LEONHARDI EULERI OPERA OMNIA
SUB AUSPICIIS SOCIETATIS SCIENTIARUM NATURALIUM HELVETICAE
EDENDA CURAVERUNT
ANDREAS SPEISER · LOUIS GUSTAVE DU PASQUIER · HEINRICH BRANDT
ERNST TROST

SERIES PRIMA · OPERA MATHEMATICA · VOLUMEN QUINTUM

LEONHARDI EULERI

COMMENTATIONES ARITHMETICAE

VOLUMEN QUARTUM

EDIDIT

RUDOLF FUETER

AUCTORITATE ET IMPENSIS
SOCIETATIS SCIENTIARUM NATURALIUM HELVETICAE

GENEVAE MCMXLIV

VENDITIONI EXPONUNT
ORELL FÜSSLI TURICI ET LIPSIAE
B. G. TEUBNER LIPSIAE ET BEROLINI

LEONHARDI EULERI

OPERA OMNIA

LEONHARDI EULERI
OPERA OMNIA

SUB AUSPICIIS
SOCIETATIS SCIENTIARUM NATURALIUM
HELVETICAE

EDENDA CURAVERUNT

ANDREAS SPEISER
LOUIS GUSTAVE DU PASQUIER
HEINRICH BRANDT
ERNST TROST

SERIES PRIMA
OPERA MATHEMATICA
VOLUMEN QUINTUM

AUCTORITATE ET IMPENSIS
SOCIETATIS SCIENTIARUM NATURALIUM HELVETICAE

GENEVAE MCMXLIV

VENDITIONI EXPONUNT
ORELL FÜSSLI TURICI ET LIPSIAE
B. G. TEUBNER LIPSIAE ET BEROLINI

LEONHARDI EULERI

COMMENTATIONES ARITHMETICAE

VOLUMEN QUARTUM

EDIDIT

RUDOLF FUETER

AUCTORITATE ET IMPENSIS
SOCIETATIS SCIENTIARUM NATURALIUM HELVETICAE

GENEVAE MCMXLIV

VENDITIONI EXPONUNT
ORELL FÜSSLI TURICI ET LIPSIAE
B. G. TEUBNER LIPSIAE ET BEROLINI

TYPIS EXCUSSIT ORELL FÜSSLI TURICI

VORWORT DER REDAKTION

Unter den nachgelassenen Papieren EULERS befinden sich neun Notizbücher sowie drei Bände sogenannter *adversaria mathematica*. Die letzteren sind von Schülern EULERS geschrieben in den Jahren 1766—1783, also während des zweiten Petersburger Aufenthaltes bis zu seinem Tod. Als PAUL HEINRICH und NICOLAUS FUSS 1844 die *opera postuma* herausgaben, veröffentlichten sie im ersten Band eine Auswahl arithmetischer Sätze aus diesen *adversaria* unter dem Titel: *Fragmenta arithmetica ex Adversariis mathematicis depromta* (Nr. 806 von ENESTROEMS Verzeichnis). Diesen fügte Tschebyscheff weitere hinzu, welche im zweiten Band unter dem Titel *Continuatio fragmentorum ex Adversariis mathematicis depromtorum* (Nr. 819 des ENESTROEMSCHEN Verzeichnisses) veröffentlicht wurden, ferner wurde diesen noch ein Fragment (Nr. 856) beigegeben. Insgesamt nehmen diese Fragmente 145 Seiten der großformatigen enggedruckten *opera postuma* ein. Es handelt sich fast durchwegs um Theoreme, die schon anderweitig publiziert sind, so daß das Interesse dieser *Adversarii* fast ausschließlich biographisch ist. Bei dem großen Umfang schien es uns nicht möglich, diese Nummern des Verzeichnisses von ENESTROEM mit in die Bände der arithmetischen Abhandlungen aufzunehmen. Wir behalten uns vor, die obengenannten Notizbücher und die drei Bände der *Adversaria mathematica* am Schluß der ganzen Ausgabe der EULERwerke in Bänden, welche Materialien zur Biographie EULERS enthalten, vollständig abzudrucken, denn die Auswahl, welche von den beiden FUSS getroffen wurde, kann für unsere Ausgabe nicht maßgebend sein. Auch sind solche Auswahlen erfahrungsgemäß von geringem Wert, denn es zeigt sich meist, daß gerade das, was weggelassen wurde, von den späteren Bearbeitern als das wichtigste angesehen wird. Eine unseres Wissens sonst nicht publizierte Formel für die Komposition zweier quadratischer Formen ist in der Übersicht zur Algebra (S. XL dieses Bandes) wiedergegeben. Wir glauben diese Abweichung vom Redaktionsplan damit gerechtfertigt zu haben. Doch soll dadurch nichts präjudiziert werden, daß nicht auch in Zukunft wie in mehreren schon erschienenen Bänden, kleinere Fragmente aufgenommen werden. Bisher handelte es sich stets um Abhandlungen von wenigen Seiten.

Zürich, Januar 1944.

ANDREAS SPEISER.

VORWORT DES HERAUSGEBERS

Der vorliegende letzte Band der *Commentationes arithmeticae* zerfällt in zwei fast gleich große Teile. Der *erste* betrifft Abhandlungen, die EULER selbst der Akademie vorgelegt hat und die von letzterer nach EULERS Tode in ihren Mémoiren zwischen 1812 und 1830 veröffentlicht worden sind. Sie betreffen nur Arbeiten aus dem Gebiete der diophantischen Gleichungen. Der *zweite* Teil dagegen bringt Abhandlungen aus dem Nachlaß EULERS, oder solche, die von Schülern niedergeschrieben worden sind. Sie sind fast alle zum ersten Male im Jahre 1849 in den *Commentationes arithmeticae collectae* von P. H. FUSS und NICOLAUS FUSS abgedruckt worden. Unter ihnen finden sich nicht vollendete Abhandlungen aus verschiedenen Epochen von EULERS Leben. Die sämtlichen Manuskripte dieses zweiten Teiles sind uns im Jahre 1910 von der Petersburger Akademie der Wissenschaften in liberaler und großzügiger Weise zur Verfügung gestellt worden. Bestimmte Teile der Manuskripte werden hier zum ersten Male publiziert.

I. Teil:

DIOPHANTISCHE GLEICHUNGEN

Alle Abhandlungen dieses Teiles stammen aus dem Jahre 1780. Beginnen wir mit der Abhandlung 748: „*Investigatio quadrilateri, in quo singulorum angulorum sinus datam inter se teneant rationem, ubi artificia prorsus singularia in analysi diophantea occurrunt*", in der das Problem gelöst wird, Vierecke anzugeben mit Winkeln, deren Sinusse in rationalem Verhältnis stehen. Sind α, β, γ, δ die vier Winkel des Viereckes, und setzt man:

$$\begin{aligned} &\sin\alpha = pt, \quad \sin\beta = qt, \quad \sin\gamma = rt, \quad \sin\delta = st, \\ &\cos\alpha = \pi\tau, \quad \cos\beta = \kappa\tau, \quad \cos\gamma = \varrho\tau, \quad \cos\delta = \sigma\tau, \end{aligned}$$

so sind nach Annahme p, q, r, s positive ganze rationale Zahlen. Zunächst findet EULER das überraschende Resultat, daß auch π, κ, ϱ, σ ganze rationale Zahlen sein müssen. Ferner sind t,τ eindeutig bestimmt; es ist

$$t^2 = \frac{v}{z}, \quad \tau^2 = \frac{1}{z},$$

wo $v = (p+q+r+s)\ (p+q-r-s)\ (p+r-q-s)\ (q+r-p-s)$,
$z = 4\,(pq-rs)\ (pr-qs)\ (qr-ps)$

wird. Damit t,τ reell werden, muß einzig etwa $p > q \geqq r > s$, und $q+r > p+s$ vorausgesetzt werden. z und v sind so beschaffen, daß alle vier Ausdrücke $z - p^2v$, $z - q^2v$, $z - r^2v$, $z - s^2v$ zugleich Quadrate werden.

Hieran schließt EULER die weitere Frage: kann man die natürlichen Zahlen p, q, r, s so bestimmen, daß die Cosinusse der Winkel selbst, d. h. τ rational wird? Es muß dann:

$$pq - rs = x^2,\ pr - qs = y^2,\ qr - rs = u^2$$

werden. Nimmt man

$$x = \frac{p+s+v}{2}\ ,\quad y = \frac{p+s-v}{2}\ ,$$

so folgt aus den beiden ersten Gleichungen:

$$q = \frac{(p+s)^2 + 2(p-s)\ v + v^2}{4(p-s)}\ ,\quad r = \frac{(p+s)^2 - 2(p-s)\ v + v^2}{4(p-s)}\ ;$$

setzt man diese Werte in der dritten Gleichung ein, so wird dieselbe von selbst zu einem Quadrat, dessen Basis u sich aus $4(p-s)u = p^2 - 6ps + s^2 - v^2$ ergibt. Solche „Zufälligkeiten" verdankt EULER seiner Divinationsgabe! Allerdings ist damit die allgemeine Lösung des Problemes noch nicht gefunden, da der Ansatz speziell ist; das allgemeine Problem harrt noch seiner Lösung. Außerdem tritt die Frage der Abschätzung hinzu, da p, q, r, s positiv sein müssen.

Die Abhandlung 753: „*Solutio succincta et elegans problematis, quo quaeruntur tres numeri tales, ut tam summae quam differentiae binorum sint quadrata*" verwendet das von EULER stetsfort benutzte Prinzip: Ist $x \pm y$ ein Quadrat für beide Vorzeichen, so muß eine Darstellung existieren:

$$x = p^2 + q^2,\ y = 2pq\ .$$

Da wir hier drei Zahlen x, y, z haben, für die die Beziehung zwischen je zweien stattfindet, muß man x auf zwei verschiedene Arten in Quadrate zerlegen. Dann ist x, y, z so bestimmt, daß $x \pm y$, $x \pm z$ Quadrate sind, und es bleibt nur noch die Bedingung zu erfüllen, daß auch $y \pm z$, d. h. $y^2 - z^2$ ein Quadrat wird. Die (nicht allgemeine) Lösung mit zwei unbestimmten Parametern p, q lautet:

$$x = P^2 + Q^2 = R^2 + S^2,\ y = 2PQ,\ z = 2RS\ ,$$

wo

$$P = 8p^2q^2(p^4 + 9q^4),\ Q = -p^8 + 2p^4q^4 - 81q^8,\ R = p^8 + 30p^4q^4 + 81q^8,\ S = 16p^4q^4\ .$$

Daß es unendlich viele Lösungen gibt, erkennt EULER auch aus dem Umstande, daß

$$X = \tfrac{1}{2}(y^2 + z^2 - x^2)\ , \quad Y = \tfrac{1}{2}(x^2 + z^2 - y^2)\ , \quad Z = \tfrac{1}{2}(x^2 + y^2 - z^2)$$

eine Lösung ist, falls x, y, z eine solche ist[1]).

Die Abhandlung 754: „*Problème de géométrie résolu par l'analyse de Diophante*" greift auf ein altes, von EULER oft behandeltes Problem zurück: Ein Dreieck mit rationalen Seiten sei gesucht, dessen Schwerpunktlinien wieder rationale Längen besitzen. Siehe zu den frühern Arbeiten über dieses Thema die Ausführungen im Vorwort zu Band I, 4[2]). Die vorliegende Abhandlung gibt eine überraschend einfache Lösung, und ist die vollkommenste, trotzdem sie keine neuen Zahlenbeispiele bringt. Sie beruht auf dem merkwürdigen *Lemma: Sind* $x^2 + 2Pxy + y^2$, $x^2 + 2Qxy + y^2$ *zwei gegebene quadratische Formen, so werden beide zu Quadraten im Bereiche der* P, Q *durch:*

$$x = 4(P + Q),\quad y = (P - Q)^2 - 4\ .$$

Besteht zwischen P *und* Q *die Relation* $PQ + 1 = n(P + Q)$, *so darf sogar* $x = 4$, $y = P + Q - 4n$ *genommen werden.*

Die Anwendung des Lemmas auf unser Problem findet so statt. Sind:

$$\begin{aligned} u^2 &= 2y^2 + 2z^2 - x^2\ , \\ v^2 &= 2z^2 + 2x^2 - y^2\ , \\ w^2 &= 2x^2 + 2y^2 - z^2\ , \end{aligned}$$

die drei rational zu lösenden diophantischen Gleichungen, so setze man:

$$\begin{aligned} y + z &= p(r + s)\ , & w + v &= 3p(r - s)\ , \\ y - z &= q(r - s)\ , & w - v &= q(r + s)\ . \end{aligned}$$

Dann reduzieren sich die drei Gleichungen auf die beiden:

$$\left(\frac{x}{p}\right)^2 = r^2 + 2Prs + s^2\ ,\quad \left(\frac{u}{q}\right)^2 = r^2 + 2Qrs + s^2\ ,$$

wo

$$P = \frac{q^2 - 5p^2}{4p^2}\ ,\quad Q = \frac{9p^2 - 5q^2}{4q^2}$$

1) Siehe auch die Besprechung der Abhandlung bei TH. L. HEATH: *Diophantus of Alexandria*, Cambridge, 1910, p. 336ff.

2) *LEONHARDI EULERI Opera omnia*, series I, vol. 4, Genevae 1941, p. XXff.

ist. Außerdem ist $PQ + 1 = -\frac{5}{4}(P + Q)$. Daher ergibt das Lemma die Lösung:

$$n = -\frac{4}{5}\,, \quad r = 4\,, \quad s = \frac{(9p^2 + q^2)\,(p^2 + q^2)}{4p^2q^2}\,.$$

Setzt man schließlich:

$$p' = 16p^2q^2\,,\ q' = (9p^2 + q^2)\,(p^2 + q^2)\,,\ r' = 2(9p^4 - q^4)\,,$$

so lauten die überaus einfachen Schlußformeln der Lösungen:

$$\begin{aligned} x = p(q' - r'),\ y + z = p(p' + q')\,, \quad & u = q(q' + r'),\ w + v = 3p(p' - q')\,, \\ y - z = q(p' - q')\,, \quad & w - v = q(p' + q')\,. \end{aligned}$$

Das einfachste Zahlenbeispiel ist $x = 68$, $y = 87$, $z = 85$.

Die Abhandlung 755: „*De casibus, quibus formulam* $x^4 + mxxyy + y^4$ *ad quadratum reducere licet*“ geht ebenfalls auf ein früher behandeltes Problem zurück. Wie in der Vorrede zu Band I, 4 p. XXIV/V bemerkt wurde, ist die Frage der „Lösung“ im EULERschen Sinne zuerst festzusetzen. Im ersten Paragraphen der vorliegenden Arbeit verlangt EULER ausdrücklich, daß er nur solche m berechnen wolle, für die es unendlich viele x, y gebe, die $x^4 + mx^2y^2 + y^4$ zu einem Quadrate machen. Dazu will er offenbar verschiedene Formeln herleiten, die nur solche Zahlen m darstellen, für die wenigstens *eine* Lösung existiert. Die gefundenen Formeln haben die Gestalt $nq^2 + r$ oder $nq^2 + rq + s$, $q = 0, \pm 1, \pm 2, \ldots$ Da ein m durch verschiedene dieser Formeln dargestellt werden kann, gibt es auch verschiedene Lösungen x, y für ein m. Diese allgemeinen Formeln ergeben also erst eine „Lösung“.

Zur Durchführung geht EULER so vor. Man nehme zwei beliebige natürliche Zahlen n, p, und setze $n^2 - 4p^4 = ly^2$, wo l quadratfrei, also eindeutig bestimmt ist. Dann soll

$$p^2m = lq^2 \pm n$$

werden, wo auch q beliebig ist, und nur der Bedingung unterliegt, daß m ganz wird. Im Falle $p = 1$, den EULER vor allem behandelt, ist diese letzte Bedingung hinfällig. Setzt man jetzt $x = 2pq$, so wird, wie eine elementare Rechnung sofort zeigt, $x^4 + mx^2y^2 + y^4$ das Quadrat von $z = 2nq^2 \pm y^2$. Im Falle $p = 1$ erhält EULER so eine erste Tabelle von unendlich vielen $m = lq^2 \pm n$.

Hält man l fest, so wird man für $p = 1$ auf die Pell'sche Gleichung $n^2 - ly^2 = 4$, oder allgemeiner, da n, y auch gebrochene Zahlen sein dürfen, so lange m ganz bleibt, auf die Gleichung

$$n^2 - ly^2 = 4k^{4\nu},\ \nu = 0, 1, 2, 3, \ldots,$$

geführt, deren Lösungen die Potenzen der Grundlösung für $v = 1$ sind. m und x ergeben sich dann aus

$$k^{2v}m = lq^2 \pm n,\ x = 2qk^v,\ v = 0, 1, 2, 3, \ldots,$$

wo q der Bedingung unterliegt, daß m ganz werden muß. Für die verschiedenen Werte von k erhält EULER neue Tabellen, die er speziell zur Berechnung negativer m auswertet.

Weitgehend verwandt mit der besprochenen Fragestellung ist die Abhandlung 758: „*De binis formulis speciei* $xx + myy$ *et* $xx + nyy$ *inter se concordibus et discordibus.*" Die beiden Formen (resp. m und n) heißen konkordant, wenn es ein Wertepaar x, y gibt, das beide Formen zugleich zu einem Quadrat macht; sonst nennt sie EULER diskordant. Setzt man $m = \nu\mu$, so wird die Form $x^2 + my^2$ für $x = \mu p^2 - \nu q^2$, $y = 2pq$ das Quadrat von $\mu p^2 + \nu q^2$. Alle Formen $x^2 + ny^2$ sind somit zu $x^2 + my^2$ konkordant, wenn man p, q so bestimmen kann, daß

$$(\mu p^2 - \nu q^2)^2 + 4np^2q^2$$

ein Quadrat wird. Dies ist aber eine biquadratische Form in p, q von derselben Bauart, wie diejenige der vorigen Abhandlung. EULER löst dieses Problem folgendermaßen: Er nimmt zwei beliebige teilerfremde Zahlen r, s, und bestimmt ϱ, σ, p, q als ganze rationale Zahlen so, daß die Bedingungen erfüllt sind:

$$pq = rs,\ \sigma r^2 - \varrho s^2 = \pm 1,$$

worauf m konkordant wird mit allen:

$$n = \left(hs^2 \pm \sigma(\mu p^2 - \nu q^2)\right)\left(hr^2 \pm \varrho(\mu p^2 - \nu q^2)\right),\ h = 0, 1, 2, 3, \ldots\ (m = \mu\nu)$$

Die beiden gegebenen Formen werden Quadrate für $x = \mu p^2 - \nu q^2$ und $y = 2pq = 2rs$. Als interessante Anwendung beweist EULER, daß $x^2 + y^2$ konkordant ist mit $x^2 + 7y^2$, dagegen diskordant mit $x^2 + 3y^2$ und $x^2 + 4y^2$. Letzterer Beweis erfolgt in geistreicher Weise mit Hilfe einer Fermatschen „Descente infinie".[1]) Bei dieser Gelegenheit sei übrigens darauf aufmerksam gemacht, daß EULER bei der Lösung von $x^2 + my^2 = z^2$ stets nur den Ansatz $y = 2pq$, $x = \mu p^2 - \nu q^2$, nicht aber $y = pq$, $2x = \mu p^2 - \nu q^2$ berücksichtigt.

In der kleinen Abhandlung 775: „*De binis numeris, quorum summa sive aucta sive minuta tam unius quam alterius quadrato producat quadrata*" werden die gesuchten Zahlen mit x/z, y/z bezeichnet. Es müssen dann die quadratischen Formen:

$$(x + y)z \pm x^2,\ (x + y)z \pm y^2$$

für beide Vorzeichen zugleich Quadrate werden. EULER berechnet einzig ein Zahlenbeispiel.

1) Siehe hierzu „Vollständige Anleitung zur Algebra", *LEONHARDI EULERI Opera omnia*, vol. 1, series I, § 229 ff., p. 461.

Die Abhandlung 776: „*Dilucidationes circa binas summas duorum biquadratorum inter se aequales*“ greift auf ein altes Problem zurück, das EULER schon zweimal behandelt hat[1]): Kann die Summe von zwei Biquadraten der Summe zweier andern Biquadraten gleich werden? Die vorliegende Arbeit ist in zwiefacher Hinsicht bemerkenswert. Einmal wird darin die Vermutung ausgesprochen, daß das in Abhandlung 428 angegebene Zahlenbeispiel falsch sei, was es in der Tat ist[2]). Anderseits ist auffallend, daß sie keine Erwähnung der Abhandlung 716 enthält, in der viel kleinere Zahlen als Lösungen des Problemes berechnet wurden. Jene Abhandlung 716 war 1778, also drei Jahre *vor* der Abhandlung 776 der Akademie eingereicht worden. Man muß daher annehmen, daß die vorliegende Arbeit aus einem frühern Zeitpunkt herstammt, aber erst 1780 verspätet der Akademie eingereicht wurde. Sie enthält zwei verschiedene Methoden zur Lösung, von denen die zweite die einfachste ist. Schreibt man die zu lösende diophantische Gleichung in der Form

$$x^4 - y^4 = z^4 - u^4,$$

so setze man:

$$x = p(r + s),\ y = p(r - s),\ z = q(m + n),\ u = q(m - n);$$

nimmt man an, daß $r^2 + s^2 = m^2 + n^2$ ist, so lautet die Bedingungsgleichung sehr einfach so:

$$\frac{q^4}{p^4} = \frac{rs}{mn}.$$

Macht man hier die Substitution:

$$r = 2(t^2 - 1),\ s = t(t^2 - 3),\ m = 2,\ n = t(t^2 - 1),$$

so ist die Bedingung $r^2 + s^2 = m^2 + n^2$ identisch in allen t erfüllt, und es wird:

$$\frac{q^4}{p^4} = t^2 - 3.$$

Man hat somit nur noch t als rationale Zahl so zu bestimmen, daß $t^2 - 3$ ein Biquadrat wird. Für

$$t = \frac{l^2 + 3k^2}{2lk}$$

wird $t^2 - 3$ ein Quadrat, und für $l = 2$, $k = 1$ das gewünschte Biquadrat, woraus eine Lösung für p, q, r, s, m, n und damit auch für x, y, z, u erhalten wird. Eigentlich wird EULER auf die interessante diophantische Gleichung:

$$v^4 + 3 = t^2$$

geführt, die er in der Abhandlung 778 behandelt hat[3]).

1) Siehe die Vorrede zu Band I, 4, p. XXII/III. Ferner HEATH a. a. O. problem 17, p. 377.
2) Siehe Band I, 3, p. XXIII dieser Werke.
3) Siehe p. 179 dieses Bandes.

Die weiteren Abhandlungen dieses Teiles kann man in zwei Gruppen einteilen. Die erste löst Aufgaben, eine oder mehrere Formen zu Quadraten zu machen. Die andere bezieht sich auf die Lösung einer Fermatschen Aufgabe. Alle diese Abhandlungen werden beherrscht von einer *neuen Methode*, die EULER zuerst in der Abhandlung 764 entwickelt hat. Er hat sie dann auf viele seiner frühern Probleme angewandt und ihre Ergiebigkeit festgestellt. Dies hat ihn veranlaßt, ihr schließlich die besondern Abhandlungen 772, 777 und 778 zu widmen, mit denen wir daher unsere Analyse beginnen wollen.

In der Abhandlung 772, der ersten der genannten drei: „*De insigni promotione Analysis Diophantaeae*" wird die neue Methode an der Aufgabe entwickelt, eine spezielle biquadratische Form:

$$a^2x^4 + 2abx^3y + cx^2y^2 + 2bdxy^3 + d^2y^4$$

im Bereiche der rationalen Zahlen zu einem Quadrate zu machen. Setzt man $c - b^2 - 2ad = mn$, so kann letztere so geschrieben werden:

$$(ax^2 + bxy + dy^2)^2 + mnx^2y^2;$$

in dieser Gestalt wird sie durch die Substitution:

$$ax^2 + bxy + dy^2 = l(mp^2 - nq^2), \quad xy = 2lpq,$$

wo l, p, q beliebige rationale Zahlen sind, in das Quadrat von $mp^2 + nq^2$ übergeführt. Es bleibt daher nur zu untersuchen, ob der Ansatz der Substitution möglich ist. Man darf ohne Spezialisierung $y = 1$, d. h. für x/y wieder x nehmen. Die Elimination von x aus den beiden Ansätzen ergibt dann:

$$4l^2ap^2q^2 + 2lbpq + d = lmp^2 - lnq^2,$$

also eine sowohl in p als in q quadratische Gleichung. Falls man verfügt: $l = -nd$, so erhält man für die Gleichung sofort die *Ausgangslösung* $p = 0, q = 1/n$. Die neue Methode besteht jetzt darin, daß man aus dieser Ausgangslösung unendlich viele neue Lösungspaare berechnet. In der Tat, setzt man in der quadratischen Gleichung für q seinen Wert $1/n$ der Ausgangslösung ein, so ergibt sich für p als Variable neben $p=0$ noch eine zweite rationale Lösung p'. Setzt man diese für p ein, so erhält man für q als Variable neben der Ausgangslösung von q noch eine zweite rationale Lösung q'. Jetzt setzt man q' ein, und erhält wieder zwei Wurzeln für p, p' und p'', usf. Das Verfahren bricht ab, wenn eine Wurzel unendlich wird. Dies ist die neue Methode!

In der Abhandlung 777: „*De resolutione huius aequationis* $0 = a + bx + cy + dxx + exy + fyy + gxxy + hxyy + ixxyy$ *per numeros rationales*" wird die Quintessenz der

neuen Methode ohne Verbindung mit einer speziellen Aufgabe entwickelt. In der Tat ist sie anwendbar auf die allgemeinste Gleichung zwischen x, y mit rationalen Koeffizienten, in der jede der beiden Variablen für sich genommen nur quadratisch auftritt. Allerdings muß EULER die Existenz einer Ausgangslösung postulieren. Darin liegt natürlich der schwache Punkt der Methode. Da aber EULER eine, ja in den meisten Fällen sogar mehrere Ausgangslösungen bei allen seinen Anwendungen findet, macht ihm diese Annahme keine Sorge. Aus jeder Ausgangslösung findet er sukzessive, wie oben angegeben wurde, die im allgemeinen unendlich vielen neuen rationalen Lösungspaare.

Die Abhandlung 778: „*Methodus nova et facilis formulas cubicas et biquadraticas ad quadratum reducendi*" dehnt die Aufgabe der Abhandlung 772 auf eine viel größere Klasse von biquadratischen, resp. kubischen Polynomen einer Variablen x aus, nämlich auf alle diejenigen, die sich in der Gestalt:

$$P^2 + QR$$

darstellen lassen, wo P, Q, R höchstens Polynome vom zweiten Grade in x mit rationalen Koeffizienten sind. EULER beweist, daß diese Darstellung für das allgemeinste Polynom vierten Grades möglich ist, falls man ein rationales $x = m$ kennt, für das dasselbe ein Quadrat wird. Um nun $P^2 + QR$ zu einem Quadrat zu machen, setzt man:

$$P^2 + QR = (P + Qy)^2 \ , \quad \text{oder} \quad 2Py + Qy^2 = R \ .$$

Dies ist aber gerade eine der in Abhandlung 777 behandelten Gleichungen. Zudem kennt man eine Ausgangslösung (wegen $x = m$), so daß die neue Methode zum Ziele führt. EULER wendet das Verfahren auf die merkwürdigen Gleichungen $3x^3 + 1$, $3x^4 + 1$, u. a. m. an.

Alle weiteren Abhandlungen des ersten Teiles sind Anwendungen dieser Methode. Zunächst seien diejenigen angeführt, die bestimmte Formen zu Quadraten machen wollen. In der Abhandlung 764: „*Resolutio facilis quaestionis difficillimae, qua haec formula maxime generalis* $vvzz(axx + byy)^2 + \Delta xxyy(avv + bzz)^2$ *ad quadratum reduci postulatur*" geht EULER so vor, daß er zuerst $av^2 + bz^2$ durch den Ansatz:

$$\sqrt{a}\ v + \sqrt{-b}\ z = (f + g\sqrt{-ab})\ (\sqrt{a}\,x + \sqrt{-b}\ y)$$

als Vielfaches von $ax^2 + by^2$ bestimmt, wo f, g beliebige rationale Zahlen sind. Dadurch werden v, z lineare Funktionen der x, y. Jetzt kann man durch $(ax^2 + by^2)^2$ kürzen, und es bleibt nur die Aufgabe, den Ausdruck

$$(fx - bgy)^2\,(fy + agx)^2 + \Delta x^2y^2\,(f^2 + abg^2)^2$$

zu einem Quadrate zu machen. Setzt man $y = 1$ und zerlegt Δ in $-4mn$, so wird dies durch den Ansatz

$$x = lpq,\ (fx - bg)\ (f + agx) = l(f^2 + abg^2)\ (mp^2 + nq^2)$$

erreicht, wo wieder über l beliebig verfügt werden kann. Durch Elimination von x ergibt sich eine Gleichung, die sowohl in p wie in q quadratisch ist, also die Gestalt hat, die die neue Methode verlangt. Die Ausgangslösung erhält man für

$$l = -\frac{nbgf}{(f^2 + abg^2)}$$

in dem Wertepaare $p = 0, q = 1/n$.

Die Abhandlung 773: „*Solutio problematis difficillimi, quo hae duae formulae* $aaxx + bbyy$ *et* $aayy + bbxx$ *quadrata reddi debent*" löst das im Titel genannte Problem in folgender Weise. Der erste Ausdruck wird ein Quadrat für:

$$\frac{ax}{by} = \frac{p^2 - q^2}{2pq},$$

der zweite für:

$$\frac{ay}{bx} = \frac{r^2 - s^2}{2rs},$$

also muß

$$\frac{rs\,(p^2 - q^2)}{pq\,(r^2 - s^2)} \quad \text{oder} \quad \frac{pq\,(p^2 - q^2)}{rs\,(r^2 - s^2)}$$

ein Quadrat werden. Ist umgekehrt dieser Ausdruck ein Quadrat, etwa $= t^2$, so sind

$$\frac{x}{y} = \frac{rs}{pq}\,t^2, \quad \frac{a}{b} = \frac{p^2 - q^2}{2rst}$$

Lösungen. Man sieht daraus, daß *vier* Variable vorliegen: x, y, a, b. Es bleibt noch übrig, die diophantische Gleichung

$$\frac{pq\,(p^2 - q^2)}{rs\,(r^2 - s^2)} = t^2$$

zu lösen. Dazu setzt Euler $s = q$, $p = rv$, so daß die neue Bedingung entsteht:

$$\left(\frac{q}{r}\right)^2 = \frac{v^3 - t^2}{v - t^2}.$$

Die rechte Seite muß somit zu einem Quadrate gemacht werden. Nimmt man:

$$\frac{v^3 - t^2}{v - t^2} = (v - z)^2,$$

so entsteht wieder zwischen v und z eine Gleichung, auf die man die neue Methode anwenden kann. Euler gibt fünf Ausgangslösungen an, die er alle entwickelt. Dabei ist t

noch ganz unbestimmt. Dies führt ihn zu der allgemeinern Aufgabe, vier Zahlen x, y, z, u so zu bestimmen, daß alle drei Ausdrücke:

$$x^2y^2 + z^2u^2, \quad x^2z^2 + y^2u^2, \quad x^2u^2 + y^2z^2$$

Quadrate werden. Diese Aufgabe kann direkt gelöst werden. Sind nämlich p, q, r beliebige Zahlen, zwischen denen die Beziehung

$$p^2 + 3q^2 = r^2$$

besteht, so ist:

$$x = 2q, \quad y = 2r, \quad z = p + q, \quad u = p - q$$

eine Lösung. Die Basen der drei Quadrate sind $p^2 + 7q^2$, $2(p^2 - pq + 2q^2)$, $2(p^2 + pq + 2q^2)$.

Eine ähnliche Aufgabe bringt die Abhandlung 774: „*Investigatio binorum numerorum formae* $xy(x^4 - y^4)$, *quorum productum sive quotus sit quadratum*“, auf die die EULER schon früher beschäftigende Frage nach zwei Zahlen führt, deren Produkt vermehrt oder vermindert um die Summe oder Differenz derselben ein Quadrat gibt[1]). In der Lösung der Aufgabe:

$$\frac{xy(x^4 - y^4)}{zt(z^4 - t^4)}$$

zu einem Quadrate zu machen, läßt uns EULER besonders tief in seine Forschungsmethode hineinblicken, weshalb sie hier kurz charakterisiert werden möge. Er geht von der ihm bekannten Lösung $x = 12$, $y = 1$, $z = 16$, $t = 11$ aus, in der $x^2 + y^2$ und $z^2 + t^2$ einen gemeinsamen Teiler besitzen. Daher verlangt er auch im allgemeinen Fall, daß

$$x^2 + y^2 = (p^2 + q^2)(u^2 + v^2), \quad z^2 + t^2 = (r^2 + s^2)(u^2 + v^2)$$

wird, woraus sich x, y, z, t durch p, q, r, s, u, v linear ausdrücken lassen. Außerdem ist in dem Zahlenbeispiel $x - y = t$, und $x + y = r^2 + s^2$. Also werden diese beiden Beziehungen auch im allgemeinen Falle vorausgesetzt, woraus

$$(p + q + \tfrac{1}{2}r)^2 + (q - p + \tfrac{1}{2}s)^2 = \tfrac{5}{4}(r^2 + s^2)$$

folgt; diese Relation erlaubt r und s linear durch p, q so darzustellen, daß die Darstellungen auch im Falle des Zahlenbeispiels erfüllt sind. Daraus folgt schließlich:

$$\frac{xy(x^4 - y^4)}{zt(z^4 - t^4)} = \frac{p^2 + q^2}{4(p + 7q)(p + 3q)}.$$

1) Siehe diese Werke, Band I, 3, p. XX und p. 148.

Also muß $(p^2 + q^2)\,(p + 7q)\,(p + 3q)$ ein Quadrat werden. Setzt man $p/q = \tau$, so ist ein Polynom 4. Grades in τ zu einem Quadrate zu machen, also gerade eine Aufgabe zu lösen, für die die neue Methode geschaffen wurde. Es können leicht 6 verschiedene Ausgangslösungen gefunden werden. p ist der Zähler, q der Nenner von τ, womit aus den unendlich vielen τ die zugehörigen x, y, z, t leicht berechnet werden.

Es wäre eine lohnende Aufgabe, die neue Methode streng zu verfolgen, insbesondere die notwendigen und hinreichenden Bedingungen anzugeben sowohl für die Existenz der Ausgangslösung als auch für das Nichtabbrechen der Reihe der aus der Ausgangslösung erhaltenen Zahlenpaare. Zu beachten ist, daß neben den von EULER angegebenen zwei Fällen, nämlich daß entweder unendlich viele rationale Lösungspaare gefunden werden, oder nach endlich vielen Schritten eine Wurzel unendlich wird und damit das Verfahren abbricht, noch ein dritter Fall auftreten kann, daß nämlich wieder eine der Ausgangslösungen gefunden wird, und man damit bloß einen endlichen Zykel von Lösungspaaren findet. Dies tritt z. B. bei der Gleichung mit der x-Axe als Symmetrieaxe:

$$x^2y^2 + x - 2 = 0$$

auf, wo $x = 1,\ y = 1$ vier Lösungen eines solchen Zykels ergeben:

$$x = 1,\ y = 1;\ x = 1,\ y = -1;\ x = -2,\ y = -1;\ x = -2,\ y = 1\,.$$

Die letzte Gruppe von Abhandlungen dieses Teiles bezieht sich auf das FERMAT*sche Problem*, zwei positive Zahlen zu finden, für die ihre Summe ein Quadrat und die Summe ihrer Quadrate ein Biquadrat ist. EULER hat hierüber schon früher gearbeitet[1]) und hier noch zwei weitere Arbeiten verfaßt. Die erste, die die neue Methode noch nicht verwendet, ist Abhandlung 763: *„De tribus pluribusve numeris inveniendis, quorum summa sit quadratum, quadratorum vero summa biquadratum"*, in der er zuerst das von FERMAT angegebene Zahlenbeispiel nachrechnet. Dann wird das Problem auf drei, vier und fünf Zahlen erweitert, deren Summe ein Quadrat, die Summe ihrer Quadrate ein Biquadrat ist. Dabei stellt sich natürlich heraus, daß das Problem um so einfacher wird, je größer die Zahl der Summanden ist, und daß auch die entsprechenden Zahlenbeispiele immer kleinere Zahlen ergeben. Da in einem dieser Beispiele für drei Summanden die Summe der Zahlen selbst schon ein Biquadrat wird, löst EULER auch noch die Aufgabe, drei Zahlen zu finden, für die die Summe und die Summe ihrer Quadrate ein Biquadrat ist[2]). Die Methode ist stets dieselbe. Zum Beispiel wird für vier Summanden x, y, z, u der Ansatz gemacht:

$$x = p^2 + q^2 + r^2 - s^2,\ y = 2ps,\ z = 2qs,\ u = 2rs\,.$$

1) Siehe diese Werke, Band I, 4, p. XXVI/VII und p. 96.

2) Siehe HEATH a. a. O. p. 363, problem 14.

Dann ist die Summe ihrer Quadrate ein Quadrat, nämlich $(p^2 + q^2 + r^2 + s^2)^2$. Man wiederholt daher die Substitution nochmals für die p, q, r, s. Hieraus entstehen für die x, y, r, u biquadratische Funktionen der neuen Parameter; die Summe dieser Funktionen ist zu einem Quadrate zu machen. Diese Aufgabe wird durch einen einfachen Ansatz gelöst, durch welchen einer der Parameter durch die drei andern linear ausgedrückt wird. Somit erhält die Lösung noch drei willkürliche Parameter.

Bei zwei Summanden wird man auf eine biquadratische Form zwischen zwei Parametern geführt, die zu einem Quadrate zu machen ist. Dies ist aber gerade eine Aufgabe, die man mit der neuen Methode lösen kann. Dies geschieht in Abhandlung 769: „*Solutio problematis Fermatiani de duobus numeris, quorum summa sit quadratum, quadratorum vero summa biquadratum, ad mentem illustris La Grange adornata.*“ Setzt man für die beiden Summanden:

$$x = p^2 - q^2, \quad y = 2pq ,$$

und hier:

$$p = r^2 - s^2, \quad q = 2rs ,$$

so wird $x^2 + y^2 = (r^2 + s^2)^4$. Es bleibt also nur noch übrig, auch $x + y$ zu einem Quadrate zu machen. Die entsprechende biquadratische Funktion von r und s lautet:

$$x + y = r^4 + 4r^3s - 6r^2s^2 - 4rs^3 + s^4 ,$$

die gerade von der Gestalt $P^2 + QR$ der Abhandlung 778 ist und nach der neuen Methode gelöst werden kann. Neue Zahlenbeispiele kann EULER jedoch nicht angeben, da die Zahlen allzugroß werden.

II. Teil:

NACHGELASSENE WERKE UND ABHANDLUNGEN

Von den nachgelassenen Werken verdienen die 16 Kapitel über Zahlentheorie besonderes Interesse. Ohne Zweifel stellen sie den Versuch eines Lehrbuches über den Gegenstand dar, das aber unvollendet geblieben ist. Das Manuskript, das von EULER eigenhändig geschrieben wurde, ist 1849 von P. H. FUSS und NIKLAUS FUSS in den „*Commentationes arithmeticae collectae*“ zum ersten Male publiziert worden unter dem von den Herausgebern hinzugefügten Titel:

„*Tractatus de numerorum doctrina Capita XVI, quae supersunt.*“

Das Werk hat von ENESTROEM die Nummer 792 erhalten. Es wirft sofort die drei Fragen auf: 1. Wann hat EULER dasselbe verfaßt? 2. Was bezweckte er mit der Abfassung? 3. Warum hat er das Werk nicht zu Ende geführt? Es scheint mir, daß man diese

Fragen mit großer Sicherheit beantworten kann. Hierzu müssen wir uns aber zunächst mit seinem Inhalte vertraut machen.

Das ganze Werk handelt nur von ganzen rationalen Zahlen. Es geht aus von der Entstehung der natürlichen Zahlen mit Hilfe der sukzessiven Addition der Einheit. Wird dieselbe Zahl mehrere Male zu sich selbst addiert, so nennt EULER die Anzahl der Summanden den *Index*. Dies führt zur Multiplikation, indem Zahl und Index vertauscht werden dürfen. Dieses *genetische* Verfahren begründet die kommutativen und assoziativen Gesetze, die aber nicht ausdrücklich ausgesprochen werden. Damit sind die *Vielfachen* der Zahlen definiert. Die Primzahlen sind Zahlen, die nur Vielfache von 1 und sich selbst sind. Die eindeutige Darstellbarkeit durch Primzahlen wird nicht streng bewiesen. Alle natürlichen Zahlen werden in Klassen eingeteilt gemäß der Anzahl ihrer Primfaktoren. Dabei zählt EULER die Anzahl der in jeder Klasse fallenden Zahlen ab, die kleiner als eine feste Zahl n sind und betrachtet das Wachstum mit n.

Auf die Frage nach den *Vielfachen* folgt die umgekehrte nach den *Teilern*. Es wird die Anzahl der Teiler einer in Primfaktoren zerlegten Zahl berechnet, sowie deren Summe, wobei EULER das Zeichen $\int n$ verwendet, das er in den im Jahre 1747 verfaßten Abhandlungen 152 und 175 eingeführt hat[1]). Hieran schließt sich ein Exkurs über vollkommene Zahlen. Außerdem wird die Formel für die Anzahl $\varphi(n)$ der zu einer gegebenen Zahl n teilerfremden Zahlen, die kleiner als n sind, genau nach der Methode abgeleitet, die EULER in der im Jahre 1758 verfaßten Abhandlung 271 angegeben hat.

Jetzt entwickelt EULER die vollständige Lehre der *Kongruenzen*, wobei einzig das GAUSS'sche Kongruenz-Zeichen fehlt und statt Modul Divisor gesagt wird. Er stellt das vollständige Restsystem, sogar dasjenige der absolut kleinsten Reste auf, besitzt völlig den Begriff der Restklasse und zeigt, wie man bei Addition und Multiplikation der Zahlen auch ihre Restklassen entsprechend zusammensetzt. Diese Theorie wendet er zunächst auf die *arithmetischen Reihen* an, indem er nach den Resten fragt, die ihre Glieder nach einem gegebenen Modul besitzen. Dies führt ihn auf die allgemeine Lösung der linearen Kongruenz:

$$a + bx \equiv 0 \pmod{n}.$$

Bei der Anwendung auf *geometrische Reihen* kann man sich auf die Reihe

$$1, a, a^2, a^3, \ldots \pmod{n}, \quad (a, n) = 1,$$

beschränken. Alle Restklassen, die durch die Potenzen von a festgelegt werden, heißen

1) Alle Jahreszahlen über die Zeiten, in denen EULER seine Abhandlungen verfaßt hat, sind ENESTROEM entnommen: GUSTAF ENESTROEM: *Verzeichnis der Schriften LEONHARD EULERS*. Zweite Lieferung. Jahresbericht der Deutsch. Math. Vereinig. Ergänzungsbände zum IV. Bd. 2. Lieferung. Leipzig, Teubner, 1913, p. 223 ff.

Reste, die nicht auftretenden Nichtreste. EULER unterscheidet somit zwischen diesen Nichtresten und den *quadratischen* Nichtresten, die er später einführt. Der Gruppencharakter der Reste in bezug auf Multiplikation wird sofort erkannt und die Existenz eines Exponenten d bewiesen, der Teiler von $\varphi(n)$ ist und für den $a^d \equiv 1 \pmod{n}$ ist. Damit hat er den allgemeinen FERMATSCHEN Satz in der gleichen Weise bewiesen, wie in der im Jahre 1758 verfaßten Abhandlung 271.

Erst jetzt beschränkt sich EULER auf den Primzahlmodul $n = p$. Seine ganze Theorie der Potenzreste krankt daran, daß EULER den Begriff der Primitivwurzel noch nicht kennt, oder jedenfalls deren Existenz nicht beweist. Erst die im Jahre 1772 verfaßte Abhandlung 449 bringt diesen enormen Fortschritt. Ist d der kleinste positive Exponent, für den $a^d \equiv 1 \pmod{p}$ ist, und ist $d < p - 1$, so zeigt EULER in derselben schönen Weise, wie in der anno 1750 verfaßten Abhandlung 241, durch sukzessive Differenzenbildung, daß nicht jede Restklasse zu d gehört. Die Theorie wird sofort auf die Formen $x^d \pm y^d$ ausgedehnt; beim untern Vorzeichen, und falls d eine Primzahl ist, besitzen z. B. alle ihre Primteiler, falls sie zu $x - y$ teilerfremd sind, sie Gestalt $1 + nd$.

Jetzt folgt die Theorie der *quadratischen Reste und Nichtreste*, wie sie EULER in der anno 1751 verfaßten Abhandlung 242 dargestellt hat, teilweise sogar mit derselben Bezeichnungsweise. Dagegen ist das Kriterium, daß a quadratischer Rest oder Nichtrest ist (mod. p), je nachdem

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

ist, das erst in der viel reiferen, im Jahre 1755 verfaßten Abhandlung 262 bewiesen wird, wohl angeführt, der Beweis ist aber nicht zwingend. Ebenso kann EULER nicht beweisen (siehe Additamentum S. 237/8), daß 2 quadratischer Rest aller Primzahlen der Form $8n + 1$ ist. Das konnte EULER erst in der oben genannten Abhandlung 449 durchführen.

Am Schlusse dieser Ausführungen gibt EULER seine Vermutungen über diejenigen Primzahlen an, für die eine gegebene Zahl n quadratischer Rest ist. Er erkennt, daß dieselben in bestimmten Restklassen (mod. $4n$) liegen müssen, und daß diese genau die Hälfte aller möglichen Restklassen (mod. $4n$) ausmachen. Damit sind wesentliche Teile des quadratischen Reziprozitätsgesetzes ausgesprochen[1]).

Besondere Aufmerksamkeit verdient die nun folgende Betrachtung der *kubischen Reste*, die EULER später leider nie mehr fortgesetzt hat. Hier hat er durch Divination Spezialfälle des EISENSTEINSCHEN *kubischen Reziprozitätsgesetzes* und des *Ergänzungssatzes* gefunden. In § 407 (S. 250) behauptet EULER, daß 2 dann und nur dann kubischer

1) Siehe hierzu die Ausführungen in der Vorrede zu Band I, 4, p. XIII.

Rest der ungeraden Primzahl $l = 3n + 1$ ist, falls sich l in der Form $q^2 + 27p^2$, p und q ganz, darstellen läßt. In der Tat läßt sich jede Primzahl $l = 3n + 1$ in der Form:

$$4l = x^2 + 27y^2$$

darstellen. Die Zahl $\omega = l\frac{x + 3y\sqrt{-3}}{2}$, $x \equiv 1 \pmod 3$, ist dann primär[1]), und nach dem kubischen Reziprozitätsgesetz wird:

$$\left\{\frac{2}{\omega}\right\} = \left\{\frac{\omega}{2}\right\}.$$

Nun ist, wenn 2 kubischer Rest (mod. l) ist,

$$\left\{\frac{2}{\omega}\right\} = 1,$$

also auch

$$\left\{\frac{\omega}{2}\right\} = 1,$$

oder wegen $(n(2) - 1) / 3 = 1$:

$$\frac{x + 3y\sqrt{-3}}{2} \equiv 1 \pmod 2,$$

was dann und nur dann erfüllt ist, wenn x, y beide gerade sind. Dann ist aber $l = q^2 + 27p^2$, wie EULER behauptet.

In § 408 gibt EULER den kubischen Restcharakter von 3 nach dem Modul $l = 3n + 1$ an. Nach EISENSTEIN[2]) ist 3 dann und nur dann kubischer Rest (mod. l), falls in der Darstellung $4l = x^2 + 27y^2$ die Zahl y durch 3 teilbar ist. Sind x, y beide gerade, so ist dies die erste Bedingung von EULER. Sind sie beide ungerade, so werden für eines der beiden Vorzeichen:

$$q = \frac{-x \mp 9y}{4}, \quad p = \frac{\pm x - 3y}{4}$$

ganz und l besitzt die Darstellung $l = q^2 + 3p^2$. Anderseits ist $-x = q \mp 3p$, $-3y = \pm q + p$; somit muß $\pm q + p$ durch 9 teilbar sein, was die zweite EULERSCHE Bedingung ist.

Um den von EULER in § 409 angegebenen kubischen Restcharakter von 5 (mod. $l \neq 5$) zu erhalten, folgert man aus dem kubischen Reziprozitätsgesetz wieder:

---

1) Siehe etwa meine *„Synthetische Zahlentheorie"*, 2. A. Berlin und Leipzig, 1925, p. 263ff.

2) G. EISENSTEIN: *Nachtrag zum cubischen Reciprocitätssatze für die aus dritten Wurzeln der Einheit zusammengesetzten complexen Zahlen. Criterien des cubischen Charakters der Zahl 3 und ihrer Teiler.* Crelle's Journal f. d. r. u. ang. Math. Bd. 28, 1844, p. 28.

$$\left\{\frac{5}{\omega}\right\} = \left\{\frac{\omega}{5}\right\} = 1 \ ;$$

da $l^8 \equiv 1 \pmod 5$ und in $k(\sqrt{-3})$ $(n(5) - 1) / 3 = 8$ ist, muß:

$$\left(\frac{x + 3y\sqrt{-3}}{2}\right)^8 \equiv 1 \quad \text{oder} \quad \left(\frac{x + 3y\sqrt{-3}}{2}\right)^4 \equiv \pm 1 \pmod 5$$

sein. Durch Ausrechnung ergibt sich, daß x oder y durch 5 teilbar sein muß. Denn wären beide zu 5 teilerfremd, so ergäbe der imaginäre Teil der Kongruenz, daß 2 quadratischer Rest (mod. 5) wäre. Sind x, y wieder beide gerade, so sind die beiden ersten EULERSCHEN Bedingungen hergeleitet. Sind sie beide ungerade, so bilde man wie vorhin q, p, und es muß dann $-x = q \mp 3p$ oder $-3y = p \pm q$ durch 5 teilbar sein, was offenbar die dritte und vierte Bedingung von EULER enthält.

Setzt man, um den in § 410 angegebenen kubischen Restcharakter von 6 zu erhalten, $\varrho = e^{\frac{2\pi i}{3}}$, so ist nach EISENSTEIN:

$$\left\{\frac{3}{\omega}\right\} = \varrho^{-\nu} \qquad (4l = x^2 + 27y^2) \ .$$

Daher wird nach dem Reziprozitätsgesetz:

$$\left\{\frac{6}{\omega}\right\} = \left\{\frac{3}{\omega}\right\} \left\{\frac{2}{\omega}\right\} = \varrho^{-\nu}\left\{\frac{\omega}{2}\right\} = 1 \ , \quad \text{d. h.} \left\{\frac{\omega}{2}\right\} = \varrho^{\nu} \ ;$$

wie vorhin ergibt dies die Kongruenz:

$$\frac{x + 3y\sqrt{-3}}{2} \equiv \varrho^{\nu} \pmod 2 \ .$$

Ist $y \equiv 0 \pmod 3$, so müssen x, y beide gerade sein, was die erste EULERSCHE Bedingung ergibt. Ist $y \equiv 1 \pmod 3$, so ist wegen $x \equiv 1 \pmod 3$ auch $y - x$ durch 3 teilbar. Die Kongruenz ergibt dann $x - y \equiv 0 \pmod 4$; also sind x, y von gleicher Parität, und zwar beide ungerade. Führt man wieder q, p ein, so kann wegen $x - y \equiv 0 \pmod 4$ nur das untere Vorzeichen gelten, und es muß:

$$3(x - y) = -4(2p + q) \equiv 0 \pmod 9$$

sein. Ist $y \equiv -1 \pmod 3$, so ist $x + y$ durch 3 teilbar. Die Kongruenz ergibt $x + y \equiv 0 \pmod 4$, weshalb x, y beide ungerade sein müssen. In q, p gilt nur das obere Vorzeichen, und es muß:

$$3(x + y) \equiv 4(2p - q) \equiv 0 \pmod 9$$

sein. Damit sind auch die zweiten Bedingungen von EULER hergeleitet.

Um den im Additamentum zu § 410 angegebenen kubischen Restcharakter von 7 herzuleiten, beachten wir, daß 7 die Norm des Primideals $(2+\sqrt{-3})$ in $k(\sqrt{-3})$ ist. Ist daher $(l, 7) = 1$ und 7 kubischer Rest (mod. l), so ist nach dem kubischen Reziprozitätsgesetz:

$$\left\{\frac{7}{\omega}\right\} = \left\{\frac{\omega}{7}\right\} = 1 ,$$

also:

$$\omega^2 = l^2\left(\frac{x+3y\sqrt{-3}}{2}\right)^2 \equiv 1 \,(\text{mod. } (2+\sqrt{-3})) , \quad \text{d. h.}$$

$$l^2\left(\frac{x+y}{2}\right)^2 \equiv 1 \,(\text{mod. } 7) \quad \text{oder} \quad l^{\frac{x+y}{2}} \equiv \pm 1 \,(\text{mod. } 7) .$$

Setzt man hier $l = \frac{1}{4}(x^2 + 27y^2) \equiv 2(x^2 - y^2)$ (mod. 7) ein und multipliziert die Kongruenz mit $(x + y)$, so wird wegen $(x + y)^3 \equiv \pm 1$ (mod. 7):

$$x - y \equiv \pm (x + y) \,(\text{mod. } 7),$$

d. h. x oder y muß durch 7 teilbar sein. Sind beide gerade, so erhält man EULERS erste und vierte Bedingung. Sind beide ungerade, so muß $-x = q \mp 3p$ oder $-3y = \pm q + p$ durch 7 teilbar sein, was die zweite und dritte EULERSCHE Bedingung ergibt.

Damit sind alle EULERSCHEN Vermutungen als richtig nachgewiesen, und es grenzt ans Unfaßbare, wie EULER diese komplizierten Bedingungen erraten konnte. Kein schlagenderes Beispiel beweist seine geniale Einsicht in mathematische Beziehungen.

Die jetzt folgenden Entwicklungen über *biquadratische Reste* bringen Vermutungen über das *biquadratische Reziprozitätsgesetz*. In § 456 (S. 258) wird behauptet, daß 2 biquadratischer Rest aller Primzahlen $l \equiv 1$ (mod. 4) der Gestalt $l = q^2 + 64p^2$ ist. Dies ist der von GAUSS bewiesene Ergänzungssatz des biquadratischen Reziprozitätsgesetzes[1]). Im Additamentum zu § 457 wird der biquadratische Restcharakter der Zahlen 3 und 5 angegeben. Diese Resultate sind von GAUSS in den art. 25 und 26 seiner zweiten Abhandlung über biquadratische Reste[2]) ebenfalls induktiv gefunden und nachher bewiesen worden. Für 5 ist dies ohne weiteres ersichtlich. Bei 3 gibt GAUSS das Gesetz für die Zahl -3 an. Ist $l = p^2 + 4q^2$ die gegebene Primzahl, so ist nach GAUSS -3 biquadratischer Rest, wenn q durch 3 teilbar ist, biquadratischer Nichtrest, aber quadratischer Rest, wenn p durch 3 teilbar ist. Somit muß, damit $+3$ biquadratischer Rest wird, im ersten Falle -1 biquadratischer Rest, im zweiten Fall -1 biquadratischer Nichtrest, dagegen

1) CARL FRIEDRICH GAUSS: *Theoria residuorum biquadraticorum*, Commentatio prima, art. 21, Werke, Bd. 2, Göttingen 1876, p. 89.

2) CARL FRIEDRICH GAUSS: *Theoria residuorum biquadraticorum*, Commentatio secunda, art. 25 und 26, Werke a. a. O. p. 96/7.

quadratischer Rest sein. Nun ist aber — 1 biquadratischer Rest oder Nichtrest, je nachdem q gerade oder ungerade ist. Daraus folgen die beiden EULERSCHEN Bedingungen.

Schließlich betrachtet EULER noch 5te und höhere Reste und quadratische Reste für zusammengesetzte Moduln.

In den beiden letzten Kapiteln bemüht sich EULER, Klarheit über die Teiler der beiden Formen $x^2 + y^2$ und $x^2 + 2y^2$ für teilerfremdes x, y zu erhalten. Der Nachweis gelingt ihm aber nicht, daß jeder Teiler der Formen wieder durch die Form darstellbar ist. Für $x^2 + y^2$ hat EULER diese Tatsache in den Abhandlungen 228 und 241 bewiesen. Die erstere stammt aus dem Jahre 1749, die zweite aus dem Jahre 1750. In der vorliegenden Arbeit kommt EULER dem Beweise sehr nahe. Alle Mittel zum spätern Beweise finden sich schon vor. Genau dasselbe läßt sich über die Theorie der Form $x^2 + 2y^2$ und die aus dem Jahre 1753 stammende Abhandlung 256 sagen.

Jetzt sind wir so weit, daß wir die zum Beginn dieses Kapitels gestellten Fragen beantworten können:

1. *Zeitpunkt der Abfassung.* Zunächst ist das Werk *vor* 1772 geschrieben, da EULER die Primitivwurzel, die er in der anno 1772 geschriebenen Abhandlung 449 einführt, noch nicht kennt. In § 384 sagt EULER, er könne nicht beweisen, daß -3 quadratischer Rest aller Primzahlen der Form $6n + 1$ sei. Diesen Beweis bringt er in der im Jahre 1759 verfaßten Abhandlung 272, weshalb das Werk sicherlich *vor* 1759 geschrieben ist. Im Additamentum zu den Paragraphen 338 und 342 sagt er, er könne nicht beweisen, daß 2 quadratischer Rest aller Primzahlen der Form $8n \pm 1$ und quadratischer Nichtrest aller Primzahlen der Form $8n \pm 3$ ist. Den Beweis hat bekanntlich LAGRANGE 1773 erbracht. Nun schreibt er neben § 338 an den Rand „*ut praecedens*", was sich offenbar auf § 337 bezieht. Da er dort den Restcharakter der Zahl — 1 angibt, so kann er im Zeitpunkt der Niederschrift noch nicht beweisen, daß — 1 quadratischer Rest aller Primzahlen der Form $4n + 1$ ist. Diesen Beweis hat er 1750 in seiner Abhandlung 241 geführt. Danach muß die Verfassung des vorliegenden Werkes *vor* 1750 erfolgt sein.

Verfolgt man andererseits aufmerksam die Inhaltsangabe des Werkes und die Zeiten der Veröffentlichung der betreffenden Resultate in eigenen Abhandlungen, so erkennt man, daß das Werk offenbar ziemlich kurz vor 1750 geschrieben worden sein muß. Es atmet in allen seinen Teilen, oft sogar in der Bezeichnungsweise, die Problemstellung und die Durchführung derjenigen Abhandlungen, die um 1750 verfaßt worden sind. Dagegen ist es viel reifer, als z. B. die im Jahre 1747 verfaßte Abhandlung 164, in der eigentlich nur eine große Zahl von induktiv gefundenen Theoremen bekannt gegeben wird, aber kein Versuch einer zusammenhängenden Theorie gemacht wird. Diese innern Gründe für die Bestimmung des Zeitpunktes der Niederschrift scheinen mir die zwingendsten zu sein. Die

ganze Entwicklung des zahlentheoretischen Schaffens von EULER läßt nur die eben formulierte Annahme zu.

Aus all diesem muß mit Sicherheit geschlossen werden, daß Euler das vorliegende Manuskript in den Jahren 1748—1750 verfaßt hat. Es stammt also aus den Jahren, in denen EULER seine großen Lehrbücher schrieb. 1745 verfaßte er die *Introductio* und 1748 die *Institutiones calculi differentialis*. Es war ein kühner Gedanke, denselben ein Lehrbuch der Zahlentheorie folgen zu lassen. Denn eine zusammenhängende Theorie dieser Disziplin gab es damals überhaupt noch nicht. Diese mußte erst von ihm geschaffen werden.

2. *Zweck des Werkes.* Aus dem zuletzt Gesagten ergibt sich, daß EULER mit seinem Lehrbuch bezweckte, aus den Einzelresultaten, die FERMAT und andere Mathematiker meist ohne Beweis hinterlassen hatten, ein zusammenhängendes Gebäude zu errichten. Er wollte für die Zahlentheorie das gleiche schaffen, wie er es in so einziger Weise in seiner *Introductio* für die Analysis gemacht hatte. Wir erkennen dies sofort aus der ganzen Anlage des Werkes, aus der breiten Basis, auf der er seine Ausführungen aufbaut.

3. *Warum hat Euler sein Manuskript nicht zu Ende geführt?* Der Grund liegt ohne Zweifel darin, daß EULER bei der Ausführung seiner Absicht immer mehr erkannte, daß die Theorie nicht so gründlich und schnell entwickelt werden konnte, wie er es sich ursprünglich gedacht hatte. Wohl besaß er dank seiner genialen Divinationsgabe den Plan des Ganzen. Allein die Beweise machten offenbar mehr Mühe und erforderten mehr Zeit, als er zu Beginn übersehen konnte. So fand er eine ganze Menge Fragen, die er nicht lösen konnte. Zum Beispiel besaß EULER zu dieser Zeit den Begriff der Primitivwurzel nach einer Primzahl noch nicht. Er sah keine Möglichkeit, seine Induktionen über das quadratische Reziprozitätsgesetz zu beweisen. Ja, nicht einmal die Restcharaktere von $-1, 2, 3$ konnte er beweisen. So mußte es ihm klar werden, daß ohne den Beweis aller dieser Resultate kein Lehrbuch verfaßt werden konnte. Bis zur Schaffung eines solchen mußten noch mehr Vorarbeiten geleistet werden. Speziell das Mißlingen des Beweises des Restcharakters von 2 und 3, den er noch auf dem eingeschobenen Blatt, das als Additamentum am Ende des Manuskriptes abgedruckt wird, versucht hat, mag ihn wohl bewogen haben, das Manuskript vorläufig liegen zu lassen. Als GAUSS fünfzig Jahre später 1801 die Publikation der „*Disquisitiones arithmeticae*" unternahm, die mit dem vorliegenden EULERSCHEN Manuskripte inhaltlich in den ersten Kapiteln weitgehendst übereinstimmen, lagen die Vorarbeiten von EULER, LAGRANGE und LEGENDRE vor, die eine neue Situation schufen. Siehe hierzu die Ausführungen am Ende der Vorrede.

Hieraus dürfen wir schließen, daß EULER die Abfassung eines Lehrbuches der Zahlentheorie als verfrüht erkannte und das Manuskript liegen ließ, um zuerst in Spezialabhandlungen die noch fehlenden Beweise zu schaffen. Da er aber nie zum Beweise seiner Ver-

mutungen über das quadratische Reziprozitätsgesetz kam, blieb das Manuskript unvollendet liegen.

Der vorliegende Neudruck hält sich genau an das von EULERS Hand geschriebene Manuskript. Gegenüber der Erstausgabe in den *Commentationes arithmeticae collectae* von 1849 sind nur unwesentliche Abänderungen zu verzeichnen. Zum Beispiel ist die eingeschaltete Seite nicht dort abgedruckt, wo sie zufällig im Manuskript auftritt, sondern wo sie inhaltlich hingehört, d. h. an den Schluß des Werkes.

Das Manuskript der nächsten Abhandlung, die von ENESTROEM den Index 793 erhalten hat:

„*Considerationes circa Analysin Diophanteam*"

ist ohne jeden Zweifel von EULER eigenhändig geschrieben worden. Die Schriftzüge sind aber sehr schwer und groß und weichen entschieden ab von der feinen und deutlichen Art, wie EULER in seinen besten Jahren zu schreiben pflegte. Die Abfassungszeit muß daher in jene Epoche fallen, in der EULER bereits mit der beginnenden Starerkrankung kämpfen mußte. Diese begann 1766 in St. Petersburg und hat nach EULERS eigenen Berichten sein Gesicht sehr stark in Mitleidenschaft gezogen[1]). Die Staroperation erfolgte erst im Jahre 1771, ohne aber eine dauernde Besserung zu zeitigen. Daraus darf man schließen, daß die Arbeit zwischen 1766 und 1770 verfaßt worden ist. Dies stimmt auch inhaltlich, da sie einen durchaus reifen Eindruck macht.

Das erste von EULER behandelte Problem verlangt drei Zahlen zu finden, für die das Produkt von je zweien, um die Einheit vermindert, ein Quadrat ergibt. Jedes der drei Produkte hat somit die Form $x^2 + 1$; das Produkt von drei solchen Ausdrücken muß also wieder ein Quadrat werden, was sehr einfach zur Lösung führt. Schwieriger wird die Frage erst, wenn man verlangt, daß die drei Zahlen *ganz* sind. Eine außerordentlich einfache und elegante spezielle Lösung ist die folgende: Es seien p, q, r, s ganze Zahlen, für die

$$ps - qr = \pm 1$$

ist. Dann ist, wie man sofort sieht, A, B, C eine Lösung, falls:

$$A = p^2 + q^2,\ B = r^2 + s^2,\ C = (p \pm r)^2 + (q \pm s)^2$$

gesetzt wird. Denn es wird:

$$AB - 1 = (pr + qs)^2,\ AC - 1 = \big(p(p \pm r) + q(q \pm s)\big)^2,\ BC - 1 = \big(r(p \pm r) + s(q \pm s)\big)^2.$$

In einem zweiten Problem wird die Aufgabe auf vier Zahlen ausgedehnt, und im dritten Problem wird das Problem so erweitert, daß vier Zahlen gesucht werden, deren

1) Siehe die Ausführungen: RUD. FUETER: *Über eine Eulersche Beweismethode in der Zahlentheorie.* Schweiz. medizin. Wochenschrift, 69. Jahrgang, 1939, S. 103—106.

Produkte zu je zweien, um eine *beliebige* Zahl vermehrt, Quadrate ergeben. Auf diese Aufgabe wird auch die letzte zurückgeführt, in der diese beliebige Zahl die Summe der vier gesuchten Zahlen ist.

Die nächsten vier Abhandlungen:

„*Recherches sur le problème de trois nombres carrés tels que la somme de deux moins le troisième fasse un nombre carré*“;

„*Solution d'un problème assez curieux, savoir: Trouver quatre nombres positifs et inégaux entre-eux, tels que la somme de deux soit toujours un carré*“;

„*Supplément au problème de quatre nombres, dont la somme de deux fasse toujours un nombre carré*“;

und

„*Recherches ultérieures et très curieuses sur le problème de quatre nombres positifs et en proportion arithmétique tels, que la somme de deux quelconques soit toujours un nombre carré*“

sind einem Manuskript der Petersburger Akademie entnommen, dessen zwei erste Abhandlungen unter dem zusammenfassenden Titel:

„*Recherches sur deux problèmes de l'analyse de Diophante, savoir: Trouver trois nombres carrés tels que la somme de deux moins le troisième fasse un nombre carré. Et trouver quatre nombres inégaux et entiers tels que la somme de deux fasse toujours un carré*“,

der Akademie am 1. März 1781, deren beiden letzten am 23. April 1781 vorgelegt wurden. Verfasser aller vier Abhandlungen ist ein „Elève de l'académie“, Alexandre Wilbrecht, der den ersten Teil selbst übergeben hat, während der zweite Teil von Euler vorgelegt wurde. Beide Teile waren unterschrieben mit: „*Calculé sous la direction de M. le professeur* Leonhard Euler *par* Alexandre Wilbrecht“, wobei aber in beiden „Calculé sous la direction de M. le professeur“ durchgestrichen und durch „*par*“ ersetzt wurde. Auf dem Umschlag des Manuskriptes ist vom Sekretär der Akademie notiert worden: „*Je ne puis deviner par qui peut avoir été faite la correction des titres*“. Die vier Abhandlungen sind in die Liste der unveröffentlichten Mémoiren Eulers nach dessen Tode aufgenommen worden. Sie sind *teilweise* von den beiden Urenkeln Eulers, P. H. Fuss und Nikolaus Fuss 1849 in den *Commentationes arithmeticae* publiziert worden, dabei aber ziemlich weitgehend umgearbeitet worden. So ist zum Beispiel in dem Abdruck der ersten Abhandlung, die von Enestroem den Index 796 erhalten hat, von insgesamt fünf Lösungsmethoden des Problemes die dritte völlig weggelassen worden, so daß die vierte und fünfte als dritte und vierte Methode erschienen. Die zweite und dritte Abhandlung sind überhaupt nicht

abgedruckt worden, so daß sie im vorliegenden Bande zum ersten Male erscheinen. Dagegen wurde die vierte in die *Commentationes arithmeticae* aufgenommen, wobei sie sehr großen Änderungen unterworfen wurde; ihr Abdruck hat von ENESTROEM den Index 797 erhalten. Die Brüder P. H. FUSS und NIKOLAUS FUSS, die die Verantwortung für die Ausgabe von 1849 tragen, haben die beiden Abhandlungen 796 und 797 gegenüber dem Manuskript in zwei Richtungen verändert:

1. Der sehr schlechte *Stil* WILBRECHTS ist durchgängig korrigiert worden. Sein unbeholfenes Französisch wurde nach Möglichkeit verbessert. Diese *Stilveränderungen* sind wegen des Umstandes, daß EULER die Abhandlungen nicht selbst verfaßte, und angesichts der Verwandtschaft der Herausgeber mit EULER in der vorliegenden Ausgabe in der Regel belassen worden. Sie sind so zahlreich, daß sie im Druck nicht kenntlich gemacht werden konnten, da sonst eine unmögliche Komplikation entstanden wäre.

2. Die Herausgeber haben *inhaltliche* Änderungen vorgenommen. *Diese sind gänzlich rückgängig gemacht worden.* Denn sie verändern teilweise vollständig die EULERSCHE mathematische Denkweise von 1781. Dies ist besonders auffällig in der Abhandlung 797, in der eine fast modern anmutende Diskussion der Gleichung vierten Grades von den Herausgebern hineingearbeitet wurde. EULER hat sicherlich alle vier Abhandlungen angeregt und mit WILBRECHT durchgesprochen. Er war sicherlich über dieselben genau unterrichtet. Somit darf ein Abdruck in EULERS Werken keine inhaltlichen Veränderungen des hinterlassenen Manuskriptes dulden.

Wenn somit rein *äußerlich* die Aufnahme der vier Abhandlungen in die Werke LEONHARD EULERS gerechtfertigt ist, so sind die *innern* Gründe hierzu noch weit zwingender. In der Tat zeigt der *Inhalt* der vier Abhandlungen, daß sie ganz im Sinne und Geiste des Meisters verfaßt sind. Einmal die Problemstellung! Die *erste Aufgabe*, drei Quadrate zu finden, für die die Summe von zweien, vermindert um das dritte wieder ein Quadrat ergibt, erinnert in der Form des diophantischen Problems an die Aufgabe der Schwerpunktlinien der Dreiecke. Sind:

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

die drei zu lösenden Gleichungen, so sieht man sofort, daß die Summe

$$s = x^2 + y^2 + z^2$$

sich auf drei verschiedene Weisen darstellen lassen muß:

$$s = u^2 + 2z^2 = v^2 + 2y^2 = w^2 + 2x^2.$$

Somit muß s das Produkt von wenigstens drei Faktoren der Form $a^2 + 2b^2$ sein. Macht man diesen Ansatz, so erhält man x, y, z, u, v, w als Funktionen von 6 Parametern, die die drei Faktoren von s bestimmen, und es bleibt nur noch die Gleichung $s = x^2 + y^2 + z^2$ zu befriedigen. Dies führt zu einer Bedingungsgleichung, die in jedem der Parameterpaare der Faktoren von s quadratisch ist. Die verschiedenen fünf Methoden, die der Verfasser angibt, beziehen sich alle mit Ausnahme der letzten auf die Lösung dieser quadratischen Gleichung. In der ersten wird z. B. der Koeffizient des quadratischen Gliedes bezüglich des Parameterpaares eines bestimmten Faktors zu null gemacht. In der zweiten wird die Diskriminante durch einen der bekannten EULERSCHEN Ansätze zu einem Quadrate gemacht. In der dritten wird dasselbe durch einen andern Ansatz zu erreichen versucht, und in der vierten wird der Umstand verwertet, daß s sich auf *vier* verschiedene Weisen bei der Zerlegung in drei Faktoren der Form $a^2 + 2b^2$ darstellen läßt. Nur die letzte fünfte Methode geht auf einen ersten Lösungsversuch zurück und ergibt folgende spezielle Lösung:

$$x = (p^4 + 4pq^3 - q^4)^2\ (p^2 + pq) + (p^4 + 4p^3q - q^4)^2\ (pq - q^2)\ ,$$
$$y = (p^4 + 4pq^3 - q^4)^2\ (p^2 + pq) - (p^4 + 4p^3q - q^4)^2\ (pq - q^2)\ ,$$
$$z = (p^2 + q^2)\ (p^4 + 4pq^3 - q^4)\ (p^4 + 4p^3q - q^4).$$

Die *zweite Aufgabe* betrifft vier Zahlen, für die die Summe von je zweien ein Quadrat ist. Dabei müssen die Zahlen positiv und von einander verschieden sein. Dadurch wird ein neues Moment in die Betrachtung gebracht. Die Aufgabe erinnert an die Abhandlung 763, in der vier Zahlen gesucht werden, deren Summe ein Quadrat, und für die die Summe ihrer Quadrate ein Biquadrat ist. Nur spielt dort wegen der zweiten Bedingung das Vorzeichen der Zahlen nicht die Rolle, wie in der vorliegenden Aufgabe.

Dieses zweite Problem wird in drei Abhandlungen gelöst, wobei in den beiden letzten noch die von EULER oft gemachte Annahme hinzukommt, daß die vier Zahlen eine arithmetische Reihe bilden, oder daß die Summe der kleinsten und größten Zahl gleich der Summe der beiden mittleren Zahlen ist. Der Gedanke der Lösung ist derselbe, wie im ersten Problem. Die Summe aller vier Zahlen muß sich auf drei verschiedene Weisen als Summe von zwei Quadraten darstellen lassen. Sind A, B, C, D die vier Zahlen, der Größe nach geordnet, und

$$A + B = x^2,\ A + C = z^2,\ B + C = w^2,\ A + D = v^2,\ B + D = u^2,\ C + D = y^2,$$

so muß die Summe $s = A + B + C + D$ sich so darstellen lassen:

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

und es wird:

$$2A = x^2 + z^2 - w^2,\ 2B = x^2 + w^2 - z^2,\ 2C = z^2 + w^2 - x^2,\ 2D = 2u^2 - x^2 + z^2 - w^2.$$

s muß wenigstens drei Faktoren der Form $a^2 + b^2$ besitzen, aus denen man x, y, z, u, v, w berechnen kann. Im Falle, daß außerdem $A + D = B + C$ sein muß, hat man $v = w$ zu setzen; im übrigen bleibt alles gleich. Die einzige Schwierigkeit, die bleibt, ist die Bedingung, daß A, B, C, D positiv ausfallen, wozu die Bedingung

$$x^2 + z^2 > w^2$$

hinreichend ist, falls man x, z, w, u in den Zerlegungen von s so wählt, daß:

$$0 < x < z < w < u$$

wird. Man hat somit nur solche Zahlen s zu nehmen, die sich derart auf drei verschiedene Weisen in Quadrate zerlegen lassen, daß diese Bedingungen erfüllbar sind.

Die letzte Abhandlung geht von der Bemerkung aus, daß die oben gefundenen Ausdrücke von A, B, C, D bei beliebigem x, z, w die drei ersten Bedingungsgleichungen befriedigen. Nimmt man noch die Bedingung $A + D = B + C$ resp. $v = w$ hinzu, so kann man D durch:

$$2D = 3w^2 - x^2 - z^2$$

gegeben denken. Dann sind vier der Bedingungsgleichungen, sowie $A + D = B + C$ erfüllt, und die beiden letzten kann man so schreiben:

$$2w^2 = x^2 + y^2 = z^2 + u^2 .$$

Daher hat man w nur auf zwei Weisen in die Summe von zwei Quadrate zu zerlegen, wodurch die Diskussion über $x^2 + z^2 > w^2$ sehr erleichtert wird. Dieser Diskussion wird der weitaus größte Teil der Abhandlung gewidmet. Sie führt auf die Frage, für welche Werte eines Parameters eine biquadratische Gleichung einer Variablen mit einer im Rationalen reduziblen kubischen Resolvente positiv ist, falls die Koeffizienten der Gleichung gegebene Funktionen des Parameters sind. Es ist dies wohl eine der frühesten vollständigen Abklärungen dieses Problems; wenn sie auch an einer speziellen Gleichung durchgeführt wird, hat die Lösung doch allgemeines Interesse. In einer Tabelle werden für die verschiedenen Werte des Parameters die Bereiche angegeben, in denen die Variable liegen muß, damit die Gleichung positiv wird.

Die Abhandlung mit dem ENESTROEMSCHEN Index 798:

„*De numeris amicabilibus*“

ist einem Manuskripte entnommen, das der Petersburger Akademie hinterlassen wurde, und in dem die Paragraphen 3 bis 7 fehlen. Die Urenkel EULERS haben in der ersten Ausgabe des Manuskriptes diese Paragraphen offenbar von sich aus durch folgende Ausführungen ergänzt:

"3. Pertinet igitur haec quaestio ad id genus, quod in contemplatione partium aliquotarum versatur; quae doctrina cum a natura quantitatum continuarum, ad quas analysis proprie est accommodata, plurimum abhorreat, prorsus singulari modo tractari debet, nisi tentando solutionem expedire velimus. Quamquam autem SCHOTENIUS ad huiusmodi problemata solvenda certam methodum sibi proposuisse videtur, dum usum calculi analytici introducere est conatus; tamen si eius ratiocinium attentius inspiciamus, praecipua solutionis pars in mera tentatione consistit, atque omni fundamento destituitur. Temere enim pro huiusmodi numeris certas assumit formulas, in quibus numeros idoneos contineri suspicatur, cum tamen eodem iure quasvis alias assumere potuisset: atque in harum ipsarum formularum evolutione plurimum casui et fortunae tribuitur; unde STIFELIUM immerito reprehendit, quod putaverit solutionem huiusmodi problematum in certa methodo comprehendi non posse. Quin potius igitur erit fatendum eam Analyseos partem, quae in scrutatione quantitatum discretarum versatur, maxime adhuc esse imperfectam, certaque principia, quibus ea superstruatur, etiam nunc desiderari. Atque ob hunc ipsum principiorum defectum ad huiusmodi problemata numerica resolvenda plurimum solertiae et perspicaciae requiritur; et plerumque singulari ratiocinii genere opus est, in quo maxima ingenii vis cernitur. Hancque ob causam, etiamsi ipsa horum problematum solutio in Analysi parum utilitatis habere videatur, tamen methodus, qua tot tantaeque difficultates superantur, fines analyseos non mediocriter promovere est censenda. Quo plures enim diversae viae ad veritatem indagandam aperiuntur, eo maiora incrementa ipsa ars inveniendi cepisse est existimanda.

4. Quemadmodum in universa Analysi usus idoneorum signorum plurimum valet, ita etiam in hoc genere, quod circa divisores et partes aliquotas numerorum instituitur, non parum utilitatis a commoda designandi ratione erit expectandum. Numeros igitur, quos hic vel contemplamur, vel quaerimus, litteris alphabeti minusculis indicabo, litteris vero maiusculis utar ad summas divisorum eorum numerorum, qui respondentibus minusculis exhibentur, repraesentandas. Ita, si a denotet numerum quemcunque integrum et affirmativum, cuiusmodi numeros in hoc negotio semper intelligere oportet, littera maiuscula respondens A indicabit summam omnium divisorum numeri a. Simili modo litterae B, C, D etc. expriment in posterum summas divisorum numerorum b, c, d etc., scilicet, si sit $a = 10$, erit $A = 18$, et si $b = 50$, erit $B = 93$. Cum igitur cujusque numeri partes aliquotae sint eiusdem divisores ipso illo numero excepto, qui, etsi sui ipsius est divisor, tamen partibus aliquotis non annumeratur, summa partium aliquotarum numeri a erit $= A - a$, nisi sit $a = 1$. Hoc enim casu, cum unitas cuiusque numeri tam divisor quam pars aliquota censeri soleat, erit quoque $A = 1$ et partium aliquotarum summa $= 1$ putatur. Verum cum unitas in huiusmodi quaestionibus non inter numeros collocari soleat, haec exceptio nullam difficultatem afferet.

5. Hoc igitur litterarum significatu praemisso, cum numerorum primorum nulla detur pars aliquota praeter unitatem, et quilibet numerus primus alios non habeat divisores praeter unitatem et se ipsum, si a fuerit numerus primus, erit $A = a + 1$. Atque, si a fuerit quaepiam potestas numeri primi p, summa divisorum eius A facile assignari poterit. Sit enim $a = p^2$, erit utique $A = 1 + p + p^2$; ac, si $a = p^3$, erit

$$A = 1 + p + p^2 + p^3 .$$

In genere autem, si denotante p numerum primum quemcunque fuerit $a = p^n$, erit $A = 1 + p + p^2 + \cdots + p^n$, qui divisores cum constituant progressionem geometricam, erit quoque: $A = \frac{p^{n+1} - 1}{p - 1}$. Unde si a fuerit potestas quaecunque numeri primi p, quicunque sit ejus exponens, erit semper $A = \frac{pa - 1}{p - 1}$. Si igitur sit a potestas binarii, erit $A = 2a - 1$; sin sit a potestas ternarii, erit $A = \frac{3a - 1}{2}$; sin potestas quinarii, erit $A = \frac{5a - 1}{4}$ et ita porro.

6. Quodsi a fuerit productum ex duobus diversis numeris primis p et q, puta $a = pq$, erit summa divisorum $A = 1 + p + q + pq = (1 + p)(1 + q)$. Simili modo, si plures habeantur numeri primi diversi p, q, r, s etc., fueritque $a = pqr$, erit $A = (1+p)(1+q)(1+r)$, et posito $a = pqrs$ erit $A = (1+p)(1+q)(1+r)(1+s)$. Cum autem sit $p + 1 = P$, $q + 1 = Q$, $r + 1 = R$ etc., si fuerit $a = pq$, erit $A = PQ$, et si sit $a = pqr$, erit $A = PQR$ etc.; quae expressionum similitudo non solum locum habet, si p, q et r sint numeri primi diversi, sed etiam dummodo fuerint numeri primi inter se, ut praeter unitatem nullum alium divisorem habeant communem. Si enim sit P summa divisorum numeri p, et Q summa divisorum ipsius q, atque hae summae P et Q praeter unitatem nullum numerum communem contineant, tum productum $a = pq$ primo eosdem habebit divisores, quos factor p, quorum summa est $= P$; deinde divisores quoque habet numeri q, quorum summa est $= Q$; in quibus quoniam unitas bis occurrit, summa utrorumque divisorum erit $= P + Q - 1$. Tertio productum pq divisibile erit per singula producta ex binis divisoribus numerorum p et q, exclusa utrinque unitate; horum autem compositorum divisorum summa erit

$$= (P - 1)(Q - 1) = PQ - P - Q + 1 ,$$

quae cum summa simplicium $P + Q - 1$ facit PQ; ita ut posito $a = pq$, sit $A = PQ$.

7. Cum igitur omnis numerus sit vel primus vel productum ex aliquot primis eorumve potestatibus, ex resolutione numerorum in factores facile eorundem summa divisorum cognoscitur. Positis enim p, q, r etc. numeris primis omnis numerus in huiusmodi forma continebitur: $a = p^m q^n r^k \ldots$ Cum igitur factoris p^m summa divisorum sit $= \frac{p^{m+1} - 1}{p - 1}$,

et factoris q^n sit $= \frac{q^{n+1}-1}{q-1}$, ipsiusque r^k summa divisorum sit $= \frac{r^{k+1}-1}{r-1}$, ob istos factores p^m, q^n, r^k inter se primos erit numeri propositi $a = p^m q^n r^k \ldots$ summa divisorum

$$A = \frac{(p^{m+1}-1)\ (q^{n+1}-1)\ (r^{k+1}-1)}{(p-1)\ (q-1)\ (r-1)} \cdot \cdot \cdot .$$

Hocque modo, ut ipse numerus a per factores exprimitur, ita quoque summa eius divisorum per factores expressa reperietur; quod in plerisque hujus generis quaestionibus resolvendis non parum habet utilitatis. Quo igitur facilius summae divisorum quorumvis numerorum inveniri atque ipsi per factores exprimi queant, in tabula annexa non solum omnium numerorum primorum millenario minorum, sed etiam eorum potestatum, quarum quidem usus occurrit, quantumque calculi molestia id permisit, summae divisorum exhibentur in factores resolutae, ita ut ope huius tabulae omnium numerorum compositorum, nisi fuerint nimis magni, divisorum summae facile excerpi queant. Ita si propositus sit numerus $a = 7560$, hic numerus primo per factores primos exprimatur hoc modo $a = 2^3 \cdot 3^3 \cdot 5 \cdot 7$. Deinde horum factorum singulorum summae divisorum in tabula quaerantur, qui erunt: $3 \cdot 5$, $2^3 \cdot 5$, $2 \cdot 3$ et 2^3; hisque invicem multiplicatis prodibit summa divisorum numeri propositi $a = 7560$, quaesita $A = 2^7 \cdot 3^2 \cdot 5^2 = 28800$. Ex quo exemplo usus istius tabulae in summis divisorum quorumvis numerorum inveniendis abunde perspicitur."

Außer den Paragraphen 3 bis 7 fehlt auch die Tabelle, die EULER im Paragraphen 14 anführt. Nun hat C. G. J. JACOBI in einer Beilage zu dem Briefe vom 24. Oktober 1847 an den einen der beiden Urenkel EULERS, P. H. FUSS, berichtet, daß sich aus dem Jahre 1847 in der Preußischen Akademie der Wissenschaften in Berlin ein eigenhändiges Manuskript von EULER erhalten habe mit dem Titel: „*De numeris amicabilibus*", dessen Übersetzung aus dem Lateinischen ins Französische vorgesehen war[1]). Dem Manuskripte sei eine Tabelle angehängt, „wo die Faktoren von $1 + p^n$ angegeben sind, wenn p eine Primzahl ist". Diese Tabelle befinde sich auch in der gedruckten Abhandlung über den Gegenstand. Letztere kann nur die Abhandlung 152 sein, die aber eine Tabelle der *Summen aller Teiler* der Primzahlen unter Tausend und ihrer ersten Potenzen enthält, wobei diese Summen in Primfaktoren zerlegt sind[2]). Es liegt offenbar ein Versehen JACOBIS vor. Ob dieses Manuskript mit dem Torso des Petersburger Manuskriptes übereinstimmt, konnte noch nicht festgestellt werden. Zeitlich stimmen beide Manuskripte überein. Denn das Berliner Manuskript ist am 23. Februar 1747 der Akademie vorgelesen worden[3]), und das

1) Siehe STAECKEL-AHRENS: *Der Briefwechsel zwischen C. G. J. Jacobi und P. H. von Fuss über die Herausgabe der Werke Leonhard Eulers.* Leipzig, 1908, p. 25.

2) Siehe *LEONHARDI EULERI Opera omnia*, vol. 2, series I, p. 90ff.

3) Ibidem, p. 29.

Petersburger Manuskript stammt aus derselben Zeit, da es vor der nach ENESTROEM im selben Jahre 1747 verfaßten Abhandlung 152 verfaßt worden sein muß. Daß letztere später sein muß, erkennt man aus der Einführung des Symbols $\int n$ für die Summe der Teiler von n, das im Petersburger Manuskript noch fehlt; dort wird die sehr praktische Bezeichnungsweise eingeführt, die Summe aller Teiler mit dem entsprechenden großen Buchstaben, also für n mit N anzugeben.

Die Abhandlung selbst ist eine schöne einfache Darstellung der Methoden, nach denen man befreundete Zahlen berechnen kann. Sie setzt diese Methoden allgemein auseinander und wendet sie auf einige wenige Exempel an. Sie bringt gegenüber der Abhandlung 152 nichts wesentlich Neues. Letztere geht viel mehr in die Détails und setzt von vornherein Zahlen von bestimmtem Typus voraus, d. h. Zahlen, für die die Art der Zerfällung in Primfaktoren vorgeschrieben ist. Dadurch werden mehr Beispiele gefunden.

Die letzte Abhandlung mit dem ENESTROEMSCHEN Index 799:

„*Fragmenta commentationis cuiusdam maioris, de invenienda relatione inter latera triangulorum, quorum area rationaliter exprimi possit, et de triangulo, in quo rectae ex singulis angulis latera opposita bisecantes sint rationales*“

hat in der ersten Ausgabe in den *Commentationes arithmeticae* nicht den vollen Titel, indem die Herausgeber nur das erste der behandelten Probleme in ihn aufnahmen. Ihr Manuskript ist ebenfalls der Petersburger Akademie hinterlassen worden. Offenbar sind die vorhandenen Paragraphen 27—34 und 49—55 Bruchstücke einer größern Abhandlung. In den Paragraphen 27—34 wird das Problem behandelt, die rationalen Seiten a, b, c eines Dreiecks so zu finden, daß sein Flächeninhalt ebenfalls rational wird, daß also

$$J = \sqrt{\sigma(\sigma - a)\ (\sigma - b)\ (\sigma - c)}\ , \quad \sigma = \frac{a + b + c}{2}\ ,$$

rational wird. Die von EULER in den nicht mehr erhaltenen ersten Paragraphen gefundene Lösung hängt von vier willkürlichen Parametern p, q, r, s ab:

$$a = \frac{(ps \pm qr)\ (pr \mp qs)}{pqrs}\ \tau\ , \quad b = \frac{p^2 + q^2}{pq}\ \tau\ , \quad c = \frac{r^2 + s^2}{rs}\ \tau\ ,$$

wo τ ein beliebiger rationaler Proportionalitätsfaktor ist. In der Tat wird für die Werte von a, b, c:

$$J = \frac{(ps \pm qr)\ (pr \mp qs)}{pqrs}\ \tau^2\ .$$

Um die Formeln herzuleiten, macht man den von EULER viel verwendeten Ansatz:

$$\sigma = prx,\ \ \sigma - a = qsx,\ \ \sigma - b = qry,\ \ \sigma - c = psy\ ,$$

wodurch $J = xypqrs$ wird. Subtrahiert man je die zweite bis vierte Gleichung von der ersten, so folgt:

$$a = x(pr - qs), \quad b = prx - rqy, \quad c = prx - psy .$$

Aus der Bedingung $2\sigma = a + b + c$ folgt:

$$(ps + qr)y = (pr - qs)x, \quad \text{d. h. } x = ps + qr, \quad y = pr - qs ;$$

setzt man diese Werte von x, y in a, b, c ein, so folgen die EULERSCHEN Gleichungen, wenn man berücksichtigt, daß a, b, c nur bis auf einen beliebigen rationalen Faktor bestimmt sind. Die doppelten Vorzeichen erhält man durch Vertauschung z. B. von r und s. Im Fragment zeigt EULER, daß die Ausdrücke für die Verhältnisse von $a : b : c$ nur scheinbar in den Seiten unsymmetrisch sind, da auch, wie man sofort erkennt:

$$a : b = \frac{r^2 + s^2}{rs} = \frac{t^2 + u^2}{tu}$$

ist, falls $t = ps \pm qr$, $u = pr \mp qs$ gesetzt wird. Ist somit die Fläche eines Dreiecks mit rationalen Seiten selbst rational, so verhalten sich je zwei Seiten zueinander wie zwei Zahlen der Gestalt $x^2 + y^2/xy$. Offenbar hatte EULER in den folgenden Paragraphen die Natur der Zahlen von der Form $x^2 + y^2/xy$ weiter untersucht.

Der zweite Teil des Fragmentes, d. h. die Paragraphen 29—51 greifen auf ein von EULER oft behandeltes Problem zurück, nämlich die Aufgabe, rationale Dreiecke mit rationalen Schwerpunktlinien zu finden. Die nicht allgemeine Lösung stellt die drei Seiten als ganze rationale Formen 5. Grades von zwei willkürlichen Parametern dar.

Zum Schluß löst EULER das Problem, drei Quadrate zu geben, für die die Summe von je zweien wieder ein Quadrat ist.

Durch den vorliegenden Band ist das gesamte zahlentheoretische Werk EULERS abgeschlossen. Man kann dieses nicht besser charakterisieren, als es einer der besten Kenner desselben, TSCHEBYSCHEFF, in der Vorrede zu der Deutschen Ausgabe seiner *Theorie der Congruenzen*[1]) getan hat. Er schreibt: „Die Grundlage zu allen Untersuchungen, welche den allgemeinen Teil der Zahlentheorie ausmachen, ist von EULER geschaffen. Den Forschungen EULERS waren vorangegangen die von FERMAT, der sich zuerst mit den Eigentümlichkeiten von Zahlen, die gewissen unbestimmten Gleichungen zu genügen haben, beschäftigt hat. Die Untersuchungen FERMATS ergaben als Resultat die Entdeckung vieler allgemeiner Theoreme der Zahlentheorie; indes übten sie ihren Einfluß nicht unmittelbar auf die Entwicklung der Wissenschaft, indem die Sätze von FERMAT ohne Beweis und ohne Anwendung blieben. In diesem Zustande dienten die Entdeckungen FERMATS den Mathematikern nur als Herausforderung zum tiefern Eindringen in die Theorie der Zahlen. Aber wie interessant auch diese Untersuchungen waren, bis EULER hatte sich niemand dazu gemeldet. Das ist auch begreiflich. Nicht um neue Anwendungen bereits bekannter Methoden, auch nicht um weitere Entwicklungen früher bereits verwendeter Methoden handelte es sich bei diesen Untersuchungen; vielmehr mußten für dieselben neue Methoden geschaffen, neue Prinzipien entdeckt werden, mit einem Worte: eine neue Wissenschaft mußte begründet werden. Dieses ist durch EULER geschehen."

A. MARKOFF hat alle Abhandlungen dieses Bandes einer ersten Durchsicht unterzogen. Seine Anmerkungen sind mit A. M. gekennzeichnet. Leider hat der Tod ihn an der Vollendung der Aufgabe verhindert. Die Anmerkungen des heutigen Herausgebers sind mit R. F. bezeichnet.

Zürich, den 31. Dezember 1943.

RUD. FUETER.

---

1) P. L. TSCHEBYSCHEFF: *Theorie der Congruenzen* (Elemente der Zahlentheorie). Deutsch mit Autorisation des Verfassers herausgegeben von Dr. H. Schapira, Berlin, Mayer & Müller, 1889.

ÜBERSICHT ÜBER DIE ZAHLENTHEORIE IN EULERS ALGEBRA

(OPERA OMNIA SERIES I VOLUMEN 1)

Verfaßt von ANDREAS SPEISER

Da EULER seine Algebra für Liebhaber geschrieben hat, so hat der Herausgeber derselben, HEINRICH WEBER, auf ein Vorwort verzichtet. Aber zum Zweck der Übersicht über die Gesamtleistungen EULERS auf dem Gebiet der Arithmetik und als Vorarbeit zu einer wissenschaftlichen Biographie dürfte es erwünscht sein, eine kurze Inhaltsangabe des arithmetischen Teiles der Algebra, nämlich des zweiten Abschnittes des zweiten Teiles, betitelt „Von der unbestimmten Analytik" (*opera omnia series I, vol. 1*, p. 326ff.), den Vorreden zu den vier rein arithmetischen Bänden hinzuzufügen.

Zunächst sei ein kleines Versehen EULERS aus einem früheren Teil, das vom Herausgeber übersehen worden ist, hier korrigiert. In § 188 des ersten Abschnittes des zweiten Teiles (l. c. p. 296) gibt EULER als Beispiel eines Falles der Cardanischen Formel, wo sich die Kubikwurzel nicht rational ausziehen läßt, folgende Gleichung an: $x^3 = 6x + 4$ mit den Wurzeln

$$x = \sqrt[3]{(2 + 2\sqrt{-1})} + \sqrt[3]{(2 - 2\sqrt{-1})} \ .$$

Man findet jedoch leicht, daß $x = -2$ eine Wurzel der Gleichung ist und daß sich die Kubikwurzeln ausziehen lassen. Sie ergeben $-1 \pm \sqrt{-1}$.

Wir wollen noch auf einige Eigentümlichkeiten, welche sich aus der uns ungewohnten schriftstellerischen Form ergeben, hinweisen. Vor allem ist eine gewisse Lässigkeit in der Ausdrucksweise festzustellen. So sagt EULER im § 169: Wenn die komplexen Faktoren $x \pm iy$ von $x^2 + y^2$ keine Faktoren haben, so hat auch ihr Produkt, nämlich $x^2 + y^2$, keine Faktoren. Dies würde aber heißen: wenn eine zusammengesetzte Zahl Summe zweier Quadrate ist, so sind es auch ihre Faktoren. Daß dies nicht selbstverständlich ist, weiß EULER sehr wohl, denn gerade am Beweis dieses Satzes hat er jahrelang gearbeitet. Ähnlich heißt es im § 191: Wenn $x^2 + cy^2$ ein Kubus ist, so muß auch $x \pm y\sqrt{-c}$ ein Kubus sein, was nicht stimmt. In Wirklichkeit verwendet EULER jedoch den umge-

kehrten Satz: wenn $x + y\sqrt{-c}$ ein Kubus ist, so ist auch die Norm $x^2 + cy^2$ ein Kubus einer rationalen Zahl.

Wir haben schon oben bemerkt, daß EULER sich an Dilettanten wendet, daß er eigentlich eine „Anleitung zum Genuß der Eigenschaften der Zahlen" geben will. Der Leser soll selber Beispiele erfinden und sich darüber freuen, wenn er etwa nach EULERS Anleitung für die Gleichung $2 - x^3 = y^2$ außer der trivialen Lösung $x = 1$ und $y = 1$ noch die folgende findet: $x = -17/4$ und $y = 71/8$. Die Probleme sind durchwegs sorgfältig ausgewählt, oft widerlegt das nächste Beispiel Vermutungen, welche das vorherige erregt. Auf diesem Weg ist EULER selber bei seinen Entdeckungen vorgegangen und dadurch ist es ihm vor allem gelungen, die allgemeine Struktur einer Theorie der binären Formen zu finden. Diese Lehre steht im Hintergrund der meisten Beispiele und EULER hat sich sein ganzes Leben damit beschäftigt. Im Brief vom 28. August 1742 schreibt er darüber an GOLDBACH: „Ich glaube fest, daß ich diese Materie bei weitem noch nicht erschöpft habe, sondern daß sich darin noch unzählig viele herrliche *proprietates numerorum* entdecken lassen." Und doch war ihm damals schon die wichtigste Eigenschaft der quadratischen Formen, freilich ohne Beweis, bekannt, daß die durch Formen der Diskriminante D darstellbaren Primzahlen in gewissen Restklassen (mod. D) liegen.

Wir wenden uns nun zu einer kurzen Besprechung der Untersuchungen. Zunächst werden lineare Gleichungen mit zwei Unbekannten behandelt und ihre Lösung wird auf den Euklidischen Algorithmus zurückgeführt. Einige Bemerkungen über mehrere lineare Gleichungen mit mehreren Unbekannten und ihre Lösung nach der sogenannten Regel COECI folgen. Im dritten Kapitel wird die Auflösung bilinearer Gleichungen mit zwei Variabeln gegeben, die keine Schwierigkeit bietet. Es sei auf die Winke zum Kongruenzkalkül in § 35 hingewiesen.

Kapitel 4 enthält das Problem, die quadratische Funktion $a + bx + cx^2$ durch rationale Werte von x zu einem Quadrat zu machen. Es ist identisch mit der Lösung folgender ternären Gleichung: $ax^2 + bxy + cy^2 = z^2$. Nach LEGENDRE genügt es, daß diese Gleichung *modulo* der Teiler der Diskriminante $D = b^2 - 4ac$ lösbar ist. Aber diesen Satz kannten weder EULER noch LAGRANGE. EULER setzt voraus, daß eine Lösung bekannt ist, und leitet hieraus die allgemeine Lösung her. Es sei die Funktion gegeben: $a + bx + f^2x^2$. Man soll alle Werte von x finden, für die sie zu einem Quadrat wird. EULER setzt sie $= (fx + m/n)^2$ und erhält eine in x lineare Gleichung, welche offenbar das Problem vollständig löst. Die Formel, welche EULER so auf wenigen Zeilen gewinnt (§ 46), lautet, homogen gemacht:

$$(fm^2 - bmn + afn^2)^2 = aM^2 + bMN + f^2N^2,$$

wo

$$M = bn^2 - 2fmn \quad \text{und} \quad N = m^2 - an^2.$$

Um sie zu beurteilen, polarisiere man die Substitution und man erhält:

$$(fx^2 - bxy + afy^2)\ (fx'^2 - bx'y' + afy'^2) = ax''^2 + bx''y'' + f^2y''^2\ ,$$

wo

$$x'' = byy' - f(xy' + yx') \quad \text{und} \quad y'' = xx' - ayy'\ .$$

Es handelt sich also um einen Spezialfall einer Kompositionsformel, welche GAUSS als eine Duplikation bezeichnet hat. Die Form $fm^2 - bmn + afn^2$ ist nur scheinbar speziell, denn man kann zeigen, daß jede Formenklasse Formen dieser Gestalt, also mit den Koeffizienten f, $-b$, af enthält, wobei man sogar f als Primzahl annehmen darf. Allgemeine Kompositionsformeln hat EULER folgende gekannt: die Komposition einer Hauptform $x^2 - ay^2$ mit $x'^2 - ay'^2$, ferner die Komposition einer beliebigen Form mit der zugehörigen Hauptform, alsdann die Komposition einer Form mit sich selbst im Sinne einer Normbildung, so daß die zugehörige Hauptform herauskommt. Schließlich noch einige weitere Formeln, von denen die interessanteste die folgende ist (in den *adversarii mathematici* Band 1 pg. 130 = *adv. math.* Band III p. 182, abgedruckt in „*Fragmenta arithmetica ex Adversariis mathematicis depromta*", *Opera postuma*, 1, 1862, p. 160 und 159): Es gilt

$$(abpp + cdqq)\ (acrr + bdss) = bcxx + adyy\ ,$$

wenn man x und y durch die Bilinearformen in p, q und r, s ersetzt:

$$x = apr + dqs \quad \text{und} \quad y = bps - cqr\ .$$

Das heißt: zwei Formen mit fehlendem mittlerem Term und derselben Diskriminante lassen sich stets komponieren und ergeben wiederum eine Form derselben Diskriminante.

Eine weitere Methode das Problem zu behandeln gibt EULER in § 54. Wenn sich die quadratische Funktion in die Gestalt überführen läßt: $p^2 + qr$, wo p, q, r Funktionen ersten Grades in x sind, so kann man setzen:

$$p^2 + qr = (p + sq)^2\ ,$$

wo s eine rationale Zahl ist. Hier hebt sich p^2 weg und man erhält: $r = 2ps + s^2q$, also eine lineare Gleichung für x, das in r, p und q steckt, bei freiem s. Das Problem ist also auch hier vollständig gelöst. Eine Verallgemeinerung auf biquadratische Funktionen bildet den Gegenstand der späteren Abhandlung 778, welche im vorliegenden Bande abgedruckt ist.

Das 5. Kapitel behandelt Fälle von quadratischen Formen, die keine Quadrate darstellen. EULER benutzt dazu die Methode der Reste nach Primzahlen. Wenn nämlich eine Form ein Quadrat darstellt, so muß sie auch *modulo* jeder Primzahl, die zu diesem Quadrat

prim ist, einen quadratischen Rest darstellen. Kann man also eine Form finden, welche z. B. modulo 3 nur die Reste 0 oder 2, niemals aber 1 liefert, so kann sie keine Quadrate darstellen. Eine solche Form ist z. B. $3x^2 + 2y^2$, sowie alle Formen, welche dieser Form modulo 3 kongruent sind, also z. B. $3x^2 + 5y^2$. In ähnlicher Weise benutzt EULER den Modul 8 und den Modul 5, schließlich den Modul 7 (§ 75).

Kapitel 6 greift das Problem an, ganze Zahlen zu finden, welche $ax^2 + b$ zu einem Quadrat machen, wobei auch a und b als ganzzahlig angenommen werden. Es handelt sich also um die Frage, ob die Form $y^2 - ax^2$ die ganze Zahl b ganzzahlig darstellt. Auch hier wird nur gezeigt, wie man aus einer schon gefundenen Darstellung unendlich viele neue gewinnen kann; dies geschieht mit Hilfe einer Komposition der Form, die hier die Hauptform ist, mit sich selber:

$$y^2 - ax^2 = (g^2 - af^2)\ (m^2 - an^2)\,,$$

wobei

$$x = fm + gn \quad \text{und} \quad y = gm + afn$$

ist. Diese Methode gibt freilich nicht alle Darstellungen von b aus der einen Gegebenen, falls b eine zusammengesetzte Zahl ist. Denn algebraisch gesprochen lautet das Problem: b soll Norm einer ganzen Zahl des Körpers $k(\sqrt{a})$ sein, EULER zeigt dagegen bloß, daß die Norm nicht verändert wird, wenn man eine Körperzahl mit einer Einheit multipliziert. Die Zahl b kann jedoch Norm einer endlichen Anzahl von algebraischen Zahlen sein, welche sich nicht um eine Einheit unterscheiden.

In § 92 wird auch der allgemeinere Fall, wo das Glied mit x vorkommt, behandelt, aber in einer andern Wendung, indem die Methode von § 46 (Kap. 4), die oben besprochen worden ist, wieder verwendet wird, ohne daß EULER darauf hinweist. Setzen wir nämlich in jenen Gleichungen $N = 1$, so geben sie eine Lösung der Gleichung $ax^2 + bx + c = y^2$. Wir haben dort bloß M durch x zu bezeichnen. Die Lösung der Gleichung $N = 1$ ist identisch mit der Lösung der PELLSCHEN Gleichung $m^2 - an^2 = 1$. Hat man m und n gefunden, so ergibt sich damit ein Wert für M, der jetzt mit x bezeichnet ist und welcher der Funktion einen ganzzahligen quadratischen Wert erteilt. Gerade dies ist aber der Inhalt unseres Paragraphen 92. Es wird vorausgesetzt, daß $ax^2 + bx + c$ für $x = f$ ein Quadrat wird. Führt man $x + f$ an Stelle von x in der Funktion ein, so wird eine Funktion entstehen, welche für c einen quadratischen Wert g^2 liefert. Setzt man nun in den Formeln von § 92 $f = 0$ und $c = g^2$, so erhält man die Formeln von § 46 wieder. Die Paragraphen 94 und 95 enthalten zwei Algorithmen, welche im wesentlichen der Potenzbildung einer Einheit des Zahlkörpers $k(\sqrt{a})$ entsprechen.

Das 7. Kapitel gibt die Methode zur Lösung der PELLSCHEN Gleichung und eine Tabelle der Lösungen für a von 2 bis 99. EULER hat in der Abhandlung 323: *De usu*

novi algorithmi in Problemate Pelliano solvendo (*opera omnia* I 3 p. 73) das Problem einer eingehenden Untersuchung unterworfen. Eine dort noch vorhandene Lücke hat E. GALOIS in seiner ersten Abhandlung *Démonstration d'un théorème sur les fractions continues périodiques* (Annales de Mathématiques de Gergonne, tome 19, p. 294; œuvres 1897 p. 1) in elegantester Weise ausgefüllt. Den ersten vollständigen Beweis gab LAGRANGE. Wir verweisen auf dessen Bemerkungen in den additions, die im Bande I 1 dieser Werke EULERS abgedruckt sind, insbesondere auf p. 631.

Die Kapitel 8—10 enthalten reizvolle Probleme, die nach einheitlicher, im Prinzip auf DIOPHANT zurückgehender Methode behandelt werden. Man nimmt wieder an, daß eine Lösung des Problemes bekannt ist und findet daraus eine neue. Wenn es gut geht, so erhält man aus dieser zweiten Lösung durch Anwendung derselben Methode eine dritte usw. Doch kann es auch vorkommen, daß die dritte mit der ersten übereinstimmt. Als Beispiel geben wir folgendes: Es soll die kubische Funktion $f^2 + bx + cx^2 + dx^3$ ein Quadrat werden. Dies geschieht für $x = 0$. Nun setze man die Funktion

$$= (f + gx)^2, \quad \text{wo} \quad g = b/2f$$

ist. Alsdann heben sich die beiden ersten Terme weg und man erhält als neue Lösung: $x = \frac{b^2 - 4cf^2}{4df^2}$. Das Verfahren versagt bloß, wenn $f^2 + bx + cx^2$ mit dem Quadrat auf der rechten Seite identisch wird. Diese Methode wird auf mannigfaltige Weise ausgebaut und durch interessante Beispiele erläutert. Ist die Funktion vom 4. Grade, so setzt man sie dem Quadrat einer Funktion zweiten Grades gleich und man kann nun, da drei Koeffizienten zur Verfügung stehen, die drei ersten Terme zum Verschwinden bringen. Man kommt wieder zu einer Gleichung ersten Grades in x, und diese liefert im allgemeinen eine neue Lösung.

Im 11. Kapitel kehrt EULER zu den quadratischen Formen zurück und behandelt ihre Zerlegung in Faktoren. Die Multiplikation der algebraischen Zahlen liefert nun unmittelbar die Komposition der Hauptform $x^2 + cy^2$. Aber auch die Nebenformen $ax^2 + cy^2$ lassen sich in die Faktoren $x\sqrt{a} \pm y\sqrt{-c}$ zerlegen und hieraus ergibt sich eine Komposition von der Art (§ 178):

$$(ap^2 + cq^2)\ (r^2 + acs^2) = a(pr - cqs)^2 + c(qr + aps)^2,$$

sowie diese

$$(ap^2 + cq^2)\ (ar^2 + cs^2) = (apr + cqs)^2 + ac(ps - qr)^2.$$

Letztere ist keine Duplikation im Sinne des 4. Kapitels, sondern eine Normbildung, da sie auf die Hauptform führt. Bei den quadratischen Formen verschmelzen eben konjugierte Idealklassen zu einer Formenklasse.

Im 12. Kapitel wird diese Zerlegung verwendet, um beliebige Potenzen durch Formen der Art $ax^2 + cy^2$ darzustellen. Man beachte das interessante Beispiel in § 196, ferner den Beweis (§ 193), daß die Gleichung $x^2 + 2 = y^3$ nur die eine ganzzahlige Lösung besitzt: $x = 5$, $y = 3$.

In den folgenden Kapiteln schickt sich EULER zu einem höheren Flug an. Zunächst, im Kapitel 13, bringt er einen schönen Beweis der FERMATSCHEN Vermutung für den Exponenten 4, daß nämlich die Summe zweier von 0 verschiedener Biquadrate kein Quadrat sein kann. Der Beweis geschieht durch eine descente indéfinie. Hierauf wird das nämliche für die Differenz zweier Biquadrate gezeigt. In § 211 wird dagegen bewiesen, daß $x^4 - 2y^4$ Quadrate darstellt. Ferner wird die Beziehung des letzteren Problems mit dem Falle $2x^4 - y^4$, der schon im § 140 behandelt worden war, aufgedeckt.

Das 14. Kapitel enthält 19 Aufgaben aller Art aus dem Gebiet der DIOPHANTISCHEN Analysis. Ein Teil derselben steht schon bei DIOPHANT. So findet sich die 5. Aufgabe (§ 219): Man soll eine Summe von zwei Quadraten auf beliebig viele Arten als Summe zweier anderer Quadrate darstellen, im zweiten Buche von DIOPHANT als 9. Problem. Ferner stehen die Aufgaben 12—14 (§ 231—233) bei DIOPHANT in III 10, IV 19 und 20, schließlich ist die 18. Aufgabe (§ 239), man solle gleichzeitig $x^2 + y$ und $y^2 + x$ zu Quadraten machen, identisch mit der Aufgabe II 20 bei DIOPHANT. Die mühevolle Aufgabe, DIOPHANTS, FERMATS und EULERS Leistungen auf diesem Gebiet zu ordnen und klar darzulegen, hat T. L. HEATH in einem Buch (*Diophantus of Alexandria. A study in the history of greek algebra.* Second edition. With a supplement containing an account of FERMAT'S theorems and problems connected with Diophantine analysis and some solutions of Diophantine problems by EULER, Cambridge 1910) in vorbildlicher Weise gelöst. Die Leser unserer Tage werden sich dieses Werkes mit großem Gewinn bedienen. Im einzelnen verweisen wir auf die Paragraphen 225—230, wo das Problem behandelt wird: Es sollen die beiden Formen $p^2 + azq^2$ und $p^2 + bzq^2$ gleichzeitig zu Quadraten werden, wobei a und b gegeben, p, q und z dagegen gesucht sind. Insbesondere wird gezeigt, daß die beiden Formen $p^2 + q^2$ und $p^2 + 3q^2$ niemals gleichzeitig Quadrate werden können, falls q von 0 verschieden ist (vgl. p. XII dieses Vorwortes). Der oben erwähnte Paragraph 231 enthält die simultane Rationalisierung von $\sqrt{xy+1}$, $\sqrt{yz+1}$, $\sqrt{zx+1}$ mit Hilfe der Formeln

$$x = \frac{p^2-1}{z}, \quad y = \frac{q^2-1}{z}, \quad z = \frac{(p^2-1)(q^2-1)-r^2}{2r}.$$

Die 19. Aufgabe (§ 240), man solle zwei Zahlen finden, deren Summe ein Quadrat, die Summe der Quadrate aber ein Biquadrat ist, hat EULER auch in Abhandlungen behandelt, vgl. *opera omnia* I 3 p. 96 und I 5 p. 67.

Im letzten Kapitel 15 löst EULER das FERMATSCHE Problem für den Exponenten 3. Ferner gibt er die allgemeine Lösung für die Gleichung $x^3 + y^3 + z^3 = t^3$, ein Problem, das er schon in der 1754 verfaßten und 1761 veröffentlichten Abhandlung 255 (*Opera omnia* I 2, p. 428) behandelt hatte und für dessen Besprechung wir auf RUDIO'S Anmerkungen und auf das Vorwort jenes Bandes hinweisen. Schließlich werden solche spezielle Lösungen dieser Gleichung gefunden, bei denen x, y, z eine arithmetische Reihe mit der Differenz 1 bilden. Bekanntlich gilt $3^3 + 4^3 + 5^3 = 6^3$.

LAGRANGE hat der französischen Übersetzung von EULERS Algebra einen Anhang beigegeben, der in unserer Ausgabe abgedruckt wurde. So inhaltsreich er an sich ist, so paßt er doch schlecht zum Vorhergehenden. LAGRANGE spricht in seiner Vorrede von einem „traité" und von „méthodique", während man EULERS Werk am ehesten als ein Schatzkästlein im HEBELSCHEN Sinne bezeichnen könnte. Wie ein Lehrbuch der Zahlentheorie nach EULER aussehen würde, kann man im vorliegenden Bande p. 182 ersehen, aber dies ist doch etwas ganz anderes, als die „Algebra". In Wahrheit sind LAGRANGE'S Additions Akademieabhandlungen im Anschluß an EULERS Arbeiten, etwa an die oben zitierte Nummer 323 von ENESTROEMS Verzeichnis. Man vermeide also eine Konfrontation der beiden Werke; im Grunde sind sie einander fremd, ähnlich wie die an sich wertvollen Zusätze gegenüber dem Urtext von JACOB BURCKHARDTS Cicerone.

INDEX

Insunt in hoc volumine indicis ENESTROEMIANI commentationes

748, 753, 754, 755, 758, 763, 764, 769, 772, 773, 774, 775, 776, 777, 778, 792, 793, 796, 797, 798, 799

pag.

748. Investigatio quadrilateri, in quo singulorum angulorum sinus datam inter se teneant rationem, ubi artificia prorsus singularia in Analysi DIOPHANTEA occurrunt 1
Mémoires de l'académie des sciences de St-Pétersbourg 5 (1812), 1815, p. 73—95

753. Solutio succincta et elegans problematis, quo quaeruntur tres numeri tales, ut tam summae quam differentiae binorum sint quadrata 20
Mémoires de l'académie des sciences de St-Pétersbourg 6 (1813/4), 1818, p. 54—65

754. Problème de géométrie résolu par l'analyse de DIOPHANTE 28
Mémoires de l'académie des sciences de St-Pétersbourg 7 (1815/6), 1820, p. 3—9

755. De casibus, quibus formulam $x^4 + mxxyy + y^4$ ad quadratum reducere licet 35
Mémoires de l'académie des sciences de St-Pétersbourg 7 (1815/6), 1820, p. 10—22

758. De binis formulis speciei $xx + myy$ et $xx + nyy$ inter se concordibus et discordibus 48
Mémoires de l'académie des sciences de St-Pétersbourg 8 (1817/8), 1822, p. 3—16

763. De tribus pluribusve numeris inveniendis, quorum summa sit quadratum, quadratorum vero summa biquadratum 61
Mémoires de l'académie des sciences de St-Pétersbourg 9 (1819/20), 1824, p. 3—13

764. Resolutio facilis quaestionis difficillimae, qua haec formula maxime generalis $vvzz(axx + byy)^2 + \triangle\, xxyy(avv + bzz)^2$ ad quadratum reduci postulatur 71
Mémoires de l'académie des sciences de St-Pétersbourg 9 (1819/20), 1824, p. 14—19

pag.

769. Solutio problematis FERMATIANI de duobus numeris, quorum summa sit quadratum, quadratorum vero summa biquadratum, ad mentem illustris LA GRANGE adornata 77
Mémoires de l'académie des sciences de St-Pétersbourg **10** (1821/2), 1826, p. 3—6

772. De insigni promotione Analysis DIOPHANTAEAE 82
Mémoires de l'académie des sciences de St-Pétersbourg 11, 1830, p. 1—11

773. Solutio problematis difficillimi, quo hae duae formulae $aaxx + bbyy$ et $aayy + bbxx$ quadrata reddi debent 94
Mémoires de l'académie des sciences de St-Pétersbourg **11**, 1830, p. 12—30

774. Investigatio binorum numerorum formae $xy(x^4 - y^4)$, quorum productum sive quotus sit quadratum 116
Mémoires de l'académie des sciences de St-Pétersbourg **11**, 1830, p. 31—45

775. De binis numeris, quorum summa sive aucta sive minuta tam unius quam alterius quadrato producat quadrata 131
Mémoires de l'académie des sciences de St-Pétersbourg **11**, 1830, p. 46—48

776. Dilucidationes circa binas summas duorum biquadratorum inter se aequales 135
Mémoires de l'académie des sciences de St-Pétersbourg, **11**, 1830, p. 49—57

777. De resolutione huius aequationis

$$0 = a + bx + cy + dxx + exy + fyy + gxxy + hxyy + ixxyy$$

per numeros rationales 146
Mémoires de l'académie des sciences de St-Pétersbourg **11**, 1830, p. 58—68

778. Methodus nova et facilis formulas cubicas et biquadraticas ad quadratum reducendi 157
Mémoires de l'académie des sciences de St-Pétersbourg **11**, 1830, p. 69—91

792. Tractatus de numerorum doctrina capita sedecim, quae supersunt 182
Commentationes arithmeticae **2**, 1849, p. 503—575

pag.

793. Considerationes circa Analysin DIOPHANTEAM 284
Commentationes arithmeticae 2, 1849, p. 576—587

796. Recherches sur le problème de trois nombres carrés tels que la somme de deux quelconques moins le troisième fasse un nombre carré 303
Commentationes arithmeticae 2, 1849, p. 603—616

Solution d'un problème assez curieux, savoir: trouver quatre nombres positifs et inégaux entr'eux tels que la somme de deux soit toujours un carré 330
Manuscriptum academiae scientiarum Petropolitanae relictum. Prima editio

Supplément au problème de quatre nombres, dont la somme de deux fassent toujours un nombre carré 337
Manuscriptum academiae scientiarum Petropolitanae relictum. Prima editio

797. Recherches ultérieures et très curieuses sur le problème de quatre nombres positifs et en proportion arithmétique tels que la somme de deux quelconques soit toujours un nombre carré 340
Commentationes arithmeticae 2, 1849, p. 617—625

798. De numeris amicabilibus 353
Commentationes arithmeticae 2, 1849, p. 627—636

799. Fragmenta commentationis cuiusdam maioris, de invenienda relatione inter latera triangulorum, quorum area rationaliter exprimi possit, et de triangulo, in quo rectae ex singulis angulis latera opposita bisecantes sint rationales 366
Commentationes arithmeticae 2, 1849, p. 648—651

Index nominum 371

INVESTIGATIO QUADRILATERI IN QUO SINGULORUM ANGULORUM SINUS DATAM INTER SE TENEANT RATIONEM UBI ARTIFICIA PRORSUS SINGULARIA IN ANALYSI DIOPHANTEA OCCURRUNT

Commentatio 748 indicis Enestroemiani
Mémoires de l'académie des sciences de St-Pétersbourg 5 (1812), 1815, p. 73—95
Conventui exhibita die 1. maii 1780

1. Sint p, q, r, s anguli quadrilateri quaesiti, quorum sinus eandem inter se teneant rationem quam isti numeri dati: a, b, c, d. Iam quia summa horum quatuor angulorum aequatur quatuor rectis, inde statim deducimus has tres aequationes:

$$\text{I.}\quad \sin.(p+q) + \sin.(r+s) = 0\,,$$
$$\text{II.}\quad \sin.(p+r) + \sin.(q+s) = 0\,,$$
$$\text{III.}\quad \sin.(p+s) + \sin.(q+r) = 0\,,$$

quarum quidem quaelibet binas reliquas in se complectitur; interim tamen plurimum iuvabit omnes tres considerasse, cum inde solutio multo simplicior et elegantior derivari queat.

