 \cdot 7$, unde fit $h' = -2$, ita ut nunc aequatio examinanda sit haec $5zz - 3xx = -2yy$ sive $3xx - 2yy = 5zz$, ubi $f = 3$, $g = -2$ et $h = 5$. Sumto ergo $k = tt - 6$, fiat $t = 1$, erit $k = -5$ et $h' = -1$, ergo pervenimus ad hanc aequationem: $3xx - 2yy = -zz$ sive $2yy - zz = 3xx$, ubi habemus $f = 2, g = -1, h = 3$. Erit ergo $k = tt - 2$; quod quum nullo modo fieri possit, omnes istae aequationes ideoque et ipsa proposita sunt impossibiles.

EXEMPLUM 5

57. Sit proposita aequatio $3xx + 7yy = 178zz$, ubi ut antea $f = 3$, $g = 7$, at $h = 178 = 2 \cdot 89$ duplo maior quam casu praecedente[1]). Posito igitur $tt = 89n - 21$ pro n relinquuntur numeri

5, 8, 9, 14, 18, 20, 24, 29, 30, 33, 38, 44 .

Reperitur autem $n = 14$, unde fit $t = 35$, sicque erit $k = 14 \cdot 89$ hincque $h' = 2 \cdot 14 = 4 \cdot 7$ ideoque $h' = 7$, qui numerus, quum ipsi numero g sit aequalis, indicat aequationem nostram esse possibilem.

PROBLEMA 4

58. *Postquam aequatio $fxx + gyy = hzz$ methodo praecedente possibilis fuerit inventa, dum tandem valores ex h inventi perducti fuerint ad f sive ad g, determinare ipsa quadrata xx et yy, quibus aequatio evadit possibilis.*

1) Editio princeps: Posito ergo $k = tt - 21$, ex praecedente patet pro t sumi debere 23. R. F.

SOLUTIO

Quia solutio praecedens ad sequentes formulas est perducta

$$k = aa + fg = hh', \quad k' = bb + fg = h'h'', \quad k'' = cc + fg = h''h''' \text{ etc.},$$

habebimus $hk = h^2h' = h' \cdot \square$, hincque $hk^2 = h'k \cdot \square$. Simili modo reperiemus

$$h' \cdot \square = h''k', \text{ item } h'' \cdot \square = h'''k''; \text{ etc.}$$

Sit nunc $h''' = f$; erit $h'' \cdot \square = fk''$, hinc $h' \cdot \square = fk''k'$ ac tandem $h \cdot \square = fkk'k''$; consequenter habebimus $h \cdot \square$, hoc est

$$hzz = f(aa + fg)(bb + fg)(cc + fg)(dd + fg) \text{ etc.},$$

quod productum manifesto reducitur ad $f(A^2 + fgB^2)$, ita ut hinc fiat $hzz = fA^2 + ffgB^2$, quocirca nanciscimur $x = A$ et $y = fB$, sicque Problema est resolutum.

DE QUIBUSDAM EXIMIIS PROPRIETATIBUS CIRCA DIVISORES POTESTATUM OCCURRENTIBUS

Commentatio 557 indicis Enestroemiani
Opuscula analytica 1, 1783, p. 242—295
[Conventui exhibita die 25. januarii 1773]

1. Constat omnes progressiones geometricas, veluti

$$1,\ a,\ a^2,\ a^3,\ a^4 \text{ etc.},$$

ita esse comparatas, ut, dum singuli termini per numerum quemcunque N, qui ad a sit primus, dividuntur, residua post certum intervallum iterum eodem ordine revertantur[1]); et quia primum residuum est unitas, semper dabitur eiusmodi potestas a^n, quae per N divisa iterum relinquat unitatem; sequentes vero potestates a^{n+1}, a^{n+2}, a^{n+3} etc. eadem residua praebebunt, quae ex terminis a, a^2, a^3 etc. sunt nata. Deinde etiam demonstratum est, si N fuerit numerus primus, tum semper potestatem a^{N-1} iterum pro residuo unitatem exhibere[2]). Saepenumero autem ista potestas a^{N-1} minima est, quae per N divisa unitatem relinquit; interdum vero etiam usu venit, ut minor potestas a^n idem praestet; tum autem semper n est pars aliquota exponentis $N-1$; atque hinc nascitur quaestio attentione nostra non indigna:

Quaenam pro quovis divisore N sit minima potestas a^n, ex qua residuum oriatur $= 1$?

1) Vide imprimis Commentationem 262, *Leonhardi Euleri Opera omnia*, series I, vol. 2, p. 493. Vide etiam praefationem illius voluminis, p. XXX. F. R.

2) De hoc theoremate Fermatiano vide praeter Commentationem 262 modo laudatam etiam Commentationes 54 et 134 illius voluminis I 2, p. 33 et 62, necnon praefationem iam laudatam, p. XIV et XVI. F. R.

Atque hinc quaestio alia latius patens proponi potest:

Quaenam sit infima potestas a^n, quae per datum numerum N divisa datum relinquat residuum r?

Quae quaestio huc redit, ut exhibeatur minima formula $a^x - r$, quae per datum numerum N fuerit divisibilis. Quin etiam quaestio adhuc generalius proponi potest, ut

investigetur exponens x, quo haec formula $fa^x + g$ reddatur divisibilis per datum numerum N.

2. Solutio huius Problematis imprimis requiritur ad numeros perfectos investigandos. Cum enim forma horum numerorum sit $2^{n-1}(2^n - 1)$, quoties $2^n - 1$ fuerit numerus primus, statim evidens est hoc evenire non posse, nisi ipse exponens n fuerit numerus primus; quandoquidem huiusmodi forma $2^{\alpha\beta} - 1$ semper habet divisores $2^\alpha - 1$ et $2^\beta - 1$. Neque vero vicissim sequitur, quoties n fuerit numerus primus, tum etiam formulam $2^n - 1$ fore numerum primum. Plures enim casus iam sunt explorati, quibus hoc non evenit; veluti si fuerit $n = 11$, $n = 23$; item $n = 29$, $n = 37$[1]); ac praeterea sine dubio pluribus aliis casibus, quos omnes nondum explorare licuit. Alia autem via non patet ad hos casus investigandos praeter eam, qua olim sum usus, quae ita se habebat: Fingatur formulae $2^n - 1$ divisor, si quem habet, esse [numerus primus] $2p + 1$; et cum formula $2^{2p} - 1$ semper divisorem habeat $2p + 1$, sequitur hoc fieri non posse, nisi n fuerit pars aliquota ipsius $2p$, sive $2p$ multiplum ipsius n. Sumto ergo $p = \lambda n$, fiet divisor $2\lambda n + 1$; ex quo concluditur, si formula $2^n - 1$ non sit numerus primus, eam alios divisores certe habere non posse, nisi qui in forma $2\lambda n + 1$ contineantur; atque hoc principio olim sum usus in investigatione numerorum primorum. Simili modo cum olim assertionem FERMATII[2]) examinassem, qua asseverarat, formulam $2^n + 1$ semper esse numerum primum, quoties exponens n fuerit ipse potestas binarii, quaestionem supra memoratam in subsidium vocare sum coactus, qua post plures calculos tandem inveni formulam

1) Vide commentationem 26 (indicis ENESTROEMIANI): *Observationes de theoremate quodam* FERMATIANO *aliisque ad numeros primos spectantibus*, Comment. acad. sc. Petrop. 6 (1732/3), 1738, p. 103—107, *LEONHARDI EULERI Opera omnia* series I, vol. 2, p. 1—5, praecipue p. 3. R. F.

2) Vide p. 2 commentationis supra laudatae. R. F.

$2^{32} + 1$ divisorem habere 641; ex quo nunc quaestio formari potest: quaenam sit binarii potestas infima, quae unitate aucta fiat per 641 divisibilis?[1]) Methodus quidem, qua olim sum usus, per calculos satis taediosos procedebat; nunc autem se mihi obtulit alia methodus multo simplicior et expeditior non solum hos memoratos casus circa potestates binarii resolvendi, sed quae adeo ad quaestionem illam generalissimam adplicari possit, qua scilicet quaeritur infima potestas a^x, ut formula $fa^x + g$ per datum numerum N fiat divisibilis. Hanc ergo novam methodum hic breviter sum expositurus; hunc autem in finem sequentia Lemmata sunt praemittenda:

LEMMA 1

3. Si numerus quicunque A per alium N divisus relinquat residuum r, tum etiam omnes hi numeri: $r \mp N$, $r \mp 2N$, $r \mp 3N$ et in genere $r \mp \lambda N$, aeque tanquam residua spectari possunt, quandoquidem hae ipsae formulae per N divisae relinquunt r.

LEMMA 2

4. Si numerus A per divisorem N divisus relinquat residuum a, numerus vero B per eundem divisus residuum b, tum productum AB per N divisum relinquet residuum ab. Hinc ergo potestates A^2, A^3, A^4 etc. dabunt residua a^2, a^3, a^4 etc., quae pro lubitu, divisione per N facta, ad minimos valores reducere licet.

LEMMA 3

5. Si proposito divisore N potestas a^x residuum det $= r$, potestas vero a^ν residuum $= s$, tum potestas $a^{x+\nu}$ residuum dabit $= rs$; unde etiam hae potestates a^{2x}, a^{3x}, a^{4x} etc. residua producent r^2, r^3, r^4 etc.

LEMMA 4

6. Si ut ante pro divisore N potestas a^x praebeat residuum r, potestas vero a^ν residuum s, hinc etiam assignari poterit residuum respondens pote-

1) Loco cit. p. 3. R. F.

stati $a^{x-\nu}$, quod quidem foret $= \frac{r}{s}$, si r per s dividi posset. Quia autem loco r sumere licet $r \mp \lambda N$, semper λ ita definiri poterit, ut haec forma $r \mp \lambda N$ per s dividi queat, ac tum quotus dabit ipsum residuum potestati $a^{x-\nu}$ respondens.

LEMMA 5

7. Si pro divisore N potestas a^x relinquat r, fiatque $r \mp \lambda N = a^\alpha s$, ita ut $a^\alpha s$ tanquam residuum spectari possit, tum potestas $a^{x-\alpha}$ residuum relinquet s, quandoquidem dividendum et residuum semper per communem divisorem deprimere licet.

PROBLEMA GENERALE

8. *Proposita formula $fa^x + g$, invenire minimum exponentem x, quo haec formula per datum numerum N fiat divisibilis, siquidem id fuerit possibile.*

SOLUTIO

Quaestio ergo huc reducitur, ut forma fa^x per numerum datum N divisa relinquat residuum $= -g$. Quia nunc per Lemma primum pro residuo etiam haberi potest $-g \mp \lambda N$, facile λ ita assumere licebit, ut haec formula factorem obtineat a, vel adeo eius altiorem potestatem a^α. Sit igitur $-g \mp \lambda N = a^\alpha r$, atque per Lemma postremum quantitas $fa^{x-\alpha}$ per N divisa residuum relinquet $= r$. Iam simili modo fiat $r \mp \lambda N = a^\beta s$, et quantitas $fa^{x-\alpha-\beta}$ dabit residuum s, sicque ulterius progredi licebit, sumendo $s \mp \lambda N = a^\gamma t$; tum vero etiam $t \mp \lambda N = a^\delta u$; porro $u \mp \lambda N = a^\varepsilon v$ etc.; quo pacto quantitas $a^{x-\alpha-\beta-\gamma-\delta-\varepsilon}$ per N divisa residuum relinquet $= v$; haeque operationes eousque continuentur, donec perveniatur ad residuum $= f$; ita ut haec quantitas $fa^{x-\alpha-\beta-\gamma-\text{etc.}}$ residuum det $= f$; id quod semper continget, siquidem quaestio fuerit possibilis; atque hoc adeo antequam numeri ab exponente subtrahendi $\alpha + \beta + \gamma + \delta + \varepsilon +$ etc. superent numerum $N - 1$, quia si exponentes ipsius a ultra hunc limitem continuentur, eadem residua recurrunt. Cum autem ad talem casum fuerit perventum, quo residuum est f, quia hoc evenit, si exponens ipsius a fuerit $= 0$, hinc concludemus $x = \alpha + \beta + \gamma + \delta +$ etc. Omnes ergo has operationes ita succincte repraesentasse iuvabit:

$$\begin{aligned} -g \mp \lambda N &= a^{\alpha} r \\ r \mp \lambda N &= a^{\beta} s \\ s \mp \lambda N &= a^{\gamma} t \\ t \mp \lambda N &= a^{\delta} u \\ &\cdots\cdots\cdots \\ z \mp \lambda N &= a^{\zeta} f \end{aligned}$$

hincque deducitur conclusio $x = \alpha + \beta + \gamma + \delta + \cdots + \zeta$. Sin autem nunquam perveniatur ad tale residuum f, antequam summa $\alpha + \beta + \gamma + \delta + \cdots$ usque ad $N - 1$ ascendat, Problema pro impossibili est habendum.

Quanquam hae operationes expedite instituuntur, tamen eas saepenumero haud mediocriter contrahere licebit, praecipue si perventum fuerit ad exiguum residuum, puta t, respondens formulae $fa^{x-\delta}$, ponendo $\delta = \alpha + \beta + \gamma$; tum enim eius quadratum t^2 respondebit formulae $f^2 a^{2x-2\delta}$, quae per primam dividatur, ut formula $fa^{x-2\delta}$ respondeat residuo $\frac{t^2}{-g}$, quod si non fuerit numerus integer, loco t^2 scribendo $t^2 \mp \lambda N$ facile eo reducitur. Quin etiam cubus residui t^3 respondebit formulae $f^3 a^{3x-3\delta}$, quae per quadratum primae divisa dabit formulae $fa^{x-3\delta}$ residuum $= \frac{t^3}{g^2}$. Quin etiam binas formulas diversas in se invicem ducere licebit, et per primam dividendo iterum ad novam huiusmodi formulam pervenietur. Imprimis autem hoc compendium maximum usum praestabit, ubi ad residua satis parva fuerit perventum; quorum potestates etiam superiores facile capiuntur, atque insuper fuerit primum residuum $-g$ numerus satis parvus vel adeo unitas.

COROLLARIUM

9. Quoniam has operationes clare descripsimus, eas adplicemus ad casus magis speciales. Ac primo quidem occurrit formula $2^x \mp 1$. Pro variis igitur divisoribus quaeramus exponentem x, ut potestas 2^x residuum relinquat ∓ 1. Sufficiet autem hoc residuum $+1$ statuisse; si enim 2^x fuerit minima potestas residuum dans $= +1$, tum potestas $2^{\frac{1}{2}x}$ necessario dabit residuum $= -1$, siquidem x fuerit numerus par; sin autem x fuerit impar, hic casus plane est impossibilis.

EXEMPLUM 1

10. Quaeratur minima potestas 2^x, quae per 23 divisa relinquat 1, sive ut $2^x - 1$ divisibilis fiat per 23. Hic igitur est $N = 23$, $a = 2$ et primum residuum $= 1$; unde operationes nostrae sequenti modo procedent:

$$\begin{aligned} +1 + 23 &= +24 = +2^3 \cdot 3 \\ +3 - 23 &= -20 = -2^2 \cdot 5 \\ -5 - 23 &= -28 = -2^2 \cdot 7 \\ -7 + 23 &= +16 = +2^4 \cdot 1 . \end{aligned}$$

Sic iam perventum est ad residuum optatum $+1$ ob $f = 1$; sicque concludimus $x = 11$. Cum ergo formula $2^{11} - 1$ sit divisibilis per 23 et 11 numerus impar, nulla plane datur formula $2^x + 1$ per 23 divisibilis.

EXEMPLUM 2

11. Proponatur divisor 41, per quem formula $2^x - 1$ reddi debeat divisibilis. Ergo ob $N = 41$, $a = 2$, $f = 1$ et primum residuum $= 1$, habebimus:

$$\begin{aligned} +1 - 41 &= -40 = -2^3 \cdot 5 \\ -5 + 41 &= +36 = +2^2 \cdot 9 \\ +9 - 41 &= -32 = -2^5 \cdot 1 . \end{aligned}$$

Hic iam subsistere possumus; cum enim potestas 2^{x-10} relinquat -1, eius quadratum 2^{2x-20} relinquet $+1$, et per primam formam dividendo prodit 2^{x-20} pro residuo $+1$ optato; sicque habemus $x = 20$. Simul autem hinc patet potestati 2^{10} residuum convenire -1, ita ut formulae simplicissimae per 41 divisibiles sint $2^{10} + 1$ et $2^{20} - 1$.

EXEMPLUM 3

12. Pro divisore 73 quaeratur formula simplicissima $2^x \mp 1$ per eum divisibilis. Hic est $N = 73$, $a = 2$ et sumto primo residuo $= +1$ fiet

$$\begin{aligned} +1 - 73 &= -72 = -2^3 \cdot 9 \\ -9 + 73 &= +64 = +2^6 \cdot 1 , \end{aligned}$$

ubi ergo iam subsistere licet, eritque $x = 9$, unde formula $2^9 - 1$ per 73 est divisibilis; et quia 9 est numerus impar, nulla plane datur formula $2^x + 1$ per eundem numerum N divisibilis.

EXEMPLUM 4

13. Proponatur divisor $N = 77$, et sumto primo residuo $= 1$, calculus ita se habebit:

$$\begin{aligned}
+ 1 - 77 &= - 76 = -2^2 \cdot 19 \\
-19 - 77 &= - 96 = -2^5 \cdot 3 \\
- 3 - 77 &= - 80 = -2^4 \cdot 5 \\
- 5 + 77 &= + 72 = +2^3 \cdot 9 \\
+ 9 - 77 &= - 68 = -2^2 \cdot 17 \\
-17 + 77 &= + 60 = +2^2 \cdot 15 \\
+15 + 77 &= + 92 = +2^2 \cdot 23 \\
+23 + 77 &= +100 = +2^2 \cdot 25 \\
+25 - 77 &= - 52 = -2^2 \cdot 13 \\
-13 + 77 &= + 64 = +2^6 \cdot 1,
\end{aligned}$$

unde $x = 30$; ita ut $2^{30} - 1$ sit simplicissima forma per 77 divisibilis. Hinc tamen non sequitur istam $2^{15} + 1$ divisibilem esse per 77, propterea quod 77 non est numerus primus; etsi enim $2^{30} - 1$ divisibile est per 77, neutiquam sequitur alterutrum eius factorum $2^{15} + 1$ sive $2^{15} - 1$ divisibilem esse debere, quemadmodum rite concludere liceret, si divisor esset numerus primus; hoc enim casu fieri potest, ut alter factor per 7, alter vero per 11 sit divisibilis; ac revera, cum $2^5 + 1$ per 11 sit divisibile, etiam $2^{15} + 1$ per 11 erit divisibile; at vero per 7 divisibilis est altera formula $2^{15} - 1$, quia factorem habet $2^3 - 1 = 7$.

EXEMPLUM 5

14. Sit divisor $N = 89$, et sumto iterum primo residuo $= 1$, faciemus:

$$\begin{aligned}
+ 1 - 89 &= - 88 = -2^3 \cdot 11 \\
-11 - 89 &= -100 = -2^2 \cdot 25 \\
-25 + 89 &= + 64 = +2^6 \cdot 1.
\end{aligned}$$

Hinc ergo $x = 11$, sicque formula $2^{11} - 1$ divisorem habet 89; nulla autem datur formula alterius speciei $2^{11} + 1$.

EXEMPLUM 6

15. Sit divisor $N = 105$, eritque:

$$\begin{aligned} +\ 1 - 105 &= -\ 104 = -\ 2^3 \cdot 13 \\ -\ 13 + 105 &= +\ 92 = +\ 2^2 \cdot 23 \\ +\ 23 + 105 &= +\ 128 = +\ 2^7 \cdot 1\,. \end{aligned}$$

Summa exponentium $= 12$; ergo $x = 12$, et formula $2^{12} - 1$ divisibilis erit per 105. At quia 105 non est numerus primus, non sequitur fore $2^6 + 1$ per 105 divisibile. Tantum enim dividi potest per 5, dum altera formula $2^6 - 1$ divisibilis est per $3 \cdot 7$.

EXEMPLUM 7

16. Sit $N = 223$ et primum residuum $= 1$, fiet:

			Summae exponentium
$+\ 1 + 223$	$= +\ 224$	$= +\ 2^5 \cdot 7$	5
$+\ 7 - 223$	$= -\ 216$	$= -\ 2^3 \cdot 27$	8
$-\ 27 + 223$	$= +\ 196$	$= +\ 2^2 \cdot 49$	10
$+\ 49 + 223$	$= +\ 272$	$= +\ 2^4 \cdot 17$	14
$+\ 17 + 223$	$= +\ 240$	$= +\ 2^4 \cdot 15$	18
$+\ 15 - 223$	$= -\ 208$	$= -\ 2^4 \cdot 13$	22
$-\ 13 - 223$	$= -\ 236$	$= -\ 2^2 \cdot 59$	24
$-\ 59 + 223$	$= +\ 164$	$= +\ 2^2 \cdot 41$	26
$+\ 41 + 223$	$= +\ 264$	$= +\ 2^3 \cdot 33$	29
$+\ 33 + 223$	$= +\ 256$	$= +\ 2^8 \cdot 1$	37

Summa exponentium $= 37$, ergo $x = 37$, et formula $2^{37} - 1$ divisibilis per 223. Hinc quia 37[1]) est numerus impar, certum est nullam dari formulam $2^x + 1$ per 223 divisibilem.

17. Quo nunc pateat, quomodo hae operationes possint sublevari, subsistamus iam in quinta, ubi residuum prodiit 15 et summa exponentium $= 18$; unde haec potestas 2^{x-18} residuum dat 15. Sumantur quadrata, et potestas 2^{2x-36} residuum dat 225 sive 2; haec iam per primam divisa praebet pro potestate 2^{x-36} residuum $2 = 2^1 \cdot 1$, ergo potestas 2^{x-37} praebet residuum 1, unde iam liquet esse $x = 37$.

1) Editio princeps: 23. Correxit R. F.

EXEMPLUM 8

18. Sit $N = 641$ et primum residuum $= 1$, fiet:

			Summae exponentium
$+ 1 - 641$	$= -640$	$= -2^7 \cdot 5$	7
$- 5 + 641$	$= +636$	$= +2^2 \cdot 159$	9
$+ 159 + 641$	$= +800$	$= +2^5 \cdot 25$	14
$+ 25 - 641$	$= -616$	$= -2^3 \cdot 77$ [1])	17
$- 77 + 641$	$= +564$	$= +2^2 \cdot 141$	19
$+ 141 - 641$	$= -500$	$= -2^2 \cdot 125$	21
$- 125 + 641$	$= +516$	$= +2^2 \cdot 129$	23
$+ 129 - 641$	$= -512$	$= -2^9 \cdot 1$	32

ubi iam subsistere possumus. Quia enim residuum est -1, si pro primo residuo sumsissemus -1, ut formula quaereretur $2^x + 1$ per 641 divisibilis, omnia sequentia residua signo contrario adfecta prodiissent et ultimum fuisset $+1$; unde rite concludimus esse $x = 32$, ita ut iam formula $2^{32} + 1$ sit divisibilis per 641. Evidens autem est pro minima formula huius formae $2^x - 1$ fore $x = 64$.

19. Hunc autem laborem mirifice contrahere licet. Statim enim post primam operationem subsistere possemus, quae pro potestate 2^{x-7} praebet residuum -5 [2]). Sumamus statim potestatem quartam, et pro 2^{4x-28} habebimus residuum 625, sive $-16 = -2^4 \cdot 1$, ita ut 2^{4x-32} [3]) conveniat residuum -1. Dividendo igitur per cubum primae, seu 2^{3x}, cuius residuum itidem est 1, etiam huius potestatis 2^{x-32} residuum erit -1, id quod ante per ambages eruimus.

EXEMPLUM 9

20. Sit $N = 385 = 5 \cdot 7 \cdot 11$ et primum residuum $= 1$, erit:

			[Summae exponentium]
$+ 1 - 385$	$= -384$	$= -2^7 \cdot 3$	7
$- 3 - 385$	$= -388$	$= -2^2 \cdot 97$	9
$- 97 + 385$	$= +288$	$= +2^5 \cdot 9$	14
$+ 9 - 385$	$= -376$	$= -2^3 \cdot 47$	17
$- 47 - 385$	$= -432$	$= -2^4 \cdot 27$	21

1) Editio princeps: $-3^3 \cdot 77$. Correxit R. F.
2) Editio princeps: 5. Correxit R. F.
3) Editio princeps: 2^{x-32}. Correxit R. F.

			[Summae exponentium]
$-27-385$	$=-412$	$=-2^2\cdot 103$	23
$-103-385$	$=-488$	$=-2^3\cdot 61$	26
$-61+385$	$=+324$	$=+2^2\cdot 81$[1])	28
$+81-385$	$=-304$	$=-2^4\cdot 19$	32
$-19-385$	$=-404$	$=-2^2\cdot 101$	34
$-101+385$	$=+284$	$=+2^2\cdot 71$	36
$+71+385$	$=+456$	$=+2^3\cdot 57$	39
$+57-385$	$=-328$	$=-2^3\cdot 41$	42
$-41+385$	$=+344$	$=+2^3\cdot 43$	45
$+43+385$	$=+428$	$=+2^2\cdot 107$	47
$+107+385$	$=+492$	$=+2^2\cdot 123$	49
$+123+385$	$=+508$	$=+2^2\cdot 127$	51
$+127+385$	$=+512$	$=+2^9\cdot 1$	60

ergo $x = 60$, ita ut formula $2^{60} - 1$ divisibilis sit per 385, quod etiam inde concludi potuisset, quod divisoris nostri factores sunt 5, 7, 11, quorum primus 5 est divisor formulae $2^2 + 1$, secundus 7 est formulae $2^3 - 1$, tertius 11 est formulae $2^5 + 1$; at formula per has tres divisibilis simplicior non datur quam $2^{60} - 1$.

21. Videamus nunc, quomodo hae operationes contrahi potuissent. Tertia operatione prodiit potestas 2^{x-14} residuum dans 9; unde eius quadratum 2^{2x-28} residuum praebet 81; cubus autem 2^{3x-42} praebet residuum 729, sive 344, sive -41; hinc quarta potestas 2^{4x-56} dabit residuum -369, sive $+16 = 2^4\cdot 1$, ergo per 2^4 dividendo potestas 2^{4x-60} dat residuum $+1$ et dividendo per 2^{3x}, cuius residuum etiam est $+1$, potestas 2^{x-60} residuum dabit $+1$, uti modo invenimus.

EXEMPLUM 10

22. Sit $N = 311$, fietque:

			[Summae exponentium]
$+1+311$	$=+312$	$=+2^3\cdot 39$	3
$+39-311$	$=-272$	$=-2^4\cdot 17$	7
$-17-311$	$=-328$	$=-2^3\cdot 41$	10
$-41-311$	$=-352$	$=-2^5\cdot 11$	15
$-11+311$	$=+300$	$=+2^2\cdot 75$	17
$+75-311$	$=-236$	$=-2^2\cdot 59$	19

1) Editio princeps: $9^2\cdot 81$. Correxit R. F.

			[Summae exponentium]
$-59+311$	$=+252$	$=+2^2\cdot 63$	21
$+63-311$	$=-248$	$=-2^3\cdot 31$	24
$-31+311$	$=+280$	$=+2^3\cdot 35$	27
$+35-311$	$=-276$	$=-2^2\cdot 69$	29
$-69-311$	$=-380$	$=-2^2\cdot 95$	31
$-95+311$	$=+216$	$=+2^3\cdot 27$	34
$+27-311$	$=-284$	$=-2^2\cdot 71$	36
$-71+311$	$=+240$	$=+2^4\cdot 15$	40
$+15-311$	$=-296$	$=-2^3\cdot 37$	43
$-37-311$	$=-348$	$=-2^2\cdot 87$	45
$-87+311$	$=+224$	$=+2^5\cdot 7$	50
$+7-311$	$=-304$	$=-2^4\cdot 19$	54
$-19+311$	$=+292$	$=+2^2\cdot 73$	56
$+73+311$	$=+384$	$=+2^7\cdot 3$	63
$+3-311$	$=-308$	$=-2^2\cdot 77$	65
$-77-311$	$=-388$	$=-2^2\cdot 97$	67
$-97-311$	$=-408$	$=-2^3\cdot 51$	70
$-51+311$	$=+260$	$=+2^2\cdot 65$	72
$+65+311$	$=+376$	$=+2^3\cdot 47$	75
$+47-311$	$=-264$	$=-2^3\cdot 33$	78
$-33-311$	$=-344$	$=-2^3\cdot 43$	81
$-43+311$	$=+268$	$=+2^2\cdot 67$	83
$+67-311$	$=-244$	$=-2^2\cdot 61$	85
$-61-311$	$=-372$	$=-2^2\cdot 93$	87
$-93-311$	$=-404$	$=-2^2\cdot 101$	89
$-101-311$	$=-412$	$=-2^2\cdot 103$	91
$-103+311$	$=+208$	$=+2^4\cdot 13$	95
$+13+311$	$=+324$	$=+2^2\cdot 81$	97
$+81+311$	$=+392$	$=+2^3\cdot 49$	100
$+49+311$	$=+360$	$=+2^3\cdot 45$	103
$+45+311$	$=+356$	$=-2^2\cdot 89$[1])	105
$+89+311$	$=+400$	$=+2^4\cdot 25$	109
$+25+311$	$=+336$	$=+2^4\cdot 21$	113
$+21+311$	$=+332$	$=+2^2\cdot 83$	115

1) In editione principe operationes 37mae usque ad 43ias signis falsis affectae sunt.
Correxit R. F.

			[Summae exponentium]
$+ 83 - 311$	$= -228$	$= -2^2 \cdot 57$	117
$- 57 - 311$	$= -368$	$= -2^4 \cdot 23$	121
$- 23 + 311$	$= +288$	$= +2^5 \cdot 9$	126
$+ 9 + 311$	$= +320$	$= +2^6 \cdot 5$	132
$+ 5 + 311$	$= +316$	$= +2^2 \cdot 79$	134
$+ 79 - 311$	$= -232$	$= -2^3 \cdot 29$	137
$- 29 - 311$	$= -340$	$= -2^2 \cdot 85$	139
$- 85 - 311$	$= -396$	$= -2^2 \cdot 99$	141
$- 99 + 311$	$= +212$	$= +2^2 \cdot 53$	143
$+ 53 + 311$	$= +364$	$= +2^2 \cdot 91$	145
$+ 91 - 311$	$= -220$	$= -2^2 \cdot 55$	147
$- 55 + 311$	$= +256$	$= +2^8 \cdot 1$	155

ergo $x = 155$, sicque minima formula per 311 divisibilis est $2^{155} - 1$.

Si substitissemus in 25^ta^ operatione, habuissemus 2^{x-75}, eiusque residuum 47; et sumtis quadratis 2^{2x-150}, sive per principalem dividendo, 2^{x-150} cum residuo 2209, sive $32 = 2^5 \cdot 1$; unde potestas 2^{x-155} residuum optatum producit $+1$. Sin autem in operatione 17^ma^ substitissemus, habuissemus 2^{x-50} cum residuo 7, sumtisque cubis 2^{3x-150} cum residuo 343, sive $32 = 2^5 \cdot 1$; ita ut iam potestas 2^{3x-155}, sive etiam 2^{x-155} residuum det $+1$; unde sequitur $x = 155$, ut ante.

EXEMPLUM 11

23. Sit divisor $N = 233$, et sumto primo residuo $= 1$, faciemus:

			Summae exponentium
$+ 1 - 233$	$= -232$	$= -2^3 \cdot 29$	3
$- 29 + 233$	$= +204$	$= +2^2 \cdot 51$ [1])	5
$+ 51 + 233$	$= +284$	$= +2^2 \cdot 71$	7
$+ 71 + 233$	$= +304$	$= +2^4 \cdot 19$	11
$+ 19 + 233$	$= +252$	$= +2^2 \cdot 63$	13
$+ 63 + 233$	$= +296$	$= +2^3 \cdot 37$	16
$+ 37 - 233$	$= -196$	$= -2^2 \cdot 49$	18
$- 49 + 233$	$= +184$	$= +2^3 \cdot 23$	21
$+ 23 + 233$	$= +256$	$= +2^8 \cdot 1$	29

[ergo $x = 29$, sicque minima formula per 233 divisibilis est $2^{29} - 1$].

1) Editio princeps: $+ 2^3 \cdot 51$. Correxit R. F.

SCHOLION

24. Hac igitur methodo pro quolibet divisore N facile computatur formula simplicissima $2^x \pm 1$ per eum divisibilis. Haud igitur abs re visum est tabulam hic adiungere, in qua pro omnibus numeris primis usque ad 400 simplicissimae formulae exhibentur; divisores autem primos commode in quatuor ordines, secundum formas $8n+1$, $8n-1$, $8n+3$ et $8n-3$ distribui conveniet:

N $8n+1$	$2^x \pm 1$	N $8n-1$	$2^x \pm 1$
1	$2^0 - 1$	7	$2^3 - 1$
17	$2^4 + 1$	23	$2^{11} - 1$
41	$2^{10} + 1$	31	$2^5 - 1$
73	$2^9 - 1$	47	$2^{23} - 1$
89	$2^{11} - 1$	71	$2^{35} - 1$
97	$2^{24} + 1$	79	$2^{39} - 1$
113	$2^{14} + 1$	103	$2^{51} - 1$
137	$2^{34} + 1$	127	$2^7 - 1$
193	$2^{48} + 1$	151	$2^{15} - 1$
233	$2^{29} - 1$ [1])	167	$2^{83} - 1$
241	$2^{12} + 1$	191	$2^{95} - 1$
257	$2^8 + 1$	199	$2^{99} - 1$
281	$2^{35} + 1$	223	$2^{37} - 1$
313	$2^{78} + 1$	239	$2^{119} - 1$
337	$2^{21} - 1$	263	$2^{131} - 1$
353	$2^{44} + 1$	271	$2^{135} - 1$
401	$2^{100} + 1$	311	$2^{155} - 1$
		359	$2^{179} - 1$
		367	$2^{183} - 1$
		383	$2^{191} - 1$
		431	$2^{215} - 1$

1) Editio princeps: $2^{29} + 1$. Correxit R. F.

N $8n+3$	2^x+1	N $8n-3$	2^x+1
3	2^1+1	5	2^2+1
11	2^5+1	13	2^6+1
19	2^9+1	29	$2^{14}+1$
43	2^7+1	37	$2^{18}+1$
59	$2^{29}+1$	53	$2^{26}+1$
67	$2^{33}+1$	61	$2^{30}+1$
83	$2^{41}+1$	101	$2^{50}+1$
107	$2^{53}+1$	109	$2^{18}+1$
131	$2^{65}+1$	149	$2^{74}+1$
139	$2^{69}+1$	157	$2^{26}+1$
163	$2^{81}+1$	173	$2^{86}+1$
179	$2^{89}+1$	181	$2^{90}+1$
211	$2^{105}+1$	197	$2^{98}+1$
227	$2^{113}+1$	229	$2^{38}+1$
251	$2^{25}+1$	269	$2^{134}+1$
283	$2^{47}+1$	277	$2^{46}+1$
307	$2^{51}+1$	293	$2^{146}+1$
331	$2^{15}+1$	317	$2^{158}+1$
347	$2^{173}+1$	349	$2^{174}+1$
371	$2^{185}+1$	373	$2^{186}+1$
379	$2^{189}+1$	389	$2^{194}+1$
		397	$2^{22}+1$

Hos casus probe perpendentes stabilire poterimus sequens Theorema, quod eo magis notatu dignum videtur, quod firma demonstratione etiamnum indiget.

THEOREMA [1]

25. *Si numerus primus* $2p+1$ *fuerit formae* $8n \mp 1$, *per eum semper divisibilis erit formula* $2^p - 1$; *sin autem habeat hanc formam:* $8n \mp 3$, *per eum divisibilis erit formula* $2^p + 1$[1]).

1) Confer commentationem 449 (indicis Enestroemiani): *Demonstrationes circa residua ex divisione potestatum per numeros primos resultantia*, Novi comment. acad. sc. Petrop. 18 (1773), 1774, p. 85—135, § 86, *Leonhardi Euleri Opera omnia*, series I, vol. 3, p. 275 et notam [1]) p. 276. R. F.

Cum enim formula $2^{2p} - 1$ semper divisibilis sit per numerum primum $2p + 1$, necesse est, ut alterutra harum formularum: $2^p - 1$ vel $2^p + 1$ per eundem dividi queat; quod cum aeque valeat de omnibus aliis potestatibus $a^{2p} - 1$, dummodo a ad $2p + 1$ fuerit primus, prouti pro a alios atque alios valores assumamus, sequentia Theoremata vera deprehenduntur:

THEOREMA 2

26. *Si numerus primus* $2p + 1$ *fuerit formae* $12n \mp 1$, *per eum semper divisibilis erit formula* $3^p - 1$. *Sin autem habeat formam* $12n \mp 5$, *per eum divisibilis erit formula* $3^p + 1$.

THEOREMA 3

27. *Sumto* $a = 5$, *si* $2p + 1$ *fuerit numerus primus, utrum per eum divisibilis sit sive formula* $5^p - 1$ *sive* $5^p + 1$, *sequens tabella declarat:*

Si fuerit $2p + 1$	divisibilis erit
$20n \mp 1$	$5^p - 1$
$20n \mp 3$	$5^p + 1$
$20n \mp 7$	$5^p + 1$
$20n \mp 9$	$5^p - 1$

THEOREMA 4

28. *Sumto* $a = 6$, *si fuerit* $2p + 1$ *numerus primus, utrum per eum divisibilis sit sive formula* $6^p - 1$, *sive* $6^p + 1$, *sequens tabella declarat:*

Si fuerit $2p + 1$	divisibilis erit
$24n \pm 1$	$6^p - 1$
$24n \pm 5$	$6^p - 1$
$24n \pm 7$	$6^p + 1$
$24n \pm 11$	$6^p + 1$

THEOREMA 5

29. *Sumto* $a = 7$, *si fuerit* $2p + 1$ *numerus primus, utrum per eum divisibilis sit sive formula* $7^p - 1$ *sive formula* $7^p + 1$, *ex sequenti tabella patet:*

Si fuerit $2p + 1$	divisibilis erit
$28n \pm 1$	$7^p - 1$
$28n \pm 3$	$7^p - 1$
$28n \pm 5$	$7^p + 1$
$28n \pm 9$	$7^p - 1$
$28n \pm 11$	$7^p + 1$
$28n \pm 13$	$7^p + 1$

THEOREMA 6

30. *Sumto* $a = 8$, *si fuerit* $2p + 1$ *numerus primus, utrum per eum divisibilis sit sive formula* $8^p - 1$, *sive* $8^p + 1$, *sequens tabella ostendit:*

Si fuerit $2p + 1$	divisibilis erit
$32n \pm 1$	$8^p - 1$
$32n \pm 3$	$8^p + 1$
$32n \pm 5$	$8^p + 1$
$32n \pm 7$	$8^p - 1$
$32n \pm 9$	$8^p - 1$
$32n \pm 11$	$8^p + 1$
$32n \pm 13$	$8^p + 1$
$32n \pm 15$	$8^p - 1$

THEOREMA 7

31. *Sumto* $a = 10$, *si fuerit* $2p + 1$ *numerus primus, utrum per eum divisibilis sit sive formula* $10^p - 1$ *sive* $10^p + 1$, *ex sequenti tabella perspicitur:*

Si fuerit $2p+1$	divisibilis erit
$40n \pm 1$	$10^p - 1$
$40n \pm 3$	$10^p - 1$
$40n \pm 7$	$10^p + 1$
$40n \pm 9$	$10^p - 1$
$40n \pm 11$	$10^p + 1$
$40n \pm 13$	$10^p - 1$
$40n \pm 17$	$10^p + 1$
$40n \pm 19$	$10^p + 1$

THEOREMA GENERALE

32. *Quicunque fuerit numerus a, si $2p+1$ denotet numerum primum et casu $p = f$ innotuerit, utrum formula $a^f - 1$, an $a^f + 1$ divisibilis sit per $2f+1$, tum generatim eiusdem generis formula sive $a^p - 1$ sive $a^p + 1$ divisibilis erit per $2p+1$, si fuerit $2p+1 = 4an \mp (2f+1)$, quicunque numerus pro n accipiatur, dummodo inde prodeat $2p+1$ numerus primus.*

COROLLARIUM 1

33. Ex praecedentibus Theorematibus satis liquet, casu $f = 0$ semper formulam $a^p - 1$ divisibilem fore per $2p+1 = 4an \mp 1$, quoties scilicet hic numerus fuerit primus.

COROLLARIUM 2

34. Sin autem sit $f = 1$, prouti sive $a - 1$, sive $a + 1$ per 3 dividi potest, simili casu generatim sive formula [$a^p - 1$ sive formula] $a^p + 1$ per numerum primum $2p+1$ erit divisibilis, quoties $2p+1$ in hac forma: $4an \pm 3$ continetur.

SCHOLION

35. Theoremata autem particularia allata facile ulterius continuari possunt, si sequens Problema in subsidium vocetur, cuius quidem solutio firmissimis rationibus innititur.

PROBLEMA

36. *Quicunque fuerit numerus a, si $2p + 1$ denotet numerum primum, quovis casu oblato investigare, utrum formula $a^p - 1$ an altera $a^p + 1$ divisibilis sit per $2p + 1$.*

SOLUTIO

Quaerantur omnia residua, quae ex divisione quadratorum per numerum $2p + 1$ resultant, quae sint $1, \alpha, \beta, \gamma, \delta$ etc. multitudine $= p$, numeri autem ab his diversi non residua adpellentur[1]). Quo facto si numerus a inter residua reperiatur, tum semper formula $a^p - 1$ erit divisibilis; sin autem numerus a inter non-residua occurrat, tum altera formula $a^p + 1$ divisibilis erit.

Haec autem regula ita demonstratur: Si fuerit a residuum ex cuiusdam quadrati x^2 divisione per $2p + 1$ natum, tum erit $x^2 - a$ per $2p + 1$ divisibile; sive aequabitur cuipiam multiplo $m(2p + 1)$, ita ut sit $a = x^2 - m(2p + 1)$. Hinc ergo fiet $a^p = (x^2 - m(2p + 1))^p$, quae potestas per $2p + 1$ divisa idem residuum relinquet ac potestas $(x^2)^p$; verum haec potestas abit in x^{2p}, quae per $2p + 1$ divisa certe unitatem relinquit. Ex quo sequitur etiam potestatem a^p unitatem relinquere, sive formulam $a^p - 1$ esse divisibilem.

COROLLARIUM

37. Cum residua $1, \alpha, \beta, \gamma, \delta$ etc. minora esse soleant quam divisor $2p+1$, iis adhuc annumerari licet $1 + (2p + 1)$, $\alpha + (2p + 1)$, $\beta + (2p + 1)$ etc., quod observandum est, si numerus a maior fuerit divisore $2p + 1$.

SCHOLION

38. Cum igitur in hoc negotio maximi sit momenti tam residua quam non-residua nosse, pro divisoribus primis minoribus sequentem tabulam hic adiiciamus; superfluum autem foret, non-residua adposuisse.

---

1) 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—58. *Leonhardi Euleri Opera omnia,* series I, vol. 2, p. 338—372, praecipue p. 343. R. F.

Divisor	Residua
3	1, 4, 7, 10, 13, 16, 19, 22, 25 etc.
5	1, 4, 6, 9, 11, 14, 16, 19, 21, 24 etc.
7	1, 2, 4, 8, 9, 11, 15, 16, 18, 22 etc.
11	1, 3, 4, 5, 9, 12, 14, 15, 16, 20, 23 etc.
13	1, 3, 4, 9, 10, 12, 14, 16, 17, 22, 23, 25, 27 etc.
17	1, 2, 4, 8, 9, 13, 15, 16, 18, 19, 21, 25, 26, 30 etc.
19	1, 4, 5, 6, 7, 9, 11, 16, 17, 20, 23, 24, 25, 26 etc.
23	1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18, 24, 25, 26, 27 etc.
29	1, 4, 5, 6, 7, 9, 13, 16, 20, 22, 23, 24, 25, 28 etc.
31	1, 2, 4, 5, 7, 8, 9, 10, 14, 16, 18, 19, 20, 25, 28 etc.
37	1, 3, 4, 7, 9, 10, 11, 12, 16, 21, 25, 26, 27, 28, 30, 33, 34, 36 etc.
	etc.

Ope huius tabulae sequentia Theoremata particularia facillime derivabimus.

THEOREMA 8

39. *Sumto* $a = 11$, *si fuerit* $2p + 1$ *numerus primus, utrum per eum divisibilis sit formula* $11^p - 1$, *sive* $11^p + 1$, *sequens tabella ostendit:*

Si fuerit $2p + 1$	divisibilis erit
$44n \pm 1$	$11^p - 1$
$44n \pm 3$	$11^p + 1$
$44n \pm 5$	$11^p - 1$
$44n \pm 7$	$11^p - 1$
$44n \pm 9$	$11^p - 1$
$44n \pm 13$	$11^p + 1$
$44n \pm 15$	$11^p + 1$
$44n \pm 17$	$11^p + 1$
$44n \pm 19$	$11^p - 1$
$44n \pm 21$	$11^p + 1$

THEOREMA 9

40. *Sumto* $a = 12$, *si fuerit* $2p + 1$ *numerus primus, utrum per eum divisibilis sit sive forma* $12^p + 1$ *sive* $12^p - 1$, *ex sequenti tabella patet:*

Si fuerit $2p + 1$	divisibilis erit
$48n \pm 1$	$12^p - 1$
$48n \pm 5$	$12^p + 1$
$48n \pm 7$	$12^p + 1$
$48n \pm 11$	$12^p - 1$
$48n \pm 13$	$12^p - 1$
$48n \pm 17$	$12^p + 1$
$48n \pm 19$	$12^p + 1$
$48n \pm 23$	$12^p - 1$

THEOREMA 10

41. *Sumto a successive* $= 13, 14, 15$, *si fuerit* $2p + 1$ *numerus primus, utrum per eum divisibilis sit sive forma* $a^p + 1$ *sive* $a^p - 1$, *ex sequentibus tabellis patet:*

$a = 13$		$a = 14$		$a = 15$	
$2p + 1$		$2p + 1$		$2p + 1$	
$52n \pm 1$	$13^p - 1$	$56n \pm 1$	$14^p - 1$	$60n \pm 1$	$15^p - 1$
$52n \pm 3$	$13^p - 1$	$56n \pm 3$	$14^p + 1$	$60n \pm 7$	$15^p - 1$
$52n \pm 5$	$13^p + 1$	$56n \pm 5$	$14^p - 1$	$60n \pm 11$	$15^p - 1$
$52n \pm 7$	$13^p + 1$	$56n \pm 9$	$14^p - 1$	$60n \pm 13$	$15^p + 1$
$52n \pm 9$	$13^p - 1$	$56n \pm 11$	$14^p - 1$	$60n \pm 17$	$15^p - 1$
$52n \pm 11$	$13^p + 1$	$56n \pm 13$	$14^p - 1$	$60n \pm 19$	$15^p + 1$
$52n \pm 15$	$13^p + 1$	$56n \pm 15$	$14^p + 1$	$60n \pm 23$	$15^p + 1$
$52n \pm 17$	$13^p - 1$	$56n \pm 17$	$14^p + 1$	$60n \pm 29$	$15^p + 1$
$52n \pm 19$	$13^p + 1$	$56n \pm 19$	$14^p + 1$		
$52n \pm 21$	$13^p + 1$	$56n \pm 23$	$14^p + 1$		
$52n \pm 23$	$13^p - 1$	$56n \pm 25$	$14^p - 1$		
$52n \pm 25$	$13^p - 1$	$56n \pm 27$	$14^p + 1$		

ADDITAMENTUM

Quae hactenus sunt tradita, plerumque adhuc firmis demonstrationibus destituuntur; omnia autem dubia maximam partem diluentur sequentibus propositionibus, quibus simul omnia ad multo maiorem evidentiae gradum evehentur.

THEOREMA 1

1. *Si formula* $4p + (2q + 1)^2$ *fuerit numerus primus, per eumque omnia quadrata dividantur, inter residua occurret tam* $+ p$ *quam* $- p$.

DEMONSTRATIO

In his residuis primo occurrunt omnia quadrata, quatenus sunt ipso divisore, quem littera D designemus, minora; praeterea vero ex quadratis maioribus, veluti Q^2, nascuntur residua $Q^2 - D$ vel $Q^2 - \lambda D$. Quin etiam notum est ad residua referri posse omnes formulas $Q^2 \mp \lambda D$. Capiatur igitur $Q^2 = (2q + 1)^2$, et ob $D = 4p + (2q + 1)^2$ residuum prodit $-4p$; ergo etiam inter residua erit $-p$, quia generatim, si inter residua fuerit $\alpha^2 \beta$, tum ibidem quoque semper β reperitur. Porro quoniam hic divisor $4p + (2q + 1)^2$ in forma $4n + 1$ continetur, iam demonstratum est[1]) singula residua utroque signo $+$ et $-$ adfecta reperiri; unde manifestum est nostro casu tam $+ p$ quam $- p$ inter residua reperiri debere.

COROLLARIUM 1

2. Quia tam $+ p$ quam $- p$ est residuum, dabuntur formulae tam $xx + pyy$ quam $xx - pyy$ per propositum divisorem D divisibiles.

1) Vide commentationem p. 42 laudatam (imprimis p. 356 et sequentes). R. F.

COROLLARIUM 2

3. Cum autem hae formae: $xx + pyy$ et $xx - pyy$ alios non admittant divisores, nisi qui in certis formulis contineantur, necesse est, ut etiam numerus [primus] sub iisdem formulis comprehendatur.

COROLLARIUM 3

4. Quia, posito divisore $= 2m + 1$, numerus omnium residuorum tantum est $= m$, dum reliqui numeri omnes ad non-residua sint referendi, hinc sequitur etiam formulam $p^m - 1$ divisibilem fore per $2m + 1$, dummodo $2m + 1$ fuerit numerus primus. Quia enim omnes potestates ipsius p quoque sunt residua, horumque numerus tantum est m, necesse est, ut potestas p^m iterum ad unitatem, seu p^0 reducatur, hincque $p^m - 1$ dividi poterit per divisorem $2m + 1$.

THEOREMA 2

5. *Si formula* $4p - (2q + 1)^2$ *fuerit numerus primus, per eumque omnia quadrata dividantur, in residuis semper occurret numerus* p*; at eius negativum* $-p$*, sive quod eodem redit* $D - p$*, denotante* D *divisorem, ad non-residua refertur.*

DEMONSTRATIO

Praeter ipsa quadrata, divisore minora, etiam inter residua occurret quadratum $(2q + 1)^2$, divisore auctum, ideoque $4p$; ergo etiam, ob rationem ante allegatam, occurret numerus p. Et quia hic divisor $4p - (2q + 1)^2$ est numerus formae $4n - 1$, ubi nullum residuum utroque signo $+$ et $-$ adfectum occurrit, sequitur $-p$ inter non-residua reperiri debere[1]).

COROLLARIUM 1

6. Quia ergo p certe est residuum, dabitur formula $xx - pyy$ per nostrum divisorem divisibilis, unde etiam divisor eiusmodi formam habebit, qualem divisores formulae $xx - pyy$ postulant.

---

1) Vide notam p. 45. R. F.

COROLLARIUM 2

7. At quia $-p$ est non-residuum, nulla dabitur formula $xx + pyy$ per nostrum divisorem divisibilis, unde etiam divisor e formula generali, quae omnes divisores ipsius $xx + pyy$ complectitur, excluditur.

COROLLARIUM 3

8. Ob rationem ante allegatam, si divisor vocetur $2m + 1$, formula $p^m - 1$ per eum divisibilis esse debet; neque vero haec formula $(-p)^m - 1$ erit divisibilis, id quod etiam per se est perspicuum. Cum enim divisor noster formam habeat $4n - 1$, fiet $m = 2n - 1$, ideoque numerus impar, et $(-p)^m = -p^m$; quare cum $p^m - 1$ sit divisibile, certe haec formula $-p^m - 1$ sive $p^m + 1$ non erit divisibilis.

THEOREMA 3

9. *Si* $4n + 1$ *fuerit numerus primus, per eumque omnia quadrata dividantur, inter residua omnes occurrent numeri sive in hac forma generali:* $n - qq - q$ *sive in hac:* $qq + q - n$ *contenti.*

DEMONSTRATIO

Manifestum est divisorem nostrum $4n + 1$ infinitis modis ad formam $4p + (2q + 1)^2$ reduci posse. Posito enim $4n + 1 = 4p + (2q + 1)^2$ fiet $n = p + q^2 + q$, ideoque $p = n - q^2 - q$; unde sequitur, quicunque numerus pro q accipiatur, numerum $n - qq - q$ inter residua reperiri; deinde quia etiam $-p$ est residuum (§ 1), manifestum est etiam omnes numeros in hac forma $qq + q - n$ fore residua.

COROLLARIUM 1

10. Hoc ergo modo, dum pro q successive accipiuntur omnes numeri 0, 1, 2, 3, 4, 5 etc. infiniti, prodibunt numeri ad residua referendi, qui tamen omnes ad multitudinem $2n$ se reduci patientur, quandoquidem plura residua diversa non dantur quam $2n$.

COROLLARIUM 2

11. Necesse igitur est, ut omnes numeri, sive in forma $n - qq - q$ sive in forma $qq + q - n$ contenti, omnia plane praebeant residua, divisori $4n + 1$ convenientia. Quin etiam ex aliquot huiusmodi residuis reliqua sponte nascuntur, cum tam potestates quoque singulorum, quam producta ex binis pluribusve pariter in residuis occurrere debeant; unde patet, si iam prodierint residua $\alpha\gamma$ et $\beta\gamma$, tum etiam residuum fore $\alpha\beta$. Quia enim productum $\alpha\beta\gamma^2$ est residuum, omisso quadrato γ^2 etiam $\alpha\beta$ erit residuum.

COROLLARIUM 3

12. Quodsi ergo compertum fuerit residuum $\alpha\beta$, ex alio autem casu residuum prodeat α, etiam alter factor β erit residuum.

SCHOLION

13. Cum huiusmodi combinationes binorum residuorum pluribus, immo infinitis modis institui queant, hinc iam maxime verisimile videtur, praeter ipsos numeros in formulis $n - qq - q$ et $qq + q - n$ contentos etiam omnes eorum factores primos in residuis occurrere, quae coniectura utrum fundamento certo innitatur necne, per sequentia exempla exploremus. Hunc in finem exponamus numeros in formula $qq + q$ contentos, qui sunt

0, 2, 6, 12, 20, 30, 42, 56, 72, 90, 110, 132, 156,
182, 210, 240, 272, 306, 342, 380, 420 etc.,

et quemadmodum residua hinc nata littera p designamus, ita residua prima seu simplicia littera r indicemus, et quo facilius perspiciatur omnes factores numerorum p quoque esse residua, ipsos numeros p per suos factores primos repraesentemus:

1°. Sit $4n + 1 = 5$; erit $n = 1$.

$p = 1, 1, 5, 11, 19, 29, 41, 5 \cdot 11, 71$ etc.
$r = 1, 5, 11, 19, 29, 41, 71$ etc.,

ubi patet numeri compositi p, qui est unicus $5 \cdot 11$, ipsos factores quoque esse residua.

2°. Sit $4n + 1 = 13$; $n = 3$.

$p = 3, 1, 3, 3^2, [17,] 3^3, 3 \cdot 13, 53, 3 \cdot 23$ etc.
$r = 1, 3, 13, [17,] 23, 53$ etc.

3°. Sit $4n + 1 = 17$; $n = 4$.

$p = 2^2, 2, 2, 2^3, 2^4, 2 \cdot 13, 2 \cdot 19, 2^2 \cdot 13, 2^2 \cdot 17, 2 \cdot 43$ etc.
$r = 1, 2, 13, 17, 19, 43$ etc.

4°. Sit $4n + 1 = 29$; $n = 7$.

$p = 7, 5, 1, 5, 13, 23, 5 \cdot 7, 7^2, 5 \cdot 13, 83, 103$ etc.
$r = 1, 5, 7, 13, 23, 83, 103$ etc.

5°. Sit $4n + 1 = 37$; $n = 9$.

$p = 3^2, 7, 3, 3, 11, [3 \cdot 7,] 3 \cdot 11, 47, [3^2 \cdot 7,] 3^4, 101$ etc.[1])
$r = 1, 3, 7, 11, 47, 101$ etc.

6°. Sit $4n + 1 = 41$; $n = 10$.

$p = 2 \cdot 5, 2^3, 2^2, 2, 2 \cdot 5, 2^2 \cdot 5, 2^5, 2 \cdot 23, 2 \cdot 31, 2^4 \cdot 5, 2^2 \cdot 5^2$ etc.
$r = 1, 2, 5, 23, 31$ etc.,

ubi patet in numeris p nullos factores primos conspici, qui non simul sint residua.

7°. Sit $4n + 1 = 53$; $n = 13$.

$p = 13, 11, 7, 1, 7, 17, 29, 43, 59, 7 \cdot 11, 97$ etc.
$r = 1, 7, 11, 13, 17, 29, 43, 59, 97$ etc.

8°. Sit $4n + 1 = 61$; $n = 15$.

$p = 3 \cdot 5, 13, 3^2, 3, 5, 3 \cdot 5, 3^3, 41, 3 \cdot 19, 3 \cdot 5^2, 5 \cdot 19$ etc.
$r = 1, 3, 5, 13, 19, 41$ etc.

9°. Sit $4n + 1 = 73$; $n = 18$.

$p = 2 \cdot 3^2, 2^4, 2^2 \cdot 3, 2 \cdot 3, 2, 2^2 \cdot 3, 2^3 \cdot 3, 2 \cdot 19, 2 \cdot 3^3, 2^3 \cdot 3^2, 2^2 \cdot 23$ etc.
$r = 1, 2, 3, 19, 23$ etc.

10°. Sit $4n + 1 = 89$; $n = 22$.

$p = 2 \cdot 11, 2^2 \cdot 5, 2^4, 2 \cdot 5, 2, 2^3, 2^2 \cdot 5, 2 \cdot 17, 2 \cdot 5^2, 2^2 \cdot 17, 2^3 \cdot 11$ etc.
$r = 1, 2, 5, 11, 17$ etc.

11°. Sit $4n + 1 = 97$; $n = 24$.

$p = 2^3 \cdot 3, 2 \cdot 11, 2 \cdot 3^2, 2^2 \cdot 3, 2^2, 2 \cdot 3, 2 \cdot 3^2, 2^5, 2^4 \cdot 3, 2 \cdot 3 \cdot 11, 2 \cdot 43$ etc.
$r = 1, 2, 3, 11, 43$ etc.

1) Editio princeps: $p = \ldots, 11, 19, 3 \cdot 11, 43, 59, 7 \cdot 11, 101$, etc.
$r = \ldots, 11, 19, 43, 59, 101$, etc. Correxit R. F.

12°. Sit $4n + 1 = 101$[1]); $n = 25$.

$p = 5^2$, 23, 19, 13, 5, 5, 17, 31, 47, $5 \cdot 13$, $5 \cdot 17$ etc.

$r = 1$, 5, 13, 17, 19, 23, 31, 47 etc.

13°. Sit $4n + 1 = 109$; $n = 27$.

$p = 3^3$, 5^2, $3 \cdot 7$, $3 \cdot 5$, 7, 3, $3 \cdot 5$, [29][2]), $3^2 \cdot 5$, $3^2 \cdot 7$, 83 etc.

$r = 1$, 3, 5, 7, [29][3]), 83 etc.

14°. Sit $4n + 1 = 113$; $n = 28$.

$p = 2^2 \cdot 7$, $2 \cdot 13$, $2 \cdot 11$, 2^4, 2^3, 2, $2 \cdot 7$, $2^2 \cdot 7$, $2^2 \cdot 11$, $2 \cdot 31$, $2 \cdot 41$ etc.

$r = 1$, 2, 7, 11, 13, 31, 41 etc.

15°. Sit $4n + 1 = 137$; $n = 34$.

$p = 2 \cdot 17$, 2^5, $2^2 \cdot 7$, $2 \cdot 11$, $2 \cdot 7$, 2^2, 2^3, $2 \cdot 11$, $2 \cdot 19$, $2^3 \cdot 7$, $2^2 \cdot 19$ etc.

$r = 1$, 2, 7, 11, 17, 19 etc.

16°. Sit $4n + 1 = 149$; $n = 37$.

$p = 37$, $5 \cdot 7$, 31, 5^2, 17, 7, 5, 19, $5 \cdot 7$, 53, 73 etc.

$r = 1$, 5, 7, 17, 19, 31, 37, 53, 73 etc.

17°. Sit $4n + 1 = 157$; $n = 39$.

$p = 3 \cdot 13$[4]), 37, $3 \cdot 11$, 3^3, 19, 3^2, 3, 17, $3 \cdot 11$, $3 \cdot 17$, 71 etc.

$r = 1$, 3, 11, [13,] 17, 19, 37, 71 etc.

18°. Sit $4n + 1 = 173$; $n = 43$.

$p =$ [43,] 41, 37, 31, 23, 13, 1, 13, 29, 47, 67 etc.

$r = 1$, 13, 23, 29, 31, 37, 41, [43,] 47, 67 etc.

19°. Sit $4n + 1 = 181$; $n = 45$.

$p = 3^2 \cdot 5$, 43, $3 \cdot 13$, $3 \cdot 11$, 5^2, $3 \cdot 5$, 3, 11, 3^3[5]), $3^2 \cdot 5$, $5 \cdot 13$ etc.

$r = 1$, 3, 5, 11, 13, 43 etc.[6]).

20°. Sit $4n + 1 = 193$; $n = 48$.

$p = 2^4 \cdot 3$, $2 \cdot 23$, $2 \cdot 3 \cdot 7$, $2^2 \cdot 3^2$, $2^2 \cdot 7$, $2 \cdot 3^2$, $2 \cdot 3$, 2^3, $2^3 \cdot 3$, $2 \cdot 3 \cdot 7$, $2 \cdot 31$ etc.

$r = 1$, 2, 3, 7, 23, 31 etc.

21°. Sit $4n + 1 = 197$; $n = 49$.

$p = 7^2$, 47, 43, 37, 29, 19, 7, 7, 23, 41, 61 etc.

$r = 1$, 7, 19, 23, 29, 37, 41, 43, 47, 61 etc.

1) Editio princeps: 111.
2) Editio princeps: $3 \cdot 13$.
3) Editio princeps: 13.
4) Editio princeps: $3 \cdot 19$.
5) Editio princeps: 2^3.
6) Editio princeps: 1, 2, 3, ...

Correxit R. F.

SCHOLION

14. Ex his omnibus exemplis manifesto liquet nullos numeros primos sub littera p tamquam factores occurrere, qui non simul ipsi sint residua; quae veritas certe omnem attentionem eo magis meretur, quod ex sola inductione est conclusa, neque etiamnunc firma demonstratione corroborata; quia tamen in omnibus allatis exemplis tam luculenter se offert, neutiquam desperandum videtur. Qui autem hanc investigationem suscipere voluerit, probe perpendat hanc egregiam proprietatem tum tantum locum habere, quando $4n + 1$ est numerus primus; si enim non est primus, plurimi occurrunt casus, quibus hoc secus evenit. Huius generis exemplum est, quo $n = 11$; tum enim prodit $p = 11, 3^2, 5, 1, 3^2, 19, 31, [3^2 \cdot 5,] 61, 79, 3^2 \cdot 11$ etc., unde de numero 3 nihil plane concludere licet, an ad residua pertineat necne? Quod autem casibus, quibus $4n + 1$ est numerus primus, semper succedat, ratio fortasse in eo est quaerenda, quod pro divisore $2n + 1$ numerus residuorum semper est n, dum contra, si $2n + 1$ non est primus, numerus residuorum multo est minor; id quod in caussa esse videtur, quod in allato exemplo circa numerum 3 nihil decidatur. Quicquid autem sit, nullum plane dubium superesse videtur, quominus sequens stabiliatur

CONCLUSIO

15. Quoties numerus $4n + 1$ fuerit primus, per eumque omnia quadrata dividantur, non solum omnes numeri in hac formula: $n - qq - q$, sive etiam hac: $qq + q - n$ contenti, inter residua occurrunt ipsi, sed etiam omnes plane factores primi, ex quibus illi sint compositi.

THEOREMA 4

16. *Si* $4n - 1$ *fuerit numerus primus et per eum omnia quadrata dividantur, inter residua omnes occurrent numeri in hac formula* $n + qq + q$ *contenti.*

DEMONSTRATIO

Hic etiam clarum est numerum $4n - 1$ infinitis modis sub hac forma $4p - (2q + 1)^2$ repraesentari posse; posito enim $4n - 1 = 4p - (2q + 1)^2$, fiet $n = p - q^2 - q$, sive $p = n + q^2 + q$. Cum ergo $4p - (2q + 1)^2$ sit

numerus primus, ante demonstratum est numerum p inter residua reperiri; quocirca etiam omnes numeri in hac formula contenti $n + qq + q$ inter residua reperientur.

COROLLARIUM 1

17. Si ergo pro q omnes numeri 0, 1, 2, 3, 4 etc. substituantur, infiniti huiusmodi oriuntur numeri, quos tamen omnes ad multitudinem $2n - 1$ deprimere licet, siquidem isti numeri $n + qq + q$ per divisorem $4n - 1$ dividantur.

COROLLARIUM 2

18. Necesse ergo est hoc modo omnia plane prodire residua, quandoquidem etiam tam potestates, quam producta singulorum istorum numerorum inter residua reperiuntur; unde ut ante sequitur, si iam habeantur duo residua α et $\alpha\beta$, tum etiam β fore residuum; quin etiam si $\alpha\gamma\gamma$ fuerit residuum, ipsum α quoque erit residuum.

SCHOLION

19. Cum eiusmodi bina residua infinitis modis combinari possint, maxime verisimilis est suspicio praeter ipsos numeros in forma $n + qq + q$ contentos etiam omnes eorum factores primos in residuis occurrere; quae coniectura utrum, pariter ut ante, certo fundamento nitatur necne, per sequentia exempla exploremus. Iam supra autem exposuimus numeros in formula $qq + q$ contentos, unde pro quolibet numero primo residua simplicia, pariter ut ante, littera r indicemus.

1°. Sit $4n - 1 = 3$; erit $n = 1$.

$p = 1, 3, 7, 13, 3\cdot 7, 31, 43, 3\cdot 19, 73, 7\cdot 13, 3\cdot 37$ etc.
$r = 1, 3, 7, 13, 19, 31, 37, 43, 73$ etc.

2°. Sit $4n - 1 = 7$; erit $n = 2$.

$p = 2, 2^2, 2^3, 2\cdot 7, 2\cdot 11, 2^5, 2^2\cdot 11, 2\cdot 29, 2\cdot 37, 2^2\cdot 23, 2^4\cdot 7$ etc.
$r = 1, 2, 7, 11, 23, 29, 37$ etc.

3°. Sit $4n - 1 = 11$; erit $n = 3$.

$p = 3, 5, 3^2, 3\cdot 5, 23, 3\cdot 11, 3^2\cdot 5, 59, 3\cdot 5^2, 3\cdot 31, 113$ etc.
$r = 1, 3, 5, 11, 23, 31, 59, 113$ etc.

4°. Sit $4n - 1 = 19$; erit $n = 5$.

$p = 5, 7, 11, 17, 5^2, 5\cdot 7, 47, 61, 7\cdot 11, 5\cdot 19, 5\cdot 23$ etc.

$r = 1, 5, 7, 11, 17, 19, 23, 47, 61$ etc.

5°. Sit $4n - 1 = 23$; $n = 6$.

$p = 2\cdot 3, 2^3, 2^2\cdot 3, 2\cdot 3^2, 2\cdot 13, 2^2\cdot 3^2, 2^4\cdot 3, 2\cdot 31, 2\cdot 3\cdot 13, 2^5\cdot 3, 2^2\cdot 29$ etc.

$r = 1, 2, 3, 13, 29, 31$ etc.

6°. Sit $4n - 1 = 31$; erit $n = 8$.

$p = 2^3, 2\cdot 5, 2\cdot 7, 2^2\cdot 5, 2^2\cdot 7, 2\cdot 19, 2\cdot 5^2, 2^6, 2^4\cdot 5, 2\cdot 7^2, 2\cdot 59$ etc.

$r = 1, 2, 5, 7, 19, 59$ etc.

7°. Sit $4n - 1 = 43$; erit $n = 11$.

$p = 11, 13, 17, 23, 31, 41, 53, 67, 83, 101, 11^2$ etc.

$r = 1, 11, 13, 17, 23, 31, 41, 53, 67, 83, 101$ etc.

8°. Sit $4n - 1 = 47$; $n = 12$.

$p = 2^2\cdot 3, 2\cdot 7, 2\cdot 3^2, 2^3\cdot 3, 2^5, 2\cdot 3\cdot 7, 2\cdot 3^3, 2^2\cdot 17, 2^2\cdot 3\cdot 7, 2\cdot 3\cdot 17, 2\cdot 61$ etc.

$r = 1, 2, 3, 7, 17, 61$ etc.

9°. Sit $4n - 1 = 59$; $n = 15$.

$p = 3\cdot 5, 17, 3\cdot 7, 3^3, 5\cdot 7, 3^2\cdot 5, 3\cdot 19, 71, 3\cdot 29$ etc.

$r = 1, 3, 5, 7, 17, 19, 29, 71$ etc.

10°. Sit $4n - 1 = 67$; $n = 17$.

$p = 17, 19, 23, 29, 37, 47, 59, 73, 89, 107, 127$ etc.

$r = 1, 17, 19, 23, 29, 37, 47, 59, 73, 89, 107, 127$ etc.

11°. Sit $4n - 1 = 71$; $n = 18$.

$p = 2\cdot 3^2, 2^2\cdot 5, 2^3\cdot 3, 2\cdot 3\cdot 5, 2\cdot 19, 2^4\cdot 3, 2^2\cdot 3\cdot 5, 2\cdot 37, 2\cdot 3^2\cdot 5, 2^2\cdot 3^3,$
$2^7, 2\cdot 3\cdot 5^2$ etc.

$r = 1, 2, 3, 5, 19, 37$ etc.

12°. Sit $4n - 1 = 79$; $n = 20$.

$p = 2^2\cdot 5, 2\cdot 11, 2\cdot 13, 2^5, 2^3\cdot 5, 2\cdot 5^2, 2\cdot 31, 2^2\cdot 19, 2^2\cdot 23, 2\cdot 5\cdot 11$ etc.

$r = 1, 2, 5, 11, 13, 19, 23, 31$ etc.

13°. Sit $4n - 1 = 83$; $n = 21$.

$p = 3\cdot 7, 23, 3^3, 3\cdot 11, 41, 3\cdot 17, 3^2\cdot 7, 7\cdot 11, 3\cdot 31, 3\cdot 37$ etc.

$r = 1, 3, 7, 11, 17, 23, 31, 37, 41$ etc.

14°. Sit $4n - 1 = 103$; $n = 26$.

$p = 2\cdot 13, 2^2\cdot 7, 2^5, 2\cdot 19, 2\cdot 23, 2^3\cdot 7, 2^2\cdot 17, 2\cdot 41, 2\cdot 7^2, 2^2\cdot 29$ etc.

$r = 1, 2, 7, 13, 17, 19, 23, 29, 41$ etc.

SCHOLION

20. Ex his exemplis iterum abunde patet omnes plane numeros primos in numeris p contentos ipsos quoque esse residua. Evidens autem est, ut primum hoc de minoribus numeris fuerit certum, de maioribus nullum amplius dubium relinqui; at vero in numeros p binarius non ingreditur, nisi iam fuerit in ipso numero primo n; ternarius autem, nisi in duobus primis insit, ex tota serie p excluditur. Eodem modo patet quinarium, nisi in tribus primis insit, quoque excludi; septenarius autem penitus excluditur, nisi in quatuor primis iam occurrat, et sic de reliquis. Unde patet in continuatione ulteriori istius seriei nullos numeros primos minores ingredi posse, qui non iam ante fuerint ingressi; quae observatio fortasse ad demonstrationem deducere posset. Verum hic iterum probe notetur hanc insignem proprietatem tantum locum habere, quoties $4n - 1$ fuerit numerus primus; si enim esset compositus, tum utique eiusmodi numeri primi occurrere possunt, de quibus neutiquam liquet, utrum in ordinem r sint referendi. Veluti si fuerit $n = 30 = 2 \cdot 3 \cdot 5$, tum numeri pro p ita se habebunt:

$$p = 2 \cdot 3 \cdot 5,\ 2^5,\ 2^2 \cdot 3^2,\ 2 \cdot 3 \cdot 7,\ 2 \cdot 5^2,\ 2^2 \cdot 3 \cdot 5,\ 2^3 \cdot 3^2,\ 2 \cdot 43,\ 2 \cdot 3 \cdot 17,\ 2^3 \cdot 3 \cdot 5,\ 2^2 \cdot 5 \cdot 7,\ 2 \cdot 3^4\ ^{1}) \text{ etc.}$$

Hic quidem statim adparet binarium ad residua esse referendum; quo sublato iudicium redit ad sequentes numeros:

$$3 \cdot 5,\ 3^2,\ 3 \cdot 7,\ 5^2,\ 43,\ 3 \cdot 17,\ 5 \cdot 7,\ 3^4 \text{ etc.}$$

Hinc autem nullo modo concludi potest sive 3 sive 5 sive 7 in residuis reperiri; et fieri posset, ut singuli essent non-residua, quandoquidem producta ex binis non-residuis producunt residua; verum etiam hinc numerus $4n - 1 = 119$ non est primus. De primis autem certa videtur haec

CONCLUSIO

21. Quoties numerus $4n - 1$ fuerit primus, per eumque dividantur omnia quadrata, non solum omnes numeri in forma $n + qq + q$ contenti inter residua occurrunt ipsi, sed etiam omnes plane factores primi, ex quibus illi sunt compositi.

---

1) Editio princeps: 9^2. Correxit R. F.

THEOREMA GENERALE

22. *Denotante T numerum quemcunque in hac formula $(2q+1)^2 - 4at$ contentum, si fuerit vel $4as + T$ vel $4as - T$ numerus primus, per eumque quadrata dividantur, tum in residuis semper reperietur numerus a*[1]).

DEMONSTRATIO

Cum enim sit $T = (2q+1)^2 - 4at$, numerus ille primus erit vel $4as - 4at + (2q+1)^2$, vel $4as + 4at - (2q+1)^2$. Illo casu habebimus $p = a(s-t)$, hoc vero $p = a(s+t)$, sicque in utroque casu p factorem habet a, qui ergo per praecedentes conclusiones in residuis ex quadratis ortis occurret.

COROLLARIUM 1

23. Hoc ergo modo numeri T ex quadratis $(2q+1)^2$ formati infra $4a$ deprimi poterunt; sicque multitudo horum valorum ad numerum determinatum reducetur, etiamsi numeri $(2q+1)^2$ in infinitum progrediantur. Inventis autem omnibus ipsius T valoribus ipso $4a$ minoribus, si illis continuo addantur multipla ipsius $4a$, hos valores in infinitum continuare licebit.

COROLLARIUM 2

24. Quia numerus a inter residua quadratorum occurrit, semper dabitur formula $xx - ayy$ per numerum illum primum divisibilis, sive is sit $4as + T$ sive $4as - T$; ac si iste numerus primus vocetur $2m+1$, tum formula $a^m - 1$ divisorem habebit $2m+1$.

SCHOLION

25. Quot autem valores diversos littera T infra $4a$ sortiatur, id pendet ab indole numeri a, sive is fuerit primus sive compositus; atque hoc discrimen probe est notandum, cum ulterior evolutio harum formularum pro casibus, quibus a est numerus compositus, commode expediri nequeat, nisi casus, quibus a est numerus primus, ante fuerint explorati.

---

1) Confer Conclusionem Commentationis 552 (indicis Enestroemiani): *Observationes circa divisionem quadratorum per numeros primos*, Opuscula analytica 1, 1783, p. 69—84, *Leonhardi Euleri Opera omnia*, series I, vol. 3, p. 512. R. F.

THEOREMA [5]

26. *Si a fuerit numerus primus, puta $2\alpha + 1$, tum numerus valorum litterae T ipso $4a$ minorum erit $= \alpha$, et totidem numeri formae $4n + 1$ inde excludentur.*

DEMONSTRATIO

Omnes valores diversi litterae T ipso $4a$ minores colliguntur ex quadratis imparibus minoribus quam $a^2 = (2\alpha + 1)^2$, quae ergo sunt 1, 9, 25, 49, $\ldots(2\alpha - 1)^2$, quorum numerus utique est α. Perspicuum autem est ex quadratis maioribus quam a eosdem prorsus valores ipsius T resultare, qui ex minoribus prodierunt. Sit enim quadratum quodvis maius $(a + \beta)^2$, hocque comparetur cum quadrato minore $(a - \beta)^2$, et quia eorum differentia $4a\beta$ divisibilis est per $4a$, utrinque idem residuum oriatur necesse est. Facile autem porro intelligitur ex omnibus quadratis ipso a^2 minoribus diversa residua nasci debere. Quia iam T denotat numeros formae $4n + 1$, videamus, quot huiusmodi numeri ab unitate usque ad $4a = 8\alpha + 4$ occurrant. Facile autem patet eorum numerum fore $= 2\alpha + 1$, inter quos occurrit unus per a divisibilis; quo excluso multitudo reliquorum est $= 2\alpha$; quare cum multitudo valorum idoneorum ipsius T sit $= \alpha$, evidens est totidem numeros formae $4n + 1$ inde excludi.

COROLLARIUM 1

27. Quia omnes valores litterae T in forma $4n + 1$ continentur, si omnes numeri huius formae ab unitate usque ad $4a$ scribantur, eorum semissis tantum praebet veros valores litterae T, reliqui vero omnes inde excluduntur. Utamur autem littera Θ ad huiusmodi numeros exclusos denotandos.

COROLLARIUM 2

28. Cum ergo omnes numeri formae $4n + 1$, qui sunt:

1, 5, 9, 13, 17, 21, 25, 29, 33 etc.,

pro quovis casu numeri a sive ad ordinem terminorum $T = (2q + 1)^2 - 4at$, sive ad ordinem exclusorum Θ referantur, operae pretium erit ambos istos ordines pro minoribus saltem ipsius a valoribus, qui quidem sint primi,

exhibere; atque utile erit non solum primam periodum horum numerorum ipso $4a$ minorum, sed etiam sequentes periodos, addendo continuo $4a$, ob oculos exponere:

1°. Sit $a = 2$; erit $4a = 8$.

$$\begin{array}{l|l|l|l|l|l|} T = 1 & 9 & 17 & 25 & 33 & \\ \Theta = 5 & 13 & 21 & 29 & 37 & \end{array} \text{ etc.}$$

2°. Sit $a = 3$; erit $4a = 12$.

$$\begin{array}{l|l|l|l|l|l|} T = 1 & 13 & 25 & 37 & 49 & 61 \\ \Theta = 5 & 17 & 29 & 41 & 53 & 65 \end{array} \text{ etc.}$$

Quia hic a erat 3, quadrata per 3 divisibilia excludi debebant.

3°. Sit $a = 5$; erit $4a = 20$.

$$\begin{array}{l|l|l|l|l|} T = 1, 9 & 21, 29 & 41, 49 & 61, 69 & 81, 89 \\ \Theta = 13, 17 & 33, 37 & 53, 57 & 73, 77 & 93, 97 \end{array} \text{ etc.}$$

Hic scilicet ex ordine Θ exclusimus numerum 5, utpote ipsi a aequalem.

4°. Sit $a = 7$; erit $4a = 28$.

$$\begin{array}{l|l|l|l|} T = 1, 9, 25 & 29, 37, 53 & 57, 65, 81 & \\ \Theta = 5^{1}), 13, 17 & 33, 41, 45 & 61, 69, 73 & \end{array} \text{ etc.}$$

Hic in ordine Θ omisimus numerum 21, utpote per $a = 7$ divisibilem.

5°. Sit $a = 11$; $4a = 44$.

$$\begin{array}{l|l|l|} T = 1, 5, 9, 25, 37 & 45, 49, 53, 69, 81 & 89, 93, 97, 113, 125 \\ \Theta = 13, 17, 21, 29, 41 & 57, 61, 65, 73, 85 & 101, 105, 109, 117, 129 \end{array} \text{ etc.}$$

6°. Sit $a = 13$; $4a = 52$.

$$\begin{array}{l|l|l|} T = 1, 9, 17, 25, 29, 49 & 53, 61, 69, 77, 81, 101 & \\ \Theta = 5, 21, 33, 37, 41, 45 & 57, 73, 85, 89, 93, 97 & \end{array} \text{ etc.}$$

7°. Sit $a = 17$; $4a = 68$.

$$\begin{array}{l|l|} T = 1, 9, 13, 21, 25, 33, 49, 53 & \\ \Theta = 5, 29, 37, 41, 45, 57, 61, 65 & \end{array} \text{ etc.}$$

8°. Sit $a = 19$; $4a = 76$.

$$\begin{array}{l|l|} T = 1, 5, 9, 17, 25, 45, 49, 61, 73 & 77, 81, 85, 93, 101, 121, 125, 137, 149 \\ \Theta = 13, 21, 29, 33, 37, 41, 53, 65, 69 & 89, 97, 105, 109, 113, 117, 129, 141, 145 \end{array} \text{ etc.}$$

9°. Sit $a = 23$; $4a = 92$.

$$\begin{array}{l|l|} T = 1, 9, 13, 25, 29, 41, 49, 73, 77, 81, 85 & \\ \Theta = 5, 17, 21, 33, 37, 45, 53, 57, 61, 65, 89 & \end{array} \text{ etc.}$$

1) Editio princeps: 1. Correxit R. F.

10°. Sit $a = 29$; $4a = 116$.

$T = 1, 5, 9, 13, 25, 33, 45, 49, 53, 57, 65, 81, 93, 109$
$\Theta = 17, 21, 37, 41, 61, 69, 73, 77, 85, 89, 97, 101, 105, 113$ | etc.

SCHOLION

29. Hinc ergo pro istis numeris primis a innotescunt tam valores litterae T, quam litterae Θ, quos ita intelligere decet, ut, quoties formula $4as + T$ vel $4as - T$ fuerit numerus primus, puta $2m + 1$, tum semper exhiberi possit formula $xx - ayy$ per $2m + 1$ divisibilis; tum vero etiam semper formula $a^m - 1$ eundem habebit divisorem $2m + 1$, ita ut iam plura Theoremata supra allata, scilicet quoties a fuerit numerus primus, ita succincte possimus enuntiare, ut, quoties fuerit $4as \mp T$ numerus primus $= 2m + 1$, tum semper formula $a^m - 1$ eundem admittat divisorem; quo observato nullum amplius dubium supererit, quin numeri sub ordine Θ comprehensi contraria gaudeant proprietate, quam iam ita enuntiare licebit, ut, quoties formula $4as \mp \Theta$ fuerit numerus primus $= 2m + 1$, tum non amplius formula $a^m - 1$ per eum sit divisibilis; unde cum formula $a^{2m} - 1$ semper sit divisibilis, sequitur hoc casu semper formulam $a^m + 1$ per numerum primum $2m + 1$ fore divisibilem. Atque haec duo enuntiata omnes casus supra allatos exhauriunt, quibus numerus a erat primus; quando autem a habet factores, res secus se habet, hosque casus peculiari modo tractari conveniet.

PROBLEMA

30. *Si numerus a fuerit compositus, puta $a = fg$, invenire numeros utriusque indolis per litteras T et Θ designatos.*

SOLUTIO

Hic igitur quaeruntur omnes divisores primi $2m + 1$ sub formula $4fgs \mp T$ contenti, per quos formula $(fg)^m - 1$ sit divisibilis; id quod duplici modo fieri potest, vel quando hae duae formulae: $f^m - 1$ et $g^m - 1$ per $2m + 1$ sunt divisibiles, vel etiam hae duae formulae: $f^m + 1$ et $g^m + 1$. Priore enim casu, cum sit

$$(fg)^m - 1 = g^m(f^m - 1) + g^m - 1,$$

utique haec formula per $2m + 1$ dividi poterit. Iam pro numeris primis f et g divisores primi hoc praestantes supra sunt inventi, quos distinctionis gratia ita repraesentemus:

$$4fgs \mp T^{(f)} \quad \text{et} \quad 4gfs \mp T^{(g)};$$

quae duae formulae in unam coalescent, si ex valoribus supra datis litterarum $T^{(f)}$ et $T^{(g)}$ eos excerpamus, qui utrique sunt communes. Hi enim si littera T comprehendantur, utique omnes numeri primi huius formae $4fgs \mp T$ quaesito satisfacient. Posteriore autem casu, quo formulae $f^m + 1$ et $g^m + 1$ divisorem habent $2m + 1$, quia est

$$(fg)^m - 1 = f^m(g^m + 1) - f^m - 1,$$

huic formulae idem divisor conveniet. Pro hoc autem casu supra vidimus formam divisorum primorum esse

$$4fgs \mp \Theta^{(f)} \quad \text{et} \quad 4gfs \mp \Theta^{(g)};$$

quare si ex valoribus litterae Θ pro numeris f et g ii, qui ipsis sunt communes, excerpantur, eos nunc etiam valoribus litterae T accenseri oportet; sicque omnes valores quaesiti litterae T obtinebuntur, si tam numeri formulis $T^{(f)}$ et $T^{(g)}$ communes, quam etiam ii, quos formulae $\Theta^{(f)}$ et $\Theta^{(g)}$ communes habent, coniungantur atque usque ad terminum $4fg = 4a$ producantur; quem in finem iam supra valores harum litterarum ultra primam periodum continuavimus. His autem inventis reliqui numeri formae $4n + 1$ hinc exclusi valores dabunt litterae Θ, quos etiam ita colligere licet, ut eo referantur tam termini litteris $T^{(f)}$ et $\Theta^{(g)}$, quam litteris $T^{(g)}$ et $\Theta^{(f)}$ communes.

EXEMPLUM

31. Quia haec operatio facillime exemplo illustrabitur, sit $a = 15$ ideoque $f = 3$ et $g = 5$, pro quo utroque numero ex supra allatis depromantur valores litterarum T et Θ. Inde igitur habebimus:

$$\begin{aligned} \text{Pro } f = 3 \begin{cases} T^{(f)} &= 1, 13, 25, 37, 49, 61. \\ \Theta^{(f)} &= 5, 17, 29, 41, 53, 65. \end{cases} \\ \text{Pro } g = 5 \begin{cases} T^{(g)} &= 1, 9, 21, 29, 41, 49, 61, 69. \\ \Theta^{(g)} &= 13, 17, 33, 37, 53, 57, 73, 77, \end{cases} \end{aligned}$$

quos valores ultra terminum $4a = 4fg = 60$ continuavimus.

Iam litterae $T^{(f)}$ et $T^{(g)}$ sequentes habent terminos communes: 1, 49, litterae autem $\Theta^{(f)}$ et $\Theta^{(g)}$ communes habent istos terminos: 17, 53, qui numeri coniunctim praebent valores litterae T pro isto casu. At pro littera Θ capiantur primo termini communes ex litteris $T^{(f)}$ et $\Theta^{(g)}$, qui sunt 13, 37; tum vero etiam numeri litteris $T^{(g)}$ et $\Theta^{(f)}$ communes, qui sunt 29, 41. Consequenter pro casu proposito $a = 15$ valores litterarum T et Θ per primam periodum, usque ad $4a = 60$ continuati, erunt:

$$T = 1, 17, 49, 53.$$
$$\Theta = 13, 29, 37, 41.$$

Hic scilicet occurrunt omnes numeri formae $4n + 1$, qui quidem ad 15 sunt primi; et leviter attendenti patet totidem semper terminos in utrumque ordinem T et Θ ingredi.

SCHOLION

32. Quo haec postrema observatio melius intelligatur, regula haud adeo communis notetur, quae ostendit, quot ab unitate usque ad datum numerum N occurrant numeri ad ipsum primi, ubi quidem statim patet, si N fuerit ipse numerus primus, tum omnes praecedentes, quorum multitudo est $N - 1$, simul quoque ad eum esse primos; sin autem N fuerit numerus utcunque compositus, semper repraesentari poterit hac forma generali

$$N = a^{\alpha} \cdot b^{\beta} \cdot c^{\gamma} \cdot d^{\delta} \ldots\ldots,$$

ubi a, b, c etc. denotant numeros primos; tum autem multitudo numerorum ad N primorum ipsoque minorum erit[1])

$$(a - 1)\, a^{\alpha-1} \cdot (b - 1)\, b^{\beta-1} \cdot (c - 1)\, c^{\gamma-1} \ldots\ldots$$

Cum nunc nostro casu sit $N = 60 = 2^2 \cdot 3^1 \cdot 5^1$, erit multitudo numerorum ad N primorum ipsoque minorum

$$= 1 \cdot 2 \cdot 2 \cdot 4 = 16,$$

qui cum omnes sint impares et tam formae $4n + 1$ quam formae $4n - 1$, nostrae formae $4n + 1$ tantum aderunt numeri 8, quorum semissis ad lit-

1) Vide commentationem 271 (indicis Enestroemiani): *Theoremata arithmetica nova methodo demonstrata*, Novi comment. acad. sc. Petrop. 8 (1760/1), 1763, p. 74—104, *Leonhardi Euleri Opera omnia*, series I, vol. 2, p. 531—555. R. F.

teram T, reliqui vero ad litteram Θ referuntur. Utamur ergo hac regula inventa ad numeros T et Θ pro simplicioribus numeris a ex binis factoribus primis constantibus evolvendos:

1°. Sit $a = 2 \cdot 3$; $4a = 24$.

$T = 1, 5 \mid 25, 29 \mid 49, 53 \mid 73, 77.$
$\Theta = 13, 17 \mid 37, 41 \mid 61, 65 \mid 85, 89.$

2°. Sit $a = 2 \cdot 5$; $4a = 40$.

$T = 1, 9, 13, 37 \mid 41, 49, 53, 77.$
$\Theta = 17, 21, 29, 33 \mid 57, 61, 69, 73.$

3°. Sit $a = 2 \cdot 7$; $4a = 56$.

$T = 1, 5, 9, 13, 25, 45 \mid 57, 61, 65, 69, 81, 101.$
$\Theta = 17, 29, 33, 37, 41, 53 \mid 73, 85, 89, 93, 97, 109.$

4°. Sit $a = 2 \cdot 11$; $4a = 88$.

$T = 1, 9, 13, 21, 25, 29, 49, 61, 81, 85.$
$\Theta = 5, 17, 37, 41, 45, 53, 57, 65, 69, 73.$

5°. Sit $a = 2 \cdot 13$; $4a = 104$.

$T = 1, 5, 9, 17, 21, 25, 37, 45, 49, 81, 85, 93.$
$\Theta = 29, 33, 41, 53, 57, 61, 69, 73, 77, 89, 97, 101.$

6°. Sit $a = 3 \cdot 5$; $4a = 60$.

$T = 1, 17, 49, 53.$
$\Theta = 13, 29, 37, 41.$

7°. Sit $a = 3 \cdot 7$; $4a = 84$.

$T = 1, 5, 17, 25, 37, 41.$
$\Theta = 13, 29, 53, 61, 65, 73.$

PROBLEMA

33. *Si a fuerit numerus utcunque compositus, invenire valores litterarum T et Θ, qui illi conveniunt.*

SOLUTIO

Primo notetur, si a fuerit quadratum, puta ff, quia pro binis factoribus f et f tam litterae T quam Θ inter se conveniunt, omnes plane numeri formae $4m + 1$, quatenus scilicet ad f sunt primi, ad ordinem T sunt referendi,

ita ut ordo Θ plane vacuus relinquatur, id quod natura rei manifesto postulat. Cum enim sit $a = ff$, ideoque $a^m = f^{2m}$, semper formula $f^{2m} - 1$ divisibilis est per numerum primum $2m + 1$, sicque forma $a^m + 1$ nunquam hunc divisorem admittit. Deinde si fuerit $a = ffg$, quoniam pro ff in ordine T omnes numeri occurrunt, in Θ vero nulli, manifestum est pro hoc casu in ordinem T eosdem numeros ingredi, qui pro simplici numero g sunt inventi; neque vero ex ambobus Θ ullus praeterea accedet, omitti vero debent ii numeri, qui ad ff non sunt primi. Denique si a fuerit productum ex pluribus numeris primis, veluti $a = fghk$; quaerantur pro factoribus fg et hk numeri ad ordines T et Θ referendi, ex quibus deinceps valores harum litterarum pro ipso numero f perinde concludentur, uti in Problemate praecedente.

EXEMPLUM

34. Sit $a = 30 = 2 \cdot 3 \cdot 5$, ideoque $4a = 120$; sumantur primo litterae T et Θ pro numero $3 \cdot 5 = 15$, qui autem usque ad 120 continuentur, qui sunt:

pro $3 \cdot 5$ $\left\{ \begin{array}{l} T = 1, 17, 49, 53, 61, 77, 109, 113. \\ \Theta = 13, 29, 37, 41, 73, 89, 97, 101. \end{array} \right.$

Cum his comparentur ambae formae factori 2 respondentes, atque termini communes utrique T reperiuntur

1, 17, 49, 113,

termini autem communes utriusque litterae Θ sunt

13, 29, 37, 101,

quocirca ordines quaesiti T et Θ pro numero $a = 30$ erunt:

$T = 1, 13, 17, 29, 37, 49, 101, 113$ etc.
$\Theta = 41, 53, 61, 73, 77, 89, 97, 109$ etc.

SCHOLION

35. Colligamus iam omnia hactenus inventa, ac pro omnibus numeris a, exceptis ipsis quadratis, usque ad 30 formas numerorum primorum $2m + 1$ ordine exhibeamus, per quos vel $a^m - 1$ vel $a^m + 1$ fit divisibilis:

a.	$2m + 1$	$a^m \mp 1$.
2.	$8s \mp 1$,	$2^m - 1$.
	$8s \mp 5$,	$2^m + 1$.
3.	$12s \mp 1$,	$3^m - 1$.
	$12s \mp 5$,	$3^m + 1$.
5.	$20s \mp 1, 9$,	$5^m - 1$.
	$20s \mp 13, 17$,	$5^m + 1$.
6.	$24s \mp 1, 5$,	$6^m - 1$.
	$24s \mp 13, 17$,	$6^m + 1$.
7.	$28s \mp 1, 9, 25$,	$7^m - 1$.
	$28s \mp 5, 13, 17$,	$7^m + 1$.
8.	$32s \mp 1, 9, 17, 25$,	$8^m - 1$.
	$32s \mp 5, 13, 21, 29$,	$8^m + 1$.
10.	$40s \mp 1, 9, 13, 37$,	$10^m - 1$.
	$40s \mp 17, 21, 29, 33$,	$10^m + 1$.
11.	$44s \mp 1, 5, 9, 25, 37$,	$11^m - 1$.
	$44s \mp 13, 17, 21, 29, 41$,	$11^m + 1$.
12.	$48s \mp 1, 13, 25, 37$,	$12^m - 1$.
	$48s \mp 5, 17, 29, 41$,	$12^m + 1$.
13.	$52s \mp 1, 9, 17, 25, 29, 49$,	$13^m - 1$.
	$52s \mp 5, 21, 33, 37, 41, 45$,	$13^m + 1$.
14.	$56s \mp 1, 5, 9, 13, 25, 45$,	$14^m - 1$.
	$56s \mp 17, 29, 33, 37, 41, [53,]$	$14^m + 1$.
15.	$60s \mp 1, 17, 49, 53$,	$15^m - 1$.
	$60s \mp 13, 29, 37, 41$,	$15^m + 1$.
17.	$68s \mp 1, 9, 13, 21, 25, 33, 49, 53$,	$17^m - 1$.
	$68s \mp 5, 29, 37, 41, 45, 57, 61, 65$,	$17^m + 1$.
18.	$72s \mp 1, 17, 25, 41, 49, 65$,	$18^m - 1$.
	$72s \mp 5, 13, 29, 37, 53, 61$,	$18^m + 1$.
19.	$76s \mp 1, 5, 9, 17, 25, 45, 49, 61, 73$,	$19^m - 1$.
	$76s \mp 13, 21, 29, 33, 37, 41, 53, 65, 69$,	$19^m + 1$.
20.	$80s \mp 1, 9, 21, 29, 41, 49, 61, 69$,	$20^m - 1$.
	$80s \mp 13, 17, 33, 37, 53, 57, 73, 77$,	$20^m + 1$.

21.	$84s \mp$ 1, 5, 17, 25, 37, 41,	$21^m - 1.$
	$84s \mp$ 13, 29, 53, 61, 65, 73,	$21^m + 1.$
22.	$88s \mp$ 1, 9, 13, 21, 25, 29, 49, 61, 81, 85,	$22^m - 1.$
	$88s \mp$ 5, 17, 37, 41, 45, 53, 57, 65, 69, 73,	$22^m + 1.$
23.	$92s \mp$ 1, 9, 13, 25, 29, 41, 49, 73, 77, 81, 85,	$23^m - 1.$
	$92s \mp$ 5, 17, 21, 33, 37, 45, 53, 57, 61, 65, 89,	$23^m + 1.$
24.	$96s \mp$ 1, 5, 25, 29, 49, 53, 73, 77,	$24^m - 1.$
	$96s \mp$ 13, 17, 37, 41, 61, 65, 85, 89,	$24^m + 1.$
26.	$104s \mp$ 1, 5, 9, 17, 21, 25, 37, 45, 49, 81, 85, 93,	$26^m - 1.$
	$104s \mp$ 29, 33, 41, 53, 57, 61, 69, 73, 77, 89, 97, 101,	$26^m + 1.$
27.	$108s \mp$ 1, 13, 25, 37, 49, 61, 73, 85, 97,	$27^m - 1.$
	$108s \mp$ 5, 17, 29, 41, 53, 65, 77, 89, 101,	$27^m + 1.$
28.	$112s \mp$ 1, 9, 25, 29, 37, 53, 57, 65, 81, [85,] 93, 109,	$28^m - 1.$
	$112s \mp$ 5, 13, 17, 33, 41, 45, 61, 69, 73, 89, 97, 101,	$28^m + 1.$
29.	$116s \mp$ 1, 5, 9, 13, 25, 33, 45, 49, 53, 57, 65, 81, 93, 109,	$29^m - 1.$
	$116s \mp$ 17, 21, 37, 41, 61, 69, 73, 77, 85, 89, 97, 101, 105, 113,	$29^m + 1.$
30.	$120s \mp$ 1, 13, 17, 29, 37, 49, 101, 113,	$30^m - 1.$
	$120s \mp$ 41, 53, 61, 73, 77, 89, 97, 109,	$30^m + 1.$

Nunc igitur omnia, quae ante fuerant tradita, satis clare perspicere licet atque in hoc genere nihil aliud superesse videtur, quam ut binae illae conclusiones ex observationibus deductae firmis demonstrationibus muniantur.

Postquam pro quovis numero a, sive primo, sive composito, valores litterarum T et Θ fuerint inventi, sequentia duo Theoremata notari merentur:

I. *Omnes divisores primi formae* $xx - ayy$ *in alterutra harum formarum:* $4as + T$, *vel* $4as - T$ *continentur.*

II. *Omnes divisores primi huius formae:* $xx + ayy$ *in alterutra harum formularum:* $4as + T$ *vel* $4as - \Theta$ *continentur.*

Sponte autem patet pro x et y eiusmodi numeros sumi debere, ut bina membra xx et ayy nullum habeant divisorem communem.

PROPOSITA QUACUNQUE PROGRESSIONE AB UNITATE INCIPIENTE QUAERITUR QUOT EIUS TERMINOS AD MINIMUM ADDI OPORTEAT UT OMNES NUMERI PRODUCANTUR

Commentatio 558 indicis ENESTROEMIANI
Opuscula analytica 1, 1783, p. 296—309
[Conventui exhibita die 22. martii 1773]

Huius generis est notissimum illud theorema FERMATII sive BACHETTI, quod omnis numerus sit summa vel quatuor vel pauciorum quadratorum[1]), cuius demonstrationem post FERMATIANUM, quae intercidit, Cel. LA GRANGE in medium attulit[2]), ego vero etiam non ita pridem ex aliis principiis deductam cum Academia communicavi[3]). Memoratus autem FERMATIUS praeterea affirmaverat, se quoque demonstrasse, omnes numeros esse summas vel trium pauciorumve numerorum trigonalium, tum vero etiam quinque pauciorumve numerorum pentagonalium, item sex pauciorumve sexagonalium et ita porro. Horum autem theorematum nullum adhuc solide demonstratum comparavit.

Nuper vero etiam Ill. BEGUELIN, Berolinensis Academiae socius, huiusmodi theoremata adhuc multo latius ad omnes numeros pyramidales seu

1) Vide notam 4, p. 358, vol. 2, seriei I. R. F.

2) Vide notam 2, p. 370, vol. 2, seriei I. R. F.

3) 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—58, *LEONHARDI EULERI Opera omnia*, series I, vol. 2, p. 338—372. R. F.

figuratas extendit, qui quidem ex summatione numerorum polygonalium continue repetita nascuntur[1]). Ad haec explicanda denotet nobis Θ numerum terminorum ad minimum addendorum, ut omnes plane numeri producantur, atque Vir ingeniosissimus pro seriebus sequentibus valores litterae Θ subnexos dedit:

					Θ
$1,$	$1+a,$	$1+2a,$	$1+3a,$	$1+4a$ etc.	a
$1,$	$2+a,$	$3+3a,$	$4+6a,$	$5+10a$ etc.	$a+2$
$1,$	$3+a,$	$6+4a,$	$10+10a,$	$15+20a$ etc.	$a+4$
$1,$	$4+a,$	$10+5a,$	$20+15a,$	$35+35a$ etc.	$a+6$
$1,$	$5+a,$	$15+6a,$	$35+21a,$	$70+56a$ etc.	$a+8$
$1,$	$6+a,$	$21+7a,$	$56+28a,$	$126+84a$ etc.	$a+10$
			etc.		

unde in genere concluditur, fore pro hac serie generali:

$$1, \frac{n+a}{1}, \frac{(n+1)(n+2a)}{1\cdot 2}, \frac{(n+1)(n+2)(n+3a)}{1\cdot 2\cdot 3}, \frac{(n+1)(n+2)(n+3)(n+4a)}{1\cdot 2\cdot 3\cdot 4} \text{ etc.}$$

numerum $\Theta = a + 2n - 2$, quae forma non solum complectitur omnes numeros polygonales, sed etiam omnes series summatrices ex illis natas; ex quo hoc theorema utique maximam attentionem meretur. Tantum autem est dolendum, quod ipse inventor fateatur, se solidam eius demonstrationem neutiquam possidere, sed tantum, quasi per transennam, eius veritatem ope principii rationis sufficientis agnoscere. Etsi autem huic principio in huiusmodi investigationibus nihil plane tribuendum esse arbitror, veritatem tamen istius propositionis ob alias rationes agnoscere cogor; quin etiam hoc ipsum theorema iam ante triginta et plures annos in adversariis meis consignatum reperitur.

Has igitur insignes numerorum proprietates perpendenti sine dubio maxime dolendum videbitur nos etiamnunc earum demonstratione indigere, idque eo magis, quod vix adhuc prima principia sint stabilita, ex quibus demonstrationes desideratae peti queant; quamobrem constitui hic ista principia adcuratius investigare, unde fortasse, quicquid in hoc genere etiam-

1) Confer M. Beguelin: *Recherches sur les nombres triangulaires relativement au théorème général de Mr.* Fermat *concernant les nombres polygonaux.* Nouv. mém. de l'acad. roy. des sc. et bell. lettr., 1773, p. 203. R. F.

num desideratur, tandem haurire licebit. Hunc in finem consideremus progressionem quamcunque ab unitate incipientem, quae sit:

$$1, A, B, C, D, E, F \text{ etc.},$$

de qua, quot eius terminis ad minimum sibi invicem addendis opus sit, ut omnes plane numeri producantur, quaeritur; atque hunc ipsum numerum quaesitum littera Θ indicemus; quo quidem non solum termini diversi, sed et iidem aliquoties repetiti contineri sunt intelligendi. Hanc igitur investigationem sequenti modo ex primis principiis deducere conabor.

1. Consideremus igitur initio solum primum seriei terminum, qui est $= 1$, ac manifestum est hinc usque ad secundum terminum A omnes numeros produci non posse, nisi statuatur $\Theta = A - 1$, siquidem numerus $A - 1$ ex totidem unitatibus constans toties primum terminum 1 repetendum postulat; unde quaecunque fuerit nostra series, iam clare perspicimus numerum quaesitum Θ certe minorem esse non posse quam $A - 1$.

2. Nunc praeter primum terminum 1 admittamus quoque secundum A, ad quem usque modo vidimus statui debere $\Theta = A - 1$. Hinc autem ulterius progrediendo numerus proxime sequens ex totidem terminis compositus erit $2A - 2$, quippe qui constat ex secundo termino A semel sumto et primo termino 1 tot vicibus sumto, quot formula $A - 2$ indicat, quandoquidem hic numerus ita repraesentari potest: $A + 1\,(A - 2)$, ita ut multitudo terminorum iunctorum sit $1 + A - 2 = A - 1$. Numerus vero immediate sequens $2A - 1$ non amplius per tot terminos se produci patitur, quia est $2A - 1 = A(1) + 1(A - 1)$, unde ad eum producendum requiruntur termini $1 + A - 1 = A$; quocirca hucusque progressi habemus $\Theta = A$. Nondum enim ad tertium terminum B respicimus; si enim foret $B = 2A - 1$, vel adeo minor, tum haec ratio cessaret et praecedens valor $\Theta = A - 1$ adhuc subsisteret; sin autem tertius terminus B superet istum limitem $2A - 1$, tum certe statui debebit $\Theta = A$, unitate scilicet maior quam casu praecedente.

3. Removeamus autem tertium terminum B ulterius, et cum numerus $2A - 1$ requirat A terminos, evidens est numerum $3A - 1$ requisiturum esse $A + 1$ terminos, cum sit $3A - 1 = A + (2A - 1)$, quarum pars prior unum continet terminum, posterior vero A terminos; unde si B superet hunc

limitem $3A - 1$, ad eum usque habebimus $\Theta = A + 1$. Ulterius autem progrediendo numerus $4A - 1$ requiret terminos $A + 2$; numerus vero $5A - 1$ requiret terminos $A + 3$; atque in genere numerus $nA - 1$ requiret terminos $A + n - 2$, siquidem tertius terminus B illo fuerit maior.

4. His colligendis, si tertius terminus B contineatur inter binos limites modo assignatos, valorem numeri Θ concludimus sequenti modo:

Si B contineatur intra	erit Θ
$A - 1$ et $2A - 1$	$A - 1$
$2A - 1$ et $3A - 1$	A
$3A - 1$ et $4A - 1$	$A + 1$
$4A - 1$ et $5A - 1$	$A + 2$
.	.
.	.
.	.
$nA - 1$ et $(n + 1)A - 1$	$A + n - 2$.

Consequenter, si ponamus esse $B > nA - 1$, attamen $B < (n + 1)A - 1$, quia hinc sequitur $n < \frac{B+1}{A}$ et tamen $n > \frac{B+1}{A} - 1$, his valoribus substitutis fiet

$$\Theta < A - 2 + \frac{B+1}{A}$$

et tamen

$$\Theta > A - 3 + \frac{B+1}{A}.$$

Sufficit autem pro Θ sumere numerum integrum proxime minorem priori, vel proxime maiorem altera formula. Cum igitur usque ad terminum A fuerit $\Theta = A - 1$, usque ad B progrediendo hic valor augmentum accipiet, quod ita se habebit ex formula priore:

$$\Theta < A - 1 + \frac{B - A + 1}{A};$$

ex posteriore autem:

$$\Theta > A - 1 + \frac{B - 2A + 1}{A}.$$

5. Hucusque nostra investigatio feliciter successit; ut nunc ulterius progrediamur, ponamus numerum hactenus inventum $= \vartheta$, qui denotat, quot terminis opus est ad omnes numeros ab unitate usque ad terminum B producendos, ita ut sit vel

$$\vartheta < A - 1 + \frac{B - A + 1}{A},$$

vel

$$\vartheta > A - 1 + \frac{B - 2A + 1}{A},$$

quippe qui numeri tantum ex binis numeris initialibus 1 et A componuntur. Nunc autem admisso etiam tertio termino B, totidem terminis, vel pauciori-bus, iungendis, ultra B procedamus, donec perveniamus ad numerum $B + b$, quem non amplius ex ϑ terminis componere liceat, sed qui requirat $\vartheta + 1$ terminos; tum vero manifestum est, ulterius progrediendo numerum $2B + b$ requirere $\vartheta + 2$ terminos; similique modo porro numerus $3B + b$ requiret $\vartheta + 3$ terminos; numerus $4B + b$ vero $\vartheta + 4$ terminos; et in genere numerus $nB + b$ requiret $\vartheta + n$ terminos.

6. Quodsi ergo sequens terminus C non superet limitem $B + b$, numerus ϑ nullum accipiet augmentum; sin autem maior sit, neque tamen maior secundo limite $2B + b$, ad numerum ϑ unitas erit addenda; sin autem ulterius crescat, neque tamen limitem $3B + b$ superet, augmentum accedet $= 2$; unde palam est, si C excedat limitem $nB + b$, neque tamen ultra sequentem $(n + 1)B + b$[1]) crescat, augmentum fore $= n$. Sumamus ergo $C > nB - b$, quia erit $n < \frac{C - b}{B}$, ad hunc usque terminum C multitudo terminorum erit

$$= \vartheta + n < \vartheta + \frac{C - b}{B},$$

ubi scilicet numerum integrum proxime minorem capi oportet. Sin autem sumeremus formulam $\vartheta + \frac{C - B - b}{B}$, tum numerus integer proxime maior capi deberet; sicque ad hunc usque terminum C numerus noster quaesitus erit

$$\Theta = A - 1 + \frac{B - 2A + 1}{A} + \frac{C - B - b}{B},$$

ubi pro utraque fractione numerus integer proxime maior sumi debet.

1) Editio princeps: $(a + 1)B + b$. Correxit R. F.

7. Istum numerum denuo indicemus littera ϑ, atque ultra C progrediamur, tot vel paucioribus terminis iungendis, donec perveniamus ad numerum $C + c$, quem non amplius producere liceat, sed qui requirat $(\vartheta + 1)$ terminos, ac ratiocinium ut ante instituendo evidens est usque ad terminum sequentem D numerum illum ϑ augmentum capere $\frac{D-C-c}{C}$, si scilicet loco fractionis numerus integer proxime maior accipiatur; quocirca usque ad hunc terminum nanciscimur numerum nostrum quaesitum:

$$\Theta = A - 1 + \frac{B-2A+1}{A} + \frac{C-B-b}{B} + \frac{D-C-c}{C}.$$

8. Quodsi simili modo post terminum D pergamus usque ad numerum $D + d$, qui non amplius ex tot terminis componatur, sed uno plus requirat, tum usque ad terminum sequentem E praecedens valor litterae Θ insuper augmentum accipiet $= \frac{E-D-d}{D}$ sicque, quousque libuerit, ulterius procedere licet. Hic autem non est dissimulandum huiusmodi laborem non nisi summa cum molestia suscipi posse; quin etiam, quocunque iam fuerimus progressi, nunquam tamen certi esse poterimus de vero valore ipsius Θ, si progressio adeo in infinitum continuetur. Interim tamen, quousque has operationes produxerimus, semper tuto concludere poterimus pro serie in infinitum continuata verum valorem Θ certe non fore minorem eo, quem invenimus; ac si satis longe fuerimus progressi, plerumque iste valor inventus haud a veritate aberrabit.