2. Nunc istorum angulorum tam sinus quam cosinus sequenti modo designemus:

$$\sin. p = ax\,,\quad \cos. p = \sqrt{1 - aaxx} = A\,,$$
$$\sin. q = bx\,,\quad \cos. q = \sqrt{1 - bbxx} = B\,,$$
$$\sin. r = cx\,,\quad \cos. r = \sqrt{1 - ccxx} = C\,,$$
$$\sin. s = dx\,,\quad \cos. s = \sqrt{1 - ddxx} = D\,,$$

et iam totum negotium eo redit, ut quantitas x rite determinetur. Hinc igitur erit

$$\sin.(p+q) = axB + bxA\,,$$
$$\sin.(r+s) = cxD + dxC\,,$$

unde prima aequatio statim induet hanc formam:

$$aB + bA + cD + dC = 0 .$$

Hinc quidem secundum praecepta Algebrae formulae radicales A, B, C, D quadrata continuo sumendo successive eliminari possent; verum hoc modo non solum ad aequationem maxime complicatam perveniretur, sed etiam signa harum formularum radicalium nullo amplius modo innotescerent, quo ipso tota solutio nimis prodiret ambigua et incerta. Quamobrem longe aliam viam sum initurus, qua istud incommodum penitus evitabitur, simulque solutio satis concinna et elegans eruetur.

3. Ternae ergo aequationes initio memoratae istis denominationibus adhibitis sequentes nobis suppeditabunt aequationes:

$$\begin{aligned} &\text{I.} \quad aB + bA + cD + dC = 0 , \\ &\text{II.} \quad bC + cB + dA + aD = 0 , \\ &\text{III.} \quad dB + bD + cA + aC = 0 , \end{aligned}$$

unde iam facile intelligitur rationes inter binas litterarum maiuscularum definiri posse, quod commodissime fit per hanc combinationem generalem:

$$\text{I. } \lambda + \text{II. } \mu + \text{III. } \nu = 0 .$$

4. Ut ergo hinc littera D extirpetur, fieri debet

$$\lambda c + \mu a + \nu b = 0 .$$

At vero littera C elidetur, sumendo

$$\lambda d + \mu b + \nu a = 0 .$$

Harum iam duarum aequationum, si posterior per b multiplicat a apriore in a ducta auferatur, ut littera ν extirpetur, prodibit ista aequatio:

$$\lambda(ac - bd) + \mu(aa - bb) = 0 ,$$

unde erit

$$\frac{\lambda}{\mu} = \frac{aa - bb}{bd - ac} .$$

Et quia hic tantum ratio in computum venit, sumamus

$$\lambda = aa - bb \quad \text{et} \quad \mu = bd - ac\,,$$

quibus valoribus in altera postremarum aequationum substitutis prodit

$$\nu = bc - ad\,.$$

5. Surrogemus nunc istos valores in aequatione assumta

$$\text{I. } \lambda + \text{II. } \mu + \text{III. } \nu = 0\,,$$

et quoniam ambae litterae C et D ex calculo expelluntur, littera A iam factorem habebit $\lambda b + \mu d + \nu c$, qui induit hanc formam:

$$-b^3 + b(aa + cc + dd) - 2acd\,.$$

At vero littera B factorem habebit $\lambda a + \mu c + \nu d$ sive

$$a^3 - a(bb + cc + dd) + 2bcd\,.$$

Hinc igitur istam deducimus rationem:

$$\frac{A}{B} = \frac{a^3 - a(bb + cc + dd) + 2bcd}{b^3 - b(aa + cc + dd) + 2acd}\,,$$

atque ex hac forma facile concluditur fore simili modo

$$\frac{A}{C} = \frac{a^3 - a(bb + cc + dd) + 2bcd}{c^3 - c(aa + bb + dd) + 2abd}\,,$$

$$\frac{A}{D} = \frac{a^3 - a(bb + cc + dd) + 2bcd}{d^3 - d(aa + bb + cc) + 2abc}\,.$$

6. His formulis inventis ponamus brevitatis gratia

$$\begin{aligned}
\alpha &= a^3 - a(bb + cc + dd) + 2bcd\,,\\
\beta &= b^3 - b(aa + cc + dd) + 2acd\,,\\
\gamma &= c^3 - c(aa + bb + dd) + 2abd\,,\\
\delta &= d^3 - d(aa + bb + cc) + 2abc\,,
\end{aligned}$$

ita ut sit

$$\frac{A}{B} = \frac{\alpha}{\beta}\,,\ \frac{A}{C} = \frac{\alpha}{\gamma}\,,\ \frac{A}{D} = \frac{\alpha}{\delta}\,;$$

unde intelligimus nostrorum angulorum cosinus A, B, C, D eandem inter se tenere rationem, quam habent isti numeri α, β, γ, δ, qui ex numeris datis a, b, c, d facile formantur. Ex quo manifestum est, si ratio cosinuum singulorum angulorum p, q, r, s loco sinuum esset praescripta, hac methodo etiam non difficulter solutionem inveniri posse.

7. Quoniam igitur cosinus angulorum proportionales sunt litteris $\alpha, \beta, \gamma, \delta$, statuamus cos. $p = \alpha y$, cos. $q = \beta y$, cos. $r = \gamma y$, cos. $s = \delta y$; sicque totum negotium iam eo est reductum, ut valores binarum litterarum incognitarum x et y investigari debeat, ad quod has duas formulas in subsidium vocasse sufficiet:

$$\text{I.}\quad aaxx + \alpha\alpha yy = 1\,, \qquad \text{II.}\quad bbxx + \beta\beta yy = 1\,,$$

quarum differentia

$$(aa - bb)\,xx + (\alpha\alpha - \beta\beta)\,yy = 0$$

nos perduceret ad relationem inter x et y; at vero potius inde investigemus seorsim tam xx quam yy. Primo igitur ab aequatione posteriore ducta in $\alpha\alpha$ prior ducta in $\beta\beta$ subtrahatur, et obtinebimus hanc aequationem:

$$(\alpha\alpha bb - \beta\beta aa)\,xx = \alpha\alpha - \beta\beta\,^{1})\,.$$

Contra autem prior per bb, posterior vero per aa multiplicata, dat

$$(\alpha\alpha bb - \beta\beta aa)\,yy = bb - aa\,.$$

8. Incipiamus ab hac postrema aequatione, quae per factores ita repraesentetur:

$$(\alpha b + \beta a)\,(\alpha b - \beta a)\,yy = (b + a)\,(b - a)\,,$$

et iam substitutis pro α et β valoribus supra datis erit

$$\alpha b + \beta a = 2cd\,(aa + bb) - 2ab\,(cc + dd)$$

sive

$$\alpha b + \beta a = 2\,(ac - bd)\,(ad - bc)\,.$$

Porro vero erit

$$\alpha b - \beta a = 2\,(ab - cd)\,(aa - bb)\,,$$

consequenter

$$yy = \frac{1}{4\,(ac - bd)\,(bc - ad)\,(ab - cd)}\,.$$

1) Editio princeps: $\beta\beta - aa$. Correxit A. M.

9. Pro altera aequatione, qua xx determinatur, modo vidimus factorem membri eius sinistri esse

$$\alpha\alpha bb - \beta\beta aa = 4(bb - aa)(bc - ad)(ac - bd)(ab - cd).$$

At vero pro membro dextro $\alpha\alpha - \beta\beta$[1]) habebimus primo

$$\alpha + \beta = (a + b)(bb - 2ab + aa - cc + 2cd - dd)$$
$$= (a + b)\left((b - a)^2 - (c - d)^2\right) = (a + b)(b - a + c - d)(b - a - c + d).$$

Deinde vero erit

$$\alpha - \beta = (a - b)(bb + 2ab + aa - cc - 2cd - dd)$$
$$= (a - b)\left((b + a)^2 - (c + d)^2\right) = (a - b)(b + a + c + d)(b + a - c - d).$$

Quia nunc productum horum factorum membro sinistro aequatur, utrinque per $aa - bb$ dividendo obtinebimus

$$xx = \frac{(b + a + c + d)\ (b + a - c - d)\ (b - a + c - d)\ (b - a - c + d)}{4(ad - bc)\ (ac - bd)\ (ab - cd)};$$

hocque modo nostrum problema penitus est solutum, eiusque solutio ita se habet:

PROBLEMA

Si in quadrilatero sinus angulorum inter se teneant eandem rationem ut numeri dati a, b, c, d, ipsos angulos invenire.

SOLUTIO

10. Sint p, q, r, s anguli quaesiti ponanturque eorum sinus et cosinus:

$$\begin{aligned} \text{sin. } p &= ax, & \text{cos. } p &= \alpha y, \\ \text{sin. } q &= bx, & \text{cos. } q &= \beta y, \\ \text{sin. } r &= cx, & \text{cos. } r &= \gamma y, \\ \text{sin. } s &= dx, & \text{cos. } s &= \delta y, \end{aligned}$$

primo pro sinibus invenimus esse

$$xx = \frac{(a + b + c + d)\ (a + b - c - d)\ (a + c - b - d)\ (b + c - a - d)}{4(ab - cd)\ (ac - bd)\ (bc - ad)},$$

1) Editio princeps: $\beta\beta - aa$. Correxit A. M.

ubi singulos factores ita ordinavimus, ut cum ordine litterarum conveniant, scilicet, si horum numerorum maximus sit a et minimus d, in numeratore tres priores factores manifesto sunt positivi; quare, quo etiam quartus sit positivus, requiritur, ut quoque sit $b + c > a + d$. Simili modo in denominatore bini factores priores manifesto sunt positivi, unde etiam necesse est, ut pro tertio sit bc maius quam ad.

11. Pro cosinibus invenimus, eodem litterarum ordine observato, esse

$$yy = \frac{1}{4(ab-cd)\ (ac-bd)\ (bc-ad)}\ .$$

Praeterea vero invenimus

$$\alpha = a^3 - a\,(bb + cc + dd) + 2bcd\,,$$
$$\beta = b^3 - b\,(aa + cc + dd) + 2acd\,,$$
$$\gamma = c^3 - c\,(aa + bb + dd) + 2abd\,,$$
$$\delta = d^3 - d\,(aa + bb + cc) + 2abc\,.$$

Antequam autem has formulas ulterius perpendamus, nonnulla exempla evolvamus numeros a, b, c, d ita assumendo, ut a sit maximus et d minimus, summa mediorum autem $b + c$ maior quam $a + d$.

EXEMPLUM 1

12. Sit $a = 4, b = 3, c = 3$ et $d = 1$, atque ex his valoribus deducimus litteras $\alpha, \beta, \gamma, \delta$ hoc modo: $\alpha = 6$, $\beta = -27$, $\gamma = -27$, $\delta = 39$. Deinde vero prodit $x = \frac{\sqrt{11}}{6\sqrt{5}}$ et $y = \pm\frac{1}{18\sqrt{5}}$. Semper enim duae solutiones locum habent, quoniam, si summa quatuor angulorum fuerit 360°, summa complementorum eorundem etiam est 360°. Hinc ergo sinus et cosinus angulorum quaesitorum ipsique anguli erunt, ut haec tabula eos indicat:

$$\text{sin. } p = \frac{4\sqrt{11}}{6\sqrt{5}},\ \text{cos. } p = \pm\frac{1}{3\sqrt{5}},\ p = 81°, 25', 37'',$$
$$\text{sin. } q = \frac{3\sqrt{11}}{6\sqrt{5}},\ \text{cos. } q = \mp\frac{3}{2\sqrt{5}},\ q = 132\ ,\ 7\ ,\ 50\ ,$$
$$\text{sin. } r = \frac{3\sqrt{11}}{6\sqrt{5}},\ \text{cos. } r = \mp\frac{3}{2\sqrt{5}},\ r = 132\ ,\ 7\ ,\ 50\ ,$$
$$\text{sin. } s = \frac{\sqrt{11}}{6\sqrt{5}},\ \text{cos. } s = \pm\frac{13}{6\sqrt{5}},\ s = \begin{array}{r} 14\ ,\ 18\ ,\ 43\ , \\ \hline 360\ ,\ -\ ,\ -\ . \end{array}$$

EXEMPLUM 2

13. Sit $a = 8$, $b = 7$, $c = 6$, $d = 1$, eritque $\alpha = -92$, $\beta = -268$, $\gamma = -356$, $\delta = 524$. Porro vero erit $x = \sqrt{\frac{12 \cdot 22}{25 \cdot 41 \cdot 17}}$ et $y = \pm \sqrt{\frac{1}{4 \cdot 50 \cdot 41 \cdot 34}}$, sive

$$x = 0{,}1230880 \quad \text{et} \quad y = \pm 0{,}0018939,$$

$$l \sin. p = 9{,}9933055, \quad \text{angulus } p = 100°,\ 2',\ 4'',$$
$$l \sin. q = 9{,}9353135, \quad q = 120,\ 30,\ 6,$$
$$l \sin. r = 9{,}8683668, \quad r = 132,\ 23,\ 37,$$
$$l \sin. s = 9{,}0902155, \quad s = 7,\ 4,\ 13,\ ^{1})$$
$$360, —, —.$$

EXEMPLUM 3

14. Sit $a = 15$, $b = 14$, $c = 11$ et $d = 6$, eritque $\alpha = -72$, $\beta = -624$, $\gamma = -1176$, $\delta = +1584$. Porro fiet $xx = \frac{12 \cdot 46 \cdot 6 \cdot 4}{2^2 \cdot 12^2 \cdot 9^2 \cdot 8^2}$ et $yy = \frac{1}{2^2 \cdot 12^2 \cdot 9^2 \cdot 8^2}$ sive

$$y = \frac{1}{2 \cdot 12 \cdot 9 \cdot 8} = \frac{1}{1728} \quad \text{et} \quad x = \frac{\sqrt{23}}{72}.$$

Hinc ergo sinus et cosinus nostrorum angulorum et ipsi anguli erunt

$$\sin. p = \frac{5}{24}\sqrt{23}, \quad \cos p = -\frac{1}{24}, \quad p = 92°,\ 23',\ 16'',$$
$$\sin. q = \frac{7}{36}\sqrt{23}, \quad \cos. q = -\frac{13}{36}, \quad q = 111,\ 10,\ 6,$$
$$\sin. r = \frac{11}{72}\sqrt{23}, \quad \cos. r = -\frac{49}{72}, \quad r = 132,\ 53,\ 14,$$
$$\sin. s = \frac{1}{12}\sqrt{23}, \quad \cos. s = +\frac{11}{12}, \quad s = 23,\ 33,\ 24,$$
$$360, —, —.$$

Hoc exemplum ideo est notatu dignum, quod omnes cosinus prodierint rationales.

15. Quo autem indoles huius solutionis clarius perspiciatur, indagemus conditiones necessarias, ut anguli evadant reales; ubi quidem assumemus

1) Editio princeps: $p = 100^0\,2'\,1''$, $r = 132^0\,23'\,39''$, $s = 7^0\,4',14''$. Correxit R. F.

numerorum a, b, c, d primum a esse maximum, d vero minimum; tum vero esse $b > c$. Ac primo quidem constat, ut valor pro yy inventus prodeat positivus, quia bini factores $ab - cd$ et $ac - bd$ manifesto sunt nihilo maiores, necesse esse, ut factor $bc - ad$ etiam fiat positivus sive ut $bc > ad$. Praeterea vero, ut etiam valor ipsius xx fiat positivus, quoniam tres priores factores per se sunt nihilo maiores, res eo redit, ut ultimus factor $b + c - a - d$ quoque sit nihilo maior, hoc est $b + c > a + d$; verum hae duae conditiones ad solam posteriorem $b+c>a+d$ revocantur. Quoties enim fuerit $b+c>a+d$, semper quoque erit $bc > ad$, sed non vice versa. Ad hoc ostendendum ponamus $a = b + t$ et $c = d + u$, et, quia $b+c > a + d$, erit $u > t$; hinc, cum sit $bc = bd + bu$ et $ad = bd + dt$, horum valorum prior manifesto maior est posteriore, quia $b > d$ et $u > t$, ideoque $bu > dt$ et $bc > ad$.

16. Loco fractionis pro xx inventae scribamus brevitatis gratia $xx = \frac{v}{z}$, ita ut sit

$$v = (a + b + c + d)(a + b - c - d)(a + c - b - d)(b + c - a - d)$$

et

$$z = 4(ab - cd)(ac - bd)(bc - ad),$$

atque vidimus fore $yy = \frac{1}{z}$. Hinc ergo erit $\sin. p = a\sqrt{\frac{v}{z}}$ et $\cos. p = \frac{\alpha}{\sqrt{z}}$; unde sequitur fore $\frac{aav}{z} + \frac{\alpha\alpha}{z} = 1$, ideoque $z - aav = \alpha\alpha$, quo observato sequens problema DIOPHANTEUM resolvi poterit, cuius solutio alias satis ardua foret.

PROBLEMA DIOPHANTEUM

Propositis quatuor numeris quadratis aa, bb, cc, dd invenire duos numeros z et v, ut $z - aav$, $z - bbv$, $z - ccv$, $z - ddv$ fiant numeri quadrati.

SOLUTIO

17. Ex praecedentibus manifestum est huic problemati satisfactum iri sumendo

$$v = (a + b + c + d)(a + b - c - d)(a + c - b - d)(b + c - a - d)$$

et

$$z = (ab - cd)(ac - bd)(bc - ad),$$

quae solutio non solum ob simplicitatem summa attentione digna videtur, sed etiam imprimis ideo, quod per praecepta cognita Analyseos indeterminatae plerumque solutiones maxime intricatae reperirentur. Interim tamen etiam ista solutio ex hac ipsa Analysi satis commode sequenti modo erui potest.

18. Cum quatuor formulae praescriptae quadrata effici debeant, etiam earum productum erit quadratum, quod quo facilius referri queat, statuamus

$$aa + bb + cc + dd = P ;$$

tum vero

$$aabb + aacc + aadd + bbcc + bbdd + ccdd = Q ,$$
$$aabbcc + aabbdd + aaccdd + bbccdd = R ,$$

denique

$$abcd = S ,$$

hincque ipsum productum sequenti modo expressum reperitur:

$$z^4 - Pz^3v + Qzzvv - Rzv^3 + SSv^4 ;$$

quod ut quadratum reddatur, statuamus eius radicem

$$zz - \tfrac{1}{2}Pzv + Svv ,$$

cuius quadratum a producto illo ablatum relinquet

$$(Q - 2S - \tfrac{1}{4}PP)\, z = (R - PS)\, v \text{ [1]} ,$$

unde fit

$$\frac{v}{z} = \frac{Q - 2S - \frac{1}{4}PP}{R - PS} = \frac{4Q - 8S - PP}{4(R - PS)} .$$

19. Evolvamus seorsim tam numeratorem quam denominatorem; ac pro numeratore reperiemus:

$$4Q - 8S - PP = 2aabb + 2aacc + 2aadd + 2bbcc + 2bbdd + 2ccdd$$
$$- a^4 - b^4 - c^4 - d^4 - 8abcd , \text{ [2]}$$

quae expressio facile in sequentes factores resolvitur:

$$4Q - 8S - PP$$
$$= (a + b + c + d)(a + b - c - d)(a + c - b - d)(b + c - a - d) .$$

1) Editio princeps: $(Q - \frac{1}{4}PP)\, z = (R - PS)\, v$; hic error reperitur etiam in sequentibus formulis. Correxit A. M.

2) In editione principe $-8abcd$ deest. Correxit A. M.

Simili modo pro denominatore fiet

$$R - PS = aabbcc + aabbdd + aaccdd + bbccdd \\ - a^3bcd - ab^3cd - abc^3d - abcd^3 ,$$

quod resolvitur in hos factores:

$$R - PS = (ab - cd)(ac - bd)(bc - ad) ,$$

qui ergo valores cum solutione praecedente egregie conveniunt. Verum hinc plus non sequitur, nisi quod productum quatuor formularum propositarum sit quadratum, sicque adhuc dubium superesse potest, num etiam singulae formulae fiant quadrata.

20. Tertium exemplum ante allatum occasionem suppeditat conditiones investigandi, sub quibus valor pro yy inventus fiat quadratum, quamobrem adhuc istud problema adiungamus.

PROBLEMA DIOPHANTEUM

Quatuor numeros a, b, c, d, quorum a sit maximus et d minimus, tum vero $b+c>a+d$, ita determinare, ut tres istae formulae: 1°) $ab-cd$, 2°) $ac-bd$, 3°) $bc-ad$ *evadant numeri quadrati.*

SOLUTIO

21. Pro adimplendis binis prioribus conditionibus ponamus

$$ab - cd = xx \quad \text{et} \quad ac - bd = yy ,$$

hincque fiet $axx + dyy = b(aa - dd)$, tum vero $ayy + dxx = c(aa - dd)$, unde deducimus

$$b = \frac{axx + dyy}{aa - dd} \quad \text{et} \quad c = \frac{ayy + dxx}{aa - dd} .$$

His valoribus substitutis tertia conditio postulat, ut sit

$$\frac{(axx + dyy)(ayy + dxx)}{(aa - dd)^2} - ad = \square ,$$

id quod non adeo est facile.

22. Quo huic conditioni satisfaciamus, tractemus primo casum quo $x = y$, et facta multiplicatione per $(aa - dd)^2$ ista formula quadratum reddi debebit:

$$(a + d)^2 x^4 - ad(aa - dd)^2 = \square ,$$

quae per $(a + d)^2$ divisa dat

$$x^4 - ad(a - d)^2 = \square ;$$

haecque conditio adimplebitur, si statuamus $x = \frac{a+d}{2}$; sic enim prodit

$$a^4 + 4a^3d + 6aadd + 4ad^3 + d^4 - 16ad(a - d)^2 = \square ,$$

quod penitus evolutum praebet hanc formulam sponte quadratam:

$$a^4 - 12a^3d + 38aadd - 12ad^3 + d^4 = \square ,$$

cuius radix est $aa - 6ad + dd$.

23. Cum autem hoc casu fieret $b = c$, ut etiam alios casus hinc eruamus, statuamus $x = \frac{a+d+v}{2}$ et $y = \frac{a+d-v}{2}$, hincque reperietur

$$xx = \frac{(a + d)^2 + 2(a + d)v + vv}{4} ,$$

$$yy = \frac{(a + d)^2 - 2(a + d)v + vv}{4} ,$$

eritque primo

$$axx + dyy = \frac{(a + d)^3 + 2v(aa - dd) + (a + d)vv}{4} ,$$

$$ayy + dxx = \frac{(a + d)^3 - 2v(aa - dd) + (a + d)vv}{4} ,$$

quamobrem habebimus

$$b = \frac{(a + d)^2 + 2(a - d)v + vv}{4(a - d)} ,$$

$$c = \frac{(a + d)^2 - 2(a - d)v + vv}{4(a - d)} .$$

24. Nunc productum bc sequenti modo commode exprimetur:

$$bc = \frac{(a + d)^4 + 2(a + d)^2 vv + v^4 - 4(a - d)^2 vv}{16(a - d)^2}$$

sive

$$bc = \frac{(a + d)^4 - 2(aa - 6ad + dd)vv + v^4}{16(a - d)^2} .$$

Hinc igitur erit

$$bc - ad = \frac{(a+d)^4 - 2(aa - 6ad + dd)vv + v^4 - 16ad(a-d)^2}{16(a-d)^2},$$

unde quadratum fieri debet haec formula:

$$(aa - 6ad + dd)^2 - 2(aa - 6ad + dd)vv + v^4 = \square,$$

quod utique evenit; eius enim radix est $aa - 6ad + dd - vv$. Difficillimum autem foret solutionem indagare, nisi iam sponte pateret formam hanc esse quadratum, cum desint potestates impares.

25. Hinc ergo patet litteram v in calculum introductam penitus arbitrio nostro relinqui, unde licebit conditiones praescriptas penitus adimplere. Primo scilicet, cum sit $b + c = \frac{(a+d)^2 + vv}{2(a-d)}$, quae quantitas superare debet $a + d$, sequitur fore $v > \sqrt{a^2 - 2ad - 3dd}$, quae conditio primo est observanda. Praeterea vero, quia esse debet $a > b$, hinc deducimus hanc determinationem:

$$4a(a-d) > (a+d)^2 + 2(a-d)v + vv$$

sive $4a(a-2d) > (a-d+v)^2$, consequenter

$$v < 2\sqrt{a(a-2d)} - (a-d),$$

sicque habemus duos limites, intra quos valor ipsius v accipi debet; unde patet ante omnia requiri, ut sit $a > 2d$, quia alioquin conditionibus praescriptis satisfieri non liceret. Operae igitur pretium erit hanc solutionem aliquot exemplis illustrare.

EXEMPLUM 1

26. Sit $a = 3d$, et limites, intra quos v subsistere debet, erunt $v > 0$ et $v < 2d\sqrt{3} - 2d$ sive $v < 1{,}464 \cdot d$. Sumto igitur v intra hos limites erit

$$b = \frac{16dd + 4dv + vv}{8d} \quad \text{et} \quad c = \frac{16dd - 4dv + vv}{8d}.$$

Casus autem simplicissimus eruitur sumendo $v = d$, quo pacto fiet $b = \frac{21}{8}d$ et $c = \frac{13}{8}d$, sive posito $d = 8$ quatuor numeri quaesiti erunt:

$$a = 24, \quad b = 21, \quad c = 13, \quad d = 8.$$

Sumatur $v = \frac{1}{2}d$ sive $d = 2$ et $v = 1$ ideoque $a = 6$, eritque $b = \frac{73}{16}$ et $c = \frac{57}{16}$, unde per 16 multiplicando quatuor numeri quaesiti erunt

$$a = 96, \quad b = 73, \quad c = 57, \quad d = 32.$$

EXEMPLUM 2

27. Sumamus $a = \frac{5}{2}d$, sive, ut fractiones tollantur, sumatur $d = 2$ et $a = 5$, atque limites pro v erunt $vv > -7$, quod sponte evenit, et

$$v < 2\sqrt{5} - 3 < 1{,}472,$$

tum vero erit $b = \frac{49 + 6v + vv}{12}$ et $c = \frac{49 - 6v + vv}{12}$. Hic ergo iterum sumere licet $v = 1$, unde fit $b = \frac{14}{3}$ et $c = \frac{11}{3}$, et per 3 multiplicando quatuor numeri quaesiti erunt

$$a = 15, \quad b = 14, \quad c = 11, \quad d = 6,$$

quod est ipsum tertium exemplum supra allatum. Sumto autem $v = \frac{1}{2}$ fiet $b = \frac{209}{48}$ et $c = \frac{185}{48}$, hincque

$$a = 240, \quad b = 209, \quad c = 185, \quad d = 96.$$

EXEMPLUM 3

28. Sit $a = 4$ et $d = 1$, erit $b = \frac{25 + 6v + vv}{12}$ et $c = \frac{25 - 6v + vv}{12}$. At vero limites pro v erunt $v > \sqrt{5} > 2{,}236$ et $v < 4\sqrt{2} - 3 < 2{,}656$. Sumatur ergo $v = 2{,}5 = \frac{5}{2}$, eritque $b = \frac{185}{48}$ et $c = \frac{65}{48}$, ideoque quatuor numeri quaesiti erunt

$$a = 192, \quad b = 185, \quad c = 65, \quad d = 48.$$

ALIA SOLUTIO

29. Sumatur $d = 1$, ut sit $b = \frac{axx + yy}{aa - 1}$ et $c = \frac{ayy + xx}{aa - 1}$. Nunc pro

initio ponamus $x = 2y$, fietque $b = \frac{(4a+1)yy}{aa-1}$ et $c = \frac{(a+4)yy}{aa-1}$. Hinc formula $bc - a$, quae quadratum esse debet, induet hanc formam:

$$(4aa + 17a + 4)y^4 - a(aa-1)^2 = \square .$$

Quia autem hic a in posteriore membro ad quintam potestatem assurgit, statuamus $y = (a+1)z$, ut formula per $(a+1)^2$ dividi queat, ac reperietur

$$(a+1)^2(4aa + 17a + 4)z^4 - a(a-1)^2 = \square .$$

30. Videamus nunc, qualis forma sit proditura sumto $z = 1$, ac reperiemus hanc:

$$4a^4 + 24a^3 + 44aa + 24a + 4 = \square ,$$

quae per 4 divisa fit $a^4 + 6a^3 + 11aa + 6a + 1 = \square$, ubi praeter omnem expectationem evenit, ut ista formula revera sit quadratum, quippe cuius radix est $aa + 3a + 1$. Quare cum pro hoc casu sit $y = a + 1$, in sequentem usum notetur esse

$$(a+1)^4(4aa + 17a + 4) - a(aa-1)^2 = \square$$

eiusque radix

$$= 2(a+1)(aa + 3a + 1) .$$

31. Ut hinc solutionem magis generalem eruamus, statuamus

$$y = a + 1 - v \quad \text{et} \quad x = 2(a+1) - v ;$$

facile enim est praevidere facta substitutione prodituram esse formulam quarti gradus, cuius tam primus terminus quam ultimus fient quadratum, quae conditio in Analysi DIOPHANTEA maximi est momenti. Cum igitur hinc sit

$$xx = 4(a+1)^2 - 4(a+1)v + vv$$

et

$$yy = (a+1)^2 - 2(a+1)v + vv ,$$

fiet

$$axx + yy = (4a+1)(a+1)^2 - (4a+2)(a+1)v + (a+1)vv ,$$
$$ayy + xx = (a+4)(a+1)^2 - (2a+4)(a+1)v + (a+1)vv ,$$

quarum formarum productum dempto membro $a(aa-1)^2$ debet reddi quadratum. At vero illud productum reperitur, ut sequitur:

$$(4a+1)(a+4)(a+1)^4 - 12(aa+3a+1)(a+1)^3 v$$
$$+ (13aa+30a+13)(a+1)^2 vv - 6(a+1)^3 v^3 + (a+1)^2 v^4 ,$$

a quo iam subtrahi debet membrum posterius $a(aa-1)^2$, quod a primo membro sublatum relinquit, ut supra vidimus, quantitatem absolutam $4(aa+3a+1)^2(a+1)^2$; quamobrem tota formula per $(a+1)^2$ divisa evadet

$$4(aa+3a+1)^2 - 12(aa+3a+1)(a+1)v$$
$$+ (13aa+30a+13)vv - 6(a+1)v^3 + v^4 ,$$

quam formulam quadratum reddi oportet.

32. Hanc autem formulam accuratius perpendenti mirabili profecto casu patebit eam iam revera esse quadratum, quippe cuius radix deprehenditur esse

$$2(aa+3a+1) - 3(a+1)v + vv ;$$

quamobrem, cum haec formula iam sponte sua prodierit quadratum, quantitas v nulla determinatione indiget, sed penitus arbitrio nostro relinquitur. Hinc ergo sumtis binis litteris a et v pro lubitu, litterae b et c inde ita definiuntur, ut sit

$$b = \frac{(4a+1)(a+1) - (4a+2)v + vv}{a-1} ,$$
$$c = \frac{(a+4)(a+1) - (2a+4)v + vv}{a-1} ,$$

quo pacto formula $bc - a$, ut vidimus, sponte fit quadratum.

33. Nihil aliud igitur superest, nisi ut reliquis conditionibus praescriptis satisfiat, quibus postulatur: 1°) ut sit $b + c > a + 1$, 2°) ut sit $b < a$, 3°) ut sit $c < a$. Prima autem conditio praebet

$$5(a+1)^2 - 6(a+1)v + 2vv > aa - 1 ,$$

quae transmutatur in hanc:

$$9(a+1)^2 - 12(a+1)v + 4vv > aa - 2a - 3 ,$$

seu extracta radice

$$2v - 3(a+1) > \sqrt{(a+1)(a-3)}\ ^{1}) ,$$

ideoque

1) Valor membri sinistri signo positivo capiendus est. R. F.

$$v > \frac{3(a+1) \pm \sqrt{(a+1)\,(a-3)}}{2}\ ^{1}),$$

unde gemini limites concluduntur

$$1°)\ v > \frac{3(a+1) + \sqrt{(a+1)\,(a-3)}}{2},$$

$$2°)\ v < \frac{3(a+1) - \sqrt{(a+1)\,(a-3)}}{2}.$$

Soli ergo valores intra hos limites contenti excluduntur.

34. Secunda conditio, qua $b < a$, praebet

$$(4a+1)(a+1) - (4a+2)v + vv < aa - a,$$

quae transformatur in hanc:

$$(2a+1)^2 - 2(2a+1)v + vv < aa - 2a;$$

hinc radice extracta fiet $v < 2a + 1 \pm \sqrt{aa - 2a}$ [2]), unde iterum duo limites stabiliuntur, scilicet $v < 2a + 1 + \sqrt{aa - 2a}$ et $v > 2a + 1 - \sqrt{aa - 2a}$; unde sequitur valores ipsius v intra hos limites accipi debere.

35. Tertia conditio postulat, ut sit $c < a$, unde prodit

$$(a+4)(a+1) - (2a+4)v + vv < aa - a,$$

sive $(a+2)^2 - 2(a+2)v + vv < aa - 2a$, ideoque

$$v < a + 2 + \sqrt{aa - 2a} \quad \text{et} \quad v > a + 2 - \sqrt{aa - 2a}.$$

36. Quodsi hos limites inter se comparemus, statim patet eos adimpleri non posse, si capiatur $a < 2$; deinde vero, si $a = 2$, limites illi nullum intervallum inter se relinquunt; ex quo intelligitur solutionem locum habere non posse, nisi sit $a > 2$. Quoniam igitur $2a + 1$ semper maius erit quam $a + 2$, perspicuum est, dummodo fuerit $v < a + 2 + \sqrt{aa - 2a}$, tum quoque fore

$$v < 2a + 1 + \sqrt{aa - 2a},$$

1) $>$ pro signo superiore, $<$ pro signo inferiore locum habet. R. F.

2) $<$ pro signo superiore, $>$ pro signo inferiore locum habet. R. F.

unde iste limes est superfluus. Deinde, dummodo fuerit

$$v > 2a + 1 - \sqrt{aa - 2a},$$

multo magis erit

$$v > a + 2 - \sqrt{aa - 2a};$$

quamobrem duo tantum limites nobis relinquuntur, scilicet:

$$v > 2a + 1 - \sqrt{aa - 2a},$$

$$v < a + 2 + \sqrt{aa - 2a},$$

qui duo limites, quia nunquam in unum coalescere possunt, semper aliquod intervallum inter se relinquunt, intra quod valor ipsius v cadere debet. Praeterea vero necesse est, ut v extra binos limites supra inventos cadat, qui erant

$$v > \frac{3(a+1) + \sqrt{(a+1)\ (a-3)}}{2} \quad \text{aut}^1) \quad v < \frac{3(a+1) - \sqrt{(a+1)\ (a-3)}}{2},$$

quas conditiones aliquot exemplis illustremus.

EXEMPLUM 1

37. Existente $d = 1$ sumatur $a = 3$, eritque

$$b = \frac{52 - 14v + vv}{2} \quad \text{et} \quad c = \frac{28 - 10v + vv}{2}.$$

Nunc vero v cadere debet intra hos limites: $v > 7 - \sqrt{3}$ [et] $< 5 + \sqrt{3}$, sive $v > 5{,}268$ et $v < 6{,}732$. Praeterea vero esse debet vel $v > 6$ vel $v < 6$, quibus ergo satisfit, dum ne sit $v = 6$[2]). Sumamus ergo $v = 5\frac{1}{2} = \frac{11}{2}$, fietque $b = \frac{21}{8}$ et $c = \frac{13}{8}$. Multiplicando per 8 quatuor nostri numeri erunt $a = 24$, $b = 21$, $c = 13$, $d = 8$, quem casum iam supra invenimus, etiamsi haec methodus diversissima sit a praecedente solutione. Sumamus etiam $v = \frac{13}{2}$, erit $b = \frac{13}{8}$ et $c = \frac{21}{8}$, hincque $a = 24$, $b = 13$, $c = 21$, $d = 8$, qui casus praecedenti prorsus est similis, hoc solo discrimine, quod literae b et c sint permutatae.

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

2) EULERUS primo casu solum v tanquam numerum integrum considerat. Hoc casu erit $a = 3$, $b = c = 2$, $d = 1$. R. F.

EXEMPLUM 2

38. Sumatur $a = \frac{5}{2}$, eritque $b = \frac{77 - 24v + 2vv}{3}$ [1]) et $c = \frac{91 - 36v + 4vv}{6}$; tum vero limites, intra quos valor litterae v cadere debet, erunt $v > 6 - \frac{1}{2}\sqrt{5}$ et $v < \frac{9 + \sqrt{5}}{2}$ sive $v > 4{,}882$ et $v < 5{,}618$; limites vero, extra quos hic valor cadere debet, sunt imaginarii, qui ergo nullos plane valores excludunt. Sumamus igitur $v = 5$, eritque $b = \frac{7}{3}$ et $c = \frac{11}{6}$, unde nanciscimur hos valores: $a = 15$, $b = 14$, $c = 11$, $d = 6$, qui est iterum casus iam ante inventus.

EXEMPLUM 3

39. Sit $a = 4$, et prodibit $b = \frac{85 - 18v + vv}{3}$ et $c = \frac{40 - 12v + vv}{3}$. Limites, intra quos v sumi debet, hoc casu sunt $9 - \sqrt{8}$ et $6 + \sqrt{8}$ sive in decimalibus 6,17 et 8,83; cadere autem v debet extra limites 6,382 et 8,618. Unde intelligitur valorem ipsius v vel intra hos limites: 6,17 et 6,38 vel intra[2]) hos: 8,62 et 8,83 cadere debere. Sumamus pro prioribus $v = 6\frac{1}{4} = \frac{25}{4}$, ut sit $b = \frac{185}{48}$ et $c = \frac{65}{48}$, unde quatuor numeri erunt $a = 192$, $b = 185$, $c = 65$, $d = 48$, qui casus iterum convenit cum ultimo exempli tertii superioris solutionis.

40. Propter egregium consensum inter exempla, quae ex utraque solutione sunt deducta, summo iure suspicamur ambas solutiones prorsus inter se convenire; unde operae pretium erit istam convenientiam accuratius perscrutari. Cum igitur prima solutio dedisset

$$b = \frac{(a+1)^2 + 2(a-1)v + vv}{4(a-1)}\ [3]) \quad \text{et} \quad c = \frac{(a+1)^2 - 2(a-1)v + vv}{4(a-1)},$$

in posteriore loco v scribamus u, ut relationem inter v et u exploremus, eritque ex secunda solutione

$$b = \frac{(4a+1)(a+1) - 2(2a+1)u + uu}{a-1} \quad \text{et} \quad c = \frac{(a+4)(a+1) - 2(a+2)u + uu}{a-1}.$$

1) Editio princeps: $\frac{77 - 24v + vv}{3}$. Correxit A. M.

2) Editio princeps: extra. Correxit A. M.

3) Editio princeps: $b = \frac{(a+1)^2 + 2(a+1)v + vv}{4(a-1)}$. Correxit R. F.

Iam bini valores ipsius b inter se aequati dant hanc aequationem:

$$(a+1)^2 + 2(a-1)v + vv = 4(4a+1)(a+1) - 8(2a+1)u + 4uu,$$

bini vero valores ipsius c istam:

$$(a+1)^2 - 2(a-1)v + vv = 4(a+4)(a+1) - 8(a+2)u + 4uu.$$

Harum vero altera ab altera subtracta praebet

$$12(aa-1) - 8u(a-1) - 4v(a-1) = 0,$$

ex qua aequatione sequitur $v = 3(a+1) - 2u$.

41. Substituamus in prioribus valoribus pro b et c inventis istum valorem loco v, et calculo peracto reperimus

$$b = \frac{(4a+1)\ (a+1) - 2(2a+1)u + uu}{a-1},$$

$$c = \frac{(a+4)\ (a+1) - 2(a+2)u + uu}{a-1},$$

quae cum perfecte congruant cum formulis superioribus, certum est posteriorem solutionem a priore prorsus non discrepare, etiamsi per operationes prorsus diversas sit eruta. Nihilo vero minus utraque analysis summa attentione digna est censenda; idque eo magis, quod per praecepta solita in arte DIOPHANTEA vix ullam solutionem elicere liceat, qua simul conditionibus praescriptis, scilicet, ut fiat tam $b + c > a + d$ quam $b < a$ et $c < a$, satisfieri posset.

SOLUTIO SUCCINCTA ET ELEGANS PROBLEMATIS QUO QUAERUNTUR TRES NUMERI TALES UT TAM SUMMAE QUAM DIFFERENTIAE BINORUM SINT QUADRATA

Commentatio 753 indicis ENESTROEMIANI
Mémoires de l'académie des sciences de St-Pétersbourg 6 (1813/4), 1818, p. 54—65
Conventui exhibuit die 11. maii 1780

1. Etsi hoc problema iam a variis auctoribus est tractatum et resolutum, sequens tamen solutio omni attentione digna videtur, ideo quod non solum plura calculi artificia involvat, sed etiam facili negotio plures solutiones, alias inventu difficillimas, suppeditat.

2. Sint x, y, z tres numeri quaesiti, quorum maximus sit x, minimus vero z, ac statim patet ponendo $x = pp + qq$ et $y = 2pq$ fore $x + y = (p + q)^2$ et $x - y = (p - q)^2$. Simili modo, ponendo $x = rr + ss$ et $z = 2rs$, erit $x + z = (r + s)^2$ et $x - z = (r - s)^2$, sicque iam quatuor conditionibus est satisfactum, si modo fuerit $rr + ss = pp + qq$. Tum vero adhuc duae conditiones adimplendae restant, scilicet ut $y + z = 2pq + 2rs$ et $y - z = 2pq - 2rs$ quadrata reddantur.

3. Ut primo fiat $rr + ss = pp + qq$, statuatur $x = (aa + bb)(cc + dd)$; tum enim iste valor duplici modo in duo quadrata resolvi potest. Fiet enim

$$p = ac + bd, \qquad r = ad + bc,$$
$$q = ad - bc, \qquad s = ac - bd.$$

Hinc ergo habebimus

$$y = 2(aacd + abdd - abcc - bbcd) \text{ et } z = 2(aacd + abcc - abdd - bbcd),$$

hincque adeo

$$y + z = 4cd(aa - bb) \quad \text{et} \quad y - z = 4ab(dd - cc),$$

quas ergo duas formulas adhuc quadrata reddi oportet.

4. Faciamus igitur primo productum:

$$yy - zz = 16abcd\,(aa - bb)\,(dd - cc) = \square\,,$$

unde primo necesse est, ut haec formula:

$$ab(aa - bb) \cdot cd(dd - cc)$$

ad quadratum revocetur. Hunc in finem statuamus:

$$cd(dd - cc) = nnab(aa - bb)\,,$$

et quia res a relatione inter binas litteras a, b et c, d pendet, ponere licebit $d = a$, unde habebimus:

$$c(aa - cc) = nnb(aa - bb)\,;$$

unde deducitur

$$aa = \frac{nnb^3 - c^3}{nnb - c}\,,$$

quae ergo fractio ad quadratum reduci debet.

5. Hoc autem facile praestabitur ponendo $a = b + c$, ut fiat

$$\frac{nnb^3 - c^3}{nnb - c} = bb + 2bc + cc\,,$$

qua aequatione evoluta termini b^3 et c^3 utrinque se destruent; nascetur enim ista aequatio:

$$0 = (2nn - 1)\,bbc + (nn - 2)\,bcc\,;$$

unde colligitur

$$\frac{b}{c} = \frac{2 - nn}{2nn - 1}\,.$$ [1]

6. Quodsi ergo ponamus $b = 2 - nn$ et $c = 2nn - 1$, erit $a = nn + 1$. Nunc totum negotium eo reducitur, ut vel haec formula: $ab(dd - cc)$ vel haec: $cd(aa - bb)$ reddatur quadratum. Prior autem formula ob $d = a$ et $d + c = 3nn$ et $d - c = 2 - nn$ erit

$$ab(dd - cc) = 3nn(nn + 1)\,(2 - nn)^2\,,$$

quae quadratum erit, dummodo fuerit $3(nn + 1) = \square$.

1) Editio princeps: $\frac{2 - nn}{nn - 1}$. Correxit A. M.

7. At vero ista formula $3(nn+1)$ nullo modo quadratum effici potest; interim tamen remedium facile adhiberi potest, dummodo loco valoris $a = b + c$ statuatur $a = c - b$, quo facto fiet

$$\frac{nnb^3 - c^3}{nnb - c} = bb - 2bc + cc\,,$$

unde evolvendo colligitur

$$\frac{b}{c} = \frac{nn+2}{2nn+1}\,.$$

8. Ponatur ergo $b = nn + 2$ et $c = 2nn + 1$, erit $a = nn - 1 = d$; unde ista formula $ab(dd - cc)$ reducitur ad hanc:

$$3nn(nn-1)(nn+2)^{2}\,[1])\,.$$

Tantum ergo opus est, ut ista formula $3(nn-1)$ efficiatur quadratum, id quod facillime praestatur, quia $nn - 1$ habet factores[3]. Quodsi enim ponatur

$$3(nn-1) = \frac{ff}{gg}(n+1)^2\,,$$

fieri debet $3(n-1) = \frac{ff}{gg}(n+1)$, unde fit

$$n = \frac{ff + 3gg}{3gg - ff}\,.$$

9. Hoc igitur modo omnibus conditionibus praescriptis est satisfactum, unde regrediamur ad quantitates supra introductas. Ac primo quidem ex hoc valore pro n invento deducimus:

$$a = d = \frac{12ffgg}{(3gg-ff)^2}\,,\quad b = nn + 2 = \frac{3f^4 - 6ffgg + 27g^4}{(3gg-ff)^2}$$

et

$$c = \frac{3f^4 + 6ffgg + 27g^4}{(3gg-ff)^2}\,.$$

Iam vero quia tota solutio tantum a ratione inter litteras a, b, c, d pendet, primo denominatores omittamus, numeratores vero per communem divisorem 3 dividamus, hocque modo sequentes obtinebimus valores:

$$\begin{aligned} a = d &= 4ffgg\,,\\ b &= f^4 - 2ffgg + 9g^4\,,\\ c &= f^4 + 2ffgg + 9g^4\,. \end{aligned}$$

1) In hac formula EULERUS signum negativum omittit. R. F.

Ex his derivemus litteras p, q, r, s, quae erunt:

$$p = 8ffgg(f^4 + 9g^4), \qquad r = f^8 + 30f^4g^4 + 81g^8,$$
$$q = -f^8 + 2f^4g^4 - 81g^8\ ^{1}), \qquad s = 16f^4g^4.$$

Praestat autem a primis valoribus f et g pro arbitrio assumtis per gradus primo ad litteras a, b, c, d, hinc vero porro ad litteras p, q, r, s, hinc denique ad ipsos numeros quaesitos x, y, z ascendere. Ubi imprimis notasse iuvabit hunc calculum per valores negativos neutiquam turbari; semper enim eorum loco valores positivos tuto scribere licet. Hanc investigationem nonnullis exemplis illustremus.

EXEMPLUM 1
quo $f = 1$ *et* $g = 1$

10. Hic ergo erit $a = d = 4$, $b = 8$, $c = 12$, qui valores depressi fiunt $a = d = 1$, $b = 2$, $c = 3$. Hinc porro colligimus $p = 5$, $q = 5$, $r = 7$, $s = 1$, unde $x = 50$, $y = 50$, $z = 14$, qui valores utique satisfaciunt; verum ista solutio ob simplicitatem ab indole quaestionis excludenda est.

EXEMPLUM 2
quo $f = 2$ *et* $g = 1$

11. Hic erit $a = 16, b = 17, c = 33, d = 16$. Hinc ergo porro deducitur $p = 800, q = 305, r = 817, s = 256$, quamobrem ipsi numeri quaesiti erunt:

$$x = 733025, \quad y = 488000, \quad z = 418304.$$

Hinc autem erit:

$$x + y = 1105^2, \qquad x - y = 495^2,$$
$$x + z = 1073^2, \qquad x - z = 561^2,$$
$$y + z = 952^2, \qquad y - z = 264^2.$$

EXEMPLUM 3
quo $f = 3$ *et* $g = 1$

12. Hic ergo erit $a = 36, b = 72, c = 108$; sive per 36 deprimendo erit $a = 1, b = 2, c = 3, d = 1$. Hinc ergo ad ipsum exemplum primum revolvimus, id quod semper evenit, quando pro f multiplum ternarii accipitur. Posito enim $f = 3h$ fiet $n = \frac{gg + 3hh}{gg - 3hh}$, quae a praecedente forma non discrepat.

1) Editio princeps: $q = -(f^4 - 9g^4)^2$. Correxit A. M.

EXEMPLUM 4

quo $f = 1$ *et* $g = 2$

13. Hic erit $a = 16$, $b = 137$, $c = 153$, $d = 16$, ideoque $p = 4640$, $q = 20705$, $r = 21217$, $s = 256$. Hinc autem ipsi numeri quaesiti x, y, z nimis fiunt magni, quam ut operae pretium sit eos evolvere.

NOTA

14. Quoniam inventis numeris a, b, c, d hincque p, q, r, s ipsa solutio ita est adornata, ut fiat $x + y = (p + q)^2$, $x - y = (p - q)^2$, $x + z = (r + s)^2$ et $x - z = (r - s)^2$, quadrata etiam, quibus formulae $y + z$ et $y - z$ aequantur, evolvi conveniet. Invenimus autem $y + z = 4cd(aa - bb)$, quae, substitutis valoribus supra inventis, per f et g expressis, reducitur ad hanc formam:

$$4(f^4 + 2ffgg + 9g^4)^2\, 4ffgg(f^4 - 6ffgg + 9g^4),$$

quae manifesto est quadratum, cuius radix:

$$4fg(ff - 3gg)(f^4 + 2ffgg + 9g^4),$$

ita ut iam sit:

$$\sqrt{y + z} = 4fgc(ff - 3gg).$$

Simili modo cum sit $y - z = 4ab(dd - cc)$, erit

$$y - z = 4 \cdot 4ffgg(f^4 - 2ffgg + 9g^4)^2\,(f^4 + 6ffgg + 9g^4),$$

ideoque

$$\sqrt{y - z} = 4fg(ff + 3gg)\,(f^4 - 2ffgg + 9g^4) = 4fgb(ff + 3gg).$$

15. Ceterum, quamquam haec solutio innumerabiles valores satisfacientes pro x, y, z complectitur, ea tamen neutiquam pro generali est habenda. Quoniam enim supra paragraphis 5 et 7 posuimus $a = b + c$ et $a = c - b$, evidens est hanc positionem maxime esse particularem, quandoquidem huic aequationi infinitis aliis modis satisfieri potest. Interim tamen hic observasse iuvabit, postquam hac methodo numeri idonei pro x, y, z fuerint inventi, ex iis facile alios, qui sint X, Y, Z, derivari posse sumendo

$$X = \frac{yy + zz - xx}{2}, \quad Y = \frac{xx + zz - yy}{2} \quad \text{et} \quad Z = \frac{xx + yy - zz}{2}.$$

Tum enim

$$\begin{aligned} X + Y &= zz = \square, & Y - X &= xx - yy = \square, \\ X + Z &= yy = \square, & Z - X &= xx - zz = \square, \\ Y + Z &= xx = \square, & Z - Y &= yy - zz = \square. \end{aligned}$$

Hoc autem modo statim ad numeros praegrandes deducimur. Similique modo continuo ad numeros maiores pertingere licet.

ADDITAMENTUM

16. Pauciores ambages requirit sequens problema affine et iam saepius tractatum.

PROBLEMA

Invenire tria quadrata, xx, yy, zz, ita ut binorum differentiae sint quadrata.

SOLUTIO

17. Posito $x = pp + qq$ et $y = 2pq$ fiet $xx - yy = (pp - qq)^2$. Simili modo posito $x = rr + ss$ et $z = 2rs$ fiet $xx - zz = (rr - ss)^2$. Tantum igitur superest, ut $yy - zz = 4(ppqq - rrss)$ reddatur quadratum, postquam scilicet factum fuerit:

$$pp + qq = rr + ss\,,$$

quod fit, uti supra est ostensum, sumendo

$$p = ac + bd,\ \ q = ad - bc,\ \ r = ad + bc,\ \ s = ac - bd\,.$$

Hinc autem, ut $yy - zz$ fiat quadratum, istud productum

$$abcd(aa - bb)\,(dd - cc)$$

fiat quadratum, quod vidimus fieri sumtis

$$a = d = nn \pm 1\,,\ \ b = 2nn \mp 1 \text{ et } c = nn \mp 2\,.^{1})$$

18. Quodsi iam loco n scribamus $\frac{m}{n}$, habebimus sequentes geminas determinationes:

$$a = d = mm \mp nn\,,\ \ b = 2mm \pm nn\,,\ \ c = mm \pm 2nn\,.$$

Hinc ergo sumendo pro m et n numeros simpliciores sequens tabula exhibet plures valores idoneos pro literis a, d, b, c. Ubi notandum est, si neuter numerorum m et n fuerit per 3 divisibilis, tum valores ex signis superioribus ortos per 3 deprimi posse, uti in sequente tabula factum est.

1) Litterae b et c permutatae sunt. R. F.

TABULA

exhibens valores idoneos pro litteris a, b, c, d

m	n	$a=d$	b	c	m	n	$a=d$	b	c
1	1	0	1	1	7	1	16	33	17
		2	1	1			50	97	47
2	1	1	3	2	7	2	15	34	19
		5	7	2			53	94	41
3	1	8	19	11	7	3	40	107	67
		10	17	7			58	89	31
3	2	5	22	17	7	4	11	38	27
		13	14	1			65	82	17
4	1	5	11	6	7	5	8	41	33
		17	31	14			74	73	1
4	3	7	41	34	7	6	13	134	121
		25	23	2			85	62	23
5	1	8	17	9	8	1	21	43	22
		26	49	23			65	127	62
5	2	7	18	11	8	3	55	137	82
		29	46	17			73	119	46
5	3	16	59	43	8	5	13	51	38
		34	41	7			89	103	14
5	4	3	22	19	8	7	5	59	54
		41	34	7			113	79	34
6	1	35	73	38	10	1	33	67	34
		37	71	34			101	199	98
6	5	11	97	86					
		61	47	14					

Qui applicationem facere voluerit, notet tam litteras a et d quam c et b inter se permutari posse. Ac si numeri negativi prodeant, signum negationis omittetur, quo observato calculus fiet satis facilis.

EXEMPLUM DESUMTUM EX NUMERIS $m = 2$ ET $n = 1$ PRO SIGNIS INFERIORIBUS

19. Hic igitur est $a = 5$, $b = 7$, $c = 5$, $d = 2$ [1]; unde fit $p = 39$, $q = 25$, $r = 45$, $s = 11$; unde:

$$x = 2146, \quad y = 1950, \quad z = 990 \text{ sive}$$
$$x = 1073\text{[2]}, \quad y = 975, \quad z = 495\text{[3]}.$$

20. Praeterea notari meretur ex qualibet solutione huius problematis facile deduci posse solutionem praecedentis, quo quaeruntur tres numeri X, Y, Z, ita ut binorum tam summa quam differentia sit quadratum, quemadmodum modo ante animadvertimus; quia autem ibi fractiones occurrerent, sumantur quadrupla:

$$X = 2(yy + zz - xx),$$
$$Y = 2(xx + zz - yy),$$
$$Z = 2(xx + yy - zz),$$

qui ergo omnes tres numeri semper erunt pares ideoque diversae prorsus sunt indolis ab illis numeris, quas solutio superior suppeditavit, ubi scilicet unus trium numerorum necessario est impar, quia alioquin deprimi possent.

---

1) Litterae c et d permutatae sunt. R. F.
2) Editio princeps: 1023. Correxit R. F.
3) Editio princeps: 445. Correxit R. F.

PROBLEME DE GEOMETRIE RESOLU PAR L'ANALYSE DE DIOPHANTE

Commentatio 754 indicis Enestroemiani
Mémoires de l'académie des sciences de St-Pétersbourg 7 (1815/6), 1820, p. 3—9
Présenté à la Conférence le 4 Mars 1782

1. Le sujet du problème dont il s'agit dans ce mémoire, est tiré de la Trigonométrie rationnelle. On demande les trois côtés x, y, z d'un triangle dont les lignes tirées des angles par le centre de gravité du triangle soyent toutes trois exprimées en nombres rationnels; c'est-à-dire, on demande trois nombres x, y, z tels que

$$2xx + 2yy - zz = \square ,$$
$$2yy + 2zz - xx = \square ,$$
$$2zz + 2xx - yy = \square .$$

J'ai déjà donné, à différentes reprises[1]), des solutions de ce problème, sans qu'aucune m'ait entièrement satisfait. Celle que je présente ici réunit à beaucoup d'élégance la plus grande généralité. Mais avant d'entrer en matière il sera bon de faciliter la solution par le Lemme suivant:

LEMME

2. *Deux nombres de la forme:*

$$A^2 + 2PAB + B^2 \quad et \quad A^2 + 2QAB + B^2 ,$$

seront toujours quarrés, lorsque

$$A = 4(P + Q) \quad et \quad B = (P - Q)^2 - 4 .$$

DEMONSTRATION

Multiplions l'une de ces formes par l'autre, et nous aurons le produit suivant:

$$A^4 + 2(P + Q)\,A^3B + 2(2PQ + 1)\,A^2B^2 + 2(P + Q)\,AB^3 + B^4.$$

1) Voir les mémoires 451, 713 et 732 de l'indice d'Enestroem, *Leonhardi Euleri, Opera omnia*, I. 3, p. 282, I. 4, p. 290, p. 399 et surtout la préface du volume I. 4, p. XX/XXI. R. F.

Soit la racine de cette quantité quarrée

$$A^2 + (P + Q)\,AB - B^2\,,$$

et puisque le quarré est

$$A^4 + 2(P + Q)A^3B + \big((P + Q)^2 - 2\big)A^2B^2 - 2(P + Q)AB^3 + B^4,$$

en comparant cette forme avec la précédente on voit que, pour que l'une soit égale à l'autre, il faut que

$$\big((P - Q)^2 - 4\big)\,A = 4(P + Q)\,B\,,$$

donc

$$A = 4(P + Q) \quad \text{et} \quad B = (P - Q)^2 - 4\,.$$

Substituant ces valeurs dans l'une ou l'autre des deux formes du lemme, elle devient un quarré. Par exemple la première en y faisant ces substitutions deviendra:

$$16(P + Q)^2 + 2P\big(4(P + Q)\,(P - Q)^2 - 16(P + Q)\big) + (P - Q)^4 - 8(P - Q)^2 + 16\,,$$

où il faut remarquer que

$$(P - Q)^4 + 8P(P + Q)\,(P - Q)^2 = (P - Q)^2(3P + Q)^2\,,$$
$$16(P + Q)^2 - 32P(P + Q) - 8(P - Q)^2 = -8(P - Q)\,(3P + Q)\,.$$

De cette façon la forme se réduit à

$$\big((P - Q)\ (3P + Q) - 4\big)^2\,.$$

Or le produit des deux formes du lemme étant un quarré et la première l'étant aussi, il est clair que l'autre forme doit être nécessairement de même un quarré. Aussi la racine se trouvera-t-elle, par des procédés semblables, être

$$(Q - P)\,(3Q + P) - 4\,.$$

COROLLAIRE

3. A l'égard des valeurs de A et B il faut remarquer:

1°) qu'à cause de la permutabilité évidente de ces deux quantités, on pourra aussi faire:

$$A = (P - Q)^2 - 4 \quad \text{et} \quad B = 4(P + Q)\,;$$

2°) que ces valeurs peuvent être simplifiés dans certains cas. Car puisque $(P-Q)^2 = (P+Q)^2 - 4PQ$, en mettant cette valeur dans l'expression de B, on aura $B = (P+Q)^2 - 4(PQ+1)$, de sorte que, toutes les fois que

$$PQ + 1 = n(P+Q),$$

on pourra diviser A et B par le même nombre $P+Q$, et on aura

$$A = 4 \quad \text{et} \quad B = P + Q - 4n.$$

Quant aux racines des deux formes proposées, savoir

$$(P-Q)(3P+Q) - 4 \quad \text{et} \quad (Q-P)(3Q+P) - 4,$$

comme la première peut être représentée par

$$(P+Q)(P-Q) + 2P(P-Q) - 4,$$

et que

$$2P(P-Q) - 4 = 2P(P+Q) - 4(PQ+1),$$

à cause de $PQ + 1 = n(P+Q)$ on pourra diviser par $P+Q$, de sorte que la racine de la première forme [sera]

$$= 3P - Q - 4n,$$

et, à cause de la permutabilité de P et Q, la racine de l'autre forme sera

$$[=] 3Q - P - 4n.$$

SOLUTION DU PROBLEME PROPOSE

4. Soit

$$\begin{aligned} 2xx + 2yy - zz &= pp, \\ 2xx + 2zz - yy &= qq, \\ 2yy + 2zz - xx &= rr, \end{aligned}$$

et en mettant

$$xx + yy + zz = s,$$

on aura

$$pp + 3zz = qq + 3yy = rr + 3xx = 2s.$$

Ensuite on trouve aussi que

$$\begin{aligned} 2pp + 2qq - rr &= 9xx, \\ 2pp + 2rr - qq &= 9yy, \\ 2qq + 2rr - pp &= 9zz. \end{aligned}$$

Quoique ces propriétés ne contribuent en aucune manière à la solution du problème, elles méritoient bien d'être remarquées ici en passant. Quant à la solution même, elle se déduit des opérations suivantes.

5. Prenons la différence de la première et seconde de nos trois équations fondamentales, qui sera

$$pp - qq = 3(yy - zz) ,$$

ou bien, en facteurs on aura

$$(p + q)(p - q) = 3(y + z)(y - z) .$$

Soit

$$p + q = \frac{3a}{b}(y - z) , \qquad p - q = \frac{b}{a}(y + z) ,$$

et la somme des quarrés sera

$$(p + q)^2 + (p - q)^2 = 2pp + 2qq = \frac{9aa}{bb}(y - z)^2 + \frac{bb}{aa}(y + z)^2 .$$

Or les équations fondamentales donnent

$$2pp + 2qq = 8xx + 2yy + 2zz ,$$

ou bien

$$2pp + 2qq = 8xx + (y + z)^2 + (y - z)^2 ,$$

d'où l'on tire cette équation entre x, y, z:

$$\frac{9aa}{bb}(y - z)^2 + \frac{bb}{aa}(y + z)^2 = 8xx + (y + z)^2 + (y - z)^2 ,$$

qui peut aussi être représentée ainsi:

$$8xx = \frac{9aa - bb}{bb}(y - z)^2 + \frac{bb - aa}{aa}(y + z)^2 .$$

6. La troisième équation fondamentale $2yy + 2zz - xx = rr$ se transforme aisément en celle-ci:

$$(y + z)^2 + (y - z)^2 - xx = rr ,$$

qui multipliée par 8 devient

$$8rr = 8(y + z)^2 + 8(y - z)^2 - 8xx ,$$

équation qui, si l'on met à la place de $8xx$ la valeur trouvée au précédent paragraphe, sera

$$8rr = \frac{9(bb-aa)}{bb}(y-z)^2 + \frac{9aa-bb}{aa}(y+z)^2 .$$

7. Mettons maintenant

$$y+z = a(c+d), \qquad y-z = b(c-d),$$

et les deux expressions trouvées pour $8xx$ et $8rr$ prendront les formes suivantes:

$$2xx = 2aa(cc+dd) + cd(bb - 5aa),$$
$$2rr = 2bb(cc+dd) + cd(9aa - 5bb),$$

qui, divisées l'une par $2aa$ et l'autre par $2bb$, donneront:

$$\frac{xx}{aa} = cc + dd + \frac{bb-5aa}{2aa}\cdot cd ,$$

$$\frac{rr}{bb} = cc + dd + \frac{9aa-5bb}{2bb}\cdot cd .$$

8. En comparant ces deux expressions avec les formes du lemme, nous verrons que

$$A = c, \; B = d, \; P = \frac{bb-5aa}{4aa} \quad \text{et} \quad Q = \frac{9aa-5bb}{4bb} .$$

De ces valeurs on déduit aisément:

$$n(P+Q) = \frac{n(b^4 - 10aabb + 9a^4)}{4aabb}, \qquad PQ + 1 = -\frac{5}{4}\,\frac{(b^4 - 10aabb + 9a^4)}{4aabb};$$

donc $n = -\frac{5}{4}$.

9. Or en vertu du corollaire du paragraphe 3 il y a $A = 4$ et $B = P + Q - 4n$, donc

$$c = 4 \quad \text{et} \quad d = \frac{(9aa+bb)\,(aa+bb)}{4aabb},$$

portant

$$y+z = \frac{a\big(16aabb + (9aa+bb)\,(aa+bb)\big)}{4aabb},$$

$$y-z = \frac{b\big(16aabb - (9aa+bb)\,(aa+bb)\big)}{4aabb} .$$

Et puisque, en vertu du même corollaire,

$$\frac{x}{a} = 3P - Q - 4n \quad \text{et} \quad \frac{r}{b} = 3Q - P - 4n ,$$

nous aurons aussi

$$x = \frac{a\big((9aa + bb)\,(aa + bb) - 2(9a^4 - b^4)\big)}{4aabb} ;$$

$$r = \frac{b\big((9aa + bb)\,(aa + bb) + 2(9a^4 - b^4)\big)}{4aabb} .$$

Enfin on aura

$$p + q = \frac{3a}{b}(y - z) ,$$

$$p - q = \frac{b}{a}(y + z) .$$

10. Mettons pour abréger

$$C = 16aabb ,$$
$$D = (9aa + bb)\,(aa + bb) ,$$
$$F = 2(9a^4 - b^4) ,$$

et en supprimant le diviseur commun $4aabb$, nous aurons

$$\begin{array}{rcr} x = a(D - F) , & \| & r = b(D + F) , \\ y + z = a(C + D) , & \| & p + q = 3a(C - D) , \\ y - z = b(C - D) , & \| & p - q = b(C + D) . \end{array}$$

EXEMPLE 1

11. Soit $a = 1$ et $b = 2$, et on aura $C = 64$, $D = 65$, $F = -14$, donc

$$\begin{array}{rcr} x = 79 , & \| & r = 102 , \\ y + z = 129 , & \| & p + q = -3 , \\ y - z = -2 , & \| & p - q = 258 , \end{array}$$

par conséquent on aura

$$\begin{array}{rcr} x = 79 , & \| & p = \frac{255}{2} , \\ y = \frac{127}{2} , & \| & q = \frac{261}{2} , \\ z = \frac{131}{2} , & \| & r = 102 . \end{array}$$

EXEMPLE 2

12. Soit $a = 2$ et $b = 1$, de sorte que $C = 64$, $D = 185$ et $F = 286$, donc

$$\begin{array}{rl||rl} x &= -202\,, & r &= +471\,, \\ y+z &= +498\,, & p+q &= -726\,, \\ y-z &= -121\,, & p-q &= +249\,. \end{array}$$

On aura donc

$$\begin{array}{rl||rl} x &= 202\,, & p &= \frac{477}{2}\,, \\ y &= \frac{377}{2}\,, & q &= \frac{975}{2}\,, \\ z &= \frac{619}{2}\,, & r &= 471\,. \end{array}$$

13. Si l'on veut avoir des solutions en nombres entiers, il est évident qu'on n'a qu'à multiplier par 2 tous les six nombres de chacun des deux exemples précédens. En voilà encore quelques solutions:

68	87	85
158	127	131
159	325	314
619	377	404
477	277	446
569	881	640[1]).

1) La première solution est celle des nombres $\frac{2p}{3}, \frac{2q}{3}, \frac{2r}{3}$ du premier exemple; la deuxième le double des nombres du premier exemple; la troisième est celle des nombres $\frac{2p}{3}, \frac{2q}{3}, \frac{2r}{3}$ du deuxième exemple; la quatrième est le double des nombres du deuxième exemple. Voir § 4. EULER a déjà donné tous ces exemples, quand il a traité le problème pour la première fois. Voire I. 3, p. 290, 291, 294 et 295. R. F.

DE CASIBUS QUIBUS FORMULAM $x^4 + mxxyy + y^4$ AD QUADRATUM REDUCERE LICET[1)]

Commentatio 755 indicis ENESTROEMIANI
Mémoires de l'académie des sciences de St-Pétersbourg 7 (1815/6), 1820, p. 10—22
Conventui exhibuit die 2. maii 1782

1. Huius formulae iam dudum Analystis casus innotuere nonnulli, quibus eam nullo modo ad quadratum revocare licet paucissimis casibus exceptis, quibus una vel altera litterarum x et y evanescit, vel ambae sunt inter se aequales. Priore enim casu formula proposita semper esset quadratum, quicquid fuerit m; altero casu vero, quia posito $x = y = 1$ formula fit $m + 2$, casus idonei forent $m = ii - 2$, ex quibus autem casibus plerumque alios eruere non licet. Hic igitur eiusmodi valores pro m investigare constitui integri, sive positivi sive negativi, pro quibus innumerabiles litterarum x et y valores exhiberi queant, siquidem methodus constat ex quovis casu cognito alios eruendi. Casus autem, quibus iam demonstratum est hoc neutiquam fieri posse, sunt potissimum $m = \pm 1$ et $m = \pm 6$, quibus addere licet $m = 7$ et $m = 14$[2)]. Ceterum sponte patet, si fuerit $m = \pm 2$, formulam semper esse quadratum, quicunque valores litteris x et y tribuantur.

2. Quodsi iam ponamus $x^4 + mxxyy + y^4 = zz$, erit $m = \frac{zz - x^4 - y^4}{xxyy}$, quae formula utique omnes valores idoneos pro m in se complectitur. Verum quia mihi propositum est in eius tantum valores integros inquirere, hanc expressionem a fractionibus liberari oportet, quod fit ponendo

$$z = axxyy - (xx \pm yy) ;$$

1) Confer Commentationem indicis ENESTROEMIANI 696, quae eundem titulum habet; *LEONHARDI EULERI Opera omnia*, volumen I. 4, p. 235. R. F.

2) Vide notam 1) p. 235, voluminis I. 4, supra laudati. R. F.

tum enim fit

$$m = aaxxyy - 2a(xx \pm yy) \pm 2,$$

quae expressio ad hanc formam reducitur

$$m = (axx \mp 2)(ayy - 2) \mp 2,$$

unde fit

$$m \pm 2 = (axx \mp 2)(ayy - 2),$$

quae formula iam innumerabiles valores integros pro m praebet, siquidem pro a, x, y numeri quicunque integri accipiantur.

3. At vero etiam numeri integri hinc prodire possunt, etiamsi litterae a valores fracti tribuantur, quos igitur potissimum hic investigare convenit. Patet autem hoc infinitis modis evenire posse, quando x et y fuerint numeri compositi. Hunc in finem statuamus $x = pq$ et $y = rs$; tum vero ponatur $a = \frac{b}{pprr}$. Hoc enim modo obtinebimus

$$m \pm 2 = \frac{(bqq \mp 2rr)(bss - 2pp)}{pprr},$$

ubi, quia p, q et r, s sunt numeri inter se primi, alio modo ad numeros integros pervenire non licet, nisi prior numeratoris factor divisionem admittat per pp, alter vero per rr; unde hanc expressionem ita repraesentari oportet:

$$m \pm 2 = \frac{bqq \mp 2rr}{pp} \times \frac{bss - 2pp}{rr},$$

quarum fractionum utraque numerus integer evadere debet.

4. Incipiamus a posteriore et ponamus

$$bss - 2pp = crr,$$

ita ut

$$bss - crr = 2pp.$$

Statuamus porro

$$bss + crr = 2n,$$

ut fiat

$$bss = n + pp \quad \text{et} \quad crr = n - pp,$$

ita ut sit

$$bcrrss = nn - p^4 .$$

Faciamus $bc = \lambda$, et quia $rs = y$, erit $nn - p^4 = \lambda yy$. Sumtis igitur pro lubitu numeris n et p, erit yy maximus factor quadratus formulae $nn - p^4$, et littera λ exprimet reliquum factorem.

5. Quia igitur fecimus $\frac{bss - 2pp}{rr} = c$, erit nunc

$$m \pm 2 = \frac{bcqq \mp 2crr}{pp} .$$

Erat autem $crr = n - pp$, quo valore substituto ob $bc = \lambda$ habebimus hanc formulam satis concinnam:

$$m \pm 2 = \frac{\lambda qq \mp 2n \pm 2pp}{pp} ,$$

ex qua colligitur

$$m = \frac{\lambda qq \mp 2n}{pp} ,$$

ubi, quia numeros n et p, una cum λ, tamquam cognitos spectamus, pro q eiusmodi valores quaeri oportet, ut $\lambda qq \mp 2n$ divisionem admittat per pp. Interim tamen ratione numeri p evenire potest, ut hoc praestari nequeat; unde imprimis curare debemus, ut pro p eiusmodi numeros assumamus, unde valores integri pro m prodeant.

6. Electis igitur pro litteris n et p numeris ad libitum, formulae $nn - p^4$ maximus factor quadratus sumatur pro yy, factor vero non quadratus pro λ, tum pro q eiusmodi investigantur valores, ut fiat

$$m = \frac{\lambda qq \mp 2n}{pp}$$

numerus integer; quodsi fuerit praestitum, habebitur $x = pq$; praeterea vero, ob $y = rs$ et $a = \frac{b}{pprr}$, formula pro z assumta evadet

$$z = axxyy - (xx \pm yy) = bqqss - ppqq \mp rrss .$$

Erat autem $bss = n + pp$, quo substituto fit

$$z = nqq \mp rrss = nqq \mp yy .$$

In his formulis omnes plane valores, quos quaerimus pro m, necessario erunt contenti.

7. Istae autem formulae pluribus modis mutari possunt, quorum sequens potissimum ad calculum est accommodatus. Ponendo scilicet $n = 2i$, $p = 2t$, $q = 2u$, $y = 2v$ erit $x = 4tu$. Tum autem ista habebitur formula canonica: $ii - 4t^4 = \lambda vv$, fietque $m = \frac{\lambda uu \mp i}{tt}$. Facta iam substitutione reperitur $z = 8iuu \mp 4vv$. Quia igitur tantum ratio inter x et y in computum ingreditur, si eos [sic] valores ad dimidium redigantur, ut fiat $x = 2tu$ et $y = v$, tum z reducetur ad partem quartam, eum [sic] fiat $z = 2iuu \mp vv$.

8. Etsi posterior solutio ex priore derivata est, tamen ea latius patet, quoniam in valore ipsius m signum ambiguum etiam numeros impares afficere potest, dum in priore tantum pares affecit, atque prior in posteriore contineatur, quando i est numerus par. Quamobrem sola solutione posteriore uti conveniet. Ac ne multitudo litterarum calculum confundat, hanc solutionem sequenti modo constituamus.

9. Sumtis pro lubitu binis numeris pro n et p, fiat

$$n^2 - 4p^4 = (n + 2pp)(n - 2pp) = \lambda yy ,$$

ubi yy maximum factorem quadratum denotat in hac formula contentum, λ vero factorem non quadratum, sicque statim altera variabilium x et y innotescit. Tum vero erit $m = \frac{\lambda qq \pm n}{pp}$, ubi q ita accipi debet, ut iste numerus fiat integer, quo facto habebitur $x = 2pq$, $z = 2nqq \pm yy$. Hic autem ob rationes iam allegatas casus excludi debent, quibus fit $x = y$, quia scilicet inde novos valores pro x et y eruere non liceret.

10. Veritas huius solutionis ex ipsa formula proposita

$$zz = x^4 + mxxyy + y^4$$

immediate sequenti modo ostendi potest. Cum enim sit

$$4p^4 = nn - \lambda yy \quad \text{et} \quad mpp = \lambda qq \pm n,$$

ob $x = 2pq$ habebimus

$$x^4 = 16p^4q^4 = 4nnq^4 - 4\lambda q^4 yy.$$

Porro erit membrum

$$mxxyy = 4mppqqyy = 4\lambda q^4 yy \pm 4nqqyy,$$

unde

$$zz = 4nnq^4 \pm 4nqqyy + y^4 = (2nqq \pm yy)^2.$$

Iam pro variis valoribus, qui pro p assumi possunt, sequentes casus evolvamus.

Evolutio casus primi, quo $p = 1$

11. Hoc igitur casu primo habebimus $nn - 4 = \lambda yy$; deinde erit in integris $m = \lambda qq \pm n$, tum vero erit $x = 2q$ et $z = 2nqq \pm yy$. Unde pro variis valoribus loco n assumtis plures solutiones nascuntur, quarum praecipuas, simpliciores quidem, in sequenti tabula ab oculos ponamus:

n	y	λ	m	x	z
0	2	—1	$-qq \pm 0$	$2q$	$0qq \pm 4$
1	1	—3	$-3qq \pm 1$	$2q$	$2qq \pm 1$
2	y	0	$+0qq \pm 2$	$2q$	$4qq \pm yy$
3	1	5	$5qq \pm 3$	$2q$	$6qq \pm 1$
4	2	3	$3qq \pm 4$	$2q$	$8qq \pm 4$
5	1	21	$21qq \pm 5$	$2q$	$10qq \pm 1$
6	4	2	$2qq \pm 6$	$2q$	$12qq \pm 16$
7	3	5	$5qq \pm 7$	$2q$	$14qq \pm 9$
8	2	15	$15qq \pm 8$	$2q$	$16qq \pm 4$
9	1	77	$77qq \pm 9$	$2q$	$18qq \pm 1$
10	4	6	$6qq \pm 10$	$2q$	$20qq \pm 16$
11	3	13	$13qq \pm 11$	$2q$	$22qq \pm 9$
12	2	35	$35qq \pm 12$	$2q$	$24qq \pm 4$

Quam tabulam, prout necessitas postulat, facile ulterius continuare licet.

12. Quaelibet harum solutionum ob numerum q arbitrio nostro relictum innumerabiles suppeditat valores pro numero m, qui adeo ob signum ambiguum ipsius m duplicantur. At vero meminisse oportet hinc casus excludi debere, quibus fit $x = y$. Tota ceterum haec evolutio mira facilitate expediri potest. Quod, ut exemplo ostendamus, sumamus $n = 7$ et $q = 4$, et pro signo inferiore habebimus $m = 73$, $y = 3$ et $x = 8$; tum vero $z = 215$. Erit igitur $8^4 + 73 \cdot 9 \cdot 64 + 81 = 215^2$, quod egregie congruit.

13. Ex his formulis valores pro littera m computavi, ubi quidem tantum ad numeros positivos respexi eosque omnes infra 200 in sequenti tabula exhibeo:

Catalogus valorum litterae m ex casu $p = 1$ desumtorum

2, 8, 12, 13, 16, 17, 23, 24, 26, 27, 31,
33, 36, 38, 41, 42, 44, 48, 49, 52, 55, 56,
[57], 61, 63, 64, 66, 67, 68, 71, 73, 77, 78,
79, 83, 84, 86, 87, 89, 90, 92[1]), 94, 95, 96,
100, 104, 106, 107, 112, 118, 122, 127, 128, 131, 132,
133, 134, 135, 137, 140, [141], 143, 151, 152[2]), 156, 159,
160, [161], 162, 166, 168, 169, 171, 172, 173, 174[3]), 177,
178, [181], 183, 184, 187, 188, 191, 194, 196, 197, 198,
199, 200[4]).

14. Formulae illae, ex quibus hi numeri sunt derivati, eo magis sunt faecundae, quo minor fuerit numerus λ, atque adeo, in quibus haec littera λ maiorem habet valorem, eae prorsus ad hunc finem sunt inutiles. Quamobrem plurimum interierit eas formulas, ubi λ est numerus satis parvus, hic apponere

$$\begin{aligned} m &= 2qq \pm (6, 34, 198, 1154 \text{ etc.}) \\ y &= 4, 24, 140, 816 \text{ etc.} \end{aligned}$$

1) Editio princeps: 91. Id est $92 = 2 \cdot 7^2 - 6$. Correxit A. M. et R. F.
2) Editio princeps: 153. Id est $152 = 35 \cdot 2^2 + 12$. Correxit A. M. et R. F.
3) Numerus 174 calculo probari non potuit. A. M. et R. F.
4) Numeri 57, 141, 161 et 181 desunt in editione principe: $57 = 5 \cdot 6^2 - 123$, $141 = 11 \cdot 7^2 - 398$, $161 = 3 \cdot 7^2 + 14$, $181 = 3 \cdot 31^2 - 2\,702$. A. M. et R. F.

$$\begin{aligned} m &= 3qq \pm (4, 14, 52, 194, 724, 2702 \text{ etc.}) \\ y &= 2, 8, 30, 112, 418, 1560 \text{ etc.} \end{aligned}$$

$$\begin{aligned} m &= 5qq \pm (3, 7, 18, 47, 123, 322, 843 \text{ etc.}) \\ y &= 1, 3, 8, 21, 55, 144, 377 \text{ etc.} \end{aligned}$$

$$\begin{aligned} m &= 6qq \pm (10, 98, 970, 9602 \text{ etc.}) \\ y &= 4, 40, 396, 3920 \text{ etc.} \end{aligned}$$

$$\begin{aligned} m &= 7qq \pm (16, 254, 4048 \text{ etc.}) \\ y &= 6, 96, 1530 \text{ etc.} \end{aligned}$$

$$\begin{aligned} m &= 10qq \pm (38, 1442 \text{ etc.}) \\ y &= 12, 456 \text{ etc.} \end{aligned}$$

$$\begin{aligned} m &= 11qq \pm (20, 398 \text{ etc.}) \\ y &= 6, 120 \text{ etc.} \end{aligned}$$

$$\begin{aligned} m &= 15qq \pm (8, 62, 488 \text{ etc.}) \\ y &= 2, 16, 126 \text{ etc.} \end{aligned}$$

Quoniam numeri supra dati ex solo casu $p = 1$ sunt deducti, nisi reliqui casus praeterea alios praebeant, omnes illos numeros, qui in catalogo non continentur, iis forent adnumerandi, de quibus demonstratum est formulam propositam numquam quadratum reddi posse, id quod mox accuratius explorabimus.

Evolutio casus secundi, quo $p = 2$

15. Hic ergo erit $nn - 64 = \lambda yy$ et $m = \frac{\lambda qq \pm n}{4}$, $x = 4q$ et $z = 2nqq \pm yy$, ubi statim evidens est pro n nullos numeros impariter pares, seu formae $4i + 2$, accipi posse, quia alioquin m nullo modo integer fieri posset. At si pro n numerus pariter par sumeretur, etiam q par esse deberet, ac tum formula pro m data iam in casu praecedente contineretur; unde patet pro n non nisi numeros impares accipi debere. Sumto igitur $n = 1$ erit $\lambda yy = -63$ ideoque $\lambda = -7$ et $y = 3$, unde habebitur $m = \frac{-7qq \pm 1}{4}$, ubi solum signum inferius valebit; pro q vero numeros impares assumi conveniet. Posito igitur $q = 2t + 1$ reperitur $m = -7(tt + t) - 2$, unde tantum numeri negativi resultant. Tum autem erit $x = 4(2t + 1)$ et $z = 2(2t + 1)^2 - 9$.

16. Quo autem numeros positivos non nimis magnos obtineamus, sumamus $n = 17$, eritque $nn - 64 = 9 \cdot 25 = \lambda yy$, unde fit $\lambda = 1$ et $y = 15$; tum vero erit $m = \frac{qq - 17}{4}$, $x = 4q$ et $z = 34qq - 225$. Statuatur $q = 1 + 2t$, erit in integris $m = tt + t - 4$, tum vero

$$x = 4(1 + 2t) \quad \text{et} \quad z = 34(1 + 2t)^2 - 225 .$$

Hinc pro valoribus

$$t = 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10,\ 11,\ 12 \quad \text{etc.}$$

nascitur

$$m = -2,\ 2,\ 8,\ 16,\ 26,\ 38,\ 52,\ 68,\ 86,\ 106,\ 128,\ 152 \quad \text{etc.},$$

qui autem numeri omnes, solo ultimo excepto, in superiore catalogo continentur[1]).

17. Simili ratione casus, quibus sumitur $p = 3,\ 4,\ 5,\ 6$ etc., tractari possent. Numeri autem, qui pro m inveniuntur, plerumque iam in superiore tabula reperiuntur. Hic autem adhuc adiiciam casus nonnullos, qui novos valores pro n praebent, inter quos praecipue summam attentionem meretur casus $m = 60$, qui praeter omnem expectationem se obtulit posito $p = 7$, ita ut

$$nn - 4 \cdot 7^4 = (n - 98)(n + 98) = \lambda yy \quad \text{et} \quad m = \frac{\lambda qq \pm n}{49} ;$$

tum vero $x = 14q$ et $z = 2nqq \pm yy$. Sumsi autem $n = 102$, ut fieret $\lambda yy = 4 \cdot 200$, unde fit $\lambda = 2$ et $y = 20$, hincque colligitur $m = \frac{2qq \pm 102}{49}$, qui numerus evadit integer sumendo $q = 39$ et adhibendo signum inferius; prodit enim $m = 60$, ubi $x = 14 \cdot 39$ et $y = 20$, sive semisses sumendo $x = 273$ et $y = 10$.

18. Eodem modo novum valorem $m = 189$ erui ex casu $p = 8$, unde fit $\lambda yy = (n - 128)(n + 128)$. Sumsi igitur $n = 297$, ut fieret $\lambda yy = 169 \cdot 425$, sive $\lambda yy = 17 \cdot 25 \cdot 169$, ita ut $\lambda = 17$ et $y = 5 \cdot 13 = 65$. Tum vero erit $m = \frac{17qq \pm 297}{64}$, quae expressio[2]) ad numerum integrum perducit ponendo $q = 27$; fit enim $m = 189$, pro quo valore erit $x = 16 \cdot 27$, $y = 65$, $z = 594 \cdot 27^2 - 65^2$.

1) Confer notam 2, p. 40. R. F.
2) pro signo inferiore. R. F.

19. Catalogo valorum idoneorum pro m etiam hos adnumerandos esse deprehendi: $m = 99$, $m = 145$ et $m = 155$. Priore casu fit $x = 312$, $y = 215$, $z = 676081$, secundo casu $x = 159$, $y = 40$ et tertio $x = 104$, $y = 95$. Neque tamen asseverare ausim me hoc modo omnes valores pro m infra 200 obtinuisse, cum formulae tantopere complicatae perduxerint ad novos valores infra 200. Hinc patet istam investigationem maxime esse arduam[1]).

METHODUS ELEGANTIOR

inveniendi numeros m, ut fiat $x^4 + mxxyy + y^4 = zz$.

20. Sumto pro lubitu numero α fiat $\alpha\alpha - 4 = \lambda\beta\beta$, et supra ostensum est[2]), si capiatur $m = \lambda\zeta\zeta \pm \alpha$, fore $x = \beta$, $y = 2\zeta$ et $z = \beta\beta \pm 2\alpha\zeta\zeta$, quod autem mox denuo demonstrabitur. Iam quia praecipuum momentum in numero λ situm est, notetur innumeros dari posse pro α valores, qui idem λ producant. Ad hos valores inveniendos sequentes formentur binae series recurrentes ex scala relationis α, -1 formatae[3]):

0,	1,	2,	3, ...	n
2,	α,	$\alpha\alpha - 2$,	$\alpha^3 - 3\alpha$, ...	$\mathfrak{A}$
0,	β,	$\alpha\beta$,	$\alpha\alpha\beta - \beta$, ...	$\mathfrak{B}$

eritque

$$\mathfrak{A} = \left(\frac{\alpha + \beta\sqrt{\lambda}}{2}\right)^n + \left(\frac{\alpha - \beta\sqrt{\lambda}}{2}\right)^n,$$

tum vero etiam

$$\mathfrak{B}\sqrt{\lambda} = \left(\frac{\alpha + \beta\sqrt{\lambda}}{2}\right)^n - \left(\frac{\alpha - \beta\sqrt{\lambda}}{2}\right)^n.$$

21. Iam cum sit $\left(\frac{\alpha + \beta\sqrt{\lambda}}{2}\right)\left(\frac{\alpha - \beta\sqrt{\lambda}}{2}\right) = 1$, erit $\mathfrak{A}^2 - \lambda\mathfrak{B}^2 = 4$, ita ut $\mathfrak{A}^2 - 4 = \lambda\mathfrak{B}^2$, quae forma cum similis sit primae, sequitur, sumto $m = \lambda ff \pm \mathfrak{A}$, ubi f iterum ab arbitrio pendet, fore $x = \mathfrak{B}$, $y = 2f$ et $z = \mathfrak{B}^2 \pm 2\mathfrak{A}ff$, cuius veritas immediate ex formula proposita ostenditur; fiet enim

$$z = \sqrt{x^4 + mxxyy + y^4} = \mathfrak{B}^2 \pm 2\mathfrak{A}ff.$$

---

1) Editio princeps post paragraphum 19 continet Supplementum (§ 26—§ 28 huius editionis). Hic ordo ab editoribus editionis principis certe per errorem adhibitus est, quia methodo § 20—§ 25 exposita in calculis supplementi necessario utitur. Hancobrem § 22—§ 27 editionis principis numeris 20—25 affectae sunt. R. F.

2) Hoc loco EULERUS casum $p = 1$ mutatis notationibus denuo tractat. R. F.

3) id est: $\alpha\mathfrak{A}_{n-1} - \mathfrak{A}_{n-2} = \mathfrak{A}_n$, $\alpha\mathfrak{B}_{n-1} - \mathfrak{B}_{n-2} = \mathfrak{B}_n$. R. F.

22. Percurramus casus simpliciores, quibus λ non nimis magnum prodit, eosque hic exhibeamus

$\alpha = 3$	$\mathfrak{A} = 2, 3, 7, 18, 47, 123, 322, 843$ etc.
$\beta = 1$	$\mathfrak{B} = 0, 1, 3, 8, 21, 55, 144, 377$ etc.
$\lambda = 5$	$m = 5ff \pm \mathfrak{A}$[1]
$\alpha = 4$	$\mathfrak{A} = 2, 4, 14, 52, 194, 724, 2702$ etc.
$\beta = 2$	$\mathfrak{B} = 0, 2, 8, 30, 112, 418, 1560$ etc.
$\lambda = 3$	$m = 3ff \pm \mathfrak{A}$[1]
$\alpha = 5$	$\mathfrak{A} = 2, 5, 23, 110, 527, 2525$ etc.
$\beta = 1$	$\mathfrak{B} = 0, 1, 5, 24, 115, 551$ etc.
$\lambda = 21$	$m = 21ff \pm \mathfrak{A}$
$\alpha = 6$	$\mathfrak{A} = 2, 6, 34, 198, 1154$ etc.
$\beta = 4$	$\mathfrak{B} = 0, 4, 24, 140, 816$ etc.
$\lambda = 2$	$m = 2ff \pm \mathfrak{A}$[1]
$\alpha = 8$	$\mathfrak{A} = 2, 8, 62, 488$ etc.
$\beta = 2$	$\mathfrak{B} = 0, 2, 16, 126$ etc.
$\lambda = 15$	$m = 15ff \pm \mathfrak{A}$[1]
$\alpha = 10$	$\mathfrak{A} = 2, 10, 98, 970$ etc.
$\beta = 4$	$\mathfrak{B} = 0, 4, 40, 396$ etc.
$\lambda = 6$	$m = 6ff \pm \mathfrak{A}$[1]
$\alpha = 11$	$\mathfrak{A} = 2, 11, 119, 1298$ etc.
$\beta = 3$	$\mathfrak{B} = 0, 3, 33, 360$[2] etc.
$\lambda = 13$	$m = 13ff \pm \mathfrak{A}$[1]
$\alpha = 16$	$\mathfrak{A} = 2, 16, 254, 4048$ etc.
$\beta = 6$	$\mathfrak{B} = 0, 6, 96, 1530$ etc.
$\lambda = 7$	$m = 7ff \pm \mathfrak{A}$.

Ex his igitur valoribus plurimos valores idoneos pro m derivari [sic] poterunt tam positivos quam negativos. Praeterea notandum est pro λ etiam numeros fractos accipi posse, ita tamen, ut inde pro m numeri integri oriantur.

1) Vide paragraphum 11, quae easdem solutiones continet. R. F.

2) Editio princeps: 352. Correxit A. M.

SOLUTIO GENERALIS

23. Introducendo igitur fractiones ponamus $\alpha = \frac{a}{c}$ et $\beta = \frac{b}{c}$, ita ut $aa - 4cc = \lambda bb$, et ambae series recurrentes erunt:

$$2, \frac{a}{c}, \frac{aa-2cc}{cc}, \frac{a^3-3acc}{c^3}, \ldots \frac{A}{c^n}$$

$$0, \frac{b}{c}, \frac{ab}{cc}, \frac{aab-bcc}{c^3}, \ldots \frac{B}{c^n},$$

quarum denominatores secundum potestates ipsius c procedunt, numeratores vero seriem recurrentem constituunt, cuius scala relationis est $a, -cc$ [1]). Cum igitur sit $\mathfrak{A} = \frac{A}{c^n}$ et $\mathfrak{B} = \frac{B}{c^n}$, erit $A^2 - 4c^{2n} = \lambda B^2$; tum vero fiet $m = \frac{\lambda c^n ff \pm A}{c^n}$, existente $x = \frac{B}{c^n}$, $y = 2f$ et $z = \frac{B^2 \pm 2c^n Aff}{c^{2n}}$.

24. Evidens autem est valorem m integrum fieri non posse, nisi fuerit denominator c^n quadratum. Statuatur ergo $n = 2\nu$ et sumatur $f = \frac{\mathfrak{f}}{c^\nu}$, eritque $m = \frac{\lambda \mathfrak{f}\mathfrak{f} \pm A}{c^{2\nu}}$, ubi $\mathfrak{f}$ ita sumi oportet, ut numerator evadat divisibilis per denominatorem. Tum autem, quia pro x, y, z fractiones prodeunt et tantum ratio inter x et y in calculum ingreditur, multiplicetur per $c^{2\nu}$, fietque $x = B$ et $y = 2\mathfrak{f}c^\nu$, existente $z = B^2 \pm 2A\mathfrak{f}\mathfrak{f}$.

25. Hic observandum est plerumque signorum ambiguorum alterutrum tantum locum habere posse, casibus exceptis, quibus denominator $c^{2\nu}$ est summa duorum quadratorum, quibus casibus utrumque signum locum habet. Tum vero, si fuerit $a < 2c$, manifestum est valorem λ semper negativum fieri debere, unde, quia littera A signo ambiguo est affecta, pro m tam valores negativi quam positivi oriuntur.

SUPPLEMENTUM

De valoribus numeri m, ut haec formula $x^4 - mxxyy + y^4$ fiat quadratum

26. Evidens est hoc negotium per formulas supra datas [2]) expediri posse, si modo littera m ibi negative capiatur; hocque modo id commodi nanciscimur,

1) id est: $aA_{n-1} - ccA_{n-2} = A_n$, $aB_{n-1} - ccB_{n-2} = B_n$. R. F.

2) in paragrapho 10. R. F.

ut pleraeque illarum formularum, ubi $\lambda > n$, nullum usum praestent; in quibus autem $\lambda < n$, inde certus tantum valorum numerus deduci possit. Omnes autem casus in sequentibus formulis continentur:

Casus		m	x	y
$c = 2$	$a = 1$	$2 + 15s + 15ss$	1	$4\ (1 + 2s)$
		$2 + 15s + 60ss$	7	$8\ (1 + 8s)$
		$2 + 45s + 240ss$	33	$16\ (3^{1}) + 32s)$
$c = 2$	$a = 3$	$2 + 7s + 7ss$	3	$4\ (1 + 2s)$
		$2 + 21s + 28ss$	3	$8\ (3 + 8s)$
		$2 + 35s + 112ss$	45	$16\ (5 + 32s)$
$c = 3^{2})$	$a = 2$	$2 + 16s + 18ss$	8	$6\ (4 + 9s)$
		$2 + 32s + 162ss$	112	$18\ (8 + 81s)$
$c = 3$	$a = 4$	$2 + 20s + 45ss$	8	$6\ (2 + 9s)$
		$2 + 80s + 405ss$	16	$18\ (8 + 81s)$
$c = 3$	$a = 5$	$2 + 22^{3})s + 99ss$	5	$6\ (1 + 9s)$
$c = 5$	$a = 1$	$2 + 66s + 275ss$	3	$10\ (3 + 25s)$
	$a = 1$	$9 + 88s + 275ss$	3	$10\ (4 + 25s)$
	$a = 2$	$2 + 48s + 150ss$	8	$10\ (4 + 25s)$
	$a = 2$	$4 + 36s + 150ss$	8	$10\ (3 + 25s)$
	$a = 6$	$2 + 12s + 25ss$	48	$10\ (6 + 25s)$
	$a = 6$	$2 + 16s + 25ss$	48	$10\ (8 + 25s)$
$c = 6$	$a = 11$	$2 + 23s + 207ss$	11	$12\ (1 + 18s)$
$c = 7$	$a = 2$	$2 + 48s + 147ss$	16	$14\ (8 + 49s)$
	$a = 4$	$2 + 60s + 245ss$	24	$14\ (6 + 49s)$
	$a = 11$	$2 + 30s + 147ss$	55	$14\ (5 + 49s)$
	$a = 13$	$2 + 18s + 147ss$	39	$14\ (3 + 49s)$
$c = 13$	$a = 10$	$2 + 20s + 169ss$	240	$26(10 + 169s)$
	$a = 10$	$2 + 48s + 169ss$	240	$26(24 + 169s)$

1) Editio princeps: 1. Correxit A. M.
2) Editio princeps: 2. Correxit A. M.
3) Editio princeps: 225. Correxit A. M.

27. Ex his formulis sequentes valores ipsius m, cum suis x et y, ad terminum 200 usque computavi:

m	x	y	m	x	y	m	x	y	m	x	y	m	x	y
32	1	12	51	3	88	132[6])	112	18.73	190	8	280	[186]	[11]	[12.17]
92	1	20	72	3	104	196	112	18.89	15	48	190	101	16	14.41
182	1	28	156	3	152	[27]	[8]	[42]	39	48	310	197	16	14.57
47	7	56	191[2])	3	168	[67]	[8]	[66]	78	48	440	187	24	14.43
[77]	[7]	[72]	79	45	16.27	[142]	[8]	[96]	126	48	560	119	55	14.44
197	33	16.29	149	45	16.37	79	5	48	191	48	690	179	55	14.54
16	3	12	4	8	30	123	5	60	11	48	170	[131]	[39]	[14.46]
44	3	20	36	8	78	196	3	210	43	48	330	[167]	[39]	[14.52]
86[1])	3	28	42	8	84[3])	104[7])	8	210	70	48	420	151	240	26.159
142	3	36	106	8	132[4])	200[8])	8	290	134	48	580	191	240	26.179
9	3	40	116	8	138[5])	118	8	220	179	48	670	123	240	26.145

28. Huic catalogo porro superstructa est sequens tabula completa omnium[9]) valorum m infra 200, quibus formula

$$x^4 - mxxyy + y^4$$

quadratum reddi potest:

1 , 2, 4, 9 , 11 , 13 , 15, 16, 25 , 26, 27 , 28,
36 , 39, 40, 42 , 43 , 44 , 47, 49, 51 , 64, 32 , 67,
70 , 72, 74, 76[10]), 77 , 78 , 79, 81, 86 , 89, 90 , 92,
96 , 100, 101, 102[10]), 103 , [104], 106, 109, 113 , [116], 118 ,
119 , 121, 123, 126 , [131], [132], 134, 136, 142 , 144, 146 ,
148 , 149, 151, 156 , 166 , 167 , 169, 179, 182 , [186],
[187], 188, 189, 190 , 191 , 193 , 196, 197, 198[10]), 200 .

1) Editio princeps: 76, 3, 25. Correxit A. M.
2) Editio princeps: 189. Correxit A. M.
3) Editio princeps: 96. Correxit A. M.
4) Editio princeps: 120. Correxit A. M.
5) Editio princeps: 150. Correxit A. M.
6) Editio princeps: 182. Correxit A. M.
7) Editio princeps: 102. Correxit A. M.
8) Editio princeps: 198. Correxit R. F.
9) Demonstratio omnes valores infra 200 in catalogo contineri deest. R. F.
10) Vide paragraphum 27, ubi *Eulerus* hunc numerum per errorem computavit. R. F.

DE BINIS FORMULIS SPECIEI $xx + myy$ ET $xx + nyy$ INTER SE CONCORDIBUS ET DISCORDIBUS

Commentatio 758 indicis ENESTROEMIANI
Mémoires de l'académie des sciences de St-Pétersbourg 8 (1817/8), 1822, p. 3—16
Conventui exhibuit die 5. junii 1780

1. In Analysi DIOPHANTEA frequentissime occurrere solent huiusmodi binae formulae, de quibus quaeritur, utrum ambae simul quadrata effici queant necne. Quod discrimen cum maximi sit momenti et ad insignes numerorum proprietates perducat, eas huius generis formulas, quae quadrata reddi possunt, vocabo *concordantes*, eas autem, ubi hoc nullo modo fieri potest, *discordantes*. Ita, cum demonstratum sit has formulas $xx + yy$ et $xx - yy$[1]) numquam simul quadrata effici posse, eae erunt discordantes; cuiusmodi etiam sunt hae duae formulae $xx + yy$ et $xx + 2yy$[1]) ac plurimae aliae nunc quidem cognitae. Contra vero etiam dantur innumerabiles formulae concordantes, cuiusmodi sunt $xx + yy$ et $xx + 7yy$. Sumto enim $x = 3$ et $y = 4$ fit $xx + yy = 5^2$ et $xx + 7yy = 11^2$. Quemadmodum igitur formulae concordantes et discordantes distingui queant, hic accuratius investigare constitui.

2. Primum autem observasse iuvabit huiusmodi binas formulas pluribus modis in alias transformari posse, quae eiusdem sint indolis. Ita hae duae formulae:

$$xx + myy = zz\,,$$
$$xx + n\,yy = vv\,,$$

1) Confer LEONHARDI EULERI: „*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 et Commentationem 702 indicis ENESTROEMIANI, *LEONHARDI EULERI Opera omnia*, series I, vol. 4, p. 255. R. F.

facile transmutantur in formas sequentes:

$zz - myy = xx$	$vv - nyy = xx$
$zz + (n - m)\,yy = vv$	$vv + (m - n)\,yy = zz$
$zz - xx = myy$	$vv - xx = nyy$
$(m - n)\,xx + nzz = mvv$ [1]	$mvv + (n - m)\,xx = nzz$

$$zz - vv = (m - n)\,yy$$
$$nzz - mvv = (n - m)\,xx\,.$$

Hae igitur sex variationes ita sunt comparatae, ut, si earum quaecunque fuerit vel concordans vel discordans, reliquae omnes eiusdem sint naturae. Quo praemisso solutio sequentis problematis maximi momenti erit censenda.

PROBLEMA

Proposita hac formula : $xx + myy = zz$, *ubi* m *denotet numerum integrum quemcunque, sive positivum sive negativum, investigare omnes formulas* $xx + nyy = vv$, *quae cum proposita sint concordantes.*

SOLUTIO

3. Hic igitur proposito quocunque numero m omnes numeri n requiruntur, quae cum forma proposita binas formulas concordantes exhibeant, quae ergo quaestio potissimum pendet ab indole numeri m, sive sit primus sive compositus. Si enim pluribus modis in duos factores inter se primos resolvi queat, etiam pluribus modis sequens investigatio institui poterit. Hancobrem statim ponamus $m = \mu\nu^2$); ubi facile patet, si m fuerit numerus primus vel potestas numeri primi, alterum factorum μ et ν unitati aequalem accipi debere. Quo plures autem numerus m contineat factores inter se primos, eo pluribus modis eum ad formam $\mu\nu$ revocare licebit.

4. Primo ergo in genere valores quantitatum x et y ita assignemus, ut formula proposita $xx + myy$ fiat quadratum, quod praestabitur sumendo $x = \pm(\mu pp - \nu qq)$ et $y = 2pq$; tum enim fiet $xx + myy = (\mu pp + \nu qq)^2$; ita ut hoc casu sit $z = \mu pp + \nu qq$. Iam hi valores in formula quaesita $xx + nyy = vv$ substituti dabunt hanc aequationem:

$$(\mu pp - \nu qq)^2 + 4npppqq = vv\,.$$

1) Editio princeps: nvv. Correxit A. M.
2) μ et ν sine factore communi. R. F.

5. Quare cum tota quaestio huc redeat, ut omnes idonei valores pro numero n investigentur, ex hac aequatione statim deducimus

$$n = \frac{vv - (\mu pp - \nu qq)^2}{4ppqq};$$

ubi loco formulae $\mu pp - \nu qq$ retineamus literam x, dummodo notetur eius valorem eo pluribus modis diversum esse posse, quo plures factores numerus propositus $m = \mu\nu$ complectatur. Simul vero etiam intelligitur literam x tam negative quam positive accipi posse. Hoc ergo modo habebimus numerum $n = \frac{vv - xx}{4ppqq}$, ubi ergo pro v omnes eiusmodi valores quaeri debebunt, ut numerator divisionem per denominatorem admittat. Quare cum numerator etiam in duos factores resolvi queat, ita ut sit

$$n = \frac{(v + x)\ (v - x)}{4ppqq},$$

primo evidens est utrumque numeratoris factorem parem esse debere; tum vero intelligitur, si alter per quempiam factorem ipsius $ppqq$ fuerit divisibilis, alterum eius complementum complecti debere. Evidens autem est hos binos valores ipsius $ppqq$ inter se primos esse debere, propterea quod numeri v et x necessario inter se sunt primi.

6. Hic primo quidem productum $ppqq$ statim praebet duos factores inter se primos pp et qq; ubi etiam pro altero sumi potest $ppqq$, pro altero vero unitas. Cum autem usu venire queat, ut productum $ppqq$ etiam aliis modis in duos factores inter se primos resolvi possit, quos semper quadratos esse debere manifestum est, ponamus generatim $ppqq = rrss$, atque litteram v ita determinemus, ut alter numeratoris factor $v + x$ divisibilis evadat per $2rr$, alter vero $v - x$ per $2ss$.

7. Hanc ob rem ponamus $v + x = 2frr$ et $v - x = 2gss$, ut hoc modo prodeat ipse numerus quaesitus $n = fg$. Ex illis vero aequalitatibus statim colligitur

$$v = frr + gss \quad \text{et} \quad x = frr - gss.$$

Cum autem quantitas x tamquam cognita spectari debeat, hic potissimum quaeritur, quales numeri pro f et g accipi debeant, ut fiat $frr - gss = x$, sive hoc problema erit resolvendum: quomodo datis numeris r, s, x definiri debeant f et g, ut huic conditioni $frr - gss = x$ satisfiat? Id quod, si numeri

r, s et x essent determinati, per notas Analyseos operationes facile praestari posset. At vero hic solutione generali est opus, quam sequenti modo obtinebimus.

8. Pro numeris rr et ss quaeramus ope methodi iam satis cognitae binos numeros ϱ et σ, ut fractio $\frac{\varrho}{\sigma}$ proxime accedat ad fractionem $\frac{rr}{ss}$, sive ut sit

$$\sigma rr - \varrho ss = \pm 1 .$$

Constat autem talem fractionem $\frac{\varrho}{\sigma}$ per eas operationes inveniri posse, quibus maximus communis divisor numerorum rr et ss quaeri solet. Hanc ob rem, quicunque numeri per rr et ss designentur, istos numeros ϱ et σ tamquam cognitos spectare licebit.

9. His igitur numeris ϱ et σ inventis capiamus

$$f = hss + \sigma x \quad \text{et} \quad g = hrr + \varrho x ,$$

tum enim, quia fieri debet $frr - gss = \pm x$, his valoribus substitutis fiet $frr - gss = x(\sigma rr - \varrho ss)$ ideoque ob $\sigma rr - \varrho ss = \pm 1$ utique evadet $frr - gss = [\pm]x$, hocque modo nostrum problema iam perfecte erit solutum. Cum enim sit $n = fg$, nunc erit

$$n = (hss + \sigma x)(hrr + \varrho x) ,$$

qui ergo valor semper producit numerum compositum, nisi alter factorum abeat in unitatem. Ubi meminisse oportet primo pro x plures assignatos fuisse valores pro factoribus numeri $m = \mu\nu$. Praeterea vero etiam pro r et s saepe plures dari possunt valores, ut fiat $rs = pq$, quae geminae varietates a se invicem non pendent, ita ut cum singulis valoribus ipsius x singulos valores ipsarum r et s combinare liceat. Ex quo patet hanc solutionem problematis maxime esse generalem, atque adeo omnes valores idoneos pro numero n continere.

10. Quoniam igitur hic inventio fractionis $\frac{\varrho}{\sigma}$, quae fractioni $\frac{rr}{ss}$ proxime sit aequalis, praecipue requiritur, istam aequalitatem proxime veram hoc signo $\boxplus$ designemus, ita ut sit $\frac{rr}{ss} \boxplus \frac{\varrho}{\sigma}$, quo nihil aliud significatur, nisi quod sit $\sigma rr - \varrho ss = \pm 1$. Sumtis ergo pro lubitu binis rr et ss, sequentem tabulam adiungo, quae numeros ϱ et σ indicat:

$rr : ss$	$\varrho : \sigma$	$rr : ss$	$\varrho : \sigma$	$rr : ss$	$\varrho : \sigma$
1 : 1	1 : 0	64 : 1	1 : 0	121 : 1	1 : 0
4 : 1	1 : 0	64 : 9	7 : 1	121 : 4	30 : 1
9 : 1	1 : 0	64 : 25	23 : 9	121 : 9	27 : 2
9 : 4	2 : 1	64 : 49	17 : 13	121 : 16	53 : 7
16 : 1	1 : 0			121 : 25	29 : 6
16 : 9	7 : 4	81 : 1	1 : 0	121 : 36	37 : 11
25 : 1	1 : 0	81 : 4	20 : 1	121 : 49	42 : 17
25 : 4	6 : 1	81 : 16	5 : 1	121 : 64	17 : 9
25 : 9	11 : 4	81 : 25	13 : 4	121 : 81	3 : 2
25 : 16	11 : 7	81 : 49	38 : 23	121 : 100	23 : 19
36 : 1	1 : 0	81 : 64	19 : 15		
36 : 25	13 : 9			144 : 1	1 : 0
49 : 1	1 : 0			144 : 25	23 : 4
49 : 4	12 : 1	100 : 1	1 : 0	144 : 49	47 : 16
49 : 9	11 : 2	100 : 9	11 : 1	144 : 121	25 : 21
49 : 16	3 : 1	100 : 49	49 : 24		
49 : 25	2 : 1	100 : 81	21 : 17		
49 : 36	15 : 11				

11. Ope huius tabulae facile erit solutionem problematis expedire. Sumantur enim pro r et s successive omnes valores a minimis 1 et 1 incipiendo, et pro singulis excerpantur numeri ϱ et σ; tum pro quolibet casu r et s quaerantur omnia producta pq ipsi rs aequalia, quod eo pluribus modis fieri poterit, quo plures affuerint factores. Tum vero pro singulis p et q quaerantur valores ipsius $x = \mu pp - \nu qq$, id quod duplici modo fieri poterit, quia etiam erit $x = \nu pp - \mu qq$. Quo facto singuli valores pro x inventi dabunt infinitos valores pro numero quaesito, cum sit

$$n = (hss \pm \sigma x)\,(hrr \pm \varrho x)\,,$$

hocque modo operationes continuando plurimos numeros pro n sumendos obtinebimus.

EXEMPLUM

Proposita formula $xx + yy = zz$ *investigare omnes formulas concordantes*

$$xx + nyy = vv\,^{1})\,.$$

12. Hic ergo erit $\mu = \nu = 1$ et $x = pp - qq$. Sumatur nunc $r = 2$ et $s = 1$, eritque $\varrho = 1$ et $\sigma = 0$. Quia igitur $rs = 2$, unico modo fiet $p = 2$ et $q = 1$, eritque $x = 3$, quocirca hinc habebimus $n = h(4h \pm 3)$, unde pro n iam deducuntur sequentes valores:

$$n = 1,\ 7,\ 10,\ 22,\ 27,\ 45,\ 52,\ 76,\ 85\ [\text{etc.}]\,.$$

Simili modo sumatur $r = 3$ et $s = 1$, ubi iterum erit $\varrho = 1$ et $\sigma = 0$, tum vero unico modo fiet $p = 3$ et $q = 1$, ideoque $x = 8$, hinc $n = h(9h \pm 8)$, unde oriuntur sequentes valores pro n:

$$1,\ 17,\ 20,\ 52,\ 57\ [\text{etc.}]\,.$$

Eodem modo sumtis $r = 3$ et $s = 2$, ut sit $\varrho = 2$ et $\sigma = 1$, habebimus duplici modo $p = 6$ et $q = 1$, et $p = 3$ et $q = 2$, unde duo casus nascuntur, scilicet $x = 35$, et $x = 5$. Ex priore orietur $n = (4h \pm 35)\,(9h \pm 70)$, unde infra centenarium nulli occurrunt valores praeter hos:

$$n = -6,\ 11,\ 49,\ 100\,.$$

At vero pro altero casu fiet $n = (4h \pm 5)\,(9h \pm 10)$, unde oriuntur hi valores:

$$n = 1,\ 24\,.$$

Hinc iam satis clare intelligitur, quomodo ulterius sit operandum.

Hoc autem modo calculum satis longe prosecuti pro n sequentes valores infra centenarium sumus adepti. Primo quidem istos positivos:

$n = 1, 7, 10, 11, 17, 20, 22, 24, 27, 30, 31, 34, 41, 42, 45, 49, 50, 52, 57,$
$[58], 59, 60, 61, 71, 72, 74, 76, [77], 79, 85, 86, 92, 94, 97, 99,$

tum vero negativos sequentes:

$$n = -6, -18, -35, [-36, -45], -47, -55, [-56],$$
$$-60, -76, -88, -90, -98\,.$$

1) Confer Commentationem 702: *De novo genere quaestionum arithmeticarum, pro quibus solvendis certa methodus adhuc desideratur*, nova acta sc. Petrop. 11 (1793), 1798, p. 78—93. *Leonhardi Euleri Opera omnia*, series I, vol. 4, p. 255—268.

13. Interim tamen asseverare non ausim nullos alios praeterea dari valores pro n. Quidam enim horum valorum orti demum sunt ex numeris satis magnis pro r et s assumtis. Veluti valor $n = 59$ prodiit ex numero $x = 11$, sive ex casu $p = 6$ et $q = 5$[1]), unde fit $y = 60$; tum enim utique erit

$$11^2 + 60^2 = 61^2 \quad \text{et} \quad 11^2 + 59 \cdot 60^2 = 461^2 .$$

Simili modo casus $n = 86$ ortus est ex valoribus $x = 1295$ et $y = 72$. Erit enim [2])

$$1295^2 + 72^2 = 1297^2$$
$$1295^2 + 86 \cdot 72^2 = 1457^2 .$$

Numerus autem $n = -47$ oritur ex casu $x = 612$ et $y = 35$. Erit enim[3]):

$$612^2 + 35^2 = 613^2 \quad \text{et} \quad 612^2 - 47 \cdot 35^2 = 563^2 .$$

14. Cum igitur neutiquam affirmare liceat omnes numeros in hac tabula non contentos dare formulas discordantes cum formula $xx + yy = zz$, methodum subiungam quamlibet formulam $xx + nyy = vv$ explorandi, utrum sit concordans an discordans cum formula $xx + yy = zz$. Ex casu autem notissimo formularum discordantium $xx + yy$ et $xx - yy$ supra iam derivavimus $xx + yy$ et $xx + 2yy$, quae certe etiam sunt discordantes. Quamobrem has formulas $xx + yy$ et $xx + 3yy$ hic ad examen revocabo.

PROBLEMA

Explorare, utrum hae duae formulae $xx + yy = \square$ *et* $xx + 3yy = \square$ *sint concordantes an discordantes.*

SOLUTIO

15. Numerorum x et y alter necessario erit par, alter impar. Facile autem patet in formula posteriore x non esse posse parem; foret enim y impar et $3yy$ numerus formae $8\alpha + 3$, qui cum quadrato pari numquam quadratum efficere potest. Erit ergo x impar et y par. Pro priore formula erit

$$x = pp - qq \quad \text{et} \quad y = 2pq ,$$

1) Editio princeps: $r = 6$ et $s = 5$. Casus $n = 59$ ortus est ex valoribus $r = 15$, $s = 2$, $\varrho = 56$, $\sigma = 1$, $n = (4h \pm 11)$ $(225h \pm 616)$ pro $h = 3$. Correxit R. F.

2) $r = 9$, $s = 4$, $\varrho = 5$, $\sigma = 1$, $x = 1295$, $n = (16h \pm 1295)$ $(81h \pm 6475)$ pro $h = 81$. R. F.

3) Ex casu $r = 7$, $s = 5$, $x = 1224$. R. F.

ubi ergo iterum numerorum p et q alter est par, alter impar. Hinc igitur posterior formula evadet

$$xx + 3yy = p^4 + 10ppqq + q^4 = \square ,$$

quae formula reducitur ad hanc:

$$(pp + qq)^2 + 2(2pq)^2 .$$

Statuamus ergo $pp + qq = \pm rr \mp 2ss$ et $2pq = 2rs$ ideoque $pq = rs$.

16. Hic iam tuto assumere licet $q = 1$, siquidem pro p, r, s etiam fractiones admittere velimus. Habebimus ergo $p = rs$ et nostra aequatio erit $rrss + 1 = \pm (rr - 2ss)$. Ex signis superioribus deducimus

$$rr = \frac{1 + 2ss}{1 - ss} ,$$

quae fractio, si loco s scribamus $\frac{s}{t}$, reducitur ad hanc $\frac{tt + 2ss}{tt - ss}$, quae, an quadratum producere queat necne, quaeritur.

17. Hic ante omnia est observandum numeratorem et denominatorem alium divisorem communem habere non posse praeter ternarium, unde uterque vel ipse erit quadratum vel triplum quadratum. Priore casu ergo habebimus $tt + 2ss = aa$ et $tt - ss = bb$, unde fit $tt = bb + ss$ et $aa = bb + 3ss$, quae formulae similes sunt ipsis propositis, ideoque eandem sortem sequentur. Posteriore casu erit $tt + 2ss = 3aa$ et $tt - ss = 3bb$. Ex posteriore erit $tt = ss + 3bb$, unde fit $3aa = 3ss + 3bb$, sive $aa = ss + bb$, quae formulae iterum ipsi propositae sunt similes.

18. Ex inferioribus signis erit $rr = \frac{2ss - 1}{ss + 1}$, ubi iterum loco s scribamus $\frac{s}{t}$, quo fiat

$$rr = \frac{2ss - tt}{ss + tt} ,$$

ubi divisor communis praeter ternarium non datur. Casus, quo numerator et denominator sunt primi inter se, praebet $2ss - tt = aa$, $ss + tt = bb$, ubi statim ingens absurdum se offert. Summa enim foret $aa + bb = 3ss$. Constat autem summam duorum quadratorum numquam per 3 dividi posse. Sumatur $2ss - tt = 3aa$ et $ss + tt = 3bb$, unde sequitur $ss = aa + bb$, hincque porro $tt = 2bb - aa$ et $ss + tt = 3bb$, quod iterum per se est absurdum.

19. Ex his coniunctim iam sequitur, si formulae propositae essent concordantes, ex iis aliae eiusdem indolis sequerentur, atque adeo multo minores; quamobrem, cum in minoribus numeris nullus casus possibilis assignari queat, evictum est ambas formulas propositas esse discordantes.

PROBLEMA

Proposita formula $xx + yy = \square$ *explorare, utrum haec formula* $xx + 4yy = \square$ *sit concordans necne.*

SOLUTIO

20. Hic statim patet x esse debere numerum imparem. Iam pro priore ponatur $x = pp - qq$ et $y = 2pq$; ubi patet numerorum p et q alterum debere esse parem, alterum imparem. Hinc altera formula fiet

$$xx + 4yy = p^4 + 14ppqq + q^4 = \square ,$$

quae formula abit in hanc:

$$(pp + qq)^2 + 3(2pq)^2 = \square ,$$

ubi prius quadratum est impar. Ponatur ergo $pp + qq = \pm (rr - 3ss)$, $2pq = 2rs$ sive $pq = rs$. Hic si quemquam offendat, quod ante sumserimus $q = 1$, calculum in integris instituamus, sumendo $pq = rs = abcd$, et ponamus $p = ab$, $q = cd$, $r = ac$, $s = bd$, quibus valoribus substitutis erit:

$$aabb + ccdd = \pm (aacc - 3bbdd) .$$

21. Signum superius nobis dabit

$$\frac{aa}{dd} = \frac{cc + 3bb}{cc - bb} ,$$

cuius numerator et denominator alium factorem communem habere nequit excepto numero 4[1]), qui cum ipse sit quadratum, necesse est, ut uterque fiat quadratum. Statuatur ergo $cc + 3bb = ff$ et $cc - bb = gg$, eritque

$$cc = bb + gg \quad \text{et} \quad 4bb + gg = ff ,$$

quae formulae conveniunt cum ipsis propositis, quorum tamen termini minores sunt quam x et y.

1) c et b sine factore communi. R. F.

22. Signa inferiora nobis dabunt

$$\frac{aa}{dd} = \frac{3bb - cc}{bb + cc},$$

ubi alius divisor communis non occurrit praeter 4; unde tam numerator quam denominator debet esse quadratum. Quodsi ergo ponatur

$$3bb - cc = ff \quad \text{et} \quad bb + cc = gg,$$

ex priore erit $3bb = cc + ff$, quod iam est absurdum. Cum igitur ista operatio vel perducat ad formulas propositis similes, vel contradictionem involvat, hoc certum est signum formulas propositas esse discordantes.

23. Hic autem iure obiici potest fieri posse, ut numerator et denominator fiant dupla quadrata, scilicet $3bb - cc = 2ff$ et $bb + cc = 2gg$, quod revera fieri sponte patet, casu $b = c$, unde fit $f = g = b$, consequenter etiam $a = d$, $p = q$, ideoque $x = 0$, quo ergo casu utique ambae formulae propositae fient quadrata. Hoc autem aliis casibus evenire numquam posse hoc modo ostendi potest. Cum enim hinc fiat $cc = 2gg - bb$ et $2bb - gg = ff$, ista quatuor quadrata cc, gg, bb, ff forent in progressione arithmetica, quod autem numquam fieri posse iam dudum[1]) est demonstratum solo casu excepto, quo inter se sunt aequalia.

24. Subiungamus autem adhuc casum, quo binae formulae propositae revera sunt concordantes.

PROBLEMA

Proposita formula $xx + yy = \square$ *explorare, utrum haec formula:*
$xx + 7yy = \square$ *sit concordans necne.*

SOLUTIO

25. Pro priore sumamus ut hactenus $x = pp - qq$ et $y = 2pq$, et posterior dabit

$$p^4 + 26ppqq + q^4 = \square,$$

quae transformatur in hanc:

$$(pp + qq)^2 + 6(2pq)^2 = \square,$$

pro qua poni potest primo $pp + qq = \pm(rr - 6ss)$ et $pq = rs$, vel secundo $pp + qq = \pm(3rr - 2ss)$ et $pq = rs$. Pro utraque ergo statuamus

1) Id est $gg - cc = bb - gg = ff - bb$. Vide § 34 huius Commentationis. R. F.

$pq = rs = abcd$, sitque $p = ab$, $q = cd$, $r = ac$, $s = bd$, sicque pro prima formula habebimus:

$$aabb + ccdd = \pm (\ aacc - 6bbdd),$$

et pro altera

$$aabb + ccdd = \pm (3aacc - 2bbdd).$$

Ob signa ergo ambigua quatuor casus sunt evolvendi.

26. Pro priore casu erit

$$\frac{aa}{dd} = \frac{cc + 6bb}{cc - bb},$$

ubi, cum divisor communis sit [unitas aut] 7, primo fiat

$$cc + 6bb = ff \quad \text{et} \quad cc - bb = gg,$$

unde fit $cc = bb + gg$ et $ff = 7bb + gg$, quae formulae ipsis propositis sunt similes. Ponamus porro $cc + 6bb = 7ff$ et $cc - bb = 7gg$; hincque fiet $cc = bb + 7gg$ et $ff = bb + gg$, quae denuo propositis sunt similes.

27. Pro secundo casu erit

$$\frac{aa}{dd} = \frac{6bb - cc}{bb + cc},$$

ubi iterum divisor communis esse potest 7; quare statuendo $6bb - cc = ff$ et $bb + cc = gg$ foret $6bb = cc + ff$, quod est absurdum. Statuamus ergo $6bb - cc = 7ff$ et $bb + cc = 7gg$, quae posterior suppositio iam per se est absurda.

28. Tertius casus dat

$$\frac{aa}{dd} = \frac{cc + 2bb}{3cc - bb},$$

ubi divisor communis iterum est [unitas aut] 7. At vero ponendo hic $cc + 2bb = ff$ et $3cc - bb = gg$ foret $3cc = bb + gg$, quod denuo est absurdum. Statuamus ergo $cc + 2bb = 7ff$ et $3cc - bb = 7gg$, hinc fit $cc = 7ff - 2bb$ et $gg = 3ff - bb$ sive $3ff = bb + gg$, quod est absurdum.

29. Restat igitur quartus casus, qui dat

$$\frac{aa}{dd} = \frac{2bb - cc}{bb + 3cc},$$

ubi statim in oculos occurrit casum $b = c = 1$ satisfacere; tum enim fiet $a = 1$ et $d = 2$. Hinc autem nanciscimur $p = 1$, $q = 2$, ideoque $x = 3$ et $y = 4$; unde utique fiet

$$xx + yy = 5^2 \quad \text{et} \quad xx + 7yy = 11^2 ,$$

consequenter evidens est formulas propositas esse concordantes.

SUPPLEMENTUM

30. Cum solutio penultimi problematis non satis sit concinna et perspicua, eius loco sequens theorema subiungamus.

THEOREMA

Hae duae formulae $xx + yy = \square$ *et* $xx + 4yy = \square$ *sunt discordantes sive impossibile est pro* x *et* y *eiusmodi valores assignare, qui utramque reddant quadratum exceptis duobus casibus* $x = 0$ *et* $y = 0$.

DEMONSTRATIO

31. Incipiamus a posteriore formula $xx + 4yy$, quae cum etiam sit summa duorum quadratorum, certe erit $x = pp - qq$ et $y = pq$; tum enim fiet $xx + 4yy = (pp + qq)^2$. Hinc autem prior formula hanc induet formam:

$$p^4 - ppqq + q^4 = \square ,$$

quae manifesto aequivalet huic:

$$(pp + qq)^2 - 3(pq)^2 = \square .$$

Quamobrem, quo hoc fiat, statuamus $pp + qq = rr + 3ss$ et $pq = 2rs$. Sic enim fiet $xx + yy = (rr - 3ss)^2$.

32. Statuamus porro $pq = 2rs = 2abcd$, fiatque $p = 2ab$, erit $q = cd$; tum vero sit $r = ac$, erit $s = bd$, qui valores substituti hanc praebent aequationem:

$$4aabb + ccdd = aacc + 3bbdd ,$$

unde sequitur

$$\frac{aa}{dd} = \frac{3bb - cc}{4bb - cc}$$

vel etiam

$$\frac{aa}{dd} = \frac{cc - 3bb}{cc - 4bb} ;$$

ubi, cum nullus divisor communis occurrat, siquidem tam p et q quam r et s supponantur primi inter se, tam numerator quam denominator seorsim debet esse quadratum. Pro priore ergo ponatur $3bb - cc = ff$ et $4bb - cc = gg$, quae utraque positio est absurda. Quare pro altera formula ponamus $cc - 3bb = ff$ et $cc - 4bb = gg$. Ex ista statim fit $cc = gg + 4bb$, unde altera evadit $ff = gg + bb$, quae cum sint ipsis propositis perfecte similes atque minores, manifesto hinc sequitur veritas theorematis.

COROLLARIUM 1

33. Cum igitur istae formulae $xx + yy$ et $xx + 4yy$ sint discordantes, etiam omnes eius variationes initio memoratae erunt discordantes, scilicet

$xx + yy = zz$	$zz - yy = xx$	$vv - 4yy = xx$
$xx + 4yy = vv$	$zz + 3yy = vv$	$vv - 3yy = zz$
$zz - xx = yy$	$vv - xx = 4yy$	$vv - zz = 3yy$
$4zz - 3xx = vv$[1])	$vv + 3xx = 4zz$	$4zz - vv = 3xx$

COROLLARIUM 2

34. Praeterea vero etiam illae formulae, ad quas in solutione superiore sumus perducti, certe sunt discordantes, scilicet:

$$2bb - gg = ff,$$
$$2gg - bb = cc,$$

quoniam non dantur quatuor quadrata in progressione arithmetica. Hinc ergo etiam omnes variationes erunt discordantes, quae sunt:

$2xx - yy = zz$	$2xx - zz = yy$	$yy + zz = 2xx$
$2yy - xx = vv$	$3xx - 2zz = vv$	$3yy - zz = 2vv$
$2yy - vv = xx$	$xx + vv = 2yy$	$2zz + vv = 3xx$
$3yy - 2vv = zz$	$3xx - vv = 2zz$	$zz + 2vv = 3yy$

COROLLARIUM 3

35. Denique etiam formulae biquadraticae, quae se obtulerunt, sunt impossibiles. Ita, cum ex theoremate sit $p^4 - ppqq + q^4 = \square$ impossibilis, impossibilis quoque erit haec forma: $p^4 + 14ppqq + q^4 = \square$, hincque etiam plures aliae formulae, quae per transformationem hinc formari possunt.

1) Editio princeps: $4vv$. Correxit A. M.

DE TRIBUS PLURIBUSVE NUMERIS INVENIENDIS QUORUM SUMMA SIT QUADRATUM QUADRATORUM VERO SUMMA BIQUADRATUM[1]

Commentatio 763 indicis ENESTROEMIANI
Mémoires de l'académie des sciences de St-Pétersbourg 9 (1819/20), 1824, p. 3—13
Conventui exhibita die 18. maii 1780

1. Celebre est et nuper ab illustri LAGRANGE singulari studio pertractatum problema a FERMATIO olim propositum, quo quaeruntur duo numeri integri positivi, quorum summa sit quadratum, quadratorum vero summa biquadratum[2]). Hinc occasionem arripui istam quaestionem ad tres pluresve numeros extendendi, certa spe fretus eius solutionem sine tantis ambagibus expediri posse. Postquam autem rem tentassem, mox deprehendi easdem difficultates, quibus ipsum problema FERMATIANUM involvitur. Tandem vero omnia haec obstacula feliciter superavi atque adeo satis modicos numeros quaestioni satisfacientes sum adeptus, dum minimi numeri problematis FERMATIANI ultra billionem ascendunt. Istam igitur methodum, qua sum usus, hic propositurus ero, postquam scilicet prima tentamina, longissimos calculos minantia, in medium attulero.

2. Sint x, y, z tres numeri positivi, quorum summa debeat esse $= AA$, quadratorum vero summa $xx + yy + zz = B^4$, atque ob numeros positivos statim patet esse debere $A^4 > B^4$ ideoque $A > B$, propterea quod A^4 praeter ipsa quadrata xx, yy, zz insuper duplicia producta ex binis complectitur. Cum igitur sit $x = AA - y - z$, posui $y + z = p$ et $y - z = q$, unde fit $yy + zz = \frac{pp + qq}{2}$. Quia ergo habemus $x = AA - p$, aequatio secunda dabit

1) Confer IV. problema Commentationis 560 indicis ENESTROEMIANI: *Miscellanea analytica.* Opuscula analytica 1, 1783. *LEONHARDI EULERI Opera omnia*, series I, vol. 4, p. 96. R. F.

2) LAGRANGE: *Sur quelques problèmes de l'analyse de Diophante.* Nouv. Mém. de l'acad. royale d. Sc. et B. L. de Berlin, 1777. *Oeuvres*, publiées p. J.-A. Serret, Paris, 1869, t. IV, p. 377. Vide praecipue p. 379/80. R. F.

$$A^4 - 2AAp + pp + \frac{pp+qq}{2} = B^4,$$

unde deducimus $qq = 2(B^4 - A^4) + 4AAp - 3pp$, quae formula nullo modo quadratum reddi potest, nisi constet unicus saltem casus, quo hoc eveniat.

3. Quodsi formula $2B^4 - 2A^4$ evadere posset quadratum, quod autem est impossibile, res nulla laboraret difficultate. Relinquitur igitur casus, ubi $2B^4 - A^4$ fit quadratum, puta $= CC$; tum enim erit

$$qq = CC - A^4 + 4AAp - 3pp,$$

quae forma reducta ad $qq = CC - (AA - p)(AA - 3p)$ statim praebet hanc positionem: $q = C - v(AA - p)$, qua evoluta reperitur

$$p = \frac{-2Cv + AA(1+vv)}{3+vv},$$

hocque valore substituto prodit

$$q = \frac{3C - 2AAv - Cvv}{3+vv}.$$

4. Cum autem hic ante omnia binis litteris A et B eiusmodi valores tribui debeant, ut fiat $2B^4 - A^4 = CC$, hoc modo ad ipsum problema FERMATIANUM revolvimur. Quare cum tales valores non nisi in maximis numeris exhiberi queant, nulla plane spes affulget huius methodi ope ad solutiones in modicis numeris perveniendi. — Alia igitur nobis ineunda erit via huiusmodi quaestiones tractandi, quae a tantis difficultatibus sit immunis. Talis autem via se mihi optimo successu obtulit, cuius vis quo melius perspiciatur, ab ipso problemate FERMATIANO inchoabo.

PROBLEMA I

Invenire duos numeros integros positivos x et y, quorum summa sit quadratum, quadratorum vero summa biquadratum.

SOLUTIO

5. Incipiamus a posteriore conditione. Ac primo quidem formula $xx + yy$ reddetur quadratum, ponendo $x = aa - bb$ et $y = 2ab$; tum enim erit $xx + yy = (aa + bb)^2$. Insuper igitur haec formula $aa + bb$ quadratum

reddi debet, quod pari modo fiet ponendo $a = pp - qq$ et $b = 2pq$; hoc enim modo proveniet $xx + yy = (pp + qq)^4$, sicque posteriori conditioni iam plene est satisfactum. Tantum igitur superest, ut priori conditioni, qua $x + y$ quadratum effici debet, satisfiat.

6. Ex factis igitur positionibus reperitur

$$x = aa - bb = p^4 - 6ppqq + q^4 \quad \text{et} \quad y = 4p^3q - 4pq^3 \ ;$$

quamobrem sequens formula quarti gradus ad quadratum reduci debet:

$$p^4 + 4p^3q - 6ppqq - 4pq^3 + q^4 \, ,$$

pro quo efficiendo praenotandum est binos numeros p et q esse debere positivos. Deinde etiam necesse est, ut sit $p > q$, quia aliter numerus y fieret negativus. Denique etiam requiritur, ut fiat $a > b$, ut pro x prodeat numerus positivus.

7. Formula autem inventa resolvetur ponendo eius radicem:

$$\sqrt{x + y} = pp - 2pq + qq \, ,$$

unde colligitur $\frac{p}{q} = \frac{3}{2}$ sive $p = 3$ et $q = 2$, qui ergo numeri iam sunt positivi, et $p > q$. Quia autem hinc fit $a = 5$ et $b = 12$, pro x resultat valor negativus, reiiciendus. Hanc ob rem secundum praecepta cognita novam operationem institui oportebit, quem in finem maneat $q = 2$ at vero statuamus $p = 3 + v$, unde sequentes valores deducimus:

$$\begin{aligned} p^4 &= 81 + 108v + 54vv + 12v^3 + v^4 \, , \\ 4p^3q &= 216 + 216v + 72vv + 8v^3 \, , \\ 6p^2q^2 &= 216 + 144v + 24vv \, , \\ 4pq^3 &= 96 + 32v \, , \\ q^4 &= 16 \, , \end{aligned}$$

quibus collectis formula supra data hanc formam induit:

$$1 + 148v + 102vv + 20v^3 + v^4 = x + y \, ,$$

cuius radix, si statuatur

$$\sqrt{x + y} = 1 + 74v - vv \, ,$$

perducit ad hanc aequationem: $1343 = 42v$ sive $v = \frac{1343}{42}$; unde fit $p = 3 + v = \frac{1469}{42}$, existente $q = 2$. Hae ergo litterae ad numeros integros perductae fient $p = 1469$ et $q = 84$. Ex his porro colligitur $a = 1385 \cdot 1553$ et $b = 168 \cdot 1469$ sive $a = 2150905$ et $b = 246792$. Unde manifestum est ob $a > b$ etiam ipsos numeros x et y ambos proditurus esse positivos, qui, etsi adeo billionem excedant, tamen sunt minimi problemati satisfacientes: Hi numeri autem sunt

$$x = 4{,}565{,}486{,}027{,}761$$
$$y = 1{,}061{,}652{,}293{,}520$$

qui sunt iidem, quos FERMATIUS aliique post eum invenerunt[1]). Eorum summa est quadratum numeri 2,372,159, quadratorum vero summa est biquadratum numeri 2,165,017.

PROBLEMA II

Invenire tres numeros integros positivos x, y, z, quorum summa sit quadratum, quadratorum vero summa biquadratum.

SOLUTIO

8. Incipiamus iterum a summa quadratorum, quae primo quadratum reddatur, ponendo $x = aa + bb - cc$, $y = 2ac$, $z = 2bc$; sic enim fiet $xx + yy + zz = (aa + bb + cc)^2$; ubi ergo $aa + bb + cc$ denuo quadratum effici debet, quod fiet ponendo simili modo $a = pp + qq - rr$, $b = 2pr$, $c = 2qr$; sic enim obtinebitur $xx + yy + zz = (pp + qq + rr)^4$, ita ut posterior conditio iam sit adimpleta.

9. Exprimamus nunc ipsas litteras x, y, z per p, q, r eritque:

$$x = p^4 + q^4 + r^4 + 2ppqq + 2pprr - 6qqrr,$$
$$y = 4qr(pp + qq - rr),$$
$$z = 8pqrr.$$

Hinc ergo erit:

$$x + y + z = p^4 + q^4 + r^4 + 2ppqq + 2pprr - 6qqrr + 4ppqr + 4q^3r - 4qr^3 + 8pqrr,$$

1) Vide Commentationem ipsius LAGRANGE p. 61, in nota 2) laudatam, p. 380, et *Oeuvres de* FERMAT, observationem 2 ad quaestionem XXVI, libris VI. Arithmeticorum Diophanti Alexandrini additam. *Oeuvres de* FERMAT, publiées p. M. P. Tannery, t. 1. Paris 1891, p. 336. R. F.

quae forma primum secundum potestates ipsius p disposita ita se habet:

$$x + y + z = p^4 + 2(q + r)^2 pp + 8pqrr + q^4 + 4q^3 r - 6qqrr - 4qr^3 + r^4 ,$$

quam ita quadratum reddi oportet, ut singulae litterae p, q, r fiant positivae, simulque sit $pp + qq > rr$. Praeterea vero etiam necesse est, ut valores litterarum a, b, c ita sint comparati, ut fiat $aa + bb > cc$.

10. Quia in hac formula potestas tertia ipsius p deest, radix statui poterit $pp + (q + r)^2$. Sic enim tam potestas quarta quam secunda tolletur, et ex residuis terminis definiri poterit $p = \frac{3}{2}q + r$, qui valor ob simplicitatem eius solutiones multo concinniores pollicetur, quam in praecedente problemate obtinuimus. Sumto autem $p = \frac{3}{2}q + r$ erit

$$a = \frac{13}{4} qq + 3qr, \quad b = 3qr + 2rr, \quad c = 2qr,$$

ubi iam ambas litteras q et r pro lubitu assumere licet.

EXEMPLUM 1

11. Sumamus $q = 2$ et $r = 1$, ut fiat $p = 4$, tum prodibit $a = 19$, $b = 8$, $c = 4$; unde ipsi numeri quaesiti deducuntur, qui erunt $x = 409$, $y = 152$, $z = 64$. Horum numerorum summa est $x + y + z = 625 = 25^2$, quadratorum vero summa $x^2 + y^2 + z^2 = 194481 = 441^2 = 21^4$.

EXEMPLUM 2

12. Maneat $q = 2$ et sumatur etiam $r = 2$, fietque $p = 5$; tum vero erit $a = 25$, $b = 20$, $c = 8$. Hinc ipsi numeri quaestioni satisfacientes erunt $x = 961$, $y = 400$, $z = 320$, quorum summa est $x + y + z = 1681 = 41^2$ et summa quadratorum $x^2 + y^2 + z^2 = 1185921 = 33^4$.

ALIA SOLUTIO PROBLEMATIS

13. Cum ante formulam biquadraticam secundum potestates ipsius p coordinaverimus, nunc eam secundum ordinem potestatum litterae q disponemus, quo facto erit

$$x + y + z = q^4 + 4q^3 r + 2(pp - 3rr)qq + 4r(pp + 2pr - rr)q + (pp + rr)^2,$$

cuius radix, ut bini priores termini cum ultimo tollantur, statui debet $qq + 2qr - pp - rr$, unde evolutione facta colligitur

$$q = \frac{2pr(p + r)}{2rr - pp} .$$

EXEMPLUM

14. Sumatur $p = 1$ et $r = 1$, ut fiat $q = 4$, hincque colligitur $a = 16$, $b = 2$, $c = 8$, sive per 2 deprimendo $a = 8$, $b = 1$, $c = 4$; unde porro erit $x = 49$, $y = 64$, $z = 8$. Hinc fit

$$x + y + z = 11^2 \quad \text{et} \quad xx + yy + zz = 9^4 .$$

Isti numeri sine dubio sunt simplicissimi problemati satisfacientes.

PROBLEMA III

Invenire quatuor numeros x, y, z, v, quorum summa sit quadratum, quadratorum vero summa biquadratum.

SOLUTIO

15. Ut primo summa quadratorum reddatur quadratum, capiatur $x = aa + bb + cc - dd$, $y = 2ad$, $z = 2bd$, $v = 2cd$. Sic enim quadratorum summa fiet $(aa + bb + cc + dd)^2$, cuius radix denuo quadratum reddetur ponendo $a = pp + qq + rr - ss$, $b = 2ps$, $c = 2qs$, $d = 2rs$. Ne iam calculus, ob terminorum multitudinem, nimis prolixus evadat, ponamus brevitatis gratia $qq + rr - ss = A$, ut habeamus $a = pp + A$. Hinc iam sequitur fore

$$x = p^4 + 2App + AA + 4ppss + 4qqss - 4rrss ,$$
$$y = 4rspp + 4Ars ,$$
$$z = 8prss \quad \text{et} \quad v = 8qrss .$$

16. Iam summa numerorum quaesitorum, secundum potestates ipsius p disposita, erit

$$p^4 + 2(A + 2ss + 2rs)pp + 8prss + AA + 4qqss - 4rrss + 4Ars + 8qrss ,$$

quae, cum debeat esse quadratum, eius radix statuatur

$$pp + (A + 2ss + 2rs) ,$$

unde facta substitutione prodibit ista aequatio:

$$2pr + qq + 2qr - 2rr - ss - 2rs - A = 0 .$$

Restituto igitur loco A valore assumto habebimus

$$p = s + \frac{3}{2} r - q ,$$

ubi iam litterae q, r, s pro lubitu assumi possunt. Evolvamus aliquot casus, sumtisque pro q, r, s valoribus positivis tantum cavendum est, ne valor ipsius x fiat negativus, quod facile evitabitur, dummodo q non nimis magnum capiatur.

EXEMPLUM 1

17. Sumatur $r = 2$, $q = 1$ et $s = 1$, eritque $p = 3$; unde porro fit $a = 13$, $b = 6$, $c = 2$, $d = 4$, atque hinc colliguntur ipsi numeri quaesiti $x = 193$, $y = 104$, $z = 48$, $v = 16$, quorum summa est

$$x + y + z + v = 361 = 19^2 ,$$

summa vero quadratorum erit

$$xx + yy + zz + vv = (pp + qq + rr + ss)^4 = 15^4 .$$

EXEMPLUM 2

18. Maneat $r = 2$, sumatur autem $s = 1$ et $q = 2$, eritque $p = 2$, unde colligitur fore $a = 11$, $b = 4$, $c = 4$, $d = 4$; hincque $x = 137$, $y = 88$, $z = 32$, $v = 32$, quorum summa $x + y + z + v = 289 = 17^2$, quadratorum vero summa

$$x^2 + y^2 + z^2 + v^2 = 13^4 .$$

EXEMPLUM 3

19. Manente $r = 2$ sit $s = 1$ et $q = 3$, erit $p = 1$. Hinc valores litterarum a, b, c, d erunt $a = 13$, $b = 2$, $c = 6$, $d = 4$; unde porro fit $x = 193$, $y = 104$, $z = 16$, $v = 48$, sicque ipsum exemplum 1 recurrit.

Hoc modo plurima talia exempla facili negotio expediri possunt.

PROBLEMA IV

Invenire quinque numeros integros positivos x, y, z, v, w, quorum summa sit quadratum, quadratorum vero summa biquadratum.

SOLUTIO

20. Ut quadratorum summa fiat quadratum, sumatur

$$x = aa + bb + cc + dd - ee, \quad y = 2ae, \quad z = 2be, \quad v = 2ce, \quad w = 2de .$$

Ut vero prodeat biquadratum, statuatur porro

$$a = pp + qq + rr + ss - tt, \quad b = 2pt, \quad c = 2qt, \quad d = 2rt, \quad e = 2st ;$$

at brevitatis gratia ponatur $qq + rr + ss - tt = A$, ut sit $a = pp + A$, atque hinc sequitur fore

$$x = p^4 + 2Appp + AA + 4pptt + 4qqtt + 4rrtt - 4sstt,$$
$$y = 4stpp + 4Ast, \quad z = 8pstt, \quad v = 8qstt, \quad w = 8rstt.$$

21. Summa iam numerorum quaesitorum secundum potestates ipsius p disposita est:

$$p^4 + 2pp(A + 2tt + 2st) + 8pstt + AA + 4qqtt + 4rrtt - 4sstt + 4Ast + 8qstt + 8rstt,$$

cuius radix statuatur $pp + A + 2st + 2tt$; unde sumto quadrato resultat sequens aequatio:

$$2ps + qq + 2qs + rr + 2rs - 2ss - tt - 2st - A = 0,$$

unde, loco A restituto suo valore, prodit $p = t + \frac{3}{2}s - r - q$; ubi iam quatuor habentur numeri pro arbitrio sumendi.

EXEMPLUM

22. Sumatur $s = 2$, $t = 1$, $r = 1$, $q = 1$, eritque $p = 2$. Hinc ergo erit $a = 9$, $b = 4$, $c = 2$, $d = 2$, $e = 4$, ideoque numeri quaesiti erunt $x = 89$, $y = 72$, $z = 32$, $v = 16$, $w = 16$, quorum summa

$$x + y + z + v + w = 225 = 15^2,$$

quadratorum autem summa

$$x^2 + y^2 + z^2 + v^2 + w^2 = 11^4.$$

Similique modo plura exempla satis simplicia ex nostris formulis derivari possunt.

COROLLARIUM

23. Quodsi valores pro littera p inventos consideremus et inter se comparemus, facile inde lex patescet, cuius ope ad plures numeros progredi licebit, namque:

Pro casu 3 invenimus $p = r + \frac{3}{2}q$,

„ „ 4 „ $p = s + \frac{3}{2}r - q$,

„ „ 5 „ $p = t + \frac{3}{2}s - r - q$,

sicque pro casu sex numerorum reperietur $p = u + \frac{3}{2}t - s - r - q$, et ita porro, unde quaestio generalis pro quotcunque numeris proposita iam perfecte soluta est censenda.

SCHOLION

24. Cum in exemplo primo problematis II summa ipsorum numerorum inventa sit 25^2, ideoque iam biquadratum, hinc formari potest nova quaestio, circa quotcunque numeros inveniendos, quorum tam summa quam quadratorum summa sint biquadrata; verum hanc quaestionem attentius consideranti mox patebit, quamlibet solutionem ante inventam etiam ad hanc conditionem accommodari posse. Quodsi enim fuerit summa numerorum quotcunque $x+y+z+$ etc. $= AA$ et summa quadratorum $x^2+y^2+z^2+$ etc. $= B^4$, statuantur ipsi numeri quaesiti AAx, AAy, AAz etc.; tum enim eorum summa erit $AA \cdot AA = A^4$, ideoque biquadratum; quadratorum vero summa erit $A^4 \cdot B^4$. Quia autem hoc modo numeri quaesiti communem inter se habent factorem, si ista conditio insuper praescribatur, ut numeri inveniendi sint inter se primi sive nullum communem divisorem habeant, tum quaestio certe non parum ardua erit censenda. Interim tamen sequenti modo etiam tales quaestiones facile resolvi poterunt.

PROBLEMA V

Invenire tres numeros positivos inter se primos x, y, z, quorum tam summa quam quadratorum summa sint biquadrata.

SOLUTIO

25. Posito, uti in problemate secundo, $x = aa + bb - cc$, $y = 2ac$, $z = 2bc$, fiat porro $a = pp + qq - rr$, $b = 2pr$, $c = 2qr$ factaque substitutione statuatur ipsorum numerorum summae radix quadrata $= pp + (q+r)^2$, et cum supra invenerimus $p = r + \frac{3}{2}q$, necesse est, ut ista expressio $pp + (q+r)^2$ denuo reddatur quadratum. Eius ergo radix statuatur $p + \frac{f(q+r)}{g}$, hincque orietur ista aequatio:

$$gg(q+r) = 2fgp + ff(q+r) .$$

26. Scribatur nunc loco p valor inventus $r + \frac{3}{2}q$, et aequatio hanc induet formam: $(ff - gg)(q + r) + fg(2r + 3q) = 0$, unde deducitur

$$\frac{q}{r} = \frac{ff + 2fg - gg}{gg - 3fg - ff}\ ^{1}) .$$

Ecce ergo ista problematis solutio ita se habebit:

Sumantur $q = ff + 2fg - gg$ et $r = gg - 3fg - ff$, eritque

$$p = \tfrac{1}{2}ff - \tfrac{1}{2}gg ,$$

ex quibus valoribus primo litterae a, b, c, hincque porro ipsi numeri quaesiti x, y, z infinitis modis formari poterunt.

27. Sumatur exempli gratia $f = 1$ et $g = 3$, eritque $q = 2$, $r = 1$ et $p = 4$[2]). Hinc ergo concludimus fore $a = 19$, $b = 8$, $c = 4$; unde numeri quaesiti erunt $x = 409$, $y = 152$, $z = 64$, quorum summa est

$$x + y + z = 625 = 5^4 \quad \text{et} \quad [\text{quadratorum summa}] \quad x^2 + y^2 + z^2 = 21^4 .$$

28. Imprimis autem limites sunt investigandi, intra quos litteras f et g accipere liceat. Hunc in finem mutantur signa atque habebimus

$$q = gg - 2fg - ff \quad \text{et} \quad r = ff + 3fg - gg , \qquad [p = \tfrac{1}{2}gg - \tfrac{1}{2}ff] ,$$

quorum valorum, ut prior fiat positivus, debet esse $\frac{g}{f} > 1 + \sqrt{2} > 2{,}414$; at ut r fiat positivum, fieri debet $\frac{g}{f} < \frac{3 + \sqrt{13}}{2} < 3{,}303$. Sumatur ergo $f = 2$ et $g = 5$, eritque $q = 1$, $r = 9$, $p = \frac{21}{2}$, sive in integris $p = 21$, $q = 2$, $r = 18$; unde fit $a = 121$, $b = 756$, $c = 72$, hincque porro $x = 580993$, $y = 17424$, $z = 108864$, quorum summa

$$x + y + z = 29^4 ,$$

quadratorum vero summa

$$x^2 + y^2 + z^2 = 769^4 .$$

29. Simili igitur modo hanc quaestionem pro pluribus numeris quaesitis haud difficulter resolvere licebit; quamobrem huic argumento non amplius immoror; sufficiet enim methodum exposuisse omnia huius generis problemata commode et expedite resolvendi.

1) Editio princeps: $\frac{q}{r} = \frac{ff + 2fg - gg}{gg + 3fg - ff}$. Correxit A. M.

2) Signa numerorum q, r, p permutata sunt. Vide § 28. R. F.

RESOLUTIO FACILIS QUAESTIONIS DIFFICILLIMAE QUA HAEC FORMULA MAXIME GENERALIS $vvzz(axx + byy)^2 + \Delta xxyy(avv + bzz)^2$ AD QUADRATUM REDUCI POSTULATUR

Commentatio 764 indicis ENESTROEMIANI
Mémoires de l'académie des sciences de St-Pétersbourg 9 (1819/20), 1824, p. 14—19
Conventui exhibita die 12. iunii 1780

1. Etsi hic quatuor litterae incognitae x, y, z, v occurrunt, quae tamen ad duas tantum rationes $x : y$ et $v : z$ revocantur, neutra tamen earum pro cognita assumi potest, cum saepissime reductio ad quadratum fieret impossibilis; quamobrem tota quaestio huc reducitur, ut ambae istae rationes exquirantur, quibus formula ad quadratum reduci queat; tum vero imprimis omnes plane solutiones requiruntur, quod quomodo fieri sine ambagibus possit, in hac dissertatione novo plane modo ostendere constitui. Notandum autem hic est a, b, Δ arbitrio nostro plane esse relictas.

2. Ante omnia autem hic observandum est nullam plane viam patere, qua quaesito satisfieri queat, nisi litterae v et z ita definiantur, ut formula $avv + bzz$ divisorem involvat formulam $axx + byy$, quod quomodo in genere fieri possit in sequenti lemmate sum ostensurus.

LEMMA

Invenire valores pro litteris v et z, ut formula $avv + bzz$ *divisionem admittat per formulam* $axx + byy$.

SOLUTIO

3. Multiplicetur utraque formula per a, ut utriusque factores simplices sint $av \pm z\sqrt{-ab}$ et $ax \pm y\sqrt{-ab}$. Iam ponatur

$$av + z\sqrt{-ab} = (ax + y\sqrt{-ab})(f + g\sqrt{-ab}),$$

factaque evolutione partes rationales et irrationales seorsim inter se aequentur, ac pro partibus rationalibus habebimus $av = afx - abgy$ ideoque

$$v = fx - bgy .$$

Pro partibus autem irrationalibus fiet $z = fy + agx$. Quamobrem si statuamus

$$v = fx - bgy \quad \text{et} \quad z = fy + agx ,$$

fiet

$$avv + bzz = (ff + abgg)(axx + byy) .$$

4. Praemisso hoc lemmate resolutionem quaestionis propositae sequenti problemate complectamur:

PROBLEMA

Invenire omnes valores litterarum x, y, v, z, quibus haec formula:

$$vvzz(axx + byy)^2 + \Delta xxyy(avv + bzz)^2$$

evadat quadratum.

SOLUTIO

5. Vi lemmatis praemissi statuamus $v = fx - bgy$ et $z = fy + agx$, et quoniam nunc formula proposita divisionem per quadratum $(axx + byy)^2$ admittit, supererit, ut facta divisione ad quadratum reducatur ista formula:

$$vvzz + \Delta xxyy(ff + abgg)^2 .$$

Est vero

$$vz = afgxx + (ff - abgg)xy - bfgyy ,$$

sicque quadratum reddi debebit haec expressio:

$$(afgxx + (ff - abgg)xy - bfgyy)^2 + \Delta xxyy(ff + abgg)^2 ,$$

quae, quo simplicior reddatur, dividatur utrinque per quadratum $(ff + abgg)^2$, ac ponatur brevitatis gratia

$$\frac{afg}{ff + abgg} = A , \quad -\frac{bfg}{ff + abgg} = B \quad \text{et} \quad \frac{ff - abgg}{ff + abgg} = C ,$$

hocque modo quadrato aequanda erit ista formula

$$(Axx + Cxy + Byy)^2 + \Delta xxyy .$$

6. Quo hoc concinnius fieri possit, loco Δ scribamus $-4mn$, ut istam habeamus formulam:

$$(Axx + Cxy + Byy)^2 - 4mnxxyy = \square ,$$

quod praestabitur, uti constat, statuendo

$$Axx + Cxy + Byy = \lambda(mpp + nqq) \quad \text{et} \quad xy = \lambda pq ;$$

tum enim formula nostra aequabitur huic quadrato: $\lambda\lambda(mpp - nqq)^2$. Iam nihil impedit, quominus statuamus $y = 1$, cum hic tantum ratio inter x et y spectetur. Tum igitur erit $x = \lambda pq$ atque altera aequatio fiet

$$A\lambda\lambda ppqq + C\lambda pq + B = \lambda mpp + \lambda nqq ,$$

quae est aequatio quadratica tam respectu litterae p quam ipsius q, ideoque pro utraque binos valores simul exhibebit.

7. Ordinemus ergo primo aequationem respectu litterae p, quae erit

$$(A\lambda\lambda qq - \lambda m)pp + C\lambda pq + B - \lambda nqq = 0 ;$$

unde patet, si pro quolibet ipsius q valore binae radices ipsius p sint p et p', fore

$$p + p' = -\frac{C\lambda q}{A\lambda\lambda qq - \lambda m} = \frac{Cq}{m - A\lambda qq} .$$

Simili modo aequatio respectu litterae q disposita fiet:

$$(A\lambda\lambda pp - \lambda n)qq + C\lambda pq + B - \lambda mpp = 0 ,$$

ita ut, si pro quolibet p valores ipsius q statuantur q et q', fiat

$$q + q' = \frac{Cp}{n - A\lambda pp} .$$

Unde intelligitur, dummodo pro p et q binos habeamus valores idoneos, ex iis ope harum formularum innumerabiles alios erui posse, quemadmodum iam fusius ostendi[1]).

1) Vide Commentationem 279: *De resolutione formularum quadraticarum indeterminatarum per numeros integros.* LEONHARDI EULERI *Opera omnia*, series I, vol. 2, p. 576. R. F.

8. At vero facillime ex ipsa aequatione quadratica tales valores elici possunt. Posito enim $p = 0$ fit $qq = \frac{B}{\lambda n}$; quodsi ergo sumamus $\lambda = Bn$, fiet $q = \frac{1}{n}$, hicque casus solus sufficit, ex quo innumerabiles alii erui poterunt. Quamobrem sit ubique $\lambda = Bn$, ut fiat $x = Bnpq$; tum igitur constituamus hanc seriem: p, q, p', q', p'' etc., ubi ergo bini termini initiales erunt $p = 0$ et $q = \frac{1}{n}$, hincque per has formulas ob $\lambda = Bn$ sequentes termini successive ita determinabuntur:

$$p' = \frac{Cq}{m - ABnqq} - p = \frac{C}{mn - AB},$$
$$q' = \frac{Cp'}{n - ABnp'p'} - q = \frac{mnCC - (mn - AB)^2}{n(mn - AB)^2 - nABCC},$$ etc.

quae progressio, quando omnes litterae per numeros determinatos dantur, haud difficulter ulterius continuari poterit.

9. Isti valores evoluti pro $x = Bnpq$ sequentes praebent:

$$0, \frac{BC}{mn - AB}, \frac{BC(mnCC - (mn - AB)^2)}{(mn - AB)^3 - ABCC(mn - AB)},$$

qui singuli iam innumerabiles solutiones complectuntur, quoniam litteris f et g valores quoscunque tribuere licet. Deinde etiam quilibet horum valorum adhuc alium suppeditat. Nam quia aequatio ita est comparata, ut posito $x = \frac{1}{t}$ abeat in hanc:

$$(A + Ct + Btt)^2 - 4mntt = \square,$$

haec a priore in hoc tantum discrepat, quod litterae A et B sint permutatae, unde facta hac permutatione singuli valores pro x inventi dabunt totidem valores pro t, qui ergo inversi novos valores pro x praebent. Ita cum sit $x = \frac{BC}{mn - AB}$, erit $t = \frac{AC}{mn - AB}$, ideoque novus valor erit $\frac{mn - AB}{AC}$, quod idem de omnibus reliquis valoribus pro x inventis est tenendum.

10. Postquam pro x inventa fuerit fractio quaecunque $\frac{M}{N}$, quia sumsimus $y = 1$, ut ad numeros integros revertamur, capi oportebit $x = M$ et $y = N$, unde porro colligetur $v = fM - bgN$ et $z = fN + agM$. Hoc ergo modo problemati plene erit satisfactum, cum adeo infinities infinitos valores satisfacientes assignare liceat.

EXEMPLUM

11. Proposita sit haec formula ad quadratum redigenda:

$$vvzz(xx + yy)^2 + xxyy(vv + zz)^2 .$$

Hic igitur erit $a = 1$, $b = 1$ et $\Delta = 1 = -4mn$, unde sumi poterit $m = \frac{1}{2}$ et $n = -\frac{1}{2}$. Ex his valoribus fiet

$$A = \frac{fg}{ff + gg}, \quad B = -\frac{fg}{ff + gg}^{1}), \quad C = \frac{ff - gg}{ff + gg} .$$

Hinc ergo valores supra evoluti erunt $0, -\frac{4fg(ff - gg)}{4ffgg - (ff + gg)^2}$[2]). Sumamus igitur $f = 2$ et $g = 1$, erit $x = \frac{8}{3}$[3]); quamobrem ponamus $x = 8$ et $y = 3$, fietque $v = 13$ et $z = 14$. Cum igitur sit $vz = 182$, $xx + yy = 73$, $xy = 24$, $vv + zz = 365 = 5 \cdot 73$, quadratum esse debet $182^2 \cdot 73^2 + 24^2 \cdot 5^2 \cdot 73^2$, dividendo ergo per $2^2 \cdot 73^2$ reperietur $91^2 + 12^2 \cdot 5^2 = 109^2$.

12. Quaestio proposita adhuc generalior reddi similique modo resolvi posset, si proponeretur ad quadratum reducenda haec formula:

$$vvzz(axx + 2bxy + czz)^2 + \Delta xxyy(avv + 2bvz + czz)^2 ,$$

quae autem, ob id ipsum, quod b non nihilum, nulla plane laborat difficultate. Sumi enim adeo possunt ambae litterae v et z pro lubitu, et facta evolutione prodibit talis forma:

$$A^2x^4 + 2Bx^3y + Cxxyy + 2Dxy^3 + E^2y^4 ,$$

cuius resolutio adeo methodo vulgari expediri potest.

13. Interim tamen, si similis solutio desideretur, quae perinde locum habere queat, sive b sit 0 sive minus, talis solutio pari modo succedet ut ante, si modo sequens lemma in subsidium vocetur.

---

1) Editio princeps: $B = \frac{fg}{ff + gg}$. Correxit R. F.

2) Editio princeps: $\frac{fg(ff - gg)}{ffgg - (ff + gg)^2}$. Correxit A. M.

3) Editio princeps: $\frac{3}{8}$. Correxit A. M.

LEMMA

Invenire idoneos valores pro litteris v et z, ut ista formula $avv + 2bvz + czz$ *divisibilis evadat per hanc* $axx + 2bxy + cyy$.

SOLUTIO

14. Multiplicetur utraque formula per a, ut utriusque factores simplices sint $av + bz \pm z\sqrt{bb - ac}$ et $ax + by \pm y\sqrt{bb - ac}$, quorum ergo ille per hunc divisibilis reddi debet. Hunc in finem statuatur

$$av + bz + z\sqrt{bb - ac} = (ax + by + y\sqrt{bb - ac})\,(f + g\sqrt{bb - ac})\,;$$

tum vero facta evolutione partes rationales et irrationales seorsim inter se aequentur, unde pro rationalibus reperietur

$$av + bz = afx + bfy + gy(bb - ac)\,.$$

Pro irrationalibus autem erit

$$z = agx + bgy + fy\,,$$

qui valor in praecedente substitutus dat

$$v = (f - bg)\,x - cgy\,,$$

quibus valoribus loco z et v introductis formula proposita $avv + 2bvz + czz$ aequabitur huic producto:

$$(axx + 2bxy + cyy)\,(ff + (ac - bb)\,gg)\,,$$

atque nunc totus calculus ut ante expediri poterit.

SOLUTIO PROBLEMATIS FERMATIANI DE DUOBUS NUMERIS QUORUM SUMMA SIT QUADRATUM QUADRATORUM VERO SUMMA BIQUADRATUM AD MENTEM ILLUSTRIS LA GRANGE ADORNATA[1)]

Commentatio 769 indicis ENESTROEMIANI
Mémoires de l'académie des sciences de St-Pétersbourg 10 (1821/2), 1826, p. 3—6
Conventui exhibita die 5. iunii 1780

1. In solutionibus huius problematis, quae hactenus passim in medium sunt allatae, Illuster LA GRANGE id potissimum merito reprobat, quod nimium casui et vagis tentaminibus tribuatur, unde fit, ut certi esse nequeamus omnesne solutiones, atque adeo simplicissimas, hoc modo inventas esse[2)]. Huic igitur desiderato sequenti analysi satisfactum iri confido.

2. Sint x et y bini numeri quaesiti, ita ut esse debeat $x + y = \square$ et $xx + yy = \square^2$, si pro conditione posteriore sumamus $x = pp - qq$ et $y = 2pq$, fiet $xx + yy = (pp + qq)^2$. Quod si porro statuatur

$$p = rr - ss \quad \text{et} \quad q = 2rs\,,$$

fiet $pp + qq = (rr + ss)^2$, ideoque $xx + yy = (rr + ss)^4$, uti requiritur. Hinc autem erit $x = r^4 - 6rrss + s^4$ et $y = 4rs(rr - ss)$.

3. Pro conditione priore ergo summa numerorum erit

$$x + y = r^4 + 4r^3s - 6rrss - 4rs^3 + s^4\,,$$

1) Confer Commentationem 763 indicis ENESTROEMIANI, huius voluminis p. 61. R. F.
2) Vide Commentationem ipsius LAGRANGE, p. 61 in nota 2), p. 61, laudatam: R. F.

quae formula idcirco quadratum est efficienda. Hunc in finem, ne quidquam tentamini tribuatur, istam expressionem sub hac forma repraesento:

$$x + y = (rr + 2rs - ss)^2 - 8rrss ,$$

ita ut iam talis formula: $AA - 2BB$ quadratum reddi debeat, quod fit sumendo $A = tt + 2uu$ et $B = 2tu$; tum enim fiet

$$AA - 2BB = (tt - 2uu)^2 .$$

4. Nunc loco A et B scribamus nostros valores et habebimus

$$rr + 2rs - ss = tt + 2uu \quad \text{et} \quad 2rs = 2tu ,$$

hocque modo summa numerorum nostrorum erit $x + y = (tt - 2uu)^2$, ideoque iam ambabus conditionibus erit satisfactum, dummodo formulae modo inventae fuerint expeditae.

5. Quoniam autem haec duo producta rs et tu inter se aequalia esse debent, loco litterae s hic tuto unitatem assumere licebit. Quamquam enim tum pro r fractiones sint prodituraе, id solutioni neutiquam officit, quia solutio in fractis inventa facile ad integros reducitur. Hoc igitur modo erit $r = tu$, qui valor in altera aequatione substitutus dabit

$$ttuu + 2tu - 1 = tt + 2uu ,$$

sicque totum negotium reductum est ad iustam relationem inter t et u inveniendam. Sive ergo t per u vel u per t definire velimus, resolutio aequationis quadraticae binas sequentes suppeditabit formulas:

$$t = \frac{u \pm \sqrt{2u^4 - 1}}{1 - uu} \quad \text{et} \quad u = \frac{t \pm \sqrt{t^4 - 2}}{2 - tt} .$$

Quin etiam hinc statim valores radicalium pro sequenti usu sponte se produnt, ut extractione radicis non amplius indigeamus. Ex priore enim erit

$$\sqrt{2u^4 - 1} = t(1 - uu) - u ;$$

ex altera vero $\sqrt{t^4 - 2} = u(2 - tt) - t$. Hic autem commode usu venit, ut utraque formula geminos praebeat valores.

6. Incipiamus a formula priore, quia casus $u = 1$ statim in oculos incurrit. Quoniam vero hoc casu denominator $1 - uu$ evanescit, recurrendum est ad remedium notissimum, quo poni solet $u = 1 - \omega$, denotante ω quantitatem evanescentem, ita ut eius potestates altiores tuto reiicere liceat. Hinc igitur erit $2u^4 = 2 - 8\omega$ ideoque

$$\sqrt{2u^4 - 1} = \sqrt{1 - 8\omega} = 1 - 4\omega \quad \text{et} \quad 1 - uu = 2\omega ,$$

hincque colligitur[1]) $t = \frac{3}{2}$, qui valor in altera formula substitutus dat

$$\sqrt{t^4 - 2} = \frac{7}{4} .$$

7. Progrediamur nunc ad alteram aequationem, pro qua iam novimus valores $u = 1$ et $t = \frac{3}{2}$, et quia geminos valores complectitur, novum valorem pro u elicimus, scilicet $u = -13$. Hunc valorem feramus in priorem formulam, pro qua iam novimus alterum valorem esse $t = \frac{3}{2}$, ex quo innotescit

$$\sqrt{2u^4 - 1} = t(1 - uu) - u ,$$

unde, ob $u = -13$ et $t = \frac{3}{2}$, erit $\sqrt{2u^4 - 1} = \pm 239$. Nunc vero haec ipsa aequatio nobis insuper praebet novum valorem pro t, scilicet $t = -\frac{113}{84}$.

8. Simili modo istum valorem inferamus in alteram aequationem, et quia erat $u = -13$[2]), inde deducimus

$$\sqrt{t^4 - 2} = u(2 - tt) - t = \pm \frac{7967}{7056}\ ^{3}) ,$$

quo valore adhibito altera radix nobis dabit novum valorem pro u, scilicet $u = -\frac{1525}{1343}$ [4]). Quodsi denuo iste valor in priore formula assumatur, pro t iterum novum adipiscimur valorem, sicque quousque libuerit facile progredi licebit. Mox autem ob numeros immensos laborem abrumpere cogemur.

---

1) pro signo inferiore. R. F.

2) Editio princeps: — 239. Correxit A. M.

3) Editio princeps: $-\frac{311485}{7056}$ Correxit A. M.

4) Editio princeps hoc loco et in § 9: $\frac{301993}{1343}$. Correxit A. M.

9. Vis igitur istius novae methodi in hoc consistit, quod singulis valoribus ipsius t gemini valores ipsius u, eodemque modo singulis ipsius u gemini valores ipsius t respondeant, quos ergo, quousque sumus progressi, hic conspectui exhibeamus

$$u = 1 \;,\; t = \frac{3}{2} \;;$$

$$u = -13 \;,\; t = -\frac{113}{84} \;;$$

$$u = -\frac{1525}{1343} \;,$$

quorum valorum quilibet cum binis adiacentibus combinari potest. Ex talibus autem binis valoribus ipsi numeri quaesiti x et y hoc modo determinantur

$$x = t^4u^4 - 6ttuu + 1 \;,$$
$$y = 4tu(ttuu - 1) \;.$$

Facile autem perspicitur hoc modo omnes plane solutiones possibiles necessario prodire debere[1]).

10. Hic imprimis notatu dignum est, quod valores pro litteris t et u successive inventi egregio ordine progrediantur, ita ut ex singulis facile sequentes definiri queant. Ita si habeantur duo quicunque valores pro t et u, qui formulae $t = \frac{u \pm \sqrt{2u^4 - 1}}{1 - uu}$ satisfaciant, cum sit $\sqrt{2u^4 - 1} = t(1 - uu) - u$, ob signum radicale ambiguum insuper alius valor pro t eruetur, quem si ponamus $= t'$, erit quoque $t'(1 - uu) = 2u - t(1 - uu)$, ideoque $t' = \frac{2u}{1 - uu} - t$.

11. Eodem modo ex iisdem valoribus t et u cognitis per alteram formulam $u = \frac{t \pm \sqrt{t^4 - 2}}{2 - tt}$, ob $\sqrt{t^4 - 2} = u(2 - tt) - t$, alius valor pro u elici poterit, qui, si ponatur $= u'$, erit

$$u'(2 - tt) = 2t - u(2 - tt), \text{ ideoque } u' = \frac{2t}{2 - tt} - u \;.$$

1) Haec affirmatio non demonstratur. R. F.

Hi valores, cum sint cogniti, per utramque formulam denuo alii novi erui poterunt, qui si ordine designentur per t'', u''; t''', u''' etc., ob

$$t' = \frac{2u}{1-uu} - t \quad \text{et} \quad u' = \frac{2t}{2-tt} - u ,$$

simili modo habebimus

$$t'' = \frac{2u'}{1-u'u'} - t' \text{ et } u'' = \frac{2t'}{2-t't'} - u' ,$$

tum vero

$$t''' = \frac{2u''}{1-u''u''} - t'' \text{ et } u''' = \frac{2t''}{2-t''t''} - u'' ;$$

et ita porro.

DE INSIGNI PROMOTIONE ANALYSIS DIOPHANTAEAE

Commentatio 772 indicis ENESTROEMIANI
Mémoires de l'académie des sciences de St-Pétersbourg 11, 1830, p. 1—11
Conventui exhibita die 12. iunii 1780

1. Quando in Analysi DIOPHANTAEA ad formulas biquadraticas quadrato aequandas pervenitur, methodus eas tractandi adhuc parum est exculta et nimis taediosas ambages requirit, quando plures solutiones desideramus. Qualibet enim solutione inventa formula biquadratica per substitutionem continuo in alias formas transmutari debet, quibus operationibus mox ad tam enormes numeros pervenitur, ut vix quisquam tantum laborem suscipere voluerit.

2. Cum igitur nuper pro problemate notissimo, quo duo numeri requiruntur, quorum summa sit quadratum, quadratorum vero summa biquadratum[1]), in solutionem satis commodam et concinnam incidissem, mox perspexi eandem methodum multo magis generalem reddi posse. Semper enim in usum vocari poterit, quoties talis formula biquadratica ad quadratum reducenda proponitur:

$$aax^4 + 2abx^3y + cxxyy + 2bdxy^3 + ddy^4 = \square .$$

Quia enim ad hanc formam reduci potest:

$$(axx + bxy + dyy)^2 + (c - bb - 2ad)\,xxyy ,$$

ponamus brevitatis gratia $c - bb - 2ad = mn$, ut habeamus

$$(axx + bxy + dyy)^2 + mnxxyy = \square ,$$

huic satisfiet statuendo

1) Vide Commentationem 769 indicis ENESTROEMIANI, huius voluminis p. 77. R. F.

$$axx + bxy + dyy = \lambda(mpp - nqq) \quad \text{et} \quad xy = 2\lambda pq \ ;$$

tum enim nostra formula evadet quadratum, scilicet $\lambda\lambda(mpp + nqq)^2$, ubi notetur, quo plures numerus mn habeat factores, eo pluribus modis hanc expressionem immutari posse.

3. Hic omnes numeros m, n, p, q tanquam integros spectamus; sin autem fractos admittere velimus, loco y unitatem scribere licebit, sicque erit $x = 2\lambda pq$, qui valor in praecedente aequatione substitutus praebet

$$4\lambda\lambda appqq + 2\lambda bpq + d = \lambda mpp - \lambda nqq \ ,$$

quae aequatio, cum sit quadratica respectu utriusque litterae p et q, pro utraque radicem extrahendo inveniemus has duas formulas:

$$p = \frac{-\lambda bq \pm \sqrt{\lambda md + \lambda\lambda(bb - 4ad + mn)qq - 4\lambda^3 anq^4}}{4\lambda\lambda aqq - \lambda m}$$

$$q = \frac{-\lambda bp \pm \sqrt{-\lambda nd + \lambda\lambda(bb - 4ad + mn)pp + 4\lambda^3 amp^4}}{4\lambda\lambda app + \lambda n} \ .$$

4. Quia littera λ nostro arbitrio est relicta, haud difficile erit ei talem valorem tribuere, ut in altera saltem formula extractio radicis quadratae succedat, quam si fuerimus nacti, ita ut pro p et q determinatos valores impetravimus, inde sequenti modo plures alios valores atque adeo infinitos eruere licebit. Sint enim p et q valores inventi, atque ob ambiguitatem signi radicalis pro p simul alius valor innotescit, qui si ponatur p', erit

$$p + p' = -\frac{2bq}{4\lambda aqq - m} \ .$$

Hic iam valor p' in altera formula loco p substitutus dabit quoque novum valorem pro q, qui sit q', eritque simili modo

$$q + q' = -\frac{2bp'}{4\lambda ap'p' + n} \ ^{1}) \ .$$

Neque vero opus est istam alteram substitutionem facere, cum inventio novorum valorum pro p et q sequenti modo facillime expediri queat.

1) Editio princeps: $\frac{-2bp}{4\lambda app + n}$. Correxit A. M.

5. Simul enim atque duos valores p et q fuerimus nacti, inde statim sequens series assignari poterit: $p, q, p', q', p'', q'', p''', q'''$ etc., cum sit

$$p' = -\frac{2bq}{4\lambda aqq - m} - p \quad , \qquad q' = -\frac{2bp'}{4\lambda ap'p' + n} - q \; ,$$

$$p'' = -\frac{2bq'}{4\lambda aq'q' - m} - p' \quad , \qquad q'' = -\frac{2bp''}{4\lambda ap''p'' + n} - q' \; ,$$

$$p''' = -\frac{2bq''}{4\lambda aq''q'' - m} - p'' \quad , \qquad q''' = -\frac{2bp'''}{4\lambda ap'''p''' + n} - q'' \; ,$$

etc. etc.

6. Quin etiam ambas litteras p et q permutare possumus, ut obtineamus hanc seriem: q, p, q', p', q'', p'' etc., ubi iterum erit:

$$q' = -\frac{2bp}{4\lambda app + n} - q \quad , \qquad p' = -\frac{2bq'}{4\lambda aq'q' - m} - p \; ,$$

$$q'' = -\frac{2bp'}{4\lambda ap'p' + n} - q' \quad , \qquad p'' = -\frac{2bq''}{4\lambda aq''q'' - m} - p' \; ,$$

etc. etc.

sicque sine ulla transformatione et substitutione ex binis valoribus initio cognitis p et q, quotcunque libuerit, alios valores elicere poterimus, quorum adeo lex progressionis innotescit. Unde patet hanc methodum vulgari plurimum antecellere.

7. Inventa autem tali serie litterarum p et q binis quibuslibet coniungendis adipiscemur totidem valores idoneos pro ipsa littera quaesita x, quippe cuius valores ex priori serie erunt

$$2\lambda pq, \quad 2\lambda qp', \quad 2\lambda p'q', \quad 2\lambda q'p'' \quad \text{etc.},$$

ex altera vero serie valores ipsius x erunt

$$2\lambda qp, \quad 2\lambda pq', \quad 2\lambda q'p', \quad 2\lambda p'q'' \quad \text{etc.},$$

posito scilicet $y = 1$; unde patet, si illi valores fuerint fractiones, earum denominatores pro y assumi posse, dum soli numeratores ipsi x tribuuntur.

8. Totum ergo negotium eo redit, ut bini saltem valores initiales p et q investigentur, id quod plerumque facile fieri poterit, quia littera λ a lubitu nostro pendet. Interim tamen tales valores initiales ex ipsa formula biquadratica per methodum vulgarem derivari poterunt. Sumto enim $y = 1$ huius formulae biquadraticae:

$$aax^4 + 2abx^3 + cxx + 2bdx + dd$$

radix statuat $axx + bx - d$ et calculo subducto fiet

$$x = \frac{4bd}{bb - 2ad - c} = -\frac{4bd}{mn + 4ad}$$

ob $c = mn + bb + 2ad$.

Simili modo posita radice $axx - bx - d$ fiet

$$x = \frac{bb - 2ad - c}{4ab} = \frac{-mn - 4ad}{4ab}.$$

9. Iidem valores alio quoque modo obtineri possunt. Posita enim radice $axx + bx + \frac{c - bb}{2a}$, colligitur

$$x = \frac{-mn - 4ad}{4ab},$$

quae cum praecedentium posteriore convenit. Simili modo, si radix fingeretur $d + bx + \frac{c - bb}{2d} xx$, foret

$$x = -\frac{4bd}{mn + 4ad},$$

prior valor paragraphi praecedentis. Interim tamen duobus valoribus inventis annumerari possunt etiam hi: $x = 0$ et $y = 0$, unde autem raro aliquid deduci potest.

10. Invento autem valore idoneo pro x manente $y = 1$ haud difficulter pro eo litterae p et q reperiri poterunt. Cum enim posuerimus

$$axx + bx + d = \lambda(mpp - nqq) \quad \text{et} \quad x = 2\lambda pq,$$

erit

$$\frac{axx+bx+d}{x} = \frac{mpp-nqq}{2pq} .$$

Ex cognito ergo valore fiat

$$\frac{axx+bx+d}{x} = A ,$$

ut habeamus $mpp - nqq = 2Apq$, colligitur

$$\frac{p}{q} = \frac{A+\sqrt{AA+mn}}{m} ,$$

ubi radix certo extrahi poterit, unde oriatur fractio $\frac{f}{g} = \frac{p}{q}$. Sumto igitur $p = f$ et $q = g$ sponte patescet, quid pro λ accipi debeat, ut fiat $2\lambda pq = x$, hincque statim binae series memoratae formari poterunt. Ceterum superfluum foret hanc methodum per exempla illustrare, quia insignis casus iam in dissertatione praecedente[1]) accurate est pertractatus.

11. Etsi formula hic tractata non parum restricta videtur, tamen plurimae aliae formulae maxime discrepantes ope idoneae substitutionis ad eam reduci possunt, cuiusmodi est ista satis generalis $\alpha A^4 \pm \beta B^4 = \square$, vel posito $\frac{A}{B} = C$ haec simplicior $\alpha C^4 \pm \beta = \square$, dummodo casus praesto sit, quo ea fit quadratum, veluti casu $C = 1$, ita ut tum sit $\alpha \pm \beta = \square$. Omnes autem huiusmodi formulae ad nostram formam reducentur ope substitutionis $C = \frac{1+x}{1-x}$; tum enim posito $\alpha + \beta = aa$ ista formula induet hanc formam:

$$aa + 4(\alpha - \beta)x + 6aaxx + 4(\alpha - \beta)x^3 + aax^4 = \square ,$$

quae pro casu, quo $a = 1$, manifesto reducitur ad hanc:

$$(a + 2(\alpha - \beta)x + axx)^2 + 16\alpha\beta xx ,$$

quam ergo secundum praecepta praescripta tractare licebit, id quod aliquot exemplis illustrasse iuvabit.

---

1) *Solutio Problematis* FERMATIANI *de duobus numeris, quorum summa sit quadratum, quadratorum vero summa biquadratum* (vide Mémoires de l'acad. d. sc. de St-Pétersbourg, tome 10, p. 3) [huius voluminis p. 77].

EXEMPLUM 1

Formulae $2A^4 - B^4 = \square$.

12. Haec formula convenit cum ea, unde vulgo bini numeri, quorum summa sit quadratum, quadratorum vero summa biquadratum, derivari solet. Facto ergo $\frac{A}{B} = C$, ut sit $2C^4 - 1 = \square$, erit $\alpha = 2$ et $\beta = -1$, unde $\alpha + \beta = 1 = aa$, ergo $a = 1$.

Quocirca posito $C = \frac{1+x}{1-x}$ prodibit ista expressio:

$$1 + 12x + 6xx + 12x^3 + x^4 = \square ,$$

sive haec:

$$(1 + 6x + xx)^2 - 32xx = \square .$$

Statuatur ergo secundum praecepta tradita

$$1 + 6x + xx = \lambda(pp + 2qq) \quad \text{et} \quad 4x = 2\lambda pq ,$$

sive $x = \frac{1}{2}\lambda pq$ vel, ut fractiones evitemus, si loco q scribamus $2q$, ut habeamus

$$1 + 6x + xx = \lambda(pp + 8qq) \quad \text{et} \quad x = \lambda pq ,$$

nascitur ista aequatio:

$$1 + 6\lambda pq + \lambda\lambda ppqq = \lambda pp + 8\lambda qq .$$

Hinc deducuntur sequentes radices

$$p = \frac{-3\lambda q \pm \sqrt{8\lambda^3 q^4 + \lambda}}{\lambda\lambda qq - \lambda} , \qquad q = \frac{-3\lambda p \pm \sqrt{\lambda^3 p^4 + 8\lambda}}{\lambda\lambda pp - 8\lambda} ,$$

unde, cum quaelibet involvat duos valores, sequitur fore

$$p + p' = -\frac{6q}{\lambda qq - 1} \quad \text{et} \quad q + q' = -\frac{6p}{\lambda pp - 8} .$$

Videamus nunc, quinam valores pro p et q ex priore saltem formula prodeant, unde sumto $\lambda = 1$ statim se offert casus $q = 0$, unde fit $p = 1$. Praeterea vero alius casus se offert, quo $q = 1$, qui dat $p = \frac{3 \pm 3}{1 - 1}$; at vero hoc casu ipsa

aequatio quadratica dat $p = +\frac{7}{6}$. Statuamus ergo $\lambda = 1$ et geminos pro p et q habemus valores satisfacientes, quorum alteri sunt $q = 0$ et $p = 1$, alteri vero $q = 1$ et $p = +\frac{7}{6}$, ex quibus fit $x = pq$. Relationes inter valores ex p et q derivatos erunt:

$$p + p' = -\frac{6q}{qq-1} \text{ et } q + q' = -\frac{6p}{pp-8} .$$

Quocirca, si constituamus seriem q, p, q', p', q'' etc., erit

$$q' = -\frac{6p}{pp-8} - q , \quad p' = -\frac{6q'}{q'q'-1} - p ,$$
$$q'' = -\frac{6p'}{p'p'-8} - q' , \quad p'' = -\frac{6q''}{q''q''-1} - p' .$$
$$\text{etc.} \qquad\qquad \text{etc.}$$

Ex valoribus igitur $q = 0$ et $p = 1$ nascetur ista series:

$$0 , 1 , \frac{6}{7} , \frac{239}{13}^{1}) \text{ etc.}$$

Iam omnia producta ex binis terminis contiguis huius seriei dabunt valores idoneos pro x (§ 7), unde fit $C = \frac{1+x}{1-x}$. Hinc ergo pro x obtinentur hi valores: $0, \frac{6}{7}, \frac{1434}{91}$ etc., unde pro C deducuntur sequentes: $1, 13, -\frac{1525}{1343}$ etc. Alteri valores inventi $q = 1$ et $p = \frac{7}{6}$ pro serie q, p, q', p' etc. hos dant numeros: $1, \frac{7}{6}, \frac{13}{239}$ etc., unde patet priores valores pro q et p assumtos solutionem penitus exhaurire neque adeo posterioribus ad problema solvendum opus fuisse.

EXEMPLUM 2

Formulae $3A^4 + B^4 = \square$.

13. Ad quadratum ergo redigi debet haec formula $3C^4 + 1$, cui statim tres valores satisfacere deprehenduntur, scilicet

$$C = 0 , \quad C = 1 , \quad C = 2 .$$

1) Editio princeps: $\frac{239}{19}$. Correxit A. M.

Cum igitur hic sit $\alpha = 3$ et $\beta = 1$, posito $C = \frac{1+x}{1-x}$ nascetur sequens formula

$$4 + 8x + 24xx + 8x^3 + 4x^4 = \square ,$$

quae per 4 divisa fit

$$1 + 2x + 6xx + 2x^3 + x^4 = \square ,$$

quae ita repraesentata

$$(1 + x + xx)^2 + 3xx = \square$$

dabit has substitutiones:

$$1 + x + xx = \lambda(pp - 3qq) \quad \text{et} \quad x = 2\lambda pq ,$$

unde ista aequatio inter p et q emergit

$$1 + 2\lambda pq + 4\lambda\lambda ppqq = \lambda pp - 3\lambda qq ,$$

unde pro casu $\lambda = 1$ et $q = \frac{1}{2}$ statim deducitur $p = -\frac{7}{4}$. Binae autem radices quadratae pro p et q erunt

$$p = \frac{-\lambda q \pm \sqrt{\lambda - 12\lambda^3 q^4}}{4\lambda\lambda qq - \lambda} , \quad q = \frac{-\lambda p \pm \sqrt{4\lambda^3 p^4 - 3\lambda}}{4\lambda\lambda pp + 3\lambda} .$$

Ex his ergo formulis erit

$$p + p' = -\frac{2q}{4\lambda qq - 1} \quad \text{et} \quad q + q' = -\frac{2p}{4\lambda pp + 3}\text{[1]} .$$

Quoniam iam casum invenimus $\lambda = 1$ et $q = \frac{1}{2}$, unde fit $p = -\frac{7}{4}$, hinc statim nostra series q, p, q', p', q'', p'' etc. formari potest ope formularum:

$$p + p' = -\frac{2q}{4qq - 1} \quad \text{et} \quad q + q' = -\frac{2p}{4pp + 3} ,$$

atque termini huius seriei fient $\frac{1}{2}, -\frac{7}{4}, -\frac{33}{122}$ etc., unde, cum sit $x = 2pq$, hinc nanciscimur istos valores, $x = -\frac{7}{4}$ et $x = \frac{231}{244}$[2]), unde fit $C = -\frac{3}{11}$; tum enim erit $\sqrt{3C^4 + 1} = \frac{122}{121}$.

1) In editione principe factor λ numeratori et denominatori harum fractionum communis non committitur. R. F.

2) Editio princeps: $\frac{231}{448}$. Correxit A. M.

EXEMPLUM 3

Formulae $\frac{3A^4 - B^4}{2} = \square$.

14. Quia igitur quadratum esse debet $\frac{3}{2}C^4 - \frac{1}{2}$, erit $\alpha = \frac{3}{2}$, $\beta = -\frac{1}{2}$, ideoque $a = 1$ et $\alpha - \beta = 2$, oritur haec formula biquadratica

$$1 + 8x + 6xx + 8x^3 + x^4 = \square ,$$

sive

$$(1 + 4x + xx)^2 - 3(2x)^2 = \square .$$

Quamobrem statuatur

$$1 + 4x + xx = \lambda(pp + 3qq) \quad \text{et} \quad x = \lambda pq ,$$

unde prodit ista aequatio inter p et q:

$$1 + 4\lambda pq + \lambda\lambda ppqq = \lambda pp + 3\lambda qq ,$$

unde statim quosdam valores satisfacientes eruere possumus, ita ut non opus sit ad extractionem radicis confugere. Primo enim sumto $\lambda = 1$ et $q = 1$ ista aequatio dabit $p = \frac{1}{2}$, et sumto $\lambda = 3$ et $p = 1$ erit $q = \frac{1}{6}$. Hos ergo ambos casus evolvamus. Sit igitur primo $\lambda = 1$, ita ut sit $x = pq$, et novimus casum, ubi $q = 1$ et $p = \frac{1}{2}$, et quia aequatio quadratica

$$pp(qq - 1) + 4pq + 1 = 3qq ,$$

evidens est summam radicum ipsius p esse

$$p + p' = -\frac{4q}{qq - 1} ,$$

similique modo, cum sit $qq(pp - 3) + 4pq + 1 = pp$, erit

$$q + q' = -\frac{4p}{pp - 3} .$$

Hinc ergo formetur series q, p, q', p' etc., quae in numeris ita se habebit: $1, \frac{1}{2}, -\frac{3}{11}, -\frac{47}{28}$ [1]) etc., unde deducuntur hi valores pro x: $\frac{1}{2}, -\frac{3}{22}, \frac{141}{308}$, ideoque pro C sequentes $3, \frac{19}{25}, \frac{449}{167}$ etc.

1) Editio princeps: $\frac{47}{28}$. Correxit A. M.

Simili modo pro altero casu, ubi $\lambda = 3$, $p = 1$ et $q = \frac{1}{6}$, ob formulas generales $p + p' = -\frac{4q}{\lambda qq - 1}$ et $q + q' = -\frac{4p}{\lambda pp - 3}$ erit

$$p + p' = -\frac{4q}{3qq - 1} \quad \text{et} \quad q + q' = -\frac{4p}{3pp - 3},$$

hinc series p, q, p', q' etc. ita se habebit: $1, \frac{1}{6}, -\frac{3}{11}, -\frac{47}{84}$ etc. Quia igitur hic $x = 3pq$, erit iterum $x = \frac{1}{2}, -\frac{3}{22}, \frac{141}{308}$ [1]), sicque amplissimum usum huius methodi me satis abunde declarasse video.

15. Haec exempla nonnulla insignia compendia nobis suppeditarunt, quibus totum hoc negotium multo facilius et elegantius expediri potest, quae in sequenti problemate clarius explicabimus.

PROBLEMA

Proposita formula biquadratica in hac forma contenta:

$$(axx + 2bx + c)^2 - 4mnxx,$$

invenire infinitos valores ipsius x, quibus ista formula evadit quadratum.

SOLUTIO

16. Primo ista formula fit quadratum, si fuerit

$$axx + 2bx + c = \lambda(mpp + nqq) \quad \text{et} \quad x = \lambda pq;$$

tum enim eius radix erit $\lambda(mpp - nqq)$. Posito igitur $x = \lambda pq$ prior aequatio induet hanc formam:

$$\lambda\lambda appqq + 2\lambda bpq + c = \lambda mpp + \lambda nqq;$$

unde statim unus casus quaesito satisfaciens elicitur sumendo $p = 0$, tum

1) Editio princeps: $\frac{-141}{308}$. Correxit A. M.

enim erit $c = \lambda nqq$. Sumto igitur $\lambda = nc$ fiet $q = \frac{1}{n}$, hicque solus casus innumerabiles alios sequenti modo producet.

17. Cum aequatio modo inventa tam pro p quam pro q sit quadratica, pro utraque etiam geminum valorem continebit, unde, si pro quovis q gemini valores ipsius p ponantur p et p', erit ex natura aequationum

$$p + p' = \frac{2\lambda bq}{\lambda m - \lambda\lambda aqq} \quad \text{sive} \quad p + p' = \frac{2bq}{m - \lambda aqq} .$$

Simili modo pro quovis p, si gemini valores ipsius q ponantur q et q', erit

$$q + q' = \frac{2bp}{n - \lambda app} .$$

Quare, cum pro casu cognito invenerimus $\lambda = nc$, ubi scilicet erat $p = 0$ et $q = \frac{1}{n}$, erit pro omnibus reliquis casibus

$$p' = \frac{2bq}{m - nacqq} - p \quad \text{et} \quad q' = \frac{2bp}{n - nacpp} - q .$$

Harum igitur formularum ope sequentem seriem formare licebit:

$$p, q, p', q', p'', q'' \text{ etc.},$$

quippe pro qua erit

$$p' = \frac{2bq}{m - nacqq} - p , \quad q' = \frac{2bp}{n - nacpp} - q ,$$

$$p'' = \frac{2bq'}{m - nacq'q'} - p' , \quad q'' = \frac{2bp}{n - nacp'p'} - q' .$$

18. Cum igitur huius seriei ex casu cognito $p = 0$ et $q = \frac{1}{n}$ ope harum formularum termini sequentes haud difficulter formari possint, erit

$$p' = \frac{2b}{mn - ac} , \qquad q' = \frac{4mnbb - (mn - ac)^2}{n(mn - ac)^2 - 4nabbc} .$$

Si hoc modo etiam sequentes definire vellemus, ad expressiones nimis prolixas perveniremus, verum in exemplis numericis hunc laborem quousque libuerit haud difficulter continuare licebit.

19. Inventa autem hac serie valores idonei pro ipsa quantitate x expedite assignari poterunt. Cum enim ob $\lambda = nc$ sit $x = ncpq$, eius valores successivi erunt

$$x = ncpq\,[=0],\quad x = ncp'q = \frac{2bc}{mn-ac},\quad x = ncp'q' = \frac{2bc(4mnbb-(mn-ac)^2)}{(mn-ac)^3-4abbc(mn-ac)},$$

et ita porro.

20. Ex singulis autem istis valoribus ipsius x totidem alii affines sine ullo labore exhiberi poterunt. Cum enim ipsa forma proposita posito $x = \frac{1}{y}$ induat hanc formam:

$$\frac{(a+2by+cyy)^2}{y^4} - \frac{4mn}{yy} = \square\,,$$

quae per y^4 multiplicata praebet istam formulam quadrato aequandam:

$$(a+2by+cyy)^2 - 4mnyy\,,$$

quae a proposita aliter non differt, nisi ut litterae a et c sint permutatae. Quamobrem, si in omnibus valoribus pro x inventis litteras a et c inter se permutemus, totidem valores pro littera y obtinebimus, qui inversi dabunt totidem novos valores pro x, scilicet, si valor quicunque pro x inventus fuerit $x = \frac{f}{g}$, atque in quantitatibus f et g litterae a et c permutentur, unde prodeant f' et g', tum quoque erit $x = \frac{g'}{f'}$, hocque modo vix ullum dubium superesse poterit, quin pro x omnes plane valores satisfacientes eruantur.

SOLUTIO PROBLEMATIS DIFFICILLIMI QUO HAE DUAE FORMULAE $aaxx + bbyy$ ET $aayy + bbxx$ QUADRATA REDDI DEBENT

Commentatio 773 indicis ENESTROEMIANI
Mémoires de l'académie des sciences de St-Pétersbourg 11, 1830, p. 12—30
Conventui exhibita die 3. iulii 1780

1. Hanc quaestionem non solum solutu difficillimam sed etiam maximi in Analysi momenti pronunciare non dubito. Primo enim in ea evolvenda satis diu frustra desudavi; deinde vero solutio, quam tandem sum adeptus, plura insignia artificia calculi postulat, quae haud contemnenda incrementa in universam Analysin DIOPHANTEAM inferre videntur. Cum autem haec quaestio circa bina quadratorum paria aa, bb et xx, yy versetur, eorum neutrum pro lubitu assumi potest, sed ambo parem industriam et sagacitatem requirunt.

2. Ponamus igitur

$$aaxx + bbyy = zz \quad \text{et} \quad aayy + bbxx = vv\,,$$

atque his formulis tam addendis quam subtrahendis prodit

$$(aa + bb)(xx + yy) = zz + vv \quad \text{et}$$
$$(aa - bb)(xx - yy) = zz - vv\,,$$

ex quibus quidem primum speravi solutionem derivare posse; propterea quod summa quadratorum $zz + vv$ pluribus modis in duo quadrata resolubilis requiritur, tum vero etiam manifestum est formulam $zz - vv$ plures factores involvere debere. Interim tamen haec consideratio vix quicquam ad solutionem inveniendam conferre videtur. Inde enim multo labore vix tandem unicam

solutionem elicere potui, qua inveni $a = 5$, $b = 3$, $x = 7$, $y = 4$. Hinc enim fit

$$aaxx + bbyy = 35^2 + 12^2 = 37^2 \quad \text{et}$$
$$aayy + bbxx = 20^2 + 21^2 = 29^2 .$$

Verum nihil prorsus attinet conatus irritos meos fusius exponere, propterea quod tandem ad solutionem generalem et satis elegantem perveni.

3. Primo igitur, ut formula $aaxx + bbyy$ quadratum reddatur, pono

$$\frac{ax}{by} = \frac{pp - qq}{2pq} ;$$

pro altera vero formula pono

$$\frac{ay}{bx} = \frac{rr - ss}{2rs} ,$$

quarum illa per hanc divisa praebet

$$\frac{xx}{yy} = \frac{rs(pp - qq)}{pq(rr - ss)} ,$$

ubi, si utrinque per $\frac{ppqq}{rrss}$ multiplicetur, orietur $\frac{ppqqxx}{rrssyy} = \frac{pq(pp - qq)}{rs(rr - ss)}$, sicque totam resolutionem perduximus ad binas has formulas inter se prorsus similes

$$pq(pp - qq) \quad \text{et} \quad rs(rr - ss) ,$$

quarum altera per alteram divisa quadratum producere debeat, vel quod eodem redit, ut earum productum evadat quadratum, in quo negotio plures Geometrae ingenti studio sunt versati, neque tamen a quoquam resolutio satis generalis est inventa, unde non solum plures solutiones particulares ad hoc institutum satis accomodatas sum adeptus, sed etiam tandem mihi contigit in solutionem generalem incidere, qua fines Analyseos DIOPHANTAEAE plurimum proferentur.

4. Quodsi autem huiusmodi casu invenerimus quo

$$\frac{pq(pp - qq)}{rs(rr - ss)} = \frac{tt}{uu} ,$$

statim inde deducimus

$$\frac{pqx}{rsy} = \frac{t}{u} \text{ ideoque } \frac{x}{y} = \frac{rst}{pqu} ,$$

qua fractione ad minimos terminos reducta ponatur $x = rst$ et $y = pqu$. Hinc cum habuerimus

$$\frac{ax}{by} = \frac{pp - qq}{2pq} \text{ ideoque } \frac{a}{b} = \frac{u(pp - qq)}{2rst},$$

qua fractione ad minimos terminos reducta capiatur iterum

$$a = u(pp - qq) \quad \text{et} \quad b = 2rst.$$

5. Hic igitur commode in usum vocari potest tabula, quam non ita pridem in dissertatione dedi[1]), in qua huius formulae:

$$AB(AA - BB)$$

factores non quadratos exhibui. Quod si enim inde depromantur duo casus eosdem factores non quadratos continentes, eorum productum utique erit quadratum, ideoque solutionem nostri Problematis suppeditabit. In ea autem tabula statim se offerunt tales valores: $p = 5$, $q = 2$, $r = 6$, $s = 1$. Hinc enim erit

$$\frac{pq(pp - qq)}{rs(rr - ss)} = 1,$$

ideoque $t = 1$ et $u = 1$, unde ergo habebimus $\frac{x}{y} = \frac{rs}{pq} = \frac{3}{5}$ et $\frac{a}{b} = \frac{pp - qq}{2rs} = \frac{7}{4}$. Hinc ergo colligimus $a = 7$, $b = 4$, $x = 5$, $y = 3$, quandoquidem tam litteras a et b quam x et y inter se permutare licet, sicque iste casus cum ante memorato convenit.

6. Simili modo tabula allegata etiam dat hos valores: $p = 5$, $q = 2$, $r = 8$, $s = 7$, unde fit $\frac{pq(pp - qq)}{rs(rr - ss)} = \frac{1}{4}$, ergo $t = 1$ et $u = 2$. Hinc ergo habebimus

$$\frac{x}{y} = \frac{rs}{2pq} = \frac{14}{5} \quad \text{et} \quad \frac{a}{b} = \frac{pp - qq}{rs} = \frac{3}{8}.$$

---

1) Vide Commentationem 515 § 31 et 39; praecipue exempla 1, 2 et 4 in § 34, 35 et 37 contracta. *Leonhardi Euleri Opera omnia*, series I, vol. 3, p. 446—450. R. F.

Quamobrem sumi potest $a = 8$, $b = 3$, $x = 14$, $y = 5$, unde fit

$$aaxx + bbyy = 113^2 \quad \text{et} \quad aayy + bbxx = 58^2 ,$$ [1])

quae solutio a praecedente parum discrepat.

7. Adhuc alius casus ex tabula depromi potest, quo $p = 6$, $q = 5$, $r = 8$, $s = 3$, qui dat $\frac{pq(pp-qq)}{rs(rr-ss)} = \frac{1}{4}$, ergo iterum $t = 1$ et $u = 2$, unde colligitur

$$\frac{x}{y} = \frac{rs}{2pq} = \frac{2}{5} \quad \text{et} \quad \frac{a}{b} = \frac{pp-qq}{rs} = \frac{11}{24} .$$

Sumto igitur $a = 24$, $b = 11$, $x = 5$, $y = 2$, fiet

$$aaxx + bbyy = 122^2 \quad \text{et} \quad aayy + bbxx = 73^2 .$$

8. Quoniam autem hoc modo solutiones tantum singulares reperiuntur atque tabula illa ad limites satis arctos restringitur, hic potissimum in formulas generaliores sumus inquisituri, quae simul infinitam multitudinem solutionum contineant, id quod pluribus modis fieri posse observavi, etsi hae formulae tantum solutiones particulares exhibeant. Quamobrem aliquot huiusmodi solutiones particulares in medium afferamus, ex quibus innumerabiles alias solutiones derivare liceat, quibus expositis solutionem demum generalem aggrediemur.

PRIMA SOLUTIO PARTICULARIS

9. Sumamus statim $s = q$ et $r = p + q$, quo pacto fractio nostra generalis

$$\frac{pq(pp-qq)}{rs(rr-ss)} = \frac{tt}{uu}$$

ad hanc simplicem formam reducitur

$$\frac{p-q}{p+2q} = \frac{tt}{uu} ,$$

unde deducimus

$$\frac{p}{q} = \frac{uu+2tt}{uu-tt} .$$

1) Editio princeps: 38^2. Correxit R. F.

Quamobrem, si sumamus $p = uu + 2tt$ et $q = uu - tt$, fiet $r = 2uu + tt$ et $s = uu - tt$. Ex his ergo valoribus colligitur

$$\frac{x}{y} = \frac{t(2uu + tt)}{u(uu + 2tt)} \quad \text{et} \quad \frac{a}{b} = \frac{3ut}{2(uu - tt)},$$

ideoque

$$a = 3tu,\ b = 2(uu - tt),\ x = t(2uu + tt),\ y = u(uu + 2tt).$$

Ex his autem valoribus erit

$$ax = 3ttu(2uu + tt) \quad \text{et} \quad by = 2u(uu - tt)(uu + 2tt).$$

Hinc igitur colligimus

$$z = u\big((uu - tt)^2 + (uu + 2tt)^2\big) = u(2u^4 + 2ttuu + 5t^4).$$

Simili modo, cum sit

$$ay = 3tuu(uu + 2tt) \quad \text{et} \quad bx = 2t(uu - tt)(2uu + tt),$$

unde colligimus

$$v = t\big((uu - tt)^2 + (2uu + tt)^2\big) = t(2t^4 + 2ttuu + 5u^4).$$

10. Hinc igitur facili negotio plurimae solutiones singulares deduci poterunt, quia pro litteris t et u numeros quoscunque[1]) assumere licet, non solum in numeris exiguis sed etiam valores quantumvis grandos assumere licebit, cuius modi ope tabulae ante usitatae neutiquam obtineri possunt. Operae igitur pretium erit has formulas per exempla illustrare, dum scilicet litteris t et u valores pro arbitrio assignamus. At quia litterae t et u inter se permutantur, ipsi u valores maiores, t vero minores tribuamus, quia casus $t = u$ nihil daret. Hinc in sequentem tabulam plura exempla simul ante oculos ponamus:

u	2	3	3	4	4	5	5	5	5	6	6
t	1	1	2	1	3	1	2	3	4	1	5
a	1	9	9	2	18	5	5	45	10	9	45
b	1	16	5	5	7	16	7	32	3	35	11
x	3	19	44	11	123	17	36	177	88	73	485
y	4	33	51	24	136	45	55	215	95	228	516
z	5	555	471	122	2410	725	425	10525	925	8007	22551
v	5	425	509	73	2595	353	373	11211	986	3277	23825

1) Inter se primos. R. F.

SOLUTIO PARTICULARIS SECUNDA

11. Maneat $r = p + q$, et sumatur $s = p$ fietque

$$\frac{pq(pp - qq)}{rs(rr - ss)} = \frac{tt}{uu} = \frac{p - q}{2p + q},$$

unde colligitur

$$\frac{p}{q} = \frac{uu + tt}{uu - 2tt}.$$

Sumatur ergo $p = uu + tt$ atque $q = uu - 2tt$, eritque $r = 2uu - tt$ et $s = uu + tt$. Ex his valoribus sequitur fore

$$\frac{x}{y} = \frac{rst}{pqu} = \frac{t(2uu - tt)}{u(uu - 2tt)} \quad \text{et} \quad \frac{a}{b} = \frac{u(pp - qq)}{2rst} = \frac{3tu}{2(uu + tt)}.$$

Quamobrem radices quatuor nostrorum quadratorum erunt:

$$a = 3tu,\ b = 2(uu + tt),\ x = t(2uu - tt),\ y = u(uu - 2tt),$$

quae solutio a praecedente hoc tantum differt, quod tt hic sit negative sumtum manente tamen radice t eadem, unde deducuntur pro z et v sequentes valores:

$$z = u(2u^4 - 2ttuu + 5t^4) \quad \text{et} \quad v = t(2t^4 - 2ttuu + 5u^4),$$

sive in gratiam calculi

$$z = u\big((uu + tt)^2 + (uu - 2tt)^2\big),$$
$$v = t\big((uu + tt)^2 + (2uu - tt)^2\big).$$

12. Etsi hae formulae tam parum a praecedentibus differunt, tamen prorsus diversas in numeris solutiones suppeditant; quocirca ut ante loco t et u valores simpliciores accipiamus et solutiones numericas in sequenti tabula repraesentemus, ubi notandum, si loco a, b, x, y prodeant valores negativi, eorum loco semper positivos scribi posse[1]).

1) Editio princeps non continet columnam $u = 5$, $t = 2$. A. M.

u	1	2	3	3	4	4	5	5	5	5	6
t	1	1	1	2	1	3	1	2	3	4	1
a	3	3	9	9	6	18	15	15	45	30	9
b	4	5	20	13	17	25	52	29	68	41	37
x	1	7	17	28	31	69	49	92	123	136	71
y	1	4	21	3	56	8	115	85	35	35	204
z	5	29	447	255	970	1258	6025	2825	6025	4325	7575
v	5	37	389	365	625	1731	3077	2957	8511	5674	3205

SOLUTIO PARTICULARIS TERTIA

13. Sumamus hic $s = q$ ac ponamus $\frac{pq(pp-qq)}{rs(rr-ss)} = 1$, eritque

$$p(pp-qq) = r(rr-qq),$$

unde fit

$$qq = \frac{r^3-p^3}{r-p} = rr + pr + pp,$$

quae ergo formula quadratum esse debet. Cum igitur sit

$$qq = (r + \tfrac{1}{2}p)^2 + 3\left(\frac{p}{2}\right)^2,$$

sumatur $r + \frac{1}{2}p = tt - 3uu$ et $\frac{1}{2}p = 2tu$, eritque $q = tt + 3uu$. Quoniam ergo $p = 4tu$, erit $r = tt - 2tu - 3uu = (t+u)(t-3u)$. Quare cum pro praecedentibus formulis sit $t = 1$ et $u = 1$, quos valores cum praesentibus confundi non oportet, erit:

$$\frac{x}{y} = \frac{rs}{pq} \quad \text{et} \quad \frac{a}{b} = \frac{pp-qq}{2rs}.$$

Habebimus ergo

$$x = (t+u)(t-3u) \quad \text{et} \quad y = 4tu;$$

tum vero

$$a = (t-u)(t+3u) \quad \text{et} \quad b = 2(tt+3uu)\ ^{1}).$$

1) Signa valorum a, b, x, y omitti possunt. R. F.

Cum igitur sit

$$ax = (tt - uu)(tt - 9uu) \quad \text{et} \quad by = 8tu(tt + 3uu),$$

ponatur $(tt - uu)(tt - 9uu) = A^2 - B^2$ atque esse oportet

$$8tu(tt + 3uu) = 2AB,$$

ut fiat $z = A^2 + B^2$. Erit ergo $AB = 4tu(tt + 3uu)$, unde sumamus $A = tt + 3uu$ et $B = 4tu$, eritque

$$A + B = (t + 3u)(t + u) \quad \text{et} \quad A - B = (t - 3u)(t - u),$$

quocirca erit $A^2 - B^2 = (tt - uu)(tt - 9uu)$ prorsus, uti requiritur, consequenter erit nunc

$$z = (tt + 3uu)^2 + 16ttuu = t^4 + 22ttuu + 9u^4.$$

Simili modo sit

$$ay = 4tu(t - u)(t + 3u) = 4AB$$

et

$$bx = 2(t + u)(t - 3u)(tt + 3uu) = 2(A^2 - B^2).$$

Hinc enim fiet $v = 2(A^2 + B^2)$. Statuamus ergo $A + B = tt + 3uu$ et $A - B = tt - 2tu - 3uu$, unde fit $A = tt - tu$ et $B = 3uu + tu$, quod cum positione egregie convenit, consequenter erit

$$v = 2\big(tt(t - u)^2 + uu(t + 3u)^2\big).$$

En ergo solutionem nostri problematis tertiam particularem:

$$a = (t - u)(t + 3u), \qquad b = 2(tt + 3uu),$$
$$x = (t + u)(t - 3u), \qquad y = 4tu,$$
$$z = (tt + 3uu)^2 + 16ttuu,$$
$$v = 2tt(t - u)^2 + 2uu(t + 3u)^2.$$

Ubi iterum notandum est, si pro his litteris valores prodeant negativi, eos tuto in positivos verti posse. Tribuamus igitur binis litteris t et u simpliciores valores numericos, unde quidem casus $t = u$, et $t = 3u$ excludi debent, itemque casus, ubi t et u sunt impares, et solutiones hinc oriundas in sequenti tabula stipemus.

t	2	1	4	1	4	5	2	5	4
u	1	2	1	4	3	2	5	4	5
a	5	7	21	39	13	33	51	17	19
b	14	26	38	98	86	74	158	146	182
x	3	15	5	55	35	7	91	63	99
y	8	8	16	16	48	40	40	80	80
z	113	233	617	2657	4153	2969	7841	11729	14681
v	58	394	386	5426	3074	1418	14522	9298	18082

SOLUTIO GENERALIS

14. Cum totum negotium reductum sit ad resolutionem huius aequationis:

$$\frac{pq(pp-qq)}{rs(rr-ss)} = \frac{tt}{uu},$$

loco $\frac{tt}{uu}$ scribamus brevitatis gratia litteram n, ita ut sit $t = \sqrt{n}$ et $u = 1$, unde ex litteris p, q, r, s inventis numeri quaesiti a, b, x, y ita determinabuntur, ut sit

$$\frac{x}{y} = \frac{rs}{pq}\sqrt{n} \quad \text{et} \quad \frac{a}{b} = \frac{pp-qq}{2rs\sqrt{n}},$$

vel, cum litterae a et b inter se permutari queant, poni poterit

$$\frac{a}{b} = \frac{2rs}{pp-qq}\sqrt{n},$$

quibus fractionibus ad minimos terminos reductis habebuntur ipsi numeri quaesiti a, b, x, y. Nunc, quemadmodum illa aequatio principalis:

$$\frac{pq(pp-qq)}{rs(rr-ss)} = n$$

resolvi debeat, hic prorsus novam methodum apperiam, unde maxima incrementa in universam Analysin DIOPHANTAEAM redundabunt, cum a nemine adhuc ista aequatio generaliter sit evoluta.

15. Quoniam hic sola relatio inter binas litteras p et q et inter binas r et s in computum venit, sine ulla restrictione assumere licet $s = q$, ita ut sit

$$\frac{p(pp - qq)}{r(rr - qq)} = n \ ;$$

hinc colligitur

$$qq = \frac{p^3 - nr^3}{p - nr} \ .$$

Hic iam porro statuatur $p = rv$ fietque

$$\frac{qq}{rr} = \frac{v^3 - n}{v - n} \ ,$$

sicque tota investigatio eo redit, ut ista formula $\frac{v^3 - n}{v - n}$ quadrato aequetur. Communi igitur methodo utentes, productum ex numeratore in denominatorem, quod est $v^4 - nv^3 - nv + nn$, quadratum reddi deberet, cuius quidem ope statim aliquot valores pro v erui possent, quibus inventis ipsa haec formula per novas substitutiones transformari deberet, unde denuo novi valores erui possent, verum mox ad numeros tam enormes perveniretur, ut non nisi paucissimi valores modicae magnitudinis erui possent. At vero methodus mea nova nobis plurimas solutiones in numeris satis exiguis suppeditabit.

16. Statuo autem

$$\frac{v^3 - n}{v - n} = (v - z)^2 \ ,$$

ita ut sit $\frac{q}{r} = [\pm](v - z)$, dum, ut ante vidimus, est $\frac{p}{r} = v$. Facta igitur evolutione prodit haec aequatio:

$$(n + 2z)vv - z(2n + z)v + n(zz - 1) = 0 \ ,$$

quae tam respectu ipsius v quam ipsius z est quadratica, ideoque duas radices exhibet. At vero termini secundum z dispositi praebebunt hanc aequationem:

$$(n - v)zz - 2v(n - v)z - n(1 - vv) = 0 \ .$$

Quoniam igitur cuilibet factori ipsius v gemini ipsius z respondent, si hi designentur per z et z', erit ex natura aequationum

$$z + z' = 2v \ .$$

Simili modo cuilibet valori ipsius z respondent gemini ipsius v, qui si ponantur v et v', erit

$$v + v' = \frac{z(z+2n)}{2z+n},$$

unde, si iam valores pro v et z quicunque habeantur, ex iis novi pro iisdem litteris, scilicet v' et z', [obtinebuntur]; erit

$$z' = 2v - z \quad \text{et} \quad v' = \frac{z(z+2n)}{2z+n} - v .$$

Similique modo ex his valoribus denuo bini novi, hincque porro alii in infinitum reperiri poterunt, idque facili negotio, atque in hac duplici evolutione tota vis novae solutionis consistit, ita ut hoc modo plurimi valores sine ulla molesta transformatione obtineri queant, statim atque binos tantum valores pro v et z cognoverimus.

17. Tales autem valores primitivos ipsa aequatio quadratica quasi sponte nobis offert. Posito enim $v = 0$ fiet $zz - 1 = 0$, unde duo valores oriuntur $z = +1$ et $z = -1$. Simili modo posito $z = 0$ fit $vv - 1 = 0$ ideoque tam $v = +1$ quam $v = -1$, ita ut hinc iam habeamus quatuor casus, unde continuo novi valores pro litteris v et z derivari queant. Praeterea vero etiam quintus casus adiici poterit, ex positione $v = \infty$ oriundus; tum enim coefficiens ipsius vv, qui est $n + 2z$, nihilo aequari debet, unde cum fiat $z = -\frac{n}{2}$, nunc aequatio induet hanc formam: $3nv + nn - 4\,[=0]$, unde colligitur $v = \frac{4-nn}{3n}$, qui est alter valor ipsius v valori $z = -\frac{n}{2}$ respondens, dum alter erat $v = \infty$, atque ex his duobus valoribus $z = -\frac{n}{2}$ et $v = \frac{4-nn}{3n}$, ope nostrarum formularum continuo plures novi elici poterunt. Hinc ergo istos quinque casus ulterius evolvamus.

CASUS I

quo $v = 0$ *et* $z = +1$

18. Hinc igitur per nostras formulas alternatim applicandas novi valores inde oriundi reperiuntur:

1°) $v = \frac{1+2n}{2+n}$, $z = \frac{3n}{2+n}$;

2°) $v = \frac{4(nn+n-2)}{nn+10n+16} = \frac{4(n-1)}{n+8}$, $z = \frac{5nn-16n-16}{nn+10n+16}$.

In genere autem vix ulterius progredi licet. Loco n nunc restituamus $\frac{tt}{uu}$, et cum secundus valor sit

$$v = \frac{1+2n}{2+n} \quad \text{et} \quad v - z = \frac{1-n}{2+n}\ ^{1}),$$

erit

$$v = \frac{p}{r} = \frac{uu+2tt}{2uu+tt} \quad \text{et} \quad v - z = \frac{q}{r} = \frac{uu-tt}{tt+2uu}.$$

Quamobrem sumamus

$$p = uu + 2tt,\ q = uu - tt,\ r = 2uu + tt,\ s = uu - tt,$$

qui casus prorsus congruit cum solutione particulari prima supra data. Simili modo evolvamus valorem tertium ipsius v, qui erat $\frac{4(n-1)}{n+8}$, cui respondet $z = \frac{3n}{2+n}$, unde fit

$$v - z = \frac{nn-20n-8}{(2+n)\ (8+n)}.$$

Hinc ergo erit

$$\frac{p}{r} = \frac{4(tt-uu)}{tt+8uu} \quad \text{et} \quad \frac{q}{r} = \frac{t^4 - 20ttuu - 8u^4}{(2uu+tt)\ (8uu+tt)}.$$

Sumatur ergo $r = (2uu + tt)\,(8uu + tt)$ eritque

$$p = 4(tt - uu)\,(tt + 2uu) \quad \text{et} \quad q = s = t^4 - 20ttuu - 8u^4.$$

Hinc igitur porro reperitur

$$\frac{x}{y} = \frac{t(8uu+tt)}{4u(tt-uu)} \quad \text{et} \quad \frac{a}{b} = \frac{3tu(5t^4 - 16ttuu - 16u^4)}{2(2uu+tt)\ (t^4 - 20ttuu - 8u^4)},$$

unde innumerabiles novae solutiones reperiuntur.

---

1) Editio princeps continet $\frac{n-1}{2+n}$; quamobrem in formulis sequentibus $uu - tt$ loco $tt - uu$ poni debuit. Correxit A. M.

CASUS II

quo $v = 0$ *et* $z = -1$

19. Hic ergo formulis supra datis sequentes valores deducuntur:

$$v = \frac{1-2n}{n-2}\ , \quad z = -\frac{3n}{n-2}\ , \quad v = -\frac{4(n+1)}{n-8}\ .$$

Evolvamus secundum valorem ipsius v, scilicet $\frac{1-2n}{n-2}$, cui respondet $z = -1$; unde fit $v - z = \frac{n+1}{2-n}$; ergo loco n posito $\frac{tt}{uu}$ fiet

$$\frac{p}{r} = v = \frac{uu-2tt}{tt-2uu} \quad \text{et} \quad [\pm]\frac{q}{r} = v - z = \frac{tt+uu}{2uu-tt}\ .$$

Sumto ergo $r = tt - 2uu$ erit $p = uu - 2tt$ et $q = s = tt + uu$, unde iam patet hunc casum cum solutione particulari secunda convenire, quia litteras p et q inter se permutare licet, neque ergo opus est hunc casum ulterius prosequi.

20. Consideremus igitur tertium valorem ipsius v, qui erat $-\frac{4(n+1)}{n-8}$, cui respondet $z = -\frac{3n}{n-2}$. His duobus valoribus cognitis habebimus $\frac{p}{r} = v$ et $\frac{q}{r} = v - z$, sicque obtinebuntur quatuor litterae p, q, r, s, ex quibus porro facile deducuntur numeri quaesiti a, b, x, y ope formularum supra datarum

$$\frac{a}{b} = \frac{2rs}{pp-qq}\sqrt{n} \quad \text{et} \quad \frac{x}{y} = \frac{rs}{pq}\sqrt{n}\ .$$

Ad quod illustrandum evolvamus casum, quo $n = \frac{9}{4}$, eritque $z = -27$ et $v = \frac{52}{23}$. Hinc fit $v - z = \frac{673}{23}$. Hinc ergo erit $\frac{p}{r} = \frac{52}{23}$ et $\frac{q}{r} = \frac{673}{23}$. Sumatur ergo $r = 23$, erit $p = 52$ et $q = 673 = s$, unde porro sequitur $\frac{a}{b} = \frac{673}{9 \cdot 725}$ et $\frac{x}{y} = \frac{3 \cdot 23}{2 \cdot 52}$. Quatuor ergo numeri quaesiti erunt

$$a = 673, \quad b = 9 \cdot 725, \quad x = 3 \cdot 23, \quad y = 2 \cdot 52\ ^{1})\ .$$

---

1) Editio princeps: $\frac{p}{q} = \frac{53}{23}$, $p = 53$, $\frac{a}{b} = \frac{23 \cdot 673}{242 \cdot 620}$, $\frac{x}{y} = \frac{3 \cdot 23}{2 \cdot 53}$, $a = 23 \cdot 673$, $b = 242 \cdot 620$, $y = 2 \cdot 53$. Correxit A. M.

CASUS III

quo $z = 0$ *et* $v = 1$

21. Ex formulis supra datis pro hoc casu deducuntur sequentes valores:

$$z = 2\ , \quad v = \frac{3n}{n+4}\ , \quad z = \frac{4(n-2)}{n+4}\ , \quad v = \frac{5nn - 24n + 16}{nn + 12n - 16}\ ,$$

ubi primus valor ipsius v nihil prodest; secundus vero $v = \frac{3n}{n+4}$, cui respondet $z = 2$, ita ut sit $v - z = \frac{n-8}{n+4}$, dat

$$\frac{p}{r} = \frac{3tt}{tt + 4uu} \quad \text{et} \quad \frac{q}{r} = \frac{tt - 8uu}{tt + 4uu}\ .$$

Sumto ergo $r = tt + 4uu$ habebimus $p = 3tt$ et $q = s = tt - 8uu$, ex quibus porro deducimus:

$$\frac{a}{b} = \frac{t(tt - 8uu)}{4u(tt - 2uu)} \quad \text{et} \quad \frac{x}{y} = \frac{(tt + 4uu)}{3tu}\ .$$

Hae formulae reddentur concinniores, si loco u scribamus $\frac{1}{2}u$, tum enim erit:

$$\frac{a}{b} = \frac{t(tt - 2uu)}{u(2tt - uu)} \quad \text{et} \quad \frac{x}{y} = \frac{2(tt + uu)}{3tu}\ ,$$

consequenter quatuor numeri nostri quaesiti erunt:

$$a = t(tt - 2uu),\ \ b = u(2tt - uu),\ \ x = 2(tt + uu),\ \ y = 3tu,$$

qui casus iterum convenit cum solutione secunda particulari.

CASUS IV

quo $z = 0$ *et* $v = -1$

22. Hinc igitur valores derivati ita progredientur:

$$z = 0\ , \quad v = -1\ , \quad z = -2\ , \quad v = -\frac{3n}{n-4}\ , \quad z = -\frac{4(n+2)}{n-4}\ ,$$

$$v = -\frac{(5nn + 24n + 16)}{nn - 12n - 16}\ ,$$

qui valores a praecedente casu hoc tantum differunt, quod sumto n negativo etiam v et z fiunt negativi. Hinc, si ex valore $v = -\frac{3n}{n-4}$ posito $n = \frac{tt}{uu}$ litterae p, q, r, s derivantur, erit

$$p = 3tt, \quad q = s = tt + 8uu, \quad r = tt - 4uu;$$

ac si hic ut ante loco u scribamus $\frac{1}{2}u$, valores litterarum a, b, x, y quaesiti erunt:

$$a = t(tt + 2uu), \; b = u(2tt + uu), \; x = 2(tt - uu), \; y = 3tu,$$

quae formulae conveniunt cum casu particulari primo. At vero sequentes valores ipsius v in omnibus his casibus prorsus novas suppeditabunt solutiones in casibus particularibus non contentos, ex quo generalitas huius novae solutionis clarissime elucet.

CASUS V

qui incipit a $v = \infty$

23. Ex formulis ergo generalibus valores successive pro v et z ita se habebunt:

$$v = \infty, \quad z = -\frac{n}{2}, \quad v = \frac{4 - nn}{3n}, \quad z = \frac{16 - nn}{6n}, \quad v = \frac{n(64 - nn)}{8(nn + 8)}.$$

Hic iam secundus valor ipsius v, qui est $\frac{4 - nn}{3n}$, cui respondet $z = -\frac{n}{2}$, ita ut sit $v - z = \frac{8 + nn}{6n}$, posito $n = \frac{tt}{uu}$ hos praebet valores:

$$\frac{p}{r} = \frac{4u^4 - t^4}{3ttuu} \quad \text{et} \quad \frac{q}{r} = \frac{8u^4 + t^4}{6ttuu},$$

unde deducimus

$$p = 8u^4 - 2t^4, \quad r = 6ttuu, \quad q = s = 8u^4 + t^4,$$

ex quibus colligimus fore

$$\frac{a}{b} = \frac{4u(8u^4 + t^4)}{t(16u^4 - t^4)} \quad \text{et} \quad \frac{x}{y} = \frac{6t^3u}{8u^4 - 2t^4},$$

ideoque sumi poterit

$$a = 4u(8u^4 + t^4),\ b = t(16u^4 - t^4),\ x = 6t^3u,\ y = 8u^4 - 2t^4.$$

Has igitur formulas ad solutiones quasdam speciales accommodemus, tribuendo litteris t et u valores simpliciores, quas solutiones in sequenti tabula comprehendamus:

t	1	2	3	3	1	1	2
u	1	1	1	2	3	2	3
a	12	1	$4 \cdot 89$	$8 \cdot 11 \cdot 19$	$11 \cdot 12 \cdot 59$	$8 \cdot 43$	$3 \cdot 83$
b	5	0	$3 \cdot 5 \cdot 13$	$3 \cdot 7 \cdot 25$	$5 \cdot 7 \cdot 37$	$5 \cdot 17$	$2 \cdot 5 \cdot 8$
x	1	2	81	$2 \cdot 81$	9	2	$3 \cdot 6$
y	1	1	$7 \cdot 11$	17	$17 \cdot 19$	21	$7 \cdot 11$

24. His casibus litteras z et v non ultra paucos terminos assignare licuit, si quidem litterae n valorem indefinitum relinquamus; at si eius loco determinata quadrata assumamus, plerumque has series ad plurimos terminos continuare licet, id quod nonnullis exemplis ostendisse iuvabit.

EVOLUTIO SOLUTIONUM

ex casu $n = 4$ oriundarum

25. Hoc ergo casu erit $v' = \frac{z(z+8)}{2z+4} - v$ manente $z' = 2v - z$. In huius evolutione statim a casu quinto, quo $v = \infty$, incipiamus, quoniam mox videbimus in eo reliquos quatuor casus omnes comprehendi. Quoniam igitur pro hoc casu vidimus esse $z = -\frac{n}{2}$ et sequens $v = \frac{4 - nn}{3n}$, series harum litterarum sequenti modo se habebit:

$v = \infty$, $z = -2$	$v = +\frac{17}{3}$, $z = -\frac{14}{3}$
$v = -1$, $z = 0$	$v = -\frac{11}{4}$, $z = -\frac{5}{6}$
$v = +1$, $z = +2$	$v = +\frac{4}{21}$, $z = +\frac{17}{14}$
$v = \frac{3}{2}$, $z = +1$	$v = +\frac{31}{20}$, $z = +\frac{66}{35}$
$v = 0$, $z = -1$	$v = +\frac{101}{119}$, $z = -\frac{16}{85}$
$v = -\frac{7}{2}$, $z = -6$	$v = -\frac{69}{55}$, $z = -\frac{434}{187}$
$v = +5$, $z = +16$	$v = +\frac{741}{34}$, etc.

26. Hinc iam ex quovis valore v cum proximo z coniuncto (perinde enim est, sive cum praecedente sive cum sequente coniungatur) solutio nostrae quaestionis deduci potest, cum sit

$$\frac{p}{r} = v \quad \text{et} \quad \frac{q}{r} = v - z ,$$

hincque porro ob $\sqrt{n} = 2$ erit

$$\frac{a}{b} = \frac{4rs}{pp - qq} \quad \text{et} \quad \frac{x}{y} = \frac{2rs}{pq} .$$

Ita sumto $v = \frac{4}{21}$, cui respondet $z = -\frac{5}{6}$, fiet $v - z = \frac{43}{42}$. Hinc ergo erit $\frac{p}{r} = \frac{4}{21}$ et $\frac{q}{r} = \frac{43}{42}$. Sumto ergo $r = 42$ erit $p = 8$ et $q = s = 43$. Ex his valoribus denique colligitur $\frac{a}{b} = \frac{8 \cdot 43}{5 \cdot 17}$ et $\frac{x}{y} = \frac{21}{2}$, quocirca erit

$$a = 8 \cdot 43, \quad b = 5 \cdot 17, \quad x = 21, \quad y = 2 .$$

Hinc erit $ax = 3 \cdot 7 \cdot 8 \cdot 43$ et $by = 2 \cdot 5 \cdot 17$, qui factorem communem habent 2. Posito ergo

$$2 \cdot 3 \cdot 7 \cdot 43 = AB \quad \text{et} \quad 5 \cdot 17 = AA - BB ,$$

sumtoque $A = 43$ et $B = 42$ fiet $AA - BB = 5 \cdot 17$, uti requiritur, ex quo erit $\sqrt{aaxx + bbyy} = 2(43^2 + 42^2) = 7226$, quem numerum supra vocavimus z. Simili modo erit $ay = 16 \cdot 43$ et $bx = 3 \cdot 5 \cdot 7 \cdot 17$, atque hic habebimus

$$AB = 8 \cdot 43 \quad \text{et} \quad A^2 - B^2 = 3 \cdot 5 \cdot 7 \cdot 17 .$$

Sumto ergo $A = 43$ et $B = 8$ erit $A^2 - B^2 = 35 \cdot 51$, quamobrem erit $\sqrt{aayy + bbxx} = 1913$, quem numerum supra indicavimus littera v, ita ut v et z innotescunt. Ceterum, quia in serie litterarum z et v inventa occurrunt valores $v = 0$ et $z = 0$, evidens est omnes quatuor priores casus in illa involvi.

EVOLUTIO SOLUTIONUM

ex casu $n = \frac{1}{4}$ *oriundorum*

27. Hoc ergo casu erit $v' = \frac{2z(2z+1)}{8z+1} - v$ manente $z' = 2v - z$. Pro hoc iam omnes quinque casus supra constitutos percurramus:

I.	II.	III.	IV.	V.
$v = 0$	$v = 0$	$v = \infty$	$z = 0$	$z = 0$
$z = 1$	$z = -1$	$z = -\frac{1}{8}$	$v = 1$	$v = -1$
$v = \frac{2}{3}$	$v = -\frac{2}{7}$	$v = \frac{21}{4}$	$z = 2$	$z = -2$
$z = \frac{1}{3}$	$z = \frac{3}{7}$	$z = \frac{85}{8}$	$v = \frac{3}{17}$	$v = \frac{1}{5}$
$v = -\frac{4}{11}$	$v = \frac{20}{31}$	$v = \frac{341}{32 \cdot 43}$	$z = -\frac{28}{17}$	$z = \frac{12}{5}$
$z = -\frac{35}{33}$	$z = \frac{187}{7 \cdot 31}$	$z = -\frac{6969}{16 \cdot 43}$	$v = -\frac{55}{69}$	$v = \frac{119}{101}$

Evidens autem est pro v valores inversos in praecedente casu comprehendi debere, quoniam permutatis litteris p et r loco n scribi debet $\frac{1}{n}$.

28. Casum praecipuum, quo $n = 1$, ideo hic non attingimus, quoniam in casu particulari tertio iam penitus est exhaustus. Ceterum, quia hoc casu $n = 1$ aequatio quadratica inter z et v inventa evadit

$$(1 + 2z)vv - z(2 + z)v + zz - 1 = 0$$

sive

$$(1 - v)zz - 2v(1 - v)z + vv - 1 = 0 ,$$

quae aequatio cum divisorem habeat $v - 1$, evidens est posito $v = 1$ valorem respondentem z arbitrio nostro relinqui.

29. Coronidis loco problema multo magis arduum hic subiungamus, quod vix aggredi ausus fuissem, nisi praeter omnem exspectationem solutio particularis tertia eius solutionem suppeditasset.

PROBLEMA

Invenire quatuor numeros quadratos aa, bb, cc, dd eius indolis, ut productum ex binis quibusvis, una cum producto binorum reliquorum, faciat quadratum, sive ut istae tres formulae evadant quadrata:

$$aabb + ccdd = \square ,$$
$$aacc + bbdd = \square ,$$
$$aadd + bbcc = \square .$$

SOLUTIO

30. Solutio particularis tertia pro litteris a, b, x, y hos nobis suppeditavit valores:

$$a = (t - u)(t + 3u), \quad b = 2(tt + 3uu),$$
$$x = (t + u)(t - 3u), \quad y = 4tu,$$

ubi formula pro x inventa ita similis est illi pro a inventae, ut sumto u negativo altera in alteram vertatur. Quare cum sit

$$bbxx + aayy = \square ,$$

permutatis a et x etiam haec formula $aabb + xxyy$ erit quadratum; cum ex conditione problematis iam hae duae formulae:

$$aaxx + bbyy \quad \text{et} \quad aayy + bbxx$$

sint quadrata, sicque omnes has quatuor litteras a, b, x, y inter se permutare licet. Quare nil aliud opus est, nisi ut loco x et y scribamus c et d, atque solutio huius problematis maxime generalis sequentibus formulis satis simplicibus continetur:

$$a = 4tu\,, \quad b = 2(tt + 3uu)\,, \quad c = (t - u)(t + 3u)\,, \quad d = (t + u)(t - 3u),$$

ubi pro litteris t et u numeros quoscunque pro lubitu accipere licet.

31. Hinc simplicissimus casus orietur sumendo $t = 2$ et $u = 1$; tum enim fiet

$$a = 8, \quad b = 14, \quad c = 5, \quad d = 3\,.$$

Ceterum omnes solutiones in solutione particulari allatae acque satisfaciunt, quos in sequenti tabula iterum ob oculos ponamus[1]):

t	2	1	4	1	4	5	2	5	4
u	1	2	1	4	3	2	5	4	5
a	8	8	16	16	48	40	40	80	80
b	14	26	38	98	86	74	158	146	182
c	5	7	21	39	13	33	51	17	19
d	3	15	5	55	35	7	91	63	99

SOLUTIO SUCCINCTIOR

32. Quaerantur duo numeri f et g, ut sit $ff + 3gg = hh$, quod fit, uti vidimus, $f = tt - 3uu$, $g = 2tu$, tum enim erit $h = tt + 3uu$, hincque quatuor numeri quaesiti erunt

$$a = 2g, \quad b = 2h, \quad c = f + g, \quad d = f - g,$$

1) Vide p. 102 huius voluminis. R. F.

ex his porro valoribus reperitur:

$$\sqrt{aabb + ccdd} = ff + 7gg,$$
$$\sqrt{aacc + bbdd} = 2(ff - fg + 2gg),$$
$$\sqrt{aadd + bbcc} = 2(ff + fg + 2gg).$$

Hinc patet in hac solutione semper fore $c - d = a$. Quoniam vero haec solutio quasi praeter omnem expectationem sponte ex praecedentibus se obtulit, solutionem directam adiungamus.

SOLUTIO DIRECTA

33. Cum facta divisione per primum terminum hae tres formulae quadrata esse debeant:

$$1°)\ 1 + \frac{ccdd}{aabb} = \square\ ,\quad 2°)\ 1 + \frac{bbdd}{aacc} = \square\ ,\quad 3°)\ 1 + \frac{bbcc}{aadd} = \square\ ,$$

ponatur

$$\frac{cd}{ab} = \frac{pp - qq}{2pq} = P\ ,\quad \frac{bd}{ac} = \frac{rr - ss}{2rs} = R \quad \text{et} \quad \frac{bc}{ad} = \frac{tt - uu}{2tu} = T\ .$$

Ex his positionibus iam colligitur

$$\frac{d}{a} = \sqrt{PR}\ ,\quad \frac{c}{a} = \sqrt{PT}\ ,\quad \frac{b}{a} = \sqrt{RT}\ ;$$

quare ad solutionem inveniendam quaeri debent tres huiusmodi formulae P, R, T, ut producta ex binis sint quadrata. Tum enim facile numeri quaesiti a, b, c, d in integris definientur. Tales autem numeri obtinentur sumendo

$$p = 4fg, \qquad q = ff + 3gg, \qquad r = ff + 2fg - 3gg,$$
$$s = ff + 3gg, \quad t = ff - 2fg - 3gg, \quad u = ff + 3gg,$$

tum enim solutio supra data orietur, id quod nonnullis exemplis illustremus.