9. Ceterum circa illas fractiones, quibus numerum Θ constitui invenimus, notari convenit, si quae earum vel evanescat vel adeo negativa evadat, tum eius valorem esse nullum, quantumvis etiam eius valor negativus fuerit magnus, quoniam ob terminos sequentes valor praecedens nunquam potest diminui; quando autem istae fractiones sunt positivae, quamdiu earum valores unitatem non superant, eae unitati aequales sunt reputandae; quando autem unitate sunt maiores, neque tamen binarium superent, pro iis 2 scribi oportet, et ita porro. Ex quo intelligere licet, quomodo ex aliquot terminis seriei initialibus verus valor ipsius Θ elici possit, etiamsi series in infinitum continuetur; hoc scilicet eveniet, si omnes fractiones sequentes evadant negativae.

10. Mirum vero non est hoc modo investigationem istam summis plerumque difficultatibus fore implicatam, quandoquidem hic rem nimis generaliter sumus complexi, neque ad ullam legem, qua termini seriei progrediantur, respeximus. Nullum enim est dubium, quin ipsa progressionis lex plurimum ad numerum Θ reperiendum conferat; quemadmodum vidimus in serie generali initio allata, quae omnes numeros figuratos in se complectitur, de qua adfirmare possumus, numerum Θ semper esse $= a + 2n - 2$; neque tamen adhuc patet quomodo haec determinatio adhuc generalior reddi possit. Ill. quidem BEGUELIN, hoc casu inductus, erat arbitratus simili lege pro omnibus plane seriebus algebraicis ab unitate incipientibus, quarum scilicet terminum generalem formula algebraica exhibere liceat, valorem ipsius Θ sequenti modo exhiberi posse: Sit series proposita 1, A, B, C, D, E etc. ad ordinem n referenda, et formentur inde successive series differentiarum omnium ordinum, quarum termini initiales sint respective a, b, c, d etc., ultimae vero differentiae ordinis n, quae sunt constantes, sint $= i$, ita ut multitudo numerorum a, b, c, ... i sit $= n$; tum vir laudatus putavit fore $\Theta = a + n - 1$, quae formula utique cum casu numerorum figuratorum congruit. Cum enim hic sit $a = A - 1$, pro illo casu nostrum a erit $n + a - 1$, cui si addatur ob ordinem seriei numerus $n - 1$, ipsa illa formula pro Θ data resultat.

11. Leviter attendenti autem facile erit eiusmodi casus excogitare, quibus ista regula refragetur, veluti evenit in hac serie:

	1, 2, 4, 7, 11, 16, 22, 29 etc.
cuius differentiae primae	1, 2, 3, 4, 5, 6, 7 etc.
et secundae	1, 1, 1, 1, 1, 1 etc.,

quae igitur est ordinis secundi, sive $n = 2$ et $a = 1$. Secundum regulam igitur deberet esse $\Theta = 2$; certum vero est ad producendos omnes numeros ad minimum ternis terminis istius seriei addendis opus esse. Deinceps vero vir Illustris significavit se, cum istam regulam perscriberet, omisisse fractionem insuper addendam, quae sit $\frac{i}{a}$, quam quidem semper negligere liceat, si fuerit unitate minor, quemadmodum id in omnibus numeris figuratis usu venit; quando autem ad unitatem vel ultra ascendat, tum eius valorem in integris, negligendo fractionem annexam, superaddi debere. Cum nunc nostro casu differentiae ultimae sint $i = 1$, erit $\frac{i}{a} = 1$, hincque fiet $\Theta = 3$, quod cum veri-

tate egregie consentit, et nunc quidem fatendum est hanc regulam emendatam non solum numeris figuratis, sed et innumeris aliis progressionum generibus satisfacere.

12. Interim tamen etiam infinita serierum genera exhibere licet, quibus haec regula fallit, id quod plurimum intererit adcuratius ostendisse. Incipiamus ergo a secundo ordine progressionum algebraicarum, cuius differentiae secundae iam sunt constantes, ita ut hi duo tantum numeri a et b occurrant, unde earum forma generalis erit:

$1,\ 1+a,\ 1+2a+b,\ 1+3a+3b,\ 1+4a+6b,\ 1+5a+10b$ etc.;

et cum sit $n=2$ et $i=b$, secundum regulam illam deberet esse $\Theta = a+1+\frac{b}{a}$, quod, uti iam notavimus, pro numeris polygonalibus, ubi $b=a-1$[1]), egregie convenit. Quin etiam locum habere deprehenditur, quoties numerus b non multum superat numerum a; statim enim ac fractio $\frac{b}{a}$ fit satis magna, facile ostendi potest hanc regulam a veritate esse aberraturam; namque si sumamus $a=1$ et $b=100$, ut habeatur haec progressio:

$$1,\ 2,\ 103,\ 304,\ 605,\ 1006,\ 1507,\ 2108,\ 2809^{2})\ \text{etc.},$$

pro qua regula illa dat $\Theta = 102$, si hanc seriem methodo initio exposita examinemus, usque ad tertium 103 colligimus $\Theta = 51$; ad quartum terminum 304 usque $\Theta = 52$; hinc porro ad sequentem 605 prodit tantum $\Theta = 53$; qui valor non amplius augetur, etiamsi ultra sequentem 1006 progrediamur; ex quo facile intelligitur ad terminos ulteriores usque progrediendo hunc numerum vix ultra 54 auctum iri, cum tamen secundum regulam memoratam esse deberet $\Theta = 102$; error autem multo magis enormis evadet, si loco b numeri maiores accipiantur.

13. Cum hoc casu error sit tantopere enormis, operae pretium erit pro valore $a=1$, unde oritur series

$$1,\ 2,\ 3+b,\ 4+3b,\ 5+6b,\ 6+10b,\ 7+15b,\ 8+21b\ \text{etc.}$$

loco b successive numeros continuo maiores assumere, et cuilibet harum

1) Editio princeps: $a-11$. Correxit R. F.
2) Editio princeps: 2810. Correxit R. F.

serierum numerum Θ, ex observationibus erutum, adscribere, ut cum valore regulae $\Theta = 2 + b$ comparari possit.

b	Series								Θ	error
1	1,	2,	4,	7,	11,	16,	22,	. . . .	3	0
2	1,	2,	5,	10,	17,	26,	37,	. . . .	4	0
3	1,	2,	6,	13,	23,	36,	52,	. . . .	4	1
4	1,	2,	7,	16,	29,	46,	67,	. . . .	5	1
5	1,	2,	8,	19,	35,	56,	82,	. . . .	5	2
6	1,	2,	9,	22,	41,	66,	97,	. . . .	6	2
7	1,	2,	10,	25,	47,	76,	112,	. . . .	6	3
8	1,	2,	11,	28,	53,	86,	127,	. . . .	7	3
9	1,	2,	12,	31,	59,	96,	142,	. . . .	7	4
10	1,	2,	13,	34,	65,	106,	157,	. . . .	8	4

Hinc igitur patet ab initio casibus $b = 1$ et $b = 2$ regulae errorem esse nullum, hinc vero continuo magis increscere; ac si hos valores attente consideremus, facile concludemus pro hoc serierum genere fore $\Theta = 3 + \frac{1}{2}b$, unde pro casu $b = 100$ fit $\Theta = 53$.

14. Consideremus simili modo genus, quo $a = 2$, nostraque series erit:

$1, 3, 5+b, 7+3b, 9+6b, 11+10b, 13+15b, 15+21b, 17+28b$ etc.,

pro qua regula Cel. BEGUELIN dat $\Theta = 3 + \frac{b}{2}$. Exponamus igitur sequentes series cum valoribus ipsius Θ ut ante:

b	Series								Θ	error
1	1,	3,	6,	10,	15,	21,	28,	. . . .	3	0
2	1,	3,	7,	13,	21,	31,	43,	. . . .	4	0
3	1,	3,	8,	16,	27,	41,	58,	. . . .	4	0
4	1,	3,	9,	19,	33,	51,	73,	. . . .	5	0
5	1,	3,	10,	22,	39,	61,	88,	. . . .	5	0
6	1,	3,	11,	25,	45,	71,	103,	. . . .	5	1
7	1,	3,	12,	28,	51,	81,	118,	. . . .	5	1
8	1,	3,	13,	31,	57,	91,	133,	. . . .	6	1
9	1,	3,	14,	34,	63,	101,	148,	. . . .	6	1
10	1,	3,	15,	37,	69,	111,	163,	. . . .	7	1

Sin autem sumamus $b = 100$, pro hac serie:

$$1, 3, 105, 307, 609, 1011, 1513, 2115 \text{ etc.}$$

colligimus $\Theta = 37$, cum ex illa regula esse deberet $\Theta = 53$.

15. Progrediamur nunc ad progressionum ordinem tertium, ubi $n = 3$, et ternae series differentiarum incipiant ab his numeris: a, b et c, ita ut $i = c$, et secundum regulam $\Theta = a + 2 + \frac{c}{a}$; ipsa igitur progressio erit:

$$1, 1 + a, 1 + 2a + b, 1 + 3a + 3b + c, 1 + 4a + 6b + 4c,$$
$$1 + 5a + 10b + 10c, 1 + 6a + 15b + 20c \text{ etc.}$$

atque hic statim merito suspectum videtur, quod valor ipsius Θ plane non pendeat a littera b; evidens enim est, si b fuerit numerus praemagnus, etiam numerum Θ non mediocriter auctum iri. Quin etiam in genere affirmare licet numerum Θ minorem certe esse non posse, quam si esset $c = 0$; hoc autem casu per eandem regulam foret $\Theta = a + 1 + \frac{b}{a}$; quare, quoties haec formula $a + 1 + \frac{b}{a}$ maior est quam $a + 2 + \frac{c}{a}$, regula ista necessario fallere debet, si fuerit $\frac{b}{a} > 1 + \frac{c}{a}$ sive $b > a + c$.

16. Ad hoc ostendendum sumamus $a = 2$, $c = 1$ et $b = 6$; unde haec series nascitur:

$$1, 3, 11, 26, 49, 81, 123, 176, 241 \text{ etc.},$$

pro qua esse deberet $\Theta = 4 + \frac{1}{2} = 4$, cum tamen numerus 21 non in pauciores quam 5 terminos distribui possit; error autem maior erit proditurus, quo magis numerus b augebitur.

17. Quemadmodum numerus b suppeditavit unum errorum fontem, ita etiam ex numero c, si capiatur satis magnus, errores insignes nascentur. Sumamus scilicet $a = 2$, $b = 1$, $c = 10$, ut prodeat ista series:

$$1, 3, 6, 20, 55, 121, 228 \text{ etc.}$$

ideoque per regulam $\Theta = 9$; tentanti autem mox patebit hunc valorem non superare 6; ex quo manifestum est pro maioribus numeris c errores adhuc maiores esse prodituros; ubi notasse iuvabit, si b fuerit numerus praeparvus, regulam errare in defectu; sin autem c fuerit numerus praemagnus, in excessu.

18. Tutissima igitur via quicquam certi in hac re concludendi erit sine dubio, ut plures huiusmodi casus tam ex secundo et tertio progressionum ordine, uti fecimus, quam etiam ex sequentibus omni studio explorentur, et qui hunc laborem suscipere voluerit, detegit fortasse regulam quandam latius patentem et certiorem, qua huiusmodi numerorum resolutiones definiri queant.

19. Forsitan etiam non parum iuvabit progressiones geometricas considerasse, pro quibus numerus noster Θ, quo ulterius progrediamur, magis increscit. Ita in progressione dupla $1, 2^1, 2^2, 2^3, 2^4, 2^5$ etc. si in termino 2^5 subsistamus, erit $\Theta = 5$; et in genere pro omnibus numeris usque ad 2^n fit $\Theta = n$; tum vero in progressione tripla $1, 3, 3^2, 3^3, 3^4$ etc. usque ad terminum 3^n numerus noster reperitur $\Theta = 2n$; atque in genere pro progressione $1, m, m^2, m^3, m^4, m^5, m^6$ etc. usque ad terminum m^n concluditur numerus $\Theta = (m-1)n$. Hic vero notandum differentiis continuis sumendis earum terminos primos fore $m-1$, $(m-1)^2$, $(m-1)^3$ etc., ita ut litterae supra usurpatae sint hic $a = m-1$, $b = (m-1)^2$, $c = (m-1)^3$, $d = (m-1)^4$ etc.; unde concludi posset fore $\Theta = \frac{a}{1} + \frac{b}{a} + \frac{c}{b} + \frac{d}{c} + \frac{e}{d}$ etc., haec autem regula in aliis casibus multum falleret. Quin etiam in progressione hypergeometrica Wallisii

$$1, 2, 6, 24, 120, 720, 5040 \text{ etc.}$$

usque ad terminum 6 est $\Theta = 3$; usque ad 24 est $\Theta = 6$; usque ad terminum $1.2.3. \ldots . n$ erit $\Theta = \frac{n(n-1)}{2}$.

20. Verum etiam series recurrentes memorabilia nobis suppeditant exempla pro numero Θ. Ita pro hac serie notissima:

Indices	0,	1,	2,	3,	4,	5,	6,	7,	8,
termini	1,	2,	3,	5,	8,	13,	21,	34,	55 etc.,

cuius quilibet terminus est summa duorum praecedentium, si usque ad terminum indice n signatum progrediamur, erit $\Theta = \frac{n}{2}$, ubi si n fuerit impar, fractio adiuncta pro unitate est reputanda. Ulteriorem huius argumenti disquisitionem mihi quidem suscipere non vacat.

NOVA SUBSIDIA PRO RESOLUTIONE FORMULAE $axx+1=yy$[1)]

Commentatio 559 indicis Enestroemiani
Opuscula analytica 1, 1783, p. 310—328
Conventui exhibita die 23. septembris 1773

1. Problema hoc, ab auctore Pellianum dictum, quo pro dato quocunque numero a, neque quadrato neque negativo, numeri quaeruntur x, ut formula $axx + 1$ fiat quadratum, iam saepius pertractavi methodumque tradidi, cuius ope multo facilius resolvi potest quam methodo ab ipso Pellio excogitata. Interim tamen evolutio eorum casuum, qui pro x numeros praegrandes postulant, cuiusmodi est casus $a = 61$, pro quo fit $x = 226153980$ et $y = 1766319049$[2)], etiam mea methodo succincta plurimas non parum taediosas operationes exigit; unde equidem non parum praestitisse mihi videor, dum aliam prorsus viam detexi hos ipsos praemagnos numeros mira facilitate inveniendi. Ante autem quam eam apperiam, circa indolem numerorum a, quos per minores numeros x et y resolvere licet, notasse iuvabit, quoties a fuerit numerus huius formae: $a = bbcc \pm 2b$, solutionem in promtu esse, si capiatur $x = c$, tum enim fit $y = bcc \pm 1$; tum vero etiam, si fuerit $a = bbcc \pm b$ et capiatur $x = 2c$, erit $y = 2bcc \pm 1$; unde plurimos casus sine ulteriori calculo expedire licebit, qui quidem etiam methodo Pelliana satis prompte resolvi possunt. Sequentia autem problemata ad casus magis abstrusos deducent.

1) Confer hac cum dissertatione commentationem 323 (indicis Enestroemiani): *De usu novi algorithmi in problemate Pelliano solvendo*, Novi comment. acad. sc. Petrop. 11 (1765), 1767, p. 28—66, *Leonhardi Euleri Opera omnia*, series I, vol. 3, p. 73—111 et praefationem in eodem volumine adiectam p. XV—XVIII. R. F.

2) Vide commentationem in nota 1 laudatam, § 39, IV, p. 107 huius editionis. R. F.

PROBLEMA 1

2. *Si fuerit* $app - 1 = qq$, *invenire numeros* x *et* y, *ut fiat* $axx + 1 = yy$.

SOLUTIO

Ex proposita formula erit $app = qq + 1$, unde per $4qq$ multiplicando et unitatem addendo orietur $4appqq + 1 = 4q^4 + 4qq + 1 = (2qq + 1)^2$. Hinc igitur pro solutione problematis consequimur $x = 2pq$ et $y = 2qq + 1$.

COROLLARIUM 1

3. Quoties ergo evenit, ut fiat $app - 1$[1]) quadratum, facile inveniri potest x, ut haec formula $axx + 1$ fiat quadratum. Ita si fuerit $a = 5$, ob $5 \cdot 1^2 - 1 = 2^2$ erit hic $p = 1$ et $q = 2$, unde fit $x = 4$ et $y = 9$.

COROLLARIUM 2

4. Hoc autem tantum pro iis numeris a locum habere potest, qui sunt summae duorum quadratorum; caeterum haec proprietas iam ipsi PELLIO cognita fuisse videtur[2]). Hinc autem sequens problema inversum, quo ipsi isti numeri quaeruntur, evolvam.

PROBLEMA 2

5. *Investigare numeros* a, *pro quibus fieri potest* $app - 1 = qq$, *hincque ipsos numeros* x *et* y *assignare, ut fiat* $axx + 1 = yy$.

SOLUTIO

Cum debeat esse $app = qq + 1$, erit $a = \frac{qq + 1}{pp}$, sicque pro p et q eiusmodi numeri quaeri debent, ut haec fractio praebeat numerum integrum.

---

1) Editio princeps: $app + 1$. Correxit R. F.

2) Vide notam 1, p. 77, vol. 3 seriei I adiectam. Correxit R. F.

Quia igitur tam pp quam p debet esse summa duorum quadratorum[1]), statuatur

$$pp = bb + cc \text{ et } qq + 1 = (bb + cc)(ff + gg),$$

ut fiat $a = ff + gg$. Iam vero erit $q = bf + cg$ et $\pm 1 = bg - cf$. Ex datis ergo numeris b et c alteri f et g ita accipi debent, ut fiat $bg - cf = \pm 1$, quod quidem infinitis modis facile fieri potest. Tum igitur erit $q = bf + cg$, et quia numerus p ut datus spectatur, hinc concludimus fore $x = 2pq$ et $y = 2qq + 1$, quarum formularum usus quo clarius appareat, sequentia exempla adiiciemus, dum pro p nonnullos numeros, qui quidem sint summae duorum quadratorum, assumemus.

EXEMPLUM 1

6. Sit $p = 5$, erit $pp = 25 = bb + cc$, unde fit $b = 3$ et $c = 4$, tum ergo f et g tales sumi debent, ut fiat $3g - 4f = \pm 1$, indeque habebimus $a = ff + gg$ et pro hoc numero $q = 3f + 4g$, ac denique $x = 10q$ et $y = 2qq + 1$. Huiusmodi autem valores pro litteris f et g in sequenti tabella exhibemus:

$$4f - 3g = \pm 1.$$

f	1	2	4	5	7	8
g	1	3	5	7	9	11
a	2	13	41	74	130	185
q	7	18	32	43	57	68
x	70	180	320	430	570	680
y	99	649	2049	3699	6499	9249

In hac tabula occurrunt ergo casus alioquin non parum difficiles.

EXEMPLUM 2

7. Sit $p = 13$, ideoque $pp = 169 = 5^2 + 12^2$, unde fit $b = 5$ et $c = 12$. Nunc primo habetur ista aequatio: $12f - 5g = \pm 1$; tum vero erit $a = ff + gg$ et $q = 5f + 12g$, unde fit $x = 26q$ et $y = 2qq + 1$. Casus ergo hinc oriundos in sequenti tabula exhibemus:

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—13, *Leonhardi Euleri Opera omnia*, series I, vol. 2, p. 328—372. R. F.

$$12f - 5g = \pm 1.$$

f	2	3	7	8
g	5	7	17	19
a	29	58	338	425
q	70	99	239	268
x	1820	2574	6214	6968
y	9801	19603	114243	143649

EXEMPLUM 3

8. Sit $p = 17$, ideoque $pp = 289 = 8^2 + 15^2$, ergo $b = 8$ et $c = 15$, unde prima aequatio adimplenda erit $15f - 8g = \pm 1$, quo facto fiet $a = ff + gg$ et $q = 8f + 15g$, hincque porro $x = 34q$ et $y = 2qq + 1$. Casus hinc oriundos sequens tabula ostendit:

$$15f - 8g = \pm 1.$$

f	1	7
g	2	13
a	5	218
q	38	251
x	1292	8534
y	2889	126003

EXEMPLUM 4

9. Sit $p = 25$, hinc $pp = 625 = 7^2 + 24^2$, unde $b = 7$ et $c = 24$. Iam habetur ista aequatio: $24f - 7g = \pm 1$, ex qua prodit $a = ff + gg$, $q = 7f + 24g$ et $x = 2pq = 50q$ atque $y = 2qq + 1$. Hinc unicum casum evolvamus, quo $f = 2$ et $g = 7$, hinc oritur $a = 53$, tum vero fit $q = 182$, ergo $x = 9100$ et $y = 66249$.

PROBLEMA 3

10. *Si fuerit* $app - 2 = qq$, *invenire numeros* x *et* y, *ut fiat* $axx + 1 = yy$.

SOLUTIO

Cum igitur sit $app = qq + 2$, multiplicemus utrinque per qq, et adiecta unitate erit

$$appqq + 1 = q^4 + 2qq + 1,$$

unde manifesto colligitur $x = pq$ et $y = qq + 1$.

PROBLEMA 4

11. *Investigare numeros a, pro quibus fieri potest $app - 2 = qq$, hincque ipsos numeros x et y assignare, ut fiat $axx + 1 = yy$.*

SOLUTIO

Cum debeat esse $app = qq + 2$, erit $a = \frac{qq+2}{pp}$, sicque pro p et q eiusmodi numeri quaeri debent, ut illa fractio praebeat numerum integrum. Quia autem formula $qq + 2$ alios divisores non admittit, nisi qui habeant formam $bb + 2cc$[1]), etiam pro p alios numeros accipere non licet, nisi qui sint eiusdem formae, quocirca ponamus statim $pp = bb + 2cc$, fiatque

$$qq + 2 = (bb + 2cc)(ff + 2gg),$$

ut obtineatur $a = ff + 2gg$, tum vero esse oportet $cf - bg = \pm 1$, hincque orietur $q = bf + 2cg$, ac tandem $x = pq$ et $y = qq + 1$. At forma $bb + 2cc$ alios divisores primos non admittit, nisi qui sint vel huius formae: $8n + 1$, vel huius: $8n + 3$, qui ergo ita progrediuntur: 3, 11, 17, 19, 41, 43 etc. et qui ex his componuntur, quamobrem sequentia exempla percurramus.

EXEMPLUM 1

12. Sit $p = 3$, hinc $pp = 9 = 1^2 + 2 \cdot 2^2$, unde fit $b = 1$ et $c = 2$; aequatio ergo resolvenda est $2f - g = \pm 1$, quo facto erit $a = ff + 2gg$,

1) Vide commentationem 256 (indicis Enestroemiani): *Specimen de usu observationum in mathesi pura*, Novi comment. acad. sc. Petrop. 6 (1756/7), 1761, p. 185—230, *Leonhardi Euleri Opera omnia*, series I, vol. 2, p. 459—492. R. F.

$q = f + 4g$ atque hinc $x = 3q$ et $y = qq + 1$. Casus hinc oriundos sequens tabula complectitur:

$$2f - g = \pm 1.$$

f	1	1	2	2	3	3	4
g	1	3	3	5	5	7	7
a	3	19	22	54	59	107	114
q	5	13	14	22	23	31	32
x	15	39	42	66	69	93	96
y	26	170	197	485	530	962	1025

EXEMPLUM 2

13. Sit $p = 9$, erit $pp = 81 = 7^2 + 2 \cdot 4^2$, ideoque $b = 7$ et $c = 4$; hinc aequatio nostra $4f - 7g = \pm 1$; tum vero erit $a = ff + 2gg$ et $q = 7f + 8g$, hincque porro $x = 9q$ et $y = qq + 1$. Ecce ergo casus, qui hinc oriuntur:

$$4f - 7g = \pm 1.$$

f	2	5	9	12
g	1	3	5	7
a	6	43	131	242
q	22	59	103	140
x	198	531	927	1260
y	485	3482	10610	19601

EXEMPLUM 3

14. Sit $p = 11$, erit $pp = 121 = 7^2 + 2 \cdot 6^2$, ideoque $b = 7$ et $c = 6$, ergo aequatio nostra $6f - 7g = \pm 1$, tum vero $a = ff + 2gg$ et $q = 7f + 12g$, unde $x = 11q$ et $y = qq + 1$. Casus ergo erunt:

$$6f - 7g = \pm 1.$$

f	1	6	8
g	1	5	7
a	3	86	162
q	19	102	140
x	209	1122	1540
y	362	10405	19601

EXEMPLUM 4

15. Sit $p = 17$, erit $pp = 289 = 1^2 + 2 \cdot 12^2$, sicque $b = 1$ et $c = 12$, unde aequatio $12f - g = \pm 1$, tum vero habebimus $a = ff + 2gg$, $q = f + 24g$, $x = 17q$ et $y = qq + 1$, unde duos casus notasse sufficiet:

$f = 1$, $g = 11$, $a = 243$, $q = 265$, $x = 4505$ et $y = 265^2 + 1$,
$f = 1$, $g = 13$, $a = 339$, $q = 313$, $x = 17 \cdot 313$ et $y = 313^2 + 1$.

EXEMPLUM 5

16. Sit $p = 19$, erit $pp = 361 = 17^2 + 2 \cdot 6^2$, ideoque $b = 17$ et $c = 6$, et aequatio erit $6f - 17g = \pm 1$, hinc fiet

$$a = ff + 2gg,\ q = 17f + 12g,\ x = 19q \text{ et } y = qq + 1,$$

unde sequentes casus nascuntur:

Si $f = 3$ et $g = 1$, erit $a = 11$, $q = 63$, $x = 1197$ et $y = 3970$[1]).
Si $f = 14$ et $g = 5$, erit $a = 246$, $q = 298$, $x = 5662$, $y = 298^2 + 1$.

PROBLEMA 5

17. *Si fuerit* $app + 2 = qq$, *invenire numeros* x *et* y, *ut fiat* $axx + 1 = yy$.

SOLUTIO

Cum sit $app = qq - 2$, manifestum est fore $x = pq$ et $y = qq - 1$, unde ad sequens problema progredimur.

PROBLEMA 6

18. *Investigare numeros* a, *pro quibus fieri possit* $app + 2 = qq$, *hincque numeros* x *et* y *assignare, ut fiat* $axx + 1 = yy$.

---

1) Editio princeps: 3969. Correxit R. F.

SOLUTIO

Ex aequatione $app + 2 = qq$ deducitur $a = \frac{qq-2}{pp}$, ita ut pp debeat esse divisor formulae $qq - 2$, id quod evenire nequit, nisi sit pp ideoque et p numerus formae $bb - 2cc$. Hanc ob rem statuamus $pp = bb - 2cc$ et $qq - 2 = (bb - 2cc)(ff - 2gg)$, quod ut fieri possit, debet esse $cf - bg = \pm 1$; tum vero erit $q = bf - 2cg$ et $a = ff - 2gg$, atque habebimus $x = pq$ et $y = qq - 1$. Nunc vero observari convenit pro p alios numeros primos accipi non posse, nisi in alterutra harum formularum: $8n + 1$ et $8n - 1$ contentos. Quod si iam sumeretur $p = 1$, foret $a = qq - 2$, qui est casus per se notissimus, fieretque $x = q$ et $y = qq - 1$, quare ad sequentia exempla progredimur.

EXEMPLUM 1

19. Sit $p = 7$, erit $pp = 49 = 9^2 - 2 \cdot 4^2$, hinc $b = 9$ et $c = 4$, ergo aequatio nostra $4f - 9g = \pm 1$; tum vero erit $a = ff - 2gg$ et $q = 9f - 8g$, $x = 7q$ et $y = qq - 1$, unde casus sequentes evolvamus:

1°. $f = 2$, $g = 1$, $a = 2$, $q = 10$, $x = 70$ et $y = 99$,
2°. $f = 7$, $g = 3$, $a = 31$, $q = 39$, $x = 273$ et $y = 1520$,
3°. $f = 11$, $g = 5$, $a = 71$, $q = 59$, $x = 413$ et $y = 3480$,
4°. $f = 16$, $g = 7$, $a = 158$, $q = 88$, $x = 616$ et $y = 7743$ [1]).

Hic autem notari debet omnes numeros formae $bb - 2cc$ infinitis modis in eadem forma contineri posse. Ita manente $p = 7$ erit quoque $pp = 49 = 11^2 - 2 \cdot 6^2$, ita ut nunc sit $b = 11$ et $c = 6$, sicque nostra aequatio erit $6f - 11g = \pm 1$, tum vero ut ante $a = ff - 2gg$, at vero $q = 11f - 12g$ et $x = 7q$ atque $y = qq - 1$. Hinc sequentes casus evolvamus:

1°. $f = 2$, $g = 1$, $a = 2$, $q = 10$, $x = 70$ et $y = 99$,
2°. $f = 9$, $g = 5$, $a = 31$, $q = 39$, $x = 273$ et $y = 1520$;

hinc autem manifestum est eosdem casus esse prodituros, quos iam ante invenimus.

---

1) Editio princeps: 1744. Correxit R. F.

EXEMPLUM 2

20. Sit $p = 17$, erit $pp = 289 = 19^2 - 2 \cdot 6^2$, unde nostra aequatio fit $6f - 19g = \pm 1$, tum vero erit $a = ff - 2gg$, $q = 19f - 12g$ et $x = 17q$ et $y = qq - 1$.

1°. $f = 3$, $g = 1$, $a = 7$, $q = 45$, $x = 765$ et $y = 2024$,
2°. $f = 16$, $g = 5$, $a = 206$, $q = 244$, $x = 4148$ et $y = 244^2 - 1$.

EXEMPLUM 3

21. Sit $p = 23$, erit $pp = 529 = 27^2 - 2 \cdot 10^2$, ideoque $b = 27$ et $c = 10$. Aequatio ergo nostra erit $10f - 27g = \pm 1$, hincque $a = ff - 2gg$, $q = 27f - 20g$, $x = 23q$ et $y = qq - 1$. Hinc si $f = 8$, erit $g = 3$, $a = 46$, $q = 156$, $x = 3588$ et $y = 156^2 - 1$.

PROBLEMA 7

22. *Si fuerit* $app+4=qq$, *invenire numeros* x *et* y, *ut fiat* $axx+1=yy$.

SOLUTIO

Quia numerus 4 est quadratum, erit in forma desiderata $\frac{app}{4} + 1 = \frac{qq}{4}$, ita ut iam esset $x = \frac{p}{2}$ et $y = \frac{q}{2}$, si quidem essent p et q numeri pares, qui ergo casus foret maxime obvius. At si p et q sint numeri impares, notandum est ex hoc casu concludi posse secundum praecepta cognita hunc secundum casum: $x = \frac{pq}{2}$ et $y = \frac{qq}{2} - 1$, qui numeri autem etiamnum sunt fracti[1]). Hinc autem tertius casus deducatur, dum valores secundi casus per q multiplicantur et primi subtrahuntur, hinc autem prodibit

$$x = p\left(\frac{qq-1}{2}\right) \quad \text{et} \quad y = q\left(\frac{qq-3}{2}\right),$$

qui ambo valores ob q numerum imparem erunt integri, quocirca hanc sumus adepti solutionem problematis, ut sit $x = p\left(\frac{qq-1}{2}\right)$ et $y = q\left(\frac{qq-3}{2}\right)$.

1) i. e. in casu secundo p numerus impar, q numerus par est; solutio erit $x = \frac{pq}{2}$, $y = \frac{qq}{2} - 1$. In casu tertio p et q numeri impares sunt; solutio erit $x = p\frac{qq-1}{2}$, $y = q\frac{qq-3}{2}$. R. F.

COROLLARIUM

23. Si ergo fuerit $a = bb - 4$, capi poterit $p = 1$, eritque $q = b$, hincque $x = \frac{bb-1}{2}$ et $y = b\left(\frac{bb-3}{2}\right)$, ubi quidem pro b numeros impares accipi oportet, unde sequentes casus evolvisse iuvabit:

1°. Sit $b = 3$, erit $a = 5$ et $x = 4$ atque $y = 9$,
2°. sit $b = 5$, erit $a = 21$, hinc $x = 12$ atque $y = 55$,
3°. sit $b = 7$, erit $a = 45$, hinc $x = 24$ atque $y = 161$,
4°. sit $b = 9$, erit $a = 77$ et $x = 40$ atque $y = 351$,
5°. sit $b = 11$, erit $a = 117$ et $x = 60$ atque $y = 649$.

PROBLEMA 8

24. *Investigare numeros a, pro quibus fieri possit $app + 4 = qq$, hincque numeros x et y assignare, ut fiat $axx + 1 = yy$.*

SOLUTIO

Cum hinc sit $app = qq - 4$, fiet $a = \frac{qq-4}{pp}$, ubi pro p omnes numeros impares accipere licet, quandoquidem numerator $qq - 4$ est differentia duorum quadratorum. Semper igitur statui poterit $pp = bb - cc$, ponendo $b = \frac{pp+1}{2}$ et $c = \frac{pp-1}{2}$; tum vero fiat $qq - 4 = (bb - cc)(ff - gg)$, ut hinc oriatur $a = ff - gg$; ad hoc vero requiritur, ut sit $cf - bg = \pm 2$ et $q = bf - cg$, quo facto reperietur $x = p\left(\frac{qq-1}{2}\right)$ et $y = q\left(\frac{qq-3}{2}\right)$. Hinc ergo sequentia exempla evolvamus.

EXEMPLUM 1

25. Sumatur $p = 3$, fietque $b = 5$ et $c = 4$, hinc $4f - 5g = \pm 2$, porro $a = ff - gg$, $q = 5f - 4g$, $x = 3\left(\frac{qq-1}{2}\right)$ et $y = q\left(\frac{qq-3}{2}\right)$; unde casus sequentes consideremus:

1°. $f = 2$, $g = 2$, hinc $a = 0$, unde ergo nihil sequitur.
2°. $f = 3$, $g = 2$, hinc $a = 5$, $q = 7$, $x = 72$ et $y = 161$.

3°. $f = 7$, $g = 6$, hinc $a = 13$, $q = 11$, $x = 180$ et $y = 649$.

4°. $f = 8$, $g = 6$, hinc $a = 28$, $q = 16$, $x = 3 \cdot \frac{255}{2}$, qui casus inutilis.

5°. $f = 12$, $g = 10$, unde pariter nihil colligitur, necesse enim est, ut numerus f sit impar.

6°. $f = 13$ et $g = 10$, unde $a = 69$, $q = 25$, ergo $x = 936$ et $y = 7775$.

7°. $f = 17$ et $g = 14$, unde $a = 93$, $q = 29$, ergo $x = 1260$ et $y = 12151$.

8°. $f = 23$ et $g = 18$, unde $a = 205$, $q = 43$, ergo $x = 2772$ et $y = 39689$.

Hic quoque valor ipsius q in genere assignari potest ex unico valore cognito $q = 2$. Ponatur enim $q = 9n \pm 2$, eritque $qq - 4 = 81nn \pm 36n$, unde fit $a = 9nn \pm 4n$, tum vero erit

$$x = 3\left(\frac{81nn \pm 36n + 3}{2}\right) \text{ et } y = (9n \pm 2)\left(\frac{81nn \pm 36n + 1}{2}\right),$$

ubi pro n quemlibet numerum imparem assumere licet.

EXEMPLUM 2

26. Sit $p = 5$, eritque $b = 13$ et $c = 12$, ideoque $12f - 13g = \pm 2$, unde fit $a = ff - gg$ et $q = 13f - 12g$, $x = 5\left(\frac{qq-1}{2}\right)$ atque $y = q\left(\frac{qq-3}{2}\right)$, ubi iterum f debet esse numerus impar. Sit

1°. $f = 11$ et $g = 10$, hinc $a = 21$, $q = 23$, $x = 1320$ et $y = 6049$.

2°. $f = 15$ et $g = 14$, hinc $a = 29$, $q = 27$, $x = 1820$ et $y = 9801$.

Statim autem sine litterarum f et g ope statui poterit $q = 25n \pm 2$, eritque $a = 25nn \pm 4n$; tum vero ut ante erit $x = 5\left(\frac{qq-1}{2}\right)$ et $y = q\left(\frac{qq-3}{2}\right)$[1]; atque hic iam pro n quosvis numeros impares assumere licet, quorum singuli ob signum ambiguum binas dabunt solutiones.

1°. Si $n = 1$ erit $a = 25 \pm 4$ et $q = 25 \pm 2$.

2°. Si $n = 3$ erit $a = 225 \pm 12$ et $q = 75 \pm 2$.

3°. Si $n = 5$ erit $a = 625 \pm 20$ et $q = 125 \pm 2$.

4°. Si $n = 7$ erit $a = 1225 \pm 28$ et $q = 175 \pm 2$.

---

1) Editio princeps: $y = \left(\frac{qq-3}{2}\right)$. Correxit R. F.

EVOLUTIO GENERALIS

27. Si p fuerit numerus impar quicunque, sumatur $q = npp \pm 2$, eritque $a = \frac{qq-4}{pp} = nnpp \pm 4n$, tum vero habebitur $x = p\left(\frac{qq-1}{2}\right)$, $y = q\left(\frac{qq-3}{2}\right)$, quae unica solutio locum habet, quando p erit numerus primus; verum si p involvat factores inter se primos, aliae insuper solutiones locum habere possunt. Sit enim $p = rs$, fierique poterit $pp = rrss = bb - cc$, sumendo $b = \frac{rr+ss}{2}$ et $c = \frac{rr-ss}{2}$; tum quaerantur numeri f et g, ut fiat $cf - bg = \pm 2$ et statuatur $bf - cg = k$, eritque $kk - 4 = (bb - cc)(ff - gg)$ $= rrss(ff - gg)$, hincque $\frac{kk-4}{pp} = ff - gg$. Iam sumatur $q = npp \pm k$, ac reperietur $a = \frac{qq-4}{pp} = nnpp \pm 2nk + ff - gg$[1]), atque hic iterum erit $x = p\left(\frac{qq-1}{2}\right)$ et $y = q\left(\frac{qq-3}{2}\right)$.

Veluti si fuerit $p = 15 = 5 \cdot 3$, sive $r = 5$ et $s = 3$, priori modo statim habetur $q = 225n \pm 2$, hincque $a = 225nn \pm 4n$, ex posteriore vero solutione habemus $b = 17$[2]) et $c = 8$, nuncque fiet $8f - 17g = \pm 2$, sumendo $f = 4$ et $g = 2$, ideoque $ff - gg = 12$ et $k = 52$. Si ergo capiatur $q = 225n \pm 52$, prodibit $a = 225nn \pm 104n + 12$, tum vero pro utroque casu erit $x = 15\left(\frac{qq-1}{2}\right)$ et $y = q\left(\frac{qq-3}{2}\right)$.

PROBLEMA 9

28. *Si fuerit* $arr - 4 = ss$, *invenire numeros* x *et* y, *ut fiat* $axx + 1 = yy$.

SOLUTIO

Cum sit $arr = ss + 4$, multiplicando per ss et 4 addendo prodit $arrss + 4$[3]) $= s^4 + 4ss + 4 = (ss + 2)^2$, sicque ad casum praecedentem revolvimur, quo erat $app + 4 = qq$; erit scilicet nunc $p = rs$ et $q = ss + 2$, ex quibus valoribus colligimus ut ante $x = p\left(\frac{qq-1}{2}\right)$ et $y = q\left(\frac{qq-3}{2}\right)$.

1) Editio princeps: $nn\,pp \pm 2hk + ff - gg$, Correxit R. F.
2) Editio princeps: $d = 17$. Correxit R. F.
3) Editio princeps: $rrss + 4$. Correxit R. F.

COROLLARIUM

29. Hic ante omnia occurrit casus quo $a = ee + 4$, denotante e numerum imparem quemcunque, pro quo erit $r = 1$ et $s = e$. Hinc igitur fiet $p = e$ et $q = ee + 2$, hincque porro $x = p\left(\frac{qq-1}{2}\right)$ et $y = q\left(\frac{qq-3}{2}\right)$, unde sequentes casus evolvamus:

Sit 1°. $e = 1$, erit $a = 5$, $p = 1$, $q = 3$, ideoque $x = 4$ et $y = 9$,
2°. $e = 3$, erit $a = 13$, $p = 3$, $q = 11$, unde $x = 180$ et $y = 649$,
3°. $e = 5$, erit $a = 29$, $p = 5$, $q = 27$, ergo $x = 1820$ et $y = 9801$,
4°. $e = 7$, erit $a = 53$, $p = 7$, $q = 51$, ergo $x = 9100$ et $y = 66249$,
5°. $e = 9$, erit $a = 85$, $p = 9$, $q = 83$, ergo $x = 30996$ et $y = 285769$.

PROBLEMA 10

30. *Investigare reliquos numeros, ut fieri possit* $arr - 4 = ss$, *indeque assignare numeros* x *et* y, *ut fiat* $axx + 1 = yy$.

SOLUTIO

Cum sit $arr = ss + 4$, erit $a = \frac{ss+4}{rr}$; unde patet pro r alios numeros impares assumi non posse, nisi qui sint summae duorum quadratorum. Sit igitur $rr = bb + cc$ et ponatur $ss + 4 = (bb + cc)(ff + gg)$, quem in finem esse oportet $cf - bg = \pm 2$, tum vero erit $s = bf + cg$; ex cognitis autem numeris r et s erit $p = rs$ et $q = ss + 2$, unde porro concluditur $x = p\left(\frac{qq-1}{2}\right)$ et $y = q\left(\frac{qq-3}{2}\right)$; pro r ergo alios numeros accipere non licet, nisi vel 5 vel 13 vel 17 vel 25 vel 29 etc., quos casus in sequentibus exemplis evolvemus.

EXEMPLUM 1

31. Sit $r = 5$, ideoque $rr = 25 = 4^2 + 3^2$, unde $b = 4$ et $c = 3$. Hinc esse debet $3f - 4g = \pm 2$, tum vero fit $a = ff + gg$ et $s = 4f + 3g$, unde solutio conficitur ut ante.

1°. Sit $f = 2$ et $g = 1$, erit $a = 5$, $s = 11$, hincque porro $p = 55$ et $q = 123$,

unde pro x et y ingentes prodeunt numeri problemati satisfacientes, sed non minimi.

2°. Si $f = 2$ et $g = 2$, erit $a = 8$; casus autem, quibus a numerus par[1]), hic excludimus.

3°. Sit $f = 6$ et $g = 5$, erit $a = 61$, tum vero $s = 39$, hincque porro $p = 195$ et $q = 1523$; atque hinc concluduntur valores $x = 226153980$ et $y = 1766319049$[2]).

Ex casu autem primo, quo erat $s = 11$ et $\frac{11^2 + 4}{25} = 5$, statim poni potest $s = 25n \pm 11$, unde deducitur $a = 25nn \pm 22n + 5$; tum vero erit $p = 5(25n \pm 11)$ et $q = (25n \pm 11)^2 + 2$, unde denique deducitur $x = p\left(\frac{qq-1}{2}\right)$ et $y = q\left(\frac{qq-3}{2}\right)$. Hinc autem suffecerit valores numeri a derivasse, ubi quidem pro n[3]) numeros pares sumi oportet, ne a prodeat numerus par.

1°. Si $n = 0$, fit $a = 5$,

2°. si $n = 2$, fit vel $a = 61$ vel $= 149$,

3°. si $n = 4$, fit vel $a = 317$ vel $a = 493$,

pro his ergo casibus numeri x et y in immensum excrescent.

EXEMPLUM 2

32. Sit nunc $r = 13$, erit $rr = 169 = 12^2 + 5^2$, unde $b = 12$ et $c = 5$, ita ut fieri debeat $5f - 12g = \pm 2$, tum vero erit $a = ff + gg$ et $s = 12f + 5g$. Casus autem simplicissimus est $f = 2$ et $g = 1$, qui praebet $a = 5$ et $s = 29$, ex quo statim generaliter statui potest $s = 169n \pm 29$, unde deducitur $a = 169nn \pm 58n + 5$, pro quo numero fiet $p = 13(169n \pm 29)$[4]) et $q = (169n \pm 29)^2 + 2$, unde denique colligitur $x = p\left(\frac{qq-1}{2}\right)$ et $y = q\left(\frac{qq-3}{2}\right)$. At pro n numeros pares accipi oportet, ut quidem fiat a numerus impar.

1°. Si $n = 0$ fit $a = 5$ et $s = 29$, hincque $p = 13 \cdot 29$, qui autem casus per se est notus.

2°. Sit $n = 2$, erit vel $a = 565$ vel $a = 797$.

1) Editio princeps: impar. Correxit R. F.

2) vide notam[2]) p. 76 huius voluminis. Correxit R. F.

3) Editio princeps: p. Correxit R. F.

4) Editio princeps: $p = 13(179n \pm 29)$. Correxit R. F.

EXEMPLUM 3

33. Sit $r = 17$ et $rr = 289 = 15^2 + 8^2$, unde $b = 15$ et $c = 8$, fierique debet $8f - 15g = \pm 2$, hincque $a = ff + gg$ et $s = 15f + 8g$. Pro casu simplicissimo sumamus $f = 4$ et $g = 2$, unde fit $a = 20$ et $s = 76$; pro solutione ergo generali ponamus $s = 289n \pm 76$, fietque

$$a = 289nn \pm 152n + 20,$$

ubi pro n numeros impares capi convenit.

1°. Si $n = 1$, fiet $a = 309 \pm 152$ et $s = 289 \pm 76$, qui valores iam nimis sunt magni, quam quos operi pretium sit evolvisse.

EXEMPLUM 4

34. Sit $r = 25$ et $rr = 625 = 24^2 + 7^2$, ideoque $b = 24$ et $c = 7$. Iam esse debet $7f - 24g = \pm 2$, hincque erit $a = ff + gg$ et $s = 24f + 7g$. Casus simplicissimus dat $f = 10$ et $g = 3$, hincque $a = 109$ et $s = 261$; unde si statuatur $s = 625n \pm 261$, reperietur generatim $a = 625nn \pm 522n + 109$. Evolvamus autem numerice casum $a = 109$, qui methodo vulgari molestissimos calculos requirit; cum ergo sit $s = 261$, ob $r = 25$ erit $p = 6525$ et $q = 261^2 + 2 = 68123$, ex quibus desiderati numeri maximi deducuntur

$$x = 6525\left(\frac{68123^2 - 1}{2}\right) = 15140424455100,$$
$$y = 68123\left(\frac{68123^2 - 3}{2}\right) = 158070671986249.$$

EXEMPLUM 5

35. Sit $r = 29$ et $rr = 841 = 21^2 + 20^2$, ideoque $b = 21$ et $c = 20$, fierique debet $20f - 21g = \pm 2$, hinc erit $a = ff + gg$ et $s = 21f + 20g$. Casu autem simplicissimo erit $f = 2$ et $g = 2$, hinc $a = 8$ et $s = 82$; statuatur ergo $s = 841n \pm 82$, fietque $a = 841nn \pm 164n + 8$, unde autem numeri vehementer magni nascuntur.

Ex his igitur abunde perspicitur, quemadmodum ope horum subsidiorum casus problematis Pelliani alioquin difficillimi satis expedite resolvi queant.

MISCELLANEA ANALYTICA

Commentatio 560 indicis ENESTROEMIANI
Opuscula analytica 1, 1783, p. 329—344
[Conventui exhibita die 15. novembris 1773]

I. THEOREMA A CLARISSIMO WARING SINE DEMONSTRATIONE PROPOSITUM[1])

Si n fuerit numerus primus, hoc productum continuum: $1 \cdot 2 \cdot 3 \cdot \cdots \cdot (n-1)$, *unitate auctum, semper dividi potest per illum numerum primum n.*

DEMONSTRATIO

Quanquam illustris Geometra DE LAGRANGE iam geminam huius theorematis demonstrationem in novis Actis Academiae regiae scientiarum borussicae dedit[2]), Geometris haud ingratum fore arbitror, si etiam meam demonstrationem more mihi familiari communicavero. Proposito autem quocunque numero primo n alio loco ostendi[3]), quod quidem quilibet facile largietur, semper dari huiusmodi numeros, quorum singulae potestates, exponentem minorem quam $n-1$ habentes, per n divisae, diversa praebeant residua. Sit igitur a huiusmodi numerus, cuius singulae potestates

1) *Meditationes algebraicae* ab EDUARDO WARING, Cantabrigiae 1770; editio tertia 1782, p. 380, problema LXIII, 5. Theorema a Waring propositum hodie Theorema WILSONIANUM nominatur. Vide GAUSS, *Disquisiones arithmeticae*, Lipsiae 1801, art. 76, C. F. GAUSS *Werke*, I, p. 60. R. F.

2) J. L. LAGRANGE: *Démonstration d'un théorème nouveau concernant les nombres premiers*, Nouv. mém. de l'acad. r. d. sc. de Berlin (1771), 1773, p. 125. *Oeuvres de* LAGRANGE, publiées par les soins de M. I.-A. Serret, t. III, p. 425. R. F.

3) Vide commentationem 449 (indicis ENESTROEMIANI): *Demonstrationes circa residua ex divisione potestatum per numeros primos*, Novi Comm. acad. sc Petrop. 18 (1773), 1774, p. 85—135; *LEONHARDI EULERI Opera omnia*, I, vol. 3, p. 240, praecipue theorema p. 256. R. F.

$$a^0,\ a^1,\ a^2,\ a^3,\ a^4,\ \ldots\ldots\ a^{n-2}$$

per n divisae totidem diversa residua producant, quorum numerus cum sit $n-1$, in his residuis omnes occurrent numeri $1, 2, 3, 4, \ldots\ldots\ n-1$, quibus exhaustis sequens potestas a^{n-1} iterum per n divisa relinquet residuum $+1$, perinde ac prima a^0. Cum ergo post hanc haec formula $a^{n-1}-1$ demum per n sit divisibilis, ob $n-1$ numerum parem, qui sit $= 2p$, ita ut $n = 2p+1$, vel formula a^p-1 vel haec a^p+1 per numerum primum n divisibilis sit necesse est. Priore autem casu a^p residuum daret $+1$, quod cum nostrae hypothesi adversetur, posterior formula a^p+1 per n erit divisibilis, sive potestas a^p residuum dabit -1, seu $n-1$. His praemissis, quoniam singula residua $1, 2, 3, 4, \ldots\ldots\ n-1$ oriuntur ex potestatibus a^0, a^1, a^2 etc. $\ldots\ldots\ a^{n-2}$, manifestum est productum omnium eorum residuorum, scilicet productum propositum $1 \cdot 2 \cdot 3 \cdot \cdots\cdots (n-1)$, si per n dividatur, idem residuum esse relicturum, quod productum omnium earum potestatum $a^{0+1+2+3+\cdots+(n-2)}$, sive haec potestas

$$a^{\frac{(n-1)(n-2)}{2}}$$

esset daturum. Cum autem sit $n = 2p+1$, erit $n-1 = 2p$ et $n-2 = 2p-1$, ideoque haec potestas fiet a^{2pp-p}, quae reducitur ad hanc: $a^{2p(p-1)+p}$, quae est productum ex his duabus potestatibus $a^{2p(p-1)}$ et a^p. Verum iam vidimus potestatem a^{2p}, sive a^{n-1}, per n divisam residuum dare $+1$, quod idem resultabit ex omnibus eius potestatibus, cuiusmodi est $a^{2p(p-1)}$; at altera potestas a^p residuum relinquit -1, unde ipsius potestatis a^{2pp-p} residuum erit -1. Sicque haec formula $a^{2pp-p}+1$ per numerum n erit divisibilis; substituto igitur producto $1 \cdot 2 \cdot \cdots (n-1)$ in locum potestatis a^{2pp-p}, haec formula $1 \cdot 2 \cdot 3 \cdot \cdots (n-1)+1$ per numerum primum n erit divisibilis.

COROLLARIUM 1

Hinc facile plures aliae similes formulae deduci possunt, quae singulae pariter per numerum primum n erunt divisibiles, quas cum ipsa formula, unde sunt natae, hic apponamus:

$$\begin{aligned}
&1 \cdot 2 \cdot 3 \cdot \cdots\cdots (n-1)+1\\
1 \times &1 \cdot 2 \cdot 3 \cdot \cdots\cdots (n-2)-1\\
1 \cdot 2 \times &1 \cdot 2 \cdot 3 \cdot \cdots\cdots (n-3)+1\\
1 \cdot 2 \cdot 3 \times &1 \cdot 2 \cdot 3 \cdot \cdots\cdots (n-4)-1 \text{ etc.}
\end{aligned}$$

In his autem formulis numerus n non eo usque diminui debet, donec fiat [factor pertinens] $= 0$.

COROLLARIUM 2

Si porro habeatur progressio arithmetica n terminorum, cuius differentia neque sit n, neque multiplum ipsius, in ea inerit unus terminus per n divisibilis, quo excluso productum reliquorum terminorum unitate auctum semper erit divisibile per numerum n, siquidem fuerit numerus primus. Ita si sit $n = 7$ et formetur haec progressio arithmetica 7 terminorum: 2, 5, 8, 11, 14, 17, 20, reiecto termino 14 haec forma $2 \cdot 5 \cdot 8 \cdot 11 \cdot 17 \cdot 20 + 1$ dividi poterit per 7.

II. PROBLEMA

Invenire quatuor numeros integros tales, ut producta ex binis unitate aucta fiant quadrata.

SOLUTIO

Problema hoc in Elementis meis Algebrae fusius tractavi[1]), methodus vero, qua sum usus, minus erat accommodata ad numeros integros inveniendos. Haec autem quaestio eo est difficilior, quod sex conditionibus satisfieri oportet. Nunc igitur sequentem solutionem satis simplicem exhibeo. Sumtis pro lubitu duobus numeris m et n, ut fiat $mn + 1 = ll$, quatuor numeri quaesiti erunt:

$$\text{I. } m, \quad \text{II. } n, \quad \text{III. } m + n + 2l, \quad \text{IV. } 4l(l + m)(l + n),$$

quibus 6 conditiones praescriptae sequenti modo implentur:

1°. $mn + 1 = ll$,
2°. $m(m + n + 2l) + 1 = (l + m)^2$,
3°. $n(m + n + 2l) + 1 = (l + n)^2$,
4°. $4ml\,(l + m)\,(l + n) + 1 = (2ll + 2lm - 1)^2$,
5°. $4nl\,(l + m)\,(l + n) + 1 = (2ll + 2ln - 1)^2$, denique
6°. $4l\,(m + n + 2l)\,(l + m)\,(l + n) + 1 = (4ll + 2lm + 2ln - 1)^2$.

---

1) Vide opus 388[2] (indicis Enestroemiani): Leonhard Euler's *vollständige Anleitung zur Algebra*. Zweyter Theil von den verschiedenen Rechnungsarten, Verhältnissen und Proportionen. St. Petersburg, 1771. *Leonhardi Euleri Opera omnia*, series I, vol. 1, art. 233, XIV. Aufgabe, p. 465. R. F.

Hic vero plurimum observasse iuvabit numerum l tam positive quam negative accipi posse. Ita si sumatur $m = 3$ et $n = 8$, ut fiat $mn + 1 = 25$, ideoque $l = \pm 5$, casus $l = -5$ dabit hos quatuor numeros:

I. 3, II. 8, III. 1 et IV. 120.

Sin autem capiatur $l = +5$, numeri erunt

I. 3, II. 8, III. 21 et IV. 2080.

ANALYSIS AD HANC SOLUTIONEM PERDUCENS

Cum tres priores numeri m, n et $m + n + 2l$ facillime inveniantur, ponatur quartus $= z$, atque his tribus conditionibus satisfieri debebit:

1°. $mz + 1 = \square$,
2°. $nz + 1 = \square$,
3°. $(m + n + 2l)\, z + 1 = \square$.

Hinc ergo etiam harum trium formularum productum debebit esse quadratum; at calculo instituto hoc productum reperietur:

$$1 + 2(m + n + l)\, z + ((m + n + l)^2 - 1)\, zz + mn(m + n + 2l)\, z^3 = \square,$$

cuius radix, ut tria priora membra tollantur, statuatur

$$1 + (m + n + l)\, z - \tfrac{1}{2} zz,$$

cuius quadratum est:

$$1 + 2(m + n + l)\, z + ((m + n + l)^2 - 1)\, zz - (m + n + l)\, z^3 + \tfrac{1}{4} z^4,$$

unde nascitur haec aequatio:

$$mn(m + n + 2l) = -m - n - l + \tfrac{1}{4} z$$
$$\text{sive } \tfrac{1}{4} z = m + n + l + mn(m + n + 2l)$$
$$\text{sive } \tfrac{1}{4} z = (mn + 1)(m + n + l) + lmn,$$

vel quia $mn + 1 = ll$, habebimus

$$ll(m + n + l) + lmn = l(ll + lm + ln + mn) = l(l + m)(l + n),$$

quo circa invenimus

$$z = 4l(l + m)(l + n).$$

Quanquam autem hic tantum productum ex tribus formulis $mz+1$, $nz+1$, $(m+n+2l)z+1$ reddidimus quadratum, tamen, quia pro z quasi praeter exspectationem prodiit numerus integer, unde tres istae formulae inter se evadent primae, tuto concludere possumus etiam singulas ternas formulas fieri quadrata, quorum radices adeo iam supra exhibuimus.

III. PROBLEMA

Invenire numeros x et y, ut haec formula $\left(\frac{xx+1}{x}\right)^2+\left(\frac{yy+1}{y}\right)^2$ fiat quadratum.

SOLUTIO

Primo haec conditio sponte adimplebitur, si capiatur $y=\frac{x+1}{x-1}$, tum enim fiet $\frac{yy+1}{y}=\frac{2(xx+1)}{xx-1}$, unde formula proposita abibit in hanc formam:

$$\frac{(xx+1)^2}{xx}+\frac{4(xx+1)^2}{(xx-1)^2}=\frac{(xx+1)^4}{xx(xx-1)^2},$$

quae formula iam per se est quadratum. Verum quia haec solutio tantum est specialis, quo generaliorem obtineamus, statuamus

$$y=\frac{px-1}{x+p}, \quad \text{unde fiet} \quad \frac{yy+1}{y}=\frac{(pp+1)(xx+1)}{(x+p)(px-1)},$$

quare formula nostra evadet

$$\frac{(xx+1)^2}{xx}+\frac{(pp+1)^2(xx+1)^2}{(x+p)^2(px-1)^2},$$

quae per quadratum $(xx+1)^2$ divisa abit in hanc:

$$\frac{1}{xx}+\frac{(pp+1)^2}{(x+p)^2(px-1)^2},$$

quae per quadratum $xx(x+p)^2(px-1)^2$ multiplicata dat

$$(x+p)^2(px-1)^2+xx(pp+1)^2.$$

Haec iam formula quadratum effici debet, quae evoluta reducitur ad istam:

$$ppx^4 + 2p(pp-1)\,x^3 + 2(p^4 - pp + 1)\,xx - 2p(pp-1)\,x + pp\,,$$

cuius radix secundum praecepta cognita si statuatur

$$pxx + (pp-1)\,x + p\,,$$

elicietur iste valor: $x = \frac{4p}{pp-1}$, ubi ergo numerus p pro lubitu accipi potest; tum vero pro altero numero y habebimus, uti assumsimus,

$$y = \frac{px-1}{x+p} = \frac{3pp+1}{p(pp+3)}\,.$$

Hinc ergo, si sumatur $p = 2$, fiet $x = \frac{8}{3}$ et $y = \frac{13}{14}$ et

$$\frac{xx+1}{x} = \frac{73}{24} \quad \text{et} \quad \frac{yy+1}{y} = \frac{365}{182}\,,$$

quorum quadratorum summa fit quadratum radicis $\frac{73\cdot 109}{2\cdot 12\cdot 91}$.

IV. PROBLEMA

Invenire duos numeros p et q, quorum summa sit quadratum, summa vero quadratorum biquadratum.

SOLUTIO

Hoc Problema, a Leibnizio olim propositum[1]), eo magis est notatu dignum, quod minimi numeri sint vehementer magni, siquidem positivi desiderentur. Quamvis autem hoc problema iam passim occurrat solutum, tamen haec solutio attentione non indigna videtur. Ponamus autem $p + q = B^2$ et $pp + qq = A^4$. Iam a duplo posterioris aequationis $2pp + 2qq = 2A^4$ subtrahatur quadratum prioris $pp + 2pq + qq = B^4$ et residuum erit

1) Problema primum a Fermatio propositum est in observationibus ad quaestionem XXIV libri VI Diophanti. Vide Oeuvres de Fermat t. I. p. 336, Paris, 1891. Problema aliquanto generalius in litteris die 26. octobris 1674 a Leibnizio ad Oldenburg datis. Vide Leibnizens mathematische Schriften, herausgegeben von C. J. Gerhardt, 1. Abteilung, Bd. I. p. 54, Berlin 1849. R. F.

$$pp - 2pq + qq = 2A^4 - B^4,$$

ideoque

$$p - q = \sqrt{(2A^4 - B^4)},$$

sicque totum negotium huc reducitur, ut formula $2A^4 - B^4$ quadratum reddatur. Ut autem ambo numeri p et q prodeant positivi, necesse est, ut sit $B > A$. Statuamus igitur

$$\sqrt{(2A^4 - B^4)} = yy + 2xy - xx,$$

quod eveniet, si capiatur

$$A^2 = xx + yy \text{ et } B^2 = xx + 2xy - yy,$$

quas ergo binas formulas denuo ad quadrata redigi oportet. Cum autem posterior sit $(x + y)^2 - 2yy$, pro utraque conditione faciamus $y = 2abcd$; tum vero pro priore $x = aabb - ccdd$, pro posteriore autem $x + y = aacc + 2bbdd$, sic enim fiet

$$A = aabb + ccdd \text{ et } B = aacc - 2bbdd.$$

Quia autem habemus

$$x = aabb - ccdd \text{ et } y = 2abcd,$$

erit hinc

$$x + y = aabb - ccdd + 2abcd = aacc + 2bbdd,$$

unde deducimus

$$aa = \frac{2abcd - dd(2bb + cc)}{cc - bb},$$

unde radicem extrahendo reperimus

$$a = \frac{bcd \pm \sqrt{bbccdd - dd(2bb + cc)(cc - bb)}}{cc - bb},$$

unde per evolutionem fit $\frac{a}{d} = \frac{bc \pm \sqrt{(2b^4 - c^4)}}{cc - bb}$, vel per conversionem

$\frac{d}{a} = \frac{bc \mp \sqrt{(2b^4 - c^4)}}{2bb + cc}$. Hoc igitur modo resolutionem formulae $\sqrt{(2A^4 - B^4)}$ reduximus ad resolutionem alius formulae prorsus similis $\sqrt{(2b^4 - c^4)}$, unde si unicus casus constet, quo talis formula rationalis evadit, inde continuo alius casus concludi poterit. Cum igitur hoc primo eveniat sumendo $b = 1$ et $c = 1$, erit $\frac{a}{d} = \frac{1 \pm 1}{0}$, seu ex posteriori forma $\frac{d}{a} = \frac{1 \pm 1}{3}$. Sumatur ergo $\frac{d}{a} = \frac{2}{3}$, sive $a = 3$ et $d = 2$, fietque $x = 5$ et $y = 12$, tum vero $A = 13$ et $B = 1$, atque hinc:

$$yy + 2xy - xx = (x + y)^2 - 2xx = 239,$$

quae est radix quadrata formulae $2 \cdot 13^4 - 1$. Quia autem hic $B < A$, hinc nulla solutio idonea sequitur. Hoc autem casu reperto faciamus nunc $b = 13$ et $c = 1$, fietque $\sqrt{(2b^4 - c^4)} = 239$, sicque porro nanciscimur $\frac{a}{d} = \frac{13 \pm 239}{-168}$, unde ob signum ambiguum binae solutiones oriuntur: vel $\frac{a}{d} = -\frac{3}{2}$ vel $\frac{a}{d} = \frac{113}{84}$. Ex priore ergo casu habemus $a = 3$, $b = 13$, $c = 1$ et $d = -2$, unde colligimus $x = 1521 - 4 = 1517$ et $y = -156$, tum vero $A = 1525$ et $B = -1343$. Quia autem huius litterae B tantum quadratum et biquadratum occurrit, sumi poterit $B = 1343$, qui valor cum minor sit quam $A = 1525$, nullam solutionem desideratam praebet.

Consideremus ergo alterum casum, quo $\frac{a}{d} = \frac{113}{84}$, unde nostrae quaternae litterae erunt $a = 113$, $b = 13$, $c = 1$ et $d = 84$, ex quibus si colligantur valores x, y et A, B, erit $B > A$, hincque enormes illi numeri pro p et q colliguntur problemati satisfacientes.

V. PROBLEMA

Si formula $1 + Az + Bzz + Cz^3 + Dz^4 +$ etc. *fuerit productum ex factoribus* $1 + \alpha z$, $1 + \beta z$, $1 + \gamma z$, $1 + \delta z$ *etc., invenire summam potestatum omnium litterum* α, β, γ, δ *etc.*[1]).

1) Vide Commentationem 158 (indicis Enestroemiani): *Observationes analyticae variae de Combinationibus*, Comment. acad. sc. Petrop. 13 (1741/3), 1751, p. 64—93; *Leonhardi Euleri Opera omnia*, series I, vol. 2, p. 163—193. R. F.

SOLUTIO

Summas istas, quas quaerimus, ita designemus:

$$P = \alpha + \beta + \gamma + \delta + \text{etc.}$$
$$Q = \alpha^2 + \beta^2 + \gamma^2 + \delta^2 + \text{etc.}$$
$$R = \alpha^3 + \beta^3 + \gamma^3 + \delta^3 + \text{etc.}$$
$$S = \alpha^4 + \beta^4 + \gamma^4 + \delta^4 + \text{etc.},$$

ubi totum negotium huc redit, ut valores litterarum P, Q, R, S etc. per litteras A, B, C, D etc. determinentur. Hic autem ante omnia observari convenit litteram P a sola littera A pendere, quippe cui est aequalis; deinde littera Q tantum a duabus litteris A et B pendere potest, quoniam producta ex ternis litteris α, β, γ, δ etc. non ingrediuntur in compositionem quadratorum. Eodem modo littera R tantum pendebit a tribus litteris A, B et C, at littera S involvet has tantum quatuor: A, B, C et D; et ita simili modo de sequentibus.

1°. His praenotatis littera P eodem modo reperietur, ac si formula esset tantum $1 + Az$ et litterae reliquae $B, C, D, E, \ldots$ evanescerent; hoc autem casu unicus factor locum habet, qui sit $1 + az$, ita ut sit $P = a$. Iam posito hoc factore $1 + az = 0$ sive $z = -\frac{1}{a}$, ipsa formula evanescere debet, eritque idcirco $1 - \frac{A}{a} = 0$ sive $a - A = 0$, unde fit $a = P = A$, uti quidem notissimum est.

2°. Littera autem Q eundem valorem sortietur, ac si formula nostra foret $1 + Az + Bzz$, reliquis terminis evanescentibus. Haec autem formula duos habet factores, qui sint $1 + az$ et $1 + bz$, hincque erit $P = a + b$ et $Q = a^2 + b^2$. Fiat nunc $1 + az = 0$ sive $z = -\frac{1}{a}$, et hoc casu ipsa nostra formula debet evanescere, eritque

$$1 - \frac{A}{a} + \frac{B}{a^2} = 0$$

sive $a^2 - Aa + B = 0$. Eodem modo ex altero factore $1 + bz$ orietur haec aequatio: $b^2 - Ab + B = 0$. Addantur hae duae aequationes, et loco $a^2 + b^2$ scribendo Q et P loco $a + b$ orietur haec aequatio: $Q - AP + 2B = 0$, unde colligitur $Q = AP - 2B$.

3°. Verus porro valor ipsius R deducetur ex formula $1 + Az + Bz^2 + Cz^3$, cuius tres factores sint

$$(1 + az)(1 + bz)(1 + cz),$$

ita ut habeamus

$$P = a + b + c,\ Q = a^2 + b^2 + c^2 \text{ et } R = a^3 + b^3 + c^3.$$

Quemlibet horum factorum redigamus ad nihilum, et ex primo fiet $z = -\frac{1}{a}$, unde ipsa formula praebebit

$$1 - \frac{A}{a} + \frac{B}{a^2} - \frac{C}{a^3} = 0$$

sive $a^3 - Aa^2 + Ba - C = 0$. Simili modo bini reliqui factores dabunt

$$b^3 - Ab^2 + Bb - C = 0 \text{ et } c^3 - Ac^2 + Bc - C = 0,$$

quae tres aequationes iunctae dabunt

$$R - AQ + BP - 3C = 0, \text{ unde } R = AQ - BP + 3C.$$

4°. Pari modo littera S ex hac formula:

$$1 + Az + Bz^2 + Cz^3 + Dz^4$$

colligitur, cuius quatuor factores sint

$$(1 + az)\ (1 + bz)\ (1 + cz)\ (1 + dz),$$

hincque

$$P = a + b + c + d, \qquad Q = a^2 + b^2 + c^2 + d^2,$$
$$R = a^3 + b^3 + c^3 + d^3 \text{ et } S = a^4 + b^4 + c^4 + d^4.$$

Quod si nunc singuli factores seorsim nihilo aequentur et reductio fiat ut ante, orientur inde 4 sequentes aequationes:

$$a^4 - Aa^3 + Ba^2 - Ca + D = 0,$$
$$b^4 - Ab^3 + Bb^2 - Cb + D = 0,$$
$$c^4 - Ac^3 + Bc^2 - Cc + D = 0,$$
$$d^4 - Ad^3 + Bd^2 - Cd + D = 0,$$

quae additae hanc formulam suppeditant:

$$S - AR + BQ - CP + 4D = 0, \text{ hincque}$$
$$S = AR - BQ + CP - 4D.$$

Hinc iam facile intelligitur, quomodo etiam superiores potestates, scilicet T, U, V etc. ex praecedentibus formantur, quem in finem singulos hos valores ordine apponamus:

$$\begin{aligned} P &= A\,, \\ Q &= AP - 2B\,, \\ R &= AQ - BP + 3C\,, \\ S &= AR - BQ + CP - 4D\,, \\ T &= AS - BR + CQ - DP + 5E\,, \\ U &= AT - BS + CR - DQ + EP - 6F \end{aligned}$$

etc.

VI. PROBLEMA

8. *Invenire adeo quinque numeros huius indolis, ut producta ex binis unitate aucta fiant quadrata.*

SOLUTIO

Problema hoc vires analyseos Diophanteae superare censeri deberet, nisi casu quodam singulari solutio possibilis redderetur. In primo autem problemate iam exhibuimus quatuor huiusmodi numeros, eosque adeo integros, qui his conditionibus gaudent, scilicet sumtis pro lubitu duobus numeris m et n, ita ut fiat $mn + 1 = ll$, quatuor numeri satisfacientes ita se habebunt:

$$a = m\,,\ b = n\,,\ c = m + n + 2l \text{ et } d = 4l\,((l + m)(l + n))\,.$$

Nunc igitur praesens quaestio huc redit, ut quaeratur quintus numerus z, qui cum istis quatuor conditionibus praescriptis satisfaciat; requiritur ergo, ut sequentes quatuor formulae singulae reddantur quadrata:

$$1 + az = \square\,,\quad 1 + bz = \square\,,\quad 1 + cz = \square\,,\quad 1 + dz = \square\,;$$

quibus si singulis satisfieri deberet, insuperabilia obstacula occurrerent. Hic autem uti supra feliciter usu venit, ut, si modo productum harum quatuor formularum quadratum efficiatur, etiam singulae seorsim quadrata sint futura. Multiplicentur igitur hae quatuor formulae in se invicem, ac ponatur brevitatis gratia productum:

$$1 + pz + qzz + rz^3 + sz^4\,,$$

ita ut sit

$$p = a + b + c + d,\ q = ab + ac + ad + bc + bd + cd,$$
$$r = abc + abd + acd + bcd \text{ et } s = abcd.$$

Nunc statuatur radix quadrata istius formulae

$$1 + \tfrac{1}{2} pz + (\tfrac{1}{2} q - \tfrac{1}{8} pp) zz,$$

ut eius quadratum fiat

$$1 + pz + qz^2 + p(\tfrac{1}{2} q - \tfrac{1}{8} pp) z^3 + (\tfrac{1}{2} q - \tfrac{1}{8} pp)^2 z^4,$$

ubi, cum tres priores termini sponte se tollant, reliqui per z^3 divisi suppeditabunt hanc aequalitatem:

$$r + sz = p(\tfrac{1}{2} q - \tfrac{1}{8} pp) + (\tfrac{1}{2} q - \tfrac{1}{8} pp)^2 z,$$

unde colligimus quintum numerum quaesitum:

$$z = \frac{r - p(\frac{1}{2}q - \frac{1}{8}pp)}{(\frac{1}{2}q - \frac{1}{8}pp)^2 - s}.$$

Verum si indolem 4 numerorum datorum accuratius perpendamus, reperiemus semper fore $\frac{1}{2} q - \frac{1}{8} pp = \frac{-1-s}{2}$, unde denominator inventae fractionis evadet:

$$(\tfrac{1}{2}q - \tfrac{1}{8}pp)^2 - s = \frac{(s-1)^2}{4},$$

sicque commode evenit, ut hic denominator fiat quadratum; nisi enim hoc contigisset, singulae formulae:

$$1 + az,\quad 1 + bz,\quad 1 + cz,\quad 1 + dz$$

quadrata fieri non potuissent. Quod si etiam in numeratore istum valorem loco $(\frac{1}{2} q - \frac{1}{8} pp)$ substituamus, fiet $z = \frac{4r + 2p(s+1)}{(s-1)^2}$. Hoc autem numero z invento omnino decem sequentibus conditionibus satisfiet:

I°. $ab + 1 = \square$,	II°. $ac + 1 = \square$,
III°. $ad + 1 = \square$,	IV°. $bc + 1 = \square$,
V°. $bd + 1 = \square$,	VI°. $cd + 1 = \square$,
VII°. $az + 1 = \square$,	VIII°. $bz + 1 = \square$,
IX°. $cz + 1 = \square$,	X°. $dz + 1 = \square$.

COROLLARIUM

Quod autem semper sit $\frac{1}{2}q - \frac{1}{8}pp = \frac{-s-1}{2}$, sequenti modo ostendi potest. Ponatur brevitatis gratia $m+n+l=f$ et $l(l+m)(l+n)=k$, ita ut sit $k=fll+lmn$, et cum sit $a=m$, $b=n$, $c=f+l$ et $d=4k$, habebimus

$$a+b+c=2f, \text{ ergo } p=2f+4k;$$

deinde, quia

$$q=(a+b+c)d+(a+b)c+ab,$$

fiet nunc

$$q=8fk+(m+n)^2+2l(m+n)+mn,$$

quae expressio ob $mn=ll-1$ abit in hanc: $q=8fk+ff-1$; tum vero erit $s=4mnk(f+l)$, hinc erit

$$1+q+s=8fk+ff+4mnk(f+l),$$

quod an aequale sit ipsi $\frac{1}{4}pp$, videamus. At est

$$\frac{1}{4}pp=ff+4fk+4kk,$$

hisque valoribus inter se aequatis habebimus

$$8fk+ff+4mnk(f+l)=ff+4fk+4kk, \text{ sive}$$
$$4fk+4mnk(f+l)=4kk,$$

quae aequatio per $4k$ divisa dat

$$f+mn(f+l)=k=fll+lmn, \text{ sive}$$
$$f+fmn=fll^{1}), \text{ ob } mn+1=ll$$

per hypothesin, quae aequatio cum sit identica, illa: $1+q+s=\frac{1}{4}pp$ necessario est vera, unde sequitur, quod assumsimus, $\frac{1}{2}q-\frac{1}{8}pp=\frac{-s-1}{2}$.

EXEMPLUM 1

Sumamus $m=1$ et $n=3$, eritque $l=2$, unde quatuor numeri priores erunt $a=1$, $b=3$, $c=8$, $d=120$; hinc ergo colligimus:

$$p=132,\ q=1475,\ r=4224 \text{ et } s=2880;$$

1) Editio princeps: $4ll$. Correxit R. F.

ex quibus valoribus deducimus:

$$z = \frac{4 \cdot 4224 + 264 \cdot 2881}{(2879)^2},$$

quae fractio reducitur ad hanc $\frac{777480}{8288641}$, atque hinc decem conditiones praescriptae sequenti modo adimplentur:

$$\begin{aligned}
&1^\circ.\ ab + 1 = 2^2, && 2^\circ.\ ac + 1 = 3^2,\\
&3^\circ.\ ad + 1 = 11^2, && 4^\circ.\ bc + 1 = 5^2,\\
&5^\circ.\ bd + 1 = 19^2, && 6^\circ.\ cd + 1 = 31^2,\\
&7^\circ.\ az + 1 = \frac{(3011)^2}{(2879)^2}, && 8^\circ.\ bz + 1 = \frac{(3259)^2}{(2879)^2},\\
&9^\circ.\ cz + 1 = \frac{(3809)^2}{(2879)^2}, && 10^\circ.\ dz + 1 = \frac{(10079)^2}{(2879)^2}.
\end{aligned}$$

EXEMPLUM 2

Cum numerus z hinc prodierit tam vehementer magnus, evolvamus sequentem casum in fractionibus, quandoquidem fractiones admittere nunc sumus coacti. Sumatur igitur $m = \frac{1}{2}$, $n = \frac{5}{2}$, ut sit $l = \frac{3}{2}$, unde quatuor numeri priores erunt

$$a = \tfrac{1}{2},\ b = \tfrac{5}{2},\ c = 6 \text{ et } d = 48;$$

unde porro deducimus:

$$p = 57,\ q = 451\tfrac{1}{4},\ r = 931\tfrac{1}{2} \text{ et } s = 360;$$

ex his ergo deducitur:

$$z = \frac{4 \cdot 931\frac{1}{2} + 114 \cdot 361}{359^2} = \frac{44880}{359^2} = \frac{44880}{128881},$$

qui numeri multo sunt minores quam praecedentes.

SPECULATIONES CIRCA QUASDAM INSIGNES PROPRIETATES NUMERORUM

Commentatio 564 indicis Enestroemiani
Acta academiae scientiarum Petropolitanae 4 II (1780: II), 1784, p. 18—30
[Conventui exhibita die 9. octobris 1775]

1. Nullum est dubium, quin multitudo omnium fractionum diversarum, quae inter terminos 0 et 1 constitui possunt, sit infinita; unde cum multitudo omnium numerorum integrorum etiam sit infinita, manifestum est multitudinem omnium plane fractionum adhuc infinities esse maiorem; quandoquidem inter binos numeros, unitare differentes, innumerabiles fractiones diversae admitti debent. Hic autem assumitur denominatores fractionum in infinitum augeri posse; at si terminus praescribatur, quem numeratores superare non debeant, tum utique numerus fractionum, quas inter terminos 0 et 1 constituere licet, erit determinatus. Quantus autem iste numerus sit futurus, pro quovis limite, qui denominatoribus praescribitur, quaestio quidem primo intuitu non ita difficilis videtur; verum si rem attentius consideremus, tantae difficultates occurrunt, ut perfecta istius quaestionis solutio vix adhuc sperari posse videatur.

2. Quoniam enim fractiones, de quibus hic quaeritur, omnes inter se diversae esse debent, ex quolibet denominatore aliae fractiones formari nequeunt, nisi quarum numeratores non solum sint denominatore minores, sed etiam ad eundem primi, quia alioquin ad formam simpliciorem, ideoque ad denominatores minores reduci possent. Ita cum fractio $\frac{15}{24}$ reducatur ad $\frac{5}{8}$, ista fractio pro denominatore $= 24$ non amplius numerari poterit, quoniam pro denominatore 8 iam est numerata. Totum igitur negotium huc redit, ut pro quolibet denominatore, qui sit $= D$, multitudo nume-

rorum ipso minorum, et qui cum eo nullum habeant divisorem communem, assignetur, quippe qui soli pro numeratoribus accipi possunt. Ita pro denominatore 24 alii numeratores admitti nequeunt, praeter 1, 5, 7, 11, 13, 17, 19, 23, quorum multitudo est tantum 8, cuius ratio in compositione numeri 24 est sita. Si enim denominator D esset numerus primus, tum utique omnes numeri ipso minores, quorum multitudo est $D - 1$, idoneos praeberent numeratores. Quo plures autem denominator D habuerit divisores, eo magis multitudo numeratorum restringitur.

3. Hinc igitur ista quaestio nascitur: ut, proposito quocunque numero D, multitudo numerorum ipso minorum ad eumque simul primorum assignetur. Quod quo facilius praestari possit, denotet character πD multitudinem istam numerorum ipso D minorum, et qui cum eo nullum habeant divisorem communem. Ac primo quidem manifestum est, si fuerit D numerus primus, fore $\pi D = D - 1$. Ante autem quam numeros compositos examinemus, valores huius characteris πD pro omnibus numeris centenario non maioribus apponamus:

$\pi\ 1 = 0$	$\pi\ 21 = 12$	$\pi\ 41 = 40$	$\pi\ 61 = 60$	$\pi\ 81 = 54$
$\pi\ 2 = 1$	$\pi\ 22 = 10$	$\pi\ 42 = 12$	$\pi\ 62 = 30$	$\pi\ 82 = 40$
$\pi\ 3 = 2$	$\pi\ 23 = 22$	$\pi\ 43 = 42$	$\pi\ 63 = 36$	$\pi\ 83 = 82$
$\pi\ 4 = 2$	$\pi\ 24 = 8$	$\pi\ 44 = 20$	$\pi\ 64 = 32$	$\pi\ 84 = 24$
$\pi\ 5 = 4$	$\pi\ 25 = 20$	$\pi\ 45 = 24$	$\pi\ 65 = 48$	$\pi\ 85 = 64$
$\pi\ 6 = 2$	$\pi\ 26 = 12$	$\pi\ 46 = 22$	$\pi\ 66 = 20$	$\pi\ 86 = 42$
$\pi\ 7 = 6$	$\pi\ 27 = 18$	$\pi\ 47 = 46$	$\pi\ 67 = 66$	$\pi\ 87 = 56$
$\pi\ 8 = 4$	$\pi\ 28 = 12$	$\pi\ 48 = 16$	$\pi\ 68 = 32$	$\pi\ 88 = 40$
$\pi\ 9 = 6$	$\pi\ 29 = 28$	$\pi\ 49 = 42$	$\pi\ 69 = 44$	$\pi\ 89 = 88$
$\pi\ 10 = 4$	$\pi\ 30 = 8$	$\pi\ 50 = 20$	$\pi\ 70 = 24$	$\pi\ 90 = 24$
$\pi\ 11 = 10$	$\pi\ 31 = 30$	$\pi\ 51 = 32$	$\pi\ 71 = 70$	$\pi\ 91 = 72$
$\pi\ 12 = 4$	$\pi\ 32 = 16$	$\pi\ 52 = 24$	$\pi\ 72 = 24$	$\pi\ 92 = 44$
$\pi\ 13 = 12$	$\pi\ 33 = 20$	$\pi\ 53 = 52$	$\pi\ 73 = 72$	$\pi\ 93 = 60$
$\pi\ 14 = 6$	$\pi\ 34 = 16$	$\pi\ 54 = 18$	$\pi\ 74 = 36$	$\pi\ 94 = 46$
$\pi\ 15 = 8$	$\pi\ 35 = 24$	$\pi\ 55 = 40$	$\pi\ 75 = 40$	$\pi\ 95 = 72$
$\pi\ 16 = 8$	$\pi\ 36 = 12$	$\pi\ 56 = 24$	$\pi\ 76 = 36$	$\pi\ 96 = 32$
$\pi\ 17 = 16$	$\pi\ 37 = 36$	$\pi\ 57 = 36$	$\pi\ 77 = 60$	$\pi\ 97 = 96$
$\pi\ 18 = 6$	$\pi\ 38 = 18$	$\pi\ 58 = 28$	$\pi\ 78 = 24$	$\pi\ 98 = 42$
$\pi\ 19 = 18$	$\pi\ 39 = 24$	$\pi\ 59 = 58$	$\pi\ 79 = 78$	$\pi\ 99 = 60$
$\pi\ 20 = 8$	$\pi\ 40 = 16$	$\pi\ 60 = 16$	$\pi\ 80 = 32$	$\pi 100 = 40$

4. Ex hac igitur tabula patet denominatorem 2 unicam praebere fractionem, scilicet $\frac{1}{2}$, inter 0 et 1; denominatorem vero 3 dare 2; at 4 dare has duas fractiones: $\frac{1}{3}$ et $\frac{3}{4}$ et ita porro. Unde si denominatores non ultra 10 continuare velimus, numerus omnium fractionum erit 31; sin autem continuemus usque ad 20, numerus est 127; usque ad 30 progrediendo summa fractionum prodit 277, uti sequens tabella declarat.

Max. denom.	Num. fract.
10	31
20	127
30	277
40	489
50	773
60	1101
70	1493
80	1965[1])
90	2479[2])
100	3043

5. Quod si omnes plane fractiones admittere vellemus, pro denominatore maximo = 10 numerus omnium fractionum foret $1 + 2 + 3 + 4 \cdots + 9 = 45$. Hinc igitur excludi debent eae, quae reductionem admittunt. Primo igitur excludendae erunt fractiones $\frac{2}{4}$, $\frac{3}{6}$, $\frac{4}{8}$, $\frac{5}{10}$, quippe $= \frac{1}{2}$; tum vero istae: $\frac{2}{6}$ et $\frac{3}{9}$, quippe $= \frac{1}{3}$; itemque $\frac{4}{6}$ et $\frac{6}{9}$, ut pote $= \frac{2}{3}$; praeterea $\frac{2}{8}$ et $\frac{6}{8}$; ac denique $\frac{2}{10}$, $\frac{4}{10}$, $\frac{6}{10}$, $\frac{8}{10}$, quarum omnium numerus est 14, qui a 45 subtractus relinquit 31. Pro maioribus autem denominatoribus, quos admittere voluerimus, haec enumeratio nimis fiet prolixa, quae quomodo nihilo minus institui possit, videamus.

6. Sit igitur D maximus denominator, quem admittimus, ac numerus omnium plane fractionum foret

$$= 1 + 2 + 3 + 4 + \cdots + (D - 1) = \frac{DD - D}{2}.$$

1) Editio princeps: 1975. Correxit A. M.
2) Editio princeps: 2489. Correxit A. M.

Hinc iam excludi debent omnes fractiones, quarum valor est $\frac{1}{2}$, praeter ipsum $\frac{1}{2}$. Hunc in finem dividatur D per 2, et quotus, sive verus, sive proxime minor sit $= \alpha$, ac manifestum est numerum fractionum excludendarum fore $= \alpha - 1$. Deinde pro fractionibus $\frac{1}{3}$ et $\frac{2}{3}$ sit $\frac{D}{3} = \beta$, denotante β vel verum, vel vero proxime minorem, eritque numerus fractionum excludendarum $= 2(\beta - 1) = (\beta - 1)\,\pi 3$. Simili modo si ponamus $\frac{D}{4} = \gamma$, tum vero porro $\frac{D}{5} = \delta$, $\frac{D}{6} = \varepsilon$ etc., quamdiu scilicet isti quoti prodeunt unitate maiores, numeri fractionum hinc excludendarum erunt

$$(\gamma - 1)\,\pi 4,\ (\delta - 1)\,\pi 5,\ (\varepsilon - 1)\,\pi 6 \text{ etc.},$$

quibus igitur ablatis remanebit multitudo fractionum quaesita:

$$\frac{DD - D}{2} - (\alpha - 1)\,\pi 2 - (\beta - 1)\,\pi 3 - (\gamma - 1)\,\pi 4 - (\delta - 1)\,\pi 5 - \text{etc.}$$

Ita si fuerit $D = 20$, habebimus

$$\frac{20}{2} = \alpha = 10,\ \frac{20}{3} = \beta = 6,\ \frac{20}{4} = \gamma = 5,$$
$$\frac{20}{5} = \delta = 4,\ \frac{20}{6} = \varepsilon = 3,\ \frac{20}{7} = \zeta = 2,$$
$$\frac{20}{8} = \eta = 2,\ \frac{20}{9} = \theta = 2,\ \frac{20}{10} = \iota = 2.$$

Hinc igitur, ob $\frac{DD - D}{2} = 190$, multitudo fractionum diversarum erit

$$190 - 9 \cdot 1 - 5 \cdot 2 - 4 \cdot 2 - 3 \cdot 4 - 2 \cdot 2 - 1 \cdot 6 - 1 \cdot 4 - 1 \cdot 6 - 1 \cdot 4 = 190 - 63 = 127,$$

uti supra invenimus.

7. Totius igitur huius investigationis cardo in eo versatur, quomodo, proposito quocunque numero D, inveniri debeat valor characteris πD. Ac primo quidem iam supra annotavimus, si fuerit D numerus primus, tum fore $\pi D = D - 1$. Verum si D fuerit numerus compositus, determinatio

characteris πD non parum ardua deprehenditur; pendebit enim a factoribus, ex quibus numerus D componitur.

8[1]). Denotet igitur p numerum primum quemcunque, ut fit $\pi p = p - 1$, et quaeramus valorem πp^2; ubi quidem statim patet non omnes numeros ipso minores, quorum multitudo est $pp - 1$, ad eum esse primos, sed inde excludi debere illos, qui per p sunt divisibiles, qui sunt: p, $2p$, $3p$, $4p$ etc. ... $(p-1)p$. Horum autem multitudo est $p - 1$, qui ergo numerus a $pp - 1$ subtractus relinquit $p(p-1)$, ita ut sit $\pi pp = (p-1)p$. Simili modo si fuerit $D = p^3$, multitudo numerorum ipso minorum est $p^3 - 1$, unde excludi debent ii, qui per p sunt divisibiles, qui sunt

$$p,\ 2p,\ 3p,\ 4p,\ \ldots\ p(pp-1),$$

quorum multitudo cum sit $pp - 1$, erit

$$\pi p^3 = p^3 - 1 - (pp - 1) = p^3 - pp = (p-1)pp.$$

Ex quo iam facile perspicitur pro potestate quacunque in genere fore $\pi p^n = (p-1)p^{n-1}$.

9. Sit nunc q alius numerus primus a p diversus, et quaeramus valorem πpq. Primo igitur multitudo numerorum ipso pq minorum est $pq - 1$, unde ergo excludi debent omnes illi, qui sunt divisibiles tam per p quam per q. Iam vero multipla ipsius p erunt

$$p,\ 2p,\ 3p,\ 4p,\ \ldots.\ p(q-1),$$

quorum multitudo est $q - 1$. Eodem modo multitudo multiplorum ipsius q erit $p - 1$, quae cum omnia a prioribus sint diversa, multitudo numerorum excludendorum erit $p + q - 2$, ita ut hinc prodeat

$$\pi pq = pq - 1 - (p + q - 2) = pq - p - q + 1 = (p-1)(q-1),$$

1) Vide commentationem 271 (indicis Enestroemiani): *Theoremata arithmetica nova methodo demonstrata*, Novi comment. acad. sc. Petrop. 8 (1760/1), 1763, p. 74—104; *Leonhardi Euleri Opera omnia*, series I, vol. 2, p. 531—555, in qua eaedem formulae eodem methodo demonstratae sunt. R. F.

unde hoc egregium nacti sumus Theorema: *Si fuerint p et q numeri primi diversi, semper erit*

$$\pi pq = (p-1)(q-1).$$

Eodem autem modo ostendi poterit, si praeterea r et s sint numeri primi ab illis diversi, fore

$$\pi pqr = (p-1)(q-1)(r-1) \text{ et}$$
$$\pi pqrs = (p-1)(q-1)(r-1)(s-1).$$

10. Investigemus nunc valorem huius formulae: πppq, ubi omnium numerorum ppq minorum multitudo est $ppq - 1$, unde ergo primo excludi debent omnia multipla ipsius p, quorum multitudo est $pq - 1$; tum vero numerorum per q divisibilium multitudo est $pp - 1$, inter quos autem occurrunt numeri

$$pq,\ 2pq,\ 3pq,\ \ldots.\ pq(p-1),$$

qui insuper per p sunt divisibiles, quos, quia iam exclusimus, ex hoc postremo ordine tolli oportet, ita ut hic tantum remaneant $pp - 1 - (p-1) = pp - p$, quamobrem hinc obtinebimus

$$\pi ppq = ppq - 1 - (pq-1) - (pp-p) = (p-1)(q-1)p.$$

Quare cum sit

$$p(p-1) = \pi pp \text{ et } q - 1 = \pi q,$$

hinc nascitur istud Theorema: *Si p et q fuerint numeri primi diversi, tum erit*

$$\pi ppq = \pi pp \cdot \pi q = p(p-1)(q-1).$$

11. Simili modo haud difficulter intelligetur fore

$$\pi p^n q = \pi p^n \cdot \pi q = p^{n-1}(p-1)(q-1).$$

Nam quia multitudo numerorum minorum est $p^n q - 1$, hinc primo excludantur omnia multipla ipsius q, quorum numerus est $p^n - 1$, et remanebit multitudo $p^n q - p^n$. Praeterea vero etiam excludamus omnes numeros per p divi-

sibiles, quorum multitudo est $p^{n-1}q - 1$, et remanet $p^n q - p^n - p^{n-1}q + 1$. Huc autem insuper addi debent omnes termini per pq divisibiles, quorum multitudo est $p^{n-1} - 1$, unde colligitur

$$\begin{aligned} \pi p^n q &= p^n q - p^n - p^{n-1}q + p^{n-1} \\ &= p^{n-1}(pq - p - q + 1) = p^{n-1}(p-1)(q-1) . \end{aligned}$$

12. Haud dissimili modo, si numerus D fuerit productum ex duabus potestatibus quibuscunque numerorum primorum p et q diversorum, ita ut sit $D = p^\alpha q^\beta$, tum erit

$$\pi p^\alpha q^\beta = p^{\alpha-1} q^{\beta-1} (p-1)(q-1) ;$$

hincque generaliter, si litterae p, q, r, s denotent numeros primos inter se diversos, erit

$$\pi p^\alpha q^\beta r^\gamma s^\delta = p^{\alpha-1} q^{\beta-1} r^{\gamma-1} s^{\delta-1} (p-1)(q-1)(r-1)(s-1) ,$$

ex quo intelligitur fore quoque

$$\pi p^\alpha q^\beta r^\gamma s^\delta = \pi p^\alpha \cdot \pi q^\beta \cdot \pi r^\gamma \cdot \pi s^\delta .$$

Quamobrem, si modo valores characteris πD inventi fuerint pro omnibus potestatibus numerorum primorum, tum ex iis omnium plane numerorum valores characteris π expedite assignari posse manifestum est.

13. Si quis autem ope horum Theorematum pro numeris quantumvis magnis istos valores investigare voluerit, promtissime scopum obtinebit, si numerum propositum D in factores inter se primos resolvat, sive ii sint numeri primi, necne. Namque si fuerit $D = PQRS$ etc. atque hi factores P, Q, R, S nullos habeant divisores communes, tum semper erit

$$\pi PQRS = \pi P \cdot \pi Q \cdot \pi R \cdot \pi S .$$

Veluti si proponatur iste numerus: $D = 360$, ob $360 = 9 \cdot 40$ erit $\pi 360 = \pi 9 \cdot \pi 40 = 6 \cdot 16 = 96$.

14. Quod si vero progressionem istorum numerorum, qui in tabula supra data exhibentur, contemplemur, quae est 0, 1, 2, 2, 4, 2, 6, 4, 6, 4, 10, 4 etc., nullum plane ordinem in eius terminis observare licet; cum tamen in progressione numerorum, cuius singuli termini exhibent summas divisorum numerorum naturalium, insignem ordinem mihi detegere contigerit. Multo minus ergo, si ex illis numeris talis series formetur:

$$1x^2 + 2x^3 + 2x^4 + 4x^5 + 2x^6 + \text{etc.},$$

cuius terminus generalis nostro signandi modo est $x^n \pi n$, eius indoles, vel adeo summa, ullo modo per quantitates cognitas, sive algebraicas sive transcendentes, exprimi posse videtur. Quocirca utique maxime operae pretium foret in naturam huius progressionis inquirere, quandoquidem hinc scientia numerorum haud contemnendis incrementis locupletari posset.

15. Ex formula autem generali § 12 data multo facilior regula deduci potest, cuius ope pro quocunque numero proposito N valor characteris πN assignari potest, quam in sequente Problemate exponamus.

PROBLEMA

Proposito numero quocunque N invenire multitudinem omnium numerorum ipso minorum ad eumque primorum.

SOLUTIO

16. Quicunque fuerit numerus N, semper tali forma repraesentari potest, ut sit $N = p^\alpha q^\beta r^\gamma s^\delta$ etc. exsistentibus p, q, r, s [etc.] numeris primis. Invenimus autem tum fore

$$\pi N = p^{\alpha-1} q^{\beta-1} r^{\gamma-1} s^{\delta-1} \ldots (p-1)(q-1)(r-1)(s-1) \ldots .$$

Hinc igitur erit

$$\frac{\pi N}{N} = \frac{(p-1)(q-1)(r-1)(s-1) \ldots}{pqrs \ldots},$$

unde sequitur fore

$$\pi N = \frac{N(p-1)(q-1)(r-1)(s-1)\ldots}{pqrs\ldots};$$

ita ut iam non amplius opus sit exponentes $\alpha, \beta, \gamma, [\delta\ldots]$ nosse, sed sufficit omnes numeros primos $p, q, r, s\ldots$ diversos indagasse, per quos numerus propositus N est divisibilis; quibus cognitis multitudo numerorum minorum quam N, et qui simul ad eum sunt primi, erit

$$\pi N = \frac{N(p-1)(q-1)(r-1)(s-1)\ldots}{pqrs\ldots}.$$

17. Ita si verbi gratia propositus fuerit iste numerus: $N = 9450$, numeri primi, per quos hunc numerum dividere licet, sunt 2, 3, 5, 7, quandoquidem per nullos alios divisionem admittit; hinc igitur erit

$$\pi 9450 = \frac{9450 \cdot 1 \cdot 2 \cdot 4 \cdot 6}{2 \cdot 3 \cdot 5 \cdot 7} = 2160.$$

18. Quod si ergo N unicum habeat divisorem primum p, id quod evenit, quando N vel ipsi p aequatur, vel cuipiam eius potestati, tum igitur semper erit $\pi N = \frac{N(p-1)}{p}$. Scilicet si fuerit $N = p$, erit $\pi N = p - 1$; at si fuerit $N = p^n$, tum erit $\pi N = p^{n-1}(p-1)$, uti supra invenimus. Sin autem N duos tantum admittat divisores primos p et q, tum erit $\pi N = \frac{N(p-1)(q-1)}{pq}$. Ita si N alios non habeat divisores praeter 2 et 3, erit $\pi N = \frac{N}{3}$. Tales autem numeri usque ad centum sunt

6, 12, 18, 24, 36, 48, 54, 72, 96.

19. Haec ipsa autem regula facilis nos manuducit ad aliam demonstrationem multo simpliciorem. Ponamus enim numerum N divisores primos inter se diversos habere p, q et r, ac praeterea nullos alios; et quoniam multitudo omnium numerorum ipso non maiorum est $= N$, qui ergo numerus utique divisibilis erit per p, q et r, inde primo excludi debent omnes, qui per p sunt divisibiles, quorum multitudo cum sit $\frac{N}{p}$, his deletis reliquorum multitudo erit $N - \frac{N}{p} = \frac{N(p-1)}{p}$; unde iam excludamus omnes, qui sunt

per q divisibiles, quorum multitudo cum sit $\frac{N(p-1)}{pq}$, remanebunt adhuc $\frac{N(p-1)(q-1)}{pq}$. Hinc igitur insuper excludi debent ii, qui sunt per r divisibiles, quorum multitudo cum sit pars $\frac{1}{r}$ istius numeri, iis deletis numerus reliquorum erit $\frac{N(p-1)(q-1)(r-1)}{pqr}$; hocque modo solide demonstrata est nostra regula.

20. Interim tamen etiam haec regula nullum subsidium nobis suppeditat ad naturam progressionis, quam numeri πN constituunt et quae est:

1	2	3	4	5	6	7	8	9	10	11	12	[etc.],
0	1	2	2	4	2	6	4	6	4	10	4	[etc.],

explorandum. Verum si potestates quantitatis indefinitae x adiungamus ac statuamus

$$s = 1x^2 + 2x^3 + 2x^4 + 4x^5 + 2x^6 + 6x^7 + 4x^8 + 6x^9 + 4x^{10} + \text{etc.},$$

ex hac serie sequentem formare possumus:

$$\int \frac{s\,dx}{x} = \frac{xx}{2} + \frac{2x^3}{3} + \frac{x^4}{2} + \frac{4x^5}{5} + \frac{x^6}{3} + \frac{6x^7}{7} + \frac{x^8}{2} + \frac{2x^9}{3} + \frac{2x^{10}}{5} + \text{etc.},$$

ubi omnes coefficientes in formula $\frac{(p-1)(q-1)(r-1)}{pqr}$ continentur.

21. Omnes enim eae potestates ipsius x eundem habebunt coefficientem $\frac{1}{2}$, quarum exponentes solum divisorem primum admittunt, ideoque sunt potestates binarii, scilicet

$$x^2,\ x^4,\ x^8,\ x^{16},\ x^{32},\ x^{64} \text{ etc.}$$

Deinde omnes potestates, quarum exponentes sunt dignitates ternarii, quae sunt x^3, x^9, x^{27}, omnes habent eundem coefficientem $\frac{2}{3}$. Simili modo $\frac{4}{5}$ erit communis coefficiens potestatum x^5, x^{25}, x^{125} etc. At vero $\frac{1}{3} = \frac{1}{2} \cdot \frac{2}{3}$ commu-

nis erit coefficiens omnium potestatum, quarum exponentes tantum hos duos numeros primos 2 et 3 involvunt, quae sunt x^6, x^{12}, x^{18}, x^{24}, x^{36} etc. Eodemque modo res se habet de reliquis exponentibus, qui vel binos tantum, vel ternos, vel quaternos numeros primos involvunt. Quo plures autem numeri primi in exponentibus occurrunt, eo copiosiores erunt series potestatum, quae communi gaudent coefficiente.

22. Cum igitur in his ordinibus series simplicissimae sint eae, quarum exponentes progressionem geometricam constituunt, cuiusmodi est $x + x^2 + x^4 + x^8 + x^{16} +$ etc., quoniam huius seriei nullo adhuc modo summa definiri vel saltem ad formulam quampiam integralem reduci potuit, multo minus sperare licet unquam certum ordinem in hac serie generali detectum iri, unde saltem sequentes termini per praecedentes determinari queant; quod merito eo magis mirum videbitur, quod cuiusque potestatis x^n coefficiens tam facile assignare potest.

DE INDUCTIONE AD PLENAM CERTITUDINEM EVEHENDA

Commentatio 566 indicis ENESTROEMIANI
Acta academiae scientiarum Petropolitanae 4 II (1780: II), 1784, p. 38—48
[Conventui exhibita die 19. octobris 1775]

1. Notum est plerasque numerorum proprietates primum per solam inductionem esse observatas, quas deinceps Geometrae solidis demonstrationibus confirmare elaboraverunt; in quo negotio imprimis FERMATIUS summo studio et satis felici successu fuit occupatus. Maxime autem dolendum est plures eius demonstrationes iniuria temporum penitus interiisse, quo imprimis sunt referendae eae demonstrationes, quas circa resolutionem numerorum vel in tres trigonales, vel quatuor quadrata, vel quinque pentagonales, vel sex hexagonales etc. se invenisse asseveraverat. Deinceps quidem resolutio in quatuor quadrata a celeberrimo LA GRANGE[1]) et a me[2]) per certissima principia fuit evicta, neque tamen adhuc ista demonstrandi methodus ad numeros trigonales et reliquos polygonales accommodari potuit. Interim tamen istae resolutiones per solam inductionem iam ad tantum certitudinis gradum evectae sunt, ut nullis amplius dubiis locus relinqui videatur. Quin etiam ipsa inductio fortasse per certas rationes ita corro-

1) Confer notam 2, p. 370, vol. 2 seriei I. R. F.

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—58. *LEONHARDI EULERI Opera omnia*, series I, vol. 2, p. 338—372. R. F.

borari posse videtur, ut instar absolutae demonstrationis spectari possit, id quod circa resolutionem numerorum in quatuor quadrata et ternos trigonales ostendere conabor.

DE RESOLUTIONE NUMERORUM IN QUATUOR QUADRATA

2. Quanquam haec resolutio iam perfecta demonstratione est munita, tamen operae pretium erit perscrutari, quousque soli inductioni insistentes in eius veritate stabilienda pertingere valeamus. Primum igitur in subsidium vocemus insigne Theorema FERMATIANUM, quod omnis numerus primus formae $4n + 1$ semper sit summa duorum quadratorum, cuius demonstrationem equidem iam dudum perfectam protuli. Hinc igitur statim sequitur aggregatum duorum huiusmodi numerorum certo esse summam quatuor quadratorum. Aggregata autem duorum numerorum formae $4n + 1$ praebent numeros formae $4n + 2$, hoc est numeros impariter pares; unde si omnes numeri formae $4n + 2$ in duos numeros primos formae $4n + 1$ resolvi possent, etiam forent summae quatuor quadratorum, quod si fuerit ostensum, etiam semisses horum numerorum, hoc est omnes numeri impares, hincque adeo omnes plane numeri erunt summae quatuor quadratorum[1]); quandoquidem facile demonstrari potest, si numerus quispiam N fuerit summa quatuor quadratorum, tum etiam eius duplum, quadruplum, et in genere formam $2^\lambda N$, semper fore summam quatuor quadratorum. Quin etiam, si N fuerit numerus par, veluti nostro casu, scilicet $4n + 2$, tunc etiam eius semissis certe est summa quatuor quadratorum.

3. Tota ergo quaestio huc reducitur: Utrum omnes numeri impariter pares, sive formae $4n + 2$, semper in duas huiusmodi partes, quae sint formae $4n + 1$ simulque numeri primi, secari possint, id quod per inductionem investigemus. Constitutis scilicet numeris primis formae $4n + 1$, qui sunt 1, 5, 13, 17, 29, 37, 41, 53, 61, 73 etc., percurramus ordine omnes numeros formae $4n + 2$, et singulis adiungamus resolutionem in duos huiusmodi numeros primos:

1) Vide commentationem 445 (indicis ENESTROEMIANI): *Novae demonstrationes circa resolutionem numerorum in quadrata*, acta acad. sc. Petrop. 1777, II, 1780, p. 48—69; *LEONHARDI EULERI Opera omnia*, series I, vol. 3, p. 218—239, praecipue Corollarium 1, p. 231. R. F.

$$
\begin{array}{l|l|l|l}
2 = 1+1 & 46 = \begin{cases} 5+41 \\ 17+29 \end{cases} & 74 = \begin{cases} 1+73 \\ 13+61 \\ 37+37 \end{cases} & 98 = \begin{cases} 1+97 \\ 37+61^{1}) \end{cases} \\
6 = 1+5 & 50 = 13+37 & & \\
10 = 5+5 & & & \\
14 = 1+13 & 54 = \begin{cases} 1+53 \\ 13+41 \\ 17+37 \end{cases} & 78 = \begin{cases} 5+73^{2}) \\ 17+61 \\ 37+41 \end{cases} & 102 = \begin{cases} 1+101 \\ 5+97 \\ 13+89 \\ 29+73 \\ 41+61 \end{cases} \\
18 = \begin{cases} 1+17 \\ 5+13 \end{cases} & & & \\
22 = 5+17 & & 82 = \begin{cases} 29+53 \\ 41+41 \end{cases} & \\
26 = 13+13 & 58 = \begin{cases} 5+53 \\ 17+41 \\ 29+29 \end{cases} & & 106 = \begin{cases} 5+101 \\ 17+89 \\ 53+53 \end{cases} \\
30 = \begin{cases} 1+29 \\ 13+17 \end{cases} & & 86 = 13+73 & \\
34 = \begin{cases} 5+29 \\ 17+17 \end{cases} & 62 = 1+61 & & \\
38 = 1+37 & & 90 = \begin{cases} 1+89 \\ 17+73 \\ 29+61 \\ 37+53 \end{cases} & 110 = \begin{cases} 1+109 \\ 13+97 \\ 37+73 \end{cases} \\
42 = \begin{cases} 1+41 \\ 5+37 \\ 13+29 \end{cases} & 66 = \begin{cases} 5+61 \\ 13+53 \\ 29+37 \end{cases} & & \\
 & 70 = \begin{cases} 17+53 \\ 29+41 \end{cases} & 94 = \begin{cases} 5+89 \\ 41+53 \end{cases} &
\end{array}
$$

4. Talis ergo resolutio usque ad numerum 110 feliciter successit; ac si quis hunc laborem continuare voluerit, non solum semper succedere, sed etiam continuo plures resolutiones locum habere deprehendet. Interim tamen conclusio nimis foret lubrica, si quis hinc inferre vellet omnes plane numeros formae $4n + 2$ semper esse resolubiles in duos numeros [primos] formae $4n + 1$. Quanquam plerumque plures resolutiones locum inveniunt, tamen eiusmodi casus non desunt, ubi unica tantum resolutio successit, veluti in numeris 26, 38, 50, 62, 86; unde obiici posset non solum tales casus etiam in maioribus numeris occurrere, sed etiam fortasse evenire posse, ut talis resolutio plane falleret, etiamsi hoc eo minus verendum videtur, quo longius processerimus. Verum tamen quoque concedere debemus numeros primos formae $4n + 1$ continuo fieri rariores, ita ut plures resolutiones ob hanc caussam excludantur. Quin etiam, si numeri primi formae $4n + 1$ in maximis penitus cessarent, tum talis resolutio non amplius locum habere posset. At cum iam EUCLIDES demonstraverit multitudinem numerorum primorum revera esse infinitam, id etiam valere debet pro numeris primis formae $4n + 1$, qui propterea nunquam plane deficere poterunt.

5. Ob istas rationes igitur huic assertioni insistere non convenit, quod omnes plane numeri formae $4n + 2$ resolutionem in binos primos formae

1) Editio princeps: 97. Correxit R. F.
2) Editio princeps: 37. Correxit R. F.

$4n + 1$ admittant, etiamsi fortasse certum sit et aliquando rigida demonstratione confirmari queat. Interim tamen manifestum est, si multitudo numerorum formae $4n + 1$, quibus in his resolutionibus sumus usi, maior esset, quam hic assumsimus, multo minus eiusmodi casus fore metuendos, qui talem resolutionem respuerent. Illis autem numeris omni iure adiungere poterimus omnes numeros quadratos formae $4n + 1$, quippe qui numeris primis formae $4n + 1$ additi producunt numeros adeo in ternos quadratos resolubiles; quamobrem ad illos numeros formae $4n + 1$ adiiciamus quoque quadrata imparia, et usque ad centenarium nanciscemur pro nostris resolutionibus sequentes numeros:

1, 5, 9, 13, 17, 25, 29, 37, 41, 49, 53, 61, 73, 81, 89, [97].