EXEMPLUM 1

34. Sumatur $p = 6,\ r = 5,\ t = 8,$
$q = 1,\ s = 2,\ u = 7,$

ex his igitur erit $P = \frac{5 \cdot 7}{4 \cdot 3}$, $R = \frac{3 \cdot 7}{4 \cdot 5}$, $T = \frac{3 \cdot 5}{16 \cdot 7}$, unde porro colligitur

$$\sqrt{PR} = \frac{7}{4} = \frac{d}{a};$$

tum vero

$$\sqrt{PT} = \frac{5}{8} = \frac{c}{a}, \text{ denique } \sqrt{RT} = \frac{3}{8} = \frac{b}{a}.$$

Quamobrem, si sumamus $a = 8$, erit $b = 3$, $c = 5$, $d = 14$, quae est solutio simplicissima iam supra eruta.

EXEMPLUM 2

35. Sumatur $p = 6,\ r = 8,\ t = 27,$
$q = 5,\ s = 3,\ u = 22,$

unde fit

$$P = \frac{11}{4 \cdot 3 \cdot 5}, \quad R = \frac{5 \cdot 11}{16 \cdot 3}, \quad T = \frac{5 \cdot 7^2}{4 \cdot 3^3 \cdot 11};$$

hinc porro sequitur fore

$$\sqrt{PR} = \frac{11}{24} = \frac{d}{a}, \quad \sqrt{PT} = \frac{7}{36} = \frac{c}{a} \text{ et } \sqrt{RT} = \frac{35}{72} = \frac{b}{a}.$$

Sumto ergo $a = 72$ erit $b = 35$, $c = 14$, $d = 33$, qui valores prorsus discrepant ab iis, quas praecedens methodus suppeditavit, unde patet superiorem solutionem non esse generalem, sed innumeras alias praeterea solutiones locum habere posse, ad quas inveniendas methodus requiritur idoneos valores pro tribus formulis P, R, T in genere investigandi, quod negotium aliis evolvendum relinquo.

INVESTIGATIO BINORUM NUMERORUM FORMAE $xy(x^4 - y^4)$ QUORUM PRODUCTUM SIVE QUOTUS SIT QUADRATUM

Commentatio 774 indicis ENESTROEMIANI
Mémoires de l'académie des sciences de St-Pétersbourg **11**, 1830, p. 31—45
Conventui exhibita die 14. augusti 1780

1. In Analysi DIOPHANTEA plura occurrunt problemata, ad quae resolvenda requiruntur duo numeri formae $xy(xx - yy)$ vel etiam huius $xy(xx + yy)$, quorum alter per alterum divisus producat quadratum. At vero harum formularum evolutio nullo modo in genere expediri potest, sed contenti esse debemus casus quosdam particulares resolvisse, qui adeo etiam haud exiguam sagacitatem postulant, quemadmodum in aliquot dissertationibus[1]) fusius ostendi, ubi hoc argumentum omni studio pertractavi. Quare cum formula proposita $xy(x^4 - y^4)$ multo magis sit complicata, atque adeo binas illas formulas quasi in se complectatur, haud immerito dubitare licet, utrum eius evolutio vires analyseos superet necne.

2. Equidem eius solutionem vix ausus essem suscipere, nisi felici quodam casu in solutionem difficillimi cuiusdam problematis incidissem, quod binos huiusmodi numeros postulat formae

$$xy(x^4 - y^4),$$

quorum productum sit quadratum. Hinc enim ex solutione a me reperta licuit reciproce tales numeros assignare, qui conditioni propositae satisfacerent.

3. Cum igitur isti problemati resolutionem quaestionis propositae acceptam referre oporteat, haud abs re erit istud problema hic breviter commemorare; quamquam enim istud problema iam in *Tomo XV novorum Commen-*

1) Vide Commentationem praecedentem. R. F.

tariorum[1]) tractavi, hic solutionem multo faciliorem et elegantiorem sum traditurus. Problema autem ita erat enunciatum:

Invenire duos numeros, quorum productum sive auctum sive minutum tam summa quam differentia ipsorum numerorum producat numeros quadratos.

4. Statuantur bini numeri quaesiti, quoniam integri esse nequeunt, $\frac{x}{z}$ et $\frac{y}{z}$, atque necesse est, ut istae formulae:

$$xy \pm z(x+y) \quad \text{et} \quad xy \pm z(x-y)$$

fiant quadrata. Pro harum formularum priore ponamus $xy = aa + bb$, eique satisfiet sumendo $z(x+y) = 2ab$. Simili modo, si pro posteriore ponamus $xy = cc + dd$, esse oportebit $z(x-y) = 2cd$. Efficiendum igitur est, ut bini valores pro xy assumti reddantur inter se aequales, sive ut fiat

$$aa + bb = cc + dd\,.$$

Deinde, cum ex priore sit $x+y = \frac{2ab}{z}$, ex posteriore vero $x-y = \frac{2cd}{z}$, hinc colligitur fore $x = \frac{ab+cd}{z}$ et $y = \frac{ab-cd}{z}$, quorum ergo productum $\frac{aabb-ccdd}{zz}$ ipsi $aa+bb$ ut et $cc+dd$ aequari debet, unde fieri oportebit

$$zz = \frac{aabb-ccdd}{aa+bb} = \frac{aabb-ccdd}{cc+dd}\,.$$

Cum igitur xy duplici modo in summam duorum quadratorum resolubile esse debeat, statuamus $xy = (pp+qq)(rr+ss)$ hincque pro formula priore $aa+bb$ accipiatur $a = pr+qs$ et $b = ps-qr$; pro posteriore vero $c = pr-qs$, tum vero $d = ps+qr$. Hinc ergo erit

$$ab+cd = 2rs(pp-qq) \quad \text{et} \quad ab-cd = 2pq(ss-rr)\,, \text{ unde prodibit}$$

$$zz = \frac{4pqrs(pp-qq)\,(ss-rr)}{(pp+qq)\,(rr+ss)}.$$

1) Commentatio 405 indicis ENESTROEMIANI: *Solutio problematis, quo duo quaeruntur numeri, quorum productum tam summa quam differentia eorum sive auctum sive minutum fiat quadratum*, Novi comment. acad. sc. Petrop. 15 (1770), 1771, p. 29—50. *LEONHARDI EULERI Opera omnia*, series I, vol. 3, p. 148—171.

5. Cum igitur haec fractio quadratum esse debeat, etiam productum ex numeratore in denominatorem, quod est

$$4pqrs(p^4 - q^4)(r^4 - s^4),$$

quadratum esse debebit, quod manifesto reducitur ad hoc productum

$$pq(p^4 - q^4) \cdot rs(r^4 - s^4),$$

vel etiam ista fractio $\frac{pq(p^4 - q^4)}{rs(r^4 - s^4)}$ ad quadratum reduci debebit, quae ergo est ea ipsa quaestio, quam hic enodandam suscepi.

6. Cum autem istud problema mihi olim proponeretur, pluribus tentaminibus frustra institutis tandem pro binis numeris quaesitis $\frac{x}{z}$ et $\frac{y}{z}$ hos elicui valores $\frac{13 \cdot 29^2}{8 \cdot 9^2}$ et $\frac{5 \cdot 29^2}{32 \cdot 11^2}$, ex quo casu vicissim pro litteris p, q, r, s conclusi istos valores:

$$p = 12, \quad q = 1, \quad r = 16 \quad \text{et} \quad s = 11,$$

qui quomodo nostrae quaestioni satisfaciant, videamus[1]). Erit igitur:

$p = 12$	$r = 16$
$q = 1$	$s = 11$
$p + q = 13$	$r + s = 27$
$p - q = 11$	$r - s = 5$
$pp + qq = 5 \cdot 29$	$rr + ss = 13 \cdot 29$.

Hinc porro colligimus fore:

$$pq(p^4 - q^4) = 4 \cdot 3 \cdot 13 \cdot 11 \cdot 5 \cdot 29,$$
$$rs(r^4 - s^4) = 16 \cdot 11 \cdot 3 \cdot 9 \cdot 5 \cdot 13 \cdot 29,$$

unde concluditur

$$\frac{pq(p^4 - q^4)}{rs(r^4 - s^4)} = \frac{1}{4 \cdot 9}.$$

1) Confer § 35 Commentationis p. 117 laudatae (series I, vol. 3, p. 170). R. F.

7. Cum igitur casus nobis constet, quo quaestioni hic propositae satisfit, eius consideratio nos perducere poterit ad alias solutiones investigandas. Quamobrem quasdam notabiles relationes in valoribus inventis occurrentes observemus, ubi statim ista notabilis convenientia deprehenditur, quod formulae $pp + qq$ et $rr + ss$ communem habeant factorem 29, dum alteri factores sunt 5 et 13; omnes scilicet summae duorum quadratorum, quemadmodum rei natura postulat.

8. Ab hac igitur conditione incipientes statuamus

$$pp + qq = (aa + bb)(xx + yy) \quad \text{et} \quad rr + ss = (cc + dd)(xx + yy),$$

ita ut $xx + yy$ sit factor utrique formulae communis, atque hinc nanciscemur sequentes valores:

$$p = ax + by, \qquad r = cx + dy,$$
$$q = bx - ay, \qquad s = dx - cy,$$

ideoque

$$p + q = (a + b)x + (b - a)y, \qquad r + s = (c + d)x + (d - c)y,$$
$$p - q = (a - b)x + (b + a)y, \qquad r - s = (c - d)x + (d + c)y.$$

9. Porro autem efficiamus, ut utrinque duo tantum termini se mutuo destruant, atque exemplum modo datum considerantes reperimus formulam $p - q = 11$ aequalem esse formulae $s = 11$, unde in genere istam aequalitatem statuamus $p - q = s$, hincque oritur ista aequatio:

$$(a - b)x + (b + a)y = dx - cy,$$

ex qua ratio inter x et y sponte definitur; fit enim

$$\frac{x}{y} = \frac{a + b + c}{d + b - a}.$$

Quamobrem in genere statuamus $x = a + b + c$ et $y = d + b - a$. Quamquam autem hoc modo quaestio restricta videatur, tamen re perpensa nulla plane restrictio est facta. Cum enim utrinque quaecunque multipla litterarum p et q itemque r et s perinde satisfaciant, semper talia multipla capere licebit, ut fiat $p - q = s$.

10. Praeterea etiam observasse iuvabit formulam $p + q$ in exemplo aequalem esse ipsi $cc + dd$; quamobrem in genere statuamus $p + q = cc + dd$,

qua positione autem utique ingens restrictio introducitur. Substitutis ergo loco x et y valoribus modo inventis reperietur sequens aequatio:

$$(a+b)(a+b+c)+(b-a)(b-a+d)=cc+dd$$

sive

$$(a+b)^2+c(a+b)+(b-a)^2+d(b-a)=cc+dd\,,$$

cui aequationi, si utrinque addatur $\frac{1}{4}(cc+dd)$, prodibit ista:

$$(a+b+\tfrac{1}{2}c)^2+(b-a+\tfrac{1}{2}d)^2=\tfrac{5}{4}(cc+dd)\,,$$

ubi in parte sinistra habetur summa duorum quadratorum. Evidens vero est membrum dextrum duplici modo summam duorum quadratorum continere scilicet vel $(c+\frac{1}{2}d)^2+(d-\frac{1}{2}c)^2$ vel etiam $(c-\frac{1}{2}d)^2+(d+\frac{1}{2}c)^2$. Hinc, prouti utrinque quodvis quadratum sive uni sive alteri aequale statuamus, quatuor hic occurrunt combinationes sequentes:

I.

$$a+b+\tfrac{1}{2}c=c+\tfrac{1}{2}d\,,\qquad b-a+\tfrac{1}{2}d=d-\tfrac{1}{2}c\,,$$

II.

$$a+b+\tfrac{1}{2}c=d-\tfrac{1}{2}c\,,\qquad b-a+\tfrac{1}{2}d=c+\tfrac{1}{2}d\,,$$

III.

$$a+b+\tfrac{1}{2}c=c-\tfrac{1}{2}d\,,\qquad b-a+\tfrac{1}{2}d=d+\tfrac{1}{2}c\,,$$

IV.

$$a+b+\tfrac{1}{2}c=d+\tfrac{1}{2}c\,,\qquad b-a+\tfrac{1}{2}d=c-\tfrac{1}{2}d\,.$$

11. Ex his autem quatuor casibus eum eligi convenit, qui cum exemplo congruat. At si formulas hactenus inventas cum exemplo conferamus, reperiemus $a=2$, $b=1$, $c=2$, $d=3$, unde fit $x=5$, $y=2$, ita ut sit

$$xx+yy=29\,,\quad aa+bb=5\,,\quad cc+dd=13\,,$$

hincque omnes reliqui valores cum exemplo prorsus convenient. Cum igitur sit $a+b+\frac{1}{2}c=4$ et $b-a+\frac{1}{2}d=\frac{1}{2}$, eligatur ea combinatio, quae eosdem praebeat valores, at facile patebit quartam adhiberi debere. Habebimus ergo $a+b=d$, $b-a=c-d$, hincque litterae c et d ita per a et b definiuntur, ut sit $c=2b$ et $d=a+b$, ex quibus iam porro fit $x=a+3b$, $y=2b$. His igitur valoribus constitutis singuli factores utriusque formulae

$$pq(p+q)(p-q)(pp+qq) \quad \text{et} \quad rs(r+s)(r-s)(rr+ss)$$

sequenti modo expressi reperiuntur:

$$\begin{aligned}
p &= aa + 3ab + 2bb = (a+b)(a+2b)\\
q &= 3bb - ab \qquad\quad = b(3b-a)\\
p+q &= aa + 2ab + 5bb\\
p-q &= aa + 4ab - bb\\
pp+qq &= (aa+bb)(xx+yy)
\end{aligned}$$

$$\begin{aligned}
r &= 4ab + 8bb = 4b(a+2b)\\
s &= aa + 4ab - bb\\
r+s &= aa + 8ab + 7bb = (a+b)(a+7b)\\
r-s &= 9bb - aa \qquad\quad = (3b+a)(3b-a)\\
rr+ss &= (aa+2ab+5bb)(xx+yy)\,.
\end{aligned}$$

12. Coniungamus iam singulos factores utriusque formulae, ac reperiemus:

$$\begin{gathered}
pq(p^4 - q^4)\\
= (a+b)(a+2b)b(3b-a)(aa+2ab+5bb)(aa+4ab-bb)(aa+bb)(xx+yy),
\end{gathered}$$

$$\begin{gathered}
rs(r^4 - s^4)\\
= 4b(a+2b)(aa+4ab-bb)(a+b)(a+7b)(3b+a)(3b-a)\\
(aa+2ab+5bb)(xx+yy)\,.
\end{gathered}$$

Quodsi ergo priorem per posteriorem dividamus, erit

$$\frac{pq(p^4-q^4)}{rs(r^4-s^4)} = \frac{aa+bb}{4(a+7b)(a+3b)}.$$

Quamobrem, ut haec fractio quadrato aequetur, eiusmodi valores pro litteris a et b requiruntur, ut ista fractio $\frac{aa+bb}{(a+7b)(3b+a)}$ fiat quadratum vel etiam eius inversa $\frac{(a+3b)(a+7b)}{aa+bb}$, quod quidem pro nostro exemplo utique evenit sumendo $a = 2$ et $b = 1$, tum enim huius posterioris fractionis valor erit 9. Totum ergo negotium huc redit, ut ista fractio ad quadratum reducatur.

13. Ponamus hic $\frac{a}{b} = t$, ut formula quadrato aequanda sit $\frac{(t+3)\ (t+7)}{tt+1}$, atque methodum prorsus singularem hic sum traditurus ex quovis valore cognito innumeros alios inveniendi. Hunc in finem plures casus, qui quasi se sponte offerunt, notasse iuvabit, qui sunt $t = 2$, $t = 1$, $t = -2$, $t = \infty$, $t = -3$, $t = -7$. Quemadmodum igitur ex his valoribus cognitis alii novi elicere queant, hic ostendamus. Ante omnia autem productum ex numeratore in denominatorem est considerandum, quod est:

$$t^4 + 10t^3 + 22tt + 10t + 21\,,$$

quod ergo ad quadratum reduci oportet.

14. Quoniam hic tantum primus terminus est quadratum, eius radicem ita fingamus, ut etiam secundus terminus tollatur; quare haec formula aequalis statuatur huic quadrato:

$$(tt + 5t + v)^2\,,$$

hincque orietur sequens aequatio:

$$22tt + 10t + 21 = (2v + 25)tt + 10tv + vv\,,$$

quae reducitur ad hanc:

$$-3tt + 10t + 21 = 2vtt + 10tv + vv\,,$$

haecque aequatio duas continet litteras t et v, quarum utraque ad duas dimensiones assurgit, ideoque, dum altera ut cognita spectatur, altera geminos valores recipiet, qui si indicentur per t et t', nec non per v et v', ex natura aequationum constat fore:

$$t + t' = \frac{10(1-v)}{2v+3}\,,\ \text{tum vero}\ v + v' = -2t(t+5)\,,$$

quarum formularum ope, simulac constent valores pro t et v, inde novi pro iisdem litteris eruentur atque ex his simili modo denuo novi ita, ut tales operationes sine fine continuari queant.

15. Cum igitur pro t iam cogniti sint aliquot valores, videamus, quales valores ipsius v illis respondeant, quae determinatio ex ultima aequatione peti potest. Ita cum sit $t = 2$, haec aequatio evadet $vv + 28v = 29$, unde oriuntur hi duo valores $v = 1$ et $v = -29$.

Pro secundo valore $t = 1$ oritur $v = 2$ et $v = -14$.

Pro tertio valore $t = -2$ prodit $v = 1$ et $v = 11$.

Pro quarto $t = \infty$ ambo termini quadratum tt continentes se debent destruere, sicque erit $2v = -3$ sive $v = -\frac{3}{2}$, tum vero huic valori $v = -\frac{3}{2}$ respondet valor $t = -\frac{3}{4}$. Pro quinto valore $t = -3$ nanciscimur valorem $v = 6$. Denique casus $t = -7$ praebet $v = -14$.

16. Quodsi iam bini huiusmodi valores pro litteris t et v accipiantur, ex iis novi formabuntur ope harum formularum:

$$t' = \frac{10(1-v)}{2v+3} - t\,, \quad v' = -2t(t+5) - v\,.$$

Incipiamus igitur a casu $t = 2$ et $v = 1$, atque tota operatio sequenti modo procedet:

$$t = 2\,, \quad -2\,, \quad -2\,, \quad 2\,, \quad -\frac{82}{11}\,, \quad \frac{262}{649}\,,$$

$$v = 1\,, \quad 11\,, \quad 1\,, \quad -29\,, \quad -\frac{919}{121}\,.$$

In hac operatione iam continentur casus initio cogniti, unde hos iam praetermittere poterimus.

17. Progrediamur igitur ad casum quartum, quo $v = -\frac{3}{2}$ et $t = -\frac{3}{4}$, ubi valores pro v et t inverso modo scribere debemus, quia alias t' prodiret $= \infty$. Operatio igitur ita se habebit:

$$v = -\frac{3}{2}\,, \quad \frac{63}{8}\,, \quad \frac{77}{18}\,, \quad -\frac{27537}{2\cdot 2704}\,^{1})\,,$$

$$t = -\frac{3}{4}\,, \quad -\frac{35}{12}\,, \quad \frac{25}{312}\,.$$

18. Sumamus nunc $t = -3$ et $v = 6$, similique modo operationem instituendo orientur hi valores:

$$t = -3\,, \quad -\frac{1}{3}\,, \quad -\frac{41}{3}\,, \quad \frac{267}{31}\,,$$

$$v = \quad 6\,, \quad -\frac{26}{9}\,, \quad -9\cdot 26\,.$$

1) Editio princeps: $-\frac{164\cdot 27}{11\cdot 11}$. Correxit R. F.

Possunt etiam termini initiales inverti hoc modo:

$$v = \quad 6, \quad 6, \quad -\frac{26}{9}, \quad -9\cdot 26,$$

$$t = -3, \quad -\frac{1}{3}, \quad -\frac{41}{3}.$$

Evidens autem est hinc nullos novos valores emergere, cum omnes in praecedente serie iam contineantur.

19. Evolvamus denique casum ultimum, quo $t = -7$ et $v = -14$, pro quo sequentes valores eruuntur:

$$t = -7, \quad 1, \quad -\frac{17}{7}, \quad -\frac{503}{7\cdot 47}\,^{1}),$$

$$v = -14, \quad 2, \quad \frac{514}{49}.$$

Primis autem terminis v et t inverso modo positis fit:

$$v = -14, \quad -14, \quad 2, \quad \frac{514}{49},$$

$$t = -7, \quad 1, \quad -\frac{17}{7}, \quad -\frac{503}{329}\,^{2}),$$

qui autem numeri iam in praecedente serie occurrunt. Ceterum notandum est casum secundum, quo $t = 1$ et v vel $= 2$ vel $= -14$, etiam hic reperiri, qui casus supra erat praetermissus.

20. Valores ergo idonei per has operationes pro t inventi sequenti modo se habebunt:

I. $t = 2$, II. $t = -2$, III. $t = -\frac{82}{11}$, IV. $t = \frac{262}{649}$,

V. $t = -\frac{3}{4}$, VI. $t = -\frac{35}{12}$, VII. $t = \frac{25}{312}$, VIII. $t = -3$,

IX. $t = -\frac{1}{3}$, X. $t = -\frac{41}{3}$, XI. $t = \frac{267}{31}$, XII. $t = -7$,

XIII. $t = 1$, XIV. $t = -\frac{17}{7}$, XV. $t = -\frac{503}{329}\,^{2})$.

---

1) Editio princeps: $\frac{503}{7\cdot 47}$. Correxit R. F.

2) Editio princeps: $\frac{503}{329}$. Correxit R. F.

Horum igitur valorum singuli suppeditant solutionem quaestionis propositae; quemadmodum in sequente problemate ostendemus.

Ex quolibet valore idoneo pro t invento assignare quatuor numeros p, q, r, s, ita ut productum sive quotus harum formularum $pq(p^4 - q^4)$ et $rs(r^4 - s^4)$ fiat quadratum.

SOLUTIO

21. Cum sit $[t =] \frac{a}{b}$, habebuntur quoque ambo numeri a et b in integris, ex quibus litterae p, q, r, s cum derivatis sequenti modo determinabuntur:

$p = (a + b)(a + 2b)$	$r = 4b(a + 2b)$
$q = b(3b - a)$	$s = aa + 4ab - bb$
$p + q = aa + 2ab + 5bb$	$r + s = (a + b)(a + 7b)$
$p - q = aa + 4ab - bb$	$r - s = (3b + a)(3b - a)$
$pp + qq = (aa + bb)(xx + yy)$	$rr + ss = (aa + 2ab + 5bb)(xx + yy)$
$= (aa + bb)(aa + 6ab + 13bb)$	$= (aa + 2ab + 5bb)(aa + 6ab + 13bb)$.

22. Circa has formulas observandum est, 1°) si quispiam numerorum p, q, r, s prodierit negativus, eius loco semper positivum scribi posse; 2°) si prodierit vel $q > p$ vel $s > r$, hos valores inter se semper permutari posse, ita ut littera p indicet numerum maiorem, q vero minorem, similique modo r maiorem et s minorem; 3°) si eveniat, ut numeri p et q habeant communem divisorem, eum per divisionem semper tollere licet, quod idem de litteris r et s est tenendum. 4°) Evidens quoque est tam loco binarum litterarum p et q quam r et s eorum summam et differentiam scribi posse: Si enim ponamus

$$P = p + q, \quad Q = p - q, \quad R = r + s, \quad S = r - s,$$

fiet

$$PQ(P^4 - Q^4) = 8pq(p^4 - q^4);$$

similique modo fiet

$$RS(R^4 - S^4) = 8rs(r^4 - s^4),$$

ideoque et harum novarum formularum sive quotus sive productum erit etiam quadratum. 5°) Ista transformatio insignem usum praestat, si litterae p, q, r, s fuerint impares; tum enim litterae maiusculae P, Q, R, S deprimi possunt, sicque ad minores numeros pervenietur; nam si ponamus

$$P = \frac{p+q}{2}, \quad Q = \frac{p-q}{2}, \quad R = \frac{r+s}{2}, \quad S = \frac{r-s}{2},$$

fiet

$$PQ(P^4 - Q^4) = \frac{pq(p^4 - q^4)}{8} \quad \text{et} \quad RS(R^4 - S^4) = \frac{rs(r^4 - s^4)}{8} .$$

Secundum haec ergo praecepta pro valoribus ipsius t inventis litteras p, q, r, s in sequentibus exemplis assignemus.

EXEMPLUM 1

quo $t = 2$

23. Hic ergo erit $a = 2$ et $b = 1$, hincque fiet

$$p = 3 \cdot 4, \quad q = 1, \quad r = 4 \cdot 4, \quad s = 11,$$

qui ergo cum suis derivatis ita disponantur:

$p = 4 \cdot 3$	$r = 4 \cdot 4$
$q = 1$	$s = 11$
$p + q = 13$	$r + s = 3 \cdot 9$
$p - q = 11$	$r - s = 5$
$pp + qq = 5 \cdot 29$	$rr + ss = 13 \cdot 29$.

Casus porro $t = -2$ et $t = 1$, $t = -3$, $t = -7$, $t = -\frac{1}{3}$ hic omittamus, quia solutiones incongruas praeberent.

EXEMPLUM 2

quo $t = -\frac{3}{4}$

24. Cum igitur sit $a = -3$ et $b = 4$, fiet hoc casu

$p = 1$	$r = 4 \cdot 4$
$q = 4 \cdot 3$	$s = 11$
$p + q = 13$	$r + s = 27$
$p - q = 11$	$r - s = 5$
$pp + qq = 5 \cdot 29$	$rr + ss = 13 \cdot 29$,

qui autem valores cum praecedentibus tantum in eo dissentiunt, ut p et q sint permutati; hinc ergo nulla nova solutio emergit.

EXEMPLUM 3

$$quo\ t = -\frac{17}{7}$$

25. Hic ergo sumi debet $a = -17$, $b = 7$, unde hi valores orientur per 2 et 4 scilicet depressi:

$p = 3 \cdot 5$	$r = 3 \cdot 7$
$q = 7 \cdot 19$	$s = 59$.

Iam quia omnes hi numeri sunt impares, eorum loco scribantur semi-summae et semi-differentiae sicque nova problematis solutio orietur:

$p = 2 \cdot 37$	$r = 40$
$q = 59$	$s = 19$
$p + q = 133$	$r + s = 59$
$p - q = 15$	$r - s = 21$
$pp + qq = 53 \cdot 169$	$rr + ss = 53 \cdot 37$.

Ubi omnes factores non quadrati se utrinque destruunt.

EXEMPLUM 4

$$quo\ t = -\frac{41}{3}$$

26. Sumto hic $a = -41$ et $b = 3$ valores p, q, r, s, quantum licet depressi, erunt:

$$p = 7 \cdot 19\,, \quad q = 3 \cdot 5\,, \quad r = 3 \cdot 7\,, \quad s = 59\,,$$

qui casus cum praecedente perfecte congruit.

EXEMPLUM 5

$$quo\ t = -\frac{35}{12}$$

27. Cum igitur sumi debeat $a = -35$ et $b = 12$, valores pro p, q, r, s hinc erunt:

$p = 12 \cdot 71 = 852$	$r = 599$
$q = 11 \cdot 23 = 253$	$s = 11 \cdot 48 = 528$
$p + q = 5 \cdot 221$	$r + s = 23 \cdot 49$
$p - q = 599$	$r - s = 71$
$pp + qq = 37^2 \cdot 577$	$rr + ss = 5 \cdot 13 \cdot 17 \cdot 577$,

ubi iterum omnes factores non quadrati utrinque occurrunt. Eandem porro solutionem resultare ex casu $t = -\frac{82}{11}$, inde patet, quod

$$82^2 + 11^2 = 5\,(35^2 + 12^2)\,.$$

28. Praeter casum ergo iam pridem cognitum, quo

$$p = 12\,,\quad q = 1\,,\quad r = 16\,,\quad s = 11\,,$$

qui nobis instar normae in hac investigatione inserviit, duas alias novas solutiones sumus adepti, quae numeris non nimis magnis constant. Reliqui vero quatuor casus pro t inventi:

$$\frac{25}{312}\,,\quad \frac{267}{31}\,,\quad -\frac{503}{329}\,,\quad \frac{262}{649}$$

perducerent ad numeros nimis magnos, quos operae non est pretium evolvere. Ceterum in his operationibus plura occurrunt calculi artificia vix adhuc cognita, quibus Analysis non exigua incrementa accipere est censenda.

29. Hinc iam problema in *Tomo XV novorum Commentariorum* tractatum multo commodius et concinnius resolvi ac per numeros absolutos expediri poterit, quam solutionem hic subiungo.

PROBLEMA

Invenire duos numeros, quorum productum sive auctum sive minutum tam summa quam differentia ipsorum numerorum producat numeros quadratos.

---

1) Editio princeps: $\frac{503}{329}$. Correxit R. F.

SOLUTIO

30. Positis numeris quaesitis $\frac{x}{z}$ et $\frac{y}{z}$ supra iam vidimus esse $x = \frac{ab + cd}{z}$ et $y = \frac{ab - cd}{z}$; deinde introductis litteris p, q, r, s erat

$$ab + cd = 2rs(pp - qq) \quad \text{et} \quad ab - cd = 2pq(rr - ss)\ ^{1}).$$

Quamobrem numeri quaesiti erunt:

$$\frac{x}{z} = \frac{2rs(pp - qq)}{zz} \quad \text{et} \quad \frac{y}{z} = \frac{2pq(rr - ss)}{zz}.$$

Invenimus autem porro esse $zz = \frac{4pqrs(pp - qq)\ (rr - ss)}{(pp + qq)\ (rr + ss)}$, quo valore substituto ambo numeri quaesiti erunt:

$$\frac{x}{z} = \frac{(pp + qq)\ (rr + ss)}{2pq(rr - ss)} \quad \text{et} \quad \frac{y}{z} = \frac{(pp + qq)\ (rr + ss)}{2rs(pp - qq)}.$$

31. Quoniam igitur supra in exemplis tres solutiones in numeris absolutis dedimus, si ex iis valores pro litteris p, q, r, s depromamus, sequentes tres solutiones numericas nanciscemur.

I. SOLUTIO

ex § 23 *petita*

$$\frac{x}{z} = \frac{5 \cdot 29 \cdot 13 \cdot 29}{2 \cdot 12 \cdot 3 \cdot 9 \cdot 5} = \frac{13 \cdot 29^2}{8 \cdot 9^2},$$

$$\frac{y}{z} = \frac{5 \cdot 29 \cdot 13 \cdot 29}{13 \cdot 11 \cdot 32 \cdot 11} = \frac{5 \cdot 29^2}{32 \cdot 11^2},$$

quae est solutio a me primum inventa.

1) r et s inter se permutatae sunt. R. F.

II. SOLUTIO

ex § 25 petita

$$\frac{x}{z} = \frac{53 \cdot 169 \cdot 53 \cdot 37}{4 \cdot 37 \cdot 59 \cdot 59 \cdot 21} = \frac{13^2 \cdot 53^2}{3 \cdot 4 \cdot 7 \cdot 59^2},$$

$$\frac{y}{z} = \frac{53 \cdot 169 \cdot 53 \cdot 37}{38 \cdot 40 \cdot 133 \cdot 15} = \frac{37 \cdot 13^2 \cdot 53^2}{3 \cdot 7 \cdot 4^2 \cdot 5^2 \cdot 19^2}.$$

III. SOLUTIO

ex § 27 petita

$$\frac{x}{z} = \frac{37^2 \cdot 577 \cdot 5 \cdot 13 \cdot 17 \cdot 577}{24 \cdot 71 \cdot 11 \cdot 23 \cdot 23 \cdot 49 \cdot 71} = \frac{5 \cdot 13 \cdot 17 \cdot 37^2 \cdot 577^2}{11 \cdot 24 \cdot 7^2 \cdot 23^2 \cdot 71^2},$$

$$\frac{y}{z} = \frac{37^2 \cdot 577 \cdot 5 \cdot 13 \cdot 17 \cdot 577}{2 \cdot 528 \cdot 599 \cdot 5 \cdot 221 \cdot 599} = \frac{37^2 \cdot 577^2}{2 \cdot 528 \cdot 599^2}.$$ [1]

32. Subiungam hic curiositatis gratia adhuc solutionem maximis numeris contentam, quam suppeditat casus supra inventus paragraphi 20, scilicet $t = \frac{25}{312}$, unde fit $a = 25$ et $b = 312$. Hinc autem deducuntur sequentes valores:

$p = 3 \cdot 8 \cdot 13 \cdot 911$	$r = 3 \cdot 11 \cdot 13 \cdot 32 \cdot 59$
$q = 11 \cdot 59 \cdot 337$	$s = 65519$
$p + q = 5 \cdot 17 \cdot 61 \cdot 97$	$r + s = 31^2 \cdot 911$
$p - q = 65519$	$r - s = 337 \cdot 47^2$
$pp + qq = 313^2 \cdot 1312897$	$rr + ss = 5 \cdot 17 \cdot 61 \cdot 97 \cdot 1312897$,

ex quibus numeri quaesiti erunt:

$$\frac{x}{z} = \frac{5 \cdot 17 \cdot 61 \cdot 97 \cdot 313^2 \cdot 1312897^2}{3 \cdot 11 \cdot 13 \cdot 59 \cdot 4^2 \cdot 31^2 \cdot 47^2 \cdot 337^2 \cdot 911^2},$$

$$\frac{y}{z} = \frac{313^2 \cdot 1312897^2}{3 \cdot 11 \cdot 13 \cdot 8^2 \cdot 59 \cdot 65519^2}.$$

1) Editio princeps: $\frac{y}{z} = \frac{37^2 \cdot 577 \cdot 5 \cdot 13 \cdot 17 \cdot 577}{2 \cdot 528 \cdot 599 \cdot 5 \cdot 21 \cdot 599} = \frac{13 \cdot 17 \cdot 37^2 \cdot 577^2}{6 \cdot 7 \cdot 528 \cdot 599}$. Correxit A. M.

DE BINIS NUMERIS QUORUM SUMMA SIVE AUCTA SIVE MINUTA TAM UNIUS QUAM ALTERIUS QUADRATO PRODUCAT QUADRATA

Commentatio 775 indicis ENESTROEMIANI
Mémoires de l'académie des sciences de St-Pétersbourg 11, 1830, p. 46—48
Conventui exhibita die 14. augusti 1780

1. Quodsi bini numeri quaesiti ponantur $\frac{x}{z}$ et $\frac{y}{z}$, has duas formulas ambiguas: $\frac{x+y}{z} \pm \frac{xx}{zz}$ et $\frac{x+y}{z} \pm \frac{yy}{zz}$ quadrata effici oportet. Hinc ergo per zz multiplicando hae duae formulae: $(x+y)z \pm xx$ atque $(x+y)z \pm yy$ quadratis aequari debeunt. His autem conditionibus satisfaciunt hi numeri, qui sine dubio sunt minimi:

$$x = 9028 = 4 \cdot 37 \cdot 61, \quad y = 3124 = 4 \cdot 11 \cdot 71 \quad \text{et} \quad z = \frac{5 \cdot 37^2 \cdot 61^2}{2 \cdot 49 \cdot 31}.$$

Tum enim erit

$$(x+y)z = 20 \cdot 37^2 \cdot 61^2 \quad \text{et} \quad xx = 16 \cdot 37^2 \cdot 61^2,$$

quorum numerorum summa est $6^2 \cdot 37^2 \cdot 61^2$ et differentia $2^2 \cdot 37^2 \cdot 61^2$; tum vero est $yy = 16 \cdot 11^2 \cdot 71^2$, unde per 4 dividendo ostendendum est tam summam quam differentiam horum numerorum:

$$5 \cdot 37^2 \cdot 61^2 \quad \text{et} \quad 4 \cdot 11^2 \cdot 71^2$$

esse quadrata [4799^2 et 5283^2]. Cum autem sit $5 = 2^2 + 1^2$, $37^2 = 35^2 + 12^2$ et $61^2 = 60^2 + 11^2$, erit $5 \cdot 37^2 = 82^2 + 11^2$, hincque porro

$$5 \cdot 37^2 \cdot 61^2 = 5041^2 + 242^2,$$

cui summae quadratorum sive addatur sive subtrahatur duplum radicum productum, quod est

$$2 \cdot 242 \cdot 5041 = 4 \cdot 11^2 \cdot 71^2 ,$$

qui est ipse numerus sive addendus sive subtrahendus.

ANALYSIS AD HANC SOLUTIONEM DUCENS

2. Numerus $(x + y)z$ duplici modo statuatur summa duorum quadratorum, scilicet $= A^2 + B^2$ et $= C^2 + D^2$, atque manifestum est quaesito satisfieri, si fuerit $xx = 2AB$ et $yy = 2CD$. Hunc in finem fiat

$$(x + y)z = (aa + bb)(cc + dd) ,$$

unde deducitur $A = ac + bd$ et $B = ad - bc$; tum vero $C = ad + bc$ et $D = ac - bd$, sicque habebimus

$$xx = 2(ac + bd)(ad - bc) \quad \text{et} \quad yy = 2(ad + bc)(ac - bd).$$

Ut iam hae formulae evadant quadrata, ponatur $x = (ac + bd)f$ et $y = (ad + bc)g$, factaque evolutione prodibunt hae aequationes:

$$2(ad - bc) = (ac + bd)ff \quad \text{et} \quad 2(ac - bd) = (ad + bc)gg ,$$

ex quarum priore deducitur

$$\frac{a}{b} = \frac{2c + dff}{2d - cff} ,$$

ex posteriore vero

$$\frac{a}{b} = \frac{2d + cgg}{2c - dgg} .$$

Hi autem valores inter se coaequati praebent hanc aequationem:

$$cc(4 + ffgg) + 4cd(ff - gg) = dd(4 + ffgg) ,$$

unde radice extracta reperitur:

$$\frac{d}{c} = \frac{2(ff-gg) \pm \sqrt{4(ff-gg)^2 + (4+ffgg)^2}}{4+ffgg},$$

sive

$$\frac{d}{c} = \frac{2(ff-gg) \pm \sqrt{(4+f^4)\,(4+g^4)}}{4+ffgg}.$$

3. Totum ergo negotium huc redit, ut hoc productum $(4+f^4)(4+g^4)$ quadratum reddatur, et, quia duas quantitates f et g continet, alterutram pro lubitu accipere licebit. Sumamus ergo $g = 1$ fietque

$$\frac{d}{c} = \frac{2(ff-1) \pm \sqrt{5(4+f^4)}}{4+ff};$$

tum vero regrediendo erit

$$\frac{a}{b} = \frac{2d+c}{2c-d},$$

porroque $[x =]\ (ac+bd)f$ et $y = ad+bc$. Denique autem habebimus

$$z = \frac{(aa+bb)\,(cc+dd)}{x+y}.$$

4. Ponatur nunc $\sqrt{5(4+f^4)} = 5v$, ut sit

$$\frac{d}{c} = \frac{2(ff-1) \pm 5v}{4+ff}.$$

Erit ergo $25vv = 20 + 5f^4$, quae ergo formula casu $f = 1$ commode fit quadratum, hoc vero modo ad solutionem incongruam perveniretur. Ut igitur alii valores pro f eruantur, ponamus:

$$f = 1+t,$$

fietque

$$25vv = 25 + 20t + 30tt + 20t^3 + 5t^4,$$

cuius radix statuatur $5 + \alpha t + \beta tt$, et erit

$$20 + 30t + 20tt + 5t^3 = 10\alpha + (10\beta + \alpha\alpha)t + 2\alpha\beta tt + \beta\beta t^3.$$

Ut nunc bina membra priora se destruant, fieri debet $\alpha = 2$, atque, ut etiam secunda se destruant, sumi oportet $\beta = \frac{13}{5}$, sicque habebimus

$$5v = 5 + 2t + \tfrac{13}{5}tt$$

et nunc tandem remanent membra tertium et quartum, quae denuo per tt divisa praebent $t = \frac{60}{11}$. Ex quo valore invento colligitur $5v = \frac{11285}{121}$; tum vero est $f = \frac{71}{11}$, ex quibus valoribus colligitur

$$\frac{d}{c} = \frac{2(71^2 - 11^2) \pm 11285}{4 \cdot 11^2 + 71^2},$$

unde sumto signo superiore oritur

$$\frac{d}{c} = \frac{21125}{5525} = \frac{845}{221} = \frac{5 \cdot 169}{13 \cdot 17}.$$

Sumamus igitur $d = 5 \cdot 169$ et $c = 13 \cdot 17$, eritque $\frac{a}{b} = -\frac{147}{31}$. Sumto ergo $a = 147$ et $b = -31$ fiet $x = 4 \cdot 11 \cdot 13 \cdot 71$ et $y = 4 \cdot 13 \cdot 37 \cdot 61$. Hinc ergo colligitur $x + y = 4 \cdot 13 \cdot 2 \cdot 7^2 \cdot 31$ ideoque $z = \frac{5 \cdot 13 \cdot 37^2 \cdot 61^2}{2 \cdot 49 \cdot 31}$ ob $aa + bb = 10 \cdot 37 \cdot 61$ et $cc + dd = 13^2 \cdot 2 \cdot 37 \cdot 61$. Cum igitur hi tres numeri x, y, z habeant factorem communem 13, eo per divisionem sublato, valores harum litterarum ita fient simpliciores:

$$x = 4 \cdot 11 \cdot 71, \quad y = 4 \cdot 37 \cdot 61, \quad z = \frac{5 \cdot 37^2 \cdot 61^2}{2 \cdot 49 \cdot 31},$$

unde ipsi numeri quaesiti iam erunt:

$$\frac{x}{z} = \frac{8 \cdot 11 \cdot 31 \cdot 49 \cdot 71}{5 \cdot 37^2 \cdot 61^2} \quad \text{et} \quad \frac{y}{z} = \frac{8 \cdot 31 \cdot 49}{5 \cdot 37 \cdot 61},$$

qui sunt ipsi numeri initio allati. Quemadmodum autem hi numeri ex hypothesi $g = 1$ sunt deducti, simili modo ex alio quovis valore pro g assumto solutiones investigari poterunt. Quae autem mox ad immensos numeros excrescent. Ceterum notandum est sumto $g = 2$ eandem solutionem prodituram fuisse, cum $g^4 + 4 = 4 \cdot 5$, ubi quaternarius per operationes sequentes iterum ex calculo excedit.

DILUCIDATIONES CIRCA BINAS SUMMAS DUORUM BIQUADRATORUM INTER SE AEQUALES

Commentatio 776 indicis ENESTROEMIANI
Mémoires de l'académie des sciences de St-Pétersbourg **11**, 1830, p. 49—57
Conventui exhibita die 28. augusti 1780

1. In *Tomo Novorum Commentariorum* XVII, pag. 64[1]), ostendi exhiberi posse duas binorum biquadratorum sive summas sive differentias, quae sint inter se aequales, quod quidem initio non parum paradoxon videbatur. Cum enim tales formulae $A^2 \pm B^2 = 0$, $A^3 \pm B^3 \pm C^3 = 0$ demonstratae sint impossibiles, siquidem termini vel aequales vel evanescentes excludantur, videri poterat etiam hanc formulam:

$$A^4 \pm B^4 \pm C^4 \pm D^4 = 0\,,$$

atque adeo etiam pro superioribus potestatibus

$$A^5 \pm B^5 \pm C^5 \pm D^5 \pm E^5 = 0 \quad \text{et} \quad A^6 \pm B^6 \pm C^6 \pm D^6 \pm E^6 \pm F^6 = 0 \quad \text{etc.}$$

esse impossibiles. Nunc autem certi sumus pro biquadratis hanc aequalitatem $A^4 + B^4 - C^4 - D^4 = 0$ subsistere posse ideoque coniecturam illam neutiquam valere, cum loco citato huiusmodi quatuor biquadrata pluribus modis dari posse ostenderim. Numeri autem, quos ibi inveni, tam sunt praegrandes, ut veritas difficulter explorari potest; cum minimi numeri, quos invenire potui, ut fiat

1) Commentatio 428 indicis ENESTROEMIANI: „*Observationes circa bina biquadrata, quorum summam in duo alia biquadrata resolvere liceat*", nov. comment. acad. sc. Petrop. **17** (1772), 1773, p. 64. *LEONHARDI EULERI Opera omnia*, series I, vol. 3, p. 211. Confer etiam Commentationem 716 indicis ENESTROEMIANI, series I, vol. 4, p. 329. R. F.

$$A^4 + B^4 = C^4 + D^4,$$

erant

$$A = 477069, \quad B = 8497, \quad C = 310319, \quad D = 428397\,[1]).$$

2. Nuper autem, longe alia agens, casu fortuito incidi in tales numeros longe minores, qui sunt

$$A = 542, \quad B = 514, \quad C = 359, \quad D = 103\,[2]),$$

qui quomodo satisfaciant huic aequationi $A^4 - B^4 = C^4 - D^4$, hoc modo exploratur. Cum sit

$A + B = 1056 = 32 \cdot 3 \cdot 11$	$C + D = 462 = 2 \cdot 3 \cdot 7 \cdot 11$
$A - B = 28 = 4 \cdot 7$	$C - D = 256 = 2^8$
$AA - BB = 2^7 \cdot 3 \cdot 7 \cdot 11$	$CC - DD = 2^9 \cdot 3 \cdot 7 \cdot 11$

erit

$$AA - BB : CC - DD = 1 : 4,$$

quocirca summae quadratorum reciprocam tenere debent rationem, ita ut sit

$$A^2 + B^2 : C^2 + D^2 = 4 : 1,$$

quod revera evenire ita commodissime ostenditur. Cum sit

$$AA + BB = 4CC + 4DD,$$

erit

$$AA - 4DD = 4CC - BB$$

sive

$$(A + 2D)(A - 2D) = (2C + B)(2C - B).$$

Est autem

$$A + 2D = 748 = 4 \cdot 11 \cdot 17, \quad A - 2D = 2^4 \cdot 3 \cdot 7,$$
$$2C + B = 1232 = 2^4 \cdot 7 \cdot 11, \quad 2C - B = 2^2 \cdot 3 \cdot 17,$$

ideoque

$$AA - 4DD = 2^6 \cdot 3 \cdot 7 \cdot 11 \cdot 17 \quad \text{et} \quad 4CC - BB = 2^6 \cdot 3 \cdot 7 \cdot 11 \cdot 17,$$

ergo $AA - 4DD = 4CC - BB$.

---

1) Confer notam 2) p. 217, series I, vol. 3, ubi hos numeros problemati propposito satisfacere non posse demonstratur. R. F.

2) In Commentatione 716 numeri multo minores inveniuntur, qui satisfaciunt aequationi $A^4 - B^4 = C^4 - D^4$. Confer p. 341 et 342 vol. 4 seriei I. R. F.

3. Hic autem fateri cogor me nulla certa methodo ad hos numeros esse deductum neque adhuc perspicio, quomodo per viam directam ad eos perveniri queat. Quamobrem operae pretium fore arbitror totam Analysin, qua sum usus, hic explicare. Cum inde haud contemnenda incrementa in Analysin redundandura videantur, sequente igitur modo calculum institui.

4. Cum esse debeat

$$(aa + bb)(aa - bb) = (cc + dd)(cc - dd),$$

hinc formo has duas aequationes:

$$(aa + bb)p = (cc - dd)q \quad \text{et} \quad (aa - bb)q = (cc + dd)p\ ^{1});$$

quarum priore ducta in p, posteriore vero in q, earum summa praebet

$$2pqcc = aa(pp + qq) + bb(pp - qq),$$

at differentia praebet

$$2pqdd = aa(qq - pp) - bb(qq + pp),$$

unde patet esse debere $q > p$ ideoque harum aequationum utraque resolutionem admittit, si fuerit $qq - pp$ quadratum; quamobrem ponamus statim $qq - pp = ss$, ac prior aequatio hoc modo referatur:

$$bbss = aa(pp + qq) - 2ccpq,$$

quae, ut ad quadratum reduci queat, hac forma repraesentetur:

$$bbss = aa(q - p)^2 + 2pq(aa - cc).$$

Hinc iam statuamus

$$bs = a(q - p) + 2p(a - c)x.$$

Hinc igitur ob binos terminos primos se destruentes, si reliqui per $2p(a - c)$ dividantur, prodibit haec aequatio:

1) Editio princeps: $(aa + bb)p = (cc + dd)q$ et $(aa - bb)q = (cc - dd)p$. Correxit A. M.

$$2p(a-c)xx + 2a(q-p)x = q(a+c),$$

unde deducitur

$$\frac{a}{c} = \frac{2pxx+q}{2pxx+2(q-p)x-q};$$

quocirca statuamus

$$a = 2pxx + q \quad \text{et} \quad c = 2pxx + 2(q-p)x - q,$$

unde deducitur

$$bs = q(q-p) + 4pqx - 2p(q-p)xx.$$

5. Aggrediamur iam alteram aequationem, quam, ut fractiones evitemus, ita referamus

$$2ddpqss = aas^4 - bbss(pp+qq),$$

ubi, si loco a et sb valores modo inventos substituamus, ob $ss = qq - pp$ omnes termini per $2pq$ divisibiles prodibunt, orieturque sequens aequatio:

$$\begin{aligned} ddss = {} & qq(q-p)^2 - 4q(q-p)(qq+pp)x + 2(qq-pp)^2xx \\ & + 2(qq-6pq+pp)(pp+qq)xx + 8p(q-p)(pp+qq)x^3 \\ & + 4p^2(q-p)^2x^4, \end{aligned}$$

in qua formula tam primus quam ultimus terminus sunt quadrata, eamque idcirco secundum praecepta cognita pluribus modis tractare licebit.

6. Quoniam autem huius formulae evolutio in genere non parum esset taediosa, casum tantum simplicissimum evolvamus, quo $qq - pp$ fit quadratum, quod evenit sumendo $p = 3$ et $q = 5$, unde fit $ss = 16$ et $s = 4$. Hoc igitur casu valores supra inventi evadent $a = 6xx + 5$, $c = 6xx + 4x - 5$ et $4b = 10 + 60x - 12xx$ sive $2b = 5 + 30x - 6xx$. Nunc vero formula pro quarta littera d invenienda erit:

$$16dd = 100 - 1360x - 3296xx + 1632x^3 + 144x^4$$

seu

$$4dd = 25 - 340x - 824xx + 408x^3 + 36x^4,$$

atque denuo per 4 dividendo prodibit:

$$dd = \frac{25}{4} - 85x - 206xx + 102x^3 + 9x^4.$$

7. Ponamus hic primo secundum praecepta solita

$$d = \frac{5}{2} - 17x \pm 3xx,$$

eritque

$$dd = \frac{25}{4} - 85x + (289 \pm 15)xx \mp 102x^3 + 9x^4,$$

ubi termini primus, secundus et ultimus tolluntur simul vero penultimus, si signum inferius valeret, indeque nihil concludi posset; quamobrem valeat signum superius, ut sit $d = \frac{5}{2} - 17x + 3xx$, atque hinc orietur ista aequatio:

$$304xx - 102x^3 = -206xx + 102x^3,$$

unde fit $x = \frac{510}{204} = \frac{5}{2}$. Hinc ergo valores nostri erunt:

$$a = \frac{85}{2}, \quad c = \frac{85}{2}, \quad b = \frac{85}{4}, \quad d = -\frac{85}{4}.$$

Hinc ergo foret $c^4 = a^4$ et $d^4 = b^4$, quae solutio iam per se est obvia.

8. Statuamus $d = 3xx + 17x \pm \frac{5}{2}$, eritque

$$dd = 9x^4 + 102x^3 + (289 \pm 15)xx \pm 85x + \frac{25}{4},$$

ubi statim patet signum superius valere debere, unde prodit aequatio haec: $304xx + 85x = -85x - 206xx$, unde fit $x = -\frac{17}{51} = -\frac{1}{3}$. Hinc porro colligitur $a = \frac{17}{3}$, $c = -\frac{17}{3}$. Ergo iterum foret $c^4 = a^4$ ideoque necessario etiam $d^4 = b^4$; unde nihil sequeretur.

9. Statuamus $d = \frac{5}{2} - 17x + \alpha xx$, eritque

$$dd = \frac{25}{4} - 85x + (5\alpha + 289)xx - 34\alpha x^3 + \alpha\alpha x^4,$$

ubi α ita sumi oportet, ut priores tres termini tollantur, ideoque $\alpha = -99$, et reliqua aequatio per x^3 divisa erit

$$9801x + 3366 = 102 + 9x,$$

unde fit $x = -\frac{3264}{9792} = -\frac{1}{3}$, ut in casu praecedente, unde iam novimus hinc nihil ad scopum nostrum sequi.

10. Statuamus denique $d = 3xx + 17x + \alpha$, ubi α ita definiatur, ut terminus medius destruatur. Cum igitur sit

$$dd = 9x^4 + 102x^3 + (289 + 6\alpha)xx + 34\alpha x + \alpha\alpha,$$

fieri debet $289 + 6\alpha = -206$ ideoque $\alpha = -\frac{165}{2}$, tum vero reliqua aequatio erit

$$-17 \cdot 165\, x + \frac{165^2}{4} = -85\, x + \frac{25}{4},$$

unde fit $x = \frac{5}{2}$, uti in casu primo, sicque iterum isto casu omni successu caret.

11. Cum igitur hactenus nihil ad scopum nostrum simus assecuti, secundum praecepta vulgaria oporteret formulam biquadraticam inventam ita transformare, ut ponatur vel $x = \frac{5}{2} + y$ vel $x = -\frac{1}{3} + y$, hocque modo perveniremus ad alias formas biquadraticas eiusdem indolis, quae secundum casus praecedentes tractatae utique largirentur valores idoneos pro y, verum inde pro litteris a, b, c, d numeri vehementer magni essent prodituri neque ulla solutio simplicior illa, quam olim dederam, sperari posset, multo minus hinc solutio simplex nuper inventa inde exspectari posset.

12. In his operationibus loco dd tale quadratum assumitur, quo subtracto aequatio simplex relinquatur valorem ipsius x praebens, unde intelligitur pro dd etiam tale quadratum assumi posse, quo subtracto aequatio quadratica relinquatur, dummodo ea radices habeat rationales, id quod in hac aequatione generali usu venire observavi:

$$\alpha\alpha + 2\alpha\beta x + \gamma xx + 2\delta\varepsilon x^3 + \varepsilon\varepsilon x^4 = zz,$$

quoties fuerit $\beta\beta + \delta\delta - \gamma$ quadratum, sive quoties fuerit $\gamma = \beta\beta + \delta\delta - \zeta\zeta$, quod ergo accuratius prosequamur.

13. Sumamus pro zz hoc quadratum: $(\alpha + \beta x)^2$, quo ab illa forma subtracto remanebit haec quantitas:

$$xx(\gamma - \beta\beta + 2\delta\varepsilon x + \varepsilon\varepsilon xx) ,$$

quae ob $\gamma - \beta\beta = \delta\delta - \zeta\zeta$ transit in hanc formam

$$xx\big((\delta + \varepsilon x)^2 - \zeta\zeta\big) ,$$

ita ut sit

$$zz = (\alpha + \beta x)^2 + xx(\varepsilon x + \delta + \zeta)(\varepsilon x + \delta - \zeta) ,$$

unde patet duplici modo fieri $z = \alpha + \beta x$, scilicet, si fuerit vel $x = -\frac{\delta - \zeta}{\varepsilon}$ vel $x = -\frac{\delta + \zeta}{\varepsilon}$, sicque hoc modo duos valores pro x adipiscimur, qui per vulgarem operationem non reperientur. Idem commodum eveniet, si pro zz sumamus hoc quadratum $(\varepsilon x + \delta)^2 xx$. Hoc enim sublato remanet:

$$\alpha\alpha + 2\alpha\beta x + (\gamma - \delta\delta)xx ,$$

hoc est $(\alpha + \beta x)^2 - \zeta\zeta xx$, ita ut sit in genere

$$xx(\varepsilon x + \delta)^2 + \big((\beta - \zeta)x + \alpha\big)\big((\beta + \zeta)x + \alpha\big) ;$$

unde patet revera fieri $z = x(\varepsilon x + \delta)$, quoties fuerit vel

$$x = -\frac{\alpha}{\beta - \zeta} \quad \text{vel} \quad x = -\frac{\alpha}{\beta + \zeta} ,$$

ita ut hoc casu omnino quatuor novi valores pro x reperiri queant.

14. Videamus igitur, utrum nostra aequatio:

$$\frac{25}{4} - 85x - 206xx + 102x^3 + 9x^4 = dd ,$$

in illa forma generali contineatur necne. Comparatione autem instituta fiet $\alpha = \frac{5}{2}$, $\beta = -17$, $\gamma = -206$, $\delta = 17$, $\varepsilon = 3$. Erit ergo $\beta\beta + \delta\delta - \gamma = 28^2$, ideoque $\zeta = 28$, quocirca quatuor novi valores pro x resultantes erunt:

$$x = -15 , \quad x = \frac{11}{3} , \quad x = \frac{1}{18} , \quad x = -\frac{5}{22}^{1}) .$$

1) Editio princeps: $+\frac{5}{22}$. Correxit A. M.

Hic autem probe notandum est hunc egregium consensum exemplo tantum deberi, quo posuimus $p = 3$ et $q = 5$. Sin autem his litteris p et q alios tribuamus valores, ita tamen, ut $qq - pp$ evadat quadratum, rarissime iste consensus locum habebit.

15. Evolvamus igitur nunc hos valores ope huius methodi prorsus singularis inventos. Sit primo $x = -15$, quo casu fit $d = \alpha + \beta x = \frac{515}{2}$; reliquae vero litterae reperientur $a = 1355$, $b = \frac{1795}{2}$[1]), $c = 1285$, qui numeri, cum sint omnes per 5 divisibiles, ad minimos terminos revocabuntur in integris multiplicando per $\frac{2}{5}$, tum igitur quatuor nostri numeri quaesiti erunt:

$$a = 542\,, \quad b = 359\,, \quad c = 514\,, \quad d = 103\,,$$

qui sunt illi ipsi, quos initio exhibueram.

16. Secundus valor pro x inventus erat $x = \frac{11}{3}$, ubi fit

$$d = \alpha + \beta x = -\frac{359}{6}\,.$$

Reliqui porro valores erunt:

$$a = \frac{257}{3}\,, \quad b = \frac{103}{6}\,, \quad c = \frac{271}{3}\,,$$

qui per 6 multiplicati ad hos numeros revocantur:

$$a = 514\,, \quad b = 103\,, \quad c = 542\,, \quad d = 359\,,$$

qui cum praecedentibus conveniunt.

17. Consideremus nunc tertium valorem $x = \frac{1}{18}$, pro quo erit

$$d = x(\varepsilon x + \delta) = \frac{103}{108}\,;$$

1) EULERUS signum numeri b omittit. R. F.

tum vero reliquae litterae hos nanciscentur valores:

$$a = \frac{271}{54}\ ^{1}) , \quad b = \frac{359}{108} , \quad c = \frac{257}{54} ,$$

multiplicando erit in numeris integris:

$$a = 542 , \quad b = 359 , \quad c = 514 , \quad d = 103 .$$

18. Sit denique $x = -\frac{5}{22}$ eritque $d = \frac{1795}{22^2}$, tum vero

$$a = \frac{2570}{22^2} , \quad b = \frac{515}{22^2} , \quad c = \frac{2710}{22^2} ,$$

sive per 5 dividendo et per 22^2 multiplicando fiet in numeris integris:

$$a = 514 , \quad b = 103 , \quad c = 542 , \quad d = 359 .$$

19. Praeterea vero formula nostra pro dd inventa etiam hac insigni gaudet proprietate, quod, si extremi tantum termini tollantur, pars reliqua exhibeat aequationem quadraticam resolubilem. Posito enim loco dd hoc quadrato $(\frac{5}{2} + 3xx)^2$ hoc sublato remanebit ista aequatio:

$$102xx - 221x - 85 = 0 ,$$

quae per 17 divisa fit $6xx - 13x - 5 = 0$, unde fit $x = \frac{5}{2}$ et $x = -\frac{1}{3}$, qui sunt iidem valores, quos supra operatio prima et secunda praebuerat.

ALIA ANALYSIS AD EANDEM SOLUTIONEM DUCENS

20. Ut fiat $a^4 - b^4 = c^4 - d^4$, ponatur

$$a = m(f + g) , \quad b = m(f - g) , \quad c = n(h + k) , \quad d = n(h - k) .$$

Tum enim erit $m^4 fg(ff + gg) = n^4 hk(hh + kk)$, et nunc statim ponatur $ff + gg = hh + kk$, ut fiat $m^4 fg = n^4 hk$ sive $\frac{n^4}{m^4} = \frac{fg}{hk}$, ita ut haec fractio $\frac{fg}{hk}$ reddi debeat biquadratum.

1) Editio princeps: $\frac{171}{54}$. Correxit A. M.

21. Statuamus nunc

$$ff + gg = hh + kk = (\alpha\alpha + \beta\beta)(\gamma\gamma + \delta\delta),$$

unde litterae ita determinari poterunt:

$$f = \alpha\gamma + \beta\delta, \quad g = \alpha\delta - \beta\gamma, \quad h = \alpha\delta + \beta\gamma, \quad k = \alpha\gamma - \beta\delta,$$

quamobrem esse debebit $\frac{n^4}{m^4} = \frac{(\alpha\gamma + \beta\delta)(\alpha\delta - \beta\gamma)}{(\alpha\delta + \beta\gamma)(\alpha\gamma - \beta\delta)}$. Ut haec formula ad pauciores litteras reducatur, ponamus $\alpha = \beta x$ et $\gamma = \delta y$, fietque

$$\frac{n^4}{m^4} = \frac{(xy + 1)(x - y)}{(xy - 1)(x + y)}.$$

22. Ista quidem formula solutu est difficillima, si modo ad quadratum reduci deberet, unde vix ulla spes affulget, quemadmodum ea adeo ad biquadratum reduci liceat. Interim tamen forte fortuna incidi in modum omnes difficultates superandi, qui in hoc consistit, ut ponam $y = \frac{x}{xx - 2}$; tum enim erit:

$$xy + 1 = \frac{2(xx - 1)}{xx - 2}, \quad x - y = \frac{x(xx - 3)}{xx - 2},$$

$$xy - 1 = \frac{2}{xx - 2}, \quad x + y = \frac{x(xx - 1)}{xx - 2},$$

quocirca nostra aequatio erit $\frac{n^4}{m^4} = xx - 3$, quae iam facillime ad quadratum perducitur ponendo

$$x = \frac{pp + 3qq}{2pq},$$

tum erit

$$xx - 3 = (pp - 3qq)^2,$$

quocirca extracta radice erit

$$\frac{nn}{mm} = \frac{pp - 3qq}{2pq},$$

quae ergo formula denuo quadratum reddi debet; quadratum ergo fieri debet

$$2pq(pp - 3qq),$$

ubi statim casus simplicissimus in oculos incurrit sumendo $p = 2$ et $q = 1$; tum enim fiet $\frac{n}{m} = \frac{1}{2}$, ideoque $n = 1$ et $m = 2$.

23. Nunc igitur erit $x = \frac{7}{4}$ ideoque $y = \frac{28}{17}$. Quare, cum sit

$$\frac{\alpha}{\beta} = \frac{7}{4} \text{ et } \frac{\gamma}{\delta} = y = \frac{28}{17},$$

statuere poterimus $\alpha = 7$, $\beta = 4$, $\gamma = 28$, $\delta = 17$, ex quibus valoribus porro colligimus

$$f = 264\,, \quad g = 7\,, \quad h = 231\,, \quad k = 128\,,$$

ex quibus ipsi numeri quaesiti ita definiuntur, ut sit:

$$a = 542\,, \quad b = 514\,, \quad c = 359\,, \quad d = 103\,,$$

qui sunt ipsi numeri ante inventi.

24. Postquam hac occasione numeros ex Commentariorum loco supra citato descriptos attentius considerassem, mox deprehendi in iis errorem calculi esse commissum[1]), quo emendato numeri quaestioni satisfacientes multo minores reperiuntur. Erit enim

$$A = 12231\,, \quad B = 10203\,, \quad C = 10381\,, \quad D = 2903^2),$$

qui post eos, quos hic invenimus, pro minimis videntur habendi. Maiores autem numeri ibi traditi recte se habere sunt deprehensi.

25. Quamquam autem hoc modo resolutio huius aequationis

$$A^4 + B^4 - C^4 - D^4 = 0$$

feliciter successit, tamen inde nullum subsidium ad istam aequationem resolvendam: $A^4 + B^4 + C^4 - D^4 = 0$, ita ut nulla summa trium biquadratorum exhiberi posse videatur biquadrato aequalis. Quin etiam equidem hactenus sum occupatus in quatuor biquadratis inveniendis, quorum summa esset pariter biquadratum, etiamsi iste casus secundum analogiam possibilis videatur. At vero quinque biquadrata pluribus modis dari posse observavi, quorum summa est biquadratum.

1) Vide notam 1), p. 136. R. F.

2) Confer p. 216 vol. 3 seriei I. R. F.

DE RESOLUTIONE HUIUS AEQUATIONIS
$0 = a + bx + cy + dxx + exy + fyy + gxxy + hxyy + ixxyy$
PER NUMEROS RATIONALES

Commentatio 777 indicis ENESTROEMIANI
Mémoires de l'académie des sciences de St.-Pétersbourg **11**, 1830, p. 58—68
Conventui exhibita die 9. octobris 1780

1. Haec formula nihilo aequanda complectitur in genere omnes functiones rationales integras duarum variabilium x et y, quarum utraque non ultra secundam dimensionem assurgit. Ista igitur expressio comprehendere potest novem terminos omnino, quos commode sequenti schemate quadratico repraesentari licet:

	1	x	xx
1	a	b	d
y	c	e	g
yy	f	h	i

Circa hanc igitur expressionem istam quaestionem evolvendam suscipio, quomodo pro binis variabilibus x et y valores rationales investigari oporteat, quae aequationi satisfaciant.

2. Ante omnia autem hic dispiciendum est, utrum forma proposita resolutionem in duos factores rationales admittat necne, quando quidem priori casu quaestio nulla plane laborat difficultate. Duplici autem modo evenire potest, ut tales expressiones duos factores involvant. Primo enim ea potest esse productum ex talibus duobus factoribus:

$$(\alpha + \beta x + \gamma xx)\,(\delta + \varepsilon y + \zeta yy) = 0\,.$$

Horum enim factorum dummodo alteruter radices rationales contineat, alteram variabilem prorsus pro lubitu accipere licebit. Sin autem neuter horum factorum nihilo aequatus radices rationales complectatur, tum etiam aequationi propositae nullo modo satisfieri poterit.

3. Alter modus, quo factores locum habere possunt, ita se habet:

$$(\alpha + \beta x + \gamma y + \delta xy)\,(\varepsilon + \zeta x + \eta y + \theta xy) = 0\,.$$

Resolutio enim hic infinitis modis in genere succedit. Posito enim priore factore $\alpha + \beta x + \gamma y + \delta xy = 0$, ex eo ultro sequitur $y = \frac{-\alpha - \beta x}{\gamma + \delta x}$, ita ut, quomodocunque alterutra variabilium accipiatur, alterius valor facillime assignare possit, idque adeo duplici modo ob geminos factores, quorum uterque nihilo aequari potest.

4. His autem casibus remotis resolutio quaestionis propositae non parum est ardua, siquidem methodus desideratur omnes plane valores investigandi, qui pro x et y substituti aequationi satisfaciant. Utralibet enim variabilis pro cognita accipiatur, alterius determinatio deducit ad resolutionem aequationis quadraticae, ideoque oritur formula radicalis ad rationalitatem perducenda, quam duplicem resolutionem accuratius perpendamus.

5. Consideremus igitur primo variabilem x tamquam cognitam, ac posito brevitatis gratia:

$$a + bx + dxx = P\,,$$
$$c + ex + gxx = Q\,,$$
$$f + hx + ixx = R\,,$$

aequatio hanc induet formam

$$P + Qy + Ryy = 0\,,$$

unde radice extracta oritur:

$$y = \frac{-Q \pm \sqrt{QQ - 4PR}}{2R}\,,$$

ubi ergo omnes valores ipsius x desiderantur, quibus ista formula radicalis $\sqrt{QQ - 4PR}$ rationalis reddatur. Ista autem forma irrationalis, si loco P, Q, R valores assumti restituantur, evadet:

$$\sqrt{\left((c + ex + gxx)^2 - 4(a + bx + dxx)\,(f + hx + ixx)\right)}\,.$$

Facta autem evolutione prodit sequens expressio non parum complexa:

$$(cc - 4af) + (2ce - 4ah - 4bf)x + (2cg + ee - 4df - 4bh - 4ai)x^2 + (2eg - 4dh - 4bi)x^3 + (gg - 4di)x^4 ,$$

quam ergo ad quadratum reduci oportet.

6. Quoniam haec formula est biquadratica, constat eius resolutionem ne suscipi quidem posse, nisi saltem unus casus innotescat, quo ea evadat quadratum (ac saepenumero etiam unicus talis casus non sufficit). Cognito autem uno casu, veluti $x = n$, secundum praecepta Analyseos solita statui debet $x = n + z$, ut obtineatur nova formula, unde valorem ipsius z deducere liceat, qui sit n', tum simili modo ulterius statui solet $z = n' + z'$, ut hoc modo valor z' innotescat, eodemque modo continuo ulterius progredi licet.

7. Evidens autem est hanc solvendi methodum maxime esse molestam ac plerumque vix ultra tertiam operationem ob numeros nimis magnos continuari posse; quamobrem hic methodum plane novam sum traditurus, cuius ope sine repetitis substitutionibus facillime ex valore iam cognito continuo novi valores deduci queant, quae ergo methodus in Analysin DIOPHANTEAM insigne incrementum allatura est censenda.

8. Ante omnia igitur hic assumo cognitum esse valorem $x = m$, cui respondeat $y = n$, et quia inter x et y nacti sumus istam aequationem quadraticam $P + Qy + Ryy = 0$, ubi est, uti assumsimus, $P = a + bx + dxx$, $Q = c + ex + gxx$ et $R = f + hx + ixx$, huic aequationi per hypothesin satisfiet sumendo $x = m$ et $y = n$; at vero eidem valori $x = m$ gemini valores pro y convenient, scilicet praeter $y = n$ adhuc alius, qui sit $y = n'$, qui facillime innotescet, cum ex natura aequationum sit

$$n + n' = -\frac{Q}{R} \quad \text{ideoque} \quad n' = -\frac{Q}{R} - n .$$

Vel etiam, cum sit

$$nn' = \frac{P}{R} ,$$

habebitur quoque

$$n' = \frac{P}{nR} ;$$

hocque ergo modo ex datis valoribus $x = m$ et $y = n$ novus valor ipsius y, scilicet n', obtinebitur.

9. Simili modo etiam tractari potest forma aequationis, unde ex dato y definitur x. Ponendo brevitatis gratia $a + cy + fyy = S$, $b + ey + hyy = T$, $d + gy + iyy = U$, habebitur haec aequatio

$$S + Tx + Uxx = 0 ;$$

unde patet cuilibet valori ipsius y duos respondere valores ipsius x, quorum summa semper erit $= -\frac{T}{U}$, productum autem $= \frac{S}{U}$. Quare, cum constet valor $y = n$, eique respondeat $x = m$, si alter valor ipsius x sit m', erit

$$m + m' = -\frac{T}{U} \quad \text{ideoque} \quad m' = -\frac{T}{U} - m ,$$

tum vero etiam

$$mm' = \frac{S}{U} \quad \text{ideoque} \quad m' = \frac{S}{mU} ,$$

unde iam patet harum formularum ope ex binis valoribus m et n continuo novos alios derivari posse, ita ut non opus sit ulla substitutione uti, qua forma proposita in alias formas transmutetur.

10. Hinc igitur tradi possunt praecepta pro omnibus huius generis quaestionibus resolvendis, quae in sequente problemate exponamus:

PROBLEMA

Proposita aequatione inter binas variabiles x et y in forma generali nostra contenta, si innotescant idonei valores pro x et y, ex iis alios novos elicere.

SOLUTIO

11. Talis aequatio ob binas variabiles x et y duplici modo repraesentetur:

I. $P + Qy + Ryy = 0$, II. $S + Tx + Uxx = 0$,

ubi ergo in priore litterae P, Q, R erunt functiones ipsius x, in posteriore vero litterae S, T, U functiones ipsius y. Iam denotent x et y ipsos valores iam cognitos, et quia cuilibet x respondent duae y, quarum si altera designetur per y', erit

$$y + y' = -\frac{Q}{R} \text{ vel etiam } yy' = \frac{P}{R} .$$

Simili modo, cum cuilibet y respondeant duae x, quarum altera si sit x', erit

$$x + x' = -\frac{T}{U} \text{ vel } xx' = \frac{S}{U} .$$

12. Cum nunc valores x et y habeantur cogniti, ex formula posteriore reperitur $x' = -\frac{T}{U} - x$ vel etiam $x' = \frac{S}{Ux}$, hic novus valor pro x inventus combinetur cum valore cognito y, indeque ex priore formula reperietur novus valor pro y, qui erit $y' = -\frac{Q}{R} - y$ vel etiam $y' = \frac{P}{Ry}$. Hic iam valor cum immediate praecedente x coniunctus praebebit ex forma posteriore novum valorem pro x, qui erit $x' = -\frac{T}{U} - x$ vel etiam $x' = \frac{S}{Ux}$, hocque modo progrediendo series infinita orietur, alternatim valores idoneos pro x et y exhibens, quorum bini contigui aequationi propositae satisfacient.

13. Quodsi ambae variabiles x et y permutentur, alia similis series erui poterit, scilicet incipiendo ab y et x, ex priori formula novus valor pro y reperitur, qui erit $y' = -\frac{Q}{R} - y$ vel $y' = \frac{P}{Ry}$. Ex hoc valore cum cognito x coniuncto colligitur novus valor $x' = -\frac{T}{U} - x$ vel $x' = \frac{S}{Ux}$, qui denuo coniunctus cum proximo praecedente y dabit $y' = -\frac{Q}{R} - y$ vel $y' = \frac{P}{Ry}$, hocque modo etiam sine fine progredi licebit. Interdum tamen alterutra harum serierum abrumpi potest, quando pervenitur vel ad $x = \infty$ vel ad $y = \infty$, tum enim ulterius progredi non licet.

14. Talibus autem valoribus pro x et y inventis, cum ex resolutione prioris formulae fiat $y = -\frac{Q \pm \sqrt{QQ - 4PR}}{2R}$, omnes valores pro x inventi

reddent formulam $QQ - 4PR$ quadratum. Simili modo, cum ex altera aequatione sit $x = -\frac{T \pm \sqrt{TT - 4SU}}{2U}$, omnes valores pro y inventi reddent formulam $TT - 4SU$ quadratum. Quo autem usus horum praeceptorum clarius appareat, aliquot exempla subiungamus.

EXEMPLUM 1

15. Proposita sit haec aequatio:

$$xxyy - xy + 4 = xx + yy ,$$

ubi statim patet sumto $x = 0$ fore $y = \pm 2$, similique modo, si $y = 0$, fiet $x = \pm 2$. Praeterea etiam notetur casus, quo $x = 1$; tum enim fiet $y = 3$, eodemque modo, si $y = 1$, fit $x = 3$, qui ergo sunt casus cogniti, ex quibus innumeros alios derivare licebit.

16. Hunc in finem repraesentatur aequatio proposita duplici modo:

$$\text{I.}\quad 4 - xx - xy + yy(xx - 1) = 0 ,$$
$$\text{II.}\quad 4 - yy - yx + xx(yy - 1) = 0 .$$

Ex harum prima oritur $y + y' = \frac{x}{xx - 1}$ vel etiam $yy' = \frac{4 - xx}{xx - 1}$. Eodem modo ex altera oritur $x + x' = \frac{y}{yy - 1}$ vel etiam $xx' = \frac{4 - yy}{yy - 1}$.

17. Incipiamus nunc a valoribus $x = 0$ et $y = 2$, unde ex formula posteriore fit $x' = \frac{2}{3}$, ex hoc porro cum praecedente $y = 2$ prior formula dat $y' = -\frac{16}{5}$. Hic porro valor cum praecedente $x = \frac{2}{3}$ coniunctus dat $x' = -\frac{78}{77}$, ex quo porro fit $y' = -\frac{1102}{31}$. Hos igitur valores ordine disponamus:

$$x = 0 , \quad y = 2 , \quad x = \frac{2}{3} , \quad y = -\frac{16}{5} , \quad x = -\frac{78}{77} , \quad y = -\frac{1102}{31} \text{ etc.}$$

18. Si incipiamus a valoribus $x = 0$ et $y = -2$, iidem prodibunt valores signis tantum mutatis, quod etiam eveniet permutandis variabilibus, sumendo $y = 0$ et $x = \pm 2$; tum enim prodibunt pro x valores, quos antea pro y invenimus, et vicissim. Invertendo porro, si incipiamus ab $y = 2$ et $x = 0$, sequens valor pro y erit -2, unde manifesto prodit series secundo loco commemorata.

19. Verum valor, qui praeterea nobis est cognitus, novos producit valores; incipiendo enim ab $x = 1$ et $y = 3$ erit $x' = -\frac{5}{8}$, $y' = -\frac{77}{39}$, $x'' = -\frac{31}{19 \cdot 29}$. Quodsi ordine inverso incipere vellemus, ponendo $y = 3$ et $x = 1$ fit statim $y = \infty$, sicque iam tota progressio sistitur. Valores autem hic inventi ordine dispositi erunt

$$x = 1\,,\quad y = 3\,,\quad x = -\frac{5}{8}\,,\quad y = -\frac{77}{39}\,,\quad x = -\frac{31}{19 \cdot 29}\ [\text{etc.}]\,,$$

ubi notandum eosdem valores etiam signis mutatis atque adeo valoribus x et y inter se permutatis quaesito pariter satisfacere, sicque pro solutione problematis duas series in infinitum procedentes sumus adepti.

20. Cum in hoc exemplo habeamus $P = 4 - xx$, $Q = -x$, $R = xx - 1$, tum vero $S = 4 - yy$, $T = -y$, $U = yy - 1$, erit

$$QQ - 4PR = 16 - 19xx + 4x^4\,.$$

Similique modo

$$TT - 4SU = 16 - 19yy + 4y^4\,,$$

quae cum sint similes inter se, ista formula: $16 - 19zz + 4z^4$ semper evadet quadratum, si loco z sumamus tam valores pro x quam pro y inventos, qui ergo valores ordine dispositi sunt:

$$0\,,\quad 2\,,\quad \frac{2}{3}\,,\quad \frac{16}{5}\,,\quad \frac{78}{77}\,,\quad \frac{1102}{31}\,^{1})\,,$$

$$1\,,\quad 3\,,\quad \frac{5}{8}\,,\quad \frac{77}{39}\,,\quad \frac{31}{19 \cdot 29}\,.$$

Veluti, si sumamus $z = \frac{5}{8}$, erit $16 - 19zz + 4z^4 = \frac{97^2}{32^2}$.

21. Haec insignis proprietas isti innititur fundamento, quod in aequatione proposita binae variabiles x et y inter se commutari possunt; quoties ergo aequatio proposita ita fuerit comparata, semper eadem proprietas locum habebit, ut valores pro litteris x et y inventi permutationem admittant, ita ut,

1) Editio princeps: $\frac{1102}{32}$. Correxit R. F.

cum series horum valorum fuerit inventa, quilibet bini termini eius contigui pro litteris x et y sine discrimine accipi queant. Operae igitur pretium erit omnes istos casus in genere evolvere.

EXEMPLUM 2

22. Proposita inter binas variabiles x et y hac aequatione:

$$\alpha + \beta(x + y) + \gamma(xx + yy) + \delta xy + \varepsilon xy(x + y) + \zeta xxyy = 0 ,$$

ubi x et y permutationem admittunt, investigare omnes valores ipsarum x et y huic aequationi satisfacientes.

23. Reducatur aequatio proposita ad hanc formam:

$$\alpha + \beta x + \gamma xx + y(\beta + \delta x + \varepsilon xx) + yy(\gamma + \varepsilon x + \zeta xx) = 0 ,$$

unde fit pro forma nostra generali:

$$P = \alpha + \beta x + \gamma xx ,$$
$$Q = \beta + \delta x + \varepsilon xx ,$$
$$R = \gamma + \varepsilon x + \zeta xx ,$$

qui iidem valores, permutatis x et y, valebunt pro litteris S, T, U; unde pro binis valoribus eiusdem litterae habebimus $y + y' = -\frac{Q}{R}$ vel etiam $yy' = \frac{P}{R}$.

24. Sint nunc A et B bini valores cogniti pro litteris x et y; ex iis sequentes, qui sint C, D, E etc., per sequentes formulas definientur:

$$C = -\frac{\beta + \delta B + \varepsilon BB}{\gamma + \varepsilon B + \zeta BB} - A \text{ sive } C = \frac{\alpha + \beta B + \gamma BB}{A(\gamma + \varepsilon B + \zeta BB)} ;$$

tum vero

$$D = -\frac{\beta + \delta C + \varepsilon CC}{\gamma + \varepsilon C + \zeta CC} - B \text{ sive } D = \frac{\alpha + \beta C + \gamma CC}{B(\gamma + \varepsilon C + \zeta CC)} ,$$

$$E = -\frac{\beta + \delta D + \varepsilon DD}{\gamma + \varepsilon D + \zeta DD} - C \text{ sive } E = \frac{\alpha + \beta D + \gamma DD}{C(\gamma + \varepsilon D + \zeta DD)} \text{ [1)]} .$$

etc. etc.

1) Editio princeps: $\frac{\alpha + \beta D + \gamma DD}{B(\gamma + \varepsilon D + \zeta DD)}$. Correxit R. F.

Inventa igitur hac serie, quilibet bini termini contigui pro x et y assumi poterunt. Ita si sumamus $x = D$, erit vel $y = C$ vel $y = E$; utroque enim modo aequationi nostrae satisfiet.

25. Iidem porro etiam termini huius seriei semper formulam $QQ - 4PR$ reddent quadratum, quae, cum aeque valeat pro x et y, earum loco scribamus novam litteram z, et cum sit

$$P = \alpha + \beta z + \gamma zz\,, \quad Q = \beta + \delta z + \varepsilon zz\,, \quad R = \gamma + \varepsilon z + \zeta zz\,,$$

facta evolutione pro formula $QQ - 4PR$ talis expressio reperietur:

$$\mathfrak{A} + \mathfrak{B}z + \mathfrak{C}zz + \mathfrak{D}z^3 + \mathfrak{E}z^4,$$

ubi erit:

$$\begin{aligned}
\mathfrak{A} &= \beta\beta - 4\alpha\gamma\,,\\
\mathfrak{B} &= 2\beta\delta - 4\alpha\varepsilon - 4\beta\gamma\,,\\
\mathfrak{C} &= \delta\delta - 2\beta\varepsilon - 4\alpha\zeta - 4\gamma\gamma\,,\\
\mathfrak{D} &= 2\delta\varepsilon - 4\beta\zeta - 4\gamma\varepsilon\,,\\
\mathfrak{E} &= \varepsilon\varepsilon - 4\gamma\zeta\,.
\end{aligned}$$

26. Igitur formula ad quartam dimensionem ipsius z exsurgere potest, cuiusmodi formulae in Analysi DIOPHANTEA difficillime non nisi per longos calculos ad quadratum reduci possunt. At vero series terminorum A, B, C, D etc. ita est comparata, ut eius quilibet terminus pro z assumtus hanc formulam reddat quadratum.

EXEMPLUM 3

27. Proposita sit ista aequatio:

$$xxy - xyy + xx + yy - 2 = 0\,,$$

cui primo satisfaciunt valores $x = 1$ et $y = 1$; tum vero etiam $x = -1$ et $y = -1$. Haec aequatio ad nostram formam $P + Qy + Ryy$ reducta dat $P = xx - 2$, $Q = xx$, $R = 1 - x$. Altera vero forma $S + Tx + Uxx$ erit $S = yy - 2$, $T = -yy$, $U = 1 + y$, unde deducimus has formulas:

$$y + y' = \frac{xx}{x-1} \text{ vel etiam } yy' = \frac{xx-2}{1-x};$$

tum vero

$$x + x' = \frac{yy}{y+1} \text{ vel etiam } xx' = \frac{yy-2}{1+y}.$$

28. Ope harum formularum, si incipiamus ab his valoribus $x = 1$ et $y = 1$, sequentes investigentur:

$$x' = -\frac{1}{2}, \quad y' = -\frac{7}{6}, \quad x'' = -\frac{23}{3}, \quad y'' = -\frac{73}{13}, \quad x''' = \frac{217}{13 \cdot 20}.$$

Pro altero casu cognito incipiamus ab $y = -1$ et $x = -1$, et valores sequentes ordine erunt:

$$y' = \frac{1}{2}, \quad x' = \frac{7}{6}, \quad y'' = \frac{23}{3}, \quad x'' = \frac{73}{13}, \quad y''' = -\frac{217}{13 \cdot 20}.$$

Hi valores posteriores conveniunt praecedentibus mutatis tam signis quam binis litteris x et y, cuius ratio est evidens ex ipsa aequatione proposita.

29. Cum hic sit:

$$QQ - 4PR = x^4 + 4x^3 - 4xx - 8x + 8,$$

ista formula evadet quadratum, quoties pro x quispiam valorum inventorum substituatur, qui sunt ordine:

$$1, \quad -1, \quad -\frac{1}{2}, \quad \frac{7}{6}, \quad -\frac{23}{3}, \quad \frac{73}{13}, \quad \frac{217}{13 \cdot 20} \text{ etc.}$$

Veluti si sumamus $x = \frac{7}{6}$, erit

$$QQ - 4PR = \frac{43^2}{36^2}.$$

EXEMPLUM 4

30. Proposita sit haec aequatio:

$$xxyy - x - y + 1 = 0,$$

cui sumto $x = 0$ satisfacit $y = 1$; at sumto $y = 0$ satisfacit $x = 1$. Iam quia formulae nostrae erunt

$$y + y' = \frac{1}{xx} \quad \text{et} \quad yy' = \frac{1-x}{xx},$$

tum vero

$$x + x' = \frac{1}{yy} \quad \text{et} \quad xx' = \frac{1-y}{yy}.$$

Hinc incipiendo a valoribus $x = 0$ et $y = 1$ sequentes erunt $x' = 1$, $y' = 0$, $x'' = \infty$. Tum alter casus $y = 0$ et $x = 1$ dat ut ante $y' = 1$, $x' = 0$, $y'' = \infty$, unde patet hinc alios valores non obtineri, praeter

$$x = 0, \quad y = 0, \quad x = 1,$$
$$y = 1, \quad x = 1, \quad y = 1,$$

neque tamen hinc concludere licet nullos alios valores satisfacere. Si enim alius insuper valor cognitus daretur, ex eo fortasse alios novos eruere liceret. At revera alii valores prorsus non dantur. Constat autem plurimas dari formulas, quae paucis tantum quibusdam casibus quadrata reddi possunt.

METHODUS NOVA ET FACILIS FORMULAS CUBICAS ET BIQUADRATICAS AD QUADRATUM REDUCENDI

Commentatio 778 indicis ENESTROEMIANI
Mémoires de l'académie des sciences de St-Pétersbourg 11, 1830, p. 69—91
Conventui exhibita die 16. octobris 1780

1. Quando in Analysi DIOPHANTEA pervenitur ad formulas cubicas vel adeo biquadraticas quadrato aequandas, ante omnia necesse est, ut unus saltem casus innotescat, quo hoc eveniat; tum vero praecepta constant ex tali casu cognito alium eruendi, quo invento formulam propositam ope certae substitutionis in aliam transformari oportet, unde simili modo novus valor investigari solet. Hoc modo per continuo repetitas substitutiones et transformationes totum negotium absolvi debet, quae autem mox ob numeros continuo maiores occurrentes tam fiunt molestae ac taediosae, ut vix quisquam reperiatur, qui has operationes aliquoties reiterare voluerit. Quamobrem non dubito, quin methodus, quam hic sum traditurus, insigne incrementum Analysi sit allatura, cuius beneficio sine ulla substitutione vel transformatione ex casu quovis cognito alios derivare licet, cuius quidem methodi iam aliquot specimina in medium attuli, hic autem eam dilucide explicare eiusque usum ostendere accuratius constitui.

2. Sit igitur formula ad quadratum reducenda:

$$A + Bx + Cxx + Dx^3 + Ex^4 = V,$$

ac totum negotium huc redit, ut ista formula ad hanc speciem revocetur

$$V = PP + QR,$$

ubi litterae P, Q, R tales designent formas:

$$P = a + bx + cxx\,,$$
$$Q = d + ex + fxx\,,$$
$$R = g + hx + ixx\,,$$

tum enim, cum V debeat esse quadratum, statuatur eius radix $= P + Qy$, unde orietur ista aequatio:

$$2Py + Qyy = R\,,$$

quam in posterum *canonicam* vocemus, in qua ergo duae variabiles x et y reperientur, quarum utraque non ultra secundam dimensionem exsurgit, ita ut cuilibet valori ipsius x gemini valores ipsius y respondeant ac vicissim cuilibet valori ipsius y duo valores ipsius x. Haec ergo aequatio substitutis valoribus ita erit comparata:

$$yy(d + ex + fxx) + 2y(a + bx + cxx) - g - hx - ixx = 0\,,$$

unde pro variabili x formabitur ista aequatio:

$$xx(fyy + 2cy - i) + x(eyy + 2by - h) + dyy + 2ay - g = 0\,,$$

ubi brevitatis gratia ponamus:

$$fyy + 2cy - i = S\,,$$
$$eyy + 2by - h = T\,,$$
$$dyy + 2ay - g = U\,,$$

ita ut habeamus hanc aequationem:

$$Sxx + Tx + U = 0\,,$$

quam ergo cum altera aequatione

$$Qyy + 2Py - R = 0$$

convenire necesse est.

3[1]). Cum igitur cuilibet valori ipsius x respondeant duo valores ipsius y, quorum alter sit y, alter vero y', ex natura aequationum habebitur:

$$y + y' = -\frac{2P}{Q} \quad \text{et} \quad yy' = -\frac{R}{Q}\,.$$

1) Ab hoc loco in editione principe numeri paragraphorum unitate aucti sunt. R. F.

Simili modo, cum singulis valoribus ipsius y respondeant duo valores ipsius x, qui sint x et x', erit

$$x + x' = -\frac{T}{S} \text{ et } xx' = \frac{U}{S},$$

quarum formularum ope ex cognitis quibusvis valoribus ipsarum x et y alii novi assignari poterunt, ex quibus deinde pariter alii novi, hocque modo sine fine plures erui poterunt, in qua insigni proprietate consistit natura novae methodi, quam hic sum traditurus, quae ergo sine ullis substitutionibus et transformationibus continuo plures novos valores idoneos suppeditat.

4. Quod quo clarius appareat, ponamus primos valores ipsarum x et y cognitos esse $x = \alpha$ et $y = \beta$ et, quia valori $y = \beta$ respondent duo valores ipsius x, quorum alter est α, alter vero, qui sit γ, reperietur ex hac formula:

$$\gamma = -\frac{(e\beta\beta + 2b\beta - h)}{f\beta\beta + 2c\beta - i} - \alpha \; ;$$

eodem modo, quia ipsi γ respondent duo valores ipsius y, quorum alter habetur β, si alter statuatur $= \delta$, erit

$$\delta = -\frac{2(a + b\gamma + c\gamma\gamma)}{d + e\gamma + f\gamma\gamma} - \beta \; .$$

Nunc quia ipsi δ respondet primo $x = \gamma$, si alter ponatur $= \varepsilon$, reperietur:

$$\varepsilon = -\frac{(e\delta\delta + 2b\delta - h)}{f\delta\delta + 2c\delta - i} - \gamma \; ,$$

hocque modo ulterius progrediendo habebimus:

$$\zeta = -\frac{2(a + b\varepsilon + c\varepsilon\varepsilon)}{d + e\varepsilon + f\varepsilon\varepsilon} - \delta \; , \qquad \eta = -\frac{(e\zeta\zeta + 2b\zeta - h)}{f\zeta\zeta + 2c\zeta - i} - \varepsilon \; ,$$

etc. etc.

Unde patet hanc seriem secundum legem satis simplicem, quousque libuerit, continuari posse. Inventis autem terminis huius seriei: α, β, γ, δ, ε etc., alterni α, γ, ε, η etc. praebebunt valores ideoneos pro littera x, quibus formula proposita revera fit quadratum.

5. Possunt etiam bini valores cogniti $x = \alpha$ et $y = \beta$ in ordine permutari, ita ut incipiamus ab $y = \beta$ et $x = \alpha$; atque ope earundem formularum similis series retrograda formari poterit, cuius tertius terminus erit novus valor ipsius y, quartus ipsius x, quintus ipsius y et ita porro, ita ut istius seriei termini secundus, quartus, sextus etc. etiam valores idoneos pro littera x sint exhibituri. Interdum quidem usu venit, ut alterutra harum serierum alicubi abrumpatur, quod contingit, quando ad terminum infinite magnum pervenitur. Quin etiam eiusmodi casus occurrere possunt, quibus valores ipsius x iterum ad praecedentes revolvuntur, id quod necessario evenire debet pro eiusmodi formulis, quae vel unico tantum casu vel tantum duobus tribusve quadrata evadere possunt; veluti evenit pro hac formula $1 + x^3 = \square$, quae tantum tribus casibus quadratum fieri potest[1]).

6. Cum autem hae operationes institui nequeunt, nisi pro litteris x et y valores idonei, quos posuimus $x = \alpha$ et $y = \beta$, fuerint cogniti, tales valores plerumque suppeditat ipsa aequatio canonica

$$yyQ + 2yP - R = 0 .$$

Si enim fieri queat $Q = 0$ sive $d + ex + fxx = 0$, quod evenit, quando fuerit $ee - 4df = \square$, tum erit $y = \frac{R}{2P}$. Deinde si fuerit $R = 0$, hoc est $g + hx + ixx = 0$, quod fit, quando fuerit $hh - 4gi = \square$, tum bini prodeunt valores pro y, alter $y = 0$, alter $y = -\frac{2P}{Q}$. Hoc igitur modo evenire potest, ut pro x quatuor valores idonei reperiantur simulque iis valores ipsius y respondentes innotescant. Praeterea vero etiam altera forma aequationis canonicae, quae erat $Sxx + Tx + U = 0$, valores idoneos praebere potest, si enim reddi queat $S = fyy + 2cy - i = 0$, unde pro y duo valores resultare possunt. Id contingit, quando fuerit $cc + fi = \square$; tum autem erit $x = -\frac{U}{T}$. Denique etiam, quando fuerit $U = dyy + 2ay - g = 0$, quod evenit, si $aa + dg = \square$, pro x gemini prodeunt valores, alter $x = 0$, alter $x = -\frac{T}{S}$, unde ergo etiam plures casus cogniti erui possunt. Omnes autem istos valores cognitos, qui immediate ex aequatione canonica derivantur, vocemus *primi-*

1) Confer § 12 et sequentes. R. F.

tivos, quandoquidem ex his per praecepta ante tradita innumerabiles alii deduci possunt. Ad hoc autem imprimis requiritur, ut formula proposita V quadrato aequanda ad hanc formam: $V = PP + QR$ redigi queat. Hoc igitur aliquot exemplis illustremus.

EXEMPLUM 1

7. Sit formula quadrato aequanda:

$$V = 4xx + (x-1)(3xx - x - 1) \quad \text{sive} \quad V = 3x^3 + 1,$$

erit

$$P = 2x, \quad Q = x - 1, \quad R = 3xx - x - 1,$$

unde aequationis canonicae prior forma erit:

$$(x-1)yy + 4xy - (3xx - x - 1)\,[= 0],$$

altera vero forma:

$$-3xx + (yy + 4y + 1)x - (yy - 1) = 0,$$

unde binae formulae, quas vocemus *directrices*, erunt:

$$y + y' = -\frac{4x}{x-1}, \quad x + x' = \frac{yy + 4y + 1}{3}.$$

At vero ex formula priore canonica oritur valor cognitus $x = 1$, cui respondet $y = \frac{1}{4}$; altera autem forma facto $yy - 1 = 0$ praebet vel $y = +1$ vel $y = -1$, quorum priori respondet vel $x = 0$ vel $x = 2$; alteri vero $y = -1$ respondet etiam vel $x = 0$ vel $x = -\frac{2}{3}$.

8. Instituamus igitur operationes supra praescriptas et incipiamus primo a valoribus $x = 1$ et $y = \frac{1}{4}$, ac reperiemus sequentem seriem:

$$x = 1, \quad y = \frac{1}{4}, \quad x = -\frac{5}{16}, \quad y = -\frac{101}{84} \text{ etc.}$$

Sumamus nunc $x = 0$ et $y = 1$, unde formulae directrices producent sequentem seriem valorum idoneorum:

$$x = 0, \quad y = 1, \quad x = 2, \quad y = -9, \quad x = \frac{40}{3}, \quad y = \frac{173}{37} \text{ etc.}$$

Invertamus ordinem incipiendo ab $y = 1$ et $x = 0$; series valorum idoneorum erit:

$$y = 1\ ,\quad x = 0\ ,\quad y = -1\ ,\quad x = -\frac{2}{3}\ ,\quad \left[y = -\frac{3}{5}\right]\ ,\quad x = \frac{8}{25}\ \text{etc.}$$

In his iam seriebus omnes reliqui valores primitivi continentur. In praecedente autem serie ordinem valorum primitivorum $x = 1$ et $y = \frac{1}{4}$ ideo non invertimus, quia sequens y iam prodiisset infinitum.

9. Formula ergo proposita $V = 3x^3 + 1$ ad quadratum reducitur his valoribus ipsius x:

$$x = 0\ ,\quad x = 1\ ,\quad x = -\frac{2}{3}\ ,\quad x = 2\ ,\quad x = -\frac{5}{16}\ ,\quad x = \frac{8}{25}\ ,\quad x = \frac{40}{3}\ \text{etc.},$$

qui quomodo satisfaciant, videamus.

$$\begin{aligned}
&\text{Si } x = 0\ , && \text{fit } V = 1^2\ ,\\
&\text{si } x = 1\ , && \text{fit } V = 2^2\ ,\\
&\text{si } x = -\frac{2}{3}\ , && \text{fit } V = \frac{1}{3^2}\ ,\\
&\text{si } x = 2\ , && \text{fit } V = 5^2\ ,\\
&\text{si } x = -\frac{5}{16}\ , && \text{fit } V = \frac{61^2}{64^2}\ ,\\
&\text{si } x = \frac{8}{25}\ , && \text{fit } V = \frac{131^2}{125^2}\ ,\\
&\text{si } x = \frac{40}{3}\ , && \text{fit } V = \frac{253^2}{3^2}
\end{aligned}$$

etc.

EXEMPLUM 2

10. Proposita sit haec formula quadrato aequanda:

$$V = xx + (xx + 1)(xx - 2) \quad \text{sive} \quad V = x^4 - 2\ ,$$

ubi est $P = x$, $Q = xx + 1$, $R = xx - 2$. Hinc aequatio canonica erit:

$$(xx + 1)\,yy + 2xy - (xx - 2) = 0\ ;$$

altera autem eius forma erit:

$$(yy - 1)xx + 2yx + (yy + 2) = 0\,,$$

unde formantur hae formulae directrices:

$$y' = -\frac{2x}{xx+1} - y \quad \text{et} \quad x' = -\frac{2y}{yy-1} - x\,.$$

Prior autem forma, cum neque fieri queat $Q = 0$ neque $R = 0$, nullos dat valores primitivos; altera autem forma dat $S = 0$ ideoque $y = \pm 1$, cui respondet $x = \mp \frac{3}{2}$. Praeterea vero, cum fieri nequeat $U = yy + 2 = 0$, alios valores primitivos non suppeditat.

11. Incipiamus igitur a valoribus $y = 1$ et $x = -\frac{3}{2}$, et formulae directrices sequentem nobis administrant seriem valorum:

$$y = 1\,,\quad x = -\frac{3}{2}\,,\quad y = -\frac{1}{13}\,^{1})\,,\quad x = \frac{113}{84}\,^{2})\,.$$

Invertendo autem $x = -\frac{3}{2}$, $y = 1$, $x = \infty$. Alteri autem valores primitivi $x = +\frac{3}{2}$ et $y = -1$ eosdem manifesto producent valores signis tantum mutatis, qui ergo, quoniam in formula proposita tantum occurrit xx, novas solutiones non dabunt. Valores ergo ipsius x hactenus inventi sunt

$$x = \pm\frac{3}{2} \quad \text{et} \quad x = [\pm]\frac{113}{84}\,,$$

quibus formula proposita $x^4 - 2$ quadratum redditur hoc modo:

$$\text{Si} \quad x = \frac{3}{2}\,, \quad \text{erit} \quad V = \frac{7^2}{4^2}\,,$$

$$\text{si} \quad x = \frac{113}{84}\,, \quad \text{erit} \quad V = \frac{7967^2}{7056^2}\,.$$

1) Editio princeps: $\frac{1}{13}$. Correxit A. M.

2) Editio princeps: $-\frac{113}{84}$. Correxit A. M.

EXEMPLUM 3

12. Proposita sit haec formula quadrato aequanda:

$$V = (x+1)^2 + x(x+1)(x-2) \text{ sive } V = x^3 + 1,$$

quam certum est aliis casibus quadratum fieri non posse praeter $x = 0$, $x = -1$ et $x = 2$[1]), id quod etiam nostrae operationes declarabunt. Cum autem hic sit $P = x + 1$ et $QR = x(x+1)(x-2)$, sumamus $Q = x(x+1)$ et $R = x - 2$; aequatio ergo canonica erit

$$x(x+1)yy + 2(x+1)y - (x-2) = 0,$$

cuius altera forma erit $yyxx + (yy + 2y - 1)x + (2y + 2) = 0$. Formulae autem directrices ita se habebunt:

$$y' = -\frac{2}{x} - y \quad \text{et} \quad x' = -\frac{(yy + 2y - 1)}{yy} - x .$$

Ex priori forma posito $Q = 0$ oriuntur duo valores primitivi vel $x = 0$ vel $x = -1$, pro quorum priore fit $y = -1$, pro altero $y = \infty$. Facto autem $R = 0$ sive $x = 2$ erit vel $y = 0$ vel $y = -1$. Altera autem forma posito $S = 0$ dat $y = 0$, cui respondet $x = 2$; at posito $U = 0$ dat $y = -1$, cui respondet $x = 2$, quos ergo valores primitivos evolvamus.

13. Sit igitur primo $x = 0$ et $y = [-]1$, et formulae nostrae directrices producent:

$$x = 0, \quad y = -1, \quad x = 2, \quad y = 0, \quad x = \infty .$$

Invertendo

$$y = -1, \quad x = 0, \quad y = \infty .$$

Sumamus nunc hos primitivos valores $x = -1$, $y = \infty$, qui dant

$$x = -1, \quad y = \infty, \quad x = 0, \quad y = \infty, \quad x = 0 \text{ etc.}$$

Sumatur denique $x = 2$ et $y = 0$, et valores erunt:

$$x = 2, \quad y = 0, \quad x = \infty, \quad y = 0, \quad x = \infty \text{ etc.}$$

Patet ergo ex omnibus primitivis, qui erant $x = 0$, $x = -1$, $x = 2$, nullos alios novos deduci posse.

1) Confer Theorema 10 Commentationis 98, *Leonhardi Euleri Opera omnia* vol. 2, seriei I, p. 56. R. F.

EXEMPLUM 4

14. Proposita sit quadrato aequanda haec formula:

$$V = xx + (xx - 1)(2xx + 1) \quad \text{sive} \quad V = 2x^4 - 1 ,$$

ad quam pervenitur, quando quaeruntur duo numeri, quorum summa sit quadratum, quadratorum vero summa biquadratum.[1]) Cum igitur hic sit $P = x$, $Q = xx - 1$, $R = 2xx + 1$, erit aequatio canonica ita expressa:

$$(xx - 1)yy + 2xy - (2xx + 1) = 0 ,$$

eiusque inversa

$$(yy - 2)xx + 2yx - (yy + 1) = 0 .$$

Hinc formulae directrices erunt:

$$y' = -\frac{2x}{xx - 1} - y \quad \text{et} \quad x' = -\frac{2y}{yy - 2} - x .$$

Prior forma posito $Q = 0$ dat $x = \pm 1$, cui respondet $y = \pm \frac{3}{2}$; at $R = 0$ nihil dat. Ex altera forma itidem nulli valores primitivi oriuntur.

15. Evolvamus ergo valores $x = 1$ et $y = \frac{3}{2}$, ex quibus per formulas directrices reperiuntur:

$$x = 1 , \quad y = \frac{3}{2} , \quad x = -13 , \quad y = -\frac{113}{84} \text{ etc.}$$

Permutando autem primos valores fient

$$y = \frac{3}{2} , \quad x = 1 , \quad y = \infty .$$

Reliqui primitivi non nisi signo differunt, ideoque eosdem praebent valores. At vero valor $x = 13$ dat $V = 239^2$.

16. Hactenus autem assumsimus formulam propositam quadrato aequandam:

$$A + Bx + Cxx + Dx^3 + Ex^4 = V$$

---

1) Confer Commentationes 560 et 763, *Leonhardi Euleri Opera omnia* vol. 4 seriei I, p. 96, et p. 61 huius voluminis. R. F.

iam esse ad formam $PP + QR$ revocatam atque insuper aequationem canonicam inde formatam $Qyy + 2Py - R = 0$ eiusque alteram formam $Sxx + Tx + U = 0$ ita esse comparatam, ut saltem una harum aequalitatum

$$Q = 0, \quad R = 0, \quad S = 0, \quad U = 0$$

praebeat radicem rationalem, quod si non eveniat, operationes supra descriptae ne institui quidem possunt, nisi forte divinando casus quispiam reperiri queat, quo formula proposita revera evadat quadratum. Quodsi enim hoc modo innotuerit valor ipsius x, ei respondens y ex aequatione canonica derivare poterit; unde deinceps operationes praescriptae institui poterunt.

17. Verum etiam reductio formulae propositae ad formam $PP + QR$ saepenumero maxime est difficilis, praecipue si nullus casus iam fuerit cognitus. Quoties autem unus saltem casus, quo formula proposita quadratum evadit, innotuerit, tum ea semper ad formam $PP + QR$ reduci et, quia casus iam est cognitus, operationes optimo successu institui poterunt. Quemadmodum igitur ex casu cognito formula proposita ad formam $PP + QR$ reduci queat, imprimis nobis erit ostendendum, quo ista tractatio completa reddatur, id, quod in sequentibus problematibus expediemus.

PROBLEMA I

Si proposita fuerit formula cubica haec:

$$A + Bx + Cxx + Dx^3 = V,$$

quae evadat quadratum casu $x = a$, eam ad formam $PP + QR$ revocare indeque aequationem canonicam constituere, ex qua deinceps operationes supra descriptas instituere liceat.

SOLUTIO

18. Fiat igitur posito $x = a$ nostra formula:

$$A + Ba + Caa + Da^3 = ff,$$

tum sumto $P = f$ semper pro QR eiusmodi formula prodibit, quae in factores resolvi potest, quarum ergo alter pro Q alter pro R accipi poterit. Tum enim erit $QR = V - ff$, unde loco ff valorem substituendo itemque loco V prodibit:

$$QR = B(x - a) + C(xx - aa) + D(x^3 - a^3),$$

ideoque

$$QR = (x - a)\big(B + C(x + a) + D(xx + ax + aa)\big),$$

ubi iam sumi poterit

$$Q = x - a \quad \text{et} \quad R = B + C(x + a) + D(xx + ax + aa).$$

Possent etiam hi valores inter se permutari; verum hinc nullum discrimen in valoribus ipsius x, quos operationes nostrae suppeditabunt, orietur.

19. Inventis iam valoribus litterarum P, Q, R aequatio canonica erit:

$$yy(x - a) + 2fy - B - C(x + a) - D(xx + ax + aa) = 0,$$

unde pro valore cognito $x = a$ fit:

$$y = \frac{B + 2Ca + 3Daa}{2f},$$

et iam facile erit ex his valoribus ope formularum supra datarum innumerabiles alios valores litterarum x et y eruere, nisi forte ad valores infinitos perveniatur vel iidem recurrant.

20. Hic autem non absolute necesse est, ut sumatur $P = f$, sed pari successu eius loco talis functio ipsius x assumi posset, quae posito $x = a$ abeat in f, tum enim prorsus ut ante $V - PP$ factorem habebit $x - a$. Interim tamen hinc nulli alii valores pro x prodibunt; tota enim res eo redibit, ac si pro y sumeremus $y + W$ denotante W functionem quandam ipsius x, unde pro calculi facilitate expediet statui $P = f$.

PROBLEMA II

Si formula proposita cubica:

$$V = A + Bx + Cxx + Dx^3$$

duobus casibus $x = a$ et $x = b$ quadratum evadat, eam ad formam $PP + QR$ ita reducere, ut aequatio canonica utrumque valorem $x = a$ et $x = b$ involvat.

SOLUTIO

21. Ponamus igitur casu $x = a$ fieri

$$A + Ba + Caa + Da^3 = ff,$$

at vero altero casu $x = b$ fieri

$$A + Bb + Cbb + Db^3 = gg,$$

atque pro aequatione canonica statuamus

$$V = (p + q(x - a) + y(x - a)(x - b))^2$$

sive

$$V = pp + 2pq(x - a) + 2py(x - a)(x - b) + qq(x - a)^2 + 2qy(x - a)^2(x - b) + yy(x - a)^2(x - b)^2,$$

ubi p et q denotent certas quantitates constantes ab x non pendentes, quas sequenti modo definire licebit.

22. Ponamus primo $x = a$, et, quia tum fit $V = ff$, habebimus hanc aequationem: $ff = pp$ ideoque $p = f$; deinde ponamus $x = b$, et, quia tum fit $V = gg$, nostra aequatio hanc induet formam:

$$gg = ff + 2fq(b - a) + qq(b - a)^2,$$

unde fit

$$g = f + q(b - a)$$

ideoque

$$q = \frac{g - f}{b - a}\ ^{1}) .$$

Inventis nunc binis valoribus p et q sumatur $P = p + q(x - a)$, atque manifestum est formulam $V - PP$ factorem habituram esse $(x - a)(x - b)$, unde statuamus $V - PP = M(x - a)(x - b)$; atque nunc fiat

$$V = (P + y(x - a)(x - b))^2$$

factaque evolutione et translato PP ad alteram partem tota aequatio divisibilis erit per $(x - a)(x - b)$ orieturque

$$M = 2Py + yy(x - a)(x - b).$$

1) In editione principe sequitur: quibus valoribus substitutis. R. F.

Quod autem facta evolutione aequatio prodeat per $(x-a)(x-b)$ divisibilis, inde colligi potest, quod ambo casus $x=a$ et $x=b$ inter se permutari possunt; quare, cum formula $V-PP$ sponte factorem habeat $x-a$, necesse est, ut etiam habeat factorem $x-b$. Quia enim invenimus $P=f+\frac{(g-f)(x-a)}{b-a}$, facta permutatione erit $P=g+\frac{(f-g)(x-b)}{a-b}$, hae duae formulae prorsus inter se congruunt. Quare, cum formula $V-PP$ divisibilis fuerit per $x-a$, etiam divisibilis erit per $x-b$ ideoque etiam per productum $(x-a)(x-b)$.

EXEMPLUM

23. Sit

$$V=3x^3+1,$$

quae aequatio casu $x=1$ fit $V=2^2$, casu autem $x=2$ fit $V=5^2$, ideoque habebimus $a=1$, $f=2$, $b=2$, $g=5$, unde fiet $P=3x-1$. Hinc igitur fiet $V-PP=3x^3-9xx+6x$[1]), quae est divisibilis per $(x-1)(x-2)$, cum sit $V-PP=(x-1)(x-2)3x$, quamobrem hoc casu erit $M=3x$. Quocirca pro formula $3x^3+1$ quadrato aequanda aequatio canonica erit:

$$3x=2(3x-1)y+(x-1)(x-2)yy.$$

Altera igitur forma erit

$$yyxx+(6y-3yy-3)x+2yy-2y=0.$$

Prior forma ex $Q=0$ dat statim ipsos valores perse cognitos $x=1$ et $x=2$; at vero $R=0$ dat $x=0$. Altera forma ex $S=0$ praebet $y=0$ et $x=0$; ex $U=0$ fit $y=0$ vel $y=1$, quibus respondet $x=0$, sicque habemus tres valores primitivos $x=0$, $x=1$, $x=2$, quibus conveniunt $y=0$, $y=1$, $y=\frac{3}{4}$, $y=\frac{3}{5}$.

24. Formulae iam directrices erunt:

$$y'=-\frac{2(3x-1)}{(x-1)(x-2)}-y \quad \text{et} \quad x'=\frac{3yy-6y+3}{yy}-x.$$

1) Editio princeps: $3x^3+9xx+6x$. Correxit R. F.

Hinc percurramus casus cognitos, ac primo quidem $x = 0$ et $y = 0$ nihil dat; at vero invertendo obtinetur:

$$y = 0\,, \quad x = 0\,, \quad y = 1\,, \quad x = 0\,, \quad y = 0 \quad \text{etc.}\,,$$

unde patet primum valorem $x = 0$ ad nullos novos valores perducere. Sumamus igitur $x = 1$, $y = \frac{3}{4}$, atque series erit:

$$x = 1\,, \quad y = \frac{3}{4}\,, \quad x = -\frac{2}{3}\,, \quad y = \frac{3}{5}\,, \quad x = 2, [y = \infty]\,;$$

ordinem invertendo:

$$y = \frac{3}{4}\,, \quad x = 1\,, \quad y = \infty\,, \quad x = 2\,.$$

Denique, si sumatur $x = 2$ et $y = \frac{3}{5}$, valores erunt:

$$x = 2\,, \quad y = \frac{3}{5}\,, \quad x = -\frac{2}{3}\,, \quad y = \frac{3}{4}\,, \quad x = 1\,, \quad y = \infty\,,$$

invertendo autem nihil prodit. Mirum est hanc aequationem canonicam pro x alios valores non suppeditare, praeter $x = 0$, $x = 1$, $x = 2$, $x = -\frac{2}{3}$, cum tamen idem casus iam supra sit tractatus in exemplo primo, ubi adeo innumerabiles casus invenire licuit. Unde intelligitur plurimum interesse, ut aequatio canonica idonea eligatur. Praesenti scilicet casu perperam duo valores primitivi ad aequationem canonicam constituendam sunt adhibiti. Praestat enim unico valore cognito uti secundum problema I, quod operae pretium erit ostendisse.

25. Utamur ergo unico valore cognito $x = 1$, quo casu fit $V = 4 = 2^2$, sicque habebimus $a = 1$ et $f = 2$. Per primum igitur problema habebimus $P = 2$ ideoque

$$QR = 3(x^3 - 1) = 3(x - 1)\,(xx + x + 1)\,.$$

Sumamus ergo $Q = x - 1$, erit $R = 3(xx + x + 1)$, et aequatio canonica erit

$$(x - 1)yy + 4y - 3(xx + x + 1) = 0\,,$$

cuius altera forma est

$$-3xx + (yy - 3)x + 4y - yy - 3 = 0\,,$$

unde formulae directrices erunt:

$$y' = -\frac{4}{x - 1} - y \quad \text{et} \quad x' = \frac{yy - 3}{3} - x\,.$$

Ex priore autem aequatione posito $Q = 0$ fit $x = 1$, cui respondet $y = \frac{9}{4}$; at vero posito $R = 0$ nullus prodit valor rationalis. Ex altera aequatio $S = 0$ itidem nihil dat; at vero $U = 0$ dat $y = 1$, cui respondet $x = 0$ et $x = -\frac{2}{3}$; praeterea dat $y = 3$, cui respondet $x = 2$.

26. Incipiamus ab $x = 1$ et $y = \frac{9}{4}$, et reperientur sequentes valores idonei:

$$x = 1\ ,\quad y = \frac{9}{4}\ ,\quad x = -\frac{5}{16}\ ,\quad y = \frac{67}{84}\ \text{etc.}$$

Inversio autem ordinis nihil praebet ob sequens $y = \infty$. Evolvamus ergo casum primitivum $y = 1$ et $x = 0$, fietque series valorum:

$$y = 1\ ,\quad x = 0\ ,\quad y = 3\ ,\quad x = 2\ ,\quad y = -7\ ,\quad x = \frac{40}{3}\ \text{etc.}\ ,$$

ordinem autem invertendo:

$$x = 0\ ,\quad y = 1\ ,\quad x = -\frac{2}{3}\ ,\quad y = \frac{7}{5}\ ,\quad x = \frac{8}{25}\ \text{etc.}$$

In his operationibus reliqui bini casus primitivi iam continentur, quos ergo superfluum foret prosequi. Atque hic iam omnes valores supra inventi prodierunt.

27. Neque vero ob hanc circumstantiam secundum problema omni usu carere censendum est. Postquam enim pro exemplo allato sumto $P = 3x - 1$ invenimus

$$QR = 3x(x - 1)\,(x - 2)^{1})\,,$$

et sumsimus

$$Q = 3x \quad \text{et} \quad R = (x - 1)\,(x - 2)\ ;$$

unde aliquos tantum valores pro x eruere licuit. At vero productum illud $3x(x - 1)\,(x - 2)$ aliis duobus modis in duos factores discerpi potest, sumendo vel $Q = 3(x - 1)$ et $R = x(x - 2)$ vel $Q = 3(x - 2)$ et $R = x(x - 1)$; tum vero hi duo casus secundum praecepta evoluti omnes valores idoneos pro x dedissent, uti tentanti facile patebit. Ex quo generatim hoc probe tenendum erit: quoties pro QR reperitur productum ex tribus vel quatuor factoribus simplicibus constans, omnes plane resolutiones in duos factores pro Q et R sumendos in usum vocari et operationes supra traditas institui debere. Tum

1) Editio princeps: $3(x - 1)\,(x - 2)$. Correxit R. F.

enim asseverare non dubito omnes plane valores idoneos pro x repertum iri, id quod in sequentibus problematibus probe est observandum. Quamobrem progrediamur ad formulas biquadraticas sub hac forma generali

$$A + Bx + Cxx + Dx^3 + Ex^4$$

contentas ad quadratum reducendas.

PROBLEMA III

Proposita tali formula quadrato aequanda:

$$A + Bx + Cxx + Dx^3 + Ex^4 = V,$$

quae quadrâtum evadat casu $x = a$, *eam ad formam* $PP + QR$ *reducere hincque aequationem* $Qyy + 2Py - R = 0$ *formare.*

SOLUTIO

28. Sumto $x = a$ fiat $V = ff$ et supra iam ostendimus sumto $P = f$, unde fit $QR = V - ff$, hanc expressionem factorem habituram esse $x - a$; in altero ergo factore x ad tertiam potestatem ascendet, quem ergo neque pro Q neque pro R assumere licet, nisi forte factorem simplicem involvat, quem cum $x - a$ coniungere liceret. Quare hoc casu excepto negotium alio modo est instituendum, id quod facillime sequenti modo praestabitur.

29. Cum formula proposita V posito $x = a$ quadratum praebeat $= ff$, ponatur statim $x = a + t$, atque manifestum est talem formulam esse prodituram:

$$V = ff + \alpha t + \beta tt + \gamma t^3 + \delta t^4,$$

quam ergo ad speciem $PP + QR$ reduci oportet. Hunc in finem sumamus

$$P = f + \frac{\alpha t}{2f},$$

unde orietur

$$QR = V - PP = \left(\beta - \frac{\alpha\alpha}{4ff}\right) tt + \gamma t^3 + \delta t^4,$$

quae ergo forma hos continet factores:

$$tt\left(\beta - \frac{\alpha\alpha}{4ff} + \gamma t + \delta tt\right),$$

quorum alterum pro Q alterum pro R assumere licebit; perinde vero est, quinam pro Q vel pro R accipiatur. Tum autem aequatio canonica erit $Qyy + 2Py - R = 0$, unde facile altera forma ad potestates ipsius x accommodata formari poterit, quo facto constructio seriei litterarum x et y nulla amplius laborat difficultate, cum constet casus $t = 0$ sive $x = a$. Quin etiam hic, si lubuerit, loco t valor $x - a$ restitui poterit.

30. Alio autem praeterea modo aequatio canonica formari poterit ponendo

$$P = f + \frac{\alpha t}{2f} + \theta tt ,$$

sumendo θ ita, ut etiam terminus βtt tollatur, quod fit posito $\theta = \frac{\beta}{2f} - \frac{\alpha\alpha}{8f^3}$; tum autem reperietur $QR = \gamma' t^3 + \delta' t^4 = t^3(\gamma' + \delta' t)$, unde pro Q et R hi valores accipi poterunt: tt et $t(\gamma' + \delta' t)$. Reliqua vero ut ante expedientur.

EXEMPLUM

31. Sit formula proposita

$$V = 2x^4 - 1 ,$$

quae casu $x = 1$ fit quadratum, sicque erit $a = 1$ et $f = 1$; unde posito $x = 1 + t$ fiet

$$V = 1 + 8t + 12tt + 8t^3 + 2t^4 ;$$

quare, si pro priore solutione sumamus $P = 1 + 4t$, prodibit:

$$QR = V - PP = tt(2tt + 8t - 4) .$$

Sumto ergo $Q = tt$ erit $R = 2tt + 8t - 4$, quocirca aequatio canonica erit

$$ttyy + 2(1 + 4t)y - (2tt + 8t - 4) [= 0] ,$$

cuius altera forma ad t instructa erit

$$(yy - 2)tt + (8y - 8)t + 2y + 4 [= 0] ;$$

hincque formulae nostrae directrices erunt:

$$y' = -\frac{2(1 + 4t)}{tt} - y \quad \text{et} \quad t' = -\frac{8(y - 1)}{yy - 2} - t .$$

32. Nunc vero valorem primitivum habemus $t = 0$, cui respondet $y = -2$; praeterea vero aequatio $U = 0$ etiam dat $y = -2$, ita ut hi duo valores primitivi conveniant. Inchoemus ergo nostram seriem a terminis $x = 0$ et $y = [-]2$, eaque erit

$$t = 0\,, \quad y = -2\,, \quad t = 12\,, \quad y = \frac{95}{72} \quad \text{etc.}\,,$$

hinc ergo valores ipsius x erunt $x = 1$ et $x = 13$.

33. Applicemus etiam alteram solutionem et statuamus

$$P = 1 + 4t - 2tt\,,$$

fietque

$$QR = V - PP = tt(24t - 2tt)\,,$$

quia igitur alter factor necessario est tt, sumamus $Q = tt$ et $R = 2t(12 - t)$, sicque aequatio canonica erit:

$$ttyy + 2(1 + 4t - 2tt)y - 2t(12 - t) = 0\,,$$

cuius altera igitur forma ita se habebit:

$$(yy - 4y + 2)tt + 8(y - 3)t + 2y = 0\,,$$

unde formantur directrices, quae erunt:

$$y' = -\frac{2(1 + 4t - 2tt)}{tt} - y\,, \quad t' = -\frac{8(y - 3)}{yy - 4y + 2} - t\,.$$

34. Quod iam ad valores primitivos attinet, ex priore aequationis canonicae forma $Q = 0$ dat $t = 0$, cui respondet $y = 0$; aequatio vero $R = 0$ dat $t = 12$, cui respondet $y = 0$. Ex posteriore vero forma aequatio $S = 0$ nullum dat valorem rationalem; et $U = 0$ dat $y = 0$, qui iam in praecedentibus continetur. Incipiamus ergo seriem a $t = 0$ et $y = 0$ et sequens terminus erit $t = 12$; et quia alter primitivus $t = 12$ iam occurrit, pro eo novam operationem instituere non est opus.

PROBLEMA IV

Proposita formula biquadratica:

$$V = A + Bx + Cxx + Dx^3 + Ex^4 ,$$

si duo dentur casus $x = a$ et $x = b$, quibus ea fiat quadratum, eam reducere ad formam $V = PP + QR$ hincque aequationem canonicam constituere.

SOLUTIO

35. Pro casu $x = a$ fiat $V = ff$, et pro altero casu $x = b$ fiat $V = gg$, atque nunc pro P talis formula requiritur, ut QR obtineat factorem $(x - a)\,(x - b)$. Quamobrem, si ponatur vel $x = a$ vel $x = b$, fieri debet $PP = V$, ideoque $P = \sqrt{V}$. Hunc in finem statuamus $P = p + qx$, et, quia pro casu $x = a$ fit $\sqrt{V} = f$, habebitur haec aequatio $p + qa = f$; pro altero vero casu $x = b$ fiet $p + bq = g$; ubi probe notandum est litteras f et g tam negative quam positive accipi posse. At vero ex istis binis aequalitatibus colligitur:

$$p = \frac{bf - ag}{b - a} \quad \text{et} \quad q = \frac{g - f}{b - a} .$$

36. Ex his igitur valoribus productum $QR = V - PP$ certo habebit factorem $(x - a)\,(x - b)$. Sit igitur

$$QR = M(x - a)\,(x - b) ,$$

ac, si M nullos contineat factores rationales, necessario statui debebit

$$Q = (x - a)\,(x - b) \quad \text{et} \quad R = M ;$$

at si M etiam involvat duos factores reales, puta $M = (x - \zeta)\,(x - \eta)$, uterque vel cum $x - a$ vel cum $x - b$ coniungi poterit, unde duo novae positiones oriuntur sicque tres aequationes canonicae formari poterunt.

EXEMPLUM

37. Sit

$$V = 1 + 7xx + x^4 ,$$

quae forma casu $x = 0$ fit 1, casu vero $x = 1$ fit 9. Erit ergo $a = 0$, $f = \pm 1$; deinde $b = 1$ et $g = \pm 3$, unde aliud discrimen non nascitur, nisi ex aequalitate et inaequalitate signorum. Sint igitur signa aequalia $f = 1$ et $g = 3$, fiet nostra formula

$$P = p + qx = 1 + 2x .$$

Pro casu vero $f = -1$ et $g = 3$ fit $P = p + qx = -1 + 4x$; utrumque ergo casum evolvamus.

38. Pro priore erit

$$QR = V - PP = x^4 + 3xx - 4x \quad \text{sive} \quad QR = x(x-1)(xx + x + 4) ,$$

ubi posterior factor nullas continet radices reales. Fiat ergo

$$Q = x(x-1) \quad \text{et} \quad R = xx + x + 4 ,$$

et aequatio canonica erit:

$$x(x-1)yy + 2(1 + 2x)y - (xx + x + 4) = 0 ,$$

cuius altera forma est:

$$(yy - 1)xx + (4y - yy - 1)x + 2y - 4 = 0 ,$$

unde hae formulae directrices oriuntur:

$$y' = -\frac{2(1 + 2x)}{x(x-1)} - y , \quad x' = \frac{yy - 4y + 1}{yy - 1} - x .$$

39. Ex priore forma aequationis canonicae aequatio $Q = 0$ praebet $x = 0$, cui respondet $y = 2$; deinde etiam praebet $x = 1$, cui respondet $y = 1$. Ex altera autem forma aequatio $S = 0$ fit vel $y = 1$, cui respondet $x = 1$, vel $y = -1$, cui respondet $x = -1$. Denique ex aequatione $U = 0$ fit $y = 2$, cui respondet $x = 0$ et $x = -1$. Quia autem in formula proposita tantum potestates pares ipsius x occurrunt, perinde est, sive x habeat valorem negativum sive positivum, duo tantum valores primitivi relinquuntur $x = 0$ et $x = 1$, unde seriem quaeramus pro $x = 0$ et $y = 2$, quae erit

$$x = 0 , \quad y = 2 , \quad x = -1 , [y = -1] , \quad x = \infty \text{ [1]} ;$$

1) Editio princeps: $y = \infty$. Correxit R. F.

ordinem autem invertendo statim ad infinitum deducimur. Quare incipiamus ab $x = 1$ et $y = 1$, unde series oritur

$$x = 1\,, \quad y = 1\,, \quad x = \infty\,,$$

atque etiam invertendo nihil oritur. Unde concludere licet formulam propositam quadratum fieri non posse praeter binos casus alias cognitos $x = 0$ et $x = 1$.

40. Consideremus interim etiam casum, quo $P = -1 + 4x$, eritque

$$QR = x^4 - 9xx + 8x = x(x-1)\,(xx\,[+\,x] - 8)\,,$$

quamobrem sumamus $Q = x(x-1)$ et $R = xx\,[+\,x] - 8$, et aequatio canonica erit:

$$x(x-1)yy + 2(4x-1)y - (xx + x - 8) = 0\,,$$

cuius altera forma ita se habet:

$$(yy-1)xx + (8y - yy - 1)x - 2y + 8 = 0\,.$$

Formulae autem directrices erunt:

$$y' = -\frac{2(4x-1)}{x(x-1)} - y \quad \text{et} \quad x' = -\frac{(8y - yy - 1)}{yy - 1} - x\,.$$

41. Hic iterum habemus valores primitivos $x = 0$ et $x = 1$, quorum priori respondet $y = 4$, posteriori vero $y = [-]\,1$. Ex altera forma prodit vel $y = +1$ vel $y = -1$, quorum illi respondet $x = -1$, huic vero $x = +1$. Denique ex $U = 0$ fit $y = 4$, cui respondet $x = 0$ et $x = -1$. Incipiamus a terminis $x = 0$ et $y = 4$, series valorum erit

$$x = 0, \quad y = 4, \quad x = -1, \quad y = 1, \quad x = \infty\,.$$

Sumamus $x = 1$ et $y = -1$[1]), fiet series

$$x = 1\,, \quad y = [-]\,1\,, \quad x = \infty\,.$$

Hic iam reliqui casus omnes continentur, unde certum manet alios praeterea nullos dari valores idoneos.

1) Editio princeps: $y = -\frac{7}{6}$. Correxit A. M.

PROBLEMA V

Si in formula proposita quadrato aequanda:

$$V = A + Bx + Cxx + Dx^3 + Ex^4$$

tres constent casus, quibus ea fit quadratum, scilicet $x = a$, $x = b$, $x = c$, *quibus fiat* $V = ff$, $V = gg$, $V = hh$, *eam reducere ad formam* $PP + QR$ *indeque aequationem canonicam formare.*

SOLUTIO

42. Hic igitur quantitatem P ita definire oportet, ut productum $QR = V - PP$ obtineat factores $(x - a)(x - b)(x - c)$; quamobrem necesse est, ut casibus $x = a$, $x = b$, $x = c$ fiat $QR = 0$ ideoque $PP = V$ et $P = \sqrt{V}$. Hunc in finem statuatur $P = p + qx + rxx$, et, quia [casu] $x = a$ fit $V = ff$ ideoque $\sqrt{V} = \pm f$, casu vero $x = b$ erit $\sqrt{V} = \pm g$ et pro casu $x = c$ habebitur $\sqrt{V} = \pm h$; unde [sic!] nascuntur hae tres aequationes:

$$\text{I.} \quad \pm f = p + qa + raa,$$
$$\text{II.} \quad \pm g = p + qb + rbb,$$
$$\text{III.} \quad \pm h = p + qc + rcc.$$

Ex his iam tribus aequationibus eliciantur valores litterarum p, q, r, id quod pluribus modis fieri poterit ob signa ambigua radicum f, g, h; quibus inventis colligatur valor producti $QR = V - PP$, quod cum iam habeat tres factores simplices $x - a$, $x - b$, $x - c$, quia non ultra quartam potestatem ipsius x ascendit, necesse est, ut etiam quartus factor sit simplex, qui ergo novum valorem pro x suppeditabit.

43. Quoniam igitur QR quatuor factores simplices continet, producta binorum pro litteris Q et R accipi poterunt; perinde autem est, utrum pro Q vel R assumatur, unde tres casus oriri poterunt, prout primus factor $x - a$ vel cum secundo $x - b$ vel cum tertio $x - c$ vel cum quarto modo invento combinetur. Quacunque autem combinatione utamur, posito $V = (P + Qy)^2$ ob $V = PP + QR$ orietur ista aequatio canonica $Qyy + 2Py - R = 0$, cuius deinde alteram formam $Sxx + Tx + U = 0$ elicere possumus, quo

facto constitutis formulis directricibus $y + y' = -\frac{2P}{Q}$ vel $yy' = -\frac{R}{Q}$, tum vero $x + x' = -\frac{T}{S}$ sive $xx' = \frac{U}{S}$, innumerabiles alios valores idoneos pro x investigare licebit, nisi forte numerus horum valorum ob indolem formulae propositae fuerit finitus.

44. Si ex tribus aequationibus pro litteris p, q, r datis has litteras in genere determinare vellemus, in formulas valde complexas incideremus, cum tamen quovis casu oblato negotium facillime absolvatur. Quamobrem usum huius solutionis in exemplo speciali ostendamus.

EXEMPLUM

45. Proposita sit ista formula

$$V = 1 + 3x^4 ,$$

quae his tribus casibus $x = 0$, $x = 1$, $x = 2$ evadit quadratum; scilicet casu $x = 0$ fit $V = 1$, casu vero $x = 1$ fit $V = 4$ et casu $x = 2$ fit $V = 49$. Quamobrem posito $P = p + qx + rxx$ orientur tres sequentes aequationes:

1. Si $x = 0$, erit $\pm 1 = p$,
2. si $x = 1$, erit $\pm 2 = p + q + r$,
3. si $x = 2$, erit $\pm 7 = p + 2q + 4r$.

Sumamus autem omnes tres radices positive, eritque $p = 1$, duae reliquae vero aequationes erunt $1 = q + r$ et $6 = 2q + 4r$, unde eruitur $r = 2$ et $q = -1$, sicque habebimus

$$P = 1 - x + 2xx .$$

46. Hinc igitur reperiemus $QR = V - PP$, hoc est:

$$QR = -x^4 + 4x^3 - 5xx + 2x = -x(x-1)(x-2)(x-1) ,$$

quamobrem sumamus $Q = (x-1)^2$ et $R = -x(x-2)$, unde ob $P = 1 - x + 2xx$ habebitur aequatio canonica:

$$(x-1)^2yy + 2(1 - x + 2xx)y + x(x-2) = 0 ,$$

cuius altera forma erit:

$$(yy + 4y + 1)xx - 2(yy + y + 1)x + y(y + 2) = 0 ,$$

unde formulae directrices oriuntur:

$$y' = -\frac{2(1 - x + 2xx)}{(x-1)^2} - y \quad \text{et} \quad y' = \frac{x(x-2)}{(x-1)^2 y} ,$$

$$x' = \frac{2(yy + y + 1)}{yy + 4y + 1} - x \quad \text{et} \quad x' = \frac{y(y+2)}{(yy + 4y + 1)x} .$$

47. Incipiamus a valore cognito $x = 0$, cui respondet $y = 0$, hincque series valorum erit:

$$x = 0 , \quad y = 0 , \quad x = 2 , \quad y = -14 , \quad x = \frac{28}{47} \text{ etc.}$$

Invertendo autem ordinem prodeunt sequentes valores:

$$y = 0 , \quad x = 0 , \quad y = -2 , \quad x = -2 , \quad y = -\frac{4}{9} , \quad x = -\frac{28}{47} \text{ etc.}$$

Sit nunc $x = 1$, cui respondet $y = \frac{1}{4}$, hinc series ista

$$x = 1 , \quad y = \frac{1}{4} , \quad x = \frac{3}{11} \text{ etc.}$$

At invertendo haec

$$y = \frac{1}{4} , \quad x = 1 , \quad y = \infty .$$

Superfluum foret a tertio valore $x = 2$ incipere, quia in praecedentibus iam continetur.

48. Sumamus nunc $Q = x(x - 1)$ eritque $R = -(x - 1)(x - 2)$, unde aequatio canonica erit:

$$x(x - 1)yy + 2(1 - x + 2xx)y + (x - 1)(x - 2) = 0 ,$$

cuius altera forma est:

$$(yy + 4y + 1)xx - (yy + 2y + 3)x + 2(y + 1) = 0 .$$

Formulae ergo directrices erunt:

$$y' = -\frac{2(1-x+2xx)}{x(x-1)} - y \quad \text{sive} \quad y' = \frac{x-2}{xy},$$

$$x' = \frac{yy+2y+3}{yy+4y+1} - x \quad \text{sive} \quad x' = \frac{2(y+1)}{(yy+4y+1)x}.$$

49. Incipiamus iterum ab $x = 0$, cui hic respondet $y = -1$, unde valores idonei hinc nati:

$$x=0,\ y=-1,\ x=-1,\ y=-3,\ x=-2,\ y=-\frac{2}{3},\ x=\frac{3}{11} \text{ etc.}$$

tum vero invertendo fiet

$$y=-1,\quad x=0,\quad y=\infty.$$

Sit porro $x = 1$, cui respondet $y = 0$, unde sequentes deducuntur valores:

$$x=1,\quad y=0,\quad x=2,\quad y=-7,\quad x=-\frac{3}{11},\quad y=-\frac{25}{21}\ ^{1}) \text{ etc.}$$

50. Simili modo etiam reliqui casus aequationis canonicae tractari poterunt, ubi una quaepiam radicum f, g, h sumitur negative, unde alii valores pro P oriuntur, verum his uberius evolvendis non immoror, cum, quae hactenus sunt allata, abunde sufficiant ad utilitatem et praestantiam huius novae methodi declarandam.

---

2) Editio princeps: $\frac{25}{11}$. Correxit A. M.

[TRACTATUS DE NUMERORUM DOCTRINA CAPITA SEDECIM QUAE SUPERSUNT] [1)]

Commentatio 792 indicis ENESTROEMIANI
Prima editio: Commentationes arithmeticae 2, 1849, p. 503—575
Haec editio congruit cum manuscripto manu Euleri facto et academiae scientiarum Petropolitanae relicto

CAPUT 1
DE COMPOSITIONE NUMERORUM

1. (Definitio.) *Numerus* est multitudo unitatum.

2. (Corollarium.) Quilibet ergo numerus indicat, quot unitates in eo contineantur.

3. (Corollarium.) Ab unitate incipiendo numeri sunt 1, 2, 3, 4, 5, 6 etc., quorum quisque praecedentem unitate superat.

4. (Corollarium.) Quia quemque numerum unitate augere licet, series numerorum in infinitum progreditur.

5. (Corollarium.) Cum primus, scilicet, unitas praecedentem etiam unitate superet, praecedens nihilum 0 sit, necesse est.

6. (Scholion.) Hic tantum de numeris integris sermo est, ad quos definitio est restricta, unde fractos multoque magis surdos hinc excludi oportet.

7. Si numerus quicunque sit a, erunt eum sequentes $a + 1$, $a + 2$, $a + 3$, $a + 4$ etc., quorum primus $a + 1$ datum a superat unitate, secundus $a + 2$ duabus unitatibus, tertius $a + 3$ tribus etc.

8. Simili modo proposito numero a antecedentes erunt $a - 1$, $a - 2$, $a - 3$, $a - 4$ etc., quorum primus $a - 1$ a dato a unitate deficit, secundus $a - 2$ duabus unitatibus, tertius $a - 3$ tribus et ita porro.

9. Si numero a tot unitates addantur, quot numerus b continet, oritur $a + b$; sin autem a numero a tot unitates auferantur, quot numerus b continet, oritur $a - b$; illo casu numerus b numero a additus, hoc vero ab eo subtractus dicitur.

1) Hic titulus a primis editoribus additus est. R. F.

10. Si idem numerus a sibi ipsi addatur, oritur eius duplum $a + a$, quod ita scribitur $2a$; si idem denuo addatur, prodit triplum $3a$; tum eodem numero a insuper addito eius quadruplum $4a$ et ita porro, quae in genere vocantur eius multipla.

11. Multipla ergo numeri a sunt $2a$, $3a$, $4a$, $5a$ etc., quorum quodque praecedens superat ipso numero a; horumque respectu ipse numerus a simplum vocatur.

12. Si a esset unitas, eius multipla omnes plane numeros praeberent; at si a non est unitas sed multitudo unitatum, eius multipla non omnes numeros praebebunt; hocque casu dabuntur numeri, qui non sunt multipla ipsius a.

13. Cum multipla ipsius a sint $2a$, $3a$, $4a$, $5a$ etc., inter ea primo non reperiuntur omnes numeri ipso a minores, qui sunt 1, 2, 3,..., $(a - 1)$; totidemque non-multipla occurrent a quovis multiplo usque ad sequens.

14. Si ergo fuerit α numerus minor quam a, tum neque α neque hi numeri $a + \alpha$, $2a + \alpha$, $3a + \alpha$, $4a + \alpha$ etc. inter multipla ipsius a reperiuntur.

15. Quia ob $\alpha < a$ est $2a - \alpha$ minus quam $2a$ simulque maius quam a, numerus $2a - \alpha$ non erit multiplum ipsius a, neque ullus horum numerorum $a - \alpha$, $2a - \alpha$, $3a - \alpha$, $4a - \alpha$ etc. inter multipla ipsius a continetur.

16. Proposito ergo quocunque numero b, qui non sit multiplum ipsius a, is vel ipso a erit minor, vel ita superabit aliquod eius multiplum, ut tamen minor sit multiplo sequente.

17. Cum multipla binarii sint 2, 4, 6, 8, 10 etc. (eius simplo non excluso), numeri reliqui ab his unitate differunt. Simili modo ob ternarii multipla 3, 6, 9, 12, 15 etc. reliqui numeri ab his vel unitate vel binario distant.

18. Duplum cuiusque numeri a, scilicet $2a$, est etiam multiplum binarii. Cum enim a sit multitudo unitatum $1 + 1 + 1 + 1$ etc., duplicatio ita repraesentetur, unde additione prodit:

$$\begin{aligned} a &= 1 + 1 + 1 + 1 \text{ etc.,} \\ a &= 1 + 1 + 1 + 1 \text{ etc.,} \\ 2a &= 2 + 2 + 2 + 2 \text{ etc.} \end{aligned}$$

19. Vel cum numerus a sit multitudo unitatum, numerus a duplicabitur singulis unitatibus bis sumendis, unde oritur multitudo binariorum. Ex quo patet duplum $2a$ toties continere binarium, quoties a continet unitatem.

20. Simili modo triplum $3a$ toties continebit ternarium, quoties ipse numerus a unitatem, eritque itaque $3a$ multiplum ternarii, quod etiam de omnibus multiplis est intelligendum.

21. Index[1]) multipli vocatur numerus indicans, quoties multiplum in se contineat simplum, ita index dupli est binarius, tripli ternarius, quadrupli quaternarius etc.

22. Si numerus a toties sumatur, quot numerus n continet unitates, multipli inde orti index est n; ipsum autem multiplum hoc ita exprimitur na, ita ut na denotet multiplum ipsius a, cuius index sit n.

23. Tale ergo multiplum na ipsius a est etiam multiplum indicis n, quandoquidem toties in se continet indicem, quoties ipse numerus a continet unitatem.

24. Hinc ergo patet multiplum numeri a, cuius index sit n, congruere cum eo multiplo numeri n, cuius index sit a; quare, cum illud multiplum per na, hoc vero per an exprimatur, erit $na = an$.

25. Cum in quovis multiplo na tam numerus a, cuius multiplum sumitur, quam index multipli n inter se permutari queant, hi duo numeri a et n sine discrimine factores appellantur, multiplo autem ipsi na nomen producti seu facti indi solet.

26. Quemadmodum quisque numerus est multiplum unitatis, cuius ipse est index, ita etiam est sui ipsius simplum indice existente unitate. In posterum ergo tam multipla unitatis quam simpla cuiusque numeri a denominatione multiplorum segregabimus.

27. Multipla ergo nobis erunt eiusmodi numeri, qui cuiuspiam numeri praeter unitatem sunt multipla (excluso simplo); constabunt ergo duobus factoribus, quorum alter alterius respectu tamquam index spectari potest.

28. Factum ergo ab, cuius factores sunt a et b, est multiplum tam ipsius a quam ipsius b; quatenus est multiplum ipsius a, index est b, quatenus autem est multiplum ipsius b, index est a.

29. Multipla huius facti ab simul erunt multipla tam ipsius a quam ipsius b. Sit nab tale multiplum, cuius index sit n, et, quia etiam est multiplum ipsius n, erit multiplum uniuscuiusque horum numerorum n, a et b.

30. Hinc patet etiam in facto ex tribus factoribus constante tres factores inter se esse permutabiles, atque tale factum abc non solum esse multiplum singulorum a, b, c, sed etiam factorum ex binis ab, ac, bc.

31. Si in serie numerorum 1, 2, 3, 4, 5, 6, 7 etc. omnia multipla deleantur, reliqui numeri non erunt multipla ullius numeri (quandoquidem simpla excludimus); hique numeri vocantur simplices vel primi.

---

1) Index hic idem significat ac coefficiens. R. F.

32. Deletis, scilicet, multiplis binarii 4, 6, 8, 10, 12 etc. restat haec series 1, 2, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21 etc. Hinc porro extinguantur multipla ternarii 6, 9, 12, 15, 18, 21 etc., quae quidem adhuc adsunt, et restat 1, 2, 3, 5, 7, 11, 13, 17, 19, 23 etc.; ita relinquentur tandem numeri primi

1, 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59 etc.[1])

33. Si ergo p sit numerus primus, is neque inter multipla binarii neque inter multipla cuiusquam alius numeri occurrit, neque ergo huiusmodi facto ab ullo modo exhiberi potest, nisi sit vel $a = 1$ vel $b = 1$, quos autem casus exclusimus (paragraphus 26).

34. Omnes numeri, qui non sunt primi, vocantur compositi; unde patet omnes numeros compositos esse multipla aliorum numerorum minorum; qui cum iterum sint primi vel multipla aliorum denuo minorum, multipla autem cuiusvis producti sint simul multipla singulorum eius factorum, sequitur omnes numeros compositos tandem reduci ad multipla numerorum primorum.

35. Omnis ergo numerus vel est primus vel multiplum cuiuspiam numeri primi; quo posteriori casu, cum numerus sit compositus, omnis numerus compositus exhiberi potest producto, cuius singuli factores sint numeri primi.

36. Inter numeros compositos primum occurrunt ii, qui constant duobus tantum factoribus primis. Veluti si p et q denotent duos numeros primos quoscunque, productum pq in genere exhibebit eiusmodi numeros compositos primae speciei, qui duobus tantum constant factoribus primis.

37. Talis ergo numerus compositus pq erit tam multiplum numeri q indice existente p, quam multiplum ipsius p indice existente q, neque vero ullius alius numeri erit multiplum. Si enim esset multiplum alius cuiuspiam numeri a indice existente b, hi numeri a et b eius essent factores contra hypothesin.[2])

38. Huiusmodi autem productum pa, cuius quidem factor p est primus, alter vero a compositus factores habens α, β, γ etc., non solum erit multiplum numerorum p et a, sed etiam inter multipla numerorum α, β, γ etc. occurret.

39. Post numeros compositos duobus factoribus primis constantes considerandi veniunt ii, qui tribus factoribus primis constant, cuius ergo speciei forma est pqr denotantibus p, q, r numeros primos quoscunque.

40. Tum vero sequentur numeri compositi, qui sunt producta ex quaternis numeris primis, quorum forma erit $pqrs$. Sequentes autem species erunt producta vel ex quinis vel senis vel septenis etc. numeris primis constantia.

1) EULERUS admittit unitatem inter numeros primos contra conventionem nostram. Vide paragraphum 62. R. F.

2) Demonstratio numeros a et b nunquam factores producti pq fieri posse deest. R. F.

41. Hinc omnes numeri ita in classes distribuentur, ut prima contineat omnes numeros primos singulos, secunda producta ex binis primis, tertia producta ex ternis primis, quarta ex quaternis, quinta ex quinis et ita porro.

42. Post unitatem ergo numeri primae classis seu primi centenario non maiores sunt: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

43. Numeri vero secundae classis centenario minores sunt:

$2 \cdot 2 = 4$
$2 \cdot 3 = 6$
$2 \cdot 5 = 10$
$2 \cdot 7 = 14$
$2 \cdot 11 = 22$
$2 \cdot 13 = 26$
$2 \cdot 17 = 34$
$2 \cdot 19 = 38$
$2 \cdot 23 = 46$
$2 \cdot 29 = 58$
$2 \cdot 31 = 62$
$2 \cdot 37 = 74$
$2 \cdot 41 = 82$
$2 \cdot 43 = 86$
$2 \cdot 47 = 94$

$3 \cdot 3 = 9$
$3 \cdot 5 = 15$
$3 \cdot 7 = 21$
$3 \cdot 11 = 33$
$3 \cdot 13 = 39$
$3 \cdot 17 = 51$
$3 \cdot 19 = 57$
$3 \cdot 23 = 69$
$3 \cdot 29 = 87$
$3 \cdot 31 = 93$

$5 \cdot 5 = 25$
$5 \cdot 7 = 35$
$5 \cdot 11 = 55$
$5 \cdot 13 = 65$
$5 \cdot 17 = 85$
$5 \cdot 19 = 95$

$7 \cdot 7 = 49$
$7 \cdot 11 = 77$
$7 \cdot 13 = 91$

44. Tum vero numeri tertiae classis centenario inferiores sunt:

$2 \cdot 2 \cdot 2 = 8$
$2 \cdot 2 \cdot 3 = 12$
$2 \cdot 2 \cdot 5 = 20$
$2 \cdot 2 \cdot 7 = 28$
$2 \cdot 2 \cdot 11 = 44$
$2 \cdot 2 \cdot 13 = 52$
$2 \cdot 2 \cdot 17 = 68$
$2 \cdot 2 \cdot 19 = 76$
$2 \cdot 2 \cdot 23 = 92$

$2 \cdot 3 \cdot 3 = 18$
$2 \cdot 3 \cdot 5 = 30$
$2 \cdot 3 \cdot 7 = 42$
$2 \cdot 3 \cdot 11 = 66$
$2 \cdot 3 \cdot 13 = 78$

$2 \cdot 5 \cdot 5 = 50$
$2 \cdot 5 \cdot 7 = 70$

$2 \cdot 7 \cdot 7 = 98$

$3 \cdot 3 \cdot 3 = 27$
$3 \cdot 3 \cdot 5 = 45$
$3 \cdot 3 \cdot 7 = 63$
$3 \cdot 3 \cdot 11 = 99$

$3 \cdot 5 \cdot 5 = 75$

45. Quartae autem classis numeri infra 100 sunt:

$2 \cdot 2 \cdot 2 \cdot 2 = 16$	$2 \cdot 2 \cdot 3 \cdot 3 = 36$	$2 \cdot 3 \cdot 3 \cdot 3 = 54$
$2 \cdot 2 \cdot 2 \cdot 3 = 24$	$2 \cdot 2 \cdot 3 \cdot 5 = 60$	$2 \cdot 3 \cdot 3 \cdot 5 = 90$
$2 \cdot 2 \cdot 2 \cdot 5 = 40$	$2 \cdot 2 \cdot 3 \cdot 7 = 84$	
$2 \cdot 2 \cdot 2 \cdot 7 = 56$		$3 \cdot 3 \cdot 3 \cdot 3 = 81$
$2 \cdot 2 \cdot 2 \cdot 11 = 88$	$2 \cdot 2 \cdot 5 \cdot 5 = 100$	

46. Quintae classis numeri centenario non maiores sunt:

$2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 32$	$2 \cdot 2 \cdot 2 \cdot 2 \cdot 5 = 80$
$2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 = 48$	$2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 = 72$

47. In sexta classe huiusmodi numeri duo occurrunt:

$$2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 64 \qquad 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 = 96$$

Sequentes autem classes nullos continent numeros centenario minores.

48. Cuiusque classis numeri charactere peculiari distinguuntur a numeris aliarum classium, et quilibet numerus ita ad certam quandam classem pertinet, ut non simul ad ullam aliam referri possit.

49. Quodsi ergo p, q, r, s etc. denotent numeros primos, formae harum classium ita exhiberi possunt:

Forma classis I ... p,
classis II ... pq,
classis III ... pqr,
classis IV ... $pqrs$,
classis V ... $pqrst$,
classis VI ... $pqrstu$,
etc.

50. Quoniam in his classibus omnes numeri continentur, si seriem numerorum naturalem 1, 2, 3, 4 etc. usque ad n continuemus, ita ut multitudo numerorum sit $= n$, ac multitudo numerorum primorum in hac serie contentorum sit $= \alpha$, multitudo numerorum secundae classis $= \beta$, tertiae classis $= \gamma$, quartae $= \delta$ et ita porro, necesse est, sit $\alpha + \beta + \gamma + \delta +$ etc. $= n$. Ita vidimus, si sumatur $n = 100$, fore $\alpha = 26$ (unitate inter numeros primos comprehensa), $\beta = 34$, $\gamma = 22$, $\delta = 12$, $\varepsilon = 4$, $\zeta = 2$, $\eta = 0$, estque utique $26 + 34 + 22 + 12 + 4 + 2 = 100$.

51. Si n denotet potestatem binarii, multitudo numerorum cuiusque classis ad numerum n usque ita se habebit:

numerus n	*multitudo numerorum*									
	α	β	γ	δ	ε	ζ	η	ϑ	ι	$\varkappa$
2	2									
4	3	1								
8	5	2	1							
16	7	6	2	1						
32	12	10	7	2	1					
64	19	22	13	7	2	1				
128	32	42	30	14	7	2	1			
256	55	82	60	34	15	7	2	1		
512	98	157	125	71	36	15	7	2	1	
1024	173	304	256	152	77	37	15	7	2	1

52. Si indolem numerorum attentius contemplemur, facile percipiemus ab initio numeros primos frequentissime occurrere, compositos autem rarissime interspersos esse debere. Quo longius autem progrediamur, eo plures reperientur numeri compositi, contra autem pauciores primi.

53. Deinde etiam notari oportet in progressione numerorum primorum 1, 2, 3, 5, 7, 11, 13, 17, 19 etc. nullum plane ordinem apparere, unde lex huius progressionis definiri possit; etiamsi in genere certum sit, quo longius progrediamur, minus frequentes eos esse debere.

54. Tabulae habentur, in quibus numeri primi secundum centurias sunt dispositi[1]); atque in prima centuria ab 1 ad 100 sunt 26[2]) numeri primi, in secunda 21, in sequentibus vero pauciores; neque tamen eorum multitudo continuo minuitur, sed potius admodum irregulariter modo crescit, modo decrescit. Sic a 200 ad 300 occurrunt 16 numeri primi, at a 400 ad 500 sunt 17, totidemque adhuc a 1400 ad 1500. Porro a 79700 ad 79800 tres tantum reperiuntur numeri primi. Hoc tamen non obstante in centuria a 90000 ad 90100 adhuc 13 numeri primi deprehenduntur.

1) Vide notam 3), p. 104, vol. 2 seriei I et praefationem vol. 3 seriei I, p. X et sequentes. R. F.
2) Unitate inclusa. R. F.

CAPUT 2
DE DIVISORIBUS NUMERORUM

55. Quatenus quidam numerus est multiplum alius numeri, eatenus hic illius dicitur divisor, et index multiplicitatis vocari solet quotus ex divisione ortus.

56. Ita si numerus N fuerit multiplum ipsius a indice existente n, ut sit $N = na$, numerus a erit divisor numeri N, et index n praebebit quotum. Scilicet, si numerus $N = na$ per a dividatur, quotus erit n.

57. Cum numeri n et a inter se sint permutabiles, hocque respectu factores appellentur, numerus $N = na$ etiam divisorem habebit n, quotusque tum erit a. In genere ergo divisor per quotum multiplicatus ipsum numerum divisum reproducit.

58. Cum quilibet numerus sit sui ipsius simplum, unitas cuiusque numeri est divisor, ipseque numerus quotus. Tum vero quilibet numerus est sui ipsius divisor quoto existente unitate.

59. Quilibet ergo numerus N primo unitatem pro divisore habet, eritque tum ipse numerus N quotus. Deinde etiam quilibet numerus N se ipsum habet pro divisore quoto existente unitate.

60. Nullus numerus alios habet divisores, nisi quorum est multiplum (simplo ex idea multipli hic non excluso). Si enim alium haberet divisorem, eo ipso huius futurus esset multiplum quoto praebente indicem multipli.

61. Cum igitur numerus primus nullius alius numeri praeter unitatem sit multiplum, numerus primus alios non habet divisores praeter unitatem et se ipsum. Scilicet, si p denotet numerum primum, eius divisores erunt 1 et p, neque praeter hos ullos habet alios.

62. Numeri ergo primi seu primae classis duos tantum habent divisores excepta unitate, quippe quae unicum habet; quam ob causam etiam unitas numeris primis non accenseri solet.

63. Numeri secundae classis, qui constant duobus factoribus primis pq, quia sunt multipla utriusque, praeter divisores 1 et pq etiam divisores habent p et q, ita ut omnes eorum divisores sint 1, p, q et pq.

64. Casus autem hic seorsim est perpendendus, quo ambo factores p et q sunt inter se aequales, quoniam eundem numerum non bis inter divisores numerare licet. Hinc numeri pp, qui sunt quadrata numerorum primorum, tres tantum habent divisores 1, p et pp.

65. Hanc ob causam numeros secundae classis in duas species subdividi

convenit, quarum prior continet numeros formae pp et divisores habet tres: 1, p, pp; altera vero species continet numeros formae pq denotantibus litteris p, q numeros primos diversos. Huiusque speciei numeri habebunt quaternos divisores: 1, p, q, pq .

66. Simili modo classis tertia subdividi debet in tres species, quarum formae sunt p^3, p^2q, pqr, siquidem p, q, r denotent numeros primos diversos; vel enim omnes tres factores sunt aequales vel bini tantum vel omnes tres inaequales.

67. Pro tertia autem classe numerorum

speciei primae p^3 divisores erunt quatuor: 1, p, p^2, p^3,
„ secundae p^2q „ „ sex: 1, p, q, p^2, pq, p^2q,
„ tertiae pqr „ „ octo: 1, p, q, r, pq, pr, qr, pqr,

neque praeterea alii divisores locum habere possunt.

68. Classis quarta, quae numeros quatuor factoribus primis constantes continet, prout horum factorum [nulli vel] bini vel tres vel omnes quatuor fuerint aequales, subdividenda est in quinque species, quarum formae sint I. p^4, II. p^3q, III. p^2q^2, IV. p^2qr, V. $pqrs$.

69. Iam facile erit omnes divisores cuiusque speciei in classe quarta enumerare:

Speciei	divisores erunt	
I. p^4	quinque:	1, p, p^2, p^3, p^4,
II. p^3q	octo:	1, p, q, p^2, pq, p^3, p^2q, p^3q,
III. p^2q^2	novem:	1, p, q, p^2, pq, q^2, p^2q, pq^2, p^2q^2,
IV. p^2qr	duodecim:	1, p, q, r, p^2, pq, pr, qr, p^2q, p^2r, pqr, p^2qr,
V. $pqrs$	sedecim:	1, p, q, r, s, pq, pr, ps, qr, qs, rs, pqr, pqs, prs, qrs, $pqrs$.

70. In classe quinta, quae numeros ex quinque factoribus primis com positos complectitur, ob aequalitatem aliquot factorum sequentes species constitui oportebit:

I. p^5, II. p^4q, III. p^3q^2, IV. p^3qr, V. p^2q^2r, VI. p^2qrs, VII. $pqrst$.

71. Tum vero singularum harum specierum divisores ita enumerabuntur:

Speciei		divisores erunt
I. p^5	sex:	$1, p, p^2, p^3, p^4, p^5$.
II. p^4q	decem:	$1, p, q, p^2, pq, p^3, p^2q, p^4, p^3q, p^4q$.
III. p^3q^2	duodecim:	$1, p, q, p^2, pq, q^2, p^3, p^2q, pq^2, p^3q, p^2q^2, p^3q^2$.
IV. p^3qr	sedecim:	$1, p, q, r, p^2, pq, pr, qr, p^3, p^2q, p^2r, pqr, p^3q, p^3r, p^2qr, p^3qr$.
V. p^2q^2r	octodecim:	$1, p, q, r, p^2, pq, pr, q^2, qr, p^2q, p^2r, pq^2, pqr, q^2r, p^2q^2, p^2qr, pq^2r, p^2q^2r$.
VI. p^2qrs	viginti quatuor:	$1, p, q, r, s, p^2, pq, pr, ps, qr, qs, rs, p^2q, p^2r, p^2s, pqr, pqs, prs, qrs, p^2qr, p^2qs, p^2rs, pqrs, p^2qrs$.
VII. $pqrst$	triginta duo:	$1, p, q, r, s, t, pq, pr, ps, pt, qr, qs, qt, rs, rt, st, pqr, pqs, pqt, prs, prt, pst, qrs, qrt, qst, rst, pqrs, pqrt, pqst, prst, qrst, pqrst$.

72. Simili modo reliquarum classium species constituentur singularumque specierum divisores omnes assignabuntur. Simul autem hac ratione patebit natura singulorum divisorum atque tam classis quam species, quorsum singuli sunt referendi.

73. Si numeri N divisores sint: $1, \alpha, \beta, \gamma, \delta, \ldots, N$ isque multiplicetur per numerum primum p, qui in eo nondum contineatur, tum productum Np praeter illos divisores $1, \alpha, \beta, \gamma, \delta, \ldots, N$ insuper eosdem per p multiplicatos $p, \alpha p, \beta p, \gamma p, \delta p, \ldots, Np$ pro divisoribus habebit, ideoque numerus divisorum duplo erit maior.

74. At si ille numerus N per quadratum numeri primi p, qui in ipso non insit tamquam factor, multiplicetur, numerus divisorum triplicabitur. Primo enim productum Np^2 eosdem habebit divisores, quos numerus N; tum vero eosdem per p multiplicatos, ac tertio eosdem per p^2 multiplicatos.

75. Simili modo, si p sit numerus primus in N non contentus numerusque N per p^3 multiplicetur, productum Np^3 habebit primo omnes divisores numeri N, deinde eosdem per p, porro eosdem per p^2, ac denique eosdem per p^3 multiplicatos, quo pacto multitudo divisorum producti Np^3 quadruplo maior est quam numeri N.

76. Atque in genere, si numeri N multitudo divisorum sit $= m$ isque per potestatem p^λ numeri primi p[1]) multiplicetur, producti Np^λ multitudo divisorum erit $(\lambda + 1)\, m$; ubi notasse iuvabit ipsius potestatis p^λ multitudinem divisorum esse $\lambda + 1$.

77. Hinc patet regula facilis multitudinem divisorum cuiuscunque numeri definiendi: Sit enim $p^\lambda q^\mu r^\nu s^\xi$ forma numeri propositi; et quia numeri p^λ multitudo divisorum est $\lambda + 1$, erit numeri $p^\lambda q^\mu$ multitudo divisorum $(\lambda + 1)\ (\mu + 1)$, huius vero numeri $p^\lambda q^\mu r^\nu$ erit $(\lambda + 1)(\mu + 1)(\nu + 1)$, porroque huius $p^\lambda q^\mu r^\nu s^\xi$ erit $(\lambda + 1)\ (\mu + 1)\ (\nu + 1)\ (\xi + 1)$. Classis autem, ad quam hic numerus est referendus, indicatur numero $\lambda + \mu + \nu + \xi$, qui est summa exponentium.

78. Infiniti ergo numeri exhiberi possunt, quorum multitudo divisorum sit data. Si enim multitudo divisorum sit $= a$ existente a numero primo, numeri quaesiti in hac forma p^{a-1} continentur denotante p numerum primum quemcunque.

79. Si a, b, c, d etc. denotent numeros primos pariter ac litterae p, q, r, s etc., numeri, quorum multitudo divisorum est ab, sunt vel p^{ab-1} vel $p^{a-1}q^{b-1}$; quorum autem multitudo divisorum est abc, ii sunt vel p^{abc-1} vel $p^{ab-1}\, q^{c-1}$ vel $p^{ac-1}\, q^{b-1}$ vel $p^{bc-1}\, q^{a-1}$ vel $p^{a-1}\, q^{b-1}\, r^{c-1}$, ubi litterae a, b, c etc. eundem quoque numerum primum significare possunt, dummodo litterae p, q, r etc. significent diversos.

80. Hinc, si multitudo divisorum sit $= 2$, soli numeri primi satisfaciunt seu numeri in hac forma p contenti. Tum vero, si fuerit

multitudo divisorum:	forma numerorum est:
3	p^2,
4	p^3, pq,
5	p^4,
6	p^5, p^2q,
7	p^6,
8	p^7, p^3q, pqr,
9	p^8, p^2q^2,
10	p^9, p^4q,
11	p^{10},
12	p^{11}, p^5q, p^3q^2, p^2qr.

1) Non contenti in divisoribus numeri N. R. F.

81. Cognita ergo forma cuiusque numeri, classe, scilicet, eiusque specie, quo est referendus, non solum multitudo divisorum, sed etiam ipsi divisores ope regularum traditarum assignari possunt.

CAPUT 3
DE SUMMA DIVISORUM CUIUSQUE NUMERI

82. Proposito quocunque numero n summam omnium eius divisorum hoc modo $\int n$ designemus, ita ut haec scriptura $\int n$ denotet summam divisorum numeri n[1]).

83. Cum ergo unitas alium divisorem praeter se ipsam non habeat, erit $\int 1 = 1$; cuiusque vero alius numeri summa divisorum se ipso erit maior, erit, scilicet, $\int n > n$, nisi sit $n = 1$.

84. Pro numeris primis p, quia alios non agnoscunt divisores praeter se ipsos et unitatem, erit $\int p = p + 1$. Tum vero pro potestatibus numerorum primorum erit

$$\int p^1 = p + 1 = \frac{pp - 1}{p - 1},$$
$$\int p^2 = pp + p + 1 = \frac{p^3 - 1}{p - 1},$$
$$\int p^3 = p^3 + pp + p + 1 = \frac{p^4 - 1}{p - 1},$$

et in genere

$$\int p^n = p^n + p^{n-1} + p^{n-2} + \cdots + 1 = \frac{p^{n+1} - 1}{p - 1}.$$

85. Cum numerorum in forma pq contentorum divisores sint $1, p, q, pq$, erit eorum summa:

$$1 + p + q + pq = (1 + p)(1 + q), \quad \text{ideoque} \quad \int pq = (p + 1)(q + 1).$$

Simili modo erit ex classe tertia:

$$\int p^2q = (pp + p + 1)(q + 1) \quad \text{et} \quad \int pqr = (p + 1)(q + 1)(r + 1).$$

86. Eodem modo in reliquis classibus divisores in unam summam colligere liceret; verum quo indoles harum summarum clarius perspiciatur, consideremus

1) Vide Commentationes 152 et 175 indicis ENESTROEMIANI: *De numeris amicabilibus* et *Découverte d'une loi tout extraordinaire des nombres par rapport à la somme de leurs diviseurs.* 1750/1, *LEONHARDI EULERI Opera omnia*, vol. 2 seriei I, p. 86 et 241, ubi EULERUS signum $\int n$ introduxit. R. F.

in genere numerum N, cuius divisores sint $1, \alpha, \beta, \gamma, \delta, \ldots, N$, quorum summa sit $\int N$. Multiplicetur ille per numerum primum p in eo non contentum, et productum Np praeter illos divisores insuper eosdem per p multiplicatos habebit, quorum ergo summa erit $p \int N$, unde colligitur fore:

$$\int Np = (p+1) \int N = \int p \int N.$$

87. Eodem modo ex paragrapho 74 colligitur, si numerus N per quadratum numeri primi p in ipso non contenti multiplicetur, producti Np^2 summam divisorum fore:

$$(1 + p + p^2) \int N \quad \text{seu} \quad \int Np^2 = \int N \cdot \int p^2;$$

eodemque modo fore: $\int Np^3 = \int N \cdot \int p^3$ et ita porro.

88. Hinc pro singulis classibus et speciebus divisorum summae ita exprimentur

$$\begin{aligned}
&\int p = 1 + p, \\
&\hline
&\int p^2 = 1 + p + p^2, \\
&\int pq = (1+p)(1+q), \\
&\hline
&\int p^3 = 1 + p + p^2 + p^3, \\
&\int p^2 q = (1 + p + p^2)(1+q), \\
&\int pqr = (1+p)(1+q)(1+r), \\
&\hline
&\int p^4 = 1 + p + p^2 + p^3 + p^4, \\
&\int p^3 q = (1 + p + p^2 + p^3)(1+q), \\
&\int p^2 q^2 = (1 + p + p^2)(1 + q + q^2), \\
&\int p^2 qr = (1 + p + p^2)(1+q)(1+r), \\
&\int pqrs = (1+p)(1+q)(1+r)(1+s), \\
&\qquad\qquad \text{[etc.]}
\end{aligned}$$

89. Ex his formulis deducimus sequentes conclusiones:

$$\begin{aligned}
&\int p^2 = p^2 + \int p = 1 + p \int p, \\
&\int p^3 = p^3 + \int p^2 = 1 + p \int p^2 = 1 + p + p^2 \int p, \\
&\int p^4 = 1 + p \int p^3 = 1 + p + p^2 \int p^2 = 1 + p + p^2 + p^3 \int p, \\
&\int p^5 = 1 + p \int p^4 = 1 + p + p^2 \int p^3 = 1 + p + p^2 + p^3 \int p^2 \\
&\quad = 1 + p + p^2 + p^3 + p^4 \int p, \\
&\qquad\qquad \text{etc.}
\end{aligned}$$

unde patet esse in genere

$$\int p^n = 1 + p \int p^{n-1} = 1 + p + p^2 \int p^{n-2} = 1 + p + p^2 + p^3 \int p^{n-3} \text{ etc.}$$

90. Proposito ergo numero N, cuius summam divisorum assignari oporteat, resolvatur is in suos factores primos, sitque $N = p^\lambda q^\mu r^\nu s^\xi$ [1]), quo facto erit

$$\int N = \int p^\lambda \cdot \int q^\mu \cdot \int r^\nu \cdot \int s^\xi .$$

91. Dummodo ergo tam numerorum primorum ipsorum quam eorum potestatum summae divisorum assignari queant, omnium plane numerorum summae divisorum definiri poterunt.

92. Pro ipsis numeris primis p, cum sit $\int p = p + 1$, summa divisorum semper erit numerus par, nisi sit $p = 2$, quo casu est $\int 2 = 3$. Si enim sit $p = 2a - 1$, erit $\int (2a - 1) = 2a$. At ob $\int p^2 = p^2 + p + 1$ summa divisorum quadrati cuiusvis numeri primi semper erit numerus impar ac subinde adeo numerus primus, veluti $\int 2^2 = 7$, $\int 3^2 = 13$, $\int 5^2 = 31$.

93. Deinde, si N sit cubus numeri primi seu $N = p^3$, erit

$$\int p^3 = 1 + p + p^2 + p^3 = (1 + p)(1 + p^2),$$

ideoque numerus compositus, ac nisi sit $p = 2$, ad minimum erit summa divisorum divisibilis per 4, quia uterque factor $1 + p$ et $1 + p^2$ est par. Erit ergo $\int p^3 = (1 + p^2) \int p$.

94. Si numerus N sit potestas quarta numeri primi seu $N = p^4$, erit summa divisorum $\int p^4 = 1 + p + p^2 + p^3 + p^4$, ideoque semper impar, fierique adeo poterit, ut ea sit numerus primus, veluti $\int 2^4 = 31$.

95. Si sit $N = p^5$, quia est $\int p^5 = 1 + p + p^2 + p^3 + p^4 + p^5$, erit summa divisorum

$$\int p^5 = (1 + p + p^2)(1 + p^3) = (1 + p)(1 + p + p^2)(1 - p + p^2),$$

ideoque numerus compositus, qui ex summis inferiorum potestatum ita componitur, ut sit

$$\int p^5 = (1 - p + p^2) \int p \cdot \int p^2 .$$

96. Proposito autem producto MN, cuius factores M et N nullum habeant factorem primum communem, erit $\int MN = \int M \cdot \int N$, quae ergo summa divisorum eo magis erit composita, quo plures numeri primi dispares ingrediantur.

97. Proposito numero quocunque N, cuius summa divisorum sit $\int N$, si is per numerum primum p multiplicetur, summa divisorum producti Np

1) p, q, r, s significant numeros primos diversos. R. F.

semper maior est quam $p\int N$. Nam $\int Np$ primum complectitur omnes divisores numeri N per p multiplicatos, quorum summa est $p\int N$, ac praeterea etiam eos divisores numeri N, qui per p non sunt affecti.

98. Hoc etiam ita bipartito ostenditur. Primo si numerus primus p non contineatur in N, erit utique $\int Np = \int p \cdot \int N = (1+p)\int N = p\int N + \int N$, quo casu sine dubio est $\int Np > p\int N$.

99. At si p iam contineatur in N, ut sit $N = Mp^n$, erit $\int N = \int M \cdot \int p^n$, sed $\int Np = \int M \cdot \int p^{n+1}$. Ex superioribus vero constat esse $\int p^{n+1} = 1 + p\int p^n$, unde colligitur $\int Np = \int M + p\int p^n \cdot \int M$, ita ut sit $\int Np = p\int N + \int M$, ideoque $\int Np > p\int N$.

100. Numerorum naturali ordine progredientium summae divisorum ita se habebunt[1]):

$\int 1 = 1$	$\int 13 = 14$	$\int 25 = 31$	$\int 37 = 38$	$\int 49 = 57$
$\int 2 = 3$	$\int 14 = 24$	$\int 26 = 42$	$\int 38 = 60$	$\int 50 = 93$
$\int 3 = 4$	$\int 15 = 24$	$\int 27 = 40$	$\int 39 = 56$	$\int 51 = 72$
$\int 4 = 7$	$\int 16 = 31$	$\int 28 = 56$	$\int 40 = 90$	$\int 52 = 98$
$\int 5 = 6$	$\int 17 = 18$	$\int 29 = 30$	$\int 41 = 42$	$\int 53 = 54$
$\int 6 = 12$	$\int 18 = 39$	$\int 30 = 72$	$\int 42 = 96$	$\int 54 = 120$
$\int 7 = 8$	$\int 19 = 20$	$\int 31 = 32$	$\int 43 = 44$	$\int 55 = 72$
$\int 8 = 15$	$\int 20 = 42$	$\int 32 = 63$	$\int 44 = 84$	$\int 56 = 120$
$\int 9 = 13$	$\int 21 = 32$	$\int 33 = 48$	$\int 45 = 78$	$\int 57 = 80$
$\int 10 = 18$	$\int 22 = 36$	$\int 34 = 54$	$\int 46 = 72$	$\int 58 = 90$
$\int 11 = 12$	$\int 23 = 24$	$\int 35 = 48$	$\int 47 = 48$	$\int 59 = 60$
$\int 12 = 28$	$\int 24 = 60$	$\int 36 = 91$	$\int 48 = 124$	$\int 60 = 168$

101. Inter has divisorum summas non omnes occurrunt numeri, sed usque ad 60 excluduntur sequentes:

2, 5, 9, 10, 11, 16, 17, 19, 21, 22, 23, 25, 26, 27, 29, 33, 34, 35, 37, 41, 43, 45, 46, 47, 49, 50, 51, 52, 53, 55, 58, 59.

Numeri autem, qui summas divisorum exprimunt, sunt:

1, 3, 4, 6, 7, 8, 12, 13, 14, 15, 18, 20, 24, 28, 30, 31, 32, 36, 38, 39, 40, 42, 44, 48, 54, 56, 57, 60.

1) Vide tabulam Commentationis 175, p. 193 laudatae, *Leonhardi Euleri Opera omnia*, vol. 2 seriei I, p. 244. R. F.

102. Hinc patet duos pluresve numeros quandoque eandem divisorum summam praebere, veluti:

$$\begin{array}{ll} \int 6 = \int 11 = 12 & \int 14 = \int 15 = \int 23 = 24 \\ \int 10 = \int 17 = 18 & \int 20 = \int 26 = \int 41 = 42 \\ \int 16 = \int 25 = 31 & \int 33 = \int 35 = \int 47 = 48 \\ \int 21 = \int 31 = 32 & \int 24 = \int 38 = \int 59 = 60 . \\ \int 34 = \int 53 = 54 & \\ \int 28 = \int 39 = 56 & \end{array}$$

103. Problema hic proponi solet, quo quaeritur numerus, qui ad summam divisorum suorum habeat datam rationem; scilicet, ut sit $N : \int N = n : m$ sive $\frac{\int N}{N} = \frac{m}{n}$, ubi quidem primo necesse est, ut sit $m > n$; si enim esset $m = n$, foret $N = 1$.

104. Ratione $m : n$ in minimis terminis expressa numerus N vel ipsi n vel cuipiam eius multiplo aequalis erit. Statuatur ergo $N = an$, eritque $\int N = \int an = am$. At nisi sit $a = 1$, est $\int an > a \int n$, hincque $m > \int n$. Quocirca, si fuerit $m < \int n$, nulla solutio locum habet; sin autem $m = \int n$, unica datur solutio, scilicet $N = n$.

105. Nisi ergo sit vel $m = \int n$ vel $m > \int n$, problema solutionem non admittit. Priori quidem casu numerus quaesitus N ipsi n aequabitur, neque praeterea ulla alia dabitur solutio. Posteriori vero casu, quo $m > \int n$, numerus N aequabitur multiplo cuipiam ipsius n, puta $N = an$, siquidem ulla solutio locum habet. Dantur enim utique eiusmodi rationes $m : n$, quibus nequaquam satisfieri potest, etiamsi sit $m > \int n$.

106. Numerus perfectus est, cuius summa divisorum ipsi duplo est aequalis[1]). Ita si fuerit $\int N = 2N$, erit N numerus perfectus. Qui si sit par, erit huiusmodi $2^n A$ existente A numero impari sive primo sive composito. Cum ergo sit $N = 2^n A$, erit

$$\int N = (2^{n+1} - 1) \int A = 2^{n+1} A, \quad \text{unde fit } \frac{\int A}{A} = \frac{2^{n+1}}{2^{n+1} - 1}.$$

107. Quia huius fractionis $\frac{2^{n+1}}{2^{n+1} - 1}$ numerator unitate tantum superat denominatorem, excedere nequit summam divisorum denominatoris; erit ergo vel aequalis vel minor. Posteriori casu nulla datur solutio, prior vero existere

1) Manuscriptum: maior. Correxit R. F.

nequit, nisi sit $2^{n+1} - 1$ numerus primus. Quare quoties $2^{n+1} - 1$ fuerit numerus primus, ei A aequalis capi debet, eritque numerus perfectus $= 2^n (2^{n+1} - 1)$.

108. Omnes ergo numeri perfecti pares in hac formula $2^n (2^{n+1} - 1)$ continentur, siquidem $2^{n+1} - 1$ fuerit numerus primus, quod quidem evenire nequit, nisi $n + 1$ sit numerus primus; etiamsi non omnes primi pro $n + 1$ assumti praebeant $2^{n+1} - 1$ primum. Utrum vero praeter hos numeros perfectos pares dentur quoque impares necne, nemo adhuc demonstravit.

109. Si daretur numerus perfectus impar, omnes eius factores impares sint, necesse est. Sit ergo $= ABCD$ etc., oportetque fieri $\int A \cdot \int B \cdot \int C \cdot \int D \ldots = 2ABCD \ldots$ numero impariter pari. Quare inter summas divisorum $\int A$, $\int B$, $\int C$, $\int D$,... unica debet esse impariter par, reliquae omnes impares; omnes ergo factores $A, B, C, D, \ldots$ praeter unum erunt potestates pares numerorum primorum, unus autem ille vel numerus primus formae $4n + 1$ vel eiusdem potestas, cuius exponens sit $4\lambda + 1$. Sicque talis numerus perfectus huiusmodi habebit formam $(4n + 1)^{4\lambda+1} PP$ existente P numero impari et $4n + 1$ primo.

110. Plurima alia problemata huc referenda, quibus alia proponitur relatio inter numeros investigandos eorumque summas divisorum, hic praetermitto, quoniam ex traditis principiis methodus ea solvendi non difficulter elicitur.

CAPUT 4

DE NUMERIS INTER SE PRIMIS ET COMPOSITIS

111. Duo numeri, qui praeter unitatem nullum alium habent factorem seu divisorem communem, vocantur numeri primi inter se; qui autem praeter unitatem alium habent divisorem communem, vocantur compositi inter se. Ita 8 et 15 sunt numeri inter se primi, at 9 et 15 numeri inter se compositi.

112. Unitas ergo est ad omnes numeros prima. Scilicet denotante n numerum quemcunque, numeri 1 et n sunt numeri primi inter se, quia praeter unitatem nullum alium admittunt divisorem communem.

113. Pari modo duo numeri unitate differentes n et $n + 1$ sunt primi inter se; quoscunque enim divisores habuerit numerus n, nullus eorum dividere potest numerum $n + 1$. Namque, si p sit divisor numeri n, numerus proxime maior per p divisibilis erit $n + p$, neque vero $n + 1$ divisionem per p admittet.

114. Numerus primus p ad omnes numeros, nisi qui eius sunt multipla, est primus; hinc numeri a et p sunt primi inter se, nisi sit vel $a = p$ vel $a = np$. Ergo numerus primus p ad omnes numeros se minores est primus.

115. Multitudo numerorum dato numero a minorum est $a - 1$, inter quos quot sint ad a vel primi vel compositi, operae pretium est definire; quoniam inde iudicium ad omnes numeros ipso a maiores facile extenditur.

116. Sit enim $b < a$, ac si b et a fuerint primi inter se, etiam omnes hi numeri $b + a$, $b + 2a$, $b + 3a$ etc. ad a erunt primi; ac si b et a habuerint communem divisorem, idem erit divisor numerorum $b + a$, $b + 2a$ etc.

117. Si ergo a sit numerus primus $= p$, quia omnes numeri ipso minores ad eum sunt primi, horum multitudo est $= p - 1$.

118. Si sit $a = 2p$[1]), ab 1 ad a dantur p numeri pares, qui ergo ad a non sunt primi; deinde etiam ipse numerus p ad a non est primus. Auferantur hi a numeris omnibus ab 1 usque ad a, quorum multitudo est $= 2p$, ac relinquentur $p - 1$, totidemque ad a erunt primi.

119. Si sit $a = 3p$[2]), inter numeros ipso non maiores primum ii, qui sunt per 3 divisibiles, ad eum non sunt primi, quorum multitudo est $= p$; deinde insuper p et $2p$ ad a non sunt primi; reliqui, quorum multitudo est $3p - p - 2 = 2(p - 1)$, omnes ad $a = 3p$ erunt primi.

120. Simili modo, si $a = 5p$[3]), numeri, qui cum a communem habent divisorem, sunt primo omnes per 5 divisibiles, quorum multitudo est $= p$, ac praeterea, qui per p sunt divisibiles, nempe p, $2p$, $3p$ et $4p$, ipse enim numerus $5p$ iam ante est notatus; unde multitudo numerorum ad a compositorum est $p + 4$; ideoque multitudo numerorum ad a primorum $= 4p - 4 = 4(p - 1)$, qui, scilicet, ipso a non sunt maiores.

121. Generalius, si sit $a = pq$ existente utroque factore p et q primo, ab unitate ad a dantur p numeri per q divisibiles, scilicet q, $2q$, $3q$, . . ., pq; deinde dantur q numeri per p divisibiles, scilicet p, $2p$, $3p$, . . ., qp, quorum ultimus pq iam est numeratus. Multitudo ergo omnium numerorum a non superantium, qui ad a sunt compositi, erit $= p + q - 1$, unde reliqui, quorum multitudo est

$$= pq - p - q + 1 = (p - 1)(q - 1),$$

ad a erunt primi.

---

1) $p \neq 2$. R. F.
2) $p \neq 3$. R. F.
3) $p \neq 5$. R. F.

122. Hic autem pro p et q numeros primos diversos sumsimus. Nam si esset $a = p^2$, alii numeri ad a non essent compositi, nisi qui sunt per p divisibiles, quorum multitudo cum sit $= p$, reliquorum, qui ad a sunt primi, multitudo erit $= p^2 - p = p(p-1)$.

123. Simili modo, si sit $a = p^3$, quia alium divisorem primum praeter p non habet, omnes numeri ab 1 ad a ad a compositi sunt $p, 2p, 3p, \ldots, p^2 \cdot p$, quorum multitudo cum sit p^2, reliqui numeri omnes, quorum multitudo est $p^3 - p^2 = p^2(p-1)$, ad a erunt primi.

124. Hinc in genere patet, si a fuerit potestas quaecunque p^n numeri primi p, multitudinem numerorum ad a primorum, qui quidem ipso a non sint maiores, fore $= p^{n-1}(p-1)$.

125. Sit $a = p^2 q$ existentibus p et q numeris primis diversis, et cum a alios non habeat divisores primos praeter p et q, numeri ad a compositi vel erunt per p divisibiles, qui sunt $p, 2p, 3p, \ldots, pq \cdot p$ multitudine $= pq$, vel per q divisibiles, qui sunt $q, 2q, 3q, \ldots, p^2 \cdot q$ multitudine $= p^2$. Inter hos vero occurrunt, qui ibi iam sunt numerati: $pq, 2pq, 3pq, \ldots, p \cdot pq$ multitudine $= p$, ita ut multitudo omnium ad a compositorum sit $= pq + p^2 - p$. Quare reliqui, quorum multitudo est $= p^2 q - pq - p^2 + p = p(p-1)(q-1)$, omnes ad a erunt primi.

126. Sit $a = pqr$ existentibus p, q, r numeris primis diversis, ac numeri ad a compositi sunt divisibiles

primo:	per p,	scilicet	$p, 2p, 3p, \ldots, qr \cdot p$,	multitudine	qr,
secundo:	per q,	„	$q, 2q, 3q, \ldots, pr \cdot q$,	„	pr,
tertio:	per r,	„	$r, 2r, 3r, \ldots, pq \cdot r$,	„	pq.

Hic autem bis numerantur divisibiles per pq multitudine r, tum divisibiles per pr multitudine q, ac denique divisibiles per qr multitudine p, qui inde auferantur; at hoc modo numerus ipse pqr penitus tolleretur, qui ergo iterum est adiiciendus. Sicque multitudo numerorum ad a compositorum erit

$$qr + pr + pq - r - q - p + 1 ;$$

unde reliqui, quorum multitudo est

$$pqr - qr - pr - pq + r + q + p - 1 = (p-1)(q-1)(r-1),$$

ad numerum $a = pqr$ erunt primi.

127. Ex his colligetur pro omnibus numerorum generibus fore,

si sit numerus propositus:	multitudinem numerorum ipso a minorum ad eumque primorum
$a = p$,	$p - 1$,
$a = p^2$,	$p(p-1)$,
$a = pq$,	$(p-1)(q-1)$,
$a = p^3$,	$p^2(p-1)$,
$a = p^2 q$,	$p(p-1)(q-1)$,
$a = pqr$,	$(p-1)(q-1)(r-1)$,
$a = p^4$,	$p^3(p-1)$,
$a = p^3 q$,	$p^2(p-1)(q-1)$,
$a = p^2 q^2$,	$p(p-1)q(q-1)$,
$a = p^2 qr$,	$p(p-1)(q-1)(r-1)$,
$a = pqrs$,	$(p-1)(q-1)(r-1)(s-1)$.

128. Quo autem haec conclusio firmius corroboretur neque inductioni nimium indulgeatur, consideremus hanc formam $a = Mp$, ubi M sit numerus quicunque et p primus in M non contentus. Ponamus autem ab 1 ad M multitudinem numerorum ad M primorum esse $= \mu$, ideoque multitudinem numerorum ad M compositorum $= M - \mu$.

129. Cum ergo ab 1 ad M sint $M - \mu$ numeri compositi ad M, ab 1 ad Mp erunt $p(M - \mu)$ numeri compositi ad M, qui ergo etiam erunt compositi ad Mp. Sed praeterea ad Mp compositi sunt isti: $p, 2p, 3p, \ldots, M \cdot p$ multitudine M; unde autem expungendi sunt ii, qui iam ad M sunt compositi, quorum multitudo est $M - \mu$; sicque tantum relinquentur μ numeri, qui tantum ad Mp, non vero ad M sunt compositi. Quare ab 1 ad Mp omnino ad Mp compositi erunt tot: $p(M - \mu) + \mu$, et reliqui, quorum multitudo est $Mp - p(M - \mu) - \mu = \mu(p - 1)$, ad numerum Mp erunt primi.

130. Simili modo ostenditur, si numerus propositus sit $= Mp^n$ existente p numero primo in M non contento atque μ fuerit multitudo numerorum ad M primorum, qui quidem inter limites 1 et M contineantur, tum multitudinem omnium numerorum infra Mp^n ad hunc ipsum numerum Mp^n primorum fore $= \mu p^{n-1}(p - 1)$.

131. Quaeramus enim numeros compositos ad Mp^n, qui vel ad M vel ad p erunt compositi. At ab 1 ad Mp^n multitudo numerorum ad M compositorum est $= p^n(M - \mu)$; qui vero ad p sunt compositi, erunt: $p, 2p, 3p, \ldots, Mp^{n-1} \cdot p$

multitudine $= Mp^{n-1}$. Hinc autem excludi oportet eos, qui iam ad M sunt compositi, quorum multitudo est $p^{n-1}(M-\mu)$; sicque multitudo eorum, qui ad Mp^n, non vero ad M sunt compositi, erit $= Mp^{n-1} - p^{n-1}(M-\mu) = p^{n-1}\mu$, unde omnino ab 1 ad Mp^n multitudo numerorum ad Mp^n compositorum est $= p^n(M-\mu) + p^{n-1}\mu$. Quocirca reliqui, quorum multitudo est $Mp^n - p^n(M-\mu) - p^{n-1}\mu = \mu p^{n-1}(p-1)$, erunt ad Mp^n primi.

132. Cum ergo multitudo numerorum ad p^n primorum ipsoque minorum sit $= p^{n-1}(p-1)$, ex praecedente propositione summo rigore concludimus: Si numerus propositus sit $= p^\lambda q^\mu r^\nu s^\xi$ etc., fore multitudinem omnium numerorum ad eum primorum ipsoque minorum [1])

$$= p^{\lambda-1}(p-1)\cdot q^{\mu-1}(q-1)\cdot r^{\nu-1}(r-1)\cdot s^{\xi-1}(s-1) \text{ etc.}$$

133. Si igitur M et N fuerint numeri inter se primi, atque multitudo numerorum ab 1 ad M primorum ad M sit $= m$, multitudo vero numerorum ab 1 ad N primorum ad N sit $= n$, tum multitudo numerorum ad productum MN primorum ipsoque non maiorum erit $= mn$.

134. Hinc patet multitudinem omnium numerorum primorum, quemadmodum iam EUCLIDES demonstravit, finitam esse non posse. Si enim ultimus et maximus numerus primus esset $= p$, statuatur numerus M aequalis producto omnium numerorum primorum $M = 2\cdot 3\cdot 5\cdot 7\ldots p$, qui ergo ad omnes plane numeros esset compositus; cum igitur idem numerus M ad $M-1$ vel $M+1$ certe sit primus, patet assertionem esse absurdam.

135. Ex superioribus autem patet inter numeros ipso M minores non solum numerum $M-1$, sed etiam plures alios ad M certe esse primos, cum multitudo horum numerorum ad M primorum sit $= 1\cdot 2\cdot 4\cdot 6\ldots(p-1)$, quae eo est maior, quo plures numeri primi in se invicem multiplicentur.

136. Ponamus $m = 1\cdot 2\cdot 4\cdot 6\ldots(p-1)$ existente $M = 2\cdot 3\cdot 5\cdot 7\ldots p$; et cum ab 1 ad M tot sint numeri ad M primi, quot m continet unitates, hi vel ipsi erunt primi vel compositi ex primis, qui sint ipso p maiores.

137. Si ab 1 ad M fuerint m numeri ad M primi, ab 1 ad $2M$ erunt $2m$ numeri ad M primi, et in genere ab 1 ad NM erunt Nm numeri ad M primi. In quovis enim intervallo

$$1\ldots M,\quad M+1\ldots 2M,\quad 2M+1\ldots 3M,\quad 3M+1\ldots 4M \text{ etc.}$$

multitudo numerorum ad M primorum est eadem.

1) Vide Commentationem 271 indicis ENESTROEMIANI: *Theoremata arithmetica nova methodo demonstrata*, novi comm. acad. sc. Petrop. 8 (1760/1), 1763; *LEONHARDI EULERI Opera omnia*, vol. 2 seriei I, p. 531, ubi EULERUS hanc formulam simili methodo demonstrat. R. F.

138. Si N designet alium numerum quemcunque atque ab 1 ad N fuerint n numeri ad N primi, ab 1 ad MN erunt Mn numeri ad N primi. At in eodem intervallo sunt Nm numeri ad M primi. Qui autem sunt primi ad MN, ii quoque sunt primi tam ad M quam ad N.

139. Ante autem ostendimus, si hi numeri M et N fuerint primi inter se, tum in intervallo $1 \ldots MN$ tot dari numeros ad MN primos, quot mn contineat unitates; hique numeri in utraque praecedente multitudine Mn et Nm occurrunt.

[*Additamentum ad Caput IV*][1]): *De maximo communi divisore eiusque inventione*:

Si A et B sint primi [inter se], inveniri potest multiplum ipsius A, quod per B divisum relinquat datum numerum C.

Qui numeri inter se fuerint primi, eorum potestates quaecunque inter se erunt primi.

Si A sit primus ad B atque etiam ad C, erit quoque ad BC primus.

Si productum AB sit divisibile per [numerum] primum p, alteruter factor per eum erit divisibilis.

Si A et B sint primi inter se, inveniri possunt numeri m et n, ut fiat $mA - nB = 1$ vel alii cuivis numero dato.

Si sit φ maximus communis factor numerorum A et B, tum $\frac{A}{\varphi}$ et $\frac{B}{\varphi}$ erunt primi inter se.

CAPUT 5
DE RESIDUIS EX DIVISIONE NATIS

140. Si numerus a non sit multiplum numeri b, divisio illius per hunc non succedit, et excessus numeri a supra multiplum ipsius b proxime minus vocatur *residuum* ex divisione ortum. Ita, si sit $a = mb + r$, erit r residuum ex divisione numeri a per b natum.

141. Hinc patet residuum r semper minus esse numero b seu divisore; si enim esset aequale seu $r = b$, aucto indice multipli m unitate foret a verum multiplum ipsius b, scilicet $a = (m + 1)\,b$; et si esset $r > b$, augendo indicem m reduceretur infra b.

142. Proposito ergo divisore quocunque b, si dividendus a fuerit multiplum ipsius b, residuum erit $= 0$; sin autem a non fuerit multiplum ipsius b,

1) Omnia additamenta EULERUS margini adscripsit. R. F.

residuum erit vel 1 vel 2 vel 3 vel quicunque alius numerus minor quam b, ita ut multitudo residuorum, quae oriri possunt, sit $b-1$ vel adeo b, si cyphra simul numeretur.

143. Pro quovis ergo divisore b omnes numeri in tot classes distribui possunt, quot b continet unitates. Prima nempe classis continebit omnes numeros multiplos ipsius b seu formae mb, secunda eos, qui per b divisi pro residuo relinquunt 1, tertia eos, qui 2, quarta eos, qui 3, et denique ultima, qui relinquunt $b-1$.

144. Ita sumto 2 pro divisore duae habentur classes, quarum prima continet numeros formae $2m$, altera vero numeros formae $2m+1$. Numeri prioris classis vocantur pares, posterioris vero impares.

145. Si ternarius pro divisore assumatur, omnes numeri in tres classes distinguentur: prima complectitur numeros formae $3m$, secunda numeros formae $3m+1$, ac tertia numeros formae $3m+2$.

146. Si divisor statuatur $=4$, quaternae classes omnium numerorum his quatuor formis comprehenduntur:

$$\text{I. } 4m, \quad \text{II. } 4m+1, \quad \text{III. } 4m+2, \quad \text{IV. } 4m+3,$$

ubi prima classis nomen sortita est numerorum pariter parium, tertia vero numerorum impariter parium. At secunda et quarta numeros impares in duas classes subdivisos exhibent.

147. Simili modo divisor 5 has quinque numerorum classes suppeditat:

$$\text{I. } 5m, \quad \text{II. } 5m+1, \quad \text{III. } 5m+2, \quad \text{IV. } 5m+3, \quad \text{V. } 5m+4;$$

ac divisor 6 praebet has sex classes:

$$\text{I. } 6m, \quad \text{II. } 6m+1, \quad \text{III. } 6m+2, \quad \text{IV. } 6m+3, \quad \text{V. } 6m+4, \quad \text{VI. } 6m+5,$$

et ita porro pro quovis alio divisore.

148. Sic igitur quilibet numerus pro quovis divisore ad certam quandam classem refertur seu certa quadam forma exprimitur, quod, cum divisorum numerus in infinitum augeri queat, infinitis modis fieri potest.

149. Si enim numerus fuerit minor divisore proposito, ipse ut residuum spectari potest indice multipli evanescente; ita, si sit $a<b$, erit $a=mb+a$ existente $m=0$; numerus ergo 3 respectu divisoris 5 pertinet ad classem $5m+3$.

150. Quaelibet classis infinitos continet numeros in arithmetica progressione crescentes secundum differentiam divisori aequalem. Ita in genere, si divisor sit b et residuum r, omnes numeri ad classem $mb + r$ relati sunt:

$$r, \quad b + r, \quad 2b + r, \quad 3b + r, \quad 4b + r, \quad 5b + r \quad \text{etc.},$$

cuius progressionis arithmeticae terminus generalis est ipsa formula $mb + r$, unde est nata.

[*Additamentum*[1])]: Si a per b divisum det residuum r, tum na per nb divisum dabit residuum nr.

Si a per b divisum det residuum r, communis factor numerorum a et b, si quem habent praeter unitatem, simul erit factor residui r. Vicissim, si b et r habeant communem factorem, idem quoque factor erit ipsius a.

Si a et b sint numeri inter se primi et $a > b$, erit $a = mb + p$ et $b > p$; tum vero $b = np + q$ et $p > q$[2]), sicque tandem ad unitatem pervenietur.

151. Formula $mb + r$ etiam hoc modo $(m + 1)\, b - b + r$ potest repraesentari, sicque residuo positivo r aequivalens censendum est residuum negativum $-(b - r)$; unde patet ideam residuorum latius extensam etiam numeros negativos complecti.

152. Hinc divisore b existente $= 2$ formula numerorum imparium $2m + 1$ etiam ita $2m - 1$ repraesentari potest; atque si divisor b sit $= 3$, classis numerorum, qui per 3 divisi relinquunt binarium, etiam formula $3m - 1$ continetur; sicque omnes numeros in una harum trium formularum $3m$, $3m + 1$ et $3m - 1$ contineri necesse est.

153. Quare si residua negativa admittere velimus, omnes formulas $mb \pm r$ ita repraesentare poterimus, ut residuum r semissem divisoris b non superet. Si enim esset $r > \frac{1}{2} b$, pro r sumamus $-(b - r)$, eritque $b - r < \frac{1}{2} b$.

154. Simili modo, cum sit $mb + r = (m - 1)\, b + b + r$, residuo r etiam aequivalet residuum $b + r$ vocabulo in latiori sensu accepto. Generatim ergo residua minus proprie ita dicta $b + r$, $2b + r$, $3b + r$ etc. aequivalent residuo r proprie sic dicto.

155. Scilicet divisore existente b omnis numerus, etiamsi sit maior quam b, tamquam residuum spectari potest, qui ad residuum proprie ita dictum reducetur divisorem b inde toties auferendo, quoties fieri licet, quod adeo negativa admittendo infra semissem ipsius b deprimi poterit.

---

1) Vide notam p. 203. R. F.

2) Manuscriptum: $p > 0$. Correxit R. F.

156. Ita, si divisor sit 6 et residuum 16, hoc residuum improprium reducetur ad proprium 4, atque adeo ad negativum -2, sive istae formulae $6m + 16$, $6m + 4$, $6m - 2$ pro aequivalentibus sunt habendae, quia omnes numeri in una contenti simul in reliquis continentur.

157. Circa residua plures insignes proprietates perpendi oportet. Si numerus A per divisorem d divisus praebeat residuum α, numeri quoque $A + d$, $A + 2d$, $A + 3d$ etc. idem relinquent residuum α, at numerus $A + 1$ per eundem divisus dabit residuum $\alpha + 1$, et generaliter numerus $A + n$ residuum dabit $\alpha + n$, quod, si excedat divisorem d, eo subtrahendo, quoties fieri potest, ad minimam formam reducetur.

158. Simili modo, si sumto divisore d numero A residuum conveniat α, numeri quoque $A - d$, $A - 2d$, $A - 3d$ etc. idem relinquent residuum, at numero $A - 1$ residuum conveniet $\alpha - 1$, et numero $A - n$ residuum $\alpha - n$, quod si forte sit negativum, additione divisoris d ad positivum reducetur.

159. Sumto divisore d, si numero A conveniat residuum α, numero vero B residuum β, aggregato horum numerorum $A + B$ conveniet residuum $\alpha + \beta$, quod congruit cum $\alpha + \beta - d$, si forte sit $\alpha + \beta > d$. Hinc patet, si sit $\alpha + \beta = d$, fore $A + B$ multiplum ipsius d.

160. Iisdem positis differentiae numerorum $A - B$ conveniet residuum $\alpha - \beta$ vel etiam $\alpha - \beta + d$, si forte sit $\beta > \alpha$. Unde, si sit $\alpha = \beta$, seu si numeri A et B paria relinquant residua, eorum differentia erit per divisorem d divisibilis.

161[1]). Sumto divisore d, si numerus A praebeat residuum α, eius duplum $2A$ dabit residuum 2α vel etiam $2\alpha - d$; triplum vero $3A$ dabit residuum 3α, cuius, si sit maius quam d, minima forma erit vel $3\alpha - d$ vel $3\alpha - 2d$. Atque in genere multipli cuiusvis nA residuum erit $n\alpha$ sive $n\alpha - md$.

162. Si divisore posito $= d$ numero A respondeat residuum α, numero vero B residuum β, producto AB residuum conveniet $\alpha\beta$, quod, si forte maius fuerit quam divisor d, reducitur ad $\alpha\beta - d$ vel $\alpha\beta - md$.

163. Erit enim $A = md + \alpha$ et $B = nd + \beta$, unde fit productum

$$AB = mnd^2 + (m\beta + n\alpha)\,d + \alpha\beta\ ;$$

cuius partes priores cum sint per d divisibiles, postrema $\alpha\beta$ pro residuo haberi potest.

1) Ab hac paragrapho in manuscripto numeri paragraphorum unitate aucti sunt. R. F.

164. Hinc colligimus, si numerus A per d divisus relinquat residuum α, eius quadrato A^2 respondere residuum α^2, eiusque cubo A^3 residuum α^3, et potestati cuiuscunque A^n residuum α^n, quod divisione per d facta porro ad minimam formam reducetur.

165. Quare si numero A per d diviso relinquatur residuum $= 1$, omnes eius potestates A^2, A^3, A^4 etc. per eundem divisorem d divisi idem residuum relinquent $= 1$. At si residuum numeri A sit -1, aequipollens ipsi $d-1$, potestatem parium A^2, A^4, A^6, A^8 etc. residua erunt $+1$, imparium vero -1.

166. Denique notandum est, si numerus A per d divisus praebeat residuum α, tum fore $A - \alpha$ per numerum d divisibilem. Unde, cum A^n pro divisore d det residuum α^n, erit quoque $A^n - \alpha^n$ per d divisibile.

CAPUT 6

DE RESIDUIS EX DIVISIONE TERMINORUM PROGRESSIONIS ARITHMETICAE ORTIS [1])

167. Incipiamus a serie numerorum naturalium, cuius termini 1, 2, 3, 4 etc. per divisorem quemcunque d divisi dabunt residua 1, 2, 3, 4 etc., donec perveniatur ad terminum d, cui residuum convenit $= 0$, sequentes vero termini $d+1$, $d+2$, $d+3$ etc. eodem ordine residua 1, 2, 3 etc. reddent, usque ad $2d$, cuius residuum iterum evanescit, et ita porro.

168. Sit iam proposita progressio arithmetica quaecunque

$$a, \quad a+b, \quad a+2b, \quad a+3b, \quad a+4b, \quad a+5b \quad \text{etc.},$$

cuius singuli termini per divisorem d dividantur, et ex primo oritur residuum a, quod idem ante non recurret, quam perveniatur ad terminum $a+nb$, cuius pars nb per d divisibilis existat, et post hunc terminum residua eodem ordine prodibunt atque ab initio.

[*Additamentum*][2]): Haec residua excedent numero a residua orta ex progressione $0, b, 2b, 3b, 4b$ etc., quare hanc evolvisse sufficiet.

169. Primum quidem statim liquet hinc plura diversa residua resultare non posse, quam divisor d contineat unitates. Unde, si ab initio iam tot diversa

1) Confer Commentationem 271 indicis ENESTROEMIANI, novi comm. acad. sc. Petrop. 8 (1760/1), 1763; *LEONHARDI EULERI Opera omnia* vol. 2 seriei I, p. 531. R. F.

2) Vide notam p. 203. R. F

residua prodierint, necesse est, ut deinceps priores iterum redeant. Semper autem terminus $a + db$, cuius index est $d + 1$, idem praebet residuum ac primus a.

170. Si differentia progressionis b fuerit factor divisoris d, vel si saltem b et d communem habeant factorem φ, ut sit $b = B\varphi$ et $d = D\varphi$, tum antequam ad terminum $a + db$ perveniatur, primum residuum a revertetur; scilicet, hoc continget in termino $a + Db$, cuius index est $D + 1$, quoniam $Db = BD\varphi = Bd$ per d est divisibile.

171. Hic ergo duos casus evolvi conveniet, alterum, quo divisor d et differentia progressionis b sunt numeri inter se primi, alterum vero, quo sunt numeri inter se compositi, seu quo habent quempiam factorem communem praeter unitatem.

172. Si divisor d et differentia progressionis b fuerint numeri primi inter se, primum residuum a ante non recurrit quam in termino $a + db$; si enim ex termino quodam antecedente $a + (d - n)b$ resultaret, esset $(d - n)b$ ac proinde etiam nb per d divisibile, ideoque etiam n, quod foret absurdum.

173. Ad definienda ergo residua considerari oportet terminos progressionis a primo a usque ad $a + (d - 1)b$, quorum multitudo est d, quos terminos ordine compositos cum suis residuis ita repraesentemus:

Indices:	1,	2,	3,	4,	5,	.....,	d,
Progressio:	a,	$a + b$,	$a + 2b$,	$a + 3b$	$a + 4b$,	.....,	$a + (d - 1)b$,
Residua:	α,	β,	γ,	δ,	ε,	.....,	λ.

174. Primum ergo observo cuncta haec residua, quorum multitudo est $= d$, inter se esse diversa. Quemadmodum enim primum α non amplius occurrere ostensum est, ita etiam secundum β semel tantum adesse docetur. Si enim ex termino $a + nb$ existente $n < d$ idem oriretur residuum, foret differentia terminorum $(n - 1)b$ per d divisibilis, ideoque et $n - 1$, quod repugnat.

175. Cum igitur omnia residua α, β, γ, δ, ..., λ sint inter se diversa eorumque multitudo sit $= d$, inter ea omnes numeri ipso d minores una cum cyphra occurrent, numeri, scilicet, 0, 1, 2, 3, ..., $(d - 1)$ occurrent, quorum multitudo pariter est $= d$.

176. Quare, si r fuerit numerus quicunque minor quam divisor d, dabitur certe progressionis terminus $a + nb$ existente $n < d$, qui per d divisus relinquat residuum r. Ac sumto $r = 0$ dabitur eiusmodi terminus $a + nb$ per d divisibilis.

177. Si terminus $a + nb$ residuum praebeat r, erit $a + nb - r$ per d divisibile. Unde, si b et d sint numeri inter se primi et $a - r$ denotet numerum quemcunque, semper dabitur numerus n minor quam d, ita ut numerus $a - r + nb$ fiat per d divisibilis.

178. Sit $a + mb$ terminus per d divisibilis existente $m < d$, ac terminus sequens $a + (m + 1)b$ residuum dabit b, praecedens vero $a + (m - 1)b$ residuum $-b$ seu $d - b$. Sit porro $a + nb$ terminus, qui per d divisus unitatem relinquat, atque illo numero hinc ablato differentia $(n - m)b$ etiam unitatem relinquet.

179. Ponamus $n - m = p$, ut numerus pb per d divisus unitatem relinquat, sumtoque termino $a + mb$ per d divisibili termino $a + (m + p)b$ conveniet residuum $= 1$, termino $a + (m + 2p)b$ residuum $= 2$, termino $a + (m + 3p)b$ residuum $= 3$ et in genere termino $a + (m + np)b$ residuum $= n$.

180. Si $m + np$ fuerit maius divisore d, hic toties inde auferatur, donec remaneat numerus $k < d$, et terminus $a + kb$ per d divisus relinquet residuum $= n$.

181. Facilius autem termini data residua relinquentes definiri possunt, dum innotuerit productum pb, quod per d divisum relinquat unitatem. Cum enim terminus primus a relinquat α, terminus $a + npb$ relinquet $\alpha + n$.

182. Si ergo datum residuum fuerit $= r$, ponatur $\alpha + n = r$, et ob $n = r - \alpha$ invento p terminus residuum r praebens erit $a + (r - \alpha)pb$; vel etiam generaliter $a + ((r - \alpha)p \pm \mu d)b$, ubi μ ita assumere licet, ut fiat $(r - \alpha)p \pm \mu d < d$[1]).

183. Totum ergo negotium huc redit, ut numeri b id investigetur multiplum pb, quod per d divisum unitatem relinquat. Cum itaque $pb - 1$ per d sit divisibile, posito $pb - 1 = qd$ numeros p et q investigari oportet, ut fiat $pb - qd = 1$. Semper autem p infra d assignari poterit.

184. Saepe eiusmodi productum πb facilius reperitur, quod per d divisum relinquat $d - 1$ seu -1; tum autem hoc productum $(d - \pi)b$ residuum praebebit $= +1$, ita ut invento π futurum sit $p = d - \pi$. Tum igitur terminus $a + ((\alpha - r)\pi \pm \mu d)b$ datum residuum r relinquat.

185. Consideremus nunc etiam residua, quae oriuntur, si differentia progressionis b et divisor d non fuerint numeri inter se primi. Atque iam vidimus, si factor communis sit φ, ut sit $b = B\varphi$ et $d = D\varphi$, iam terminum $a + Db$ idem praebere residuum quod primus a.

1) et > 0. R. F.

186. Quare, si φ fuerit maximus factor communis numerorum b et d, quoniam primum residuum a vel α demum in termino $a + Db$ recurrit, plura residua diversa locum habere nequeunt quam numero D; neque ergo omnes numeri divisore d minores inter residua occurrent.

187. Quo haec residua facilius scrutemur, ponamus esse $a = 0$, sintque termini progressionis cum suis residuis:

Indices:	1,	2,	3,	4,	.....,	D,
Termini:	0,	$B\varphi$,	$2B\varphi$,	$3B\varphi$,	.....,	$(D-1)B\varphi$,
Residua:	0,	$\beta\varphi$,	$\gamma\varphi$,	$\delta\varphi$,	.....,	$\lambda\varphi$;

manifestum enim est, si hi termini per $d = D\varphi$ dividantur, residua quoque per φ esse divisibilia.

188. Nam, si mB divisum per D praebeat residuum r, erit $mB = nD + r$ ideoque $mB\varphi = nD\varphi + r\varphi$. Unde, si $mB\varphi$ per $D\varphi = d$ dividatur, residuum erit $r\varphi$, multiplum ipsius φ. Cum igitur pro r omnes numeri ipso D minores prodire queant, etiam inter illa residua omnia multipla ipsius φ, quae quidem divisorem $d = D\varphi$ non superant, occurrere debent, quorum multitudo utique est $= D$.

189. Si ad singulos terminos adiiciamus numerum a, eodem singula residua augebuntur, quae ergo ita se habebunt existente $b = B\varphi$ et $d = D\varphi$:

Indices:	1,	2,	3,	4,	5, ...,	D,
Termini:	a,	$a + b$,	$a + 2b$,	$a + 3b$,	$a + 4b$, ...,	$a + (D-1)b$,
Residua:	a,	$a + \beta\varphi$,	$a + \gamma\varphi$,	$a + \delta\varphi$,	$a + \varepsilon\varphi$, ...,	$a + \lambda\varphi$,

ubi series $\beta, \gamma, \delta, \varepsilon, \ldots, \lambda$ omnes numeros ipso D minores continet.

190. Hoc ergo casu ex serie residuorum excluduntur omnes numeri, qui numero a minuti non sunt divisibiles per φ seu maximum communem divisorem differentiae b et divisoris d.

191. Cum numeri B et D sint primi inter se, eiusmodi multiplum prioris, puta mB, exhiberi potest, quod per D divisum datum relinquat residuum r; tum autem nostrae progressionis terminus $a + mB\varphi$ seu $a + mb$ per $D\varphi = d$ divisus relinquet residuum $a + r\varphi$.

[*Additamentum*][1]): Methodus definiendi formulam $ax + b$, ut ea per datum numerum d fiat divisibilis.

1) Vide notam p. 203. R. F.

CAPUT 7

DE RESIDUIS EX DIVISIONE TERMINORUM PROGRESSIONIS GEOMETRICAE ORTIS

192. Progressionem geometricam in genere ita repraesentamus: a, ab, ab^2, ab^3, ab^4, ab^5 etc., cuius termini, si per numerum quemcunque d dividantur, eiusmodi dabunt residua, quae facile ex residuis huius progressionis $1, b, b^2, b^3$ etc. colligi possunt his, scilicet, per a multiplicandis.

193. Haec ergo de residuis quaestio ad meras potestates revocatur, ita ut residuum definiendum sit, quod potestas quaecunque b^n per datum numerum d divisa relinquit. Ubi quidem casus distingui convenit, quibus numeri b et d sunt vel primi inter se vel compositi.

194. Si sit $b = p\varphi$ et $d = q\varphi$[1]), quaeratur residuum ex $p^n\varphi^{n-1}$ ortum, si per q dividatur, illudque per φ multiplicatum dabit residuum ortum ex divisione numeri $p^n\varphi^n$ per $q\varphi$; hocque modo deducimur ad divisionem eiusmodi potestatis b^n per d, ubi b et d sint numeri inter se primi.[2])

195. Sint ergo b et d numeri inter se primi, et residua ex divisione potestatum ipsius b oriunda ita indicentur:

$$\begin{array}{ll} \text{Potestates:} & 1, b, b^2, b^3, b^4, b^5, b^6, b^7 \text{ etc.,} \\ \text{Residua:} & 1, \alpha, \beta, \gamma, \delta, \varepsilon, \xi, \eta \text{ etc.,} \end{array}$$

quae omnia ad divisorem d quoque erunt prima, quia d ad omnes potestates ipsius b est primus.

196. Quia haec residua $1, \alpha, \beta, \gamma, \delta$ etc. omnia sunt minora quam d, ea omnia a se invicem diversa esse non possunt. Quin, si multitudo numerorum ad d primorum eoque simul minorum sit μ, plura residua diversa resultare nequeunt, quam μ continet unitates.

197. Cum ergo innumerabiles potestates paria praebeant residua, si ponamus b^m et b^{m+n} idem dare residuum, harum potestatum differentia $b^{m+n} - b^m = b^m(b^n - 1)$ per d erit divisibilis. Quia igitur b^m ad d est primus, sequitur $b^n - 1$ per d esse divisibile seu potestatem b^n dare residuum $= 1$.

198. Quia plura quam μ residua diversa occurrere nequeunt, si progressio ad terminum b^μ continuetur, ob terminorum numerum $= \mu + 1$ unum saltem residuum bis occurret, sicque casus ante positus continget, ante-

1) p et q sine divisore communi. R. F.
2) Haec observatio non est evidens. R. F.

quam $m + n$ superet μ, unde potestas b^n residuum $= 1$ reproducens dabitur, ita ut n non superet μ.

199. Ponamus post unitatem b^n infimam esse potestatem, quae per d divisa unitatem relinquat, atque sequentes potestates b^{n+1}, b^{n+2}, b^{n+3} etc. eadem praebebunt residua, quae potestates initiales b, b^2, b^3 etc., donec perveniatur ad potestatem b^{2n}, quae iterum unitatem pro residuo relinquet.

200. Cum igitur a potestate b^n progrediendo eadem residua recurrant, atque ab initio non solum omnes potestates b^0, b^n, b^{2n}, b^{3n}, b^{4n} etc. idem relinquent residuum 1, sed etiam hae b^1, b^{n+1}, b^{2n+1}, b^{3n+1}, b^{4n+1} etc. idem habebunt residuum, quin etiam istae b^m, b^{n+m}, b^{2n+m}, b^{3n+m} etc. per d divisae aequalia residua relinquent.

201. Posita ergo b^n infima potestate unitatem pro residuo relinquente, ita ut n non excedat μ, multitudinem numerorum ipso d minorum ad eumque primorum, omnes antecedentes potestates $1, b, b^2, b^3, \ldots, b^{n-1}$ disparia praebebunt residua, quae deinceps eodem ordine recurrent. Si enim duo eorum essent paria, minor valor pro n haberetur contra hypothesin.

202. Quodsi ergo in residuis omnes numeri ad divisorem d primi eoque minores occurrant, quorum multitudo est $= \mu$, erit $n = \mu$, atque $b^\mu - 1$ per d erit divisibile. Sin autem non omnes illi numeri ad d primi inter residua occurrant, necesse est, ut sit $n < \mu$. Ostendemus autem his casibus n esse partem aliquotam ipsius μ.

203. Si non omnes numeri ad d primi eoque minores, quorum multitudo est $= \mu$, inter residua, quorum multitudo est $= n$, occurrant, eos, qui ex ordine residuorum excluduntur, nomine *non-residuorum* appellabo, ita ut multitudo residuorum n cum multitudine *non-residuorum* exhaurire debeat numerum μ.[1])

204. Si in serie residuorum $1, \alpha, \beta, \gamma$ etc. occurrant numeri r et s, in ea quoque occurret numerus rs seu residuum ipsi aequivalens. Si enim residua r et s respondeant potestatibus b^ϱ et b^σ, potestati $b^{\varrho+\sigma}$ respondebit residuum rs. Hincque inter residua occurret numerus $r^f s^g$ sumtis exponentibus f et g utcunque.

205. Vicissim, si potestati b^ϱ conveniat residuum r, potestati vero $b^{\varrho+\sigma}$ residuum rs vel $rs - \lambda d$, tum potestati b^σ conveniet residuum s. Nam producto $b^\varrho s$ conveniet residuum rs, idem quod potestati $b^{\varrho+\sigma}$; hinc differentia $b^{\varrho+\sigma} - b^\varrho s = b^\varrho (b^\sigma - s)$ per d erit divisibilis. Quare, cum b^ϱ ad d sit primus, necesse est, sit $b^\sigma - s$ per d divisibile, sicque potestati b^σ respondebit residuum s.

1) Non-residuum hoc loco aliud significat quam paragrapho 290. R. F.

206. Si ergo numeri r et rs inter residua reperiantur, certum est et numerum s ibidem repertum iri. Quodsi iam series residuorum $1, \alpha, \beta, \gamma, \delta$ etc., quorum numerus est $= n$, non omnes numeros ipso d minores ad eumque primos complectatur, quorum multitudo est $= \mu$, dabitur unus pluresve, quos in classem non-residuorum referri oportet.

207. Sit x tale non-residuum, ac manifestum est etiam hos numeros $\alpha x, \beta x, \gamma x, \delta x$ etc. inter non-residua reperiri; nam, si αx in residuis inveniretur, quia α ibidem extat, etiam x ibidem reperiri deberet contra hypothesin. Ex unico ergo non-residuo necessario sequuntur tot non-residua, quot habentur residua, scilicet numero n. Sunt enim haec non-residua inter se aeque disparia ac ipsa residua $1, \alpha, \beta, \gamma, \delta$ etc.; ac, si ibi duo aequalia darentur, etiam hic talia esse deberent, quod foret absurdum.

[*Additamentum*][1]): Si x et y non-residua, erit $y = \alpha x$ et $xy = \alpha xx$, iam si numerus non-residuorum = numero residuorum; demonstrandum est xx inter residua contineri.

208. Statim ergo atque est $n < \mu$, ad minimum dantur n non-residua, quae si omnia complectantur, erit tam residuorum quam non-residuorum numerus $= n + n$ ipsi μ aequandus, unde fit $n = \frac{\mu}{2}$; hinc si $n < \mu$, fieri nequit, ut numerus residuorum n semissem numeri μ superet.

209. Si in modo expositis non-residuis $x, \alpha x, \beta x, \gamma x$ etc. non omnia occurrant, sit y numerus $< d$ ad eumque primus, qui neque in his non-residuis neque residuis reperiatur, atque simili modo etiam hi numeri $\alpha y, \beta y, \gamma y$ etc. a praecedentibus diversi ad non-residua referri debent, sicque denuo n numeri ad non-residua accedunt.

210. Si his duobus ordinibus nondum omnia non-residua exhauriantur, novus ordo accedet pariter n terminis constans; ac fortasse denuo novus totidem constans terminis; unde colligitur numerum omnium non-residuorum, nisi sit nullus, vel ipsi numero n vel eius duplo vel triplo vel in genere multiplo cuicunque aequari.

211. Cum igitur omnia non-residua una cum residuis multitudinem omnium numerorum ipso divisore d minorum ad eumque primorum exhaurire debeant, erit vel $n = \mu$ vel $2n = \mu$ vel $3n = \mu$ etc., sicque semper exponens n est pars aliquota numeri μ.

---

1) Vide notam p. 203. Assertio huius additamenti generaliter non vera est. R. F.

212. Quodsi ergo b et d sint numeri inter se primi, et μ denotet multitudinem omnium numerorum ad d primorum ipsoque minorum, tum vero b^n fuerit minima potestas post casum $n = 0$, quae per d divisa unitatem relinquat, tum erit vel $n = \mu$ vel n aequabitur parti cuipiam aliquotae ipsius μ, ita ut sit $n = \frac{\mu}{m}$ existente m divisore quopiam ipsius μ.

213. Cum autem post potestatem b^n etiam omnes istae b^{2n}, b^{3n}, b^{4n} etc. unitatem pro residuo agnoscant, semper potestas $b^{mn} = b^\mu$ per d divisa unitatem relinquet. Hinc dum b et d fuerint numeri inter se primi, haec formula $b^\mu - 1$ semper per numerum d erit divisibilis[1]).

214. Si praeterea etiam c et d fuerint numeri inter se primi, quoniam $c^\mu - 1$ divisionem per d admittit, harum formularum differentia $b^\mu - c^\mu$ semper per numerum d erit divisibilis, dummodo uterque numerus b et c ad d fuerit primus.

215. Si pro d sumamus numerum primum p, erit $\mu = p - 1$, atque haec formula $b^{p-1} - 1$ semper erit per p divisibilis, nisi ipse numerus b fuerit multiplum ipsius p. Fieri autem potest, ut forma simplicior $b^n - 1$ etiam divisionem per p admittat, ubi autem necessario requiritur, ut exponens n sit pars aliquota ipsius $p - 1$.

216. Si divisor sit $d = pq$ existentibus p et q numeris primis inaequalibus, neque b alterutrum horum numerorum complectatur, tum ob $\mu = (p-1)(q-1)$ haec forma $b^{(p-1)(q-1)} - 1$ per d erit divisibilis.

217. Ac si existentibus p, q, r, s numeris primis inaequalibus fuerit $d = p^\lambda q^\mu r^\nu s^\xi$ ac b numerus quicunque ad d primus, tum posito

$$m = p^{\lambda-1}(p-1)\, q^{\mu-1}(q-1)\, r^{\nu-1}(r-1)\, s^{\xi-1}(s-1)$$

haec forma $b^m - 1$ semper per d erit divisibilis; atque interdum fieri potest, ut formula simplicior $b^n - 1$ existente n parte quapiam aliquota ipsius m divisibilis evadat.

218. Sed retineamus divisorem generalem d, sitque μ multitudo numerorum ipso minorum ad eumque primorum, pro b autem sumatur numerus quicunque ad d primus, cuius minima potestas per d divisa unitatem relinquens

---

1) Hoc celeberrimum theorema FERMATIANUM EULERUS eadem methodo demonstravit in Commentatione 271 indicis ENESTROEMIANI, novi comm. acad. sc. Petrop. 8 (1760/1), 1763, § 55. *LEONHARDI EULERI Opera omnia*, vol. 2 seriei I, p. 531 et 554. R. F.

sit b^n, atque vidimus necessario fore vel $n = \mu$ vel $n = \frac{1}{2}\mu$ vel $n = \frac{1}{3}\mu$ vel $n = \frac{1}{4}\mu$ vel $n = \frac{1}{5}\mu$, siquidem μ tales partes aliquotas admittat, quos casus diligentius evolvi conveniet.

219. Statim quidem suspicari licet hoc discrimen ab indole numeri b pendere, ita ut pro dato divisore d certi numeri pro b sumti praebeant $n = \mu$, alii $n = \frac{1}{2}\mu$, alii $n = \frac{1}{3}\mu$, alii $n = \frac{1}{4}\mu$ seu adhuc minori parti aliquotae ipsius μ.

220. Quaecunque autem n sit pars aliquota ipsius μ, si binae potestates b^n et c^n unitatem relinquant, etiam composita $(bc)^n$ unitatem relinquet. Deinde etiam manifestum est potestatem $(b \pm \lambda d)^n$ per d divisam esse relicturam unitatem.

221. Cum potestas b^μ semper unitatem relinquat, quaeramus numeros pro b sumendos, ut etiam $b^{\frac{1}{2}\mu}$ unitatem relinquat, quo casu ante omnia necesse est, ut μ sit numerus par, quod quidem semper evenit, nisi sit $d = 2$.

222. Si iam capiatur $b = ee$, ita ut e sit numerus ad d primus, certum est $b^{\frac{1}{2}\mu} = e^\mu$ unitatem relinquere, quod etiam evenit, si $b = ee \pm \lambda d$. Minores ergo numeri pro b sumendi sunt residua, quae ex divisione numerorum quadratorum per d resultant, si modo quadrata ad d fuerint prima.

223. Simili modo potestas $b^{\frac{1}{3}\mu}$ per d divisa unitatem relinquet, si fuerit $b = e^3$, et generalius, si $b = e^3 \pm \lambda d$. Minores ergo valores ipsius b idonei sunt residua ex divisione cuborum ad d primorum per ipsum numerum d orta. Evidens autem est hoc evenire non posse, nisi numerus μ sit per 3 divisibilis.

224. Si μ per 4 sit divisibile, tum potestas $b^{\frac{1}{4}\mu}$ per d divisa unitatem relinquet, si fuerit $b = e^4$ et generalius $b = e^4 \pm \lambda d$. Minores ergo numeri sunt residua, quae ex divisione biquadratorum per d oriuntur iis, scilicet, tantum biquadratis sumendis, quae ad d sunt prima.

225. In genere ergo, si numerus μ divisibilis sit per ν, potestas $b^{\frac{\mu}{\nu}}$ per d divisa unitatem relinquet, si capiatur $b = e^\nu$ vel adeo $b = e^\nu \pm \lambda d$, ita ut idonei numeri pro b substituendi sint residua, quae ex divisione potestatum ordinis ν per numerum d oriuntur potestatibus illis ad d existentibus primis.

226. Sufficit ergo pro b numeros sumsisse ipso d minores, qui quidem ad eum sint primi; atque unitas quidem pro b sumta omnia residua unitati aequalia reddit, ita ut hoc casu semper sit $n = 1$ seu $n = \frac{\mu}{\mu}$. Casus autem iste solus relinquitur, si capiatur divisor $d = 2$, quippe quo fit $\mu = 1$.

227. Sit divisor $d = 3$, erit $\mu = 2$, et praeter casum $b = 1$, quo $n = 1$, habebimus casum $b = 2$, unde oritur progressio geometrica cum suis residuis:

Progressio geometrica:	1, 2, 2^2, 2^3, 2^4 etc.,
Residua:	1, 2, 1 , 2 , 1 etc.,

ubi est $n = 2$ seu $n = \mu$.

228. Sit divisor $d = 4$, erit $\mu = 2$, et praeter casum $b = 1$, quo $n = 1 = \frac{1}{2}\mu$, habemus casum $b = 3$.

Progressio geometrica:	1, 3, 3^2, 3^3, 3^4 etc.,
Residua:	1, 3, 1 , 3 , 1 etc.,

hinc ergo fit $n = 2 = \mu$.

229. Sit divisor $d = 5$, erit $\mu = 4$, et habebimus hos casus:

	$b = 1$	$b = 2$	$b = 3$	$b = 4$
Progressio geometrica	1, 1	1, 2, 2^2, 2^3, 2^4	1, 3, 3^2, 3^3, 3^4	1, 4, 4^2
Residua	1, 1	1, 2, 4 , 3 , 1	1, 3, 4 , 2 , 1	1, 4, 1
	$n = 1$	$n = 4$	$n = 4$	$n = 2$

Duobus ergo casibus hic est $n = 4$, uno $n = 2$ et uno $n = 1$.

230. Si divisor $d = 6$, erit $\mu = 2$, et duo erunt casus:

	$b = 1$	$b = 5$
Progressio geometrica	1, 1	1, 5, 5^2
Residua	1, 1	1, 5, 1
	$n = 1$	$n = 2$

231. Si divisor $d = 7$, erit $\mu = 6$ totidemque habentur casus:

	$b = 1$	$b = 2$	$b = 3$	$b = 4$
Progressio geometrica	1, 1	1, 2, 2^2, 2^3	1, 3, 3^2, 3^3, 3^4, 3^5, 3^6	1, 4, 4^2, 4^3
Residua	1, 1	1, 2, 4 , 1,	1, 3, 2 , 6 , 4 , 5 , 1	1, 4, 2 , 1
	$n = 1$	$n = 3$	$n = 6$	$n = 3$

	$b = 5$	$b = 6$
Progressio geometrica	1, 5, 5^2, 5^3, 5^4, 5^5, 5^6	1, 6, 6^2
Residua	1, 5, 4 , 6 , 2 , 3 , 1	1, 6, 1
	$n = 6$	$n = 2$

232. Si divisor $d = 8$, erit $\mu = 4$ totidemque casus:

	$b = 1$	$b = 3$	$b = 5$	$b = 7$
Progressio geometrica	1, 1	1, 3, 3^2	1, 5, 5^2	1, 7, 7^2
Residua	1, 1	1, 3, 1	1, 5, 1	1, 7, 1
	$n = 1$	$n = 2$	$n = 2$	$n = 2$

Nullo ergo casu erit $n = \mu$, sed tribus $n = \frac{1}{2}\mu$ et uno casu $n = \frac{1}{4}\mu$.

233. Si divisor sit $d = 9$, erit $\mu = 6$ totidemque casus:

	$b = 1$	$b = 2$	$b = 4$
Progressio geometrica	1, 1	1, 2, 2^2, 2^3, 2^4, 2^5, 2^6	1, 4, 4^2, 4^3
Residua	1, 1	1, 2, 4 , 8 , 7 , 5 , 1	1, 4, 7 , 1
	$n = 1$	$n = 6$	$n = 3$

	$b = 5$	$b = 7$	$b = 8$
Progressio geometrica	1, 5, 5^2, 5^3, 5^4, 5^5, 5^6	1, 7, 7^2, 7^3	1, 8, 8^2
Residua	1, 5, 7 , 8 , 4 , 2 , 1	1, 7, 4 , 1	1, 8, 1
	$n = 6$	$n = 3$	$n = 2$

234. Si sit divisor $d = 10$, erit $\mu = 4$:

	$b = 1$	$b = 3$	$b = 7$	$b = 9$
Progressio geometrica	1, 1	1, 3, 3^2, 3^3, 3^4	1, 7, 7^2, 7^3, 7^4	1, 9, 9^2
Residua	1, 1	1, 3, 9 , 7 , 1	1, 7, 9 , 3 , 1	1, 9, 1
	$n = 1$	$n = 4$	$n = 4$	$n = 2$

235. Sit $d = 11$, erit $\mu = 10$ totidemque casus:

	$b = 1$	$b = 2$	$b = 3$
Progressio geometrica. . .	1, 1	1, 2, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9, 2^{10}	1, 3, 3^2, 3^3, 3^4, 3^5
Residua . . .	1, 1	1, 2, 4 , 8 , 5 , 10, 9 , 7 , 3 , 6 , 1	1, 3, 9 , 5 , 4 , 1
	$n = 1$	$n = 10$	$n = 5$

	$b = 4$	$b = 5$
Progressio geometrica	1, 4, 4^2, 4^3, 4^4, 4^5	1, 5, 5^2, 5^3, 5^4, 5^5
Residua	1, 4, 5 , 9 , 3 , 1	1, 5, 3 , 4 , 9 , 1
	$n = 5$	$n = 5$

	$b = 6$
Progressio geometrica	1, 6, 6^2, 6^3, 6^4, 6^5, 6^6, 6^7, 6^8, 6^9, 6^{10}
Residua	1, 6, 3 , 7 , 9 , 10, 5 , 8 , 4 , 2 , 1
	$n = 10$

	$b = 7$
Progressio geometrica	1, 7, 7^2, 7^3, 7^4, 7^5, 7^6, 7^7, 7^8, 7^9, 7^{10}
Residua	1, 7, 5 , 2 , 3 , 10 , 4 , 6 , 9 , 8 , 1
	$n = 10$

	$b = 8$
Progressio geometrica	1, 8, 8^2, 8^3, 8^4, 8^5, 8^6, 8^7, 8^8, 8^9, 8^{10}
Residua	1, 8, 9 , 6 , 4 , 10 , 3 , 2 , 5 , 7 , 1
	$n = 10$

	$b = 9$	$b = 10$
Progressio geometrica	1, 9, 9^2, 9^3, 9^4, 9^5	1, 10, 10^2
Residua	1, 9, 4 , 3 , 5 , 1	1, 10, 1
	$n = 5$	$n = 2$

236. Sit $d = 12$, erit $\mu = 4$ totidemque casus:

	$b = 1$	$b = 5$	$b = 7$	$b = 11$
Progressio geometrica	1, 1	1, 5, 5^2	1, 7, 7^2	1, 11, 11^2
Residua	1, 1	1, 5, 1	1, 7, 1	1, 11, 1
	$n = 1$	$n = 2$	$n = 2$	$n = 2$

Hic ergo semper est $n < \mu$, tribus casibus, scilicet, $n = \frac{1}{2}\mu$ et uno $n = \frac{1}{4}\mu$.

237. Si sit divisor $d = 13$, erit $\mu = 12$, et pro minima potestate b^n, quae per 13 divisa relinquit unitatem, reperitur

si b	1,	2,	3,	4,	5,	6,	7,	8,	9,	10,	11,	12,
est n	1,	12,	3,	6,	4,	12,	12,	4,	3,	6,	12,	2.

238. Quemadmodum semper, si $b = 1$, fit $n = 1$, quicunque fuerit divisor d, ita etiam sumto $b = d - 1$ fit $n = 2$ seu $(d-1)^2$ per d divisum relinquit unitatem, quod in potestate prima numquam contingit[1]). De reliquis autem valoribus pro b assumtis difficilius est iudicium.

239. Quoniam potestas $(kd + 1)^n$ per d divisa relinquit 1, si fuerit $kd + 1 = bc$, et potestas b^n per d divisa relinquat etiam unitatem, tum quoque potestas c^n unitatem relinquet. Cum enim b^n relinquat 1, productum $b^n c^n$ relinquet c^n, at per hypothesin $b^n c^n$ relinquit 1; ergo in aestimatione residuorum c^n aequivalet unitati, seu c^n per d divisum unitatem relinquet.

240. Quare, si b^n fuerit minima potestas per d divisa unitatem relinquens, sitque $bc = kd + 1$, minima potestas ipsius c unitatem relinquens vel erit c^n vel adhuc minor exponente existente parte aliquota ipsius n. At si minor potestas ipsius c, puta $c^{\frac{n}{\nu}}$, relinqueret unitatem, etiam talis potestas ipsius b relinqueret unitatem; quod cum sit contra hypothesin, sequitur, si b^n fuerit minima potestas unitatem relinquens, etiam c^n fore minimam potestatem 1 relinquentem.

241. Ita posito $d = 13$, quia 5^4 est minima potestas unitatem relinquens, si sit $5c = 13k + 1$, erit quoque c^4 minima potestas unitatem relinquens. Verum, ut fiat $13k + 1$ per 5 divisibile, sumi debet $k = 5\lambda - 2$, eritque

1) $d \neq 2$. R. F.

$c = 13\lambda - 5$, cuius minimus valor est $c = 8$, ita ut etiam 8^4 sit minima potestas per 13 divisa unitatem relinquens.

242. Quicunque autem fuerit numerus b minor quam d ad eumque primus, semper quoque dabitur numerus c, etiam minor quam d ad eumque primus, ut sit $bc = kd + 1$, neque plures. Si enim duo dentur, ut esset tam $bc = kd + 1$ quam $be = ld + 1$, foret $bc - be = b(c - e)$ per d divisibile, unde ob b et d primos esset $c - e$ per d divisibile, quod, cum c et e sint minores quam d, fieri nequit, nisi sit $e = c$. Hoc autem evenire potest, ut fiat $c = b$, quod semper contingit, si sit vel $b = 1$ vel $b = d - 1$.

CAPUT 8

DE POTESTATIBUS NUMERORUM, QUAE PER NUMEROS PRIMOS DIVISAE UNITATEM RELINQUUNT[1])

243. Quodcunque residuum potestas a^n per numerum d divisa relinquit, idem etiam relinquent omnes potestates eiusdem exponentis $(a + \lambda d)^n$, atque, si n fuerit numerus par, idem residuum relinquet etiam potestas $(\lambda d - a)^n$, unde iudicium residuorum ad numeros a divisore d minores revocatur.

244. Sit iam divisor d numerus primus quicunque, et quia binarius nullam habet difficultatem, ponatur $d = 2p + 1$, eritque $2p$ multitudo numerorum ipso d minorum ad eumque primorum. Iam si a sit numerus quicunque ad d primus, quod fit, dummodo a non sit d eiusve multiplum, vidimus eius potestatem a^{2p} per $d = 2p + 1$ divisam semper unitatem relinquere.

245. Saepe autem evenire potest, ut etiam potestas inferior a^n existente $n < 2p$ per eundem numerum $d = 2p + 1$ divisa unitatem relinquat; tum autem exponens n certo est pars aliquota ipsius $2p$. Quod ergo si evenit, non solum formula $a^{2p} - 1$, sed etiam formula $a^n - 1$ per numerum primum $2p + 1$ erit divisibilis.

246. Quodsi ergo formula $a^n - 1$ fuerit divisibilis per numerum primum $2p + 1$, erit etiam formula $a^{mn} - 1$ divisibilis, unde, cum formula $a^{2p} - 1$ certo sit etiam per $2p + 1$ divisibilis, erit etiam differentia $a^{mn} - a^{2p}$ seu $a^{2p}(a^{mn-2p} - 1)$ divisibilis; quare, cum factor a^{2p} divisionem non admittat, alter $a^{mn-2p} - 1$ divisibilis sit, necesse est, quicunque numerus pro m sumatur.

1) Vide Commentationes 134 et 262 indicis ENESTROEMIANI, novi comm. acad. sc. Petrop. 1 (1747/48), 1750, p. 20, et 7 (1758/9), 1761, p. 49; *LEONHARDI EULERI Opera omnia*, series I, vol. 2, p. 62 et p. 493. R. F.

247. Sit λ maximus communis divisor numerorum n et $2p$; ac si formula $a^n - 1$ fuerit divisibilis per numerum primum $2p + 1$, etiam haec formula $a^\lambda - 1$ per $2p + 1$ erit divisibilis. Sit enim $n = \alpha\lambda$ et $2p = \beta\lambda$, ut α et β sint numeri primi inter se, et quoniam tam $a^{\alpha\lambda} - 1$ quam $a^{\beta\lambda} - 1$ sunt multipla ipsius $2p + 1$, etiam hae formulae $a^{\mu\alpha\lambda} - 1$ et $a^{\nu\beta\lambda} - 1$ erunt multipla. At ob α et β numeros primos [inter se], μ et ν ita accipi possunt, ut fiat $\mu\alpha = \nu\beta + 1$, unde differentia erit $a^{\nu\beta\lambda+\lambda} - a^{\nu\beta\lambda} = a^{\nu\beta\lambda}(a^\lambda - 1)$, quae cum sit divisibilis per $2p + 1$, necesse est, sit $a^\lambda - 1$ per $2p + 1$ divisibile.

248. Si ergo n est numerus ad $2p$ primus, forma $a^n - 1$ divisibilis esse nequit per numerum primum $2p + 1$, nisi sit $a - 1$ per eundem divisibile. Unde, si $a - 1$ non sit multiplum numeri primi $2p + 1$, formula $a^n - 1$ per eum divisibilis esse nequit, nisi n et $2p$ sint numeri inter se compositi; quorum si maximus communis divisor sit λ, adeo haec formula $a^\lambda - 1$ per $2p + 1$ erit divisibilis.