6. Videamus igitur, quomodo resolutiones numerorum formae $4n + 2$ in huiusmodi binas partes succedant.

$$
\begin{array}{l|l|l|l}
2 = 1+1 & 42 = \begin{cases} 1+41 \\ 5+37 \\ 13+29 \\ 17+25 \end{cases} & 62 = \begin{cases} 1+61 \\ 9+53 \\ 13+49 \\ 25+37 \end{cases} & 82 = \begin{cases} 1+81 \\ 29+53 \\ 41+41 \\ 9+73 \end{cases} \\
6 = 1+5 & & & \\
10 = \begin{cases} 1+9 \\ 5+5 \end{cases} & & & \\
14 = \begin{cases} 1+13 \\ 5+9 \end{cases} & 46 = \begin{cases} 5+41 \\ 9+37 \\ 17+29 \end{cases} & 66 = \begin{cases} 5+61 \\ 13+53 \\ 17+49 \\ 25+41 \\ 29+37 \end{cases} & 86 = \begin{cases} 5+81 \\ 13+73 \\ 25+61 \\ 37+49 \end{cases} \\
18 = \begin{cases} 1+17 \\ 5+13 \\ 9+9 \end{cases} & 50 = \begin{cases} 1+49 \\ 9+41 \\ 13+37 \\ 25+25 \end{cases} & & \\
22 = \begin{cases} 5+17 \\ 9+13 \end{cases} & & 70 = \begin{cases} 9+61 \\ 17+53 \\ 29+41 \end{cases} & 90 = \begin{cases} 1+89 \\ 9+81 \\ 17+73 \\ 29+61 \\ 37+53 \\ 41+49 \end{cases} \\
26 = \begin{cases} 1+25 \\ 9+17 \\ 13+13 \end{cases} & 54 = \begin{cases} 1+53 \\ 5+49 \\ 13+41 \\ 17+37 \\ 25+29 \end{cases} & 74 = \begin{cases} 1+73 \\ 13+61 \\ 25+49 \\ 37+37 \end{cases} & \\
30 = \begin{cases} 1+29 \\ 5+25 \\ 13+17 \end{cases} & & & 94 = \begin{cases} 5+89 \\ 13+81 \\ 41+53 \end{cases} \\
34 = \begin{cases} 5+29 \\ 9+25 \\ 17+17 \end{cases} & 58 = \begin{cases} 5+53 \\ 9+49 \\ 17+41 \\ 29+29 \end{cases} & 78 = \begin{cases} 5+73 \\ 17+61 \\ 25+53 \\ 29+49 \\ 37+41 \end{cases} & \\
38 = \begin{cases} 1+37 \\ 9+29 \\ 13+25 \end{cases} & & & 98 = \begin{cases} 1+97 \\ 9+89 \\ 17+81 \\ 25+73 \\ 37+61 \\ 49+49 \end{cases}
\end{array}
$$

7. Adiectis igitur quadratis ad nostros numeros primos formae $4n + 1$, omnes resolutiones tam notabiliter increverunt, et manifesto in maioribus numeris multo magis increscent, ut nullo modo metuendum videatur, ut unquam unica tantum resolutio, multo minus plane nulla sit successura; hocque modo inductio supra facta iam tantopere est corroborata, ut solidae demonstrationi aequiparare posse videatur. Sin autem nihilominus aliquis adhuc obiicere vellet rem nondum satis esse comprobatam, is tamen concedere erit coactus, si multitudinem numerorum illorum formae $4n + 1$ insuper augere liceret, tum plane nulli amplius obiectioni locum relinqui.

8. Quoniam enim numeri illi formae $4n + 1$ ad nostrum scopum eatenus sunt accommodati, quatenus sunt vel ipsi quadrati, vel in duos quadratos resolubiles, iis insuper adiungi poterunt producta ex binis pluribusve numeris eiusdem generis; siquidem demonstratum est productum ex duobus pluribusve numeris, qui singuli sint summae duorum quadratorum, semper etiam in duo quadrata resolvi posse. Quocirca ad superiorem classem istorum numerorum adhuc adiungere poterimus sequentes:

45, 65, 85, 117, 125, 145, 153, 185, 205, 221 [etc.].

His autem numeris adiectis manifestum est numerum omnium resolutionum tantopere, et continuo magis augeri, ut plane impossibile sit, ut talis resolutio unquam fallere posset. Ita cum in praecedentibus resolutionibus numerus 82 tantum quatuor resolutiones habuerit, nunc sequentes locum habebunt:

$$82 = 1 + 81,\ 9 + 73,\ 17 + 65,\ 29 + 53,\ 37 + 45,\ 41 + 41,$$

sicque duae novae resolutiones accesserunt. Quamobrem his rationibus veritas theorematis, quod omnis numerus sit summa quatuor quadratorum, prorsus extra omne dubium posita est censenda. Interim tamen facile concedimus hanc demonstrationem non tanta evidentia esse praeditam, quanta in rigidis demonstrationibus desiderari solet.

DE RESOLUTIONE NUMERORUM IN TERNOS TRIGONALES

9.[1]) Si numerus N fuerit summa trium trigonalium, hoc est

$$N = \frac{xx+x}{2} + \frac{yy+y}{2} + \frac{zz+z}{2},$$

1) Ab hoc numeri paragraphorum in editione principe sunt: 5, 6, 7, 8, 9, 10, 11. R. F.

erit

$$8N + 3 = (2x + 1)^2 + (2y + 1)^2 + (2z + 1)^2 .$$

Quodsi igitur demonstrari queat omnes numeros formae $8N + 3$ esse summas trium quadratorum, tum etiam demonstratum erit omnes plane numeros N esse summas trium trigonalium; forma enim $8N + 3$ nonnisi tribus quadratis imparibus aequalis esse potest. Unde si fuerit

$$8N + 3 = (2x + 1)^2 + (2y + 1)^2 + (2z + 1)^2 ,$$

erit vicissim

$$N = \frac{xx + x}{2} + \frac{yy + y}{2} + \frac{zz + z}{2} ,$$

ideoque summa trium trigonalium.

10. Nunc in subsidium vocemus theorema supra memoratum, quod omnis numerus primus formae $4n + 1$ sit summa duorum quadratorum, ideoque $4n + 1 = aa + bb$; atque evidens est etiam eius duplum $8n + 2$ fore summam duorum quadratorum; est enim

$$8n + 2 = (a + b)^2 + (a - b)^2 .$$

Quod si ergo singulis his numeris $8n + 2$ addamus quadrata imparia, quae sunt formae $8m + 1$, aggregata erunt utique summae trium quadratorum; horum autem aggregatorum forma erit $8n + 3$; quocirca quaestio huc redit: num omnes numeri formae $8N + 3$ ita in duas partes dividi queant, ut una sit quadratum impar, altera duplum numeri primi formae $4n + 1$; quod ut in minoribus numeris saltem exploremus, ista dupla usque ad 200 ordine exponamus:

2, 10, 26, 34, 58, 74, 82, 106, 122, 146, 178, 194, 202.

11. Nunc igitur omnes numeros formae $8N + 3$ percurramus et videamus, an omnes componi queant ex quopiam numero huius ordinis et quadrato impari, quae ad eundem terminum usque sunt

1, 9, 25, 49, 81, 121, 169, 225,

quod tentamen ita repraesentetur:

$$
\begin{array}{rl}
3 = & 1 + 2 \\
11 = & \left\{\begin{array}{l} 1 + 10 \\ 9 + 2 \end{array}\right. \\
19 = & 9 + 10 \\
27 = & \left\{\begin{array}{l} 1 + 26 \\ 25 + 2 \end{array}\right. \\
35 = & \left\{\begin{array}{l} 1 + 34 \\ 9 + 26 \\ 25 + 10 \end{array}\right. \\
43 = & 9 + 34 \\
51 = & \left\{\begin{array}{l} 25 + 26 \\ 49 + 2 \end{array}\right. \\
59 = & \left\{\begin{array}{l} 1 + 58 \\ 25 + 34 \\ 49 + 10 \end{array}\right. \\
67 = & 9 + 58
\end{array}
\qquad
\begin{array}{rl}
75 = & \left\{\begin{array}{l} 1 + 74 \\ 49 + 26 \end{array}\right. \\
83 = & \left\{\begin{array}{l} 1 + 82 \\ 9 + 74 \\ 25 + 58 \\ 49 + 34 \\ 81 + 2 \end{array}\right. \\
91 = & \left\{\begin{array}{l} 9 + 82 \\ 81 + 10 \end{array}\right. \\
99 = & 25 + 74 \\
107 = & \left\{\begin{array}{l} 1 + 106 \\ 25 + 82 \\ 49 + 58 \\ 81 + 26 \end{array}\right. \\
115 = & \left\{\begin{array}{l} 9 + 106 \\ 81 + 34 \end{array}\right.
\end{array}
\qquad
\begin{array}{rl}
123 = & \left\{\begin{array}{l} 1 + 122 \\ 49 + 74 \\ 121 + 2 \end{array}\right. \\
131 = & \left\{\begin{array}{l} 9 + 122 \\ 25 + 106 \\ 49 + 82 \\ 121 + 10 \end{array}\right. \\
139 = & 81 + 58 \\
147 = & \left\{\begin{array}{l} 1 + 146 \\ 25 + 122 \\ 121 + 26 \end{array}\right. \\
155 = & \left\{\begin{array}{l} 9 + 146 \\ 49 + 106 \\ 81 + 74 \\ 121 + 34 \end{array}\right.
\end{array}
\qquad
\begin{array}{rl}
163 = & 81 + 82 \\
171 = & \left\{\begin{array}{l} 25 + 146 \\ 49 + 122 \\ 169 + 2 \end{array}\right. \\
179 = & \left\{\begin{array}{l} 1 + 178 \\ 121 + 58 \\ 169 + 10 \end{array}\right. \\
187 = & \left\{\begin{array}{l} 9 + 178 \\ 81 + 106 \end{array}\right. \\
[195 = & \left\{\begin{array}{l} 1 + 194 \\ 169 + 26 \\ 49 + 146 \\ 121 + 74] \end{array}\right.
\end{array}
$$

12. Hinc igitur iam sine nimia temeritate concludi videatur omnes plane numeros formae $8n + 3$ resolvi posse in duas partes, quarum altera sit quadratum, altera autem duplum numeri primi $4n + 1$. Cum enim numerus quadratorum, quae adhiberi possunt, continuo crescat, combinationum numerus etiam continuo magis augetur; unde si talis resolutio usquam falleret, in minoribus numeris fallere debuisset. Interim tamen, quia hic occurrerunt eiusmodi casus, qui unam tantum resolutionem admittunt, veluti contigit in numeris 67, 99, 139, 163, quoniam tales sine dubio in sequentibus non deerunt, non immerito vereri licet, ne talis resolutio uspiam plane deficiat. Quanquam igitur ista conclusio forsitan veritate consentanea esse queat, tamen ei non confidamus.

13. Cum autem classis illa numerorum $8n + 2$ haud mediocrem amplificationem admittat, dum scilicet quadrata imparia duplicata ipsis adiungimus, quippe quae per se sunt summae duorum quadratorum, prorsus non amplius erit metuendum, ne unquam resolutio fiat impossibilis. Praeterea vero etiam insuper dupla eorum numerorum compositorum formae $4n + 1$, qui scilicet sint producta ex duobus pluribusve numeris primis eiusdem formae, adiicere poterimus, unde istorum omnium numerorum formae $8n + 2$ haec progressio resultabit:

2, 10, 18, 26, 34, 50, 58, 74, 82, 90, 98, 106, 122,
130, 146, 162, 170, 178, 194, 202 etc.

14. Hos igitur novos numeros in subsidium vocando resolvamus eos tantum numeros, qui in superiori tabula unicam resolutionem admiserunt, hoc modo:

$$\begin{aligned}
19 &= 1 + 18 = 9 + 10 \\
43 &= 9 + 34 = 25 + 18 \\
67 &= 9 + 58 = 49 + 18 \\
99 &= 1 + 98 = 9 + 90 = 25 + 74 = 49 + 50 = 81 + 18 \\
139 &= 9 + 130 = 49 + 90 = 81 + 58 = 121 + 18 \\
163 &= 1 + 162 = 81 + 82
\end{aligned}$$

Hic igitur videmus ad minimum unam resolutionem accessisse, in maioribus autem numeris adhuc plures accedere debebunt. His igitur probe perpensis Geometrae iudicent, utrum haec inductio, tot rationibus corroborata, non solidae demonstrationi aequivalere sit censenda.

15. Quanquam autem haec conclusio nulla ulteriori confirmatione indigere videtur, tamen ex alio principio prorsus diverso haud exiguum firmamentum afferri potest, scilicet: quod omnes numeri primi formae $8n + 3$ semper sint formae $2aa + bb$, ideoque per se in tria quadrata resolubiles, id quod iam solide est demonstratum[1]). Hinc autem sequitur etiam eosdem numeros primos octenario auctos etiam esse summas trium quadratorum. Si enim fuerit $8n + 3 = 2aa + bb$, erit

$$8n + 11 = (a + 2)^2 + (a - 2)^2 + bb\,,$$

quamobrem iam certi sumus superiorem resolutionem nunquam in numeris primis $8n + 3$, neque etiam in sequentibus $8n + 11$ fallere posse; atque hoc etiam valet de numeris $8n + 35$; siquidem est

$$8n + 35 = (a + 4)^2 + (a - 4)^2 + bb\,,$$

1) Vide notam 1 p. 485, vol. 2 seriei I. R. F.

quod proinde etiam valebit de omnibus his numeris $8n + 3 + 8pp$, denotante p numerum quemcunque. Porro vero, cum etiam demonstratum sit omnes numeros primos formae $8n + 1$ esse quoque numeros formae $2aa + bb$, talia producta duorum numerorum primorum $(8p + 1)(8q + 3)$, qui utique sunt numeri formae $8n + 3$, semper esse numeros eiusdem formae $2aa + bb$, ideoque istos numeros sive octenario, sive numero 32, sive in genere numero $8rr$ auctos, certe esse summas trium quadratorum. His igitur considerationibus adiunctis theorema FERMATIANUM de numeris trigonalibus summo rigore demonstratum censeri debebit. Interim tamen fateri cogimur hoc modo necessitatem, cur ita fieri debeat, non clare perspici posse.

CONSIDERATIONES SUPER THEOREMATE FERMATIANO DE RESOLUTIONE NUMERORUM IN NUMEROS POLYGONALES

Commentatio 586 indicis ENESTROEMIANI
Opuscula analytica 2, 1785, p. 3—15
[Conventui exhibita die 12. decembris 1774]

1. Hoc theorema FERMATIANUM[1]) in se complectitur sequentes assertiones numero infinitas:

I. *Omnem numerum esse summam trium trigonalium vel pauciorum.*
II. *Omnem numerum esse summam quatuor tetragonalium seu quadratorum vel pauciorum.*
III. *Omnem numerum esse summam quinque pentagonalium, vel pauciorum.*
IV. *Omnem numerum esse summam sex hexagonalium vel pauciorum.*
V. *Omnem numerum esse summam septem heptagonalium vel pauciorum.*
etc.

Quorum theorematum cum FERMATIUS asseverasset demonstrationem a se esse inventam, dubitari certe nequit eius demonstrationem certissimis principiis fuisse innixam; ex quo eo magis dolendum est eam post eius obitum prorsus periisse, ut nullum plane vestigium reperiri potuerit, cum sine dubio plerique Geometrae in his demonstrationibus investigandis frustra desudaverint. Hinc quidem excipienda est secunda assertio de resolutione numerorum in quatuor quadrata, cuius perfecta demonstratio ab Ingeniosissimo LA GRANGE[2]) in lucem est protracta, quae autem ex eiusmodi prin-

1) Vide notam 1, p. 65 huius voluminis. R. F.
2) Vide notam 2, p. 65 huius voluminis. R. F.

cipiis est deducta, ut inde nullum plane subsidium ad reliqua demonstranda exspectari possit.

2. Ingens igitur discrimen inter resolutionem in quadrata et reliquos numeros polygonales intercedere est censendum, quod potissimum in hoc consistit, quod resolutio in quaterna quadrata ad omnes plane numeros tam fractos quam integros se extendat, cum resolutio in alios polygonales tantum ad numeros integros restringatur, atque adeo nonnisi sub certa limitatione veritati sit consentanea. Resolutio enim in ternos trigonales manifesto tantum ad numeros integros adstringitur, cum infinitae dentur fractiones, quas nullo modo in ternas partes, in formula $\frac{xx+x}{2}$ contentas, resolvere licet; veluti si pro fractione $\frac{1}{2}$ statuere vellemus

$$\frac{1}{2} = \frac{xx+x}{2} + \frac{yy+y}{2} + \frac{zz+z}{2},$$

multiplicando per 8 deberet esse

$$4 = 4xx + 4x + 4yy + 4y + 4zz + 4z,$$

hincque tribus unitatibus additis fieret

$$7 = (2x+1)^2 + (2y+1)^2 + (2z+1)^2.$$

Demonstratum autem est numerum 7 nullo modo esse posse summam trium quadratorum. Quocirca si quis demonstrationem huius partis ita instituere voluerit, ut, proposito numero quocunque N, hanc aequationem:

$$N = \frac{xx+x}{2} + \frac{yy+y}{2} + \frac{zz+z}{2}$$

sibi resolvendam proponeret, oleum atque operam perdiderit.

3. Porro vero etiam resolutio in quinque pentagonales ad numeros integros adstringitur, sed longe alio modo atque in trigonalibus usu venit. Nam si inter numeros pentagonales etiam fractiones in formula $\frac{3xx-x}{2}$ contentas admittere velimus, tum omnes plane numeros adeo in quatuor

pentagonales discerpere liceret. Proposito enim numero quocunque N si statuamus

$$N = \frac{3xx - x}{2} + \frac{3yy - y}{2} + \frac{3zz - z}{2} + \frac{3vv - v}{2},$$

per 24 multiplicando fiet

$$24N = 36xx - 12x + 36yy - 12y + 36zz - 12z + 36vv - 12v,$$

unde quatuor unitatibus additis fiet

$$24N + 4 = (6x - 1)^2 + (6y - 1)^2 + (6z - 1)^2 + (6v - 1)^2.$$

Cum igitur numerus $24N + 4$ certo sit summa quatuor quadratorum, quae sit $aa + bb + cc + dd$, hinc reperiemus

$$x = \frac{a+1}{6}, \quad y = \frac{b+1}{6}, \quad z = \frac{c+1}{6}, \quad v = \frac{d+1}{6},$$

atque horum radicum numeri pentagonales iunctim sumti numero proposito N aequabuntur. Nihilo vero minus si tantum numeros integros admittamus, uti FERMATIUS manifesto postulat, utique dantur eiusmodi numeri, quos in pauciores quam quinque pentagonales neutiquam resolvere licet.

4. Praeterea vero, etiamsi hinc fractiones excludamus et tantum numeros integros admittere velimus, tamen novam limitationem adiicere, atque ex ordine pentagonalium omnes eos, quorum radices sunt numeri negativi, excludere debemus. Cum enim formula generalis numerorum pentagonalium $\frac{3xx - x}{2}$ pro radicibus x negative sumtis praebeat hos numeros: 2, 7, 15, 26, 40 etc., si etiam hos admittere vellemus, non amplius quinque, sed tantum tres numeri pentagonales sufficerent omnibus plane numeris producendis, atque talis gemina limitatio multo magis pro sequentibus numeris polygonalibus est necessaria, ut theoremata FERMATIANA veritati sint consentanea, quae limitatio sine dubio in caussa est, quod nulli adhuc Geometrae post FERMATIUM ad demonstrationem horum casuum penetrare licuerit.

5. Cum igitur in demonstrationibus, quae desiderantur, harum restrictionum ratio necessario sit habenda, ipsa theoremata FERMATIANA sub alia forma repraesentemus, quae istas limitationes iam in se contineat, quod commodissime sequenti modo fieri posse videtur.

PRO RESOLUTIONE IN NUMEROS TRIGONALES

6. Consideretur series potestatum

$$1 + x + x^3 + x^6 + x^{10} + x^{15} + x^{21} + x^{28} + x^{36} + x^{45} + \text{etc.},$$

in qua potestates ipsius x progrediuntur secundum ipsos numeros trigonales

$$0,\ 1,\ 3,\ 6,\ 10,\ 15,\ 21,\ 28 \text{ etc.},$$

ac primo manifestum est, si huius seriei quadratum capiatur, alias potestates ipsius x occurrere non posse, nisi quarum exponentes sint summae duorum numerorum trigonalium. Eodem modo intelligitur, si eiusdem seriei capiatur cubus, in eo alias potestates non occurrere, nisi quarum exponentes sint summae trium numerorum trigonalium. Quocirca primum theorema FERMATII huc reducitur, ut, si pro cubo assumtae seriei statuatur haec series per omnes potestates ipsius x ascendens:

$$1 + Ax + Bxx + Cx^3 + Dx^4 + Ex^5 + Fx^6 + Gx^7 + Hx^8 + \text{etc.},$$

demonstretur in hac serie nullum plane coefficientem nihilo fore aequalem. Ex ipsa autem formatione manifestum est nullum horum coefficientium fieri posse negativum.

PRO RESOLUTIONE IN NUMEROS TETRAGONALES SEU QUADRATOS

7. Hic consideretur ista series potestatum:

$$P = 1 + x + x^4 + x^9 + x^{16} + x^{25} + x^{36} + \text{etc.},$$

cuius biquadratum P^4, si evolvatur, omnes complectetur potestates ipsius x, quarum exponentes sunt summae quatuor quadratorum; atque adeo cuius-

que coefficiens ostendet, quot variis modis exponens ipsius x in quatuor quadrata distribui queat; quare pro hoc casu demonstrari oportet, si ponatur

$$P^4 = 1 + Ax + Bxx + Cx^3 + Dx^4 + Ex^5 + Fx^6 + \text{etc.},$$

quae scilicet series per omnes potestates ipsius x ascendat, nullum coefficientium A, B, C, D, E etc. esse evaniturum. Hoc enim si fuerit demonstratum, simul erit evictum omnes plane numeros in quatuor quadrata resolvi posse[1]).

PRO RESOLUTIONE IN NUMEROS PENTAGONALES

8. Consideretur series potestatum ipsius x, quarum exponentes secundum numeros pentagonales ascendant, quae sit

$$P = 1 + x + x^5 + x^{12} + x^{22} + x^{35} + x^{51} + \text{etc.},$$

eiusque evolvatur potestas quinta, quae sit

$$P^5 = 1 + Ax + Bx^2 + Cx^3 + Dx^4 + Ex^5 + \text{etc.}$$

per omnes plane potestates ipsius x ascendens, ac demonstrandum est in hac serie nullum prorsus coefficientem reperiri, qui sit nihilo aequalis.

PRO RESOLUTIONE IN NUMEROS POLYGONALES QUOSCUNQUE

9. Sit π numerus laterum polygonorum, et cum formula generalis omnes istos numeros polygonales complectens sit $= \frac{1}{2}(\pi - 2)zz - \frac{1}{2}(\pi - 4)z$, posita scilicet radice $= z$, sint omnes numeri polygonales hinc ordine resultantes $0, \alpha, \beta, \gamma, \delta, \varepsilon, \zeta, \eta$ etc., ubi quidem constat esse

$$\alpha = 1,\ \beta = \pi,\ \gamma = 3\pi - 3,\ \delta = 6\pi - 8,\ \varepsilon = 10\pi - 15,\ \zeta = 15\pi - 24 \text{ etc.};$$

tum vero consideretur series infinita

1) Eodem modo theorema demonstratum fuit a C. G. J. Jacobi: *Gesammelte Werke*, Band I. Berlin, 1881, p. 239. R. F.

$$P = 1 + x^\alpha + x^\beta + x^\gamma + x^\delta + x^\varepsilon + x^\zeta + \text{etc.}$$

huiusque seriei sumatur potestas exponentis $= \pi$, quae sit

$$P^\pi = 1 + Ax + Bxx + Cx^3 + Dx^4 + Ex^5 + \text{etc.}$$

per omnes plane potestates ipsius x ascendens, ac demonstrandum erit in hac serie nullum occurrere coefficientem nihilo aequalem; unde patet, si modo hoc demonstrari in genere posset, simul omnia theoremata FERMATIANA fore demonstrata.

10. In hoc igitur negotio non parum fortasse proderit, si evolutionem istius potestatis P^π in genere docuero, simulque ostendero, quomodo omnes coefficientes seriei evolutae a praecedentibus pendeant, ex iisque determinentur. Hunc in finem coefficientes singularum potestatum ipsius x idoneis characteribus designemus, sitque potestatis x^n coefficiens $[n]$; quandoquidem hoc modo statim perspicitur, ad quamnam potestatem quisque coefficiens referatur. Nunc igitur investigemus, quomodo quilibet coefficiens $[n]$ ex praecedentibus, qui sunt $[n-1]$, $[n-2]$, $[n-3]$, $[n-4]$ etc., determinetur. Hoc enim modo iudicium facillime instituetur, num quis coefficiens nihilo aequalis fieri possit, id quod forsan eo facilius ostendi poterit, cum certum sit nullum coefficientem fieri posse negativum.

11. Cum igitur posito

$$P = 1 + x^\alpha + x^\beta + x^\gamma + x^\delta + x^\varepsilon + \text{etc.}$$

quaeri debeat istius seriei potestas exponentis π, statuamus $S = P^\pi$, eritque sumtis logarithmis $lS = \pi lP$, hincque differentiando $\frac{dS}{S} = \frac{\pi dP}{P}$, unde formetur ista aequatio:

$$P\frac{x\,dS}{dx} = \frac{\pi S x\,dP}{dx},$$

pro qua ergo erit

$$\frac{x\,dP}{dx} = \alpha x^\alpha + \beta x^\beta + \gamma x^\gamma + \delta x^\delta + \varepsilon x^\varepsilon + \zeta x^\zeta + \text{etc.},$$

quae ergo series per λS multiplicata idem productum generare debet, quod oritur, si ipsa series

$$P = 1 + x^\alpha + x^\beta + x^\gamma + x^\delta + \text{etc.}$$

per formulam $\frac{xdS}{dx}$ multiplicetur.

12. Ponatur igitur secundum characteres ante descriptos:

$$S^{1}) = 1 + [1]\, x + [2]\, x^2 + [3]\, x^3 + [4]\, x^4 + \text{etc.},$$

ubi notetur primum terminum 1 aequivalere termino [0], unde fiet

$$\frac{xdS}{dx} = 1\,[1]\, x^1 + 2\,[2]\, x^2 + 3\,[3]\, x^3 + 4\,[4]\, x^4 + \text{etc.},$$

hisque seriebus constitutis perpendamus, quot modis proposita potestas x^n in utroque producto $P\frac{xdS}{dx}$ et $\pi\frac{SxdP}{dx}$ occurrat.

13. Cum igitur ambo multiplicatores P et $\frac{xdP}{dx}$ alias potestates ipsius x non contineant, nisi quarum exponentes sunt α, β, γ, δ etc., manifestum est seriei S terminum $[n]x^n$ ex aliis terminis praecedentibus resultare non posse, praeter hos:

$$[n-\alpha]x^\alpha, \quad [n-\beta]x^\beta, \quad [n-\gamma]x^\gamma \text{ etc.};$$

quamobrem omissis reliquis terminis consideremus tantum istos, ita ut habeamus:

$$S = [n]x^n \cdots + [n-\alpha]x^{n-\alpha} \cdots + [n-\beta]x^{n-\beta} \cdots + [n-\gamma]x^{n-\gamma} \cdots + \text{etc.},$$

ubi per se manifestum est hos terminos tantum eo usque continuari debere, quoad exponentes $[n-\alpha]$, $[n-\beta]$, $[n-\gamma]$ etc. non fiunt negativi. Multiplicetur igitur ista forma per

$$\frac{\pi xdP}{dx} = \pi\alpha x^\alpha + \pi\beta x^\beta + \pi\gamma x^\gamma + \pi\delta x^\delta + \text{etc.}$$

1) Editio princeps: *R.* Correxit A. M.

et productum sequentes terminos potestatem x^n continentes suppeditabit:

$$\pi\alpha\,[n-\alpha]\,x^n + \pi\beta\,[n-\beta]\,x^n + \pi\gamma\,[n-\gamma]\,x^n + \text{etc.}$$

14. Deinde iisdem terminis retentis erit

$$\frac{x\,dS}{dx} = n\,[n]\,x^n \cdots + (n-\alpha)\,[n-\alpha]\,x^{n-\alpha} \cdots + (n-\beta)\,[n-\beta]\,x^{n-\beta} \cdots + (n-\gamma)\,[n-\gamma]\,x^{n-\gamma} \cdots + (n-\delta)\,[n-\delta]\,x^{n-\delta} \cdots + \text{etc.},$$

quae forma ducta in seriem

$$P = 1 + x^\alpha + x^\beta + x^\gamma + x^\delta + \text{etc.}$$

sequentes praebebit terminos potestatem x^n continentes:

$$n\,[n]\,x^n + (n-\alpha)\,[n-\alpha]\,x^n + (n-\beta)\,[n-\beta]\,x^n + (n-\gamma)\,[n-\gamma]\,x^n + \text{etc.}$$

Quamobrem cum hoc productum priori debeat esse aequale, obtinebimus sequentem aequationem:

$$n\,[n] + (n-\alpha)\,[n-\alpha] + (n-\beta)\,[n-\beta] + (n-\gamma)\,[n-\gamma] + \text{etc.} = \pi\alpha\,[n-\alpha] + \pi\beta\,[n-\beta] + \pi\gamma\,[n-\gamma] + \pi\delta\,[n-\delta] + \text{etc.}$$

15. Hinc igitur patet coefficientem $[n]$ ab iis tantum praecedentium, quorum characteres sunt

$$[n-\alpha],\ [n-\beta],\ [n-\gamma] \text{ etc.},$$

pendere, ita ut sit

$$n\,[n] = (\pi\alpha - (n-\alpha))\,[n-\alpha] + (\pi\beta - (n-\beta))\,[n-\beta] + (\pi\gamma - (n-\gamma))\,[n-\gamma] + \text{etc.}$$

Ubi quidem primo non est metuendum, ne ob terminos negativos unquam valor ipsius $[n]$ proditurus sit negativus, quandoquidem hoc naturae rei repugnaret; et quia valor ipsius $[n]$ certe est numerus integer, evidens est omnes terminos in dextro membro iunctim sumtos semper valorem prae-

bere debere vel n, vel $2n$, vel $3n$, vel $4n$, vel etc., nisi forte inde prodeat 0, quod igitur demonstrandum est nunquam eveniri posse, si quidem theorema FERMATIANUM fuerit veritati consentaneum, atque literae α, β, γ, δ etc. denotent ordine omnes numeros polygonales pro numero laterum $= \pi$.

16. Manifestum autem est hanc determinationem coefficientis $[n]$ maxime esse generalem, neque tantum ad numeros polygonales extendi. Quaecunque enim series numerorum pro litteris α, β, γ, δ etc. accipiatur, aequatio inventa semper habebit locum, et coefficiens $[n]$ indicabit, quot variis modis numerus n possit esse summa π terminorum istius seriei:

$$0,\ \alpha,\ \beta,\ \gamma,\ \delta,\ \varepsilon,\ \zeta,\ \eta \text{ etc.},$$

hincque numerus π ita definiri poterit, ut nullus huiusmodi coefficiens $[n]$ prodeat nihilo aequalis. Evidens enim est numerum π semper tantum accipi posse, ut dextrum membrum nostrae aequationis nunquam prodeat negativum. Quaeri autem semper solet minimus valor, qui pro π assumtus hoc sit praestaturus; unde patet hanc methodum ad infinitas alias quaestiones huius generis pari fortasse successu applicari posse.

17. Caeterum in genere notasse iuvabit, nisi fuerit $\alpha = 1$, semper fore $[n] = 0$, quamdiu fuerit $n < \alpha$; unde in omnibus huiusmodi quaestionibus necesse est, ut sit $\alpha = 1$, quem quidem terminum semper praecedere solet terminus $= 0$, siquidem series pro P assumta ab unitate incipiat.

APPLICATIO AD NUMEROS TRIGONALES

18. Quo natura aequationis inventae clarius percipiatur, eam ad numeros trigonales applicemus, pro quibus erit $\alpha = 1$, $\beta = 3$, $\gamma = 6$, $\delta = 10$, $\varepsilon = 15$ etc., tum vero, sumto exponente $\pi = 3$, nostra formula inventa hanc induet formam:

$$n[n] = (4 - n)[n - 1] + (12 - n)[n - 3] + (24 - n)[n - 6] + (40 - n)[n - 10] + \text{etc.}$$

Hinc ergo, a numeris minimis incipiendo, sequentes nanciscemur reductiones:

$1\,[1] = 3\,[0]$, ergo $[1] = 3$

$2\,[2] = 2\,[1] = 6$, ergo $[2] = 3$

$3\,[3] = 1\,[2] + 9\,[0] = 12$, ergo $[3] = 4$

$4\,[4] = 0\,[3] + 8\,[1] = 24$, ergo $[4] = 6$

$5\,[5] = -1\,[4] + 7\,[2] = 15$, ergo $[5] = 3$

$6\,[6] = -2\,[5] + 6\,[3] + 18\,[0] = 36$, ergo $[6] = 6$

$7\,[7] = -3\,[6] + 5\,[4] + 17\,[1] = 63$, ergo $[7] = 9$

$8\,[8] = -4\,[7] + 4\,[5] + 16\,[2] = 24$, ergo $[8] = 3$

$9\,[9] = -5\,[8] + 3\,[6] + 15\,[3] = 63$, ergo $[9] = 7$

$10\,[10] = -6\,[9] + 2\,[7] + 14\,[4] + 30\,[0] = 90$, ergo $[10] = 9$

$11\,[11] = -7\,[10] + 1\,[8] + 13\,[5] + 29\,[1] = 66$, ergo $[11] = 6$

$12\,[12] = -8\,[11] + 0\,[9] + 12\,[6] + 28\,[2] = 108$, ergo $[12] = 9$

$13\,[13] = -9\,[12] - 1\,[10] + 11\,[7] + 27\,[3] = 117$, ergo $[13] = 9$

$14\,[14] = -10\,[13] - 2\,[11] + 10\,[8] + 26\,[4] = 84$, ergo $[14] = 6$

$15\,[15] = -11\,[14] - 3\,[12] + 9\,[9] + 25\,[5] + 45\,[0] = 90$, ergo $[15] = 6$

$16\,[16] = -12\,[15] - 4\,[13] + 8\,[10] + 24\,[6] + 44\,[1] = 240$, ergo $[16] = 15$

$17\,[17] = -13\,[16] - 5\,[14] + 7\,[11] + 23\,[7] + 43\,[2] = 153$, ergo $[17] = 9$

$18\,[18] = -14\,[17] - 6\,[15] + 6\,[12] + 22\,[8] + 42\,[3] = 126$, ergo $[18] = 7$

$19\,[19] = -15\,[18] - 7\,[16] + 5\,[13] + 21\,[9] + 41\,[4] = 228$, ergo $[19] = 12$

$20\,[20] = -16\,[19] - 8\,[17] + 4\,[14] + 20\,[10] + 40\,[5] = 60$, ergo $[20] = 3$

Hinc igitur patet seriei $1 + x + x^3 + x^6 + x^{10} + x^{15} +$ etc. cubum evolvi in hanc seriem:

$$1 + 3x^1 + 3x^2 + 4x^3 + 6x^4 + 3x^5 + 6x^6 + 9x^7 + 3x^8 + 7x^9 + 9x^{10} + 6x^{11} + 9x^{12} + 9x^{13} + 6x^{14} + 6x^{15} + 15x^{16} + 9x^{17} + 7x^{18} + \text{etc.}$$

19. In hac evolutione non iniucundum erat videre, quomodo priora membra negativa a sequentibus positivis semper superentur atque excessus semper per numerum n divisibilis prodierit, id quod etiam perinde in forma generali necessario usu venire debet. Quod quo clarius in oculos incurrat, aequationem generalem sub hac forma exhibeamus:

$$n[n] = ((\pi + 1)\alpha - n)[n - \alpha] + ((\pi + 1)\beta - n)[n - \beta] + ((\pi + 1)\gamma - n)[n - \gamma] \text{ etc.},$$

unde partibus negativis ad sinistram translatis erit

$$n\,([n] + [n - \alpha] + [n - \beta] + [n - \gamma] + [n - \delta] + \text{etc.})$$
$$= (\pi + 1)\,(\alpha[n - \alpha] + \beta[n - \beta] + \gamma[n - \gamma] + \delta[n - \delta] + \text{etc.})\,.$$

Hinc igitur intelligimus: primo summam omnium horum valorum

$$\alpha[n - \alpha] + \beta[n - \beta] + \gamma[n - \gamma] + \text{etc.}$$

semper fore divisibilem per numerum n, nisi forte $\pi + 1$ fuerit per n divisibile; deinde summam horum valorum

$$[n] + [n - \alpha] + [n - \beta] + [n - \gamma] + \text{etc.}$$

semper esse divisibilem per numerum $\pi + 1$, nisi forte ipse numerus n per eum divisionem admittat.

20. Neque vero hae eximiae proprietates tantum in numeris polygonalibus, quos hic potissimum contemplamur, locum habent, sed etiam generalissime observari debent, quaecunque numerorum series pro litteris α, β, γ etc. assumatur, etiamsi ea nulli certae legi fuerit adstricta. Ad vero haec ipsa circumstantia non multum pro scopo nostro polliceri videtur, quandoquidem theoremata FERMATIANA tum demum veritati consentanea censeri debent, quando pro litteris α, β, γ, δ etc. ipsi numeri polygonales ordine scribuntur; ita ut, si earum ordo tantillum perturbaretur, demonstratio etiam ipsa hinc petenda claudicare deberet; quocirca ad legitimam demonstrationem horum theorematum inveniendam necessario opus erit, ut simul etiam ipsa lex progressionis litterarum α, β, γ, δ etc. in computum ducatur, id quod utrum cum ista methodo commode coniungi queat, necne, non tam facile perspicitur. Interim tamen istae considerationes fortasse aliis aliquam lucem accendere poterunt, quo felicius ad has veritates penetrare valeant.

DE RELATIONE INTER TERNAS PLURESVE QUANTITATES INSTITUENDA

Commentatio 591 indicis Enestroemiani
Opuscula analytica 2, 1785, p. 91—101
[Conventui exhibita die 14. augusti 1775]

1. Propositis duabus quantitatibus A et B, earum relatio seu ratio definitur, dum quaeruntur duo numeri integri α et β, iique minimi, ut fiat $\alpha A = \beta B$; unde si quantitates A et B fuerint inter se commensurabiles, istos numeros α et β semper accurate assignare licebit; sin autem sint incommensurabiles, numeros α et β ita dare licebit, ut discrimen inter formulas αA et βB sit minimum, vel ita parvum, ut propius ad aequalitatem inter has formulas αA et βB accedi nequeat, nisi pro α et β maiores numeri adhibeantur. Hocque modi solvi solet problema olim a Wallisio propositum[1]), quo, propositis duobus numeris quantumvis magnis A et B, rationes in minoribus numeris requiruntur, qui tam exacte eorum rationem exprimant, quam fieri potest numeris non maioribus adhibendis.

2. Simili modo si tres proponantur quantitates A, B et C, reperiri poterunt tres numeri integri α, β et γ, ut fiat $\alpha A = \pm \beta B \mp \gamma C$; et quidem omnes possibiles valores pro his numeris α, β, γ assignare licebit, quibus inventis haud difficile erit minimos numeros pro α, β et γ exhibere, atque hoc modo relatio inter ternas quantitates propositas A, B et C planissime indicari videtur. Methodus autem hos tres numeros α, β, γ investigandi similis erit illi, qua relatio inter duas tantum quantitates definiri solet, et

1) Confer Johannis Wallis S. T. D. *Opera mathematica*. Oxoniae 1693, volumen alterum, p. 418 et sequentes. R. F.

quae eiusmodi operationibus absolvitur, quibus maximus communis divisor duorum numerorum indagari solet, id quod sequenti exemplo illustremus.

3. Propositae igitur sint tres sequentes quantitates: $A = 49$, $B = 59$ et $C = 75$, et quaerantur numeri a, b, c, ut fiat $49a + 59b + 75c = 0$, ubi quidem a, b, c numeros integros, sive positivos sive negativos significent. Iam dividatur aequatio illa per minimam propositarum quantitatum, scilicet per 49, et quoti ex posterioribus terminis oriundi resolvantur in partes integras et fractas ac seorsim exhibeantur; quae quoniam iunctim sumtae nihilo debent aequari, partes integras statuamus aequales numero integro $+ d$, fractae autem eidem numero negativo $-d$; hocque modo duae hinc nascentur aequationes

$$a + b + c = d \quad \text{et} \quad \frac{10b + 26c}{49} = -d .$$

Iam ex postrema aequatione fit $10b + 26c + 49d = 0$, quae prorsus ut prima tractetur, scilicet per 10 divisa dabit

$$b + 2c + 4d = +3e \quad \text{et} \quad \frac{6c + 9d}{10} = -3e .$$

Hic scilicet, quia numeri 6 et 9 communem divisorem habent 3, loco simplicis litterae e statim scripsimus $3e$, sicque nova aequatio erit $2c + 3d + 10e = 0$, quae, per 2 divisa, similique modo distributa, suppeditat has aequationes:

$$c + d + 5e = +f \quad \text{et} \quad \frac{d}{2} = -f ,$$

quae ultima statim dat $d = -2f$, atque hic operationes terminantur, quoniam nullae amplius insunt fractiones.

4. Cum igitur esse debeat $d = -2f$, littera autem e non sit determinata, per has duas litteras e et f praecedentes sequenti modo regrediendo definientur:

$$c = 3f - 5e, \; b = 13e + 2f \text{ et } a = -8e - 7f .$$

Solutio ergo generalis nostrae quaestionis, sive relatio inter ternos numeros propositos 49, 59, 75 sequenti aequatione continebitur:

$$-(8e + 7f)\,49 + (13e + 2f)\,59 + (3f - 5e)\,75 = 0\,,$$

ubi pro e et f numeros quoscunque accipere licet.

5. Videamus igitur, quales numeros pro e et f accipi conveniat, ut haec aequatio fiat simplicissima. Sumatur primo $f = 1$ et $e = -1$, et relatio inventa erit

$$1 \cdot 49 - 11 \cdot 59 + 8 \cdot 75 = 0\,;$$

at si sumamus $e = 0$ et $f = -1$, relatio erit

$$7 \cdot 49 - 2 \cdot 59 - 3 \cdot 75 = 0\,,$$

quae sine dubio est simplicissima forma relationis. Atque ex hoc exemplo iam satis perspicuum est, quantumvis magnae fuerint quantitates A, B et C, quoniam continuo ad divisores minores devenimus, tandem omnes plane fractiones tolli ac pro numeris a, b, c semper numeros integros obtineri.

6. Cum igitur res sit manifesta, quando quantitates propositae A, B, C, D sunt rationales, sive commensurabiles inter se, etiam evidens est, si istae quantitates fuerint irrationales vel adeo transcendentes, tum operationes hic usitatas nunquam terminari, neque idcirco talem relationem exactam ullo modo exhiberi posse; veruntamen, quod his casibus imprimis est notandum, si memoratae operationes alicubi abrumpantur, tum eiusmodi relationes esse prodituras, quae quidem rem non exacte, attamen vero proxime exhibeant, id quod saepenumero usui esse poterit, quando inter huiusmodi quantitates relatio tantum proxime vera, et quidem in minimis desideratur. Quomodo autem huiusmodi casibus calculum tractare conveniat, nonnullis exemplis ostendemus.

7. Sint igitur ternae quantitates $A = 1$, $B = \sqrt{2}$ et $C = \sqrt{3}$, ac primo, ut operationes ante adhibitae locum invenire possint, has quantitates irrationales in fractiones decimales convertamus, quas quidem non ultra sextam notam continuemus. Est vero

$$\sqrt{2} = 1{,}414214 \text{ et } \sqrt{3} = 1{,}732051\,.$$

Iam per 1000000 multiplicando tota investigatio ad numeros integros revocetur, quandoquidem tota relatio in rationibus, quas hae quantitates inter

se tenent, subsistit, hocque modo aequatio principalis $a + b\sqrt{2} + c\sqrt{3} = 0$ transformabitur in hanc:

$$1000000\,a + 1414214\,b + 1732051\,c = 0\,,$$

quae divisa per 1000000 et ut supra in binas partes distributa dabit

$$a + b + c = +d \quad \text{et} \quad \frac{414214\,b + 732051\,c}{1000000} = -d\,;$$

postrema igitur ad integros reducta praebet

$$414214\,b + 732051\,c + 1000000\,d = 0\,,$$

haecque aequatio per 414214 divisa eodemque modo tractata deducit ad has aequationes:

$$b + c + 2d = +e \quad \text{et} \quad \frac{317837\,c + 171572\,d}{414214} = -e\,,$$

quarum postrema reducitur ad hanc:

$$317837\,c + 171572\,d + 414214\,e = 0^{1})\,.$$

Tractetur ista aequatio eodem modo, ut prodeant hae aequationes:

$$d + c + 2e = +f \quad \text{et} \quad \frac{146265\,c + 71070\,e}{171572} = -f\,,$$

quarum postrema ad integros reducta ita se habet:

$$146265\,c + 71070\,e + 171572\,f = 0\,,$$

quae per 71070 divisa praebet

$$e + 2c + 2f = +g \quad \text{et} \quad \frac{4125\,c + 29432\,f}{71070} = -g\,;$$

posterior reducta fit

1) Editio princeps: $\frac{317837\,c + 171572\,d}{171572} + 414214\,e = 0$. Correxit A. M.

$$4125c + 29432f + 71070g = 0,$$

unde per 4125 dividendo se produnt hae duae aequationes:

$$c + 7f + 17g = +h \quad \text{et} \quad \frac{575f + 945g}{4125} = -h^{1}),$$

at haec posterior ad integros reducta praebet istam:

$$575f + 945g + 4125h = 0.$$

Dividatur nunc per 575 prodibitque

$$f + g + 7h = +i \quad \text{et} \quad \frac{370g + 100h}{575} = -i$$

sive

$$\frac{74g + 20h}{115} = -i,$$

quae reducta fit

$$74g + 20h + 115i = 0,$$

unde per 20 dividendo hae oriuntur aequationes:

$$h + 3g + 5i = +k \quad \text{et} \quad \frac{14g + 15i}{20} = -k.$$

---

1) Ipsius $-h$ valor verus est $\frac{557f + 945g}{4125}$. Quamobrem ad finem § 8 omnes computationes vitiosae evadunt. Computatio vera ita se habet:

$$\begin{array}{rr} & 557f + 945g + 4125h = 0 \\ & f + g + 7h = i \\ \hline \text{sequitur} & 388g + 226h + 557i = 0 \\ & g + h + 2i = k \\ \hline \text{sequitur} & 162g + 105i + 226k = 0 \\ & g + i + 2k = l \\ \hline \text{sequitur} & 57g + 16k + 105l = 0 \\ & 3g + k + 6l = m \\ \hline \text{sequitur} & 9g + 9l + 16m = 0 \end{array}$$

hincque $g = 1$, $l = -1$, $m = 0$, quae est solutio simplicissima. Ex his paulatim obtinetur: $k = 3$, $i = -8$, $h = 18$, $f = -135$, $c = 946$, $e = -1621$, $d = 2161$, $b = -6889$, $a = 8104$.

Unde habebitur haec aequatio proxime vera

$$8104 - 6889\sqrt{2} + 946\sqrt{3} = 0,$$

quae cum valoribus radicum proxime sumtis maxime convenit. Correxit R. F.

8. Hoc modo has operationes continuari liceret, quousque libuerit; verum quia fractiones decimales non ultra sextam figuram sunt productae, per has operationes ultimae numerorum nostrorum figurae continuo magis fiunt incertae, unde in ultima aequatione binos numeros 14 et 15 tanquam aequales inter se spectare licebit, unde capi poterit $g = 1$ et $i = -1$, fietque $k = 0$, atque hinc regrediendo sequentes valores reperientur:

$$h = 2,\ f = -16,\ c = 97,\ e = -161,\ d = 209,\ b = -676,\ a = 788,$$

sicque relatio quaesita ita se habebit:

$$788 - 676\sqrt{2} + 97\sqrt{3} = 0$$

sive

$$676\sqrt{2} - 97\sqrt{3} = 788,$$

cuius error vix ultra sextam figuram decimalem exsurget.

9. Quantumvis autem haec relatio ad veritatem accedat, tamen inde neutiquam concludere licet eam penitus veritati esse consentaneam. Si enim, denotantibus a, b, c numeros rationales, esset exacte $a = b\sqrt{2} + c\sqrt{3}$, tum sumtis quadratis foret $aa = 2bb + 3cc + 2bc\sqrt{6}$, hincque $\sqrt{6} = \frac{aa - 2bb - 3cc}{2bc}$, ideoque $\sqrt{6}$ foret numerus rationalis, quod utique maxime esset absurdum; atque hoc idem etiam de omnibus aliis numeris radicalibus cuiuscunque ordinis est tenendum, ita ut quaelibet quantitas irrationalis natura sua tantopere discrepet ab omnibus aliis irrationalibus tam eiusdem quam diversorum graduum, ut nulla plane relatio rationalis inter plures huiusmodi quantitates surdas diversas locum habere possit.

10. Utrum autem quantitates transcendentes, veluti qui peripheriam circuli involvunt sive logarithmi, etiam cum nullis quantitatibus radicalibus comparari queant, adhuc maxime incertum videtur, siquidem a nemine adhuc talis impossibilitas est ostensa. Tantum quidem satis evictum videtur peripheriam π circuli, cuius diameter $= 1$, nullam comparationem cum formulis radicalibus quadraticis simplicibus admittere, quoniam aliter fractio continua ipsi π aequalis indices periodicos habere deberet, quod tamen neutiquam evenire videtur[1]). Num autem quantitas π cum talibus formulis compositis nullo prorsus modo comparari queat, in dubio relinquere cogimur;

1) Confer commentationem 71 (indicis Enestroemiani), *Leonhardi Euleri Opera omnia*, series I, vol. 14, p. 187, imprimis observationes p. 194. R. F.

quamobrem talem investigationem pro relatione quantitatum π, $\sqrt{2}$ et $\sqrt{3}$ methodo modo exposita suscipiamus.

11. Evolvamus igitur modo explicato hanc aequationem:

$$a\sqrt{2} + b\sqrt{3} + c\pi = 0\,,$$

quae in numeris integris proxime veris ita se habet:

$$1414214a + 1732051b + 3141593c = 0\,,$$

quae per minimum numerum divisa praebet has aequationes:

$$a + b + 2c = d \quad \text{et} \quad \frac{317837b + 313165c}{1414214} = -d\,.$$

Postrema aequatio ergo in integris fit

$$317837b + 313165c + 1414214d = 0\,,$$

quae iterum per minimum numerum dividatur, quo facto produnt hae duae aequationes:

$$c + b + 4d = e \quad \text{et} \quad \frac{4672b + 161554d}{313165} = -e\,,$$

quae posterior reducta fit

$$4672b + 161554d + 313165e = 0\,.$$

Dividendo per 4672 hae colliguntur aequationes:

$$b + 34d + 67e = f \quad \text{et} \quad \frac{2706d + 141e}{4672} = -f\,.$$

12. Operationes has ulterius non prosequor, quoniam, si exacta daretur relatio, ea sine dubio non adeo complicata esset futura. Prope veras autem tales relationes exhibuisse parum iuvaret. Unde sententia satis certa videtur, quod peripheria circuli tam peculiare genus quantitatum transcendentium constituat, ut cum nullis aliis quantitatibus, sive surdis, sive alius generis transcendentibus, nullo modo se comparari patiatur.

13. Infinita autem alia dantur transcendentium genera, quae neque ad circulum neque ad logarithmos reduci possunt, etiamsi quampiam affinitatem cum his quantitatibus tenere videantur; ac si forte tales quantitates cum hactenus cognitis exactam quandum relationem tenerent, quam directe ex principiis analyticis definire non licet, haec methodus unicam viam suppeditare videtur, cuius beneficio huiusmodi relationes quasi divinando explorare licebit.

14. Huiusmodi igitur casum singularem, qui talem relationem non respuere videtur, hic accuratius evolvam, scilicet summam seriei reciprocae cuborum

$$1 + \frac{1}{2^3} + \frac{1}{3^3} + \frac{1}{4^3} + \frac{1}{5^3} + \frac{1}{6^3} + \text{ etc.},$$

quam nullo adhuc modo sive ad circulum sive ad logarithmos reducere potui, cum tamen summae potestatum parium omnes per potestates pares ipsius π exhiberi queant, summa autem primarum potestatum

$$1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \frac{1}{5} - \text{ etc.}$$

logarithmum binarii exprimat.

15. Cum igitur haec series reciproca cuborum

$$1 - \frac{1}{2^3} + \frac{1}{3^3} - \frac{1}{4^3} + \frac{1}{5^3} - \frac{1}{6^3} + \text{ etc.}$$

cubum huius seriei

$$1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \frac{1}{5} - \frac{1}{6} + \text{ etc.}$$

in se complectatur, probabile videtur, in eius summa $(\log. 2)^3$ occurrere debere, neque tamen cuipiam multiplo huius quantitatis aequari certum est. Deinde vero, cum eadem series in se complectatur productum ex binis praecedentibus, scilicet:

$$1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \frac{1}{5} - \text{etc.} = l2 \quad \text{et} \quad 1 + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \frac{1}{5^2} + \text{etc.} = \frac{\pi\pi}{6},$$

suspicari licet, ibidem quoque productum $\frac{\pi\pi}{6}l2$ occurrere; quamobrem operae pretium erit inquirere, num forte summa seriei reciprocae cuborum tali formulae compositae:

$$\alpha(l2)^3 + \beta\frac{\pi\pi}{6}\cdot l2$$

aequetur, ita ut α et β sint numeri rationales.

16. Per approximationes autem olim summam seriei reciprocae cuborum ita assignavi[1]):

$$1 + \frac{1}{2^3} + \frac{1}{3^3} + \frac{1}{4^3} + \text{etc.} = 1{,}202056903\,,$$

unde si eius pars quarta subtrahatur, prodit summa huius seriei:

$$1 - \frac{1}{2^3} + \frac{1}{3^3} - \frac{1}{4^3} + \frac{1}{5^3} - \text{etc.} = 0{,}901542677\,,$$

quam brevitatis gratia ponamus $= A$, et quaeramus numeros a, b, c, ut fiat

$$aA + b(l2)^3 + cl2\cdot\frac{\pi\pi}{6} = 0\,,$$

ubi cum sit

$$\frac{\pi\pi}{6} = 1{,}644934066 \quad \text{et} \quad l2 = 0{,}693147180\,,$$

colligimus fore proxime

$$(l2)^3 = 0{,}333025 \quad \text{et} \quad l2\cdot\frac{\pi\pi}{6} = 1{,}140182\,,$$

unde relatio evolvenda erit

$$901543a + 333025b + 1140182c = 0\,.$$

17. Pro hac igitur aequatione operationes instituantur ut supra, eritque dividendo per 333025

1) Vide opus 212 (indicis Enestroemiani): *Institutiones calculi differentialis cum eius usu in analysi finitorum, ac doctrina serierum*, Petrop. 1755, p. 456. *Leonhardi Euleri Opera omnia*, series I, vol. 10, p. 349. R. F.

$$b + 2a + 3c = d \quad \text{et} \quad \frac{235493a + 141107c}{333025} = -d;$$

at posterior ad integros reducta praebet

$$235493a + 141107c + 333025d = 0,$$

unde dividendo per 141107 deducimus has aequationes:

$$a + c + 2d = e \quad \text{et} \quad \frac{94386a + 50811d}{141107} = -e$$

sive

$$94386a + 50811d + 141107e = 0,$$

qua aequatione divisa per 50811 colligitur

$$a + d + 2e = f \quad \text{et} \quad \frac{43575a + 39485e}{50811} = -f;$$

at haec posterior reducta ad integros fit

$$43575a + 39485e + 50811f = 0,$$

unde porro dividendo per minimum numerum oriuntur hae aequationes:

$$a + e + f = +g \quad \text{et} \quad \frac{4090a + 11326f}{39485} = -g$$

sive

$$4090a + 11326f + 39485g = 0,$$

unde formentur hae aequationes:

$$a + 2f + 9g = +h \quad \text{et} \quad \frac{3146f + 2675g}{4090} = -h$$

etc.

18. Superfluum foret has operationes ulterius continuare, quoniam hinc iam satis intelligere licet nullam dari relationem tam concinnam inter ternas quantitates assumtas, ut veritati consentanea censeri posset. Cum igitur investigationem huius summae reciprocae cuborum tot variis modis frustra explorare tentassem atque haec methodus etiam inutiliter sit in usum vocata, merito de tali inventione desperandum videtur.

DE SUMMA SERIEI EX NUMERIS PRIMIS FORMATAE $\frac{1}{3}-\frac{1}{5}+\frac{1}{7}+\frac{1}{11}-\frac{1}{13}-\frac{1}{17}+\frac{1}{19}+\frac{1}{23}-\frac{1}{29}+\frac{1}{31}-$ etc. UBI NUMERI PRIMI FORMAE $4n-1$ HABENT SIGNUM POSITIVUM FORMAE AUTEM $4n+1$ SIGNUM NEGATIVUM

Commentatio 596 indicis Enestroemiani
Opuscula analytica 2, 1785, p. 240—256
[Conventui exhibita die 2. octobris 1775]

1. Cum iam Euclides demonstrasset multitudinem numerorum primorum revera esse infinitam, ego iam pridem ostendi etiam summam seriei reciprocae numerorum primorum, scilicet

$$\frac{1}{2}+\frac{1}{3}+\frac{1}{5}+\frac{1}{7}+\frac{1}{11}+\frac{1}{13}+\frac{1}{17}+\frac{1}{19}+\text{ etc.},$$

esse infinite magnam, atque adeo referre logarithmum summae seriei harmonicae

$$1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\frac{1}{5}+\text{ etc.},$$

id quod non parum mirum videbatur, cum vulgo summa seriei harmonicae ad genus quasi infimum infinitorum referri soleat. Cum autem non solum logarithmus numeri infiniti sit etiam infinitus, sed etiam logarithmi horum ipsorum logarithmorum etiamnunc sint infiniti, manifestum est dari insuper

infinitos gradus inferiores infinitorum. Ita si A denotet summam seriei reciprocae numerorum primorum, etiam lA adhuc erit infinite magnus, sed ad ordinem infinitorum infinities inferiorem pertinere censendus est; tum vero etiamnunc hae formulae: llA, $lllA$, $llllA$ etc. erunt infinitae, quanquam quaelibet earum infinities sit minor quam praecedens.

2. Quoniam porro numeri primi praeter binarium quasi a natura in duas classes distinguuntur, prouti fuerint vel formae $4n + 1$ vel formae $4n - 1$, dum priores omnes sunt summae duorum quadratorum, posteriores vero ab hac proprietate penitus excluduntur; series reciprocae ex utraque classe formatae, scilicet:

$$\frac{1}{5} + \frac{1}{13} + \frac{1}{17} + \frac{1}{29} + \text{ etc. et } \frac{1}{3} + \frac{1}{7} + \frac{1}{11} + \frac{1}{19} + \frac{1}{23} + \text{ etc.},$$

ambae erunt pariter infinitae, id quod etiam de omnibus speciebus numerorum primorum est tenendum. Ita si ex numeris primis ii tantum excerpantur, qui sunt formae $100n + 1$, cuiusmodi sunt 101, 401, 601, 701 etc., non solum multitudo eorum est infinita, sed etiam summa huius seriei ex illis formatae, scilicet:

$$\frac{1}{101} + \frac{1}{401} + \frac{1}{601} + \frac{1}{701} + \frac{1}{1201} + \frac{1}{1301} + \frac{1}{1601} + \frac{1}{1801} + \frac{1}{1901} + \text{ etc.},$$

etiam est infinita.

3. Consideremus hic autem imprimis discrimen inter numeros primos formae $4n + 1$ et $4n - 1$, et quia ambae series ex utroque ordine formatae sunt infinitae et quasi eiusdem ordinis, nullum est dubium, quin earum differentia habeat valorem determinatum. Hanc ob rem terminis ex forma $4n - 1$ formatis tribuamus signum $+$, reliquis vero signum $-$, ut orietur ista series:

$$\frac{1}{3} - \frac{1}{5} + \frac{1}{7} + \frac{1}{11} - \frac{1}{13} - \frac{1}{17} + \frac{1}{19} + \frac{1}{23} - \frac{1}{29} + \frac{1}{31} - \text{ etc.},$$

in qua nullus plane ordo in signis cernitur. Hoc tamen non obstante videamus, quomodo eius summa vero saltem proxime assignari queat. Non

parum enim probabile videtur istam summam, si non fuerit rationalis vel irrationalis, saltem ad quodpiam genus notabile quantitatum transcendentium pertinere debere. Interim tamen, quoniam non solum non in signis, verum etiam multo minus in ipsis fractionibus nullus plane ordo perspicitur, primo intuitu nulla patere videtur via, qua ad eius summam pervenire liceat.

4. Quando autem contemplamur seriem notissimam LEIBNITZIANAM pro quadratura circuli datam[1])

$$\frac{\pi}{4} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \frac{1}{11} + \text{ etc.},$$

videmus in ea omnes numeros impares formae $4n+1$ habere signum $+$, reliquos vero formae $4n-1$ signum $-$, unde mutatis signis omnes termini nostrae seriei cum suis signis in hac serie LEIBNITZIANA occurrunt. Quod si ergo ex hac serie omnes numeros compositos expungamus, tandem praeter unitatem ipsa nostra series proposita, contrariis signis, remanebit. Quamobrem summam nostrae seriei obtinebimus, si ex serie LEIBNITZIANA successive omnes numeros compositos excludamus, quandoquidem omnium terminorum, qui per quamvis operationem excluduntur, summa facile assignare licebit.

5. Incipiamus igitur ab ipsa serie LEIBNITZIANA, statuendo

$$A = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \frac{1}{11} + \frac{1}{13} - \frac{1}{15} + \frac{1}{17} - \frac{1}{19} + \text{ etc.},$$

ita ut sit $A = \frac{\pi}{4}$, ex eaque primo omnes numeros compositos per 3 divisibiles excludamus. Quem in finem hinc formemus istam seriem:

$$(A-1)\frac{1}{3} = -\frac{1}{9} + \frac{1}{15} - \frac{1}{21} + \frac{1}{27} - \frac{1}{33} + \frac{1}{39} - \text{ etc.},$$

quae utique continet omnes numeros compositos per 3 divisibiles, unde si haec series ad illam addatur, omnes isti numeri compositi excludentur fietque

1) Editio princeps: $\frac{\pi}{2}$. Correxit R. F.

$$\frac{4}{3}A-\frac{1}{3}=1-\frac{1}{3}+\frac{1}{5}-\frac{1}{7}-\frac{1}{11}+\frac{1}{13}+\frac{1}{17}-\frac{1}{19}-\frac{1}{23}+\frac{1}{25}+\text{etc.}=B,$$

ita ut sit $B=\frac{4}{3}A-\frac{1}{3}$. In hac igitur serie, cuius summam novimus, nulli amplius numeri compositi per 3 divisibiles occurrunt, sed primus terminus compositus hic occurrens est $+\frac{1}{25}$.

6. Nunc igitur ex postrema hac serie omnes terminos per 5 divisibiles excludamus, quem in finem hinc formemus istam seriem:

$$\left(B-1+\frac{1}{3}\right)\frac{1}{5}=\frac{1}{25}-\frac{1}{35}-\frac{1}{55}+\frac{1}{65}+\frac{1}{85}-\frac{1}{95}-\text{ etc.},$$

quae omnes complectitur terminos per quinque divisibiles, qui adhuc in seriem B ingrediebantur, et quidem iisdem signis affectos, quare hac serie ab illa ablata remanebit haec:

$$\frac{4}{5}B+\frac{1}{5}\left(1-\frac{1}{3}\right)=1-\frac{1}{3}+\frac{1}{5}-\frac{1}{7}-\frac{1}{11}+\frac{1}{13}+\frac{1}{17}-\frac{1}{19}-\frac{1}{23}+\text{ etc.},$$

ubi iam ab initio omnes termini sunt numeri primi, et non primus, qui hic occurret, erit $\frac{1}{49}$, sequentes vero $\frac{1}{77}$, $-\frac{1}{91}$. Ponamus autem summam huius seriei $=C$, ut sit

$$C=\frac{4}{5}B+\frac{1}{5}\left(1-\frac{1}{3}\right).$$

7. Nunc igitur hinc excludamus omnes terminos, qui adhuc per septem sunt divisibiles, quos complectetur sequens forma:

$$\left(C-1+\frac{1}{3}-\frac{1}{5}\right)\frac{1}{7}=-\frac{1}{49}-\frac{1}{77}+\frac{1}{91}+\text{ etc.},$$

quorum terminorum signa sunt contraria, quare haec series ad seriem C addita dabit

$$\frac{8}{7}C-\frac{1}{7}\left(1-\frac{1}{3}+\frac{1}{5}\right)=1-\frac{1}{3}+\frac{1}{5}-\frac{1}{7}-\frac{1}{11}+\frac{1}{13}+\frac{1}{17}-\text{ etc.},$$

in qua primus terminus compositus erit $+\frac{1}{121}$, sequentes vero $-\frac{1}{11\cdot 13}$, $-\frac{1}{11\cdot 17}$ etc. Hanc autem seriem vocemus D, ut sit

$$D=\frac{8}{7}C-\frac{1}{7}\left(1-\frac{1}{3}+\frac{1}{5}\right).$$

8. Iam ex serie modo inventa D expungamus terminos, qui adhuc sunt per 11 divisibiles, quos complectetur ista forma:

$$\left(D-\left(1-\frac{1}{3}+\frac{1}{5}-\frac{1}{7}\right)\right)\frac{1}{11}^{1)}=-\frac{1}{121}+\frac{1}{143}+\frac{1}{187}-\text{ etc.},$$

qui termini in serie D contraria habent signa; quamobrem si haec series ad illam addatur, isti termini excludentur prodibitque

$$\frac{12}{11}D-\frac{1}{11}\left(1-\frac{1}{3}+\frac{1}{5}-\frac{1}{7}\right)=1-\frac{1}{3}+\frac{1}{5}-\frac{1}{7}-\frac{1}{11}+\text{ etc.},$$

in qua primus terminus non primus est $\frac{1}{169}$; istam autem seriem designemus littera E, ita ut sit

$$E=\frac{12}{11}D-\frac{1}{11}\left(1-\frac{1}{3}+\frac{1}{5}-\frac{1}{7}\right).$$

9. Ex hac igitur serie excludamus omnes terminos, qui adhuc insunt per 13 divisibiles, quos ergo complectetur haec forma:

$$\left(E-1+\frac{1}{3}-\frac{1}{5}+\frac{1}{7}+\frac{1}{11}\right)\frac{1}{13}=\frac{1}{169}+\frac{1}{221}-\text{ etc.},$$

hique termini eadem habent signa ac in ipsa serie E. Haec igitur series ab illa debet subtrahi, unde prodit

$$\frac{12}{13}E+\frac{1}{13}\left(1-\frac{1}{3}+\frac{1}{5}-\frac{1}{7}-\frac{1}{11}\right)=1-\frac{1}{3}+\frac{1}{5}-\frac{1}{7}-\frac{1}{11}+\text{ etc.},$$

1) Editio princeps: $D-\left(1+\frac{1}{3}-\frac{1}{5}+\frac{1}{7}\right)\frac{1}{11}$. Correxit R. F.

ubi primus terminus non primus est $\frac{1}{289}$. Totam autem hanc seriem designemus littera F, ut sit

$$F = \frac{12}{13}E + \frac{1}{13}\left(1-\frac{1}{3}+\frac{1}{5}-\frac{1}{7}-\frac{1}{11}\right).$$

10. Quod si nunc istas operationes ulterius continuemus, dum successive hinc excludimus terminos adhuc per 17 divisibiles, tum vero per 19, per 23 etc., tandem relinquetur tantum series numerorum primorum post unitatem sequentium, quae si designetur littera Z, quam ut infinitesimam spectari oportet, erit utique

$$Z = 1-\frac{1}{3}+\frac{1}{5}-\frac{1}{7}-\frac{1}{11}+\frac{1}{13}+\frac{1}{17}-\frac{1}{19}-\text{ etc.},$$

consequenter seriei in titulo propositae summa erit $1-Z$. Ac manifestum est ad hunc valorem continuo propius accedere istas formulas:

$$1-A,\ 1-B,\ 1-C,\ 1-D,\ 1-E,\ 1-F \text{ etc.}$$

11. Quemadmodum autem valores omnium harum litterarum successive ex antecedentibus colligi debeant, ex sequentibus formulis fiet manifestum:

$$B = \frac{4}{3}A - \frac{1}{3}\cdot 1$$
$$C = \frac{4}{5}B + \frac{1}{5}\left(1-\frac{1}{3}\right)$$
$$D = \frac{8}{7}C - \frac{1}{7}\left(1-\frac{1}{3}+\frac{1}{5}\right)$$
$$E = \frac{12}{11}D - \frac{1}{11}\left(1-\frac{1}{3}+\frac{1}{5}-\frac{1}{7}\right)$$
$$F = \frac{12}{13}E + \frac{1}{13}\left(1-\frac{1}{3}+\frac{1}{5}-\frac{1}{7}-\frac{1}{11}\right)$$
$$G = \frac{16}{17}F + \frac{1}{17}\left(1-\frac{1}{3}+\frac{1}{5}-\frac{1}{7}-\frac{1}{11}+\frac{1}{13}\right)$$
$$H = \frac{20}{19}G - \frac{1}{19}\left(1-\frac{1}{3}+\frac{1}{5}-\frac{1}{7}-\frac{1}{11}+\frac{1}{13}+\frac{1}{17}\right)$$
$$I = \frac{24}{23}H - \frac{1}{23}\left(1-\frac{1}{3}+\frac{1}{5}-\frac{1}{7}-\frac{1}{11}+\frac{1}{13}+\frac{1}{17}-\frac{1}{19}\right)$$
etc.

Ubi notandum, si denominator primus fuerit formae $4n+1$, tum numeratorem primae partis fore unitate minorem, sive $4n$, alteram vero partem addi debere. Sin autem denominator primus fuerit $4n-1$, tum numeratorem primae partis fore unitate maiorem, sive $4n$, alteram partem vero hoc casu subtrahi debere.

12. Quo nunc omnes hos valores in numeris per fractiones decimales exprimamus, ante omnia notetur esse

$$A = \frac{\pi}{4} = 0{,}7853981634\,.$$

Pro reliquis autem litteris computentur sequentes valores:

$$\begin{aligned}
1-\tfrac{1}{3} &= b = 0{,}6666666666\\
1-\tfrac{1}{3}+\tfrac{1}{5} &= c = 0{,}8666666666\\
1-\tfrac{1}{3}+\tfrac{1}{5}-\tfrac{1}{7} &= d = 0{,}7238095238\\
1-\tfrac{1}{3}+\tfrac{1}{5}-\tfrac{1}{7}-\tfrac{1}{11} &= e = 0{,}6329004329\\
1-\tfrac{1}{3}+\tfrac{1}{5}-\tfrac{1}{7}-\tfrac{1}{11}+\tfrac{1}{13} &= f = 0{,}7098235098\\
1-\tfrac{1}{3}+\tfrac{1}{5}-\tfrac{1}{7}-\tfrac{1}{11}+\tfrac{1}{13}+\tfrac{1}{17} &= g = 0{,}7686470392\\
1-\tfrac{1}{3}+\tfrac{1}{5}-\tfrac{1}{7}-\tfrac{1}{11}+\tfrac{1}{13}+\tfrac{1}{17}-\tfrac{1}{19} &= h = 0{,}7160154603\\
1-\tfrac{1}{3}+\tfrac{1}{5}-\tfrac{1}{7}-\tfrac{1}{11}+\tfrac{1}{13}+\tfrac{1}{17}-\tfrac{1}{19}-\tfrac{1}{23} &= i = 0{,}6725371994\,,
\end{aligned}$$

in quo ordine primus terminus a unitate aequatur.

13. Pro computo autem ipsarum litterarum A, B, C, D, E etc. praestabit sequentibus uti formulis, quibus simul valores numericos harum litterarum adscribamus

$$B = A + \frac{1}{3}(A - a) = 0{,}713864$$
$$C = B - \frac{1}{5}(B - b) = 0{,}704424$$
$$D = C + \frac{1}{7}(C - c) = 0{,}681247$$
$$E = D + \frac{1}{11}(D - d) = 0{,}677377$$
$$F = E - \frac{1}{13}(E - e) = 0{,}673956$$
$$G = F - \frac{1}{17}(F - f) = 0{,}676066$$
$$H = G + \frac{1}{19}(G - g) = 0{,}671193$$
$$I = H + \frac{1}{23}(H - h) = 0{,}669245$$
$$K = I - \frac{1}{29}(I - i) = 0{,}669358\,.$$

14. Quanquam autem calculum huc usque produximus, tamen ultra tertiam figuram decimalem de summa nostrae seriei certi esse non possumus, atque adeo in dubio relinquere cogimur, utrum ista summa aliquanto maior vel minor sit quam 0,669. Sin autem hunc valorem pro vero assumamus, ipsa series proposita

$$\frac{1}{3}-\frac{1}{5}+\frac{1}{7}+\frac{1}{11}-\frac{1}{13}-\frac{1}{17}+\frac{1}{19}+ \text{ etc.}$$

summam habebit 0,331, ideoque hic valor tantillo foret minor quam $\frac{1}{3}$. Quoniam vero ablato $\frac{1}{5}$, iterum addi debeat $\frac{1}{7}+\frac{1}{11}$, quarum fractionum summa maior est quam $\frac{1}{5}$, utique fieri posset, ut verus valor superaret $\frac{1}{3}$, id quod hoc loco in dubio est relinquendum. Datur vero alia methodus multo accuratius in summam huius seriei inquirendi, quam hic evolvemus, quandoquidem operae pretium videtur veram huius seriei summam propius cognovisse.

15. Eadem methodo, qua hic ex prima serie LEIBNITZIANA successive terminos compositos expulimus, si omnes plane terminos praeter unitatem removeamus, reperiemus

$$\frac{\pi}{4} = \frac{3}{4} \cdot \frac{5}{4} \cdot \frac{7}{8} \cdot \frac{11}{12} \cdot \frac{13}{12} \cdot \frac{17}{16} \cdot \frac{19}{20} \cdot \text{ etc.},$$

ubi in numeratoribus omnes numeri primi occurrunt praeter 2, denominatores vero sunt numeri pariter pares unitate vel maiores vel minores. Deinde vero si ista series reciproca quadratorum imparium:

$$1 + \frac{1}{3^2} + \frac{1}{5^2} + \frac{1}{7^2} + \frac{1}{9^2} + \frac{1}{11^2} + \frac{1}{13^2} + \text{ etc.},$$

cuius summam ostendi esse $= \frac{\pi\pi}{8}$, simili modo tractetur, reperietur

$$\frac{\pi\pi}{8} = \frac{3 \cdot 3}{2 \cdot 4} \cdot \frac{5 \cdot 5}{4 \cdot 6} \cdot \frac{7 \cdot 7}{6 \cdot 8} \cdot \frac{11 \cdot 11}{10 \cdot 12} \cdot \frac{13 \cdot 13}{12 \cdot 14} \cdot \text{ etc.},$$

ubi iterum in numeratoribus omnes numeri primi bis occurrunt, in denominatoribus vero iidem tam unitate aucti quam minuti. Quare si hanc expressionem per quadratum illius, quod est

$$\frac{\pi\pi}{16} = \frac{3 \cdot 3}{4 \cdot 4} \cdot \frac{5 \cdot 5}{4 \cdot 4} \cdot \frac{7 \cdot 7}{8 \cdot 8} \cdot \frac{11 \cdot 11}{12 \cdot 12} \cdot \frac{13 \cdot 13}{12 \cdot 12} \cdot \text{ etc.},$$

dividamus, quotus erit

$$2 = \frac{4}{2} \cdot \frac{4}{6} \cdot \frac{8}{6} \cdot \frac{12}{10} \cdot \frac{12}{14} \cdot \text{ etc.},$$

ubi omnes numeri primi tam unitate aucti quam minuti occurrunt, et numeri pariter pares in numeratore, impariter pares vero in denominatore constituuntur.

16. Postrema haec expressio igitur hoc modo exhiberi poterit:

$$2 = \frac{3+1}{3-1} \cdot \frac{5-1}{5+1} \cdot \frac{7+1}{7-1} \cdot \frac{11+1}{11-1} \cdot \frac{13-1}{13+1} \cdot \text{ etc.};$$

hinc ergo logarithmis hyperbolicis sumendis habebimus:

$$l2 = l\frac{3+1}{3-1} + l\frac{5-1}{5+1} + l\frac{7+1}{7-1} + l\frac{11+1}{11-1} + l\frac{13-1}{13+1} + \text{ etc.}$$

Constat autem per series infinitas esse in genere

$$\frac{1}{2}l\frac{a+1}{a-1} = \frac{1}{a} + \frac{1}{3a^3} + \frac{1}{5a^5} + \frac{1}{7a^7} + \frac{1}{9a^9} + \text{ etc.},$$

hincque:

$$\frac{1}{2}l\frac{a-1}{a+1} = -\frac{1}{a} - \frac{1}{3a^3} - \frac{1}{5a^5} - \frac{1}{7a^7} - \frac{1}{9a^9} - \text{ etc.}$$

Quodsi igitur harum formularum ope omnes illos logarithmos in series infinitas convertamus, nanciscemur quidem innumeras series infinitas, quas autem ad series facilius tractabiles reducere licebit.

17. Primo igitur omnium illorum logarithmorum semisses accipi oportet, et quia hic de logarithmis hyperbolicis agitur, ob

$$l\,2 = 0{,}6931471805$$

erit

$$\frac{1}{2}l\,2 = 0{,}3465735902,$$

ex altera autem parte logarithmi ita ordinentur:

$$\begin{aligned}
\frac{1}{2}l\,\frac{3+1}{3-1} &= \frac{1}{3} + \frac{1}{3\cdot 3^3} + \frac{1}{5\cdot 3^5} + \frac{1}{7\cdot 3^7} + \frac{1}{9\cdot 3^9} + \text{ etc.}\\
\frac{1}{2}l\,\frac{5-1}{5+1} &= -\frac{1}{5} - \frac{1}{3\cdot 5^3} - \frac{1}{5\cdot 5^5} - \frac{1}{7\cdot 5^7} - \frac{1}{9\cdot 5^9} - \text{ etc.}\\
\frac{1}{2}l\,\frac{7+1}{7-1} &= \frac{1}{7} + \frac{1}{3\cdot 7^3} + \frac{1}{5\cdot 7^5} + \frac{1}{7\cdot 7^7} + \frac{1}{9\cdot 7^9} + \text{ etc.}\\
\frac{1}{2}l\,\frac{11+1}{11-1} &= \frac{1}{11} + \frac{1}{3\cdot 11^3} + \frac{1}{5\cdot 11^5} + \frac{1}{7\cdot 11^7} + \frac{1}{9\cdot 11^9} + \text{ etc.}\\
\frac{1}{2}l\,\frac{13-1}{13+1} &= -\frac{1}{13} - \frac{1}{3\cdot 13^3} - \frac{1}{5\cdot 13^5} - \frac{1}{7\cdot 13^7} - \frac{1}{9\cdot 13^9} - \text{ etc.}
\end{aligned}$$

etc.

18. Hinc iam verticaliter descendendo consideremus sequentes series pariter infinitas:

$$O = \frac{1}{3} - \frac{1}{5} + \frac{1}{7} + \frac{1}{11} - \frac{1}{13} - \frac{1}{17} + \frac{1}{19} + \text{ etc.}$$
$$P = \frac{1}{3^3} - \frac{1}{5^3} + \frac{1}{7^3} + \frac{1}{11^3} - \frac{1}{13^3} - \frac{1}{17^3} + \frac{1}{19^3} + \text{ etc.}$$
$$Q = \frac{1}{3^5} - \frac{1}{5^5} + \frac{1}{7^5} + \frac{1}{11^5} - \frac{1}{13^5} - \frac{1}{17^5} + \frac{1}{19^5} + \text{ etc.}$$
$$R = \frac{1}{3^7} - \frac{1}{5^7} + \frac{1}{7^7} + \frac{1}{11^7} - \frac{1}{13^7} - \frac{1}{17^7} + \frac{1}{19^7} + \text{ etc.}$$
$$S = \frac{1}{3^9} - \frac{1}{5^9} + \frac{1}{7^9} + \frac{1}{11^9} - \frac{1}{13^9} - \frac{1}{17^9} + \frac{1}{19^9} + \text{ etc.}$$
$$\text{etc.}$$

Quarum serierum prima O est ea ipsa, cuius summam hic investigare nobis est propositum.

19. His igitur seriebus ita per litteras maiusculas designatis habebimus istam aequationem:

$$\frac{1}{2}l2 = O + \frac{1}{3}P + \frac{1}{5}Q + \frac{1}{7}R + \frac{1}{9}S + \frac{1}{11}T + \text{ etc.},$$

unde si summae serierum P, Q, R, S etc. essent cognitae, inde impetraremus facile summam seriei O quaesitam; foret enim

$$O = \frac{1}{2}l2 - \frac{1}{3}P - \frac{1}{5}Q - \frac{1}{7}R - \frac{1}{9}S - \text{ etc.}$$

20. At vero summas serierum P, Q, R etc. ex seriebus ordinis, ubi omnes numeri impares occurrunt, concludere poterimus eodem modo, quo supra seriem ipsam O ex serie LEIBNITZIANA

$$1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \frac{1}{11} + \text{ etc.}$$

elicuimus. Hunc in finem evolvi hac methodo oportebit sequentes series ordinatas:

$$\mathfrak{P} = 1 - \frac{1}{3^3} + \frac{1}{5^3} - \frac{1}{7^3} + \frac{1}{9^3} - \frac{1}{11^3} + \frac{1}{13^3} - \frac{1}{15^3} + \text{ etc.}$$
$$\mathfrak{Q} = 1 - \frac{1}{3^5} + \frac{1}{5^5} - \frac{1}{7^5} + \frac{1}{9^5} - \frac{1}{11^5} + \frac{1}{13^5} - \frac{1}{15^5} + \text{ etc.}$$
$$\mathfrak{R} = 1 - \frac{1}{3^7} + \frac{1}{5^7} - \frac{1}{7^7} + \frac{1}{9^7} - \frac{1}{11^7} + \frac{1}{13^7} - \frac{1}{15^7} + \text{ etc.}$$
$$\mathfrak{S} = 1 - \frac{1}{3^9} + \frac{1}{5^9} - \frac{1}{7^9} + \frac{1}{9^9} - \frac{1}{11^9} + \frac{1}{13^9} - \frac{1}{15^9} + \text{ etc.}$$
$$\mathfrak{T} = 1 - \frac{1}{3^{11}} + \frac{1}{5^{11}} - \frac{1}{7^{11}} + \frac{1}{9^{11}} - \frac{1}{11^{11}} + \frac{1}{13^{11}} - \frac{1}{15^{11}} + \text{ etc.}$$
etc.

Harum autem omnium serierum summas iam pridem per quadraturam circuli, scilicet per similes potestates ipsius π expressas dedi, sequenti modo[1]):

$$\mathfrak{P} = \frac{1}{1\cdot 2}\cdot\frac{\pi^3}{2^4} \qquad \mathfrak{T} = \frac{50521}{1.....10}\cdot\frac{\pi^{11}}{2^{12}}$$
$$\mathfrak{Q} = \frac{5}{1\cdot 2\cdot 3\cdot 4}\cdot\frac{\pi^5}{2^6} \qquad \mathfrak{U} = \frac{2702765}{1.....12}\cdot\frac{\pi^{13}}{2^{14}}$$
$$\mathfrak{R} = \frac{61}{1.....6}\cdot\frac{\pi^7}{2^8} \qquad \mathfrak{V} = \frac{199360981}{1.....14}\cdot\frac{\pi^{15}}{2^{16}}$$
$$\mathfrak{S} = \frac{1385}{1.....8}\cdot\frac{\pi^9}{2^{10}} \qquad \mathfrak{W} = \frac{19391512145}{1.....16}\cdot\frac{\pi^{17}}{2^{18}}$$
etc.

21. Hos igitur valores in fractionibus decimalibus usque ad sextam figuram evolvamus, eritque

	Differentiae
$\mathfrak{P} = 0{,}9689462$	0,0272116
$\mathfrak{Q} = 0{,}9961578$[2])	0,0033969
$\mathfrak{R} = 0{,}9995547$	0,0003952
$\mathfrak{S} = 0{,}9999499$	0,0000448
$\mathfrak{T} = 0{,}9999947$	0,0000050
$\mathfrak{U} = 0{,}9999997$	0,0000005
etc.	etc.

1) Confer opus 212 (indicis Enestroemiani): *Institutiones calculi differentialis etc.* Petropoli 1755, p. 542. *Leonhardi Euleri Opera omnia* series I, vol. 10, p. 418. R. F.

2) Editio princeps: 0,9961557. Correxit A. M.

22. Ut nunc hinc valores litterarum P, Q, R etc. eruamus, eadem methodo utamur, qua supra ex serie

$$1-\frac{1}{3}+\frac{1}{5}-\frac{1}{7}+\frac{1}{9}-\frac{1}{11}+\text{ etc.}$$

omnes terminos compositos exterminavimus, quandoquidem loco horum numerorum simplicium eorum potestates scribi convenit. Hanc igitur operationem in genere pro his litteris doceamus. Consideremus igitur hanc seriem:

$$\mathfrak{Z}=1-\frac{1}{3^n}+\frac{1}{5^n}-\frac{1}{7^n}+\frac{1}{9^n}-\frac{1}{11^n}+\text{ etc.},$$

cuius summam, ut supra factum est, littera A designemus, ut sit $A=\mathfrak{Z}$, hincque sequentes litteras B, C, D etc. eliciamus per sequentes formulas:

$$\begin{aligned}
&B=A+\frac{1}{3^n}(A-a) && \text{existente } a=1\\
&C=B-\frac{1}{5^n}(B-b) && b=1-\frac{1}{3^n}\\
&D=C+\frac{1}{7^n}(C-c) && c=1-\frac{1}{3^n}+\frac{1}{5^n}\\
&E=D+\frac{1}{11^n}(D-d) && d=1-\frac{1}{3^n}+\frac{1}{5^n}-\frac{1}{7^n}\\
&F=E-\frac{1}{13^n}(E-e) && e=1-\frac{1}{3^n}+\frac{1}{5^n}-\frac{1}{7^n}-\frac{1}{11^n}\\
&\text{etc.} && \text{etc.}
\end{aligned}$$

Quibus valoribus inventis eorum complementa ad unitatem, scilicet $1-A$, $1-B$, $1-C$, $1-D$ etc., promptissime ad valorem quaesitum

$$Z=\frac{1}{3^n}-\frac{1}{5^n}+\frac{1}{7^n}+\frac{1}{11^n}-\frac{1}{13^n}-\text{ etc.}$$

appropinquabunt.

23. Haec igitur praecepta generalia applicemus primo ad valorem litterae P, unde incipiendum erit a valore

$$\mathfrak{P}=0{,}9689462=A\,,$$

et quia hic est $n=3$, habebimus

$$a = 1, \quad b = 0{,}9629630, \quad c = 0{,}9709630, \quad d = 0{,}9680476;$$

pluribus valoribus non erit opus. Hinc igitur colligemus sequentes valores:

$$B = A - \frac{1}{3^3} \cdot 0{,}0310538 = 0{,}9677961$$
$$C = B - \frac{1}{5^3} \cdot 0{,}0048331 = 0{,}9677574$$
$$D = C - \frac{1}{7^3} \cdot 0{,}0032056 = 0{,}9677481$$
$$E = D - \frac{1}{11^3} \cdot 0{,}0002995 = 0{,}9677479.$$

Ulterius procedi non est opus; quamobrem hinc habebimus

$$P = 1 - E = 0{,}0322521,$$

unde iam colligimus

$$\frac{1}{2}l2 - \frac{1}{3} \cdot 0{,}0322521 = 0{,}3358229.$$

24. Sumamus nunc $n = 5$ et habebimus

$$A = \mathfrak{Q} = 0{,}9961578,$$

tum vero erit

$$a = 1, \quad b = 0{,}9958847, \quad c = 0{,}9962048, \quad d = 0{,}9961453^{1}),$$

hinc igitur reperiemus

$$B = A - \frac{1}{3^5} \cdot 0{,}0038422 = 0{,}9961420$$
$$C = B - \frac{1}{5^5} \cdot 0{,}0002573 = 0{,}9961419.$$

Erit igitur

$$Q = 1 - C = 0{,}0038581$$

ideoque

$$\frac{1}{2}l2 - \frac{1}{3}P - \frac{1}{5}Q = 0{,}3350513.$$

1) Editio princeps: 0,9961753. Correxit A. M.

25. Sit nunc $n = 7$ et $A = \mathfrak{R} = 0{,}9995547$, tum vero $a = 1$, $b = 0{,}9995428$, hinc igitur fiet

$$B = A - \frac{1}{3^7} \cdot 0{,}0004453 = 0{,}9995545,$$

unde iam habemus

$$R = 1 - B = 0{,}0004455$$

ideoque

$$\frac{1}{2}l2 - \frac{1}{3}P - \frac{1}{5}Q - \frac{1}{7}R = 0{,}3349877\,.$$

26. Cum in hoc calculo tantum non fuerit $B = A$, in sequentibus nequidem littera B erit opus, quamobrem habebimus

$$S = 1 - \mathfrak{S} = 0{,}0000501$$

hincque

$$\frac{1}{9}S = 0{,}0000056\,.$$

Deinde vero erit

$$T = 1 - \mathfrak{T} = 0{,}0000053$$

hincque

$$\frac{1}{11}T = 0{,}0000005\,,$$

denique

$$U = 1 - \mathfrak{U} = 0{,}0000003 \text{ et } \frac{1}{13}U = 0{,}0000000\,.$$

Particulis igitur his a praecedente valore ablatis prodit

$$O = 0{,}3349816\,.$$

Unde patet hunc valorem adhuc aliquanto maiorem esse quam $\frac{1}{3}$.

27. Nunc igitur certi esse possumus summam seriei infinitae huius

$$\frac{1}{3} - \frac{1}{5} + \frac{1}{7} + \frac{1}{11} - \frac{1}{13} - \frac{1}{17} + \frac{1}{19} + \text{ etc.}$$

esse satis exacte = 0,3349816. Investigandum iam foret, num iste valor non quampiam teneat rationem notabilem, sive ad peripheriam circuli π, sive ad eius logarithmum hyperbolicum, quandoquidem supra observavimus seriem reciprocam numerorum primorum

$$\frac{1}{2}+\frac{1}{3}+\frac{1}{5}+\frac{1}{7}+\frac{1}{11}+\text{ etc.}$$

exprimere logarithmum hyperbolicum seriei harmonicae completae

$$1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\frac{1}{5}+\frac{1}{6}+\text{ etc.},$$

unde videri potest istam seriem numerorum primorum

$$\frac{1}{3}-\frac{1}{5}+\frac{1}{7}+\frac{1}{11}-\frac{1}{13}-\frac{1}{17}+\text{ etc.}$$

etiam continere logarithmum eiusdem seriei completae

$$1-\frac{1}{3}+\frac{1}{5}-\frac{1}{7}+\frac{1}{9}-\frac{1}{11}+\text{ etc.},$$

cuius summa est $\frac{\pi}{4}$. Hunc in finem subiungam logarithmum hyperbolicum ipsius π, quem olim[1]) reperi

1,14472,98858,49400,17414,34273,51353,05865.

Videndum igitur erit, num forte sit summa inventa $O = l\pi - lN$, ita ut N sit numerus satis simplex. Verum huiusmodi investigationes plerumque sine ullo successu instituuntur.

28. Ope posterioris methodi autem non solum summam seriei propositae elicuimus, sed etiam eius potestatum imparium, quas summas hic conspectui exponamus.

1) Confer opus 101 (indicis Enestroemiani): *Introductio in analysin infinitorum*, t. primus, Lausannae, 1748, p. 151; *Leonhardi Euleri Opera omnia*, series I, vol. 8, p. 202.

$$\frac{1}{3}-\frac{1}{5}+\frac{1}{7}+\frac{1}{11}-\frac{1}{13}-\frac{1}{17}+\frac{1}{19}+\text{etc.} = 0{,}3349816$$

$$\frac{1}{3^3}-\frac{1}{5^3}+\frac{1}{7^3}+\frac{1}{11^3}-\frac{1}{13^3}-\frac{1}{17^3}+\frac{1}{19^3}+\text{etc.} = 0{,}0322521$$

$$\frac{1}{3^5}-\frac{1}{5^5}+\frac{1}{7^5}+\frac{1}{11^5}-\frac{1}{13^5}-\frac{1}{17^5}+\frac{1}{19^5}+\text{etc.} = 0{,}0038602$$

$$\frac{1}{3^7}-\frac{1}{5^7}+\frac{1}{7^7}+\frac{1}{11^7}-\frac{1}{13^7}-\frac{1}{17^7}+\frac{1}{19^7}+\text{etc.} = 0{,}0004455$$

$$\frac{1}{3^9}-\frac{1}{5^9}+\frac{1}{7^9}+\frac{1}{11^9}-\frac{1}{13^9}-\frac{1}{17^9}+\frac{1}{19^9}+\text{etc.} = 0{,}0000501$$

$$\frac{1}{3^{11}}-\frac{1}{5^{11}}+\frac{1}{7^{11}}+\frac{1}{11^{11}}-\frac{1}{13^{11}}-\frac{1}{17^{11}}+\frac{1}{19^{11}}+\text{etc.} = 0{,}0000053^{1})$$

$$\frac{1}{3^{13}}-\frac{1}{5^{13}}+\frac{1}{7^{13}}+\frac{1}{11^{13}}-\frac{1}{13^{13}}-\frac{1}{17^{13}}+\frac{1}{19^{13}}+\text{etc.} = 0{,}0000003^{2})$$

etc.

29. Ipsae quidem hae summae sine dubio parum attentionis merentur, nisi forte ad quantitates cognitas reduci potuerint. Verum quia in his seriebus neque ipsi termini secundum certam legem progrediuntur, neque etiam in signis plus vel minus certus ordo observatur, ista disquisitio primo intuitu plane impossibilis videri potuisset, quamobrem ipsa methodus, qua ad earum summas pertigimus, utique omni attentione digna est censenda, idque eo magis, quod satis abstrusis serierum potestatum proprietatibus innititur. Nisi enim summae serierum

$$1-\frac{1}{3^n}+\frac{1}{5^n}-\frac{1}{7^n}+\frac{1}{9^n}-\text{etc.}$$

pro casibus, quibus n est numerus impar, fuissent cognitae, tota haec investigatio frustra fuisset suscepta.

---

1) Editio princeps: 0,0000056. Correxit A. M.

2) Editio princeps: 0,0000005. Correxit A. M.

DE INSIGNI PROMOTIONE SCIENTIAE NUMERORUM

Commentatio 598 indicis ENESTROEMIANI
Opuscula analytica, 2, 1785, p. 275—314
[Conventui exhibita die 26. octobris 1775]

1. Eximia omnino sunt, quae celeberrimus LA GRANGE in Comment. Academiae Regiae Borussicae pro Anno 1773[1]) de divisoribus formulae generalissimae $Btt + Ctu + Duu$ demonstravit, et maximam lucem in scientia numerorum, quae etiamnunc tantis tenebris est involuta, accendunt. Ob hoc ipsum autem, quod ista tractatio maxime est generalis, ii, qui non satis sunt exercitati in huiusmodi speculationibus, non parum difficultatis offendunt neque vim talium sublimium demonstrationum satis perspicere valent. Quamobrem haud inutile erit omnia momenta, quibus hae demonstrationes innituntur, diligentius explicare atque ad formulas magis speciales accommodare, quandoquidem hoc modo omnia facilius intelligi poterunt. Deinde imprimis accuratius exponam, quantum firmamentum hinc plurimis theorematibus, quorum veritatem per solam inductionem mihi quidem cognoscere licuit, afferri possit, unde multo clarius patebit, quantum adhuc ad eorum perfectam demonstrationem desideretur.

LEMMA

2. Si p et q fuerint numeri inter se primi, tum omnes plane numeri in hac forma generali $\alpha p \pm \beta q$ comprehendi possunt, idque infinitis modis.

Huius lemmatis demonstratio per se facilis passim invenitur.

1) LAGRANGE: *Recherches d'arithmétiques.* Nouv. Mém. de l'acad. royale des sc. de Berlin, année 1773, p. 265. *Oeuvres de Lagrange,* publ. par les soins de M. J.-A. Serret, t. 3, Paris 1869, p. 695.

PROBLEMA 1

3. *Si p et q sint numeri inter se primi, n vero denotet numerum quemcunque datum, sive positivum sive negativum, invenire omnes divisores huius formulae: $pp + nqq$.*

SOLUTIO

Denotet D divisorem quemcunque numeri in hac forma $pp + nqq$ contenti, sitque d quotus ex hac divisione ortus, ita ut sit $Dd = pp + nqq$. Hic iam statim evidens est numerum d ad q fore primum; si enim q haberet divisorem communem, eundem quoque p habere deberet, contra hypothesin; quamobrem numerus p per d et q ita exprimi poterit, ut sit $p = \alpha d \pm \beta q$, quo valore substituto fiet

$$Dd = \alpha\alpha dd \pm 2\alpha\beta dq + (\beta\beta + n)qq,$$

ideoque divisor

$$D = \alpha\alpha d \pm 2\alpha\beta q + \left(\frac{\beta\beta + n}{d}\right)qq,$$

ubi ergo $\frac{\beta\beta + n}{d}$ erit numerus integer, qui sit $= h$, ita ut habeatur

$$D = \alpha\alpha d \pm 2\alpha\beta q + hqq,$$

pro qua forma scribamus

$$D = frr \pm gqr + hqq,$$

ita ut sit $f = d$, $r = \alpha$, $g = 2\beta$, et ob $h = \frac{\beta\beta + n}{d}$ erit $fh = \beta\beta + n$; hincque fiet $4fh - gg = 4n$. Hinc igitur patet omnes divisores formae $pp + nqq$ semper contineri in hac forma:

$$D = frr \pm gqr + hqq,$$

dummodo fuerit $4fh - gg = 4n$. Ac vicissim, si fuerit

$$D = frr \pm gqr + hqq,$$

erit

$$4Df = 4ffrr \pm 4fgqr + 4fhqq;$$

ideoque ob $4fh = 4n + gg$ erit

$$4Df = (2fr \pm gq)^2 + 4nqq,$$

quae forma a proposita non discrepat, si modo dividatur per 4.

COROLLARIUM 1

4. In genere igitur omnes divisores formulae propositae $pp + nqq$ comprehendere licebit in ista formula latissime patente: $frr + grs + hss$, dummodo fuerit $4fh - gg = 4n$, sive $fh - \frac{1}{4}gg = n$; unde patet innumeras huiusmodi formulas exhiberi posse, quoniam numerum g pro lubitu accipere licet. Ex eo autem numeros f et h ita definiri oportet, ut fiat $4fh = 4n + gg$.

SCHOLION

5. Quoniam autem innumerabiles huiusmodi formulas: $frr + grs + hss$ exhibere licet, in quibus sit $4fh - gg = 4n$[1]), parum hinc lucri ad nostrum institutum afferri videtur. Proposito enim quocunque numero D, ad diiudicandum, utrum esse possit divisor formae $pp + nqq$, omnes illae innumerabiles formulae considerari deberent, num forte iste numerus D in quapiam illarum contineatur. Praecipuum igitur inventum, quod Illustri La Grange acceptum referre debemus, in hoc consistit, quod infinitam illam huiusmodi formularum multitudinem ad exiguum numerum pro quovis casu revocare docuit, id quod in sequente problemate exponamus.

PROBLEMA 2

6. *Formam generalem divisorum ante inventam,* $frr + grs + hss$, *in qua sit* $4fh - gg = 4n$, *in aliam eiusdem formae,* $f'tt + g'tu + h'uu$, *transmutare, in qua sit* $g' < f'$ *vel* h', *manente proprietate* $4f'h' - g'g' = 4n$.

SOLUTIO

Ponamus esse $f < h$ et numerum g quantumvis esse maiorem quam f, ac statuamus $r = t - \alpha s$, quo valore substituto orietur ista forma:

$$ftt + (g - 2\alpha f)ts + (\alpha\alpha f - \alpha g + h)ss;$$

1) Editio princeps, hic et in § 6, 7 et 8: n. Correxit R. F.

ubi manifesto α ita assumi poterit, ut fiat $g - 2\alpha f < f$, ubi quidem animadvertendum est nihil referre, utrum $g - 2\alpha f$ prodeat positivum an negativum. Statuatur igitur $g - 2\alpha f = \pm g'$, ita ut certe sit $g' < f'$, tum vero ob analogiam loco f scribatur f' et $\alpha\alpha f - \alpha g + h = h'$ eritque

$$4f'h' - g'g' = 4fh - gg = 4n.$$

Hoc igitur modo forma proposita reducta est ad hanc:

$$f'tt \pm g'ts + h'ss,$$

in qua certe est $g' < f'$. Quod si iam eveniat, ut g' adhuc maius fuerit quam h', tum simili modo ista formula in aliam transformari poterit, in qua coëfficiens medius utrovis extremo sit minor, unde patet formam propositam

$$frr \pm grs + hss$$

semper in aliam similis formae

$$f'tt \pm g'tu + h'uu$$

converti posse, in qua g' minus sit quam f' et h', simulque etiam fiat $4f'h' - g'g' = 4n$.

COROLLARIUM 1

7. Hoc igitur modo infinita multitudo formularum $frr + grs + hss$, in qua $4fh - gg = 4n$, plerumque ad satis exiguum numerum reduci potest, dum scilicet omnes illae formulae excludi possunt, in quibus coëfficiens medius g maior est alterutro extremorum.

COROLLARIUM 2

8. Cum igitur sit tam $f > g$ quam $h > g$, erit $4fh > 4gg$. Sit igitur $4fh = 4gg + \Delta$, et cum esse debeat $4fh - gg = 4n$, erit $3gg + \Delta = 4n$, ideoque $3gg < 4n$, hinc ergo $g < \sqrt{\frac{4n}{3}}$; quamobrem loco g successive eos tantum valores assumsisse sufficiet, qui sunt minores quam $\sqrt{\frac{4n}{3}}$, ex quibus

singulis facile colligentur valores litterarum f et h ex aequatione $4fh = gg + 4n$, quo facto omnes plane divisores formae $pp + nqq$ certe continebuntur in quapiam harum formularum simpliciorum.

SCHOLION

9. Quoniam aequatio $4fh - gg = 4n$ locum habere nequit, nisi g sit numerus par, pro g statim scribamus $2g$, ut forma d sit $frr + 2grs + hss$, existente $fh - gg = n$, quae ergo forma semper ita reduci potest, ut sit $2g < f$ vel $< h$. Haec autem reductio commodissime per gradus institui potest, dum loco α in superiori reductione scribitur unitas. Ita si fuerit divisor

$$D = frr + 2grs + hss,$$

erit quoque

$$D = f'rr + 2g'rs + h'ss,$$

existente duplici modo vel

$$f' = f, \; g' = f - g \text{ et } h' = f - 2g + h,$$

vel etiam

$$h' = h, \; g' = h - g \text{ et } f' = f - 2g + h,$$

quoniam membra extrema inter se commutare licet. Quod si hic nondum fuerit $2g' < f'$ seu $2g' < h'$, ista operatio tam diu continuari debet, donec fiat $2g < f$ vel h; ubi notandum in his formulis terminum medium $2grs$ tam positivum quam negativum accipi posse, propterea quod numeri r et s denotare possunt omnes numeros integros sive positivos sive negativos. His igitur praemissis investigemus omnes divisores primos numerorum vel in hac forma: $pp + nqq$, vel in hac: $pp - nqq$ contentorum; si quidem divisores compositi ex primis componuntur, ita ut cognitis omnibus divisoribus primis simul omnes compositi habeantur.

PROBLEMA 3

10. *Invenire omnes divisores primos numerorum in hac forma: $pp + nqq$ contentorum, existentibus numeris p et q tam inter se primis quam respectu numeri n*[1]).

1) Inde numerus n positivus est. R. F.

SOLUTIO

I. Quia enim hic de divisoribus primis tantum sermo est, nisi p esset quoque primus ad n, formula $pp + nqq$ etiam admitteret omnes divisores numeri n, qui propterea nullam investigationem requirunt et sponte se produnt. Sit ergo D divisor quicunque formae $pp + nqq$, ac modo vidimus semper fore

$$D = frr + 2grs + hss\,,$$

existente $fh - gg = n$, ita ut sit tam $2g < f$ quam $2g < h$; quare cum hinc sit $f > 2g$ et $h > 2g$, erit $fh > 4gg$. Sit igitur $fh = 4gg + \triangle$, et quia $fh - gg = n$, erit $3gg + \triangle = n$, ideoque $gg < \frac{n}{3}$ et $g < \sqrt{\frac{n}{3}}$. Hac igitur conditione multitudo formarum pro divisore D ad eo minorem numerum reducitur, quo minor fuerit numerus n. Cum igitur sit

$$D = frr + 2grs + hss\,,$$

erit

$$Df = ffrr + 2fgrs + fhss\,,$$

ideoque ob $fh = gg + n$ fiet

$$Df = (fr + gs)^2 + nss\,,$$

quae est ipsa forma proposita. Simili modo permutatis litteris f et h erit quoque

$$Dh = (hs + gr)^2 + nrr\,,$$

unde patet, si fuerit Df numerus formae $pp + nqq$, tum etiam productum Dh fore eiusdem formae, ita ut sufficiat alterutram invenisse. Pro quovis ergo casu quaerantur omnes valores litterae f, qui sint f, f', f'', f''' etc., atque omnes divisores primi D ita erunt comparati, ut vel D, vel Df, vel Df', vel Df'' etc. sint numeri formae $pp + nqq$. Haecque sequuntur ex demonstrationibus Illustris La Grange.

II. Haec igitur coniungamus cum iis, quae iam olim de formis horum divisorum primorum sum commentatus, ubi ostendi omnes hos divisores comprehendi posse in huiusmodi expressione: $4ni + a$, dum scilicet a

denotat certos numeros primos ad $4n$ simulque minores quam $4n$, ubi tantum semissis talium numerorum occurrit, reliquis hinc prorsus exclusis. Unde si α denotet hos numeros exclusos, affirmari poterit nullos numeros, in forma $4ni + \alpha$ contentos, esse posse divisores formae $pp + nqq$. Istae autem formae egregie conveniunt cum praecedentibus. Si enim fuerit $D = pp + nqq$, alteruter numerorum p et q debet esse impar, ideoque q vel par vel impar. Sit primo q par, ideoque qq numerus formae $4i$, fiet $D = 4ni + pp$. Unde patet litteram illam a complecti omnes numeros quadratos impares et primos ad $4n$, sive residua, quae ex divisione horum quadratorum, per $4n$ facta, remanent. Sin autem fuerit q numerus impar, ideoque qq formae $4i + 1$, hinc fiet $D = 4ni + pp + n$. Unde patet litteram a etiam complecti omnes numeros formae $pp + n$, qui quidem ad $4n$ sint primi, vel eorum residua ex divisione per $4n$ remanentia. Iidem vero etiam numeri pro a resultant, si fuerit Df numerus formae $pp + nqq$, id quod in exemplis facilius ostendi poterit.

III. His expositis, cum forma $4ni + a$ complectatur omnes divisores formae $pp + nqq$, altera autem forma $4ni + \alpha$ nullos divisores in se involvat, ex priori forma $4ni + a$ excludi debebunt omnes numeri divisibiles per quempiam numerum formae $4ni + \alpha$. Quod si igitur demonstrari posset hoc modo ex formula $4ni + a$ omnes plane numeros excludi, qui nequeunt esse divisores formae $pp + nqq$, tum manifesto sequeretur omnes numeros primos formae $4ni + a$ certe esse divisores formae $pp + nqq$, quandoquidem tantum numeros compositos hoc modo exclusimus. Totum ergo negotium huc redit, ut demonstretur formulam $4ni + \alpha$ omnes plane continere numeros primos, qui nequeunt esse divisores formae $pp + nqq$; quod si demonstrari posset, nihil amplius in hoc genere desideraretur.

COROLLARIUM 1

11. Pro quovis ergo numero n omnes numeri ipso $4n$ minores ad eumque primi in duas classes distribuentur, quarum alteram littera a, alteram vero littera α designavimus, ita ut formula $4ni + a$ contineat omnes divisores formae $pp + nqq$, altera vero formula $4ni + \alpha$ divisores illos penitus excludat, neque ullus numerus istius formae unquam esse possit divisor formulae $pp + nqq$. Multitudo autem numerorum utriusque classis semper

est eadem; scilicet si multitudo omnium numerorum minorum quam numerus $4n$ ad eumque primorum fuerit $= 2\lambda$ (semper enim iste numerus est par), prior forma a continet λ numeros, totidemque etiam continebit altera forma α.

COROLLARIUM 2

12. Circa has formulas: $4ni + a$ et $4ni + \alpha$ iam olim demonstravi[1]), si numeri a et a' in priore classe occurrant, tum ibi quoque occurrere productum aa', id quod etiam de pluribus numeris huius classis est intelligendum, qui si fuerint a, a', a'', a''' etc., etiam producta tam ex binis quam pluribus horum numerorum, atque adeo etiam omnes eorum potestates in eadem classe reperientur, postquam scilicet per $4n$ divisi ad residua minora quam $4n$ fuerint reducti. Deinde etiam demonstravi, si α fuerit numerus posterioris classis, tum in eadem quoque reperiri debere numeros $a\alpha$, $a'\alpha$, $a''\alpha$, $a'''\alpha$ etc. Unde patet multitudinem numerorum posterioris classis minorem esse non posse quam primae classis. Quod autem multitudo utrinque sit prorsus aequalis, id etiam facile demonstrari potest. Tum vero etiam hoc certum est, si α, α', α'', α''' etc. fuerint numeri posterioris classis, tum tam eorum quadrata quam eorum producta ex binis in priorem classem ingredi, producta autem ex ternis iterum in classe posteriore reperiri.

COROLLARIUM 3

13. Omnia igitur, quae adhuc in hoc genere desiderari possunt, huc redeunt, ut demonstretur classem $4ni + \alpha$ omnes continere numeros primos, qui nequeant esse divisores formae $pp + nqq$; tum enim evictum erit omnes numeros primos formae prioris $4ni + a$ certe esse divisores cuiuspiam numeri formae $pp + nqq$.

PROBLEMA 4

14. *Invenire omnes divisores primos numerorum in hac forma: $pp - nqq$ contentorum, ubi quidem, ut ante, p et q non solum sint primi inter se, sed etiam primi ad n.*

---

1) Vide commentationem 557 huius voluminis, praecipue Additamentum p. 45. R. F.

SOLUTIO

I. Conditio, quod p sit etiam primus ad n, ideo tantum hic adiicitur, quia alias etiam omnes divisores numeri n hic in censum venirent, quos tamen hic excludimus, utpote per se manifestos. Hic igitur primo patet, si fuerit D divisor primus formae $pp - nqq$, tum etiam fore divisorem formae $nqq - pp$, siquidem fuerit nqq maius quam pp. Nam si fuerit D divisor formae $pp - nqq$, erit quoque divisor formae $npp - nnqq$, quae forma, si loco nq scribamus r, abit in hanc: $npp - rr$. Deinde eodem modo ut ante patet semper fore

$$D = frr + 2grs + hss,$$

existente $fh - gg = -n$, hancque formam semper ita reduci posse, ut fiat $2g < f$ simulque $2g < h$, ubi quidem signa numerorum f et h non respiciuntur, si forte alterutrum membrum fiat negativum; quare cum, ob $f > 2g$ et $h > 2g$, sit $fh > 4gg$, evidens est fieri non posse

$$fh - gg = -n,$$

nisi vel f vel h fuerit negativum, unde forma divisoris ita debet constitui, ut sit

$$D = frr + 2grs - hss,$$

fierique debet $-fh - gg = -n$, sive $fh + gg = +n$. Quoniam igitur $fh > 4gg$, necesse est, ut sit $5gg < n$, ideoque $g < \sqrt{\frac{n}{5}}$, ita ut hoc casu pauciores valores pro g relinquantur. Tum autem erit

$$Df = ffrr + 2fgrs - fhss^{1}),$$

sive

$$Df = (fr + gs)^2 - nss,$$

quae est forma ipsa proposita. Porro autem erit

$$Dh = nrr - (gr - hs)^2,$$

quae est forma nostra inversa $npp - qq$. Hinc igitur intelligitur, si fuerit Df numerus formae $pp - nqq$, tum eo ipso formulam Dh fore numerum formae $npp - qq$.

1) Editio princeps: $ffrr + 2grs - fhss$. Correxit R. F.