249. Si igitur a^n fuerit minima potestas ipsius a, quae per numerum primum $2p + 1$ [divisa] unitatem relinquit, tum certe est n pars aliquota numeri $2p$. Tum autem, si fuerit $ab = k(2p + 1) + 1$, erit etiam b^n minima potestas ipsius b, quae per $2p + 1$ divisa unitatem relinquit.

250. Si n sit numerus primus et formula $a^n - 1$ divisibilis per numerum primum $2p + 1$, vel erit n pars aliquota ipsius $2p$ (quia alius communis divisor locum non habet) vel, si fuerit ad $2p$ primus, numerus $a - 1$ per $2p + 1$ erit divisibilis. Quare praeter divisores ipsius $a - 1$ formula $a^n - 1$ alios divisores primos non admittit, nisi huiusmodi formae $2p + 1$, ut $2p$ sit multiplum ipsius n. Unde omnes eius divisores primi in hac forma $2mn + 1$ continebuntur[1]).

251. Quare haec forma $a^3 - 1$ praeter divisorem $a - 1$ alios divisores primos non admittit nisi formae $6m + 1$, qui sunt 7, 13, 19, 31, 37, 43, 61, 67, 73, 79, 97 etc. Cum ergo $aa + a + 1$ sit factor ipsius $a^3 - 1$, etiam is per nullos alios numeros primos est divisibilis.

252. Simili modo forma $a^5 - 1$ praeter divisorem $a - 1$ alios non habet, nisi qui in forma $10m + 1$ contineantur, quales sunt 11, 31, 41, 61, 71 etc. Quare etiam tales numeri $a^4 + a^3 + aa + a + 1$, nisi sint primi, alios divisores non admittunt.

253. Quoniam numeri perfecti inveniuntur, quoties formula $2^n - 1$ est numerus primus, primum patet hoc evenire non posse, nisi n sit numerus

1) $n \neq 2$; si $n = 2$, forma generalis est $mn + 1$. R. F.

primus. At si n fuerit talis, formula $2^n - 1$ certe alios non habet divisores nisi formae $2mn+1$ [1]), unde exploratio, utrum sit primus necne, faciliori negotio absolvitur.

254. Cum $a^{2p} - 1$ semper sit divisibile per numerum primum $2p + 1$, illa autem forma constet factoribus $a^p - 1$ et $a^p + 1$, necesse est, ut alteruter per $2p + 1$ sit divisibilis. Vidimus autem, si sit $a = ee \pm \lambda(2p + 1)$, fore $a^p - 1$ divisibilem; his ergo casibus formula $a^p + 1$ per $2p + 1$ certe non est divisibilis.

255. Hic quaestio oritur, num forte semper formula $a^p - 1$ per $2p + 1$ sit divisibilis, ideoque numquam altera $a^p + 1$, quod casu, quo p est numerus impar, statim negandum esse patet. Quia enim tum $a^p + 1$ factorem habet $a + 1$, ista formula sumto $a = 2p$ manifesto per $2p + 1$ fit divisibilis.

256. In genere autem sequenti modo ostendi potest formulam $a^n - 1$ existente $n < 2p$ non semper divisibilem esse per numerum primum $2p + 1$, sed dari utique eiusmodi numeros pro a adhibendos, quibus divisio formulae $a^n - 1$ non succedat, quod per deductionem ad absurdum sic commodissime demonstrabitur. [2])

257. Qui enim hoc negaverit, affirmare debet omnes has formulas $1^n - 1$, $2^n - 1$, $3^n - 1$, $4^n - 1$, $5^n - 1$, . . ., $(n + 1)^n - 1$ [3]) per $2p + 1$ esse divisibiles, ideoque etiam earum differentias tam primas $2^n - 1^n$, $3^n - 2^n$, $4^n - 3^n$, $5^n - 4^n$ etc. quam secundas $3^n - 2 \cdot 2^n + 1^n$, $4^n - 2 \cdot 3^n + 2^n$, $5^n - 2 \cdot 4^n + 3^n$ etc. et sequentes omnes.

258. Differentiae autem ordine n sunt constantes, quae, si littera N indicentur, ita exprimuntur, ut sit

$$N = (n + 1)^n - n \cdot n^n + \frac{n(n-1)}{1 \cdot 2}(n-1)^n - \frac{n(n-1)(n-2)}{1 \cdot 2 \cdot 3}(n-2)^n + \text{etc.},$$

cuius expressionis valores pro variis valoribus ipsius n facile colliguntur:

Si $n = 1$, est $N = 2 - 1 = 1$,
si $n = 2$, est $N = 3^2 - 2 \cdot 2^2 + 1 = 2 = 1 \cdot 2$,
si $n = 3$, est $N = 4^3 - 3 \cdot 3^3 + 3 \cdot 2^3 - 1 = 6 = 1 \cdot 2 \cdot 3$,
si $n = 4$, est $N = 5^4 - 4 \cdot 4^4 + 6 \cdot 3^4 - 4 \cdot 2^4 + 1 = 24 = 1 \cdot 2 \cdot 3 \cdot 4$
etc.

---

1) $n \neq 2$. R. F.

2) Confer Commentationem 241 indicis ENESTROEMIANI, novi comm. acad. sc. Petrop. 5 (1754/5), 1760, p. 3; *LEONHARDI EULERI Opera omnia*, vol. 2 seriei I, p. 328. R. F.

3) Manuscriptum: $n^n - 1$. $(n + 1)^{n+1} - 1$ per hypothesin factorem $2p + 1$ habet, si $n + 1 < 2p + 1$; propterea demonstratio non valet casu $n = 2p$. Correxit R. F.

259. Ad quod clarius ostendendum sit pro n scribendo $n + 1$:

$$P = (n+2)^{n+1} - (n+1)\,(n+1)^{n+1} + \frac{(n+1)n}{1\cdot 2}n^{n+1} - \frac{(n+1)n(n-1)}{1\cdot 2\cdot 3}(n-1)^{n+1} + \text{etc.},$$

et a termino anteriori incipiendo

$$P = (n+1)^{n+1} - (n+1)\,n^{n+1} + \frac{(n+1)n}{1\cdot 2}\,(n-1)^{n+1} - \text{etc.}$$

At valor ipsius N ita repraesentari potest

$$N = (n+1)^n - n^{n+1} + \frac{n}{1\cdot 2}\,(n-1)^{n+1} - \frac{n(n-1)}{1\cdot 2\cdot 3}\,(n-2)^{n+1} + \text{etc.},$$

quae per $n + 1$ multiplicata praebet valorem ipsius P, ita ut sit $P = (n+1)N$.

260. Cum igitur casu $n = 1$ sit $N = 1$, casu $n = 2$ erit $N = 1 \cdot 2$, casu $n = 3$ erit $N = 1 \cdot 2 \cdot 3$, et in genere pro numero quocunque n erit $N = 1 \cdot 2 \cdot 3 \ldots n$. At haec differentia ordinis n non est divisibilis per numerum primum $2p + 1$, ob $n < 2p$; unde sequitur non omnes terminos seriei paragrapho 257 expositae per eum esse divisibiles.

261. Sit $6p + 1$ numerus primus, et cum forma $a^{6p} - 1$ per eum sit divisibilis, nisi a eius sit multiplum, dabuntur casus, quibus etiam $a^{2p} - 1$ per eum dividi poterit, scilicet sumto $a = e^3 \pm \lambda(6p + 1)$. Tum vero etiam dantur casus, quibus formula $a^{2p} - 1$ non erit divisibilis per istum numerum primum $6p + 1$, uti ex demonstratione modo allata patet

262. Cum ante ostenderimus formulam $a^{3p} - 1$ fore per $6p + 1$ divisibilem, si fuerit

$$a = cc \pm \lambda(6p + 1),$$

nunc colligere licet, si numerus a simul in hac forma $cc \pm \lambda(6p + 1)$ et in hac $e^3 \pm \lambda(6p + 1)$ contineatur, tum etiam formulam $a^p - 1$ per $6p + 1$ fore divisibilem, id quod quoque continget, si fuerit $a = e^6 \pm \lambda(6p + 1)$.

263. Si sit $4p + 1$ numerus primus, ut $a^{4p} - 1$ per eum sit divisibile, tum adeo $a^p - 1$ per eum dividi poterit, si fuerit $a = e^4 \pm \lambda(4p + 1)$. Dantur vero etiam casus, quibus formula $a^p - 1$ [divisionem] non admittet; iis ergo vel $a^p + 1$ vel $a^{2p} + 1$ certe per $4p + 1$ erit divisibile.

CAPUT 9

DE DIVISORIBUS NUMERORUM FORMAE $a^n \pm b^n$

264. Posito $2p + 1$ numero primo, dum a et b eius non sint multipla, tam haec formula $a^{2p} - 1$ quam ista $b^{2p} - 1$ per eum erit divisibilis; ideoque etiam earum differentia $a^{2p} - b^{2p}$ semper per numerum primum $2p + 1$ divisionem admittet.

265. Ponamus iam numerum $a^n - b^n$ divisibilem esse per numerum primum $2p + 1$, et ut exploremus, quomodo hoc fieri possit, ponamus φ esse maximum communem divisorem numerorum n et $2p$, ita ut posito $n = \alpha\varphi$ et $2p = \beta\varphi$ numeri α et β futuri sint primi inter se.

266. Cum autem α et β sint numeri primi inter se, fieri potest $\mu\alpha = \nu\beta + 1$. Quare, cum $a^{\alpha\varphi} - b^{\alpha\varphi}$ per $2p + 1$ sit divisibilis, etiam $a^{\mu\alpha\varphi} - b^{\mu\alpha\varphi}$, hoc est $a^{(\nu\beta+1)\varphi} - b^{(\nu\beta+1)\varphi}$ erit divisibilis, tum vero ob $a^{\beta\varphi} - b^{\beta\varphi}$ quoque hic numerus $a^{\nu\beta\varphi} - b^{\nu\beta\varphi}$, necnon idem per a^{φ} multiplicatus, scilicet $a^{(\nu\beta+1)\varphi} - a^{\varphi} b^{\nu\beta\varphi}$.

267. Auferatur haec posterior forma a praecedente, et differentia $a^{\varphi} b^{\nu\beta\varphi} - b^{(\nu\beta+1)\varphi} = b^{\nu\beta\varphi}(a^{\varphi} - b^{\varphi})$ divisibilis erit per numerum primum $2p + 1$; at $b^{\nu\beta\varphi}$ per eum non est divisibilis, ergo alter factor $a^{\varphi} - b^{\varphi}$ divisibilis sit, necesse est.

268. Quare, si numerus $a^n - b^n$ divisibilis sit per numerum primum $2p + 1$ fueritque φ maximus communis divisor numerorum n et $2p$, etiam hic numerus $a^{\varphi} - b^{\varphi}$ per $2p + 1$ divisibilis erit, et nisi posterior divisionem admittat, ne prior quidem admittet.

269. Quodsi ergo n et $2p$ fuerint numeri inter se primi seu unitas maximus eorum communis divisor, nisi $a - b$ sit divisibile per $2p + 1$, etiam $a^n - b^n$ per hunc numerum primum divisionem non admittet.

270. Divisores ergo primos numeri $a^n - b^n$ investigaturi praeter divisores ipsius $a - b$, qui sponte se offerunt, reliquos quaerere debemus inter eos numeros primos $2p + 1$, in quibus $2p$ ad n non est primus sed compositus.

271. Unde, si n sit numerus primus, omnes divisores numeri $a^n - b^n$ praeter eos, quos $a - b$ continet, tantum inter numeros primos huius formae $\lambda n + 1$ quaerere debemus, siquidem a et b sint numeri primi inter se, quam conditionem adiici debere manifestum est.

272. Pro variis ergo valoribus ipsius n divisores primi formae $a^n - b^n$ praeter $a - b$ quaeri debent, ut sequitur:

formae	divisores quaeri debent inter hos numeros primos
$a^2 - b^2$	$2\lambda + 1$: 3, 5, 7, 11, 13, 17, 19, nullis exclusis,
$a^3 - b^3$	$3\lambda + 1$: 7, 13, 19, 31, 37, 43, 61, 67, 73, 79, 97 etc.
$a^5 - b^5$	$5\lambda + 1$: 11, 31, 41, 61, 71, 101 etc.
$a^7 - b^7$	$7\lambda + 1$: 29, 43, 71, 113, 127 etc.
$a^{11} - b^{11}$	$11\lambda + 1$: 23, 67, 89, 199, 331 etc.
	etc.

[*Additamentum*][1]): Ad divisores formae $a^n - b^n$ etiam accedere potest ipse numerus n. Ex $a^3 - b^3$ sequitur numerum $aa + ab + bb$ alios divisores habere non posse nisi $3\lambda + 1$; ergo $3\lambda - 1$ certe non sunt divisores.

273. Si n non sit numerus primus sed productum duorum primorum, puta $n = \alpha\beta$, divisores primi formae $a^{\alpha\beta} - b^{\alpha\beta}$ praeter $a - b$ continentur in forma $2p + 1$ existente $2p$ ad $\alpha\beta$ non primo, unde, prout vel α vel β vel adeo $\alpha\beta$ fuerit maximus communis divisor, forma divisorum primorum erit vel $\lambda\alpha + 1$ vel $\lambda\beta + 1$ vel $\lambda\alpha\beta + 1$, in quarum prima λ non debet continere β, in secunda autem non α, in tertia vero non limitatur.

274. At divisores formae $\lambda\alpha + 1$ simul dividunt $a^\alpha - b^\alpha$, et divisores formae $\lambda\beta + 1$ simul hanc $a^\beta - b^\beta$, siquidem in priore λ sit numerus primus ad β, in posteriore autem ad α.

275. Quare, si formulae $a^{\alpha\beta} - b^{\alpha\beta}$ ii tantum divisores desiderentur, qui non simul dividant vel $a^\alpha - b^\alpha$ vel $a^\beta - b^\beta$, ii quaeri debent inter numeros primos formae $\lambda\alpha\beta + 1$; sin autem tantum divisores formae $a^\alpha - b^\alpha$ excludere velimus, reliquos inter numeros primos $\lambda\beta + 1$ quaerere debemus.

276. Sit $\alpha = 2$ et $\beta = 2$, atque omnes divisores primi huius numeri $a^4 - b^4$, qui non simul dividant $a^2 - b^2$, continebuntur in forma $4\lambda + 1$; hique ergo divisores erunt numeri $a^2 + b^2$; unde patet numeros formae $a^2 + b^2$ alios divisores primos [excepto numero 2] non admittere, nisi qui sint formae $4\lambda + 1$ [2]).

277. Sit $\alpha = 3$ et $\beta = 2$, atque omnes divisores primi numerorum $a^6 - b^6$, qui non simul dividant $a^3 - b^3$, continentur in forma $2\lambda + 1$; qui

1) Vide notam p. 203. R. F.

2) Vide Commentationem 134 p. 220 laudatam, art. 16, p. 68 et Commentationem 164 indicis ENESTROEMIANI, comm. acad. sc. Petrop. 14 (1744/6), 1751, p. 151; *LEONHARDI EULERI Opera omnia*, series I, vol. 2, p. 194. R. F.

autem insuper quoque non $a^2 - b^2$ dividant in hac $6\lambda + 1$; hi ergo erunt divisores formae $a^2 - ab + b^2$, neque tales numeri alios divisores agnoscunt.

278. Ex his in genere colligimus, si definiendi sint divisores numeri $a^{2m} - b^{2m}$, qui non simul sint divisores numeri $a^m - b^m$, hoc est, si desiderentur divisores numeri $a^m + b^m$, eos inter numeros primos huius formae $2\lambda m + 1$ quaeri oportere. Hinc autem excluditur divisor $a + b$, si m sit numerus impar[1]).

279. Ita pro variis valoribus ipsius m faciamus hanc tabulam:

Numerorum formae	divisores quaeri debent inter numeros primos	
	formae	qui sunt
$a^2 + b^2$	$4\lambda + 1$	5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97
$a^3 + b^3$	$6\lambda + 1$	7, 13, 19, 31, 37, 43, 61, 67, 73, 79, 97
$a^4 + b^4$	$8\lambda + 1$	17, 41, 73, 89, 97, 113, 137, 193
$a^5 + b^5$	$10\lambda + 1$	11, 31, 41, 61, 71, 101, 131, 151, 181
$a^6 + b^6$	$12\lambda + 1$	13, 37, 61, 73, 97, 109, 157, 181, 193
$a^7 + b^7$	$14\lambda + 1$	29, 43, 71, 113, 127, 197, 211, 239
$a^8 + b^8$	$16\lambda + 1$	17, 97, 113, 193, 241, 257, 337
		etc.

Hic casus, ubi exponens est potestas binarii, prae reliquis sunt notandi, quia in reliquis generatim divisores assignari possunt. Tales ergo numeri $a^{2^n} + b^{2^n}$ alios divisores primos non habent, nisi qui in forma $2^{n+1}\lambda + 1$ contineantur.

280. At $a^n - b^n$ dividi poterit per numerum primum $mn + 1$, si numeri a et b ita fuerint comparati, ut $ax^m - by^m$ fiat divisibile per $mn + 1$; dum scilicet pro x et y numeri assignari queant, quibus ista conditio adimpleatur, tum certe $a^n - b^n$ per $mn + 1$ erit divisibile.

281. Si enim $ax^m - by^m$ sit divisibile per $mn + 1$, tum etiam $a^n x^{mn} - b^n y^{mn}$ erit divisibile. At semper divisibilis est haec forma $x^{mn} - y^{mn}$, ideoque etiam ista $a^n x^{mn} - a^n y^{mn}$; quamobrem etiam differentia $ay^{mn} - b^n y^{mn}$, ac proinde $a^n - b^n$ per numerum primum $mn + 1$ divisibilis erit.

---

1) Et divisores $a^{\frac{m}{n}} + b^{\frac{m}{n}}$, si n sit factor numeri imparis m. R. F.

282. Si ergo pro a et b eiusmodi numeri assumantur, ut $a^n - b^n$ non sit divisibile per numerum quempiam primum $mn + 1$, tum nulli numeri pro x et y assignari poterunt, ut $ax^m - by^m$ per eundem numerum primum $mn + 1$ divisionem admittat, nisi quidem uterque numerus x et y sit eiusdem multiplum; statuuntur autem x et y primi inter se.

283. Sic cum $2^2 - 1$ tantum per 3 sit divisibile, fueritque $2m + 1$ numerus primus, tum, nisi sit $m = 1$, nullus numerus in hac forma contentus $2x^m - y^m$ per illum numerum primum $2m + 1$ dividi poterit.

Ita posito	nullus numerus	divisibilis erit per
$m = 2$	$2x^2 - y^2$	5
$m = 3$	$2x^3 - y^3$	7
$m = 5$	$2x^5 - y^5$	11
$m = 6$	$2x^6 - y^6$	13
	etc.	

CAPUT 10
DE RESIDUIS DIVISIONE QUADRATORUM PER NUMEROS PRIMOS ORTIS

284. Quod residuum relinquitur, si quadratum a^2 per numerum quemvis d dividitur, idem quoque relinquitur, si haec infinita quadrata $(nd \pm a)^2$ per eundem numerum d dividantur.

285. Quare, si residua examinare velimus, quae divisione numerorum quadratorum per datum numerum d relinquuntur, sufficiet quadrata considerasse, quorum radices sint ipso hoc divisore d minores, ideoque haec

$$1, 4, 9, 16, \ldots, (d-4)^2, (d-3)^2, (d-2)^2, (d-1)^2,$$

quorum numerus est $d - 1$.

286. At quadrata extrema 1 et $(d-1)^2$, et quaevis bina ab extremis aeque remota paria dant residua; unde, si $d - 1$ sit numerus par, plura residua diversa resultare nequeunt, quam $\frac{1}{2}(d-1)$, et si $d - 1$ est numerus impar, ob unum in medio positum, quam $\frac{1}{2}d$.

287. Sit iam d numerus primus, et quia binarii iudicium in promptu est, ponatur $d = 2p + 1$, cum nunc omnia residua ex his quadratis resultent

$$1, 4, 9, \ldots, (p-2)^2, (p-1)^2, p^2,$$

eorum numerus maior esse nequit quam p, unde manifestum est non omnes numeros ipso $d = 2p + 1$ minores, quorum multitudo est $2p$, inter residua occurrere, sed ad minimum eorum semissem excludi.

288. Primum autem dico omnia residua ex his quadratis $1, 4, 9, \ldots, p^2$ oriunda inter se esse inaequalia; si enim duo quadrata ipso p^2 non maiora, puta m^2 et n^2, idem darent residuum, eorum differentia $m^2 - n^2$, ideoque vel $m - n$ vel $m + n$ per divisorem primum $d = 2p + 1$ esset divisibilis, quod, cum ob $m < \frac{1}{2}d$ et $n < \frac{1}{2}d$ sit $m + n$ minus quam d, fieri nequit.

289. Cum igitur omnia residua ex divisione quadratorum $1, 4, 9, \ldots, p^2$ per numerum primum $d = 2p + 1$ orta sint inaequalia, ea ita repraesentemus:

radices:	$1, 2, 3, 4, 5, 6, \ldots, p,$
quadrata:	$1, 4, 9, 16, 25, 36, \ldots, p^2,$
residua:	$1, \alpha, \beta, \gamma, \delta, \varepsilon, \ldots, \pi,$

et multitudo horum residuorum erit $= p$.

290. Cum iam multitudo omnium numerorum ipso divisore $2p + 1$ minorum, qui simul ad eum sunt primi, sit $= 2p$, patet horum numerorum semissem ex ordine residuorum excludi, quos ideo *non-residua* appellemus[1]). Erit ergo multitudo *non-residuorum* pariter $= p$, quae litteris germanicis $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D}$ etc. indicemus.

291. Si ergo pro quovis divisore primo $2p + 1$ haec *non-residua* invenerimus, affirmare poterimus nullum dari numerum quadratum xx, ita ut $xx - \mathfrak{A}$ esset per $2p + 1$ divisibile, denotante $\mathfrak{A}$ non-residuum quodcunque. Ac tales formulae $xx - \mathfrak{A}$ per $2p + 1$ individuae tot semper exhiberi possunt, quot p continet unitates.

292. Pro quovis ergo divisore primo $2p + 1$ numeri ipso minores distinguuntur in duas classes, quarum altera *residua*, altera vero *non-residua* complectitur, et utraque totidem continet numeros, ita ut quasi cuivis residuo suum respondeat non-residuum. Indolem ergo harum duarum classium accuratius scrutari conveniet.

---

1) Vide Commentationem 242 indicis ENESTRŒMIANI, novi comm. acad. sc. Petrop. 5 (1754/5), 1760, p. 18, art. 16, corollarium 4; *LEONHARDI EULERI Opera omnia*, series I, vol. 2, p. 343. R. F.

293. Si in ordine residuorum occurrant duo numeri m et n, in eodem quoque occurret eorum productum mn seu residuum ei aequivalens. Oriatur enim residuum m ex quadrato a^2 et n ex b^2, atque ex producto a^2b^2, quod pariter est quadratum, orietur residuum mn.

294. Si ergo inter residua sit numerus quicunque m, ibidem quoque reperientur omnes eius potestates m^2, m^3, m^4 etc. vel residua iis aequivalentia. Tum vero, si praeterea adsit numerus n, in eodem residuorum ordine quoque aderunt numeri mn, m^2n, mn^2 et in genere $m^\mu n^\nu$.

295. Ordo ergo residuorum $1, \alpha, \beta, \gamma, \ldots, \pi$ pro quovis divisore primo $2p + 1$ hanc insignem habet proprietatem, ut in eodem quoque producta ex binis pluribusve terminis quibuscunque occurrant, siquidem secundum indolem residuorum ad minimos valores revocentur.

296. Hoc eo magis est notatu dignum, quod ordo residuorum determinato terminorum [multitudine] constat, quorum scilicet numerus tantum sit $= p$ exclusis totidem numeris non-residuis. Hoc tamen non obstante, quomodocunque residua per multiplicationem inter se combinentur, tamen perpetuo numeri in eodem ordine iam contenti occurrunt.

297. Sit m numerus quicunque in ordine residuorum occurrens divisore primo existente $2p + 1$, ac supra vidimus, si termini progressionis geometricae $1, m, m^2, m^3, m^4$ etc. per $2p + 1$ dividantur, inter residua quoque omnia producta ex binis contineri; sicque in residuis harum potestatum nulli occurrent numeri, qui non simul in residuis quadratorum reperiantur.

298. Cum igitur multitudo residuorum ex potestatibus oriundorum superare nequeat multitudinem ex quadratis ortorum, quae est $= p$, manifestum est vel potestatem m^p vel adhuc inferiorem residuum praebere $= 1$. Quod quidem iam ostendimus, nam, si m ex quadrato aa oriatur, erit $m = aa - k(2p + 1)$ et $m^p - 1$ manifesto per numerum primum $2p + 1$ est divisibile.

299. Sed ad residua quadratorum revertentes notemus, si ibi occurrant numeri m et mn, tum etiam necessario ibidem numerum n reperiri debere. Si enim residuum m oriatur ex quadrato aa, et mn ex quadrato bb, ex naa quoque residuum mn nascetur, unde $bb - naa$ per $2p + 1$ erit divisibile existentibus a et b ad $2p + 1$ primis.

300. At si $bb - naa$ divisibile est per $2p+1$, etiam $(b+k(2p+1))^2 - naa$ erit divisibile. Semper autem k ita assumere licet, ut fiat $b + k(2p + 1) = ac$,

seu ut $k(2p+1)$ per a divisum relinquat [—] b. Dabitur ergo numerus c, ut sit $aacc - naa$, hoc est $cc - n$ per $2p+1$ divisibile, quare quadratum cc dabit residuum n.

301. Si in ordine residuorum sit numerus α, non-residuorum vero numerus $\mathfrak{A}$, productum $\alpha\mathfrak{A}$ in ordine non-residuorum certe reperietur. Si enim in ordine residuorum esset, ibidem quoque foret $\mathfrak{A}$ contra hypothesin.

302. Si in ordine residuorum occurrat productum mn, eiusque alter factor m in ordine non-residuorum, alter quoque n certo in eodem ordine non-residuorum reperietur; si enim hic n esset in residuis, eodem quoque m pertineret.

303. Si duo non-residua $\mathfrak{A}$ et $\mathfrak{B}$ in se ducantur, productum incidet in ordinem residuorum. Nam, cum in ordine residuorum omnia quadrata occurrant, primo evidens est omnia quadrata $\mathfrak{A}^2$, $\mathfrak{B}^2$, $\mathfrak{C}^2$ etc. ibi esse; quod vero etiam producta binorum $\mathfrak{AB}$ ibidem reperiantur, ulteriori indiget probatione iam instituenda.

304. Cognitis residuis $1, \alpha, \beta, \gamma$ etc., quorum numerus est $= p$ divisore primo existente $2p+1$, non-residua quidem eo ipso dantur, cum sint reliqui numeri minores quam $2p+1$, quorum numerus itidem est $= p$. At dato uno non-residuo $\mathfrak{A}$ reliqua omnia ex ipsis residuis ita determinantur, ut sint $\mathfrak{A}, \alpha\mathfrak{A}, \beta\mathfrak{A}, \gamma\mathfrak{A}$ etc., reductione scilicet ad minimos terminos facta. Sunt enim hi numeri inaequales inter se, et eorum multitudo $= p$.

305. Duo igitur quaecunque non-residua $\mathfrak{D}$ et $\mathfrak{E}$ spectari possunt tamquam huiusmodi producta $\delta\mathfrak{A}$ et $\varepsilon\mathfrak{A}$ existentibus δ et ε residuis, $\mathfrak{A}$ vero non-residuo; unde productum duorum quorumvis non-residuorum erit $\mathfrak{DE} = \delta\varepsilon\mathfrak{AA}$, ubi $\delta\varepsilon$ utpote productum duorum residuorum in ordine residuorum reperitur.

306. Tum vero in ordine residuorum occurrit etiam $\mathfrak{AA}$, quia in eo omnia plane quadrata seu residua aequivalentia reperiuntur. Quare, cum tam $\delta\varepsilon$ quam $\mathfrak{AA}$ sit residuum, eorum productum quoque $\mathfrak{DE}$ residuum sit, necesse est, sicque productum duorum quorumvis non-residuorum certe in ordine residuorum continetur.

307. Combinatio ergo duorum numerorum pro indole residuorum et non-residuorum ita se habet:

1. Productum ex duobus residuis est residuum.
2. Productum ex residuo et non-residuo est non-residuum.
3. Productum ex duobus non-residuis est residuum.

308. Non mediocriter haec illustrabuntur, si residua et non-residua ex divisione quadratorum per numeros primos contemplemur:

Divisor	3	5	7	11	13
Residua	1	1, 4	1, 4, 2	1, 4, 9, 5, 3	1, 4, 9, 3, 12, 10
Non-residua	2	2, 3	3, 5, 6	2, 6, 7, 8, 10	2, 5, 6, 7, 8, 11

Divisor	17	19
Residua	1, 4, 9, 16, 8, 2, 15, 13	1, 4, 9, 16, 6, 17, 11, 7, 5
Non-residua	3, 5, 6, 7, 10, 11, 12, 14	2, 3, 8, 10, 12, 13, 14, 15, 18

Divisor	23
Residua	1, 4, 9, 16, 2, 13, 3, 18, 12,[1]) 8, 6
Non-residua	5, 7, 10, 11,[2]) 14, 15, 17, 19, 20, 21, 22

Divisor	29
Residua	1, 4, 9, 16, 25, 7, 20, 6, 23, 13, 5, 28, 24, 22
Non-residua	2, 3, 8, 10, 11, 12, 14, 15, 17, 18, 19, 21, 26, 27

Divisor	59
Residua	1, -2, 3, 4, 5, -6, 7, -8, 9, -10, -11, 12, -13, -14, 15, 16, 17, -18, 19, 20, 21, 22, -23, -24, 25, 26, 27, 28, 29.

[*Additamentum*][3]): Ergo si $4n - 1$ est primus, vel $xx + myy$ vel talis forma $xx - myy$ per eum est divisibilis.

309. Complementum residui vocemus numerum, qui cum residuo faciat divisorem; ita si divisore existente $= d$ sit quodpiam residuum $= r$, eius complementum erit $d - r$.

310. Si cuiuspiam residui complementum occurrat in ordine residuorum, etiam omnium residuorum complementa ibidem occurrent. Nam, si in ordine residuorum $1, \alpha, \beta, \gamma, \delta$ etc. occurrat $d - \alpha$ divisore existente d, hoc residuum $d - \alpha$ etiam per $-\alpha = -1 \cdot \alpha$ repraesentari potest, quare, cum tam α quam productum $-1 \cdot \alpha$ sit residuum, etiam -1 erit residuum, ideoque etiam $-\beta, -\gamma, -\delta$ etc., quibus aequivalent complementa reliquorum residuorum.

1) Manuscriptum: 11. Correxit A. M.
2) Manuscriptum: 12. Correxit A. M.
3) Vide notam p. 203. R. F.

311. In serie ergo residuorum vel nullius vel omnium complementa occurrent. Ex superioribus exemplis patet, si divisor sit vel 3 vel 7 vel 11 vel 19 vel 23, nullius residui complementum in residuis reperiri, sed ea esse non-residua. Sin autem divisor sit 5 vel 13 vel 17 vel 29, in ordine residuorum quoque singulorum complementa inveniri.

312. Si divisor sit $2p + 1$ primus, atque in residuis quoque singulorum complementa occurrant, quoniam bina ita inter se cohaerent, ut alterum alterius sit complementum, neque idem sui ipsius complementum esse potest, ob $2p + 1$ semissem non admittentem, numerus residuorum necessario erit par.

313. Cum igitur numerus residuorum sit $= p$, nisi p sit numerus par, fieri nequit, ut residuorum complementa sint etiam residua. Quare, si p sit numerus impar, certum est nullius residui complementum in ordine residuorum contineri; ideoque omnium residuorum complementa ordinem non-residuorum constituent.

314. Sit igitur p numerus impar $= 2q - 1$, ut divisor primus sit $4q - 1$, atque omnium residuorum complementa erunt non-residua. Ita si quodpiam residuum sit α, eius complementum $4q - 1 - \alpha$ erit non-residuum, seu nullum datur quadratum, quod per $4q - 1$ divisum relinquat $4q - 1 - \alpha$.

315. Cum igitur α quodcunque quadratum denotare possit, puta nn, nullum datur quadratum, quod numero $4q - 1 - nn$ minutum per $4q - 1$ dividi queat. Hinc $mm - (4q - 1 - nn)$ seu $mm + nn$ numquam per numerum primum formae $4q - 1$ divisibile existet, nisi forte uterque numerus m et n seorsim per eum sit divisibilis.

316. Demonstratum ergo est summam duorum quadratorum inter se primorum dividi non posse per ullum numerum primum huius formae $4q - 1$. Quodsi ergo talis binorum quadratorum summa habeat divisores primos, ii certo erunt huius formae $4q + 1$ remoto scilicet binario, qui etiam quandoque divisor esse potest ambobus quadratis sumtis imparibus.

317. Quando residuorum complementa inter residua deprehenduntur, complementa non-residuorum etiam erunt non-residua; ac si unius residui complementum fuerit non-residuum, omnium residuorum complementa inter non-residua, atque complementa omnium non-residuorum vicissim erunt residua.

318. Si divisore existente $2p + 1$ sit p numerus par, his solis casibus evenire potest, ut residuorum complementa quoque sint residua; quod autem

semper sint residua, hinc nondum est evictum. Ad hoc autem comparari debent haec residua cum residuis ex serie potestatum ortis ab eodem divisore $2p + 1$, si series potestatum ita fuerit comparata, ut multitudo residuorum aequalis sit multitudini non-residuorum.

319. Sit $1, a, a^2, a^3$ etc. huiusmodi series potestatum, quae p residua diversa praebeat divisore existente primo $= 2p + 1$, ita ut omnia residua futura sint

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

ipsas scilicet potestates tamquam residuis aequivalentes adhibendo. Non-residua autem sint totidem numero ita expressa: $A, Aa, Aa^2, Aa^3, \ldots, Aa^{p-1}$ [1]).

320. Hic iam residua pariter ac residua quadratorum ita sunt comparata, ut 1° ab unitate incipiant, 2° producta binorum residuorum quoque sint residua, 3° producta ex residuo et non-residuo inter non-residua occurrant. Unde concludere licet producta ex binis non-residuis iterum in ordinem residuorum transire.

[*Additamentum*][2]): Si $a^p - 1$ divisibile est per $2p + 1$, tum a certe est residuum quadratorum. Si enim esset non-residuum, omnia reliqua residua, quae sunt $a\alpha$, $a\beta$, $a\gamma$ etc., eandem haberent proprietatem, ideoque omnes numeri x ita essent comparati, ut $x^p - 1$ per $2p + 1$ dividi posset, quod est absurdum[3]).

321. Cum enim in residuis quadratorum res ita se habeat, ubi numerus non-residuorum aequalis est numero residuorum, si in residuis potestatum secus eveniret et producta ex binis non-residuis iterum darent non-residuum, multitudo non-residuorum superaret multitudinem residuorum, contra hypothesin.

322. Hoc autem firmius ita ostendi potest: Cum A quodvis non-residuum denotare possit, ac tum aliud quodvis non-residuum ita repraesentari possit, ut sit Aa^n, productum binorum non-residuorum erit AAa^n, quod si esset non-residuum, aequivaleret tali formae Aa^m vel tali Aa^{m+vp}, ita ut m maius sit quam n, ideoque differentia $Aa^m - AAa^n$ foret per $2p + 1$ divisibilis.

---

1) Hoc loco residua et non-residua idem significant ac paragrapho 203. R. F.

2) Vide notam p. 203. R. F.

3) Vide theorema et demonstrationem in paragraphis 256—260. R. F.

323. Cum autem neque A neque a^n per $2p + 1$ dividi queat, foret $a^{m-n} - A$ per $2p + 1$ divisibile, seu potestas a^{m-n} per $2p + 1$ divisa relinqueret residuum A. Cum autem A non sit residuum, sequitur hanc hypothesin esse absurdam, ideoque productum duorum non-residuorum non in forma Aa^m, quae omnia non-residua complectitur, contineri ideoque necessario inter residua occurrere debere.

324. Quare, si a sit eiusmodi numerus, ut a^p sit minima potestas, quae per numerum primum $2p + 1$ divisa unitatem relinquat, ideoque ex divisione terminorum progressionis geometricae $1, a, a^2, a^3, a^4, \ldots, a^{p-1}$ tot residua diversa oriantur, quot p continet unitates, totidemque dentur non-residua, certum est omnia producta binorum non-residuorum in ordine residuorum contineri.

325. Cum autem omnes numeri divisore $2p + 1$ minores vel in residuis vel in non-residuis contineantur, singulorum quadrata in ordine residuorum certo occurrent; quod cum etiam eveniat in residuis ex quadratis ortis, sequitur ambos ordines residuorum tam ex quadratis quam ex superiori progressione geometrica ortos plane inter se congruere.[1])

326. Quodsi ergo pro divisore primo $2p + 1$ sint residua ex quadratis orta $1, \alpha, \beta, \gamma, \delta$ etc., tum vero $\mathfrak{A}$ fuerit quodvis non-residuum, hic numerus $\mathfrak{A}$ etiam inter non-residua reperietur, quae progressioni geometricae $1, a, a^2, a^3, \ldots, a^{p-1}$ respondent, si quidem a^p fuerit minima potestas unitatem pro residuo praebens.

327. Iam supra vidimus, si a fuerit residuum ex quadratis ortum, fore $a^p - 1$ certo per $2p + 1$ divisibile; nunc autem patet, si a fuerit non-residuum respectu quadratorum, tum a^p non esse minimam potestatem ipsius a, quae per $2p + 1$ divisa unitatem relinquat. Ergo vel unitatem non relinquet, vel dabitur adhuc minor $a^{\frac{p}{\nu}}$, quae unitatem relinquet.

328. Si sit a eiusmodi numerus, ut potestas eius a^p per numerum primum $2p + 1$ [divisa] relinquat unitatem, tum a certe inter residua quadratorum continetur. Hoc evidens est, si a^p sit minima potestas istius indolis. Sin autem non sit minima, id eo magis verum esse videtur. Nam, si detur minor, ex residuis illis numero p quaedam transeunt in ordinem non-residuorum. Si enim $a^{\frac{1}{2}p}$ sit minima, tum a adeo inter residua biquadratorum, sin $a^{\frac{1}{3}p}$, inter residua

1) Hanc conclusionem non rigorosam esse videtur. R. F.

potestatum sextarum etc., ergo semper inter residua quadratorum continebitur. [1])

329. Si ergo a fuerit non-residuum ratione quadratorum, tum $a^p - 1$ certe non est divisibile per $2p + 1$; unde, si a sit complementum cuiuspiam residui, puta $a = d - \alpha$ ponendo $d = 2p + 1$, tum $(d - \alpha)^p - 1$ non est divisibile per $2p + 1$; at $\alpha^p - 1$ certe est divisibile ob α residuum, unde differentia $(d - \alpha)^p - \alpha^p$ etiam non erit divisibilis.

330. At haec differentia esset divisibilis, si p esset numerus par; quare, nisi p sit numerus impar, illa conditio, qua $(d - \alpha)^p - 1$ indivisibile per $2p + 1$ assumsimus, hoc est, qua $d - \alpha$ est non-residuum, subsistere nequit.

331. At si p sit numerus par, complementum cuiuspiam residui α, puta $d - \alpha$, certe est residuum, propterea, quod $(d - \alpha)^p - 1$ per $2p + 1$ est divisibile; si enim esset non-residuum, haec divisibilitas locum habere non posset.

332. Si ergo sit $p = 2q$ numerusque primus divisor propositus $= 4q+1$, tum inter residua quadratorum etiam singulorum complementa deprehendentur, hoc est, si residua fuerint $1, \alpha, \beta, \gamma$ etc., etiam residua erunt $-1, -\alpha, -\beta, -\gamma$ etc.

333. Pro quovis ergo quadratorum ex hac progressione $1, 4, 9, 16, \ldots, 4qq$ assumto dabitur aliud, quod ad illud additum producit summam per $4q + 1$ divisibilem; seu, cum multitudo horum quadratorum sit $= 2q$ et quodlibet habeat quasi suum coniugatum, dabuntur q paria duorum quadratorum diversa, quorum summa sit per $4q + 1$ divisibilis.

[*Additamentum*][2]): Semper duo exhiberi possunt quadrata, quorum summa divisibilis sit per numerum primum $4q + 1$, et quidem alterum quadratum ad lubitum assumi potest.[3])

334. Et quia singula quadrata non superant $4qq$, binorum summa certe minor est quam $8qq$; unde, si talis summa per $4q + 1$ dividatur, quotus certe erit minor quam $2q$. Hic autem quotus, nisi sit $= 2$, etiam erit vel numerus primus formae $4n + 1$ vel talium aliquod productum (paragraphus 316).

335. Quoties ergo divisor primus est formae $4q + 1$, toties inter residua quadratorum occurrit $4q$ ideoque etiam q, tamquam complementum unitatis, cui aequivalet -1; parique modo ibidem etiam occurrunt omnia reliqua

---

1) Demonstratio celebris criterii numerum a esse residuum vel non-residuum quadraticum, prout a^p unitatem relinquat vel non, hoc loco nondum data est. R. F.

2) Vide notam p. 203. R. F.

3) Vide paragraphum 354. R. F.

quadrata negativa — 4, — 9, — 16 etc., ita ut residua constituantur complexa tam quadratorum ipsorum quam eorundem negative sumtorum una cum productis ex binis quibusque, quorum tamen omnium numerorum, si per divisorem $4q + 1$ ad minimam formam perducantur, multitudo erit $= 2q$, ita ut totidem excludantur.

336. Contra autem, si divisor primus sit formae $4q-1$, tum -1 et omnia quadrata negativa inter non-residua referuntur. Si enim -1 esset residuum, foret $(-1)^{2q-1} - 1$ divisibile per $4q - 1$, quod autem fieri nequit. Praecedente autem casu, si -1 esset non-residuum divisore existente $4q + 1$, tum $(-1)^{2q} - 1$ non esset divisibile per $4q + 1$, quod perinde est falsum.

[*Additamentum*][1]): Non ergo datur summa duorum quadratorum per talem numerum primum $4q - 1$ divisibilis.

337. Sola autem quadrata semper in ordine residuorum reperiuntur, reliqui vero numeri pro ratione divisoris mox inter residua mox inter non-residua cadunt, quemadmodum modo vidimus -1 esse residuum, si divisor sit $4q + 1$, at -1 esse non-residuum, si divisor sit $4q - 1$.

338. Pro ceteris numeris non-quadratis simile discrimen observatur. Scilicet, numerus $+2$ inter residua reperitur, quoties divisor primus est vel huius $8q + 1$ vel huius formae $8q - 1$ seu $8q + 7$. Reliquis casibus, quibus divisor est vel $8q + 3$ vel $8q + 5$, numerus $+2$ inter non-residua locum occupat.

[*Additamentum*][1]): Hoc autem non ut praecedens demonstratione muniri potest.

339. At numerus -2 inter residua occurrit casibus, quibus divisor primus est vel $8q + 1$ vel $8q + 3$; idem vero numerus -2 inter non-residua cadit casibus, quibus divisor primus est vel $8q + 5$ vel $8q + 7$.

340. Numerus porro $+3$ est residuum, si divisor primus sit vel $12q + 1$ vel $12q + 11$; at idem erit non-residuum, si divisor sit vel $12q + 5$ vel $12q + 7$. Verum numerus -3 est residuum, si divisor primus sit vel $12q + 1$ vel $12q + 7$; at -3 erit non-residuum, si divisor sit $12q + 5$ vel $12q + 11$.

341. Numerus $+4$ semper ad residua refertur, et de -4 idem est iudicium ac de -1. Numerus autem 5 reperitur inter residua, si divisor sit vel $20q + 1$ vel $20q + 9$ vel $20q + 11$ vel $20q + 19$; at -5 inter residua deprehenditur, si divisor sit vel $20q + 1$ vel $20q + 3$ vel $20q + 7$ vel $20q + 9$.

1) Vide notam p. 203. R. F.

342. Colligamus haec, ut uni conspectui exponantur:

Inter residua erit numerus	si divisor primus fuerit
+ 1	$4q + (1, 3)$
— 1	$4q + 1$
+ 2	$8q + (1, 7)$ $xx - 2yy$ alios divisores primos non admittit, nisi formae $8q + (1, 7)$
— 2	$8q + (1, 3)$
+ 3	$12q + (1, 11)$
— 3	$12q + (1, 7)$
+ 5	$20q + (1, 9, 11, 19)$
— 5	$20q + (1, 3, 7, 9)$
+ 6	$24q + (1, 5, 19, 23)$
— 6	$24q + (1, 5, 7, 11)$
+ 7	$28q + (1, 3, 9, 19, 25, 27)$
— 7	$28q + (1, 9, 11, 15, 23, 25)$
+ 10	$40q + (1, 3, 9, 13, 27, 31, 37, 39)$
— 10	$40q + (1, 7, 9, 11, 13, 19, 23, 37)$
+ 11	$44q + (1, 9, 25, 5, 7, 37, 39, 19, 35, 43)$
— 11	$44q + (1, 9, 25, 5, 37, 3, 15, 23, 27, 31)$
+ 12	$48q + (1, 11, 13, 23, 25, 35, 37, 47)$
— 12	$48q + (1, 13, 25, 37, 7, 19, 31, 43)$
+ 14	$56q + (1, 5, 9, 13, 25, 45, 11, 31, 43, 47, 51, 55)$
— 14	$56q + (1, 5, 9, 13, 25, 45, 3, 15, 19, 23, 27, 39)$
+ 15	$60q + (1, 7, 11, 17, 43, 49, 53, 59)$
— 15	$60q + (1, 17, 49, 53, 19, 23, 31, 47)$
	etc.

[*Additamentum*][1]): Si $xx = mn + r$, tum quadratum xx tam per m quam n divisum idem relinquet residuum r. Ergo si residuum r convenit divisori m, convenit etiam divisori n.

1) Vide notam p. 203. R. F.

Si divisor	inter non-residuum	[inter] residuum
$4n-1$	-1	
$8n-1$	-2	$+2$
$8n-3$	± 2	
$12n-1$	-3	$+3$
$12n-7$	± 3	
$8n \pm 3$	$+2$	

Hoc demonstrari potest; at si divisor $8n+1$, inter residua est $+2$, quod autem hinc non demonstratur.

343. Haec autem hactenus tantum inductione nituntur, atque ad demonstrationem investigandam iuvabit sequentia observasse. Primo numerus [impar] quicunque $\pm n$ inter residua reperietur, si divisor primus fuerit formae $4nq+1$ vel adeo $4nq+ii$, denotante i numerum imparem quemcunque. Deinde etiam numerus positivus $+n$ erit residuum, si divisor primus fuerit formae $4nq-1$ vel generalius $4nq-ii$; pro his autem divisoribus numerus negativus $-n$ inter non-residua reperietur.[1])

344. Si numerus positivus n[2]) sit residuum pro divisore d, erit etiam residuum pro divisore primo quocunque formae $4nq \pm d$ vel adeo $4nq \pm dii$; at si numerus negativus $-n$ sit residuum pro divisore d, erit is quidem residuum pro divisore $4nq+d$, at non-residuum pro divisore $4nq-d$.

345. Si numerus positivus n fuerit residuum pro divisore d, deinde etiam pro divisore e, erit etiam residuum pro divisore primo quocunque formae $4nq \pm de$. At si numerus negativus $-n$ fuerit residuum pro divisoribus d et e, erit quoque residuum pro divisore quocunque primo formae $4nq+de$; pro divisoribus autem $4nq-de$ inter non-residua referetur.

346. Si numerus positivus n fuerit non-residuum pro divisoribus d et e, certe erit residuum pro divisoribus primis omnibus formae $4nq \pm de$; at si numerus negativus $-n$ sit non-residuum pro divisoribus d et e, is erit residuum pro omnibus divisoribus primis formae $4nq+de$; pro divisoribus autem formae $4nq-de$ erit non-residuum.

---

1) EULERUS hoc loco et in paragraphis sequentibus casus legis fundamentalis residuorum quadraticorum exponit. R. F.

2) Hic et in paragraphis sequentibus omnes numeri n, d, e, i semper sunt impares. R. F.

347. Quicunque numerus [impar] $\pm n$ proponatur, erit is semper residuum, si divisor primus fuerit in aliqua talium formarum $4nq+A$, $4nq+B$, $4nq+C$ etc. contentus, quarum numerus aequatur semissi multitudinis numerorum ad $4n$ primorum eoque minorum. Sin autem divisor in reliquis formis contineatur, erit is non-residuum.

348. Hic autem excipi debent casus, quibus numerus n est quadratus, quippe qui semper inter residua occurrit, quicunque divisores accipiantur. Ac si n sit quadratum negativum, eadem ratio valet ac pro -1.

349. Primum igitur demonstrari debet, si divisor primus sit $4nq+ii$ existente i numero impari inter residua quadratorum semper occurrere tam numeros n et q quam eorum negativa $-n$ et $-q$. Sit $i=2m+1$, et quia divisor $4nq+4mm+4m+1$ est formae $4p+1$, inter residua continetur quadratum negativum $-4mm-4m-1$, ideoque numerus $4nq$, et ob 4 residuum etiam numerus nq, itemque $-nq$; quare vel ambo numeri n et q simul inter residua vel ambo simul inter non-residua occurrere deberent, unde dum alteruter fuerit inter residua, et alter ibidem reperiatur, necesse est.

350. Si n non esset residuum, nullum daretur quadratum xx, ut $xx-n$ divisibile esset per $4nq+4mm+4m+1$. Si ergo demonstrari posset dari huiusmodi quadratum, evicta esset veritas propositionis. Vel si n esset non-residuum, haec expressio $n^{2nq+2mm+2m}-1$ non esset divisibilis per numerum primum; quare, si contrarium demonstrari posset, haberemus, quod intendimus.

[*Additamentum*][1]): Si n esset non-residuum, foret quoque non-residuum nzz, ideoque etiam

$$\pm nzz \mp y(4nq+4mm+4m+1),$$

quae expressio, si uno saltem casu esset quadratum, propositum constaret. Quod ob signa ambigua semper uno saltem casu evenire debere videtur, idque eo magis, cum etiam n et q sint permutabiles, quin etiam verum est, etsi divisor non sit primus. Dubium, si $n=3$, $q=5$, $2m+1=5$, $\pm 3zz \pm 85y = \square$ vel $\pm 5zz \pm 85y = \square$ effici nequit. Ergo demonstratio ita est adornanda, ut divisor statuatur primus.

351. Deinde, si divisor primus sit $4nq-4mm-4m-1$, inter residua quadratorum occurrere numerum n, inter non-residua vero numerum $-n$ demonstrari oportet. Pari autem iure inter residua erit numerus q, et inter non-residua $-q$. Cum autem inter residua certo sit $(2m+1)^2$, ibidem erit $4nq$ ideoque etiam nq.

1) Vide notam p. 203. R. F.

352. Concessis ergo his propositionibus, etsi demonstratio nondum patet, posito i numero impari et $4nq \pm ii$ primo, pro divisore primo $4nq + ii$ cum residua sint n et $-n$, item naa et $-naa$, semper eiusmodi quadratum xx dabitur, ut sit $xx - naa$ divisibile per $4nq + ii$, deinde etiam eiusmodi quadratum yy, ut sit $yy + naa$ divisibile per $4nq + ii$.

353. At divisore primo existente $4nq - ii$, ob residuum naa semper datur quadratum xx, ut sit $xx - naa$ divisibile per $4nq - ii$; nullum autem existit quadratum yy, ut $yy + naa$ fiat per $4nq - ii$ divisibile, quia hoc casu $-naa$ est non-residuum.

354. Cum $4nq + ii$ sit numerus formae $4p + 1$, semper dabitur summa duorum quadratorum $ff + gg$ per eum divisibilis, quorum alterum ff pro lubitu assumi potest. Quare, si $xx - naa$ divisibile sit per $4nq + ii$, inveniri potest quadratum yy, ut fiat $xx + yy$ per $4nq + ii$ divisibile, ac tum erit etiam $yy + naa$ per eundem divisibile.

355. Cum $4nq - ii$ sit formae $4p - 1$, nulla datur summa quadratorum per $4nq - ii$ divisibilis; quare, si $xx - naa$ fuerit per $4nq - ii$ divisibile, fieri nequit, ut $yy + naa$ per eundem divisibile existat; foret enim quoque summa $xx + yy$ divisibilis, quod est absurdum.

356. Sumto divisore primo $d = 4nq + ii$, quia datur forma $xx + naa$ per eum divisibilis, dabitur etiam forma $yy + qaa$ per eum divisibilis, unde etiam $qxx - nyy$. Dabitur vero etiam forma $yy - qaa$ divisibilis, ac propterea quoque talis forma $qxx + nyy$.

357. Si divisor primus sit $d = 4nq - ii$, quia dantur tales formulae $xx - naa$, item $yy - qaa$ per eum divisibiles, etiam haec forma $qxx - nyy$ per d erit divisibilis. Cum autem talis forma $yy + qaa$ non per d sit divisibilis, nulla quoque huiusmodi forma $qxx + nyy$ per d erit divisibilis.

358. Verum etiamsi hae propositiones demonstrari possent, reliquae, quas supra observavimus, nondum essent evictae. Ex paragrapho 344, si detur quadratum per d divisum relinquens residuum positivum n, dabitur quoque relinquens naa; tum autem existente $4nq \pm d$ numero primo dabitur quoque quadratum xx, quod per $4nq \pm d$ divisum relinquat idem residuum, seu $xx - naa$ divisibile erit per $4nq + d$.

359. Scilicet, si fuerit $bb - naa$ per d divisibile, semper talis numerus $xx - naa$ dabitur divisibilis per numerum primum $4nq \pm d$. Quin etiam denotante i numerum imparem eiusmodi forma $xx - naa$ exhiberi potest, quae sit divisibilis per numerum primum $4nq \pm dii$.

360. Si detur quadratum bb, quod per d divisum relinquat residuum negativum $-n$ vel $-naa$, dabitur etiam quadratum xx, quod per numerum primum $4nq + dii$ divisum relinquet $-n$ vel $-naa$. Scilicet, si d sit divisor formae $bb + ncc$, dabitur x, ut sit $xx + naa$ divisibile per numerum primum $4nq + dii$.

361. Verum, si d divisor formae huiusmodi $bb + ncc$, nulla dabitur huiusmodi forma $xx + naa$, quae sit divisibilis per talem numerum primum $4nq - dii$. Veluti, si sit $n = 3$, sumatur $d = 7$, quia $2^2 + 3 \cdot 1 = 7$; atque certum est huius formae $xx + 3aa$ numeros nullos admittere divisores talis formae $12q - 7ii$, cuiusmodi sunt: 5, 17, 29, 41, 53, 65, 77, 89, 101, 9, 21, 33, 45.[1])

362. Ex paragrapho 345 sequitur, si d et e fuerint divisores cuiuspiam numeri huius formae $aa - nbb$, tum semper dari quadratum xx, ut $xx - ncc$ sit divisibile per numerum primum $4nq \pm deii$, quod quidem ex praecedente deduci posset demonstrando, si $aa - nbb$ habeat divisorem d, aliaque similis $ff - ngg$ divisorem e, dari etiam $hh - nkk$ divisibilem per productum de.

[*Additamentum*][2]): Hoc patebit, si residua quadratorum per numeros compositos divisorum perpendemus.

363. Denique notatu dignum est, quod numerus n ac propterea etiam naa inter residua quadratorum occurrere nequeat, nisi divisor primus sit huius formae $4nq + \alpha$, ubi α non omnes numeros ad $4n$ primos eoque minores significat, sed eorum tantum semissem, altera semisse penitus exclusa. Sicque omnes divisores primi formae $xx - naa$ talem habent formam $4nq + \alpha$ denotante α aliquot numeros, totidemque exclusis.[3])

364. Similis est ratio numerorum formae $xx + naa$, cuius divisores primi adstringuntur ita ad formam $4nq + \alpha$, ut totidem numeri excludantur ab α, quot admittuntur. Utroque autem casu omnia quadrata imparia ii pro α valent, et si α valeat, etiam αii valebit.

365. Ut demonstrationes has desideratas tentemus, consideremus divisorem primum $4p + 1$, et cum duorum quadratorum summa $aa + bb$ exhiberi queat per eum divisibilis, ita ut alterum pro lubitu assumi possit, auferatur $(4p + 1)bb$, eritque $aa - 4pbb$ per $4p + 1$ divisibile; seu dabitur quadratum

1) Theorema solum pro numeris primis valet. Est, exempli gratia, $9^2 + 3 \cdot 1^2 = 4 \cdot 21$. R. F.

2) Vide notam p. 203. R. F.

3) Confer Commentationes 598 et 610 indicis Enestroemiani et praefationem vol. 4 seriei I, *Leonhardi Euleri Opera omnia*, vol. 4 seriei I, p. 163, 197 et XIII. R. F.

aa, quod per $4p + 1$ divisum relinquit $4pbb$, dabitur ergo quoque relinquens p; seu dabitur forma $aa - pbb$ per $4p + 1$ divisibilis.

366. Cum etiam detur forma $aa - bb$ per $4p + 1$ divisibilis, addendo $(4p + 1)\,bb$ dabitur etiam talis forma $aa + pbb$ per $4p + 1$ divisibilis; quae quidem iam inde patent, quod, si quadrata per numerum primum $4p + 1$ dividantur, in residuis tam $+ p$ quam $- p$ reperiantur.

367. Sit autem divisor primus $4ffp + ii$ denotante i numerum imparem, et quia tam forma $aa + bb$ quam $aa - bb$ per eum divisibilis exhiberi potest, hincque $iiaa + iibb$ et $iiaa - iibb$, inde auferendo, hinc vero addendo $(4ffp + ii)\,bb$ habebuntur formulae $iiaa - 4ffpbb$ et $iiaa + 4ffpbb$ per $4ffp + ii$ divisibiles; seu inter residua quadratorum erunt $\pm 4ffpbb$ ideoque etiam $\pm p$. Dabuntur ergo numeri tam huius $xx + pyy$, quam huius $xx - pyy$ formae per $4ffp + ii$ divisibiles.

[*Additamentum*][1]): Prius manifestum; nam $\frac{xx + pyy}{4ffp + ii}$ = integer, si $x = i$, $y = 2f$.

Ut $xx - 2yy$ divisibile sit per 41:

$$x = 7,\ 10,\ 13,\ 14,\ 17,$$
$$y = 2,\ 3,\ 8,\ 4,\ 1.$$

Ut $xx - 2yy$ divisibile sit per 17:

$x = 12,$	$5,$	$11,$	$6,$	$10,$	$7,$	$16,$	$1,$	$13,$	$4,$
$y = 2,$		$1,$		$4,$		$3,$		$5.$	

368. Si ergo concessis superioribus observationibus divisor primus in quapiam harum formularum contineatur: $4rq + 1$, $4rq + \alpha$, $4rq + \beta$, $4rq + \gamma$, $4rq + \delta$ etc., ubi numeri $1, \alpha, \beta, \gamma, \delta$ etc. sunt primi ad $4r$ eoque minores, quorum tamen tantum semissis hic occurrit, tum inter residua quadratorum certe occurrit numerus r; similique modo pro residuo $-r$ tales formulae divisorum habentur, quae cum illis conveniunt, si divisor sit formae $4p + 1$, ab iis autem discrepant, si divisoris forma fuerit $4p - 1$.

369. Observari etiam meretur, ex formis $4rq + 4m + 1$ semissem excludi tam pro residuo $+ r$ quam $- r$, quorum divisores pro hac forma sunt communes. At ex forma $4rq + 4m - 1$ semissis valet pro residuo $+ r$, alter pro residuo $- r$, et qui divisores pro altero residuo valent, pro altero excluduntur.

1) Vide notam p. 203. R. F.

CAPUT 11

DE RESIDUIS EX DIVISIONE CUBORUM PER NUMEROS PRIMOS NATIS

370. Divisore primo existente $d = 2p + 1$, quod residuum relinquit cubus a^3, idem relinquent etiam hi cubi $(a + d)^3$, $(a + 2d)^3$ etc. et generaliter $(a + nd)^3$, ex quo sufficiet eos tantum cubos considerasse, quorum radices sunt ipso d minores, qui sunt:

$$1, 8, 27, 64, \ldots, (d-4)^3, (d-3)^3, (d-2)^3, (d-1)^3.$$

371. Sit r residuum, quod horum cuborum quicunque relinquit a^3, et manifestum est cubum $(d-a)^3$ relicturum residuum $-r$ seu $d-r$. Quare, si inter residua cuborum occurrat numerus quicunque r, ibidem quoque occurret eius negativum $-r$ seu $d-r$, quod illius complementum vocatur.

372. Sint $1, \alpha, \beta, \gamma, \delta$ etc. residua ex divisione cuborum per numerum primum $d = 2p + 1$ orta, quorum, si omnia a se invicem fuerint diversa, numerus erit $= d - 1$; ideoque omnes numeri ipso d minores ibi occurrent. Sin autem qui numeri bis vel pluries occurrant, inde quidem numeri excludentur inter non-residua referendi.

[*Additamentum*][1]): In his residuis occurrunt omnes cubi ipso d^3 minores ad minimos valores reducti, tum etiam producta ex binis, ternis etc.

373. Investigaturi, an fieri possit, ut idem numerus r inter residua bis occurrat, ponamus ex cubis a^3 et b^3, quorum radices a et b sint ipso divisore d minores et inaequales, idem residuum r resultare, atque eorum differentia $b^3 - a^3 = (b-a)(aa + ab + bb)$ per d erit divisibilis. Cum autem, ob d primum, ad eum factor $b - a$ sit primus, necesse est alterum factorem $aa + ab + bb$ esse divisibilem per d.

374. At si cubus b^3 idem praebeat residuum ac cubus a^3, cuivis alii cubo c^3 respondebit cubus e^3 idem quoque atque ille residuum relinquens. Si enim cubi a^3 et b^3 idem residuum praebeant, etiam hi a^3x^3 et b^3x^3 ad minimos valores reducendo, seu $(ax - md)^3$ et $(bx - nd)^3$ idem producent residuum. Quia vero a et d sunt numeri inter se primi, semper x et m ita accipere licet, ut $ax - md$ dato numero c aequetur, hincque erit $e = bx - nd$, diversus ab c et ipso d minor; si enim esset $e = c$, foret $ax - md = bx - nd$, hincque $(a - b)x$ divisibile per d; at nec $a - b$ nec x est divisibile.

1) Vide notam p. 203. R. F.

375. Statim ergo atque unum residuum bis occurrit, omnia bis occurrent; ideoque multitudo diversorum residuorum ad semissem deprimitur. Hoc autem evenire nequit, nisi divisor d sit divisor talis formae $aa + ab + bb$, existentibus a et b ipso d minoribus. Sin autem non fuerit divisor talis formae, omnia residua erunt diversa eorumque multitudo $= d - 1 = 2p$.

376. Praebeant cubi a^3 et b^3 idem residuum r, ita ut $aa + ab + bb$ sit divisibile per d, eritque etiam $3a^3 + 3a^2b + 3ab^2$ per d divisibile; auferatur $a^3 - b^3$, ut habeatur

$$2a^3 + 3a^2b + 3ab^2 + b^3 = a^3 + (a + b)^3$$

per d divisibile. Quia ergo a^3 relinquit r, relinquet cubus $(a + b)^3$ residuum $-r$, hincque cubus hic $(d - a - b)^3$ vel $(2d - a - b)^3$ dabit residuum $+r$.

377. Statim ergo ac duo habentur cubi a^3 et b^3 idem residuum r relinquentes, dabitur quoque tertius $(d - a - b)^3$ vel $(2d - a - b)^3$ idem residuum relinquens, cuius radix minor quam d ab utraque praecedentium a et b erit diversa. Neque enim esse potest $d - a - b = a$ neque $2d - a - b = a$; foret enim $b = d - 2a$ vel $b = 2d - 2a$, ideoque b^3 relinqueret residuum $-8a^3$ vel $-8r$. Quia vero per hypothesin relinquit r, haecque duo residua r et $-8r$ aequivalentia esse nequeunt, ob differentiam $= 9r$ non divisibilem per d praeter casum $d = 3$, qui per se est perspicuus, sequitur duo residua aequalia semper tertium assumere.

378. Si ergo duo cubi a^3 et b^3 idem praebeant residuum r, dabitur eo ipso tertius c^3 idem residuum exhibens, cuius radix ita est comparata, ut summa omnium $a + b + c$ sit vel $= d$ vel $= 2d$ ob $c = d - a - b$ vel $c = 2d - a - b$, quia singulae sunt minores quam d. Sicque ex duobus semper facile reperitur tertius.

379. Hinc autem colligere licet infra cubum d^3 plures tribus cubis a^3, b^3, c^3 nunquam dari, qui idem residuum relinquant; si enim daretur quartus ab iis diversus e^3, etiam hi:

$$(\lambda d - a - e)^3, \quad (\lambda d - b - e)^3, \quad (\lambda d - c - e)^3$$

idem praeberent residuum, forentque a praecedentibus diversi. Nam, si esset $\lambda d - a - e = b$, foret $a + b + e$ divisibile per d, ideoque $e = c$ contra hypothesin; non solum ergo quatuor sed adeo septem haberemus cubos idem residuum dantes.

380. Hinc autem binis combinandis denuo plures elici possent cubi ipso d^3 minores idem residuum relinquentes, ita ut tandem omnes cubi essent prodituri. Cum autem concesso uno residuo r, aliud detur diversum $-r$, manifestum est non plures tribus dari cubos ipso d^3 minores, qui idem residuum exhibeant.

381. In serie ergo residuorum $1, \alpha, \beta, \gamma$ etc., quorum multitudo est $= d - 1 = 2p$, vel omnia sunt inaequalia vel terna inter se aequalia; quod posterius fieri nequit, nisi $2p$ sit numerus per 3 divisibilis. Quare si p non divisibile sit per 3, certum est omnia residua inter se fore inaequalia, ideoque omnes numeros ipso d minores in residuis occurrere.

382. Cum omnes numeri primi exceptis 2 et 3 in alterutra harum formularum $6q + 1$ et $6q - 1$ contineantur, si divisor primus sit $6q - 1$, in residuis omnes numeri ipso minores occurrunt, neque ulla dantur non-residua. Sin autem divisor sit $6q + 1$, fieri potest, ut multitudo residuorum diversorum sit tantum $2q$, sicque $4q$ dentur non-residua.

383. Vidimus autem praeterea hunc ultimum casum locum habere, si divisor sit talis formae $aa + ab + bb$ divisor, unde patet, ut supra iam animadvertimus, talem formam alios divisores primos non admittere, nisi formae $6q + 1$. At quadruplum illius $4aa + 4ab + 4bb = (2a + b)^2 + 3bb$ redit ad hanc formam $aa + 3bb$, cuius divisores primi illa insigni proprietate gaudent.

384. Quaerendi ergo ii sunt divisores quadratorum, qui pro residuo relinquunt -3 vel $-3bb$, qui supra observati sunt (paragraphus 340) in his duabus formulis $12q + 1$ et $12q + 7$ ad hanc unam $6q + 1$ redeuntibus contineri, unde vicissim concludere licet omnes numeros primos huius formae $6q + 1$ illa proprietate praeditos esse; verum plena huius rei demonstratio adhuc desideratur.

385. Hoc autem concesso consequimur hanc propositionem: Quoties divisor primus fuerit formae $6q + 1$, toties residua cuborum ab 1 ad $216q^3$ non omnia inter se sunt inaequalia, sed ob terna aequalia multitudo residuorum inaequalium tantum est $2q$; eruntque reliqui numeri divisore minores, quorum multitudo est $4q$, non-residua. Quoties vero divisor primus non est formae $6q + 1$, toties omnia residua inter se sunt inaequalia, neque ulla dantur non-residua.

386. Tantum ergo divisores primos formae $6q + 1$ perpendi opus est, pro quibus multitudo non-residuorum duplo maior est quam multitudo residuorum. Casus autem simpliciores evolvamus:

Pro divisore	7	13	19
Residua	1, 6	1, 8, 5, 12	1, 8, 7, 11, 12, 18
Non-residua	2, 3 5, 4	2, 4, 3, 6 11, 9, 10, 7	2, 3, 4, 5, 6, 9 17, 16, 15, 14, 13, 10

Pro divisore	31
Residua	1, 8, 27, 2, 16, 15, 29, 4, 23, 30
Non-residua	3, 5, 6, 7, 9, 10, 11, 12, 13, 14 28, 26, 25, 24, 22, 21, 20, 19, 18, 17

Pro divisore	37
Residua	1, 8, 27, 14, 31, 10, 6, 23, 29, 11, 26, 36
Non-residua	2, 3, 4, 5, 7, 9, 12, 13, 15, 16, 17, 18 35, 34, 33, 32, 30, 28, 25, 24, 22, 21, 20, 19

Pro divisore	43
Residua	1, 8, 27, 21, 39, 11, 4, 32, 22, 16, 35, 2, 41, 42
Non-residua	3, 5, 6, 7, 9, 10, 12, 13, 14, 15, 17, 18, 19, 20 40, 38, 37, 36, 34, 33, 31, 30, 29, 28, 26, 25, 24, 23

387. Pro quovis ergo divisore primo formae $6q + 1$ in residuis occurrunt omnes cubi eo minores, deinde eorum complementa $6q$, $6q - 7$, $6q - 26$, $6q - 63$ etc. Porro etiam producta ex binis. Tum vero etiam, si ibi sit quodpiam productum mn cum altero factore m, ibidem quoque alter factor n reperietur.

388. Si enim a^3 relinquat mn, et b^3 relinquat m, posito divisore $6q+1 = d$ fieri potest $a = fb - gd$, ideoque f^3b^3 relinquet mn; at nb^3 etiam relinquit mn, sicque $f^3b^3 - nb^3$ ac propterea quoque $f^3 - n$ divisibile erit per d, seu f^3 relinquet n.

389. Si divisore primo existente $d = 6q + 1$, inter residua cuborum occurrat numerus α, tum $\alpha^{2q} - 1$ erit per d divisibile. Unde residua, quae ex divisione progressionis geometricae $1, \alpha, \alpha^2, \alpha^3, \alpha^4, \ldots, \alpha^{2q}$ per eundem divisorem oriuntur, convenient cum residuis cuborum.

390. Vicissim autem ostendi debet, si $a^{2q} - 1$ divisibile sit per divisorem primum $6q + 1$, numerum a certo inter residua cuborum occurrere, quod quidem, si $2q$ non sit divisibile per 3, facile patet. Si enim sit $2q = 3k \pm 1$,

cum $a^{2q} = a^{3k \pm 1}$ inter residua cuborum occurrat, utpote unitati aequivalens, ibidem vero sit a^{3k}, ibidem reperiatur a, necesse est.

391. Superest ergo, ut ostendatur, si sit $2q = 3k$ et $a^{3k} - 1$ dividi queat per $6q + 1 = 9k + 1$, tum a fore inter residua cuborum. Si enim a esset non-residuum, reliqua non-residua omnia, quae sunt a, $a\alpha$, $a\beta$, $a\gamma$, $a\delta$ [etc.] et a^2, $a^2\alpha$, $a^2\beta$, $a^2\gamma$ etc. eadem proprietate gauderent, ut eorum potestates exponentis $2q$ unitate minutae essent divisibiles per $6q + 1$; ergo omnes numeri hanc haberent proprietatem, quod esset absurdum[1]). a^{3k} ibi quidem certe reperitur utpote cubus, sed inde demonstratio peti debet, quod residuum a^{3k} unitati aequivaleat.

392. Verum cum residua potestatum $1, a, a^2, a^3$ etc. diversa sint numero $2q$ pariter atque in residuis cuborum, et ambo ordines incipiant ab unitate et communes habeant terminos a^3, a^6, a^9 etc., tum vero reliquae proprietates ipsis sint communes, ordo potestatum nullos terminos ab altero diversos continere potest.

393. Si autem ad non-residua cuborum per numerum primum $6q + 1$ divisorum attendamus, id quidem certum est, si mn sit residuum, at m non-residuum, fore quoque n non-residuum. Non vero vicissim omnia producta ex binis non-residuis praebent residuum; at omnia producta ex residuo quocunque in non-residuum sunt non-residua.

394. Primo enim quadrata singulorum non-residuorum quoque inter non-residua continentur; scilicet, si A sit non-residuum, quoque AA erit non-residuum; hoc vero non-residuum AA per non-residuum A multiplicatum certo dat residuum, quia est cubus.

395. Si enim AA esset residuum, foret $A^{4q} - 1$ divisibile per $6q + 1$; at cum $A^{6q} - 1$ certe sit divisibile, foret etiam $A^{6q} - A^{4q}$, hoc est $A^{2q} - 1$ divisibile, ideoque A esset residuum cuborum contra hypothesin. Quare, si AA sit residuum, etiam A erit residuum, et contra, si A sit non-residuum, erit quoque AA non-residuum.

396. Si ergo divisore primo existente $= 6q + 1$ residua cuborum sint $1, \alpha, \beta, \gamma, \delta$ etc. atque unicum habeatur non-residuum A, primo omnes hi numeri A, $A\alpha$, $A\beta$, $A\gamma$ etc., deinde etiam isti A^2, $A^2\alpha$, $A^2\beta$, $A^2\gamma$ etc. erunt non-residua; qui numeri cum omnes a se invicem sint diversi, manifestum est, quod iam demonstravimus, multitudinem non-residuorum duplo esse maiorem quam residuorum.

1) Vide theorema paragraphi 256 et paragraphum 397. R. F.

397. Hinc etiam patet, si divisor primus sit $6q + 1$, tantum $2q$ residua diversa locum habere posse; si enim omnes numeri inter residua occurrerent, in genere $a^{2q} - 1$ esset per $6q + 1$ divisibile, quicquid esset $a < 6q + 1$, quod cum sit absurdum ideoque unum saltem detur non-residuum, eo ipso $4q$ non-residua sequuntur.

398. Cum igitur ex unico non-residuo A obtineantur duo ordines non-residuorum, prior A, $A\alpha$, $A\beta$, $A\gamma$ etc. et posterior A^2, $A^2\alpha$, $A^2\beta$, $A^2\gamma$ etc., uterque tot continens terminos quot ordo residuorum, producta ex binis ordinis alterutrius in altero ordine reperiuntur et producta ex binis utriusque ordinis fiunt residua.

399. Si adhuc dubitemus, an hoc modo omnia non-residua ex uno obtineantur, sit B non-residuum in neutro ordine contentum, et non-residua erunt tam B, $B\alpha$, $B\beta$, $B\gamma$ etc. quam B^2, $B^2\alpha$, $B^2\beta$, $B^2\gamma$ etc. utrobique totidem numero, quot dantur residua, et omnes hi numeri a praecedentibus erunt diversi. Praeterea vero vel AB vel AB^2 non erit residuum altero certe existente residuo, altero non-residuo.

[*Additamentum*][1]): Demonstrari debet ambo simul non esse posse non-residua. Si AB est non-residuum, vel in ordine A vel B vel A^2 vel B^2 continetur; at singula sunt absurda, ergo esset AB residuum.

400. Si AB non est residuum, binos ordines non-residuorum ita repraesentare poterimus:

Ordo prior: A, $A\alpha$, $A\beta$, $A\gamma$ etc., B, $B\alpha$, $B\beta$, $B\gamma$ etc.,
Ordo posterior: A^2, $A^2\alpha$, $A^2\beta$, $A^2\gamma$ etc., B^2, $B^2\alpha$, $B^2\beta$, $B^2\gamma$ etc.,

et quivis numerus ordinis prioris A per quemlibet posterioris multiplicatus praebet residuum et quidem per quemlibet diversum; unde plura residua prodirent, quam revera sunt, quod esset absurdum[2]).

401. Cum ergo ex divisore primo $6q + 1$ tantum $2q$ residua existant, dato quovis cubo a^3 dabitur alius b^3, minor quam $(6q + 1)^3$, quorum differentia per $6q + 1$ erit divisibilis, ideoque $aa + ab + bb$ per eum quoque erit divisibilis. Omnis ergo numerus primus $6q + 1$ est divisor talis numeri $aa + 3bb$ vel talis $aa + 3$ vel $3aa + 1$.

---

1) Vide notam p. 203. R. F.

2) Hae observationes EULERI non sufficiunt ad demonstrationem assertionis. R. F.

402. Speciminis loco sit divisor 373, et tam residua cuborum quam non-residua utriusque ordinis ita se habebunt:

Residua ±	*Non-residua* ordinis I ±	*Non-residua* ordinis II ±
1, 7, 8, 12, 13	2, 3, 5, 14, 16	4, 6, 9, 10, 11
17, 18, 19, 20, 22	21, 24, 26, 34, 35	15, 25, 28, 29, 32
23, 27, 30, 31, 33	36, 38, 39, 40, 44	37, 42, 43, 48, 52
41, 45, 49, 50, 55	46, 47, 51, 53, 54	63, 68, 70, 71, 72
56, 58, 64, 67, 74	57, 59, 60, 61, 62	73, 76, 77, 78, 79
75, 84, 86, 87, 91	65, 66, 69, 81, 82	80, 88, 92, 94, 102
96, 97, 104, 109, 111	83, 85, 89, 90, 93	103, 105, 106, 108, 114
113, 119, 125, 126, 129	95, 98, 99, 100, 101	117, 118, 120, 122, 124
133, 136, 137, 139, 140	107, 110, 112, 115, 116	127, 130, 131, 132, 138
142, 144, 145, 146, 152	121, 123, 128, 134, 135	141, 143, 149, 153, 159
154, 156, 157, 158, 160	147, 148, 150, 151, 155	162, 164, 166, 170, 171
161, 163, 167, 169, 176	165, 168, 172, 174, 179	173, 175, 177, 178, 180
184, 185.	181, 182.	183, 186.
numero $2 \cdot 62 = 124$	*numero* $= 124$	*numero* $= 124$

403. Cum igitur divisore primo existente $6q + 1$ multitudo non-residuorum duplo maior sit quam multitudo residuorum, etiam pauciores erunt divisores, pro quibus datus numerus inter residua contineatur. Ita datus numerus a erit residuum, si divisor fuerit factor talis formae $x^3 \pm ay^3$ vel etiam talis $x^3 \pm aay^3$; si enim sit $x^3 \pm ay^3 = dn$, cubus x^3 per d divisus residuum dat ay^3, sicque etiam a erit in residuis.

404. Quaeri ergo debent numerorum $x^3 \pm ay^3$ divisores primi, et pro nostro quidem instituto ii tantum, qui simul sunt formae $6q + 1$. Hoc modo posito $a = 2$ binarius inter residua reperietur, quoties divisor formae $6q + 1$ fuerit numerus huius seriei:

31, 43, 109, 127, 157, 223, 229, 277, 283, 307, 397, 433, 439, 457, 499, 601, 643, 691, 727, 733, 739, 811, 919, 997, 1021, 1051, 1069, 1093 .

405. Si ergo sit $6n + 1$ talis numerus, tam 2 quam 2^2 erit residuum, tum $2^{2n} - 1$ per eum erit divisibilis ideoque vel $2^n - 1$ vel $2^n + 1$. At si $6n + 1$

fuerit vel formae $8m + 1$ vel $8m + 7$, hoc est vel $n = 4m$ vel $n = 4m + 1$, tum etiam $2^{3n} - 1$ per $6n + 1$ est divisibile; unde patet his casibus, quibus n vel $4m$ vel $4m + 1$, fore $2^n - 1$ per $6n + 1$ divisibile; casibus autem, quibus n est vel $4m + 2$ vel $4m + 3$, non $2^n - 1$, sed $2^n + 1$ per $6n + 1$ divisibile erit.

406. Ita superiores numeros huc transferendo:

per	divisibile est	per	divisibile est
31	$2^{10} - 1$ et $2^5 - 1$	499	$2^{166} - 1$ et $2^{83} + 1$
43	$2^{14} - 1$ „ $2^7 + 1$	601	$2^{200} - 1$ „ $2^{100} - 1$
109	$2^{36} - 1$ „ $2^{18} + 1$	643	$2^{214} - 1$ „ $2^{107} + 1$
127	$2^{42} - 1$ „ $2^{21} - 1$	691	$2^{230} - 1$ „ $2^{115} + 1$
157	$2^{52} - 1$ „ $2^{26} + 1$	727	$2^{242} - 1$ „ $2^{121} - 1$
223	$2^{74} - 1$ „ $2^{37} - 1$	733	$2^{244} - 1$ „ $2^{122} + 1$[1]
229	$2^{76} - 1$ „ $2^{38} + 1$	739	$2^{246} - 1$ „ $2^{123} + 1$
277	$2^{92} - 1$ „ $2^{46} + 1$	811	$2^{270} - 1$ „ $2^{135} + 1$
283	$2^{94} - 1$ „ $2^{47} + 1$	919	$2^{306} - 1$ „ $2^{153} - 1$
307	$2^{102} - 1$ „ $2^{51} + 1$	997	$2^{332} - 1$ „ $2^{166} + 1$
397	$2^{132} - 1$ „ $2^{66} + 1$	1021	$2^{340} - 1$ „ $2^{170} + 1$
433	$2^{144} - 1$ „ $2^{72} - 1$	1051	$2^{350} - 1$ „ $2^{175} + 1$
439	$2^{146} - 1$ „ $2^{73} - 1$	1069	$2^{356} - 1$ „ $2^{178} + 1$
457	$2^{152} - 1$ „ $2^{76} - 1$	1093	$2^{364} - 1$ „ $2^{182} + 1$

407. Si hos divisores, quibus binarius pro residuo convenit, attentius perpendamus, observabimus eos omnes resultare ex hac forma $27pp + qq$, quoties ea fuerit numerus primus, verum hanc observationem demonstratione confirmare nondum licet[2]).

408. Si eos divisores primos formae $6q + 1$ quaeramus, quibus inter residua 3 conveniat, eos reperiemus:

61, 67, 73, 103, 193, 307, 367, 439, 577, [727], [997], 1021 etc.,

qui, si coniecturae locum relinquamus, in forma $3pp + qq$ continentur, si fuerit vel $p = 9n$ vel $p \pm q = 9n$[3]).

1) Manuscriptum: $2^{122} - 1$. Correxit A. M.

2) Hic est casus particularis theorematis EISENSTEINIANI. Vide praefationem huius voluminis. R. F.

3) Confer G. EISENSTEIN: „*Nachtrag zum cubischen Reciprocitätssatze für die aus dritten Wurzeln der Einheit zusammengesetzten complexen Zahlen. Criterien des cubischen Charakters der Zahl* 3 *und ihrer Teiler*“, Crelle's Journal f. r. u. ang. Math., Bd. 28 (1844), p. 28. Vide etiam praefationem huius voluminis. R. F.

409. Ii autem divisores primi formae $6q + 1$, qui in residuis cuborum habent 5, reperiuntur ex forma $x^3 \pm 5y^3$, cuius divisores esse debent 13, 67, 127, [163], 181, 199, 241, 487, 739 etc., quos in forma $3pp + qq$ sub his conditionibus contineri observamus: 1° si $p = 15n$, 2° si $p = 3m$ et $q = 5n$, 3° si $p \pm q = 15n$, et 4° si $p \pm 2q = 15n$[1]).

410. Si inter residua occurrere debeat 6, divisores reperiuntur

7, 37, 139, 163, 181, 241, 307, 337, 349, 379, [439], 631, 727, 751, 997, [1021] [etc.],

qui in forma $3pp + qq$ contineri deprehenduntur, si fuerit vel $p = 9n$ vel $2p \pm q = 9n$. Harum autem observationum veritas tantum coniecturae innititur, neque inductione ulterius commode progredi licet.

[*Additamentum*][2]): Ut 7 sit residuum divisorque $3pp + qq$, debet esse vel $p = 3m$ et $q = 7n$ vel $p \pm q = 21n$ vel $4p \pm q = 7n$ vel $p = 21m$ vel $p \pm 2q = 7n$.

Ut 10 sit residuum pro divisore $3pp + qq$, debet esse vel $p = 5n$ vel $q = 5n$[1]).

CAPUT 12

DE RESIDUIS EX DIVISIONE BIQUADRATORUM PER NUMEROS PRIMOS ORTIS

411. Si divisor primus sit d, quod residuum a biquadrato a^4 relinquitur, idem non solum a biquadratis $(d + a)^4$, $(2d + a)^4$ etc., sed etiam a $(d - a)^4$ relinquitur; unde, si $d = 2p + 1$, plura quam p residua diversa resultare nequeunt.

412. Si residua sint $1, \alpha, \beta, \gamma, \delta$ etc., quorum multitudo maior esse nequit quam p, in iis occurrent omnia biquadrata ad minimam, scilicet, formam reducta, quae insuper hac gaudebunt proprietate, ut producta ex binis in iisdem reperiantur.

413. Haec ergo residua nascuntur ex biquadratis

$$1, 16, 81, 256, \ldots, p^4,$$

quae utrum pro dato divisore primo $2p + 1$ omnia inter se futura sint diversa necne, diligentius inquiri convenit.

1) Vide praefationem huius voluminis. R. F.

2) Vide notam p. 203. R. F.

414. Ac primo quidem patet, si unum bis occurrat, scilicet ex biquadratis a^4 et b^4, tum ob $b^4 - a^4$ per $d = 2p + 1$ divisibile fieri poterit $b = md \pm na$, unde et $n^4a^4 - a^4$ erit divisibile, sicque etiam $n^4 - 1$. Tum ergo quoque c^4 et n^4c^4 paria producent residua, singulaque residua bis occurrent.

415. Si ergo divisor d sit divisor formulae $b^4 - a^4$ sumtis a et b minoribus quam $\frac{1}{2}d$ ideoque formulae $bb + aa$, quia neque $b - a$ neque $b + a$ per eum divisibile esse potest, tum singula residua bis occurrent. Contra vero, si non sit factor talis formae $bb + aa$, omnia residua erunt diversa.

416. At per paragraphum 279 omnes divisores primi formae $bb + aa$ in forma $4q + 1$ continentur; quare, si divisor propositus fuerit formae $4q - 1$, ex divisione biquadratorum certe $2q - 1$ diversa residua emergunt, totidemque habebuntur non-residua, neque plura. Quos casus primum evolvamus.

417. Sit ergo divisor primus $4q - 1$, et residua diversa ex biquadratis oriunda $1, \alpha, \beta, \gamma, \delta$ etc., quorum numerus erit $2q - 1$, non-residua autem sint $A\ B, C, D$ etc. totidem numero. Ac primo patet, si A fuerit non-residuum, etiam $A\alpha, A\beta, A\gamma$ [etc.] fore non-residua. Si enim Aa^4 esset residuum ex biquadrato b^4 ortum, foret $b^4 - Aa^4$ per d divisibile. At est $b = ma \pm nd$, unde et $m^4a^4 - Aa^4$ ideoque $m^4 - A$ esset divisibile per d, et m^4 relinqueret A contra hypothesin.

418. Haec proprietas adeo ad omnes divisores extenditur, ita ut semper productum ex residuo in non-residuum sit non-residuum. At productum ex duobus non-residuis AB, siquidem divisor primus sit $4q - 1$, certe est residuum; si enim esset non-residuum, conveniret cum termino Aa^4, ita ut $Aa^4 - AB$ ac propterea $a^4 - B$ per d esset divisibile contra hypothesin.

419. Hoc ergo casu, quo divisor est $= 4q - 1$, residua biquadratorum eadem praedita sunt proprietate, atque residua quadratorum, quin etiam cum iis plane convenirent pro eodem divisore. Omnia enim residua biquadratorum in residuis quadratorum continentur, et cum multitudine sint paria, prorsus eadem sint, necesse est, unde hic de residuis et non-residuis eadem valent, quae supra exposuimus.

420. Sit iam divisor primus $4q + 1$, et residua $1, \alpha, \beta, \gamma, \delta$ etc. omnia hanc habent proprietatem, ut $\alpha^q - 1$ divisibilis sit per $4q + 1$. Haec quidem residua etiam continebuntur in residuis quadratorum pro eodem divisore $4q + 1$; at vicissim, non omnia residua quadratorum simul sunt residua biquadratorum, quod ita ostenditur.

421. Quodvis residuum quadratorum per x^2 potest repraesentari, quod si esset residuum biquadratorum, foret $x^{2q} - 1$ divisibile per $4q + 1$, deno-

tante x numerum quemcunque minorem divisore; nempe $1^{2q} - 1$, $2^{2q} - 1$, $3^{2q} - 1$, $4^{2q} - 1, \ldots, (2q)^{2q} - 1$ dividi possent per $4q + 1$, quod cum fieri nequeat[1]), non omnia quadrata in residuis biquadratorum occurrunt.

422. Si x^2 in residuis biquadratorum non occurrat, ibidem non occurrant quoque αx^2, βx^2, γx^2, δx^2 etc., quae cum sint residua quadratorum, patet in residuis quadratorum, quorum multitudo est $2q$, tot ad minimum esse non-residua biquadratorum, quot fuerint residua biquadratorum; unde patet multitudinem residuorum biquadratorum vel esse $= q$ vel adhuc minorem, quod posterius autem fieri nequit.

423. Quo haec facilius evolvere liceat, divisores simpliciores formae $4q + 1$ examinemus et tam residua quam non-residua biquadratorum consideremus:

Pro divisore	5	13	17	29
Residua	1	1, 3, 9	1, 4, 13, 16	1, 16, 23, 24, 20, 7, 25
Non-residua	2	2, 6, 5	3, 12, 5, 14	2, 3, 17, 19, 11, 14, 21
	4	4, 12, 10	9, 2, 15, 8	4, 6, 5, 9, 22, 28, 13
	3	8, 11, 7	10, 6, 11, 7	8, 12, 10, 18, 15, 27, 26

Pro divisore	37
Residua	1, 16, 9, 12, 33, 10, 26, 34, 7
Non-residua	2, 32, 18, 24, 29, 20, 15, 31, 14
	4, 27, 36, 11, 21, 3, 30, 25, 28
	8, 17, 35, 22, 5, 6, 23, 13, 19.

424. Ex his exemplis videmus numerum residuorum esse $= q$, quem iam demonstravimus maiorem esse non posse. Non-residuorum numerus triplo est maior, quae in ternas classes distinximus, cum cuiusvis classis numeri peculiaribus proprietatibus gaudeant.

425. Has tres classes commodissime ita constituere licet; cum dentur quadrata in residuis non occurrentia, sit xx tale quadratum, et certum est neque x neque x^3 in residuis reperire posse. Si ergo residua sint $1, \alpha, \beta, \gamma, \delta, \varepsilon$ etc., ternae non-residuorum classes erunt:

I. x, αx, βx, γx, δx etc.,
II. x^2, αx^2, βx^2, γx^2, δx^2 etc.,
III. x^3, αx^3, βx^3, γx^3, δx^3 etc.

1) Vide paragraphum 256. R. F.

426. Quaevis classis tot continet terminos, quot sunt residua, et omnes termini harum classium sunt a se invicem diversi. Eiusdem quidem classis termini manifesto sunt diversi. Diversitas autem terminorum in diversis classibus ita ostendetur.

427. Si αx aequivaleret ipsi βx^2, foret $\beta x^2 - \alpha x$ ideoque $\beta x - \alpha$ per $4q + 1$ divisibile; unde, cum α sit residuum, βx quoque esset residuum ipsi aequivalens, quod esset absurdum. Simili modo, si αx vel αx^2 conveniret cum βx^3, foret vel $\alpha - \beta x^2$ vel $\alpha - \beta x$ divisibile per $4q + 1$, ideoque βx^2 vel βx in residua transiret contra hypothesin.

428. Hinc si numerus residuorum sit $= n$, numerus non-residuorum erit $3n$, vel saltem non erit minor quam $3n$. Ac si in tribus memoratis classibus omnia non-residua contineantur, necesse est, sit multitudo tam residuorum quam non-residuorum iunctim sumta $= 4q$, ideoque $n = q$.

429. His classibus ita, ut fecimus, dispositis manifestum est producta ex binis non-residuis tam primae quam tertiae classis in classe secunda contineri; deinde vero producta vel ex binis terminis secundae classis vel ex termino primae in terminum tertiae in ordinem residuorum transgredi. Productum autem ex termino primae in terminum secundae classis reperitur in tertia classe, at productum ex secunda classe in tertiam reperitur in prima.

430. Hinc intelligitur neque in prima neque in tertia classe numerum quadratum locum habere posse, quoniam is in se ipsum ductus foret residuum. Sola ergo secunda classis continet quadrata, et quoniam residua etiam ut quadrata spectari possunt, multitudo omnium quadratorum est $= 2n$.

431. Si secunda classis cum residuis omnia quadrata complectatur, quae ut residua diversa respectu divisoris $4q + 1$ spectari possunt, quorum numerus est $= 2q$, ut in residuis quadratorum vidimus, ob $2n = 2q$ ideoque $4n = 4q$, omnes numeri ipso divisore minores habentur, neque ulla dabuntur non-residua in nostris tribus classibus non contenta, eritque $n = q$.

432. Si ergo quis dubitet, an in nostris tribus non-residuorum classibus omnes occurrant numeri, qui non sint residua, hoc dubium tolletur, si ostendamus nullum dari quadratum non-residuum, quod non in secunda classe contineatur. Si enim yy esset tale quadratum, inde statim tres novae classes non-residuorum emergerent, foretque iam numerus non-residuorum $= 6n$, ac si nunc non-residua essent completa, foret $7n = 4q$.

433. Verum quod tale quadratum yy tres novas classes non-residuorum post se trahens non detur, ita ostenditur: Sint tres classes ex tali quadrato oriundae et prioribus adiiciendae

IV. y , αy , βy , γy etc.,
V. y^2, αy^2, βy^2, γy^2 etc.,
VI. y^3, αy^3, βy^3, γy^3 etc.,

quarum singulae n terminos continebunt, ac duo casus examinari oportet, alterum, quo xy esset residuum, alterum, quo esset non-residuum.

434. Sit xy residuum, atque omnes termini classis quartae per x multiplicati, scilicet xy, αxy, βxy, γxy etc., numero n erunt residua. Verum etiam omnes termini classis tertiae per x multiplicati, scilicet x^4, αx^4, βx^4, γx^4 etc., sunt residua totidem numero, atque ab illis diversa; nam, si αxy et βx^4 convenirent, foret $\alpha y - \beta x^3$ divisibile per divisorem, et αy caderet in classem tertiam contra hypothesin. Prodirent ergo $2n$ residua diversa; quod cum sit absurdum, fieri nequit, ut xy sit residuum.

435. Remoto ergo casu, quo xy est residuum, ponamus xy esse non-residuum, et cum in sex classibus omnia non-residua comprehendantur, in una earum xy occurrere deberet. Sive autem ponamus xy ipsi αx sive αx^2 sive αx^3 sive αy sive αy^2 sive αy^3 aequivalere, sequeretur absurdum, dum y vel esset residuum vel in classem I vel II non-residuorum caderet; vel etiam x esset residuum vel in classem IV vel V caderet.

436. Cum igitur sex classes non-residuorum admitti nequeant, vel tantum tres sunt constituendae, quod volumus, vel plures quam sex. Quod posterius eveniret, si nondum omnia quadrata non-residua in classe II et V occurrerent. Sit ergo zz non-residuum in neutra harum classium contentum, et ex eo resultabunt tres novae classes singulae n terminis constantes:

VII. z , αz , βz etc.,
VIII. z^2, αz^2, βz^2 etc.,
IX. z^3, αz^3, βz^3 etc.

437. Nunc vero ut paragrapho 434 ostendetur neque xy neque xz neque yz esse posse residuum, quia inde plura residua, quam revera sunt, sequerentur. Deinde, si xy in quapiam sex primorum classium contineretur, eadem incommoda orirentur quae ante; ex quo xy in quapiam trium postremarum classium esse deberet. Videamus ergo, num xy ipsi αz aequivalere posset.

438. At si xy ipsi αz aequivaleret, xz, quia certe est non-residuum, vel ipsi βy vel βy^2 vel βy^3 aequivaleret; quare cum $xy - \alpha z$ vel $xz - \beta y^\nu$ denotante ν vel 1 vel 2 vel 3 essent divisibilia per $4q + 1$, foret $z(xy - \alpha z) - y(xz - \beta y^\nu)$, hoc est $\beta y^{\nu+1} - \alpha z^2$, quoque divisibile, sicque αz^2

aequivaleret ipsi $\beta y^{\nu+1}$, ideoque in alia classe contineretur, quod aeque esset absurdum.

439. Sic igitur demonstratum est, si divisor primus fuerit $4q + 1$, residua diversa biquadratorum fore numero $= q$, neque plura neque pauciora non-residua autem tribus classibus comprehendi, quarum quaelibet constet q terminis.

440. Quare, cum residua diversa ex biquadratis $1, 2^4, 3^4, 4^4, \ldots, 16q^4$, quorum multitudo est $= 2q$, oriantur, bina debent esse aequalia. Hinc si a sit numerus quicunque minor quam $2q$, dabitur semper alius b et quidem unicus pariter non maior quam $2q$, ut b^4 et a^4 aequalia relinquant residua, seu ut $b^4 - a^4$ per $4q + 1$ sit divisibile.

441. Cum autem tam $b - a$ quam $b + a$ minus sit quam $4q + 1$, erit $aa + bb$ per $4q + 1$ divisibile. Hinc proposito numero primo $4q + 1$ semper summa duorum quadratorum $aa + bb$ per eum divisibilis exhiberi potest, ita ut neutra radix superet $2q$, et quidem alterum quadratum pro lubitu assumi potest.

442. Supra autem iam ostendimus summam duorum quadratorum $aa + bb$ inter se primorum praeter binarium alios divisores primos non admittere nisi formae $4n + 1$. Unde concludi posse videtur omnes numeros primos formae $4q + 1$ ipsos esse summas duorum quadratorum, certe autem vel $2(4q + 1)$ vel $5(4q + 1)$ vel $13(4q + 1)$ etc. erit summa duorum quadratorum.

443. Etsi iam evictum est plura duobus biquadratis, quorum radices $2q$ non excedant, non dari idem residuum relinquentes, tamen hoc etiam seorsim demonstrari potest. Sint enim tres numeri a, b, c non excedentes $2q$, ut tam $aa + bb$ quam $aa + cc$ et $bb + cc$ per $4q + 1$ essent divisibilia, atque etiam differentiae $aa - cc$, $aa - bb$, $bb - cc$ forent divisibiles. At cum neque $a - c$ neque $a + c$ per $4q + 1$ dividi possit, productum quoque $aa - cc$ dividi non poterit.

444. Nova ergo ratione demonstravimus, si divisor primus sit $4q + 1$, multitudinem residuorum diversorum ex biquadratis oriundorum esse $= q$, neque minorem esse posse; unde non-residuorum multitudo erit $3q$ in ternas classes supra memoratas distinguenda.

445. Residua ergo biquadratorum, quae sint $1, \alpha, \beta, \gamma, \delta$ etc. ex divisore primo $4q + 1$ oriunda, hanc habent proprietatem, ut $\alpha^q - 1$, $\beta^q - 1$, $\gamma^q - 1$ etc. per eum numerum primum $4q + 1$ divisionem admittant. Utrum autem omnia residua huic proprietati refragentur necne, videndum est.

446. Sit xx non-residuum, et x atque x^3 pariter erunt non-residua. Iam si $(xx)^q - 1$ seu $x^{2q} - 1$ esset divisibile per $4q + 1$, omnes termini αx^2, βx^2, γx^2 etc. eadem proprietate gauderent, qua cum per se gaudeant ipsa residua, omnia quadrata ab 1 usque ad $4qq$ eadem proprietate essent praedita.

447. Omnibus ergo numeris ab 1 usque ad $2q$ ista conveniret proprietas, ut eorum potestates exponentis $2q$ per $4q + 1$ divisae unitatem relinquerent; sicque omnes differentiae inter binos terminos huius seriei $1, 2^{2q}, 3^{2q}, 4^{2q}, \ldots,$ $(2q)^{2q}$ per $4q + 1$ essent divisibiles, quod autem absurdum esse iam supra ostensum est.[1])

448. Hisce conficitur id, quod erat propositum, scilicet, si quadratum xx fuerit non-residuum, tum $x^{2q} - 1$ certe non esse divisibile per $4q + 1$. Multo minus autem, cum x et x^3 etiam sint non-residua, hae formulae $x^q - 1$ vel $x^{3q} - 1$ divisibiles erunt per $4q + 1$; unde patet, si $a^q - 1$ divisionem admittat per $4q + 1$, tum numerum a necessario inter biquadratorum residua reperiri.

449. Quando ergo potestas a^q per numerum primum $4q + 1$ divisa unitatem relinquit, tum omnia residua ex serie potestatum $1, a, a^2, a^3, a^4$ etc. orta in nostris residuis biquadratorum continebuntur. Et vicissim, si a non sit residuum biquadratorum, formula $a^q - 1$ certe non erit divisibilis per $4q + 1$.

450. Si q sit numerus impar, inter residua non occurret numerus -1 vel $4q$, quia $(-1)^q - 1$ certe per $4q + 1$ dividi nequit. Hoc ergo casu, si residua sint $1, \alpha, \beta, \gamma, \delta$ etc., eorum negativa $-1, -\alpha, -\beta, -\gamma$ etc., seu $4q, 4q + 1 - \alpha, 4q + 1 - \beta, 4q + 1 - \gamma$ etc. certe inter non-residua reperientur.

451. Hinc sequitur, si q sit numerus impar, non dari duo biquadrata a^4 et b^4, quorum summa $a^4 + b^4$ esset per numerum $4q + 1$ divisibilis. Si enim residuum ipsi a^4 conveniens esset α, alterius b^4 esset $-\alpha$, quod autem fieri non posse modo ostendimus.

452. Contra autem, si q sit numerus par, inter residua biquadratorum certe occurrit -1; si enim esset non-residuum, non esset $(-1)^q - 1$ per $4q + 1$ divisibile. Cum igitur sit divisibile, patet propositum, scilicet inter residua biquadratorum simul singulorum negativa seu complementa contineri.

453. Si ergo q sit numerus par et $4q + 1$ numerus primus, seu si $8q + 1$ sit numerus primus, proposito quocunque biquadrato a^4 aliud dabitur b^4, ita ut eorum summa $a^4 + b^4$ sit per $8q + 1$ divisibilis. Ita dato numero a semper

1) Vide paragraphum 256. R. F.

inveniri potest numerus x, ut biquadratorum summa $a^4 + x^4$ divisibilis sit per 17 vel 41 vel 73 vel 89 vel 97 etc.

454. Contra autem nulla dabitur duorum biquadratorum summa, quae esset divisibilis per ullum numerum huius seriei: 5, 13, 29, 37, 53, 61, 101 etc.; multo vero minus per ullum numerum primum formae $4q - 1$, quia ne summa duorum quidem quadratorum per talem numerum est divisibilis.

455. Summa ergo duorum biquadratorum inter se primorum praeter binarium alios divisores habere nequit, nisi qui contineantur in forma $8q + 1$[1]); ita est:

$1 + 2^4 = 17$
$1 + 3^4 = 2 \cdot 41$
$1 + 4^4 = 257$
$1 + 5^4 = 2 \cdot 313$
$1 + 6^4 = 1297$
$1 + 7^4 = 2 \cdot 1201$
$1 + 8^4 = 17 \cdot 241$
$1 + 9^4 = 2 \cdot 17 \cdot 193$
$1 + 10^4 = 73 \cdot 137$

$2^4 + 3^4 = 97$
$2^4 + 5^4 = 641$
$2^4 + 7^4 = 2417$
$2^4 + 9^4 = 6577$
$3^4 + 4^4 = 337$
$3^4 + 5^4 = 2 \cdot 353$
$3^4 + 7^4 = 2 \cdot 17 \cdot 73$
$3^4 + 8^4 = 4177$
$3^4 + 10^4 = 17 \cdot 593$[2])
$4^4 + 5^4 = 881$
$4^4 + 7^4 = 2657$

$4^4 + 9^4 = 17 \cdot 401$
$5^4 + 6^4 = 17 \cdot 113$
$5^4 + 7^4 = 2 \cdot 17 \cdot 89$
$5^4 + 8^4 = 4721$
$5^4 + 9^4 = 2 \cdot 3593$
$6^4 + 7^4 = 3697$
$7^4 + 8^4 = 73 \cdot 89$
$7^4 + 9^4 = 2 \cdot 4481$
$7^4 + 10^4 = 12401$
$8^4 + 9^4 = 10657$
$9^4 + 10^4 = 16561$

456. Si iam quaeratur, quibus divisoribus binarius in residuis reperiatur, id quidem in casibus evolutis [paragrapho] 423 nusquam evenit. At ubi 2 occurrit, ibi etiam 2α occurrit; ideoque divisor $4q + 1$ factor esse debet talis numeri $a^4 - 2b^4$ seu $2b^4 - a^4$; unde concluduntur hi divisores:

73, 89, 113, 233, 281, 353, 593, 617, 937, 1249, [1753], 1889, 2273, 2393, 4177, [4513], 4721, 4801, 6529 etc.,

qui numeri in forma $64pp + qq$ contenti videntur.[3])

---

1) Vide Commentationem 134 p. 220 laudatam, art. 21, *Leonhardi Euleri Opera omnia*, vol. 2 seriei I, p. 70. R. F.

2) Manuscriptum: $3^4 + 10^4 = 2.17.593$. Correxit R. F.

3) Hic est casus particularis theorematis Gaussii de residuis biquadraticis. Confer Commentationem primam: Theoria residuorum biquadraticorum, art. 21, Carl Friedrich Gauss *Werke*, Bd. 2, Göttingen 1876, p. 89. Vide etiam praefationem huius voluminis. R. F.

457. Numeri autem in formula $64pp + qq$ contenti sunt:

73, 89, 113, 233, 257, 281, 337, 353, 577, 593, 601, 617, 881, 937, 1033, 1049, 1097, 1153, 1193, 1201, [1217], 1249 etc.,

ubi, cum omnes praecedentes occurrant et reliqui quaesito satisfaciant, nihil est, quod de veritate coniecturae dubitemus, et cum omnes hi numeri sint formae $8n + 1$, in residuis tam -2 quam $+2$ reperietur.

[*Additamentum*][1]): Ut 3 sit residuum, divisor esse debet $pp + qq$, ut sit vel $p = 12m$ vel $p = 3(2m + 1)$ et $q = 4n + 2$. Ut 5 sit residuum, divisor fit $= 100pp + qq$[2]).

458. Omnes divisores primos formae $4q + 1$ usque ad 101 examinando inter residua semper occurrit numerus q, ita ut esset $q^q - 1$ divisibile per $4q + 1$, quod si generatim esset verum, simul inter residua forent numeri q, q^2, q^3, $16q$, $81q$, $256q$, $16qq$, $81qq$; hincque -4, $q - 20\left[= \frac{(4q+1)-81}{4}\right]$, -64, $-4q$.

459. Haec observatio per supra paragrapho 338 allatam confirmatur, ubi animadvertimus numerum 2 inter residua quadratorum esse, si divisor primus sit formae $8p + 1$, esse autem non-residuum, si divisor sit formae $8p + 5$; quare $2^{4p} - 1$ est divisibile per $8p + 1$, at $2^{4p+2} - 1$ non est divisibile per $8p + 5$; quare, cum $2^{8p+4} - 1$ sit divisibile, necesse est, sit $2^{4p+2} + 1$ per $8p + 5$ divisibile.

460[3]). Hinc cum forma $4q + 1$ ad $8p + 1$ redeat, si q sit numerus par, hoc casu $2^{2q} - 1$ seu $4^q - 1$ per $4q + 1$ est divisibile, ideoque numerus 4 eiusque etiam negativum -4 inter residua biquadratorum reperiri debet. At si q sit numerus impar, quo casu $4q + 1$ ad $8p + 5$ redit, erit $2^{2q} + 1$ seu $4^q + 1$ vel, quod eodem redit, $(-4)^q - 1$ per $4q + 1$ divisibile; ita ut etiam hoc casu -4 inter residua biquadratorum occurrere debeat.

461. Pro divisore ergo primo $4q + 1$ sive q sit numerus par sive impar, in residuis biquadratorum semper reperitur -4, unde, cum ob 1 etiam $-4q$ adsit, quoque q adesse debet, sicque altera observatio per alteram confirmatur.

---

1) Vide notam p. 203. R. F.

2) Vide praefationem huius voluminis. R. F.

3) Ab hoc loco numeri paragraphorum in manuscripto duabus unitatibus aucti sunt. R. F.

CAPUT 13
DE RESIDUIS EX DIVISIONE SURDESOLIDORUM PER NUMEROS PRIMOS ORTIS

462. Si divisor [primus] sit d, et a^5 relinquat α, tum $(d - a)^5$ relinquet $-\alpha$, sicque omnia residua nascentur ex his potestatibus 1, 2^5, 3^5, 4^5, . . ., $(d - 1)^5$, quae si omnia fuerint diversa, eorum numerus est $= d - 1$.

463. Sint 1, α, β, γ etc. omnia residua diversa, et in iis occurrent producta ex binis; quin etiam, si quod productum mn ibi adsit cum altero factore m, etiam alter n aderit. Nam, si mn nascatur ex a^5 et m ex b^5, ex nb^5 nascetur etiam mn, eritque $a^5 - nb^5$ divisibile per d. At fieri potest $a = fb \pm gd$, ideoque a^5 idem relinquit residuum quod $f^5 b^5$; sic, cum $f^5 b^5 - nb^5$ ac propterea $f^5 - n$ divisibile sit per d, in residuis erit n.

464. Si in residuis est a, ibi erunt quoque a^2, a^3, a^4; sed a^5 quidem semper inest. Hinc vicissim, si in residuis sit a^2, ibidem quoque erit $a^3 = a^5 : a^2$; et ob a^4 quoque residuum erit etiam a residuum. Ergo quaecunque potestas a^n (dum n non fuerit multiplum quinarii) fuerit residuum, eius omnes potestates a, a^2, a^3 etc. erunt simul residua.

465. Sit m multitudo residuorum 1, α, β, γ, δ etc. pro divisore primo $2q + 1$, et si omnes numeri divisore minores in residuis occurrant, erit $m = 2q$, ac tales quidem casus dari mox patebit.

466. Si fuerit $m < 2q$, dabitur numerus non-residuum, cuiusmodi sit A, hincque primo non-residua erunt A, $A\alpha$, $A\beta$ etc. numero m; tum vero, quia A^2, A^3 et A^4 sunt non-residua, ex [iis] quoque m nova obtinentur, ita ut unum non-residuum A involvat quatuor classes non-residuorum:

I. A , $A\alpha$, $A\beta$, $A\gamma$ etc.,
II. A^2, $A^2\alpha$, $A^2\beta$, $A^2\gamma$ etc.,
III. A^3, $A^3\alpha$, $A^3\beta$, $A^3\gamma$ etc.,
IV. A^4, $A^4\alpha$, $A^4\beta$, $A^4\gamma$ etc.

467. Statim ergo atque unum non-residuum habetur, simul oriuntur $4m$ non-residua, quae si fuerint omnia, necesse est, ut sit $m + 4m = 2q$, ideoque $5m = 2q$ et $m = \frac{2q}{5}$; nisi ergo q multiplum quinarii, non-residua adesse nequeunt.

468. At si praeter 4 classes novum daretur non-residuum B, ex eo denuo quatuor classes orirentur:

V. B , $B\alpha$, $B\beta$, $B\gamma$ etc.,
VI. B^2, $B^2\alpha$, $B^2\beta$, $B^2\gamma$ etc.,
VII. B^3, $B^3\alpha$, $B^3\beta$, $B^3\gamma$ etc.,
VIII. B^4, $B^4\alpha$, $B^4\beta$, $B^4\gamma$ etc.

Iam sive AB dicatur esse residuum sive non-residuum, absurdum sequitur; unde omnia non-residua, siquidem dantur, a quatuor prioribus classibus exhauriri necesse est.

469. Certum ergo est, quoties in divisore primo $2q + 1$ numerus q non fuerit multiplum quinarii, toties omnes numeros in residuis occurrere eorumque multitudinem esse $= 2q$. Neque ergo dantur duo numeri a et b minores quam $2q + 1$, ut $a^5 - b^5$ esset per $2q + 1$ divisibile; hincque etiam

$$a^4 + a^3 b + aabb + ab^3 + b^4$$

per nullum numerum primum $2q + 1$ dividi potest, in quo q non sit multiplum quinarii.

470. Omnes ergo divisores primi numerorum huius formae

$$a^4 + a^3 b + aabb + ab^3 + b^4$$

seu huius $a^5 - b^5$ excluso divisore $a - b$ in hac formula $10p + 1$ continentur, iique numeri nullo modo dividi poterunt per ullum numerum in aliqua harum formularum $10p + 3$, $10p + 7$ et $10p + 9$ contentum.

471. At si divisor primus sit $10p + 1$, non omnes numeri in ordine residuorum occurrent; si enim omnes occurrerent, foret $x^{2p} - 1$ semper divisibile per $10p + 1$, quicquid fuerit x, seu differentiae omnium harum potestatum $1, 2^{2p}, 3^{2p}, 4^{2p}, \ldots, (2p+1)^{2p}$ per $10p + 1$ essent divisibiles, cuius absurditas iam supra est ostensa.[1])

472. Quare, si divisor primus sit $10p + 1$, numerus residuorum diversorum tantum est $= 2p$, et $8p$ habebuntur non-residua; unde semper quini dabuntur numeri ipso $10p + 1$ minores a, b, c, d, e, quorum potestates quintae paria producunt residua.

473. Scilicet, proposito numero quocunque a quatuor semper assignari possunt alii b, c, d, e, singuli divisore $10p + 1$ minores, ut per eum divisibiles sint

hi numeri	ac propterea isti quoque
$b^5 - a^5$	$b^4 + ab^3 + a^2b^2 + a^3b + a^4$,
$c^5 - a^5$	$c^4 + ac^3 + a^2c^2 + a^3c + a^4$,
$d^5 - a^5$	$d^4 + ad^3 + a^2d^2 + a^3d + a^4$,
$e^5 - a^5$	$e^4 + ae^3 + a^2e^2 + a^3e + a^4$.

[*Additamentum*][2]): Haec eadem demonstratio ad praecedentes potestates accommodari potest.

1) Vide paragraphum 256. R. F.
2) Vide notam p. 203. R. F.

474. Differentiae ergo etiam harum primae a tribus sequentibus per eundem divisorem dividi poterunt; hae autem differentiae, cum sint divisibiles per $b - c$, $b - d$, $b - e$, abeunt in has:

$$b^3 + b^2c + bc^2 + c^3 + ab^2 + abc + ac^2 + a^2b + a^2c + a^3,$$
$$b^3 + b^2d + bd^2 + d^3 + ab^2 + abd + ad^2 + a^2b + a^2d + a^3,$$
$$b^3 + b^2e + be^2 + e^3 + ab^2 + abe + ae^2 + a^2b + a^2e + a^3.$$

475. Porro vero harum differentias, sigillatim per $c - d$ et $c - e$ divisas, etiam per $10p + 1$ divisibiles esse opportet, quae sunt:

$$c^2 + cd + d^2 + bc + bd + b^2 + ac + ad + ab + a^2,$$
$$c^2 + ce + e^2 + bc + be + b^2 + ac + ae + ab + a^2,$$

harumque denuo differentia, quae per $d - e$ divisa est

$$e + d + c + b + a\ ^{1}).$$

476. Hinc apparet quinos numeros a, b, c, d, e, quorum potestates quintae per numerum primum $10p + 1$ divisae paria relinquunt residua, ita esse comparatos, ut eorum summa $a + b + c + d + e$ etiam per eundem sit divisibilis. Cum autem singuli minores sint quam $10p + 1$, eorum summa est vel $10p + 1$ vel $2(10p + 1)$ vel $3(10p + 1)$ vel $4(10p + 1)$.

477. Cum numeros negativos etiam ut residua spectare liceat, haec summa $a + b + c + d + e$ ut nihilo aequalis considerari potest, unde datis quatuor a, b, c, d, quintus sponte datur, scilicet $e = -a - b - c - d$, qui cum sit unicus, patet plures quam quinque non dari.

478. En ergo novam demonstrationem, quod numerus residuorum diversorum pro quocunque divisore primo $2q + 1$ sit vel $= 2q$ vel $= \frac{2q}{5}$, et quod prius quidem semper eveniat, si q non sit multiplum quinarii, posterius semper, si fuerit $q = 5p$. Priori casu omnes numeri divisore minores sunt residua, posteriori tantum quinta eorum pars.

479. Posito igitur divisore primo $10p + 1$ multitudo residuorum diversorum est $= 2p$, inter quae cuiusvis residui negativum quoque occurrit, ex quo eorum multitudo est par. Tum vero idem residuum quinque potestatibus diversis, quarum radices sint divisore minores, convenit, quas notasse iuvabit.

---

1) Haec formula sequitur ex congruentia:
$$x^5 - a^5 \equiv (x - a)(x - b)(x - c)(x - d)(x - e) \pmod{10p + 1}.$$ R. F.

480. Tales divisores cum sint 11, 31, 41, 61, 71, 101 etc., consideremus primo divisorem $10p + 1 = 11$, quo fit $p = 1$:

Residua	ex potestatibus	Classes non-residuorum			
		I.	II.	III.	IV.
1	1^5, 3^5, 4^5, 5^5, 9^5	2	4	8	5
10	2^5, 6^5, 7^5, 8^5, 10^5	9	7	3	6

481. Sit divisor $10p + 1 = 31$ et $p = 3$, habebimus:

Residua	ex potestatibus	Classes non-residuorum			
		I.	II.	III.	IV.
1	1^5, 2^5, 4^5, 8^5, 16^5	2	4	8	16
5	7^5, 14^5, 19^5, 25^5, 28^5	10	20	9	18
26	3^5, 6^5, 12^5, 17^5, 24^5	21	11	22	13[1])
6	11^5, 13^5, 21^5, 22^5, 26^5	12	24	17	3
25	5^5, 9^5, 10^5, 18^5, 20^5	19	7	14	28
30	15^5, 23^5, 27^5, 29^5, 30^5	29	27	23	15

482. Sit divisor primus $10p + 1 = 41$ ideoque $p = 4$, erunt:

Residua	ex potestatibus	Classes non-residuorum			
		I.	II.	III.	IV.
1	1^5, 10^5, 16^5, 18^5, 37^5	2	4	8	16
40	4^5, 23^5, 25^5, 31^5, 40^5	39	37	33	25
3	11^5, 12^5, 28^5, 34^5, 38^5	6	12	24	7
38	3^5, 7^5, 13^5, 29^5, 30^5	35	29	17	34
9	5^5, 8^5, 9^5, 21^5, 39^5	18	36	31	21
32	2^5, 20^5, 32^5, 33^5, 36^5	23	5	10	20
14	15^5, 22^5, 24^5, 27^5, 35^5	28	15	30	19
27	6^5, 14^5, 17^5, 19^5, 26^5	13	26	11	22

1) Manuscriptum: 21, 10, 20, 9. Correxit A. M.

483. Sit divisor primus $10p + 1 = 61$ et $p = 6$, erunt:

Residua	ex potestatibus	Classes non-residuorum			
		I.	II.	III.	IV.
1	1^5, 9^5, 20^5, 34^5, 58^5	2	4	8	16
60	3^5, 27^5, 41^5, 52^5, 60^5	59	57	53	45
13	12^5, 25^5, 42^5, 47^5, 57^5	26	52	43	25
48	4^5, 14^5, 19^5, 36^5, 49^5	35	9	18	36
14	5^5, 39^5, 45^5, 46^5, 48^5	28	56	51	41
47	13^5, 15^5, 16^5, 22^5, 56^5	33	5	10	20
11	8^5, 11^5, 28^5, 37^5, 38^5	22	44	27	54
50	23^5, 24^5, 33^5, 50^5, 53^5	39	17	34	7
21	10^5, 17^5, 29^5, 31^5, 35^5	42	23	46	31
40	26^5, 30^5, 32^5, 44^5, 51^5	19	38	15	30
29	6^5, 21^5, 43^5, 54^5, 59^5	58	55	49	37
32	2^5, 7^5, 18^5, 40^5, 55^5	3	6	12	24

484. Proposito ergo quocunque divisore primo formae $10p + 1$, dabitur numerus a [1]), ut $a^5 - 1$ per eum sit divisibilis, quam proprietatem quoque habebunt numeri a^2, a^3, a^4, quorum potestates quintae etiam unitatem relinquunt. Sequentes termini a^5, a^6 etc. ab his non sunt diversi, cum sit $a^5 = n(10p + 1) + 1$, sicque a^5 ipsi 1, a^6 ipsi a, a^7 ipsi a^2 etc. aequivaleat.