II. Accommodemus haec etiam ad eam formam divisorum, quam olim exhibui[1]); ac primo quidem si fuerit $D = pp - nqq$, pro casibus, quibus q est numerus par, ideoque qq formae $4i$, fiet $D = pp - 4ni$; unde si ponatur $D = 4ni + a$, ob $pp > 4ni$, si ponatur $pp = 4nk + b$, prodibit talis forma: $D = 4ni + b$, ita ut sit $a = b$, ideoque omnes numeros quadratos ad $4n$ primos in se complectatur. Sin autem sit q numerus impar, ideoque qq formae $4i + 1$, fiet $D = pp - n - 4ni$, positoque iterum $pp = 4nk + b$ prodit $D = 4ni + b - n$, ita ut hoc casu sit $a = b - n$, ubi b denotare potest omnes numeros quadratos, vel residua inde orta. Simili modo si fuerit $D = npp - qq$, evidens est valores pro a hinc prodituros praecedentium fore negativos, ita ut a comprehendat omnes numeros quadratos, deinde etiam omnes numeros formae $pp - n$, tam positive quam negative sumtos; quamobrem forma omnium divisorum ita exhiberi poterit, ut sit $4ni \pm a$, forma autem pro numeris ex classe divisorum exclusis erit $4ni \pm \alpha$, quorum multitudo aequalis est priori, scilicet α semper totidem sortietur valores, quot habet littera a.

III. Quo igitur etiam in hoc genere nihil amplius desiderari queat, id tantum superest, ut demonstretur formam posteriorem $4ni \pm \alpha$ omnes plane continere numeros primos, qui nunquam esse queant divisores ullius numeri vel formae $pp - nqq$, vel $npp - qq$.

COROLLARIUM 1

15. De his binis formulis: $4ni \pm a$ et $4ni \pm \alpha$, quarum illa omnes divisores involvit, haec vero excludit, eadem valent, quae ante sunt tradita. Scilicet si a, a', a'' etc. ad priorem classem pertineant, ibidem quoque reperientur tam omnes potestates quam producta ex binis pluribusve horum numerorum; tum vero si α sit numerus posterioris classis, ibidem quoque occurrent omnes numeri $a\alpha$, $a'\alpha$, $a''\alpha$ etc., ita ut multitudo horum numerorum minor esse nequeat quam prioris classis.

COROLLARIUM 2

16. Quoniam littera a complectitur omnia quadrata, ante omnia eius valor erit $= 1$, tum vero etiam 9, 25 etc., nisi numerus n habeat divisorem

1) Vide notam p. 170. R. F.

vel 3, vel 5 etc. His enim casibus ista quadrata excludi oportet, quia alioquin forma $4ni \pm a$ numerus primus fieri non posset.

SCHOLION

17. His igitur generalibus praeceptis expositis omnia clariora evadent, si casus particulares evolvamus; hic enim plura adhuc occurrent, quae in genere attingere non licuit. Sufficiet autem id in aliquibus exemplis ostendisse, quibus pertractatis non difficile erit tabulam construere, quae pro omnibus casibus formas divisorum primorum exhibeat.

EXEMPLUM 1

18. Invenire omnes divisores primos numerorum in formula $pp + qq$ contentorum, dum scilicet pro p et q assumantur numeri inter se primi.

SOLUTIO

Posito divisore primo

$$D = frr + 2grs + hss,$$

ob $n = 1$ debet esse $fh = gg + 1$, tum vero $g < \sqrt{\frac{1}{3}}$; unde patet pro g alium valorem assumi non posse praeter 0; tum autem erit $fh = 1$ ideoque tam $f = 1$ quam $h = 1$, sicque omnes divisores in hac forma $D = rr + ss$ continebuntur, ita ut summa duorum quadratorum alios divisores non admittat, nisi qui ipsi sint summae duorum quadratorum. Altera autem forma divisorum erit $4i + 1$, et excludentur omnes numeri formae $4n + 3$ sive $4n - 1$. Quod si ergo demonstrari posset formulam $4i - 1$ omnes plane continere numeros primos, qui nequeunt esse divisores formae $pp + qq$, tum simul demonstratum esset etiam omnes divisores primos formae $4i + 1$ fore summam duorum quadratorum. Hoc autem iam dudum a me post FERMATIUM est demonstratum[1]).

1) Vide commentationem 241 (indicis ENESTROEMIANI): *Demonstratio theorematis Fermatiani omnem numerum primum formae* $4n + 1$ *esse summam duorum quadratorum.* Novi comment. acad. sc. Petr. 5 (1754/5), 1760, p. 3—13; *LEONHARDI EULERI Opera omnia*, series I, vol. 2, p. 328—337.
R. F.

EXEMPLUM 2

[18a.] Invenire omnes divisores primos formae $pp - qq$.

SOLUTIO

Hoc exemplum ad problema quartum refertur, estque $n = 1$, et quia debet esse $g < \sqrt{\frac{1}{5}}$, necessario fieri oportet $g = 0$, ideoque $fh = 1$, unde oritur haec forma divisorum: $D = rr - ss$, quae utique continet omnes plane numeros primos excepto binario. Quamquam enim haec forma habet factores $r + s$ et $r - s$, tamen continet omnes primos, si fuerit $r - s = 1$, cuius ratio est peculiaris. Id etiam altera divisorum forma declarat, qua, ob $a = 1$, fit $4i \pm 1$, in qua omnes plane numeri impares continentur, ita ut hoc casu nulli excludantur, alteraque forma $4i \pm \alpha$ hoc solo casu nullum locum habeat. Ceterum hic casus proprie huc non pertinet, quia divisores formae $pp - qq$ per se constant.

EXEMPLUM 3

19. Invenire omnes divisores primos formae $pp + 2qq$.

SOLUTIO

Hic casus pertinet ad problema tertium, existente $n = 2$, unde cum debeat esse $g < \sqrt{\frac{2}{3}}$, erit $g = 0$, ideoque $fh = 2$, hinc forma divisorum erit $= rr + 2ss$. Unde patet numeros formae $pp + 2qq$ alios non admittere divisores, nisi qui sint eiusdem formae, quod quidem etiam iam dudum est demonstratum. Altera autem forma $D = 8i + a$, ob $a = pp$, vel etiam $a = pp + 2$, pro a hos dat valores: 1 et 3, ita ut omnes divisores formae $pp + 2qq$ sint vel $8i + 1$ vel $8i + 3$. Formae ergo, quae ex classe divisorum excluduntur, sunt $8i + 5$ et $8i + 7$, quas igitur sub forma $8i + \alpha$ complecti oportet. Quod si ergo demonstrari posset solos numeros primos harum formarum ex classe divisorum excludi, simul demonstratum esset omnes numeros primos priorum formarum $8n + 1$ et $8n + 3$ contineri in formula $pp + 2qq$, id quod quidem iam est ostensum[1]). Ceterum binae

1) Vide Commentationem 256 (indicis Enestroemiani): *Specimen de usu observationum in mathesi pura*, Novi comment. acad. sc. Petrop. 6 (1756/7), 1761, p. 185—230; *Leonhardi Euleri Opera omnia*, series I, vol. 2. p. 459—492. R. F.

posteriores formulae etiam ita exprimi possunt: $8i - 1$ et $8i - 3$, ita ut valores ipsius α sint negativi ipsius a, id quod in genere de divisoribus formae $pp + nqq$ est tenendum.

EXEMPLUM 4

20. Invenire omnes divisores primos formae $pp - 2qq$ sive $2pp - qq$.

SOLUTIO

Ex problemate quarto est $n = 2$, ideoque, ob $g < \sqrt{\frac{2}{5}}$, erit iterum $g = 0$ et $fh = 2$, unde pro divisoribus erit $D = rr - 2ss$, vel etiam $D = 2rr - ss$; unde patet has formas nullos alios divisores admittere, nisi qui ipsi sint eiusdem formae. Pro forma autem $D = 8i + a$, quia est $a = pp$, vel etiam $a = pp - 2$, valores pro a erunt ± 1, ergo omnes divisores continebuntur in forma $8i \pm 1$; excluduntur ergo omnes numeri formae $8i \pm 3$. Unde si soli numeri primi formae $8i \pm 3$ ex classe divisorum excludantur, necesse est, ut omnes numeri primi formae $8i \pm 1$ in forma proposita contineantur[1]).

COROLLARIUM 1

21. Cum in problemate tertio reductio divisorum ad formam $pp + nqq$ plerumque unico tantum modo succedat, in casu problematis quarti talis reductio semper infinitis modis succedit; semper enim numeros p et q infinitis modis ita assumere licet, ut vel ipse divisor D vel Df formulae $pp - nqq$ aequetur.

COROLLARIUM 2

22. Casu autem huius exempli notari meretur, si fuerit $D = pp - 2qq$, tum etiam fore $D = 2rr - ss$, quoniam hae duae formae inter se aequales fieri possunt, iis enim aequatis fit

$$pp + ss = 2(qq + rr) = (q + r)^2 + (q - r)^2 ,$$

ita ut sit $p = q + r$ et $s = q - r$.

1) Vide notam p. 38 huius voluminis. R. F.

EXEMPLUM 5

23. Invenire divisores primos formae $pp + 3qq$.

SOLUTIO

Quia hic est $n = 3$, ideoque $g < 1$, tantum erit $g = 0$, hincque divisor $D = rr + 3ss$, ita ut etiam hoc casu omnes divisores primi sint formae $pp + 3qq$. Quia autem limes pro g inventus ipsi unitati aequatur, quam superare non debet, evolvamus etiam casum $g = 1$, unde fit $fh = 4$ ideoque vel $f = 1$ et $h = 4$, vel $f = 2$ et $h = 2$. Priori casu fit

$$D = rr + 2rs + 4ss = (r + s)^2 + 3ss,$$

quae est ipsa forma proposita. Altero casu fit

$$D = 2rr + 2rs + 2ss,$$

quae forma cum factorem habeat 2, statui debet

$$D = rr + rs + ss,$$

quae autem pariter ad propositam reducitur. Nam si s est numerus par, puta $s = 2t$, erit

$$D = rr + 2rt + 4tt = (r + t)^2 + 3tt;$$

sin autem s est numerus impar, etiam r debebit esse impar, quia alioquin ad casum praecedentem revolveremur; erit ergo $r + s$ numerus par, unde posito $r = 2t - s$ fiet

$$D = 4tt - 2ts + ss = 3tt + (t - s)^2,$$

unde patet superiorem conclusionem etiamnunc valere, semperque esse $D = rr + 3ss$. Deinde pro formula $12i + a$ ob $a = pp$ erit $a = 1$, tum vero formula $a = pp + 3$ dat $a = 7$, unde omnes divisores continebuntur in alterutra harum formularum: $12i + 1$ vel $12i + 7$, quas coniunctim ita repraesentemus: $12i + 1, + 7$, vel etiam hoc modo $12i + 1, - 5$. Si enim omnes valores ipsius a infra $2n$ in genere deprimere liceat, admittendis

scilicet numeris negativis, tum altera formula $12i \pm \alpha$, in qua nullus divisor continetur, erit $12i + 5$ et $12i + 11$, vel $12i - 1$, $+ 5$, unde patet in genere valores ipsius α negativos esse ipsius a.

EXEMPLUM 6

[23a.] Invenire divisores [primos] formulae $pp - 3qq$ [sive] etiam $3pp - qq$.

SOLUTIO

Applicando hic problema quartum erit $n = 3$, ideoque $g < \sqrt{\frac{3}{5}}$, consequentur $g = 0$ et $fh = 3$, unde divisor erit $D = rr - 3ss$. Hinc patet hos numeros nullos alios divisores admittere, nisi qui sint eiusdem formae. Deinde pro formula $12i \pm a$, ob $a = pp$, vel $a = 3 - pp$, alii valores non prodeunt, praeter $a = 1$, ita ut omnes divisores contineantur in hac forma: $12i \pm 1$. Formula igitur divisores excludens erit $12i \pm 5$.

SCHOLION

24. Istas formulas iam olim expedivi[1]), et demonstravi eas alios divisores non admittere, nisi qui sint eiusdem formae, id quod in maioribus numeris pro n assumtis non semper contingit. Conveniet autem eos casus excludere, quibus n est vel numerus quadratus, vel per quadratum divisibilis. Si enim foret $n = kmm$, tum formula $pp \pm kmmqq$ conveniret cum hac: $pp \pm kqq$.

EXEMPLUM 7

25. Invenire divisores [primos] numerorum $pp + 5qq$.

SOLUTIO

Ob $\sqrt{\frac{5}{3}} > g$ erit vel $g = 0$ vel $g = 1$; priori casu fit $fh = 5$, posteriori vero $fh = 6$. Prior casus dat divisorem $D = rr + 5ss$, quae est ipsa forma proposita; posterior vero dat vel

1) Vide Commentationem 164 (indicis Enestroemiani): *Theoremata circa divisores numerorum in hac forma paa ± qbb contentorum.* Comment. acad. sc. Petrop. **14** (1744/6), 1751, p. 151—181; *Leonhardi Euleri Opera omnia*, series I, vol. 2, p. 194—222.

$$D = rr + 2rs + 6ss, \text{ vel}$$
$$D = 2rr + 2rs + 3ss,$$

quarum formarum illa per reductionem ad primam redit, cum sit

$$D = (r + s)^2 + 5ss;$$

haec vero ab illa discrepat, cum inde fiat

$$2D = 4rr + 4rs + 6ss = (2r + s)^2 + 5ss;$$

unde patet omnes divisores vel ipsos esse numeros huius formae, vel eorum dupla, ita ut, si ipse divisor D non fuerit formae $pp + 5qq$, eius duplum $2D$ certe futurum sit huius formae. Deinde pro forma $20i + a$, ob $a = pp$, eius valores hinc nati erunt 1 et 9, ex altera autem formula $= pp + 5$ colliguntur iidem valores 1 et 9. Quia vero hic tantum de divisoribus agitur, pro a etiam sumi poterit $\frac{pp+5}{2}$, unde oriuntur valores 3, 7, sicque formula omnes divisores continens erit $20i + 1, + 3, + 7, + 9$, contra vero formula divisores excludens erit $20i - 1, - 3, - 7, - 9$. Si iam demonstrari posset istam postremam formulam continere omnes numeros primos, qui nequeunt esse divisores formae propositae, simul demonstratum foret omnes numeros primos in priore forma contentos certo esse divisores cuiuspiam numeri formae $pp + 5qq$, ideoque vel ipsos vel eorum dupla eandem formam habere debere. Tales autem numeri usque ad centum sunt

1, 3, 7, 23, 29, 41, 43, 47, 61, 67, 83, 89.

EXEMPLUM 8

26. Invenire divisores [primos] numerorum formae $pp - 5qq$.

SOLUTIO

Hic ex problemate quarto est $n = 5$, unde ob $g < \sqrt{\frac{n}{5}}$ sumi poterit $g = 0$, vel etiam $g = 1$. Nihil enim nocet sumere $g = 1$; superfluum tantum foret ipsi maiorem valorem tribuere. At $g = 0$ dat divisorem $rr - 5ss$, hoc est formae propositae; alter vero valor $g = 1$ dat $fh = 4$ ideoque vel

$$D = rr + 2rs - 4ss, \text{ vel}$$
$$D = 2rr + 2rs - 2ss.$$

Prior reducitur ad $D = (r+s)^2 - 5ss$, hoc est ad propositam; posterior vero per 2 divisa dat divisorem

$$D = rr + rs - ss,$$

quae forma etiam ad propositam reducitur, quod ita ostendo. Vel ambo numeri r et s erunt impares, vel alter par, alter impar. Pro casu posteriore sit $s = 2t$ eritque

$$D = rr + 2rt - 4tt, \text{ sive } D = (r+t)^2 - 5tt.$$

Sin autem ambo numeri sint impares, erit eorum summa $r + s$ par, puta $2t$, ideoque $r = 2t - s$, unde fit

$$D = 4tt - 2ts - ss = 5tt - (t+s)^2.$$

Patet igitur omnes divisores numerorum formae propositae quoque eiusdem esse formae. Iam pro forma $20i \pm a$ valor $a = pp$ praebet 1 et 9, alter autem valor $a = 5 - pp$ praebet itidem 1 et 9, ita ut omnes divisores contineantur in hac forma $20i \pm 1$, ± 9. Altera autem forma divisores excludens erit $20i \pm 3$, ± 7.

SCHOLION

27. Quoniam ex his exemplis iam satis liquet, quomodo pro minoribus numeris n singulas has operationes institui oporteat, aliquot exempla circa numeros maiores adhuc afferamus.

EXEMPLUM 9

28. Invenire omnes divisores primos numerorum formae $pp + 17qq$.

SOLUTIO

Cum sit $\sqrt{\frac{17}{3}} < 3$, pro g habebimus tres valores 0, 1, 2. Primo sit $g = 0$, ideoque $fh = 17$, hinc divisor oritur D[1]$ = rr + 17ss$, ideoque ipsius formae

1) Editio princeps: *G.* Correxit R. F.

propositae. Secundo sumatur $g = 1$, erit $fh = 18 = 1 \cdot 18 = 2 \cdot 9 = 3 \cdot 6$, unde nascuntur hae formae:

1°. $D = rr + 2rs + 18ss = (r + s)^2 + 17ss$,
2°. $D = 2rr + 2rs + 9ss$, unde fit

$$2D = 4rr + 4rs + 18ss = (2r + s)^2 + 17ss,$$

ita ut $2D$ sit formae propositae.

3°. $D = 3rr + 2rs + 6ss$,

cuius triplum induit formam propositam: $[3D = (3r + s)^2 + 17ss]$.

Tertio sit $g = 2$ ideoque $fh = 21 = 1 \cdot 21 = 3 \cdot 7$; unde oritur

1°. $D = rr + 4rs + 21ss = (r + 2s)^2 + 17ss$,
2°. $D = 3rr + 4rs + 7ss$,

cuius triplum iterum formam propositam induit. Quamobrem omnes divisores ita erunt comparati, ut vel ipsi, vel eorum dupla, vel eorum tripla habeant formam propositam. Quod deinde ad formam $68i + a$ attinet, valor $a = pp$ praebet numeros 1, 9, 25, 49, 13, 53, 33, 21; alter autem valor $a = pp + 17$ dat 21, 33 [etc.], qui numeri cum praecedentibus conveniunt. Quia autem hic etiam subdupla et subtripla occurrere possunt, primo patet formam $a = \frac{pp}{2}$ nullos dare valores idoneos; at $a = \frac{pp}{3}$ sequentes praebet numeros: 3, 27, 7, 11, 39, 23, 31, 63. Deinde vero formula $a = \frac{pp + 17}{2}$ dat 9, [13,] 21 etc., qui numeri iam occurrunt. Denique formula $a = \frac{pp + 17}{3}$ praebet 7, 11, 27 etc., qui itidem iam adsunt. Quamobrem omnes valores idonei pro a erunt

1, 3, 7, 9, 11, 13, 21, 23, 25, 27, 31, 33, 39, 49, 53, 63.

Hi autem numeri multo facilius inveniri possunt; statim enim atque aliquos tantum reperimus, quoniam novimus eorum producta ex binis pluribusve etiam occurrere debere, ante omnia autem omnes numeri quadrati per se occurrunt, ex quibus, quia etiam 3 occurrit, iam omnes plane repe-

riuntur. Quod si iam omnes hos numeros infra semissem numeri 68 deprimamus, dum maiorum complementa ad 68 signo — affecta apponimus, tum valores ipsius a sequentem seriem constituent:

$$+1,\ +3,\ -5,\ +7,\ +9,\ +11,\ +13,\ -15,\ -19,\ +21,$$
$$+23,\ +25,\ +27,\ -29,\ +31,\ +33.$$

Si iam omnium horum numerorum signa mutemus, obtinebimus omnes valores litterae α pro formula $68i + \alpha$, ex qua omnes divisores sunt exclusi.

COROLLARIUM 3

29. Hinc igitur perspicuum est etiam pro omnibus aliis numeris positivis loco n assumtis in valoribus litterae a omnes plane occurrere numeros impares minores quam $2n$, et qui simul ad n sint primi, dum alii signo $+$, alii signo $-$ sunt affecti.

EXEMPLUM 10

30. Invenire omnes divisores primos numerorum in hac formula: $pp - 19qq$, vel etiam $19pp - qq$ contentorum.

SOLUTIO

Hic igitur ob $n = 19$ erit $g < \sqrt{\frac{19}{5}}$, ideoque $g < 2$, unde habebimus vel $g = 0$ vel $g = 1$. Sit primo $g = 0$ eritque divisor $D = rr - 19ss$ ob $fh = 19$, ideoque hi divisores iam sunt ipsius formae propositae. Sit porro $g = 1$ fietque

$$fh = 19 - 1 = 18 = 1 \cdot 18 = 2 \cdot 9 = 3 \cdot 6;$$

unde tres casus sunt evolvendi:

1°. $D = rr + 2rs - 18ss = (r + s)^2 - 19ss$,

quae forma iam in proposita continetur.

2°. $D = 2rr + 2rs - 9ss$,

cuius duplum ad formam propositam redit.

3°. $D = 3rr + 2rs - 6ss$,

cuius triplum in forma proposita continetur. Sicque omnes divisores quaesiti vel ipsi, vel eorum dupla, vel eorum tripla in forma proposita continentur. Deinde pro forma $4ni \pm a$, sive $76i \pm a$ valores ipsius a ex sequentibus formulis derivari debent:

1°. $a = pp$ dat 1, 9, 25, 49, 5, 45, 17, 73, 61.

2°. $a = \frac{pp}{2}$ dat nullos valores idoneos, quia omnes forent pares.

3°. $a = \frac{pp}{3}$, sive $a = 3tt$, praebet hos valores:
3, 27, 75, 71, 15, 59, 51, 67, 31.

4°. $a = 19 - pp$ dat 15, 3 etc.,

qui iam occurrunt,

5°. $a = \frac{19-pp}{2}$ dat 9, 5, 3 etc.,

qui iidem iam adsunt.

6°. $a = \frac{19-pp}{3}$ dat 5, 1, 15 etc.,

qui etiam adsunt. Quamobrem omnes numeri idonei pro a assumendi, quoniam tam positive quam negative accipi possunt, infra 38 deprimi possunt, dum scilicet maiorum complementa ad 76 apponuntur:

1, 3, 5, 9, 15, 17, 25, 27, 31.

Pro altera autem forma $76i \pm \alpha$, in qua nulli divisores occurrere possunt, valores ipsius α sunt sequentes:

7, 11, 13, 21, 23, 29, 33, 35, 37.

SCHOLION

31. Hactenus alios numeros pro n non assumsimus, praeter primos, quamobrem etiam adhuc adiungamus duo exempla circa numeros compositos.

EXEMPLUM 11

32. Invenire omnes divisores primos numerorum in hac forma contentorum: $pp + 30qq$.

SOLUTIO

Hic ob $n = 30$ et $g < \sqrt{10}$, loco g quatuor valores assumi conveniet, 0, 1, 2, 3, quos ergo singulos percurramus:

I. $g = 0$ praebet $fh = 30$, unde pro divisore D sequentes formulae nascuntur:

1°. $D = rr + 30ss$,
2°. $D = 2rr + 15ss$,
3°. $D = 3rr + 10ss$,
4°. $D = 5rr + 6ss$,

quarum prima cum forma proposita congruit, tum vero secundae duplum, tertiae triplum et quartae quintuplum; ubi notetur loco quintupli etiam sextuplum sumi posse, quandoquidem si fuerit

$$5D = pp + 30qq,$$

tum etiam erit

$$6D = pp + 30qq.$$

II. Sit iam $g = 1$, erit $fh = 31$, unde unica forma nascitur

$$D = rr + 2rs + 31ss = (r + s)^2 + 30ss,$$

quae est ipsa forma proposita.

III. Sit $g = 2$, erit $fh = 34 = 1 \cdot 34 = 2 \cdot 17$; unde duae formae nascuntur:

1°. $D = rr + 4rs + 34ss = (r + 2s)^2 + 30ss$,
2°. $D = 2rr + 4rs + 17ss$,

cuius duplum ad formam propositam reducetur.

IV. Sit $g = 3$ eritque $fh = 39 = 1 \cdot 39 = 3 \cdot 13$, unde iterum duae nascuntur formae:

1°. $D = rr + 6rs + 39ss = (r + 3s)^2 + 30ss$,
2°. $D = 3rr + 6rs + 13ss$,

cuius triplum induit formam propositam. Ex his igitur sequitur omnes divisores D ita esse comparatos, ut vel D, vel $2D$, vel $3D$, vel $6D$ in forma proposita contineantur. Deinde vero pro forma $4ni + a = 120i + a$ ante omnia notetur multitudinem omnium numerorum minorum quam 120 simulque ad 120 primorum esse 32, unde iam certo inferre possumus numerum valorum tam litterae a quam α esse 16. Cum igitur primo in a omnes numeri quadrati occurrant, formula $a = pp$ dabit hos tantum numeros: 1 et 49; at vero formae $\frac{pp}{2}$, $\frac{pp}{3}$ et $\frac{pp}{6}$ nullos plane praebent numeros ad 120 primos. Altera vero forma $a = pp + 30$ praebet hos tantum numeros: 31, 79. Hinc autem porro $a = \frac{pp + 30}{2}$, sive haec: $a = 2tt + 15$ praebet 17, 23, 47, 113. Porro $a = \frac{pp + 30}{3}$, sive $a = 3tt + 10$ praebet 13, 37. Haec igitur forma tantum dat duos valores. Denique $a = \frac{pp + 30}{6}$, sive $a = 6tt + 5$ dat hosce: 11, 29, 59, 101. Hoc autem modo tantum 14 prodierunt valores pro littera a, ita ut duo adhuc desiderentur. Verum hic perpendendum est loco formulae $pp + 30$ generalius poni potuisse $pp + 30qq$, unde sumendo $p = 3t$ et per 3 dividendo statui poterit $a = 3tt + 10qq$. Sit nunc $q = 2$, fietque $a = 3tt + 40$, unde casus $t = 1$ praebet $a = 43$, at $t = 3$ dat $a = 67$; hocque modo nacti sumus omnes 16 valores ipsius a, qui ordine ita procedunt:

1, 11, 13, 17, 23, 29, 31, 37, 43, 47, 49, 59, 67, 79, 101, 113.

Quod si iam loco numerorum maiorum quam 60 eorum complementa ad 120 cum signo — scribantur, isti numeri ita disponi poterunt:

$$+1, -7, +11, +13, +17, -19, +23, +29, +31, +37,$$
$$-41, +43, +47, +49, -53, +59,$$

ubi omnes plane numeri impares ad 30 primi occurrunt vel signo + vel — affecti, ubi si signa mutentur, habebuntur omnes valores litterae α pro formula $120i + \alpha$, cuius omnes numeri ex classe divisorum excluduntur.

COROLLARIUM 1

33. Omnes ergo divisores numerorum formae $pp + 30qq$ in quatuor classes distribuuntur, quarum prima continet eos, qui ipsi sunt formae $pp + 30qq$; secunda classis vero eos, quorum dupla sunt eius formae; tertia, quorum tripla, et quarta denique eos, quorum quintupla vel etiam sextupla ad formam $pp + 30qq$ reduci possunt. Hae igitur quatuor classes, si formam propositam $pp + 30qq$ littera F, divisores vero littera D designemus, hoc modo repraesentari possunt:

$$\text{I. } D = F, \quad \text{II. } 2D = F, \quad \text{III. } 3D = F, \quad \text{IV. } 5D = F;$$

ubi notasse iuvabit, si fuerit $2D = F$, tum etiam fore $15D = F$; similique modo si fuerit $3D = F$, erit etiam $10D = F$; at si fuerit $5D = F$, erit etiam $6D = F$.

COROLLARIUM 2

34. Quando dicimus omnes divisores numerorum formae propositae $pp + 30qq$ in forma $120i + a$ contineri, id non ita est intelligendum, quasi omnes numeri in formula $120i + a$ contenti essent divisores, sed inde excludi debent omnes illi, qui per quempiam numerum formae $120i + \alpha$ sunt divisibiles. His autem sublatis maxime probabile videtur omnes reliquos numeros formulae $120i + a$, ideoque imprimis numeros primos, certe fore divisores cuiuspiam numeri formae $pp + 30qq$. Isti autem numeri primi in formula $120i + a$ contenti facili negotio quousque libuerit assignari possunt, quippe qui hoc ordine usque ad 240 progrediuntur:

1, 11, 13, 17, 23, 29, 31, 37, 43, 47, 59, 67, 79, 101, 113,
131, 137, 149, 151, 157, 163, 167, 179, 199, 233.

COROLLARIUM 3

35. Quoniam omnes divisores sunt quadruplicis generis, inde etiam valores ipsius a in quatuor classes distribui conveniet, prouti inde oriuntur divisores vel primae, vel secundae, vel tertiae, vel quartae classis, quibus ergo subscribamus characteres cuiusque classis 1, 2, 3, 6, hoc modo:

1, 11, 13, 17, 23, 29, 31, 37, 43, 47, 49, 59, 67, 79, 101, 113
1, 6, 3, 2, 2, 6, 1, 3, 3, 2, 1, 6, 3, 1, 6, 2.

Hic igitur notari meretur singulas classes quater occurrere[1]).

EXEMPLUM 12

36. Invenire omnes divisores primos numerorum in hac forma: $pp - 30qq$, sive in hac: $30pp - qq$ contentorum.

SOLUTIO

Cum hic sit $\sqrt{\frac{30}{5}} < 3$, pro littera g habemus tantum tres valores 0, 1, 2. Hinc cum sit $fh = 30 - gg$, pro primo casu erit $fh = 30$, pro secundo $fh = 29$ et pro tertio $fh = 26$, quos igitur casus evolvamus.

I. Sit $g = 0$ et hinc nascuntur sequentes valores:

1°. $D = rr - 30ss$,
2°. $D = 2rr - 15ss$,
3°. $D = 3rr - 10ss$[2]),
4°. $D = 5rr - 6ss$.

II. Si $g = 1$, unica forma nascitur

$$D = rr + 2rs - 29ss = (r + s)^2 - 30ss,$$

quae ergo est ipsa forma proposita.

III. Si $g = 2$, oriuntur duae formulae

1°. $D = rr + 4rs - 26ss = (r + 2s)^2 - 30ss$;

iterum ipsa proposita

2°. $D = 2rr + 4rs - 13ss$,

---

1) Haec assertio omnes divisores formae propositae in classes distribui posse vera est, quia genus formarum determinantis —30 unam modo classem secundum definitionem Gaussii continet. R. F.

2) Editio princeps: $D = 2rr - 10ss$. Correxit A. M.

cuius duplum fit numerus formae propositae. Hinc ergo nascuntur quadruplicis generis divisores, qui posita littera F pro formula proposita sunt

$$\text{I. } D = F^{1}), \quad \text{II. } 2D = F, \quad \text{III. } 3D = F, \quad \text{IV. } 6D = F.$$

Deinde vero pro formula omnes divisores continente $120i \pm a$ erit primo vel $a = pp$, vel $a = \frac{pp}{2}$, vel $a = \frac{pp}{3}$, vel $a = \frac{pp}{6}$, unde alii numeri ad 30 primi oriri nequeunt nisi ex prima forma $a = pp$, ideoque duo tantum valores hinc nascuntur: scilicet 1 et 49. Altera autem forma erat $a =$ vel $30 - pp$, vel $\frac{30-pp}{2}$, vel $\frac{30-pp}{3}$, vel $\frac{30-pp}{6}$, quarum prima $a = 30 - pp$ praebet hos numeros: 29, 19, 91. Quia autem loco 30 ponere possumus $30qq$, formula $a = 120 - pp$ praebet insuper hos valores: 119, 71. Secunda ad formam $a = 2tt - 15$ reducta dat hosce numeros: 13, 7, 17, 83, 113, 107. Huic vero formulae aequivalet $15pp - 2qq$, ergo sumto $p = 3$ erit quoque $a = 135 - 2qq$, unde prodeunt 13, 7, 103 [, 37]; ideoque insuper novus 103 accedit. Ex tertia forma $a = 3tt - 10$ hosce novos numeros nanciscimur: 7, 17, forma autem affinis $a = 10tt - 3$ praebet insuper 37. Ex ultima forma $5tt - 6$ nascuntur hi valores: 1, 119; ex forma vero affini $a = 6tt - 5$ isti: 1, 19, 49, 91. Hinc imprimis notandum est eosdem numeros ex diversis classibus oriri posse. Prodierunt autem hactenus:

1, 7, 13, 17, 19, 29, 37, 49, 71, 83, 91, 103, 107, 113, 119,

quorum valorum numerus quidem tantum est 15, cum esse deberet 16; quia autem novimus cuiusque numeri complementum ad 120 etiam occurrere debere, iste defectus facile suppletur. Deerat scilicet 101 tanquam complementum ipsius 19. Quia autem numeri a tam positive quam negative accipi possunt, complementa reiicere licet, ita ut pro a habeamus octo sequentes valores:

1, 7, 13, 17, 19, 29, 37, 49,

reliqui igitur numeri praebent valores litterae α, qui erunt totidem

11, 23, 31, 41, 43, 47, 53, 59.

1) Editio princeps: *E.* Correxit A. M.

COROLLARIUM 1

37. Hoc igitur casu, admisso meo theoremate, quod omnes numeri primi in forma $4ni + a$ contenti simul sint divisores numerorum formae $pp \pm nqq$, numeri primi ex nostra formula $120i \pm a$ orti usque ad 240 sunt sequentes:

1, 7, 13, 17, 19, 29, 37, 71, 83, 101, 103, 107, 113, 127, 137,
139, 149, 157, 191, [211,] 223, 227, 233[, 239].

COROLLARIUM 2

38. Quoniam in hac evolutione vidimus eosdem numeros ex diversis classibus ortos esse, manifestum est nequicquam quatuor classes diversas esse constitutas, sed binas earum in unam coalescere posse. Primo enim omnes divisores quartae classis, pro quibus erat $5D = F$, sive etiam $6D = F$, iam in prima classe $D = F$ reperiuntur, ita ut semper, quoties fuerit $5D = F$, etiam futurum sit $D = F$. Simili modo divisores tertiae classis etiam continentur in classe secunda. Quod si enim fuerit $3D = F$, semper etiam erit $2D = F$, quamobrem omnes divisores pro forma proposita $pp - 30qq$, vel $30pp - qq$ ad duas tantum classes priores revocari possunt: semper enim erit vel $D = F$ vel $2D = F$.

COROLLARIUM 3

39. Omnes igitur numeri primi ex nostra forma $120i \pm a$ oriundi duplicis erunt generis, dum vel ipsi vel eorum dupla formam propositam haberi possunt, quos simili modo ut ante distingui conveniet, subscribendo singulis valoribus characteres vel 1 vel 2

1,	7,	13,	17,	19,	29,	37,	49
1,	2,	2,	2,	1,	1,	2,	1.

Ubi notetur ambos characteres totidem occurrere[1]).

1) Vide notam 1) p. 186. R. F.

SCHOLION

40. Quod si ergo pro numeris cuiuscunque formae $pp \pm nqq$ omnes divisores primi desiderentur, eos facillime ex nostra forma generali $4ni + a$ assignare licet; dum contra, si formulis ab Illustri La Grange exhibitis uti vellemus, opus foret maxime molestum ex singulis formis $frr + 2grs + hss$ omnes numeros primos elicere; quamobrem maxime est optandum, ut demonstratio firma illius mei asserti detegatur, quippe quo demum ista Theoria ad summum perfectionis gradum evehetur. Arbitror autem talem demonstrationem mox fortasse sperari posse, si sequentia momenta probe perpendantur.

1). Postquam pro formula proposita quacunque $pp \pm nqq$ ambae meae formulae $4ni + a$ et $4ni + \alpha$ fuerint constitutae, eae simul omnes plane numeros impares ad propositum n primos complectuntur; tum vero omnes divisores ad formam priorem $4ni + a$ referuntur; nulli autem numeri alterius formae $4ni + \alpha$ possunt esse divisores propositae, sive omnes numeri posterioris formae ex classe divisorum penitus excluduntur.

2). Probe perpendatur quovis casu omnes valores ipsius a egregia lege inter se cohaerere, ita ut omnes coniunctim quasi ambitum quendam completum constituant, in quo nihil deficiat nihilque abundet, quandoquidem omnia producta ex binis pluribusve horum numerorum iterum in eadem classe occurrunt, ita ut, simul atque aliqui valores idonei pro a fuerint inventi, ex iis reliqui omnes facile definiri queant, praecipue quoniam omnes numeri quadrati eorumve residua respectu divisoris $4n$ certe ingrediuntur. Unde si hoc modo omnia producta atque etiam potestates numerorum iam inventorum inserantur, mox tota ista classis ita adimplebitur, ut multitudo omnium numerorum huc pertinentium semper sit semissis omnium plane numerorum ad $4n$ primorum eoque minorum; altera vero semissis praebebit classem numerorum α, qui nullo modo divisores evadere possunt.

3). Hinc igitur patet ambas istas classes discrimine maxime memorabili et in natura ipsa numerorum fundato a se invicem discrepare atque adeo essentialiter a se invicem distingui, ita ut numeri alterius classis natura sua ab altera classe prorsus sint diversi.

4). Quoniam nulli numeri classis $4ni + \alpha$ unquam esse possunt divisores ullius numeri formae $pp \pm nqq$, ista classis tanquam origo spectari

debet omnium numerorum, quorum natura ab indole divisorum abhorret, quae repugnantia quoque ad omnes numeros extendi debet, qui divisibiles sunt per ullum numerum classis $4ni + \alpha$. Si enim tales numeri possent esse divisores, etiam isti huius classis numeri forent divisores, id quod naturae rei repugnat.

5). Cum autem producta ex binis numeris classis $4ni + \alpha$ in classem divisorum $4ni + a$ transeant, manifestum est in prima classe plurimos occurrere debere ab indole divisorum alienas; omnes scilicet eos, qui per ullum numerum alterius classis sunt divisibiles.

6). Quod si iam omnes isti numeri in classe $4ni + a$ deleantur sive excludantur, qui natura divisorum refragantur, maxime probabile videtur reliquos numeros omnes indole divisorum fore praeditos. Cum hoc modo tantum numeri compositi expungantur, evidens est omnes plane numeros primos in forma $4ni + a$ contentos revera fore divisores cuiuspiam numeri formae $pp \pm nqq$. Totum ergo negotium huc redit, ut isti probabilitati vis perfectae demonstrationis concilietur. Haec autem veritas, siqua est, elegantius ita proponi potest.

THEOREMA DEMONSTRANDUM

41. *Si fuerit a divisor cuiuspiam numeri formae $pp + nqq$, ita ut sit $aD = pp + nqq$, tum quoties $4ni + a$ est numerus primus, toties quoque erit $D(4ni + a)$ numerus formae $pp + nqq$*[1]).

Hic autem sequentia notari oportet: 1). Numeros p et q inter se esse debere primos. 2). Divisorem a etiam primum esse debere ad n, quoniam divisores ipsius n hinc excluduntur. 3). Quod si forte eveniat, ut numerus $D(4ni + a)$ non videatur in forma $pp + nqq$ contineri, tum semper eius quadruplum, vel etiam eius productum per aliud quadratum, certe in ea contineri. Quoniam igitur hoc casu erit

$$D(4ni + a) = \left(\frac{p}{2}\right)^2 + n\left(\frac{q}{2}\right)^2,$$

1) Theorema verum est sub restrictione 3) infra indicata. Confer praefationem huius voluminis. R. F.

haec resolutio nullam exceptionem mereri est censenda. Ita cum sit $27 = 4^2 + 11 \cdot 1^2$, erit $a = 27$ et $n = 11$ et $D = 1$, unde formula $4ni + a$ evadit $44i + 27$, quae casu $i = 1$ praebet 71, hoc est numerum primum; neque tamen in integris esse potest $71 = pp + 11qq$. Est vero

$$4 \cdot 71 = 284 = 3^2 + 11 \cdot 5^2,$$

ideoque

$$71 = \left(\frac{3}{2}\right)^2 + 11 \cdot \left(\frac{5}{2}\right)^2.$$

Tales autem casus raro occurrunt et ideo non sunt excipiendi, quia numeri formulae $4ni + \alpha$ ita ex classe divisorum excluduntur, ut, etiamsi pro p et q numeri fracti accipiantur, tamen nunquam divisores esse queant.

SCHOLION

42. Superfluum foret has investigationes ad huiusmodi formulas: $mpp \pm nqq$ extendere, cum omnes divisores numerorum formae $mpp \pm nqq$ semper sint etiam divisores numerorum formae $pp \pm mnqq$. Quae igitur olim in Tomo XIV Comment. Vet. Academiae de divisoribus numerorum formae $mpp \pm nqq$[1]) sum commentatus et magnam partem ex sola inductione conclusi, nunc per egregias proprietates ab Illustri La Grange demonstratas non solum plurimum illustrantur, sed etiam ad multo maiorem certitudinis gradum perducuntur, ita ut iam nihil amplius desideretur, nisi ut solida demonstratio theorematis allati detegatur, quam nunc quidem mox exspectare licebit. Mea autem methodus imprimis hac gaudet praerogativa, quod eius ope omnes plane divisores huiusmodi formularum $mpp \pm nqq$ assignari et, quousque libuerit, continuari possunt, id quod insuper sequenti exemplo declarabo.

EXEMPLUM 13

43. Invenire omnes divisores formae $pp + 39qq$.

Primo igitur per formulas Illustris La Grange quaeramus omnes diversas formas horum divisorum, et cum sit $n = 39$ ideoque $\sqrt{\frac{39}{3}} < 4$, sufficiet pro q assumere hos quatuor valores: 0, 1, 2, 3.

1) Vide notam p. 177. R. F.

I. Valor igitur $g = 0$ praebet $fh = 39$, unde hae duae formae nascuntur:

1°. $rr + 39ss$, 2°. $3rr + 13ss$,

quarum prior dat divisores $D = F$ et altera $3D = F$, denotante F formam propositam.

II. Valor $g = 1$ dat $fh = 40$, unde nascuntur istae formae:

1°. $D = rr + 2rs + 40ss = (r + s)^2 + 39ss$,

ideoque $D = F$.

2°. $D = 2rr + 2rs + 20ss$,

quae forma autem numerus primus esse nequit.

3°. $D = 4rr + 2rs + 10ss$,

quae forma itidem non dat numeros primos.

4°. $D = 5rr + 2rs + 8ss$,

unde fit $5D = F$, vel etiam $8D = F$.

III. Casus $g = 2$ dat $fh = 43$, unde unica forma oritur:

$D = rr + 4rs + 43ss = (r + 2s)^2 + 39ss$,

ideoque $D = F$.

IV. Casus denique $g = 3$ praebet $fh = 48$, unde sequentes formae numeros primos continentes oriuntur:

1°. $D = rr + 6rs + 48ss = (r + 3s)^2 + 39ss$,

ideoque $D = F$.

2°. $D = 3rr + 6rs + 16ss$

dat $3D = F$, vel etiam $16D = F$. Hinc igitur patet omnino dari tria genera divisorum:

1) $D = F$, 2) $3D = F$, [3)] $5D = F$.

Quibus constitutis evolvamus formulam $4ni + a = 156i + a$, ubi primo notetur omnium numerorum ad 156 primorum ipsoque minorum multitudinem esse 48, unde usque ad semissem 78 erunt 24, quorum singuli vel

positive vel negative sumti praebent valores pro littera a. Isti ergo numeri erunt:

$$1,\ 5,\ 7,\ 11,\ 17,\ 19,\ 23,\ 25,\ 29,\ 31,\ 35,\ 37,\ 41^{1}),\ 43,$$
$$47,\ 49,\ 53,\ 55,\ 59,\ 61,\ 67,\ 71,\ 73,\ 77,$$

ubi primo quadrata habent signum $+$, qui ergo sunt

$$+1,\ +25,\ +49;$$

reliquorum vero numerorum quadrata divisione per 156 deprimantur infra 78, unde fiet

$$11^2 = -35,\quad 17^2 = -23,\quad 19^2 = +49,\quad 23^2 = +61^{2}).$$

Pro reliquis numeris consideremus formam $pp + 39$, unde sumto $p = 1$ prodit 40, cuius numeri ad genus tertium pertinentis divisor 5 habet signum $+$. Iam quia praecedentes numeri ad genus primum sunt referendi, eorum producta per 5 etiam ad genus tertium referri debebunt, unde nascentur sequentes numeri:

$$+5,\ +41,\ -31,\ -19,\ -67,\ -7.$$

Sit nunc $p = 2$ eritque $4 + 39 = 43$, qui est divisor primae classis, unde etiam numeri huius classis iam inventi per 43 multiplicati dabunt divisores primae classis, qui autem, cum numerus 43 sit nimis magnus, facilius ex sequentibus reperientur. Sumatur igitur $p = 3$ eritque $pp + 39 = 48$, cuius divisor 3 iam est exclusus. Sit ergo $p = 4$ eritque $16 + 39 = 55$, cuius divisorem 5 iam tractavimus; alter vero divisor 11 etiam ad tertiam classem pertinet; per hunc ergo numeri primae classis multiplicati erunt:

$$+11,\ +59,\ -37,\ -73,\ +71,\ +47.$$

Multiplicentur etiam numeri tertiae classis per 11 et producta depressa, qui sunt

$$+55,\ -17,\ -29,\ -53,\ +43,\ -77,$$

1) Editio princeps: 51. Correxit A. M.

2) Signum aequalitatis in his formulis eadem significat, quae signum congruentiae a Gaussio definitum. R. F.

revertentur ad classem primam. Hoc modo omnes nostri numeri signa sua debita sunt adepti, qui cum vel ad primam vel ad tertiam classem referantur, manifestum est nullos divisores secundae classis relinqui. Omnes scilicet hi numeri iam in prima classe continentur, quamobrem omnes valores ipsius a cum characteribus suis I vel III subscriptis ita se habebunt:

$+1$,	$+5$,	-7,	$+11$,	-17,	-19,	-23,	$+25$,	-29,	-31,	-35,	-37,
I	III	III	III	I	III	I	I	I	III	I	III

$+41$,	$+43$,	$+47$,	$+49$,	-53,	$+55$,	$+59$,	$+61$,	-67,	$+71$,	-73,	-77
III	I	III	I	I	I	III	I	III	III	III	I.

Neque vero classis secunda prorsus est inutilis: dantur enim numeri primi, quos ad primam classem retulimus, quorum resolutio in integris non succedit atque adeo denominatorem quadratum 16 postulat, cuiusmodi numerus est 61[1]), qui aliter ad primam classem redigi nequit, nisi hoc modo: $61 = \left(\frac{25}{4}\right)^2 + 39\left(\frac{3}{4}\right)^2$. Est vero $3 \cdot 61 = 183 = 12^2 + 39 \cdot 1^2$. Quod si iam valores negativi pro a inventi in positivos convertantur, sumendis complementis ad 156 sequentes valores prodibunt:

1,	5,	11,	25,	41,	43,	47,	49,	55,	59,	61,	71,	79,	83,	89,	103[2]),
I	III	III	I	III	I	III	I	I	III	I	III	I	III	III	I

119,	121,	125,	127,	133,	137,	139,	149
III	I	III	I	I	III	I	III.

Nunc igitur omnes numeri primi in forma $156i + a$ contenti certe erunt divisores cuiuspiam numeri formae $pp + 39qq$, atque adeo vel ipsi, vel eorum quintupla, vel etiam tripla erunt numeri huius formae. Hinc ergo omnes divisores primi ab 1 usque ad 312 erunt sequentes:

1, 5, 11, 41, 43, 47, 59, 61, 71, 79, 83, 89, 103[3]), 127, 137, 139, 149, 157, 167, 181, 197, 199, 211, 227, 239, 277, 281, 283, 293.

---

1) Vide notam p. 190. R. F.

2) Editio princeps: 113. Correxit A. M.

3) Editio princeps: 113. Correxit A. M.

COROLLARIUM 1

44. Quo facilius intelligatur, cur hoc casu classis secunda ad primam sit revoluta, iam supra ostendimus, si divisor fuerit

$$D = frr + 2grs + hss,$$

existente $fh = gg + n$, tum non solum Df, sed etiam Dh ad formam $pp + nqq$ reduci posse. Hinc autem generalius si fuerit

$$k = ftt + 2gtu + huu,$$

tum productum Dk etiam erit numerus formae $pp + nqq$; facto enim calculo reperitur

$$Dk = (frt + g(ts + ru) + hsu)^2 + n(ts - ru)^2.$$

Quod si ergo k fieri queat quadratum, vel divisibile per quadratum, tum hoc quadratum omitti poterit. Nam si fuerit $Dkll$ numerus formae $pp + nqq$, tum, etiam admissis fractionibus, erit quoque Dk eiusdem formae. Ita nostro casu pro divisoribus secundae classis erat

$$D = 3rr + 13ss,$$

ideoque $k = 3tt + 13uu$, cuius valor sumto $t = 1$ et $u = 1$ fiet $k = 16$, qui cum sit numerus quadratus, haec forma ad primam reducitur.

COROLLARIUM 2

45. Nunc igitur omnia theoremata, quae circa huiusmodi divisores olim in Comment. veter. Tomo XIV dederam, multo maiorem gradum certitudinis sunt adepta, postquam a celeb. La Grange formae istorum divisorum sunt demonstratae; atque nullum dubium esse videtur, quin mox, quod in hoc genere adhuc desideratur, perfecta demonstratione muniatur.

COROLLARIUM 3

46. Antequam hoc argumentum penitus deseram, memorabilem adhuc observationem adiungam circa signa numerorum a, dum scilicet omnes eius valores infra $2n$ deprimuntur. Cum enim horum numerorum primus et ultimus simul sumti fiant $2n$, dispiciendum est, utrum hi duo numeri habeant vel paria signa vel disparia, utroque enim casu bini quicunque horum numerorum ab extremis aequidistantes, quorum ergo summa semper est $2n$, etiam habebunt sive eadem signa sive contraria. Ita nostro casu, quo erat $2n = 78$, ultimus 77 habebat signum —, dum primus 1 semper habet signum +, unde etiam signa binorum ab extremis aeque distantium perpetuo erunt contraria. E contrario autem in exemplo 11, ubi erat $2n = 60$, ultimus numerus 59 habebat signum +, unde etiam bini quicunque alii ab extremis aequidistantes eodem signo affecti deprehenduntur, cuius quidem phaenomeni ratio haud difficulter investigari poterit. Huiusmodi autem observationes laborem investigationis divisorum non mediocriter sublevant.

NOVAE DEMONSTRATIONES CIRCA DIVISORES NUMERORUM FORMAE $xx+nyy$[1)]

Commentatio 610 indicis Enestroemiani

Nova acta academiae scientiarum Petropolitanae 1 (1783), 1787, p. 47—74

Summarium ibidem p. 224—226

Conventui exhibita die 20. novembris 1775

SUMMARIUM

M. Euler avoit déjà donné dans le Tome XIV des anciens Commentaires[2]) un grand nombre de Théorèmes sur les diviseurs des nombres de la forme $xx + nyy$; mais ces Théorèmes sont sans démonstrations; et il a avoué lui-même ne les avoir trouvés que par induction. Les Théorèmes relatifs à cet objet qu'il avoit donnés dans la suite, dans les Tomes IV, VI et VIII des nouveaux Commentaires[3]), sont munis en partie de démonstrations; mais ils ne vont que jusqu'aux nombres de la forme $xx + 3yy$. M. de la Grange à qui l'on doit tant de belles démonstrations sur la nature et les propriétés des nombres, a poussé plus loin ces recherches dans un mémoire intitulé: *Recherches d'Arithmétique*, inséré aux nouveaux mémoires de l'Académie Royale des Sciences et Belles-Lettres de Berlin pour l'année 1773[4]); et c'est la lecture de ce mémoire qui a fourni à feu M. Euler l'occasion de reprendre cette matière.

Il débute par la démonstration du Théorème, que si l'on divise tous les nombres quarrés par un nombre premier P, le nombre de tous les résidus différens qui en résultent, soit toujours $\frac{1}{2}(P-1)$. Tous les nombres plus petits que P étant au nombre de $P-1$, dont celui des résidus $\frac{1}{2}(P-1)$ n'est que la moitié, le nombre de ceux qui sont exclus de la classe des résidus sera donc aussi $\frac{1}{2}(P-1)$, que l'Auteur nomme *non-résidus*.

1) Vide commentationem praecedentem p. 163. R. F.

2) *Theoremata circa divisores numerorum in hac forma paa ± qbb contentorum*, Comment. acad. sc. Petrop. 14 (1744/6), 1751, p. 151—181; *Leonhardi Euleri Opera omnia*, series I, vol 2, p. 194—222. R. F.

3) Voir les commentationes 228, 256 et 272 (indicis Enestroemiani), *Leonhardi Euleri Opera omnia*, series I, vol. 2, p. 295, 459 et 556. R. F.

4) Voir la note p. 163 de ce volume. R. F.

Le second Théorème, que M. EULER démontre de deux manières, c'est que, si la lettre a marque un résidu quelconque, et que le nombre n est contenu dans la forme $\lambda P - a$, on puisse toujours assigner deux nombres x et y, tels que la forme $xx + nyy$ soit divisible par P. D'où il suit que, si α marque un non-résidu et n un nombre de la forme $\mu P - \alpha$, la forme $xx + nyy$ ne puisse jamais être divisible par P.

Tous les nombres étant ou de la forme $\mu P - a$, ou de la forme $\mu P - \alpha$, il faut distribuer, pour chaque diviseur premier P, tous les nombres en deux classes, dont l'une contient tous les nombres n qui rendent la forme $xx + nyy$ divisible par P, et l'autre ceux qui excluent ce diviseur. Cela remarqué l'Auteur est en état de résoudre ce Problème: La lettre n marquant un nombre positif quelconque, trouver tous les nombres premiers qui puissent être diviseurs des nombres de la forme $xx + nyy$. La Solution de ce Problème est accompagnée d'une table qui, pour toutes les valeurs de n, depuis 1 jusqu'à 50, marque tous les diviseurs premiers des nombres de la forme $xx + nyy$.

Cette table qu'on peut assez facilement continuer à volonté pour des valeurs plus grandes de n, est suivie de la Solution d'un Problème analogue pour les cas où n est un nombre négatif, savoir $n = -m$, et qui est pareillement accompagnée d'une table pour tous les diviseurs premiers des nombres de la forme $xx - myy$, ou $myy - xx$, depuis $m = 2$ jusqu'à $m = 24$.

M. EULER finit ce mémoire par les deux Théorèmes suivans:

1°.) Si n est de la forme $4k + 1$ ou $4k + 2$, les nombres de la forme $4ni + 2n - 1$[1]) seront diviseurs de la forme $xx + nyy$, toutes les fois qu'ils sont premiers.

2°.) Si n est de la forme $4k$ ou $4k - 1$, les nombres de la forme $4ni - 2n + 1$ seront diviseurs des nombres de la forme $xx + nyy$, toutes les fois qu'ils sont premiers.

Théorèmes que l'illustre Géomètre n'a fait qu'énoncer, leur vérité étant évidente par les raisonnemens qui les précèdent dans cet intéressant mémoire.

Cum nuper eximia inventa Illustris DE LA GRANGE super divisoribus numerorum formae $xx + nyy$ recensuissem et cum meis observationibus, quas olim plerumque per inductionem erueram, contulissem, quippe quae inde haud exiguum firmamentum acceperant, non dubitavi mox perfectas demonstrationes, quae adhuc desiderabantur, polliceri. Fretus scilicet eram sagacitate acutissimi viri DE LA GRANGE, qua iam plures huius generis demonstrationes felicissimo successu in lucem produxit. Postquam autem omnes circumstantias, ad quas in hac investigatione est attendendum, accuratius perpendissem, mihi quoque contigit praecipua momenta, quibus istae exoptatae demonstrationes innituntur, perspicere, quae igitur hic exponere constitui.

1) Edition principale: $4ni + 2n + 1$. Corrigé par A. M.

THEOREMA 1

1. *Si omnes numeri quadrati per numerum quemcunque primum* P (*binario excepto, quippe cuius ratio per se est manifesta*) *dividantur, numerus omnium residuorum diversorum*[1]), *quae inde resultare possunt, semper est* $= \frac{1}{2}(P-1)$.

DEMONSTRATIO

Omnes numeri per propositum primum P non divisibiles in aliqua harum formularum continentur: $\lambda P \pm 1$, $\lambda P \pm 2$, $\lambda P \pm 3$, $\lambda P \pm 4$, ..., $\lambda P \pm \omega$, in quarum ultima est $\omega = \frac{1}{2}(P-1)$, quarum ergo formularum numerus est $\frac{1}{2}(P-1)$. Iam vero, si quadrata cuiusque harum formularum, veluti $(\lambda P \pm a)^2$, per numerum P dividantur, idem remanebit residuum, quod ex quadrato aa resultat, unde, cum a non superet numerum $\omega = \frac{1}{2}(P-1)$, manifestum est numerum residuorum, quae ex divisione quadratorum per numerum primum P oriri possunt, maiorem esse non posse quam $\frac{1}{2}(P-1)$. Haecque omnia residua nascuntur ex quadratis 1, 4, 9, 16, ... $\omega\omega$, exsistente $\omega = \frac{1}{2}(P-1)$, quae, quamdiu sunt minora quam P, ipsa erunt residua; sin autem fuerint maiora, per divisionem infra P deprimi possunt, ita ut omnia minora evadant quam P, uti ex natura divisionis est manifestum. Superest igitur, ut demonstretur numerum horum residuorum minorem esse non posse quam $\frac{1}{2}(P-1)$, id quod inde patebit, si ostenderimus omnia quadrata non maiora quam $\omega\omega$ diversa producere residua. Hunc in finem sint aa et bb duo huiusmodi quadrata, quae si per P divisa idem praeberent residuum, eorum differentia $bb - aa$ foret per P divisibilis; quia igitur P est numerus primus, vel $b + a$ vel $b - a$ deberet esse divisibile per P, quia vero tam a quam b non superant $\omega = \frac{1}{2}(P-1)$, manifestum est tam $b + a$ quam $b - a$ numeros ipso P minores esse, ideoque certe per P dividi non posse; unde evidens est numerum residuorum diversorum etiam minorem non esse quam $\frac{1}{2}(P-1)$. Sicque demonstratum est numerum omnium residuorum diversorum esse $= \frac{1}{2}(P-1)$.

COROLLARIUM 1

2. Quod si ergo litterae latinae a, b, c, d etc. denotent omnia residua, quae ex divisione numerorum quadratorum per numerum primum P resul-

1) qui non sunt divisibiles per numerum primum P. Vide commentationem 242 (indicis Enestroemiani), *Leonhardi Euleri Opera omnia*, series I, vol. 2, p. 338 et sequentes. R. F.

tare possunt, earum multitudo semper erit $\frac{1}{2}(P-1)$, in iisque semper occurrent quadrata 1, 4, 9, 16 etc., quatenus ipso numero P sunt minora, reliqua vero nascuntur ex quadratis maioribus quam P.

COROLLARIUM 2

3. Cum omnia residua a, b, c, d etc. sint minora quam divisor P, eorumque numerus tantum sit $\frac{1}{2}(P-1)$, dum omnium numerorum ipso P minorum multitudo est $P-1$; horum tantum semissis classem residuorum constituit, reliqui vero numeri, quorum multitudo etiam est $\frac{1}{2}(P-1)$, ex hac classe penitus excluduntur, quos ergo litteris graecis α, β, γ, δ etc. designemus et *non-residua*[1]) appellemus, ita ut pro quovis numero primo P omnes numeri ipso minores in duas classes sint referendi, quarum altera continet omnia residua a, b, c, d etc., altera vero non-residua α, β, γ, δ etc. In utraque autem classe perpetuo totidem continebuntur numeri, quorum multitudo est $\frac{1}{2}(P-1)$.

COROLLARIUM 3

4. Si ergo a denotet residuum quodcunque, omnes numeri quadrati continebuntur in hac formula generali: $\lambda P + a$, et semper coëfficientem λ ita accipere licebit, ut ista formula evadat quadratum; contra autem, si α denotet non-residuum quodcunque, haec formula $\lambda P + \alpha$ nunquam fieri poterit quadratum, quicunque numeri loco λ accipiantur.

SCHOLION

5. Iam olim plures egregias proprietates tam residuorum quam non-residuorum demonstravi, quas omnes hic repetere superfluum foret; sequentes autem tantum hic meminisse iuvabit[2]):

1°. Quod producta ex binis residuis, veluti ab, semper etiam in classe residuorum occurrant, postquam scilicet divisione per P ad valores minimos fuerint reducta, unde patet etiam omnes potestates cuiusque residui in eadem classe reperiri debere.

---

1) Vide p. 343 commentationis in nota p. 199 laudatae. R. F.

2) Vide commentationem in nota p. 199 laudatam. R. F.

2°. Sin autem residua per quodpiam non-residuum multiplicentur, producta semper in classe non-residuorum reperientur; unde patet ex unico non-residuo α reliqua omnia reperiri posse, dum scilicet residua a, b, c, d [etc.] per α multiplicentur.

3°. Sin autem bina non-residua, veluti α et β, in se invicem multiplicentur, producta $\alpha\beta$ in classem residuorum incidunt, producta vero ex ternis non-residuis iterum evadunt non-residua, ex quaternis vero denuo residua, et ita porro.

4°. Tum vero etiam, si quodvis residuum a per aliud residuum b dividatur, etiam quotus in classe residuorum reperietur, siquidem a dividi queat per b; sin vero dividi nequeat, semper dabitur tale multiplum ipsius P, quod sit μP, ut formula $\mu P + a$ divisionem per b admittat; atque etiam hoc casu quotus semper reperietur in classe residuorum.

THEOREMA 2

6. *Denotante a residuum quodcunque, quod ex divisione quadratorum per numerum primum P oriri potest, si numerus n contineatur in formula $\lambda P - a$, semper assignari poterunt numeri x et y tales, ut forma $xx + nyy$ divisionem admittat per numerum primum P.*

DEMONSTRATIO

Ponamus numerum primum P divisorem esse cuiuspiam numeri in forma $xx + nyy$ contenti, ita ut sit $\mu P = xx + nyy$; erit ergo $nyy = \mu P - xx$. Verum quadratum xx in forma $\lambda P + a$ continetur, quo substituto fiet $nyy = (\mu - \lambda)P - a = \nu P - a$, ideoque

$$n = \frac{\nu P - a}{yy}.$$

Quia autem yy est quadratum, in classe residuorum continetur, consequenter erit etiam $\frac{a}{yy}$ residuum, ideoque sub a comprehendi potest, unde in integris habebimus $n = \lambda P - a$. Hinc igitur vicissim sequitur[1]), quoties n fuerit

1) Haec observatio in alia demonstratione p. 204 probatur. R. F.

numerus in forma $\lambda P - a$ contentus, tum semper exhiberi posse numerum formae $xx + nyy$ divisibilem per numerum primum P.

COROLLARIUM 1

7. Hinc ergo etiam intelligitur, si α denotet quodcunque non-residuum respectu numeri primi P, fueritque n numerus in hac forma $\mu P - \alpha$ contentus, tum hunc numerum primum P nullo modo divisorem fieri posse ullius numeri in forma $xx + nyy$ contenti.

COROLLARIUM 2

8. Cum igitur omnes plane numeri vel in forma $\mu P - a$, vel in $\mu P - \alpha$ contineantur, hinc discimus pro quovis numero primo P omnes numeros in duas classes distribui, quarum utraque totidem contineat numeros, propterea quod multitudo valorum ipsius a eadem est ac valorum ipsius α, quarum classium altera omnes continebit numeros n, unde formula $xx + nyy$ recipere queat divisorem P; altera vero classis reliquos continebit numeros, qui si pro n accipiantur, formula $xx + nyy$ nullo modo per P divisibilis esse queat.

SCHOLION 1

9. Quo haec exemplo clariora reddantur, consideremus numerum primum 13, pro quo residua reperiuntur: 1, 4, 9, 3, 12, 10, non-residua vero: 2, 5, 6, 7, 8, 11; atque ut forma $xx + nyy$ divisibilis esse queat per 13, numerus n in aliqua sex sequentium formularum contentus esse debet:

$$13\lambda - 1,\ 13\lambda - 4,\ [13\lambda - 9,]\ 13\lambda - 3,\ 13\lambda - 12,\ 13\lambda - 10,$$

sicque valores idonei pro isto numero n ordine naturali dispositi erunt sequentes:

1, 3, 4, 9, 10, 12, 14, 16, 17, 22, 23, 25, 27, 29, 30, 35, 36, 38, 40,
42, 43, 48, 49, 51, 53, 55, 56, 61, 62, 64, 66, 68, 69, 74, 75, 77, 79,
81, 82, 87, 88, 90, 92, 94, 95, 100,

quorum numerus usque ad 100 est 46. Reliqui ergo numeri, qui divisorem 13 a formula $xx + nyy$ penitus excludunt, deletis iis, qui ipsi per 13 sunt divisibiles, ordine erunt isti:

2, 5, 6, 7, 8, 11, 15, 18, 19, 20, 21, 24, 28, 31, 32, 33, 34, 37, 41, 44, 45, 46, 47, 50, 54, 57, 58, 59, 60, 63, 67, 70, 71, 72, 73, 76, 80, 83, 84, 85, 86, 89, 93, 96, 97, 98, 99,

quorum numerus est 47, ideoque tantum non aequalis priori. Ratio autem, cur multipla ipsius 13 exclusimus, est, quod de formula $xx + 13vyy$, utrum divisorem 13 accipiat, quaestio esse non potest, quia manifesto numerus $[x]$ deberet esse divisibilis per 13.

SCHOLION 2

10. Quoniam vis nostrae demonstrationis clarius in exemplis perspicitur, contemplemur alium numerum primum 19, pro quo novem residua sunt: 1, 4, 9, 16, 6, 17, 11, 7, 5, novem vero non-residua: 2, 3, 8, 10, 12, 13, 14, 15, 18. Hinc igitur formula $xx + nyy$ divisorem 19 recipere poterit, si numerus n in sequenti forma contineatur:

$$n = 19\lambda - (1, 4, 9, 16, 6, 17, 11, 7, 5);$$

sin autem n contineatur in sequenti formula:

$$n = 19\lambda - (2, 3, 8, 10, 12, 13, 14, 15, 18),$$

tum nullus numerus formae $xx + nyy$ per 19 dividi poterit. Valores igitur idonei pro numero n usque ad centum ordine erunt

2, 3, 8, 10, 12, 13, 14, 15, 18, 21, 22, 27, 29, 31, 32, 33, 34, 37, 40, 41, 46, 48, 50, 51, 52, 53, 56, 59, 60, 65, 67, 69, 70, 71, 72, 75, 78, 79, 84, 86, 88, 89, 90, 91, 94, 97, 98,

quorum multitudo est 47. Reliqui vero numeri ad hunc scopum inepti, exclusis multiplis ipsius 19, erunt numero 48 sequentes:

1, 4, 5, 6, 7, 9, 11, 16, 17, 20, 23, 24, 25, 26, 28, 30, 35, 36, 39, 42, 43, 44, 45, 47, 49, 54, 55, 58, 61, 62, 63, 64, 66, 68, 73, 74, 77, 80, 81, 82, 83, 85, 87, 92, 93, 96, 99, 100.

SCHOLION 3

11. Quo autem facilius intelligatur, quomodo quovis casu, ubi numerus n idoneum habet valorem, formula $xx + nyy$ divisibilis reddatur per numerum

primum P, notetur hoc semper fieri posse, dum pro x et y numeri non maiores quam $\frac{1}{2}(P-1)$ accipiantur, atque adeo alterum horum numerorum y pro lubitu accipi posse. Sit igitur $y=1$, ita ut habeatur haec formula: $xx+n$, numerique n residuum nascatur r; tum igitur pro xx id quaeratur quadratum, cui conveniat residuum $P-r$, ac manifesto summa $xx+n$ per P erit divisibilis. Hoc autem semper fieri posse evidens est, cum sit $n=\lambda P-a$, unde fit residuum $r=P-a$, ideoque $P-r=a$, sicque pro xx id sumi debet quadratum, cui respondet residuum a. Ita sumto $P=13$ accipiatur pro n, pro lubitu, valor idoneus ex supra inventis, veluti $n=82$, et quaeratur x ita, ut fiat forma $xx+82$ per 13 divisibilis. Hic autem sit residuum $r=4$, hincque $P-r=9$; erit ergo $x=3$ et formula 3^2+82 per 13 dividi potest. Simili modo si pro divisore 19 sumatur $n=88$, inde oritur residuum $r=12$, ideoque $P-r=7$; quadratum autem, quod per 19 divisum relinquit 7, est 64, sicque formula 8^2+88 prodit divisibilis per 19. Atque hinc deduci potest facilior et concinnior demonstratio nostri theorematis.

ALIA DEMONSTRATIO THEOREMATIS 2

12. Ostendi scilicet potest, si fuerit $n=\lambda P-a$, tum semper dari numerum x, ut formula $xx+n$ divisionem admittat: tantum enim pro xx id sumatur quadratum, quod per P divisum relinquat a, quod ergo erit formae $\mu P+a$; quare ob $n=\lambda P-a$, erit formula $xx+n=(\mu+\lambda)P$, ideoque manifesto divisibilis per numerum P.

SCHOLION 1

13. Cum igitur pro quolibet numero primo P facile omnes valores numeri n exhiberi queant, quibus forma $xx+nyy$ divisionem per P admittere potest, quandoquidem, denotante a residua omnia ex divisione quadratorum per P oriunda, invenimus $n=\lambda P-a$, manifestum est pro n etiam infinitos valores negativos dari, qui oriuntur, si pro λ etiam numeri negativi accipiantur. Quamobrem non inutile erit pro numeris primis simplicioribus formulas exhibere, quae omnes valores idoneos numeri n contineant, quibus forma $xx+nyy$ per numerum primum P divisibilis reddi queat, quas igitur hic apponemus.

P	n
3	$3\lambda - 1$
5	$5\lambda - (1, 4)$
7	$7\lambda - (1, 4, 2)$
11	$11\lambda - (1, 4, 9, 5, 3)$
13	$13\lambda - (1, 4, 9, 3, 12, 10)$
17	$17\lambda - (1, 4, 9, 16, 8, 2, 15, 13)$
19	$19\lambda - (1, 4, 9, 16, 6, 17, 11, 7, 5)$
23	$23\lambda - (1, 4, 9, 16, 2, 13, 3, 18, 12, 8, 6)$
29	$29\lambda - (1, 4, 9, 16, 25, 7, 20, 6, 23, 13, 5, 28, 24, 22)$
31	$31\lambda - (1, 4, 9, 16, 25, 5, 18, 2, 19, 7, 28, 20, 14, 10, 8)$
37	$37\lambda - (1, 4, 9, 16, 25, 36, 12, 27, 7, 26, 10, 33, 21, 11, 3, 34, 30, 28)$
41	$41\lambda - (1, 4, 9, 16, 25, 36, 8, 23, 40, 18, 39, 21, 5, 32, 20, 10, 2, 37, 33, 31)$
43	$43\lambda - (1, 4, 9, 16, 25, 36, 6, 21, 38, 14, 35, 15, 40, 24, 10, 41, 31, 23, 17, 13, 11)$
47	$47\lambda - (1, 4, 9, 16, 25, 36, 2, 17, 34, 6, 27, 3, 28, 8, 37, 21, 7, 42, 32, 24, 18, 14, 12)$

COROLLARIUM

14. Si ergo n fuerit numerus negativus, puta $n = -m$, sumto λ negativo erit $m = \lambda P + a$, quae forma cum contineat omnes numeros quadratos, quicunque numerus primus pro P accipiatur, patet, si fuerit m numerus quadratus, scilicet $m = k^2$, numeros formae $xx - kkyy$ per omnes plane numeros primos divisibiles exsistere posse, quo ergo casu nulli numeri primi excluduntur, id quod per se est manifestum, quoniam formula $xx - kkyy$ in genere factores habet $x + ky$ et $x - ky$, quorum uterque per omnes numeros primos divisibilis reddi potest, id quod nullo alio casu fieri licet.

SCHOLION 2

15. Quemadmodum respectu cuiusvis numeri primi P omnes numeri in duas classes distinguuntur, quarum altera continet valores idoneos litterae n, ut formula $xx + nyy$ per eum numerum primum P divisibilis reddi queat, altera vero eos numeros, qui talem divisionem respuunt, ac praeterea multitudo numerorum in utraque classe contentorum eadem deprehenditur, ita vicissim pro quolibet numero n omnes numeros primos etiam in duas classes distingui oportet, quarum altera continebit eos, qui divisores exsistere

possunt formae $xx + nyy$, altera vero reliquos, qui nullo modo huius formae divisores exsistere possunt. Pro utraque autem classe iam olim formulas dedi generales[1]), similes illis, quibus hic pro quolibet numero primo valores idoneos numeri n ab ineptis distinxi: hoc tantum discrimine, quod, dum hic formulae divisorem P respiciunt, ibi numerus $4n$ divisoris locum obtineat. Scilicet pro divisoribus primis numerorum formae $xx + nyy$ dedi talem formam: $4ni + A$, pro iis vero, qui nullo modo divisores esse possunt, talem: $4ni + \mathfrak{A}$, ubi litterae A et $\mathfrak{A}$ simul complectuntur omnes numeros ad $4n$ primos ipsoque minores, ex quibus littera A continet eos, qui ad divisionem sunt apti, littera vero $\mathfrak{A}$ eos, qui excluduntur. Cum igitur has formulas olim per inductionem elicuissem, nunc nullum amplius dubium superesse potest, quin prior formula $4ni + A$ complectatur omnes numeros primos, per quos formulam $xx + nyy$ dividere licet, dum altera $4ni + \mathfrak{A}$ eos involvit, qui nullo modo divisores exsistere possunt. Interim tamen has ambas formulas sequenti modo ex positis principiis derivare licebit.

PROBLEMA

Proposito numero quocunque n positivo, assignare omnes numeros primos, per quos numeri formae $xx + nyy$ divisionem admittere queant.

SOLUTIO

16. Denotet P divisorem quemcunque primum formae propositae $xx + nyy$, sitque λ quotus ex hac divisione oriundus, atque habebimus hanc aequationem: $\lambda P = xx + nyy$, quam expressionem transformemus ponendo $x = 2nr + s$ et $y = 2t + u$, prodibitque ista aequatio:

$$\lambda P = 4n(nrr + rs + tu + tt) + ss + nuu\,,$$

cuius loco, quia $nrr + rs + tu + tt$ omnes numeros designare potest, scribamus brevitatis gratia λi, ut scilicet prius membrum per λ dividi possit, atque habebimus hanc aequalitatem: $P = 4ni + \frac{ss + nuu}{\lambda}$.

1) Vide p. 168 et 169 huius voluminis. R. F.

17. Hoc igitur modo iam nacti sumus formam supra memoratam: $4ni + A$, simulque patet loco A sumi debere omnes numeros ex formula $\frac{ss + nuu}{\lambda}$ resultantes, ubi, cum λ quemcunque numerum designare possit, littera A tam omnes numeros ipsos in forma $ss + nuu$ contentos, quam eorum divisores omnes in se comprehendet. Quoniam autem nostra forma numeros primos exhibere debet, loco A alios numeros accipere non licebit, nisi qui ad $4n$ fuerint primi, quos ergo oportebit esse impares simulque primos ad ipsum numerum n, sive cum n nullum habere debent divisorem communem.

18. Primo igitur inter valores litterae A, sumendo $u = 0$ et $\lambda = 1$, occurrent omnes numeri quadrati ss impares et ad n primi, vel ipsi, vel divisione per $4n$ facta depressi. Deinde sumendo $u = 1$, manente $\lambda = 1$, etiam occurrent omnes numeri in forma $ss + n$ contenti, quatenus scilicet ad $4n$ fuerint primi; ubi quidem plurimum notasse iuvabit, postquam iam aliquot numeri idonei pro A fuerint inventi, qui sint a, b, c, d, e etc., etiam omnia producta ex binis, scilicet ab, ac, bc etc., ibidem occurrere debere, cuius rei ratio est, quod producta ex pluribus numeris formae $ss + nuu$ semper ad eandem formam reducere licet.

19. Quod vero ad eos valores ipsius A attinet, qui oriuntur, si λ non fuerit unitas, seu qui tantum sint divisores formae $ss + nuu$, quorum multitudo videri posset indefinita, recurrere debemus ad theorema Illustris DE LA GRANGE, quo demonstravit omnes divisores numerorum formae $ss + nuu$ semper contineri in hac formula: $fpp \pm 2gpq + hqq$, exsistente $fh = gg + n$, neque has formulas ulterius continuari opus esse, quamdiu fuerit vel $2g < f$, vel $2g < h$, quarum formarum numerus semper est satis modicus. Hinc igitur semper pro A accipere licebit vel f vel h, nisi forte ad $4n$ non fuerint primi. Hoc enim casu pro A sumi conveniet vel numeros $f \pm 2g + h$, vel $4f \pm 4g + h$, vel $f \pm 4g + 4h$ etc., quatenus scilicet hi numeri fuerint primi ad $4n$. Simulac vero unicus talis valor fuerit repertus, is per eos, qui iam ante sunt inventi, multiplicatus dabit totidem novos valores idoneos pro A.

20. Hoc autem modo mox omnes valores idoneos pro A adipiscemur, cum eorum numerus semper aequetur semissi omnium numerorum minorum

quam $4n$ ad eumque primorum. Hinc si multitudo omnium istorum numerorum fuerit $= 2k$ (eum enim semper esse parem aliunde constat[1])), multitudo valorum litterae A semper erit $= k$, solo casu excepto, quo n est numerus quadratus negativus, quippe quo omnes plane hi numeri locum inveniunt; reliquis vero casibus omnibus multitudo numerorum exclusorum itidem erit $= k$, qui si designentur litteris graecis α, β, γ, δ etc., hi dabunt omnes valores litterae $\mathfrak{A}$ pro formula $4ni + \mathfrak{A}$, quae omnes continet numeros primos, qui nullo modo divisores esse possunt ullius numeri in forma $xx + nyy$ contenti.

21. Quod ad ipsos valores ipsius A attinet, qui oriuntur ex forma $fpp \pm 2gpq + hqq$, quia haec forma, sive per f sive per h multiplicetur, reducitur ad formam $xx + nyy$ ob $fh = gg + n$, his casibus erit sive $\lambda = f$, sive $\lambda = h$, ita ut tum pro numeris primis inde natis tam fP quam hP semper futurus sit numerus formae $xx + nyy$, ubi ergo sufficiet minorem horum duorum numerorum f et h accepisse, ita ut pronunciare liceat: quoties numerus primus P fuerit divisor cuiuspiam numeri formae $xx + nyy$, tum vel ipsum hunc numerum P, vel eius multiplum fP fore quoque numerum formae eiusdem $xx + nyy$.

22. Cum igitur formula $4ni + \mathfrak{A}$ certe omnes numeros contineat, qui nullo modo esse possunt divisores formae $xx + nyy$, necesse est, ut omnes numeri primi in forma $4ni + A$ contenti simul sint divisores cuiuspiam formae $xx + nyy$.

COROLLARIUM 1

23. Quod multitudo valorum litterae $\mathfrak{A}$ semper aequalis sit multitudini valorum ipsius A, quos ponimus a, b, c, d, e etc., inde patet, quod, si unicus innotuerit, veluti α, ad $\mathfrak{A}$ referendus, tum etiam omnia producta αa, αb, αc, αd etc. ad eandem classem pertinere, unde tamen unicum casum, quo $n = -mm$, excipi oportet, quoniam hoc casu nulli prorsus valores pro $\mathfrak{A}$ dantur.

---

1) Vide p. 170 huius voluminis. R. F.

COROLLARIUM 2

24. Quoniam pro quovis numero n forma divisorum GRANGIANA $fpp \pm 2gpq + hqq$ exiguam variationem recipit, quandoquidem ea semper ita reduci potest, ut $2g$ fiat minus quam f vel h, si valores isti minores designentur littera f, tum omnes divisores primi numerorum formae $xx + nyy$ vel ipsi erunt eiusdem formae, vel per f multiplicati, unde si f alios non habeat valores praeter unitatem, quod evenit casibus $n = 1$, $n = \pm 2$ et $n = \pm 3$, tum omnes divisores primi his casibus quoque ipsi habebunt eandem formam.

COROLLARIUM 3

25. Quoniam omnes valores pro littera A debent esse numeri impares, omnes formae $fpp \pm 2gpq + hqq$ hinc sunt excludendae, in quibus ambo numeri f et h pares. Quare cum sit $fh = gg + n$, numerum $gg + n$ ita in duos factores resolvi convenit, ut alter saltem evadat impar, unde si numerus $gg + n$ plures habeat divisores pares, plures resolutiones tanquam inutiles erunt reiiciendae.

SCHOLION 1

26. Quemadmodum valores litterae A pro forma $4ni + A$ sunt minores quam $4n$, ita si negativos introducere velimus, eos infra $2n$ deprimere licebit. Observavi autem porro pro omnibus casibus, quibus n est numerus positivus, multitudinem istorum valorum ipsius A ad semissem redigi posse, ita ut singuli non superent ipsum numerum n, si scilicet non ad formam $4ni$, sed ad eius dimidium tantum $2ni$ referantur. Hic autem duos casus probe a se invicem distingui oportet, prouti n vel in alterutra harum formularum: $4k$ et $4k - 1$, vel in alterutra harum: $4k + 1$ et $4k + 2$ continetur. Hoc enim posteriori casu singulis valoribus ipsius A signum ambiguum, sive $\pm$, sive $\mp$, praefigi debet, quorum signorum superiora valeant, quoties i fuerit numerus par, inferiora autem, quoties impar. Hoc igitur modo sequens tabula est constructa tres columnas complexa, quarum prima exhibet valores numeri n ordine naturali procedentes, secunda formulas pro divisoribus P, tertia vero indices littera f supra indicatos, quos ita interpretari decet, ut, quoties P fuerit numerus primus, eius productum per quempiam indicum f fiat numerus formae $xx + nyy$.

TABULA EXHIBENS OMNES DIVISORES PRIMOS PRO NUMERIS FORMAE $xx + nyy$, UNA CUM INDICIBUS f

Ubi circa signa ambigua est observandum superiora valere, quoties i numerus par, inferiora vero, quoties i numerus impar.

n	Divisores P	f
1	$2i \pm 1$	1
2	$4i \pm 1$	1
3	$6i + 1$	1
4	$8i + 1, -3$	1
5	$10i \pm 1, \pm 3$	1, 2
6	$12i \pm 1, \pm 5$	1, 2
7	$14i + 1, -3, -5$[1])	1
8	$16i + 1, +3, -5, -7$	1, 3
9	$18i \pm 1, \pm 5, \mp 7$	1, 2
10	$20i \pm 1, \mp 3, \pm 7, \pm 9$	1, 2
11	$22i + 1, +3, +5, -7, +9$	1, 3
12	$24i + 1, -5, +7, -11$	1, 3
13	$26i \pm 1, \mp 3, \mp 5, \pm 7, \pm 9, \pm 11$	1, 2
14	$28i \pm 1, \pm 3, \pm 5, \pm 9, \mp 11, \pm 13$	1, 2, 3
15	$30i + 1, -7, -11, -13$	1, 3
16	$32i + 1, -3, +5, -7, +9, -11, +13, -15$	1, 4
17	$34i \pm 1, \pm 3, \mp 5, \pm 7, \pm 9, \pm 11, \pm 13, \mp 15$	1, 2, 3
18	$36i \pm 1, \mp 5, \mp 7, \pm 11, \mp 13, \pm 17$	1, 2, 3
19	$38i + 1, -3, +5, +7, [+9,] +11, -13, -15, +17$	1, 4
20	$40i + 1, +3, +7, +9, -11, -13, -17, -19$	1, 3, 4
21	$42i \pm 1, \pm 5, \pm 11, \mp 13, \pm 17, \pm 19$	1, 2, 3, [5]
22	$44i \pm 1, \mp 3, \mp 5, \mp 7, \pm 9, \pm 13, \pm 15, \mp 17, \pm 19, \pm 21$	1, 2
23	$46i + 1, +3, -5, -7, +9, -11, +13, -15, -17, -19, -21$	1, 3
24	$48i + 1, +5, +7, +11, -13, -17, -19, -23$	1, 3, [4], 5
25	$50i \pm 1, \mp 3, \mp 7, \pm 9, \mp 11, \pm 13, \pm 17$[2]), $\mp 19, \pm 21, \mp 23$	1, 2

1) Editio princeps: + 5. Correxit A. M.

2) Editio princeps: ∓ 17. Correxit A. M.

n	Divisores P	f
26	$52i \pm 1, \pm 3, \pm 5, \pm 7, \pm 9, \mp 11, \pm 15, \pm 17, \mp 19, \pm 21, \mp 23, \pm 25$	1.2,3,[5]
27	$54i + 1, -5$[1]$), + 7, - 11, + 13, - 17, + 19$[2]$), - 23, + 25$	1, 4
28	$56i + 1, - 3, - 5, + 9, + 11, - 13, + 15, - 17, - 19, + 23, + 25, - 27$	1, 4
29	$58i \pm 1, \pm 3, \pm 5, \mp 7, \pm 9, \pm 11, \pm 13, \pm 15, \mp 17, \pm 19, \mp 21, \mp 23, \pm 25, \pm 27$	1, 2, 3, 5
30	$60i \pm 1, \mp 7, \pm 11, \pm 13, \pm 17, \mp 19, \pm 23, \pm 29$	1, 2, 3, 5
31	$62i + 1, - 3, + 5, + 7, + 9, - 11, - 13, - 15, - 17, + 19, - 21, - 23, + 25, - 27, - 29$	1, 5
32	$64i + 1, + 3, - 5, - 7, + 9, + 11, - 13, - 15, + 17, + 19, - 21, - 23, + 25, + 27, - 29, - 31$	1, 3, 4
33	$66i \pm 1, \mp 5, \pm 7, \mp 13, \pm 17, \pm 19, \pm 23, \pm 25, \pm 29, \mp 31$	1,2,3,[6]
34	$68i \pm 1, \mp 3, \pm 5, \pm 7, \pm 9, \mp 11, \mp 13, \mp 15, \pm 19, \mp 21, \pm 23, \pm 25, \mp 27, \pm 29, \pm 31, \pm 33$	1, 2, 5
35	$70i + 1, + 3, + 9, + 11, + 13, + 17, - 19, - 23, + 27, + 29, - 31, + 33$	1,[3,]4,5
36	$72i + 1, + 5, - 7, - 11, + 13, + 17, - 19, - 23, + 25, + 29, - 31, - 35$	1, 3, 4, 5
37	$74i \pm 1, \mp 3, \mp 5, \mp 7, \pm 9, \mp 11, \mp 13, \pm 15, \mp 17, \pm 19, \pm 21, \pm 23, \pm 25, \mp 27, \mp 29, \pm 31, \pm 33, \pm 35$	1, 2
38	$76i \pm 1, \pm 3, \mp 5, \pm 7, \pm 9, \mp 11, \pm 13, \mp 15, \pm 17, \pm 21, \pm 23, \pm 25, \pm 27, \pm 29, \mp 31, \mp 33, \mp 35$[3]$)$	1, 2, 3, 6
39	$78i + 1, + 5, - 7, + 11, - 17, - 19, - 23, + 25, - 29, - 31, - 35, - 37$	1, 3, 5
40	$80i + 1, - 3, + 7, + 9, + 11, + 13, - 17, + 19, - 21, + 23, - 27, - 29, - 31, - 33, + 37, - 39$	1, 4, 5, 7
41	$82i \pm 1, \pm 3, \pm 5, \pm 7, \pm 9, \pm 11, \mp 13, \pm 15, \mp 17, \pm 19, \pm 21, \mp 23, \pm 25, \pm 27, \mp 29, \mp 31, \pm 33, \pm 35, \pm 37, \mp 39$	1,2,3,5,6

1) Editio princeps: + 5. Correxit A. M.
2) Editio princeps: — 13, + 17, — 19. Correxit A. M.
3) Editio princeps: ∓ 37. Correxit A. M.

n	Divisores P	f
42	$84i \pm 1, \mp 5, \mp 11, \pm 13, \pm 17, \mp 19, \pm 23, \pm 25, \pm 29, \pm 31, \mp 37, \pm 41$	1, 2, 3, 6
43	$86i + 1, -3, -5, -7, +9, +11, +13, +15, +17, -19, +21, +23, +25, -27, -29, +31, -33, +35, -37, -39, +41$	1, 4
44	$88i + 1, +3, +5, -7, +9, -13, +15, -17, -19, -21, +23, +25, +27, -29, +31, -35, +37, -39, -41, -43$	1, 3, 4, 5
45	$90i \pm 1, \pm 7, \mp 11, \mp 13, \mp 17, \mp 19, \pm 23, \pm 29, \mp 31, \mp 37, \pm 41, \pm 43$	1,2,3,5,7
46	$92i \pm 1, \mp 3, \pm 5, \mp 7, \pm 9, \pm 11, \mp 13, \mp 15, \mp 17, \pm 19, \pm 21, \pm 25, \mp 27, \mp 29, \pm 31, \mp 33, \mp 35, \pm 37, \pm 39, \pm 41, \pm 43, \pm 45$	1, 2, 5
47	$94i + 1, +3, -5, +7, +9, -11, -13, -15, +17, -19, +21, -23, +25, +27, -29, -31, -33, -35, +37, -39, -41, -43, -45$	1, 3, 7
48	$96i + 1, -5, +7, -11, +13, -17, +19, -23, +25, -29, +31, -35, +37, -41, +43, -47$	1, 3, 4, 7
49	$98i \pm 1, \mp 3, \pm 5, \pm 9, \mp 11, \pm 13, \mp 15, \pm 17, \mp 19, \mp 23, \pm 25, \mp 27, \pm 29, \mp 31, \pm 33, \pm 37, \mp 39, \pm 41, \mp 43, \pm 45, \mp 47$	1, 2, 5
50	$100i \pm 1, \pm 3, \mp 7, \pm 9, \pm 11, \mp 13, \pm 17, \pm 19, \mp 21, \mp 23, \pm 27, \mp 29, \mp 31, \pm 33, \mp 37, \mp 39, \pm 41, \pm 43, \mp 47, \pm 49$	1, 2, 3, 6

SCHOLION 2

27. Haec tabula facili negotio, quousque libuerit, continuari potest. Proposito enim quocunque numero n, pro formula $2ni + A$ quaerantur primo omnes numeri primi minores quam n simulque ad n primi, quibus signum $+$ tribuatur, si n fuerit formae vel $4k$ vel $4k-1$; casibus autem, quibus n est formae $4k+1$ vel $4k+2$, praefigendum est signum ambiguum $\pm$; reliquis vero numeris primis praefigatur sive signum $-$ sive ambiguum $\mp$. Quodsi n divisores habeat impares, eos omnes ex valoribus ipsius A excludi oportet, reliqui vero numeri primi desumantur ex divi-

soribus numerorum in hac formula $n + xx$ contentorum, dum loco x successive scribuntur ordine numeri 1, 2, 3, 4, 5 etc., quos autem non ultra $\frac{1}{2}n$ continuare opus est. Si enim p denotet maximum numerum primum minorem quam n, nisi is fuerit divisor formae $n + xx$, sumto $x < \frac{1}{2}p$, tum certe non erit divisor, quantumvis magni numeri scribantur. Hoc ergo modo facile omnes numeri loco A scribendi deteguntur, quibus inventis numeri compositi facile ex ipsa compositione colliguntur, dum signum cuiusque producti ex signis factorum more solito formatur. Totam hanc operationem operae pretium erit aliquot exemplis declarare. Sit igitur primo $n = 40$, ideoque formae $4k$, unde omnes valores A signis simplicibus afficientur. Quia iam 37 est maximus numerus primus infra 40, sufficiet numeros x usque ad 18 continuasse. Hos ergo valores formae $40 + xx$ hic una cum singulis divisoribus primis infra 40, praeter 5, apponamus:

$n + xx$	Divisores	$n + xx$	Divisores
41	—	140	7
44	11	161	7, 23
49	7	184	23
56	7	209	11, 19
65	13	236	—
76	19	265	—
89	—	296	37
104	13	329	7
121	11	364	7, 13

Hinc ergo numeri primi signo + afficiendi sunt $+1$, $+7$, $+11$, $+13$, $+19$, $+23$, $+37$, reliqui vero numeri primi minores quam 40 habebunt signum —, eruntque -3, -17, -29, -31, atque ex his numeri compositi erunt $+9$, -21, -27, -33, -39, quocirca formula pro divisoribus primis P erit sequens:

$$80i + 1, \ -3, \ +7, \ +9, \ +11, \ +13, \ -17, \ +19, \ -21,$$
$$+23, \ -27, \ -29, \ -31, \ -33, \ +37, \ -39.$$

Pro altero exemplo sumatur $n = 41$, qui numerus cum sit formae $4k + 1$, signa ambigua erunt adhibenda. Quaerantur igitur primo omnes divisores

primi numerorum formae $41 + xx$, quos non ultra $x = 18$ continuare est opus, quia maximus numerus primus infra 41 est 37, cuius dimidium est 18; haec ergo operatio ut ante instituatur[1]).

$n + xx$	Divisores	$n + xx$	Divisores
42	3, 7	141	3, —
45	3, 5	162	3
50	5	185	5, 37
57	3, 19	210	3, 5, 7
66	3, 11	237	3, —
77	7, 11	266	7, 19
90	3, 5	297	3, 11
105	3, 5, 7	330	3, 5, 11
122	—	365	5, —

Numeri ergo primi signo $\pm$ afficiendi sunt ± 1, ± 3, ± 5, ± 7, ± 11, ± 19, ± 37, reliqui vero signo $\mp$ afficiendi sunt ∓ 13, ∓ 17, ∓ 23, ∓ 29, ∓ 31, unde numeri compositi colliguntur ± 9, ± 15, ± 21, ± 25, ± 27, ± 33, ± 35, ∓ 39, quare formula pro divisoribus primis P ita se habebit:

$$82i \pm 1, \pm 3, \pm 5, \pm 7, \pm 9, \pm 11, \mp 13, \pm 15, \mp 17, \pm 19, \pm 21, \mp 23, \pm 25, \pm 27, \mp 29, \mp 31, \pm 33, \pm 35, \pm 37, \mp 39.$$

SCHOLION 3

28. Quod ad indices f pro quovis numero n attinet, forma generalis, quam Illustris DE LA GRANGE pro divisoribus formae $xx + nyy$ dedit, considerari debet, quae erat $fpp + 2gpq + hqq$, exsistente $fh = n + gg$, ubi notetur plures huiusmodi formulas quovis casu non opus esse formari, quam ubi $2g$ non excedit f; praeterea autem hic pro f sumimus minorem factorem formulae $n + gg$; tum vero necesse est, ut alter numerorum f et h sit par, hocque pacto facile erit omnes indices f assignare. Ita pro priori exemplo

1) Vide C. F. GAUSS: *Disquisitiones arithmeticae*, Lipsiae 1801, art. 151; *C. F. GAUSS Werke* I, p. 117. In hoc loco Gauss demonstrationem Euleri non esse rigorosam observat. R. F.

supra allato, ubi $n = 40$, sumatur primo $g = 0$, eritque $fh = 40 = 5 \cdot 8$, sicque erit $f = 5$; deinde sumto $g = 1$ fiet $fh = 41$, ideoque $f = 1$; sumto porro $g = 2$ erit $fh = 44$, ideoque $f = 4$; sumto autem $g = 3$, ob $fh = 49$ esse poterit $f = 7$, unde omnes valores ipsius f erunt 1, 4, 5, 7. Pro altero exemplo, quo $n = 41$, valor $g = 0$ tantum dat $f = 1$; valor $g = 1$ praebet $fh = 42$, hincque vel $f = 2$, vel $f = 3$, vel $f = 6$; porro valor $g = 2$ praebet $fh = 45$, unde colligitur $f = 5$; denique valor $g = 3$ dat $fh = 50$, unde iterum sequitur $f = 5$, sicque omnes valores pro f sunt 1, 2, 3, 5, 6. Hinc ergo colligimus, quoties pro formula $xx + 41yy$ prodeat P numerus primus, tum semper fore vel P, vel $2P$, vel $3P$, vel $5P$, vel $6P$, certum numerum formae $xx + 41yy$. Veluti sumto $i = 1$, quia est $82 - 3 = 79$, ideoque numerus primus, statim patet hunc ipsum numerum 79 in forma $xx + 41yy$ non contineri, neque etiam eius duplum 158; at eius triplum 237 est $14^2 + 41 \cdot 1^2$. Simili modo pro P etiam reperitur numerus primus 73, qui neque ipse, neque eius duplum, neque triplum in proposita forma continetur, at vero eius quintuplum 365 est $= 18^2 + 41 \cdot 1^2$.

PROBLEMA

Si n fuerit numerus negativus, puta $n = -m$, invenire formulam generalem pro omnibus numeris primis, qui exsistere possunt divisores cuiuspiam numeri formae $xx - myy$, vel etiam formae $myy - xx$.

SOLUTIO

29. Solutio huius problematis instituatur uti praecedentis, scribendo scilicet $-m$ loco n, tum vero, si P denotet divisorem primum formulae propositae, quoniam is necessario esse debet positivus, etiam numerum i negativum accipi convenit, unde formula supra inventa evadet

$$P = 4mi + \frac{ss - muu}{\lambda},$$

vel etiam

$$P = 4mi - \frac{ss - muu}{\lambda},$$

ex quo manifestum est omnes numeros primo membro $4mi$ adiungendos tam positive quam negative accipi posse, ita ut generatim habeamus $P = 4mi \pm A$, ubi A denotat omnes divisores, sive formulae $ss - m$, sive formulae $m - ss$, qui quidem ad $4m$ sint primi, unde ex his divisoribus excluduntur primo omnes numeri pares, deinde etiam ii impares, qui cum numero m communem involvunt divisorem.

30. Quodsi multitudo omnium numerorum ad $4m$ primorum eoque minorum sit $= 4k$, numerus valorum ipsius A tantum erit $= k$, qui autem ob signa ambigua censendus est $= 2k$, ita ut numerus exclusorum itidem sit $= 2k$. Hoc observato, si a fuerit divisor formae $m - ss$, vel $ss - m$, tum, quoties $4mi \pm a$ fuerit numerus primus, is semper erit divisor numeri cuiuspiam formae propositae; contra autem, si α fuerit numerus hinc exclusus, tum certe affirmare licet nullum numerum formae $4mi \pm \alpha$ unquam divisorem esse posse formae propositae.

31. Ex theoremate autem Illustris DE LA GRANGE omnes divisores formae propositae continentur in hac formula generali: $fpp \pm 2gpq - hgg$, exsistente $fh = m - gg$, quas autem formulas eo usque tantum continuare opus est, donec $2g$ superet f; semper enim nobis denotet f minorem binorum factorum, in quos numerus $m - gg$ resolvitur. Praeterea vero, ut casu praecedente, alter numerorum f et h sumi debet impar; unde intelligitur pro quovis casu multitudinem valorum ipsius f satis fore modicam, quibus inventis omnes divisores primi P vel ipsi vel per quempiam valorem ipsius f multiplicati in forma proposita continebuntur, idque non unico modo, uti casu praecedente usu venit, sed infinitis adeo modis.

32. Hinc autem merito excludimus casus, quibus m est numerus quadratus, quia tum omnes plane numeri primi, nullo excluso, evadere possunt divisores formae propositae, id quod etiam inde patet, quod pro A sumi debent omnes divisores formulae $ss - m$; hinc enim, si fuerit $m = ll$ et capiatur $s = l$, haec formula fit 0, at vero ciphra per omnes plane numeros est divisibilis.

COROLLARIUM 1

33. Quodsi ergo a fuerit divisor cuiuspiam numeri formae $xx - myy$, tum omnes numeri primi tam in hac forma $4mi + a$, quam in hac $4mi - a$, certe erunt divisores cuiuspiam numeri formae propositae; tum vero etiam vel ipsi vel per quempiam valorem ipsius f multiplicati in eadem forma continebuntur.

COROLLARIUM 2

34. Quoniam omnes valores ipsius A tam positive quam negative accipiuntur, eos non ultra terminum $2m$ continuari necesse est, ideoque si numeri $m - ss$, vel $ss - m$, ordine scribantur, valores litterae s non ultra $\frac{1}{2}p$ continuare opus est, siquidem p denotet maximum numerum primum minorem quam $2m$.

COROLLARIUM 3

35. Cum valores producti fh sint m, $m-1$, $m-4$, $m-9$, $m-16$, $m-25$ etc., qui ab initio decrescunt, si ex quopiam maiore sumatur fh, in minoribus vero occurrant sive fk, sive kk, ita ut k sit $< f$, tum in indices loco f referri debet k; unde si fuerit $k = 1$, multitudo indicum hinc non augebitur; si enim fuerit fP formae $xx - myy$, sive $myy - xx$, tum etiam semper hP eandem habebit formam, ideoque etiam kP eandem formam habebit.

SCHOLION 1

36. Postquam omnes numeri primi ipso $4m$ minores simulque ad eum primi fuerint notati, qui sint a, b, c, d etc., reliqui etiam notentur, qui sint α, β, γ, δ etc., et numeri compositi vel erunt producta ex numeris a, b, c, d etc., vel producta ex binis exclusorum α, β, γ, δ etc. Quodsi ergo P denotet omnes divisores primos numerorum formae $xx - myy$, sumamus Π pro denotandis numeris inde exclusis, erit

$$P = 4mi \pm (a, b, c, d, e \text{ etc.}),$$
$$\Pi = 4mi \pm (\alpha, \beta, \gamma, \delta, \varepsilon \text{ etc.}),$$

unde pro quovis numero m istae binae formulae facile construentur; semper autem ambae pari terminorum numero constabunt. Veluti si fuerit $m = 21$, ita ut ex divisoribus excludi debeant numeri 3 et 7 cum suis multiplis, evolvantur numeri ex forma $21 - ss$ oriundi, nullo respectu habito sive sint positivi sive negativi, et pro quovis notentur divisores primi, praeter 3 et 7, non superantes $2m = 42$, quae operatio hoc modo instituatur.

$21 - ss$	Divisores	$21 - ss$	Divisores
21	—	79	—
20	5	100	5
17	17	123	41
12	—	148	37
5	5	175	5
4	—	204	17
15	5	235	—
28	—	268	—
43	—	303	—
60	5	340	17, 5

Hinc ergo valores pro litteris a, b, c, d sunt 5, 17, 37, 41, exclusi vero, litteris α, β, γ, δ etc. denotati, sunt 11, 13, 19, 23, 29, 31; ad illos igitur accedit compositus 25, ita ut ambae nostrae formulae futurae sint

$$P = 84i \pm (1, 5, 17, 25, 37, 41),$$
$$\Pi = 84i \pm (11, 13, 19, 23, 29, 31).$$

Sicque utraque forma eodem terminorum numero constat, id quod semper fieri necesse est. Pro productis autem fh, prouti ex terminis decrescentibus oriuntur, habebimus sequentia: $3 \cdot 7$, $4 \cdot 5$, $3 \cdot 4$, $1 \cdot 5$, $1 \cdot 4$, ex quorum minimis 5 et 4 patet unitatem tantum inter indices esse referendam. Hinc ex $3 \cdot 4$ etiam 3 ad unitatem reducitur, unde concluditur unicum dari indicem 1. Hic conveniebat etiam formulas afferre pro numeris, qui nullo modo divisores esse possunt, quas in superiori tabula superfluum fuisset adiungere, quoniam si in formulis pro P datis singula signa in contraria mutentur, tum eae praebebunt omnes numeros Π.

TABULA EXHIBENS OMNES DIVISORES PRIMOS PRO NUMERIS FORMAE VEL $xx - myy$ VEL $myy - xx$, UNA CUM INDICIBUS f

Ubi perpetuo signa ambigua simul locum inveniunt.

m	P et Π	f
2	$8i \pm 1$	1
	$8i \pm 3$	
3	$12i \pm 1$	1
	$12i \pm 5$	
5	$20i \pm (1, 9)$	1
	$20i \pm (3, 7)$	
6	$24i \pm (1, 5)$	1
	$24i \pm (7, 11)$	
7	$28i \pm (1, 3, 9)$	1
	$28i \pm (5, 11, 13)$	
8	$32i \pm (1, 7, 9, 15)$	1
	$32i \pm (3, 5, 11, 13)$	
10	$40i \pm (1, 3, 9, 13)$	1, 2
	$40i \pm (7, 11, 17, 19)$	
11	$44i \pm (1, 5, 7, 9, 19)$	1
	$44i \pm (3, 13, 15$[1]$), 17, 21)$	
12	$48i \pm (1, 11, 13, 23)$	1
	$48i \pm (5, 7, 17, 19)$	
13	$52i \pm (1, 3, 9, 17, 23, 25)$	1
	$52i \pm (5, 7, 11, 15, 19, 21)$	
14	$56i \pm (1, 5, 9, 11, 13, 25)$	1
	$56i \pm (3, 15, 17, 19, 23, 27)$	
15	$60i \pm (1, 7, 11, 17)$	1, 2
	$60i \pm (13, 19, 23, 29)$	
17	$68i \pm (1, 9, 13, 15, 19, 21, 25, 33)$	1
	$68i \pm (3, 5, 7, 11, 23, 27, 29, 31)$	
18	$72i \pm (1, 7, 17, 23, 25, 31)$	1
	$72i \pm (5, 11, 13, 19, 25, 35)$	
19	$76i \pm (1, 3, 5, 9, 15, 17, 25, 27, 31)$	1
	$76i \pm (7, 11, 13, 21, 23, 29, 33, 35, 37)$	

1) Editio princeps: 11, 13. Correxit R. F.

m	P et Π	f
20	$80i \pm (1, 9, 11, 19, 21, 29, 31, 39)$	1
	$80i \pm (3, 7, 13, 17, 23, 27, 33, 37)$	
21	$84i \pm (1, 5, 17, 25, 37, 41)$	1
	$84i \pm (11, 13, 19, 23, 29, 31)$	
22	$88i \pm (1, 3, 7, 9, 13, 21, 25, 27, 29, 39)$	1
	$88i \pm (5, 15, 17, 19, 23, 31, 35, 37, 41, 43)$	
23	$92i \pm (1, 7, 9, 11, 13, 15, 19, 25, 29, 41, 43)$	1
	$92i \pm (3, 5, 17, 21, 27, 31, 33, 35, 37, 39, 45)$	
24	$96i \pm (1, 5, 19, 23, 25, 29, 43, 47)$	1
	$96i \pm (7, 11, 13, 17, 31, 35, 37, 41)$	

SCHOLION 2

37. Manifestum hic est formulas P et Π pro casu $m = 24$ non differre ab iis, quae pro casu $m = 6$ sunt datae, quemadmodum rei natura postulat, quoniam forma $xx - 6yy$ redigitur ad formam $xx - 24yy$, dum in priore loco y scribitur $2y$, quae convenientia in genere locum habere debet, si numerus m per 4 aliumve numerum quadratum multiplicetur. Eadem quoque harmonia reperitur in formulis prioris problematis; interim tamen discrimen intercedere potest ratione indicum f, quam ob caussam tales casus a se invicem distinximus. His igitur expeditis coronidis loco subiungam duo theoremata, quibus in casibus prioris problematis formulae P ad membrum $2ni$ sunt reductae, et quorum veritatem ex hactenus traditis haud difficulter cognoscere licebit.

THEOREMA 3

38. *Si fuerit* $n = 4k + 1$, *vel* $n = 4k + 2$, *quoties fuerit* $4ni + 2n - 1$[1]) *numerus primus, is erit divisor formae* $xx + nyy$.

THEOREMA 4

39. *Si fuerit vel* $n = 4k$, *vel* $n = 4k - 1$, *tum, quoties fuerit* $4ni - 2n + 1$ *numerus primus, is erit divisor formae* $xx + nyy$.

1) Editio princeps: $4ni + 2n + 1$. Correxit A. M.

DE SINGULARI GENERE QUAESTIONUM DIOPHANTEARUM ET METHODO MAXIME RECONDITA EAS RESOLVENDI

Commentatio 683 indicis Enestroemiani
Nova acta academiae scientiarum Petropolitanae 9 (1791), 1795, p. 3—18
Summarium ibidem p. 165
Conventui exhibita die 13. januarii 1777

SUMMARIUM

Sachant que toutes les puissances des nombres de la forme $aa + nbb$ sont toujours des nombres d'une forme semblable $xx + nyy$, il se présente ici un nouveau genre de questions indéterminées, pour la résolution desquelles l'Analyse de Diophante n'offre aucun secours, savoir: d'assigner de toutes ces puissances des nombres de la forme $aa + nbb$ celles, dans lesquelles ou x ou y obtienne la plus petite valeur? C'est de ce problème qu'on trouve la solution dans le mémoire présent; et cette solution est d'autant plus remarquable, qu'elle est fondée uniquement sur la considération des facteurs imaginaires du binome $aa + nbb$ et sur des calculs purement trigonométriques. Cette courte notice suffira pour inspirer aux amateurs de recherches de cette nature la curiosité de lire le mémoire même.

1. Notum est omnes potestates numerorum huius formae $aa + nbb$ semper esse similis formae, scilicet $xx + nyy$; unde si proponatur numerus $N = aa + nbb$, eius potestas quaecunque N^λ semper exprimi poterit per talem formulam:

$$N^\lambda = xx + nyy,$$

ubi pro singulis potestatibus numeri N tam x quam y certos valores sortientur. Erit enim

$$N^2 = (aa - nbb)^2 + n(2ab)^2,$$
$$N^3 = (a^3 - 3naabb)^2 + n(3aab - nb^3)^2,$$
$$N^4 = (a^4 - 6naabb + nnb^4)^2 + n(4a^3b - 4nab^3)^2,$$

unde lex progressionis iam satis elucet et facile potestates, quousque lubuerit, continuari poterunt, ope huius Lemmatis, quod, si fuerit

$$N = aa + nbb \quad \text{et} \quad M = cc + ndd,$$

semper sit

$$MN = (ac - nbd)^2 + n(ad + bc)^2.$$

2. Cum igitur, si fuerit $N = aa + nbb$, omnes eius potestates eandem habeant formam, ita ut sit $N^\lambda = xx + nyy$, novum genus quaestionum, quas hic tractare institui, in hoc consistit, ut eae potestates ipsius N investigentur, in quibus vel numerus x vel y evadat minimus, seu ipsi unitati aequalis. Quoniam enim hi numeri nunquam evanescunt, in integris etiam minorem valorem quam 1 recipere non poterunt; manifestum autem est in methodo DIOPHANTEA nullam reperiri viam huiusmodi quaestiones resolvendi.

3. Quo indoles huiusmodi quaestionum clarius percipiatur, consideremus omnes potestates binarii, quae semper in hac forma $xx + 7yy$ contineri deprehenduntur, si modo pro prima et secunda potestate etiam fractiones admittantur, si quidem habebitur

$$2 = \left(\frac{1}{2}\right)^2 + 7\left(\frac{1}{2}\right)^2 \quad \text{et} \quad 4 = \left(\frac{3}{2}\right)^2 + 7\left(\frac{1}{2}\right)^2;$$

altiores vero potestates omnes in integris tali forma exhiberi possunt, quemadmodum ex sequentibus exemplis elucet:

$$\begin{aligned}
2^3 &= 8 = (1)^2 + 7(1)^2, \text{ ergo } x = 1 \text{ et } y = 1,\\
2^4 &= 16 = (3)^2 + 7(1)^2, \text{ ergo } x = 3 \text{ et } y = 1,\\
2^5 &= 32 = (5)^2 + 7(1)^2, \text{ ergo } x = 5 \text{ et } y = 1,\\
2^6 &= 64 = (1)^2 + 7(3)^2, \text{ ergo } x = 1 \text{ et } y = 3,\\
2^7 &= 128 = (11)^2 + 7(1)^2, \text{ ergo } x = 11 \text{ et } y = 1,\\
2^8 &= 256 = (9)^2 + 7(5)^2, \text{ ergo } x = 9 \text{ et } y = 5,\\
2^9 &= 512 = (13)^2 + 7(7)^2, \text{ ergo } x = 13 \text{ et } y = 7,\\
2^{10} &= 1024 = (31)^2 + 7(3)^2, \text{ ergo } x = 31 \text{ et } y = 3.
\end{aligned}$$

Ubi imprimis moneri oportet in his resolutionibus pro x et y alios numeros non esse admittendos, nisi qui inter se sint primi, si quidem numeri compositi nulla difficultate laborant; namque si in genere fuerit $N^\lambda = xx + nyy$, erit quoque

$$N^{\lambda+2} = (Nx)^2 + n(Ny)^2;$$

hanc ob causam hic perpetuo numeros x et y inter se primos assumi conveniet.

4. Quodsi ergo in casu allato $2^\lambda = xx + 7yy$ quantitas y debeat esse minima, ea manifesto unitati debet esse aequalis, ideoque quaestio huc reducitur, quinam numeri pro x accipi queant, ut formula $xx + 7$ exhibeat potestatem binarii. Ex exemplis autem superioribus patet id fieri casibus $x = 3$, $x = 5$, $x = 11$, dehinc autem alius casus non occurrit usque ad $x = 181$, hinc enim prodit $(181)^2 + 7 = 2^{15}$, sicque requiritur methodus hos casus a priori investigendi. His praemissis vis sequentis problematis haud difficulter perspicietur.

PROBLEMA GENERALE

Si fuerit $N = aa + nbb$, eas investigare potestates ipsius N, quibus fiat $N^\lambda = xx + n$, quo casu utique valor ipsius y in formula generali $xx + nyy$ evadit omnium minimus.

SOLUTIO

5. Hic plurimum iuvabit formulam $aa + nbb$ in suos factores imaginarios resolvisse, quippe quae resolutio iam summum usum in Analysi praestitit[1]); erit igitur

$$N = (a + b\sqrt{-n})\,(a - b\sqrt{-n}),$$

unde quaelibet potestas in genere hoc modo exprimetur:

$$N^\lambda = (a + b\sqrt{-n})^\lambda\,(a - b\sqrt{-n})^\lambda.$$

Talium autem formularum potestates semper simili ratione exprimuntur, unde si fuerit

1) Numerus n positivus esse oportet. R. F.

$$(a + b\sqrt{-n})^\lambda = A + B\sqrt{-n},$$

erit

$$(a - b\sqrt{-n})^\lambda = A - B\sqrt{-n},$$

hincque facta multiplicatione habebitur $N^\lambda = A^2 + nB^2$; sicque quaestio huc redit, quibusnam casibus valor litterae B unitati evadat aequalis; quodsi forte fieri nequeat, ii saltem casus quaerantur, quibus littera B minimum accipiet valorem.

6. Quo autem hoc minimum litterae B perscrutari queamus, recurramus ad formulam notissimam imaginariorum, cui universa theoria angulorum plerumque innititur, scilicet $\cos.\Phi + \sqrt{-1}\sin.\Phi$, quippe cuius omnes potestates simili modo exprimi possunt, cum sit:

$$(\cos.\Phi + \sqrt{-1}\sin.\Phi)^\lambda = \cos.\lambda\Phi + \sqrt{-1}\sin.\lambda\Phi.$$

Hunc in finem statuamus:

$$a + b\sqrt{-n} = p(\cos.\Phi + \sqrt{-1}\sin.\Phi),$$

atque esse oportebit $a = p\cos.\Phi$, $b\sqrt{n} = p\sin.\Phi$, unde colligitur $\text{tang.}\Phi = \frac{b\sqrt{n}}{a}$, hincque porro:

$$\sin.\Phi = \frac{b\sqrt{n}}{\sqrt{(aa + nbb)}} \quad \text{et} \quad \cos.\Phi = \frac{a}{\sqrt{(aa + nbb)}}.$$

Invento autem angulo Φ factor ille realis p colligitur fore

$$p = \sqrt{(aa + nbb)}.$$

Quare cum sit $N = aa + nbb$, quaeratur angulus Φ, ut sit $\text{tang.}\Phi = \frac{b\sqrt{n}}{a}$, sive

$$\sin.\Phi = \frac{b\sqrt{n}}{\sqrt{N}} \quad \text{et} \quad \cos.\Phi = \frac{a}{\sqrt{N}};$$

et quia tum erit $p = \sqrt{N}$, ista transformatio nobis praebet

$$(a + b\sqrt{-n}) = \sqrt{N}\,(\cos.\Phi + \sqrt{-1}\,\sin.\Phi),$$

ideoque etiam

$$a - b\sqrt{-n} = \sqrt{N}\,(\cos.\Phi - \sqrt{-1}\,\sin.\Phi).$$

7. His iam formulis introductis erit potestas quaecunque ipsius N, scilicet:

$$N^\lambda = \overset{\lambda}{N^{\frac{}{2}}}\,(\cos.\lambda\Phi + \sqrt{-1}\,\sin.\lambda\Phi) \cdot \overset{\lambda}{N^{\frac{}{2}}}\,(\cos.\lambda\Phi - \sqrt{-1}\,\sin.\lambda\Phi),$$

unde facta evolutione prodit aequatio identica $N^\lambda = N^\lambda$. At vero si ponamus, uti fecimus, $N^\lambda = (A + B\sqrt{-n})\,(A - B\sqrt{-n})$, litterae A et B ita definientur, ut sit

$$A = \overset{\lambda}{N^{\frac{}{2}}}\cos.\lambda\Phi \quad \text{et} \quad B = \frac{\overset{\lambda}{N^{\frac{}{2}}}\sin.\lambda\Phi}{\sqrt{n}},$$

hincque erit $N^\lambda = A^2 + nB^2$.

8. Cum igitur ii casus quaerantur, quibus littera B minimum sortitur valorem, quaestio huc redit, ut pro λ ii investigentur numeri integri, quibus haec formula $\frac{\overset{\lambda}{N^{\frac{}{2}}}\sin.\lambda\Phi}{\sqrt{n}}$ minimum adipiscatur valorem, quod manifesto eveniet, si sin. $\lambda\Phi$ minimum valorem accipiet, quod utique eveniret, si angulus $\lambda\Phi$ fieret vel π, vel 2π, vel 3π, vel 4π etc., vel in genere $i\pi$ denotante i numerum quemcunque integrum, π vero angulum duobus rectis aequalem, tum enim adeo prodiret sin. $\lambda\Phi = 0$, ideoque etiam $B = 0$. Quoniam autem plerumque angulus Φ cum peripheria circuli est incommensurabilis, fieri nequit, ut evadat $\lambda\Phi = i\pi$. In eos igitur casus inquirere debemus, quibus angulus $\lambda\Phi$ quam minime discrepet ab $i\pi$. Quodsi enim fuerit $\lambda\Phi = i\pi + \omega$, denotante ω angulum valde parvum, tum utique erit sin. $\lambda\Phi = \pm$ sin. ω. His ergo casibus formula nostra $B = \frac{\overset{\lambda}{N^{\frac{}{2}}}\sin.\lambda\Phi}{\sqrt{n}}$ utique eo minorem accipiet valorem, quo minor fuerit angulus ω; ubi quidem probe perpendi oportet, quando λ fuerit numerus satis magnus, tum valorem litterae B unitatem excedere posse, etiamsi angulus

ω fuerit quam minimus. Interim tamen perspicuum est hac methodo omnes valores exponentis λ prodire debere, quibus littera B minimos adipiscitur valores, etiamsi non omnes sint $= 1$, simul vero hoc modo omnes casus, quibus sit $B = 1$, certe reperiri debere.

9. Cum igitur proxime esse oporteat $\lambda\Phi = i\pi$, proxime quoque erit $\frac{\lambda}{i} = \frac{\pi}{\Phi}$. Quamobrem si methodo iam satis nota omnes fractiones quaerantur, quae proxime accedant ad fractionem $\frac{\pi}{\Phi}$, harum fractionum numeratores dabunt valores exponentis λ, denominatores vero ipsius i; et quo accuratius istae fractiones cum fractione $\frac{\pi}{\Phi}$ convenient, eo minores valores pro littera B resultabunt, quorum omnium minimi erunt ii, quibus fit $B = 1$.

EXEMPLUM 1

10. Evolvamus secundum haec praecepta casum, quo $a = 1$, $b = 1$ et $n = 2$, ita ut numerus noster propositus sit $N = 3$, atque $3^\lambda = A^2 + 2B^2$, sicque eae potestates ternarii investigari debeant, quibus fiat $3^\lambda = A^2 + 2$, quod evenit casu $B = 1$. Praeterea vero simul eos casus investigemus, quibus B fit numerus satis parvus, veluti 2 vel 4 vel 5 etc., propterea quod casus $B = 3$ hinc excluduntur. Hic quidem statim isti casus se offerunt: $3^1 = (1)^2 + 2$, $3^3 = (5)^2 + 2$; unde quaeritur, an tales casus etiam in maioribus potestatibus existant.

11. Cum igitur sit $a = 1$, $b = 1$ et $n = 2$, quaeri oportet angulum Φ, ut sit tang. $\Phi = \sqrt{2}$ ideoque l tang. $\Phi = 10{,}1505150$, unde colligitur $\Phi = 54^0\ 44'\ 8''{,}19$, quem angulum in minuta secunda convertamus, quo facilius eum cum π comparare queamus, eritque $\Phi = 197048''{,}19$. Quare cum sit $\pi = 648000''$, erit fractio nostra resolvenda $\frac{\pi}{\Phi} = \frac{64800000}{19704819}$, cuius numerator per denominatorem dividatur, tum vero residuum dabit divisorem pro sequente divisione, in qua praecedens divisor fiet dividendus, hocque modo eaedem operationes instituantur, quibus vulgo maximus communis divisor quaeri solet, ubi imprimis quoti ex singulis divisionibus oriundi sollicite notentur:

5685543	19704819	64800000	3
	17056629	59114457	3
389163	2648190	5685543	2
	2334978	5296380	6
75951	313212	389163	1
	303804	313212	4
687	9408	75951	8
	8931	75264	13
210	477	687	1
	420	477	2
39	57	210	3
	39	171	1
3	18	39	2
	18	36	6
	0	3	

12. Iam ex his quotis ordine dispositis formentur more solito fractiones, dum continuo tam numeratores quam denominatores per indices suprascriptos multiplicantur et praecedentes adduntur, prouti hic videre licet:

$$\begin{array}{cccccccccc} 3; & 3; & 2; & 6; & 1; & 4; & 8; & 13; & 1; \\ \frac{1}{0}; & \frac{3}{1}; & \frac{10}{3}; & \frac{23}{7}; & \frac{148}{45}; & \frac{171}{52}; & \frac{832}{253}; & \frac{6827}{2076}; & \frac{89583}{27241}. \end{array}$$

Hae enim fractiones continuo propius ad ipsam fractionem propositam $\frac{\pi}{\Phi}$ accedent; ubi imprimis notari oportet, quod eae fractiones, quae maioribus indicibus respondent, caeteris paribus quam minime a veritate aberrent. Has igitur fractiones, quousque licuerit, percurramus. Prima quidem $\frac{1}{0}$ statim dat $\lambda = 1$, unde fit $3^1 = (1)^2 + 2$. Secunda fractio $\frac{3}{1}$ praebet $\lambda = 3$, unde fit $3^3 = 5^2 + 2$, quae ergo, aeque ac prima, exacte quaesito satisfacit, propterea quod indices 3 et 3 iam satis sunt notabiles. Ex tertia vero fractione $\frac{10}{3}$ oritur $\lambda = 10$, eritque $3^{10} = 59049 = A^2 + 2B^2$, ubi foret $B = 0$ et $A = 243$, quam resolutionem autem hic reiicimus. At vero mox patet esse $59049 = (241)^2 + 2(22)^2$,

ubi igitur est $B = 22$, neque autem hic valor tam parvus est quam desideratur; cuius rei ratio est, quod index suprascriptus 2 non satis est magnus. Idem autem iste valor pro B inventus ex ipsis formulis nostris elici potest. Cum enim invenerimus $B = \frac{\overset{\lambda}{N^2} \sin.\lambda\Phi}{\sqrt{n}}$, ob $\lambda = 10$, $N = 3$, $n = 2$ et $\Phi = 54^0\ 44'\ 8'',19$, erit $\lambda\Phi = 547^0\ 21'\ 22''$, hinc auferendo 360^0 erit $\lambda\Phi = 187^0\ 21'\ 22'' = \pi + 7^0\ 21'\ 22''$; ex quo angulo calculus sequenti modo per logarithmos instituatur:

$$\begin{aligned} l \sin.\lambda\Phi &= 9{,}1073320 \\ l\, 3^5 &= 2{,}3856063 \\ \text{Summa} &= 1{,}4929383 \\ \text{Subtr. } l\sqrt{2} &= 0{,}1505150 \\ lB &= 1{,}3424233, \text{ ergo } B = 22. \end{aligned}$$

Quin etiam ex nostris formulis valor litterae $A = \overset{\lambda}{N^2} \cos.\lambda\Phi$ definiri potest hoc modo:

$$\begin{aligned} l \cos.\lambda\Phi &= 9{,}9964108 \\ l\, 3^5 &= 2{,}3856063 \\ lA &= 2{,}3820171, \text{ ergo } A = 241. \end{aligned}$$

13. Simili modo evolvamus sequentem fractionem $\frac{23}{7}$, quae, quia respondet indici satis magno 6, promittit notabilem solutionem. Hic igitur erit $\lambda = 23$, unde colligitur $\lambda\Phi = 1258^0\ 55'\ 8''$ et peripheriam auferendo, quoties fieri potest, $\lambda\Phi = 178^0\ 55'\ 8'' = \pi - 1^0\ 4'\ 52''$, unde litterae A et B sequenti modo computentur:

$l \cos.\lambda\Phi = 9{,}9999227$[1])	$l \sin.\lambda\Phi = 8{,}2757219$
$l \overset{23}{N^2} = 5{,}4868944$	$l \overset{23}{N^2} = 5{,}4868944$
$lA = 5{,}4868171$[2])	Summa $= 3{,}7626163$
ideoque $A = 306773$	$l\sqrt{2} = 0{,}1505150$
	$lB = 3{,}6121013$
	ideoque $B = 4093$.

1) Editio princeps: 276. Correxit A. M.
2) Editio princeps: 220. Correxit A. M.

Hinc ergo fit $3^{23} = (306773)^2 + 2\,(4093)^2$, ubi igitur valor litterae B valde prodit magnus, etiamsi index 6 sit satis notabilis. Hinc igitur iam tuto concludi potest ex sequentibus fractionibus multo adhuc maiores valores pro B esse proditurus, quos adeo hac methodo ob insufficientiam tabularum logarithmicarum definire haud licebit.

EXEMPLUM 2

14. Quoniam omnes potestates binarii, uti vidimus, in forma $xx + nyy$ continentur, quaeramus eas potestates, pro quibus valor ipsius y fit quam minimus, atque adeo unitati aequalis. Hic ergo erit $N = 2$, $n = 7$, tum vero $a = \frac{1}{2}$ et $b = \frac{1}{2}$, unde ergo quaeri debet angulus Φ, ut fiat tang. $\Phi = \frac{b\sqrt{n}}{a} = \sqrt{7}$, ideoque l tang. $\Phi = 10{,}4225490$, consequenter ipse angulus $\Phi = 69^0\,17'\,42'',67$. Quare si ponamus $2^\lambda = A^2 + 7B^2$, erit

$$A = 2^{\frac{\lambda}{2}} \cos.\lambda\Phi \quad \text{et} \quad B = \frac{2^{\frac{\lambda}{2}} \sin.\lambda\Phi}{\sqrt{7}}.$$

15. Ut iam valor ipsius B prodeat quam minimus, in eos casus inquirere debemus, quibus sinus anguli $\lambda\Phi$ minimus evadit. Totum ergo negotium redit ad evolutionem fractionis $\frac{\pi}{\Phi}$, cui fractio $\frac{\lambda}{i}$ proxime debet esse aequalis. At vero in minutis secundis habebimus $\Phi = 249462'',67$, ita ut ob $\pi = 648000''$ evolvi oporteat hanc fractionem: $\frac{\pi}{\Phi} = \frac{64800000}{24946267}$, unde sequentes quoti orientur: 2, 1, 1, 2, 16, 6, 1, 2, 7, 1, 6, 1, 9, 11, 2, ex quibus sequentes fractiones continuo propius ad verum valorem accedentes formantur:

$$\begin{array}{llllllll} 2; & 1; & 1; & 2; & 16; & 6; & 1; & 2; \\ \frac{1}{0}; & \frac{2}{1}; & \frac{3}{1}; & \frac{5}{2}; & \frac{13}{5}; & \frac{213}{82}; & \frac{1291}{497}; & \frac{1504}{579}. \end{array}$$

Ex harum fractionum primis statim prodeunt casus notissimi, veluti ex quarta fit $\lambda = 5$, unde colligitur $\lambda\Phi = 2\pi - 13^0\,31'\,26'',65$, ex quo angulo litterae A et B hunc in modum derivantur:

$l \cos. \lambda\Phi = 9{,}9877885$	$l \sin. \lambda\Phi = 9{,}3689443$
$l N^{\frac{5}{2}} = 0{,}7525750$	$l N^{\frac{5}{2}} = 0{,}7525750$
$l A = 0{,}7403635$	Summa $= 0{,}1215193$
ideoque $A = 5{,}5$.	$l \sqrt{7} = 0{,}4225490$
	$l B = 9{,}6989703$
	ideoque $B = 0{,}5$.

Unde sequitur fore $2^5 = (5\frac{1}{2})^2 + 7\,(\frac{1}{2})^2$, ideoque per 4 multiplicando erit $2^7 = (11)^2 + 7\,(1)^2$.

16. Quinta autem fractio $\frac{13}{5}$ hic est memorabilis, quia habet indicem 16, ideoque valde parvum valorem pro B pollicetur. Sit igitur $\lambda = 13$, eritque $13\,\Phi = 900^0\ 50'\ 14'',71$, sive binis rectis, quoties fieri potest, subductis, erit $13\,\Phi = 0^0\ 50'\ 14'',71$, unde litterae A et B sequenti modo definientur:

$l \cos. \lambda\Phi = 9{,}9999536$	$l \sin. \lambda\Phi = 8{,}1648107$
$l 2^{\frac{13}{2}} = 1{,}9566949$	$l 2^{\frac{13}{2}} = 1{,}9566949$
$l A = 1{,}9566485$	Summa $= 0{,}1215056$
$A = 90{,}5$	$l \sqrt{7} = 0{,}4225490$
	$l B = 9{,}6989566$
	ideoque $B = 0{,}49999 = 0{,}5$,

unde sequitur fore $2^{13} = (90\frac{1}{2})^2 + 7\,(\frac{1}{2})^2$, sive per 4 multiplicando erit $2^{15} = (181)^2 + 7\,(1)^2$, ubi valor ipsius B tam parvus prodiit, quoniam index respondens 16 est praemagnus.

17. Hinc iam satis intelligitur ex sequentibus fractionibus tales casus, quibus B fiat vel $\frac{1}{2}$ vel 1, resultare non posse, nisi indices suprascripti adhuc multo fuerint maiores, quod cum non eveniat, satis tuto affirmare licet in maioribus potestatibus binarii nullas amplius occurrere, quae sint formae $A^2 + 7$. Quod quo facilius perspiciatur, consideremus sequentem fractionem $\frac{213}{82}$, indici 6 subscriptam, unde fit $\lambda = 213$. Hinc cum sit $13\,\Phi = 900^0\,50'\,14'',71$ et $200\,\Phi = 13859^0\ 2'\ 14''$, erit $213\,\Phi = 14759^0\ 52'\ 28'',71$, unde totam peripheriam, quadragies sumtam, subtrahendo remanet $213\,\Phi = 359^0\ 52'\ 28'',71$,

cuius complementum ad totam peripheriam est $0^0\ 7'\ 31'',29$. Calculus ergo ita se habebit:

$l \cos. 213\Phi = 9{,}9999990$	$l \sin. 213\Phi = 7{,}3400396$
$l\, 2^{\frac{213}{2}} = 32{,}0596943$	$l\, 2^{\frac{213}{2}} = 32{,}0596943$
$l A = 32{,}0596933$	Summa $= 29{,}3997339$
	$l \sqrt{7} = 0{,}4225490$
	$l B = 28{,}9771849.$

18. Hinc igitur patet hoc casu numerum A ex triginta tribus figuris constare, quas ergo ex tabulis ne quidem reperire licet; at vero alter numerus B, etiamsi respective sit minimus, hic tamen adhuc usque ad 29 figuras excurrit, quae ergo pariter per tabulas inveniri nequeunt; cuius rei ratio in eo manifesto est sita, quod potestas $2^{\frac{\lambda}{2}}$ tam enormiter magna evasit; ex quo perspicuum est multo minus in altioribus potestatibus minores valores pro B exspectari posse. His igitur missis aliud problema huic affine subiungamus, quo ii casus quaeruntur, quibus littera A minimum sortitur valorem.

PROBLEMA

Si fuerit $N = aa + nbb$, quoniam omnes eius potestates N^λ eandem formam $A^2 + nB^2$ accipiunt, investigare eas potestates, pro quibus littera A minimum adipiscatur valorem.

SOLUTIO

19. Hoc problema simili ratione ac praecedens resolvi poterit. Quaeratur scilicet angulus Φ, ut sit tang. $\Phi = \frac{b\sqrt{n}}{a}$, unde erit ut ante

$$A = N^{\frac{\lambda}{2}} \cos. \lambda\Phi \quad \text{et} \quad B = \frac{N^{\frac{\lambda}{2}} \sin. \lambda\Phi}{\sqrt{n}}.$$

Quare, ut littera A minimum acquirat valorem, necesse est, ut cos. $\lambda\Phi$ evadat minimus, id quod eveniet, si fiat proxime $\lambda\Phi = \frac{\pi}{2}$ vel $\frac{3\pi}{2}$ vel $\frac{5\pi}{2}$ etc. ideoque generaliter $\lambda\Phi = \frac{(2i+1)\pi}{2}$, unde debet esse proxime $\lambda = \frac{2i+1}{2} \cdot \frac{\pi}{\Phi}$, sive $\frac{2\lambda}{2i+1} = \frac{\pi}{\Phi}$.

20. Totum ergo negotium huc redit, ut omnes fractiones quaerantur ipsi $\frac{\pi}{\Phi}$ proxime aequales, quemadmodum iam fecimus pro superiore problemate; at vero ex his fractionibus eae tantum hic adhiberi poterunt, quarum numeratores sint numeri pares, denominatores vero impares; ac si talis fractio occurrat, quae sit $\frac{2f}{2g+1}$, sumi oportebit $\lambda = f$; tum enim, ob cos. $\lambda\Phi$ minimum, numerus A minimum valorem obtinebit, qui ergo erit vel 1 vel etiam unitate maior, quando scilicet minores valores locum habere nequeunt; contra vero evidens est his casibus alterum numerum B maximum esse adepturum valorem.

21. Applicemus hoc ad binos casus supra tractatos, ac primo quidem pro priore erat $N = 3$, $a = 1$, $b = 1$ et $n = 2$, unde prodiit tang. $\Phi = \sqrt{2}$ et $\Phi = 54^0\,44'\,8'',19$; hinc autem fractiones ipsi $\frac{\pi}{\Phi}$ proxime aequales repertae sunt:

$$3,\ 3,\ 2,\ 6,\ 1,\ 4,\ 8,\ 13,\ 1,$$
$$\frac{1}{0},\ \frac{3}{1},\ \frac{10}{3},\ \frac{23}{7},\ \frac{148}{45},\ \frac{171}{52},\ \frac{832}{253},\ \frac{6827}{2076},\ \frac{89583}{27241},$$

inter quas occurrit fractio numeratorem parem habens $\frac{10}{3}$, unde fit $\lambda = 5$, ideoque potestas $3^5 = 243$, quae manifesto est $(1)^2 + 2\,(11)^2$, ita ut hic sit $A = 1$ et $B = 11$, quos valores etiam formulae supra datae praebent. Cum enim sit $\lambda = 5$, erit $\lambda\Phi = 273^0\,40'\,40'',95$ sive $\lambda\Phi = 93^0\,40'\,40'',95$ sive eius complementum ad 180^0, $86^0\,19'\,19'',05$, unde calculus ita se habet:

$l \cos. \lambda\Phi = 8{,}8071973$	$\sin. \lambda\Phi = 9{,}9991046$
$l\,3^{\frac{5}{2}} = 1{,}1928032$	$l\,3^{\frac{5}{2}} = 1{,}1928032$
$lA = 0{,}0000005$	Summa $= 1{,}1919078$
ideoque $A = 1$	$l\sqrt{2} = 0{,}1505150$
	$lB = 1{,}0413928$
	ideoque $B = 11$.

22. Hactenus quidem tantum fractiones principales ipsi $\frac{\pi}{\Phi}$ proxime aequales exhibuimus, dantur vero etiam huiusmodi fractiones minus princi-

pales, quae oriuntur ex indicibus suprascriptis, si unitate vel minuantur vel augeantur. Cum enim indices sint quoti ex divisione oriundi, facile intelligitur, ubi quotus fuerit $= 9$, ibi quoque sumi potuisse sive $9 - 1$ sive $9 + 1$. Hoc observato subscribamus seriei illarum fractionum principalium etiam minus principales, sequenti modo:

$$\begin{array}{ccccc} 3, & 3, & 2, & 6, & 1, \\ \frac{1}{0}, & \frac{3}{1}, & \frac{10}{3}, & \frac{23}{7}, & \frac{148}{45}, \\ & \frac{2}{1}, & \frac{7}{2}, & \frac{13}{4}, & \frac{125}{38}, \\ & \frac{4}{1}, & \frac{13}{4}, & \frac{33}{10}, & \frac{171}{52}. \end{array}$$

Hic igitur occurrunt numeratores pares 2 et 4, unde fit vel $\lambda = 1$ vel $\lambda = 2$; priore casu est $3^1 = (1)^2 + 2\,(1)^2$, altero vero $3^2 = (1)^2 + 2\,(2)^2$, sicque utroque casu $A = 1$, quod quidem tantum evenit in fractionibus initialibus.

23. Simili modo pro altero casu, quo erat $N = 2$, $n = 7$, $a = \frac{1}{2}$ et $b = \frac{1}{2}$, prodiit angulus $\Phi = 69^0\,17'\,42'',67$, et fractio $\frac{\pi}{\Phi}$ dederat quotos 2, 1, 1, 2, 16, 6, 1, unde sequentes formantur fractiones tam principales, quam minus principales:

$$\begin{array}{ccccc} \frac{1}{0}, & \frac{2}{1}, & \frac{3}{1}, & \frac{5}{2}, & \frac{13}{5}, \\ & \frac{1}{1}, & & \frac{2}{1}, & \left[\frac{8}{3}\right], \\ & \frac{3}{1}, & \frac{5}{2}, & \frac{8}{3}, & \frac{18}{7}, \end{array}$$

unde numeratores pares praebent vel $\lambda = 1$ vel $\lambda = 4$ vel $\lambda = 9$. Ex primo valore $\lambda = 1$ fit $2^1 = (\frac{1}{2})^2 + 7\,(\frac{1}{2})^2$, sive $2^3 = (1)^2 + 7\,(1)^2$. Ex secundo valore fit $2^4 = (\frac{1}{2})^2 + 7\,(\frac{3}{2})^2$ sive $2^6 = (1)^2 + 7\,(3)^2$. Tertio habemus $\lambda = 9$, pro quo casu calculum nostrum instituamus, et ob

$$\lambda\Phi = 623^0\,39'\,24'',03 = 3\pi + 83^0\,39'\,24'',03$$

erit

$l \cos. \lambda\Phi = 9{,}0433074$	$l \sin. \lambda\Phi = 0{,}9973329$
$l \overset{9}{N^2} = 1{,}3546350$	$l \overset{9}{N^2} = 1{,}3546350$
$lA = 0{,}3979424$	Summa $= 1{,}3519679$
ideoque $A = 2{,}5$	$l\sqrt{7} = 0{,}4225490$
	$lB = 0{,}9294189$
	ideoque $B = 8{,}5$

sicque erit $2^9 = (\frac{5}{2})^2 + 7(\frac{17}{2})^2$, sive per 4 multiplicando erit $2^{11} = (5)^2 + 7\,(17)^2$. Atque hinc tuto concludere licet pro maioribus exponentibus λ valores litterae A continuo multo maiores esse proditurus. Caeterum quia hic calculi genus prorsus singulare occurrit, speramus hanc speculationem Geometris non esse displicituram.

DE CASIBUS QUIBUS HANC FORMULAM $x^4+kxxyy+y^4$ AD QUADRATUM REDUCERE LICET

Commentatio 696 indicis Enestroemiani
Nova acta academiae scientiarum Petropolitanae 10 (1792), 1797, p. 27—40
Summarium ibidem p. 219—220
Conventui exhibita die 28. Aprilis 1777

SUMMARIUM

On scait qu'en mettant à la place de k les valeurs numériques 1, 3, 4, 5, 6, 7 etc. la formule proposée ne sauroit jamais devenir un quarré, quelques valeurs qu'on donnât à x et à y[1]), tandis que pour les cas $k = \pm 2$ et $k = -nn$, la réduction n'a aucune difficulté. Lors donc qu'on demande quels nombres entiers on pourra mettre à la place de k, pour que la formule proposée soit réductible à un quarré, l'Analyse de Diophante offre différens moyens. Mais de quelque méthode qu'on fasse usage pour résoudre le problème, il reste toujours quelque doute, si l'on a trouvé toutes les valeurs possibles, ou non.

Dans le présent Mémoire l'Auteur a tenté, pour trouver ces valeurs de k, un moyen singulier qui paroît même être contraire à la nature de la question, en représentant k sous la forme irrationelle $P + \sqrt{Q}$, ce qui étant mis à la place de k, la formule proposée étant de la forme $X + Y\sqrt{Q}$, elle ne sauroit être un quarré, à moins que $XX - QYY$ ne soit un quarré. Or la racine de ce quarré aura nécessairement la forme $x^4 + Pxxyy - y^4$, dont le quarré, égalé à $XX - QYY$, conduit à cette équation: $4Pyy - (Q-4)xx = 0$, à laquelle satisfont les valeurs $P = fxx$ et $Q = 4fyy + 4$, de sorte que $k = fxx \pm 2\sqrt{(fyy+1)^2}$), où tout se réduit à rendre un quarré la formule connue de Pell: $fyy + 1$.

Cette ingénieuse méthode ne laisse pas d'avoir le même défaut dont nous avons parlé au commencement de cet extrait, savoir de nous laisser incertains, si de cette manière on puisse trouver toutes les valeurs possibles de k; et l'Auteur avoue qu'il nous manque encore une méthode sûre de résoudre ce Problème, dont la solution complette lui paroît surpasser les forces actuelles de l'Analyse.

1) Dans le cas $k = 6$ Euler a démontré que l'expression ne peut jamais devenir un carré; voir le mémoire 98 (suivant l'Index d'Enestrŏm): *Theorematum quorundam arithmeticorum demonstrationes*, Comment. acad. sc. Petrop. 10 (1738), 1747, *Leonhardi Euleri Opera omnia*, vol. 2, ser. I, p. 38, Corollarium 5 et 6, p. 48/9. Dans le cas $k = 7$ la proposition n'est pas vrai: l'expression donne pour $x = y = 1$ le carré 3^2. Dans le mémoire 755 qui paraîtra dans le vol. 5, sér. I Euler affirme seulement, que cette solution ne permet pas d'en déduire une infinité d'autres solutions. R. F.

2) Edition principale: $R = xx \pm 2\sqrt{(fzz+1)}$. Corrigé par R. F.

1. Super hac formula primum observo inde omnes casus excludi debere, quibus numerorum x et y alteruter esset $= 0$, quoniam tum haec formula sponte evaderet quadratum, quicunque numeri loco k acciperentur. Secundo porro observo, si sumeretur vel $k = 2$ vel $k = -2$, formulam iam sponte esse quadratum, quicunque numeri pro x et y statuerentur. Tertio vero observari convenit omnia quadrata negativa loco k assumta nulla difficultate laborare. Si enim ponatur $k = -nn$, formula evadet $x^4 - nnxxyy + y^4$, quae ergo in quadratum abit sumendo vel $x = ny$ vel $y = nx$, sicque pro littera k ultro se offerunt casus $k = \pm 2$ et $k = -nn$; unde quaestio in hoc versatur, ut omnes reliqui valores pro k investigentur, quibus reductio formulae propositae ad quadratum locum habere queat.

2. Cum igitur postulentur omnes numeri integri pro k accipiendi, quibus formula reductionem ad quadratum admittit, methodus DIOPHANTEA varios modos suppeditat id praestandi. Verum quacunque utamur methodo, semper aliquod dubium relinquitur, an inde omnes plane valores idonei obtineantur; etiamsi facile sit innumerabiles valores idoneos exhibere, ut hoc modo omnes numeri inepti cognosci queant, cuiusmodi sunt $k = 1$ vel $k = 3$ vel $k = 4$ vel $k = 5$ vel $k = 6$ etc., pro quibus iam solide demonstratum est reductionem ad quadratum nullo modo locum habere posse.

3. Quod si enim quadrati, cui formula nostra aequari debet, radix statuatur $= xx + \frac{pyy}{q}$[1]), prodit

$$k = \frac{2p}{q} + \frac{pp}{qq} \cdot \frac{yy}{xx} - \frac{yy}{xx},$$

qui valor ut fiat integer, primo patet pro q sumi debere divisorem ipsius yy, id quod eo pluribus modis fieri potest, quo plures factores numerus y involvit; unde iam patet istam methodum nimis esse vagam, quam ut omnes plane casus in genere exhiberi queant. Si igitur huic conditioni satisfecerimus, ut sit $yy = aq$, aequatio inventa dabit $kxx = \frac{2pxx + app}{q} - aq$. Requiritur igitur porro, ut formula $2pxx + app$, sive $2xx + ap$, divisionem per q admittat, quod si fuerit effectum et Q sit valor huic fractioni aequalis, insuper, cum iam sit $k = \frac{Q - aq}{xx}$, effici debet, ut quantitas $Q - aq$ evadat divisibilis per xx. Ex quo iam satis intelligitur hac methodo perfectam enumerationem omnium valorum idoneorum ipsius k sperari non posse.

1) ubi p, q numeri primi inter se sunt. R. F.

4. Idem defectus se exerit, quando radicem quadratam formulae propositae statuimus $xx + \frac{p}{q}xy \pm yy$, tum enim facta evolutione reperitur

$$kxy = \frac{2p}{q}(xx \pm yy) \pm 2xy + \frac{pp}{qq}xy,$$

sive

$$k = \frac{2p}{q} \cdot \frac{xx \pm yy}{xy} \pm 2 + \frac{pp}{qq},$$

quae forma etiamsi facile ad numeros integros revocatur hincque infiniti numeri idonei erui possunt, tamen pariter ingens relinquitur dubium, num hoc modo omnes plane valores idonei, nullo praetermisso, obtineri queant.

5. Nuper autem, cum haec perpendissem, incidi in methodum prorsus singularem, quae primo intuitu adeo naturae quaestionis adversari videtur. Considero enim valorem litterae k quasi esset formula irrationalis, in binomio $P + \sqrt{Q}$ contenta, ita ut sit $k = P + \sqrt{Q}$. Evidens enim est, postquam in genere omnes valores pro P et Q fuerint inventi, id insuper effici debere, ut Q reddatur numerus quadratus; hoc autem valore substituto formula proposita abibit pariter in tale binomium, cuius pars rationalis erit $x^4 + Pxxyy + y^4$, irrationalis vero $xxyy\sqrt{Q}$, quod igitur quadratum effici debet. Constat autem hoc fieri non posse, nisi quadratum partis rationalis, ablato quadrato partis irrationalis, fiat quadratum; hinc autem pervenitur ad sequentem formam:

$$x^8 + 2Px^6yy + (2 + PP - Q)x^4y^4 + 2Pxxy^6 + y^8.$$

6. Cum iam haec forma in genere debeat esse quadratum, quicunque numeri pro x et y accipiantur, manifestum est eius radicem aliam formam habere non posse, nisi vel $x^4 + Pxxyy + y^4$ vel $x^4 + Pxxyy - y^4$. At vero prior hic locum habere nequit, perduceret enim ad $Q = 0$; unde adhibeamus alteram formam, cuius quadratum est

$$x^8 + 2Px^6yy + (-2 + PP)x^4y^4 - 2Pxxy^6 + y^8,$$

cui si formula inventa aequalis statuatur, pervenitur ad hanc aequationem:

$$4x^4y^4 - Qx^4y^4 + 4Pxxy^6 = 0,$$

quae per xxy^4 divisa praebet:

$$4Pyy - Qxx + 4xx = 0,$$

cui ut satisfiat, statuatur $P = fxx$, hincque sponte se prodit $Q = 4fyy + 4$, ubi id commodi sumus assecuti, ut nullae amplius fractiones sint abigandae.

7. Quoniam igitur invenimus $P = fxx$ et $Q = 4fyy + 4$, binomium pro numero k accipiendum fiet $k = fxx + 2\sqrt{(fyy + 1)}$, nihilque iam amplius superest, nisi ut formula $fyy + 1$ reddatur quadratum, quae cum sit ipsa formula PELLIANA, evidens est hoc infinitis modis praestari posse, dum pro f pro lubitu omnes numeros positivos assumere licet, exceptis solis numeris quadratis; quamobrem huc transferri poterunt, quae circa hanc formulam iam olim sum commentatus, ubi pro singulis valoribus f usque ad 100 valores requisitos ipsius y in tabula sum complexus:[1])

f	y	f	y	f	y	f	g
2	2	29	1820	53	9100	76	6630
3	1	30	2	54	66	77	40
5	4	31	273	55	12	78	6
6	2	32	3	56	2	79	9
7	3	33	4	57	20	80	1
8	1	34	6	58	2574	82	18
10	6	35	1	59	69	83	9
11	3	37	12	60	4	84	6
12	2	38	6	61	226153980	85	30996
13	180	39	4	62	8	86	1122
14	4	40	3	63	1	87	3
15	1	41	320	65	16	88	21
17	8	42	2	66	8	89	53000
18	4	43	531	67	5967	90	2
19	39	44	30	68	4	91	165
20	2	45	24	69	936	92	120
21	12	46	3588	70	30	93	1260
22	42	47	7	71	413	94	221064
23	5	48	1	72	2	95	4
24	1	50	14	73	267000	96	5
26	10	51	7	74	430	97	6377352
27	5	52	90	75	3	98	10
28	24					99	1

1) Vide commentationem 323: *De usu novi algorithmi in problemate Pelliano solvendo*, Novi comment. acad. sc. Petr. 11 (1795), 1767, p. 28—66; *LEONHARDI EULERI Opera omnia* ser. I. vol. 3, p. 73—111, ubi eadem tabula p. 109/10 datur. R. F.

8. Quin etiam, si loco k istum valorem substituamus, deprehendemus formulam nostram propositam revera fieri quadratum. Prodit enim

$$x^4 + fx^4yy + y^4 + 2xxyy\sqrt{(fyy + 1)},$$

quae manifesto est quadratum huius formae:

$$yy + xx\sqrt{(fyy + 1)},$$

quemadmodum periculum facienti mox patebit. Ex quo intelligimus etiam pro omnibus valoribus idoneis litterae k statim radicem quadratam ipsius formulae propositae assignari posse. Ita si fuerit $f = 2$ et $y = 2$, hinc fit $k = 2xx + 6$, ex quo valore formula evadit

$$9x^4 + 24xx + 16 = (3xx + 4)^2 .$$

9. Contemplemur iam accuratius formulam pro k inventam $k = fxx + 2\sqrt{(fyy + 1)}$, ubi per se manifestum est membrum posterius radicale tam positive quam negative accipi posse, ita ut sit

$$k = fxx \pm 2\sqrt{(fyy + 1)} ;$$

quare si primo sumamus $x = 1$ et $y = 1$, erit $k = f \pm 2\sqrt{(f + 1)}$. Iam ut haec formula reddatur rationalis, ponatur $f + 1 = nn$, ideoque $f = nn - 1$, eritque

$$k = nn \pm 2n - 1 = (n \pm 1)^2 - 2 .$$

Sicque pro k iam habentur omnes numeri quadrati binario minuti, unde usque ad centum pro k sumi poterunt sequentes valores:

2, 7, 14, 23, 34, 47, 62, 79, 98.

10. Maneat $y = 1$, at x relinquatur indefinitum, sumtoque $f = nn - 1$ prodibit ista formula:

$$k = (nn - 1)\, xx \pm 2n ,$$

quae iam infinitam multitudinem valorum idoneorum pro k suppeditat. Ubi imprimis notasse iuvabit nihil impedire, quominus pro x fractiones accipiantur, dummodo valor ipsius k prodeat numerus integer, quandoquidem sola ratio

inter x et y est spectanda; unde si prodierit $x = \frac{p}{q}$, quoniam sumsimus $y = 1$, sumi debebit $x : y = p : q$.

11. Percurramus igitur casus simpliciores numeri n; ac si eveniat, ut $nn - 1$ habeat factorem quadratum, puta $nn - 1 = maa$, statui poterit $x = \frac{z}{a}$, fietque hinc $k = mzz \pm 2n$, tum vero erit $x : y = z : a$, hincque nata est sequens tabula:

n	k	$x : y$	n	k	$x : y$
2	$3zz \pm 4$	$z : 1$	31	$15zz \pm 62$	$z : 8$
3	$2zz \pm 6$	$z : 2$	33	$17zz \pm 66$	$z : 8$
4	$15zz \pm 8$	$z : 1$	35	$34zz \pm 70$	$z : 6$
5	$6zz \pm 10$	$z : 2$	37	$38zz \pm 74$	$z : 6$
6	$35zz \pm 12$	$z : 1$	39	$95zz \pm 78$	$z : 4$
7	$3zz \pm 14$	$z : 4$	48	$47zz \pm 96$	$z : 7$
8	$7zz \pm 16$	$z : 3$	49	$6zz \pm 98$	$z : 20$
9	$5zz \pm 18$	$z : 4$	50	$51zz \pm 100$	$z : 7$
10	$11zz \pm 20$	$z : 3$	51	$26zz \pm 102$	$z : 10$
11	$30zz \pm 22$	$z : 2$	53	$78zz \pm 106$	$z : 6$
13	$42zz \pm 26$	$z : 2$	55	$21zz \pm 110$	$z : 12$
15	$14zz \pm 30$	$z : 4$	63	$62zz \pm 126$	$z : 8$
17	$2zz \pm 34$	$z : 12$	65	$66zz \pm 130$	$z : 8$
19	$10zz \pm 38$	$z : 6$[1]	71	$35zz \pm 142$	$z : 12$
23	$33zz \pm 46$	$z : 4$	73	$37zz \pm 146$	$z : 12$
24	$23zz \pm 48$	$z : 5$	80	$79zz \pm 160$	$z : 9$
25	$39zz \pm 50$	$z : 4$	82	$83zz \pm 164$	$z : 9$
26	$3zz \pm 52$	$z : 15$	97	$3zz \pm 194$	$z : 56$
28	$87zz \pm 56$	$z : 3$	99	$2zz \pm 198$	$z : 70$

12. Hactenus scilicet pro f solos numeros integros admisimus; verum etiam fracti admitti possunt, dummodo pro k numeri integri resultent. Quod si enim in genere statuamus $x = 2v$, fiet $k = 4fvv + \sqrt{(4fyy + 4)}$, ubi evidens est sufficere, dummodo $4f$ fuerit numerus integer. Ponatur ergo $4f = g$, eritque $k = gvv + \sqrt{(gyy + 4)}$; ubi quia pro x sumsimus numerum parem,

1) Editio princeps: 12. Correxit A. M.

intelligitur hic pro y tantum numeros impares accipi debere, quia alioquin in casus praecedentes reverteremur.

13. Iam in hac formula statuamus $y = 1$, ut sit $k = gvv \pm \sqrt{(g+4)}$, et nunc, ut $g + 4$ evadat quadratum, primo omnium sumi poterit $g = -3$, unde oritur $k = -3vv \pm 1$; ubi cum sit $x = 2v$, erit $x : y = 2v : 1$, ex qua formula meri numeri negativi pro k resultant, qui usque ad centum erunt:

$$-2,\ -4,\ -11,\ -13,\ -26,\ -28,\ -47,\ -49,\ -74,\ -76,$$

ad quos insuper, uti initio innuimus, quadrata negativa accedunt, scilicet:

$$-1,\ -4,\ -9,\ -16,\ -25,\ -36,\ -49,\ -64,\ -81,\ -100.$$

14. Pro reliquis valoribus ipsius g statuamus $g + 4 = nn$, fietque $k = (nn - 4)\, vv \pm n$. Hic ergo, ut supra, si evadat $nn - 4 = maa$ et loco av scribatur z, erit $k = mzz \pm n$; ubi cum sit $v = \frac{x}{2}$, erit $z = \frac{ax}{2}$, ideoque $x = \frac{2z}{a}$, hincque ratio inter x et y erit $x : y = 2z : a$.

15. In hac autem formula sufficiet pro n numeros tantum impares sumsisse, quandoquidem ex paribus praecedentes formulae redirent. Hoc notato sequentes formulae speciales pro k obtinentur:

n	k	$x : y$	n	k	$x : y$
1	$-3zz \pm 1$	$2z : 1$	27	$29zz \pm 27$	$2z : 5$
3	$5zz \pm 3$	$2z : 1$	29	$93zz \pm 29$	$2z : 3$
5	$21zz \pm 5$	$2z : 1$	47	$5zz \pm 47$	$2z : 21$
7	$5zz \pm 7$	$2z : 3$	51	$53zz \pm 51$	$2z : 7$
9	$77zz \pm 9$	$2z : 1$	79	$77zz \pm 79$	$2z : 9$
11	$13zz \pm 11$	$2z : 3$	83	$85zz \pm 83$	$2z : 9$
23	$21zz \pm 23$	$2z : 5$	119	$13zz \pm 119$	$2z : 33$
25	$69zz \pm 25$	$2z : 3$	123	$5zz \pm 123$	$2z : 55$

16. Ex his iam formulis haud difficulter omnes valores numeri k, usque ad 100, computari possunt, qui cum sponte distinguantur in positivos et negativos, utrosque seorsim in tabulis subiunctis referamus, et cuilibet valori adiungamus rationes inter x et y, unde hi numeri producuntur.

TABULA PRIOR

exhibens omnes valores positivos ipsius k centenario minores

k	Rationes	k	Rationes	k	Rationes
2	Omnes	41	$\frac{3}{4}$	71	$\frac{5}{1}$
7	$\frac{1}{1}$	42	$\frac{1}{6}$	73	$\frac{3}{8}$
8	$\frac{2}{1}$	44	$\frac{4}{1}, \frac{5}{2}, \frac{3}{2}, \frac{11}{70}$	77	$\frac{1}{8}$
12	$\frac{3}{2}$	47	$\frac{1}{1}$	78	$\frac{3}{1}, \frac{10}{21}$
13	$\frac{3}{4}$	48	$\frac{1}{6}$[2]), $\frac{1}{6}$	79	$\frac{1}{1}, \frac{5}{1}, \frac{1}{4}$
14	$\frac{1}{1}$[1])	49	$\frac{9}{56}$	83	$\frac{1}{8}$
16	$\frac{2}{1}, \frac{5}{12}$	52	$\frac{2}{1}, \frac{4}{1}, \frac{2}{21}$	84	$\frac{5}{12}$
17	$\frac{1}{4}$	55	$\frac{1}{15}$	86	$\frac{2}{1}$
23	$\frac{1}{1}, \frac{3}{1}, \frac{1}{4}$	56	$\frac{5}{2}$	87	$\frac{3}{8}$
24	$\frac{3}{2}$	57	$\frac{12}{55}$	89	$\frac{5}{4}, \frac{1}{4}, \frac{8}{33}$
26	$\frac{2}{1}$	61	$\frac{5}{4}$	90	$\frac{6}{35}$
27	$\frac{3}{4}$	62	$\frac{1}{1}$	92	$\frac{7}{2}$
31	$\frac{3}{1}$	63	$\frac{3}{4}$	94	$\frac{3}{2}$
33	$\frac{8}{21}$	64	$\frac{3}{2}, \frac{7}{12}, \frac{2}{15}$	95	$\frac{7}{15}$
34	$\frac{1}{1}$	66	$\frac{3}{1}$	96	$\frac{4}{3}$
36	$\frac{1}{12}$	67	$\frac{4}{21}$	98	$\frac{1}{1}$
38	$\frac{2}{1}$	68	$\frac{2}{1}$	100	$\frac{4}{15}$

1) Editio princeps: $\frac{1}{11}$. Correxit A. M.

2) Editio princeps: $\frac{1}{12}$. Correxit R. F.

TABULA POSTERIOR

exhibens omnes valores negativos ipsius k centenario minores

k	Rationes	k	Rationes	k	Rationes
1	$\frac{1}{1}$	28	$\frac{1}{6}$	67	$\frac{4}{33}$
2	Omnes	32	$\frac{1}{12}$	70	$\frac{4}{35}$
4	$\frac{2}{1}$, $\frac{4}{15}$	36	$\frac{1}{6}$, $\frac{9}{70}$	74	$\frac{1}{10}$
9	$\frac{3}{1}$	40	$\frac{2}{15}$	76	$\frac{1}{10}$
11	$\frac{1}{4}$	42	$\frac{2}{21}$	78	$\frac{6}{55}$
13	$\frac{1}{4}$	43	$\frac{8}{55}$	81	$\frac{1}{9}$
16	$\frac{1}{4}$	44	$\frac{3}{20}$	86	$\frac{3}{28}$
25	$\frac{1}{5}$	47	$\frac{1}{8}$	89	$\frac{1}{12}$
26	$\frac{1}{6}$	49	$\frac{1}{7}$, $\frac{1}{15}$, $\frac{1}{8}$	92	$\frac{1}{20}$
27	$\frac{4}{21}$	64	$\frac{1}{8}$	100	$\frac{1}{10}$

17. Quemadmodum in nostris formulis pro k inventis, quae sunt

$$k = (nn - 1)\,xx \pm 2n \quad \text{et} \quad k = (nn - 4)\,vv \pm n\,,$$

loco x et y numeros fractos admisimus, ita etiam pro n fractiones admitti poterunt, dummodo ita fuerint comparatae, ut inde valores integri pro k reperiantur, quo observato investigatio harum formularum multo facilius institui poterit. Sumto enim $y = 1$, ut formula $x^4 + kxx + 1$ quadratum effici debeat, quaecunque eius fuerit radix, eam semper sub hac formula: $fxx \pm 1$ comprehendere licebit. Hinc autem statim prodit $k = (ff - 1)\,xx \pm 2f$, quae erat formula nostra prior, in qua si statuatur $x = 2v$ et $2f = g$, prodit altera formula $k = (gg - 4)\,vv \pm g$, cui respondet ratio $\frac{x}{y} = \frac{2v}{1}$.

18. Quod si iam loco g fractiones introducere velimus, facile patet statui debere $g = \frac{a}{bb}$, ac praeterea $v = bz$: hoc enim modo prodibit $k = \frac{(aa - 4b^4)}{bb} zz \pm \frac{a}{bb}$, cui respondet ratio $\frac{2bz}{1}$, atque hic pro a et b eiusmodi numeros accipi oportet, ut pro k prodeant numeri integri. Requiritur ergo, ut numerus $aazz \pm a$, hoc est, ut $azz \pm 1$ divisionem per bb admittat, tum enim erit

$$k = a \cdot \frac{azz \pm 1}{bb} - 4bbzz;$$

hocque adeo in genere praestari potest ponendo $a = b^4 + 1$, erit enim

$$k = \frac{(b^4 - 1)^2 zz}{bb} \pm \frac{b^4 + 1}{bb}.$$

Hic iam ponatur $z = \frac{t}{b^4 - 1}$, ut habeatur $k = \frac{tt \pm b^4 + 1}{bb}$, ubi ergo $tt \pm 1$ per bb divisibile reddi debet, unde prodit $k = \frac{tt \pm 1}{bb} \pm bb$. Quomodocunque autem haec formula evolvatur, omnes numeri in ea contenti iam in formulis superioribus contineri videntur.

19. Hinc igitur patet in Analysi adhuc desiderari methodum certam, cuius ope omnes valores ipsius k assignari atque adeo quousque libuerit continuari queant. Quin etiam ex formula fracta fortasse eiusmodi numeri erui posse videntur, qui in formulis integris supra exhibitis non contineantur; veluti se mihi obtulit iste numerus $k = 131$, quem primo intuitu ex formulis supra datis derivari posse non videbatur, cum tamen in formula $(nn - 4)zz \pm n$ contineatur, si posito $z = 6$ pro n vel fractio $\frac{11}{4}$ vel $\frac{25}{9}$ sumatur. Postea vero deprehendi hunc ipsum numerum ex formula $k = 21zz \pm 110$ oriri; num autem hoc semper eveniat, etiamnunc dubitare licet, unde perfecta solutio etiamnunc plane vires Analyseos superare videtur. Quaestio igitur ista maximi momenti sequenti modo proponi potest:

Invenire methodum, cuius ope omnes numeri integri assignari queant, qui ex formula $(nn - 4)zz \pm n$ *resultare possint, si loco litterarum* n *et* z *non solum numeri integri sed etiam fracti accipiantur.*

Huius autem quaestionis enodatio certe insignia incrementa in Analysin DIOPHANTEAM esset illatura.

UTRUM HIC NUMERUS 1000009 SIT PRIMUS NECNE INQUIRITUR

Commentatio 699 indicis ENESTROEMIANI
Nova acta academiae scientiarum Petropolitanae 10 (1792), 1797, p. 63—73[1])
Summarium ibidem p. 222—223
Conventui exhibita die 16. martii 1778

SUMMARIUM

Dans un Mémoire inséré au Tome XIX des Nouveaux Commentaires de l'Académie, intitulé: *De tabula numerorum primorum usque ad Millionem et ultra continuanda, in qua simul omnium numerorum non primorum minimi divisores exprimantur*[2]), feu M. Euler avoit exposé une méthode très facile de construire une table des nombres premiers, et il y avoit donné un modèle de ces tables, contenant les nombres premiers depuis un million jusqu'à 1002000, parmi lesquels se trouvoit aussi le nombre 1000009[3]). Mais ayant eu dans la suite des occasions de douter que ce nombre soit effectivement premier, il l'a soumis à un examen particulier, et cet examen fait le sujet du présent Mémoire.

Dans cette recherche tout revient à savoir, si le nombre proposé 1000009, qui est évidemment la somme des deux quarrés 1000^2 et 3^2, puisse être décomposé encore d'une autre manière en deux nombres quarrés, parce qu'il est démontré que, si cette décomposition a lieu, le nombre n'est certainement pas premier. Or l'Auteur trouve que le nombre en question est non seulement la somme des quarrés de 1000 et de 3, mais qu'il est aussi la somme des quarrés de 972 et de 235; d'où il suit que 1000009 a un diviseur premier 293,

1) Vide finem commentationis 498 indicis ENESTROEMIANI: Extrait d'une lettre de M. EULER à M. BÉGUELIN, Nouv. mém. acad. sc. Berlin 1776, 1779, p. 337—339. *LEONHARDI EULERI, Opera Omnia*, series I, vol. 3, p. 418—420. R. F.

2) Voir le mémoire 467 (indicis ENESTROEMIANI): Novi comment. acad. sc. Petrop. 19 (1774), 1775, p. 132—183, *LEONHARDI EULERI Opera omnia*, series I, vol. 3, p. 359—404. R. F.

3) Consulter la note p. 403 du vol. 3, citée sous 2). R. F.

qui avoit été omis dans la construction de la table mentionnée des nombres premiers contenus entre 1000000 et 1002000.

C'est en suivant le même procédé que l'Auteur examine aussi le nombre 1000081, qui est pareillement la somme de deux quarrés, savoir 1000^2 et 9^2; mais s'étant assûré que c'est la seule décomposition en deux nombres quarrés que ce nombre admet, il en infère qu'il est effectivement premier, tel que le donne la table en question.

L'Auteur observe que de la même manière on peut examiner tout nombre de la forme $4n + 1$, s'il est premier, ou non, pourvu que le dernier chifre en soit ou 1 ou 9; vu que, lorsqu'un tel nombre est résoluble en deux quarrés, l'un ou l'autre de ces quarrés est certainement divisible par 5. Que s'il se trouve que le nombre donné est résoluble d'une seule manière en deux quarrés, il sera premier, mais que si la décomposition en deux quarrés a lieu de deux ou plusieurs manières, il ne sera pas premier et on trouvera ses diviseurs de la manière enseignée dans ce Mémoire. Si enfin le nombre proposé n'est pas du tout résoluble en deux quarrés, il aura, pour le moins, deux facteurs premiers de la forme $4n - 1$.

1. Cum hic numerus manifesto sit summa duorum quadratorum, scilicet $1000^2 + 3^2$, quaestio huc redit: num iste numerus adhuc alio modo in duo quadrata dividi queat? Si enim id nullo modo fieri potest, hic numerus certe erit primus; sin autem adhuc alio modo talis resolutio succedat, tum non erit primus atque tum adeo eius divisores assignare licebit. Quare si unum quadratum statuamus $= xx$, inquirendum est, utrum altera pars, scilicet: $1000009 - xx$, evadere queat quadratum praeter casus $x = 3$ et $x = 1000$, id quod sequenti modo explorari poterit.

2. Quoniam iste numerus definit in 9, alterum quadratum necessario dividi poterit per 5, atque adeo per 25. Statuamus igitur hanc formulam $1000009 - xx$ esse divisibilem per 25, ac perspicuum est necessario esse debere $x = 25a + 3$; tum enim habitur haec formula:

$$1000000 - 6 \cdot 25\,a - 25^2 aa\,,$$

quae divisa per 25 abit in hanc: $40000 - 6a - 25aa$, quae ergo forma quadratum esse debet.

3. Hic duo casus sunt considerandi, prouti a fuerit vel numerus par, vel impar. Sit pro priori casu $a = 2b$, et facta divisione per 4 quadratum esse debet haec formula:

$$A = 10000 - 3b - 25bb .$$

Pro altero casu sit $a = 4c + 1$, et formula quadratum reddenda erit

$$B = 39969 - 224c - 400cc ,$$

quae utique quadratum impar esse potest; sin autem pro eodem casu statuamus $a = 4d - 1$, haec resultat formula:

$$C = 39981 + 176d - 400dd ,$$

quae, quia per 8 divisa relinquit 5, quadratum nunquam esse potest, ita ut tantum binae formulae A et B sint examinandae.

EVOLUTIO FORMULAE
$B = 39969 - 224c - 400cc$

4. Hic igitur litterae c successive omnes valores 0, 1, 2, 3 etc. tam positivos quam negativos tribuamus, et quoniam a numero absoluto 39969 subtrahi debet formula $400cc \pm 224c$, prout c fuerit numerus vel positivus vel negativus, istos numeros successive subtrahendos in duabus columnis, una cum eorum differentiis annotemus:

c	$400\,cc - 224c$	Diff.	c	$400\,cc + 224c$	Diff.
0	0		0	0	
		176			624
1	176		1	624	
		976			1424
2	1152		2	2048	
		1776			2224
3	2928		3	4272	
		2576			3024
4	5504		4	7296	

Ubi statim patet pro utroque casu differentias continuo crescere per 800.

5. Istae igitur differentiae a numero illo absoluto 39969 continuo subtrahantur, id quod commode etiam per binas columnas fieri poterit; ubi ergo videndum erit, an usquam numeri quadrati resultent.

39969	39969	31089	28849
176	624	4176	4624
39793	39345	26913	24225
976	1424	4976	5424
38817	37921	21937	18801
1776	2224	5776	6224
37041	35697	16161	12577
2576	3024	6576	7024
34465	32673	9585	5553
3376	3824	7376	
31089	28849	*2209	

6. In utroque hoc calculo unicum occurrit quadratum $*2209 = 47^2$; unde patet numerum propositum non esse primum, quemadmodum in dissertatione Tomo XIX novorum Commentariorum: *De tabula numerorum primorum usque ad millionem et ultra continuanda*[1]) inserta, est consignatus, sed habere divisores; ad quos inveniendos notetur hoc quadratum provenisse ex valore $c = -10$, unde fit $a = -39$; tum vero colligitur $x = 25a + 3 = -972$, hincque

$$1000009 - xx = 55225 = 235^2,$$

ita ut hanc duplicem resolutionem habeamus:

$$1000^2 + 3^2 = 972^2 + 235^2,$$

hinc transponendo

$$1000^2 - 235^2 = 972^2 - 3^2,$$

unde sequitur

$$(1000 - 235)(1000 + 235) = (972 - 3)(972 + 3),$$

sive $1235 \cdot 765 = 969 \cdot 975$. Hinc fit $\frac{1235}{975} = \frac{969}{765}$, quae fractiones deprimuntur ad hanc simplicissimam: $\frac{19}{15}$, unde denique concluditur[2]) nostrum numerum

1) Vide notam 2) p. 245. R. F.

2) Vide commentationem 228 indicis Enestroemiani: „De numeris, qui sunt aggregata duorum quadratorum, Novi comment. acad. sc. Petrop. 4 (1752/3), 1758, *Leonhardi Euleri Opera omnia*, series I, vol. 2, p. 295, praecipue propositionem 7, p. 316. R. F.

cum summa quadratorum $19^2 + 15^2$ communem habere divisorem, qui ergo erit 293, atque revera reperimus esse

$$1000009 = 293 \cdot 3413 .$$

Ex quo patet in tabulam memoratae dissertationis, ubi omnes numeri primi intra 1000000 et 1002000 contenti exhibentur, errorem irrepsisse, inde natum, quod consideratio divisoris primi 293 est praetermissa.

EVOLUTIO FORMULAE
$A = 10000 - 3b - 25bb$

7. Haec formula est pars centesima formulae $1000009 - xx$, ad quam igitur evolvendam iterum duo casus sunt distinguendi, alter quo b est numerus par, alter vero quo impar. Pro priori casu evidens est, nisi b sit numerus pariter par, formulam propositam quadratum esse non posse. Sit igitur $b = 4c$, et forma resultans, per 4 divisa, fiet $2500 - 3c - 100cc$, quae num quadratum esse queat, praeter casum $c = 0$, haud difficulter apparebit. Primo enim evidens est esse non posse $c = \pm 1$; deinde pariter sumi nequit $c = \pm 2$. Sit igitur $c = \pm 3$, et formula nostra evadet $2500 - 900 \pm 9 = 1600 \pm 9$, quod quadratum esse nequit. Sin autem sumatur $c = \pm 4$, fiet

$$2500 - 1600 \pm 12 = 900 \pm 12 ,$$

certe non quadratum. Denique sumto $c = \pm 5$ pariter quadratum oriri nequit; prodit enim

$$2500 - 2500 \pm 15 = 0 \pm 15 .$$

8. Pro altero casu, ubi b numerus impar, statuatur primo $b = 4d + 1$, ac formula proposita evadet

$$9972 - 212d - 400dd ,$$

quae divisa per 4 fit

$$2493 - 53d - 100dd ,$$

quae casu $d = 0$ manifesto non est quadratum. Sumatur igitur $d = \pm 1$ prodibitque 2393 ± 53, pariter non quadratum; at casus $d = \pm 2$ praebet 2093 ± 106; casus vero $d = \pm 3$ dat 1593 ± 159, ex quorum neutro quadra-

tum resultat, neque ex casu $d = \pm 4$, quippe qui dat 893 ± 212. Casus denique $d = -5$ praebet $-7 + 265$. Sit denique b numerus formae $4d - 1$, prodibitque

$$9978 + 188d - 400dd,$$

qui numerus, cum sit par neque tamen per 4 divisibilis, quadratum esse nequit.

9. Quo vis huius calculi magis eluceat, examinemus adhuc alium huiusmodi numerum in duo quadrata resolubilem, qui sit $1000081 = 1000^2 + 9^2$, et videamus utrum adhuc alio modo in duo quadrata resolvi possit, quorum alterum, uti in casu praecedente, necessario per 5 debet esse divisibile. Posito igitur uno quadrato $= xx$ videamus, an reliqua pars $1000081 - xx$ possit esse quadratum per 5 sive per 25 divisibile.

10. Hunc in finem statuamus $x = 25y + 9$, fietque formula illa

$$1000000 - 18 \cdot 25y - 25^2 yy,$$

quae per 25[1]) divisa abit in hanc simplicem:

$$40000 - 18y - 25yy.$$

Sit nunc primo y numerus par, hoc est $y = 2a$, et formula iterum per 4 divisa ita se habet:

$$A = 10000 - 9a - 25aa.$$

Secundo pro numero impari statuatur: 1^0 $y = 4b + 1$, prodibitque

$$B = 39957 - 272b - 400bb,$$

qui numerus est impar et per 8 divisus relinquit 5, ideoque quadratum esse nequit, unde penitus omitti debet formula B. 2^0 statuamus $y = 4c - 1$, et formula erit:

$$C = 39993 + 128c - 400cc,$$

ubi numerus 39993 per 8 divisus relinquit 1, ideoque propiori examini est subiiciendus.

1) Editio princeps: 4. Correxit A. M.

EVOLUTIO FORMULAE

$$C = 39993 + 128c - 400cc$$

11. Quoniam hic a numero absoluto 39993 successive subtrahi debent numeri in forma $400cc \pm 128c$ contenti, in subsidium calculi, ut supra, subtrahendos numeros cum differentiis, prouti c fuerit vel positivum vel negativum, in sequenti tabula apponamus:

c	$400\,cc - 128\,c$	Diff.	c	$400\,cc + 128\,c$	Diff.
0	0		0	0	
		272			528
1	272		1	528	
		1072			1328
2	1344		2	1856	
		1872			2128
3	3216		3	3984	

Ubi iterum differentiae continuo 800 crescunt.

12. Subtrahamus ergo a numero absoluto 39993 continuo has differentias octingentis crescentes, qui calculus ita se habebit:

39993	39993	30633	29353
272	528	4272	4528
39721	39465	26361	24825
1072	1328	5072	5328
38649	38137	21289	19497
1872	2128	5872	6128
36777	36009	15417	13369
2672	2928	6672	6928
34105	33081	8745	6441
3472	3728	7472	
30633	29353	1273	

Hic igitur nullum plane quadratum occurrit.

EVOLUTIO FORMULAE
$$A = 10000 - 9a - 25aa .$$

13. Ponamus loco a numerum parem, qui adeo debebit esse pariter par, sitque idcirco $a = 4e$, ita ut facta divisione per 4 oriatur haec forma: $2500 - 9e - 100ee$. Hic igitur a numero absoluto successive subtrahi debent numeri in forma $100ee \pm 9e$ contenti, qui igitur in sequenti tabula, prouti e fuerit numerus vel positivus vel negativus, referuntur:

e	$100\,ee - 9\,e$	Diff.	e	$100\,ee + 9\,e$	Diff.
0	0		0	0	
		91			109
1	91		1	109	
		291			309
2	382		2	418	
		491			509
3	873		3	927	

Has igitur differentias ducentis crescentes a numero absoluto 2500 continuo subtrahamus sequenti modo:

2500	2500
91	109
2409	2391
291	309
2118	2082
491	509
1627	1573
691	709
936	864
891	
45	

ubi igitur nulli occurrunt quadrati, praeter 2500, qui autem numerus ad quadratum notum 1000^2 perducit.

14. Sit nunc a numerus impar, ac primo quidem formae $4f + 1$, unde formula nostra evadit
$$9966 - 236f - 400ff^{1}) ,$$

1) Editio princeps: $4ff$. Correxit A. M.

qui numerus cum sit impariter par, quadratum esse nequit. Statuamus ergo $a = 4f - 1$, et formula prodit

$$9984 + 164f - 400ff^{1}),$$

ideoque pariter par; at per 4 divisa ea abit in hanc:

$$2496 + 41f - 100ff.$$

Hic igitur a numero absoluto numeri in forma $100ff \pm 41f$ sunt subtrahendi, qui, prouti f fuerit numerus positivus vel negativus, ita se habebunt:

f	$100ff - 41f$	Diff.	f	$100ff + 41f$	Diff.
0	0		0	0	
		59			141
1	59		1	141	
		259			341
2	318		2	482	
		459			541
3	777		3	1023	

Subtrahantur iam differentiae ducentis crescentes a numero absoluto:

2496	2496
59	141
2437	2355
259	341
2178	2014
459	541
1719	1473
659	741
1060	732
859	
201	

Quoniam igitur in toto hoc calculo nullum quadratum occurrit, certum est numerum propositum 1000081 unico tantum modo in duo quadrata resolvi posse, ideoque certo esse numerum primum, qualis in tabula dissertationis memoratae exhibetur; atque hic imprimis memorabile est, quod tam facili calculo de hac veritate sumus certiores facti.

Editio princeps: $4ff$. Correxit A. M.

15. Dolendum autem est hanc methodum non ad omnes numeros explorandos adhiberi posse, sed restringi ad eos tantum numeros, qui non solum sint summae duorum quadratorum, sed qui desinant insuper in 1 vel 9; quia de his tantum valet, quod alterum quadratum divisibile sit per 5.

16. Interim tamen hac methodo omnes plane numeri in forma $4n + 1$ contenti et sive in 1 sive in 9 desinentes pari successu examinari possunt; quandoquidem novimus, si tales numeri in duo quadrata resolvi queant, alterum certo per 5 esse divisibile. Tum autem, calculo secundum praecepta data instituto, si reperiatur numerum propositum unico modo in duo quadrata resolvi posse, id certum erit signum illum primum; sin autem hoc duobus pluribusve modis fieri queat, inde eius factores assignare licebit eo modo, quo supra usi sumus. Quod si vero eveniat, ut numerus propositus nullo plane modo in duo quadrata dividi queat, tum id etiam erit signum talem numerum non esse primum, etiamsi eius factores hinc definire non licet; tantum autem concludere licet duos ad minimum factores habere primos formae $4n - 1$.

DE NOVO GENERE QUAESTIONUM ARITHMETICARUM PRO QUIBUS SOLVENDIS CERTA METHODUS ADHUC DESIDERATUR

Commentatio 702 indicis Enestroemiani
Nova acta academiae scientiarum Petropolitanae 11 (1793), 1798, p. 78—93
Summarium ibidem p. 162—163
Conventui exhibita die 19. maii 1777

SUMMARIUM

La question qui fait le sujet de ce Mémoire consiste à trouver tous les nombres entiers N tels que les formules $A^2 + B^2$ et $A^2 + NB^2$ deviennent l'une et l'autre à la fois des quarrés. En mettant $A = xx - yy$ et $B = 2xy$, on sçait que la première devient un quarré; et comme l'autre doit aussi devenir un quarré, en mettant ce quarré $= zz$, on obtient $N = \frac{zz-(xx-yy)^2}{4xxyy}$, de sorte que la question se reduit à trouver pour z des valeurs telles que N devienne un nombre entier, ce qui arrive en mettant ou

$$z = xx + 2\alpha xxyy + yy, \text{ ou } z = xx + 2\alpha xxyy - yy,$$

d'où l'on tire les valeurs suivantes pour N:

$$N = (\alpha xx + 1)(\alpha yy + 1),$$
$$N = (\alpha xx - 1)(\alpha yy + 1) + 1,$$

d'où, en donnant successivement à α les valeurs 1, 2, 3, 4, 5, 6 etc. puis aussi des fractions, M. Euler trouve, parmi les 100 premiers nombres naturels, les nombres suivans pour N qui satisfont au problème: 7, 10, 11, 17, 20, 22, 23, 24, 27, 30, 31, 34, 41, 42, 45, 49, 50, 52, 53, 57, 58, 59, 60, 61, 64, 68, 71, 72, 74, 76, 77, 79, 81, 82, 85, 86, 90, 92, 94, 97, 99, 100.

Or ces nombres sont tels qu'il est impossible d'y découvrir un critère propre à faire distinguer les valeurs convenables de N de celles qui ne le sont pas. C'est pourquoi M. Euler a mis ce problème au nombre de ceux, pour la résolution desquels l'Analyse n'a

pas encore de méthode sûre et certaine; et il en est de même du problème de trouver tous les nombres entiers N contenus dans la forme

$$N = (xx + 1)(yy + 1) \quad \text{et} \quad N = (xx - 1)(yy - 1),$$

x et y étant des nombres rationnels quelconques, soit entiers, soit fractionnaires.

1. Occasionem de huiusmodi quaestionibus cogitandi mihi suppeditavit problema DIOPHANTEUM, quo quaeruntur omnes numeri integri pro N accipiendi, ut ambae istae formulae $A^2 + B^2$ et $A^2 + NB^2$ simul quadrata reddi queant. Satis enim constat infinitos numeros hinc excludi, quibus conditioni praescriptae neutiquam satisfieri queat. Veluti si fuerit $N = -1$, demonstratio iam in vulgus nota est, quod hae duae formulae $A^2 + B^2$ et $A^2 - B^2$ nullo modo simul quadrata evadere queant. Idem quoque evenit, si capiatur $N = 2$ vel $N = 3$ vel $N = 4$ vel $N = 5$ vel etiam $N = 6$[1]). Post unitatem enim primus numerus idoneus pro N accipiendus est $N = 7$; quandoquidem sumtis $A = 3$ et $B = 4$, ut $A^2 + B^2 = 25$, erit quoque $A^2 + NB^2 = 121$. Praeterea vero infiniti alii exhiberi possunt huiusmodi numeri idonei tam posititivi quam negativi; semper autem infiniti dantur alii, qui ex hoc ordine penitus excluduntur. Quamobrem quaestio non parum est curiosa, atque attentione satis digna: quemadmodum omnes numeros idoneos pro N accipiendos indagari oporteat? Ubi imprimis criteria desiderantur, quorum ope numeri idonei ab ineptis distingui queant.

2. Ante omnia autem evidens est ab hac quaestione penitus removeri debere casum, quo alterum quadratorum A^2 et B^2 evanesceret, siquidem, si esset $B = 0$, ambae formulae ultro erunt quadrata; sumto autem $A = 0$, omnes numeri quadrati pro N assumti satisfacerent. His ergo casibus exclusis primo conditioni priori, qua formula $A^2 + B^2$ quadratum reddi debet, est satisfaciendum; quod fit ponendo $A = xx - yy$ et $B = 2xy$, tum enim erit $A^2 + B^2 = (xx + yy)^2$, ubi ambos numeros x et y pro lubitu accipere licet, si modo excludantur casus, quibus vel alteruter horum numerorum evanescit, vel ambo inter se aequales capiuntur; quandoquidem priori casu foret $B = 0$, posteriori vero fieret $A = 0$, quos casus modo a nostra tractatione exclusimus.

3. Substituamus nunc istos valores pro A et B assignatos in formula $A^2 + NB^2$, et prodibit haec expressio: $(xx - yy)^2 + 4Nxxyy$, quam ergo

1) Vide librum „Vollständige Anleitung zur Algebra von Hrn. Leonhard Euler". Zweyter Teil. St. Petersburg, 1770, § 223—230; *LEONHARDI EULERI, Opera omnia*, series I, vol. 1, p. 454—464. R. F.

quadratum effici oportet. Potuisset illa quidem quadrato cuicunque aequalis statui, indeque valor ipsius N definiri. Verum quia requiritur, ut N prodeat numerus integer, in id erit incumbendum, cuiusmodi quadrato ista expressio aequalis statui debeat, ut inde pro N numerus integer resultet. Si enim quadratum illud statuatur $= zz$, ex aequatione

$$(xx - yy)^2 + 4Nxxyy = zz$$

elicitur

$$N = \frac{zz - (xx - yy)^2}{4xxyy}.$$

Necesse igitur est, ut numerator huius fractionis per denominatorem divisibilis evadat.

4. In genere autem hoc duplici modo fieri posse observavi, si sumatur vel $z = xx + 2\alpha xxyy + yy$ vel $z = xx + 2\alpha xxyy - yy$. Si enim pro α etiam numeri fracti tam positivi quam negativi admittantur, quemcunque valorem habuerit quantitas z, ea semper in utraque harum formularum comprehendi poterit. Evolvamus igitur valores, qui hinc pro nostro numero N resultant, ac prior quidem forma nobis dabit

$$N = \alpha\alpha xxyy + \alpha xx + \alpha yy + 1 = (\alpha xx + 1)(\alpha yy + 1);$$

ex altera autem forma reperitur

$$N = \alpha\alpha xxyy + \alpha xx - \alpha yy = (\alpha xx - 1)(\alpha yy + 1) + 1.$$

5. Certum igitur est omnes plane valores idoneos ipsius N in his formulis contineri debere, si modo pro littera α non solum numeri integri, sed etiam fracti quicunque admittantur; dum pro binis litteris x et y sufficit solos numeros integros assumsisse, propterea quod numeri illi primitivi A et B semper tanquam integri spectari possunt sine ulla quaestionis restrictione[1]). Quin etiam quilibet valor ipsius N in utraque formula contineri debet, quoniam altera ex altera deduci potest. Si enim in priori ponamus $\alpha xx + 1 = \beta xx$, id quod semper fieri licet, quoniam pro α et β etiam fractiones admittuntur, ob $\alpha = \frac{\beta xx - 1}{xx}$ prior forma evadet $= \beta\beta xxyy - \beta yy + \beta xx$, quae est ipsa forma posterior, si silicet ibi loco α scribatur β. Interim tamen, quia haec

1) Haec propositio non est manifesta, quia $B = 2xy$ numerus par ponitur. R. F.

reductio per fractiones est facta, praestabit utraque forma primo inventa in sequentibus uti; quandoquidem eae essentialiter a se invicem distinguuntur, dum prior, utpote productum ex duobus factoribus, semper numeros compositos producit, posterior vero etiam numeros primos suppeditare potest. Veluti ponendo $\alpha = 1$, $x = 2$ et $y = 1$ prodit $N = 7$.

6. Quin etiam in genere litteram α negative accipere licet, hincque quatuor formulas generales pro N nanciscemur, quae erunt:

$$\begin{aligned} &\text{I.} \quad N = (\alpha xx + 1)(\alpha yy + 1), \\ &\text{II.} \quad N = (\alpha xx - 1)(\alpha yy + 1) + 1, \\ &\text{III.} \quad N = (\alpha xx - 1)(\alpha yy - 1), \\ &\text{IV.} \quad N = (\alpha xx + 1)(\alpha yy - 1) + 1. \end{aligned}$$

Evidens autem est quartam formam a secunda non esse diversam, quia tantum numeri x et y permutantur, qui vero ex sua natura sunt permutabiles.

7. Cum igitur totum negotium eo redeat, ut hinc numeri integri pro N eliciantur, manifestum est hoc semper usu venire, quando litterae α valores integri tribuuntur. Hos igitur casus primum consideremus, indeque actu omnes valores ipsius N usque ad 100 eliciamus. Ubi probe meminisse oportet amborum numerorum x et y neutrum nihilo aequalem statui posse; neque vero etiam inter se aequales capi debere. Sumamus igitur primo $\alpha = 1$, ac prima forma erit $N = (xx + 1)(yy + 1)$. Quia igitur numeri in forma $zz + 1$ contenti sunt 2, 5, 10, 17, 26, 37, 50, 65, 82, 101, producta ex binis horum numerorum valores idoneos pro N exhibebunt, si modo quadrata horum numerorum excludantur. Hoc observato numeri idonei centenario non maiores erunt 10, 20, 34, 50, 52, 74, 85, 100.

8. Manente $\alpha = 1$ forma tertia dabit

$$N = (xx - 1)(yy - 1).$$

Hinc cum numeri formae $zz - 1$ sint 0, 3, 8, 15, 24, 35, 48, 63, 80, 99, producta ex binis horum numerorum diversis quoque valores idoneos pro N praebebunt, qui ad 100 usque erunt 24, 45, 72. Secunda autem forma, casu $\alpha = 1$, erit

$$N = (xx - 1)(yy + 1) + 1,$$

quae forma duplicis generis numeros involvit, qui sunt

$$zz - 1 = 0,\ 3,\ 8,\ 15,\ 24,\ 35,\ 48,$$
$$zz + 1 = 2,\ 5,\ 10,\ 17,\ 26,\ 37,\ 50,$$

et singuli numeri superioris seriei per singulos inferioris multiplicati, si ad productum unitas adiiciatur, dabunt valores idoneos pro N, si modo nullus superiorum per subscriptum multiplicetur. Hinc ergo valores idonei pro N ad 100 usque erunt 7, 17, 31, 41, 49, 52, 71, 76, 79, 97.

9. Sumamus nunc $\alpha = 2$, et ex forma prima habebimus

$$N = (2xx + 1)(2yy + 1)\ ;$$

unde cum numeri formae $2zz + 1$ sint 3, 9, 19, 33, 51, 73, 99, quorum producta ex binis diversis sunt sumenda, hinc prodeunt pro N sequentes numeri: 27, 57, 99. Forma autem tertia dat

$$N = (2xx - 1)(2yy - 1)\ .$$

Hinc cum numeri formae $2zz - 1$ sint 1, 7, 17, 31, 49, 71, 97, producta ex binis diversis praebent sequentes valores idoneos pro N: 7, 17, 31, 49, 71, 97[1]). Forma autem secunda praebet

$$N = (2xx - 1)(2xx + 1) + 1\ ,$$

ubi duplicis generis factores erunt:

$$2zz - 1 = 1,\ 7,\ 17,\ [31],\ 49,\ 71,\ 97,$$
$$2zz + 1 = 3,\ 9,\ 19,\ [33],\ 51,\ 73,\ 99[2]).$$

Hinc exclusis numeris subscriptis producta ex superioribus per inferiores unitate aucta dabunt valores pro N idoneos, qui ad 100 usque sunt hi: 10, 20, 22, [34], 52, 74, 94, 100[3]).

---

1) Editio princeps: 79. Correxit A. M.
2) Editio princeps: 100. Correxit A. M.
3) Editio princeps: 101. Correxit A. M.

10. Sit nunc $\alpha = 3$, ac prima forma dat

$$N = (3xx + 1)(3yy + 1),$$

unde numeri huius formae $3zz + 1$ sunt 4, 13, 28, 49, 76. Hinc igitur producta ex binis diversis sumendo, unicus tantum oritur numerus idoneus pro N infra 100, scilicet 52. At ex forma tertia fit

$$N = (3xx - 1)(3yy - 1);$$

unde quia numeri formae $3zz - 1$ sunt 2, 11, 26, 47, 74, producta ex binis diversis dant 22, 52, 94. Ex forma autem secunda

$$N = (3xx - 1)(3yy + 1) + 1$$

prodeunt sequentes pro N valores: 27, 45, 57, 99.

11. Superfluum foret pro α sumere 4. Nam quia $4xx$ et $4yy$ sunt quadrata, casus eodem rediret ac $\alpha = 1$. Sit igitur $\alpha = 5$, ac prima forma dat

$$N = (5xx + 1)(5yy + 1),$$

unde infra 100 nullus numerus idoneus prodit. Ex forma autem tertia

$$N = (5xx - 1)(5yy - 1)$$

prodit 76. At secunda forma

$$N = (5xx - 1)(5yy + 1) + 1$$

praebet 85.

12. Si porro statuere velimus $\alpha = 6$, nullus numerus infra centenarium inde nascitur. Quamobrem, si omnes numeros inventos colligamus, valores integri pro α assumti pro N sequentes numeros idoneos in ordine dispositos praebent: 7, 10, 17, 20, 22, 24, 27, 31, 34, 41, 45, 49, 50, 52, 57, 71, 72, 74, 76, 79, 85, 94, 97, 99, 100.

13. Plurimum autem falleretur, si quis putaret plures valores idoneos usque ad centenarium non dari. Nullum enim est dubium, quin etiam valores

fracti pro α assumti quosdam quoque centenario minores numeros pro N producant, quos casus ut perscrutemur, necesse est in eas fractiones pro α accipiendas inquirere, unde valores integri pro N oriri queant, id quod in sequente problemate expediemus.

PROBLEMA

Investigare eas fractiones pro α accipiendas, unde ista formula generalis: $(\alpha xx \pm 1)(\alpha yy \pm 1)$ valores integros adipisci possit.

SOLUTIO

14. Ista investigatio potissimum pendet ab indole binorum numerorum x et y, quos non solum semper tanquam integros, sed etiam primos inter se spectare licet. Res autem nunc praecipue huc redit, utrum ambo hi numeri x et y factores habeant, necne, quandoquidem ab his factoribus fractiones per α introductae tolli debent. Statuamus igitur in genere $x = pq$ et $y = rs$, quippe qua positione defectus factorum non excluditur, quia nihil impedit, quominus pro p et s unitas accipiatur. Caeterum quia x et y sunt primi inter se, p, q, r, s ut primi inter se spectari poterunt; hoc modo formula proposita erit

$$N = (\alpha ppqq \pm 1)(\alpha rrss \pm 1).$$

15. Statuamus nunc pro α hanc fractionem: $\alpha = \frac{a}{qqss}$, ubi iam littera a numeros integros quoscunque designet, atque formula proposita sequentem induet formam:

$$\left(\frac{app}{ss} \pm 1\right)\left(\frac{arr}{qq} \pm 1\right) = \left(\frac{app \pm ss}{ss}\right)\left(\frac{arr \pm qq}{qq}\right).$$

Ubi observasse iuvabit, quia tam numeri p et s quam q et r sunt primi inter se, neutram harum duarum fractionum in numerum integrum abire posse, propterea quod ex numero a tam factor qq quam ss excluditur; verum permutentur ambo denominatores, ut obtineatur ista forma:

$$\left(\frac{app \pm ss}{qq}\right)\left(\frac{arr \pm qq}{ss}\right),$$

ubi iam nihil impedit, quominus utraque haec fractio numero integro aequari possit, quandoquidem fieri potest, ut tam $app \pm ss$ divisibile fiat per qq, quam $arr \pm qq$ divisibile per ss.

16. Ut autem prius eveniat, ex proprietatibus numerorum iam satis cognitis oportet, ut q sit numerus formae $aff \pm gg$[1]); tum enim semper pro p numeros integros tales invenire licebit, ut forma $app \pm ss$ fiat divisibilis per qq. Simili modo etiam requiritur, ut sit s formae $aff \pm gg$; tum enim pariter semper numeri integri pro r assignari poterunt, quibus forma $arr \pm qq$ divisionem per ss admittat.

17. Hoc problemate soluto, si statuamus $x = pq$ et $y = rs$, sumto $\alpha = \frac{a}{qqss}$, tres nostrae formae generales pro N inventae sequenti modo repraesentabuntur:

$$\text{I. } N = \left(\frac{app + ss}{qq}\right)\left(\frac{arr + qq}{ss}\right),$$

$$\text{II. } N = \left(\frac{app - ss}{qq}\right)\left(\frac{arr + qq}{ss}\right) + 1,$$

$$\text{III. } N = \left(\frac{app - ss}{qq}\right)\left(\frac{arr - qq}{ss}\right),$$

ubi pro litteris p, q, r, s eiusmodi valores accipi debent, ut binae illae fractiones ad numeros integros revocentur; ex quo intelligitur has formas infinities esse generaliores quam praecedentes.

18. Maximum autem discrimen hinc statim elucet, quod, cum priores formae nunquam ad numeros negativos pro N perducant, hic tam forma secunda quam tertia innumerabiles alios numeros negativos exhibere queat, quando scilicet vel $app < ss$, vel $arr < qq$, ex quo solo iam certo sequitur has formulas posteriores innumerabiles praebere posse valores idoneos pro N, qui in formulis primo inventis plane non contineantur.

19. Hae autem formulae ita latissime patent, ut difficillimum sit omnes casus in iis contentos repraesentare; quamobrem casus saltem quosdam maxime speciales evolvamus. Ac primo quidem sumamus $a = 1$ et $s = 1$, et

1) Haec conditio non est valida, nisi numerus classium formarum binariarum quadraticarum determinantis $\mp a$ unitati aequalis est. R. F.

forma nostra prima dabit $N = \left(\frac{pp+1}{qq}\right)(rr + qq)$, ubi ergo tantum opus est, ut qq fiat divisor formulae $pp + 1$, id quod statim evenit sumendo $p = 7$ et $q = 5$, sicque enim fiet $N = 2(rr + 25) = 2rr + 50$[1]). Hinc autem pro N infra 100 sequentes novi prodeunt valores: 58, 68, 82.

20. Quoniam secunda forma etiam hoc modo referri potest: $\left(\frac{app+ss}{qq}\right)\left(\frac{arr-qq}{ss}\right) + 1$, sumto $a = 1$ et $s = 1$ erit $N = \left(\frac{pp+1}{qq}\right)(rr - qq) + 1$. Hinc sumto $p = 7$ et $q = 5$ erit $N = 2rr - 49$[1]), unde primum pro N isti numeri negativi prodeunt: -17, -31, -41, -47, positivi autem infra 100 hinc oriundi sunt: 23, 49, 79. Deinde vero formula $pp + 1$ per numerum quadratum dividi nequit, usque ad $p = 18$ et $q = 5$, unde prodit $\frac{pp+1}{qq} = 13$, ideoque ex forma prima fit

$$N = 13(rr + 25) = 13rr + 325^{2}),$$

ex secunda autem forma fit $N = 13rr - 324$. Hinc autem nulli numeri infra 100 oriuntur.

21. Maneat $a = 1$ et $s = 1$, ac forma tertia dabit

$$N = \left(\frac{pp-1}{qq}\right)(rr - qq),$$

secunda vero dabit

$$N = \left(\frac{pp-1}{qq}\right)(rr + qq) + 1,$$

quae formulae satis sunt foecundae in numeris idoneis pro N exhibendis, quoniam pluribus modis $\frac{pp-1}{qq}$ potest esse numerus integer. Primo silicet sumto $p = 3$ capi poterit $q = 2$, unde prior forma erit $N = 2rr - 8$[3]), posterior vero $N = 2rr + 9$[3]); illa igitur praebet hunc numerum negativum: $N = -6$, hos vero positivos: 10, 24, 42, 64, 90; ex posteriore vero oriuntur hi positivi: 11, 17, 27, 41, 59, 81.

---

1) $r \neq 7 \cdot 5$, ne x aequalis y fiat. Euler in sequentibus formulis conditionem $x \neq y$ neglegit; in casu $x = y$ N semper quadratum fit. R. F.

2) $r \neq 18 \cdot 5$. R. F.

3) $r \neq 2 \cdot 3$. R. F.

22. Sit nunc $p = 5$ et $q = 2$, et ambae formulae erunt $N = 6rr - 24$ et $N = 6rr + 25$[1]). Ex illa prodit numerus negativus -18; positivi vero 30, 72. Ex altera vero oriuntur hi numeri: 31, 49, 79. Sumatur nunc $p = 7$ et $q = 4$, et ambae formulae erunt $N = 3rr - 48$ et $N = 3rr + 49$[2]). Prior dat hos negativos: -45, -36, -21; positivos vero hos: 27, 60, 99. Altera forma dat hos positivos: 52, 61, 76, 97.

23. Sumamus nunc $p = 8$ [et $q = 3$], et formulae nostrae erunt $N = 7rr - 63$ et $N = 7rr + 64$[3]). Ex priore oriuntur hi negativi: -56, -35; et positivus 49. Secunda vero forma praebet hos positivos: 71, 92.

24. Sumto porro $p = 9$, capi poterit $q = 4$, unde formulae nostrae fiunt $N = 5rr - 80$ et $N = 5rr + 81$[4]). Prima praebet hos negativos: -75, -60, -35; positivos vero hos: 45, 100. Altera vero praebet 86.

25. Sumto porro $p = 10$, erit $q = 3$, et formulae erunt $N = 11rr - 99$ et $N = 11rr + 100$. Prima forma dat hos negativos numeros: -88, -55; positivum vero 77. Si hoc modo ulterius progredi velimus, unicus novus numerus infra 100 reperitur, scilicet -90.

26. Hactenus igitur sequentes numeros negativos pro N sumus adepti: -6, -17, -18, -21, -31, -35, -36, -41, -45, -47, -55, -56, -60, -75, -88, -90; at vero numeri positivi hactenus inventi et in ordinem redacti sunt: 7, 10, 11, 17, 20, 22, 23, 24, 27, 30, 31, 34, 41, 42, 45, 49, 50, 52, 57, 58, 59, 60, 61, 64, 68, 71, 72, 74, 76, 77, 79, 81, 82, 85, 86, 90, 92, 94, 97, 99, 100.

27. Hic ordo numerorum negativorum adhuc satis est magnus, dum ex casibus magis complicatis insuper plures alii oriuntur; at vero ordo positivorum ex talibus casibus vix uno vel altero augebitur, uti mox docebimus. Maneat adhuc $a = 1$, at ponatur $s = 2$, atque forma prima dabit

$$N = \left(\frac{pp+4}{qq}\right)\left(\frac{rr+qq}{4}\right),$$

1) $r \neq 2 \cdot 5$. Vide notam 1) p. 263. R. F.
2) $r \neq 4 \cdot 7$. R. F.
3) $r \neq 3 \cdot 8$. R. F.
4) $r \neq 4 \cdot 9$. R. F.

quae autem, quoniam summa duorum quadratorum nunquam per 4 est divisibilis, praetermitti debet; hinc autem forma secunda[1]) praebet

$$N = \left(\frac{pp+4}{qq}\right)\left(\frac{rr-qq}{4}\right) + 1 .$$

Hic iam sumatur $p = 11$ et $q = 5$, fietque $N = 5\left(\frac{rr-25}{4}\right) + 1$. Statuatur porro $r = 2t + 1$, eritque $N = 5(tt + t) - 29$, unde nascuntur isti numeri negativi: -19, -29; ad positivos vero hinc nullus accedit.

28. Manente $s = 2$ et $a = 1$, forma tertia praebet

$$N = \left(\frac{pp-4}{qq}\right)\left(\frac{rr-qq}{4}\right),$$

secunda vero

$$N = \left(\frac{pp-4}{qq}\right)\left(\frac{rr+qq}{4}\right) + 1 ,$$

quae autem, ob rationem ante memoratam, est omittenda. Sumatur nunc primo $p = 7$ et $q = 3$, eritque $N = 5\left(\frac{rr-9}{4}\right)$, quae forma, posito $r = 2t + 1$, abit in $N = 5(tt + t) - 10$, unde oritur numerus negativus -10, positivus vero nullus novus hinc oritur. Sumto autem $p = 11$, $[q = 3]$, erit

$$N = 13\left(\frac{rr-9}{4}\right) = 13(tt + t - 2) ,$$

unde nascitur iste numerus negativus: -26, positivorum autem nullus novus accedit.

29. Casu autem postremo si sumamus $p = 1$ et $q = 1$, erit $N = -3\left(\frac{rr-1}{4}\right)$, quae posito $r = 2t + 1$ abit in hanc: $N = -3(tt + t)$, unde oriuntur sequentes numeri negativi: -6, -18, -36, -60, -90, qui autem omnes iam sunt inventi. Sumatur vero $s = 3$ et $p = 1$ et $q = 2$, orietur hinc forma $N = -2\left(\frac{rr-4}{9}\right)$. Ponatur hic $r = 9t + 2$ fietque $N = -2(9tt + 4t)$, unde sumto $t = -1$, prodit $N = -10$. Ex $t = 1$ fit $N = -26$. At $t = -2$ praebet -56.

1) Ubi s et q mutantur. R. F.

30. Nimis longum autem foret omnes huiusmodi casus prosequi, praesertim cum nunquam certi esse possemus omnes valores idoneos pro N invenisse, siquidem terminus ultra 100 extenderetur; hanc ob rem tantum aliquos casus speciales subiungamus, unde saltem novi numeri positivi deduci queant. Pro forma autem prima, manente $a = 1$, erit

$$N = \left(\frac{pp + ss}{qq}\right)\left(\frac{rr + qq}{ss}\right),$$

ubi iam notavimus hos factores integros fieri non posse, nisi numeri q et s sint summae duorum quadratorum. Sin autem pro forma secunda sit

$$N = \left(\frac{pp + ss}{qq}\right)\left(\frac{rr - qq}{ss}\right) + 1,$$

sufficiet, ut tantum q sit summa duorum quadratorum. Hic ergo sumamus $p = 4$ et $s = 3$, at vero $q = 5$, ut prodeat

$$N = \frac{rr - 25}{9} + 1 = \frac{rr - 16}{9}.$$

Posito ergo hic $r = 9t + 4$, prodit $N = 9tt + 8t$, unde autem nulli novi numeri deducuntur.

31. Consideremus casum, quo $\frac{pp + ss}{qq} = 1$, simul vero ambo numeri q et s sint summae duorum quadratorum, ut prima forma locum habere possit, id quod eveniet sumendo $p = 12$, $s = 5$ et $q = 13$, fietque $N = \frac{rr + 169}{25}$, quae fractio, si evadat integra casu $r = f$, etiam numeros integros dabit ponendo $r = 25t \pm f$; tum enim prodibit

$$N = 25tt \pm 2tf + \frac{ff + 169}{25},$$

haec conditio autem adimplebitur, sumendo $r = 25t \pm 9$, hinc enim fiet

$$N = 25tt \pm 18t + 10,$$

unde oriuntur sequentes valores: 10, 17, 53, 74, quorum 53 plane est novus. Si forma secunda pro iisdem positionibus uti vellemus, haberetur

$$N = \frac{rr - 169}{25} + 1 = \frac{rr - 144}{25},$$

quae si ponatur $r = 25t \pm 13$, transit in hanc formam:

$$N = 25tt \pm 26t + 1, \quad \text{sive} \quad N = (t \pm 1)(25t \pm 1),$$

unde patet hanc formam iam in principali, quae erat

$$N = (\alpha xx \pm 1)(\alpha yy \pm 1),$$

contineri sumendo $\alpha = t$, $x = 1$ et $y = 5$, unde novi numeri non sunt expectandi.

32. Ex iis igitur, quae hactenus sunt tradita, patet valores idoneos positivos pro numero N usque ad 100 hoc ordine procedere:

7,	10,	11,	17,	20,	22,	23,	24,	27,	30,	31,	34,	41,	42,
45,	49,	50,	52,	53,	57,	58,	59,	60,	61,	64,	68,	71,	72,
74,	76,	77,	79,	81,	82,	85,	86,	90,	92,	94,	97,	99,	100.

Sequentes autem ex hoc ordine exclusi sunt putandi:

2,	3,	4,	5,	6,	8,	9,	12,	13,	14,	15,	16,	18,	19,	21,
25,	26,	28,	29,	32,	33,	35,	36,	37,	38,	39,	40,	43,	44,	
46,	47,	48,	51,	54,	55,	56,	62,	63,	65,	66,	67,	69,	70,	
73,	75,	78,	80,	83,	84,	87,	88,	89,	91,	93,	95,	96,	98.	

Quomodocunque autem hos binos ordines contemplemur, nullum plane patescit criterium, quo numeri idonei et inepti a se invicem distinguantur; unde affirmare haud dubito certam methodum huiusmodi quaestiones resolvendi in Analysi etiamnunc esse incognitam.

33. Cum autem quaestio, quam hactenus tractavimus, sit quodammodo complicata, aliquas quaestiones simpliciores speciminis loco, hic subiungam, quas, quam diu methodus memorata latuerit, pariter resolvere non licet.

QUAESTIO 1

34. *Si litterae x et y denotent numeros quoscunque rationales tam fractos quam integros, investigare omnes numeros integros N, qui in hac formula: $N = (xx + 1)(yy + 1)$ contineantur.*

Hic quidem primo patet, sumto $x = 0$ sequentes numeros occurrere:

1, 2, 5, 10, 17, 26, 37, 50, 65, 82 etc.

Praeterea vero manifestum est in ista forma non solum quadrata singulorum horum numerorum, sed etiam producta ex binis quibusque occurrere, quae sunt

4, 10, 20, 25, 34, 50, 52, 74, [85], 100.

Hi scilicet numeri ex valoribus integris litterarum x et y nascuntur; verum innumerabiles alii oriri possunt ex valoribus fractis. Si enim ponamus $x = \frac{p}{q}$ et $y = \frac{r}{s}$, fiet

$$N = \left(\frac{pp + qq}{qq}\right)\left(\frac{rr + ss}{ss}\right), \quad \text{sive} \quad N = \left(\frac{pp + qq}{ss}\right)\left(\frac{rr + ss}{qq}\right),$$

ubi manifestum est infinitis modis fieri posse, ut tam $pp + qq$ per ss quam $rr + ss$ per qq divisionem admittat. Hic igitur potissimum certa methodus desideratur, quae omnes plane valores idoneos pro N, usque ad terminum quemcunque, assignare valeat.

QUAESTIO 2

35. *Si x et y denotent omnes numeros rationales tam fractos quam integros, investigare omnes numeros integros, qui in hac formula: $N = (xx - 1)(yy - 1)$ contineantur.*

Hic autem ex valoribus integris ipsarum x et y numeri resultantes facile assignantur ac describi possunt; at vero ex fractionibus $x = \frac{p}{q}$ et $y = \frac{r}{s}$ innumerabiles alii resultare possunt, quorum indolem et nexum cum prioribus perscrutari — hoc opus hic labor est!

DE FORMULIS SPECIEI $mxx+nyy$ AD NUMEROS PRIMOS EXPLORANDOS IDONEIS EARUMQUE MIRABILIBUS PROPRIETATIBUS[1)]

Commentatio 708 indicis Enestroemiani
Nova acta academiae scientiarum Petropolitanae 12 (1794), 1801, p. 22—46
Summarium ibidem p. 60—62
Conventui exhibita die 16. martii 1778

SUMMARIUM

Lorsque m et n sont des nombres positifs, si un nombre N est contenu de deux manières différentes dans la forme $mxx + nyy$, de sorte que $N = maa + nbb$ et $N = mcc + ndd$, en reduisant la fraction $\frac{a \pm c}{b \pm d}$ à ses moindres termes $\frac{p}{q}$, de même que la fraction $\frac{mpp}{nqq} = \frac{r}{s}$, dans le cas que $r + s$ est un nombre impair, il sera facteur du nombre N; s'il est pair, sa moitié $\frac{r+s}{2}$ sera facteur de ce nombre N. De là il suit que tout nombre contenu plus d'une façon dans la forme $mxx + nyy$ sera un nombre *composé* ou *non-premier*.

Cependant il faut se garder d'en conclure que tous les nombres qui ne sont contenus que d'une seule manière dans la forme $mxx + nyy$ soyent premiers; car il y a très certainement une infinité de valeurs pour m et n, pour lesquelles la formule $mxx + nyy$ renferme des nombres composés, quoiqu'ils n'y soyent contenus que d'une seule manière; tandis qu'il y en a d'autres nombres m et n, pour lesquelles la proposition inverse mention-

1) Vide Commentationem 498 indicis Enestroemiani: Extrait d'une lettre de M. Euler à M. Béguelin, Nouv. mém. acad. sc. de Berlin, 1776, 1779, p. 337—339. *Leonhardi Euleri, Opera omnia*, series I, vol. 3, 418—420. R. F.

Cf. F. Grube: Über einige Euler'sche Sätze aus der Theorie der quadratischen Formen (Zeitschrift für Mathematik und Physik, XIX. Jahrgang, 1874). Ibi Euleri demonstrationes completae sunt. A. M.

née a évidemment lieu. Il est donc intéressant de connoître les valeurs de m et n qui rendent la formule $mxx + nyy$ telle qu'un nombre qui n'y est contenu que d'une seule façon soit premier. C'est le sujet qui a occupé feu M. EULER dans le présent Mémoire, où il donne une table de ces nombres m et n qu'il appelle nombres *congrus* et dont il y démontre les propriétés remarquables suivantes:

1. Si la formule $mxx + nyy$ est congrue, la formule $mnxx + yy$ le sera aussi, et *vice versa*.
2. Dans la suite des nombres congrus mn il ne se trouve d'autres nombres quarrés que 1, 4, 9, 16 et 25.
3. Lorsque un nombre congru est de la forme $4\alpha - 1$, son quadruple $4(4\alpha - 1)$ sera aussi un nombre congru.
4. Si i est un nombre impair et que $4i$ est un nombre congru, son quadruple $16i$ sera aussi un nombre congru.
5. λ étant un nombre quelconque, si $\lambda\lambda i$ est un nombre congru, i même sera aussi un nombre congru.
6. Si un nombre congru est de la forme $3\alpha - 1$, son noncuple $9(3\alpha - 1)$ sera aussi un nombre congru.
7. Si un nombre impair de la forme $4\alpha + 1$ est congru, son quadruple $4(4\alpha + 1)$ ne sçauroit l'être.
8. Si un nombre congru est de la forme $4\alpha + 2$, son quadruple $4(4\alpha + 2)$ le sera aussi.
9. Si i marque un nombre impair et que $8i$ est un nombre congru, son quadruple $32i$ ne scauroit être tel.
10. Et si $16i$ est un nombre congru, son quadruple $64i$ ne sçauroit l'être.
11. i étant un nombre congru d'une forme quelconque; si $i + aa = pp < 4i$, p étant nombre premier, son quadruple $4i$ ne sçauroit être un nombre congru.

Parmi les nombres naturels depuis 1 jusqu'à 10000 M. EULER n'a pu trouver que 65 nombres congrus, et il lui paroît vraisemblable qu'il n'y en a pas d'avantage; ce qui seroit d'autant plus remarquable que dans toute l'Analyse on ne connoît jusqu'ici aucune suite de nombres qui consistât en un nombre de termes fini.

1. Hic praecipue respicio ad eam huiusmodi formularum proprietatem, qua constat omnes numeros, qui in tali forma $mxx + nyy$ duplici modo continentur, certe non esse primos, siquidem numeri m et n ambo fuerint positivi; si enim alter eorum esset negativus, utique evenire posset, ut idem numerus primus pluribus modis in tali formula contineretur. Veluti si $m = 2$ et $n = -1$, in formula $2xx - yy$ numerus primus 7 pluribus adeo modis continetur, scilicet:

I. Si $x = 2$ II. Si $x = 4$ III. Si $x = 8$
$y = 1$ $y = 5$ $y = 11$

atque adeo infinitis aliis modis hoc contingere potest.

2. Verum si ambo numeri m et n fuerint positivi, uti deinceps perpetuo supponemus, tum quoties quispiam numerus N duplici modo in formula $mxx + nyy$ continetur, ita ut sit

$$N = maa + nbb = mcc + ndd ,$$

eius factores per hanc regulam satis facilem semper inveniri possunt. Formetur enim primo fractio $\frac{p}{q} = \frac{a \pm c}{b \pm d}$ ad minimos terminos reducenda; hincque formetur alia fractio $\frac{r}{s} = \frac{mpp}{nqq}$ pariter ad formam simplicissimam reducenda, quo facto erit $r + s$ factor numeri N, siquidem $r + s$ fuerit numerus impar, sin autem fuerit par, tum eius semissis $\frac{r+s}{2}$ factor erit numeri N; et quoniam ob ambiguitatem signi quatuor variationes locum habent, binae dabunt unum ipsius N factorem, binae reliquae vero alterum[1]).

3. Quo hoc clarius perspiciatur, sequens perpendamus exemplum. Consideremus formulam $7\,xx + 3\,yy$, ubi $m = 7$ et $n = 3$, in qua numerus 391 duplici modo continetur, cum sit primo

$$391 = 7 \cdot 2^2 + 3 \cdot 11^2 ,$$

tum vero etiam

$$391 = 7 \cdot 7^2 + 3 \cdot 4^2 .$$

Hinc ergo erit $\frac{p}{q} = \frac{7 \pm 2}{11 \pm 4}$, cuius ergo quaterni valores erunt

I. $\frac{p}{q} = \frac{3}{5}$; II. $\frac{p}{q} = \frac{9}{7}$; III. $\frac{p}{q} = \frac{1}{3}$; IV. $\frac{p}{q} = \frac{5}{7}$;

hinc iam porro deducantur sequentes fractiones:

---

1) Vide Commentationem 708a indicis Enestroemiani: Extrait d'une lettre de M. Fuss à M. Béguelin, Nouv. mém. de l'acad. sc. Berlin 1776, 1779, p. 340—346. *Leonhardi Euleri Opera omnia*, series I, vol. 3, p. 421—428. R. F.

I. $\frac{r}{s} = \frac{7 \cdot 3^2}{3 \cdot 5^2} = \frac{21}{25}$; II. $\frac{r}{s} = \frac{7 \cdot 9^2}{3 \cdot 7^2} = \frac{27}{7}$; III. $\frac{r}{s} = \frac{7 \cdot 1^2}{3 \cdot 3^2} = \frac{7}{27}$; IV. $\frac{r}{s} = \frac{7 \cdot 5^2}{3 \cdot 7^2} = \frac{25}{21}$.

Hic ergo prodit ubique $r + s$ numerus par, ideoque semissem capiendo ex primo et quarto oritur factor 23, at vero ex secundo et tertio colligitur alter factor 17; revera autem est $391 = 17 \cdot 23$.

4. Contemplemur etiam sequens exemplum non parum memorabile, quo $m = 5$ et $n = 3$, atque in formula $5\,xx + 3\,yy$ numerus 512 duplici modo continetur, cum sit primo

$$512 = 5 \cdot 1^2 + 3 \cdot 13^2$$

et

$$512 = 5 \cdot 4^2 + 3 \cdot 12^2,$$

unde fit $\frac{p}{q} = \frac{4 \pm 1}{13 \pm 12}$, cuius quatuor valores sunt

$$\text{I. } \frac{p}{q} = \frac{1}{5}; \quad \text{II. } \frac{p}{q} = \frac{5}{1}; \quad \text{III. } \frac{p}{q} = \frac{3}{25}; \quad \text{IV. } \frac{p}{q} = \frac{3}{1};$$

unde fractiones $\frac{r}{s}$ fient:

$$\text{I. } \frac{r}{s} = \frac{5 \cdot 1^2}{3 \cdot 5^2} = \frac{1}{15}; \qquad \text{II. } \frac{r}{s} = \frac{5 \cdot 5^2}{3 \cdot 1^2} = \frac{125}{3};$$

$$\text{III. } \frac{r}{s} = \frac{5 \cdot 3^2}{3 \cdot 25^2} = \frac{3}{125}; \qquad \text{IV. } \frac{r}{s} = \frac{5 \cdot 3^2}{3 \cdot 1^2} = \frac{15}{1};$$

ergo formula $\frac{r+s}{2}$ ex primo et quarto dat factorem 8, ex secundo vero et tertio factorem 64, quorum productum utique est 512.

5. Verum idem hic numerus 512 insuper duobus aliis modis in eadem formula $5xx + 3yy$ continetur; priori scilicet modo reperitur

$$512 = 5 \cdot 8^2 + 3 \cdot 8^2,$$

posteriori vero modo

$$512 = 5 \cdot 10^2 + 3 \cdot 2^2,$$

hinc ergo plures alios factores reperire licebit, id quod mirum non est, quia numerus 512 pluribus modis in duos factores resolvi potest. Veluti prima et

postrema resolutio dant $\frac{p}{q} = \frac{10 \pm 1}{13 \pm 2}$, unde hae quatuor emergunt fractiones:

$$\text{I. } \frac{p}{q} = \frac{11}{15}; \quad \text{II. } \frac{p}{q} = \frac{1}{1}; \quad \text{III. } \frac{p}{q} = \frac{3}{5}; \quad \text{IV. } \frac{p}{q} = \frac{9}{11};$$

unde pro $\frac{r}{s}$ sequentes orientur fractiones:

$$\text{I. } \frac{r}{s} = \frac{5 \cdot 11^2}{3 \cdot 15^2} = \frac{121}{135}; \quad \text{II. } \frac{r}{s} = \frac{5 \cdot 1^2}{3 \cdot 1^2} = \frac{5}{3};$$

$$\text{III. } \frac{r}{s} = \frac{5 \cdot 3^2}{3 \cdot 5^2} = \frac{3}{5}; \quad \text{IV. } \frac{r}{s} = \frac{5 \cdot 9^2}{3 \cdot 11^2} = \frac{135}{121};$$

unde factores ex $\frac{r+s}{2}$ oriundi erunt alter 128, alter vero 4, quorum productum utique est 512.

6. Cum igitur haec propositio sit certissima: *Quod omnes numeri plus uno modo in eadem formula* $mxx + nyy$ *contenti non sint primi sed compositi, ideoque numeri primi unico tantum modo in tali formula contineri queant*; contemplemur huius propositionis inversam, quae ita enunciabitur: *Quod omnes numeri compositi in formula* $mxx + nyy$ *contenti etiam plus uno modo in eadem contineantur, vel quod omnes numeri unico tantum modo in ista formula contenti certe sint primi.*

7. Statim autem patet hanc propositionem inversam in genere admitti non posse, cum innumerabiles casus exhiberi queant, quibus numeri valde compositi in talibus formulis unico tantum modo continentur. Ita si $m = 7$ et $n = 2$, in formula $7xx + 2yy$ iste numerus compositus 15 certe unico tantum modo continetur, scilicet quando $x = 1$ et $y = 2$. Quin etiam in eadem formula iste numerus compositus $1807 = 13 \cdot 139$ unico tantum modo contineri deprehenditur, scilicet quando $x = 1$ et $y = 30$. Ex quo manifesto apparet istam propositionem inversam, quod numeri unico tantum modo in tali formula $mxx + nyy$ contenti etiam sint numeri primi, in genere veritati non esse consentaneam.