485. Cum quinque numeri, quorum potestates quintae per $10p + 1$ divisae unitatem relinquunt, ita repraesentari queant 1, a, a^2, a^3, a^4, si b^5 det residuum α, quinque habebuntur numeri b, ab, a^2b, a^3b, a^4b, quorum potestates quintae per $10p + 1$ divisae idem relinquunt residuum α.

486. Quia idem ad altiores potestates extendi potest, proposito quocunque numero primo $mn + 1$, semper dabitur numerus a, ut $a^m - 1$ per eum sit divisibile; eiusque potestates omnes eadem praeditae erunt proprietate. Erit autem a minor quam divisor $mn + 1$, talesque numeri diversi tot, quot m continet unitates, exhiberi possunt.

487. Proposito porro divisore primo $mn + 1$, si per eum potestates 1^m, 2^m, 3^m, 4^m etc. dividantur, usque ad $(mn)^m$, plura residua diversa non relinquentur quam n, ideoque dabuntur $(m - 1)n$ numeri divisore minores, qui non sunt residua.

1) $a \neq 1$. R. F.

488. Si post unitatem a sit minimus numerus, cuius potestas a^m per $mn + 1$ divisa unitatem relinquat, cuiusmodi numerus semper datur et quidem unicus, tum, si potestas b^m relinquat α, omnium horum numerorum $b, ab, a^2b, a^3b, \ldots, a^{m-1}b$, quorum multitudo est $= m$, potestates exponentis m idem residuum α relinquent.

489. Si $m = 2$, minima potestas a^2, quae per numerum primum $2n + 1$ divisa relinquit unitatem, est, ut sequitur:

$2n + 1$	n	a^2
3	1	2^2
5	2	4^2
7	3	6^2
11	5	10^2
etc.		

Hoc ergo casu semper est $a = 2n$.

490. Si $m = 3$, potestates a^3, quae per $3n + 1$ divisae unitatem relinquunt, sunt:

$3n + 1$	n	Potestates	$3n + 1$	n	Potestates
7	2	$1^3, 2^3, 4^3$	61	20	$1^3, 13^3, 47^3$
13	4	$1^3, 3^3, 9^3$	67	22	$1^3, 29^3, 37^3$
19	6	$1^3, 7^3, 11^3$	73	24	$1^3, 8^3, 64^3$
31	10	$1^3, 5^3, 25^3$	79	26	$1^3, 23^3, 55^3$
37	12	$1^3, 10^3, 26^3$	97	32	$1^3, 35^3, 61^3$
43	14	$1^3, 6^3, 36^3$	103	34	$1^3, 46^3, 56^3$

491. Sit $m = 4$ et potestates a^4, quae per $4n + 1$ divisae relinquunt unitatem, sunt:

$4n + 1$	n	Potestates	$4n + 1$	n	Potestates
5	1	$1^4, 2^4, 4^4, 3^4$	53	13	$1^4, 23^4, 52^4, 30^4$
13	3	$1^4, 5^4, 12^4, 8^4$	61	15	$1^4, 11^4, 60^4, 50^4$
17	4	$1^4, 4^4, 16^4, 13^4$	73	18	$1^4, 27^4, 72^4, 46^4$
29	7	$1^4, 12^4, 28^4, 17^4$	89	22	$1^4, 34^4, 88^4, 55^4$
37	9	$1^4, 6^4, 36^4, 31^4$	97	24	$1^4, 22^4, 96^4, 75^4$
41	10	$1^4, 9^4, 40^4, 32^4$	101	25	$1^4, 10^4, 100^4, 91^4$

492. Si $m = 5$, potestates a^5, quae per $5n + 1$ divisae relinquunt 1, sunt, ut ante iam vidimus:

$5n + 1$	n	Potestates
11	2	1^5, 3^5, 9^5, 5^5, 4^5
31	6	1^5, 2^5, 4^5, 8^5, 16^5
41	8	1^5, 10^5, 18^5, 16^5, 37^5
61	12	1^5, 9^5, 20^5, 58^5, 34^5
71	14	1^5, 5^5, 25^5, 54^5, 57^5
101	20	1^5, 36^5, 84^5, 95^5, 87^5

493. Sit $m = 6$ et senae potestates a^6, quae per $6n + 1$ divisae unitatem relinquunt, sunt:

$6n + 1$	n	Potestates
7	1	1^6, 2^6, 4^6, 6^6, 5^6, 3^6
13	2	1^6, 3^6, 9^6, 12^6, 10^6, 4^6
19	3	1^6, 7^6, 11^6, 18^6, 12^6, 8^6

Hic scilicet, eaedem potestates, quae pro casu $m = 3$ prodeunt, quibus totidem ex radicibus negativis ortae sunt adiiciendae.

494. Sit $m = 7$, et potestates a^7, quae per $7n + 1$ divisae unitatem relinquunt, sunt:

$7n + 1$	n	Potestates
29	4	1^7, 7^7, 20^7, 24^7, 23^7, 16^7, 25^7
43	6	1^7, 4^7, 16^7, 21^7, 41^7, 35^7, 11^7
71	10	1^7, 20^7, 45^7, 48^7, 37^7, 30^7, 32^7
113	16	1^7, 16^7, 30^7, 28^7, 109^7, 49^7, 106^7

495. Iam observavimus uno horum numerorum cognito reliquos ex eius potestatibus oriri. Verum methodus talem numerum investigandi haec promptissima videtur: Proposito divisore primo $mn + 1$ quaerantur duae potestates a^m et b^m idem residuum praebentes; tum quaeratur x, ut sit $x = \frac{b + p(mn+1)}{a}$, et x^m unitatem relinquet. Semper autem p ita capi potest, ut x fiat numerus integer.

496. Si divisore [primo] existente $mn + 1$ potestates exponentis m unitatem relinquentes sint 1^m, α^m, β^m, γ^m, δ^m etc. numero m, tum $1, \alpha, \beta, \gamma, \delta$ etc. erunt residua ex progressione geometrica $1, \alpha, \alpha^2, \alpha^3, \alpha^4$ etc. orta[1]); erunt ergo etiam ex serie potestatum 1^n, 2^n, 3^n, 4^n, 5^n, 6^n etc. nata.

497. En ergo methodum facillimam unum saltem numerum α inveniendi, ut $\alpha^m - 1$ per $mn + 1$ fiat divisibile, scilicet pro α semper sumi potest 2^n, seu residuum ex hac potestate binarii ortum, quin etiam valores idonei ex 3^n, 5^n etc. peti possunt; cognito autem uno reliqui facile innotescunt.

498. Si divisore primo existente $mn + 1$ in residuis potestatum 1^n, 2^n, 3^n, 4^n etc. occurrat numerus N, ibi quoque occurret numerus Na^n; dabiturque numerus x, ut $x^n - Na^n$ per $mn + 1$ fiat divisibile, eritque etiam $N^m - 1$ per $mn + 1$ divisibile.

499. Vicissim autem, si $N^m - 1$ per $mn + 1$ est divisibile, erit N residuum potestatis cuiusdam x^n; si enim esset non-residuum, omnia reliqua non-residua pari essent praedita proprietate, ideoque omnes numeri; forentque omnes hi numeri $1^m - 1$, $2^m - 1$, $3^m - 1$ etc. divisibiles per $mn + 1$, quod autem fieri nequit. [2])

500. Posito divisore primo $mn + 1$ sint potestatum 1^m, 2^m, 3^m, 4^m etc. residua $1, A, B, C, D$ etc., potestatum vero 1^n, 2^n, 3^n, 4^n etc. residua $1, \alpha, \beta, \gamma, \delta$ etc., ac potestates omnes 1^m, α^m, β^m, γ^m, δ^m etc. residuum relinquent 1; hae vero potestates 1^n, A^n, B^n, C^n etc. residuum relinquent 1, ideoque hae formae $\alpha^m - A^n$ erunt divisibiles per $mn + 1$.

CAPUT 14

DE RESIDUIS EX DIVISIONE QUADRATORUM PER NUMEROS COMPOSITOS ORTIS

[*De divisore* $2(2p + 1) = d$]

501. Sint $1, \alpha, \beta, \gamma, \delta$ etc. residua, quae ex divisione quadratorum per numerum primum $2p + 1$ oriuntur, quorum numerus est $= p$; ac videamus primo, quaenam residua oriantur, si divisio fiat per duplum $2(2p + 1)$; atque hic quidem excludamus quadrata paria; tantum enim ea quadrata, quae ad divisorem sunt prima, consideremus.

1) Hoc generaliter verum non est, nisi α recte eligatur. R. F.

2) Vide paragraphum 256. R. F.

502. Multitudo autem quadratorum, quorum radices sunt divisore minores, est $= 2p$, et quoniam quadrata aa et $(4p + 2 - a)^2$ idem relinquunt residuum, multitudo residuorum diversorum maior esse nequit quam p; erit ergo vel $= p$ vel minor quam p.

503. Minor scilicet esset, si darentur duo quadrata aa et bb, ut non esset $b = 4p + 2 - a$, quae idem relinquerent residuum. Foret autem tum $bb - aa = (b - a)(b + a)$ divisibile per $2(2p + 1)$, et alter factor per 2, alter per $2p + 1$ divisibilis esse deberet. At uno existente pari alter quoque erit par, ideoque per totum divisorem divisibilis, unde foret $b = 2(2p + 1) - a$.

504[1]). Multitudo ergo residuorum diversorum, quae quidem ex quadratis ad divisorem primis oriuntur, erit $= p$, totidem numero, quot ex divisore primo $2p + 1$ nascuntur. Ac si residua ex divisore $2(2p + 1)$ orta sint 1, A, B, C, D etc., eorum numerus est $= p$, et ibidem occurrent producta ex binis.

505. Dantur autem $2p$ numeri ad hunc divisorem primi eoque minores, unde, cum eorum tantum semissis residua constituat, alter semissis dabit ordinem non-residuorum, quae si sint $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D}$ etc., eorum numerus erit $= p$, et producta ex horum binis iterum fient residua.

506. Contemplemur quaedam exempla in iisque tam residua, quae ex divisore primo $2p + 1$, quam ex eius duplo $2(2p + 1)$ nascuntur, simulque apponamus non-residua ad divisorem prima:

Divisor	3	6	5	10	7	14	11	22
Residua	1	1	1, 4	1, 9	1, 2, 4	1, 9, 11	1, 3, 9, 5, 4	1, 3, 9, 5, 15
Non-residua	2	5	2, 3	3, 7	3, 5, 6	3, 5, 13	2, 6, 7, 8, 10	7, 13, 17, 19, 21

Divisor	13	26
Residua	1, 3, 4, 9, 10, 12	1, 3, 9, 17, 23, 25
Non-residua	2, 5, 6, 7, 8, 11	5, 7, 11, 15, 19, 21

Divisor	17	34
Residua	1, 2, 4, 8, 9, 13, 15, 16	1, 9, 13, 15, 19, 21, 25, 33
Non-residua	3, 5, 6, 7, 10, 11, 12, 14	3, 5, 7, 11, 23, 27, 29, 31

1) Manuscriptum continet duas paragraphos 504. R. F.

507. Repraesentemus rem in genere:

Divisor	$2p+1$	$2(2p+1)$
Residua	$1, \alpha, \beta, \gamma, \delta$ etc.	$1, A, B, C, D$ etc.
Non-residua	$\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \mathfrak{d}, \mathfrak{e}$ etc.	$\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \mathfrak{D}, \mathfrak{E}$ etc.

et primo observamus omnia residua divisoris $2(2p+1)$ vel ipsa vel numero $2p+1$ minuta constituere residua divisoris $2p+1$.

508. Scilicet, vel A vel $A-(2p+1)$ in residuis $1, \alpha, \beta, \gamma$ etc. occurrit. Cum enim detur quadratum impar aa, ut sit $aa - A$ per $2(2p+1)$ divisibile, erit quoque per $2p+1$ divisibile, unde A etiam inter residua divisoris $2p+1$ reperiatur necesse est, vel $A-(2p+1)$, si fuerit $A > 2p+1$.

509. Numeri porro impares seriei $1, \alpha, \beta, \gamma$ etc. in serie $1, A, B, C, D$ etc. occurrunt, pares autem ibi non reperiuntur, at vero iidem aucti numero $2p+1$. Sit enim α numerus impar, et cum $aa-\alpha$ sit divisibile per $2p+1$, erit $aa-\alpha = n(2p+1)$. Iam a vel est par vel impar. Si impar, erit $aa-\alpha$ par, ac propterea etiam n par, sicque $aa-\alpha$ divisibile erit per $2(2p+1)$.

510. At si a sit par, erit $2p+1-a$ impar, atque etiam

$$(2p+1-a)^2 - \alpha = n(2p+1),$$

ubi n fiet par, ita ut haec formula quoque per $2(2p+1)$ sit divisibilis; unde si α sit numerus impar, certe inter residua $1, A, B, C$ etc. continebitur.

511. At si α sit numerus par, eius loco inter residua divisoris $2p+1$ considerari potest $\alpha + 2p + 1$, qui cum sit impar, ob rationes allatas etiam inter residua divisoris $2(2p+1)$ reperiri debet.

512. Datis ergo residuis $1, \alpha, \beta, \gamma$ etc. ex divisore primo $2p+1$ ortis, ex iis statim concinnari potest series residuorum $1, A, B, C$ etc. ex duplo divisore $2(2p+1)$ ortorum, illorum scilicet, quae sunt imparia ipsa ponendo, paria autem numero $2p+1$ augendo.

513. Simili modo ex serie non-residuorum $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \mathfrak{d}$ etc. divisori $2p+1$ respondentium formabitur series non-residuorum divisori $2(2p+1)$ respondentium, dum imparia ipsa sumuntur, paria vero numero $2p+1$ augentur.

De divisore $4(2p+1) = d$

514. Multitudo numerorum hoc divisore minorum ad eumque primorum est $2 \cdot 1 \cdot 2p = 4p$, et non solum quadrata aa et $(d-a)^2$ idem relinquunt residuum, sed dantur praeterea duo alia bb et $(d-b)^2$. Fieri enim potest $bb - aa = (b-a)(b+a) = 4n(2p+1)$ sumendo $b - a = 2n$ et $b + a = 2(2p+1)$, unde fit $b = 2(2p+1) - a$, sicque quaternorum quadratorum idem residuum relinquentium radices sunt: a, $2(2p+1)-a$, $2(2p+1)+a$, $4(2p+1)-a$.

515. Plura autem quam quatuor dari non possunt, unde hoc casu numerus residuorum tantum est p, uti pro divisore primo $2p+1$; at numerus non-residuorum est $3p$, ut ex subiunctis exemplis videre licet:

Divisor	3	12	5	20	7	28
Residua	1	1	1, 4	1, 9	1, 2, 4	1, 9, 25
Non-residua	2	5 7 11	2, 3	3, 7 11, 19 13, 17	3, 5, 6	3, 27, 19 5, 17, 13 11, 15, 23

Divisor	11	44
Residua	1, 3, 9, 5, 4	1, 9, 25, 5, 37
Non-residua	2, 6, 7, 8, 10	3, 27, 31, 15, 23 7, 19, 43, 35, 39 13, 29, 17, 21, 41

Divisor	13	52
Residua	1, 3, 4, 9, 10, 12	1, 9, 25, 49, 29, 17
Non-residua	2, 5, 6, 7, 8, 11	3, 27, 23, 43, 35, 51 5, 45, 21, 37, 41, 33 7, 11, 19, 31, 47, 15

516. Sint pro divisore $2p+1$ residua $1, \alpha, \beta, \gamma, \delta$ etc. et pro divisore $4(2p+1)$ residua $1, A, B, C, D$ etc. multitudine aequalia, ac primo patet ex his residuis illa reperiri, scilicet ex serie $1, A, B, C, D$ etc., quae sunt minora quam $2p+1$, ipsa in serie $1, \alpha, \beta, \gamma, \delta$ etc. continentur; quae vero sunt maiora, minui debent numero $2p+1$ vel eius duplo vel eius triplo.

517. Deinde observo inter residua 1, A, B, C, D etc. nullum numerum huius formae $4q - 1$ contineri. Cum enim quadratum aa demto numero $4q - 1$ nequeat esse divisibile per 4, fieri non potest, ut sit $aa - (4q - 1)$ multiplum ipsius $4(2p + 1)$, unde numeri 3, 7, 11, 15, 19, 23 [etc.] semper sunt inter non-residua.

518. Si in serie $1, \alpha, \beta, \gamma, \delta$ etc. occurrat numerus impar formae $4q + 1$, idem quoque in serie $1, A, B, C, D$ etc. occurret; nam, si $aa - (4q + 1)$ sit divisibile per $2p + 1$, quoque divisibile erit $(2p + 1 \pm a)^2 - (4q + 1)$; et quia numerorum a et $2p + 1 \pm a$ alter certe est par, alter impar, sumatur a impar, et $aa - (4q + 1)$ per 4 erit divisibile, unde etiam per $4(2p + 1)$, ita ut pro hoc divisore $4q + 1$ futurum sit residuum.

519. At si numerus impar $4q - 1$ sit residuum divisoris $2p + 1$, non erit residuum divisoris $4(2p + 1)$, uti iam vidimus; tum vero $2(2p + 1) + 4q - 1$, quia redit ad formam $4r + 1$, certe inter residua divisoris $4(2p + 1)$ continebitur.

520. Si numerus par $2q$ sit residuum divisoris $2p + 1$, tum vel $2q + 2p + 1$ vel $2q + 3(2p + 1)$ erit residuum divisoris $4(2p + 1)$, prout vel hic vel ille numerus fuerit formae $4r + 1$, alter enim formae $4r - 1$ semper excluditur.

521. Scilicet, si sit $p = 2m$ et $4m + 1$ numerus primus, si $4q$ sit residuum divisoris $4m + 1$, tum $4q + 4m + 1$ erit residuum divisoris $4(4m + 1)$; at si $4q + 2$ residuum divisoris $4m + 1$, tum $4q + 2 + 3(4m + 1)$ erit residuum divisoris $4(4m + 1)$.

522. Sit $p = 2m - 1$ et $4m - 1$ numerus primus; si $4q$ sit residuum divisoris $4m - 1$, tum $4q + 3(4m - 1)$ erit residuum divisoris $4(4m - 1)$. At si $4q + 2$ sit residuum divisoris $4m - 1$, tum $4q + 2 + 4m - 1 = 4q + 4m + 1$ erit residuum divisoris $4(4m - 1)$.

523. Ope harum regularum ex singulis residuis divisoris primi $2p + 1$ totidem residua divisoris $4(2p + 1)$ reperiuntur; unumquodque enim vel ipsum vel auctum numero $2p + 1$ vel $2(2p + 1)$ vel $3(2p + 1)$, ut prodeat numerus formae $4q + 1$, erit residuum divisoris $4(2p + 1)$.

524. Ex quovis autem residuo divisoris $2p + 1$ unum quoque non-residuum pro divisore $4(2p + 1)$ elicitur formae $4q - 1$; tum vero ex quovis non-residuo divisoris $2p + 1$ bina non-residua pro divisore $4(2p + 1)$ prodeunt; si enim illud sit par, addendo $2p + 1$ et $2(2p + 1)$, sin sit impar, addendo 0 et $2(2p + 1)$ duo non-residua obtinentur.

De divisore $8(2p+1) = d$

525. Hic semper octo dantur numeri minores quam d, quorum quadrata per d divisa relinquunt idem residuum; scilicet, uno numero existente a reliqui septem sunt

$$2(2p+1) \pm a, \quad 4(2p+1) \pm a, \quad 6(2p+1) \pm a, \quad 8(2p+1) - a,$$

neque plures exhiberi possunt.

526. Quare, cum multitudo numerorum ipso d minorum ad eumque primorum sit $= 4 \cdot 1 \cdot 2p = 8p$, horumque octoni idem praebeant residuum, manifestum est numerum residuorum diversorum fore $= p$, non-residuorum vero $= 7p$.

527. Deinde patet inter residua occurrere non posse ullum numerum formae $4q - 1$ vel alterutrius huius $8q - 1$, $8q - 5$; neque vero etiam inter residua esse potest numerus formae $8q + 5$, propterea quod forma $xx - (8q + 5)$ nunquam per 8 neque ergo per $8(2p + 1)$ dividi potest, quia est $xx = 8n + 1$ ob x imparem.

528. Alia igitur residua non locum habent, nisi quae sint formae $8n + 1$, et quia divisor est $16p + 8$, pro n sumi possunt omnes numeri ab 0 usque ad $2p$. At ex forma $8n + 1$ excluditur vel $2p + 1$ vel $3(2p + 1)$ vel $5(2p + 1)$ vel $7(2p + 1)$, quae, scilicet, est formae $8n + 1$, ita ut tantum $2p$ huiusmodi numeri relinquantur, quorum autem semissis solum residua constituit.

529. Ex his autem numeris formae $8n + 1$, quorum multitudo est $2p$, si unicus constet, qui sit non-residuum, eo per singula residua multiplicando obtinentur reliqua non-residua numero p, praeterea vero reliqui numeri impares sive formae $8n + 3$ sive $8n + 5$ sive $8n + 7$ suppeditant adhuc $6p$ residua.

530. Divisor ergo $8(2p + 1)$ totidem praebet residua, quot divisor $2p + 1$, quae si sint $1, \alpha, \beta, \gamma, \delta$ etc., ex singulis residua divisoris $8(2p + 1)$ elicientur addendo eiusmodi multiplum ipsius $2p + 1$, ut aggregatum fiat formae $8n + 1$, veluti ex hoc exemplo videre licet:

Pro divisore 13 residua:	1,	3,	4,	9,	10,	12,
adde:	0,	$6 \cdot 13$,	13,	0,	$3 \cdot 13$,	13,
pro divisore 104 residua:	1,	81,	17,	9,	49,	25.

531. Si pro divisore $8(2p + 1)$ fuerit A [residuum], erit $A^p - 1$ divisibile per $8(2p + 1)$; ac si hoc evenerit, erit A vicissim residuum quadratorum.

Scilicet, si $A^p - 1$ sit divisibile per $8(2p+1)$, semper assignari potest quadratum xx, ut sit $xx - A$ divisibile per $8(2p+1)$.

De divisore $3(2p+1) = d$, $[p \neq 1]$

532. Multitudo numerorum hoc divisore minorum et ad eum primorum est $= 2 \cdot 2p = 4p$, inter quos duo ad minimum sunt, quorum quadrata idem residuum relinquunt, scilicet a^2 et $(d-a)^2$, unde numerus diversorum residuorum maior quam $2p$ esse nequit.

533. Praeterea vero, cum a per 3 non sit divisibile, vel $2p+1-2a$ vel $2(2p+1)-2a$ per 3 erit divisibile; sit quotus $= m$, et quadratum numeri $3m+a$ idem relinquet residuum, ergo vel $2p+1-a$ vel $2(2p+1)-a$, indeque praeterea vel $2(2p+1)+a$ vel $2p+1+a$ idem quoque residuum relinquet.

534. Hoc modo cum semper quaterna quadrata idem dent residuum, numerus residuorum diversorum erit tantum $= p$, ideoque idem ac pro divisore $2p+1$. In residuis autem nequit esse ullus numerus formae $3n-1$, cum nullum quadratum tali numero minutum per 3 neque ergo per $3(2p+1)$ dividi queat.

535. Omnia ergo residua divisoris $3(2p+1)$ erunt numeri formae $3n+1$, et si residua divisoris $2p+1$ sint $1, \alpha, \beta, \gamma$ etc., quodlibet vel ipsum vel numero $2p+1$ vel $2(2p+1)$ auctum, quo prodeat numerus formae $3n+1$, erit residuum divisoris $3(2p+1)$.

Pro divisore $(2p+1)(2q+1) = d$, $[p \neq q]$

536. Sint pro divisore $2p+1$ residua $1, \alpha, \beta, \gamma, \delta$ etc. numero $= p$, et pro divisore $2q+1$ residua $1, \pi, \varrho, \sigma, \tau$ etc. numero $= q$, ac numeri utrique ordini communes erunt residua divisoris $d = (2p+1)(2q+1)$.

537. At ad priorem ordinem pertinere censendus est numerus $m(2p+1)+\alpha$, ubi m ita potest definiri, ut fiat aequalis vel $n(2q+1)+1$ vel $n(2q+1)+\pi$ etc., sicque ex quovis residuo divisoris $2p+1$ producuntur q residua divisoris $2q+1$, sicque omnino pq residua diversa pro divisore $(2p+1)(2q+1)$ obtinentur.

538. Sit huiusmodi divisor compositus $5 \cdot 7 = 35$, et cum sint residua pro divisore 5 haec duo 1, 4 et pro 7 haec tria 1, 2, 4, ergo pro divisore 35 residua erunt $7n+1$, $7n+2$, $7n+4$, quae scilicet vel in forma $5m+1$,

vel $5m + 4$ continentur. Erunt ergo haec residua numero sex: 1, 29; 16, 9; 11, 4.

539. Cum pro divisore $(2p + 1)(2q + 1)$ tantum dentur pq residua diversa, quaterna quadrata idem praebebunt residuum, quorum unum si sit $= aa$, reliquorum trium radices erunt:

$$(2p + 1)(2q + 1) - a, \quad m(2p + 1) - a, \quad n(2p + 1) + a,$$

sumendis numeris m et n ita, ut $m(2p + 1) - 2a$ et $n(2p + 1) + 2a$ dividi queant per $2q + 1$, quod ob $2p + 1$ et $2q + 1$ primos inter se semper fieri potest, ut m et n sint minores quam $2q + 1$.

CAPUT 15

DE DIVISORIBUS NUMERORUM FORMAE $xx + yy$ [1])

540. Hinc primo excludo casus, quibus numeri x et y habent communem divisorem; si enim maximus communis divisor esset $= \varphi$ et $x = p\varphi$ et $y = q\varphi$, ut p et q forent primi inter se, haberetur $xx + yy = (pp + qq)\varphi\varphi$, et inventio divisorum reduceretur ad formam $pp + qq$.

541. Sint ergo x et y primi inter se, atque evenire potest, ut $xx + yy$ fiat numerus primus, cui probando vel unicus casus sufficeret, quorum simplicissimus est 2. Ut autem $xx + yy$ fiat numerus primus, statim excluduntur casus, quibus ambo numeri x et y sunt impares.

542. Ponatur ergo alter par alter impar, et evidens est omnes numeros primos $xx + yy$ in hac forma $4n + 1$ contineri debere, sicque nullus numerus formae $4n - 1$ duorum quadratorum summa esse potest.

543. Sin autem x et y sint numeri impares seu $x = 2p + 1$ et $y = 2q + 1$, fieri poterit, ut semissis $\frac{xx + yy}{2} = 2pp + 2p + 2qq + 2q + 1$ fiat numerus primus. At est

$$2pp + 2p + 2qq + 2q + 1 = (p + q + 1)^2 + (p - q)^2,$$

iterum summa duorum quadratorum, quorum alterum par alterum impar ob summam radicum $2p + 1$ imparem.

---

1) Confer Commentationem 228 indicis ENESTROEMIANI, novi comm. acad. sc. Petrop. 4 (1752/3), 1758, p. 3; *LEONHARDI EULERI Opera omnia*, series I, vol. 2, p. 295, ubi theoremata simili methodo demonstrata sunt. R. F.

544. Si summa duorum quadratorum $aa + bb$ per aliam summam duorum quadratorum $cc + dd$ multiplicetur, productum $(aa + bb)(cc + dd)$ iterum erit summa duorum quadratorum, cum sit $= (ac \pm bd)^2 + (ad \mp bc)^2$, quod ob ambiguitatem signi duplici modo evenire potest.

545. Hic inversa propositio se offert, si summa duorum quadratorum $pp + qq$ divisionem admittat per summam duorum quadratorum $aa + bb$, fore etiam quotum duorum quadratorum summam, cuius veritas autem inde non sequitur, sed peculiarem demonstrationem requirit.

546. Ad hoc demonstrandum primum animadverto formam $pp + qq$ per $aa + bb$ esse divisibilem, quanticunque sint numeri p et q, semper eos reduci posse ad numeros minores quam $aa + bb$ atque adeo quam $\frac{1}{2}(aa + bb)$, cum, si $pp + qq$ sit divisibile per $aa + bb$, etiam

$$(\pm \alpha(aa + bb) \pm p)^2 + (\pm \beta(aa + bb) \pm q)^2$$

divisibile evadat.

547. At si $\frac{pp + qq}{aa + bb}$ sit summa duorum quadratorum $cc + dd$ seu $p = ac + bd$ et $q = ad - bc$, sumendo

$$p' = ac + bd + \alpha(aa + bb) \quad \text{et} \quad q' = ad - bc + \beta(aa + bb)\,^1),$$

tum $p'p' + q'q'$ utique per $aa + bb$ divisionem admittet, eritque quotus

$$= cc + dd + 2\alpha(ac + bd) + 2\beta(ad - bc) + (\alpha\alpha + \beta\beta)(aa + bb),$$

qui etiam est summa duorum quadratorum $(c + \alpha a - \beta b)^2 + (d + \alpha b + \beta a)^2$.

548. Verum haec altius sunt petenda; dico ergo primo, si divisor $aa + bb$ sit numerus primus, per quem forma $pp + qq$ sit divisibilis, quotum esse summam duorum quadratorum; quod etsi in genere verum est existente $aa + bb$ etiam numero composito, tamen demonstratio ab hoc casu derivanda videtur.

549. Cum a et b sint numeri primi inter se, ad eos p ita referri potest, ut sit $p = ma - nb$, idque infinitis modis; iam si esset $q = na + mb$, foret utique $\frac{pp + qq}{aa + bb} = mm + nn$; at si non sit $q = na + mb$, ponatur $q = na + mb + s$ eritque

$$pp + qq = (aa + bb)(mm + nn) + 2s(na + mb) + ss.$$

1) In manuscripto p' per p $(= ac + bd)$ et q' per q $(= ad - bc)$ designatur. R. F.

550. Cum ergo $2s(na + mb) + ss$ sit divisibile per $aa + bb$, vel s vel $s + 2(na + mb)$ divisibile sit, necesse est. Priori casu ponatur $s = t(aa + bb)$, erit

$$\frac{pp + qq}{aa + bb} = mm + nn + t(t(aa + bb) + 2(na + mb))$$
$$= mm + 2mbt + ttbb + nn + 2nat + aatt = (m + bt)^2 + (n + at)^2,$$

ideoque summa duorum quadratorum.

551. Altero casu ponatur $s + 2(na + mb) = t(aa + bb)$, erit $s = t(aa + bb) - 2(na + mb)$, ideoque

$$\frac{pp + qq}{aa + bb} = mm + nn + tt(aa + bb) - 2t(na + mb) = (m - bt)^2 + (n - at)^2,$$

ita ut utroque casu quotus sit summa duorum quadratorum.

552. Si ergo $pp + qq$ sit divisibile per numerum primum $aa + bb$, demonstratum est quotum esse quoque summam duorum quadratorum. Hinc, si quotus non esset summa duorum quadratorum, divisor non foret numerus primus formae $aa + bb$, hoc est, vel si esset primus, non esset formae $aa + bb$, vel si esset formae $aa + bb$, non esset primus; vocabula autem quoti et divisoris inter se permutare licet.

553. Denotent brevitatis gratia litterae A, B, C, D etc. numeros primos formae $aa + bb$, et si summa duorum quadratorum $pp + qq$ divisibilis sit per talium numerorum productum $ABC\ldots$, quotus quoque erit summa duorum quadratorum. Est enim $\frac{pp + qq}{A} = rr + ss$, tum vero $\frac{rr + ss}{B} = tt + uu$ atque $\frac{tt + uu}{C} = xx + yy$, unde fit $\frac{pp + qq}{ABC} = xx + yy$.

554. Si ergo summa duorum quadratorum $pp + qq$ divisibilis esset per numerum non-summam duorum quadratorum, quotus, si esset primus, non foret summa duorum quadratorum, et si esset compositus, non foret productum ex talibus numeris primis, qui singuli essent summae duorum quadratorum.

555. Quare, si summa duorum quadratorum $pp + qq$ unum habeat factorem, qui non sit summa duorum quadratorum, inter reliquos factores primos ad minimum unus, qui etiam non sit summa duorum quadratorum, reperiatur necesse est.

556. Nunc igitur investigemus, an summa duorum quadratorum $pp + qq$ inter se primorum per ullum numerum $\mathfrak{A}$, qui non sit summa duorum quadra-

torum, divisibilis esse queat. Ad hoc sumamus $pp + qq$ divisibile esse per talem numerum $\mathfrak{A}$, atque etiam $(p - m\mathfrak{A})^2 + (q - n\mathfrak{A})^2$ divisibilis erit per $\mathfrak{A}$, quorum radices, si p et q sint primi inter se, etiam erunt primae inter se [1]).

557. Poterit ergo talis summa duorum quadratorum $pp + qq$ exhiberi, quorum radices p et q minores sint quam $\mathfrak{A}$, quin etiam minores quam $\frac{1}{2}\mathfrak{A}$; cum etiam $(\mathfrak{A} - p)^2 + (\mathfrak{A} - q)^2$ divisionem admittere debeat, quorum quadratorum radices minores erunt quam $\frac{1}{2}\mathfrak{A}$, si p et q eo essent maiores.

558. Dabitur ergo summa duorum quadratorum $pp + qq$ minor quam $\frac{1}{2}\mathfrak{A}\mathfrak{A}$ (cum sit $p < \frac{1}{2}\mathfrak{A}$ et $q < \frac{1}{2}\mathfrak{A}$) per numerum $\mathfrak{A}$ divisibilis; ponatur quotus $= \mathfrak{B}$, qui etiam vel ipse non erit summa duorum quadratorum, vel factorem talem habebit, eritque $\mathfrak{B} < \frac{1}{2}\mathfrak{A}$.

559. Cum iam $pp + qq$ divisibile sit per $\mathfrak{B}$, exhiberi poterit summa duorum quadratorum $rr + ss$ minor quam $\frac{1}{2}\mathfrak{B}\mathfrak{B}$, divisibilis per $\mathfrak{B}$, et quotus $\mathfrak{C}$, qui erit minor quam $\frac{1}{2}\mathfrak{B}$, pariter non erit summa duorum quadratorum, per quem cum divisibilis sit $rr + ss$, dabitur $tt + uu < \frac{1}{2}\mathfrak{C}\mathfrak{C}$ divisibilis per $\mathfrak{C}$, et quotus $\mathfrak{D} < \frac{1}{2}\mathfrak{C}$ itidem non erit summa duorum quadratorum.

560. Hoc modo tandem pervenietur ad summam duorum quadratorum quantumvis parvam, quae foret divisibilis per numerum non-summam duorum quadratorum, quod cum sit absurdum, necessario sequitur summam duorum quadratorum inter se primorum non esse divisibilem per ullum numerum, qui ipse non sit summa duorum quadratorum.

561. Proposito autem numero primo quocunque formae $4n + 1$, quia inter residua quadratorum est -1 vel $4n$, semper summa duorum quadratorum per eum divisibilis exhiberi potest, unde sequitur omnes numeros primos formae $4n + 1$ esse summas duorum quadratorum.

562. Deinde cum numeri formae $4n - 1$ nunquam esse possint summae duorum quadratorum, nulla summa duorum quadratorum inter se primorum per ullum talem numerum $4n - 1$ divisibilis esse potest.

563. Desideratur autem demonstratio succinctior, qua probetur, si summa duorum quadratorum $pp + qq$ divisibilis fuerit per summam duorum quadratorum $aa + bb$, quotum necessario quoque esse summam duorum quadratorum, quod sequenti ratiocinio perficere tentemus.

---

1) A „quorum“ usque ad „se“ ad marginem scriptum est. R. F.

564. In divisore $aa + bb$ numeros a et b inter se primos assumere licet; si enim non essent primi inter se, sublatione communis factoris tales redderentur; erit ergo $aa + bb$ tam ad a quam ad b primus. Unde quicunque numeri fuerint p et q, ii ita repraesentari poterunt

$$p = m(aa + bb) \pm fa \quad \text{et} \quad q = n(aa + bb) \pm gb,$$

id quod infinitis modis fieri potest.

565. Cum igitur $pp + qq$ sit divisibile per $aa + bb$, etiam $ffaa + ggbb$ per $aa + bb$ erit divisibile, atque ob illas infinitas resolutiones omnes casus, quibus $ffaa + ggbb$ per $aa + bb$ divisibile evadit, prodire debent, ergo etiam casus $g = f$ prodeat necesse est, quoniam hoc divisio succedit.

[*Additamentum*][1]): Hic dubium esse potest, an casus $g = f$ necessario ex divisibilitate formulae $pp + qq$ sequatur. Hoc dubium est fundatum; nam sit

$$a = 7,\ b = 4,\ p = 17,\ q = 6, \quad aa + bb = 65,\ pp + qq = 325;$$

fieri autem nequit $17 = 65m \pm 7f$ simul $6 = 65n \pm 4f$, unde haec posterior demonstratio reiicienda.
$\frac{17^2 + 6^2}{7^2 + 4^2} = 1^2 + 2^2$, etsi nullo modo sit $17 = 1 \cdot 7 \pm 2 \cdot 4$ vel $17 = 2 \cdot 7 \pm 1 \cdot 4$.

566. Hoc concesso habebimus $p = m(aa + bb) \pm fa$ et $q = n(aa + bb) \pm fb$; unde fit

$$\frac{pp + qq}{aa + bb} = \begin{cases} mm(aa + bb) \pm 2fma \\ nn(aa + bb) \pm 2fnb \end{cases} + ff,$$

quae expressio est $= (f \pm ma \pm nb)^2 + (\pm na \mp mb)^2$, ideoque summa duorum quadratorum.

567. Hinc ergo statim sequitur, si quotus non sit summa duorum quadratorum, neque divisorem talem esse posse, neque ergo productum ex duobus numeris, quorum alter est summa duorum quadratorum alter secus, summa duorum quadratorum esse potest.

568. Coniunctis cum hisce, quae ante paragraphum 557 et sequentes sunt proposita, evincitur summam duorum quadratorum inter se primorum nullos habere divisores, nisi qui ipsi sint summae duorum quadratorum, tum vero omnes numeros primos formae $4n + 1$ esse summas duorum quadratorum.

---

1) Vide notam p. 203. Ex divisibilitate solum sequitur $f^2 - g^2 = (f - g)(f + g)$ per $a^2 + b^2$ divisibile esse; si $a^2 + b^2$ non est numerus primus, $f - g$ et $f + g$ per factores diversos numeri $a^2 + b^2$ divisibiles esse possunt. Vide paragraphum 580. R. F.

569. Si numerus quispiam N duplici modo est summa quadratorum, scilicet

$$N = aa + bb = cc + dd\,,$$

tum non est primus. Cum enim sit $aa - cc = dd - bb$, erit $d + b = \frac{m(a+c)}{n}$ et $d - b = \frac{n(a-c)}{m}$, unde $b = \frac{m(a+c)}{2n} - \frac{n(a-c)}{2m}$, hinc

$$N = aa + bb = \frac{(mm+nn)}{4mmnn}\left(nn(a-c)^2 + mm(a+c)^2\right) =$$

$$= \frac{(mm+nn)}{4mm}\left((a-c)^2 + (b+d)^2\right),$$

ubi denominator alterum numeratoris factorem tollere nequit:

$$(a+c)(a-c) = (b+d)(d-b) = pqrs,\quad a+c = pq,\quad a-c = rs,$$
$$b+d = pr,\quad d-b = qs,$$

$$a = \frac{pq+rs}{2},\ b = \frac{pr-qs}{2},\ aa + bb = \frac{1}{4}(pp+ss)(qq+rr).$$

CAPUT 16

DE DIVISORIBUS NUMERORUM FORMAE $xx + 2yy$ [1]

570. Sumtis x et y inter se primis vel ambo sunt impares vel alteruter tantum par, ergo vel x vel y erit par; ex quo tres resultant casus considerandi, qui cuiusmodi numeros ratione paritatis et imparitatis praebeant, investigasse iuvabit.

571. Si ambo numeri x et y sint impares, eorum quadrata sunt numeri formae $8n + 1$, fietque $xx + 2yy$ numerus formae $8n + 3$; sin autem x impar et y par, ob $xx = 8m + 1$ et $2yy = 2 \cdot 4n$ fiet $xx + 2yy$ numerus formae $8n + 1$.

1) Vide Commentationem 164 p. 225 laudatam et Commentationem 256 indicis ENESTROEMIANI, novi comm. acad. sc. Petrop. 6 (1756/7), 1761; *LEONHARDI EULERI Opera omnia*, series I, vol. 2, p. 459. R. F.

572. Si x sit par et y impar, ponatur $x = 2z$, et fiet $xx + 2yy = 2(2zz + yy)$; iam cum y sit impar, prout z fuerit vel par vel impar, erit vel $xx + 2yy = 2(8n + 1)$ vel $xx + 2yy = 2(8n + 3)$.

573. Omnes ergo numeri in forma $xx + 2yy$ contenti, dum x et y sunt primi inter se vel saltem non ambo pares, si fuerint impares, pertinebunt vel ad formam $8n + 1$ vel ad $8n + 3$; sin autem illi numeri sint pares, vel ad formam $2(8n + 1)$ vel ad $2(8n + 3)$ erunt referendi, et casu hocposteriori eorum semisses, scilicet $2zz + yy$, sunt etiam numeri formae $xx + 2yy$.

574. Numeri ergo impares, qui sunt vel formae $8n + 5$ vel formae $8n + 7$, certe non sunt numeri formae $xx + 2yy$, neque etiam dupla earum formarum in hac continentur, unde infiniti dantur numeri in forma $xx + 2yy$ non contenti.

575. Productum autem duorum numerorum huius formae in eadem forma continetur; est enim

$$(aa + 2bb)(cc + 2dd) = (ac \pm 2bd)^2 + 2(ad \mp bc)^2,$$

unde simul patet talia producta duplici modo in ista forma contineri.

576. Iam demonstrandum est, si numerus $pp + 2qq$ dividi queat per $aa + 2bb$, fore quotum etiam istius formae. Notetur hic ob a et b primos ad $aa + 2bb$ infinitis modis fieri posse

$$p = m(aa + 2bb) \pm fa \quad \text{et} \quad q = n(aa + 2bb) \pm gb,$$

hincque fore $ffaa + 2ggbb$ per $aa + 2bb$ divisibile.

577. Si concedatur hoc modo omnes formulas $ffaa + 2ggbb$ per $aa + 2bb$ divisibiles obtineri, ibi etiam continebitur casus $gg = ff$ seu $g = \pm f$[1]), unde prodit

$$\frac{pp + 2qq}{aa + 2bb} = \begin{cases} mm(aa + 2bb) \pm 2mfa \\ 2nn(aa + 2bb) \pm 4nfb \end{cases} + ff = (f \pm ma \pm 2nb)^2 + 2(mb \mp na)^2.$$

578. Hoc autem, quod concedendum postulavi, ita confirmari potest. Sint $1, \alpha, \beta, \gamma, \delta$ etc. residua, quae ex divisione quadratorum per numerum $aa + 2bb$ oriuntur, atque in istis residuis continebuntur tam omnia quadrata, quam $-2bb$ et -2 seu omnia quadrata negativa duplicata, hoc est -2, -2α, -2β, -2γ etc.

1) Vide ad hanc demonstrationem additamentum ad § 565, p. 278 huius voluminis. R. F.

579. Iam quodcunque residuum quadratum qq per $aa + 2bb$ divisum relinquat, cum poni possit $q = n(aa + 2bb) \pm gb$, id per $ggbb$ exhiberi potest, et residuum ex divisione ipsius $2qq$ ortum per $2ggbb$; quadratum ergo pp per $aa + 2bb$ divisum relinquere debet $-2ggbb$, cuius loco poni potest $aagg$, sicque quadrata pp et $aagg$ paria relinquent residua, sicque fieri potest

$$p = m(aa + 2bb) \pm ag .$$

580. At haec demonstratio est reiicienda, nisi sit $aa + 2bb$ numerus primus; nam, si sit primus, ob $ffaa + 2ggbb$ et $ggaa + 2ggbb$ divisibile per $aa + 2bb$ necesse est, sit $ff - gg$ ideoque vel $f - g$ vel $f + g$ divisibile; utrovis autem casu, ob $aa + 2bb$ iam in altera parte contentum, prodit vel $g = +f$ vel $g = -f$; quae conclusio locum non habet, si $aa + 2bb$ sit numerus compositus, cum tunc $f - g$ per alterum eius factorem et $f + g$ per alterum divisibile esse posset.

581. Si numerus $pp + 2qq$ per numerum $\mathfrak{A}$, qui non sit formae $xx + 2yy$, dividi queat, quotus non erit numerus primus formae $xx + 2yy$; quare, si quotus sit primus, non erit formae $xx + 2yy$; at si sit compositus, certe non omnes factores primi erunt huius formae.

582. Denotent enim A, B, C, D etc. numeros primos formae $xx + 2yy$, ac si $pp + 2qq$ esset divisibile per $ABCD$ etc., quotus certe esset formae $xx + 2yy$; ergo, si quotus seu alter multiplicator non sit formae $xx + 2yy$, fieri nequit, ut alter factor sit productum talium numerorum primorum.

583. Quare, si $pp + 2qq$ dividi queat per numerum $\mathfrak{A}$ ex forma $xx + 2yy$ exclusum, quotus, si sit primus, non erit huius formae vel, si sit compositus, factorem certe habebit non huius formae.

[*Additamentum*][1]): Ergo $pp + 2qq$ per nullos numeros primos formae $8n + 5$ et $8n + 7$ dividi potest; unde, si quadrata per tales numeros primos dividantur, inter non-residua erit -2. Si

$$\frac{xx + nyy}{aa + nbb} = \text{integro, erit } \frac{bbxx - aayy}{aa + nbb} = \text{integro et } \frac{aaxx - nnbbyy}{aa + nbb} = \text{integro.}$$

584. Denotent $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D}$ etc. numeros primos ex forma $xx + 2yy$ exclusos, et vidimus $pp + 2qq$ non esse posse $A\mathfrak{A}$ neque $AB\mathfrak{A}$ neque $ABC\mathfrak{A}$; quare certum est inter factores primos numerorum $pp + 2qq$ vel nullum vel duos ad minimum numeros $\mathfrak{A}$, $\mathfrak{B}$ contineri.

2) Vide notam p. 203. R. F.

585. Hinc autem nondum concludi potest, si unus factor, etiamsi sit compositus, ipsius $pp + 2qq$ fuerit formae $xx + 2yy$, etiam alterum fore huius formae. Demonstrandum restat numerum $pp + 2qq$ non esse posse formae vel $\mathfrak{AB}$ vel $A\mathfrak{AB}$ vel $AB\mathfrak{AB}$, quod si esset, foret utique $\mathfrak{AB}$ numerus huius formae.

586. Visuri autem, an $pp + 2qq$ per numerum $\mathfrak{A}$ non formae $xx + 2yy$ dividi queat, quod si fieri posset, foret $p < \frac{1}{2}\mathfrak{A}$ et $q < \frac{1}{2}\mathfrak{A}$, unde $pp + 2qq < \frac{3}{4}\mathfrak{AA}$, quotusque $< \frac{3}{4}\mathfrak{A}$, qui esset vel ipse numerus non $xx + 2yy$ vel factorem talem haberet $\mathfrak{B}$, qui cum etiam factor esset ipsius $pp + 2qq$, minimus talis numerus $\mathfrak{B}$ assignari posset, divisor formae cuiuspiam $xx + 2yy$, quod cum fieri nequeat, numeri $pp + 2qq$ nullos habent divisores primos, qui non ipsi sint formae $xx + 2yy$.

[*Additamentum*][1]): *Tentamen demonstrationis, quod, si divisor primus sit* $8q + 7$, *in residuis reperiatur* 2.

Ponamus esse in residuis 2, et cum ibidem sit $(2q + m)^2$, erit quoque $8qq + 8mq + 2mm$, hincque $8mq + 2mm - 7q$ et $2mm - 7m - 7q$ et $2mm - 7m + q + 7$, quod si nunquam fiat non-residuum, patebit propositum. At non-residua repraesentari possunt per quadrata negativa, quorum dupla etiam erunt non-residua per hypothesin; sit ergo

$$2mm - 7m + q + 7 = -2aa + 8bq + 7b, \text{ fietque:}$$

$$q = \frac{2aa + 2mm - 7m + 7 - 7b}{8b - 1} \quad \text{et} \quad 8q + 7 = \frac{16aa + 16mm - 56m + 49}{8b - 1} = \frac{(4a)^2 + (4m - 7)^2}{8b - 1},$$

foretque $8q - 7$ divisor ipsius $(4a)^2 + (4m - 7)^2$, quod cum fieri nequit, sequitur ex residuo 2 nullum deduci absurdum, cuiusmodi necessario resultare deberet, si 2 non esset residuum.

Si $2mm - 7m + q + 7$ ponatur $= -aa$ $[+ 8bq + 7b]$, fit

$$8q + 7 = \frac{2(2a)^2 + (4m - 7)^2}{8b - 1};$$

nunc demonstrandum restat $2xx + yy$ nunquam divisibile esse per $8q + 7$.

$8xx - (2y + 1)^2$ alios divisores primos non habet, nisi formae $8n - 1$ et $8n + 1$,

1) Hoc additamentum, quod ad paragraphos 338 et 340 pertinere videtur, EULERUS in pagina intercalata scripsit. R. F.

$\frac{8xx-1}{7}$ integer, si $x = 7a \pm 1$, $\frac{8xx-1}{23}$ integer, si $x = 23a \pm 7$,

$\frac{8xx-1}{31}$ integer, si $x = 31a \pm 2$, $\frac{8xx-1}{47}$ integer, si $x = 47a \pm 10$,

$\frac{8xx-1}{17}$ integer, si $x = 17a \pm 7$, $\frac{8xx-1}{41}$ integer, si $x = 41a \pm 6$.

Vel ita pro divisore [primo] $8q + 7$:

Si 2 esset non-residuum, in genere $2mm - 7m - 7q \pm \alpha(8q + 7)$ esset non-residuum; in genere autem residuum est

$$(4q + n)^2 = 16qq + 8nq + nn = 8nq + nn - 14q = nn - 14q - 7n = \\ = nn + 2q - 7n + 14 \pm \beta(8q + 7),$$

omnes ergo numeri continerentur in alterutra harum formularum:

$$2mm - 7m - 7q \pm \alpha(8q + 7), \quad nn - 7n - 14q \pm \beta(8q + 7).$$

Si unicus assignari posset hic non contentus, demonstratio esset perfecta; vel si idem numerus in utraque contineretur, quod fit, si posito $m = f + g$, $n = f + 2g$ fuerit $ff - 2gg + 7g + 7q$ divisibile per $8q + 7$.

Theorema: Si divisor [*primus est formae*] $12q + 11$, *erit* 3 *residuum.*

Ponamus 3 esse residuum, ac si nullum absurdum inde sequatur, pro vero erit habendum. Erit ergo -3 non-residuum, et omnia non-residua $-3aa$. At residuum est $(2q + m)^2$ et $12qq + 12mq + 3mm$, hincque $3mm - 11q - 11m$, item $3mm + q - 11m + 11$, quod nunquam potest esse non-residuum $-3aa$; ponatur enim

$$3mm - 11m + 11 + q = -3aa + 12bq + 11b,$$

erit

$$q = \frac{3aa + 3mm - 11m + 11 - 11b}{12b - 1}, \text{ unde fit } 12q + 11 =$$

$$= \frac{36aa + 36mm - 132m + 121}{12b - 1} = \frac{(6a)^2 + (6m - 11)^2}{12\,b - 1},$$

quod cum sit absurdum, $3mm - 11m + 11 + q$ nunquam inter non-residua continebitur.

CONSIDERATIONES CIRCA ANALYSIN DIOPHANTEAM

Commentatio 793 indicis ENESTROEMIANI
Prima editio: Commentationes arithmeticae 2, 1849, p. 576—587
Haec editio congruit cum manuscripto manu Euleri facto et academiae scientiarum Petropolitanae relicto.

1. Saepe ac multum mecum cogitavi, an non liceret eam Analyseos partem, quae DIOPHANTEA appellari solet, veluti reliquas Matheseos disciplinas, ad certa capita revocare, quibus constitutis universus huius Analyseos complexus perspici et cuique problemati caput, ad quod referri oporteat, assignari queat, ut hinc principia statim innotescant, ex quibus cuiusque problematis solutionem peti conveniat. Verum postquam complures quaestiones huc pertinentes omni studio pertractassem, singulas fere sibi prorsus peculiares methodos et calculi artificia postulare deprehendi, ut propemodum totidem huius Analyseos capita constituenda videantur, quot problemata particularia in hoc genere proponi possunt. Ex quo nullo adhuc modo intelligere licet, quomodo pro hac Analyseos parte principia generalia constitui eamque in certas partes distribui oporteat.

2. Divisio quidem huius Analyseos in duas partes statim se offert, quarum altera eiusmodi problemata in se complectitur, quorum solutiones ita per formulas generales exhiberi queant, ut omnes plane solutiones in iis contineantur ex iisque derivari queant. Altera autem pars in eiusmodi quaestionibus solvendis versatur, quarum solutio generalis neutiquam in certis formulis comprehendi potest, sed ita institui solet, ut ex qualibet solutione iam inventa aliae novae deduci queant, quo in negotio tamen iterum fere infinita varietas pro diversa problematum indole cernitur; et quoniam nunc quidem maxima pars problematum, quae in Analysi DIOPHANTEA tractari solent, ad hanc alteram partem est referenda, multo minus methodi ad ea solvenda accommodatae ad certas classes revocari posse videntur.

3. Neque vero illa divisio problematum inde petita, quod alia solutionem generalem in certis formulis analyticis contentam admittant, alia vero tantum solutiones particulares recipiant, quae tamen continuo ad alias novas perducant, tam certo est stabilita, ut haec duo problematum genera ob suam naturam penitus a se invicem dirimantur, cum utique evenire queat, ut problemata, quae ad posteriorem partem referenda videntur, certis adhibitis artificiis generaliter resolvi queant. Cuiusmodi est problema de tribus cubis inveniendis, quorum summa sit cubus[1]), cuius solutiones antehac tantum particulares sunt datae, donec equidem eius solutionem generalem exhibui, ita ut hoc problema nunc primae parti accensendum videatur.

4. Cum igitur hactenus plura problemata DIOPHANTEA sim perscrutatus, unde multitudo ac varietas methodorum, quibus ad ea solvenda uti convenit, maxime elucet, nunc aliud eius generis problema, quod quidem apud Auctores passim occurrit, contemplabor, quod ita se habet:

PROBLEMA 1

Invenire tres numeros v, x, y, quorum binorum productum summa eorundem auctum producat numerum quadratum, ita ut hae tres formulae

$$vx + v + x,\ vy + v + y,\ xy + x + y$$

quadrata reddi debeant.

Deinde vero eandem quaestionem ad quatuor huiusmodi numeros extendam, quandoquidem tum maximae difficultates occurrunt, dum haec quaestio, uti est proposita, generaliter resolvi potest, ac solutio tantum in numeris integris certa artificia postulat.

5. Ad hoc problema resolvendum ponamus $v + 1 = A$, $x + 1 = B$ et $y + 1 = C$, ut sequentes tres formulae $AB - 1$, $AC - 1$ et $BC - 1$ quadrata fieri debeant. Statuamus igitur primo $AB = pp + 1$, $AC = qq + 1$ et $BC = rr + 1$, eritque

$$ABC = \sqrt{(pp + 1)(qq + 1)(rr + 1)}.$$

1) Vide Commentationem 255 indicis ENESTROEMIANI, *LEONHARDI EULERI Opera omnia*, vol. 2 seriei I, p. 428. R. F.

Quo iam haec formula facilius rationalis efficiatur, litteras p et q datas spectemus, ponamusque $(pp+1)(qq+1) = mm+nn$, ut sit $m = pq \pm 1$ et $n = p \mp q$, fietque

$$ABC = \sqrt{(mm+nn)(rr+1)} = \sqrt{((mr+n)^2 + (nr-m)^2)},$$

quae radix statuatur $= mr + n + t(nr - m)$, ut prodeat

$$nr - m = 2mrt + 2nt + nrtt - mtt,$$

hincque:

$$r = \frac{m(tt-1) - 2nt}{n(tt-1) + 2mt}.$$

6. Erit ergo

$$rr + 1 = \frac{(mm+nn)(tt+1)^2}{(n(tt-1)+2mt)^2} \quad \text{et} \quad ABC = \frac{(mm+nn)(tt+1)}{n(tt-1)+2mt},$$

unde ob $BC = rr + 1$ reperitur:

$$A = \frac{n(tt-1)+2mt}{tt+1},$$

et ob $mm + nn = (pp+1)(qq+1)$:

$$B = \frac{(pp+1)(tt+1)}{n(tt-1)+2mt} \quad \text{et} \quad C = \frac{(qq+1)(tt+1)}{n(tt-1)+2mt},$$

existente $m = pq \pm 1$ et $n = p \mp q$.

7. En ergo solutionem maxime generalem nostri problematis, in qua adeo binos numeros p et q pro lubitu accipere licet, ita ut binae formulae $AB - 1$ et $AC - 1$ datis quadratis aequentur; et cum littera t etiamnunc arbitrio nostro permittatur, pro tertia formula $BC - 1$ infinita quadrata reperiri possunt, unde hoc problema sine ullo dubio ad primam partem, ubi solutiones generales exhibere licet, erit referendum. Verum cum hoc modo terni numeri quaesiti plerumque prodeant fracti, si solutiones in integris desiderentur, alia artificia in hunc finem adhiberi conveniet, quae hic exposuisse iuvabit.

SOLUTIO PROBLEMATIS PER NUMEROS INTEGROS

8. Quoniam numeros p et q ut datos spectamus, solutio ita facilius obtinetur. Posito $AB = 1 + pp$ et $AC = qq + 1$, ut sit

$$B = \frac{pp+1}{A} \quad \text{et} \quad C = \frac{qq+1}{A},$$

erit statim:

$$BC - 1 = \frac{(pp+1)(qq+1)}{AA} - 1 = \frac{mm+nn-AA}{AA},$$

quae forma cum esse debeat quadratum, sumatur $A = n = p - q$ seu $p = q + A$, fietque

$$B = A + 2q + \frac{qq+1}{A} \quad \text{et} \quad C = \frac{qq+1}{A},$$

unde numeros A et q ita accipi conveniet, ut A sit divisor ipsius $qq + 1$. Quare necesse est pro A capi summam duorum quadratorum, ac tum semper pro q infinitos valores assignari licebit, ut $qq + 1$ divisionem per A admittat, veluti ex sequentibus exemplis patebit:

1°. Sit $A = 1$ et $q = u$, erunt tres numeri quaesiti:

$$A = 1, \quad B = uu + 2u + 2 \quad \text{et} \quad C = uu + 1.$$

2°. Sit $A = 2$, sumique oportet $q = 2u - 1$, unde prodeunt numeri quaesiti:

$$A = 2, \quad B = 2uu + 2u + 1, \quad C = 2uu - 2u + 1.$$

3°. Sit $A = 5$, sumique oportet $q = 5u \pm 2$, unde duae resultant solutiones:

$$A = 5, \quad B = 5uu + 14u + 10, \quad C = 5uu + 4u + 1,$$
$$A = 5, \quad B = 5uu + 6u + 2, \quad C = 5uu - 4u + 1.$$

Sicque binis A et C duplex valor ipsius B respondet, scilicet

$$A = 5, \quad C = 5uu + 4u + 1, \quad B = 5uu + 14u + 10 \text{ vel } B = 5uu - 6u + 2.$$

4°. Sit $A = ff + gg$ et k minimus numerus, cuius quadratum unitate auctum per A sit divisibile, ut sit $\frac{kk+1}{ff+gg} = h$. Iam ponatur $q = (ff+gg)u + k$, eruntque tres numeri quaesiti

$$A = ff + gg, \quad C = (ff + gg)uu + 2ku + h$$

et

$$B = (ff + gg)uu + 2(ff + gg + k)u + ff + gg + 2k + h,$$

ubi observo, si ambo numeri k et u capiantur negative, ut valor ipsius C maneat idem, tum pro B alium insuper prodire valorem

$$B = (ff + gg)\,uu - 2\,(ff + gg - k)\,u + ff + gg - 2k + h\,.$$

9. Alio autem modo prorsus singulari solutiones in integris facile inveniri possunt, qui ita procedit. Capiantur binae fractiones $\frac{a}{b}$ et $\frac{c}{d}$ tam parum a se invicem discrepantes, ut sit $ad - bc = \pm 1$; inde formetur tertia $\frac{c \pm a}{d \pm b}$, quae ad utramque priorum simili modo erit comparata. Quo facto tres numeri quaesiti ita se habebunt:

$$A = aa + bb, \quad B = cc + dd, \quad C = (c \pm a)^2 + (d \pm b)^2\,,$$

namque ob $ad - bc = \pm 1$ erit:

$$\begin{aligned} AB &= (ac + bd)^2 + 1, \\ AC &= (ac \pm aa + bd \pm bb)^2 + 1, \\ BC &= (cc \pm ac + dd \pm bd)^2 + 1. \end{aligned}$$

10. Hinc simpliciores solutiones obtinentur sequentes:

$\frac{a}{b}$,	$\frac{c}{d}$,	$\frac{a \pm c}{b \pm d}$	A	B	C
$\frac{0}{1}$,	$\frac{1}{f}$,	$\frac{1}{f+1}$	1	$ff + 1$	$ff + 2f + 2$
$\frac{1}{1}$,	$\frac{f-1}{f}$,	$\frac{f}{f+1}$	2	$2ff - 2f + 1$	$2ff + 2f + 1$
$\frac{1}{2}$,	$\frac{f}{2f-1}$,	$\frac{f+1}{2f+1}$	5	$5ff - 4f + 1$	$5ff + 6f + 2$
$\frac{1}{2}$,	$\frac{f}{2f-1}$,	$\frac{f-1}{2f-3}$	5	$5ff - 4f + 1$	$5ff - 14f + 10$
$\frac{1}{3}$,	$\frac{f}{3f-1}$,	$\frac{f+1}{3f+2}$	10	$10ff - 6f + 1$	$10ff + 14f + 5$
$\frac{1}{3}$,	$\frac{f}{3f-1}$,	$\frac{f-1}{3f-4}$	10	$10ff - 6f + 1$	$10ff - 26f + 17$

Unde patet has solutiones convenire cum praecedentibus.

11. Datis autem duobus numeris A et B, ut sit $AB - 1 = \square = pp$, tertius C infinitis modis inveniri potest sequenti modo: Cum tam $AC - 1$ quam $BC - 1$ quadratum esse debeat, statuatur primo productum $ABCC - (A + B)C + 1 = (mC + 1)^2$, unde reperitur

$$C = \frac{A + B + 2m}{AB - mm},$$

unde fit

$$AC - 1 = \frac{(A + m)^2}{AB - mm} \quad \text{et} \quad BC - 1 = \frac{(B + m)^2}{AB - mm}.$$

Tantum ergo superest, ut $AB - mm = pp + 1 - mm$ reddatur quadratum, puta $= nn$, seu ut sit $mm + nn = pp + 1$. Hunc in finem sumantur duae fractiones a et α, ut sit $aa + \alpha\alpha = 1$, fiatque $[\pm]\, m = ap + \alpha$ et $n = \alpha p - a$, ex quo habebitur

$$C = \frac{A + B \pm 2(ap + \alpha)}{(\alpha p - a)^2},$$

ubi sumtis pro lubitu duobus numeris f et g, capi oportet

$$a = \frac{ff - gg}{ff + gg} \quad \text{et} \quad \alpha = \frac{2fg}{ff + gg}.$$

12. Hinc adeo plures valores pro C in integris inveniri possunt; sumto enim $f = 1$ et $g = 0$, prodit

$$C = A + B \pm 2p.$$

Deinde posito $f = 2p$ et $g = 1$, prodit

$$C = (A + B)(4pp + 1)^2 \pm 2p(4pp + 1)(4pp + 3).$$

Tum vero etiam sumendo $f = 4pp + 1$ et $g = 2p$ fit

$$C = (A + B)(16p^4 + 12pp + 1)^2 \pm 2p(16p^4 + 12pp + 1)(16p^4 + 20pp + 5).$$

Porro positio $f = 8p^3 + 4p$ et $g = 4pp + 1$ dat quoque duos novos valores integros. Ex quo intelligere licet in genere formam tertii numeri C fore

$$C = (A + B)M^2 \pm 2pMN,$$

ubi quantitates M et N has series recurrentes constituunt:

$M = 1, \quad 4pp + 1, \quad 16p^4 + 12pp + 1, \quad 64p^6 + 80p^4 + 24pp + 1$ etc.,
$N = 1, \quad 4pp + 3, \quad 16p^4 + 20pp + 5, \quad 64p^6 + 112p^4 + 56pp + 7$ etc.,

quarum utriusque scala relationis est $4pp + 2, -1$[1]), ita ut in genere sit

$$M = \frac{(\sqrt{(1+pp)} + p)^{2\lambda+1} + (\sqrt{(1+pp)} - p)^{2\lambda+1}}{2\sqrt{(1+pp)}}$$

et

$$N = \frac{(\sqrt{(1+pp)} + p)^{2\lambda+1} - (\sqrt{(1+pp)} - p)^{2\lambda+1}}{2p} .$$

Vel posito $2p = q$ et denotante $n[= 2\lambda]$ numerum parem quemcunque erit:

$$M = q^n + \frac{(n-1)}{1} q^{n-2} + \frac{(n-2)\ (n-3)}{1\cdot 2} q^{n-4} + \frac{(n-3)\ (n-4)\ (n-5)}{1\cdot 2\cdot 3} q^{n-6} + \text{etc.},$$

$$N = q^n + \frac{(n+1)}{1} q^{n-2} + \frac{(n+1)\ (n-2)}{1\cdot 2} q^{n-4} + \frac{(n+1)\ (n-3)\ (n-4)}{1\cdot 2\cdot 3} q^{n-6} + \text{etc.}$$

PROBLEMA 2

Invenire quatuor numeros, ut binorum productum una cum summa eorundem binorum faciat quadratum; seu, quod eodem redit, invenire quatuor numeros A, B, C, D, ut binorum producta unitate minuta sint quadrata, sicque hae sex formulae

$$AB - 1, \quad AC - 1, \quad AD - 1, \quad BC - 1, \quad BD - 1, \quad CD - 1$$

fiant quadrata.

13. Pro solutione huius problematis spectemus duos numeros A et B tamquam datos, ut sit $AB - 1 = pp$ seu $AB = pp + 1$; ac sumto $aa + \alpha\alpha = 1$ statuatur tertius numerus $C = \frac{A + B + 2(ap + \alpha)}{(\alpha p - a)^2}$. Simili modo sumto $bb + \beta\beta = 1$ ponatur quartus numerus $D = \frac{A + B + 2(bp + \beta)}{(\beta p - b)^2}$; sicque iam erit satisfactum his conditionibus

$$AB - 1 = \square, \quad AC - 1 = \square, \quad BC - 1 = \square, \quad AD - 1 = \square, \quad BD - 1 = \square,$$

1) Id est: $M_\lambda = (4pp + 2)\ M_{\lambda-1} - M_{\lambda-2}$, $N_\lambda = (4pp + 2)\ N_{\lambda-1} - N_{\lambda-2}$. R. F.

ita ut tantum restet sexta conditio implenda, qua esse debet $CD - 1 = \square$, quae propterea dat

$$(A + B)^2 + 2(A + B)((a + b)p + \alpha + \beta) + 4(ap + \alpha)(bp + \beta) - (\alpha p - a)^2(\beta p - b)^2 = \square ,$$

cui ita satisfieri oportet, ut simul fiat $AB = pp + 1$.

14. Praeter a, α, b, β spectetur etiam p ut datum, et cum sit

$$B = \frac{pp + 1}{A} \quad \text{et} \quad A + B = \frac{AA + pp + 1}{A} ,$$

quadratum effici debebit haec forma:

$$\begin{aligned} &A^4 + 2A^3(a + b)p + 2AA(pp + 1) + 2A(pp + 1)(a + b)p + (pp + 1)^2 , \\ &+ 2A^3(\alpha + \beta) + 4AA(ap + \alpha)(bp + \beta) + 2A(pp + 1)(\alpha + \beta) \\ &- AA(\alpha p - a)^2(\beta p - b)^2 \end{aligned}$$

cuius radix statuatur

$$AA + A((a + b)p + \alpha + \beta) - pp - 1 ,$$

unde nascetur haec aequatio:

$$\begin{aligned} &AA\big(((a + b)p + \alpha + p))^2 - 4(pp + 1) - 4(ap + \alpha)(bp + \beta) + \\ &+ (\alpha p - a)^2(\beta p - b)^2\big) = 4A(pp + 1)((a + b)p + \alpha + \beta) , \end{aligned}$$

ex qua elicitur

$$A = \frac{4(pp + 1)((a + b)p + \alpha + \beta)}{((a + b)p + \alpha + \beta)^2 - 4(pp + 1) - 4(ap + \alpha)(bp + \beta) + (\alpha p - a)^2(\beta p - b)^2} .$$

15. Quamquam haec solutio neutiquam est generalis, siquidem ex formula quarti ordinis est derivata, tamen, quoniam numeros a, α, b, β cum p pro arbitrio assumere licet, dum sit $aa + \alpha\alpha = 1$ et $bb + \beta\beta = 1$, innumerabiles suppeditat solutiones, circa quas nil aliud desiderari videtur, nisi quod numeri prodeant non solum fracti sed etiam praemagni ac subinde etiam negativi. Simpliciores autem solutiones ex casu, quo $\alpha = 0$, $\beta = 0$ et $a = 1$, $b = -1$, obtinebuntur, ubi fit $C = A + B + 2p$ et $D = A + B - 2p$ existente $AB = pp + 1$; tum igitur erit

$$CD - 1 = (A + B)^2 - 4pp - 1 = \square .$$

Quare, si statuatur $(A+B)^2 = qq + 4pp + 1$, erit $(A-B)^2 = qq - 3$, ex quo fiat $A - B = q - r$, ut prodeat

$$q = \frac{rr+3}{2r} \quad \text{et} \quad A - B = \frac{3-rr}{2r} .$$

Iam invento q sit $A + B = 2p + s$, fietque

$$p = \frac{qq+1-ss}{4s} \quad \text{et} \quad A + B = \frac{qq+1+ss}{2s} .$$

Si hic capiatur $r = 1$, [ut sit $q = 2$], erunt numeri quaesiti

$$A = \frac{ss+2s+5}{4s} , \quad B = \frac{ss-2s+5}{4s} , \quad C = \frac{5}{s} , \quad D = s .$$

Posito $r = 2$, ut sit $q = \frac{7}{4}$, habebuntur

$$A = \frac{16ss+8s+65}{64s} , \quad B = \frac{16ss-8s+65}{64s} \text{ [1]} , \quad C = \frac{65}{16s} , \quad D = s ,$$

qui fient omnes unitate maiores sumto $s = \frac{7}{2}$:

$$A = \frac{289}{224} , \quad B = \frac{233}{224} , \quad C = \frac{65}{56} , \quad D = \frac{7}{2} ,$$

et sumto $s = \frac{15}{4}$:

$$A = \frac{4}{3} , \quad B = \frac{13}{12} , \quad C = \frac{13}{12} , \quad D = \frac{15}{4} .$$

16. Praeterea etiam solutio particularis notari meretur, qua sumtis $b = -a$ et $\beta = -\alpha$ fit

$$C = \frac{A+B+2(ap+\alpha)}{(\alpha p - a)^2} \quad \text{et} \quad D = \frac{A+B-2(ap+\alpha)}{(\alpha p - a)^2} ,$$

et ob

$$B = \frac{pp+1}{A}$$

prodit haec aequatio

$$\begin{aligned} A^4 &+ 2AA(pp+1) + (pp+1)^2 = \square , \\ &- 4AA(ap+\alpha)^2 \\ &- AA(\alpha p - a)^4 \end{aligned}$$

1) Valores A et B permutati sunt. R. F.

qua reducta ad hanc formam

$$(AA - pp - 1)^2 + AA\,(\alpha p - a)^2\,(4 - (\alpha p - a)^2) = \square$$

evidens est hoc fieri sumendo $\alpha p - a = 2$ seu $p = \frac{2+a}{\alpha}$, hincque

$$B = \frac{pp+1}{A}\left[= \frac{5+4a}{\alpha\alpha A}\right], \quad C = \frac{A + B + \frac{2(2a+1)}{\alpha}}{4} = \frac{\alpha(A+B) + 4a + 2}{4\alpha}$$

et

$$D = \frac{\alpha(A+B) - 4a - 2}{4\alpha},$$

ubi adeo A pro lubitu accipi potest.

17. Si hic ponamus $a = \frac{ff-gg}{ff+gg}$ et $\alpha = \frac{2fg}{ff+gg}$ et pro m et n sumamus numeros quoscunque, quatuor numeri quaesiti prodibunt sequenti modo expressi:

$$A = \frac{m(ff+gg)}{2nfg}, \qquad B = \frac{n(9ff+gg)}{2mfg},$$

$$C = \frac{(m+3n)^2 ff + (m-n)^2 gg}{8mnfg}, \quad D = \frac{(m-3n)^2 ff + (m+n)^2 gg}{8mnfg},$$

quae solutio, etsi est particularis, tamen satis late patet, ob quatuor numeros f, g, m, n arbitrio nostro relictos. Sit, exempli gratia, $f = 1$, $g = 2$, et $m = 5$, $n = 6$, erunt numeri satisfacientes

$$A = \frac{25}{24}, \quad B = \frac{39}{10}, \quad C = \frac{533}{480}, \quad D = \frac{653}{480},$$

unde fit

$$AB - 1 = \left(\frac{7}{4}\right)^2, \quad AC - 1 = \left(\frac{19}{48}\right)^2, \quad AD - 1 = \left(\frac{31}{48}\right)^2,$$

$$BC - 1 = \left(\frac{73}{40}\right)^2, \quad BD - 1 = \left(\frac{83}{40}\right)^2, \quad CD - 1 = \left(\frac{343}{480}\right)^2.$$

Cum autem hae solutiones omnes in numeris fractis consistant praeter simplicissimam, quae est

$$A = 1, \quad B = 2, \quad C = 5, \quad D = 1,$$

quaestio oritur satis curiosa, num praeterea non aliae solutiones in numeris integris reperiri queant.

PROBLEMA 3

Invenire quatuor numeros, ut binorum productum dato numero n auctum sit numerus quadratus.

18. Sint A, B, C, D quatuor numeri quaesiti, et cum $AB + n$ esse debeat quadratum, ponatur $A = naa - bb$ et $B = ncc - dd$, ut fiat

$$AB = (nac - bd)^2 - n(ad - bc)^2;$$

quare, dum sit $ad - bc = \pm 1$, haec conditio adimpletur. Quare eiusmodi fractiones $\frac{a}{b}$ et $\frac{c}{d}$ investigari oportet, ut sit $ad - bc = \pm 1$, quod cum facile praestetur, idem eveniet in fractionibus $\frac{a+c}{b+d}$ et $\frac{a-c}{b-d}$, cum utraque illarum coniunctis. Statuamus ergo

$$\begin{aligned} A &= naa - bb, & B &= ncc - dd, \\ C &= n(a+c)^2 - (b+d)^2, & D &= n(a-c)^2 - (b-d)^2, \end{aligned}$$

nihilque aliud superest, nisi ut $CD + n$ reddatur quadratum, hoc est

$$\begin{aligned} nn(aa - cc)^2 - 2n(ab - cd)^2 + (bb - dd)^2 &= \square, \\ - 2n(ad - bc)^2 & \\ + \ n & \end{aligned}$$

seu ob $(ad - bc)^2 = 1$,

$$\begin{aligned} nn(aa - cc)^2 - 2n(ab - cd)^2 + (bb - dd)^2 &= \square, \\ - \ n & \end{aligned}$$

quae autem aequatio tantum solutionem particularem continet.

19. Solutionem autem generalem ut supra impetrabimus ponendo $AB = pp - n$; tum, quia pro C esse debet tam $AC + n = \square$ quam $BC + n = \square$, ponatur productum

$$nn + n(A + B)C + ABCC = nn + 2nCx + CCxx,$$

fiet

$$C = \frac{n(A + B - 2x)}{xx - AB} \quad \text{et} \quad AC + n = \frac{n(A - x)^2}{xx - AB},$$

unde patet $\frac{xx - AB}{n}$ quadratum esse debere. Statuatur ergo

$$xx - AB = xx - pp + n = nyy \quad \text{seu} \quad xx - nyy = pp - n.$$

Simili modo ponamus $vv - nzz = pp - n$, ut obtineamus

$$C = \frac{A + B - 2x}{yy} \quad \text{et} \quad D = \frac{A + B - 2v}{zz},$$

ac superest, ut reddatur quadratum

$$(A + B)^2 - 2(x + v)(A + B) + nyyzz + 4xv.$$

At ob $B = \frac{pp - n}{A}$ et $A + B = \frac{AA + pp - n}{A}$ habebitur

$$\begin{aligned} A^4 - 2A^3(x + v) + 2AA(pp - n) - 2A(pp - n)(x + v) + (pp - n)^2 \\ + nAAyyzz \\ + 4AAxv \end{aligned}$$

quadrato aequandum. Statuatur radix $AA - A(x + v) - (pp - n)$, eritque

$$AA(x+v)^2 - 4AA(pp-n) - nAAyyzz - 4AAxv + 4A(x+v)(pp-n) = 0,$$

$$\text{seu} \quad A = \frac{4(x+v)(pp-n)}{nyyzz+4(pp-n)-(x+v)^2+4xv},$$

$$\text{seu} \quad A = \frac{4(x+v)(pp-n)}{n(yy-1)(zz-1)+2xv+2pp-3n},$$

$$\text{seu} \quad A = \frac{4(x+v)(pp-n)}{nyyzz-2n(yy+zz)+(v+x)^2}.$$

20. Solutio particularis satis concinna hinc obtinetur ut supra sumendo $v = -x$, ut fiat $z = y$ atque

$$C = \frac{A+B-2x}{yy} \text{ et } D = \frac{A+B+2x}{yy},$$

existente $AB = pp - n = xx - nyy$; cum enim quadratum esse debeat haec forma:

$$A^4 + 2AA(pp - n) + nAAy^4 - 4AAxx + (pp - n)^2$$

seu

$$(AA - pp + n)^2 + nAAyy(yy - 4),$$

evidens est hoc fieri sumto $y = 2$, ut sit $pp = xx - 3n$. Ponatur $p = x - t$, fiet

$$x = \frac{3n + tt}{2t} \text{ et } p = \frac{3n - tt}{2t} \text{ seu } p = \frac{3nuu - tt}{2tu} \text{ et } x = \frac{3nuu + tt}{2tu},$$

hinc

$$AB = \frac{(nuu - tt)(9nuu - tt)}{4ttuu}.$$

Quocirca habebimus

$$A = \frac{f(nuu - tt)}{2gtu}, \qquad B = \frac{g(9nuu - tt)}{2ftu},$$

$$C = \frac{n(f + 3g)^2 uu - (f - g)^2 tt}{8fgtu}, \quad D = \frac{n(f - 3g)^2 uu - (f + g)^2 tt}{8fgtu}^{1}).$$

Circa hanc solutionem notari convenit esse $C + D = \frac{A + B}{2}$.

PROBLEMA 4

Invenire quatuor numeros, ut binorum producta singula summa numerorum aucta fiant numeri quadrati.

21. Inventis per problema praecedens quatuor numeris A, B, C, D, quorum binorum producta dato numero n aucta fiunt quadrata, statuantur numeri quatuor quaesiti mA, mB, mC, mD, et cum sit $mm(AB + n)$ quadratum seu $mmAB + mmn = \square$, efficiendum erit tantum, ut numerus mmn aequalis fiat summae horum quatuor numerorum $m(A + B + C + D)$, unde statim reperitur multiplicator quaesitus

$$m = \frac{A + B + C + D}{n}.$$

Quodsi ergo numeri A, B, C, D ex paragrapho praecedente accipiantur, ob $C + D = \frac{A + B}{2}$ habebitur

$$m = \frac{3(A + B)}{2n} = \frac{3n(ff + 9gg)uu - 3(ff + gg)tt}{4nfgtu}.$$

Hic igitur non solum quatuor litterae f, g et t, u, sed etiam numerus n pro lubitu accipi possunt, ita ut haec solutio latissime pateat, etiamsi non sit generalis.

1) Valores C et D permutati sunt. R. F.

22. Quoniam autem hic numerus n arbitrio nostro relinquitur, ex aequatione paragraphi praecedentis $pp = xx - 3n$ statim sumamus

$$n = \frac{xx - pp}{3}, \text{ ut sit } AB = \frac{4pp - xx}{3};$$

hinc ponamus

$$A = \frac{f(2p + x)}{3g} \quad \text{et} \quad B = \frac{g(2p - x)}{f},$$

erit

$$A + B = \frac{2(ff + 3gg)p + (ff - 3gg)x}{3fg},$$

hinc

$$C = \frac{2(ff + 3gg)p + (ff - 6fg - 3gg)x}{12fg}, \quad D = \frac{2(ff + 3gg)p + (ff + 6fg - 3gg)x}{12fg}.$$

Nunc igitur ob

$$A + B + C + D = \frac{2(ff + 3gg)p + (ff - 3gg)x}{2fg},$$

erit multiplicator communis

$$m = \frac{6(ff + 3gg)p + 3(ff - 3gg)x}{2fg(xx - pp)}.$$

23. Possunt hic adeo bini numeri A et B pro lubitu assumi, unde fit

$$2p + x = \frac{3Ag}{f} \quad \text{et} \quad 2p - x = \frac{Bf}{g},$$

hinc

$$p = \frac{3Agg + Bff}{4fg} \quad \text{et} \quad x = \frac{3Agg - Bff}{2fg},$$

atque

$$n = \frac{(9Agg - Bff)(Agg - Bff)}{16ffgg};$$

tum vero

$$C = \frac{A + B}{4} + \frac{3Agg - Bff}{4fg}, \quad D = \frac{A + B}{4} - \frac{3Agg - Bff}{4fg},$$ [1])

ac denique multiplicator $m = \frac{3(A + B)}{2n}$. Si hic ad fractiones tollendas ponamus $A = 4afg$ et $B = 4bfg$, erit

1) Valores C et D permutati sunt. R. F.

$$C = (a+b)ff + 3agg - bff \text{ et } D = (a+b)ff - 3agg + bff,$$

atque $n = (9agg - bff)(agg - bff)$, tum vero

$$m = \frac{6(a+b)ff}{(9agg - bff)(agg - bff)}.$$

24. Si sumamus $f = 1$ et $g = 1$, erit $A = 4a$, $B = 4b$, $C = 4a$, $D = 2b - 2a$ et multiplicator

$$m = \frac{6(a+b)}{(9a-b)(a-b)} = \frac{6(a+b)}{(b-a)(b-9a)},$$

qui ut fiat positivus, capi debet $b > 9a$; sit ergo

1°. $a = 1$, $b = 10$, erit $A = 4$, $B = 40$, $C = 4$, $D = 18$ et $m = \frac{6 \cdot 11}{9 \cdot 1} = \frac{22}{3}$;

2°. $a = 1$, $b = 11$, erit $A = 4$, $B = 44$, $C = 4$, $D = 20$ et $m = \frac{6 \cdot 12}{10 \cdot 2} = \frac{18}{5}$;

3°. $a = 1$, $b = 13$, erit $A = 4$, $B = 52$, $C = 4$, $D = 24$ et $m = \frac{6 \cdot 14}{12 \cdot 4} = \frac{7}{4}$,

unde quatuor numeri quaesiti erunt integri

$$mA = 7, \quad mB = 91, \quad mC = 7, \quad mD = 42,$$

quorum summa est = 147.

Hic autem desiderari potest, quod duo quaesitorum numerorum sint aequales, quod etiam evenit sumendo $f = 3g$. [1])

25. Ut igitur numeros inaequales nanciscamur, sumamus $f = 2$ et $g = 1$, fietque

$$A = 8a, \; B = 8b, \; C = 5a - 2b, \; D = 6b - a$$

et

$$m = \frac{12(a+b)}{(9a-4b)(a-4b)} = \frac{12(a+b)}{(4b-9a)(4b-a)},$$

1) Hoc casu evenit $B = D$. R. F.

unde casus simpliciores erunt

1°. $a=5$, $b=1$, hinc $A=40$, $B=8$, $C=23$, $D=1$ et $m=\frac{72}{41}$;

2°. $a=11$, $b=2$, hinc $A=88$ [1]), $B=16$, $C=51$, $D=1$ et $m=\frac{12\cdot 13}{91\cdot 3}=\frac{4}{7}$;

3°. $a=3$, $b=7$, hinc $A=24$, $B=56$, $C=1$, $D=39$ et $m=\frac{12\cdot 10}{1\cdot 25}=\frac{24}{5}$.

Ponamus etiam $f=3$ et $g=2$, ut consequamur

$$A=24a,\quad B=24b,\quad C=18a-3b,\quad D=15b-6a$$

et

$$m=\frac{36(a+b)}{9(4a-b)\ (4a-9b)}=\frac{4(a+b)}{(4a-b)\ (4a-9b)},$$

sicque patet hinc praecedentem solutionem enasci.

26. Verum solutio adeo in integris prodit ponendo $f=5$ et $g=1$, unde fit

$A=20a$, $B=20b$, $C=8a-20b$, $D=2a+30b$ et $m=\frac{30(a+b)}{(25b-9a)\ (25b-a)}$.

Sumatur iam $a=19$, $b=7$ fietque:

$$A=380,\quad B=140,\quad C=12,\quad D=248 \text{ et } m=\frac{30\cdot 26}{4\cdot 156}=\frac{5}{4}.$$

Quare quatuor numeri quaesiti erunt

I. 475, II. 175, III. 15, IV. 310,

quorum summa est $975=25\cdot 39$. Alii numeri integri sunt[2])

I. 504, II. 96, III. 36, IV. 264,

quorum summa est $=900$.

27. Hinc etiam solvi potest hoc problema:

quo quaeruntur quatuor numeri eiusmodi, ut binorum producta summa omnium minuta fiant numeri quadrati.

1) Manuscriptum: 44. R. F.

2) pro $f=7$, $g=1$, $a=21$, $b=4$, $m=\frac{6}{7}$. R. F.

Solutio enim ex praecedente facile deducitur, dum pro multiplicatore m numerus capitur negativus. Unde in numeris integris sequens solutio obtinetur:

I. 80, II. 24, III. 8, IV. 44,

quorum summa est 156, quibusque hoc modo quaestioni satisfit:

$$80 \cdot 24 - 156 = 1764 = 42^2, \quad 80 \cdot 8 - 156 = 484 = 22^2,$$
$$80 \cdot 44 - 156 = 3364 = 58^2, \quad 24 \cdot 8 - 156 = 36 = 6^2,$$
$$24 \cdot 44 - 156 = 900 = 30^2, \quad 8 \cdot 44 - 156 = 196 = 14^2.$$

APPENDIX

28. Adiungam hic problema prorsus singulare, olim mihi propositum,[1]) quod vires Analyseos DIOPHANTEAE omnino transcendere videtur, quandoquidem solutio ad formulam sexti gradus quadrato aequandam perducit, dum adhuc operationes istius Analyseos non ultra quartum gradum sunt promotae. Problema autem hoc, cuius tandem unam solutionem sum adeptus, ita se habet:

Invenire duos numeros, quorum productum ita sit comparatum, ut, sive addatur sive subtrahatur tam summa quam differentia eorum, semper prodeant numeri quadrati.

Positis ergo numeris quaesitis $\frac{x}{n}$ et $\frac{y}{n}$ requiritur, ut sit

$$\text{tam } xy \pm n(x+y) = \square \quad \text{quam } xy \pm n(x-y) = \square .$$

Cum nunc sit $AA + BB \pm 2AB$ quadratum, capiatur xy ita, ut duplici modo in duo quadrata resolvi possit. Hunc in finem posito

$$xy = (pp + qq)(rr + ss)$$

erit duplici modo

vel $A = pr + qs$ et $B = ps - qr$, vel $A = ps + qr$ et $B = pr - qs$;

quare statuatur:

$n(x+y) = 2(pr+qs)(ps-qr)$ et $n(x-y) = 2(ps+qr)(pr-qs)$,

ut fiat

1) Vide Commentationem 405 indicis ENESTROEMIANI, *LEONHARDI EULERI Opera omnia*, vol. 3 seriei I, p. 148. R. F.

$$\sqrt{(xy + n(x+y))} = pr + qs + ps - qr\,,$$
$$\sqrt{(xy - n(x+y))} = pr + qs - ps + qr\,,$$
$$\sqrt{(xy + n(x-y))} = ps + qr + pr - qs\,,$$
$$\sqrt{(xy - n(x-y))} = ps + qr - pr + qs\,.$$

29. Iam factae positiones praebent

$$\frac{x+y}{x-y} = \frac{(pr+qs)\,(ps-qr)}{(ps+qr)\,(pr-qs)} = \frac{pprs + pqss - pqrr - qqrs}{pprs - pqss + pqrr - qqrs}\,,$$

unde fit

$$\frac{x}{y} = \frac{rs(pp-qq)}{pq(ss-rr)}\,.$$

Ponamus ergo

$$x = mrs\,(pp - qq) \text{ et } y = mpq\,(ss - rr),$$

eritque

$$x + y = m\,(pr + qs)\,(ps - qr)\,,$$

ideoque $n = \frac{2}{m}$, ut numeri quaesiti fiant

$$\frac{x}{n} = \frac{1}{2}\,mmrs\,(pp - qq) \quad \text{et} \quad \frac{y}{n} = \frac{1}{2}\,mmpq(ss - rr)\,.$$

Nunc ob $xy = (pp + qq)\,(rr + ss)$ habebimus hanc aequationem resolvendam

$$mmpqrs\,(pp - qq)\,(ss - rr) = (pp + qq)\,(rr + ss)\,,$$

quae utique ita est comparata, ut per nulla artificia adhuc cognita confici possit.

30. Facile autem perspicitur id effici oportere, ut haec fractio quadratum evadat:

$$\frac{pq(pp-qq)\;(pp+qq)}{rs(ss-rr)\;(rr+ss)} = \square\,,$$

tum igitur ob

$$mm = \frac{(pp+qq)\;(rr+ss)}{pqrs(pp-qq)\;(ss-rr)}$$

erit

$$\frac{x}{n} = \frac{(pp+qq)\;(rr+ss)}{2pq(ss-rr)} \quad \text{et} \quad \frac{y}{n} = \frac{(pp+qq)\;(rr+ss)}{2rs(pp-qq)}\,,$$

dummodo formulae $pq\,(pp - qq)\,(pp + qq)$ et $rs\,(ss - rr)\,(rr + ss)$ rationem quadratam inter se teneant[1]).

1) Confer Commentationem 774 indicis ENESTROEMIANI, Mémoires de l'acad. des sc. de St-Pétersbourg, 11, 1830, p. 31, huius voluminis p. 116, ubi problema resolutum est. R. F.

31[1]). Ad hoc praestandum alia non patere videtur via, nisi ut simplicioribus numeris pro A et B assumendis, huius formulae

$$AB(AA - BB)(AA + BB)$$

plures valores evolvantur, donec duo occurrant rationem quadratam inter se tenentes. Hoc modo reperi istam conditionem impleri sumendo $p = 12$, $q = 1$, $s = 16$ et $r = 11$, unde fit

$$pq(pp - qq)(pp + qq) = 4 \cdot 3 \cdot 5 \cdot 11 \cdot 13 \cdot 29 \quad \text{et}$$
$$rs(ss - rr)(rr + ss) = 144 \cdot 3 \cdot 5 \cdot 11 \cdot 13 \cdot 29 .$$

Quamobrem ambo numeri quaesiti sunt:

$$\frac{x}{n} = \frac{5 \cdot 13 \cdot 29 \cdot 29}{8 \cdot 3 \cdot 5 \cdot 27} = \frac{13 \cdot 841}{8 \cdot 81} = A , \qquad \frac{y}{n} = \frac{5 \cdot 13 \cdot 29 \cdot 29}{32 \cdot 11 \cdot 11 \cdot 13} = \frac{5 \cdot 841}{32 \cdot 121} = B ,$$

qui duo numeri si dicantur A et B, fit

$$\sqrt{(AB + A + B)} = \frac{29 \cdot 329}{16 \cdot 9 \cdot 11}\left[= \frac{9541}{1584}\right], \quad \sqrt{(AB - A - B)} = \frac{29 \cdot 33}{16 \cdot 9 \cdot 11} = \frac{29}{48},$$

$$\sqrt{(AB + A - B)} = \frac{841 \cdot 11}{16 \cdot 9 \cdot 11} = \frac{841}{144} , \quad \sqrt{(AB - A + B)} = \frac{841 \cdot 3}{16 \cdot 9 \cdot 11} = \frac{841}{528} .[2])$$

---

1) Manuscriptum: 30. Correxit R. F.

2) Hanc solutionem EULERUS iam in Commentatione p. 300 laudata invenit. Vide vol. 3 seriei I p. 171, ubi bini termini permutati sunt. R. F.

RECHERCHES SUR LE PROBLEME DE TROIS NOMBRES CARRES TELS QUE LA SOMME DE DEUX [QUELCONQUES] MOINS LE TROISIEME FASSE UN NOMBRE CARRE

Commentatio 796 indicis ENESTROEMIANI
Prima editio: Commentationes arithmeticae 2, 1849, p. 603—616
Haec editio congruit cum manuscripto manu A. WILBRECHTI facto et academiae scientiarum Petropolitanae relicto[1])
Présenté à l'académie de St-Pétersbourg le 1er mars 1781

1. Soient x, y, z les racines des trois carrés cherchés, les équations seront

$$\begin{aligned} 1°.\quad & yy + zz - xx = pp\,, \\ 2°.\quad & xx + zz - yy = qq\,, \\ 3°.\quad & xx + yy - zz = rr\,. \end{aligned}$$

Si l'on ajoute ces équations deux à deux, elles produiront les équations suivantes:

$$\begin{aligned} pp + qq &= 2zz\,, \\ pp + rr &= 2yy\,, \\ qq + rr &= 2xx\,, \end{aligned}$$

d'où l'on voit qu'en résolvant notre problème, celui-ci sera aussi resolu:

1) Le manuscrit contient l'ensemble de quatre mémoires: de celui-ci et des trois mémoires publiés p. 330, 337 et 340 de ce tome. Son auteur l'a présenté à l'académie de St-Pétersbourg sous le titre général:

„Recherches sur deux problèmes de l'analyse de DIOPHANTE, savoir: trouver trois nombres carrés tels que la somme de deux moins le troisième fasse un nombre carré; et trouver quatre nombres inégaux et entiers tels que la somme de deux fasse toujours un carré.

Calculé sous la direction de Monsieur le Professeur LEONHARD EULER par ALEXANDRE WILBRECHT."

La dernière phrase est effacée par une main inconnue et remplacée par: *„par Monsieur LEONHARD EULER"*. Voire en outre les explications apportées dans la préface sur le manuscrit et la première édition de 1849. R. F.

Trouver trois nombres carrés dont la demi-somme de deux quelconques d'entre eux produise aussi un carré, puisque

$$\frac{pp+qq}{2} = zz\ , \quad \frac{pp+rr}{2} = yy \quad et \quad \frac{qq+rr}{2} = xx\ .$$

2. De plus il est évident qu'ayant trouvé les trois nombres x, y, z, tous leurs multiples satisferont pareillement, savoir: nx, ny, nz. De sorte que tous ces cas ne renferment qu'une seule solution, et par conséquent nous ne chercherons dans la suite que trois nombres tels, qu'ils n'aient aucun diviseur commun. D'où il est d'abord évident que tous les trois nombres cherchés ne seront pas pairs. Or, avec quelque attention, on verra de suite que ces trois nombres doivent être tous impairs; car tout carré pair est de la forme $4aa$ et tout carré impair de la forme $4(aa+a)+1$[1]); donc si nous supposons deux de nos carrés pairs, c'est-à-dire $xx = 4aa$, $y = 4bb$, et le troisième impair: $zz = 4(cc+c)+1$, il en résultera pour $xx+yy-zz$ cette expression $4(aa+bb-cc-c)-1$, qui ne saurait jamais être un carré. Si nous supposons ensuite deux seulement impairs et le troisième pair, comme

$$xx = 4(aa+a)+1, \quad y = 4(bb+b)+1, \quad z = 4cc,$$

nous aurons pour $xx+yy-zz$ cette expression $4(aa+a+bb+b-cc)+2$, qui ne saurait non plus être un carré. Mais posant tous les trois carrés impairs, par exemple

$$xx = 4(aa+a)+1, \quad yy = 4(bb+b)+1, \quad zz = 4(cc+c)+1,$$

nous aurons pour $xx+yy-zz$ la forme $4(aa+a+bb+b-cc-c)+1$, qui peut très bien représenter un carré.

3. Cette considération nous montre d'abord, que si l'on voulait chercher quatre nombres carrés tels, que la somme de trois moins le quatrième fasse un nombre carré, la recherche serait inutile, puisque la question est absolument impossible. Pour le prouver, on n'a qu'à parcourir tous les cas par rapport aux pairs et impairs. En effet,

1°. si trois carrés sont pairs, savoir:

$$xx = 4aa, \quad yy = 4bb, \quad z = 4cc \quad \text{et} \quad vv = 4(dd+d)+1\ ,$$

1) Manuscrit: $4aa+1$. La même erreur se trouve dans tous les carrés des nombres impairs des § 2 et 3. R. F.

on aura pour $xx + yy + zz - vv$ la valeur $4(aa+bb+cc-dd-d)-1$, qui ne peut jamais être un carré.

2°. Soient seulement deux pairs et deux impairs, ou bien

$$xx = 4aa, \quad yy = 4bb, \quad zz = 4(cc+c)+1, \quad v = 4(dd+d)+1,$$

on aura pour $xx - yy + zz + vv$ cette forme

$$4(aa - bb + cc + c + dd + d) + 2,$$

qui ne peut jamais être un carré.

3°. Supposons à présent seulement un seul carré pair, savoir

$$xx = 4aa, \; yy = 4(bb+b)+1, \; zz = 4(cc+c)+1, \quad vv = 4(dd+d)+1,$$

nous aurons pour $yy + zz + vv - xx$ la forme

$$4(bb + b + cc + c + dd + d - aa) + 3,$$

qui encore n'est jamais un nombre carré.

4°. Enfin soient tous les quatre nombres impairs, c'est-à-dire

$$xx = 4(aa+a)+1, \quad yy = 4(bb+b)+1, \quad zz = 4(cc+c)+1, \quad v = 4(dd+d)+1,$$

on aura pour $xx + yy + zz - vv$ la valeur

$$4(aa + a + bb + b + cc + c - dd - d) + 2^{1}),$$

qui ne peut nonplus représenter un nombre carré.

4. Après ces considérations, examinons de quelle manière on pourrait arriver à une solution du problème proposé. Pour cet effet je remarque que nos deux premières équations peuvent être représentées sous cette forme générale

$$zz \pm (yy - xx) = \text{à un carré quelconque.}$$

1) Manuscrit: 3. R. F.

Or $AA + BB \pm 2AB$ est toujours un carré parfait; donc, comparant cette formule avec la précédente, nous aurons $zz = AA + BB$, $yy - xx = 2AB$, et pour rendre $AA + BB$ un carré parfait il ne faut que supposer $A = aa - bb$, $B = 2ab$, et nous aurons pour $zz : (aa + bb)^2$; donc

$$z = aa + bb .$$

D'après ces suppositions la valeur de $yy - xx$ sera $4ab(aa - bb)$. Et si nous comparons ces deux produits ensembles, savoir

$$(y + x)(y - x) = 2ab \cdot (2aa - 2bb),$$

nous trouvons que $y + x = 2ab$ et $y - x = 2(aa - bb)$; par conséquent:

$$x = bb + ab - aa \quad \text{et} \quad y = aa + ab - bb .$$

Ainsi, en prenant pour les valeurs de x, y et z les expressions

$$bb + ab - aa, \quad aa + ab - bb \quad \text{et} \quad aa + bb ,$$

les deux premières équations seront satisfaites. Il ne s'agit donc que de satisfaire aussi à la troisième équation qui, par la substitution de ces valeurs de x, y, z, devient

$$xx + yy - zz = a^4 + b^4 - 4aabb = rr.$$

5. Tout revient donc à trouver pour a et b de tels nombres, que la formule $a^4 + b^4 - 4aabb$ devienne un carré. Or, comme cette formule ne renferme que les puissances pairs, elle ne saurait être résoluble à moins qu'un cas ne soit déjà connu. Il est facile de remarquer que cette condition sera remplie, si l'on prend $a = 2b$. Ainsi mettons $a = b(t + 2)$, et nous aurons

$$a^4 + b^4 - 4aabb = b^4 (t^4 + 8t^3 + 20tt + 16t + 1) .$$

Supposons que la racine de cette expression soit $b^2(tt + 8t + 1)$; alors le carré sera $b^4(t^4 + 16t^3 + 66tt + 16t + 1)$. En le comparant avec le carré précédent, on trouvera:

$$8t^3 + 46tt = 0 \quad \text{ou} \quad 8t + 46 = 0 ,$$

d'où l'on tirera $t = -\frac{23}{4}$; par conséquent $t + 2 = -\frac{15}{4}$ et $a = -\frac{15b}{4}$. Or,

puisqu'il est indifférent que les valeurs de a et b soient positives ou négatives, nous prendrons $a = 15$, $b = 4$, et nous aurons $x = 149$, $y = 269$, $z = 241$, qui paraissent être les plus petits nombres cherchés. De là, par conséquent, nous trouverons $p = 329$, $q = 89$, $r = 191$.

6. Comme cette solution est tirée de l'équation $yy - xx = 4ab(aa - bb)$ par la décomposition du second membre en ses facteurs $2ab$ et $2(aa - bb)$, il s'en suit qu'on pourrait exprimer généralement les valeurs de y et de x de cette manière:

$$y + x = \frac{2m}{n} ab \quad \text{et} \quad y - x = \frac{2n}{m} (aa - bb) .$$

Mais, après des calculs très pénibles, on ne parviendrait toujours qu'à des solutions très particulières. Cependant, la solution suivante mérite toute notre attention. Supposons $y + x = 2a(a + b)$ et $y - x = 2b(a - b)$; d'où nous tirons

$$yy + xx = 2(a^4 + 2a^3 b + 2aabb - 2ab^3 + b^4) .$$

De là, si l'on ôte zz, on obtiendra cette formule:

$$a^4 + 4a^3 b + 2aabb - 4ab^3 + b^4 = rr ,$$

qui est le carré complet de $aa + 2ab - bb$; donc les valeurs de a et b sont entièrement arbitraires. Mais si l'on considère les valeurs de x, y et z qui sont $aa + bb$, $aa + 2ab - bb$ et $aa + bb$, on trouvera que x et z sont égaux, et pour cette raison la solution ne saurait être admise.

7. On pourrait employer encore bien d'autres méthodes pour la solution du problème. Mais toutes ont ce grand défaut de ne donner que des solutions très particulières, et cela après des calculs très longs et très difficiles. C'est pourquoi j'exposerai ici une méthode tout-à-fait singulière, et qui, sans beaucoup de peine, fournira une infinité de formules générales pour les trois nombres x, y et z, lesquelles, à leur tour, donneront une infinité de solutions. Cependant, il s'en faut de beaucoup que toutes ces formules contiennent toutes les solutions possibles.

METHODE FACILE POUR TROUVER DES SOLUTIONS PLUS GENERALES [PREMIERE METHODE]

8. Si nous supposons que la somme des trois carrés cherchés soit

$$s = xx + yy + zz,$$

d'où il suit que la même somme s est aussi égale à $pp + qq + rr$, c'est-à-dire à la somme des trois carrés, qui expriment la différence des conditions requises, nos équations deviendront

$$\begin{aligned} 1^\circ.\quad & s - 2xx = pp, \quad \text{ou} \quad s = pp + 2xx, \\ 2^\circ.\quad & s - 2yy = qq, \quad \text{ou} \quad s = qq + 2yy, \\ 3^\circ.\quad & s - 2zz = rr, \quad \text{ou} \quad s = rr + 2zz, \end{aligned}$$

d'où l'on voit que s doit être, de trois manières différentes, la somme d'un carré et d'un double carré.

9. Considérons donc plus soigneusement les nombres contenus dans cette forme $aa + 2bb$. Je remarque premièrement que, lorsqu'un tel nombre est premier, il ne peut avoir cette forme que d'une seule manière; car s'il était résoluble de deux manières, de sorte que s fût égale à $aa + 2bb$ et aussi égale à $cc + 2dd$, il s'en suivrait que $aa - cc = 2dd - 2bb$ et par conséquent

$$\frac{a+c}{d+b} = \frac{2(d-b)}{a-c}.$$

Or puisque ces deux fractions sont égales, supposons qu'après avoir été réduites aux plus petits termes, elles soient $\frac{m}{n}$. De là nous aurons $\frac{a+c}{d+b} = \frac{m}{n}$, ou $a + c = mf$, $d + b = nf$; pareillement $\frac{2(d-b)}{a-c} = \frac{m}{n}$ et $d - b = mg$, $a - c = 2ng$, et par conséquent

$$2a = mf + 2ng, \quad 2b = nf - mg.$$

Mais puisque $4s = 4aa + 8bb$, en substituant au lieu de $2a$ et $2b$ leurs valeurs, nous aurons

$$4s = ff(mm + 2nn) + 2gg(mm + 2nn),$$

ou bien

$$4s = (ff + 2gg)(mm + 2nn),$$

ce qui ne peut avoir lieu, s étant un nombre premier. Il faut donc que s ait deux facteurs dont chacun est de la forme $aa + 2bb$.

10. Il suit de là que la somme s ne saurait être un nombre premier, et il est démontré qu'un nombre de la forme $aa + 2bb$ ne peut être divisible que par des nombres de la même forme, lorsque a et b sont premiers entre eux. Ainsi s est un produit de deux ou de plusieurs nombres premiers de la même forme $aa + 2bb$. Mais on verra bientôt que deux facteurs premiers ne suffisent pas pour produire une triple résolution; donc s doit avoir au moins trois facteurs premiers de la forme $aa + 2bb$. Encore dans ce cas s doit être de la même forme[1]).

11. Observons ici que tout nombre impair de la forme $aa + 2bb$ est toujours ou de la forme $8n + 1$ ou $8n + 3$, et que, lorsque le nombre est pair et de la forme $aa + 2bb$, il est le double de l'une ou de l'autre de ces deux formules. La forme $aa + 2bb$ se rapporte au premier cas $8n + 1$, lorsque a est impair et b pair, et au second $8n + 3$, quand a et b sont impairs. Ainsi, tout autre nombre impair ou de la forme $8n + 5$ ou $8n + 7$ est entièrement exclu du nombre des diviseurs de la forme $aa + 2bb$. Donc tous les nombres qui sont divisibles par quelques-uns de ceux-ci: 5, 7, 13, 15, 21, 23, 29, 31, [35], 37, 39, 45, 47, 53, 55 etc., ne peuvent pas être compris dans la forme $aa + 2bb$.

12. Il est très remarquable que tous les nombres premiers, tant de la forme $8n + 1$ que $8n + 3$, sont toujours réductibles à un carré plus le double d'un carré, mais d'une seule manière; en voici des exemples

$8n + 1$	$8n + 3$	
$17 = 3^2 + 2 \cdot 2^2$	$3 = 1^2 + 2 \cdot 1^2$	$67 = 7^2 + 2 \cdot 3^2$
$41 = 3^2 + 2 \cdot 4^2$	$11 = 3^2 + 2 \cdot 1^2$	$83 = 9^2 + 2 \cdot 1^2$
$73 = 1^2 + 2 \cdot 6^2$	$19 = 1^2 + 2 \cdot 3^2$	$107 = 3^2 + 2 \cdot 7^2$
$89 = 9^2 + 2 \cdot 2^2$	$43 = 5^2 + 2 \cdot 3^2$	$131 = 9^2 + 2 \cdot 5^2$
$97 = 5^2 + 2 \cdot 6^2$	$59 = 3^2 + 2 \cdot 5^2$	$139 = 11^2 + 2 \cdot 3^2$
$113 = 9^2 + 2 \cdot 4^2$		
$137 = 3^2 + 2 \cdot 8^2$		

1) Le manuscrit contient ici la preuve de cette affirmation. R. F.

13. Dans toutes ces décompositions on ne saurait découvrir le moindre ordre, et pourtant ce qu'il y a de très remarquable, c'est qu'on peut même démontrer la vérité rigoureusement. Pour cet effet, il ne s'agit que de prouver, qu'étant proposé un nombre quelconque premier de la forme $8n + 1$ ou $8n + 3$, on peut toujours assigner un produit de la forme $aa + 2bb$, qui admette l'un ou l'autre pour facteur. Cette démonstration se tire d'un très beau théorème de FERMAT, savoir que la forme $c^{2m} - 1$ est toujours divisible par le nombre $2m + 1$, lorsque celui-ci est premier [et ne divise pas c]. Par conséquent, si le nombre $8n + 1$ est premier, il sera toujours un facteur de la formule $c^{8n} - 1$, quel que soit c, pourvu qu'il ne soit pas un multiple de $8n + 1$. Mais comme la quantité $c^{8n} - 1$ a deux facteurs qui sont $(c^{4n} + 1)$ $(c^{4n} - 1)$, il faut donc que l'un ou l'autre soit divisible par $8n + 1$.

Supposons que ce soit $c^{4n} + 1$ qui admette la division; ainsi, puisque c^{4n} est un bicarré, nous aurons $f^4 + 1$ en mettant au lieu de ce bicarré f^4. Or

$$f^4 + 1 = (ff - 1)^2 + 2ff,$$

qui est un carré plus le double d'un carré et par conséquant divisible par $8n + 1$.

14. Quant à l'autre formule $8n + 3$, chaque nombre premier de la forme $8n + 3$ est un diviseur de $c^{8n+2} - 1$ et par conséquent de $c^{4n+1} + 1$ ou de $c^{4n+1} - 1$. Soit $c = 2$, la formule $c^{4n+1} - 1$ revient à la suivante $2 \cdot 2^{4n} - 1$, qui ne peut jamais être divisible par $8n + 3$, parce que tous les diviseurs de la forme $2ff - 1$ sont ou $8n + 1$ ou $8n - 1$, et jamais $8n + 3$. Donc $2^{4n+1} + 1$ ou $2 \cdot 2^{4n} + 1$ qui est de la forme $gg + 2ff$, sera nécessairement divisible par $8n + 3$, d'où il est aisé de remarquer que $8n + 3$ étant premier est de la forme $gg + 2ff$.

Après cette digression, qui paraît n'être pas inutile, revenons à notre problème. Nous avons vu, que la somme s doit avoir au moins trois facteurs; ainsi posons la égale à $(aa + 2bb)(cc + 2dd)(ff + 2gg)$, et pour abréger le calcul soit

$$(aa + 2bb)(cc + 2dd) = mm + 2nn,$$

alors nous aurons

$$m = ac \pm 2bd, \quad n = bc \mp ad.$$

De là notre somme deviendra $s = (mm + 2nn)(ff + 2gg)$, que nous supposerons égale à $zz + 2vv$, et nous aurons pareillement

$$z = mf \pm 2ng \quad \text{et} \quad v = nf \mp mg.$$

15. Substituons maintenant au lieu de m et n les valeurs trouvées, et nous aurons quatre valeurs différentes pour z et v, savoir pour z:

$$\begin{aligned}
&1°.\ f(ac + 2bd) + 2g(bc - ad),\\
&2°.\ f(ac + 2bd) - 2g(bc - ad),\\
&3°.\ f(ac - 2bd) + 2g(bc + ad),\\
&4°.\ f(ac - 2bd) - 2g(bc + ad),
\end{aligned}$$

et pour v les suivantes:

$$\begin{aligned}
&1°.\ f(bc - ad) - g(ac + 2bd),\\
&2°.\ f(bc - ad) + g(ac + 2bd),\\
&3°.\ f(bc + ad) - g(ac - 2bd),\\
&4°.\ f(bc + ad) + g(ac - 2bd).
\end{aligned}$$

16. Voilà donc quatre valeurs différentes de z et v. Mais comme il n'en faut que trois, à cause des trois valeurs de $s = pp + 2xx$, $s = qq + 2yy$ et $s = rr + 2zz$, nous ne prendrons que les trois premières valeurs de z et v, savoir:

$$\begin{aligned}
&f(ac + 2bd) + 2g(bc - ad) = p, \qquad && f(bc - ad) - g(ac + 2bd) = x,\\
&f(ac + 2bd) - 2g(bc - ad) = q, \qquad && f(bc - ad) + g(ac + 2bd) = y,\\
&f(ac - 2bd) + 2g(bc + ad) = r, \qquad && f(bc + ad) - g(ac - 2bd) = z.
\end{aligned}$$

17. Cherchons à présent par le moyen des valeurs x, y, z la somme de leurs carrés qui aura cette forme $s = Aff + Bgg + 2Cfg$, où:

$$\begin{aligned}
A &= 3bbcc - 2abcd + 3aadd,\\
B &= 3aacc + 4abcd + 12bbdd,\\
C &= -(bc + ad)(ac - 2bd).
\end{aligned}$$

La différence entre cette expression de la somme s et sa valeur précédente:

$$\begin{aligned}
s &= (aa + 2bb)(cc + 2dd)(ff + 2gg)\\
&= ff(aacc + 2bbcc + 2aadd + 4bbdd) + 2gg(aacc + 2bbcc + 2aadd + 4bbdd)
\end{aligned}$$

sera donc nulle ou:

$$Fff + Ggg + 2Cfg = 0,$$

où:

$$\begin{aligned}
F &= bbcc - 2abcd + aadd - aacc - 4bbdd,\\
G &= aacc + 4abcd + 4bbdd - 4bbcc - 4aadd,\\
C &= -(bc + ad)(ac - 2bd).
\end{aligned}$$

Nous voilà donc parvenus à la solution de notre problème; car il ne s'agit plus dans l'équation $Fff + Ggg + 2Cfg = 0$ qui renferme les six lettres a, b, c, d, f, g, que de trouver des valeurs convenables pour les six lettres, afin de satisfaire à cette égalité, et de là nous trouverons x, y, z comme aussi p, q, r.

18. Étant donc arrivé à l'égalité $Fff + Ggg + 2Cfg = 0$, qui donne

$$\frac{f}{g} = \frac{-C \pm \sqrt{(CC - FG)}}{F},$$

il faudrait chercher de telles valeurs pour a, b, c, d, que $CC - FG$ devienne un carré. Mais cela nous plongerait dans de très grands embarras, que nous voudrions éviter. Heureusement nous sommes tombés sur un cas, où l'équation $Fff + Ggg + 2Cfg = 0$ se réduit facilement au premier degré, savoir quand F est égal à 0; alors on a $Ggg + 2Cfg = 0$, ou

$$\frac{f}{g} = -\frac{G}{2C}.$$

Ainsi, en réduisant $-\frac{G}{2C}$ aux plus petits termes, si l'on prend le numérateur pour f et le dénominateur pour g, toutes les formules trouvées ci-dessus seront exprimées en nombres rationels. C'est en quoi consiste le mérite de cette méthode.

19. Remarquons maintenant que la valeur

$$\begin{aligned} &bbcc - 2abcd + aadd - aacc - 4bbdd = \\ &= (bb - aa)\,cc + (aa - 4bb)\,dd - 2abcd, \end{aligned}$$

trouvée pour F, peut être exprimée comme produit de deux facteurs:

$$F = \big((b + a)\,c + (a + 2b)\,d\big)\,\big((b - a)\,c + (a - 2b)\,d\big).$$

Ainsi on pourra égaler à zéro ou l'un ou l'autre de ces deux facteurs, pour que F devienne zéro. Du premier on tire

$$\frac{c}{d} = \frac{-a - 2b}{b + a},$$

du second

$$\frac{c}{d} = \frac{2b - a}{b - a}.$$

Il y aura donc une double détermination pour les lettres c et d et par conséquent aussi une double solution du problème.

20. De la même manière nous pourrions faire évanouir la valeur de G, et puisque elle est égale à

$$aacc + 4abcd + 4bbdd - 4bbcc - 4aadd =$$
$$= (aa - 4bb)\,cc + (4bb - 4aa)\,dd + 4abcd\,,$$

elle doit avoir aussi deux facteurs:

$$G = ((a + 2b)\,c - (2b + 2a)\,d)\;((a - 2b)\,c - (2b - 2a)\,d)\,,$$

et nous aurons $\dfrac{c}{d} = \dfrac{2b + 2a}{a + 2b}$ et $\dfrac{c}{d} = \dfrac{2b - 2a}{a - 2b}$.

Mais ces valeurs ne conduiraient pas à des solutions nouvelles; ainsi il suffira de nous en tenir aux valeurs tirées de $F = 0$.

21. Voilà donc une solution assez simple du problème proposé, et qui fournira en même temps une infinité de solutions particulières. Pour cela, il n'y aura qu'à suivre les règles suivantes:

1°. Après avoir pris à volonté les deux nombres a et b, cherchons les valeurs de c et d par l'une ou l'autre de ces deux formules

$$\frac{c}{d} = \frac{-a - 2b}{b + a} \quad \text{ou} \quad \frac{c}{d} = \frac{2b - a}{b - a}\,,$$

puisque chacune conduira à une solution.

2°. Cherchons ensuite les valeurs de C et G d'après les formules

$$C = -(bc + ad)\,(ac - 2bd)\,,$$
$$G = (aa - 4bb)\,cc + (4bb - 4aa)\,dd + 4abcd\,,$$

et nous aurons:

$$\frac{f}{g} = \frac{(aa - 4bb)\,cc + 4\,(bb - aa)\,dd + 4abcd}{2(bc + ad)\;(ac - 2bd)}\,,$$

c'est-à-dire, après avoir réduit cette fraction à ses plus petits termes, il faudra prendre f égal au numérateur, et g au dénominateur.

3°. Ayant ainsi trouvé les valeurs de f et g, on aura immédiatement celles de x, y, z par ces formules

$$x = f(bc - ad) - g(ac + 2bd),$$
$$y = f(bc - ad) + g(ac + 2bd),$$
$$z = f(bc + ad) - g(ac - 2bd),$$

qui sont les racines des trois nombres cherchés.

4°. Enfin les lettres p, q, r se trouveront aussi d'après ces formules

$$p = f(ac + 2bd) + 2g(bc - ad),$$
$$q = f(ac + 2bd) - 2g(bc - ad),$$
$$r = f(ac - 2bd) + 2g(bc + ad).$$

Eclaircissons ces règles par quelques exemples.

EXEMPLE 1

Soit $a = 1$ et $b = 1$, alors $\frac{c}{d}$ sera égale dans le premier cas à $-\frac{3}{2}$, et dans le second à $\frac{1}{0}$, ce qui ne conduit à rien. Ainsi supposons $c = 3$ et $d = -2$; $\frac{f}{g}$ sera $= -\frac{51}{14}$, soit $f = 51$ et $g = -14$. Alors

$$x = 51(3 + 2) + 14(3 - 4) = 241, \qquad p = -51 - 28 \cdot 5 = -191,$$
$$y = 51(3 + 2) - 14(3 - 4) = 269, \qquad q = -51 + 28 \cdot 5 = 89,$$
$$z = 51(3 - 2) + 14(3 + 4) = 149, \qquad r = 51 \cdot 7 - 28 = 329,$$

enfin $s = 3 \cdot 17 \cdot 2993$ ou $= 3 \cdot 17 \cdot 41 \cdot 73$ [1]).

EXEMPLE 2

Soit $a = 1$ et $b = 2$, alors $\frac{c}{d} = -\frac{5}{3}$ ou $= \frac{3}{1}$; développons donc l'un et l'autre cas.