8. Interim tamen plures casus pro binis numeris m et n ita sunt comparati, ut propositio illa inversa egregie cum veritate consentiat, inter quos

notissimus est casus, quo $m = 1$ et $n = 1$ et formula nostra summa duorum quadratorum $xx + yy$; siquidem iam rigorose est demonstratum omnes numeros, qui unico tantum modo sunt summae duorum quadratorum, semper etiam esse primos, dummodo fuerint impares, atque numeri x et y primi inter se, quae levis limitatio sponte sua patet. Atque hoc ipso principio iam olim sum usus ad numeros praegrandes examinandos, utrum sint primi necne[1]). Statim enim atque ostensum fuerit numerum quantumvis magnum (imparem) unico tantum modo esse summam duorum quadratorum, etiam certum est eum esse primum.

9. Eadem quoque indole praeditae sunt sequentes formulae simpliciores, veluti:

$$2xx + yy\,;\quad 3xx + yy\,;\quad 3xx + 2yy\,;\quad 5xx + yy\,;$$
$$5xx + 2yy\,;\quad 5xx + 3yy\,;\quad 6xx + yy\,;\quad 6xx + 5yy \text{ etc.},$$

de quarum plerisque a Geometris iam demonstratum, vel saltem observatum est, quod omnes numeri in quapiam earum unico tantum modo contenti etiam certe sint primi, si modo paucissimi casus, per se perspicui, excipiantur; scilicet quando numeri vel sunt pares, vel cum numeris m et n communem divisorem recipiunt. Quin etiam in certis formulis evenire potest, ut adeo potestates binarii unico modo contineantur, veluti numerus 8 in formula $5xx + 3yy$ et numerus 16 in formula $15xx + yy$, quibus ergo casibus potestates binarii numeris primis aequivalere sunt censendae, propterea quod non diversos factores involvunt.

10. Hinc igitur intelligimus in formula $mxx + nyy$ ingens intercedere discrimen, cum aliae ita sint comparatae, ut omnes numeri unico modo in iis contenti recte pro primis haberi queant, dum aliae hac insigni proprietate sunt destitutae, quemadmodum in formula $7xx + 2yy$ usu venire iam ante observavimus. Quam ob rem, cum istud discrimen non solum sit maximi momenti, sed etiam in ipsa natura harum formularum fundatum, plurimum conveniet duas talium formularum classes constituere atque a se invicem sollicite distinguere, quandoquidem hic nobis propositum est insignes atque adeo mirabiles proprietates prioris classis accuratius evolvere, quam ergo sequenti definitione determinemus.

1) Vide commentationem 699 indicis Enestroemiani huius voluminis p. 246. R. F.

DEFINITIO

Quando numeri m et n ita sunt comparati, ut omnes numeri unico modo in formula $mxx + nyy$ contenti sint vel ipsi primi vel tantum binarium vel quempiam factorem numerorum m et n involvant, vel etiam certis casibus sint potestates binarii, tales formulas in sequentibus formulas congruas appellabimus; ubi quidem per se perspicuum est ambos numeros x et y inter se primos accipi debere.

11. Hic igitur probe tenendum est numeros semel tantum in tali formula congrua $mxx + nyy$ contentos non statim pro primis esse habendos, propterea quod evenire potest, ut denotante p numerum primum quemcunque isti numeri etiam formam habeant vel $2p$ vel δp, existente δ divisore producti mn. Hic autem posterior casus penitus cessat, quando numerus x primus ad n, simulque y primus ad m accipiatur. Deinde vero etiam iam observavimus potestates quoque binarii unico tantum modo in certis formulis veluti $5xx + 3yy$ contineri posse, quae tamen formula nihilominus pro congrua est habenda, cum omnes numeri impares ad $3 \cdot 5 = 15$ primi et unico modo in hac formula contenti semper revera sint primi. Ita quia numerus 107 unico modo in ista formula continetur, sumendo scilicet $x = 4$ et $y = 3$, is recte pro primo haberi potest.

12. Quoniam igitur in hoc iudicio non solum numeri primi ipsi p sed etiam $2p$ et δp instar primorum spectari queant, denotante δ divisorem quempiam numeri mn, quibus adeo certis casibus etiam potestates binarii annumerare licet, vicissim sequitur omnes reliquos numeros, quos revera compositos vocemus, qui in tali formula congrua $mxx + nyy$ continentur, simul quoque plus quam uno modo in ea contineri debere. Veluti quia numerus $527 = 5 \cdot 10^2 + 3 \cdot 3^2$ non est primus, sed factoribus constat $17 \cdot 31$, is insuper alio modo in eadem formula continetur, scilicet est $527 = 5 \cdot 2^2 + 3 \cdot 13^2$, atque ex hac duplici resolutione per regulam supra datam factores numeri 527 sequenti modo eruuntur. Cum primo sit $\frac{p}{q} = \frac{10 \pm 2}{13 \pm 3}$, quaterni eius valores erunt

$$1^\circ.\ \frac{p}{q} = \frac{3}{4};\quad 2^\circ.\ \frac{p}{q} = \frac{6}{5};\quad 3^\circ.\ \frac{p}{q} = \frac{1}{2}\quad \text{et}\quad 4^\circ.\ \frac{p}{q} = \frac{4}{5};$$

unde porro altera fractio $\frac{r}{s} = \frac{mpp}{nqq}$ producit hos valores:

$$1°.\ \frac{r}{s} = \frac{15}{16};\quad 2°.\ \frac{r}{s} = \frac{12}{5};\quad 3°.\ \frac{r}{s} = \frac{5}{12}\quad \text{et}\quad 4°.\ \frac{r}{s} = \frac{16}{15};$$

unde aggregatum $r + s$ praebet duos factores 31 et 17.

13. Stabilita hac definitione formularum congruarum reliquas omnes hac insigni proprietate destitutas distinctionis gratia incongruas appellabimus easque hoc charactere designare licebit, quod etiam numeri revera compositi exhiberi queant, qui in talibus formulis unico tantum modo contineantur, veluti evenit in hac formula incongrua $7xx + 5yy$, in qua iste numerus compositus $273 = 3 \cdot 7 \cdot 13$ unico tantum modo continetur, scilicet quando $x = 2$ et $y = 7$.

14. Totum ergo negotium huc redit, ut regulam certam tradamus, cuius ope formulas congruas ab incongruis discernere liceat. Quoniam autem hic duo numeri m et n in considerationem sunt ducendi, universa haec quaestio ope sequentis theorematis ad considerationem unici numeri revocari potest.

THEOREMA

Si formula $mxx + nyy$ est congrua, tum etiam haec formula $mnxx + yy$ erit congrua, ac vicissim.

DEMONSTRATIO

15. Ponamus enim formulam $mxx + nyy$ esse congruam, alteram vero $mnxx + yy$ esse incongruam. Daretur igitur numerus revera compositus C unico tantum modo in hac formula contentus, qui sit $C = mnaa + bb$; hinc ergo foret $nC = mnnaa + nbb$ quoque unico modo, ideoque etiam unico modo in formula $mxx + nyy$ contineretur, existente scilicet $x = na$ et $y = b$; unde sequeretur formulam $mxx + nyy$ non esse congruam, contra hypothesin; unde necessario concludi oportet, quoties altera harum duarum formularum fuerit congrua, necessario quoque alteram futuram esse congruam.

16. Eodem modo etiam liquet, si altera harum formularum fuerit incongrua, etiam alteram talem esse futuram. Quare cum infra ostendetur hanc formulam $60xx + yy$ esse congruam, quoniam hic bini numeri m et n pluribus modis accipi possunt, haec sola formula congrua etiam sequentes omnes pariter congruas progignet:

$$30xx + 2yy\,; \quad 20xx + 3yy\,; \quad 15xx + 4yy\,; \quad 12xx + 5yy$$
$$\text{et tandem } 10xx + 6yy\,.$$

17. Hanc ob rem ad omnes formulas congruas constituendas sufficiet omnes valores producti mn assignasse, cum deinde ex factoribus huiusmodi producti facillime omnes plane formulae congruae derivari queant.

DEFINITIO

Omnes numeros, quos loco producti mn assumere licet, ut formulae $mxx + nyy$ evadant congruae, in posterum appellabimus numeros idoneos vel etiam congruos, dum reliquos omnes incongruos vocabimus.

18. Cum hoc idem argumentum iam nuper tractaverim, atque adeo omnes numeros idoneos sive congruos exhibuerim, primo quidem hoc phaenomenon maxime mirandum se obtulit, quod multitudo istorum numerorum neutiquam in infinitum excrescat, verum adeo non plures quam 65 huiusmodi numeros complectatur. Hos numeros, quoniam mihi propositum est plures proprietates eorum maxime memorabiles in medium afferre, ante omnia hic designemus.

CATALOGUS[1])
omnium numerorum idoneorum seu congruorum

1. 1	14. 16	27. 48	40. 120	53. 312
2. 2	15. 18	28. 57	41. 130	54. 330
3. 3	16. 21	29. 58	42. 133	55. 345
4. 4	17. 22	30. 60	43. 165	56. 357
5. 5	18. 24	31. 70	44. 168	57. 385
6. 6	19. 25	32. 72	45. 177	58. 408
7. 7	20. 28	33. 78	46. 190	59. 462
8. 8	21. 30	34. 85	47. 210	60. 520
9. 9	22. 33	35. 88	48. 232	61. 760
10. 10	23. 37	36. 93	49. 240	62. 840
11. 12	24. 40	37. 102	50. 253	63. 1320
12. 13	25. 42	38. 105	51. 273	64. 1365
13. 15	26. 45	39. 112	52. 280	65. 1848

1) Eulerus hunc catalogum indicavit in commentatione 498 (vide notam 1) p. 269, *Leonhardi Euleri Opera omnia*, series I, vol. 3, p. 419). Ibi numerus vicesimus sextus falsus est; loco 44 numerus 45 poni debet. Vide etiam p. 320 huius voluminis. Numeri eiusdem catalogi sunt determinantes formarum binariarum quadraticarum, qui possident unam modo classem in singulis generibus. Confer „Disquisitiones arithmeticae", Art. 303, C. Fr. Gauss Werke Bd. I, p. 366 et „Tafel der Anzahl der Classen binärer quadratischer Formen", ibidem Bd. II p. 450. R. F.

19. Maximus ergo numerus idoneus seu congruus est $1848 = 8 \cdot 3 \cdot 7 \cdot 11$, qui ergo felicissimo successu ad numeros primos explorandos adhiberi poterit. Si enim numerus quantumvis magnus N in forma $1848xx + yy$ contineatur, haud difficile erit investigare, utrum insuper alio modo in eadem formula contentus sit necne. Quodsi enim numerus N unico modo contineri reperiatur, atque numerus y non solum primus fuerit ad x, sed etiam ad ipsum 1848, tum tuto concludere licebit istum numerum N revera esse primum. Hoc modo nuper plures numeros primos, ad multos milliones exsurgentes, in medium protulimus, id quod multo minori labore praestari potuit, quam si, uti olim feci, summa binorum quadratorum ad hunc finem uti vellemus. Talem autem egregium usum reliqui omnes numeri idonei maiores huius tabulae praestabunt.

20. Antequam autem in proprietates maxime memorabiles horum numerorum congruorum sum inquisiturus, conveniet praecipua momenta, quibus hi numeri innituntur, breviter exponere, quae ternis sequentibus propositionibus complecti licet.

PROPOSITIO PRIMA

Nullus numerus minor quam $4mn$ plus uno modo in formula $mnxx + yy$ contineri potest, nisi forte fuerit quadratus; quia enim numerus minor supponitur quam $4mn$, excluso casu $x = 0$ pro numeris quadratis necessario esse debet $x = 1$, atque adeo iste numerus non nisi unico modo in hac formula contineri potest.

PROPOSITIO SECUNDA

Si numerus compositus, quantumvis magnus, unico tantum modo in formula $mnxx + yy$ contineatur, tum semper continuo multo minores numeri, pariter compositi, exhiberi possunt unico etiam modo in hac forma contenti, sicque tandem pervenietur ad numeros compositos minores quam $4mn$. Huius propositionis veritatem non ita pridem demonstravi[1]).

PROPOSITIO TERTIA

Si numerus mn ita fuerit comparatus, ut omnes numeri in formula $mn + yy$ contenti et minores quam $4mn$ sint vel primi vel primis aequipollentes, tum iste

1) Vide Commentationem 715 indicis Enestroemiani huius volumis p. 314. R. F.

numerus mn certe erit idoneus et formula mnxx + yy congrua. Quia enim nullus dabitur numerus compositus minor quam $4mn$ in ista formula contentus, etiam nulli dabuntur numeri compositi, quantumvis magni, unico quoque tantum modo in eadem formula contenti, sed omnes numeri unico tantum modo in ea contenti erunt vel primi vel tanquam primi spectandi.

21. Hinc facilis regula deducitur, cuius ope quoslibet numeros examinare licebit, utrum sint congrui necne. Proposito enim quocunque numero N in formula $N + yy$ loco y successive scribantur numeri 1, 2, 3, 4, 5 etc., donec perveniatur ad summam maiorem quam $4N$, atque si numeri hoc modo resultantes fuerint vel primi p vel etiam $2p$ vel δp (existente δ divisore numeri N) vel etiam potestates binarii, quibus adiungi oportet quadrata numerorum primorum, tum numerus iste N erit idoneus et formula $Nxx + yy$ congrua; sin autem hoc modo vel unicus numerus revera compositus occurrat, tum formula inter incongruas erit referenda.

22. Illustremus hanc regulam exemplo numeri 48, unde addendo quadrata usque ad limitem $y = 12$ orientur sequentes numeri vel primi vel ut primi spectandi:

$$\begin{array}{l|l}
48 + 1 = 49 = pp & 48 + 7^2 = 97 = p \\
48 + 2^2 = 52 = 4 \cdot 13 = \delta p & 48 + 8^2 = 112 = 16 \cdot 7 = \delta p \\
48 + 3^2 = 57 = 3 \cdot 19 = \delta p & 48 + 9^2 = 129 = 3 \cdot 43 = \delta p \\
48 + 4^2 = 64 = 16 \cdot 4 = 2^\lambda & 48 + 10^2 = 148 = 4 \cdot 37 = \delta p \\
48 + 5^2 = 73 = p & 48 + 11^2 = 169 = 13^2 = pp \\
48 + 6^2 = 84 = 12 \cdot 7 = \delta p &
\end{array}$$

Hinc ergo patet istum numerum utique esse idoneum, atque formulae, quae ex eo derivantur, simul erunt congruae, quae sunt $48xx + yy$ et $16xx + 3yy$, quandoquidem numeri pro m et n sumendi inter se debent esse primi.

23. Quamquam haec regula ad omnes casus facile accommodari potest, tamen etiam alia dari potest regula maxime memorabilis, qua vera indoles numerorum idoneorum multo magis declaratur, quae ita se habet:

REGULA CONDENDI TABULAM NUMERORUM IDONEORUM

24. *Ex serie omnium numerorum naturalium pro quolibet numero primo p excludantur numeri in hac forma contenti* $px - yy$, *maiores quam* $\frac{1}{4}pp$, *praeter hos* $pp - yy$; *quo facto pro singulis numeris primis p relin-*

quentur numeri idonei. Notetur autem hic loco numeri primi 2 *sumi debere eius quadratum* 4. 1ta I⁰ pro $p = 4$ excludi debent numeri formae $4x - 1 > 4$, praeter 15 et 7; numeri excludendi hinc erunt 11, 19, 23, 27, 31, 37 etc. 2⁰. Pro $p = 3$ excluduntur numeri $3x - 1$ maiores quam $\frac{9}{4}$, praeter 8 et 5; quare excludentur hi numeri: 11, 14, 17, 20, 23, 26 etc. 3⁰. Pro $p = 5$ excluduntur numeri formae $5x - 1$, -4 maiores quam $\frac{25}{4}$, praeter 24, 21, 16, 9; ergo excludendi sunt 14, 19, 29, 34, 39 etc. et 11, 26, 31, 36, 41 etc. 4⁰. Pro $p = 7$ excludi debent numeri formae $7x - 1$, -4, $-9 > \frac{49}{4}$, praeter 48, 45, 40, 33, 24, 13, unde numeri excludendi sunt 20, 27, 34 etc.; 17, 31, 38, 52, 59 etc.; 19, 26, 47, 54 etc. 5⁰. Pro $p = 11$ excluduntur numeri $11x - 1$, -4, -9, -16, $-25 > \frac{121}{4} > 30$, praeter 120, 117, 112, 105, 96, 85, 72, 57, 40, 21, sicque numeri excludendi erunt:

32,	43,	54,	65,	76,	87,	98,	109,	131,	142	etc.
51,	62,	73,	84,	95,	106,	128,	139,	150		etc.
35,	46,	68,	79,	90,	101,	123,	134,	145		etc.
39,	50,	61,	83,	94,	116,	127,	138,	149		etc.
41,	52,	63,	74,	107,	118,	129,	140,	151		etc.

hocque modo per omnes numeros primos est procedendum.

25. Quamquam haec regula aliis innititur principiis, atque non parum discrepare videtur a criterio, quo numeri isti idonei ab aliis numeris distinguuntur, tamen pulcherrimus consensus ubique deprehenditur. Praeterea vero etiam hi numeri tam egregiis proprietatibus sunt praediti, quas adeo ex principiis plurimum diversis demonstrare licet, unde operae pretium erit istas proprietates in sequentibus theorematibus ob oculos exposuisse.

THEOREMATA

quibus insignes proprietates numerorum idoneorum demonstrantur

THEOREMA 1

In ordine numerorum idoneorum alii numeri quadrati non occurrunt praeter 1, 4, 9, 16 *et* 25.

DEMONSTRATIO

26. Si numerus idoneus est quadratum ii, formula congrua $iixx + yy$ utique erit summa duorum quadratorum. Consideremus igitur numeros quoscunque compositos C, qui sint summae duorum quadratorum, quod cum semper duplici modo evenire queat, statuamus $C = aa + bb = cc + dd$, ac primo quidem fit a numerus par $= 2f$, ut sit $C = 4ff + bb$, ideoque b numerus impar[1]), cuius quadratum cum semper sit formae $4\alpha + 1$, etiam ipse numerus C eandem habebit formam; unde evidens est quadratorum cc et dd alterum par, alterum vero impar esse debere. Sit igitur $c = 2g$, eritque $C = 4gg + dd$; unde sequitur, si numerus compositus[2]) C fuerit $= 4ff + bb$, eum quoque alio modo fore $C = 4gg + dd$; ex quo manifestum est quadratum 4 esse numerum idoneum.

27. Ponamus nunc in eadem aequalitate $C = aa + bb = cc + dd$ numerum a esse multiplum ternarii, scilicet $a = 3f$, ut sit $C = 9ff + bb$; et quia b supponitur primus ad a ideoque non divisibilis per 3, eius quadratum bb habebit formam $3\alpha + 1$, unde etiam ipse numerus C eandem habebit formam $3\alpha + 1$. Hanc autem formam altera expressio $cc + dd$ habere nequit, nisi alterum quadratorum cc et dd divisibile sit per 3, alterum vero non; si enim ambo non essent divisibilia per 3, utrumque haberet formam $3\alpha + 1$, ideoque eorum summa formam esset habitura $3\alpha + 2$ diversam ab illa. Ponatur igitur $c = 3g$, ita ut sit $C = 9gg + dd$; unde patet, si numerus compositus habuerit formam $9ff + bb$, eum insuper alio modo fore $9gg + dd$. Necesse igitur est, ut quadratum 9 sit numerus idoneus.

28. Ponamus nunc esse $a = 4f$, ut sit $C = 16ff + bb$, atque demonstrandum est in altera forma $cc + dd$ vel c vel d etiam per 4 divisibile esse debere. Cum igitur numerus b sit impar, eius quadratum bb semper formam habet $8\alpha + 1$, eandemque ergo formam habebit numerus C, quam ergo formam quoque habere debet $cc + dd$; unde statim patet alterum quadratum dd esse impar, ideoque formae $8\alpha + 1$, alterum vero cc par, atque adeo per 16 divisibile, sive $c = 4g$, ideoque $C = 16gg + dd$. Quare cum, si fuerit numerus compositus $C = 16ff + bb$, necessario quoque fiat $C = 16gg + dd$, evidens est etiam quadratum 16 esse numerum idoneum.

1) si C numerus impar est. R. F.
2) impar. R. F.

29. Sit porro $a = 5f$, ideoque $C = 25ff + bb$; et quia b divisionem per 5 non admittit, eius quadratum bb formam habebit $5\alpha + 1$ vel $5\alpha + 4$, ideoque ipse numerus C alterutram formam habere debet, quam ergo eandem formam habere debet $cc + dd$; unde statim patet, si neque c neque d divisibile esset per 5, summa $cc + dd$ formam foret habitura vel $5\alpha + 0$ vel $5\alpha + 2$ vel $5\alpha + 3$, quarum nulla congruit; unde sequitur alterutrum numerorum c et d per 5 esse divisibilem. Sit igitur $c = 5g$, ideoque $C = 25gg + dd$; atque manifestum est, quoties numerus compositus C habuerit formam $25ff + bb$, semper insuper alio modo fore $C = 25gg + dd$, ideoque 25 esse numerum idoneum.

30. Tale autem ratiocinium non ulterius extendi potest. Si enim ponamus $a = 6f$, ut sit $C = 36ff + bb$, quadratum bb necessario formam habebit $6\alpha + 1$, quae ergo forma etiam ipsi C convenit; verum pro altera forma $cc + dd$ non absolute necesse est, ut sit $c = 6g$; eadem enim forma $6\alpha + 1$ resultare potest, sumendo $c = 2g$ et $d = 6h + 3$, ita ut horum numerorum alter per 2 alter vero per 3 sit divisibilis. Quia igitur g divisionem per 3 admittere non debet, eius quadratum formam habebit $3\alpha + 1$, ideoque cc formam $12\alpha + 4$, sive $6\alpha + 4$; alterum vero quadratum dd formam habet $6\alpha + 3$, quorum ergo quadratorum summa producit formam $6\alpha + 1$, perinde ut ante. Quocirca cum, si fuerit $C = 36ff + bb$, non necesse sit, ut etiam fiat $C = 36gg + dd$, hinc sequitur numerum 36 non esse numerum idoneum; quod etiam criterium primo datum declarat, quoniam $36 + 7^2 = 85 = 5 \cdot 17$, qui numerus revera est compositus et minor quam $4 \cdot 36$.

31. Quo hoc clarius appareat, consideremus casum $a = 7f$, ut sit $C = 49ff + bb$, ideoque b non divisibile per 7, unde forma ipsius bb erit $7\alpha + 1, 2, 4$, quod etiam de ipso numero C valet. Videamus igitur, num pro altera formula $cc + dd$ aliqua harum formarum resultare possit, etiamsi neque c neque d per 7 sumatur divisibile, quo ergo casu tam cc quam dd haberet formam vel $7\alpha + 1$ vel $7\alpha + 2$ vel $7\alpha + 4$, ideoque eorum summa ad has formas perducit $7\alpha + 1, 2, 3, 4, 5, 6$, hoc est omnes formas possibiles, in quibus superiores tres formae utique continentur. Quare cum neutiquam necesse sit, ut alter numerorum c et d etiam per 7 sit divisibilis, manifestum est etiam numerum 49 non esse idoneum; quod idem de numeris maioribus multo magis valebit, id quod etiam criterium nostrum manifesto declarat, cum sit $49 + 6^2 = 5 \cdot 17$, atque adeo $49 + 4^2 = 5 \cdot 13$.

THEOREMA 2

Si numerus idoneus fuerit formae $4\alpha - 1$, *tum etiam eius quadruplum* $4(4\alpha - 1)$ *erit numerus idoneus.*

DEMONSTRATIO

32. Sit brevitatis gratia $4\alpha - 1 = i$, ita ut pro quovis numero composito C sit

$$C = iaa + bb = icc + dd .$$

Iam ponamus esse $a = 2f$, ut prior forma evadat $C = 4iff + bb$, ubi ergo, ob b numerum imparem, quadratum bb habebit formam $4\alpha + 1$[1]). Quia nunc i est numerus impar, alteruter numerorum c et d erit par, alter impar, unde duos casus evolvi oportet. Sit primo $c = 2g$, et quia dd est formae $4\alpha + 1$, hoc utique congruit cum forma praecedente. Examinemus vero etiam alterum casum, quo $d = 2h$ at cc impar, ideoque formae $4\alpha + 1$; cum igitur sit $i = 4\alpha - 1$, numerus icc formam habebit $4\alpha - 1$, quae cum discrepet a forma priore $4iff + bb$, evidens est etiam numerum c parem esse debere. Sit igitur $c = 2g$, ut prodeat $C = 4igg + dd$, quam ob rem evictum est, si numerus compositus C formam habeat $4iff + bb$, necessario etiam alio modo proditurum esse $C = 4igg + dd$, sicque evictum est etiam numerum $4i$ esse idoneum, siquidem fuerit $i = 4\alpha - 1$ numerus idoneus.

COROLLARIUM

33. In tabula autem numerorum idoneorum supra allata alios numeros formae $4\alpha - 1$ non reperimus praeter 3, 7, 15, quorum etiam quadrupla 12, 28, 60 in eadem tabula reperiri videmus; quin etiam horum denuo quadrupla 48, 112, 240 etiam ibidem occurrunt, quemadmodum in sequente theoremate demonstrabimus.

THEOREMA 3

Denotante i *numerum imparem, si fuerit* $4i$ *numerus idoneus, tum etiam eius quadruplum* $16i$ *erit semper numerus idoneus.*

---

1) Eulerus litteram α duobus modis ibi et inde utitur. R. F.

DEMONSTRATIO

34. Cum $4i$ sit numerus idoneus, dabuntur numeri compositi C, ut sit $C = 4iaa + bb = 4icc + dd$, ubi ergo numeri b et d erunt impares, ideoque eorum quadrata formae $8\alpha + 1$. Ponamus iam esse $a = 2f$, ut sit $C = 16iff + bb$, qui numerus est formae $8\alpha + 1$. Quodsi iam c foret numerus impar, ob i numerum imparem, etiam icc erit impar, ideoque $4icc$ numerus formae $8\alpha + 4$, unde ob $dd = 8\alpha + 1$ forma posterior foret $8\alpha + 5$, cum prior esset $8\alpha + 1$; ex quo sequitur etiam numerum c necessario parem esse debere. Posito igitur $c = 2g$, erit utique

$$C = 16iff + bb = 16igg + dd,$$

unde manifesto sequitur numerum $16i$ quoque esse idoneum.

COROLLARIUM

35. Quando autem assumimus numerum $4i$ esse idoneum, necesse est, ut etiam ipse numerus i sit idoneus, id quod in sequente theoremate demonstrabitur.

THEOREMA 4

Si fuerit $\lambda\lambda i$ numerus idoneus, semper etiam ipse numerus i erit idoneus.

DEMONSTRATIO

36. Quia $\lambda\lambda i$ est numerus idoneus, dabuntur numeri compositi C, ut sit

$$C = \lambda\lambda iaa + bb = \lambda\lambda icc + dd;$$

ubi si ponamus $\lambda a = f$ et $\lambda c = g$, erit

$$C = iff + bb = igg + dd,$$

unde luculenter liquet etiam numerum i esse ideoneum. Quoties igitur quispiam numerus idoneus per quadratum fuerit divisibilis, etiam facta divisione quotus erit numerus idoneus.

THEOREMA 5

Si habeatur numerus idoneus formae $3\alpha - 1$, *etiam eius noncuplum semper erit numerus idoneus.*

DEMONSTRATIO

37. Posito brevitatis gratia $3\alpha - 1 = i$, ut habeamus talem aequationem:

$$C = iaa + bb = icc + dd ,$$

sumamus $a = 3f$, ut sit $C = 9iff + bb$, ubi ergo, quia b primus ad a, quadrati bb forma erit $3\alpha + 1$, ideoque ipse numerus C formae $3\alpha + 1$. Iam si in altera forma $icc + dd$ numerus c non esset divisibilis per 3, foret cc [formae] $3\alpha + 1$, ideoque icc formae $3\alpha - 1$. Nunc autem alter numerus d vel erit per 3 divisibilis vel secus; priore casu, ob dd [formae] 3α, posterior forma foret $3\alpha - 1$; posteriore casu forma prodiret 3α. Quare cum prior forma sit $C = 3\alpha + 1$, cui neutra harum convenit, necesse est, ut numerus c sit per 3 divisibilis. Posito ergo $c = 3g$, habebimus

$$C = 9iff + bb = 9igg + dd ;$$

unde manifestum est etiam numerum $9i$ esse idoneum, siquidem i fuerit numerus formae $3\alpha - 1$.

COROLLARIUM

38. In tabula autem numerorum idoneorum alii numeri formae $3\alpha - 1$ non occurrunt praeter hos tres: 2, 5, 8, quorum etiam noncupla 18, 45 et 72 in eadem tabula reperimus.

THEOREMA 6

Si numerus impar formae $4\alpha + 1$[1]) *fuerit numerus idoneus, tum eius quadruplum* $4(4\alpha + 1)$ *in tabula numerorum idoneorum occurrere nequit.*

---

1) $\alpha \neq 0$. Vide Corollarium § 40. R. F.

DEMONSTRATIO

39. Posito brevitatis gratia $4\alpha + 1 = i$ consideremus hanc aequalitatem:

$$C = iaa + bb = icc + dd\,,$$

ubi ponamus $a = 2f$, ut sit $C = 4iff + bb$. Iam nisi absolute necessarium sit, ut etiam c sit numerus par, numerus $4i$ non erit idoneus. Consideremus igitur casum, quo c numerus impar, eritque cc [formae] $4\alpha + 1$, ideoque icc formae $4\alpha + 1$; quare cum hoc casu d sit numerus par, posterior forma erit $4\alpha + 1$; unde patet necesse non esse, ut c sit numerus par, quod ipsum indicio est etiam numerum $4i$ non esse idoneum[1]).

COROLLARIUM

40. Numeri autem formae $4\alpha + 1$, qui in nostra tabula numerorum idoneorum occurrunt, sunt 1, 5, 9, 13, 21, 25, 33, 37, 45, 57, 85, 93, 105, 133, 165, 177, 253, 273, 345, 357, 385, 1365, quorum etiam nullius quadruplum in nostra tabula deprehendimus, praeter unitatis, cuius ratio est prorsus peculiaris.

THEOREMA 7

Si inter numeros idoneos occurrat numerus impariter par, sive formae $4\alpha + 2$, *tum etiam semper eius quadruplum* $4(4\alpha + 2)$ *in eadem tabula reperietur.*

DEMONSTRATIO

41. Ponatur brevitatis gratia $4\alpha + 2 = i$ et consideretur haec aequatio:

$$C = iaa + bb = icc + dd\,,$$

ac ponatur $a = 2f$, quo facto, si etiam c necessario debet esse numerus par, evictum erit numerum $4i$ esse idoneum. Hic vero ante omnia notandum, quia i est numerus par, numeros b et d esse impares, eorumque ergo quadrata formae $8\alpha + 1$, unde eorum differentia $bb - dd$ semper erit per octo divisibilis. Cum

1) Demonstratio non est rigorosa. R. F.

igitur sit $bb - dd = i(cc - 4ff)$, necesse est, ut hoc posterius membrum divisionem per 8 admittat; at vero prior factor i tantum per 2 dividi potest, unde patet alterum factorem $cc - 4ff$ divisibilem esse debere per 4, hincque sequitur numerum c necessario parem esse debere. Sit igitur $c = 2g$, ac si numerus compositus C habuerit formam $4iff + bb$, semper etiam alio modo erit $C = 4igg + dd$; unde manifesto sequitur etiam numerum $4i$ esse idoneum, siquidem numerus $i = 4\alpha + 2$ talis fuerit.

COROLLARIUM

42. Numeri autem impariter pares in tabula numerorum idoneorum occurrunt sequentes: 2, 6, 10, 18, 22, 30, 42, 58, 70, 78, 102, 130, 190, 210, 330, 462, quorum etiam singulorum quadrupla revera in tabula nostra reperiuntur.

THEOREMA 8

Denotante i numerum imparem, si fuerit $8i$ numerus idoneus, eius quadruplum $32i$ certe non erit numerus idoneus.

DEMONSTRATIO

43. Posito enim

$$C = 8iaa + bb = 8icc + dd,$$

si ponamus $a = 2f$, ut prior formula fiat $C = 32iff + bb$, videamus, num etiam necessario hinc sequatur numerum c quoque parem esse debere. Primo igitur notetur numeros b et d esse impares, ideoque differentiam quadratorum $bb - dd$ divisibilem per 8. Cum igitur sit

$$bb - dd = 8icc - 32iff = 8i(cc - 4ff),$$

quae forma sponte est divisibilis per 8, nulla necessitas adest, quod numerus c debeat esse par, consequenter etiam numerus 32 non erit idoneus[1]).

1) Demonstratio non est rigorosa. R. F.

COROLLARIUM

44. Quando numerus $8i$ est idoneus, tum etiam eius pars quarta $2i$ erit numerus idoneus. Ac si i denotet numerum imparem, modo ante vidimus etiam $8i$ esse numerum idoneum. Nunc autem intelligimus multiplicationem per 4 non ulterius locum habere posse, ita ut non solum $32i$, sed etiam $128i$ et $512i$ etc. ex ordine numerorum idoneorum excludantur.

THEOREMA 9

Denotante i numerum imparem, si fuerit $16i$ numerus idoneus, tum eius quadruplum $64i$ certe non erit numerus idoneus.

DEMONSTRATIO

45. Posito enim

$$C = 16iaa + bb = 16icc + dd\,,$$

si ponamus $a = 2f$, ob $bb - dd$ divisibile per 8, etiam forma $16i(cc - 4ff)$ per 8 divisibilis esse debet, quod cum sponte eveniat, nulla necessitas urget, ut etiam numerus c par accipi debeat; ex quo sequitur numerum $64i$ nunquam esse posse numerum idoneum[1]).

COROLLARIUM

46. Quando hic assumimus numerum $16i$ esse idoneum, per se intelligitur etiam $4i$ et i esse numerum idoneum, quare cum multiplicatio per 4 ulterius locum non habeat, ex binis postremis theorematibus conficitur nullos plane dari numeros idoneos, qui per altiorem binarii potestatem quam quartam essent divisibiles. Vidimus autem tres tantum dari tales numeros per 16 divisibiles, scilicet 48, 112 et 240; nulli autem prorsus dantur, qui per 32 vel 64 vel altiorem potestatem essent divisibiles.

THEOREMA 10

Si i fuerit numerus idoneus formae cuiuscunque, sitque $i + aa = pp$, existente p numero primo, tum eius quadruplum $4i$ ex tabula numerorum idoneorum excluditur, existente $pp < 4i$.

---

1) Demonstratio non est rigorosa. R. F.

DEMONSTRATIO

47. Quoniam $i + aa = pp$, erit $4i + 4aa = 4pp$. At si $4i$ esset numerus idoneus, tum forma $4i + xx$ esse deberet vel numerus primus vel eius duplum vel quadratum, siquidem x fuerit primus ad $4i$[1]). Iam sumatur $x = 2a - p$, qui certe ad $4i$ est primus[2]), ac prodit

$$4i + xx = 4i + 4aa - 4ap + pp,$$

quae forma, ob $4i + 4aa = 4pp$, transit in hanc:

$$4i + xx = 5pp - 4ap = p(5p - 4a),$$

quod cum non sit numerus primus, neque duplum, neque quadratum primi, evidens est numerum $4i$ idoneum non esse.

SCHOLION

48. Quemadmodum igitur initio demonstravimus in tabula numerorum idoneorum nullos alios quadratos occurrere praeter 1, 4, 9, 16 et 25, ita ex demonstrationibus sequentibus concludere possumus ex hac tabula omnes excludi numeros divisibiles per quadratos 3^2, 4^2, 5^2, 7^2, 11^2 etc. praeter paucos illos in tabula relatos, scilicet nulli occurrunt ibi numeri per 16 divisibiles, praeter 16, 48, 112 et 240; tum vero nulli per 9 divisibiles praeter 9, 18, 45 et 72; at vero per 25 solus ipse numerus 25 adest; maiora autem quadrata penitus ex ista tabula excluduntur, non solum ipsa, sed ne quidem factores esse possunt ullius numeri idonei. Interim tamen, quod in ista tabula omnes plane numeri idonei occurrant eorumque numerus non ultra 65 exsurgat, rigida demonstratio etiamnunc desideratur. Quia autem usque ad decies mille nulli alii se mihi obtulerunt, multo magis verisimillimum videtur, post hunc terminum nullos praeterea existere; id quod eo magis est notatu dignum, quod nulla adhuc in Analysi talis numerorum series occurrit, quae finito tantum terminorum numero constaret.

---

1) et xx minor quam $12i$. R. F.

2) Numerus 3 exceptionem praebet. Ponatur $i = 24$, $a = 5$, $p = 7$, ubi $7^2 < 4 \cdot 24$, x erit 3, qui certe non est primus ad $4i = 4 \cdot 24$. R. F.

INVESTIGATIO TRIANGULI IN QUO DISTANTIAE ANGULORUM AB EIUS CENTRO GRAVITATIS RATIONALITER EXPRIMANTUR

Commentatio 713 indicis Enestroemiani

Nova acta academiae scientiarum Petropolitanae 12 (1794), 1801, p. 101—113

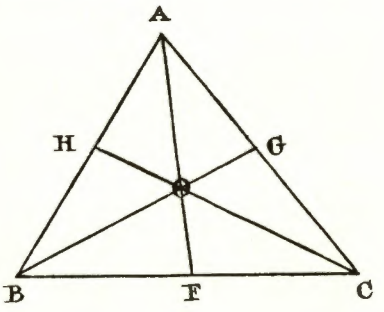
Summarium ibidem p. 68—69

Conventui exhibita die 17. Decembris 1778

SUMMARIUM

Ce Mémoire qui fera plaisir au petit nombre d'Amateurs de l'Analyse indéterminée contient une très belle solution du problème énoncé dans le titre; la voici en peu de mots: Soyent les côtés du triangle cherché $2a$, $2b$, $2c$, et les droites tirées de leurs milieux vers les angles opposés respectivement f, g, h. Prenez à volonté deux nombres q et r et cherchez $M = \frac{5qq-rr}{4qq}$ et $N = \frac{5rr-9qq}{4rr}$. Réduisez la fraction $\frac{(M-N)^2-4}{4(M+N)}$ à ses moindres termes et nommez le numérateur x et le dénominateur y, et vous aurez le côté $2a = 2qx + (M-N)qy$, et la ligne $f = rx - \frac{1}{2}(M-N)ry$. Faites $p = x + y$ et $s = x - y$, et vous aurez les côtés $2b = pr - qs$ et $2c = pr + qs$, et les lignes $g = \frac{3pq+rs}{2}$ et $h = \frac{3pq-rs}{2}$.

1. Cum centrum gravitatis trianguli reperiatur in intersectione ternarum rectarum AF, BG et CH, quae ex singulis angulis ductae latera opposita bisecant, illud erit in puncto O, ubi illae tres rectae ita se secant, ut sit $AO = \frac{2}{3}AF$, $BO = \frac{2}{3}BG$ et $CO = \frac{2}{3}CH$. Quoniam igitur requiritur, ut distantiae AO, BO



et CO rationaliter exprimantur, hoc eveniet, si totae rectae AF, BG et CH fuerint rationales, siquidem latera triangula per numeros rationales repraesententur.

2. Ponamus igitur $BF = CF = a$, $CG = AG = b$, $AH = BH = c$; praeterea vero vocemus $AF = f$, $BG = g$ et $CH = h$, ac perpendamus, quomodo istae tres lineae f, g, h per illas a, b, c exprimantur. Hunc in finem vocemus angulum $AFB = \omega$, et ex triangulo ABF habebimus hanc aequalitatem

$$AB^2 = AF^2 + BF^2 - 2AF \cdot BF \cos. \omega ,$$

at ex triangulo ACF habebimus

$$AC^2 = AF^2 + CF^2 + 2AF \cdot CF \cos. \omega ,$$

quae duae aequalitates additae praebent

$$AB^2 + AC^2 = 2AF^2 + 2BF^2$$

sive

$$4cc + 4bb = 2ff + 2aa ,$$

unde colligitur

$$ff = 2cc + 2bb - aa .$$

Simili modo erit

$$gg = 2aa + 2cc - bb \quad \text{et} \quad hh = 2aa + 2bb - cc ,$$

quocirca pro litteris a, b, c eiusmodi numeros quaeri oportet, ut istae tres formulae reddantur numeri quadrati.

3. Antequam hanc investigationem suscipiamus, consideremus casum maxime memorabilem, quo $bb + cc = 2aa$; tum enim erit $ff = 3aa$ sive $f = a\sqrt{3}$, tum vero $gg = 3cc$ sive $g = c\sqrt{3}$, et $hh = 3bb$ sive $h = b\sqrt{3}$, quae est insignis proprietas huiusmodi triangulorum, in quibus $2aa = bb + cc$.

4. Praeterea in genere observemus esse

$$ff + gg + hh = 3(aa + bb + cc).$$

Cum igitur sit $AO = \frac{2}{3}f$, multiplicando per $\frac{4}{9}$ erit

$$AO^2 + BO^2 + CO^2 = \frac{4}{3}(aa + bb + cc),$$

sicque patet semper esse

$$AO^2 + BO^2 + CO^2 = \frac{1}{3}(BC^2 + AC^2 + AB^2),$$

quae proprietas est etiam maxime notatu digna.

5. Videamus nunc, quemadmodum formulae inventae ad quadrata revocari queant, ac si incipiamus a prima $ff = 2cc + 2bb - aa$, non tam facile patet, quomodo quadratum obtineri queat; at si sub hac specie repraesentetur: $ff = (b + c)^2 + (b - c)^2 - aa$, tum secundum praecepta Analyseos statui poterit

$$f = b + c + \frac{p}{q}(b - c + a),$$

qua substitutione facta habebimus

$$(b + c)^2 + \frac{2p}{q}(b + c)(b - c + a) + \frac{pp}{qq}(b - c + a)^2 = (b + c)^2 + (b - c)^2 - aa,$$

ubi sublatis membris prioribus, posterioribus vero per factorem communem $b - c + a$ divisis orietur

$$\frac{2p}{q}(b + c) + \frac{pp}{qq}(b - c + a) = b - c - a,$$

unde commode definitur

$$a = \frac{(b - c)(qq - pp) - 2pq(b + c)}{pp + qq}.$$

Quodsi ergo litterae a iste valor tribuatur, littera quidem f rationaliter exprimetur; erit enim

$$f = \frac{(b+c)(qq-pp)+2pq(b-c)}{pp+qq};$$

at si istum valorem ipsius a in binis reliquis formulis substituere vellemus, in calculos nimis complicatos ac propemodum inextricabiles delaberemur; quam ob rem alio modo solutionem tentare convenit.

6. Iunctim contemplemur binas posteriores conditiones, quae sunt

$$gg = 2aa + 2cc - bb \quad \text{et} \quad hh = 2aa + 2bb - cc,$$

quarum differentia dat $gg - hh = 3(cc - bb)$; unde cum omnia in numeris integris desiderentur, si $cc - bb$ alios factores non haberet, praeter $c + b$ et $c - b$, statui deberet $g + h = 3(c + b)$ et $g - h = c - b$ vel $g + h = c + b$ et $g - h = 3(c - b)$. Verum ex illa positione sequeretur

$$g = 2c + b \quad \text{et} \quad h = c + 2b,$$

ex posteriore vero

$$g = 2c - b \quad \text{et} \quad h = 2b - c.$$

Hae autem binae determinationes inter se conveniunt; nam quia in formulis principalibus tantum quadrata bb et cc occurrunt, perinde est, sive litterae b et c positive sive negative accipiantur.

7. Quodsi vero loco $g = 2c + b$ hunc valorem substituamus, in aequatione $gg = 2aa + 2cc - bb$ prodit $2aa = 2bb + 2cc + 4bc$, sive $aa = (b+c)^2$, ideoque $a = b + c$. Hoc ergo casu in triangulo proposito summa duorum laterum aequalis foret tertio lateri, ideoque tria puncta A, B, C in rectam caderent, neque ergo amplius foret triangulum, sicque ista solutio penitus est reiicienda.

8. Quoniam haec solutio inde est nata, quod posuimus formulam $cc - bb$ alios factores non admittere praeter $c + b$ et $c - b$, necesse est, ut ista formula insuper alios involvat factores. Ponamus igitur esse $cc - bb = pqrs$, fierique debebit $gg - hh = 3pqrs$, unde statuatur $g + h = 3pq$ et $g - h = rs$, unde fit

$$g = \frac{3pq + rs}{2} \quad \text{et} \quad h = \frac{3pq - rs}{2};$$

ex formula vero $cc - bb = pqrs$ sumamus

$$c + b = pr \quad \text{et} \quad c - b = qs .$$

Hoc autem modo tantum differentiae binarum formularum satisfecimus $gg - hh$ et $cc - bb$, unde insuper aliae seorsim foret satisfaciendum, eodem autem redit, si insuper summae satisfiat. Cum igitur sit

$$gg + hh = 4aa + bb + cc ,$$

substitutio valorum inventorum facillime efficitur; erit enim

$$2gg + 2hh = 9ppqq + rrss ,$$

similique modo erit

$$2cc + 2bb = pprr + qqss ,$$

unde aequatio conficienda fit

$$9ppqq + rrss = 8aa + pprr + qqss ,$$

ideoque fiet

$$8aa = pp(9qq - rr) + ss(rr - qq) ,$$

ergo

$$16aa = 2pp(9qq - rr) + 2ss(rr - qq) ,$$

quam ergo formulam ad quadratum reduci oportet; quod si fuerit praestitum, duabus formulis posterioribus penitus erit satisfactum, sicque tantum supererit primae conditioni $ff = 2cc + 2bb - aa$ satisfieri.

9. Cum igitur esse debeat

$$16ff = 32cc + 32bb - 16aa ,$$

ob $2cc + 2bb = pprr + qqss$ nanciscemur hanc aequationem:

$$16ff = 16pprr + 16qqss - 2pp(9qq - rr) - 2ss(rr - qq) ,$$

sive

$$16ff = 18pp\,(rr - qq) + 2ss\,(9qq - rr)\,,$$

hoc ergo modo insuper requiritur, ut sequentes duae formulae quadrata efficiantur, quae sunt

$$16aa = 2pp\,(9qq - rr) + 2ss\,(rr - qq)$$

et

$$16ff = 18pp\,(rr - qq) + 2ss\,(9qq - rr)\,.$$

10. Quo harum formularum resolutio facilior reddatur, ponamus $p = x + y$ et $s = x - y$; tum enim conditiones implendae erunt:

I. $4aa = 4qq\,(xx + yy) + 2xy\,(5qq - rr)$ et
II. $4ff = 4rr\,(xx + yy) + 2xy\,(5rr - 9qq)\,.$

11. Quo has formulas tractabiliores reddamus, statuamus brevitatis gratia

$$\frac{5qq - rr}{4qq} = M \quad \text{et} \quad \frac{5rr - 9qq}{4rr} = N\,,$$

ac binae aequationes tractandae erunt

$$\frac{aa}{qq} = xx + yy + 2Mxy \quad \text{et} \quad \frac{ff}{rr} = xx + yy + 2Nxy\,.$$

Ecce ergo resolvendae adhuc supersunt duae formulae inter se simillimae et ita comparatae, ut utramque seorsim facillime resolvere liceat.

12. Utramque resolutionem simul suscipiamus statuendo

$$\frac{a}{q} = x + ty \quad \text{et} \quad \frac{f}{r} = x + uy\,,$$

hocque modo prodibunt sequentes formae:

$$2tx + tty = y + 2Mx \quad \text{et} \quad 2ux + uuy = y + 2Nx\,,$$

unde duplici modo nanciscimur

$$\frac{x}{y} = \frac{1 - tt}{2(t - M)} = \frac{1 - uu}{2(u - N)}\,.$$

Hos ergo duos valores inter se congruentes reddi oportet; quem in finem primo numeratores aequales statuantur, id quod duplici modo fieri potest, statuendo vel $u = t$ vel $u = -t$; priori autem casu denominatores aequales fieri nequeunt, nisi fuerit $M = N$, id quod fieri nequit. Sumamus ergo $u = -t$, ac denominatorum aequalitas praebet $u = \frac{N-M}{2} = -t$, unde fit $\frac{x}{y} = \frac{(M-N)^2-4}{4(M+N)}$, hocque modo iam omnibus conditionibus erit satisfactum. Interim tamen probe notari oportet hanc solutionem tantum esse particularem, propterea quod binae fractiones pro $\frac{x}{y}$ inventae infinitis aliis modis aequales fieri possent, etiamsi neque numeratores neque denominatores aequales statuantur. Quoniam autem alii modi ad calculos nimis perplexos perducerent, hac solutione eo magis poterimus esse contenti, quod nihilominus innumerabiles solutiones suppeditat.

13. Solutio igitur problematis propositi ita se habebit.

1°. Binae litterae q et r penitus arbitrio nostro relinquuntur, quibus igitur pro lubitu sumtis erit

$$M = \frac{5qq - rr}{4qq} \quad \text{et} \quad N = \frac{5rr - 9qq}{4rr}.$$

2°. His litteris inventis capiantur

$$x = (M - N)^2 - 4 \quad \text{et} \quad y = 4(M + N),$$

sive postquam fractio $\frac{(M-N)^2-4}{4(M+N)}$ ad minimos terminos fuerit reducta, numerator pro x, denominator vero pro y accipiatur.

3°. Deinde vero erit

$$\frac{a}{q} = x + ty = \frac{2x + (M-N)y}{2},$$

ideoque $a = qx + \frac{1}{2}(M - N)qy$; similique modo erit

$$\frac{f}{r} = x - ty = x - \frac{(M-N)y}{2},$$

ideoque $f = rx - \frac{1}{2}(M - N)ry$.

4°. Cum sit $p = x + y$ et $s = x - y$, habebitur $b + c = pr$ et $c - b = qs$, ideoque

$$c = \frac{pr + qs}{2} \quad \text{et} \quad b = \frac{pr - qs}{2},$$

sicque omnia tria latera trianguli erunt definita, quippe quae erunt

$$2a = 2qx + (M - N)qy,$$
$$2b = pr - qs \quad \text{et} \quad 2c = pr + qs.$$

5°. Denique vero ob $g + h = 3pq$ et $g - h = rs$ erit

$$g = \frac{3pq + rs}{2} \quad \text{et} \quad h = \frac{3pq - rs}{2}.$$

14. Iam innuimus binas litteras q et r, seu potius earum relationem, arbitrio nostro esse relictam; ubi primum observandum occurrit, si sumeretur $q = r$, ob $M = 1$ et $N = -1$ fieri $M + N = 0$, ideoque et $y = 0$, unde nulla solutio idonea nascitur. Idem incommodum oritur, si fuerit $r = 3q$, siquidem inde fit $M = -1$ et $N = 1$, ideoque iterum $M + N = 0$. Hanc ob rem, ut casum definitum evolvamus, eumque simplicissimum, sumamus $q = 2$ et $r = 1$, unde fit $M = \frac{19}{16}$ et $N = -\frac{31}{4}$. Sin autem sumeremus $q = 1$ et $r = 2$, tum fieret $M = \frac{1}{4}$ et $N = \frac{11}{16}$, quae posterior solutio cum sit simplicior, hunc casum data opera evolvamus.

EVOLUTIO CASUS
QUO $q = 1$ ET $r = 2$

15. Hoc ergo casu erit $M = \frac{1}{4} = \frac{4}{16}$ et $N = \frac{11}{16}$, ideoque $M + N = \frac{15}{16}$ et $M - N = -\frac{7}{16}$, unde fit $\frac{x}{y} = -\frac{65}{64}$, quocirca sumamus $x = -65$ et $y = 64$. Hinc erit porro $a = -79$ et $f = -102$ sive $a = 79$ et $f = 102$. Deinde autem erit $p = -1$ et $s = -129$, unde colligitur $c + b = -2$ et $c - b = -129$, ideoque $c = -\frac{131}{2}$ et $b = \frac{127}{2}$. Denique $g + h = -3$ et $g - h = -258$, ideoque $g = -\frac{261}{2}$ et $h = +\frac{255}{2}$.

16. Solutio ergo huius casus ita se habebit, postquam ubique per 2 fuerit multiplicatum: $a = 158$, $b = 127$, $c = 131$, $f = 204$, $g = 261$ et $h = 255$. Ubi plurimum observasse iuvabit hinc adeo aliam solutionem in minoribus numeris derivari posse; nam quia numeri f, g et h per 3 dividi possunt, eorum trientes loco litterarum a, b et c accipi poterunt, tum autem praecedentes litterae a, b, c dabunt valores pro f, g et h, ita ut hoc observato nanciscamur istam solutionem simpliciorem:

$$\begin{aligned} a &= 68, \quad b = 87, \quad c = 85, \\ f &= 158, \quad g = 127, \quad h = 131, \end{aligned}$$

id quod sequenti modo ostendi potest.

17. Cum spectatis litteris a, b et c tanquam datis alterae f, g et h ita determinari sunt inventae, ut esset

$$\begin{aligned} f &= \sqrt{(2bb + 2cc - aa)}, \\ g &= \sqrt{(2aa + 2cc - bb)}, \\ h &= \sqrt{(2aa + 2bb - cc)}, \end{aligned}$$

hinc sequitur fore

$$\begin{aligned} ff + gg + hh &= 3aa + 3bb + 3cc, \text{ hincque} \\ 2ff + 2gg + 2hh &= 6aa + 6bb + 6cc. \end{aligned}$$

Subtrahatur primo $3ff = 6bb + 6cc - 3aa$, ac prodibit

$$2gg + 2hh - ff = 9aa,$$

ita ut sit

$$3a = \sqrt{(2gg + 2hh - ff)}.$$

Eodemque modo reperietur

$$\begin{aligned} 3b &= \sqrt{(2hh + 2ff - gg)} \quad \text{et} \\ 3c &= \sqrt{(2gg + 2ff - hh)}. \end{aligned}$$

18. Quoniam igitur litterae $3a$, $3b$ et $3c$ eodem modo per f, g et h determinantur, quo ante invenimus litteras f, g et h per a, b et c determinari, con-

sideremus aliud triangulum, ad quod referantur simili modo gemini litterarum ordines a', b' et c' atque f', g' et h', ac si fuerit $a' = f$, $b' = g$ et $c' = h$, erit

$$f' = \sqrt{(2b'b' + 2c'c' - a'a')} = \sqrt{(2gg + 2hh - ff)} = 3a,$$
$$\text{ideoque } f' = 3a.$$

Eodemque modo prodibit $g' = 3b$ et $h' = 3c$, sicque ex triangulo, ad quod referuntur litterae a, b, c et f, g, h, semper aliud triangulum derivari potest, cui respondeant litterae a', b', c' et f', g', h'; si capiatur $a' = f$, $b' = g$ et $c' = h$, tum erit $f' = 3a$, $g' = 3b$ et $h' = 3c$; quod est theorema maxime notatu dignum.

19. Hinc igitur patet, si ex triangulo ante invento aliud formetur, in quo sit $a' = \frac{1}{3}f$, $b' = \frac{1}{3}g$ et $c' = \frac{1}{3}h$, tum fore $f' = a$, $g' = b$ et $h' = c$; unde prodit alterum triangulum supra exhibitum, quod pro simplicissima solutione nostri problematis merito haberi potest. Ante autem quam alia exempla percurramus, plurimum iuvabit solutionem generalem accuratius evolvere et ad calculum accommodare.

ACCURATIOR EVOLUTIO SOLUTIONIS GENERALIS

20. In solutione brevitatis gratia posuimus

$$M = \frac{5qq - rr}{4qq} \quad \text{et} \quad N = \frac{5rr - 9qq}{4rr},$$

postquam posuissemus $g + h = 3pq$ et $g - h = rs$, tum vero $c + b = pr$ et $c - b = qs$, unde invenimus

$$\frac{x}{y} = \frac{(M-N)^2 - 4}{4(M+N)},$$
$$\frac{a}{q} = x + \frac{1}{2}(M-N)y \quad \text{et}$$
$$\frac{f}{r} = x - \frac{1}{2}(M-N)y,$$

quibus valoribus inventis reliquae litterae omnes determinantur. Nunc primo loco M et N valores assumtos substituamus, atque impetrabimus:

$$1°.\ M-N=\frac{9q^4-r^4}{4qqrr}=\frac{(3qq+rr)(3qq-rr)}{4qqrr};$$

deinde vero erit

$$2°.\ M+N=\frac{10qqrr-r^4-9q^4}{4qqrr}=\frac{(9qq-rr)(rr-qq)}{4qqrr}.$$

Iam pro fractionis $\frac{x}{y}$ numeratore $(M-N)^2-4$ habebimus eius factores

$$M-N+2=\frac{9q^4-r^4+8qqrr}{4qqrr}=\frac{(9qq-rr)(rr+qq)}{4qqrr}$$

et

$$M-N-2=\frac{9q^4-r^4-8qqrr}{4qqrr}=\frac{(9qq+rr)(qq-rr)}{4qqrr},$$

unde totus numerator erit

$$(M-N)^2-4=\frac{(qq+rr)(qq-rr)(9qq+rr)(9qq-rr)}{16q^4r^4},$$

at vero denominator est

$$4(M+N)=\frac{10qqrr-r^4-9q^4}{qqrr}=\frac{(9qq-rr)(rr-qq)}{qqrr},$$

quibus inventis erit

$$\frac{x}{y}=-\frac{(qq+rr)(9qq+rr)}{16qqrr}.$$

21. Quia haec fractio ulteriorem reductionem in genere non admittit, sumamus

$$x=(qq+rr)(9qq+rr)\quad\text{et}\quad y=-16qqrr,$$

hinc iam porro ob $\frac{1}{2}(M-N)=\frac{(3qq+rr)(3qq-rr)}{8qqrr}$ reperiemus

$$\frac{a}{q}=-9q^4+10qqrr+3r^4=(qq+rr)(9qq+rr)-2(3qq+rr)(3qq-rr),$$

$$\frac{f}{r}=27q^4+10qqrr-r^4=(qq+rr)(9qq+rr)+2(3qq+rr)(3qq-rr),$$

quibus valoribus inventis ob

$$p=x+y=(qq+rr)(9qq+rr)-16qqrr=9q^4-6qqrr+r^4\ \text{et}$$
$$s=x-y=(qq+rr)(9qq+rr)+16qqrr=9q^4+26qqrr+r^4$$

prodit $c + b = pr$, $c - b = qs$, $g + h = 3pq$ et $g - h = rs$. Ex litteris ergo q et r pro lubitu assumtis omnes sex valores a, b, c et f, g, h facile eliciuntur.

EXEMPLUM 1
QUO $q = 1$ ET $r = 3$

22. Quia iam supra observavimus sumendo $q = r$ nullum reperiri triangulum, sed bina latera tertio esse aequalia, sumamus $q = 1$ et $r = 3$ prodibitque $a = 324$ et $f = 108$. Porro erit $p = 36$ et $s = 324$, hincque porro erit $c = 216$ et $b = 108$. Deinde $g = 540$ et $h = 432$, qui valores ergo sunt: $a = 324$, $b = 108$, $c = 216$, $f = 108$, $g = 540$ et $h = 432$; qui per 108 depressi abeunt in hos valores: $a = 3$, $b = 1$, $c = 2$, $f = 1$, $g = 5$ et $h = 4$; quae solutio pariter locum habere nequit, quia [summa] duorum laterum tertio reperitur aequalis.

EXEMPLUM 2
QUO $q = 2$ ET $r = 1$

23. Hic igitur erit $qq + rr = 5$ et $9qq + rr = 37$, unde colligitur $a = 202$ et $f = 471$. Deinde fit $p = 121$ et $s = 249$, hinc porro $c = \frac{619}{2}$ et $b = \frac{377}{2}$. Denique $g = \frac{975}{2}$ et $h = \frac{477}{2}$. His igitur valoribus duplicatis habebimus $a = 404$, $b = 377$, $c = 619$, $f = 942$, $g = 975$ et $h = 477$.

EXEMPLUM 3
QUO $q = 2$ ET $r = 3$

24. Hic ergo erit $qq + rr = 13$ et $9qq + rr = 45$, unde colligitur $\frac{a}{2} = 459$ et $\frac{f}{3} = 711$, porro vero $p = 9$ et $s = 1161$. Ex his fit $c = \frac{2349}{2}$ et $b = \frac{2295}{2}$, denique $g = \frac{3537}{2}$ et $h = \frac{3429}{2}$.

25. Hic ergo valores duplicati et[1]) per communem factorem 27 divisi praebent hanc solutionem: $a = 68$, $b = 85$, $c = 87$, $f = 158$, $g = 131$ et

1) Editio princeps: „per communem factorem 9 divisi praebent hanc solutionem: $a = 204$; $b = 255$ et $c = 261$; $f = 474$; $g = 393$ et $h = 381$; ubi cum numeri f, g, h divisibiles sint per 3, per theorema supra allatum orietur sequens nova solutio". A. M.

$h = 127$. Haec ergo solutio idem praebet triangulum, quod ex primo casu, quo $q = 1$ et $r = 2$, demum ope theorematis sumus nacti.

EXEMPLUM 4
QUO $q = 3$ ET $r = 5$

26. Hic ergo erit $qq + rr = 34$ et $9qq + rr = 106$, unde fit $\frac{a}{3} = 34 \cdot 106 - 4 \cdot 52 = 3396$ et $\frac{f}{5} = 3812$, porro $p = 4$ et $s = 7204$, hinc $c = 10816$ et $b = 10796$, deinde $g = 18028$ et $h = 17992$.

27. Triangulum igitur hoc exemplo inventum, quoniam singuli valores factorem habent 4, sequentibus numeris continetur: $a = 2547$, $b = 2699$, $c = 2704$, $f = 4765$, $g = 4507$ et $h = 4498$. Hinc iam satis liquet, quomodo quotcunque huiusmodi triangula exhiberi queant, quibus conditiones praescriptae adimpleantur.

DE VARIIS MODIS NUMEROS PRAEGRANDES EXAMINANDI UTRUM SINT PRIMI NECNE[1)]

Commentatio 715 indicis Enestroemiani

Nova acta academiae scientiarum Petropolitanae 13 (1795/6), 1802, p. 14—44

Summarium ibidem p. 54—56

Conventui exhibita die 16. martii 1778

SUMMARIUM

Les diverses méthodes que l'auteur donne dans ce mémoire, pour examiner de très grands nombres, s'ils sont premiers ou non, sont fondées sur la propriété: que si un nombre N est de deux manières de la forme $\alpha xx + \beta yy$, il n'est pas premier. L'examen qui fait proprement le sujet de ce mémoire est précédé de la démonstration de différens théorèmes sur la nature des nombres, qui, sans être d'un usage immédiat, ne laissent pas d'être dans une étroite liaison avec cette matière. Ces théorèmes sont:

Si $N = \alpha a^2 + \beta b^2$ et $N = \alpha A^2 + \beta B^2$:

1. Les nombres $aB + Ab$ et $aB - Ab$, après les avoir divisés par les nombres qui ne peuvent pas être facteurs de N, donneront les deux facteurs de ce nombre N.

2. Les nombres $\alpha aA + \beta bB$ et $\alpha aA - \beta bB$ auront avec le nombre N un commun diviseur.

3. Le nombre $\alpha p^2 + \beta q^2$, après avoir été divisé ou par α, ou par β, ou par $\alpha\beta$, ou par une puissance quelconque de 2, contiendra toujours un facteur du nombre N, où $p = a \pm A$ et $q = b \pm B$.

4. Le produit de deux nombres de la même forme $\alpha xx + \beta yy$ est toujours de la forme $\alpha\beta xx + yy$.

5. Le produit de deux nombres, dont l'un est de la forme $\alpha x^2 + \beta y^2$ et l'autre de la forme $\alpha\beta x^2 + y^2$, sera toujours de la forme $\alpha x^2 + \beta y^2$.

1) Vide Commentationem 708 indicis Enestroemiani huius voluminis p. 269. R. F.

6. Si un nombre non-premier est d'une seule façon de la forme $\alpha x^2 + \beta y^2$, on pourra assigner d'autres nombres non-premiers plus petits qui seront aussi d'une seule façon de la forme $\alpha x^2 + \beta y^2$.

7. Si un nombre non-premier, quelque grand qu'il soit, est d'une seule façon de la forme $\alpha\beta x^2 + y^2$, on pourra assigner d'autres nombres composés plus petits qui seront aussi d'une seule façon de cette forme $\alpha\beta x^2 + y^2$.

De la dernière proposition résulte, que si aucun nombre non-premier, moindre que $4\alpha\beta$, n'est contenu dans la forme $\alpha\beta x^2 + y^2$, aucun nombre non-premier plus grand que $4\alpha\beta$ ne sera contenu non plus dans cette forme. Desorte que tout nombre qui est d'une seule façon de la forme $\alpha\beta x^2 + y^2$ sera premier. La même chose n'est pas vraye de la forme $\alpha x^2 + \beta y^2$, à moins qu'on ne donne à α et β certaines valeurs que l'auteur appelle nombres convenables (*numeri idonei*) et c'est à la recherche de ces nombres qu'il s'occupe dans le reste de ce mémoire. Il en trouve, par des raisonnements qu'il seroit trop long de suivre 65 pareils nombres convenables qui le mettent en état d'examiner tout nombre, quelque grand qu'il soit, s'il est premier ou non.

1. Cum nimis molestum et operosum esset hoc examen per principia vulgaria instituere, dum scilicet divisio tentetur per omnes numeros primos radice quadrata numeri propositi minores, plurimum intererit eiusmodi methodos tradere, quarum ope hoc negotium multo facilius et brevius expediri queat. Tales autem methodi innituntur potissimum sequenti propositioni:

Si numerus N duplici modo contineatur in tali formula: $\alpha xx + \beta yy$, ubi α et β sunt numeri dati quicunque[1]*, tum certum est illum numerum N non esse primum, atque adeo eius divisores facile investigare poterunt.*

2. Ponamus igitur numerum quemcunque propositum N duplici modo in hac formula $\alpha xx + \beta yy$ contineri, ac primo quidem esse $N = \alpha aa + \beta bb$, tum vero etiam $N = \alpha AA + \beta BB$. Iam a priori aequatione per BB multiplicata auferatur altera per bb multiplicata, ut obtineatur haec aequatio: $N(BB - bb) = \alpha(aaBB - AAbb)$, quae per factores ita referri potest:

$$N(B + b)(B - b) = \alpha(aB + Ab)(aB - Ab),$$

unde satis patet numerum N primum esse non posse, sed certe communem factorem habere, tam cum formula $aB + Ab$ quam cum formula $aB - Ab$, quandoquidem istae formulae diversae sunt a prioribus $B + b$ et $B - b$.

1) Numeri α, β inter se primi assumuntur. R. F.

3. Quo haec conclusio clarius perspiciatur, eam aliquot exemplis illustremus. Sit scilicet $N = 77$, qui numerus duplici modo in forma $5xx + 2yy$ continetur; primo enim est

$$N = 5 \cdot 1^2 + 2 \cdot 6^2, \text{ tum vero etiam } N = 5 \cdot 3^2 + 2 \cdot 4^2 ,$$

sicque habebimus $a = 1$, $b = 6$, $A = 3$ et $B = 4$, hincque $aB + Ab = 22$, cum quo numero numerus propositus N factorem habet communem 11. Altera formula fit $aB - Ab = -14$, cum quo numero numerus N factorem communem habet 7. Sicque iam nacti sumus factores numeri propositi N, qui sunt 7 et 11.

4. Sit numerus propositus 703, qui duplici modo in forma $7xx + 3yy$ continetur; primo enim est

$$N = 7 \cdot 2^2 + 3 \cdot 15^2, \text{ tum vero est etiam } N = 7 \cdot 10^2 + 3 \cdot 1^2 .$$

Prior formula dat 152, cuius numeri cum 703 maximus communis divisor est 19; at vero numerus 703 cum altera formula — 148 divisorem habet communem 37. Est vero utique $703 = 19 \cdot 37$. Hoc etiam inde facilius patet, quod sit $152 = 8 \cdot 19$, unde, quia 8 nullum factorem ipsius 703 continet, necesse est, ut 19 eius sit factor. Simili modo, cum $148 = 4 \cdot 37$, ob eandem rationem necesse est, ut 37 sit factor numeri 703.

5. Consideremus numerum maiorem 12091 duplici modo in forma $7xx + 11yy$ contentum. Hic cum sit

1°) $12091 = 7 \cdot 40^2 + 11 \cdot 9^2$, tum vero etiam 2°) $12091 = 7 \cdot 4^2 + 11 \cdot 33^2$,

hinc forma examinanda $40 \cdot 33 \pm 4 \cdot 9$, quae per 12 divisa dat 110 ± 3. Nunc autem est 113 primus, ideoque factor numeri propositi; deinde etiam 107 pariter est primus, propterea etiam factor; revera autem est $12091 = 113 \cdot 107$.

THEOREMA 1

Si fuerit tam $N = \alpha a^2 + \beta b^2$ *quam* $N = \alpha A^2 + \beta B^2$, *tum formulae* $aB + Ab$ *et* $aB - Ab$ *praebent factores numeri N, postquam scilicet per numeros, qui factores esse nequeunt ipsius N, fuerint divisae.*

6. Possunt vero etiam ex binis resolutionibus supra exhibitis numeri N aliis modis factores investigari, scilicet a priori ducta in αA^2 subtrahatur posterior ducta in βbb, ut prodeat

$$N(\alpha A^2 - \beta b^2) = (\alpha\alpha a^2 A^2 - \beta\beta b^2 B^2)$$
$$= (\alpha aA + \beta bB)(\alpha aA - \beta bB),$$

unde patet ambas has formulas factores continere numeri N, id quod per superiora exempla etiam illustremus.

7. In exemplo § 3 erat

$$77 = 5 \cdot 1^2 + 2 \cdot 6^2 \quad \text{et} \quad 77 = 5 \cdot 3^2 + 2 \cdot 4^2,$$

unde colligitur forma $5 \cdot 1 \cdot 3 \pm 2 \cdot 6 \cdot 4$, quae per 3 depressa fit $5 \cdot 1 \pm 4 \cdot 4$. Hinc oriuntur isti duo numeri 21 et 11, quorum prior per 3 divisus dat 7.

Exemplum § 4 allatum erat

$$703 = 7 \cdot 2^2 + 3 \cdot 15^2 \quad \text{et} \quad 703 = 7 \cdot 10^2 + 3 \cdot 1^2,$$

unde forma oritur $7 \cdot 2 \cdot 10 \pm 3 \cdot 1 \cdot 15$, quae per 5 depressa dat 28 ± 9, ideoque tam 37 quam 19 sunt factores numeri propositi 703 supra inventi.

Tertium exemplum § 5 erat

$$12091 = 7 \cdot 40^2 + 11 \cdot 9^2 \quad \text{et} \quad 12091 = 7 \cdot 4^2 + 11 \cdot 33^2,$$

unde oritur haec formula: $7 \cdot 40 \cdot 4 \pm 11 \cdot 9 \cdot 33$, ex qua pro signo superiori oritur 4387, qui numerus cum numero proposito divisorem habet communem 107. Deinde pro signo inferiori fit 2147, qui cum numero proposito divisorem habet communem 113, ut ante.

THEOREMA 2

Si fuerit tam $N = \alpha a^2 + \beta b^2$ *quam* $N = \alpha A^2 + \beta B^2$, *tum etiam tam ista formula* $\alpha aA + \beta bB$ *quam* $\alpha aA - \beta bB$ *cum numero proposito* N *communem habebit divisorem, unde eius factores innotescent.*

8. Hinc autem deducuntur aliae formulae imprimis memorabiles, quae cum ipso numero N communes habebunt factores. Additis enim binis illis formulis, ut habeatur

$$2N = \alpha(a^2 + A^2) + \beta(b^2 + B^2),$$

huc addatur formula ante inventa bis sumpta $2\alpha aA \pm 2\beta bB$, vel etiam subtrahatur; quoniam enim cum ipso numero N communem habet factorem, idem factor communis in membro dextro contineri debebit. Hoc modo obtinebitur

$$2N \pm 2\alpha aA \pm 2\beta bB = \alpha(a \pm A)^2 + \beta(b \pm B)^2,$$

quae forma ideo est notabilis, quia ipsi formae propositae est similis, et quia quatuor variationes in illa locum habent, totidemque modis etiam factores numeri propositi assignari poterunt.

9. Quodsi ambae formulae $a \pm A$ et $b \pm B$ habeant factorem communem, quoniam is in N contineri nequit, eum statim e medio tolli conveniet. Veluti si haec fractio $\frac{a \pm A}{b \pm B}$ reducatur ad hanc formam simplicissimam $\frac{p}{q}$, tum ista formula $\alpha pp + \beta qq$ factorem numeri propositi praebebit, quippe qui erit communis divisor huius ipsius formulae cum numero proposito N.

10. Illustremus etiam hanc methodum per exempla supra allata, in quorum primo erat

$$77 = 5 \cdot 1^2 + 2 \cdot 6^2 \quad \text{et} \quad 77 = 5 \cdot 3^2 + 2 \cdot 4^2,$$

unde formetur fractio $\frac{p}{q} = \frac{3 \pm 1}{6 \pm 4}$, atque formula $5pp + 2qq$ dabit divisorem ipsius 77. Hinc autem erit

1°) $\frac{p}{q} = \frac{2}{5}$, tum vero formula $5 \cdot 4 + 2 \cdot 25$, per 10 depressa, dat $2 + 5 = 7$.

2°) fit $\frac{p}{q} = 2$, hincque $20 + 2 = 2 \cdot 11$.

3°) fit $\frac{p}{q} = \frac{1}{5}$, hincque formula $5 \cdot 1 + 2 \cdot 25$, per 5 depressa, dat $1 + 2 \cdot 5 = 11$. Tandem erit

4°) $\frac{p}{q} = 1$ et formula $5 \cdot 1 + 2 \cdot 1 = 7$.

11. Simili modo pro secundo exemplo, quo erat

$$703 = 7\cdot 2^2 + 3\cdot 15^2 \quad \text{et} \quad 703 = 7\cdot 10^2 + 3\cdot 1^2,$$

habebimus $\frac{p}{q} = \frac{10 \pm 2}{15 \pm 1}$, et formula $7pp + 3qq$ dabit factorem numeri 703. Hinc fit

1°) $\frac{p}{q} = \frac{3}{4}$, et factor $7\cdot 9 + 3\cdot 16$, per ternarium depressus, erit $7\cdot 3 + 16 = 37$. Porro

2°) fit $\frac{p}{q} = \frac{6}{7}$, et formula $7\cdot 36 + 3\cdot 49$, per $7\cdot 3$ depressa, dat factorem 19. Iam

3°) fit $\frac{p}{q} = \frac{1}{2}$, unde formula $7\cdot 1 + 3\cdot 4$ dat factorem 19. Tandem

4°) fiet $\frac{p}{q} = \frac{4}{7}$, unde formula $7\cdot 16 + 3\cdot 49$, per 7 depressa, praebet factorem 37.

12. Tertium denique exemplum erat

$$12091 = 7\cdot 40^2 + 11\cdot 9^2 \quad \text{et} \quad 12091 = 7\cdot 4^2 + 11\cdot 33^2,$$

ex quo fit $\frac{p}{q} = \frac{40 \pm 4}{33 \pm 9}$, et formula $7pp + 11qq$ dabit:

1°) $\frac{p}{q} = \frac{22}{21}$, hinc formula $7\cdot 22^2 + 11\cdot 21^2$, per $7\cdot 11$ depressa, dabit factorem 107. Erit

2°) $\frac{p}{q} = \frac{11}{6}$, hinc forma $7\cdot 11^2 + 11\cdot 6^2$, per 11 depressa, dat factorem 113. Porro fit

3°) $\frac{p}{q} = \frac{6}{7}$, hinc formula $7\cdot 6^2 + 11\cdot 7^2$, per 7 depressa, praebet factorem 113. Tandem erit

4°) $\frac{p}{q} = \frac{3}{2}$, unde formula $7\cdot 3^2 + 11\cdot 2^2$ statim dat factorem 107.

THEOREMA 3

Si fuerit tam $N = \alpha a^2 + \beta b^2$ *quam* $N = \alpha A^2 + \beta B^2$, *hincque formetur fractio* $\frac{p}{q} = \frac{a \pm A}{b \pm B}$, *tum ista formula* $\alpha pp + \beta qq$ *semper continebit factorem numeri propositi* N, *qui scilicet vel ipse se prodit vel facta divisione sive per* α *sive per* β *sive per* $\alpha\beta$, *quandoque etiam per alium numerum simplicissimum* 2 *eiusve potestatem.*

DEMONSTRATIO

13. Cum sit $\alpha a^2 + \beta b^2 = \alpha A^2 + \beta B^2$, erit

$$\alpha (aa - AA) = \beta (BB - bb),$$

hincque

$$\frac{a+A}{B+b} = \frac{\beta(B-b)}{\alpha(a-A)}.$$

Sit nunc $\frac{p}{q}$ fractio simplicissima huic utrique formulae aequalis, ac pro priore ponatur

$$a + A = mp \quad \text{et} \quad B + b = mq,$$

pro posteriore vero sit

$$\beta (B - b) = \alpha\beta np \quad \text{et} \quad \alpha(a - A) = \alpha\beta nq,$$

unde ergo fiet

$$B - b = \alpha np \quad \text{et} \quad a - A = \beta nq \text{ [1]}.$$

Ex his quatuor aequalitatibus definiantur numeri a, A et b, B, qui erunt

$$a = \frac{mp + \beta nq}{2}, \quad A = \frac{mp - \beta nq}{2}, \quad B = \frac{mq + \alpha np}{2} \quad \text{et} \quad b = \frac{mq - \alpha np}{2}.$$

Cum nunc sit $N = \alpha aa + \beta bb$, reperietur facta substitutione

$$N = \tfrac{1}{4}\alpha (mp + \beta nq)^2 + \tfrac{1}{4}\beta (mq - \alpha np)^2$$

sive per factores

$$N = \tfrac{1}{4}\alpha (mmpp + \beta\beta nnqq) + \tfrac{1}{4}\beta (mmqq + \alpha\alpha nnpp),$$

quae forma reducitur ad hoc productum:

1) n non est numerus integer; confer exemplum § 10. R. F.

$$\tfrac{1}{4}(mm + \alpha\beta nn)(\alpha pp + \beta qq) .$$

Unde patet formulam $\alpha pp + \beta qq$ continere divisorem numeri N, simul vero etiam patet quotum hinc ortum esse formae $mm + \alpha\beta nn$.

14. Evidens autem est in hac demonstratione litteras α et β supponi positivas; si enim altera esset negativa, evenire posset, ut factor inventus $\alpha pp + \beta qq$ abiret in unitatem, id quod unico exemplo ostendisse sufficiet, quo est $7 = 2 \cdot 8^2 - 1 \cdot 11^2$ et $7 = 2 \cdot 22^2 - 1 \cdot 31^2$. Hic ergo est $N = 7$, ideoque numerus primus; tum vero $\alpha = 2$, $\beta = 1$, $a = 8$, $b = 11$, $A = 22$ et $B = 31$, unde fit $\frac{p}{q} = \frac{22 \pm 8}{31 \pm 11}$, ita ut quatuor fractiones hinc ortae sint:

$$1°)\ \frac{p}{q} = \frac{5}{7}, \quad 2°)\ \frac{p}{q} = \frac{3}{2}, \quad 3°)\ \frac{p}{q} = \frac{1}{3} \quad \text{et} \quad 4°)\ \frac{p}{q} = \frac{7}{10},$$

ergo formulae $2pp - qq$ valores erunt 1°) 1, 2°) 14, qui prostremus, per 2 depressus, dat 7, 3°) — 7 et 4°) — 2, qui postremus redigitur ad 1. Evidens autem est litteras a et A, b et B pro lubitu tam positive quam negative accipi posse.

THEOREMA 4

Si duo numeri M et N eiusdem formae $\alpha xx + \beta yy$ in se invicem multiplicentur, productum MN semper erit formae $a\beta xx + yy$, idque duplici modo.

DEMONSTRATIO

15. Si enim ponamus

$$M = \alpha pp + \beta qq \quad \text{et} \quad N = \alpha rr + \beta ss ,$$

tum facta multiplicatione reperitur

$$MN = \alpha\alpha pprr + \beta\beta qqss + \alpha\beta ppss + \alpha\beta qqrr ,$$

quod productum manifesto reducitur ad hanc formam:

$$MN = \alpha\beta(ps \pm qr)^2 + (\alpha pr \mp \beta qs)^2 ,$$

hoc est ad formam $\alpha\beta xx + yy$, existente $x = ps \pm qr$ et $y = \alpha pr \mp \beta qs$, unde simul patet hanc resolutionem semper duplici modo fieri posse.

THEOREMA 5

Si duo numeri M et N, quorum alter M sit formae $\alpha xx + \beta yy$, *alter vero N formae* $\alpha\beta xx + yy$, *in se invicem ducantur, productum MN semper erit formae* $\alpha xx + \beta yy$, *idque duplici modo.*

DEMONSTRATIO

16. Si enim ponamus

$$M = \alpha pp + \beta qq \quad \text{et} \quad N = \alpha\beta rr + ss\,,$$

facta multiplicatione reperitur

$$MN = \alpha\alpha\beta pprr + \beta qqss + \alpha\beta\beta qqrr + \alpha ppss\,,$$

quod productum manifesto reducitur ad hanc formam:

$$MN = \alpha(\beta qr \pm ps)^2 + \beta(\alpha pr \mp qs)^2\,,$$

ideoque est formae $\alpha xx + \beta yy$, existente $x = \beta qr \pm ps$ et $y = \alpha pr \mp qs$, quae ergo resolutio, ob signa ambigua, semper duplici modo institui potest.

17. Hic animadvertisse iuvabit binas formulas $\alpha xx + \beta yy$ et $\alpha\beta xx + yy$ arctissimo vinculo inter se esse coniunctas; quod etiam inde patet, quod alteram in alteram facillime convertere liceat. Si enim in priore formula ponatur $x = \beta z$, ea abit in $\beta(\alpha\beta zz + yy)$; ac in altera si ponatur $y = \alpha v$, tum ea accipiet hanc formam: $\alpha(\beta xx + \alpha vv)$. Infra autem multo clarius patebit ambas istas formulas paribus proprietatibus esse praeditas, ita ut, quod de una demonstrabitur, id etiam de altera locum habere queat.

18. Cum igitur demonstratum sit omnes numeros, qui duplici modo in tali forma $\alpha xx + \beta yy$ continentur, certe non esse primos atque adeo eorum factores semper assignari posse, nunc quaestio maximi momenti se offert, num omnes numeri, qui unico tantum modo in tali formula continentur, etiam semper pro primis haberi queant? Hoc autem pendet a natura formulae $\alpha xx + \beta yy$, sive a numeris α et β, quorum duo genera constitui debent. Dantur enim eiusmodi valores pro his litteris, ut omnes numeri, qui unico modo in tali formula continentur, certe futuri sint primi; praeterea vero etiam dantur eiusmodi valores pro α et β, ubi talis conclusio falleret, cuiusmodi est haec formula $7xx + 2yy$, quae sumpto $x = 1$ et $y = 2$ dat numerum compositum 15, qui tamen unico tantum modo in hac formula continetur.

19. Cum igitur nobis sit propositum hinc methodum certam deducere numeros praemagnos examinandi, utrum sint primi necne, manifestum est ad hunc scopum formulas tantum prioris generis $\alpha xx + \beta yy$ adhiberi posse, de quibus scilicet certi sumus omnes numeros, qui in iis unico tantum modo contineantur, etiam revera esse primos. Hanc ob rem nobis ante omnia in certa criteria inquirere iuvabit, quibus tales formulae dignosci queant a formulis posterioris generis, in quibus etiam numeri compositi unico tantum modo contineri possunt, quas ergo formulas ab hoc instituto penitus excludi oportet; quam ob rem accuratius discrimen inter has duplicis generis formulas perscrutari conveniet.

THEOREMA 6

Si in formula $\alpha xx + \beta yy$ unico modo contineatur numerus compositus mp, existente $m > 2$[1]), tunc etiam innumerabiles alii eiusmodi numeri compositi exhiberi possunt, qui etiam unico tantum modo in hac formula contineantur.

DEMONSTRATIO

20. Hic ante omnia probe tenendum est non solum numeros α et β inter se primos esse debere, sed etiam numeros x et y inter se primos esse accipiendos, atque adeo ita, ut insuper numerus x primus sit ad β, et y ad α; quibus notatis patet etiam factores m et p ad quatuor numeros α, β, x et y primos esse futuros.

Ponamus igitur esse

$$mp = \alpha aa + \beta bb\,,$$

ac primum observo pluribus modis aliud productum mq exhiberi posse, quod unico modo in formula affini $\alpha\beta xx + yy$ contineatur. Sit enim

$$mq = \alpha\beta dd + cc\,,$$

ut hinc fiat

$$\beta ddmp - aamq = \beta\beta bbdd - aacc\,,$$

ideoque

$$m(\beta ddp - aaq) = (\beta bd + ac)\,(\beta bd - ac)\,,$$

unde si numeri d et c ita accipiantur, ut vel $\beta bd + ac$ vel $\beta bd - ac$ per m fiat divisibilis, tum hinc etiam valores idonei pro q reperientur. Sit enim $\beta bd + ac = \delta m$, erit

1) p semper > 2 poni debet. R. F.

$$\beta ddp - aaq = \delta(\beta bd - ac),$$

ideoque

$$q = \frac{\beta ddp - \delta(\beta bd - ac)}{aa},$$

unde sufficiet minimum valorem ipsius q accipere, ita ut certi esse queamus numerum mq unico modo in formula $\alpha\beta xx + yy$ contineri; quod vel inde patet, si sumpto $a = 1$ et $d = 1$ fuerit $mp = \alpha + \beta bb$, tum vero q ita sumatur, ut sit $mq < 4\alpha\beta$. Tum enim evidens est productum mq plus uno modo in formula $\alpha\beta xx + yy$ certe non contineri, quia sumpto $x = 2$ haec formula iam habitura esset valorem maiorem.

21. Ducantur nunc in se invicem binae illae formulae, ac reperietur

$$mmpq = \alpha(aacc + \beta\beta bbdd) + \beta(bbcc + \alpha\alpha aadd),$$

quae forma transformari potest in hanc:

$$mmpq = \alpha(ac \pm \beta bd)^2 + \beta(bc \mp \alpha ad)^2,$$

unde per mm dividendo colligitur

$$pq = \alpha\left(\frac{ac \pm \beta bd}{m}\right)^2 + \beta\left(\frac{bc \mp \alpha ad}{m}\right)^2,$$

ubi quidem signa ambigua duplicem resolutionem innuere videntur; verum hic probe observandum est alteram tantum in numeris fractis subsistere, ideoque a nostro instituto esse removendam. Si enim signa superiora praebeant numeros integros, inferiora dabunt fractiones; nam si summa duorum numerorum $A + B$ per m fuerit divisibilis, neque vero numeri A et B seorsim hanc divisionem admittant, tum certe differentia $A - B$ non erit divisibilis, solo casu excepto quo $m = 2$.

22. Cum igitur productum pq unico modo in integris (de quibus solis hic agitur) in formula $\alpha xx + \beta yy$ contineatur, simili modo ex hoc producto pq alia nova producta derivari poterunt, quae pariter unico tantum modo in nostra formula contineantur[1]).

1) Haec demonstratio et sequentes non sunt rigorosae. R. F.

THEOREMA 7

Quodsi productum quantumvis magnum pq unico tantum modo in formula $\alpha xx + \beta yy$ contineatur, tunc etiam minora huiusmodi producta exhiberi poterunt, quae pariter unico tantum modo contineantur.

DEMONSTRATIO

23. Ponamus enim esse $pq = \alpha ff + \beta gg$, atque haec forma comparetur cum modo ante inventa

$$\alpha\left(\frac{ac \pm \beta bd}{m}\right)^2 + \beta\left(\frac{bc \mp \alpha ad}{m}\right)^2,$$

ubi quidem signa superiora tantum valeant, hincque deducemus

$$f = \frac{ac + \beta bd}{m} \quad \text{et} \quad g = \frac{bc - \alpha ad}{m},$$

ex quibus duabus aequationibus semper pluribus modis quatuor litterae a, b, c et d definiri poterunt, unde igitur eum modum eligi conveniet, qui pro m minimum producat valorem, qui quidem semper maior erit quam 2.

24. Ex his duabus formis deducatur primo fractio $\frac{f}{g} = \frac{ac + \beta bd}{bc - \alpha ad}$, unde derivetur fractio $\frac{c}{d} = \frac{\alpha af + \beta bg}{fb - ag}$. Hic iam pro litteris a et b eiusmodi valores quaerantur, ut numerator et denominator huius fractionis minimum acquirat divisorem communem, hincque numeri c et d ad minimos valores reducantur.

25. Hoc autem sequenti modo haud difficulter praestari poterit. Ponamus Δ esse minimum communem divisorem harum duarum formularum: I. $\alpha af + \beta bg$ et II. $bf - ag$, eritque etiam Δ huius formulae inde formatae $a(\alpha ff + \beta gg)$ minimus divisor; hincque patet pro Δ sumi posse factorem quendam formae $\alpha ff + \beta gg$; unde cum huius formulae factores sint p et q, sumatur $\Delta = p$, et fractio nostra statim per Δ deprimi poterit, unde porro etiam numeri c et d innotescent, quibus inventis sponte se prodit numerus $m = \frac{ac + \beta bd}{f}$.

26. Plurimum iuvabit hoc exemplo illustrare formulae $7xx + 2yy$, ita ut sit $\alpha = 7$ et $\beta = 2$, in qua formula istud productum $59 \cdot 131 = 7729$ unico modo continetur, scilicet si $x = 19$ et $y = 51$. Habemus igitur $p = 59$, $q = 131$, $f = 19$ et $g = 51$, unde deducetur fractio

$$\frac{c}{d} = \frac{7 \cdot 19a + 2 \cdot 51b}{19b - 51a}.$$

27. Nunc a et b ita accipi poterunt, ut communis divisor numeratoris ac denominatoris evadat $\Delta = 59$; atque adeo sufficit soli denominatori hunc divisorem dedisse. Ponamus igitur $19b - 51a = 59n$, eritque $19b = 59n + 51a$, consequenter $b = 3a + 3n + \frac{2n - 6a}{19}$. Ponatur nunc $\frac{n - 3a}{19} = A$, ut sit $b = 3a + 3n + 2A$, et cum inde fiat $n - 3a = 19A$, erit $3a = n - 19A$, ideoque $a = -6A + \frac{n - A}{3}$. Ponatur porro $\frac{n - A}{3} = B$, erit $A = n - 3B$, ideoque $a = -6n + 19B$ ac denique $b = -13n + 51B$.

28. Ut iam litterae a et b quam minimae reddantur, sumatur $B = 0$ et $n = -1$, et denominator evadet $= -59$; tum erit $a = 6$ et $b = 13$, unde fiet nostra fractio $\frac{c}{d} = \frac{6 \cdot 7 \cdot 19 + 2 \cdot 13 \cdot 51}{-59} = -\frac{2124}{59} = -36$, ideoque $c = 36$ et $d = -1$, unde reperitur $m = 10$.

29. Nunc igitur nacti sumus novum productum minus $mp = 10 \cdot 59$, quod etiam in nostra forma $7xx + 2yy$ continetur, quae si fuerit $7ff + 2gg$, erit $f = 6$ et $g = 13$. Erit igitur $\frac{f}{g} = \frac{6}{13} = \frac{ac + 2bd}{bc - 7ad}$, unde reperitur $\frac{c}{d} = \frac{7 \cdot 6a + 2 \cdot 13b}{6b - 13a}$. Sumantur nunc a et b ita, ut denominator $6b - 13a$ divisorem admittat 10, quod fit sumto $a = 2$ et $b = 6$; fiet enim $\frac{c}{d} = 24$, ideoque $c = 24$ et $d = 1$, unde fit $m = 10$, ut ante, ideoque $7aa + 2bb = 10 \cdot 10$.

30. En ergo novum productum $10 \cdot 10$, pro quo fit $f = 2$ et $g = 6$. Statuatur igitur $\frac{f}{g} = \frac{2}{6} = \frac{ac + 2bd}{bc - 7ad}$, unde reperitur $\frac{c}{d} = \frac{7 \cdot 2a + 2 \cdot 6b}{2b - 6a} = \frac{7a + 6b}{b - 3a}$. Sumatur ergo $a = -2$ et $b = 4$, qui numeri, per 2 depressi, dant $a = -1$ et $b = 2$ hincque $\frac{c}{d} = 1$ ideoque $c = 1$ et $d = 1$, ex quo reperitur $m = 3$, unde fit $7aa + 2bb = 3 \cdot 5$, quod sine dubio est minimum productum.

ALIA DEMONSTRATIO EIUSDEM THEOREMATIS

31. Cum productum pq unico modo in forma illa $\alpha xx + \beta yy$ contineatur, sit $pq = \alpha ff + \beta gg$, atque evidens est factores p et q non in eadem forma contineri, quia alioquin productum duplicem resolutionem admitteret. Consideretur nunc factor minor, qui sit q, atque formula generalis $\alpha xx + \beta yy$ infinitis modis per q divisibilis fieri potest, sumendo $x = nf \pm \mu q$ et $y = ng \pm \nu q$. Prodibit enim

$$\alpha(nnff \pm 2\mu nfq + \mu\mu qq) + \beta(nngg \pm 2\nu ngq + \nu\nu qq) ,$$

quae formula, ob $nn(\alpha ff + \beta gg) = nnpq$, abit in

$$q(nnp \pm \alpha(2\mu nf \pm \mu\mu q) \pm \beta(2\nu ng \pm \nu\nu q)) ;$$

ubi litterae μ, ν et n facile ita accipi possunt, ut posterior factor, qui sit r, multo minor evadat quam q, ita ut iam habeamus productum qr, existente $r < q$. Tum vero simili modo ex hoc producto aliud denuo minus elici poterit, quod sit $= rs$, existente $s < r$; atque hac ratione mox perveniri poterit ad productum minimum, si modo in qualibet operatione valores ipsarum x et y minimi reddantur.

32. Haec clariora evadent, si ad exemplum propositum applicentur, quo erat $pq = 7 \cdot 19^2 + 2 \cdot 51^2 = 7729$, ubi ergo $p = 131$ et $q = 59$. Cum igitur hic sit $f = 19$ et $g = 51$, valores generales erunt: $x = 19n - 59\mu$ et $y = 51n - 59\nu$, qui pluribus modis multo minores reddi possunt quam f et g. Veluti sumptis n, μ et $\nu = 1$, fiet $x = -40$ et $y = -8$, qui numeri, per 8 depressi, evadunt $x = -5$ et $y = -1$, unde prodit $7xx + 2yy = 59 \cdot 3$, ideoque $r = 3$. Nunc ergo cum sit $f = 5$ et $g = 1$, novi valores erunt $x = 5n - 3\mu$ et $y = n - 3\nu$, unde valores minimi, per 2 depressi, erunt $x = 1$ et $y = 1$; quare productum minimum resultat $7 + 2 = 3 \cdot 3$; unde facile intelligitur, quomodo pro quovis casu operationes sint instituendae.

33. Totum hoc ratiocinium simili modo institui potest pro formula $\alpha\beta xx + yy$, ita ut, si numeri quantumvis magni compositi in ea semel tantum contineantur, ex iis continuo minores reperiri queant, quae pariter unico tantum modo in hac formula contineantur. Atque adeo has operationes eo usque continuare licebit, donec ad numeros compositos perveniatur, qui sint

minores quam $4\alpha\beta$. Quod etiam praecedente exemplo illustrari potest; quandoquidem numerus $59 \cdot 131$ etiam unico modo in formula $14xx + yy$ continetur, existente $x = f = 6$ et $y = g = 85$, unde novi valores erunt $x = 6n - 59\mu$ et $y = 85n - 59\nu$. Iam hic notetur litteras n et ν semper ita accipi posse, ut fiat $x = 1$; posito enim $6n - 59\mu = 1$ erit $n = 10\mu - \frac{\mu - 1}{6}$. Capiatur ergo $\mu = 1$, eritque $n = 10$ et $x = 1$, tum vero $y = 850 - 59\nu$, cuius valor minimus prodit ex $\nu = 14$, unde fit $y = 24$. Adepti igitur sumus hanc formam: $14 \cdot 1^2 + 24^2 = 59 \cdot 10$. Eadem autem forma factorem habebit 10, si sumatur $y = 24 - 10\nu = 4$, unde resultat productum adhuc minus $14 \cdot 1^2 + 4^2 = 30 = 10 \cdot 3$, quod utique minus est quam $4\alpha\beta$. Quodsi enim fuerit numerus compositus $pq < 4\alpha\beta$, hic casus locum habere nequit, nisi fuerit $x = 1$, unde y etiam datum sortietur valorem. Hinc vicissim manifesto sequitur, si nullus numerus compositus minor quam $4\alpha\beta$ in formula $\alpha\beta xx + yy$ contineatur, tales etiam in numeris maximis non dari; consequenter quoties quispiam numerus in tali formula unico tantum modo continetur, tum certo concludere poterimus illum numerum esse primum; unde sequens problema maximi momenti resolvere licebit.

PROBLEMA

Propositae formulae cuiuscunque $\alpha xx + \beta yy$ naturam perscrutari, utrum numeri unico modo in ea contenti tuto concludi queant esse primi, an vero ista conclusio fallere queat, quippe quo posteriori casu tales formulas a proposito nostro excludi oportet.

SOLUTIO

34. Primo ex iis, quae sunt allata, satis intelligitur hanc formulam eadem proprietate praeditam esse atque eius affinem $\alpha\beta xx + yy$. Sicque totum iudicium eo redit, utrum omnes numeri semel tantum in hac formula contenti tuto pro primis haberi queant necne. Ad hanc quaestionem decidendam sufficiet examinasse, utrum dentur numeri compositi minores quam $4\alpha\beta$, qui in hac formula contineantur. Si enim tales numeri occurrant, non solum haec formula $\alpha\beta xx + yy$, sed etiam illa $\alpha xx + \beta yy$ a proposito nostro est excludenda; contra autem, si nulli tales numeri compositi occurrant, utraque formula ad numeros primos explorandos tuto uti licebit; quandoquidem omnes numeri unico modo contenti certe futuri sunt primi.

35. Hinc igitur statim, quia nulli alii numeri, nisi minores quam $4\alpha\beta$, in iudicium ingrediuntur, ponatur $x = 1$, ut habeatur formula $\alpha\beta + yy$, ubi ipsi y nullos alios valores tribui opus est, nisi qui sint ad $\alpha\beta$ primi. Reliquis igitur exclusis ipsi y successive tribuantur tales valores, donec numeri resultantes terminum $4\alpha\beta$ excedant.

36. Iam nihil reliquum est, nisi ut numeri hoc modo prodeuntes examinentur, utrum sint primi, an vero compositi; si enim unicus compositus occurrat, eam formulam statim excludi oportebit. Hic autem probe est tenendum numeros quadratos in hoc iudicio inter compositos numerari non debere, propterea quod, si fuerit $\alpha\beta + yy = kk$, idem quadratum insuper alio quoque modo in formula illa $\alpha\beta xx + yy$ continetur, scilicet quando $x = 0$ et $y = k$; quamobrem, quoties in his evolutionibus numeri quadrati occurrent, ii non compositis numeris, sed primis accenseri debebunt[1]).

37. Hanc regulam illustremus exemplo formulae $7xx + 2yy$, ubi $\alpha = 7$ et $\beta = 2$, ita ut formula $14 + yy$ sit examinanda. Hic ergo valores ipsi y tribuendi primo debent esse impares, neque per 7 divisibiles, idque tantum eo usque, quamdiu numeri prodeuntes non superabunt terminum $4 \cdot 14 = 56$. Hoc examen sequenti modo commode repraesentabitur:

$14 + 1$,	3^2,	5^2,
15,	23,	39,
c,	p,	c,

ubi numeri compositi littera c, primi vero littera p designentur. Hinc igitur patet a nostro instituto excludi debere non solum formulam $14xx + yy$, sed etiam $7xx + 2yy$.

38. Simili modo examinetur formula $11xx + yy$, atque in formula $11 + yy$ ipsi y tribuantur valores ad 11 primi usque ad terminum 44, quod ergo examen ita referetur:

$11 + 1$,	2^2,	3^2,	4^2,	5^2,
12,	15,	20,	27,	36,
c,	c,	c,	c,	c.

1) Praeterea vero si etiam numeri pares prodeant, quoniam supra § 21 vidimus ex valoribus litterae m unitatem et binarium excludi: hinc si p sit numerus primus, in hac investigatione, praeter ipsum numerum p, etiam eius quadratum pp simulque eius duplum $2p$ ut primi spectari debebunt; praeterea etiam omnes potestates binarii pro primis spectari debent. [L. Euler]

Quoniam igitur hic omnes numeri resultantes sunt compositi, hunc numerum 11 maxime excludi oportet.

Examinetur nunc numerus 13, utrum excludi debeat necne, quod examen ita instituetur:

$13+1$,	2^2,	3^2,	4^2,	5^2,	6^2,
14,	17,	22,	29,	38,	49,
$2p$.	p.	$2p$.	p.	$2p$.	pp.

Hic ergo nulli numeri compositi occurrunt, unde numerus 13 ad classem numerorum idoneorum referri debebit.

Examinetur numerus 30, utrum sit idoneus, an vero excludi debeat, qui calculus ita se habebit:

$30+1^2$,	7^2
31,	79
p.	p.

Quia ergo hic etiam nullus numerus compositus prodit, numerus 30 in classe numerorum idoneorum locum habebit.

Examinetur numerus 43, et calculus ita se habebit:

$43+1^2$,	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.

Hinc ergo patet hunc numerum 43 ex classe numerorum idoneorum excludi debere.

Examinetur nunc simili modo numerus $210 = 2 \cdot 3 \cdot 5 \cdot 7$, ita ut ipsi y valores ad 210 primos tribui oporteat usque ad terminum 840

$210+1$,	11^2,	13^2,	17^2,	19^2,	23^2,
211,	331,	379,	499,	571,	739,
p.	p.	p.	p.	p.	p.

Cum igitur omnes numeri prodeuntes sint primi, numerus iste 210 pro idoneo est habendus, ex quo plures formulae sequentes formari possunt:

1.	$210xx + yy$,	5.	$30xx + 7yy$,
2.	$105xx + 2yy$,	6.	$35xx + 6yy$,
3.	$70xx + 3yy$,	7.	$21xx + 10yy$,
4.	$42xx + 5yy$,	8.	$14xx + 15yy$,

quae omnes formulae ita sunt comparatae, ut omnes numeri, qui in quapiam earum semel tantum continentur, certe futuri sint numeri primi.

39. Postquam igitur hoc modo numeri ad institutum nostrum inepti fuerint exclusi, reliqui numeri, quos idoneos appellemus, ordine in tabulam referantur, quam usque ad terminum 3000 continuare licuit; atque adeo adhuc dubium videtur, num maiores numeri idonei reperiri queant.

TABULA NUMERORUM IDONEORUM[1])

1	13	37	85	177	357
2	15	40	88	190	385
3	16	42	93	210	408
4	18	45	102	232	462
5	21	48	105	240	520
6	22	57	112	253	760
7	24	58	120	273	840
8	25	60	130	280	1320
9	28	70	133	312	1365
10	30	72	165	330	1848
12	33	78	168	345	

Hic scilicet maximus numerus idoneus est 1848, ex his factoribus compositus: $8 \cdot 3 \cdot 7 \cdot 11$; neque post hunc ullum alium maiorem mihi quidem invenire licuit, postquam istum laborem usque ad 3000 et ultra, sum exsecutus. Operae autem pretium erit in confirmationem huius tanti numeri probationem adiungere.

1) Vide tabulam p. 277 huius voluminis. R. F.

1848			1848		
+ 1	1849 = 43^2	$= pp$	+ 41^2	3529	$= p$
+ 5^2	1873	$= p$	+ 43^2	3697	$= p$
+ 13^2	2017	$= p$	+ 47^2	4057	$= p$
+ 17^2	2137	$= p$	+ 53^2	4657	$= p$
+ 19^2	2209 = 47^2	$= pp$	+ 59^2	5329 = 73^2	$= pp$
+ 23^2	2377	$= p$	+ 61^2	5569[1])	$= p$
+ 25^2	2473	$= p$	+ 65^2	6073	$= p$
+ 29^2	2689	$= p$	+ 67^2	6337	$= p$
+ 31^2	2809 = 53^2	$= pp$	+ 71^2	6889 = 83^2	$= pp$
+ 37^2	3217	$= p$	+ 73^2	7177	$= p$

40. Distinctio igitur talium formularum $\alpha xx + \beta yy$ in duas classes maxime est memorabilis et in ipsa rei natura fundata; quarum classium prior omnes tales formulas complectitur, in quibus omnes numeri semel tantum contenti tuto pro primis haberi queant, quarum criterium in hoc consistit, ut productum $\alpha\beta$ in superiore tabula numerorum idoneorum reperiatur, cuius generis simpliciores formae sunt $xx + yy$, $2xx + yy$, $3xx + yy$, quarumque proprietas ista iam pridem a Geometris est agnita et demonstrata. Ad alteram vero classem referendae sunt reliquae formae $\alpha xx + \beta xx$, in quibus etiam numeri compositi unico tantum modo contenti esse possunt, quarum criterium in hoc consistit, quod productum $\alpha\beta$ non in superiori tabula occurrit, cuiusmodi formae simpliciores sunt $5xx + 4yy$, $7xx + 2yy$, $7xx + 5yy$, $11xx + yy$ etc. Quantum autem hinc subsidium oriatur ad numeros praegrandes examinandos, utrum sint primi necne, in singulari dissertatione fusius ostendi[2]).

ADDITAMENTUM
DE NUMERIS IDONEIS INVESTIGANDIS

41. Tabula numerorum idoneorum huic dissertationi inserta eo magis est notatu digna, quod non solum omnes numeros huius naturae usque ad 2 milia exhibeat, sed etiam ultra hunc terminum nulli prorsus huiusmodi numeri occurrere videantur. Cum enim hanc investigationem usque ad 4 milia essem prosecutus, in toto hoc intervallo ne unicus quidem numerus idoneus se mihi obtulerat; unde sequitur ab hoc termino usque ad 16000 nullos certe dari

1) Editio princeps: 7417. Huius erroris causa EULERUS sequentes numeros omittit. R. F.
2) Confer commentationes 699 et 719 ind. ENESTROEMIANI huius voluminis p. 245 et 360. R. F.

numeros idoneos per 4 divisibiles; eorum enim partes quartae in praecedente intervallo reperiri deberent. Neutiquam autem probabile est ibi numeros vel impares vel impariter pares existere; ex sola enim inspectione superioris tabulae manifesto patet istos numeros continuo magis fieri compositos, siquidem ultimus huius tabulae numerus primus est 37; numerus vero, qui tantum duobus constat factoribus, est 253. Hinc igitur maxime verisimile est in tabula nostra omnes plane numeros idoneos contineri.

42. Cum isti numeri summa attentione sint digni, operae pretium erit eorum proprietates accuratius perpendisse. In hoc autem negotio imprimis attendisse iuvabit, quaenam numerorum genera ex hac tabula excludantur. Quemadmodum enim numeri primi reperiuntur, dum ex ordine omnium numerorum omnes, qui sunt compositi, delentur, ita etiam numeri idonei relinquuntur, postquam omnes ineptos deleverimus; numerorum igitur genera, quae excludi oportet, hic ante oculos constituamus.

I. Primum genus numerorum excludendorum in hac forma continetur: $4n + 3$. Si enim primum quadratum 1 addatur, prodit $4(n + 1)$, ideoque numerus compositus, solis casibus exceptis, quibus $(n + 1)$ est potestas binarii, uti evenit, si fuerit vel $n = 0$ vel $n = 1$ vel $n = 3$ vel $n = 7$. Hanc ob rem ex ordine omnium numerorum excludi debent numeri formae $4n + 3$ praeter hos tres minimos 3, 7 et 15[1]).

II. Excludi etiam debent numeri in hac forma contenti: $3n + 2$, quia addito quadrato 1 prodit $3(n + 1)$, ideoque numerus compositus, nisi fuerit vel $n = 0$, quo casu numerus fit revera primus, vel $n = 1$, quo casu prodit numerus $2 \cdot 3$ pro primo habendus, ob formam $2p$, vel $n = 2$, quo casu prodit numerus $3 \cdot 3$ formae pp, pariter pro primo habendus. Hinc ergo ex ordine omnium numerorum excludi debent omnes numeri formae $3n + 2$ praeter hos tres: 2, 5 et 8.

III. Excludi debent omnes numeri in hac forma contenti: $5n + 4$. Addita enim 1 prodit $5(n + 1)$, numerus compositus, exceptis casibus $n = 0$, $n = 1$ et $n = 4$. Quamobrem ex ordine omnium numerorum excludi debent omnes numeri formae $5n + 4$ praeter hos tres: 4, 9, 24; reliqui scilicet omnes, qui sunt [14], 19, 29, 34, 39 etc., debent deleri.

IV. Excludi debent numeri formae $5n + 1$, quia addito quadrato 4 prodit numerus $5(n + 1)$, pro composito habendus, nisi fuerit vel $n = 0$ vel

1) Generaliter omnes numeri $2^{\alpha+2} - 1$ includi deberent; EULERUS nullam demonstrationem affert, quamobrem tres numeros modo includit. R. F.

$n = 1$ vel $n = 4$; quamobrem ex ordine omnium numerorum excludi debent omnes numeri formae $5n + 1$ praeter hos tres 1, 6, 21, quibus adiungi oportet casus $n = 3$, quoniam ad numerum 16 quadratum 4 addi non convenit; sicque numeri hinc expungendi erunt 11, 26, 31, 36, 41, 46 etc.

NB. Si binae posteriores conditiones coniungantur, excludi debent numeri desinentes in 1, 4, 6 et 9, exceptis minoribus 1, 4, 6, 9, 21 et 24[1]).

V. Ob numerum primum 7 excludi debent numeri formae $7n + 6$, quia addito quadrato 1 prodit numerus compositus $7(n + 1)$, exceptis casibus $n = 0$, $n = 1$ et $n = 6$. Unde ex ordine omnium numerorum excludi debent omnes numeri formae $7n + 6$, exceptis his tribus 6, 13, 48; ita ut deleri debeant numeri 20, 27, 34, 41, 55, 62 etc.

VI. Ob eundem numerum 7 etiam excludi debet forma $7n + 5$, quia addito quadrato 9 prodit forma $7(n + 2)$, qui est numerus compositus, nisi fuerit $n = 0$ et $n = 5$. Insuper vero etiam excipiuntur casus $n = 1$, $n = 4$, $n = 7$ et $n = 10$ [etc.], quippe quibus forma $7n + 5$ divisorem habet 3, ideoque quadratum 9 eo addi non conveniet; quamobrem expungi debent omnes numeri $7n + 5$ praeter hos: 5, 12, 33, 40 [etc.].

VII. Ob eundem numerum 7 excludi debent numeri formae $7n + 3$, quia addito quadrato 4 prodit forma $7(n + 1)$, ideoque numerus compositus praeter casus $n = 0$, $n = 1$ et $n = 6$. Praeterea vero etiam intelligitur, non nisi ad numeros impares quadratum 4 addi posse; hinc ergo excludi debent omnes numeri in forma $7n + 3$ contenti praeter istos: 3, 10, 24, [38], 45, [etc.].
NB. Ob numerum ergo 7 omnes numeri in quapiam harum trium formarum $7n + 3$, $7n + 5$, $7n + 6$ contenti excludi debent praeter 3, 5, 6, 10, 12, 13, 24, [33, 38], 40, 45, 48 [etc.].

VIII. Deinde ob numerum primum 11 excludi debet forma $11n + 10$, quia addito 1 prodit $11(n + 1)$, ideoque numerus compositus praeter casus $n = 0$, $n = 1$ et $n = 10$; unde omnes numeri huius formae deleri debent praeter 10, 21, 120.

IX. Ob eundem numerum 11 excludi debet forma $11n + 8$, quia addito quadrato 25 prodit forma $11(n + 3)$, quae semper est numerus compositus praeter casum $n = 8$, quo prodit 11^2. Deinde etiam considerari debet casibus, quibus haec forma $11n + 8$ factorem habet 5, additionem quadrati 25 locum non habere. Hinc ergo omnes numeri formae $11n + 8$ excludi debent praeter hos: 8, 30, 85 [etc.].

1) Si n impar est, $5n + 1$ par erit; in hoc casu regula calculandi numeros idoneos non admittit additionem quadrati paris. R. F.

X. Ob eundem numerum 11 excludi debet forma $11n + 7$, quoniam addito quadrato 4 prodit $11(n + 1)$, numerus compositus praeter casus $n = 0$, $n = 1$ et $n = 10$; unde prodeunt numeri 7, 18 et 117, quorum postremus, ob alias rationes, scilicet ob formam $7n + 5$, iam est exclusus. Praeterea vero casus, quibus $11n + 7$ est numerus par, additionem quadrati 4 non patiuntur, ergo omnes numeri formae $11n + 7$ deleri debent, praeter 7, 18, 40 [etc.].

XI. Ob eundem numerum 11 excludi debet forma $11n + 6$, cui quadratum 16 additum producit $11(n + 2)$, ideoque numerus compositus praeter $n = 0$ et $n = 9$, hoc est praeter numeros 6 et 105. Sicque deleri debent omnes numeri formae $11n + 6$ praeter 6 et 105, quibus adiungi oportet insuper pares numeros 28, [50], 72 [etc.] quippe qui additionem quadrati 16 non admittunt.

XII. Ob eundem numerum 11 restat forma $11n + 2$, cui quadratum 9 additum dat $11(n + 1)$, unde oritur exclusio $n = 0$, $n = 1$ et $n = 10$, praeterquam quod numeri huius formae per 3 divisibiles additionem huius quadrati non patiuntur; consequenter omnes numeri $11n + 2$ sunt expungendi praeter 2, 13, 112, quibus adiungi oportet numeros huius formae per 3 divisibiles, qui sunt 24, 57 [etc.] NB. Ob numerum igitur primum 11 habentur quinque numerorum formae, quos deleri oportet, scilicet $11n + 2$, $11n + 6$, $11n + 7$, $11n + 8$, $11n + 10$, praeter scilicet paucos certos numeros, qui ob singulares rationes relinqui debent.

43. Simili modo etiam sequentes numeri primi evolvi possent, quod autem nimis foret prolixum. Contenti autem esse possumus pro singulis eas formas notasse, quas excludi oportet; hae autem formae excludendae sunt sequentes:

1° $4n + 3$
2° $3n + 2$
3° $5n + 1,\ 4$
4° $7n + 3,\ 5,\ 6$
5° $11n + 2,\ 6,\ 7,\ 8,\ 10$
6° $13n + 1,\ 3,\ 4,\ 9,\ 10,\ 12$
7° $17n + 1,\ 2,\ 4,\ 8,\ 9,\ 13,\ 15,\ 16$
8° $19n + 2,\ 3,\ 8,\ 10,\ 12,\ 13,\ 14,\ 15,\ 18$
9° $23n + 5,\ 7,\ 10,\ 11,\ 14,\ 15,\ 17,\ 19,\ 20,\ 21,\ 22$
10° $29n + 1,\ 4,\ 5,\ 6,\ 7,\ 9,\ 13,\ 16,\ 20,\ 22,\ 23,\ 24,\ 25,\ 28.$

44. Numeri autem in his formis contenti ideo excludi debent, quia semper quadratum addere licet, ita ut summa per ipsum illum numerum primum fit divisibilis. Ita numerus $29n + 13$ ideo excluditur, quia addito quadrato 16 prodit summa $29(n + 1)$ per 29 divisibilis. Quo igitur statim huiusmodi quadrata addenda obtineantur, superiores formae pro singulis numeris primis sequenti modo commode repraesentari possunt:

	$\sqrt{\square}$		$\sqrt{\square}$		$\sqrt{\square}$
$4n + 3$	1, 3	$17n + 8$	3, 14	$23n + 10$	6, 17
$3n + 2$	1, 2	$17n + 1$	4, 13	$23n + 20$	7, 16
$5n + 4$	1, 4	$17n + 9$	5, 12	$23n + 5$	8, 15
$5n + 1$	2, 3	$17n + 15$	6, 11	$23n + 11$	9, 14
$7n + 6$	1, 6	$17n + 2$	7, 10	$23n + 15$	10, 13
$7n + 3$	2, 5	$17n + 4$	8, 9	$23n + 17$	11, 12
$7n + 5$	3, 4	$19n + 18$	1, 18	$29n + 28$	1, 28
$11n + 10$	1, 10	$19n + 15$	2, 17	$29n + 25$	2, 27
$11n + 7$	2, 9	$19n + 10$	3, 16	$29n + 20$	3, 26
$11n + 2$	3, 8	$19n + 3$	4, 15	$29n + 13$	4, 25
$11n + 6$	4, 7	$19n + 13$	5, 14	$29n + 4$	5, 24
$11n + 8$	5, 6	$19n + 2$	6, 13	$29n + 22$	6, 23
$13n + 12$	1, 12	$19n + 8$	7, 12	$29n + 9$	7, 22
$13n + 9$	2, 11	$19n + 12$	8, 11	$29n + 23$	8, 21
$13n + 4$	3, 10	$19n + 14$	9, 10	$29n + 6$	9, 20
$13n + 10$	4, 9	$23n + 22$	1, 22	$29n + 16$	10, 19
$13n + 1$	5, 8	$23n + 19$	2, 21	$29n + 24$	11, 18
$13n + 3$	6, 7	$23n + 14$	3, 20	$29n + 1$	12, 17
$17n + 16$	1, 16	$23n + 7$	4, 19	$29n + 5$	13, 16
$17n + 13$	2, 15	$23n + 21$	5, 18	$29n + 7$	14, 15

Huiusmodi tabellae nobis novam methodum suppeditant numeros propositos quosvis examinandi, utrum sint idonei necne; quem in finem sequens problema adiungamus.

PROBLEMA

Numerum quemvis propositum n examinare, utrum sit idoneus necne.

SOLUTIO

45. Ex praecedentibus patet numerum n tum demum esse idoneum, quando additis quadratis minoribus, ad n primis, summae resultant, quae sunt vel numeri primi vel eorum dupla vel etiam quadrata vel adeo potestates binarii, idque usque ad terminum $4n$. Ex quo intelligitur numerum propositum n non fore idoneum, quando datur quadratum $aa < 3n$ et primum ad n, ut summa $n + aa$ evadat numerus compositus, qui, denotante p numerum primum, neque fit p neque $2p$ neque pp neque adeo 2^α.

46. Quando autem formula $n + aa$ talem numerum compositum producit, quia assumimus $n + aa < 4n$, necesse est, ut is factorem habeat primum et minorem quam $\sqrt{4n}$. Quamobrem res eo redit, ut inquiratur, num detur numerus primus $< \sqrt{4n}$, per quem quispiam numerorum in forma $n + aa$ contentorum divisionem admittat, siquidem quadratum aa fuerit ad n primum atque $aa < 3n$. Ad hoc igitur explorandum percurrantur ordine omnes numeri primi supra allati, ad examinandum, utrum numerus noster propositus n in quapiam exclusione contineatur; quod si eveniat, non tamen inde statim erit concludendum istum numerum non esse idoneum, quoniam fieri potest, ut formula $n + aa$ vel ipsi numero p vel eius duplo vel eius quadrato fiat aequalis, quippe quibus casibus, ut vidimus, exclusio locum non habet. Imprimis autem hic meminisse oportet quadratum aa ad ipsum numerum propositum primum esse debere, aliter exclusio quoque locum non habet. Quodsi ergo, percursis hoc modo omnibus numeris primis minoribus quam $\sqrt{4n}$, nulla exclusio reperiatur, tum numerus propositus pro idoneo erit habendus; tota autem haec operatio multo clarius per exempla intelligetur.

EXEMPLUM 1

47. Propositus sit numerus $n = 33$, et cum sit $\sqrt{4n} < 12$, considerentur omnes numeri primi usque ad 11, utrum iste numerus 33 in quapiam forma excludente contineatur. Statim autem perspicitur hunc numerum neque in prima forma excludente $4n + 3$ neque in secunda $3n + 2$ neque tertia $5n + 1$, 4 contineri; at vero in quarta forma pro numero primo 7 continetur, cum sit $33 = 7m + 5$, quae exclusionem innuit; quadratum autem aa, quod ipsi 33 additum divisionem per 7 producit, indicatur vel 3^2 vel 4^2; at vero prius 3^2 hic reiici debet, quia ad 33 non est primum, alterum vero 4^2, additum ad 33,

producit 49, qui numerus, cum sit quadratus, pariter nullam exclusionem parit. Dantur quidem etiam quadrata maiora, divisibilitatem per 7 producentia, scilicet $(7\alpha \pm 3)^2$, cuiusmodi sunt 10^2, 11^2, 17^2, 18^2 etc., quorum primum 10^2, utpote ad 33 primum, praebet utique summam 133 per 7 divisibilem, quae autem iam maior est quam $4 \cdot 33 = 132$, atque adeo duplici modo in forma $33xx + yy$ continetur, scilicet 1°) $x = 1$ et $y = 10$, 2°) $x = 2$ et $y = 1$.

48. Numerus ergo primus 7 nullam exclusionem gignit, sequentem autem 11 examinare non attinet, quia 11 est divisor ipsius 33, unde recte concludimus numerum 33 esse idoneum.

EXEMPLUM 2

49. Propositus sit numerus $n = 58$, ubi $\sqrt{4n} < 16$, ita ut numeros primos minores quam 16 percurri oporteat. Manifestum autem est hunc numerum neque in prima forma excludente $4n + 3$ neque in secunda $3n + 2$ neque tertia $5n + 1$, 4 neque etiam quarta $7n + 3$, 5, 6 neque quinta $11n + 2$, 6, 7, 8, 10 contineri; neque vero etiam hic numerus per ultimum 13, minorem quam 16, excluditur; unde sequitur numerum 58 revera esse idoneum.

EXEMPLUM 3

50. Sit numerus propositus $n = 345 = 3 \cdot 5 \cdot 23$, unde, quia $\sqrt{4 \cdot 345} < 38$, omnes numeros primos usque ad 37 percurri oportet. Hinc autem nulla exclusio occurrit usque ad numerum primum 19, propterea quod $345 = 19 \cdot 18 + 3$; unde quadrata addenda sunt 4^2, 15^2, quorum posterius reiicitur, quia non est primum ad 345; at prius 4^2 additum producit summam 361, quae est quadratum ipsius 19, ideoque exclusionem non gignit. Reliqua quadrata $(19n \pm 4)^2$, quae sunt 23^2, 34^2, 42^2, 53^2, 61^2, quae pariter divisibilitatem per 19 pariunt, at praeter 23^2 terminum $3n$ superant; illud autem 23^2 adhibere non licet, utpote factorem ipsius 345, quamobrem iste numerus 345 pro idoneo est habendus, nisi forte sequentes numeri primi usque ad 37 exclusionem generent. Iam post 19 sequitur numerus 23, qui hic autem in computum non venit; pro sequente 29 fit $345 = 29 \cdot 11 + 26$, quod nullam exclusionem innuit; porro vero est $345 = 31 \cdot 11 + 4$, pariter nullam exclusionem continens. Denique est $345 = 37 \cdot 9 + 12$, qua forma exclusio innuitur, quemadmodum facile pateret, si tabulas ulterius continuare liceret. Quadrata enim addenda sunt 5^2 et 32^2,

quorum priore uti non licet, quia non est primum ad 345; alterum vero 32^2 additum producit 1369, hoc est ipsum quadratum 37^2, ita ut hinc nulla exclusio locum habeat, quocirca hic numerus 345 in classem numerorum idoneorum est referendus.

EXEMPLUM 4

51. Propositus sit numerus $148 = 4 \cdot 37$, quem ergo secundum numeros primos $< \sqrt{592} < 25$ examinemus; at vero nulla exclusio innuitur usque ad 19, siquidem est $148 = 19 \cdot 7 + 15$. Quadrata igitur addenda sunt 2^2, 17^2, quorum prius hic locum non habet, alterum vero additum producit $437 = 19 \cdot 23$, qui ergo est numerus compositus $< 4 \cdot 148$; unde sequitur hunc numerum 148 non esse idoneum.

EXEMPLUM 5

52. Propositus sit numerus $522 = 2 \cdot 9 \cdot 29$, unde numeros primos usque ad 46 percurri conveniet. Minores autem formulae nullam exclusionem gignunt, usque ad numerum primum 31, per quem divisio succedit, addendo quadrata vel 6^2 vel 25^2, quorum posterius producit $1147 = 31 \cdot 37$; qui numerus compositus, cum sit minor quam 2088, manifesto hunc numerum 522 ex classe idoneorum excludit.

53. Hac methodo haud difficile est istud numerorum examen quousque lubuerit continuare. Postquam autem hunc calculum usque ad 10 000 essem prosecutus, nullus novus numerus idoneus se mihi obtulit praeter eos, quos tabula superior exhibet, ex quo ista tabula omnes plane numeros idoneos in se complecti videtur.

RESOLUTIO FORMULAE DIOPHANTEAE $ab(maa+nbb)=cd(mcc+ndd)$ PER NUMEROS RATIONALES

Commentatio 716 indicis Enestroemiani

Nova acta academiae scientiarum Petropolitanae 13 (1795/6), 1802, p. 45—63

Summarium ibidem p. 56/7

Conventui exhibuit die 1. decembris 1778

SUMMARIUM

Dans le Tome XVII des nouveaux Commentaires[1]) feu Mr. Euler s'étoit occupé du problème de trouver quatre nombres A, B, C, D tels que $A^4 + B^4 = C^4 + D^4$, ce qui se réduisoit facilement à trouver quatre nombres a, b, c, d tels que

$$ab\,(aa + bb) = cd\,(cc + dd),$$

mais quoiqu'il eut trouvé alors deux solutions de ce problème, les nombres en étoient devenus si immenses, qu'on ne sera pas étonné de voir qu'il ait repris dans la suite ce même problème, et que, selon sa coûtume, il en ait rendu la solution plus parfaite et qu'il ait généralisé ses recherches sur cette matière.

La résolution de l'équation exposée dans le titre de ce mémoire, où m et n sont des nombres donnés, consiste à prendre à volonté un nombre q, à en déduire deux valeurs

$$\alpha = \frac{nqq}{nqq-m} \quad \text{et} \quad \beta = \frac{m}{nqq-m},$$

ensuite une valeur

$$z = \frac{-3}{4\alpha+\beta(4\alpha-1)^2} \quad \text{et} \quad s = \frac{4\alpha-1}{2},$$

d'où l'on tire

$$p = q(1+z) \quad \text{et} \quad \frac{a}{c} = 1 + sz,$$

1) Commentatio 428 indicis Enestroemiani: Observationes circa bina biquadrata quorum summam in duo alia biquadrata resolvere liceat. Novi comment. acad. sc. Petrop. 17 (1772), 1773, p. 64—69. *Leonhardi Euleri Opera omnia*, series I, vol. 3, p. 211—217. R. F.

desorte que a et c seront trouvés en entiers. Enfin on aura $b = cp$ et $d = aq$, et les quatre nombres a, b, c, d ainsi trouvés seront tels que $ab(maa+nbb) = cd(mcc+ndd)$.

Moyennant cette solution, en prenant $m = 1$ et $n = 1$ et $q = 3$, on trouve quatre nombres $a = 25$, $b = 291$, $c = 193$ et $d = 75$ qui satisfont à l'équation $ab\,(aa + bb) = cd\,(cc + dd)$; et comme, en mettant $a = p + q$, $b = p - q$, $c = r + s$, $d = r - s$, l'équation devient $p^4 + q^4 = r^4 + s^4$, on obtient quatre nombres $p = 158$, $q = 133$, $r = 134$, $s = 59$ qui sont incomparablement plus petits que ceux que feu Mr. EULER avoit trouvés dans le XVII Tome des nouveaux Commentaires.

Ajoutons une propriété remarquable de l'équation $ab\,(aa + bb) = cd\,(cc + dd)$, c'est qu'en faisant

$A = (a+b)+(c+d)$, $B = (a+b)-(c+d)$, $C = (a-b)+(c-d)$, $D = (a-b)-(c-d)$, il y aura $AB\,(AA + BB) = CD\,(CC + DD)$.

1. Inter theoremata olim a FERMATIO[1]) demonstrata, et post eius obitum deperdita, imprimis maximam attentionem meretur hoc theorema: quod non dentur duae potestates cuiusque ordinis, quarum summa vel differentia sit potestas eiusdem ordinis, siquidem ordo primus et secundus excipiatur. Ita negavit FERMATIUS exhiberi posse binos numeros a et b, ut haec formula $a^n \pm b^n$ aequetur simili potestati c^n, simul atque exponens n binarium superaverit. Hoc ergo modo omnes istae positiones erunt impossibiles:

I. $a^3 \pm b^3 = c^3$; II. $a^4 \pm b^4 = c^4$; III. $a^5 \pm b^5 = c^5$;
IV. $a^6 \pm b^6 = c^6$; V. $a^7 \pm b^7 = c^7$; VI. $a^8 \pm b^8 = c^8$ etc.

2. De prima harum formularum $a^3 \pm b^3 = c^3$ veritas iam satis feliciter est ostensa, unde simul quoque veritas sequitur pro omnibus formulis, pro quibus exponens n est multiplum ternarii. Tum vero multo clarius adhuc demonstrata est formula secunda $a^4 \pm b^4 = c^4$, cum evidentissime comprobatum sit neque summam neque differentiam duorum biquadratorum posse esse quadratum, multo minus ergo biquadratum, hincque etiam evicti sunt omnes casus, quibus exponens n est multiplum quaternarii. Interim tamen eiusmodi demonstratio, quae se pariter ad omnes exponentes n extendat, maxime adhuc desideratur, neque cuiquam Geometrarum in hoc numerorum mysterium penetrare contigit.

3. Pluribus autem insignibus Geometris visum est haec theoremata latius extendi posse. Quemadmodum enim duo cubi exhiberi nequeunt, quorum

1) *Oeuvres de* FERMAT, Paris, 1891, t. I, p. 291 t. III, p. 241. R. F.

summa vel differentia sit cubus, ita etiam certum est nequidem exhiberi posse tria biquadrata, quorum summa sit pariter biquadratum, sed ad minimum quatuor biquadrata requiri, ut eorum summa prodire queat biquadratum, quamquam nemo adhuc talia quatuor biquadrata assignare potuerit. Eodem modo etiam affirmari posse videtur non exhiberi posse quatuor potestates quintas, quarum summa etiam esset potestas quinta; similique modo res se habebit in altioribus potestatibus; unde sequentes quoque positiones omnes pro impossibilibus erunt habendae:

$$\begin{aligned} &\text{I.} && a^3 + b^3 = c^3\,, \\ &\text{II.} && a^4 + b^4 + c^4 = d^4\,, \\ &\text{III.} && a^5 + b^5 + c^5 + d^5 = e^5\,, \\ &\text{IV.} && a^6 + b^6 + c^6 + d^6 + e^6 = f^6 \\ & && \text{etc.} \end{aligned}$$

Plurimum igitur scientia numerorum promoveri esset censenda, si demonstrationem desideratam etiam ad has formulas extendere liceret.

4. Primo quidem intuitu videri posset has postremas formulas non solum ad summas, sed etiam ad differentias, prouti in prima usu venit, extendi posse, ita ut etiam haec aequalitas $a^4 \pm b^4 \pm c^4 = d^4$ pro impossibili esset habenda; verum hoc longe secus se habere ante aliquot annos observavi in tomo commentariorum XVII. pag. 64[1]), ubi bina biquadrata assignavi, quorum summa in alia duo biquadrata resolvi queat, ita ut sit $a^4 + b^4 = c^4 + d^4$, unde ergo haec aequalitas $a^4 + b^4 - c^4 = d^4$ veritati neutiquam adversatur; verum numeri, quos pro his litteris a, b, c, d per calculum valde taediosum erui, valde immanes prodierunt.

5. Cum autem nuper idem argumentum tractandum suscepissem, praeter omnem expectationem incidi in numeros multo minores hac indole praeditos, atque adeo minimi numeri hoc praestantes statui possunt isti: $a = 134$, $b = 133$, $c = 158$ et $d = 59$, quandoquidem revera deprehendetur esse $134^4 + 133^4 = 158^4 + 59^4$, quem calculum exsequi haud adeo molestum est, dum contra comprobationem illorum immensorum numerorum vix quisquam tentare audebit.

---

1) Vide notam p. 329. R. F.

6. Methodus autem, qua tum temporis sum usus, ut resolverem hanc aequalitatem:

$$A^4 + B^4 = C^4 + D^4 ,$$

ita procedebat: consideravi scilicet hanc aequationem

$$A^4 - C^4 = D^4 - B^4 ,$$

ac posito

$$A = a + b , \quad C = a - b , \quad D = c + d \quad \text{et} \quad B = c - d$$

prodiit ista aequatio satis simplex:

$$ab(aa + bb) = cd(cc + dd) ;$$

sicque totum negotium ad resolutionem huius formulae reducitur. Hic autem non solum methodum ante usitatam multo tractabiliorem sum redditurus, sed etiam ad resolutionem formulae multo generalioris in titulo exhibitae

$$ab(maa + nbb) = cd(mcc + ndd)$$

sum accommodaturus, ita ut, quicunque numeri pro m et n accipiantur, semper infinitis modis numeri satisfacientes pro a, b, c, d inveniri queant.

7. Ad aequalitatem autem hanc resolvendam utor ante omnia hac transformatione:

$$b = cp \quad \text{et} \quad d = aq ,$$

hocque modo aequatio resolvenda hanc induet formam:

$$p(maa + nccpp) = q(mcc + naaqq) ,$$

unde elicitur

$$\frac{aa}{cc} = \frac{np^3 - mq}{nq^3 - mp} ,$$

sicque totum negotium huc redit, ut ista formula $\frac{np^3 - mq}{nq^3 - mp}$ ad quadratum reducatur, quod quidem sponte evenire casu $q = p$ mox in oculos incurrit, cum evadat $\frac{aa}{cc} = 1$, ideoque $c = a$; tum quoque fiet $b = d$, qui autem casus

maxime obvius pro solutione neutiquam haberi potest, quandoquidem ambo membra aequationis prodeunt identica. Interim tamen hic ipse casus ad alias solutiones manuducere poterit.

8. Cum igitur nostra formula revera quadratum evadat posito $p = q$, statuamus $p = q(1 + z)$, ita ut sumpto $z = 0$ ipse casus obvius prodeat; nunc autem nostra formula in sequentem transmutabitur:

$$\frac{aa}{cc} = \frac{nqq(1+z)^3 - m}{nqq - m(1+z)},$$

sive

$$\frac{aa}{cc} = \frac{nqq - m + 3nqqz + 3nqqzz + nqqz^3}{nqq - m - mz},$$

in qua fractione quantitas incognita z in numeratore ad tertiam potestatem, in denominatore autem non ultra primam assurgit, cuiusmodi formulas per methodos cognitas tractari posse iam satis liquet.

9. Quo hanc fractionem tractabiliorem reddamus, tam numeratorem quam denominatorem dividamus per $nqq - m$, statuamusque brevitatis gratia

$$\frac{nqq}{nqq - m} = \alpha \quad \text{et} \quad \frac{m}{nqq - m} = \beta,$$

ita ut sit $\alpha - \beta = 1$ ideoque $\alpha = 1 + \beta$, quo facto formula sequens prodibit

$$\frac{aa}{cc} = \frac{1 + 3\alpha z + 3\alpha zz + \alpha z^3}{1 - \beta z}.$$

Iam per secundam methodum, qua olim sum usus, denominator reddatur quadratum, multiplicando supra et infra per $1 - \beta z$, unde prodit

$$\frac{aa}{cc} = \frac{(1-\beta z)(1 + 3\alpha z + 3\alpha zz + \alpha z^3)}{(1-\beta z)^2}.$$

Sicque tantum opus est, ut numerator, qui evolutus fit

$$1 + (3\alpha - \beta)z + 3\alpha(1 - \beta)zz + \alpha(1 - 3\beta)z^3 - \alpha\beta z^4,$$

ad quadratum reducatur, quod praestabitur eius radicem ponendo $1 + fz + gzz$, cuius quadratum est

$$1 + 2fz + (ff + 2g)\,zz + 2fgz^3 + ggz^4 .$$

Nunc quia primi termini se mutuo sponte destruunt, binae litterae f et g ita definiantur, ut etiam secundi ac tertii termini tollantur; prius fiet sumendo $f = \frac{3\alpha - \beta}{2}$, posterius vero statuendo

$$ff + 2g = 3\alpha(1 - \beta) ,$$

unde fit

$$g = \frac{3\alpha(1-\beta)}{2} - \tfrac{1}{2}ff .$$

Quoniam igitur utrinque tantum bini termini postremi remanent, qui per z^3 divisi praebent hanc aequationem: $\alpha(1 - 3\beta) - \alpha\beta z = 2fg + ggz$, inde elicitur

$$z = \frac{\alpha(1-3\beta) - 2fg}{\alpha\beta + gg} .$$

10. Haec est ea ipsa solutio, qua iam dudum loco citato sum usus, cuius ope pro quovis valore ipsius q ad arbitrium assumpto simul innotescunt litterae α et β, unde valor idoneus pro z obtinetur, quo invento primo erit $p = q(1 + z)$, ac denique erit

$$\frac{aa}{cc} = \frac{(1 + fz + gzz)^2}{(1 - \beta z)^2} \quad \text{ideoque} \quad \frac{a}{c} = \frac{1 + fz + gzz}{1 - \beta z} ,$$

unde ergo sumi poterit

$$a = 1 + fz + gzz \quad \text{et} \quad c = 1 - \beta z ;$$

tandem vero habebitur $b = cp$ et $d = aq$, sicque quaestioni propositae erit satisfactum.

11. Hoc autem modo pro casu, quem olim tractavi, $m = n = 1$ pro q unitas accipi nequit, quia litterae α et β evaderent infinitae; iidem vero enormes numeri, quos tum exhibui, reperiuntur, dum pro q vel 2 vel 3 assumitur. Quodsi autem non fuerit $m = n$, nihil obstat, quo minus statuatur $q = 1$,

hincque solutiones satis commodae obtineri poterunt; semper autem tum erit $d = a$, quod fortasse displicere potest.

12. Hac igitur methodo repudiata aliam viam sum ingressurus, quae ad solutiones multo simpliciores perducet, quaeque ita est comparata, ut non perveniatur ad quartam potestatem ipsius z. Hunc in finem statim pono

$$\frac{a}{c} = 1 + sz,$$

ita ut habeamus:

$$\frac{1 + 3\alpha z + 3\alpha zz + \alpha z^3}{1 - \beta z} = (1 + sz)^2,$$

qua aequatione evoluta et omnibus terminis ad eandem partem translatis pervenietur ad hanc aequationem:

$$\left.\begin{array}{l} +1 + 3\alpha z + 3\alpha zz + \alpha z^3 \\ -1 - 2sz - sszz + \beta ssz^3 \\ \quad + \beta z + 2\beta szz \end{array}\right\} = 0,$$

quae redigitur ad hanc formam:

$$3\alpha - 2s + \beta + (3\alpha + 2\beta s - ss)z + (\alpha + \beta ss)zz = 0.$$

13. Ut nunc ex hac aequatione incognita z commode deduci queat, hoc imprimis duobus modis fieri poterit, quorum primus adhiberi poterit, si statuere licebit

$$\alpha + \beta ss = 0, \text{ sive } ss = -\frac{\alpha}{\beta},$$

id quod locum habere nequit, nisi $-\frac{\alpha}{\beta} = -\frac{nqq}{m}$ fuerit quadratum, quamobrem iste casus tum tantum adhiberi poterit, quando numerorum m et n alter fuerit negativus, insuperque eorum productum quadratum. Pro hoc igitur casu ponamus $m = \mu\mu$ et $n = -\nu\nu$, ut aequalitas resolvenda sit

$$ab(\mu\mu aa - \nu\nu bb) = cd(\mu\mu cc - \nu\nu dd);$$

tum igitur erit

$$\alpha = \frac{+\nu\nu qq}{\mu\mu + \nu\nu qq} \text{ et } \beta = \frac{-\mu\mu}{\mu\mu + \nu\nu qq},$$

statuique poterit

$$ss = -\frac{\alpha}{\beta} = \frac{\nu\nu qq}{\mu\mu}, \text{ ideoque } s = \frac{\nu q}{\mu}.$$

Hoc modo aequatio postrema erit

$$3\alpha - 2s + \beta + (3\alpha + 2\beta s - ss)\, z = 0,$$

unde colligitur

$$z = \frac{2s - 3\alpha - \beta}{3\alpha + 2\beta s - ss},$$

factisque substitutionibus erit

$$z = \frac{\mu\mu(\mu\mu - 3\nu\nu qq) + 2\mu\nu q(\mu\mu + \nu\nu qq)}{\mu\mu(3\nu\nu qq - 2\mu\nu q) - \nu\nu qq(\mu\mu + \nu\nu qq)}.$$

14. Hic autem praeter omnem necessitatem introduximus binas novas litteras μ et ν; nihil enim impedit, quo minus loco μa, νb, μc, νd simpliciter scribantur litterae a, b, c, d, ita ut formula resolvenda evadat

$$ab\,(aa - bb) = cd\,(cc - dd),$$

perinde ac si sumpsissemus $\mu = 1$ et $\nu = 1$, unde solutio multo brevior obtinebitur.

Resolutio formulae particularis
$ab\,(aa - bb) = cd\,(cc - dd)$

Hic igitur sumpto pro q numero quocumque erit $\alpha = \frac{qq}{1+qq}$ et $\beta = \frac{-1}{1+qq}$; tum vero sumi oportet $s = q$, unde postrema aequatio erit

$$3qq - 1 - 2q - 2q^3 + z\,(2qq - 2q - q^4) = 0,$$

ideoque

$$z = \frac{1 + 2q - 3qq + 2q^3}{q(-2 + 2q - q^3)}.$$

Hoc valore invento erit

$$p = q\,(1 + z) \quad \text{et} \quad \frac{a}{c} = 1 + qz,$$

unde porro reliquae litterae b et d facile assignabuntur.

15. Statuamus nunc primo $q = 1$, eritque $z = -2$, deinde $\frac{a}{c} = -1$, ideoque $c = -a$; porro ob $p = -1$ erit $b = a$ et $d = a$. Hoc ergo casu omnes quatuor litterae essent aequales et ambo formulae membra $= 0$. Idem prodiret, si poneremus $q = -1$; perpetuo enim observasse iuvabit, perinde esse sive ipsi q tribuatur valor positivus sive negativus. Sumamus igitur, ut idoneum exemplum proferamus, $q = 2$, eritque $z = -\frac{3}{4}$, ideoque $p = \frac{1}{2}$ et $\frac{a}{c} = -\frac{1}{2}$, ergo $c = -2a$, porro $b = -a$ et $d = 2a$. Hoc autem modo in praecedens incommodum incidimus. Sit ergo $q = 3$, eritque $z = -\frac{34}{69}$, hinc $p = \frac{35}{23}$ et $\frac{a}{c} = -\frac{11}{23}$; ita sumi poterit $a = 11$ et $c = -23$, eritque $b = -35$ et $d = 3a = 33$. Hoc modo pervenimus ad hanc aequalitatem:

$$11 \cdot 35\,(35^2 - 11^2) = 23 \cdot 33\,(33^2 - 23^2)\,,$$

cuius ratio est manifesta, cum utrumque membrum in factores evolutum praebeat $2^4 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 23$. Hinc duo triangula rectangula exhiberi possunt, quorum areae inter se sunt aequales; prioris enim catheti erunt $2 \cdot 11 \cdot 35$ et $24 \cdot 46$, alterius vero trianguli $2 \cdot 23 \cdot 33$ et $10 \cdot 56$.

Reversio ad formulam generalem $ab\,(maa + nbb) = cd\,(mcc + ndd)$

16. Quando autem in aequatione quadrata § 12 ultimum terminum zz ad nihilum redigere non licet, semper hoc fieri potest in primo termino absoluto, unde fit

$$3\alpha - 2s + \beta = 0\,,$$

ex qua aequatione elicitur

$$2s = 3\alpha + \beta\,, \quad \text{sive} \quad s = \frac{4\alpha - 1}{2}\,.$$

Hoc igitur primo termino sublato duo reliqui per z divisi dant hanc aequationem:

$$3\alpha + 2\beta s - ss + (\alpha + \beta ss)\,z = 0\,,$$

quae aequatio abit in hanc:

$$\frac{3}{4} + (\alpha + \beta ss)\, z = 0\,,$$

unde fit

$$z = \frac{-3}{4\alpha + 4\beta ss}\,.$$

Cum igitur sit $2s = 4\alpha - 1$, erit

$$z = \frac{-3}{4\alpha + \beta(4\alpha - 1)^2}\,,$$

unde deducitur sequens solutio nostri problematis, quo requiritur, ut fiat $ab\,(maa + nbb) = cd\,(mcc + ndd)$.

17. Primo posito $b = cp$ et $d = aq$ fecimus $p = q\,(1 + z)$; tum vero, sumpta littera q pro lubitu, posuimus brevitatis gratia

$$\alpha = \frac{nqq}{nqq - m} \quad \text{et} \quad \beta = \frac{m}{nqq - m}\,,$$

ita ut sit $\alpha - \beta = 1$. Quo facto invenimus

$$z = \frac{-3}{4\alpha + \beta(4\alpha - 1)^2}\,,$$

unde definitur $p = q\,(1 + z)$. Deinde posito

$$s = \frac{4\alpha - 1}{2} = \frac{3\alpha + \beta}{2}$$

invenimus esse

$$\frac{a}{c} = 1 + sz\,,$$

unde cum $1 + sz$ sit plerumque fractio, hinc ambae litterae a et c facile per numeros integros assignantur; quibus inventis erit $b = cp$ et $d = aq$, quam solutionem aliquot exemplis illustremus.

EXEMPLUM 1

quo haec formula resolvenda proponitur

$$ab\,(aa + 2bb) = cd\,(cc + 2dd)$$

18. Hic igitur est $m = 1$ et $n = 2$, unde sumpto numero $q = 1$ erit $\alpha = 2$ et $\beta = 1$, hincque $s = \frac{7}{2}$ et $z = -\frac{1}{19}$, ideoque $p = \frac{18}{19}$; tum vero $\frac{a}{c} = \frac{31}{38}$, quocirca sumamus $a = 31$ et $c = 38$, unde denique fit $b = 36$ et $d = 31$, ita ut solutio futura sit $31 \cdot 36\,(31^2 + 2 \cdot 36^2) = 38 \cdot 31\,(38^2 + 2 \cdot 31^2)$, id quod calculum instituenti mox patebit. Est enim

$$31^2 + 2 \cdot 36^2 = 3553 = 11 \cdot 17 \cdot 19 \quad \text{et} \quad 38^2 + 2 \cdot 31^2 = 3366 = 2 \cdot 3^2 \cdot 11 \cdot 17,$$

quibus factoribus substitutis utrinque prodit idem productum

$$2^2 \cdot 3^2 \cdot 11 \cdot 17 \cdot 19 \cdot 31 .$$

Alia solutio eiusdem exempli

19. Sumatur hic $q = \frac{1}{2}$, eritque $\alpha = -1$ et $\beta = -2$. Deinde vero erit $s = -\frac{5}{2}$ et $z = \frac{1}{18}$, hinc ergo colligimus $p = \frac{19}{36}$ et $\frac{a}{c} = \frac{31}{36}$. Capiatur ergo $a = 31$ et $c = 36$, ex quibus denique fit $b = 19$ et $d = \frac{31}{2}$; unde, hos numeros duplicando, habebimus $a = 62$, $b = 38$, $c = 72$ et $d = 31$, ita ut sit

$$62 \cdot 38\,(62^2 + 2 \cdot 38^2) = 72 \cdot 31\,(72^2 + 2 \cdot 31^2) ,$$

ubi per factores est $62^2 + 2 \cdot 38^2 = 6732 = 2^2 \cdot 3^2 \cdot 11 \cdot 17$ et

$$72^2 + 2 \cdot 31^2 = 7106 = 2 \cdot 11 \cdot 17 \cdot 19 .$$

Sicque utrinque prodit idem productum $2^4 \cdot 3^2 \cdot 11 \cdot 17 \cdot 19 \cdot 31$.

EXEMPLUM 2

quo haec formula resolvenda proponitur

$$ab\,(aa + 3bb) = cd\,(cc + 3dd)$$

20. Hic ergo est $m = 1$ et $n = 3$, hincque $\alpha = \frac{3qq}{3qq - 1}$ et $\beta = \frac{1}{3qq - 1}$. Sumamus nunc primo $q = 1$, ut sit $\alpha = \frac{3}{2}$ et $\beta = \frac{1}{2}$, hinc autem fiet $s = \frac{5}{2}$ et

$z = -\frac{6}{37}$, quamobrem erit $p = \frac{31}{37}$ et $\frac{a}{c} = \frac{22}{37}$. Capiatur ergo $a = 22$ et $c = 37$, fietque $b = 31$ et $d = 22$, consequenter habebimus

$$22 \cdot 31\,(22^2 + 3 \cdot 31^2) = 37 \cdot 22\,(37^2 + 3 \cdot 22^2)\,.$$

Hic scilicet erit

$$22^2 + 3 \cdot 31^2 = 3367 = 7 \cdot 13 \cdot 37 \quad \text{et} \quad 37^2 + 3 \cdot 22^2 = 2821 = 7 \cdot 13 \cdot 31\,;$$

sicque utrinque idem oritur productum, scilicet $2 \cdot 7 \cdot 11 \cdot 13 \cdot 31 \cdot 37$.

Alia solutio eiusdem exempli

21. Sumatur $q = \frac{1}{2}$ eritque $\alpha = -3$ et $\beta = -4$, hincque porro $s = -\frac{13}{2}$ et $z = \frac{3}{688}$, quocirca habebimus $p = \frac{691}{1376}$ et $\frac{a}{c} = \frac{1337}{1376}$. Capiatur ergo $a = 1337$ et $c = 1376$, unde fit $b = 691$ et $d = \frac{1337}{2}$. Duplicatis ergo valoribus habebimus $a = 2674$, $b = 1382$, $c = 2752$ et $d = 1337$.

Adhuc alia solutio eiusdem exempli

22. Sumamus hic $q = 2$, eritque $\alpha = \frac{12}{11}$ et $\beta = \frac{1}{11}$, unde fit $s = \frac{37}{22}$ et $z = -\frac{3993}{7177}$; ex quo fit $p = \frac{6368}{7177}$, porro vero $sz = -\frac{13431}{14354}$, ideoque $\frac{a}{c} = \frac{923}{14354}$. Sicque sumi poterit $a = 923$ et $c = 14354$, unde tandem fit $b = 12736$ et $d = 1846$[1]).

23. Casum principalem, quo $m = 1$ et $n = 1$, quandoquidem hinc inventio binorum biquadratorum pendet, quorum summam in alia duo biquadrata resolvere liceat, peculiari tractationi reservamus, quae ergo continebit evolutionem huius formulae $ab\,(aa + bb) = cd\,(cc + dd)$.

24. Cum igitur hic sit $m = 1$ et $n = 1$, pro quolibet numero ad lubitum assumpto q capiatur

1) Editio princeps: $z = -\frac{3993}{6977}$, $p = \frac{5968}{6977}$, $sz = -\frac{13431}{13954}$, $\frac{a}{c} = \frac{523}{13954}$, $a = 523$, $c = 13954$, $b = 11936$, $d = 1046$. Correxit A. M.

$$\alpha = \frac{qq}{qq-1} \text{ et } \beta = \frac{1}{qq-1},$$

unde porro accipiatur

$$s = \frac{3\alpha+\beta}{2} \text{ atque } z = \frac{-3}{4\alpha+\beta(3\alpha+\beta)^2},$$

quibus valoribus inventis erit

$$p = q(1+z) \text{ et } \frac{a}{c} = 1 + sz.$$

Denique vero erit $b = cp$ et $d = aq$, quibus praemissis ad exempla descendamus.

EXEMPLUM 1
QUO $q = 3$

25[1]). Evidens scilicet est hoc casu sumi non posse $q = 1$, quia litterae α et β fierent infinitae; deinde vero facile est praevidere positionem $q = 3$ simpliciorem solutionem suppeditare quam $q = 2$. Sumpto igitur $q = 3$ erit $\alpha = \frac{9}{8}$ et $\beta = \frac{1}{8}$, unde fit $s = \frac{7}{4}$ atque $z = -\frac{96}{193}$. Hinc ergo colligitur $p = \frac{291}{193}$, tum vero $sz = -\frac{168}{193}$, ideoque $\frac{a}{c} = 1 + sz = \frac{25}{193}$; quocirca capiatur $a = 25$ et $c = 193$, eritque $b = 291$ et $d = 75$. Sicque pertingimus ad hanc solutionem

$$25 \cdot 291\,(25^2 + 291^2) = 193 \cdot 75\,(193^2 + 75^2),$$

ubi notetur esse

$$25^2 + 291^2 = 85306 = 2 \cdot 13 \cdot 17 \cdot 193 \quad \text{et}$$
$$193^2 + 75^2 = 42874 = 2 \cdot 13 \cdot 17 \cdot 97.$$

Nunc autem facile perspicitur idem productum utrinque per factores eosdem prodire $2 \cdot 3 \cdot 5^2 \cdot 13 \cdot 17 \cdot 97 \cdot 193$.

26. Transferamus nunc hanc solutionem ad biquadrata, atque in genere, si fuerit $ab(aa + bb) = cd(cc + dd)$, statuatur $a = p + q$ et $b = p - q$, similique modo $c = r + s$ et $d = r - s$, prodibitque ista aequatio:

1) Inde in editione principe numeri paragraphorum unitate diminuuntur. R. F.

$$2\,(p^4 - q^4) = 2\,(r^4 - s^4)\,.$$

Hoc ergo modo erit

$$p^4 + s^4 = q^4 + r^4\,,$$

ubi notetur esse

$$p = \frac{a+b}{2}\,,\quad q = \frac{a-b}{2}\,,\quad r = \frac{c+d}{2}\quad \text{et}\quad s = \frac{c-d}{2}\,;$$

sive duplicando sumere licebit $p = a + b, q = a - b, r = c + d$ et $s = c - d$. Ex casu igitur modo invento colligimus $p = 158$, $q = 133$, $r = 134$ et $s = 59$.

27. Hi numeri prorsus conveniunt cum iis, quos initio commemoravimus, atque adeo sine dubio simplicissimam solutionem illius problematis, quod olim tractaveram, suppeditant, cum sit

$$158^4 + 59^4 = 133^4 + 134^4\,.$$

Hic autem praeter expectationem se offert alia solutio nostrae formulae $ab\,(aa + bb) = cd\,(cc + dd)$, hinc enim sequitur fore

$$158^4 - 134^4 = 133^4 - 59^4\,,$$

unde in factores resolvendo fit

$$24\cdot 292\,(158^2 + 134^2) = 74\cdot 192\,(133^2 + 59^2)\,;$$

ubi notetur ob

$$pp + qq = \tfrac{1}{2}(p+q)^2 + \tfrac{1}{2}(p-q)^2 \quad \text{fore} \quad 158^2 + 134^2 = \tfrac{1}{2}(292)^2 + \tfrac{1}{2}(24)^2,$$

similique modo $133^2 + 59^2 = \frac{1}{2}(192)^2 + \frac{1}{2}(74)^2$, quibus substitutis prodit forma nostrae similis

$$24\cdot 292\,(292^2 + 24^2) = 74\cdot 192\,(74^2 + 192^2),$$

singulisque factoribus per 2 divisis erit

$$12\cdot 146\,(146^2 + 12^2) = 37\cdot 96\,(37^2 + 96^2)\,.$$

28. Ecce ergo deducti sumus ad solutionem adhuc simpliciorem nostrae formulae $ab\,(aa + bb) = cd\,(cc + dd)$, qua est $a = 12$, $b = 146$, $c = 37$ et $d = 96$. Siquidem hi numeri notabiliter sunt minores, quam supra inventi; unde sequitur methodus generalis ex qualibet solutione nostrae formulae aliam

solutionem derivandi. Cum enim posito $a + b = p$, $a - b = q$, $c + d = r$ et $c - d = s$ prodeat haec aequalitas: $p^4 + s^4 = q^4 + r^4$, inde vicissim erit $p^4 - r^4 = q^4 - s^4$, unde sumptis factoribus erit

$$(p + r)(p - r)(pp + rr) = (q + s)(q - s)(qq + ss), \text{ sive}$$
$$(p + r)(p - r)[(p + r)^2 + (p - r)^2] = (q + s)(q - s)[(q + s)^2 + (q - s)^2].$$

Quamobrem si statuamus $p + r = a'$, $p - r = b'$, $q + s = c'$ et $q - s = d'$, habebimus $a'b'(a'a' + b'b') = c'd'(c'c' + d'd')$, quae ergo aequalitas locum habebit, si sumatur

$$a' = (a + b) + (c + d), \qquad b' = (a + b) - (c + d),$$
$$c' = (a - b) + (c - d) \quad \text{et} \quad d' = (a - b) - (c - d).$$

29. Cum igitur invenissemus $a = 291$, $b = 25$, $c = 193$ et $d = 75$, erit $a + b = 316$, $a - b = 266$, $c + d = 268$ et $c - d = 118$. Hinc colligitur fore $a' = 584$, $b' = 48$, $c' = 384$ et $d' = 148$, qui numeri per 4 depressi praebent solutionem simplicissimam, scilicet: $a' = 146$, $b' = 12$, $c' = 96$ et $d' = 37$; ita ut sit $146 \cdot 12\,(146^2 + 12^2) = 96 \cdot 37\,(96^2 + 37^2)$, ubi nempe est

$$146^2 + 12^2 = 21460 = 2^2 \cdot 5 \cdot 29 \cdot 37 \text{ et } 96^2 + 37^2 = 10585 = 5 \cdot 29 \cdot 73;$$

et nunc utrinque resultat idem productum $2^5 \cdot 3 \cdot 5 \cdot 29 \cdot 37 \cdot 73$. Ob insignem igitur usum huius regulae eam sequenti theoremate complectamur.

THEOREMA

30. *Si quatuor numeri a, b, c, d ita fuerint comparati, ut sit*

$$ab(aa + bb) = cd(cc + dd),$$

tum si inde formentur isti quaterni numeri:

$$A = (a + b) + (c + d), \qquad B = (a + b) - (c + d),$$
$$C = (a - b) + (c - d) \quad \text{et} \quad D = (a - b) - (c - d),$$

erit quoque

$$AB(A^2 + B^2) = CD(C^2 + D^2).$$

Hinc igitur patet pro qualibet solutione semper dari adhuc aliam ipsi coniugatam, ope huius theorematis inveniendam, ita ut perpetuo binae solutiones

coniugatae exhiberi queant, quae ita invicem sunt connexae, ut ope theorematis altera ex altera definiatur.

31. Quo nunc hinc alias solutiones facilius invenire liceat, formulas repertas ita adornemus, ut inde statim valores integri pro numeris a, b, c, d exhiberi queant. Hunc in finem, quoniam etiam pro q fractiones accipere licet, statim ponamus $q = \frac{f}{g}$, eritque

$$\alpha = \frac{ff}{ff-gg} \quad \text{et} \quad \beta = \frac{gg}{ff-gg},$$

unde fit

$$s = \frac{3ff+gg}{2(ff-gg)}.$$

Hinc cum porro fit

$$z = \frac{-3}{4\alpha+\beta(3\alpha+\beta)^2},$$

erit

$$z = \frac{-3(ff-gg)^3}{4f^6+f^4gg+10ffg^4+g^6},$$

unde fit

$$1+z = \frac{f^6+10f^4gg+ffg^4+4g^6}{4f^6+f^4gg+10ffg^4+g^6},$$

tum vero erit

$$sz = -\frac{3(3ff+gg)(ff-gg)^2}{2(4f^6+f^4gg+10ffg^4+g^6)},$$

ergo

$$1+sz = \frac{-f^6+17f^4gg+17ffg^4-g^6}{2(4f^6+f^4gg+10ffg^4+g^6)} = \frac{(ff+gg)(-f^4+18ffgg-g^4)}{2(4f^6+f^4gg+10ffg^4+g^6)}.$$

32. Cum igitur posuissemus

$$p = q(1+z) = \frac{f}{g}(1+z),$$

erit

$$p = \frac{f(f^6+10f^4gg+ffg^4+4g^6)}{g(4f^6+f^4gg+10ffg^4+g^6)}.$$

Denique habebamus $\frac{a}{c} = 1+sz$, unde si statuamus

$$a = (ff+gg)(-f^4+18ffgg-g^4) \quad \text{et} \quad c = 2(4f^6+f^4gg+10ffg^4+g^6),$$

cum fuerit $b = pc$ et $d = aq$, erit

$$b = \frac{2f(f^6 + 10f^4gg + ffg^4 + 4g^6)}{g}$$

et tandem

$$d = \frac{f(ff + gg)(-f^4 + 18ffgg - g^4)}{g}.$$

Multiplicemus igitur omnes hos valores per g, eritque ut sequitur:

$a = g(ff + gg)(-f^4 + 18ffgg - g^4)$, $c = 2g(4f^6 + f^4gg + 10ffg^4 + g^6)$,
$b = 2f(f^6 + 10f^4gg + ffg^4 + 4g^6)$, $d = f(ff + gg)(-f^4 + 18ffgg - g^4)$.

33. Hae quidem formulae numeros vehementer magnos producunt, qui autem plerumque per communem divisorem ad numeros multo minores redigi possunt. Veluti si, ut supra fecimus, sumamus $f = 3$ et $g = 1$, nostrae formulae dabunt $a = 800$, $b = 9312$, $c = 6176$ et $d = 2400$; hi autem numeri omnes divisionem admittunt per 32, quo pacto ad ipsos numeros supra inventos deprimuntur.

EXEMPLUM 2
QUO $f = 2$ et $g = 1$

34. Substitutis his valoribus reperiemus $a = 5 \cdot 55 = 275$, $b = 928$, $c = 626$ et $d = 550$, qui numeri ulterius ad minores deprimi non possunt. Huius solutionis etiam exhibeamus suam coniugatam secundum theorema supra datum; erit ergo $A = 2379$, $B = 27$, $C = 729$ et $D = 577$. Sicque duas nacti sumus novas solutiones.

Alia solutio aequationis
$ab(aa + bb) = cd(cc + dd)$

35. Posito ut ante $b = cp$ et $d = aq$ adepti sumus hanc aequationem: $\frac{aa}{cc} = \frac{p^3 - q}{q^3 - p}$, ita ut hanc fractionem ad quadratum redigi oporteat, ad quod praestandum hic alia via utamur, quam in forma generali adhibere non licuisset. Statuamus scilicet

$$p = 1 + \alpha z \quad \text{et} \quad q = 1 + \beta z,$$

reperieturque

$$\frac{aa}{cc} = \frac{3\alpha - \beta + 3\alpha\alpha z + \alpha^3 zz}{3\beta - \alpha + 3\beta\beta z + \beta^3 zz},$$

sicque pervenimus ad fractionem, in qua quantitas incognita z tam in numeratore quam in denominatore non ultra quadratum assurgit, cuiusmodi formulae satis commode tractari possunt, si fuerint vel primae partes absolutae quadrata, vel si partes postremae fuerint quadrata.

Evolutio casus prioris,
quo formulae $3\alpha - \beta$ *et* $3\beta - \alpha$ *sunt quadrata.*

36. Statuamus igitur

$$3\alpha - \beta = ff \quad \text{et} \quad 3\beta - \alpha = gg,$$

eritque

$$\alpha = \frac{3ff + gg}{8} \quad \text{et} \quad \beta = \frac{ff + 3gg}{8},$$

hocque modo habebimus

$$\frac{aa}{cc} = \frac{ff + 3\alpha\alpha z + \alpha^3 zz}{gg + 3\beta\beta z + \beta^3 zz},$$

quamobrem statuamus

$$aa = ff + 3\alpha\alpha z + \alpha^3 zz \quad \text{et} \quad cc = gg + 3\beta\beta z + \beta^3 zz.$$

Iam ut has formulas ad quadrata reducamus, formemus hanc aequalitatem:

$$aagg - ccff = 3(\alpha\alpha gg - \beta\beta ff)z + (\alpha^3 gg - \beta^3 ff)zz,$$

et quia hic membrum sinistrum duos habet factores $ag + cf$ et $ag - cf$, etiam membrum dextrum in duos factores resolvi oportet, quorum alter statuatur $ag + cf = \frac{z}{\lambda}$, eritque alter

$$ag - cf = 3\lambda(\alpha\alpha gg - \beta\beta ff) + \lambda(\alpha^3 gg - \beta^3 ff)z,$$

ubi ad valorem λ inveniendum primo fiat $z = 0$, et addantur quadrata horum duorum factorum, quorum summa erit

$$2(aagg + ccff) = 9\lambda\lambda(\alpha\alpha gg - \beta\beta ff)^2;$$

at vero ex ipsis formulis propositis, posito $z = 0$, ob $aa = ff$ et $cc = gg$ erit

$$2(aagg + ccff) = 4ffgg = 9\lambda\lambda(\alpha\alpha gg - \beta\beta ff)^2 ,$$

unde reperitur

$$\lambda = \frac{2fg}{3(\alpha\alpha gg - \beta\beta ff)} ,$$

quae forma, ob $ff = 3\alpha - \beta$ et $gg = 3\beta - \alpha$, abit in hanc

$$\lambda = \frac{2fg}{3(\beta - \alpha)^3} .$$

37. Invento iam hoc valore pro λ bini factores erunt

$$ag + cf = \frac{3(\beta - \alpha)^3 z}{2fg} \quad \text{et} \quad ag - cf = 2fg + \frac{2fg(\alpha^3 gg - \beta^3 ff)z}{3(\alpha\alpha gg - \beta\beta ff)} ,$$

sive

$$ag - cf = 2fg + \frac{2fg(\beta + \alpha)(\beta\beta - 3\alpha\beta + \alpha\alpha)z}{3(\beta - \alpha)^2} .$$

Statuamus autem brevitatis gratia

$$\frac{(\alpha + \beta)(\beta\beta - 3\alpha\beta + \alpha\alpha)}{3(\beta - \alpha)^2} = \Delta ,$$

ut sit

$$ag - cf = 2fg + 2fg\Delta z .$$

Addantur nunc iterum quadrata harum formarum, et prodibit:

$$2(aagg + ccff) = 4ffgg + 8ffgg\,\Delta z + 4ffgg\,\Delta^2 zz + \frac{9(\beta - \alpha)^6 zz}{4ffgg} .$$

Ex ipsis autem formulis propositis colligimus

$$2(aagg + ccff) = 4ffgg + 6(\alpha\alpha gg + \beta\beta ff)z + 2(\alpha^3 gg + \beta^3 ff)zz ,$$

ubi ergo prima membra se mutuo tollunt, reliqua per z divisa dabunt hanc aequationem:

$$6(\alpha\alpha gg + \beta\beta ff) + 2(\alpha^3 gg + \beta^3 ff)z = 8ffgg\,\Delta + 4ffgg\,\Delta^2 z + \frac{9(\beta - \alpha)^6 z}{4ffgg} ,$$

ex qua aequatione facile deducitur valor ipsius z. Has autem formulas ulterius non evolvamus, quoniam evolutio quovis casu speciali facilius instituetur.

Evolutio casus, quo $f = 3$ *et* $g = 1$

38. Hic igitur erit $\alpha = \frac{7}{2}$ et $\beta = \frac{3}{2}$, hinc ergo fiet

$$aa = 9 + \frac{147}{4}z + \frac{343}{8}zz \quad \text{et} \quad cc = 1 + \frac{27}{4}z + \frac{27}{8}zz;$$

porro vero erit $\Delta = -\frac{25}{48}$. Hinc ergo pro quantitate z invenienda habebimus hanc aequationem:

$$195 + \frac{293}{2}z = -\frac{75}{2} + \frac{625}{64}z + 16z = -\frac{75}{2} + \frac{1649}{64}z, \quad \text{sive} \quad \frac{465}{2} = -\frac{7727}{64}z,$$

unde fit $z = -\frac{14880}{7727}$. Hoc modo perveniremus ad nimis magnos numeros, quos ultra evolvere opere non est pretium.

39. Interim tamen haud difficile erit hinc adeo in genere valores idoneos pro litteris a, b, c, d exhibere. Sumptis scilicet pro lubitu binis quadratis ff et gg capiantur numeri α et β ita, ut sit

$$\frac{\alpha}{\beta} = \frac{3ff + gg}{3gg + ff};$$

scilicet postquam fractio $\frac{3ff+gg}{3gg+ff}$ ad minimos terminos fuerit reducta, numerator pro α, denominator vero pro β accipiatur, quo facto erunt numeri quaesiti[1])

$$\begin{aligned} a &= f(\alpha + \beta)(\alpha\alpha - 3\alpha\beta + \beta\beta), \\ b &= g(\beta^3 - 5\alpha\beta\beta + 4\alpha\alpha\beta - 2\alpha^3), \\ c &= g(\alpha + \beta)(\alpha\alpha - 3\alpha\beta + \beta\beta), \\ d &= f(\alpha^3 - 5\alpha\alpha\beta + 4\alpha\beta\beta - 2\beta^3). \end{aligned}$$

Vel si ponatur

$$(\alpha + \beta)(\alpha\alpha - 3\alpha\beta + \beta\beta) = \Delta,$$

erit

$$\begin{aligned} a &= f\Delta, \quad b = g(\Delta - 3\alpha(\alpha - \beta)^2), \\ c &= g\Delta \quad \text{et} \quad d = f(\Delta - 3\beta(\alpha - \beta)^2). \end{aligned}$$

Harum formularum ope exempla multo facilius evolvi poterunt

1) Vide formulas § 32, p. 345. R. F.

40. Ita si sumamus $f = 3$ et $g = 1$, erit $\frac{\alpha}{\beta} = \frac{28}{12} = \frac{7}{3}$; erit ergo $\alpha = 7$ et $\beta = 3$, hincque $\Delta = -50$, quocirca ipsi numeri quaesiti reperiuntur $a = 150$, $b = 386$, $c = 50$ et $d = 582$, qui porro per binarium depressi fiunt $a = 75$, $b = 193$, $c = 25$ et $d = 291$.

41. Consideremus nunc quoque casum, quo $f = 2$ et $g = 1$, eritque $\frac{\alpha}{\beta} = \frac{13}{7}$; quare capiatur $\alpha = 13$ et $\beta = 7$, unde fit $\Delta = -1100$, hincque ipsi numeri quaesiti prodeunt $a = 2200$, $b = 2504$, $c = 1100$, $d = 3712$, qui per 4 depressi evadunt $a = 550$, $b = 626$, $c = 275$, $d = 928$; quae solutio convenit cum solutione supra § 34 inventa.

42. Fundamentum huius Analyseos sequenti nititur problemati:

PROBLEMA

Propositis his duabus formulis: $xx + 2fxy + hyy$ nec non $xx + 2gxy + kyy$, invenire rationem inter numeros x et y, ut ambae istae formulae evadant quadrata.

SOLUTIO

43. Ponatur

$$xx + 2fxy + hyy = P^2 \quad \text{et} \quad xx + 2gxy + kyy = Q^2\,,$$

ac differentia dabit

$$PP - QQ = 2(f-g)\,xy + (h-k)\,yy.$$

Statuatur alter factor

$$P - Q = (f-g)\,y\,,$$

eritque alter

$$P + Q = 2x + \frac{(h-k)y}{f-g}\,.$$

Iam quadrata horum duorum factorum addantur, prodibitque

$$2P^2 + 2Q^2 = 4xx + \frac{4(h-k)xy}{f-g} + \frac{(h-k)^2yy}{(f-g)^2} + (f-g)^2yy\,;$$

ex ipsis autem formulis propositis erit

$$2P^2 + 2Q^2 = 4xx + 4(f+g)\,xy + 2(h+k)\,yy\,,$$

unde quia primi termini $4xx$ se destruunt, reliqui per y divisi dant hanc aequationem:

$$4(f+g)x + 2(h+k)y = \frac{4(h-k)x}{f-g} + \frac{(h-k)^2 y}{(f-g)^2} + (f-g)^2 y\,,$$

sive

$$4(f-g)\,[ff-gg-h+k]\,x = \Big((h-k)^2 + (f-g)^2\,[(f-g)^2 - 2(h+k)]\Big)y,$$

hinc igitur erit

$$\frac{x}{y} = \frac{(f-g)^4 - 2(h+k)(f-g)^2 + (h-k)^2}{4(f-g)(ff-gg-h+k)}.$$

44. Supra adhuc mentionem fecimus alius casus, quo ambae formulae pro aa et cc ad quadrata redigi queant (§ 35), ubi, ut partes postremae fiant quadrata, necesse est, ut ambo numeri α et β sint quadrata. Sit igitur $\alpha = mm$ et $\beta = nn$, eritque

$$aa = m^6 zz + 3m^4 z + 3mm - nn \quad \text{et}$$
$$cc = n^6 zz + 3n^4 z + 3nn - mm\,.$$

45. Has aequalitates ut ad formam superioris problematis revocemus, ita repraesentemus:

$$aan^6 = m^6 n^6 zz + 3m^4 n^6 z + 3mmn^6 - n^8 \quad \text{et}$$
$$ccm^6 = m^6 n^6 zz + 3n^4 m^6 z + 3nnm^6 - m^8\,,$$

et iam facta comparatione erit $x = m^3 n^3 z$, sumptoque $y = 1$ erit pro hoc casu $2fm^3 n^3 z = 3m^4 n^6 z$, unde fit

$$f = \frac{3}{2}mn^3 \quad \text{et} \quad g = \frac{3}{2}nm^3,$$

denique vero

$$h = 3mmn^6 - n^8 \quad \text{et} \quad k = 3nnm^6 - m^8,$$

unde colligitur

$$f - g = \frac{3}{2}mn(nn - mm)$$

et

$$h - k = 3mmn^6 + m^8 - 3nnm^6 - n^8 = (m^4 - n^4)(n^4 + m^4 - 3mmnn) .$$

Iam problema nobis praebet valorem

$$\frac{x}{y} = m^3n^3z = \frac{(f-g)^4 - 2(h+k)(f-g)^2 + (h-k)^2}{4(f-g)(ff-gg-h+k)} .$$

46. Coronidis loco subiungam hic adhuc aliam Analysin pro resolutione formulae $ab(aa + bb) = cd(cc + dd)$. Quoniam res perducta est ad hanc aequationem: $\frac{aa}{cc} = \frac{p^3-q}{q^3-p}$, ponatur $p = nn(q+1) - 1$, fietque

$$\frac{aa}{cc} = \frac{n^6(q+1)^3 - 3n^4(q+1)^2 + 3nn(q+1) - 1 - q}{q^3 - nn(q+1) + 1} ,$$

quae fractio per factorem $q + 1$ depressa dabit

$$\frac{aa}{cc} = \frac{n^6(q+1)^2 - 3n^4(q+1) + 3nn - 1}{qq - q + 1 - nn} ,$$

sive

$$aa = n^6qq + n^4(2nn - 3)q + (nn - 1)^3 ,$$

tum vero

$$cc = qq - q + 1 - nn \quad \text{sive} \quad n^6cc = n^6qq - n^6q - n^6(nn - 1) .$$

Pro problemate igitur capi oportebit $x = n^3q$ et $y = 1$; reliqua sunt manifesta.

FACILLIMA METHODUS PLURIMOS NUMEROS PRIMOS PRAEMAGNOS INVENIENDI

Commentatio 718 indicis Enestroemiani
Nova acta academiae scientiarum Petropolitanae 14 (1797/8), 1805, p. 3—10
Summarium ibidem p. 63—64
Conventui exhibita die 16. martii 1778

SUMMARIUM

Cette méthode consiste à chercher toutes les valeurs de a qui rendent les nombres de la forme $naa+1$ non-premiers. L'auteur explique cette méthode en l'appliquant à la formule $232aa+1$, laquelle produit toujours des nombres composés, lorsque $naa+1=nxx+yy$, et que n est un de ces nombres dont l'auteur a fait la recherche dans un mémoire: *De variis modis numeros praegrandes examinandi, utrum sint primi necne*[1]), où il y a une table de ces nombres, parmi lesquels se trouve aussi le nombre mentionné 232. Or si $232aa + 1 = 232xx + yy$, on a $232\,(aa - xx) = yy - 1$; et mettant $y = 1 \pm 58z$ on a $aa - xx = \frac{1}{2}z\,(29z \pm 1)$, ou bien $rs = \frac{1}{2}z\,(29z \pm 1)$ en posant $a + x = r$ et $a - x = s$, de sorte que $a = \frac{r+s}{2}$. En donnant donc successivement à z les valeurs 1, 2, 3, 4 etc., on obtient les valeurs r et s, et partant les valeurs a qui rendent la formule $232aa + 1$ un nombre composé. Tous ces nombres étant exclus, les autres donneront nécessairement tous les nombres premiers contenus dans cette formule, et par un calcul qui n'est ni long ni pénible on peut pousser cette recherche jusqu'à plusieurs millions.

1. Sufficiet hanc methodum unico exemplo, numerorum in hac formula $232aa + 1$ contentorum, explicasse, ubi omnes valores ipsius a investigabo,

1) Commentatio indicis Enestroemiani 715, Nova acta acad. sc. Petrop. 13 (1795/6), 1802, p. 14—44; p. 303 de ce volume. R. F.

quibus haec formula numeros compositos producit; his enim exclusis omnes reliqui numeri pro a assumti numeros primos suppeditabunt.

2. At si formula $232aa + 1$ praebeat numerum compositum, tum semper talis aequatio locum habebit:

$$232aa + 1 = 232xx + yy ,$$

propterea quod $232 = 8 \cdot 29$ est numerus idoneus[1]). Sic igitur erit

$$232(aa - xx) = yy - 1 .$$

Iam ponatur $y = 1 + 58z$, ac facta divisione per 232 prodibit ista aequatio: $aa - xx = \frac{1}{2} z (29z + 1)$, sive, quia unitatem tam positive quam negative accipere licet, erit

$$aa - xx = \tfrac{1}{2} z(29z \pm 1) .$$

3. Tribuantur nunc ipsi z ordine omnes valores 1, 2, 3 etc. et, quia formula $\frac{1}{2} z(29z \pm 1)$ certe duos factores, saepiusque plures, involvet, ea semel quoque vel pluribus modis per productum rs repraesentari poterit; cui cum aequalis esse debeat formula $aa - xx = (a + x)(a - x)$, statuatur $a + x = r$ et $a - x = s$, unde fit $a = \frac{r+s}{2}$, hocque modo reperientur valores pro a excludendi. Hic igitur evidens est ambos factores r et s simul vel pares vel impares esse debere.

4. His iam notatis sumamus $z = 1$, eritque duplici modo, pro ambiguitate signi, vel $rs = 14$ vel $rs = 15$, ubi prior valor, utpote impariter par, ad nostrum institutum est ineptus; posterior vero $rs = 15$ praebet duas exclusiones, vel enim erit $r = 15$ et $s = 1$ vel $r = 5$ et $s = 3$, unde valores pro a excludendi erunt 8 et 4.

5. Sit nunc $z = 2$, eritque $rs = 57$ vel $rs = 59$. Prior admittit duas resolutiones:

$$\begin{aligned} r &= 57, \quad r = 19, \\ s &= 1, \quad s = 3, \end{aligned}$$

1) Conf. Nov. Act. T. XIII, p. 33 [huius voluminis p. 320].

posterior unicam: $r = 59$ et $s = 1$, unde oriuntur hae tres exclusiones: $a = 29$, $a = 11$, $a = 30$.

6. Sit nunc $z = 3$, eritque vel $rs = 3 \cdot 43$ vel $rs = 3 \cdot 44$, quorum valorum resolutiones ita referentur:

$$\begin{array}{llll|llll} r = 129, & r = 43, & & & r = 66, & r = 22, & & \\ s = \ 1, & s = \ 3, & & & s = \ 2, & s = \ 6, & & \end{array}$$

unde quatuor exclusiones prodeunt

$$a = 65, \quad a = 23, \quad a = 34, \quad a = 14.$$

7. Sit $z = 4$, erit vel $rs = 230$ vel $rs = 234$, qui numeri, utpote impariter pares, nullas dant exclusiones.

8. Sit nunc $z = 5$, erit $rs = 5 \cdot 72$ vel $rs = 5 \cdot 73$, unde ex priore sequentes prodeunt resolutiones:

$$\begin{array}{llllll} r = 180, & r = 90, & r = 60, & r = 36, & r = 30, & r = 20, \\ s = \ 2, & s = \ 4, & s = \ 6, & s = 10, & s = 12, & s = 18. \end{array}$$

Hinc ergo valores ipsius a excludendi erunt 91, 47, 33, 23, 21, 19. Alter valor dat $r = 73$, $s = 5$ vel $r = 365$, $s = 1$, unde exclusiones hinc natae sunt 39 et 183.

8a[1]). Sit $z = 6$, erit vel $rs = 3 \cdot 173$ vel $rs = 3 \cdot 175$, unde sequentes resolutiones:

$$\begin{array}{llll|llllll} r = 519, & 173, & & & r = 525, & 175, & 105, & 75, & 35, & 25, \\ s = \ 1, & 3, & & & s = \ 1, & 3, & 5, & 7, & 15, & 21. \end{array}$$

Exclusiones ergo nascuntur istae:

$$260, \quad 88, \quad 263, \quad 89, \quad 55, \quad 41, \quad 25, \quad 23.$$

9. Sit nunc $z = 7$, erit vel $rs = 7 \cdot 101$ vel $rs = 7 \cdot 102$. Hic solus prior casus dat has resolutiones:

1) Editio princeps continet duas paragraphos 8. R. F.

$$r = 707, \quad r = 101,$$
$$s = 1, \quad s = 7,$$

hincque exclusiones erunt 354 et 54. Ut autem nobis terminum praescribamus, in posterum omnes exclusiones maiores quam 300 praetermittamus.

10. Sit nunc $z = 8$, erit vel $rs = 4 \cdot 3 \cdot 7 \cdot 11$ vel $rs = 4 \cdot 233$. Resolutiones hinc nascuntur sequentes:

$r =$	462,	154,	66,	42,	$r =$	466,
$s =$	2,	6,	14,	22,	$s =$	2,

unde concludimus sequentes exclusiones:

$$a = 232, \ 80, \ 40, \ 32, \ 234.$$

11. Sit $z = 9$, erit vel $rs = 9 \cdot 130$ vel $rs = 9 \cdot 131$, hinc a secunda

$$r = 393, \quad 131,$$
$$s = 3, \quad 9,$$

excluditur igitur $a = 198, \ 70$.

12. Sit $z = 10$, erit vel $rs = 3 \cdot 5 \cdot 97$ vel $rs = 5 \cdot 17 \cdot 17$, hinc

$r =$	485,	291,	97,	$r =$	289,	85,
$s =$	3,	5,	15,	$s =$	5,	17,

unde excluditur

$$a = 244, \ 148, \ 56, \ 147, \ 51.$$

13. Sit $z = 11$, erit vel $rs = 3 \cdot 11 \cdot 53$, vel $rs = 32 \cdot 5 \cdot 11$, hinc

$r =$	583,	159,	53,	440,	220,	176,	88,	80,	110,	44,
$s =$	3,	11,	33,	4,	8,	10,	20,	22,	16,	40,
hinc $a =$	293,	85,	43,	222,	114,	93,	54,	51,	63,	42.

14. Sit $z = 12$, erit vel $rs = 6 \cdot 347$ vel $rs = 6 \cdot 349$, quorum neuter dat exclusionem.

15. Sit $z = 13$, erit vel $rs = 13 \cdot 4 \cdot 47$ vel $rs = 27 \cdot 13 \cdot 7$, hinc

$r =$ 94,	351,	273,	189,	117,	91,	63,
$s =$ 26,	7,	9,	13,	21,	27,	39,
excluduntur ergo 60,	179,	141,	101,	69,	59,	51.

16. Hoc modo calculum ulterius prosequi licet, quousque visum fuerit. Exclusiones ex singulis valoribus ipsius z ortas sequenti tabula repraesentemus:

z	Exclusiones
1	4, 8,
2	11, 29, 30,
3	14, 23, 34, 65,
4	— — — —
5	19, 21, 23, 33, 39, 47, 91, 183,
6	23, 25, 41, 55, 88, 89, 260, 263,
7	54,
8	32, 40, 80, 232, 234,
9	70, 198,
10	51, 56, 147, 148, 244,
11	42, 43, 51, 54, 63, 85, 93, 114, 222, 293,
13	51, 59, 60, 69, 101, 141, 179,
14	54, [57], 58, 66, 78, 102, 135, 162, 206, 207, [286],
15	64, 68, 88, 116, 236,
16	61, 77, 103, 161, 191,
17	120, 132, 168,
18	265, 266,
19	75, 80, 88, [117], 147, 243,
21	80, 83, 85, 97, 103, 109, 128, 145, 163, 221, 235, 272,
22	84, [85], 96, 123, 276,
23	90, 122, 178,
24	92, 140, 154,
25	98, 110, 154, 194,
26	108, 145,
27	103, 105, 111, 125, 129, 147, [165], 203, 209, 241,
29	122, 134, 166, 218, 225,
30	122, 131, 133, 146, 187, 214,
31	240,
32	139, 224,
33	256,
34	130, 141, 190, [202],
35	137, 143, 162, 169, 247, 271.
37	141, 145, 171, 287,

z	Exclusiones
38	212,
39	154, 202,
40	156, 174, 178, 242,
41	162, 186,
42	160, 220, 268,
43	164, [181], 195, 199, 211, 284,
45	208,
46	191, 217, 257,
47	184,
48	185, 241, 253,
49	[192], 260,
50	191, 193, [215, 225, 279, 297],
51	196, 236, 292,
53	202, 223, 245, 260,
54	224,
56	216, 240,
58	224, 236, 296,
59	225, 231, 233, 273,
61	239, 241, 282,
62	237,
63	240,
64	246, 282,
65	252,
66	274,
67	282,
69	263, 265, 295, 263, 265,
71	278,
73	286,
75	286, 290,
78	298.

17. Inter hos numeros excludendos pro littera a nonnulli bis vel ter occurrunt, quod evenit, quando numerus $232aa + 1$ tres pluresve habet factores; ita videmus numerum 265 primo a valore $z = 18$, deinde bis a valore $z = 69$ excludi. Hoc autem casu revera numerus $232 \cdot 265^2 + 1$ constat his tribus factoribus: $59 \cdot 461 \cdot 599$, atque adeo praeter istam formam tres sequentes recipit:

$$1^\circ \quad 232 \cdot 256^2 + 1043^2,$$
$$2^\circ \quad 232 \cdot 34^2 + 4003^2,$$
$$3^\circ \quad 232 \cdot 35^2 + 4001^2.$$

18. Referamus autem in tabulam omnes hos numeros excludendos, secundum ordinem dispositos, atque eos, qui plus quam semel occurrunt, asterisco notemus:

0	4, 8,
1	11, 14, 19,
2	21, 23*, 25, [29],
3	30, 32, 33, 34, 39,
4	40, 41, 42, 43, 47,
5	51*, 54*, 55, 56, [57], 58, 59.
6	60, 61, 63, 64, 65, 66, 68, 69,
7	70, 75, 77, 78,
8	80*, 83, 84, 85*, 88*, 89,
9	90, 91, 92, 93, 96, 97, 98,
10	101, 102, 103*, 105, 108, 109,
11	110, 111, 114, 116, [117],
12	120, 122*, 123, 125, 128, 129,
13	130, 131, 132, 133, 134, 135, 137, 139,
14	140, 141*, 143, 145*, 146, 147*, 148,
15	154*, 156,
16	160, 161, 162, 163, 164, [165], 166, 168, 169,
17	171, 174, 178*, 179,
18	[181], 183, 184, 185, 186, 187,
19	190, 191*, [192], 193, 194, 195, 196, 198, 199,
20	202*, 203, 206, 207, 208, 209,
21	211, 212, 214, [215], 216, 217, 218,
22	220, 221, 222, 223, 224*, 225*,
23	231, 232, 233, 234, 235, 236*, 237, 239,
24	240*, 241*, 242, 243, 244, 245, 246, 247,
25	252, 253, 256, 257,
26	260*, 263*, 265*, 266, 268,
27	271, 272, [273], 274, 276, 278, [279],
28	282*, 284, 286*, 287,
29	290, 292, 293, 295, 296, [297], 298.

His igitur numeris exclusis reliqui omnes loco a scripti in formula $232aa + 1$ producunt numeros primos. Hos igitur valores ipsius a sequens exhibet tabula[1]):

1,	2,	3,	5,	6,	7,	9,	10,	12,	13,	15,
16,	17,	18,	20,	22,	24,	26,	27,	28,	31,	35,
36,	37,	38,	44,	45,	46,	48,	49,	50,	52,	53,
62,	67,	71,	72,	73,	74,	76,	79,	81,	82,	86,
87,	94,	95,	99,	100,	104,	106,	107,	112,	113,	115,
118,	119,	121,	124,	126,	127,	136,	138,	142,	144,	149,
150,	151,	152,	153,	155,	157,	158,	159,	167,	170,	172,
173,	175,	176,	177,	180,	182,	188,	189,	197,	200,	201,
204,	205,	210,	213,	219,	226,	227,	228,	229,	230,	238,
248,	249,	250,	251,	254,	255,	258,	259,	261,	262,	264,
267,	269,	270,	275,	277,	280,	281,	283,	285,	288,	289,
291,	294,	299;								

horum numerorum ultimi fere ad 20 milliones exsurgunt.

1) Haec tabula in editione principi et in „Opera minora collecta“ continet numeros 57, 117, 165, 181, 192, 196, 215, 273, 279, 297 et in editione principi continet numerum 29. A. M.

METHODUS GENERALIOR NUMEROS QUOSVIS SATIS GRANDES PERSCRUTANDI UTRUM SINT PRIMI NECNE[1])

Commentatio 719 indicis Enestroemiani
Nova acta academiae scientiarum Petropolitanae 14 (1797/8), 1805, p. 11—51
Summarium ibidem p. 64
Conventui exhibita die 16. martii 1778

SUMMARIUM

Si le nombre à examiner N est réductible à la forme $aa + \lambda bb$ et qu'on peut le représenter encore d'une autre manière par la forme semblable $xx + \lambda yy$, il sera certainement non-premier, et on aura $\frac{a+x}{y+b} = \lambda\frac{y-b}{a-x}$. Ayant réduit cette fraction à ses moindres termes $\lambda\frac{p}{q}$, on mettra $a + x = \lambda mp$ et $y - b = np$, et on aura $a - x = nq$ et $y + b = mq$, de sorte que $a = \frac{\lambda mp + nq}{2}$ et $b = \frac{mq - np}{2}$, et $\lambda pp + qq$ sera nécessairement un facteur du nombre proposé N. Tout revient donc dans cette recherche à s'assûrer, si le nombre $N = aa + \lambda bb$ est aussi compris dans une autre forme $xx + \lambda yy$ semblable à celle-là, ou non? Dans le premier cas on trouvera facilement ses facteurs; dans le second cas on peut être sûr que le nombre proposé est premier. L'auteur a éclairci cette méthode par l'examen de plusieurs grands nombres, parmi lesquels les plus grands nombres premiers sont 11866009, 18518809.

1. Sit N numerus propositus, et non difficile erit eum reducere ad huiusmodi formam: $N = aa + \lambda bb$; tum vero inquiratur, utrum adhuc alio modo

1) Confer Commentationes 708, 715 et 718 indicis Enestroemiani, huius voluminis p. 269, 303 et 352. R. F.

ad similem formam reduci queat. Si enim quoque fuerit $N = xx + \lambda yy$, ita ut sit

$$aa + \lambda bb = xx + \lambda yy ,$$

tum certe numerus N non erit primus, sed eius factores hoc modo assignari poterunt. Quoniam hinc est

$$aa - xx = \lambda(yy - bb) ,$$

erit

$$\frac{a+x}{y+b} = \lambda\frac{y-b}{a-x},$$

quae fractiones ad minimos terminos reducti sint $\lambda\frac{p}{q}$. Ponatur igitur

$$a + x = \lambda mp \quad \text{et} \quad y - b = np ,$$

erit

$$y + b = mq \quad \text{et} \quad a - x = nq ,$$

et hinc reperietur

$$a = \frac{\lambda mp + nq}{2} \quad \text{et} \quad b = \frac{mq - np}{2} ,$$

ex quibus valoribus erit

$$N = \tfrac{1}{4}(\lambda mm + nn)(\lambda pp + qq) ;$$

unde patet formulam $\lambda pp + qq$ vel ipsam vel eius semissem vel quadrantem esse factorem numeri propositi N.

2. Quando autem ad talem formam $N = aa + \lambda bb$ pervenimus, tum statuamus $N = xx + \lambda yy$, ubi statim facile patebit, utrum hi numeri x et y sint pares an vero impares, quo reperto statuatur vel $N - xx = \lambda yy$ vel $N - \lambda yy = xx$; ac priori quidem casu numerus x ita accipi debet, ut $N - xx$ dividi queat per numerum λ. Hoc modo ad novas formulas pervenietur, quae quadrata fieri debent, in quibus inerit numerus incognitus, qui, prout fuerit acceptus vel par vel impar, ad casus perducet seorsim evolvendos. Omnes autem istae operationes facilius exemplis docebuntur.

EXEMPLUM
$N = 10003$

3. Sit numerus examinandus $N = 10003 = 100^2 + 3 \cdot 1^2$, ubi ergo $\lambda = 3$. Statuatur $N = xx + 3yy$, et quia horum numerorum x et y alter necessario est par, alter impar, videamus ante omnia, uter eorum sit par, uter impar. Quoniam autem N est numerus formae $8n + 3$, si y esset par, foret $3yy$ numerus vel formae $8n + 4$ vel formae $8n + 0$; at tum foret xx formae $8n + 5$[1]) vel $8n + 1$, quorum neutra hic locum habere potest. Sumi ergo debebit x par, eritque xx vel formae $8n + 0$ vel formae $8n + 4$; et quia tum y est impar, erit $3yy$ formae $8n + 3$, ideoque xx formae $8n + 0$ et x numerus pariter par.

4. Quod si ergo statuamus $N - 3yy = xx$, istum numerum divisibilem esse oportet per 16; unde si ponamus $y = 1 + 2a$, haec aequatio dabit $10000 - 12a - 12aa = xx$, quae per 4 divisa abit in $2500 - 3a - 3aa = \frac{xx}{4}$. Unde patet numerum a[2]) denuo per 4 divisibilem esse debere; vel potius statim poni potuisset $y = 1 + 8a$[3]), unde prodiisset aequatio

$$625 - 3a - 12aa = \frac{xx}{16} = \square .$$

5. Nunc iam duos distinguamus casus, prouti numerus a capiatur vel par vel impar. Sit igitur primo a numerus par, et quia numerus absolutus 625 iam habet formam $8n + 1$ et $12aa$ formam $8n$, necesse est, ut etiam $3a$ divisionem per 8 admittat. Hinc statim ponatur $a = 8b$ fietque $625 - 24b - 12 \cdot 64bb = \square$. Quia igitur a numero absoluto 625 subtrahi debet forma $768bb \pm 24b$, patet valorem minimum $b = 1$ iam esse nimis magnum, hincque nullum oriri posse quadratum. Ex valore quidem $b = 0$ prodiret quadratum, sed ad casum cognitum pertinens.

6. Consideremus igitur casum, quo a est numerus impar, cuius forma cum sit duplex, vel $4n + 1$ vel $4n - 1$, statuatur primo $a = 4c + 1$, eritque $610 - 108c - 192cc = \square$, qui numerus, cum sit impariter par, quadratum esse nequit.

---

1) qui casus impossibilis est. R. F.
2) aut $a + 1$. A. M.
3) a potest numerum negativum esse. A. M.

7. Tantum igitur examinandus superest casus, quo $a = 4d - 1$[1]), qui praebet hanc aequationem: $616 + 84d - 192dd = \square$, quae per 4 divisa in hanc abit: $154 + 21d - 48dd = \frac{xx}{64} = \square$. A numero igitur absoluto 154 subtrahi debent numeri minores in forma $48dd \mp 21d$ contenti, qui sunt 27, 69, 150, quorum ultimus subtractus relinquit quadratum 4, ex valore $d = +2$ desumto. Hinc igitur erit $a = 7$, $y = 57$ et $x = 16$.

8. Nacti ergo sumus aliam insuper resolutionem numeri $N = 10003$, cognitae similem, quae est $10003 = 16^2 + 3 \cdot 57^2$. Quare cum iam habeamus $\lambda = 3$, $a = 100$, $b = 1$, $x = 16$ et $y = 57$, hinc ex § 1 erit

$$\frac{3p}{q} = \frac{116}{58} = 3 \cdot \frac{56}{84} = 3 \cdot \frac{2}{3},$$

ideoque $p = 2$ et $q = 3$, consequenter $3pp + qq = 21$, quod per 3 depressum dat 7, qui numerus revera est divisor numeri propositi 10003, quoto existente $= 1429$, numero primo.

9. Hoc exemplum innititur formula $3xx + yy$, de qua satis rigide iam est demonstratum omnes numeros, qui unico modo in ea continentur, certe esse primos; quae proprietas absolute necessaria est ad omnes numeros primos hac ratione explorandos. Nisi enim formula $\lambda xx + yy$ hac proprietate gaudeat, de numeris, qui unico modo in ea continerentur, tuto pronunciari non posset eos esse primos; veluti casu $a = 11$, quo in formula $11xx + yy$ numerus 15 unico tantum modo continetur, etiamsi certe non sit primus.

10. Quin etiam haec formula generaliori modo ita exhiberi potest: $\alpha xx + \beta yy$, de qua itidem est demonstratum omnes numeros, qui duplici modo in ea contineantur, non esse primos, sed compositos, quorum adeo factores facile assignari poterunt. Si enim duplici modo fuerit $N = \alpha aa + \beta bb$, tum vero etiam $N = \alpha AA + \beta BB$, hinc formetur fractio $\frac{p}{q} = \frac{a \pm A}{b \pm B}$; tum semper formula $\alpha pp + \beta qq$ praebebit factorem numeri N, postquam scilicet per minores divisores α, β, 2, si quos admittit, fuerit depressa.

11. Contra vero, si quispiam numerus N unico tantum modo in formula $\alpha xx + \beta yy$ contineatur, inde non semper concludi potest hunc numerum esse

1) $a = \pm 4d - 1$. A. M.

primum, siquidem innumerabiles exhiberi possunt huiusmodi formulae, in quibus etiam numeri compositi semel tantum contineantur, cuius rei exemplum iam supra attulimus. Hanc ob circumstantiam maxime necessarium est formulas huius posterioris indolis a prioribus distinguere atque a praesenti negotio prorsus excludere. Demonstravi autem alio loco[1]) regulam, cuius ope formae posterioris indolis dignosci atque adeo e medio tolli poterunt. Regula autem ista ita se habet:

12. Proposita formula $\alpha xx + \beta yy$, de qua quaeritur, utrum in ea numeri compositi unico tantum modo contineri queant necne, consideretur haec formula $\alpha\beta + zz$, ubi ipsi z omnes successive tribuantur valores ad productum $\alpha\beta$ primi, sive ii ipsius z valores excludantur, qui cum hoc producto communem habent divisorem; tum vero sufficit hos numeros ex formula $\alpha\beta + zz$ resultantes tantum usque ad terminum $4\alpha\beta$ continuare. Quod si enim omnes hi numeri fuerint primi, formula $\alpha xx + \beta yy$ tuto in nostro negotio usurpari poterit; sin autem unicus inter eos fuerit numerus compositus, tum haec formula penitus erit reiicienda. In hoc autem iudicio probe est tenendum numeros quadratos instar primorum esse spectandos, pariter ac dupla primorum et potestates binarii, quae circumstantia summi in diiudicatione nostra est momenti.

13. Illustremus hanc regulam aliquibus exemplis; ac primo quidem proposita sit haec forma: $7xx + 2yy$, unde consideretur haec expressio: $14 + zz$, ubi ipsi z successive tribuantur valores ad 14 primi: 1, 3, 5, unde resultant numeri 15, 23, 39, quorum primus cum iam sit compositus, pariter ac tertius, formulam propositam tanquam ineptam excludi oportet perinde atque hanc ad idem iudicium deducentem: $14xx + yy$.

14. Proposita formula $30xx + yy$, in forma $30 + zz$ ipsi z tribuantur valores impares ad 30 primi, qui sunt 1 et 7, unde oriuntur numeri 31 et 79, qui cum ambo sint primi, haec formula in praesenti negotio tuto adhiberi poterit, nec non sequentes hinc oriundae: $15xx + 2yy$, $6xx + 5yy$, $10xx + 3yy$.

15. Proposita sit formula $120xx + yy$; ubi in forma $120 + zz$ ipsi z tribui debent hi valores impares ad 120 primi: 1, 7, 11, 13, 17; numerus enim 19 praeberet numerum quadruplum producti $\alpha\beta = 120$ superantem. Inde

1) Confer paragraphos 9, 10 et 11 cum commentatione 715 (huius voluminis p. 303), quae continet demonstrationes. R. F.

autem colliguntur numeri sequentes: 121, 169, 241, 289, 409, qui cum sint vel primi vel quadrati, hinc concludimus formulam propositam perinde ac sequentes inde desumtas scilicet: $40xx + 3yy$, $24xx + 5yy$, $15xx + 8yy$ tanquam idoneas spectari debere et in examine tuto admitti posse.

16. Sit proposita formula $7xx + 5yy$, et in hac expressione $35 + zz$ valores ipsi z tribuendi erunt: 1, 2, 3, 4, 6, 8, 9, qui praebent hos numeros: 36, 39, 44, 51, 71, 99, 116, ubi cum adeo sex sint compositi, hanc formam omnino excludi oportet.

17. Habeatur formula $15xx + 7yy$, et in expressione $105 + zz$ ipsi z tribuendi erunt hi valores ad 105 primi: 1, 2, 4, 8, 11, 13, 16, 17, qui praebent hos numeros, omnes pro primis habendos: 106, 109, 121, 169, 226, 274, 361, 394, unde sequentes formulae in classem idoneorum sunt ponendae: $105xx + yy$, $35xx + 3yy$, $21xx + 5yy$, $15xx + 7yy$.

18. Addamus his exemplis examen formulae $57xx + yy$, et numeri loco z successive scribendi, scilicet 1, 2, 4, 5, 7, 8, 10, 11, 13 hos praebent valores formae $57 + zz$ notatu dignos: 58, 61, 73, 82, 106, 121, 157, 178, 226, qui omnes sunt vel primi vel quadrati vel dupli primorum, ita ut formula proposita certe sit inter idoneos referenda.

19. Haec sufficient ad insignem simulque facillimum usum nostrae regulae illustrandum, cuius ope casus idoneos formulae $\alpha xx + \beta yy$ ab ineptis discernere valemus; qua igitur regula stabilita, illos casus optimo cum successu adhibere poterimus ad numeros quosvis in talibus formulis contentos, utrum sint primi necne, perscrutandos. Proposito scilicet numero quocunque N facile erit illum pluribus modis ad talem formam $\alpha xx + \beta yy$ reducere, quo facto talis eligatur casus, qui per regulam supra datam non excludatur, ac dispiciatur, utrum ille numerus N unico tantum modo an vero pluribus in hac forma contineatur. Priore enim casu certe erit primus, posteriori vero compositus, cuius factores ope methodi supra traditae facile assignare licebit.

EXEMPLUM 1
$N = 100003$

20. Proponatur numerus $N = 100003$, qui manifesto in forma $10xx + 3yy$ continetur, existente $x = 100$ et $y = 1$. Videamus ergo, an iste numerus adhuc alio modo in eadem forma contineatur. Hunc in finem ponamus

$$100003 - 3yy = 10xx,$$

atque ut divisio per 10 succedat, ponatur $y = 1 + 10z$, hincque orietur $10000 - 6z - 30zz = xx$, sive facta adhuc divisione per 4 erit

$$2500 - \frac{3}{2}z - \frac{15}{2}zz = \frac{xx}{4}.$$

Hinc igitur, prouti z fuerit vel par vel impar, formemus duos casus principales. Pro primo scilicet sit $z = 2a$, orietur aequatio

$$A = 2500 - 3a - 30aa = \frac{xx}{4}.$$

Pro altero casu sit $z = 2b - 1$, orietur ista:

$$B = 2494 + 27b - 30bb = \frac{xx}{4}.$$

Evolutio Formulae

$$A = 2500 - 3a - 30aa = \frac{1}{4}xx$$

21. Hic statim patet sumto $a = 0$ prodire quadratum, praebens casum cognitum $x = 100$ et $y = 1$. Iam iterum duos casus distinxisse conveniet, quibus a est numerus vel par vel impar; ac priori quidem evidens est pro a sumi debere numerum pariter parem. Sit ergo primo $a = 4c$, et facta divisione per 4 oritur haec aequatio: $C = 625 - 3c - 120cc = \frac{1}{16}xx$. Hic igitur, quia c tam positive quam negative sumi poterit, numeri a 625 successive subtrahendi ordine erunt sequentes in forma $120cc \pm 3c$ contenti: 117, 123, 474, 486, unde autem nullum plane quadratum resultat.

22. Tribuamus nunc ipsi a valorem imparem, qui sit $a = 4d \pm 1$, et facile est videre solum signum inferius valere posse. Fiat igitur $a = 4d - 1$, et aequatio per 4 divisa evadet $D = 2473 + 228d - 480dd$. Hinc igitur a numero absoluto 2473 successive subtrahi debent numeri sequentes in forma $480dd \pm 228d$ contenti, scilicet 252, 708, 1464, 2376, unde iterum nullum quadratum resultat.

Evolutio Formulae

$$B = 2494 + 27b - 30bb = \frac{xx}{4}$$

23. Hic statim patet, si pro b capiatur numerus par, eum impariter parem esse debere. Sit igitur $b = 4e + 2$, et facta divisione per 4 aequatio hinc resultans erit $B = 607 - 93e - 120ee = \frac{xx}{16}$. A numero ergo absoluto 607 subtrahi debent sequentes in forma $120ee \pm 93e$ contenti, qui sunt 27, 213, 294; ubi autem nullum quadratum occurrit.

24. Denique pro b numeros impares tentemus. Facile autem patet poni debere $b = 4f - 1$, ita tamen, ut numerus f sit impar, qui ergo ponatur $= 2g + 1$, eritque $b = 8g + 3$, unde oritur haec aequatio:

$$2305 - 1224g - 1920gg = \frac{xx}{4}.$$

Hic ergo unicus numerus 696 ab absoluto 2305 subtrahendus occurrit, unde autem numerus non-quadratus relinquitur. Quoniam igitur ex toto hoc calculo nullus numerus quadratus prodiit, iam certo pronunciare possumus numerum propositum 100003 esse primum.

Brevior Methodus
in hunc numerum inquirendi

25. Quoniam ante habuimus $100003 = 10 \cdot 100^2 + 3 \cdot 1^2$, etiam statuere poterimus $100003 = 40 \cdot 50^2 + 3 \cdot 1^2$, ita ut sit $\alpha = 40$ et $\beta = 3$, qui casus, uti supra vidimus, admittitur. Hanc ob rem statuamus $100003 - 3yy = 40xx$, fiatque $y = 1 + 20z$[1]), et facta divisione per 40 statim pervenimus ad hanc aequationem: $2500 - 3z - 30zz = xx$; ubi duo casus considerandi occurrunt, prouti z fuerit numerus par vel numerus impar, quorum utrumque seorsim evolvamus.

26. Pro priore casu evidens est pro z sumi debere numerum pariter parem. Sit ergo $z = 4a$, et facta divisione per 4 oritur haec aequatio:

$$625 - 3a - 120aa = \frac{xx}{4}.$$

1) Ubi non necesse est z numerus integer sumi debere; $y = 9 + 20z$ itidem possibilis est. R.F.

Hic ergo a numero absoluto 625 sequentes ex forma $120aa \pm 3a$ desumti sunt subtrahendi: 117, 123, 474, 486. Hinc autem nullum occurrit quadratum praeter casum $a = 0$, qui per se iam est notus.

27. Superest, ut pro z numerum imparem scribamus, qui sit $z = 2b - 1$, fietque aequatio $2473 + 114b - 120bb = xx$, qui numerus cum sit impar ideoque debeat esse formae $8n + 1$, evidens est sumi debere $b = 4c$, unde prodit haec aequatio: $2473 + 456c - 1920cc = xx = \square$. Sumto igitur $c = \pm 1$ numeri a 2473 subtrahendi erunt 1464 et 2376, quorum neuter quadratum relinquit. Hinc eadem, quam supra, conclusio: numerum 100003 certo esse primum. Ex posteriori autem huius numeri examine intelligere licet in genere eo maius lucrum exspectari posse, quo maiores numeros pro α et β accipere liceat.

EXEMPLUM 2

$$N = 1000003$$

28. Propositus sit numerus $N = 1000003$, qui manifesto continetur in formula: $3 \cdot 1^2 + 1 \cdot 1000^2$. Quoniam autem, uti modo monuimus, expedit pro α et β numeros maiores adhibere, idem quoque numerus facile repertus est contineri in forma $3 \cdot 577^2 + 19 \cdot 8^2$, ita ut sit $\alpha = 3$ et $\beta = 19$, ideoque $\alpha\beta = 57$, qui numerus, uti commode evenit, inter idoneos iam supra est relatus[1]). Hanc ob rem statuamus $1000003 - 3xx = 19yy$, atque ipsi x talis valor tribui debet, ut formula haec divisionem per numerum 19 admittat. Quare cum in casu cognito sit $x = 577 = 30 \cdot 19 + 7$, ponamus hic $x = 7 + 19z$, et facta divisione per 19 orietur haec aequatio: $52624 - 42z - 57zz = yy$. Ubi statim duo casus considerandi occurrunt, prouti z fuerit numerus par vel impar. Pro priori casu statuatur $z = 2a$, et aequatio per 4 divisa ita se habebit:

$$13156 - 21a - 57aa = \frac{yy}{4}, \text{ quam vocemus } = A.$$

Pro altero casu ponatur $z = 4b - 1$, quoniam facile est videre valorem $z = 4b + 1$ penitus excludi. Hinc ergo orietur haec altera aequatio principalis:

$$B = 52609 + 288b - 912bb = yy.$$

Has igitur duas aequationes A et B, principales, seorsim ulterius evolvamus.

1) Vide paragraphum 18, p. 365 huius voluminis. R. F.

Evolutio Formulae

$$A = 13156 - 21a - 57aa = \frac{yy}{4}$$

29. Hic subdivisio in duos alios casus institui debet, quorum quisque iterum seorsim evolvatur. Sit primo a numerus par, et quidem $a = 4c$, qui valor, in aequatione A substitutus, producit sequentem aequationem, postquam scilicet divisio per 4 fuerit facta:

$$C = 3289 - 21c - 228cc = \frac{yy}{16}.$$

Hic ergo a numero absoluto 3289 successive subtrahi debent numeri in forma $228cc \pm 21c$ contenti, qui sunt:

si c numerus negativus: 207, 870, 1989,
si c numerus positivus: 249, 954, 2115,

unde autem nullum quadratum resultat.

30. Sumamus ergo pro a numerum imparem, qui manifesto debet esse formae $4d - 1$. Facta igitur substitutione $a = 4d - 1$ simulque divisione per 4, orietur haec aequatio:

$$D = 3280 + 93d - 228dd.$$

Hinc numeri formae $228dd \pm 93d$ a numero absoluto 3280 successive subtrahendi erunt[1]),

si d numerus negativus: 135, 726, 1773, 3276,
si d numerus positivus: 321, 1098, 2331,

quorum quartus prioris seriei dat quadratum 4 ex casu $d = -4$, unde fit $y = 8$, qui casus iam est cognitus, praeter quem hic nullum amplius quadratum occurrit.

Evolutio Formulae

$$B = 52609 + 288b - 912bb = yy$$

31. Hic ergo a numero absoluto 52609 successive subtrahantur numeri in formula $912bb \pm 288b$ contenti, quos hic in gemina columna, una cum eorum differentiis, tam pro valoribus ipsius b positivis quam negativis repraesentemus:

1) Ubi $a = -4d - 1$ ponatur. R. F.

b	$912bb - 288b$	Diff.	b	$912bb + 288b$	Diff.
0	0		0	0	
		624			1200
1	624		1	1200	
		2448			3024
2	3072		2	4224	
		4272			4848
3	7344		3	9072	

32. Iam vero loco successivae subtractionis numerorum in forma $912bb \pm 288b$ contentorum differentiae eorum augmento constanti 1824 crescentes continuo subtrahi poterunt, quos in subsidium calculi hic subiungamus:

624	1200
2448	3024
4272	4848
6096	6672
7920	8496
9744	10320
11568	12144

33. Nunc igitur hi numeri a numero absoluto 52609 continuo subtrahantur ac dispiciatur, an usquam numerus quadratus relinquatur, quem calculum commode in duabus columnis hoc modo repraesentare licet:

52609	52609
624	1200
51985	51409
2448	3024
49537	48385
4272	4848
45265	43537
6096	6672
39169	36865
7920	8496
31249	28369
9744	10320
21505	18049
11568	12144
9937	5905

ubi nullum plane quadratum occurrit, pariter ac in praecedentibus, casu scilicet cognito excepto. Hinc igitur iure concludimus numerum propositum 1000003 unico modo in forma $3xx + 19yy$ contineri ideoque certe esse primum.

34. Ex hoc exemplo clare apparet, quantum intersit in formula $\alpha xx + \beta yy$ pro α et β maiores numeros investigare, dummodo eorum productum $\alpha\beta$ in classe numerorum idoneorum contineatur, pro quibus inveniendis regula supra fuit exposita. Quamobrem, ut quovis casu statim appareat, utrum tale productum $\alpha\beta$ sit numerus idoneus necne, tabulam istorum numerorum, quousque eam continuare licuit, hic subiungamus.[1])

Tabula numerorum idoneorum $\alpha\beta$ hac proprietate praeditorum, ut omnes numeri unico modo in formula $\alpha xx + \beta yy$ contenti certe sint primi

1	16	48	120	312
2	18	57	130	330
3	21	58	133	345
4	22	60	165	357
5	24	70	168	385
6	25	72	177	408
7	28	78	190	462
8	30	85	210	520
9	33	88	232	760
10	37	93	240	840
12	40	102	253	1320
13	42	105	273	1365
15	45	112	280	1848

35. Quoties igitur numerum quempiam propositum ad talem formam $\alpha xx + \beta yy$ reducere licuerit, ut productum $\alpha\beta$ inter numeros istius tabulae contineatur, tum haec formula usurpari poterit ad examen iam saepius allatum instituendum. Conveniet autem accuratius explicare regulam, cuius ope operationes necessariae expedite institui queant, id quod in sequente Problemate ostendamus.

1) Vide eandem tabulam p. 277 et 320 huius voluminis. R. F.

PROBLEMA

Proposito numero quantumvis magno N explorare, utrum is sit primus necne.

SOLUTIO

36. Quo maior fuerit iste numerus N, eo pluribus modis eum in eiusmodi duas partes resolvere licebit, quarum utraque habeat factorem quadratum, quae sint αaa et βbb, ex quibus igitur talem eligi conveniet, ut numerorum α et β productum in tabula modo exposita contineatur, ubi quidem plurimum interierit maiores huiusmodi numeros indagare.

37. Talibus igitur numeris inventis ponamus esse $N = \alpha aa + \beta bb$, et nunc totum negotium huc redit, ut investigetur, utrum iste numerus insuper alio modo in eadem forma $\alpha xx + \beta yy$ contineatur necne. Si enim talis casus occurrat, numerus propositus non erit primus, atque tum adeo eius factores, per praecepta supra data, assignare licebit. Sin autem nullus talis casus occurrat, certo pronunciare poterimus istum numerum N esse primum.

38. Ista autem investigatio sequenti modo generaliter instituatur: Ponamus esse $N = \alpha xx + \beta yy$, ita ut sit $\alpha aa + \beta bb = \alpha xx + \beta yy$, unde formemus hanc aequationem:

$$\alpha aa - \beta(yy - bb) = \alpha xx,$$

ubi praestabit pro α maiorem numerum assumere, pro β vero minorem. Hic igitur statim patet pro y eiusmodi numerum accipi debere, ut formula $yy - bb$ divisorem α involvat. Evidens enim est non solum numeros α et β primos inter se esse debere, sed etiam tam x ad β quam y ad α primum esse statuendum.

39. Quoniam igitur $yy - bb$ per α divisibile esse debet, ante omnia erit dispiciendum, utrum α sit numerus primus necne. Priori enim casu vel $y + b$ vel $y - b$ divisorem habere debet α, unde unicus tantum casus exsurgit; sin autem α involvat factores, tum utique fieri potest, ut alter contineatur in forma $y + b$, alter vero in forma $y - b$; unde praeter illum casum adhuc unus vel plures novi casus examinari debebunt. Unicus scilicet casus occurret, si α duos tantum habeat factores; sin autem plures factores involvat, tum etiam pluribus modis in duos factores resolvi poterit, quos singulos seorsim perscrutari oportet.

40. Ponamus igitur in genere esse $\alpha = \mu\nu$, et quovis casu facile patebit, quot modis numerus α in binos huiusmodi factores resolvere licet, quotcunque etiam involvat divisores; neque etiam numeri primi hinc excluduntur, quippe quibus casibus vel pro μ vel pro ν unitas erit scribenda. Hinc ergo ponamus $y + b = \mu p$ et $y - b = \nu q$, ita ut sit $yy - bb = \mu\nu pq = \alpha pq$, et facta divisione per α aequatio deinceps resolvenda erit $aa - \beta pq = xx$.

41. Numeri autem p et q hoc modo commodissime reperiuntur. Eliminata enim littera y habebimus $2b = \mu p - \nu q$. Iam quaeratur fractio $\frac{m}{n}$ proxime aequalis fractioni $\frac{\mu}{\nu}$, ita ut $m\nu - n\mu = 1$; tum capiatur $p = \nu s - 2nb$ et $q = \mu s - 2mb$, ubi iam pro s numeros quoscunque integros accipere licet, sive positivos, sive negativos, et aequatio nostra resolvenda induet hanc formam:

$$aa - \beta(\nu s - 2nb)(\mu s - 2mb) = xx,$$

ubi iam pro s eiusmodi valores investigari debent, ut ista forma

$$aa - \beta(\nu s - 2nb)(\mu s - 2mb)$$

quadratum evadat. Totum negotium igitur eo redit, ut dispiciatur, an, tribuendo litterae s successive omnes valores tam positivos quam negativos a zyphra ad terminum usque, qui numeros praeberet negativos, an dico usquam quadratum resultare possit.

42. Evolvamus igitur singulos numeros, quos a quadrato aa subtrahi oportet, quos littera S designemus, ita ut sit $aa - S = xx$. Habebimus ergo:

s	S	
0	$4\beta mnbb$	I
± 1	$\beta(\nu \pm 2nb)(\mu \pm 2mb)$	II
± 2	$\beta(2\nu \pm 2nb)(2\mu \pm 2mb)$	III
± 3	$\beta(3\nu \pm 2nb)(3\mu \pm 2mb)$	IV
± 4	$\beta(4\nu \pm 2nb)(4\mu \pm 2mb)$	V
± 5	$\beta(5\nu \pm 2nb)(5\mu \pm 2mb)$	VI

Quoniam isti valores sat simplici lege progrediuntur, perpendamus eorum differentias, ac reperiemus:

$$\begin{aligned} \text{II} - \text{I} &= \beta(\ \mu\nu \pm 2b\,(m\nu + n\mu)) \\ \text{III} - \text{II} &= \beta(3\mu\nu \pm 2b\,(m\nu + n\mu)) \\ \text{IV} - \text{III} &= \beta(5\mu\nu \pm 2b\,(m\nu + n\mu)) \\ \text{V} - \text{IV} &= \beta(7\mu\nu \pm 2b\,(m\nu + n\mu)), \end{aligned}$$

quae manifesto in progressione arithmetica progrediuntur, cuius differentia est $2\beta\mu\nu$.

43. His differentiis inventis nihil aliud superest, nisi ut eae ordine continuo a quadrato aa, primo termino minuto, subtrahantur. Ab $aa\,[-4\beta mnbb]$ scilicet primo subtrahatur prima differentia; tum vero a residuo secunda, a residuo hinc nato tertia, porro quarta etc., quoad ad numeros negativos perveniatur; hisque operationibus ita continuatis dispiciatur, utrum usquam numerus quadratus remanserit; quod si non contigerit, numerus propositus certe pro primo erit habendus; sin autem usquam quadratum prodierit, eius radix dabit valorem ipsius x, et notato valore ipsi s conveniente etiam reperiri poterit alter numerus y, siquidem erit

$$y = b + \mu\nu s - 2\nu mb\,.$$

Quia vero supra sumsimus $m\nu - n\mu = 1$, erit nunc $y = \mu\nu s - b(m\nu + n\mu)$.

44. Quod si numerus propositus N fuerit vehementer magnus, numerum harum operationum non parum diminuere licebit, si numeri S, quos a quadrato aa continuo subtrahi oportet, in duas classes distinguantur, prouti pro s valores sive pares sive impares accipiantur. Priore enim casu, cum sit vel $s = 4n$ vel $s = 4n + 2$, plerumque eveniet, ut alter casus penitus excludatur, ob eam proprietatem, quod inde pro S numeri prodirent impariter pares. Eodem modo, si pro s sumatur numerus impar, erit vel $s = 4n + 1$ vel $s = 4n - 1$, quarum formarum altera penitus excluditur, quia omnia quadrata imparia sunt formae $8n + 1$, ita ut hoc modo numerus operationum ad semissem redigatur.

45. Quoniam initio posuimus $\alpha = \mu\nu$ hosque numeros μ et ν ut primos inter se spectavimus, id quod potissimum de factoribus imparibus est tenendum, notetur, si α sit numerus par et potestatem quamcunque ipsius binarii involvat, tum utrumque factorem $y + b = \mu p$ et $y - b = \nu q$ parem esse debere. Unde si ipsi μ valor par tribuatur, nihil impedit, quo minus et ν par statuatur, id quod facile in exemplis oblatis observare licet. Ita cum numerus

$520 = 8 \cdot 5 \cdot 13$ in tabula superiore numerorum idoneorum contineatur, secundum praecepta hic tradita in genere numeros $N = 40aa + 13bb$ evolvamus.

Evolutio generalis
numerorum contentorum in forma
$N = 40aa + 13bb$

46. Hic igitur erit $\alpha = 40$ et $\beta = 13$, atque hinc numeros x et y ex sequenti forma elicere licebit:

$$40aa - 13\,(yy - bb) = 40xx\,,$$

ubi statim duos casus distingui conveniet, quibus est vel $\mu = 10$ et $\nu = 4$ vel $\mu = 20$ et $\nu = 2$, quia scilicet ambo factores debent esse pares.

CASUS 1
quo $\mu = 10$ *et* $\nu = 4$

47. Hic igitur erit $y + b = 10p$ et $y - b = 4q$, hincque $b = 5p - 2q$. Fractioni ergo $\frac{5}{2}$ proxima erit $\frac{2}{1}$, unde statuamus $p = 2s + b$ et $q = 5s + 2b$, quibus valoribus substitutis aequatio resolvenda erit

$$aa - 13\,(2s + b)\,(5s + 2b) = xx\,.$$

Posito igitur brevitatis gratia numerum a quadrato aa subtrahendum scilicet

$$13\,(2s + b)\,(5s + 2b) = S\,,$$

si loco s successive scribamus numeros 0, ± 1, ± 2, ± 3 etc., valores ipsius S cum suis differentiis, quorum usum iam saepius explicavimus, ita se habebunt:

s	S	Diff.
0	$26bb$	
± 1	$13\,(2 \pm b)\,(5 \pm 2b)$	$130 \pm 117b$[1]
± 2	$13\,(4 \pm b)\,(10 \pm 2b)$	$390 \pm 117b$
± 3	$13\,(6 \pm b)\,(15 \pm 2b)$	$650 \pm 117b$
± 4	$13\,(8 \pm b)\,(20 \pm 2b)$	$910 \pm 117b$
etc.	etc.	etc.

1) Editio princeps loco b ubique bb exhibet. Correxit R. F.

quae differentiae continuo crescunt augmento constanti 260, unde facile, quousque libuerit, continuabuntur; ubi autem probe notetur subtractionem differentiarum fieri debere a numero $aa - 26bb$.

CASUS 2
quo $\mu = 20$ *et* $\nu = 2$

48. Hic igitur erit $y + b = 20p$ et $y - b = 2q$, unde, cum hinc fiat $b = 10p - q$, sumto $p = s$ fiet $q = 10s - b$, et aequatio resolvenda erit: $aa - 13pq = xx$ sive

$$aa - 13s(10s - b) = xx .$$

Posito igitur brevitatis gratia

$$13s(10s - b) = S ,$$

valores ipsius S, prouti s fuerit vel 0 vel ± 1 vel ± 2 vel ± 3, erunt sequentes:

s	S	Diff.
0	0	
± 1	$13(10 \pm b)$	$130 \pm 13b$
± 2	$26(20 \pm b)$	$390 \pm 13b$
± 3	$39(30 \pm b)$	$650 \pm 13b$
± 4	$52(40 \pm b)$	$910 \pm 13b$
etc.	etc.	etc.

ubi differentiae iterum manifesto augmento constanti 260 crescunt, quas igitur loco S continuo ab ipso quadrato aa subtrahi oportet.

Alia Evolutio
numerorum formae $40aa + 13bb$

49. Cum habeatur aequatio:

$$40aa - 13(yy - bb) = 40xx ,$$

tollamus primo tantum factorem parem 8, et quia b denotat numerum imparem, evidens est, dummodo pro y etiam sumatur numerus impar, formulam

$yy - bb$ fore divisibilem per 8. Ponatur igitur in genere $y = 2z \pm b$, et facta divisione per 8 habebimus hanc aequationem:

$$5aa - \frac{13}{2}(zz \pm bz) = 5xx;$$

ubi evidens est membrum medium semper esse integrum. Nunc igitur loco z talem numerum assumi oportet, ut vel z vel $z \pm b$ factorem habeat 5; perinde autem est, uter horum factorum per 5 divisibilis reddatur, propterea quod inter se sunt permutabiles, mutato scilicet signo ipsius b. Ponatur igitur $z = 5s$, et facta divisione per 5 aequatio, cui satisfieri oportet, erit:

$$aa - \frac{13}{2}(5ss \pm bs) = xx.$$

50. Hic igitur a quadrato aa subtrahi debent numeri in forma

$$\frac{13}{2}(5ss \pm bs)$$

contenti, quae si vocetur $= S$, valores ipsius S erunt, uti in sequenti tabula cum suis differentiis exhibentur.

s	S	Diff.
0	0	$\frac{13}{2}(5 \pm b)$
± 1	$\frac{13}{2}(5 \pm b)$	$\frac{13}{2}(15 \pm b)$
± 2	$\frac{13}{2}(20 \pm 2b)$	$\frac{13}{2}(25 \pm b)$
± 3	$\frac{13}{2}(45 \pm 3b)$	$\frac{13}{2}(35 \pm b)$
± 4	$\frac{13}{2}(80 \pm 4b)$	
etc.	etc.	etc.

ubi differentiae, quas a quadrato aa continuo subtrahi oportet, augmento constanti $\frac{13}{2} \cdot 10 = 65$ crescunt.

51. Quin etiam unica substitutione totus numerus 40 statim tolli potest ponendo $y = 10s \pm b$; tum enim, ob $yy - bb = 100ss \pm 20bs$, dividendo per 40 statim pervenitur ad hanc aequationem: $aa - \frac{13}{2}(5ss \pm bs) = xx$,

uti modo invenimus. Hoc igitur artificio semper uti licebit, quoties littera α valorem habeat parem, atque adeo cum potestate binarii simul unum factorem primum tollere licebit. Veluti si $\alpha = 2^\lambda f$, ita ut formula $yy - bb$ per hunc valorem divisibilis reddi debeat, statim poni poterit:

$$y = 2^{\lambda-1} fz \pm b ;$$

tum enim erit:

$$yy - bb = 2^{2\lambda-2} ffzz \pm 2^\lambda bfz ,$$

quae forma

$$2^{2\lambda-2} ffzz \pm 2^\lambda bfz$$

per $2^\lambda f$ divisa abit in hanc:

$$2^{\lambda-2} fzz \pm bz ;$$

quod igitur cum fuerit praestitum, reliqui factores per praecepta generalia, alibi tradita, facile e medio tolli poterunt. En adhuc alia, eaque simplicissima evolutio formulae $N = 40aa + 13bb$.

52. Cum posito $N = 40xx + 13yy$ aequatio prima fundamentalis hoc modo repraesentetur: $13bb - 40(xx - aa) = 13yy$, observasse iuvabit eam unica operatione resolvi posse ponendo $x = 13s \pm a$. Facta enim substitutione et divisione per 13 pervenietur ad hanc aequationem simplicissimam:

$$bb - 40(13ss \pm 2as) = yy .$$

Hic igitur a quadrato bb successive subtrahi debent valores formulae $40(13ss \pm 2as)$, qui ita (posita hac formula brevitatis gratia $= S$) ordine cum suis differentiis disponantur:

s	S	Diff.
0	0	
± 1	$40(13 \pm 2a)$	$40(13 \pm 2a)$
± 2	$40(52 \pm 4a)$	$40(39 \pm 2a)$
± 3	$40(117 \pm 6a)$	$40(65 \pm 2a)$
± 4	$40(208 \pm 8a)$	$40(91 \pm 2a)$
etc.	etc.	etc.

ubi differentiae per augmentum constans $40 \cdot 26 = 1040$ progrediuntur.

Hanc iam posteriorem resolutionem maxime succinctam aliquot exemplis illustrasse operae pretium erit.

EXEMPLUM 1

53. Sumatur $b = 81$ et $a = 1$, ita ut numerus examinandus sit 85333. Hic ergo differentiae a quadrato $bb = 6561$ continuo subtrahendae erunt $40\,(13 \pm 2)$, $40\,(39 \pm 2)$ etc., quae crescunt augmento constanti $40 \cdot 26 = 1040$; unde ob signa ambigua totus hic calculus per duas columnas absolvi poterit:

6561	6561
600	440
5961	6121
1640	1480
4321	4641
2680	2520
1641	2121

Quoniam igitur nullum residuorum ex hac subtractione natorum quadratum deprehenditur, tuto concludere possumus hunc numerum 85333 esse primum.

EXEMPLUM 2

54. Maneat $b = 81$ sitque $a = 10$, et numerus examinandus erit $N = 89293$. Hic igitur a quadrato $bb = 6561$ subtrahenda erit differentia $40\,(13 \pm 20)$, ideoque 1320 et -280; sequentes autem differentiae crescunt augmento $= 1040$. Hinc calculus ita se habet:

6561	6561
1320	−280
5241	6841
2360	760
2881	6081
	1800
	4281
	2840
	1441

Quoniam igitur hic etiam nullum quadratum occurrit, numerus propositus 89293 certe erit primus.

EXEMPLUM 3

55. Maneat adhunc $b = 81$ sumaturque $a = 19$, ut sit $N = 99733$; et ad examen huius numeri necesse est, ut a quadrato 6561 subtrahantur differentiae augmento 1040 crescentes, quarum primae sunt 2040 et — 1000, hoc modo:

6561	6561
2040	−1000
4521	7561
3080	40
1441	7521
	1080
	6441
	2120
	4321
	3160
	1161

Quia igitur hic nullum quadratum resultat, numerus 99733 etiam pro primo est habendus.

EXEMPLUM 4

56. Adiungamus exemplum numeri propositi. Maneat iterum $b = 81$ sitque $a = 17$, erit $N = 96853$ et subtractio differentiarum ita se habebit:

6561	6561
1880	−840
4681	7401
2920	200
1761	7201
	1240
	5961
	2280
	3681
	3320
	*361

Hic iam occurrit numerus quadratus * $361 = 19^2$ ipsi yy aequandus. Fit igitur $y = 19$, $s = -5$, hincque $x = 48$[1]), unde factor numeri propositi inveniri potest quaerendo fractionem $\frac{p}{q} = \frac{x \pm a}{y \pm b} = \frac{48 \pm 17}{81 \pm 19} = \frac{1}{2}$; hinc factor est $40pp + 13qq = 40 \cdot 1^2 + 13 \cdot 2^2$, qui ad minimos terminos reductus est $10 \cdot 1^2 + 13 \cdot 1^2 = 23$. Alter factor ex eadem fractione derivari potest, si sumatur $\frac{p}{q} = \frac{65}{62}$; hinc enim fiet $40pp + 13qq = 40 \cdot 65^2 + 13 \cdot 62^2$, qui factor per $4 \cdot 13$ depressus dat $10 \cdot 65 \cdot 5 + 31^2 = 4211$; at revera est $96853 = 23 \cdot 4211$.

EXEMPLUM 5

57. Sumatur $a = 40$ et $b = 1$, et numerus examinandus erit $N = 64013$. Hic autem modus procedendi a praecedentibus diversus adhiberi debet; quia enim a quadrato bb subtrahi deberent numeri in forma $40\,(13ss \pm 80s)$ contenti, quod autem fieri nequit, hic solum signum inferius valebit, ita ut successive ad quadratum $bb = 1$ addi debeant numeri in forma $S = 40\,(80s - 13ss)$ contenti, quos cum suis differentiis hic adiungamus:

s	S	Diff.
0	0	
+ 1	40 · 67	40 · 67 +
+ 2	40 · 108	40 · 41 +
+ 3	40 · 123	40 · 15 +
+ 4	40 · 112	40 · 11 —
etc.	etc.	etc.

ubi differentiae decrescunt quantitate constanti $40 \cdot 26$; quamobrem, si ad unitatem primo addamus numerum $40 \cdot 67 = 2680$, tum vero differentias sequentes decremento 1040 decrescentes: 1640, 600, — 440, — 1480, — 2520, quia inde nullum quadratum resultat, concludimus numerum 64013 esse primum.

58. His circa evolutionem numerorum in forma $40aa + 13bb$ contentorum expeditis, praestabit usum maiorum numerorum idoneorum exemplo illustrasse. Consideretur numerus $N = 999601 = 840 \cdot 34^2 + 169^2$, et examinetur,

1) Ubi $-x = 13s + a$ ponatur. R. F.

utrum hic numerus propositus plus uno modo in forma idonea $840xx + yy$ contineatur, id quod sine pluris ambagibus sequenti modo satis commode fieri licet.

59. Cum debeat esse $999601 - 840xx = yy$, ipsi x successive tribuantur numeri naturales, et numeri S a proposito subtrahendi cum suis differentiis erunt

x	S	Diff.
0	0	
1	1 · 840	1 · 840
2	4 · 840	3 · 840
3	9 · 840	5 · 840
4	16 · 840	7 · 840
etc.	etc.	etc.

Loco S iam continuo subtrahantur differentiae augmento 1680 crescentes, quae subtractiones continuae sequenti modo instituantur.

999601	958441	834961	629161	341041
840	12600	24360	36120	47880
998761	945841	810601	593041	293161
2520	14280	26040	37800	49560
996241	931561	784561	555241	243601
4200	15960	27720	39480	51240
992041	915601	756841	515761	192361
5880	17640	29400	41160	52920
986161	897961	727441	474601	139441
7560	19320	31080	42840	54600
978601	878641	696361	431761	84841
9240	21000	32760	44520	56280
969361	857641	663601	387241	28561
10920	22680	34440	46200	
958441	834961	629161	341041	

60. Hic iam duo occurrunt quadrata pro yy. Prius dat $y = 979$ et $x = 7$, posterius praebet casum cognitum $y = 169$ et $x = 34$. Numerus igitur

propositus duplici modo in forma idonea $840xx + yy$ continetur ideoque non est primus, eiusque factores sequenti modo assignari possunt. Formetur fractio: $\frac{p}{q} = \frac{x \pm a}{y \pm b}$, et ob signa ambigua hae quatuor habebuntur fractiones:

$$\frac{41}{1148} = \frac{1}{28}, \frac{41}{810}, \frac{27}{1148}, \frac{27}{810} = \frac{1}{30}.$$

Hinc forma factoris $840pp + qq$ ex priore fractione fit $840 \cdot 1 + 28^2$, sive per 28 depressus, $30 + 28 = 2 \cdot 15 + 2 \cdot 14 = 2 \cdot 29$, qui idem factor etiam prodit ex quarta fractione $\frac{p}{q} = \frac{1}{30}$; hinc enim fit factor $= 840 \cdot 1^2 + 30^2 = 60\,(14 + 15) = 60 \cdot 29$. Alter factor vel ex secunda vel tertia fractione colligitur; sumto enim $\frac{p}{q} = \frac{41}{810}$ fit factor $= 840 \cdot 41^2 + 810^2$, qui per 60 depressus est $= 14 \cdot 41^2 + 27 \cdot 405 = 34469$. Idem prodit ex fractione $\frac{p}{q} = \frac{27}{1148}$; at vero revera est $29 \cdot 34469 = 999601$.

61. Ex hoc exemplo luculenter apparet, quanti momenti sint numeri idonei maiores in perscrutandis numeris praegrandibus, utrum sint primi necne. Cum igitur numerus 1848 sit maximus idoneus, qui in nostra tabula occurrit, operae pretium erit in subsidium examinis numerorum vehementer magnorum sequens problema generalius hic adiungere.

PROBLEMA

Numerum propositum quantumvis magnum $N = 1848aa + bb$ *examinare, utrum sit primus necne.*

SOLUTIO

62. Subtrahantur ab isto numero N successive omnes numeri in hac forma $1848xx$ contenti, et si nusquam quadratum remaneat, praeter casum cognitum $x = a$, iste numerus certe erit primus. Sin autem aliud praeterea quadratum relinquatur, iste numerus erit compositus eiusque adeo factores assignare licebit. Verum quia iste calculus ob ingentes numeros continuo subtrahendos non parum est molestus, totum negotium sequenti modo facilius reddi poterit.

63. Statuatur

$$1848aa - (yy - bb) = 1848xx ,$$

et cum sit $1848 = 8 \cdot 3 \cdot 7 \cdot 11$, ponatur primo $y = 22z + b$, et facta divisione per $8 \cdot 11$ fiet

$$21aa - \tfrac{1}{2}z(11z + b) = 21xx .$$

Quod si ergo brevitatis gratia ponatur $z(11z + b) = 21pq$, aequatio nostra erit

$$aa - \tfrac{1}{2}pq = xx ,$$

quae quadruplici modo locum habere potest:

I. Si $11z + b = 21p$ et $z = q$,
II. Si $11z + b = p$ et $z = 21q$,
III. Si $11z + b = 7p$ et $z = 3q$,
IV. Si $11z + b = 3p$ et $z = 7q$.

64. Evolvamus seorsim singulos hos modos, et *pro primo casu*, ob $z = q$, erit $11q + b = 21p$, hincque $q = 2p - \frac{p+b}{11} = 2p - s$, ita ut $p + b = 11s$ ideoque $p = 11s - b$ et $q = 21s - 2b = z$, ita ut aequatio nostra fiat

$$aa - \tfrac{1}{2}(11s - b)(21s - 2b) = xx .$$

Pro secundo casu, ob $z = 21q$, erit $231q + b = p$, sicque sumto $q = s$ erit $p = 231s + b$ et $z = 21s$, unde aequatio pro hoc casu erit

$$aa - \tfrac{1}{2}s(231s + b) = xx .$$

Pro tertio casu, ob $z = 3q$, erit $33q + b = 7p$ ideoque $p = 5q - \frac{2q-b}{7} = 5q - r$, ita ut $2q - b = 7r$ et $2q = 7r + b$, sive $q = 3r + \frac{r+b}{2} = 3r + s$, unde fit $r = 2s - b$, hincque $q = 7s - 3b$ et $p = 33s - 14b$ et $z = 21s - 9b$, unde nostra aequatio erit

$$aa - \tfrac{1}{2}(7s - 3b)(33s - 14b) = xx .$$

Pro quarto casu, ob $z = 7q$, erit $77q + b = 3p$, hincque

$$p = 26q - \frac{q-b}{3} = 26q - s ,$$

existente $s = \frac{q-b}{3}$, unde fit $q = 3s + b$ ideoque $p = 77s + 26b$ et $z = 21s + 7b$, unde aequatio resolvenda erit:

$$aa - \tfrac{1}{2}(3s + b)\ (77s + 26b) = xx .$$

Ulteriorem calculum sequenti exemplo illustremus.

EXEMPLUM

65. Sumatur $a = 100$ et $b = 197$, ut numerus examinandus sit

$$N = 1848aa + bb = 18518809 ,$$

ubi facile patet numerum y maiorem fore quam 197 ideoque z fore numerum positivum. Hoc observato ad examen huius ingentis numeri instituendum singulos casus supra a se invicem separatos hic etiam in commodum calculi seorsim evolvamus.

66. *Pro casu primo* nostra aequatio erit

$$10000 - \tfrac{1}{2}(11s - b)\ (21s - 2b) = xx ;$$

et quia hinc est $z = 21s - 394$, patet numerum s maiorem esse debere quam 18[1]). Statuamus igitur $s = 18 + t$, ut fiat $z = 21t - 16$, atque aequatio nostra hanc induet formam:

$$10000 - \tfrac{1}{2}(11t \pm 1)\ (21t \mp 16) = xx .$$

Numeri S igitur a numero absoluto 10000 subtrahendi, cum suis differentiis tam pro valoribus ipsius t positivis quam negativis, in sequenti tabula referantur:

1) Hac observatione in sequente demonstratione Eulerus non utitur; nam ipsi t valores vel positivi vel negativi dantur. R. F.

t	S	Diff.	t	S	Diff.
0	— 8		0	— 8	
		38			193
+ 1	30		— 1	185	
		269			424
+ 2	299		— 2	609	
		500			655
+ 3	799		— 3	1264	
etc.	etc.	etc.	etc.	etc.	etc.

ubi differentiae crescunt augmento constanti 231. At quia primus numerus subtrahendus est — 8, continua differentiarum subtractio fieri debet a numero 10008, ut sequitur:

10008	10008
38	193
9970	9815
269	424
9701	9391
500	655
9201	8736
731	886
8470	7850
962	1117
7508	6733
1193	1348
6315	5385
1424	1579
4891	3806
1655	1810
3236	1996
1886	
1350	

ex quo igitur calculo nullum quadratum resultat.

67.[1]) *Pro casu secundo* aequatio resolvenda erit

$$10000 - \tfrac{1}{2}s(231s + 197) = xx .$$

1) Inde in editione principe numeri paragraphorum unitate augentur. R. F.

Hic ergo a numero 10000 subtrahendi sunt numeri in forma $S = \frac{1}{2}s(231s \pm 197)$ contenti, qui cum suis differentiis hic exhibentur:

s	S	Diff.	s	S	Diff.
0	0		0	0	
		214			17
+ 1	214		— 1	17	
		445			248
+ 2	659		— 2	265	
		676			479
+ 3	1335		— 3	744	
etc.	etc.	etc.	etc.	etc.	etc.

A quadrato igitur 10000 subtrahantur differentiae numero 231 crescentes:

10000	10000
214	17
9786	9983
445	248
9341	9735
676	479
8665	9256
907	710
7758	8546
1138	941
6620	7605
1369	1172
5251	6433
1600	1403
3651	5030
1831	1634
1820	3396
	1865
	1531

Ubi iterum nullus numerus quadratus occurrit praeter 10000, qui autem dat casum cognitum.

68. *Pro casu tertio* aequatio examinanda erit

$$10000 - \tfrac{1}{2}(7s - 591)\,(33s - 2758) = xx\,,$$

quae igitur, posito $s = 84 + t$, abibit in hanc:

$$10000 - \tfrac{1}{2}(7t - 3)(33t + 14) = xx .$$

Prouti igitur t valorem habet vel positivum vel negativum, numeri subtrahendi S continebuntur in hac forma: $\frac{1}{2}(7t \mp 3)(33t \pm 14)$ et erunt, uti hic exhibentur:

t	S	Diff.	t	S	Diff.
0	— 21		0	— 21	
		115			116
+ 1	+ 94		— 1	+ 95	
		346			347
+ 2	440		— 2	442	
		577			578
+ 3	1017		— 3	1020	
etc.	etc.	etc.	etc.	etc.	etc.

Iam a numero absoluto 10021 subtrahantur differentiae hic assignatae et, quousque rei natura postulat, continuatae:

10021	10021
115	116
9906	9905
346	347
9560	9558
577	578
8983	8980
808	809
8175	8171
1039	1040
7136	7131
1270	1271
5866	5860
1501	1502
4365	4358
1732	1733
2633	2625
1963	1964
670	661

ubi nullum plane quadratum occurrit.

69. *Pro casu quarto* aequatio resolvenda est

$$10000 - \tfrac{1}{2}(3s + 197)(77s + 5122) = xx .$$

Sit brevitatis gratia $s = t - 66$, erit

$$10000 - \tfrac{1}{2}(3t - 1)(77t + 40) = xx ,$$

sicque numeri subtrahendi continentur in forma $S = \tfrac{1}{2}(3t \mp 1)(77t \pm 40)$, qui cum suis differentiis sunt, uti sequitur:

t	S	Diff.	t	S	Diff.
0	— 20		0	— 20	
		137			94
+ 1	117		— 1	74	
		368			325
+ 2	485		— 2	399	
		599			556
+ 3	1084		— 3	955	
etc.	etc.	etc.	etc.	etc.	etc.

Hinc ergo ob primum numerum negativum = — 20 a numero absoluto 10020 subtrahendae erunt differentiae, quousque opus est continuatae, hoc modo:

10020	10020
137	94
9883	9926
368	325
9515	9601
599	556
8916	9045
830	787
8086	8258
1061	1018
7025	7240
1292	1249
5733	5991
1523	1480
4210	4511
1754	1711
2456	2800
1985	1942
471	858

nullum quadratum in hisce residuis occurrit.

70. Quoniam igitur in omnibus his quatuor casibus nullum quadratum est relictum, certo affirmare possumus numerum 18518809 esse primum. Ex hoc exemplo simul intelligere licet satis raro evenire posse, ut in talibus operationibus quadrata relinquantur; hanc ob rem forma $1848aa + bb$ etiam aptissima videtur ad plures inde numeros primos deducendos; tantum enim opus est valores a et b variare, quod, cum infinitis modis fieri queat, inde haud difficulter plures alii numeri primi tam ingentes reperiri poterunt, ut problemati illo FERMATIANO, quo numeros primos dato quovis maiores requiruntur, quodammodo sit satisfactum.

71. Quoniam in hoc exemplo numeri successive a quadrato aa subtrahendi iidem manent, quamdiu sumitur $b = 197$, operae pretium erit pro littera a alios quoque valores, potissimum minores, statuere, ubi totus calculus evadet facillimus. Ut autem, quando quadratum occurrit, pro xx etiam valorem respondentem ipsius y assignare liceat, meminisse oportet in initio huius solutionis positum fuisse $y = 22z + 197$; tum vero in quaternis casibus allatis statutum fuisse, ut sequitur:

Pro primo casu $z = 21s - 394$, tum vero $s = t + 18$; quamobrem, quia ipsi t tam valores positivos quam negativos tribuimus, erit $z = \pm 21t - 16$; ubi signum superius pro columna prima, inferius vero pro altera valet.

Pro secundo casu erat $z = 21s$, unde ob binas columnas cum ambiguitate signorum erit $z = \pm 21s$.

Pro tertio casu erat $z = 21s - 9 \cdot 197$, tum vero $s = t + 84$, unde cum ambiguitate signorum erit $z = \pm 21t - 9$.

Pro quarto casu erat $z = 21s + 7 \cdot 197$; tum vero posuimus $s = t - 66$, unde cum signorum ambiguitate erit $z = \pm 21t - 7$. His notatis sequentes numeros examini subiiciamus.

72. Sit $a = 1$, existente $b = 197$, et numerus propositus erit $N = 40657$. Hic igitur statim ex primo casu occurrit quadratum $aa + 8 = xx$, unde fit $xx = 9$ ideoque $x = 3$, cui respondet valor $t = 0$, ex quo fit $z = -16$, consequenter $y = 155$. Numerus igitur propositus etiam continetur in forma $1848 \cdot 3^2 + 155^2$, unde formatur fractio $\frac{p}{q} = \frac{a \pm x}{b \pm y} = \frac{1 \pm 3}{197 \pm 155}$, cuius valor simplicissimus est $\frac{p}{q} = \frac{1}{21}$. Hinc factor numeri propositi erit

$$1848pp + qq = 1848 \cdot 1^2 + 21^2,$$

qui per 21 depressus fit $88 + 21 = 109$. Numerus igitur propositus 40657 non est primus, sed divisorem habet 109, quoto existente 373.

73. Sit $a = 2$, eritque numerus propositus $N = 46201$. Hic neque ex primo neque ex secundo casu quadratum resultat, verum ex casu tertio statim fit $aa + 21 = 25 = xx$, unde fit $x = 5$, existente $t = 0$, adeoque $z = -9$, consequenter $y = -9 \cdot 22 + 197 = -1$. Ad divisorem igitur numeri propositi explorandum fiat $\frac{p}{q} = \frac{a \pm x}{b \pm y} = \frac{1}{28}$, unde pro factore haec prodit forma: $1848 \cdot 1^2 + 28^2$, [quae per 56 depressa fit] $= 33 + 14 = 47$. At revera est $N = 46201 = 47 \cdot 983$.

74. Quoniam autem hic numeros compositos non curamus, superfluum foret examen pro omnibus valoribus ipsius a hic ordine apponere. Sufficiet enim omnes numeri primi in forma $1848aa + 197^2$ contenti in sequenti tabula exhibuisse:

Tabula numerorum primorum in forma $1848aa + 197^2$ *contentorum*

Numerus primus	ex valore a
55441	3
85009	5
105337	6
129361	7
157081	8
351121	13
401017	14
454609	15
511897	16
572881	17
705937	19
933241	22
1016401	23
1103257	24
1288057	26
1487641	28
1702009	30
2995609	40
4658809	50
9094009	70
11866009	80
18518809	100

75. Omnes ergo isti numeri primi deducti sunt ex formula $1848aa + 197^2$; unde patet hinc patefactum esse fontem inexhaustum quamplurimos numeros primos ad plures milliones exsurgentes modico labore inveniendi; quandoquidem non solum in eadem formula $1848aa + 197^2$ loco 197 quoque aliis numeris uti licet, sed etiam loco numeri idonei 1848 etiam maiores eum praecedentes adhiberi possent. Ac si forte adhuc maior numerus idoneus investigari posset, pari labore insuper ad multo maiores numeros primos pertingere possemus. At vero examini instituto inveni huiusmodi numeros usque ad terminum 7000 certe non dari; quod autem ultra hunc terminum adhuc dentur numeri idonei, vix probabile videtur.

THEOREMA

Si quispiam numerus idoneus fuerit impariter par, scilicet $N = 4n + 2$, *tum etiam eius quadruplum in classe numerorum idoneorum reperietur.*

DEMONSTRATIO

76. Cum N sit numerus idoneus, intra intervallum N et $4N$ formula $Nxx + yy$ non nisi numeros primos praebebit. Dico autem hoc casu usque ad $9N$ nullos numeros compositos oriri posse; si enim talis daretur, is tam in forma $N + aa$ quam in forma $4N + bb$ contineretur. Hinc ergo foret $3N = aa - bb$; quia vero $N = 4n + 2$, ista quadratorum differentia $aa - bb$ foret $= 12n + 6$, ideoque numerus impariter par, id quod fieri nequit. Hinc igitur certum est in intervallo ab N usque ad $9N$ nullos existere posse numeros compositos ex formula $Nxx + yy$ oriundos. Ac si hinc oriantur maiores numeri compositi in intervallo ab N usque ad $16N$ contenti, ii nullo modo in forma $4Nxx + yy$ continerentur, idque ob rationem praecedentem. Si enim talis numerus compositus foret tam $4N+bb$ quam $9N+cc$, foret $bb - cc = 5N$, hoc est numerus impariter par; ex quo concluditur etiam intra intervallum $4N$ et $16N$ nullos numeros compositos formae $4Nxx + yy$ cadere posse; unde sequitur numerum $4N$ etiam esse idoneum.

77. Hoc etiam colligere licet ex ipsa tabula numerorum idoneorum supra § 34 exhibita, in qua reperiuntur sequentes numeri impariter pares: 2, 6, 10, 18, 22, 30, 42, 58, 70, 78, 102, 130, 190, 210, 330, 462, quorum ergo

quadrupla etiam, vi superioris theorematis, sunt numeri idonei, scilicet: 8, 24, 40, 72, 88, 120, 168, 232, 280, 312, 408, 520, 760, 840, 1320, 1848, qui omnes in eadem tabula occurrunt.

ALIA DEMONSTRATIO

78. Sit $2i$ numerus idoneus impariter par, ideoque i numerus impar, et quia natura numerorum idoneorum in hoc consistit, ut omnes numeri unico modo in formula $2ixx + yy$ contenti certe sint primi, necesse est, ut omnis numerus compositus, qui sit C, in eadem formula contentus simul insuper alio modo in ea contineatur. Ponamus igitur esse $C = 2iaa + bb$ et $C = 2icc + dd$, hincque fiet $2i(aa - cc) = dd - bb$; ubi observetur numeros b et d impares esse debere, quandoquidem primi esse debent ad $2i$, quamobrem quadratorum differentia $dd - bb$ per 8 erit divisibilis.

79. Consideremus iam casum, quo a est numerus par $= 2f$, ita ut sit $C = 2i \cdot 4ff + bb$, atque postrema aequatio erit $2i(4ff - cc) = dd - bb$. Hic manifestum est, ut prius huius aequationis membrum per 8 divisibile fiat, numerum c necessario parem esse debere. Sit igitur $c = 2g$, atque hinc sequitur, si numerus compositus C fuerit $= 8iff + bb$, tum adhuc alio modo fore $C = 8igg + dd$; quocirca si alius numerus quicunque N unico modo in forma $8ixx + yy$ contineatur, is certe debebit esse primus; unde manifesto concluditur etiam numerum $8i$ in tabula numerorum idoneorum contineri debere.

80. Super tabula autem numerorum idoneorum sequentes observationes fecisse operae erit pretium:

1°) Videmus in hac tabula alios numeros primos non occurrere praeter 2, 3, 5, 7, 13 et 37, atque rationes non desunt numerum 37 tanquam ultimum plane primum in classe numerorum idoneorum spectandi, siquidem, quo longius procedatur, numeri idonei eo plures factores involvant.

2°) Praeterea cum etiam dupla numerorum primorum in hoc negotio pro primis haberi debeant, etiam tales numeri pauci occurrunt, qui sunt $2 \cdot 2$, $2 \cdot 3$, $2 \cdot 5$, $2 \cdot 11$, $2 \cdot 29$, ita ut 58 pro ultimo talium numerorum habendus videatur, idque ob rationem modo ante allatam, quod scilicet numeri idonei continuo plures factores recipiant.

3°) Quoniam in isto calculo etiam quadrata numerorum primorum pro primis sunt habita, talia quadrata hic quoque pauca occurrunt, quae sunt 4, 9, 16, 25, neque enim ob eandem rationem plures admitti posse videntur.

4°) Consideremus etiam omnes eos numeros idoneos, qui tantum ex duobus factoribus constant, ubi quidem ipsum binarium reiicimus, eius vero potestates, perinde ac quadrata numerorum primorum, tanquam simplices factores spectamus. Tales numeros tabula nostra offert sequentes: $4 \cdot 3$, $3 \cdot 5$, $3 \cdot 6$, $3 \cdot 7$, $4 \cdot 6$, $4 \cdot 7$, $5 \cdot 6$, [$3 \cdot 11$], $5 \cdot 8$, $6 \cdot 7$, $6 \cdot 8$, $3 \cdot 19$, $7 \cdot 10$, $8 \cdot 9$, $6 \cdot 13$, $5 \cdot 17$, $3 \cdot 31$, $6 \cdot 17$, $16 \cdot 7$, $10 \cdot 13$, $7 \cdot 19$, $3 \cdot 59$, $10 \cdot 19$, $8 \cdot 29$, $11 \cdot 23$. Reliqui vero omnes vel tres vel adeo plures factores involvunt. His rationibus coniectura nostra non parum confirmatur, quod, quo longius progrediamur, numeri idonei continuo plures factores involvere debeant.

5°) Cum numeri idonei ab initio usque ad 11 omnes numeros complectantur, deinde vero continuo evadant rariores, maxime mirandum, mox tanta intervalla occurrere a talibus numeris prorsus vacua. Veluti in toto intervallo a 520 usque ad 760 nullus plane reperitur; deinde vero ab 840 usque ad 1320, hoc est in intervallo fere quingentorum numerorum, nullus est inventus; ac fere per simile intervallum a 1365 usque ad 1848 ne unus quidem deprehenditur.

6°) Quod autem hic maxime est mirandum, post istum numerum in tabula nostra postremum nulli alii a me sunt inventi, quamquam istum calculum usque ad 4 milia sum prosecutus, ita ut totum hoc spatium prorsus sit vacuum.

7°) Hinc autem porro concludi oportet ulterius usque ad 16000 progrediendo nullum saltem numerum idoneum pariter parem occurrere posse; si enim talis daretur, eius pars quarta in hanc classem, atque adeo ante 4000, cadere deberet. Quare cum maxime probabile sit etiam per hoc intervallum neque numeros impares neque impariter pares reperiri, hinc manifesto sequitur postremum numerum nostrae tabulae 1848 etiam revera esse ultimum, id quod utique tanquam insigne paradoxon spectari potest, propterea quod hi numeri secundum certam legem formantur, quae adeo in infinitum progredi debere videtur.

ILLUSTRATIO PARADOXI CIRCA PROGRESSIONEM NUMERORUM IDONEORUM SIVE CONGRUORUM[1])

(Vide Nova Acta T. XIV p. 51, No. 7)[2])

Commentatio 725 indicis ENESTROEMIANI

Nova acta academiae scientiarum Petropolitanae 15 (1799/1802), 1806, p. 29—32

Summarium ibidem p. 94—95

Conventui exhibita die 20. aprilis 1778

SUMMARIUM

Il faut se rappeller ici d'un mémoire de feu M. EULER, inséré dans le volume précédent des Nova Acta, sous le titre: *Methodus generalior numeros quosvis satis grandes perscrutandi, utrum sint primi necne.*[3]) Ce mémoire renferme une table de tous les nombres $\alpha\beta$ tels que tous les nombres contenus d'une seule manière dans la forme $\alpha xx + \beta yy$ soyent premiers. Le dernier nombre de cette table est 1848; et quoique l'auteur ait poussé fort loin ses recherches, il lui a été impossible de trouver encore un nombre propre à cet examen des nombres premiers au delà de 1848; ce qui l'a porté à soutenir que ce soit effectivement le dernier. Le paradoxe dont il est question dans ce petit mémoire consiste donc en ce qu'une suite de nombres formés d'après une certaine loi, ne consiste qu'en 65 termes, tandis que le nombre des termes devroit être infini. Pour expliquer en quelque façon ce paradoxe,

1) Confer etiam commentationem 708 indicis ENESTROEMIANI: De formulis speciei $mxx + nyy$ ad numeros primos explorandos idoneis, earumque mirabilibus proprietatibus; Nova acta acad. sc. Petrop. 12 (1794), 1801, p. 22—46. *LEONHARDI EULERI Opera omnia*, hoc volumen p. 269, ubi eaedem observationes indicantur. R. F.

2) Huius voluminis p. 394. Haec commentatio pars altera commentationis praecedentis esse videtur. R. F.

3) Commentatio 719 indicis ENESTROEMIANI, Nova acta acad. sc. Petrop. 14 (1797/8), 1805, p. 11—51. Ce volume p. 360. R. F.

M. EULER s'est attaché ici à montrer par une espèce de ces nombres, savoir par les nombres carrés que la table renferme, comment, non obstant la loi de progression, la multitude des nombres $\alpha\beta$, propres à l'examen de la forme $\alpha xx + \beta yy$, puisse être finie et même se reduire à un assez petit nombre de termes.

1. Insigne istud paradoxon in hoc consistebat, quod, etiamsi numeri idonei secundum certam legem formentur et progrediantur, multitudo tamen eorum non sit infinita sed tantum usque ad 65 terminos porrigatur, cuiusmodi paradoxon circa nullam adhuc aliam seriem observatum esse memini; neque vero etiam istum finitum terminorum numerum aliter stabilire mihi licuit, nisi quod post terminum 65, qui est 1848, nullus praeterea se obtulerit, etiamsi examen usque ad 10000 et ultra continuaverim.

2. Neque etiam ulla alia via patere videtur ad hoc insigne paradoxon demonstrandum. Quocirca haud parum lucis in hac re maxime abscondita afferetur, quando saltem pro certa specie horum numerorum, veluti quadratorum, demonstrari poterit eorum multitudinem revera esse terminatam neque in serie numerorum idoneorum alios numeros quadratos occurrere posse, praeter quinque priores 1, 4, 9, 16 et 25, id quod sequenti modo ex ipsa progressionis lege demonstrabo[1]).

3. Transferamus igitur regulam numeros idoneos inveniendi, loco citato expositam[2]), tantum ad numeros quadratos, quae propterea sequenti modo erit enuncianda:

Ex serie omnium numerorum quadratorum, pro quolibet numero primo p, excludantur numeri in hac forma contenti $px - yy$ et maiores quam $\frac{1}{4}pp$, praeter hos $pp - yy$; quod si pro singulis numeris primis fuerit factum, ex serie numerorum quadratorum relinquentur ii, qui sunt idonei. Inter numeros autem primos loco binarii eius quadratum 4 sumi debere vidimus. Cum autem formula $px - yy$ nullos numeros quadratos involvat, hinc nulla exclusio locum habet.

4. Idem evenit pro numero primo $p = 3$, si quidem formula $3x - yy$ nullos numeros quadratos involvit, quod idem de omnibus numeris formae

1) Vide § 25, theorema 1 commentationis in pagina praecedente sub [1]) laudatae (huius voluminis p. 280). R. F.

2) Regula numeros idoneos inveniendi non est exposita loco citato, sed in commentatione 715 indicis ENESTROEMIANI § 41 et sequentibus: Additamentum de numeris idoneis investigandis, huius voluminis p. 321. R. F.

$p = 4n - 1$ est tenendum. Si enim formula $(4n - 1)\,x - yy$ esset quadratum, puta zz, foret summa duorum quadratorum $yy + zz$ divisibilis per $4n - 1$, quod impossibile esse notum est; ex quo intelligitur pro p nobis alios numeros primos non relinqui, nisi in hac forma $4n + 1$ contentos.

5. Sit igitur $p = 5$, ita ut ex serie numerorum quadratorum excludi debeant, qui in forma $5x - yy$ continentur et qui superant $\frac{1}{4}pp = 6\frac{1}{4}$, exceptis tamen iis, qui in forma $25 - yy$ continentur, qui sunt 9 et 16, unde omnia quadrata maiora in forma $5x - yy$ contenta excludi debebunt. Cum igitur omnia quadrata per 5 non divisibilia sint vel formae $5x - 1$, vel $5x - 4$, evidens est hinc omnia quadrata per 5 non divisibilia, simulque maiora quam $6\frac{1}{4}$, excludi debere ex serie omnium numerorum quadratorum; hoc ergo facto relinquetur sequens quadratorum series: 1, 4, 9, 16, 25, 10^2, 15^2, 20^2 [etc.]. Hic scilicet post 16 alii quadrati non relinquuntur, nisi quorum radices divisibiles sunt per 5.

6. Sequens numerus formae $4x + 1$ est $p = 13$, unde numeri excludi debebunt in forma $13x - yy$ contenti, qui quidem sunt maiores quam $42\frac{1}{4}$, exceptis tamen iis, qui in forma $169 - yy$ continentur, qui sunt 25 et 144. Praeter hos ergo numeri quadrati excludendi, maiores quam $42\frac{1}{4}$, continentur in forma $13x - yy$, quae forma continet omnes plane quadratos, quorum radices non sunt per 13 divisibiles, sicque his exclusis post 25 alii non relinquentur nisi per 13 divisibiles. Per conditionem autem praecedentem alii non sunt relicti, nisi per 5 divisibiles; ex quibus ergo si auferantur omnes per 13 non divisibiles, praeter ipsum 25, quia minus quam $42\frac{1}{4}$, alii quadrati non relinquentur, nisi qui simul per 5 et 13 sint divisibiles, qui ergo omnes continentur in forma $(65\alpha)^2$; superstites ergo numeri quadrati erunt: 1, 4, 9, 16, 25, 65^2, 130^2, 195^2, 260^2 etc.

7. Sequens numerus primus formae $4n + 1$ est $p = 17$, hincque formula excludendorum erit $17x - yy$, quatenus sunt maiores quam $\frac{1}{4}pp = 72\frac{1}{4}$, exceptis tamen iis, qui in formula $17^2 - yy$ continentur, qui sunt 15^2 et 8^2, qui autem per praecedentes conditiones sunt deleti. Ex praecedenti igitur serie omnia quadrata deleri debent per 17 non divisibilia; unde patet post 25 alios non relinqui, nisi qui simul per 5, 13 et 17 sunt divisibiles, qui ergo in hac formula continentur $(5 \cdot 13 \cdot 17\alpha)^2$, quorum ergo primus est 1105^2.

8. Sequens numerus primus formae $4n + 1$ est $p = 29$, unde formula numeros excludendos continens est $29x - yy$, quatenus scilicet continet quadratos, ita ut sit $29x = yy + zz$. Haec autem formula omnes plane continet quadratos per 29 non divisibiles, quibus ergo a praecedentibus ablatis alii non supererunt, nisi qui in formula $(5 \cdot 13 \cdot 17 \cdot 29\alpha)^2$ continentur, quorum minimus est 32045.

9. Quodsi hoc modo sequentes numeros primos formae $4n + 1$ evolvamus, evidens est post quinos quadratos initiales 1, 4, 9, 16 et 25 in infinitum usque nullum alium occurrere idoneum.

10. Si igitur quaestio instituatur de numeris quadratis, qui simul sint idonei, rigide iam est demonstratum tales numeros non dari, praeter hos quinque: 1, 4, 9, 16, 25; unde iam satis clare intelligere licet, quemadmodum, non obstante lege progressionis, multitudo omnium plane numerorum idoneorum possit esse terminata, ac fortasse hoc simili modo aliquando demonstrari poterit.

11. In hac demonstratione assumsimus in forma $px - yy$ omnia contineri quadrata, quae non sint per numerum p divisibilia. Est enim $p = 4n + 1$ semper summa duorum quadratorum, quae sit $aa + bb$, ita ut habeamus

$$(aa + bb)x - yy = zz\,,$$

unde, sumpto $x = ff + gg$, colligitur in formula $px - yy$ numerum y ad p primum esse debere.

SOLUTIO FACILIOR PROBLEMATIS DIOPHANTEI CIRCA TRIANGULUM IN QUO RECTAE EX ANGULIS LATERA OPPOSITA BISECANTES RATIONALITER EXPRIMANTUR[1)]

Commentatio 732 indicis ENESTROEMIANI
Mémoires de l'académie des sciences de St-Pétersbourg 2 (1807/8), 1810, p. 10—16
Conventui exhibita die 12. augusti 1779

1. Positis trianguli lateribus $AB = 2c$, $AC = 2b$ et $BC = 2a$, si rectae bisecantes vocentur $AX = x$, $BY = y$ et $CZ = z$, ex Geometria constat quadrata harum trium rectarum sequenti modo exprimi:

$$\begin{aligned} xx &= 2bb + 2cc - aa, \\ yy &= 2cc + 2aa - bb, \\ zz &= 2aa + 2bb - cc, \end{aligned}$$

quas ergo aequationes per numeros rationales resolvi oportet[2)].

2. Ex his tribus aequationibus formentur tres sequentes:

$$\begin{aligned} &\text{I.} \quad xx - yy = 3(bb - aa) \\ &\text{II.} \quad xx + yy = 4cc + aa + bb \\ &\text{III.} \quad zz = 2aa + 2bb - cc, \end{aligned}$$

quas aequationes sequenti modo tractemus.

1) Vide commentationem 713 indicis ENESTROEMIANI, huius voluminis p. 290. R. F.

2) Hae formulae in commentatione sub [1)] laudata demonstratae sunt, vide p. 291 huius voluminis. R. F.

3. Incipiamus ab harum aequationum prima atque, ut fractiones evitemus, statuamus

$$xx - yy = 3(bb - aa) = 12\,fg\,(pp - qq)\,;$$

unde cum sit $bb - aa = 4fg(pp - qq)$, faciamus $b + a = 2f(p + q)$ et $b - a = 2g\,(p - q)$, unde erit

$$b = (f + g)\,p + (f - g)\,q \quad \text{et} \quad a = (f - g)\,p + (f + g)\,q\,.$$

Porro vero pro aequatione $xx - yy = 12fg(pp - qq)$ statuamus $x + y = 6g(p + q)$ et $x - y = 2f(p - q)$; unde fiet

$$x = (3g + f)\,p + (3g - f)q \quad \text{et} \quad y = (3g - f)p + (3g + f)q\,.$$

4. Iam aggrediamur aequationem secundam

$$xx + yy = 4cc + aa + bb\,,$$

atque ex valoribus modo inventis reperietur

$$xx + yy = 2(9gg + ff)\,(pp + qq) + 4(9gg - ff)pq\,.$$

Deinde vero erit

$$aa + bb = 2(ff + gg)\,(pp + qq) + 4(ff - gg)pq\,.$$

Cum igitur sit $4cc = xx + yy - (aa + bb)$, erit

$$4cc = 16gg(pp + qq) + (40gg - 8ff)pq\,,$$

quocirca habebimus

$$cc = 4gg(pp + qq) + (10gg - 2ff)pq\,,$$

quam ergo formulam quadratum reddi oportet.

5. Hinc iam ad tertiam aequationem progrediamur, quae est

$$zz = 2(aa + bb) - cc\,;$$

unde cum sit

$$2(aa + bb) = 4(ff + gg)(pp + qq) + 8(ff - gg)pq$$

et $$cc = 4gg(pp + qq) + (10gg - 2ff)pq,$$

erit $$zz = 4ff(pp + qq) + (10ff - 18gg)pq,$$

quae ergo est altera formula, quam ad quadratum reducere debemus.

6. Priorem harum duarum aequationum dividamus per $4gg$, posteriorem vero per $4ff$, ut habeamus sequentes formulas ad quadratum redigendas:

$$\frac{cc}{4gg} = pp + qq + 2pq\left(\frac{5gg - ff}{4gg}\right),$$

$$\frac{zz}{4ff} = pp + qq + 2pq\left(\frac{5ff - 9gg}{4ff}\right).$$

7. Ponamus iam brevitatis ergo $\frac{5gg - ff}{4gg} = m$ et $\frac{5ff - 9gg}{4ff} = n$, ita ut tota quaestio ad resolutionem istarum duarum formularum sit perducta:

$$\frac{cc}{4gg} = pp + qq + 2mpq = tt,$$

$$\frac{zz}{4ff} = pp + qq + 2npq = uu,$$

atque habebimus $c = 2gt$ et $z = 2fu$. Iam ut hae duae formulae ad quadratum reducantur, notetur esse $tt - uu = 2(m - n)pq$, quam aequationem commode ita tractare licet, ut statuatur

$$t + u = (m - n)p \quad \text{et} \quad t - u = 2q,$$

unde colligitur

$$t = \tfrac{1}{2}(m - n)p + q \quad \text{et} \quad u = \tfrac{1}{2}(m - n)p - q.$$

8. Quodsi nunc hi valores loco t et u substituantur, sumtis quadratis utrinque eadem aequatio emergit

$$pp(1 - \tfrac{1}{4}(m - n)^2) + (m + n)pq = 0,$$

quae aequatio per p divisa fit

$$p(1 - \tfrac{1}{4}(m-n)^2) + (m+n)\,q = 0\,,$$

unde sponte fluit ista ratio inter litteras p et q:

$$\frac{p}{q} = \frac{4\,(m+n)}{(m-n)^2 - 4}\,,$$

quocirca sumi poterit

$$p = 4(m+n) \quad \text{et} \quad q = (m-n)^2 - 4\,,$$

sive aeque multipla, puta in genere

$$p = 4(m+n)M \quad \text{et} \quad q = ((m-n)^2 - 4)M\,,$$

hocque modo omnibus conditionibus plene est satisfactum.

9. Inventis nunc litteris p et q erit

$$t = 2(m+n)(m-n) + (m-n)^2 - 4 = (m-n)(3m+n) - 4$$

et

$$u = (m-n)(m+3n) + 4\,,$$

unde porro has determinationes deducimus:

$$c = 2g(m-n)(3m+n) - 8g$$

et

$$z = 2f(m-n)(m+3n) + 8f\,.$$

Iuvabit autem loco t et u eorum valores ex § 7 sumsisse, ita ut sit

$$c = g(m-n)p + 2gq \quad \text{et} \quad z = f(m-n)p - 2fq\,.$$

10. Nunc igitur solutio nostri problematis sequenti modo concinnari potest:

1) Ambae litterae f et g penitus arbitrio nostro permittuntur, ex quibus definiantur litterae m et n ope harum formularum:

$$m = \frac{5gg - ff}{4gg} \quad \text{et} \quad n = \frac{5ff - 9gg}{4ff}\,.$$

2) Hinc porro quaerantur litterae p et q ope harum formularum:

$$p = 4(m + n) \quad \text{et} \quad q = (m - n)^2 - 4 ,$$

quibus inventis tam latera trianguli quam rectae bisecantes sequenti modo exprimentur.

3) Pro lateribus scilicet inventae sunt hae formulae:

$$a = (f - g)\, p + (f + g)\, q ,$$
$$b = (f + g)\, p + (f - g)\, q ,$$
$$c = 2g(m - n)\,(3m + n) - 8g = g(m - n)\, p + 2gq .$$

4) Denique rectae bisecantes ita se habebunt:

$$x = (3g + f)\, p + (3g - f)\, q ,$$
$$y = (3g - f)\, p + (3g + f)\, q ,$$
$$z = 2f(m - n)\,(m + 3n) + 8f = f(m - n)p - 2fq .$$

11. Ut rem exemplo illustremus, sumamus $f = 2$ et $g = 1$, fietque hinc $m = \frac{1}{4}$ et $n = \frac{11}{16}$; unde porro colligitur $p = \frac{15}{4}$ et $q = -\frac{975}{256}$, qui valores ad numeros integros minimos reducti dant $p = 64$ et $q = -65$. Hinc iam nostrum triangulum hoc modo determinabitur:

$$a = 131 ; \quad b = 127 ; \quad c = 158 ;$$

tum vero

$$x = 255 ; \quad y = 261 ; \quad z = 204^{1}) .$$

12. Occasione huius exempli notasse iuvabit etiam litteras x, y, z pro lateribus accipi posse, cum in genere sit

$$2xx + 2yy - zz = 9cc ,$$
$$2yy + 2zz - xx = 9aa ,$$
$$2zz + 2xx - yy = 9bb ,$$

1) Hoc exemplum iam p. 298 huius voluminis inventum est. R. F.

unde sequitur, cum numeros pro x, y, z inventos per 3 deprimere liceat, hinc simplicissimum triangulum formari posse, cuius latera sint 136, 170, 174.

13. Cum hic sit

$$m = \frac{5gg - ff}{4gg} \quad \text{et} \quad n = \frac{5ff - 9gg}{4ff},$$

erit primo

$$m + n = \frac{10ffgg - f^4 - 9g^4}{4ffgg} = -\frac{(gg - ff)(9gg - ff)}{4ffgg}.$$

Deinde vero habebitur

$$m - n = \frac{9g^4 - f^4}{4ffgg} = \frac{(3gg + ff)(3gg - ff)}{4ffgg},$$

unde colligitur

$$m - n + 2 = \frac{9g^4 + 8ffgg - f^4}{4ffgg} = \frac{(gg + ff)(9gg - ff)}{4ffgg}$$

et

$$m - n - 2 = \frac{9g^4 - 8ffgg - f^4}{4ffgg} = \frac{(gg - ff)(9gg + ff)}{4ffgg}.$$

Quare, cum invenerimus $p = 4(m + n)M$, erit iam

$$p = -\frac{(gg - ff)(9gg - ff)M}{ffgg}$$

$$\text{et} \quad q = ((m - n)^2 - 4)\ M = \frac{(g^4 - f^4)(81g^4 - f^4)}{16f^4g^4} M.$$

14. Quo nunc rationem litterarum p et q ad minimos terminos revocemus, sumamus

$$M = \frac{16f^4g^4}{(gg - ff)(9gg - ff)},$$

sicque prodibit

$$p = -16ffgg \quad \text{et} \quad q = (gg + ff)(9gg + ff).$$

Ex his iam, quia erat $t = \frac{1}{2}(m - n)p + q$, prodit nunc

$$t = (gg + ff)(9gg + ff) - 2(3gg + ff)(3gg - ff).$$

Simili modo erit $u = \frac{1}{2}(m - n)\, p - q$, unde colligitur

$$u = -(gg + ff)(9gg + ff) - 2(3gg + ff)(3gg - ff).$$

Atque ex his fiet $c = 2gt$ et $z = 2fu$.

15. Pro reliquis litteris erit primo

$$a + b = 2f(p + q) \quad \text{et} \quad b - a = 2g(p - q);$$

deinde vero erit

$$x + y = 6g(p + q) \quad \text{et} \quad x - y = 2f(p - q).$$

Harum formularum ope quotquot lubuerit exempla satis expedite resolvi, idque adeo in integris, licebit, quandoquidem omnia pendent a ratione inter numeros f et g, quos ergo semper integros assumere licet.

16. Sit $f = 1$ et $g = 2$, eritque $p = -64$ et $q = 185$. Hinc iam colligitur $t = -101$ et $u = -471$; tum vero $c = -404$ et $z = -942$. Porro vero erit $b - a = -996$ et $b + a = +242$; $x + y = 1452$ et $x - y = -498$. Erit igitur

$$a = 619; \quad b = 377; \quad c = 404;$$
$$x = 477; \quad y = 975; \quad z = 942\ ^{1}).$$

Hic observetur, cum numeri x, y, z etiam pro a, b, c usurpari queant, iis per 3 divisis oriri:

$$a = 159; \quad b = 325; \quad c = 314; \text{ tum autem erit}$$
$$x = 619; \quad y = 377; \quad z = 404.$$

1) Vide p. 301 huius voluminis. R. F.

REGULA FACILIS PROBLEMATA DIOPHANTEA PER NUMEROS INTEGROS EXPEDITE RESOLVENDI[1)]

Commentatio 739 indicis ENESTROEMIANI
Mémoires de l'académie de St. Pétersbourg 4 (1811), 1813, p. 3—17
Conventui exhibita die 30. aprilis 1778

1. Quaestiones, quae in hoc genere proponi solent, ita communiter se habent, ut, proposita huiusmodi formula secundi gradus: $\alpha xx + \beta x + \gamma$, omnes valores integri pro x inveniri debeant, unde numeri quadrati resultent; quod quo fieri possit, primo necesse est, ut casus quispiam, veluti $x = a$, iam sit cognitus; deinde insuper requiritur, ut numerus α, quo quadratum xx in hac formula afficitur, sit positivus ac praeterea non-quadratus.

2. Cognito autem tali casu $x = a$ analysis, quae adhiberi solet, ita procedit, ut primo ex casu cognito alius novus eliciatur quaestioni satisfaciens, tum vero regula tradatur ex hoc casu denuo alium derivandi, atque ita porro in infinitum. Deinde vero demonstratum est cunctos istos valores ordine inventos progressionem recurrentem constituere, cuius ergo terminus generalis omnes plane continet numeros integros, qui pro x assumti formulam propositam reddant quadratum.

1) Confer commentationes 29 et 279 indicis ENESTROEMIANI: *De solutione problematum diophantaeorum per numeros integros*, Comm. acad. sc. Petr. 6, p. 175—188, *LEONHARDI EULERI Opera omnia*, series I, vol. 2, p. 6; et *De resolutione formularum quadraticarum indeterminatarum per numeros integros*. Novi comm. acad. sc. Petr. 9, p. 3—39, *LEONHARDI EULERI Opera omnia*, series I, vol. 2, p. 576. R. F.

3. Quoniam autem haec passim abunde sunt exposita, hic ipsis principiis, unde haec solutio est deducta, non immoror, sed regulam facilem sum traditurus, cuius ope statim terminus generalis, omnes plane solutiones in se complectens, expedite assignari queat, ita ut non sit opus omnia momenta, quibus solutio completa innititur, aliunde conquirere; ipsam autem quaestionem aliquanto generalius sequenti modo proponam.

PROBLEMA

Proposita formula $\alpha xx + \beta x + \gamma$ *investigare omnes valores integros pro* x *statuendos, ut numeri hinc resultantes simul in alia simili formula secundi ordinis* $\zeta yy + \eta y + \theta$ *contineantur, ita ut, si illi numeri debeant esse quadrati, haec altera formula simpliciter abitura sit in quadratum* yy.

SOLUTIO

4. Hic igitur, uti iam ante notavimus, necesse est, ut unus saltem casus satisfaciens iam aliunde sit cognitus, pro quo ponamus esse $x = a$ et $y = b$, ita ut sit $\alpha aa + \beta a + \gamma = \zeta bb + \eta b + \theta$. Praeterea vero mox patebit etiam requiri, ut productum $\alpha\zeta$ sit numerus positivus non-quadratus. Utraque haec conditio maxime est necessaria; nisi enim casus satisfaciens esset cognitus, evenire posset, ut quaestio plane foret impossibilis; tum enim, si productum $\alpha\zeta$ esset numerus quadratus, plerumque praeter casum cognitum nullus alius locum habere posset.

5. Cum igitur requirantur idonei valores integri pro litteris x et y, qui satisfaciant huic aequationi:

$$\alpha xx + \beta x + \gamma = \zeta yy + \eta y + \theta,$$

quoniam novimus tam valores ipsius x quam ipsius y secundum seriem recurrentem progredi, in subsidium vocemus aequationem quadraticam $zz = 2sz - 1$, cuius radices brevitatis gratia sint:

$$\text{altera } p = s + \sqrt{ss - 1}, \text{ altera vero } q = s - \sqrt{ss - 1},$$

quarum ergo summa est $p + q = 2s$ et productum $pq = 1$. Notum enim est terminos generales serierum recurrentium in genere potestates quascunque talium formularum p et q continere, unde formulae pro nostris litteris x et y generaliter ita exprimi sunt concipiendae:

$$x = Ap^n + Bq^n + C \quad \text{et} \quad y = Fp^n + Gq^n + H\,,$$

unde si exponenti indefinito n tribuatur valor $n = 0$, oriatur casus cognitus $x = a$ et $y = b$; sin autem loco n successive capiantur numeri ordine 1, 2, 3, 4, 5, 6 etc., ut omnes valores satisfacientes tam pro x quam pro y oriantur.

6. Tota ergo quaestio huc redit: cuiusmodi valores tam quantitati s, qua ambae litterae p et q definiuntur, quam litteris A, B, C, F, G, H tribui conveniat, ut singuli numeri pro n assumti praebeant tam pro x quam pro y valores integros problemati satisfacientes?

7. Quoniam autem isti valores aequationi propositae

$$\alpha xx + \beta x + \gamma = \zeta yy + \eta y + \theta$$

satisfacere debent, facile intelligitur has formas propius ad hunc finem ita accommodari posse statuendo:

$$x = \frac{f}{\sqrt{\alpha}}\,p^n + \frac{g}{\sqrt{\alpha}}\,q^n - \frac{\beta}{2\alpha} \quad \text{et} \quad y = \frac{f}{\sqrt{\zeta}}\,p^n - \frac{g}{\sqrt{\zeta}}\,q^n - \frac{\eta}{2\zeta}\,.$$

Hinc enim, facta substitutione, prius aequationis nostrae membrum $\alpha xx + \beta x + \gamma$ hanc induet formam:

$$ffp^{2n} + ggq^{2n} + 2fgp^nq^n - \frac{\beta\beta}{4\alpha} + \gamma\,,$$

quae, ob $pq = 1$, reducitur ad hanc:

$$ffp^{2n} + ggq^{2n} + 2fg + \gamma - \frac{\beta\beta}{4\alpha}\,.$$

Alterum vero membrum $\zeta yy + \eta y + \theta$ ad hanc formam redit:

$$ffp^{2n} + ggq^{2n} - 2fg + \theta - \frac{\eta\eta}{4\zeta}\,,$$

et cum istae duae formae inter se debeant esse aequales, hinc orietur ista aequatio: $4fg + \gamma - \frac{\beta\beta}{4\alpha} = -\frac{\eta\eta}{4\zeta} + \theta$, ideoque:

$$4fg = \frac{\beta\beta}{4\alpha} - \frac{\eta\eta}{4\zeta} + \theta - \gamma\,.$$

8. Quoniam in hac postrema aequatione exponens variabilis n non amplius inest, sufficit, ut pro unico casu cognito $x = a$ et $y = b$ satisfaciat.

Assumimus autem casum hunc cognitum oriri statuendo $n = 0$; hinc igitur, ob $x = a$, prodibit

$$a = \frac{f+g}{\sqrt{\alpha}} - \frac{\beta}{2\alpha};$$

tum vero, ob $y = b$, erit

$$b = \frac{f-g}{\sqrt{\zeta}} - \frac{\eta}{2\zeta},$$

ex quibus duabus conditionibus ambae litterae etiamnunc incognitae f et g definiri poterunt, cum sit:

$$f + g = a\sqrt{\alpha} + \frac{\beta}{2\sqrt{\alpha}} = \frac{2\alpha a + \beta}{2\sqrt{\alpha}},$$

similique modo

$$f - g = b\sqrt{\zeta} + \frac{\eta}{2\sqrt{\zeta}} = \frac{2\zeta b + \eta}{2\sqrt{\zeta}},$$

hincque aequalitas postremo loco inventa sponte adimpletur; si quidem hinc fit:

$$(f+g)^2 - (f-g)^2 = 4fg = \alpha aa + \beta a + \frac{\beta\beta}{4\alpha} - \zeta bb - \eta b - \frac{\eta\eta}{4\zeta}.$$

Quia igitur per hypothesin est $\alpha aa + \beta\alpha + \gamma = \zeta bb + \eta b + \theta$, hinc evadit $4fg = \frac{\beta\beta}{4\alpha} - \frac{\eta\eta}{4\zeta} + \theta - \gamma$, prorsus uti conditio superior postulat.

9. Inventis igitur valoribus litterarum f et g solutio quaesita nostri problematis sequentibus binis formulis continebitur:

$$x = \frac{f}{\sqrt{\alpha}}p^n + \frac{g}{\sqrt{\alpha}}q^n - \frac{\beta}{2\alpha} \quad \text{et} \quad y = \frac{f}{\sqrt{\zeta}}p^n - \frac{g}{\sqrt{\zeta}}q^n - \frac{\eta}{2\zeta},$$

ubi ergo nihil aliud superest, nisi ut binae quantitates

$$p = s + \sqrt{ss-1} \quad \text{et} \quad q = s - \sqrt{ss-1}$$

rite determinentur; ubi manifestum est litteram s ita comparatam esse debere, ut pro x et y resultent valores rationales. Hunc in finem contemplemur casum, quo $n = 1$, qui praebebit:

$$x = \frac{(f+g)s}{\sqrt{\alpha}} + \frac{(f-g)\sqrt{ss-1}}{\sqrt{\alpha}} - \frac{\beta}{2\alpha} \quad \text{et}$$

$$y = \frac{(f-g)s}{\sqrt{\zeta}} + \frac{(f+g)\sqrt{ss-1}}{\sqrt{\zeta}} - \frac{\eta}{2\zeta}.$$

Cum igitur supra invenerimus

$$f+g=a\sqrt{\alpha}+\frac{\beta}{2\sqrt{\alpha}} \quad \text{et} \quad f-g=b\sqrt{\zeta}+\frac{\eta}{2\sqrt{\zeta}},$$

his valoribus substitutis habebimus:

$$x=as+\frac{\beta s}{2\alpha}+\frac{b\sqrt{\zeta(ss-1)}}{\sqrt{\alpha}}+\frac{\eta\sqrt{ss-1}}{2\sqrt{\alpha\zeta}}-\frac{\beta}{2\alpha},$$

sive

$$x=as+\frac{\beta(s-1)}{2\alpha}+\frac{b\sqrt{\zeta(ss-1)}}{\sqrt{\alpha}}+\frac{\eta\sqrt{ss-1}}{2\sqrt{\alpha\zeta}}.$$

Similique modo erit:

$$y=bs+\frac{\eta(s-1)}{2\zeta}+\frac{a\sqrt{\alpha(ss-1)}}{\sqrt{\zeta}}+\frac{\beta\sqrt{ss-1}}{2\sqrt{\alpha\zeta}}.$$

10. Ut igitur hae ambae expressiones ab omni irrationalitate liberentur, evidens est hoc obtineri, si modo fuerit formula $\frac{\sqrt{ss-1}}{\sqrt{\alpha\zeta}}$ quantitas rationalis. Ponatur igitur $\frac{\sqrt{ss-1}}{\sqrt{\alpha\zeta}}=r$, eritque $ss-1=\alpha\zeta rr$, hincque porro $s=\sqrt{1+\alpha\zeta rr}$, quam ergo formulam denuo rationalem esse oportet, id quod semper praestari potest ope problematis Pelliani, si modo fuerit $\alpha\zeta$ numerus positivus non-quadratus, uti iam supra innuimus.

11. Ante omnia igitur pro resolutione nostri problematis ex binis coëfficientibus α et ζ quaeratur numerus integer r, ut formula $\alpha\zeta rr+1$ evadat quadratum, tum vero sumatur $s=\sqrt{\alpha\zeta rr+1}$; et quoniam hinc fit

$$\sqrt{(ss-1)}=r\sqrt{\alpha\zeta},$$

casus $n=1$ pro x et y sequentes suppeditabit valores rationales:

$$x=as+\frac{\beta(s-1)}{2\alpha}+\zeta br+\frac{1}{2}\eta r \quad \text{et}$$

$$y=bs+\frac{\eta(s-1)}{2\zeta}+\alpha ar+\frac{1}{2}\beta r,$$

qui valores utique sunt rationales atque adeo integri, nisi forte formulae $\frac{\beta(s-1)}{2\alpha}$ et $\frac{\eta(s-1)}{2\zeta}$ adhuc fractiones involvant, quas autem quemadmodum tollere liceat, deinceps ostendemus.

12. Colligamus ergo omnia, quibus solutio nostri problematis innititur, ac primo quidem investigatis binis numeris integris r et s, ita ut sit

$$s = \sqrt{\alpha\zeta rr + 1},$$

statuatur brevitatis gratia

$$p = s + r\sqrt{\alpha\zeta} \quad \text{et} \quad q = s - r\sqrt{\alpha\zeta};$$

tum vero binae litterae f et g ita determinentur, ut sit

$$f + g = a\sqrt{\alpha} + \frac{\beta}{2\sqrt{\alpha}} \quad \text{et} \quad f - g = b\sqrt{\zeta} + \frac{\eta}{2\sqrt{\zeta}},$$

quo facto formulae generales pro valoribus integris ambarum quantitatum x et y ita se habebunt:

$$x = \frac{f}{\sqrt{\alpha}}(s + r\sqrt{\alpha\zeta})^n + \frac{g}{\sqrt{\alpha}}(s - r\sqrt{\alpha\zeta})^n - \frac{\beta}{2\alpha} \quad \text{et}$$

$$y = \frac{f}{\sqrt{\zeta}}(s + r\sqrt{\alpha\zeta})^n - \frac{g}{\sqrt{\zeta}}(s - r\sqrt{\alpha\zeta})^n - \frac{\eta}{2\zeta},$$

ubi omnes numeri integri, pro n assumti, praebebunt valores satisfacientes pro binis litteris incognitis x et y, qui, nisi sint ipsi integri, facile ad integros revocari poterunt, uti mox ostendemus.

13. Hic ante omnia observasse iuvabit, statim atque bini valores se insequentes fuerint inventi, per scalam relationis ex iis facillime sequentes omnes formari posse. Ad quod ostendendum sint pro exponente quocunque n valores satisfacientes:

$$x = \frac{f}{\sqrt{\alpha}}p^n + \frac{g}{\sqrt{\alpha}}q^n - \frac{\beta}{2\alpha} \quad \text{et} \quad y = \frac{f}{\sqrt{\zeta}}p^n - \frac{g}{\sqrt{\zeta}}q^n - \frac{\eta}{2\zeta},$$

hos autem proxime sequentes ab exponente $n + 1$ oriundi sint:

$$x' = \frac{f}{\sqrt{\alpha}}p^{n+1} + \frac{g}{\sqrt{\alpha}}q^{n+1} - \frac{\beta}{2\alpha} \quad \text{et} \quad y' = \frac{f}{\sqrt{\zeta}}p^{n+1} - \frac{g}{\sqrt{\zeta}}q^{n+1} - \frac{\eta}{2\zeta},$$

porro vero sequentes sint:

$$x'' = \frac{f}{\sqrt{\alpha}}p^{n+2} + \frac{g}{\sqrt{\alpha}}q^{n+2} - \frac{\beta}{2\alpha} \quad \text{et} \quad y'' = \frac{f}{\sqrt{\zeta}}p^{n+2} - \frac{g}{\sqrt{\zeta}}q^{n+2} - \frac{\eta}{2\zeta},$$

unde colligitur fore:

$$x'' - \lambda x' + x = \frac{f}{\sqrt{\alpha}} p^n(pp - \lambda p + 1) + \frac{g}{\sqrt{\alpha}} q^n(qq - \lambda q + 1) - \frac{\beta}{2\alpha}(2 - \lambda) .$$

Similique modo erit:

$$y'' - \lambda y' + y = \frac{f}{\sqrt{\zeta}} p^n(pp - \lambda p + 1) - \frac{g}{\sqrt{\zeta}} q^n(qq - \lambda q + 1) - \frac{\eta}{2\zeta}(2 - \lambda) .$$

14. Initio autem vidimus litteras p et q esse binas radices huius aequationis quadraticae: $zz - 2sz + 1 = 0$, ita ut sit tam $pp - 2sp + 1 = 0$ quam $qq - 2sq + 1 = 0$; quocirca, si loco λ accipiamus $2s$, habebimus:

$$x'' - 2sx' + x = \frac{\beta}{\alpha}(s - 1) ;$$

eodemque modo erit quoque

$$y'' - 2sy' + y = \frac{\eta}{\zeta}(s - 1) .$$

Consequenter simul atque invenerimus binos valores se immediate sequentes x et x', item y et y', ex iis protinus sequentes reperientur per has formulas:

$$x'' = 2sx' - x + \frac{\beta}{\alpha}(s - 1)$$

et

$$y'' = 2sy' - y + \frac{\eta}{\zeta}(s - 1) ;$$

unde evidens est, dummodo bini valores priores fuerint rationales, sequentes omnes in infinitum pariter rationales esse futuros.

15. Cum igitur primi valores ipsarum x et y, ex $n = 0$ oriundi, sint per hypothesin a et b, si immediate sequentes, ex $n = 1$ orti, designentur per a' et b', tum sequentes, ob:

$$a' = as + \frac{\beta(s - 1)}{2\alpha} + \zeta br + \tfrac{1}{2}\eta r$$

et

$$b' = bs + \frac{\eta(s - 1)}{2\zeta} + \alpha ar + \tfrac{1}{2}\beta r ,$$

erunt:

$$a'' = a(2ss - 1) + 2\zeta brs + \frac{\beta(ss-1)}{\alpha} + \eta rs \quad \text{et}$$

$$b'' = b(2ss - 1) + 2\alpha ars + \frac{\eta(ss-1)}{\zeta} + \beta rs .$$

Hos autem postremos terminos semper esse numeros integros inde patet, quod sit $ss - 1 = \alpha\zeta rr$; unde pro priore valore a'' fit fractio $\frac{\beta(ss-1)}{\alpha} = \beta\zeta rr$; pro altera autem $\frac{\eta(ss-1)}{\zeta} = \alpha\eta rr$. Hinc sequitur in genere, etiamsi valores a' et b' adhuc fractiones involvant, sequentes tamen a'' et b'' semper esse integros; quod idem intelligendum est de omnibus sequentibus alternatim sumtis; unde termini fractionibus inquinati statim evitari poterunt, si exponenti n non omnes numeros, sed pares tantum tribuamus, quod fiet ponendo:

$$x = \frac{f}{\sqrt{\alpha}}(pp)^n + \frac{g}{\sqrt{\alpha}}(qq)^n - \frac{\beta}{2\alpha}$$

et

$$y = \frac{f}{\sqrt{\zeta}}(pp)^n - \frac{g}{\sqrt{\zeta}}(qq)^n - \frac{\eta}{2\zeta} .$$

Cum igitur fuerit $p = s + \sqrt{ss-1}$ et $q = s - \sqrt{ss-1}$, erit

$$pp = 2ss - 1 + 2s\sqrt{ss-1} \quad \text{et} \quad qq = 2ss - 1 - 2s\sqrt{ss-1},$$

ita ut in praecedentibus formulis tantum opus sit loco s scribere $2ss - 1$, et loco $\sqrt{ss-1} = r\sqrt{\alpha\zeta}$ scribi debebit $2r\sqrt{a\zeta(\alpha\zeta rr + 1)}$; quamobrem, omissis terminis fractis, si x', y', x'', y'' etc. tantum integros se immediate sequentes denotent, lex progressionis ita se habebit:

$$x'' = 2(2ss - 1)x' - x + 2\beta\zeta rr \quad \text{et}$$
$$y'' = 2(2ss - 1)y' - y + 2\alpha\eta rr .$$

Praeterea vero hoc casu erit:

$$a' = a(2ss - 1) + \beta\zeta rr + 2\zeta brs + \eta rs \quad \text{et}$$
$$b' = b(2ss - 1) + \alpha\eta rr + 2\alpha ars + \beta rs .$$

EXEMPLUM 1

16. *Invenire omnes numeros trigonales, qui simul sint quadrati.*

Requiritur ergo, ut sit $\frac{xx+x}{2} = yy$, ideoque in integris $xx + x = 2yy$; ubi casus cognitus manifesto est $x = a = 1$ et $y = b = 1$, vel etiam $x = a = 0$

et $y = b = 0$, ubi perinde est, utrovis utamur. Hic igitur primo est $\alpha = 1$, $\beta = 1$ et $\gamma = 0$, tum vero $\zeta = 2$, $\eta = 0$ et $\theta = 0$. Quare cum esse debeat $s = \sqrt{\alpha\zeta rr + 1}$, erit hoc casu $s = \sqrt{2rr + 1}$, unde sumto $r = 2$ fit $s = 3$. Deinde ex casu cognito $a = 0$ et $b = 0$ habebimus $f + g = \frac{1}{2}$ et $f - g = 0$, consequenter $f = g = \frac{1}{4}$; unde formulae generales pro x et y reperiuntur:

$$x = \frac{1}{4}(3 + 2\sqrt{2})^n + \frac{1}{4}(3 - 2\sqrt{2})^n - \frac{1}{2}$$

et

$$y = \frac{1}{4\sqrt{2}}(3 + 2\sqrt{2})^n - \frac{1}{4\sqrt{2}}(3 - 2\sqrt{2})^n .$$

Hinc sumto $n = 0$ prodit ipse casus cognitus $x = 0$ et $y = 0$.

17. Sumatur nunc $n = 1$, ut prodeat secunda solutio, quae erit $x' = 1$ et $y' = 1$, qui est alter casus cognitus. Sumto autem $n = 2$, ob

$$(3 \pm 2\sqrt{2})^2 = 17 \pm 12\sqrt{2} ,$$

oritur tertia solutio $x'' = 8$ et $y'' = 6$. Neque vero opus est hos postremos valores ex ipsis formulis generalibus deducere, quoniam novimus tam valores ipsius x quam ipsius y secundum certam legem serierum recurrentium procedere. Cum igitur per § 14 sit $x'' = 6x' - x + 2$ et $y'' = 6y' - y$, hinc ex duobus casibus prioribus ambae series pro x et y ita procedent:

pro x ... 0, 1, 8, 49, 288, 1681 etc.
pro y ... 0, 1, 6, 35, 204, 1189 etc.

Hinc enim utique erit $\frac{8 \cdot 9}{2} = 6^2 = 36$; similique modo

$$\frac{49 \cdot 50}{2} = 35^2 = 1225 ; \text{ porro } \frac{288 \cdot 289}{2} = 204^2 = 41616 .$$

EXEMPLUM 2

18. *Invenire omnes numeros quadratos, qui unitate minuti sint numeri trigonales, cuiusmodi quadrata sunt* 1, 4, 16 *etc.*

Requiritur ergo, ut sit $xx - 1 = \frac{yy + y}{2}$, sive $2xx - 2 = yy + y$, ita ut sit $\alpha = 2$, $\beta = 0$ et $\gamma = -2$, tum vero $\zeta = 1$, $\eta = 1$ et $\theta = 0$; casus autem cognitus sponte se offerens est $x = a = 1$ et $y = b = 0$. Deinde ob $\alpha\zeta = 2$ erit, ut ante, $s = \sqrt{2rr + 1}$, ideoque $r = 2$ et $s = 3$. Praeterea vero habe-

bimus $f+g=\sqrt{2}$ et $f-g=\frac{1}{2}$, unde fit $f=\frac{2\sqrt{2}+1}{4}$ et $g=\frac{2\sqrt{2}-1}{4}$.

Hinc formulae generales pro x et y colliguntur:

$$x=\frac{(2\sqrt{2}+1)}{4\sqrt{2}}(3+2\sqrt{2})^n+\frac{(2\sqrt{2}-1)}{4\sqrt{2}}(3-2\sqrt{2})^n$$

et

$$y=\frac{(2\sqrt{2}+1)}{4}(3+2\sqrt{2})^n-\frac{(2\sqrt{2}-1)}{4}(3-2\sqrt{2})^n-\frac{1}{2}.$$

19. Sumto igitur $n=0$ sequitur fore $x=1$ et $y=0$, qui est ipse casus cognitus. Posito autem $n=1$ erit $x=4$ et $y=5$. Ex his duobus casibus sequentes eruuntur ope formularum $x''=6x'-x$ et $y''=6y'-y+2$, unde ergo binae sequentes series derivantur:

pro x ... 1, 4, 23, 134, 781 etc. et
pro y ... 0, 5, 32, 189, 1104 etc.,

qui quomodo satisfaciant, manifestum est, cum sit:

$$4^2-1=3\cdot 5=\frac{5\cdot 6}{2},\quad 23^2-1=22\cdot 24=\frac{32\cdot 33}{2};$$

deinde $134^2-1=133\cdot 135=\frac{189\cdot 190}{2}$.

20. Verum hoc modo non omnes obtinentur solutiones, quandoquidem initio iam observavimus satisfacere quoque valorem $x=2$ et $y=2$. Verum hic probe tenendum est ambas has series etiam retro continuari posse, ope formularum $x=6x'-x''$ et $y=6y'-y''+2$, unde insuper oriuntur sequentes valores:

pro x ... 2174, 373, 64, 11, 2, 1, 4 etc.
pro y ... —3075, —528, —91, —16, —3, 0, 5 etc.,

ubi valores negativi ipsius y facile in positivos transmutantur. Quia enim numerus trigonalis, cuius latus est negativum $-m$, est $\frac{m(m-1)}{2}$, qui est quoque trigonalis oriundus a latere $m-1$, loco $-m$ scribere licet $m-1$, unde novi valores hinc oriundi erunt more solito expressi:

pro x ... 1, 2, 11, 64, 373, 2174 etc. et

pro y ... -1, 2, 15, 90, 527, 3074 etc.,

qui aeque satisfaciunt, ac priores, cum sit:

$$2^2 - 1 = \frac{2 \cdot 3}{2},\ 11^2 - 1 = 10 \cdot 12 = \frac{15 \cdot 16}{2} \text{ etc.}$$

21. Pro hoc igitur exemplo completa solutio ex binis seriebus recurrentibus est composita, ita ut numeri quadrati, qui unitate minuti evadunt trigonales, ordine ita procedant:

$$1,\ 2^2,\ 4^2,\ 11^2,\ 23^2,\ 64^2,\ 134^2,\ 373^2,\ 781^2 \text{ etc.}$$

Haec autem duplicitas in primo exemplo non occurrit, quandoquidem series ibi inventae, etiamsi retro continuentur, novas solutiones non producunt.

EXEMPLUM 3

22. *Invenire eos numeros trigonales, qui triplicati etiamnunc sint trigonales, cuiusmodi est 1, cuius triplum pariter est trigonalis.*

Hic ergo requiritur, ut sit: $3\frac{(xx+x)}{2} = \frac{yy+y}{2}$, sive $3xx+3x = yy+y$, ita ut hic sit $\alpha = 3$, $\beta = 3$, $\gamma = 0$ et $\zeta = 1$, $\eta = 1$ et $\theta = 0$, pro casu autem cognito $x = a = 1$ et $y = b = 2$. Deinde ob $\alpha\zeta = 3$ sumi debet $s = \sqrt{(3rr+1)}$, sicque sumere licet $r = 1$ et $s = 2$; tum vero ex casu cognito deducimus $f + g = \sqrt{3} + \frac{3}{2\sqrt{3}}$ et $f - g = 2 + \frac{1}{2}$, ideoque $f = \frac{3\sqrt{3}+5}{4}$ et $g = \frac{3\sqrt{3}-5}{4}$, unde formulae generales pro x et y sunt:

$$x = \left(\frac{3\sqrt{3}+5}{4\sqrt{3}}\right)(2+\sqrt{3})^n + \left(\frac{3\sqrt{3}-5}{4\sqrt{3}}\right)(2-\sqrt{3})^n - \frac{1}{2} \text{ et}$$

$$y = \left(\frac{3\sqrt{3}+5}{4}\right)(2+\sqrt{3})^n - \left(\frac{3\sqrt{3}-5}{4}\right)(2-\sqrt{3})^n - \frac{1}{2}.$$

23. Haec autem binae formulae iustas praebent solutiones non solum, quando pro n numeri integri positivi accipiuntur, sed etiam negativi, quare cum sit:

$$(2+\sqrt{3})^{-n} = (2-\sqrt{3})^n,$$

similique modo

$$(2-\sqrt{3})^{-n} = (2+\sqrt{3})^n,$$

his notatis formulae pro altera solutione erunt:

$$x = \left(\frac{3\sqrt{3}+5}{4\sqrt{3}}\right)(2-\sqrt{3})^n + \left(\frac{3\sqrt{3}-5}{4\sqrt{3}}\right)(2+\sqrt{3})^n - \frac{1}{2} \text{ et}$$

$$y = \left(\frac{3\sqrt{3}+5}{4}\right)(2-\sqrt{3})^n - \left(\frac{3\sqrt{3}-5}{4}\right)(2+\sqrt{3})^n - \frac{1}{2},$$

unde sumto $n = 0$ utraque solutio praebet ipsum casum cognitum $x = 1$ et $y = 2$.

24. Sumamus nunc $n = 1$, ac priores formulae nobis dabunt $x = 5$ et $y = 9$, posteriores vero formulae praebent $x = 0$ et $y = 0$. Ex cognitis autem his duabus solutionibus sequentes erui possunt, ope formularum:

$$x'' = 4x' - x + 1 \quad \text{et} \quad y'' = 4y' - y + 1,$$

unde ex priore casu deducuntur sequentes solutiones:

pro x . . . 1, 5, 20, 76, 285 etc.
pro y . . . 2, 9, 35, 132, 494 etc.

Posterior vero casus praebet solutiones sequentes:

pro x . . . 1, 0, 0, 1, 5, 20, 76, 285 etc.
pro y . . . 2, 0, -1, -3, -10, -36, -133, -495 etc.

Modo ante autem vidimus numeros trigonales, quorum radices sunt negativae, puta $-m$, convenire cum radicibus $m-1$; unde intelligitur posteriorem casum nullas novas solutiones producere. Sicque omnes numeri trigonales, quorum tripla sunt etiam trigonales, hanc seriem constituunt:

0, 1, 15, 210, 2926, 40755 etc.

DE DIVISORIBUS NUMERORUM IN FORMA $mxx + nyy$ CONTENTORUM

Commentatio 744 indicis ENESTROEMIANI
Mémoires de l'académie des sciences de St-Pétersbourg 5 (1812), 1815, p. 3—23
Conventui exhibuit die 21. maii 1778

1. Hic perpetuo assumimus binos numeros x et y inter se esse primos, atque notum est numeros in tali forma contentos nunquam per omnes numeros primos dividi posse, sed semper pro qualibet forma certos numeros primos excludi, quorum multitudo quasi est semissis omnium plane numerorum primorum. Ita demonstratum est numeros in hac forma contentos $xx + yy$ per alios numeros primos dividi non posse, nisi qui sint formae $4N + 1$, ideoque omnes numeros primos formae $4N - 1$ penitus excludi.

2. Eodem modo demonstratum est numeros in hac forma contentos $2xx + yy$ alios divisores primos non admittere, nisi qui contineantur in alterutra harum formarum $8N + 1$ vel $8N + 3$, ita ut reliqui numeri primi in formis $8N + 5$ et $8N + 7$ contineantur. Simili modo omnes divisores primi numerorum formae $3xx + yy$ sunt vel formae $12N + 1$ vel $12N + 7$; reliqui vero, qui sunt vel formae $12N + 5$ vel $12N + 11$, nunquam divisores existere possunt; unde patet omnes divisores comprehendi in forma $6N + 1$, exclusos vero in forma $6N + 5$.

3. Haud absimili modo res comparata est pro generali forma $mxx + nyy$, cuius omnes divisores primi continentur in certis huiusmodi formulis: $4mnN + \alpha$, $4mnN + \beta$, $4mnN + \gamma$ etc., ubi α, β, γ etc. sunt certi numeri

quovis casu facile determinandi, exclusi autem numeri continentur in totidem aliis formulis $4mnN - \alpha$, $4mnN - \beta$, $4mnN - \gamma$ etc., id quod sequenti modo commode exprimi potest, ut pro forma generali $mxx + nyy$ forma divisorum statuatur $4mnN + \alpha$, β, γ, δ, ε etc., forma autem numerorum exclusorum $4mnN - \alpha$, $- \beta$, $- \gamma$, $- \delta$, $- \varepsilon$ etc.

4. Hic primo pro quolibet casu numerorum m et n evidens est numeros α, β, γ, δ etc. primos esse debere respectu numeri $4mn$, quia aliter numeri primi prodire non possent. Deinde etiam facile intelligere licet inter numeros α, β, γ [etc.] semper contineri unitatem atque etiam omnes numeros quadratos ad $4mn$ primos. Praeterea vero in ordine horum numerorum α, β, γ, δ etc. semper etiam occurrunt omnes potestates singulorum, tum vero etiam omnia producta ex binis vel ternis, veluti $\alpha\beta$, $\alpha\beta\gamma$, quatenus scilicet numerum $4mn$ non superant. Denique etiam notasse iuvabit quovis casu istos numeros α, β, γ, δ etc. tantum a producto mn pendere, ita ut hae duae formae generales $mxx + nyy$ et $m'xx + n'yy$ easdem divisorum formas habeant, si modo fuerit $m'n' = mn$.

5. Haud abs re fore arbitror sequentem tabulam subiunxisse, quae pro simplicioribus numeris mn ostendat formas divisorum primorum:

Valores producti mn	Forma divisorum
1	$4N + 1$,
2	$8N + 1$, 3
3	$12N + 1$, 7
5	$20N + 1$, 3, 7, 9
6	$24N + 1$, 5, 7, 11
7	$28N + 1$, 9, 11, 15, 23, 25
10	$40N + 1$, 7, 9, 11, 13, 19, 23, 37
11	$44N + 1$, 3, 5, 9, 15, 23, 25, 27, 31, 37
13	$52N + 1$, 7, 9, 11, 15, 17, 19, 25, 29, 31, 47, 49
14	$56N + 1$, 3, 5, 9, 13, 15, 19, 23, 25, 27, 39, 45
15	$60N + 1$, 17, 19, 23, 31, 47, 49, 53

6. In his scilicet formis omnes numeri, qui divisores esse possunt cuiuslibet numeri in forma $mxx + nyy$ contenti, divisione per $4mn$ facta, infra

limitem $4mn$ reducuntur. Quodsi autem velimus numeros negativos admittere, tum omnes isti numeri adeo infra $2mn$ redigi poterunt; hocque modo omnes plane numeri ad $4mn$ primi et minores quam $2mn$ occurrent, vel signo + vel signo — affecti; et quoniam complementa horum numerorum ad $4mn$ praebent numeros exclusos, tantum opus est in illis formis signa permutare, ut obtineantur omnes numeri exclusi, qui nunquam esse possunt divisores cuiusquam numeri formae $mxx + nyy$.

7. Quodsi hoc modo divisores istius formae $mxx + nyy$ disponamus, ut omnes plane numeri ad $2mn$ primi, eoque minores, occurrant, egregiae proprietates in iis deprehendentur, si cuique horum numerorum suum complementum ad $2mn$ subscribamus; hocque modo superior ordo tantum usque ad mn procedet, dum maiores ab mn usque ad $2mn$ illis subscribentur. Pro varia autem numeri mn indole patebit bina complementa sibi subscripta sive paribus affici signis sive contrariis; paribus scilicet gaudebunt signis casibus, quibus est vel $mn = 4i + 1$ vel $mn = 4i + 2$, reliquis vero binis casibus, quibus vel $mn = 4i + 3$ vel $mn = 4i + 4$, bina illa complementa contrariis signis afficientur.

8. Hoc igitur modo superiores formulas pro divisoribus numerorum in forma $mxx + nyy$ contentorum repraesentemus atque adeo ulterius continuemus:

mn	Forma divisorum
1	$4N + 1$
2	$8N + 1$ $+ 3$
3	$12N + 1$ $- 5$
4	$16N + 1, - 3$ $- 7, + 5$
5	$20N + 1, + 3$ $+ 9, + 7$
6	$24N + 1, + 5$ $+ 11, + 7$

mn	Forma divisorum
7	$28N + 1, -3, -5$ $-13, +11, +9$
8	$32N + 1, +3, -5, -7$ $-15, -13, +11, +9$
9	$36N + 1, +5, -7$ $+17, +13, -11$
10	$40N + 1, -3, +7, +9$ $+19, -17, +13, +11$
11	$44N + 1, +3, +5, -7, +9$ $-21, -19, -17, +15, -13$
12	$48N + 1, -5, +7, -11$ $-23, +19, -17, +13$
13	$52N + 1, -3, -5, +7, +9, +11$ $+25, -23, -21, +19, +17, +15$
14	$56N + 1, +3, +5, +9, -11, +13$ $+27, +25, +23, +19, -17, +15$
15	$60N + 1, -7, -11, -13$ $-29, +23, +19, +17$
16	$64N + 1, -3, +5, -7, +9, -11, +13, -15$ $-31, +29, -27, +25, -23, +21, -19, +17$
17	$68N + 1, +3, -5, +7, +9, +11, +13, -15$ $+33, +31, -29, +27, +25, +23, +21, -19$
18	$72N + 1, -5, -7, +11, -13, +17$ $+35, -31, -29, +25, -23, +19$
19	$76N + 1, -3, +5, +7, +9, +11, -13, -15, +17$ $-37, +35, -33, -31, -29, -27, +25, +23, -21$
20	$80N + 1, +3, +7, +9, -11, -13, -17, -19$ $-39, -37, -33, -31, +29, +27, +23, +21$

mn	Forma divisorum
21	$84N + 1, + 5, + 11, -13, + 17, + 19$ $+ 41, + 37, + 31, -29, + 25, + 23$
22	$88N + 1, - 3, - 5, - 7, + 9, + 13, + 15, - 17, + 19, + 21$ $+ 43, - 41, - 39, - 37, + 35, + 31, + 29, - 27, + 25, + 23$
23	$92N + 1, + 3, - 5, - 7, + 9, - 11, + 13, - 15, - 17, - 19, - 21$ $- 45, - 43, + 41, + 39, - 37, + 35, - 33, + 31, + 29, + 27, + 25$
24	$96N + 1, + 5, + 7, + 11, - 13, - 17, - 19, - 23$ $- 47, - 43, - 41, - 37, + 35, + 31, + 29, + 25$
25	$100N + 1, - 3, - 7, + 9, - 11, + 13, + 17, - 19, + 21, - 23$ $+ 49, - 47, - 43, + 41, - 39, + 37, + 33, - 31, + 29, - 27$

9. Quodsi haec exempla rite contemplemur, insignia theoremata ex iis colligere poterimus, quae eo magis omnem attentionem merebuntur, quod principia, unde demonstratio petenda videtur, plerumque prorsus sunt etiamnunc incognita, ita ut ista consideratio amplissimum campum nobis aperiat naturam numerorum profundius perscrutandi.

THEOREMA 1

10. *Denotante p numerum quemcunque ad $2mn$ primum, si fuerit $4mna + p$ divisor cuiuspiam numeri in forma $mxx + nyy$ contenti, tum omnes numeri primi in formula $4mnz + p$ contenti certe erunt divisores formae nostrae propositae; contra vero omnes plane numeri huius formae $4mnz - p$ ex classe divisorum penitus excludentur.*

THEOREMA 2

11. *Denotante p numerum ad $2mn$ primum, si fuerit $4mna + p$ numerus primus neque ullius numeri in forma $mxx + nyy$ contenti divisor, tum omnes plane numeri in forma $4mnz + p$ contenti sive sint primi sive compositi ex classe*

divisorum excludentur; contra vero omnes numeri primi formae $4mnz - p$ *certe erunt divisores cuiuspiam numeri in forma* $mxx + nyy$ *contenti.*

THEOREMA 3

12. *Denotante* p *numerum ad* $2mn$ *primum, si fuerit numerus* $2mna - p$ *divisor formae propositae* $mxx + nyy$, *tum omnes numeri primi in forma* $4mnz - p$ *contenti certe erunt divisores formae propositae; contra vero omnes plane numeri in forma* $4mnz + p$ *contenti ex classe divisorum excludentur.*

THEOREMA 4

13. *Denotante* p *numerum ad* $2mn$ *primum, si fuerit* $4mna - p$ *numerus primus neque ullius numeri in forma* $mxx + nyy$ *contenti divisor, tum omnes plane numeri in forma* $4mnz - p$ *contenti sive sint primi sive compositi ex classe divisorum excludentur; contra vero omnes numeri primi formae* $4mnz + p$ *certe erunt divisores cuiuspiam numeri in forma* $mxx + nyy$ *contenti.*

THEOREMA 5

14. *Si fuerit* mn *numerus formae vel* $4i + 1$ *vel* $4i + 2$ *atque* $4mna + p$ *divisor formae* $mxx + nyy$, *ita ut omnes numeri primi in hac forma* $4mnz + p$ *contenti sint divisores formae propositae, tum omnes numeri primi in hac forma contenti* $4mnz + 2mn - p$ *etiam erunt divisores formae propositae; contra vero omnes numeri formae* $4mnz - 2mn + p$ *vel etiam* $4mnz + 2mn + p$ *ex classe divisorum excludentur.*

THEOREMA 6

15. *Si fuerit* mn *numerus formae vel* $4i + 1$ *vel* $4i + 2$ *atque* $4mna - p$ *divisor formae* $mxx + nyy$, *ita ut omnes numeri primi in hac forma* $4mnz - p$ *contenti sint divisores formae propositae, tum omnes numeri primi in hac formula contenti* $4mnz - 2mn + p$ *etiam erunt divisores formae propositae; contra vero omnes numeri formae* $4mnz - 2mn - p$ *vel etiam* $4mnz + 2mn - p$ *ex classe divisorum excludentur.*

THEOREMA 7

16. *Si fuerit mn numerus vel formae $4i$ vel $4i-1$ atque $4mna+p$ divisor formae $mxx+nyy$, ita ut omnes numeri primi in hac forma $4mnz+p$ contenti sint divisores formae propositae, tum omnes numeri primi in hac formula contenti $4mnz-2mn+p$ etiam erunt divisores formae propositae; contra autem omnes numeri formae $4mnz-2mn-p$ ex classe divisorum excludentur.*

THEOREMA 8

17. *Si fuerit mn numerus formae vel $4i$ vel $4i-1$ atque $4mna-p$ divisor formae $mxx+nyy$, ita ut omnes numeri primi in hac forma $4mnz-p$ contenti sint divisores formae propositae, tum omnes numeri primi in hac forma contenti $4mnz+2mn-p$ etiam erunt divisores formae propositae; contra vero omnes numeri formae $4mnz-2mn-p$ ex classe divisorum excludentur.*

COROLLARIUM

18. Denotante igitur p numerum quemcunque ad $2mn$ primum, omnes numeri primi vel in forma $4mnz+p$ vel in forma $4mnz-p$ contenti certe erunt [vel] divisores formae propositae [vel ex classe divisorum excludentur].

THEOREMA 9

19. *Si in formula generali pro divisoribus formae propositae, prouti supra exhibuimus, occurrant partes f et g sive positivae sive negativae, tum etiam ibidem earum productum fg occurret atque adeo in genere non solum earum potestates quaecunque f^μ et g^ν, sed etiam omnia producta ex binis $f^\mu g^\nu$, ratione signorum rite habita, postquam scilicet hi numeri, divisione per $4mn$ facta, infra limitem $2mn$ fuerint reducti.*

COROLLARIUM

20. Hinc patet, si p denotet numerum quemcunque ad $2mn$ primum, tum semper omnes numeros primos in forma $4mnz+pp$ contentos fore divisores formae propositae; contra vero omnes numeros in forma $4mnz-pp$ contentos ex classe divisorum excludi.

ANNOTATIO

21. Super formula generali, quam hic pro divisoribus formae propositae exhibemus, probe tenendum est non de omnibus numeris in ista formula contentis affirmari posse eos esse divisores; verum hoc tantum valere de numeris primis, quandoquidem occurrere possunt casus, quibus numeri compositi in hac formula contenti constant factoribus ex classe divisorum exclusis; contra vero omnes plane numeri in formula pro exclusis data sive sint primi sive compositi perpetuo excluduntur. Caeterum nunc multo certiorem methodum tradere licebit formulas pro divisoribus omnium formularum propositarum facile condendi, id quod in sequenti problemate ostendemus.

PROBLEMA

Proposita numerorum forma quacunque $mxx + nyy$ investigare formulam generalem, quae omnium numerorum in ea contentorum divisores complectatur.

SOLUTIO

22. Hic ante omnia tenendum est pro litteris x et y perpetuo numeros inter se primos accipi debere, quia alioquin omnes plane numeri divisores existere possent. Deinde etiam statim patet semper inter divisores ipsos numeros m et n eorumque factores occurrere posse, unde nostrum problema tantum ad divisores, qui ad numeros m et n sint primi, restringitur, atque ut etiam binarius excludatur, quaeri oportebit divisores, qui sint primi ad $2mn$.

23. Supra autem praecepimus formulae principali $4mnN$ adiungere omnes numeros ad $2mn$ primos atque minores quam mn, quippe quibus numeris constabat series superior, atque hic totum negotium eo erat reductum, ut cuilibet horum numerorum signum debitum praefigatur; hic quidem sponte patet primo horum numerorum, scilicet unitati, perpetuo signum $+$ esse tribuendum et, quia signa numerorum compositorum rationem multiplicationis sequuntur, hanc investigationem tantum ad numeros primos retulisse sufficiet.

24. Sit igitur p numerus quicunque primus, minor quam mn, simulque diversus ab m et n, atque huic numero signum $+$ erit praefigendum. Quando

dabitur numerus formae $mxx + nyy$ per p divisibilis, tum semper etiam dari poterit talis numerus $mn + yy$ pariter per p divisibilis, atque adeo, ut y sit minus quam $\frac{1}{2}p$. Hinc igitur cum sit $p < mn$[1]), nihil aliud requiritur, nisi ut litterae y ordine omnes valores ab 1 usque ad $\frac{1}{2}mn$ tribuantur, numerorumque resultantium omnes divisores primi minores quam mn et ab m et n diversi notentur, quandoquidem his signum $+$ erit praefigendum.

25. His igitur numeris signatis reliquis numeris primis usque ad mn alterum signum — dari oportebit, quo facto numeris compositis in eadem serie superiori occurrentibus sua debita signa ex ratione multiplicationis praefigantur.

26. Postquam autem hoc modo superior numerorum series fuerit expedita, pro serie inferiori, quae continet complementa superiorum numerorum ad $2mn$ vel eadem signa vel diversa sunt praefigenda; prius scilicet, quando numerus mn fuerit vel formae $4i + 1$ vel $4i + 2$, posterius vero, quando eius forma fuerit vel $4i$ vel $4i - 1$, hocque modo tota formula pro divisoribus erit completa.

EXEMPLUM 1

27. Sumatur $mn = 24$, qui cum sit numerus formae $4i$, inferiori seriei signa contraria sunt danda. Iam numeri ad $2mn$ primi, minoresque quam 24, sunt 1, 5, 7, 11, 13, 17, 19, 23, qui omnes sunt etiam primi, unde in formula $24 + yy$ ipsi y ordine tribuantur valores 1, 2, 3 etc. usque ad 12, sicque orietur progressio numerorum secundum numeros impares 1, 3, 5, 7 etc. crescentium, quorum singulorum notentur divisores primi minores quam 24, ternario excluso, quod commodissime sequenti modo fiet:

24		Divisores	60		Divisores
1	25	5	13	73	—
3	28	7	15	88	11
5	33	11	17	105	7
7	40	5	19	124	—
9	49	7	21	145	—
11	60	5	23	168	7

1) Editio princeps: $p > mn$. Correxit A. M.

Hinc igitur patet solos numeros primos 1, 5, 7, 11 signo + esse afficiendos, reliquos vero signo —; unde seriem complementorum subscribendo formula pro divisoribus erit:

$$96N + 1, + 5, + 7, + 11, -13, -17, -19, -23$$
$$-47, -43, -41, -37, + 35, + 31, + 29, + 25$$

EXEMPLUM 2

28. Sit $mn = 26$, qui numerus cum sit formae $4i + 2$, series inferior eadem habere debet signa quae superior. Iam formula $26 + yy$ tribuendo ipsi y valores 1, 2, 3, usque ad 13 nobis praebebit divisores primos minores quam 26, excluso 13, uti sequens calculus ostendit:

26		Divisores	
1	27	3	
3	30	3	5
5	35	5	7
7	42	3	7
9	51	3	17
11	62	—	
13	75	5	3
15	90	3	5
17	107	—	
19	126	3	7
21	147	3	7
23	170	5	17
25	195	3	5

Numeri primi, qui hic signum + recipiunt, sunt 1, 3, 5, 7, 17; reliquis vero 11, 19, 23 signum — est praefigendum; compositis autem numeris dentur signa ex ratione multiplicationis orta, unde formula pro divisoribus sequenti modo formabitur:

$$104N + 1, + 3, + 5, + 7, + 9, -11, + 15, + 17, -19, + 21, -23, + 25$$
$$+ 51, + 49, + 47, + 45, + 43, -41, + 37, + 35, -33, + 31, -29, + 27$$

EXEMPLUM 3

29. Sumatur $mn = 27$, et cum hic numerus sit formae $4i - 1$, complementa infra scribenda signis contrariis affici debebunt. Quodsi iam formulam $27 + yy$ evolvamus, divisores primi minores quam 27, ternario excluso, signo $+$ afficiendi reperientur 1, 7, 13, 19, unde reliqui primi signum $-$ sumendi erunt 5, 11, 17, 23; quamobrem formula generalis pro divisoribus erit:

$$108\,N + 1, - 5, + 7 - 11, + 13, - 17, + 19, - 23, + 25$$
$$- 53, + 49, - 47, + 43, - 41, + 37, - 35, + 31, - 29$$

EXEMPLUM 4

30. Sumatur $mn = 28$, et cum hic numerus sit formae $4i$, complementa infra scribenda signis contrariis affici debebunt. Quodsi nunc formulam $28 + yy$ evolvamus, divisores primi minores quam 28 septenario excluso signo $+$ afficiendi erunt 1, 11, 23, reliqui vero primi signo $-$ afficiendi erunt 3, 5, 13, 17, 19; quare formula generalis pro divisoribus erit:

$$112\,N + 1, - 3, - 5, + 9, + 11, - 13, + 15, - 17, - 19, + 23, + 25, - 27$$
$$- 55, + 53, + 51, - 47, - 45, + 43, - 41, + 39, + 37, - 33, - 31, + 29$$

EXEMPLUM 5

31. Sumatur $mn = 30$, et cum hic numerus sit formae $4i + 2$, numeri infra scribendi signis iisdem quibus superiores affici debebunt. Iam numeri ad $2mn$ primi minoresque quam 30 signo $+$ afficiendi sunt 1, 11, 13, 17, 23, 29, reliqui vero numeri primi signo $-$ affecti sunt 7, 19; quare formula generalis pro divisoribus erit:

$$120\,N + 1, - 7, + 11, + 13, + 17, - 19, + 23, + 29$$
$$+ 59, - 53, + 49, + 47, + 43, - 41, + 37, + 31$$

EXEMPLUM 6

32. Sumamus $mn = 50$, et cum hic numerus sit formae $4i + 2$, complementa infra scribenda signis iisdem affici debebunt. Iam formula $50 + yy$

praebet sequentes divisores primos minores quam 50 excepto 5, qui signo + sunt afficiendi 1, 3, 11, 17, 19, 41, 43; reliqui vero primi signo — afficiendi sunt 7, 13, 23, 29, 31, 37, 47, quare formula generalis pro divisoribus erit:

$$\begin{array}{l} 200\,N + 1, + 3, - 7, + 9, + 11, - 13, + 17, + 19, - 21, - 23 \\ \quad + 99, + 97, - 93, + 91, + 89, - 87, + 83, + 81, - 79, - 77 \\ \\ \quad + 27, - 29, - 31, + 33, - 37, - 39, + 41, + 43, - 47, + 49 \\ \quad + 73, - 71, - 69, + 67, - 63, - 61, + 59, + 57, - 53, + 51 \end{array}$$

EXEMPLUM 7

33. Sumamus denique $mn = 60$, et cum hic numerus sit formae $4i$, complementa infra scribenda signis contrariis affici debebunt. Quodsi iam formulam $60 + yy$ evolvamus, divisores primi minores quam 60 exceptis 3 et 5 signo + afficiendi reperientur 1, 17, 19, 23, 31, 47, 53; unde reliqui primi, signum — sumendi, erunt 7, 11, 13, 29, 37, 41, 43, 59; quare forma generalis pro divisoribus erit:

$$\begin{array}{l} 240\,N + 1, - 7, - 11, - 13, + 17, + 19, + 23, - 29, + 31 \\ \quad - 119, + 113, + 109, + 107, - 103, - 101, - 97, + 91, - 89 \\ \\ \quad - 37, - 41, - 43, + 47, + 49, + 53, - 59 \\ \quad + 83, + 79, + 77, - 73, - 71, - 67, + 61 \end{array}$$

ADDITAMENTUM[1])

ad dissertationem de divisoribus numerorum in forma
$mxx + nyy$ contentorum

Haud abs re erit singularem observationem hic subiungere circa postremas partes cuiusque formulae divisorum, quippe quas in genere assignare licet, si modo sex casus a se invicem distinguantur.

OBSERVATIO 1

Si fuerit $mn = 4i$, tum in formula pro divisoribus data in serie superiore ultimus terminus semper erit $-(4i - 1)$, eiusque complementum ad $8i$, ipsi

1) ENESTROEM affirmat hoc Additamentum exhibitum esse conventui die 1. junii 1778. R. F.

subscribendum, erit $+(4i+1)$, quandoquidem habere debet signum contrarium. Cum enim sit $mn = 4i$, erit $mn + 1 = 4i + 1$, qui numerus, quia est primus ad mn, certe habere debet signum $+$, ideoque eius complementum, supra scribendum, signum contrarium $-$.

OBSERVATIO 2

Si fuerit $mn = 4i + 2$, quo casu complementa iisdem gaudent signis, erit $mn + 1 = 4i + 3$, qui numerus cum sit primus ad mn, habere debet signum $+$, eius ergo complementum, supra scribendum, pariter signum habebit $+$.

OBSERVATIO 3

Si fuerit $mn = 8i + 1$, quo casu bina complementa aequalibus gaudent signis, in serie superiore ultimus terminus erit $8i - 1$, eiusque complementum $= 8i + 3$, quibus ambobus signum $-$ praefigi debet, sicque hoc casu termini ultimi erunt:

$$-(8i-1)$$
$$-(8i+3).$$

Quin etiam hoc casu terminos penultimos assignare licet. Cum enim sit $mn + 4 = 8i + 5$, huic numero signum $+$, ideoque etiam eius complemento $8i - 3$ idem signum praefigendum erit; unde patet his casibus, quibus $mn = 8i + 1$, binos ultimos terminos esse:

$$+(8i-3) \quad -(8i-1)$$
$$+(8i+5) \quad -(8i+3).$$

OBSERVATIO 4

Si fuerit $mn = 8i + 3$, ultimus terminus in superiori serie erit $8i + 1$, eiusque complementum contrario signo notandum $8i + 5$. Quia autem superior numerus quadratum esse potest[1]), is signum $+$ habere debet, ideoque

1) Id est, quia $-mn = -2-(8i+1)$ et -2 residuum est, quod ex divisione quadratorum per numerum $8i+1$ oriri debet. R. F.

complementum signum —; penultimi vero numeri erunt $8i - 1$, $8i + 7$, quorum inferior, quia est $mn + 4 = 8i + 7$, signum + recipit, ideoque superior contrarium —; unde pro casibus, quibus est $mn = 8i + 3$, bini ultimi erunt:

$$-(8i - 1) \quad +(8i + 1)$$
$$+(8i + 7) \quad -(8i + 5) .$$

OBSERVATIO 5

Si fuerit $mn = 8i + 5$, ultimae formae divisorum erunt $8i + 3$, $8i + 7$, atque paribus signis afficientur, quod deprehenditur esse +[1]); penultimi autem termini erunt $8i + 1$, $8i + 9$, quorum inferior, quia est $= mn + 4$, habebit signum +, ideoque etiam supra scriptus. Consequenter casibus, quibus est $mn = 8i + 5$, in formula divisorum bini ultimi termini erunt:

$$+(8i + 1) \quad +(8i + 3)$$
$$+(8i + 9) \quad +(8i + 7) .$$

OBSERVATIO 6

Si fuerit $mn = 8i + 7$, in formula divisorum ultimi termini sunt $8i + 5$ et $8i + 9$, quorum inferior certe signum + habere debet, quia quadrata complecti potest[2]), superior vero signum —; penultimi vero termini sunt $8i + 3$ et $8i + 11$, quorum inferior, utpote $= mn + 4$, certe habet signum +, ideoque superior signum —. Quamobrem casibus, quibus est $mn = 8i + 7$, in formula pro divisoribus inventa bini ultimi termini erunt:

$$-(8i + 3) \quad -(8i + 5)$$
$$+(8i + 11) \quad +(8i + 9) .$$

---

1) Quia $-mn = -2 - (8i + 3)$. R. F.

2) Id est, quia $-mn = 2 - (8i + 9)$. R. F.