Cas 1. Soit $c = 3$ et $d = 1$, on aura $\frac{f}{g} = \frac{99}{14}$ et, par conséquent, $f = 99$ et $g = 14$; de là nous aurons

$$x = 99 \cdot 5 - 14 \cdot 7 = 397, \qquad p = 99 \cdot 7 + 28 \cdot 5 = 833,$$
$$y = 99 \cdot 5 + 14 \cdot 7 = 593, \qquad q = 99 \cdot 7 - 28 \cdot 5 = 553,$$
$$z = 99 \cdot 7 + 14 = 707, \qquad r = -99 + 28 \cdot 7 = 97,$$
$$s = 9 \cdot 11 \cdot 10193 = 9 \cdot 11 \cdot 17 \cdot 599.$$

1) Cet exemple est déjà communiqué dans le § 5. R. F.

Cas 2. Soit $c = 5$ et $d = -3$, on aura $\frac{f}{g} = -\frac{387}{238}$ et, par conséquent, $f = 387$, $g = -238$; de là

$$x = 387 \cdot 13 - 238 \cdot 7 = 3365, \quad p = 387 \cdot -7 - 2 \cdot 238 \cdot 13 = -8897,$$
$$y = 387 \cdot 13 + 238 \cdot 7 = 6697,^{1}) \quad q = 387 \cdot -7 + 2 \cdot 238 \cdot 13 = 3479,$$
$$z = 387 \cdot 7 + 238 \cdot 17 = 6755, \quad r = 387 \cdot 17 - 2 \cdot 238 \cdot 7 = 3247,$$
$$s = 9 \cdot 43 \cdot 263057 = 101\,803\,059 .$$

EXEMPLE 3

Soit $a = 3$ et $b = 1$, on aura $\frac{c}{d} = -\frac{5}{4}$ ou $= \frac{1}{2}$. Il faut remarquer ici que le dernier cas est déjà traité dans l'exemple précédent, puisque a, b, c, d sont permutables. C'est pourquoi nous ne développerons que le premier cas, où $c = 5$ et $d = -4$; $\frac{f}{g} = \frac{627}{322}$, d'où $f = 627$, $g = 322$ et, par conséquent,

$$x = 627 \cdot 17 - 322 \cdot 7 = 8405, \quad p = 627 \cdot 7 + 644 \cdot 17 = 15337,^{2})$$
$$y = 627 \cdot 17 + 322 \cdot 7 = 12913, \quad q = 627 \cdot 7 - 644 \cdot 17 = -6559,^{3})$$
$$z = 627 \cdot -7 - 322 \cdot 23 = -11795, \quad r = 627 \cdot 23 - 644 \cdot 7 = 9913,$$
$$s = 11 \cdot 57 \cdot 600497 .$$

22. Ces exemples suffisent pour montrer, comment, par ces règles, on peut facilement trouver autant de solutions qu'on voudra. Nous nous contenterons ici d'exposer les résultats les plus simples, et pour lesquels les nombres x, y, z ne surpassent pas mille.

I	II	III	IV	V
$x = 241$	397	425	595	493 [4])
$y = 269$	593	373	769	797
$z = 149$	707	205	965	937
$p = 191$	833	23	1081	1127
$q = 89$	553	289	833	697
$r = 329$	97	527	119	17

1) Manuscrit: 7697. R. F.
2) Manuscrit: 16337. R. F.
3) Manuscrit: 7559. R. F.
4) Manuscrit: 393. R. F.

SECONDE METHODE

23. La solution de notre problème a été réduite à cette équation carrée

$$Fff + Ggg + 2Cfg = 0,$$

où

$$C = -(bc + ad)(ac - 2bd) = -ab(cc - 2dd) - cd(aa - 2bb),$$
$$F = (bb - aa)cc + (aa - 4bb)dd - 2abcd,$$
$$G = (aa - 4bb)cc + (4bb - 4aa)dd + 4abcd,$$

et enfin à la formule

$$\frac{f}{g} = \frac{-C \pm V(CC - FG)}{F},$$

dans laquelle $CC - FG$ doit être un carré. Supposons donc $CC - FG = VV$, de sorte que

$$\frac{f}{g} = \frac{-C \pm V}{F}.$$

Substituant les valeurs de C, F et G, nous aurons

$$VV = (aa - 2bb)^2 c^4 + 8(aa - 2bb)abc^3 d - 4(aa - 2bb)^2 ccdd$$
$$- 16(aa - 2bb)abcd^3 + 4(aa - 2bb)^2 d^4,$$

expression qui, étant divisée par $(aa - 2bb)^2$ et abrégée par la substitution de m au lieu de $\frac{ab}{aa - 2bb}$, deviendra assez simple, savoir:

$$\frac{VV}{(aa - 2bb)^2} = c^4 + 8mc^3 d - 4ccdd - 16mcd^3 + 4d^4.$$

24. Maintenant, comme cette formule doit être un carré, supposons sa racine égale à

$$\frac{V}{aa - 2bb} = cc - 4mcd + 2dd,$$

et de là, en les comparant, on trouvera l'égalité suivante:

$$2mc - d - 2mmd = 0,$$

et, par conséquent,

$$\frac{c}{d} = \frac{2mm + 1}{2m}.$$

Ainsi, soit $c = 2mm + 1$ et $d = 2m$, notre formule deviendra

$$\frac{V}{aa - 2bb} = (2mm + 1)^2 - 8mm(2mm + 1) + 8mm = 4mm + 1 - 12m^4\ ^1).$$

25. A présent il ne s'agira plus que de prendre pour a et b des nombres à volonté, et de là on aura $m = \frac{ab}{aa - 2bb}$; si l'on substitue les valeurs déjà trouvées dans celles de C, F et V, on aura $\frac{f}{g} = \frac{-C \pm V}{F}$. On voit par là que les lettres f et g peuvent être déterminées de deux manières dans chaque cas. Or, ayant trouvé ces lettres, on pourra déterminer aisément tant les valeurs de x, y, z que celles de p, q, r. Le cas le plus simple se prévoit et se rapporte à la supposition de $a = 1$ et $b = 1$; alors $m = -1$, $c = 3$, $d = -2$ et $F = 0$; mais ce cas est précisément celui de la première méthode, c'est pourquoi on trouverait les mêmes résultats. Voici d'autres exemples:

EXEMPLE 1

Soit $a = 3$ et $b = 2$, alors $m = 6$, $c = 73$, $d = 12$, $f = -7$, $g = 17$ et enfin

$$\begin{aligned} x &= 5309, & p &= 1871, \\ y &= 3769, & q &= 5609, \\ z &= 4181, & r &= 4991. \end{aligned}$$

EXEMPLE 2

Soit ici $a = 3$ et $b = 1$, et nous aurons $m = \frac{3}{7}$, $c = 67$, $d = 42$, $f = -47$, $g = 46$ et enfin:

$$\begin{aligned} x &= 10337, & p &= 18823, \\ y &= 15883, & q &= 7967, \\ z &= 14453, & r &= 12257. \end{aligned}$$

TROISIEME METHODE

26. Cette troisième méthode est tirée de la précédente, où nous avions

$$\frac{VV}{(aa - 2bb)^2} = c^4 + 8mc^3 d - 4ccdd - 16mcd^3 + 4d^4 \quad \text{et} \quad m = \frac{ab}{aa - 2bb}.$$

1) Manuscrit: $-8m^4$. R. F.

Réduisons cette valeur sous cette forme

$$\frac{VV}{(aa-2bb)^2} = (cc-2dd)\ (cc-2dd+8mcd)\,,$$

laquelle étant divisée par $(cc-dd)^2$, et posant pour abréger $\frac{cd}{cc-2dd} = n$, on aura

$$\frac{VV}{(aa-2bb)^2\ (cc-2dd)^2} = 1+8mn\,.$$

Il ne s'agit donc ici que de rendre cette forme $1+8mn$ égale à un carré.

27. Pour cet effet soit $\sqrt{(1+8mn)} = v$, et nous aurons

$$V = v(aa-2bb)\,(cc-2dd)\ ;$$

posons la dans la valeur de $\frac{f}{g}$, nous aurons

$$\frac{f}{g} = \frac{-C \pm v(aa-2bb)\ (cc-2dd)}{F}\,.$$

Mais nous avions ci-dessus [paragraphe 23]

$$C = -ab\,(cc-2dd) - cd\,(aa-2bb)\,;$$

divisons cette valeur par $aa-2bb$ et $cc-2dd$ et nous aurons

$$\frac{C}{(aa-2bb)\ (cc-2dd)} = -(m+n)\,,$$

ainsi

$$-C = +(m+n)\,(aa-2bb)\,(cc-2dd)\,,$$

et, par conséquent,

$$\frac{f}{g} = \frac{(m+n\pm v)\ (aa-2bb)\ (cc-2dd)}{F}\,.$$

Divisons maintenant en haut et en bas par $(aa-2bb)\,(cc-2dd)$ pour avoir le numérateur $m+n\pm v$; alors le dénominateur deviendra

$$\frac{F}{(aa-2bb)\ (cc-2dd)} = \frac{bbcc-aacc+aadd-4bbdd-2abcd}{(aa-2bb)\ (cc-2dd)}\,.$$

28. Or puisque $aa - 2bb = \frac{ab}{m}$, $cc - 2dd = \frac{cd}{n}$, nous aurons aussi

$$bb = \frac{aa}{2} - \frac{ab}{2m} \quad \text{et} \quad dd = \frac{cc}{2} - \frac{cd}{2n},$$

et si l'on substitue ces valeurs de bb et dd dans celle de F, on trouvera après avoir divisé par $\frac{abcd}{mn}$ $[= (aa - 2bb)(cc - 2dd)]$ le dénominateur de notre fraction se réduire à

$$\frac{nc}{2d} - \frac{acmn}{bd} + \frac{am}{2b} - 1 - 2mn,$$

ou enfin à

$$2mn + \frac{3}{4} + \frac{1}{4}\left(\frac{aa + 2bb}{aa - 2bb}\right)\left(\frac{cc + 2dd}{cc - 2dd}\right) = u,^{1})$$

et de là notre fraction devenir:

$$\frac{f}{g} = \frac{m + n \pm v}{u}.$$

Maintenant ayant les six valeurs a, b, c, d, f et g, la solution de notre problème sera contenue dans les formules suivantes:

$$\begin{aligned}
x &= f(bc - ad) - g(ac + 2bd), \\
y &= f(bc - ad) + g(ac + 2bd), \\
z &= f(bc + ad) + g(ac - 2bd), \\
p &= f(ac + 2bd) + 2g(bc - ad), \\
q &= f(ac + 2bd) - 2g(bc - ad), \\
r &= f(ac - 2bd) + 2g(bc + ad).
\end{aligned}$$

29. Voyons à présent de quelle manière on pourra trouver des nombres convenables pour m et n, afin que $8mn + 1$ soit un carré. Remarquons ici en passant que tant

$$m = \frac{ab}{aa - 2bb} \quad \text{que} \quad n = \frac{cd}{cc - 2dd}$$

sont contenus dans cette forme générale $\frac{AB}{AA - 2BB}$, que je suppose égale à M; ainsi l'on pourra aisément construire une table, qui indiquera pour chaque nombre A et B la valeur de M, afin qu'on puisse choisir deux tels nombres de M, que leurs produits pris 8 fois plus l'unité fasse un carré. D'où il est clair

1) L'auteur a changé le signe de l'expression du dénominateur. R. F.

que ces deux valeurs de M doivent avoir le même dénominateur, ou que l'un et l'autre soient carré. Ainsi soit $\pm(AA - 2BB) = A'A' - 2B'B'$, on aura [par exemple][1]) $A' = A \pm 2B$ et $B' = A \pm B$, et quoi qu'il viendra $A'A' - 2B'B' = -AA + 2BB$, cela ne doit pas nous choquer, puisque les nombres m et n peuvent recevoir des valeurs tant positives que négatives.

30. Posons $AA - 2BB = \Delta$, de sorte que $M = \frac{AB}{\Delta}$. Il ne s'agit donc à présent que de construire une table de plusieurs valeurs de M, d'en chercher deux, qui prises pour m et n changent la formule $8mn+1$ en un carré, dont la racine est v. Or il n'est pas difficile de trouver plusieures paires de tels nombres; car il ne faut que prendre $m = n = N$, et alors vv est égal à $8NN + 1$ laquelle étant développée donne

$$vv = \left(\frac{AA + 2BB}{\Delta}\right)^2$$

et, par conséquent,

$$v = \frac{AA + 2BB}{\Delta}.$$

Mais remarquons ici que l'égalité entre les nombres m et n conduirait toujours à ce cas, où deux des carrés cherchés seraient égaux entre eux. Supposons à présent $m = \frac{AB}{AA - 2BB}$, où $a = A$ et $b = B$, puis $n = \frac{A'B'}{A'A' - 2B'B'}$ ou aussi $c = A'$ et $d = B'$, $[A'A' - 2B'B' = -AA + 2BB]$, on aurait en substituant les valeurs de A', B', $c = a \pm 2b$, $d = a \pm b$ qui est précisément le cas de la première méthode. C'est pourquoi il faut exclure ces cas de nos recherches présentes. Nous chercherons donc deux valeurs de M telles que l'une ne soit pas dérivée de l'autre, ou lorsqu'on prend $a = A$, $b = B$, il ne faut pas prendre $c = A'$ et $d = B'$.

31. Après ces remarques, on voit que pour chaque valeur de Δ on peut trouver une infinité de valeurs pour A et B, en prenant toujours $A' = A \pm 2B$ et $B' = A \pm B$, parceque par ce moyen on aura toujours la même valeur de Δ. Observons ici qu'il est indifférent que Δ soit positive ou négative; car on n'a qu'à changer le signe de A ou B. Encore, puisque $\Delta = AA - 2BB$, on verra aisément que tous les nombres Δ seront composés des nombres premiers ou de la forme $8j + 1$ ou $8j - 1$. Ainsi tous les nombres qui pourront tenir lieu de Δ seront les suivants:

1, 7, 17, 23, 31, 41, 47, 49, 71, 73, 79, 89, 97 au-dessous de 100.

1) Manuscrit: toujours. Corrigé par R. F.

32. Nous ajouterons dans les tables de Δ chaque valeur de Δ desquelles sont déduites les valeurs de A et B moindres que 100 [1]):

I

$\Delta=1$	
A	B
1	1
3	2
7	5
17	12
41	29
99	70

II

$\Delta=7$	
A	B
1	2
3	1
5	3
5	4
11	8
13	9
27	19
31	22
65	46
75	53

III

$\Delta=17$	
A	B
1	3
5	2
7	4
9	7
15	11
23	16
37	26
55	39
89	63

IV

$\Delta=23$	
A	B
5	1
3	4
7	6
11	7
19	13
25	18
45	32
61	43
109	77

V

$\Delta=31$	
A	B
1	4
7	3
9	5
13	10
19	14
33	23
47	33
79	56
113	80

VI

$\Delta=41$	
A	B
7	2
3	5
11	9
13	8
29	20
29	21
69	49
71	50

VII

$\Delta=47$	
A	B
7	1
5	6
9	8
17	11
25	17
39	28
59	42
95	67
143	101

VIII

$\Delta=49$	
A	B
1	5
9	4
11	6
17	13
23	17
43	30
57	40
103	73

IX

$\Delta=71$	
A	B
1	6
11	5
13	7
21	16
27	20
53	37
67	47
127	90

X

$\Delta=73$	
A	B
9	2
5	7
13	11
19	12
35	24
43	31
83	59
105	74

XI

$\Delta=79$	
A	B
9	1
7	8
11	10
23	15
31	21
53	38
73	52
129	91

XII

$\Delta=89$	
A	B
3	7
11	4
17	10
19	15
37	27
49	34
91	64
117	83

XIII

$\Delta=97$	
A	B
1	7
13	6
15	8
25	19
31	23
63	44
77	54
151	107

33. Puisque nous avons exclus tous les deux nombres M, dont l'un est dérivé de l'autre, on trouvera à peine dans cette table deux nombres pour M qui soient égaux à $\frac{AB}{\Delta}$, et dont le produit pris 8 fois plus l'unité fasse un nombre carré. C'est pourquoi il faudra combiner deux différentes classes entre elles, mais encore avec quelques égards; par exemple la première table ne

1) Pour calculer ce tableau il faut multiplier successivement $A + \sqrt{2}\,B$ par les unités $1 \pm \sqrt{2}$. R. F.

saurait être combinée qu'avec la VIII.; car un nombre entier multiplié par une fraction, dont le dénominateur n'est pas un carré, ne pourrait pas en produire un, à moins que l'un ou l'autre nombre de la première table ne détruise le dénominateur. Ainsi si l'on veut combiner la première table avec la seconde, il faudra prendre $M = 7 \cdot 5$ ou bien $= 99 \cdot 70$, afin que le dénominateur $\Delta = 7$ soit détruit. Soit par exemple $M = 7 \cdot 5$ et, puisque la seconde table donne d'abord $M = \frac{2}{7}$, dont le produit 10 étant multiplié par 8 plus 1 est 81, qui est le carré de 9, prenons donc $m = 35$; alors $a = 7$, $b = -5$ et n étant $= \frac{2}{7}$ donne $c = 1$, $d = -2$, et $mn = 10$ qui étant multiplié par 8 plus 1 donne 81, qui est un carré, ainsi:

$$v = 9, \quad u = \frac{368}{7} \text{ et enfin } \frac{f}{g} = \frac{m + n \pm v}{2} = \frac{155}{184} \text{ ou } = \frac{1}{2};$$

mais il faut remarquer qu'en ce cas, où $\frac{f}{g} = \frac{1}{2}$, on aura deux carrés égaux entre eux, savoir $\frac{f}{g} = \frac{c}{d}$. La première au contraire conduit à notre première solution, lorsqu'on aura divisé par 9 les nombres x, y, z. Puisque donc cette méthode ne conduit qu'à des solutions individuelles, je passerai à une quatrième méthode, où la première est portée à un plus haut degré de perfection.

QUATRIEME METHODE

34. Ayant posé, comme dans la première méthode, la somme des trois carrés cherchés $s = (aa + 2bb)(cc + 2dd)(ff + 2gg)$, je supposerai le premier facteur $aa + 2bb$ résoluble de deux manières différentes en un carré plus le double d'un carré, savoir $\alpha\alpha + 2\beta\beta = aa + 2bb$. Prenons la première forme $aa + 2bb$ pour la détermination des lettres x, y, p, q, et la dernière $\alpha\alpha + 2\beta\beta$ pour la détermination de z et r, en sorte que

$$\begin{aligned} x &= f(bc - ad) - g(ac + 2bd), & p &= f(ac + 2bd) + 2g(bc - ad), \\ y &= f(bc - ad) + g(ac + 2bd), & q &= f(ac + 2bd) - 2g(bc - ad), \\ z &= f(\beta c + \alpha d) - g(\alpha c - 2\beta d), & r &= f(\alpha c - 2\beta d) + 2g(\beta c + \alpha d). \end{aligned}$$

35. Tirant de là la somme des trois carrés $xx + yy + zz = s$, nous aurons cette formule

$$s = Aff + Bgg - 2Cfg,$$

où

$$A = 2bbcc - 4abcd + 2aadd + \beta\beta cc + 2\alpha\beta cd + \alpha\alpha dd,$$
$$B = 2aacc + 8abcd + 8bbdd + \alpha\alpha cc - 4\alpha\beta cd + 4\beta\beta dd,$$
$$C = (\alpha c - 2\beta d)(\beta c + \alpha d).$$

Soit de plus

$$D = (aa + 2bb)(cc + 2dd) = aacc + 2bbcc + 2aadd + 4bbdd;$$

nous aurons

$$s = (aa + 2bb)(cc + 2dd)(ff + 2gg) = Dff + 2Dgg.$$

36. Retranchant cette valeur de s de la formule $Aff + Bgg - 2Cfg$, nous obtiendrons l'équation

$$Fff + Ggg - 2Cfg = 0, \quad \text{où} \quad F = A - D, \quad G = B - 2D,$$

et par conséquent

$$F = (\beta\beta - aa)cc + (\alpha\alpha - 4bb)dd - 4abcd + 2\alpha\beta cd,$$
$$G = (\alpha\alpha - 4bb)cc + 4(\beta\beta - aa)dd + 8abcd - 4\alpha\beta cd,$$

lesquelles peuvent être représentées ainsi qu'il suit:

$$F = ((\beta + a)c + (\alpha + 2b)d)((\beta - a)c + (\alpha - 2b)d),$$
$$G = ((\alpha + 2b)c - 2(\beta + a)d)((\alpha - 2b)c - 2(\beta - a)d).$$

37. Cette résolution en facteurs nous met en état de faire évanouir F, en posant

$$\frac{c}{d} = \frac{-\alpha - 2b}{\beta + a} \quad \text{ou} \quad = \frac{-\alpha + 2b}{\beta - a}.$$

Alors notre équation deviendra $Ggg - 2Cfg = 0$, d'où

$$\frac{f}{g} = \frac{G}{2C}.$$

Cette formule est assez compliquée à cause de la valeur de G; mais nous la rendrons plus simple en remarquant que F étant égal à zéro la quantité G peut être remplacée par $2F + G$. Alors nous aurons:

$$2F + G = (2(\beta\beta - aa) + \alpha\alpha - 4bb)(cc + 2dd) = -(aa + 2bb)(cc + 2dd);$$

par conséquent

$$\frac{f}{g} = -\frac{(aa + 2bb)(cc + 2dd)}{2(\alpha c - 2\beta d)(\beta c + \alpha d)};$$

d'où il suit

$$f = (aa + 2bb)(cc + 2dd), \quad g = -2(\alpha c - 2\beta d)(\beta c + \alpha d).$$

38. Si l'on voulait substituer ces valeurs de c, d, f, g dans les formules finales de x, y, z et p, q, r, elles deviendraient assez compliquées. Mais voici une règle des plus simples pour trouver les nombres x, y, z et p, q, r.

REGLE POUR TROUVER AUTANT DE SOLUTIONS QU'ON VOUDRA DE NOTRE PROBLEME

39. Ayant pris à volonté deux nombres m et n, dont m doit être impair, qu'on en tire ces trois quantités

$$s = mm + 2nn, \quad t = mm - 2nn \text{ et } u = 2mn;$$

cela posé, les valeurs des six lettres x, y, z, p, q et r seront

$$\begin{aligned} x &= s(s+u)(3s+4u) - 2tt(s+2u), & p &= st(3s+4u) + 4t(s+u)(s+2u), \\ y &= s(s+u)(3s+4u) + 2tt(s+2u), & q &= st(3s+4u) - 4t(s+u)(s+2u), \\ z &= st(3s+4u) + 2t(s+2u)^2, & r &= s(s+2u)(3s+4u) - 4tt(s+2u). \end{aligned}$$

40. En considérant ces six formules, on voit d'abord qu'elles ne donnent point de solutions différentes de notre problème, soit qu'on prenne t positive ou négative, puisque le changement de t en $-t$ ne fait que changer les signes de z, p et q. Mais si l'on prend u négatif, alors ces formules subiront un grand changement. D'où l'on voit que chaque paire des nombres m et n donnera deux solutions différentes, selon qu'on prendra m et n positivement ou négativement. En voici des applications.

EXEMPLE 1

Soit $m = 1$ et $n = \pm 1$; alors $s = 3$, $t = 1$, $u = \pm 2$. Soit premièrement $u = -2$, nous aurons $s + u = 1$, $s + 2u = -1$, $3s + 4u = 1$ et, par conséquent:

$$\begin{aligned} x &= 3 \cdot 1 \cdot 1 + 2 = 5, & p &= 3 - 4 = -1, \\ y &= 3 - 2 = 1, & q &= 3 + 4 = 7, \\ z &= 3 + 2 = 5, & r &= -3 + 4 = 1. \end{aligned}$$

Mais ici deux des nombres cherchés sont égaux, c'est pourquoi cette solution ne saurait être admise.

Prenons donc $u = 2$, alors $s + u = 5$, $s + 2u = 7$, $3s + 4u = 17$ et, par conséquent:

$$\begin{aligned} x &= 3 \cdot 5 \cdot 17 - 2 \cdot 7 = 241, & p &= 3 \cdot 17 + 4 \cdot 5 \cdot 7 = 191, \\ y &= 3 \cdot 5 \cdot 17 + 2 \cdot 7 = 269, & q &= 3 \cdot 17 - 4 \cdot 5 \cdot 7 = -89, \\ z &= 3 \cdot 17 + 2 \cdot 49 = 149, & r &= 3 \cdot 7 \cdot 17 - 4 \cdot 7 = 329\ ^{1}). \end{aligned}$$

EXEMPLE 2

Soit dans cet exemple $m = 1$, $n = [\pm]\, 2$; alors $s = 9$, $t = -7$, $u = \pm 4$. Prenons premièrement $u = -4$, on aura $s + u = 5$, $s + 2u = 1$, $3s + 4u = 11$ et enfin:

$$\begin{aligned} x &= 9 \cdot 5 \cdot 11 - 98 = 397, & p &= 9 \cdot 7 \cdot 11 + 4 \cdot 7 \cdot 5 \cdot 1 = 833, \\ y &= 9 \cdot 5 \cdot 11 + 98 = 593, & q &= 9 \cdot 7 \cdot 11 - 4 \cdot 7 \cdot 5 \cdot 1 = 553, \\ z &= 7 \cdot 9 \cdot 11 + 2 \cdot 7 = 707, & r &= 9 \cdot 1 \cdot 11 - 4 \cdot 7 \cdot 7 \cdot 1 = -97, \end{aligned}$$

Soit pour le second cas $u = 4$, alors $s + u = 13$, $s + 2u = 17$, $3s + 4u = 43$ et, par conséquent:

$$\begin{aligned} x &= 9 \cdot 13 \cdot 43 - 98 \cdot 17 = 3365, \\ y &= 9 \cdot 13 \cdot 43 + 98 \cdot 17 = 6697, \\ z &= 7 \cdot 9 \cdot 43 + 14 \cdot 17^2 = 6755, \\ p &= 7 \cdot 9 \cdot 43 + 28 \cdot 13 \cdot 17 = 8897, \\ q &= 7 \cdot 9 \cdot 43 - 28 \cdot 13 \cdot 17 = 3479, \\ r &= 9 \cdot 17 \cdot 43 - 196 \cdot 17 = 3247\ ^{2}). \end{aligned}$$

DEMONSTRATION DE LA REGLE PRECEDENTE

41. Posons $aa + 2bb = \alpha\alpha + 2\beta\beta = s$, $a\alpha - 2b\beta = t$ et $a\beta + b\alpha = u$, on aura $ss = tt + 2uu$. Prenons les valeurs trouvées ci-dessus de c et d, savoir $c = -\alpha - 2b$, $d = \beta + a$. Pour ce qui concerne les deux autres, elles dérivent de celles-ci en prenant a et b négatives. On aura $cc + 2dd = 3s + 4u$, $ac + 2bd = -t$, $\alpha c - 2\beta d = -(s + 2u)$, $bc - ad = -(s + u)$ et $\beta c + \alpha d = t$; enfin $f = s(3s + 4u)$ et $g = 2t(s + 2u)$.

1) Cet exemple est déjà communiqué dans le § 5. R. F.
2) Ces deux solutions sont déjà communiquées dans le § 21. R. F.

42. Substituons maintenant ces valeurs dans les formules rapportées ci-dessus au paragraphe 34, nous trouverons les expressions suivantes:

$$\begin{aligned} x &= s(s+u)(3s+4u) - 2tt(s+2u), \\ y &= s(s+u)(3s+4u) + 2tt(s+2u), \\ z &= st(3s+4u) + 2t(s+2u)^2, \\ p &= st(3s+4u) + 4t(s+u)(s+2u), \\ q &= st(3s+4u) - 4t(s+u)(s+2u), \\ r &= s(3s+4u)(s+2u) - 4tt(s+2u), \end{aligned}$$

qui ont été rapportées dans la règle.

43. Enfin, puisque les trois lettres s, t, u ne sont assujetties qu'à vérifier l'équation $ss = tt + 2uu$, on n'a qu'à remplir cette condition, sans avoir égard aux lettres a, b, α, β, c, et prendre

$$s = mm + 2nn, \quad t = mm - 2nn, \quad u = \pm 2mn.$$

Les lettres m et n sont entièrement à notre volonté. Quant à celles de s, t, u, qui remplissent la condition $ss = tt + 2uu$, voici les plus simples valeurs:

s	3	9	11	17	19	27	33	33	41	43
t	1	7	7	1	17	23	17	31	23[1])	7
u	2	4	6	12	6	10	20	8	24	30

CINQUIEME METHODE

44. Nous avons vu au commencement que les équations

$$zz + yy - xx = pp, \quad zz + xx - yy = qq$$

seront satisfaites, si l'on prend

$$z = aa + bb, \quad yy - xx = 4ab(aa - bb), \quad p = aa + 2ab - bb,$$
$$q = aa - 2ab - bb;$$

ainsi si l'on multiplie ces formules par quelques facteurs communs, elles doivent rester valable. Supposons donc

$$z = mn(aa + bb), \quad yy - xx = 4mmnnab(aa - bb),$$

on aura:

$$p = mn(aa + 2ab - bb), \quad q = mn(aa - 2ab - bb);$$

1) Manuscrit: 7.

R. F.

par conséquant, il ne nous restera qu'à remplir la troisième condition de notre problème, savoir:

$$xx + yy - zz = rr.$$

45. Maintenant, pour que les trois valeurs x, y, z n'aient point de facteur commun, prenons

$$y + x = 2mma(a + b) \text{ et } y - x = 2nnb(a - b);$$

pour abréger l'expression, soit $aa + ab = A$ et $ab - bb = B$, de sorte que

$y + x = 2mmA$ et $y - x = 2nnB$; or $A - B = aa + bb$ et $z = mn(A - B)$.

La somme des carrés de $y + x$ et $y - x$ nous donne

$$yy + xx = 2m^4AA + 2n^4BB;$$

retranchant de là la valeur de zz, on aura

$$rr = 2m^4AA + 2n^4BB - mmnn(A - B)^2.$$

46. Pour rendre cette formule plus traitable, supposons $m = f + g$, $n = f - g$; de là on obtiendra

$$rr = \alpha f^4 + \beta f^3 g + \gamma ffgg + \beta fg^3 + \alpha g^4.$$

Si l'on développe les coefficients, on trouvera:

$$\alpha = 2AA + 2BB - (A - B)^2 = (A + B)^2,$$
$$\beta = 8AA - 8BB,$$
$$\gamma = 12(AA + BB) + 2(A - B)^2.$$

En substituant ces valeurs dans l'équation précédente, nous aurons

$$rr = (A + B)^2 f^4 + 8(AA - BB)f^3 g + \big(12(AA + BB) + 2(A - B)^2\big)ffgg + 8(AA - BB)fg^3 + (A + B)^2 g^4.$$

47. Pour ramener à présent cette formule à un carré, supposons que sa racine soit

$$r = (A + B)ff + 4(A - B)fg - (A + B)gg,$$

d'où il suit

$$rr = (A+B)^2 f^4 + 8(AA - BB) f^3 g - 2(A+B)^2 ffgg + 16(A-B)^2 ffgg - 8(AA - BB) fg^3 + (A+B)^2 g^4 .$$

Retranchant cette expression de la précédente nous obtiendrons

$$0 = 32ABffgg + 16(AA - BB) fg^3 ,$$

d'où l'on tire

$$f = AA - BB ,$$
$$g = -2AB .$$

Ayant donc pris:

$$r = (A+B) ff + 4(A-B) fg - (A+B) gg ,$$

ou bien:

$$r = (A+B)(ff - gg) + 4(A-B) fg ,$$

on pose $m = f + g$ et $n = f - g$ et, par conséquant, $ff - gg = mn$ et $4fg = mm - nn$. On aura:

$$r = mn(A+B) + (mm - nn)(A-B) .$$

Or $A + B = aa + 2ab - bb$ et $A - B = aa + bb$. Il sera donc aisé de développer nos formules pour chaque valeur des lettres a, b, puisque nous avons supposé

$$x = mmA - nnB ,$$
$$y = mmA + nnB ,$$
$$z = mn(A - B) ,$$
$$p = mn(aa + 2ab - bb) \text{ et } q = mn(aa - 2ab - bb) .$$

48. Voici la manière de s'y prendre pour trouver autant de solutions qu'on voudra. Après avoir pris à volonté a et b, on formera $A = aa + ab$, $B = ab - bb$, puis $f = AA - BB$ et $g = -2AB$, de là $m = f + g$, $n = f - g$. Ainsi, ayant déterminé ces valeurs, les nombres cherchés seront donnés par les formules suivantes:

$$x = mmA - nnB , \qquad p = mn(aa + 2ab - bb) ,$$
$$y = mmA + nnB , \qquad q = mn(aa - 2ab - bb) ,$$
$$z = mn(A - B) , \qquad r = mn(A+B) + (mm - nn)(A-B) .$$

Rapportons ici quelques exemples.

EXEMPLE 1

Soit $a = 1$, $b = 2$, nous aurons $A = 3$, $B = -2$; de là $f = 5$, $g = 12$, $m = 17$, $n = -7$; enfin les nombres cherchés seront:

$$x = 17 \cdot 17 \cdot 3 + 7 \cdot 7 \cdot 2 = 965, \quad p = 17 \cdot 7 \cdot 1 = 119,$$
$$y = 17 \cdot 17 \cdot 3 - 7 \cdot 7 \cdot 2 = 769, \quad q = 17 \cdot 7 \cdot 7 = 833,$$
$$z = 17 \cdot 7 \cdot 5 = 595, \quad r = -7 \cdot 17 \cdot 1 + 240 \cdot 5 = 1081.$$

Cette solution se trouve déjà rapportée dans le paragraphe 22.

EXEMPLE 2

Soit $a = 2$, $b = 1$, nous aurons $A = 6$, $B = 1$, $f = 35$, $g = -12$, enfin $m = 23$, $n = 47$ et, par conséquent:

$$x = 23 \cdot 23 \cdot 6 - 47 \cdot 47 \cdot 1 = 965, \quad p = 23 \cdot 47 \cdot 7 = 7567,$$
$$y = 23 \cdot 23 \cdot 6 + 47 \cdot 47 \cdot 1 = 5383, \quad q = 23 \cdot 47 \cdot -1 = -1081,$$
$$z = 23 \cdot 47 \cdot 5 = 5405, \quad r = 23 \cdot 47 \cdot 7 - 1680 \cdot 5 = -833.$$

49. Il faut observer qu'il serait superflu de prendre les nombres a et b tous deux impairs, puisqu'alors les nombres A et B seraient pairs et, par conséquent, réductibles à de moindres nombres.

EXEMPLE 3

Soit $a = 2$, $b = 3$, nous aurons $A = 10$, $B = -3$, $f = 91$, $g = 60$, $m = 151$, $n = 31$; d'où résulte

$$x = 151 \cdot 151 \cdot 10 + 31 \cdot 31 \cdot 3 = 230893,$$
$$y = 151 \cdot 151 \cdot 10 - 31 \cdot 31 \cdot 3 = 225127,$$
$$z = 151 \cdot 31 \cdot 13 = 60853,$$
$$p = 151 \cdot 31 \cdot 7 = 32767,$$
$$q = 151 \cdot 31 \cdot 17 = 79577,$$
$$r = 151 \cdot 31 \cdot 7 + 21840 \cdot 13 = 316687.^{1})$$

Observons ici que toutes les solutions trouvées par cette méthode diffèrent essentiellement de toutes celles qu'on tire des méthodes précédentes [2]).

1) Manuscrit: $151 \cdot 31 \cdot 7 - 21840 \cdot 13 = 251153$. R. F.

2) Cette observation est contraire au fait que la solution donnée par l'exemple 1 se trouve déjà rapportée dans le paragraphe 22. A. M.

SOLUTION D'UN PROBLEME ASSEZ CURIEUX SAVOIR: TROUVER QUATRE NOMBRES POSITIFS ET INEGAUX ENTR-EUX TELS QUE LA SOMME DE DEUX SOIT TOUJOURS UN CARRE

Manuscriptum manu A. WILBRECHTI factum et academiae scientiarum Petropolitanae relictum [1])
Prima editio
Présenté à l'Académie de St-Pétersbourg le 1er mars 1781

1. Parmi ces quatre nombres il ne doit y avoir qu'un seul impair, ou bien tous les quatre seront pairs ou impairement pairs, c'est-à-dire de la forme $4n+2$. La raison en est: Si tous les quatre sont pairs et non divisibles par quatre, il faut qu'ils soyent compris dans la forme $4n+2$; ensuite si deux de ces nombres sont impairs, ils ne peuvent être compris [tous les deux] ni dans la forme $4n+1$ ni $4n-1$. Enfin si l'une était de la forme $4n-1$ et l'autre $4n+1$, ils [ne] pourraient [pas tous les deux] produire ensemble avec les deux autres un carré. En effet toutes les solutions qu'on peut trouver renferment ou tous les quatre nombres impairement pairs comme ceux-ci: 98, 1346, 2018 et 5378 ou seulement un impair comme ceux-ci 4482, 6127, 8514 et 21762.

2. Si l'on voulait admettre des nombres négatifs, le problème n'aurait aucune difficulté, et même on pourrait donner des formules générales comprenant toutes les solutions possibles. Mais la condition prescrite, où tous les nombres doivent être positifs et inégaux entre eux, rend la solution extrêmement difficile; et l'on ne saurait parvenir que moyennant des artifices tout particuliers, dont on n'a fait aucun usage en d'autres occasions. C'est pourquoi la solution que nous donnerons de ce problème ne paraît pas indigne de l'attention des géomètres.

1) Voir la note p. 303. Le présent mémoire est le second du manuscrit présenté à l'académie de St-Pétersbourg. R. F.

3. Désignons les quatre nombres cherchés par les lettres A, B, C, D qui étant tous inégaux entre eux, soit A le plus petit et D le plus grand; puis selon l'ordre de la grandeur soit B le second, C le troisième, de sorte que $A < B < C < D$. Ceci étant posé, commençons par les trois plus petits A, B, C et soit $A + B = pp$, $A + C = qq$, $B + C = rr$, d'où l'on tirera

$$A = \frac{pp + qq - rr}{2}, \quad B = \frac{pp + rr - qq}{2}, \quad C = \frac{qq + rr - pp}{2}.$$

On voit d'abord que de ces trois carrés pp, qq, rr le premier est le plus petit pp et le dernier le plus grand rr. Or on voit que de ces trois carrés la somme de deux doit toujours surpasser le troisième, ce qu'on obtient dès que $pp + qq > rr$.

4. Passons maintenant au quatrième nombre D qui est le plus grand, et puisque $B + C = rr$, soit pareillement $B + D = ss$, et on aura $ss > rr$; de là on aura

$$D = ss - B = \frac{2ss - pp + qq - rr}{2},$$

qui est évidemment toujours positif. Substituons cette valeur de D, et nous aurons

$$A + D = \frac{2ss - 2rr + 2qq}{2} = ss - rr + qq = tt,$$
$$C + D = ss + qq - pp = uu.$$

Ainsi sitôt qu'on aura rempli ces deux dernières conditions, toutes les sommes de deux nombres cherchés deviendront des carrés, savoir:

$$A + B = pp, \quad A + C = qq, \quad B + C = rr,$$
$$A + D = tt, \quad B + D = ss, \quad C + D = uu,$$

et il faut toujours observer ici que $pp < qq < rr < ss$.

5. Donc pour résoudre notre problème, nous n'avons qu'à satisfaire cette double égalité:

$$ss + qq = rr + tt = pp + uu.$$

D'où l'on voit que le nombre exprimé par $ss + qq$ doit admettre au moins trois solutions différentes en deux carrés. Ainsi posant ce nombre égal à N, il faut qu'il soit au moins en trois manières résoluble en deux carrés. Il ne s'agit donc

pour cela que de parcourir tous les nombres de cette nature et d'en tirer les quatres carrés pp, qq, rr, ss, ensorte que $pp + qq > rr$.

6. On voit d'abord de là que le nombre N doit avoir au moins trois facteurs dont chacun soit la somme de deux carrés; puisque, s'il était premier, il ne pourrait admettre qu'une seule solution; s'il n'avait que deux facteurs premiers, il ne pourrait admettre que deux. Ainsi il est clair que le nombre N doit admettre au moins trois facteurs premiers de la forme $4n + 1$ et, par conséquent, être compris dans cette série:

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

au nombre desquels il faudrait ajouter aussi 2. Mais on ne le pourrait compter parmi les facteurs, puisqu'ils n'augmentent pas la résolution en deux carrés.

7. Resouvenons nous ici que ce produit $(aa + bb)(cc + dd)$ n'admet que deux solutions dans la forme $mm + nn$ qui sont

$$m = ac + bd, \qquad n = ad - bc,$$
$$m = ac - bd, \qquad n = ad + bc.$$

Ainsi de là un produit de trois facteurs $(aa + bb)(cc + dd)(ff + gg)$ admet quatre solutions, excepté le cas, où deux de ces facteurs seraient égaux entreux, puisqu'alors on n'aurait que trois. Car posant $f = c$ et $g = d$, les nouvelles résolutions seraient $(cm \pm dn)^2$ et $(cn \mp dm)^2$. Or quoique nous ayons deux valeurs pour m et n, cependant on ne tirera pas quatre valeurs différentes; puisque les valeurs de m et n seront

$(cm \pm dn)^2$	$(cn \mp dm)^2$
1. $aa(cc + dd)^2$,	1. $bb(cc + dd)^2$,
2. $aa(cc + dd)^2$,	2. $bb(cc + dd)^2$,
3. $(a(cc - dd) + 2bcd)^2$,	3. $(2acd - b(cc - dd))^2$,
4. $(a(cc - dd) - 2bcd)^2$,	4. $(2acd + b(cc - dd))^2$.

8. Pour plus de commodité, considérons un produit de trois facteurs en nombres déterminés, savoir: soit $N = 5 \cdot 13 \cdot 17 = 1105$, et nous aurons

1. $N = 33^2 + 4^2$,
2. $N = 32^2 + 9^2$,
3. $N = 31^2 + 12^2$,
4. $N = 24^2 + 23^2$.

C'est donc parmi ces quatre formules qu'il faut chercher nos trois égalités $ss + qq = rr + zz = pp + uu$, parmi lesquelles pp, qq, rr sont les plus petits et même tels que $pp + qq > rr$. Mais de pareilles valeurs ne se trouvent point ici. Ainsi doublons le nombre proposé $N = 2210$; et puisque $2aa + 2bb = (a + b)^2 + (a - b)^2$, les précédentes résolutions nous fournissent celle-ci:

1. $N = 37^2 + 29^2$,
2. $N = 41^2 + 23^2$,
3. $N = 43^2 + 19^2$,
4. $N = 47^2 + 1^2$.

Là on pourra prendre $p = 19$, $q = 23$, $r = 29$, puisque $19^2 + 23^2 - 29^2 = 7^2 = 49$ et, par conséquent,

$$A = \frac{49}{2}, \quad s = 41, \quad t = 37, \quad u = 43;$$

ainsi connaissant tous les carrés, les quatre nombres cherchés seront les suivants:

$$A = \frac{pp + qq - rr}{2} = \frac{49}{2}, \quad C = \frac{qq + rr - pp}{2} = \frac{1009}{2},$$

$$B = \frac{pp - qq + rr}{2} = \frac{673}{2}, \quad D = ss - B = \frac{2689}{2},$$

et enfin

$A + B = 19^2$, $A + C = 23^2$, $B + C = 29^2$,
$A + D = 37^2$, $B + D = 41^2$, $C + D = 43^2$.

9. Maintenant il est fort aisé de donner des nombres entiers, puisqu'on n'a qu'à multiplier les précédents par quatre; ainsi

$A = 98$, $B = 1346$, $C = 2018$, $D = 5378$,
$A + B = 38^2$, $A + C = 46^2$, $B + C = 58^2$,
$A + D = 74^2$, $B + D = 82^2$, $C + D = 86^2$.

10. Tout revient donc à décomposer chaque nombre choisi pour N en toutes les formes $mm + nn$ ou bien de trouver les racines m et n. Il est aisé donc de trouver toutes les solutions, quand on multiplie N encore par un facteur de la forme $aa + bb$. Car alors, faisant $N(aa + bb) = m'm' + n'n'$, on aura $m' = ma \pm nb$ et $n' = na \mp mb$. Ainsi prenant $N = 1105$ et $aa + bb = 37$ ou $a = 6$, $b = 1$, nous aurons deux nouvelles résolutions pour chacune des précédentes:

N	33, 4	32, 9	31, 12	24, 23
37	6, 1	6, 1	6, 1	6, 1
$37 \cdot N$	202, 9 194, 57	201, 22 183, 86[1])	198, 41 174, 103	167, 114 121, 162

Lesquelles rangées selon l'ordre convenable en donnant à m les plus grandes et à n les moindres valeurs nous aurons:

m	202	201	198	194	183	174	167	162
n	9	22	41	57	86[1])	103	114	121

Il ne s'agit donc à présent que de chercher parmi les valeurs de n trois nombres tels pour p, q, r que $pp + qq > rr$. On s'appercevra d'abord ici qu'on pourra prendre $p = 57$, $q = 86$[2]), $r = 103$; de là $s = 183$, $t = 174$, $u = 194$, et, par conséquent:

$$A = 18\,, \qquad B = 3231\,, \qquad C = 7378\,, \qquad D = 30258\,.$$

Voici un cas où l'un de nos nombres est impair et les autres impairement pairs.

11. Des mêmes valeurs de la lettre n on pourra encore prendre $p = 86$[3]), $q = 103$, $r = 114$; de là $s = 174$, $t = 167$, $u = 183$; [lesquels étant multipliés par quatre produiront les nombres entiers: $A = 10018$, $B = 19566$, $C = 32418$, $D = 101538$].

12. On tire encore des mêmes valeurs de n une solution, savoir prenant

---

1) Manuscrit: 87. Corrigé par R. F.

2) Manuscrit: $q = 87$. Par cette erreur l'auteur a donné pour A, B, C, D les valeurs inexactes:

$$\frac{149}{2}\,, \quad \frac{6289}{2}\,, \quad \frac{14929}{2}\,, \quad \frac{60689}{2}\,,$$

et a ajouté: „lesquels étant multipliés par quatre produiront des nombres entiers". Corrigé par R. F.

3) Manuscrit: $p = 87$, ce qui donne de nouveau des valeurs inexactes. C'est pourquoi on a dû supprimer le texte suivant du manuscrit: „et comme deux des valeurs de p, q, r sont impaires, on tirera tout de suite des nombres entiers pour les valeurs de A, B, etc., savoir:

$$A = 2591\,, \quad B = 4978\,, \quad C = 8018\,, \quad D = 25298\,;$$

voici un cas où l'un de nos nombres est impair et les trois autres impairement pairs".
Corrigé par R. F.

$p = 103$, $q = 114$, $r = 121$, et de là $s = 167$, $t = 162$, $u = 174$, desquels on tirera encore des valeurs entiers, savoir:

$$A = 4482, \qquad B = 6127, \qquad C = 8514, \qquad D = 21762.$$

Et nous avons déjà en même temps les carrés auxquels les sommes de chaque paire de nos nombres sont égales, savoir:

$$\begin{array}{lll} A + B = 103^2, & A + C = 114^2, & B + C = 121^2, \\ A + D = 162^2, & B + D = 167^2, & C + D = 174^2. \end{array}$$

13. Ainsi on voit de là, que plus on donne de facteurs aux nombres N, plus on tirera aussi de solutions, mais qui seront composées de très grands nombres. Or pour trouver des nombres qui soient plus petits, on prendra des puissances des nombres convenables comme de 5, 13, 17, qui nous mettront en état de donner même des formules générales comprenant à la fois une infinité de solutions. Ainsi prenant

$$N = 25(aa + bb) = mm + nn$$

on aura

$$\begin{array}{lll} m = 4a + 3b, & 5a, & 3a + 4b, \\ n = 3a - 4b, & 5b, & 4a - 3b. \end{array}$$

Nous supposons $3a - 4b$ être la valeur la plus petite de n, de sorte que $5b > 3a - 4b$ ou $a < 3b$; alors prenons $p = 3a - 4b$, $q = 5b$, $r = 4a - 3b$, on aura $s = 5a$, $t = 3a + 4b$, $u = 4a + 3b$, et enfin

$$A = \frac{32bb - 7aa}{2}, \quad B = \frac{25aa - 48ab}{2}, \quad C = \frac{7aa + 18bb}{2}, \quad D = \frac{25aa + 48ab}{2},$$

et pour que ces nombres deviennent positifs, il faudra prendre $a < b\sqrt{\frac{32}{7}}$ et $> \frac{48}{25}b$, ensorte que $\frac{a}{b}$ doit être compris entre ces deux limites 2, 138 et 1, 92.[1])

14. On peut développer pareillement cette formule $N = 5^3(aa + bb)$, et alors on prendra

$$\begin{array}{lll} p = 11b - 2a, & q = 10a - 5b, & r = 11b + 2a, \\ s = 10b + 5a, & t = 11a - 2b, & u = 11a + 2b, \end{array}$$

1) Manuscrit: 1, 092. Corrigé par R. F.

et de là

$$2A = 100aa - 188ab + 25bb, \quad 2B = 217bb + 100ab - 92aa,$$
$$2C = 100aa - 12ab + 25bb, \quad 2D = 142aa + 100ab - 17bb,$$

et la fraction $\frac{a}{b}$ doit être prise entre ces deux limites 1,74 et 2,00 [1]). Aussi prenant $a = 7$ et $b = 4$, on aura pour les quatre [nombres] cherchés:

$$A = 18, \quad B = 882, \quad C = 2482, \quad D = 4743,$$

qui selon toute apparence sont les plus petits nombres qui satisfassent au problème. Car on aura

$$A + B = 900 = 30^2, \quad A + C = 50^2, \quad A + D = 69^2,$$
$$B + C = 58^2, \quad B + D = 75^2, \quad C + D = 85^2.$$

2) Valeur exacte: 2, 17. R. F.

SUPPLEMENT AU PROBLEME DE QUATRE NOMBRES DONT LA SOMME DE DEUX FASSENT TOUJOURS UN NOMBRE CARRE

Manuscriptum manu A. WILBRECHTI factum et academiae scientiarum Petropolitanae relictum[1])
Prima editio
Présenté à l'académie de St-Pétersbourg par LEONHARD EULER le 23 avril 1781

1. Quoique ce problème soit déjà assez difficile, cependant on peut encore ajouter une condition, qui est que les quatre nombres tiennent une proportion arithmétique, ou que $A + D$ soit égale à $B + C$; par conséquent on aura les six égalités:

$$A + B = pp, \quad A + C = qq, \quad A + D = rr = B + C, \quad B + D = ss$$
$$\text{et enfin } C + D = tt.$$

2. La somme de nos quatre nombres sera donc exprimée en trois manières différentes, savoir:

$$A + B + C + D = pp + tt = qq + ss = 2rr,$$

et lorsqu'on aura satisfait à ces conditions, le problème sera entièrement résolu, si l'on obtient des valeurs positives pour les quatre nombres cherchés. Desquels A est le plus petit et égal à $\frac{pp + qq - rr}{2}$, où $pp + qq > rr$;

$$B = \frac{pp + rr - qq}{2}, \quad C = \frac{qq + rr - pp}{2}, \quad D = \frac{3rr - pp - qq}{2}.$$

1) Voir la note p. 303 et les explications dans la préface. Le présent mémoire est le troisième du manuscrit présenté à l'académie de St-Pétersbourg. R. F.

3. Puisque nous avons $2rr = pp + tt = qq + ss$, il suit, que rr et par conséquent r doit être en deux manières la somme de deux carrés. Ainsi soit $r = (aa + bb)(cc + dd) = (ac \pm bd)^2 + (ad \mp bc)^2$ égal à $xx + yy$ et nous aurons:

$$x = ac \pm bd,\ y = ad \mp bc \text{ et } rr = (xx - yy)^2 + (2xy)^2;$$

et enfin

$$2rr = (xx - yy + 2xy)^2 + (xx - yy - 2xy)^2,$$

d'où nous tirons

$$t = xx - yy + 2xy \quad \text{et} \quad p = xx - yy - 2xy,$$

et les autres valeurs de x et y donneront semblablement les lettres s et q.

4. Maintenant parcourrons quelques cas en commençant par le plus simple, et soit $r = 5 \cdot 13$. Nous tirerons les doubles valeurs pour x et y, qui seront

x	8	7
y	1	4

Les premières nous donneront $xx - yy = 63$ et $2xy = 16$; par conséquent, $t = 79$ et $p = 47$. Les secondes $xx - yy = 33$, $2xy = 56$; par conséquent, $s = 89$ et $q = 23$. Remarquons ici qu'on peut changer entre eux les valeurs de t, p et s, q ensorte que q devienne toujours plus grand que p. Ainsi nous avons $r = 65$, $p = 23$ et $q = 47$. Mais $pp + qq$ ne devient pas plus grand que rr, de sorte que ce cas ne peut pas être employé.

5. Le même inconvénient arrive en supposant $r = 5 \cdot 17$. Mais prenant $r = 5 \cdot 29 = 145$ nous aurons pour x et y les solutions suivantes

x	12	9
y	1	8

Les dernières valeurs donnent $xx - yy = 17$, $2xy = 144$; de là $s = 161$, $q = 127$. Et les premières donnent $xx - yy = 143$, $2xy = 24$ et, par conséquent, $t = 167$, $p = 119$. Ici on voit clairement que $rr < pp + qq$ ou $21025 < 30290$. Ainsi notre solution sera la suivante:

$$A = \frac{9265}{2},\quad B = \frac{19057}{2},\quad C = \frac{22993}{2},\quad D = \frac{32785}{2}.$$

Si l'on multiplie chaque nombre par 4, nous aurons:

$$A = 18530, \quad B = 38114, \quad C = 45986, \quad D = 65570,$$

et conséquemment

$$A + B = 238^2, \quad A + C = 254^2, \quad A + D = B + C = 290^2,$$
$$B + D = 322^2, \quad C + D = 334^2.$$

Par cet exemple on voit suffisamment la route qu'on doit tenir pour trouver autant de solutions qu'on voudra.

RECHERCHES ULTERIEURES ET TRES CURIEUSES SUR LE PROBLEME DE QUATRE NOMBRES POSITIFS ET EN PROPORTION ARITHMETIQUE TELS QUE LA SOMME DE DEUX QUELCONQUES SOIT TOUJOURS UN NOMBRE CARRE

Commentatio 797 indicis ENESTROEMIANI
Prima editio: Commentationes arithmeticae 2, 1849, p. 617—625
Haec editio congruit cum manuscripto manu A. WILBRECHTI facto et academiae scientiarum Petropolitanae relicto [1])
Présenté à l'académie de St-Pétersbourg par LEONHARD EULER le 23 avril 1781

1. Soient comme précédemment [2]) A, B, C, D les quatre nombres cherchés et disposés selon l'ordre de grandeur, en sorte que A soit le plus petit et D le plus grand. Les six conditions à remplir seront:

$$A + B = pp\,, \quad A + C = qq\,, \quad A + D = rr = B + C\,,$$
$$B + D = ss \text{ et } C + D = tt\,;$$

de là $2rr = pp + tt = qq + ss$, et enfin les quatre nombres cherchés seront exprimés par les carrés pp, qq, rr de la manière suivante:

$$2A = pp + qq - rr\,, \quad 2B = pp + rr - qq\,,$$
$$2C = qq + rr - pp\,, \quad 2D = 3rr - pp - qq\,,$$

et pour que tous les nombres deviennent positifs, il faut que $pp + qq > rr$.

1) Voir la note p. 303 et les explications dans la préface. Ce mémoire est le dernier des quatre présentés à l'académie de St-Pétersbourg. R. F.

2) Voir le mémoire précédent, p. 337 de ce volume. R. F.

2. De plus, on voit que r doit être égale à la somme de deux carrés; ainsi soit $r = xx + yy$, nous aurons $rr = (xx - yy)^2 + (2xy)^2$ et, par conséquent,

$$2rr = (xx - yy + 2xy)^2 + (xx - yy - 2xy)^2 ,$$

et puisque cette quantité doit représenter $pp + tt$, posons pour p la différence de ces deux formules $xx - yy$, $2xy$, et pour t la somme des mêmes formules. Exprimons maintenant r de cette sorte $x'x' + y'y'$, nous aurons

$$rr = (x'x' - y'y')^2 + (2x'y')^2$$

et

$$2rr = (x'x' - y'y' + 2x'y')^2 + (x'x' - y'y' - 2x'y')^2 ,$$

et comme cette quantité représente $qq + ss$, on prendrait pour q la différence des valeurs $x'x' - y'y'$ et $2x'y'$ et pour s la somme. Ayant

$$pp = (xx - yy)^2 - 4xy(xx - yy) + (2xy)^2 = rr - 4xy(xx - yy)$$

comme aussi

$$qq = rr - 4x'y'(x'x' - y'y') ,$$

et puisque $pp + qq > rr$, on aura

$$rr > 4xy(xx - yy) + 4x'y'(x'x' - y'y') .$$

3. Puisque r doit être la somme de deux carrés de deux manières différentes, posons donc $r = (aa + bb)(cc + dd)$, [où nous supposerons $a > b$ et $c > d$]. Pour diminuer le nombre de lettres soit $\frac{a}{b} = f$, $\frac{c}{d} = z$, f et z étant des quantités plus grandes que l'unité; on aura $r = bbdd(ff + 1)(zz + 1)$, où nous pouvons supprimer le facteur carré $bbdd$. Ainsi nous aurons

$$r = (ff + 1)(zz + 1) ,$$

d'où, et par conséquent:

$$x = fz + 1,\ x' = fz - 1,\ y = z - f,\ y' = z + f ;$$

de là:

$$xy(xx - yy) = (fz + 1)(z - f)((f + 1)z - f + 1)((f - 1)z + f + 1) = M ,$$

$$x'y'(x'x' - y'y') = (fz - 1)(z + f)((f + 1)z + f - 1)((f - 1)z - f - 1) = N .$$

Ceci étant posé, il est claire que $rr > 4(M + N)$. Remarquons en passant que les deux valeurs de M et N doivent toujours être prises positives, quand même il arrive que l'une ou l'autre des formules devienne négative; voilà pourquoi il conviendra mieux d'exprimer ainsi:

$$rr > 4(\pm M \pm N).$$

4. Pour que ces formules soient plus commodes, soit $\frac{f+1}{f-1} = \varrho$, ϱ étant une quantité plus grande que l'unité. Introduisant cette quantité dans les valeurs de $\frac{M}{(f-1)^2}$, $\frac{N}{(f-1)^2}$, tirées des équations précédentes, nous aurons

$$\frac{M}{(f-1)^2} = (fz+1)(z-f)(\varrho z-1)(z+\varrho) = P,$$

$$\frac{N}{(f-1)^2} = (fz-1)(z+f)(\varrho z+1)(z-\varrho) = Q,$$

de sorte que la condition à remplir sera

$$\frac{rr}{(f-1)^2} > 4(\pm P \pm Q),$$

où il faudra toujours prendre les signes de manière à rendre $\pm P$, $\pm Q$ positifs.

5. En considérant ces formules, on doit remarquer d'abord que les deux lettres f et ϱ sont permutables entre elles, puisqu'en les remplaçant l'une par l'autre la valeur P se change en Q et réciproquement. En effet, ayant $\varrho = \frac{f+1}{f-1}$, on aura aussi $f = \frac{\varrho+1}{\varrho-1}$, de manière que l'une se détermine par l'autre de la même façon; puis ces deux lettres se déterminent réciproquement l'une par l'autre par cette égalité $f\varrho - \varrho - f = 1$ ou bien $(f-1)(\varrho-1) = 2$.

Observons ici que dans le cas, où $f = \varrho$, on a $f-1 = \varrho-1 = \sqrt{2}$ et, par conséquent, $f = \varrho = 1 + \sqrt{2}$; dans tous les autres cas, l'une sera plus petite et l'autre surpassera ce nombre. Ainsi supposant $\varrho > f$, nous aurons $f < 1 + \sqrt{2}$, $\varrho > 1 + \sqrt{2}$. Quant au cas $f = 1$, la valeur de ϱ devient infiniment grande.

6. Ayant posé $r = (ff + 1)(zz + 1)$, on aura $rr = (ff + 1)^2(zz + 1)^2$ et de là

$$\frac{rr}{(f-1)^2} = \frac{(ff+1)^2\,(zz+1)^2}{(f-1)^2}\,.$$

Or comme $\frac{ff+1}{f-1} = \frac{\varrho\varrho+1}{\varrho-1}$, on obtiendra

$$\frac{rr}{(f-1)^2} = \frac{(ff+1)\,(\varrho\varrho+1)}{(f-1)\,(\varrho-1)}(zz+1)^2\,,$$

ce qui donne

$$\frac{rr}{(f-1)^2} = \tfrac{1}{2}(ff+1)\,(\varrho\varrho+1)\,(zz+1)^2\,,$$

la valeur du produit $(f-1)\,(\varrho-1)$ étant égale à 2, comme nous l'avons vu. Substituant cette expression de $\frac{rr}{(f-1)^2}$ dans l'inégalité précédente, nous trouverons que la condition à remplir sera la suivante:

$$(ff+1)\,(\varrho\varrho+1)\,(zz+1)^2 > 8\,(\pm P \pm Q)\,.$$

7. Développant les valeurs des lettres P et Q, nous aurons

$$P = f\varrho z^4 + (f\varrho+1)\,(\varrho-f)z^3 - (ff\varrho\varrho+1-(\varrho-f)^2)zz - (f\varrho+1)\,(\varrho-f)z + f\varrho\,,$$
$$Q = f\varrho z^4 - (f\varrho+1)\,(\varrho-f)z^3 - (ff\varrho\varrho+1-(\varrho-f)^2)zz + (f\varrho+1)\,(\varrho-f)z + f\varrho\,,$$

où le coefficient de zz peut se réduire à une forme très simple; en effet, puisque $(\varrho-f)^2 = (\varrho+f)^2 - 4f\varrho$, ce coefficient s'écrira ainsi: $ff\varrho\varrho+1+4f\varrho-(\varrho+f)^2$. Mais nous avons vu (paragraphe 5) que $\varrho+f = f\varrho-1$; donc $(\varrho+f)^2 = ff\varrho\varrho - 2f\varrho + 1$; par conséquent, ce coefficient se réduit à cette forme très simple $6f\varrho$. Ainsi nous aurons

$$P = f\varrho z^4 + (f\varrho+1)\,(\varrho-f)\,z^3 - 6f\varrho zz - (f\varrho+1)\,(\varrho-f)\,z + f\varrho\,,$$
$$Q = f\varrho z^4 - (f\varrho+1)\,(\varrho-f)\,z^3 - 6f\varrho zz + (f\varrho+1)\,(\varrho-f)\,z + f\varrho\,.$$

8. Les valeurs de P et Q étant déterminées par ces équations, il ne s'agit plus qu'à remplir cette condition

$$(ff+1)\,(\varrho\varrho+1)\,(zz+1)^2 > 8\,(\pm P \pm Q)\,;$$

de cette manière nous sommes conduits au problème suivant:

PROBLEME

9. *Le nombre f, et par conséquent aussi ϱ, étant donnés, trouver toutes les valeurs de la lettre z qui puissent remplir la condition mentionnée.*

C'est par là qu'on parviendra à une solution complète du problème principal, attendu que la lettre $f = \frac{a}{b}$ donnera les nombres a et b, et $z = \frac{c}{d}$ pareillement c et d, desquels on tirera ensuite x, y, x', y' qui conduiront aux valeurs de p, q, r et enfin à celles de A, B, C, D.

SOLUTION

10. Commençons par observer que les valeurs convenables de z sont comprises entre certaines limites, tantôt plus et tantôt moins étroites selon la valeur du nombre f, qui est toujours plus grande que 1 et moindre que $1 + \sqrt{2}$, ou bien, selon la valeur de $\varrho = \frac{f+1}{f-1}$, qui surpasse toujours $1 + \sqrt{2}$. Ces limites peuvent être facilement assignées, lorsqu'on connaît les cas, dans lesquels le premier membre de notre formule principale devient égal à l'autre, ou lorsqu'on connaît les racines de l'équation bicarrée

$$(ff + 1)(\varrho\varrho + 1)(zz + 1)^2 = 8(\pm P \pm Q),$$

qui pourra bien avoir quatre racines réelles. Mais comme nous prenons z toujours plus grand que 1, quelques-unes des racines nous seront inutiles.

11. Comme cette équation renferme deux quantités connues f et ϱ, liées entr'elles d'une équation, il sera utile d'introduire à leur place une seule lettre, qui puisse exprimer également l'une et l'autre quantité; ainsi soit

$$\frac{ff+1}{f-1} = 2n, \quad \frac{\varrho\varrho+1}{\varrho-1} = 2n.$$

Or, comme f est plus petit que ϱ, nous prendrons

$$f = n - \sqrt{(nn - 2n - 1)}, \quad \varrho = n + \sqrt{(nn - 2n - 1)},$$

et de là nous tirerons

$$f + \varrho = 2n, \quad \varrho - f = 2\sqrt{(nn - 2n - 1)} \quad \text{et enfin} \quad f\varrho = 2n + 1,$$

où $n > 1 + \sqrt{2}$. Soit ensuite $\sqrt{(nn - 2n - 1)} = k$, de sorte que $f = n - k$, $\varrho = n + k$, $\varrho - f = 2k$. A présent il n'est pas difficile d'éliminer de notre équation les deux lettres f et ϱ et d'introduire à leur place la seule lettre n.

12. Cela posé, commençons par le premier membre de notre équation; comme

$$(ff + 1)(\varrho\varrho + 1) = (f\varrho - 1)^2 + (f + \varrho)^2 ,$$

et que $f + \varrho = 2n$ et $f\varrho - 1 = 2n$, le premier membre prendra cette forme $8nn(zz + 1)^2$, et l'équation à résoudre sera

$$nn(zz + 1)^2 = \pm P \pm Q .$$

Prenons maintenant en considération les valeurs de P et Q, savoir

$$P = f\varrho z^4 + (f\varrho + 1)(\varrho - f)z^3 - 6f\varrho zz - (f\varrho + 1)(\varrho - f)z + f\varrho ,$$
$$Q = f\varrho z^4 - (f\varrho + 1)(\varrho - f)z^3 - 6f\varrho zz + (f\varrho + 1)(\varrho - f)z + f\varrho ;$$

comme $f\varrho = 2n + 1$, $\varrho - f = 2k$, ces valeurs deviendront

$$P = (2n + 1)z^4 + 4(n + 1)kz^3 - 6(2n + 1)zz - 4(n + 1)kz + 2n + 1 ,$$
$$Q = (2n + 1)z^4 - 4(n + 1)kz^3 - 6(2n + 1)zz + 4(n + 1)kz + 2n + 1 .$$

13. Pour découvrir maintenant les valeurs de z dans notre équation, il faudra considérer avec soin les signes + et — que doivent avoir les lettres P et Q. Remarquons premièrement que, lorsque $z > \varrho$, l'une et l'autre expression de P et Q sont positives; donc on les prendra avec le signe + (paragraphe 4). Mais si z est plus petit que f, alors P devient négatif et Q aussi et, par conséquent, il faudra leur donner le signe —. Enfin, si z se trouve entre f et ϱ, la lettre P sera positive et Q négative. D'après ces considérations, on voit que, selon que z est plus grand que ϱ ou plus petit que f, ou enfin contenu entre ϱ et f, on aura trois cas à développer, qui sont les suivants:

PREMIER CAS.

RECHERCHE DES VALEURS DE z PLUS GRANDES QUE ϱ.

14. Comme les deux lettres P et Q ont le signe +, nous aurons

$$P + Q = 2(2n + 1)z^4 - 12(2n + 1)zz + 2(2n + 1) ,$$

et notre équation développée à résoudre sera

$$nn(z^4 + 2zz + 1) = 2(2n + 1)(z^4 - 6zz + 1),$$

où, lorsque $nn > 2(2n + 1)$, le premier membre surpassera toujours le second; et, par conséquent, toutes les valeurs de z, depuis ϱ jusqu'à l'infini, répondront à notre but (paragraphe 5), et nous aurons toujours $pp + qq > rr$. Cela arrive, lorsque $n > 2 + \sqrt{6}$. Or, dans le cas de $n = 2 + \sqrt{6}$, on aura à cause de $nn = 10 + 4\sqrt{6}$:

$$k = \sqrt{(5 + 2\sqrt{6})} = \sqrt{3} + \sqrt{2},$$

$$[\varrho = (\sqrt{3} + \sqrt{2})(\sqrt{2} + 1),$$

$$f = (\sqrt{3} + \sqrt{2})(\sqrt{2} - 1)].$$

Donc cela aura lieu, quand

$$\varrho > (\sqrt{3} + \sqrt{2})(\sqrt{2} + 1), \quad f < (\sqrt{3} + \sqrt{2})(\sqrt{2} - 1),$$

ou bien, en réduisant en fractions décimales, lorsque $\varrho > 7{,}5957541$ et $f < 1{,}3032254$ [1]). Ainsi, toutes les fois que $f < 1{,}3032254$, ou $\varrho > 7{,}5957541$, la quantité z peut être plus grande que ϱ jusqu'à l'infini.

15. Passons maintenant au cas, où $nn < 2(2n + 1)$, ce qui arrive, lorsque $n < 2 + \sqrt{6}$, ou lorsque $f > (\sqrt{3} + \sqrt{2})(\sqrt{2} - 1)$ et, au contraire, $\varrho < (\sqrt{3} + \sqrt{2})(\sqrt{2} + 1)$. Si nous retranchons dans notre équation le premier membre du second, nous aurons

$$(4n + 2 - nn)z^4 - (24n + 12 + 2nn)zz + 4n + 2 - nn[= 0].$$

Soit pour abréger

$$\frac{nn + 12n + 6}{4n + 2 - nn} = \Delta,$$

il viendra, après avoir divisé par $4n + 2 - nn$,

$$z^4 - 2\Delta zz + 1 = 0.$$

En résolvant cette équation, on a $zz = \Delta \pm \sqrt{(\Delta^2 - 1)}$, ou enfin

$$z = \sqrt{\left(\frac{\Delta + 1}{2}\right)} \pm \sqrt{\left(\frac{\Delta - 1}{2}\right)}.$$

1) Manuscrit: $\varrho > 7{,}5957534$, $f < 1{,}3032248$. R. F.

Or puisque $z > \varrho [>1]$, la plus petite de ces deux valeurs serait inutile. Ainsi soit

$$z = \sqrt{\left(\frac{\Delta + 1}{2}\right)} + \sqrt{\left(\frac{\Delta - 1}{2}\right)}$$

et de là nous concluons que toutes les valeurs, depuis ϱ jusqu'à ce terme, fourniront des valeurs convenables pour z.

16. Supposons $f = \frac{3}{2}$[1]) et, par conséquent, $\varrho = 5$; nous aurons $n = \frac{13}{4}$, $\Delta = \left[\frac{889}{71} =\right] 12{,}52112$ et $\frac{\Delta + 1}{2} = 6{,}76056$, $\frac{\Delta - 1}{2} = 5{,}76056$; enfin $\sqrt{\left(\frac{\Delta + 1}{2}\right)} = 2{,}60$, $\sqrt{\left(\frac{\Delta - 1}{2}\right)} = 2{,}40$, et de là $z = 5$, c'est-à-dire z ne saurait surpasser ϱ que d'une fraction extrêmement petite.

SECOND CAS.
RECHERCHE DES VALEURS DE z QUI SE TROUVENT AU DESSOUS DE f

17. Ici P et Q sont négatifs, et notre équation à résoudre sera

$$nn(zz + 1)^2 = -P - Q = -2(2n + 1)z^4 + 12(2n + 1)zz - 2(2n + 1)$$
$$= -2(2n + 1)(z^4 - 6zz + 1),$$

laquelle peut être réduite à la précédente en faisant $z = \frac{v + 1}{v - 1}$; car alors on aura:

$$nn(vv + 1)^2 = 2(2n + 1)(v^4 - 6vv + 1).$$

Observons ici que les deux lettres v et z dépendent l'une de l'autre de la même manière que f et ϱ, de sorte qu'on aura semblablement $vz = v + z + 1$.

18. Ainsi nous aurons ici, de même qu'auparavant, les valeurs convenables de v entre les limites de ϱ et ∞, lorsque $\varrho > 7{,}5957541$ ou $f < 1{,}3032254$[2]), et, par conséquent, $z = \frac{v + 1}{v - 1}$ pourra être pris entre les limites de f et 1.

1) Manuscrit: $\frac{1}{2}$. R. F.

2) Voire la note p. 346. R. F.

19. Pour abréger, mettons au lieu des nombres rapportés 7,5957541 et 1,3032254[1]) simplement ceux-ci 7,5 et 1,3. D'après cela on arrivera à cette conclusion importante: toutes les fois que ϱ se trouve entre les limites 7,5 et ∞ ou bien f entre 1,3 et 1, on pourra toujours prendre le nombre z ou entre les limites ϱ et ∞ ou entre celles de f et 1.

20. Examinons à présent le cas, où $\varrho < 7{,}5$ ou $f > 1{,}3$, et commençons par le cas de $\varrho = f = 1 + \sqrt{2}$. Puisque $f = \varrho$, on aura $k = 0$ et $nn - 2n - 1 = 0$ ou $nn = 2n + 1$, par conséquent

$$\Delta = \frac{nn + 6(2n+1)}{2(2n+1) - nn} = \frac{7nn}{nn} = 7 ,$$

et enfin

$$v = 2 + \sqrt{3} = 3{,}7320508 , \quad z = \frac{v+1}{v-1} = \sqrt{3} = 1{,}7320508\,^{2}) .$$

Pour simplifier, nous remplacerons les nombres 3,7320508 et 1,7320508 par 3,7 et 1,7, et nous tirerons cette conclusion: dans le cas, où $f = \varrho = 1 + \sqrt{2}$, on pourra toujours prendre z ou entre les limites ϱ et 3,7 ou entre celles de f et 1,7. Il ne s'agit plus que de rechercher les cas, où ϱ se trouve dans les limites 7,5 et $1 + \sqrt{2}$ ou f entre celles de 1,3 et $1 + \sqrt{2}$.

21. Le cas traité précédemment par la supposition de $f = \frac{3}{2}$[3]) et $\varrho = 5$, nous donne $v = 5$, d'où il suit que $z = \frac{v+1}{v-1} = \frac{3}{2}$, c'est-à-dire que, dans ce cas, z ne pourra différer de f que d'une fraction presque nulle. Il se trouvera un autre cas, où la différence entre f et z s'évanouira entièrement, et on aura pour lors $rr = pp + qq$, laquelle circonstance conduit à cette valeur:

$$\varrho = 1 + \sqrt{2} + \sqrt{4 + 2\sqrt{2}} = 5{,}0273\,^{4}) \quad \text{et} \quad f = \frac{6{,}0273}{4{,}0273} = 1{,}496 .$$

Il suit de là que, lorsque l'on diminue ϱ au dessous de 7,5 vers le terme 5,0273, la valeur de z diminuera de plus en plus, jusqu'à devenir sensiblement égale à f[5]) .

---

1) Voire la note p. 346. R. F.

2) L'auteur a confondu les valeurs de v et z. R. F.

3) Manuscrit: $f = \frac{1}{2}$. R. F.

4) Pour $z = f$ v devient égal à ϱ qui doit alors satisfaire à l'équation $\varrho^4 - 2\Delta\varrho^2 + 1 = 0$; de là on reçoit la valeur indiquée de ϱ par un calcul élémentaire grâce à $2n = \frac{\varrho^2+1}{\varrho-1}$ et $\varrho > f > 1$. R. F.

5) Manuscrit: ϱ . R. F.

TROISIEME CAS.

RECHERCHE DES VALEURS DE z QUI SE TROUVENT ENTRE ϱ ET f

22. Dans ce cas, la valeur de P sera positive et celle de Q négative, et l'équation à résoudre sera

$$nn(zz+1)^2 = P - Q, \quad \text{ou} \quad nn(zz+1)^2 = 8(n+1)k(z^3 - z).$$

Supposons ici

$$\frac{8k(n+1)}{nn} = 4\vartheta \quad \text{ou} \quad \frac{2k(n+1)}{nn} = \vartheta ;$$

nous aurons cette équation bicarrée

$$z^4 - 4\vartheta z^3 + 2zz + 4\vartheta z + 1 = 0,$$

laquelle pourra être résolue sans qu'on ait recours au cube.

23. Supposons

$$z^4 - 4\vartheta z^3 + 2zz + 4\vartheta z + 1 = (zz - \alpha z - 1)(zz - \beta z - 1) ;$$

le produit des facteurs du second membre est

$$z^4 - (\alpha+\beta)z^3 + (\alpha\beta - 2)zz + (\alpha+\beta)z + 1,$$

lequel étant comparé avec le premier membre nous donne ces deux conditions $\alpha + \beta = 4\vartheta$, $\alpha\beta - 2 = 2$ ou bien $\alpha\beta = 4$, de là

$$\alpha - \beta = \sqrt{((\alpha+\beta)^2 - 4\alpha\beta)} = 4\sqrt{(\vartheta\vartheta - 1)},$$

ce qui prouve l'impossibilité de l'équation $nn(z^4 + 2zz + 1) = 8(n+1)k(z^3 - z)$ dans le cas, où $\vartheta < 1$. Donc, pour $\vartheta < 1$, la résolution est impossible, ou bien on ne pourra assigner aucun endroit entre les limites de f et ϱ qui puisse satisfaire à notre but.

24. Pour trouver les valeurs de n qui rendent $\vartheta < 1$, nous prendrons l'expression de ϑ qui est $\frac{2k(n+1)}{nn}$, où $k = \sqrt{(nn - 2n - 1)}$. Ainsi, nous aurons cette condition:

$$\frac{2(n+1)\sqrt{(nn - 2n - 1)}}{nn} < 1,$$

qui se réduit à cette expression $n^4 < \frac{4}{3}(2n+1)^2$; de laquelle nous tirons

$$n^2 < \frac{2(2n+1)}{\sqrt{3}} = \frac{4n}{\sqrt{3}} + \frac{2}{\sqrt{3}}, \quad \text{et} \quad n < \frac{2+\sqrt{(4+2\sqrt{3})}}{\sqrt{3}} = 1+\sqrt{3} = 2{,}7320508.$$

Il suit de là que, tant que n est plus petit que 2,7320508, ϑ sera plus petit que 1.

25. Passons maintenant au cas ou $\vartheta > 1$; alors, après avoir trouvé

$$\alpha+\beta = 4\vartheta \text{ et } \alpha-\beta = 4\sqrt{(\vartheta\vartheta-1)},$$

nous aurons

$$\alpha = 2\vartheta + 2\sqrt{(\vartheta\vartheta-1)}, \quad \beta = 2\vartheta - 2\sqrt{(\vartheta\vartheta-1)};$$

ainsi les deuxfacteurs de notre équation bicarrée $zz-\alpha z-1$ et $zz-\beta z-1$ étant égales à 0 donneront les quatre racines de z, dont la première est $z = \frac{\alpha}{2} \pm \sqrt{(\alpha\alpha+1)}$, ou en portant la valeur de α, égale à :

$$\vartheta + \sqrt{(\vartheta\vartheta-1)} \pm \sqrt{\left(2\vartheta(\vartheta+\sqrt{(\vartheta\vartheta-1)})\right)}.$$

Mais il n'est pas difficile de remarquer que

$$\vartheta + \sqrt{(\vartheta\vartheta-1)} = \left(\sqrt{\left(\frac{\vartheta+1}{2}\right)} + \sqrt{\left(\frac{\vartheta-1}{2}\right)}\right)^2;$$

donc les expressions trouvées pour les racines de notre équation se réduisent aux suivantes :

$$z = \vartheta + \sqrt{(\vartheta\vartheta-1)} \pm \sqrt{(\vartheta(\vartheta+1))} \pm \sqrt{(\vartheta(\vartheta-1))}.$$

La variation des signes de z nous donnera les autres racines de notre équation. Mais puisque nous ne cherchons que la racine comprise entre les limites de ϱ et f, nous n'aurons besoin que de la première racine avec les signes plus.

26. Nous sommes en état maintenant d'assigner pour chaque valeur proposée de f ou de $\varrho = \frac{f+1}{f-1}$ des valeurs convenables de z entre f et ϱ, en cherchant premièrement $2n = \frac{ff+1}{f-1}$ ou $= \frac{\varrho\varrho+1}{\varrho-1}$, puis $k = \sqrt{(nn-2n-1)}$, ou bien $k = n-f = \varrho-n$, puisque nous supposons toujours $f < 1+\sqrt{2}$ et $\varrho \geqslant 1+\sqrt{2}$; après avoir trouvé ceux-ci, on cherchera $\vartheta = \frac{2(n+1)k}{nn}$, et enfin la formule irrationelle trouvée fournira la valeur cherchée de z.

27. Ayant déterminé, d'après cette formule, les valeurs de z pour plusieurs nombres f ou ϱ, et les ayant jointes aux valeurs de z tirées des deux recherches précédentes, nous avons construit une table qui donne pour chaque nombre ϱ la limite qu'il faut prendre pour avoir $z < 1 + \sqrt{2}$ ou bien $v > 1 + \sqrt{2}$, afin que de notre problème principal il résulte $pp + qq > rr$. Si la fraction $\frac{a}{b}$ est plus grande que $1 + \sqrt{2}$, on la cherchera dans la première colonne de notre table sous ϱ, et alors la seconde colonne z donnera les limites pour ce nombre z et la troisième v pour celles de v. Outre cela il faut observer que les règles prescrites au commencement conduisent toujours aux mêmes valeurs des trois lettres p, q, r, soit qu'on prenne ϱ au lieu de f et v au lieu de z.

Table qui représente, pour chaque nombre ϱ, les limites tant pour z que pour v

ϱ	z	v	ϱ	z	v
2,41	1,73—2,41	2,41—3,73	5,0	1,49—1,49	5,00— 5,00
2,5	1,72—2,41	2,41—3,78	6,0	1,37—1,42	5,78— 6,40
3,0	1,71—2,41	2,41—3,82	7,0	1,21—1,38	6,25—10,64
3,5	1,66—2,41	2,41—4,00	7,5	1,00—1,36	6,53— ∞
3,75	1,64—2,20	2,63—4,11	10,0	1,00—1,33	7,00— ∞
4,0	1,61—1,83	3,42—4,25	∞	1,00—1,30	7,60— ∞
4,5	1,59—1,60	4,33—4,40			

Il faut remarquer ici que le nombre 2,41 est mis pour le terme $1 + \sqrt{2}$.

28. On voit d'ici que le nombre 5 ne pourrait être employé à la solution de notre problème, puisque toutes les deux limites de z que de v concourent ensemble. Mais, plus nous nous éloignons de ce cas singulier, plus aussi s'étendront les limites, entre lesquelles la fraction $\frac{c}{d}$ pourra être prise.

Pour éclaircir notre méthode par un exemple, prenons $\frac{a}{b} = 4$ ou bien $\frac{a}{b} = \frac{5}{3}$; l'autre fraction $\frac{c}{d}$ pourra être prise ou entre les limites 1,61 et 1,83 ou entre 3,42 et 4,25. Ainsi soit $\frac{a}{b} = \frac{4}{1}$, $\frac{c}{d} = \frac{7}{2}$, on aura

$a = 4$	$b = 1$	$x = 30$	$x' = 26$
$c = 7$	$d = 2$	$y = 1$	$y' = 15$

$xx - yy = 899$	$x'x' - y'y' = 451$
$2xy = 60$	$2x'y' = 780$
différence $= 839$	$= 329$

On prendra donc $p = 329$, $q = 839$ et ayant $r = 30^2 + 1^2 = 26^2 + 15^2 = 901$, on peut être assuré que $pp + qq > rr$, ou qu'on aura l'excès 361, dont la moitié donnera A ; il est aisé à présent de calculer tous les quatre nombres qui étant multipliés par 4 donneront:

$$A = 722, \quad B = 432242, \quad C = 2814962, \quad D = 3246482.$$

DE NUMERIS AMICABILIBUS [1)]

Commentatio 798 indicis ENESTROEMIANI
Prima editio: Commentationes arithmeticae 2, 1849, p. 627—636
Haec editio congruit cum manuscripto manu Euleri facto et academiae scientiarum Petropolitanae relicto

1. Inter omnia problemata, quae in Mathesi tractari solent, nunc quidem a plerisque nulla magis sterilia atque ab omni usu abhorrentia existimantur, quam ea, quae in contemplatione naturae numerorum et divisorum investigatione versantur. In quo iudicio hodierni mathematici a veteribus non mediocriter dissentiunt, qui huiusmodi speculationibus multo maius pretium constituere sunt soliti. Etsi enim veteres non ignoraverunt ex indagatione naturae numerorum parum utilitatis ad eam Matheseos partem, quae applicata vocari solet, et in investigatione rerum ad Physicam potissimum pertinentium est posita; tamen nihilominus in scrutandis numerorum proprietatibus multum studii et laboris consumserunt. Praeterquam enim, quod ipsis investigatio veritatis per se laudabilis atque humana cognitione digna videretur, probe etiam senserunt his rebus ipsam artem inveniendi mirum in modum amplificari, mentisque facultates ad graviora negotia expedienda aptiores reddi. Neque etiam ipsos in hac opinione deceptos fuisse summa incrementa, quibus Analysis ab his temporibus est locupletata, manifesto testantur; maxime enim verisimile videtur hanc scientiam numquam ad tantum perfectionis gradum perventuram fuisse, nisi veteres tantum studium in huiusmodi quaestionibus evolvendis, quae hodie ob sterilitatem tantopere a plerisque contemnuntur, collocavissent. Hincque eo minus dubitare licet, quin his rebus ulterius excolendis etiam in posterum Analysi insignia incrementa afferantur.

1) Confer Commentationes 100 et 152 indicis ENESTROEMIANI, *LEONHARDI EULERI Opera omnia*, series I, vol. 2, p. 59 et 86. R. F.

2. Antiquissimis iam temporibus EUCLIDES multas praeclaras numerorum proprietates collegit, veramque rationem numeros perfectos inveniendi tradidit, ut mirum sit plures recentiores mathematicos in hoc genere tam misere esse hallucinatos. Ex DIOPHANTI autem operibus luculenter apparet tam Graecos quam Arabes plurimum studii in numerorum doctrina excolenda posuisse; quod idem institutum post restauratum in Europa litterarum studium primi Matheseos cultores summa industria sunt prosecuti; hocque ipso viam ad altiores investigationes praeparaverunt. CARTESIUS[1]) certe, cui praecipuae partes promotae Analyseos merito debentur, speculationes numericas minime est aspernatus, atque multo magis in hoc negotio elaboraverunt FERMATIUS et FRENICLIUS, qui etiam acutissimum mathematicum WALLISIUM quasi invitum ad hoc studium excitaverunt, quemadmodum ex commercio epistolico secundo eius operum tomo inserto abunde perspicere licet. Inter eos vero, qui in Germania sese primo ad Algebram applicuerunt, MICHAËL STIFEL imprimis magnam laudem est adeptus, qui temporibus LUTHERI vixit. Hic, ut specimen singularis Analyseos afferret, cui enodando communia Algebrae praecepta non sufficerent, mentionem facit problematis, quo duo numeri ita affecti quaeruntur, ut omnes partes aliquotae minoris numeri simul sumtae maiorem numerum, ac vicissim omnes partes aliquotae maioris numeri simul sumtae minorem numerum producant; talesque numeros invenit 220 et 284. CARTESIUS etiam hoc problema dignum iudicavit, in quo solvendo vires suas exploraret, aliosque insuper huiusmodi numeros elicuit, qui ista proprietate gauderent; atque regulam investigavit, cuius ope plures istiusmodi numeri reperiri possunt, quam SCHOTENIUS in *Exercitationibus Mathematicis* exposuit. Neque vero haec regula est generalis, neque plures quam tres solutiones suppeditare valet[2]).

. . . . . .

8. Hinc inventio numerorum perfectorum nulla laborat difficultate; cum enim numerus perfectus vocetur, qui aequalis summae suarum partium aliquotarum, si numerus perfectus ponatur $= a$, oportebit esse $a = A - a$, ideoque $A = 2a$[3]). Iam numerus perfectus a vel est par vel impar; priori casu

1) In notis Commentationum p. 353 laudatarum (p. 60 et 86, vol. 2 seriei I huius editionis) et in praefatione vol. 2 seriei I, p. XVI, opera CARTESII et aliorum mathematicorum citata sunt. R. F.

2) In manuscripto manu Euleri facto paragraphi 3—7 desunt. Textus in prima editione non ab Eulero conscriptus est. Vide praefationem huius voluminis. R. F.

3) Si $a, b, c, \ldots$ denotant numeros quoscunque integros, litterae maiusculae $A, B, C, \ldots$ expriment summas omnium divisorum numerorum $a, b, c, \ldots$ Eulerus in posterioribus commentationibus hanc notationem per $\int a, \int b, \int c, \ldots$ supplevit. R. F.

ergo factorem habebit 2 eiusque quampiam dignitatem. Sit igitur $a = 2^n b$, erit $A = (2^{n+1} - 1)B$, ideoque $(2^{n+1} - 1)B = 2^{n+1}b$, unde fit $\frac{B}{b} = \frac{2^{n+1}}{2^{n+1}-1}$. Cum igitur fractio $\frac{2^{n+1}}{2^{n+1}-1}$ ad minores numeros reduci nequeat, necesse est, ut sit vel $b = 2^{n+1} - 1$ vel $b = (2^{n+1} - 1)c$. Prius autem fieri nequit, nisi sit $2^{n+1} - 1$ numerus primus, quia summa divisorum esse debet $= 2^{n+1}$, ideoque summa partium aliquotarum $= 1$; quoties vero est $2^{n+1} - 1$ numerus primus, toties posito $b = 2^{n+1} - 1$, erit $B = 2^{n+1}$; hincque numerus perfectus erit $a = 2^n(2^{n+1} - 1)$. Sin autem pro b sumeretur multiplum ipsius $2^{n+1} - 1$, puta $(2^{n+1} - 1)c$, eius pars aliquota foret $2^{n+1} - 1$ et c; unde omnium divisorum summa B certe non minor esset quam $2^{n+1} + c + b$; talis enim foret, si tam c quam $2^{n+1} - 1$ essent numeri primi. Fractio ergo $\frac{B}{b}$ non minor esset futura quam $\frac{2^{n+1} + c + b}{b}$, hoc est quam $\frac{2^{n+1}(1 + c)}{(2^{n+1} - 1)c}$ ob $b = (2^{n+1} - 1)c$. At fractio $\frac{2^{n+1}(1 + c)}{(2^{n+1} - 1)c}$ necessario maior est quam $\frac{2^{n+1}}{2^{n+1} - 1}$, unde pro numero b multiplum ipsius $2^{n+1} - 1$ accipi nequit. Quamobrem alii numeri perfecti pares reperiri non possunt, nisi qui contineantur in formula prius inventa $a = 2^n(2^{n+1} - 1)$ existente $2^{n+1} - 1$ numero primo; haecque est ipsa regula ab EUCLIDE praescripta. Utrum autem praeter hos dentur numeri perfecti impares necne, difficillima est quaestio; neque quisquam adhuc talem numerum invenit, neque nullum omnino dari demonstravit. Sin autem huiusmodi numeri perfecti darentur, ii necessario in hac formula: $(4m + 1)^{4n+1} xx$ continerentur, ubi $4m + 1$ denotat numerum primum et x numerum imparem.

9. Longe difficilius autem reputatur problema de numeris amicabilibus inveniendis, in quo requiruntur bini numeri, quorum alter aequalis sit summae partium aliquotarum alterius. In hoc problemate solvendo etsi SCHOTENIUS summo studio est versatus, tamen plura quam tria huiusmodi numerorum paria non invenit, quae sunt:

220 et 284,
17296 et 18416,
9363584 et 9437056[1]),

atque methodus, qua est usus, ita est comparata, ut vix plures numeri satis-

1) Vide Commentationem 100 indicis ENESTROEMIANI p. 353 laudatam, p. 60, vol. 2 seriei I huius editionis. R. F.

facientes eius ope inveniri queant. Assumsit enim pro numeris amicabilibus has formulas generales $2^n x$ et $2^n yz$, in quibus numeros x, y et z ponit primos, sumtisque successive pro n numeris determinatis tentando investigat casus, quibus numeri primi pro x, y, z substituti quaesito satisfaciant. Nemo autem putabit omnes numeros amicabiles in his formulis contineri, quippe quod non solum a SCHOTENIO non est demonstratum, sed etiam sequentes numeri amicabiles, quos equidem inveni, abunde declarant. Namque praeter tria illa paria modo mox explicando sequentes adeptus sum numeros amicabiles:

$$\begin{aligned} 4 \cdot 5 \cdot 131 \quad &\text{et} \quad 4 \cdot 17 \cdot 43\,, \\ 4 \cdot 5 \cdot 251 \quad &\text{et} \quad 4 \cdot 13 \cdot 107\,, \\ 16 \cdot 17 \cdot 5119 \quad &\text{et} \quad 16 \cdot 239 \cdot 383\,, \\ 4 \cdot 11 \cdot 17 \cdot 263 \quad &\text{et} \quad 4 \cdot 11 \cdot 43 \cdot 107\,, \\ 32 \cdot 37 \cdot 12671 \quad &\text{et} \quad 32 \cdot 227 \cdot 2111\,, \\ 4 \cdot 23 \cdot 827 \quad &\text{et} \quad 4 \cdot 23 \cdot 5 \cdot 137\,[1])\,, \end{aligned}$$

quin etiam numeri exhiberi possunt impares, quod quidem multo magis mirum videri queat, qui praescripta proprietate sint praediti, cuiusmodi sunt:

$$\begin{aligned} 3^2 \cdot 7 \cdot 13 \cdot 5 \cdot 17 \quad &\text{et} \quad 3^2 \cdot 7 \cdot 13 \cdot 107\,, \\ 3^2 \cdot 7^2 \cdot 13 \cdot 5 \cdot 41 \quad &\text{et} \quad 3^2 \cdot 7^2 \cdot 13 \cdot 251\,[2])\,, \end{aligned}$$

ex quibus satis liquet numeros amicabiles multo esse copiosiores, quam numeros perfectos, qui in serie numerorum rarissime occurrunt.

10. Hi autem numeri aliique satisfacientes non difficulter ope modi signandi ante expositi eliciuntur. Sint enim a et b bini numeri amicabiles quicunque, quoniam eorum summae divisorum sunt A et B, summaeque proinde partium aliquotarum $A - a$ et $B - b$; conditio horum numerorum praebet has aequationes: $A - a = b$ et $B - b = a$, unde fit $A = B = a + b$. Ambo ergo numeri amicabiles eandem habent divisorum summam, quae simul summae amborum numerorum est aequalis. Quo autem ad aequationes idoneas solutio perducatur, ponamus numeros amicabiles esse px et qy, existentibus x et y numeris primis[3]), ita ut sit $a = px$ et $b = qy$, eritque $A = P(x + 1)$ et $B = Q(y + 1)$; unde fit:

$$P(x + 1) = Q(y + 1) = px + qy\,.$$

1) Hi numeri amicabiles sunt numeri VIII, IX, XIV, XIX, XVI, IV Commentationis 100 indicis ENESTROEMIANI p. 353 laudatae (p. 60/61, vol. 2 seriei I huius editionis). R. F.

2) Numeri VI et VII eiusdem tabellae. R. F.

3) ubi neque x in p neque y in q contenti sunt. R. F.

Ponatur $P(x+1) = Q(y+1) = PQz$; erit $x+1 = Qz$ et $y+1 = Pz$, seu $x = Qz - 1$ et $y = Pz - 1$. Cum vero esse debeat $PQz = px + qy$, erit valoribus his pro x et y substitutis:

$$PQz = Qpz - p + Pqz - q \ , \quad \text{ideoque} \quad z = \frac{p+q}{Qp + Pq - PQ} \ .$$

Quare, ut formulae assumtae px et qy praebeant numeros amicabiles, esse oportet:

$$x + 1 = \frac{Q(p+q)}{Qp + Pq - PQ} \quad \text{et} \quad y + 1 = \frac{P(p+q)}{Qp + Pq - PQ} \ .$$

Sit n maximus communis divisor numerorum px et qy, ponaturque $p = na$ et $q = nb$[1]), ut sit $P = NA$ et $Q = NB$; et pro numeris amicabilibus has habebimus formulas

$$nax \quad \text{et} \quad nby \ ,$$

in quibus x et y esse debent numeri primi, qui ex his aequationibus definiantur:

$$x + 1 = \frac{nB(a+b)}{Bna + Anb - NAB} \ , \quad y + 1 = \frac{nA(a+b)}{Bna + Anb - NAB} \ .$$

Sumtis ergo pro a et b pro lubitu numeris determinatis erit:

$$x + 1 = \frac{(a+b)\,Bn}{(Ab + Ba)\,n - ABN} \quad \text{et} \quad y + 1 = \frac{(a+b)\,An}{(Ab + Ba)\,n - ABN} \ ,$$

ubi pro n eiusmodi sunt quaerendi numeri, ut x et y non solum fiant numeri integri, sed etiam primi.

11. Cum autem hae formulae nimis sint generales, eas specialiores reddamus; ponamus ergo $a = 1$, eritque $A = 1$, et formulae amicabiles numeros exhibentes fient

$$nx \quad \text{et} \quad nby \ ,$$

pro quibus x et y ex sequentibus aequationibus definiri debebunt

$$\frac{x+1}{B} = y + 1 = \frac{(1+b)\,n}{(B+b)\,n - BN} \ .$$

1) ubi et n ac a et n ac b primi inter se sunt. R. F.

Sit praeterea b numerus primus, ut sit $B = b + 1$; fiet

$$\frac{x+1}{b+1} = y + 1 = \frac{(1+b)n}{(1+2b)n - (1+b)N} = \frac{(1+b)n}{(2n-N)b - (N-n)} .$$

Si iam insuper pro n potestas binarii accipiatur, ut sit $N = 2n - 1$, proveniet

$$\frac{x+1}{b+1} = y + 1 = \frac{(1+b)n}{b - (n-1)} ,$$

quae formulae eos praebebunt numeros amicabiles, qui per methodum SCHOTENII et CARTESII inveniuntur. Ponantur enim successive pro n potestates binarii, erit

$$\text{pro } n = 2: \quad \frac{x+1}{b+1} = y + 1 = \frac{2(1+b)}{b-1} ,$$

$$\text{pro } n = 4: \quad \frac{x+1}{b+1} = y + 1 = \frac{4(1+b)}{b-3} ,$$

$$\text{pro } n = 8: \quad \frac{x+1}{b+1} = y + 1 = \frac{8(1+b)}{b-7} ,$$

etc.

Possunt vero pro n commode accipi alii numeri, ex quibus differentia $2n - N$ apte exprimatur; sic, si capiatur $n = 92$, erit $N = 168$, $2n = 184$, et $N - n = 76$, unde fit:

$$\frac{x+1}{b+1} = y + 1 = \frac{92(1+b)}{16b - 76} = \frac{23(1+b)}{4b - 19} .$$

Hic, si ponatur $b = 5$, erit:

$$\frac{x+1}{6} = y + 1 = \frac{6 \cdot 23}{1} = 138 \quad \text{et} \quad x + 1 = 828 ;$$

opportune autem hinc fit $y = 137$ et $x = 827$, uterque numerus primus, ita ut numeri amicabiles sint:

$$92 \cdot 827 \quad \text{et} \quad 92 \cdot 5 \cdot 137 .$$

Similique modo ex his formulis alios numeros satisfacientes elicere licet.

12. Iam non sit amplius $a = 1$, sed denotet tam a quam b numerum quemcunque primum, eritque $A = a + 1$ et $B = b + 1$; atque formulae

nax et nby dabunt numeros amicabiles, si sequentes aequationes pro x et y praebeant numeros primos:

$$\frac{x+1}{b+1} = \frac{y+1}{a+1} = \frac{n(a+b)}{(2ab+a+b)\,n - (ab+a+b+1)N},$$

seu

$$\frac{x+1}{b+1} = \frac{y+1}{a+1} = \frac{n(a+b)}{(2n-N)\,ab - (N-n)\,(a+b) - N}.$$

Hic iam iterum, si pro n sumatur potestas binarii, ut sit $N = 2n - 1$, erit:

$$\frac{x+1}{b+1} = \frac{y+1}{a+1} = \frac{n(a+b)}{ab - (n-1)\,(a+b) - 2n + 1},$$

quae fractio ante omnia ad numerum integrum est reducenda, idoneis ad hoc pro a et b numeris primis assumendis; sic posito $n = 4$ erit:

$$\frac{x+1}{b+1} = \frac{y+1}{a+1} = \frac{4(a+b)}{ab - 3(a+b) - 7}.$$

Ponatur $b = 5$ et habebitur:

$$\frac{x+1}{6} = \frac{y+1}{a+1} = \frac{4(a+5)}{2a-22} = \frac{2(a+5)}{a-11}.$$

Tententur iam successive varii valores pro a, uti ponatur $a = 13$, erit:

$$\frac{x+1}{6} = \frac{y+1}{14} = 18, \quad \text{unde fit} \quad x = 107 \quad \text{et} \quad y = 251,$$

uterque primus; ita ut numeri amicabiles hinc prodeant $4 \cdot 13 \cdot 107$ et $4 \cdot 5 \cdot 251$. In iisdem formulis ponatur porro $a = 17$, fietque

$$\frac{x+1}{6} = \frac{y+1}{18} = \frac{2 \cdot 22}{6} \quad \text{et} \quad x = 43, \quad y = 131,$$

iterum uterque primus, unde nascuntur numeri amicabiles $4 \cdot 17 \cdot 43$ et $4 \cdot 5 \cdot 131$. Possunt vero etiam pro n assumi, praeter potestates binarii, alii numeri convenientes uti $n = 44$, ut sit $N = 84$ et $N : n = 21 : 11$; unde fit:

$$\frac{x+1}{b+1} = \frac{y+1}{a+1} = \frac{11(a+b)}{ab - 10(a+b) - 21},$$

ubi positis $b = 17$ et $a = 43$, pro x et y numeri primi resultant [107 et 263].

13. Possunt etiam pro a et b producta ex duobus pluribusve numeris primis substitui. Sint enim p et q numeri primi, ac ponatur $a = cp$ et $b = dq$, ut numeri amicabiles sint $ncpx$ et $ndqy$; ob $A = Cp + C$ et $B = Dq + D$ erit:

$$Ab+Ba = (Cd+Dc)pq+Cdq+Dcp \text{ et } AB = CDpq+CDp+CDq+CD,$$

unde fiet:

$$\frac{x+1}{D(q+1)} = \frac{y+1}{C(p+1)} = \frac{n(cp+dq)}{(Cd+Dc)npq+Dcnp+Cdnq-CDNpq-CDNp-CDNq-CDN},$$

ubi pro c et d numeros quoscunque sive primos sive compositos substituere licet. Sit exempli gratia $c = 5$ et $d = 11$, erit $C = 6$ et $D = 12$ numerique amicabiles $5npx$ et $11nqy$, fietque:

$$\frac{x+1}{12(q+1)} = \frac{y+1}{6(p+1)} = \frac{n(5p+11q)}{126npq+60np+66nq-72Npq-72Np-72Nq-72N},$$

seu:

$$\frac{x+1}{2(q+1)} = \frac{y+1}{p+1} = \frac{n(5p+11q)}{(21n-12N)pq-(12N-10n)p-(12N-11n)q-12N},$$

quae expressio ne fiat negativa ob $N > n$, necesse est, ut sit $21n > 12N$ seu $7n > 4N$. Sit igitur primo $n = 2$, erit $N = 3$ atque:

$$\frac{x+1}{2(q+1)} = \frac{y+1}{p+1} = \frac{5p+11q}{3pq-8p-7q-18},$$

ergo $3p > 7$ et $p > 2$. Sit $p = 3$, erit

$$\frac{x+1}{2(q+1)} = \frac{y+1}{4} = \frac{15+11q}{2q-42},$$

unde numerus integer oritur, si $q = 23$, qui vero dat $y = 535$ non primum[1]).

---

1) Manuscriptum: $\frac{x+1}{2(q+1)} = \frac{y+1}{p+1} = \frac{5p+11q}{3pq-8p-14q-18}$, ergo $3p > 14$ et $p > 5$. Sit $p = 7$; erit $\frac{x+1}{2(q+1)} = \frac{y+1}{8} = \frac{35+11q}{7q-74}$, unde numerus integer oritur, si $q = 61$, qui vero dat $y = 15$, non primum. Correxerunt A. M. et R. F.

Quodsi vero ponatur $n = 14$, ut sit $N = 24$, prodibit:

$$\frac{x+1}{2(q+1)} = \frac{y+1}{p+1} = \frac{7(5p+11q)}{(3p-67)q-74p-144},$$

et facto $p = 23$:

$$\frac{x+1}{q+1} = \frac{y+1}{12} = \frac{7(115+11q)}{q-923}.$$

Hoc igitur modo pluribus substitutionibus faciendis plures numeri amicabiles erui poterunt.

14. Quamquam autem hoc modo multo plures inveniri possunt numeri amicabiles, quam methodo a CARTESIO et SCHOTENIO usitata, tamen hic casui plurimum debetur, cum plures positiones plerumque frustra instituantur, antequam pro x et y numeri primi prodeant. Aliam igitur aperiam viam ab hac ita diversam, ut inventio fortuita numerorum primorum non requiratur; quae derivatur ex ea numerorum amicabilium proprietate, qua uterque eandem habet divisorum summam. Facile autem est ope tabulae annexae [1]) huiusmodi numeros, quot libuerit, invenire, quorum summa divisorum sit eadem. Sint igitur v et u duo istiusmodi numeri, quorum utriusque summa divisorum sit eadem $= V$, quodsi ergo esset quoque $V = v + u$, numeri v et u forent amicabiles. Sin autem haec proprietas locum non habeat, tum saepe eorum multipla reperire licebit, quae hac proprietate gaudeant. Ponamus ergo numeros amicabiles esse av et au, erunt utique divisorum summae AV et AV aequales, dummodo a respectu utriusque numeri v et u fuerit primus; reliquum ergo est, ut sit $AV = av + au$ seu $\frac{A}{a} = \frac{v+u}{V}$, ex qua aequatione idoneus valor pro a ita quaeri potest. Reducta fractione $\frac{v+u}{V}$ ad simplicissimam formam necesse est, ut a per eius denominatorem sit divisibilis: scilicet, si fractio $\frac{v+u}{V}$ perducta sit ad $\frac{m}{n}$, ponatur $a = nb$; erit $A = NB$ et $\frac{A}{a} = \frac{NB}{nb} = \frac{m}{n}$, unde fit $\frac{B}{b} = \frac{m}{N}$. Similiter porro b divisibile erit per denominatorem huius fractionis, atque operationem ut ante instituendo, tamdiu continuetur, donec solutio vel perspiciatur vel impossibilis evadat. Notandum

1) Haec tabula deest. Vide tabulam Commentationis 152 indicis ENESTROEMIANI p. 353 laudatae (p. 90—95, vol. 2 seriei I huius editionis), quae tabula congruit cum tabula huic Commentationi annexa. Confer praefationis p. XXXIV. R. F.

vero est pro a non solum multiplum numeri n, sed quoque eius potestatis cuiuspiam assumi posse; ita ut haec investigatio plerumque pluribus modis institui queat.

15. Sumamus ergo pro v et u duos numeros, quorum eadem sit divisorum summa, ponaturque

$$v = 71, \quad u = 5 \cdot 11, \quad \text{erit} \quad V = 72 = 2^3 \cdot 3^2,$$

ita ut numeri amicabiles sint $71a$ et $55a$. Erit ergo

$$\frac{A}{a} = \frac{v+u}{V} = \frac{126}{72} = \frac{7}{4}.$$

Unde patet numerum a factorem habere debere 4 seu 2^2, vel etiam altiorem potestatem ipsius binarii. Sit igitur $a = 2^2 b$, erit

$$A = 7B \text{ et } \frac{A}{a} = \frac{7B}{4b} = \frac{7}{4},$$

ideoque $\frac{B}{b} = \frac{1}{1}$. Hinc igitur obtinetur $b = 1$ ac propterea $a = 4$ prodeuntque numeri amicabiles:

$$4 \cdot 71 = 284 \quad \text{et} \quad 4 \cdot 55 = 220.$$

Neque vero altior binarii potestas pro factore ipsius a assumi potest; posito enim

$$a = 8b, \quad \text{fit} \quad A = 15B \quad \text{et} \quad \frac{A}{a} = \frac{15B}{8b} = \frac{7}{4}, \quad \text{unde} \quad \frac{B}{b} = \frac{14}{15},$$

quae aequatio est impossibilis, cum nullus numerus ad suam divisorum summam rationem maioris inaequalitatis habere possit. Simili modo, si statuatur:

$$v = 5 \cdot 131 = 655, \quad u = 17 \cdot 43 = 731, \quad \text{erit} \quad V = 2^3 \cdot 3^2 \cdot 11,$$

et numeri amicabiles $655a$ et $731a$; debebit autem esse

$$\frac{A}{a} = \frac{v+u}{V} = \frac{1386}{2^3 \cdot 3^2 \cdot 11} = \frac{77}{4 \cdot 11} = \frac{7}{4},$$

unde ut ante fit $a = 4$, ita ut numeri amicabiles hinc reperiantur

$$4 \cdot 655 = 2620 \quad \text{et} \quad 4 \cdot 731 = 2924.$$

Pari modo, cum sequentes numeri eandem divisorum summam habeant:

$$v = 5 \cdot 251 \quad \text{et} \quad u = 13 \cdot 107,$$

erit enim $V = 2^3 \cdot 3^3 \cdot 7$, unde si numeri amicabiles statuantur:

$$5 \cdot 251a = 1255a \quad \text{et} \quad 13 \cdot 107a = 1391a,$$

erit

$$\frac{A}{a} = \frac{2646}{2^3 \cdot 3^3 \cdot 7} = \frac{7}{4},$$

unde iterum fit $a = 4$, ita ut numeri amicabiles sint futuri:

$$5020 \quad \text{et} \quad 5564.$$

16. In his exemplis inventio numeri a nihil habebat difficultatis; sumamus ergo exempla, ubi a plus laboris requirit. Statuatur

$$v = 827 \text{ et } u = 5 \cdot 137, \text{ ex utroque fit } V = 2^2 \cdot 3^2 \cdot 23.$$

Quaeratur ergo multiplicator communis a, ut sit

$$\frac{A}{a} = \frac{v+u}{V} = \frac{1512}{2^2 \cdot 3^2 \cdot 23} = \frac{42}{23}.$$

Cum igitur 23 sit factor ipsius a, ponatur $a = 23b$, erit

$$A = 2^3 \cdot 3B \quad \text{ideoque} \quad \frac{A}{a} = \frac{2^3 \cdot 3B}{23b} = \frac{2 \cdot 3 \cdot 7}{23}, \quad \text{ergo} \quad \frac{B}{b} = \frac{7}{4},$$

unde fit, ut in superioribus exemplis, $b = 4$ et $a = 4 \cdot 23$, ideoque numeri amicabiles erunt:

$$4 \cdot 23 \cdot 827 = 76084 \quad \text{et} \quad 4 \cdot 23 \cdot 5 \cdot 137 = 63020.$$

Deinde cum numeri $17 \cdot 263$ et $43 \cdot 107$ eandem habeant divisorum summam $2^4 \cdot 3^3 \cdot 11$, ponatur $v = 17 \cdot 263 = 4471$ et $u = 43 \cdot 107 = 4601$, erit $V = 2^4 \cdot 3^3 \cdot 11$, atque:

$$\frac{A}{a} = \frac{9072}{2^4 \cdot 3^3 \cdot 11} = \frac{2^4 \cdot 3^4 \cdot 7}{2^4 \cdot 3^3 \cdot 11} = \frac{21}{11}.$$

Ponatur ergo $a = 11b$, $A = 12B$, erit $\frac{A}{a} = \frac{12B}{11b} = \frac{21}{11}$ et $\frac{B}{b} = \frac{7}{4}$,

ideoque $b = 4$, $a = 4 \cdot 11 = 44$; sicque numeri amicabiles erunt:

$$4 \cdot 11 \cdot 17 \cdot 263 = 196724 \quad \text{et} \quad 4 \cdot 11 \cdot 43 \cdot 107 = 202444 .$$

Afferamus aliud exemplum, sitque

$$v = 5 \cdot 17 = 85 , \quad u = 107 , \quad \text{erit} \quad V = 2^2 \cdot 3^3 ,$$

ergo $\frac{A}{a} = \frac{192}{2^2 \cdot 3^3} = \frac{16}{9}$. Ponatur ergo $a = 3^2 b$, $A = 13B$, erit $\frac{A}{a} = \frac{13B}{9b} = \frac{16}{9}$, ergo $\frac{B}{b} = \frac{16}{13}$. Fiat porro $b = 13c$, erit $B = 14C$ et $\frac{B}{b} = \frac{14C}{13c} = \frac{16}{13}$, ergo $\frac{C}{c} = \frac{8}{7}$, unde fit $c = 7$, $b = 7 \cdot 13$ et $a = 3^2 \cdot 7 \cdot 13$. Quare hinc numeri amicabiles nascuntur:

$$3^2 \cdot 7 \cdot 13 \cdot 85 = 69615 \quad \text{et} \quad 3^2 \cdot 7 \cdot 13 \cdot 107 = 87633 .$$

Si posuissemus $a = 3^3 b$ et $A = 2^3 \cdot 5B$, prodiisset $\frac{B}{b} = \frac{6}{5}$, unde foret $b = 5$ et $a = 3^3 \cdot 5$; at cum a ad utrumque numerum v et u debeat esse primus, iste valor ob factorem 5 cum v communem est inutilis.

17. Evolvamus adhuc exemplum ultimum, quoniam in eo quaedam artificia notanda occurrunt, quae in aliis similibus problematis solvendis utilitatem habere possunt. Assumamus ergo pro v et u sequentes numeros, qui communem habent divisorum summam:

$$v = 5 \cdot 41 = 205 \quad \text{et} \quad u = 251 , \quad \text{eritque} \quad V = 2^2 \cdot 3^2 \cdot 7 .$$

Hinc ergo nascentur numeri amicabiles $205a$ et $251a$, si fuerit:

$$\frac{A}{a} = \frac{456}{2^2 \cdot 3^2 \cdot 7} = \frac{38}{3 \cdot 7} .$$

Ergo numerus a divisores habebit 3 et 7. Ponatur ergo: $a = 3b$, $A = 4B$, erit $\frac{B}{b} = \frac{19}{2 \cdot 7}$, quae aequatio iam est impossibilis, cum 19 sit minor quam summa

divisorum ipsius $2 \cdot 7$, quae est 24. Numeri autem multipli ipsius $2 \cdot 7$ multo adhuc minorem tenent rationem ad summas suorum divisorum. Ponamus ergo: $a = 3^2 b$, $A = 13 B$, erit $\frac{B}{b} = \frac{2 \cdot 3 \cdot 19}{7 \cdot 13}$, ideoque b factores habebit 7 et 13. Ponatur nunc: $b = 7c$, $B = 8C$, erit $\frac{C}{c} = \frac{3 \cdot 19}{4 \cdot 13}$, quae aequatio iterum est impossibilis, ob $3 \cdot 19 <$ summa divisorum ipsius $4 \cdot 13$. Quare ulterius tentetur haec positio: $b = 7^2 c$, $B = 3 \cdot 19 \cdot C$, erit $\frac{C}{c} = \frac{14}{13}$, unde fit $c = 13$; hincque $b = 7^2 \cdot 13$ et $a = 3^2 \cdot 7^2 \cdot 13$. Numeri ergo amicabiles ex hac positione orti erunt:

$$3^2 \cdot 7^2 \cdot 13 \cdot 205 = 1175265 \quad \text{atque} \quad 3^2 \cdot 7^2 \cdot 13 \cdot 251 = 1438983 .$$

His igitur praeceptis observatis non difficile erit tam hoc problema de numeris amicabilibus quam alia similia copiosius resolvere.

[FRAGMENTA COMMENTATIONIS CUIUSDAM MAIORIS DE INVENIENDA RELATIONE INTER LATERA TRIANGULORUM QUORUM AREA RATIONALITER EXPRIMI POSSIT ET DE TRIANGULO IN QUO RECTAE EX SINGULIS ANGULIS LATERA OPPOSITA BISECANTES SINT RATIONALES][1]

Commentatio 799 indicis ENESTROEMIANI
Prima editio: Commentationes arithmeticae 2, 1849, p. 648—651
Haec editio congruit cum manuscripto manu Euleri facto academiae scientiarum Petropolitanae relicto

. . . . . .

27. Problemate igitur proposito ita soluto, ut nihil ultra desiderari possit, siquidem solutio tradita latissime patet. Verum praeter animadversiones iam allatas, solutio adhuc alias rationes suppeditat, quarum evolutio non parum ad Analyseos incrementum conferre videtur. In huiusmodi enim quaestionibus non tam solutioni ipsi, quam usui in reliquis Analyseos partibus intentos nos esse convenit.

28. Primum igitur observo, etiamsi in formulis pro lateribus trianguli paragraphi 8 latus a longe alio modo ac reliqua b et c exprimatur, tamen ea inter se ita esse permutabilia, ut nulli prae reliquis ulla praerogativa tribui possit. Ita in casibus paragrapho 12 evolutis videmus latus a esse casu primo 14 cum in casu tertio, qui idem triangulum praebet, numerus 14 lateri c conveniat. Simili modo latera a et c in casibus congruis 2° et 9°, item 4° et 13° inter se permutantur.

29. Haec permutabilitas non obstante expressionum diversitate omni attentione digna videtur. Quae quo clarius agnoscatur, ea non solum in

1) Confer praefationis huius voluminis p. XXXV. R. F.

lateribus triangulorum, quae problemati proposito satisfaciunt, locum habere deprehenditur, sed etiam generatim in omnibus triangulis, quorum area rationaliter exprimi potest; in formulis enim pro huiusmodi triangulis paragrapho 5 datis similis disparitas inter latus a et duo reliqua b et c observatur.

30. Ad hoc ostendendum contemplemur rationem ternorum laterum huiusmodi triangulorum, quorum area est rationalis, quae ita se habet:

$$a:b:c = \frac{(ps \pm qr)\ (pr \mp qs)}{pqrs} : \frac{pp+qq}{pq} : \frac{rr+ss}{rs},$$

ubi latera b et c semper eam inter se tenent rationem, quam duae fractiones huius formae $\frac{ff+gg}{fg}$, a qua tamen fractio $\frac{(ps \pm qr)\ (pr \mp qs)}{pqrs}$ abhorrere videtur. In hac quidem signa ambigua adhibui, quoniam binis lateribus b et c gemini valores lateris a conveniunt.

31. Docendum ergo est etiam latera a et b semper talem rationem inter se tenere, qualis est inter binos numeros formae $\frac{ff+gg}{fg}$. Cum igitur sit

$$a:b = \frac{(ps \pm qr)\ (pr \mp qs)}{rs} : pp+qq,$$

dico eandem proportionem ita exprimi posse, ut sit

$$a:b = \frac{rr+ss}{rs} : \frac{xx+yy}{xy},$$

convenientia enim perspicua reddetur sumendo $x = ps \pm qr$ et $y = pr \mp qs$.

32. Posito enim $x = ps \pm qr$ et $y = pr \mp qs$, erit

$$xx+yy = (pp+qq)(rr+ss) \quad \text{et} \quad xy = (ps \pm qr)(pr \mp qs),$$

unde fit

$$\frac{rr+ss}{rs} : \frac{xx+yy}{xy} = \frac{rr+ss}{rs} : \frac{(pp+qq)\ (rr+ss)}{(ps \pm qr)\ (pr \mp qs)},$$

ideoque

$$\frac{rr+ss}{rs} : \frac{xx+yy}{xy} = \frac{(ps \pm qr)\ (pr \mp qs)}{rs} : pp+qq,$$

quae est ipsa ratio, quam formulae nostrae inter a et b praebuerunt.

33. Quare, si a, b, c sint latera trianguli, cuius area rationalis, inter bina quaeque alia ratio existere nequit, nisi quae intercedat inter binos numeros formae $\frac{ff+gg}{fg}$; ac si duo latera aliam inter se teneant rationem, nullo modo tertium latus inveniri potest, quod cum illis aream rationalem includat.

34. Quomodo ergo hae rationes, quae inter bina latera trianguli aream rationalem habentis intercedere possunt, sint comparatae, et quaenam hinc excludantur, haud abs re erit diligentius inquirere. Considerari ergo primum oportet fractiones in forma $\frac{ff+gg}{fg}$ vel potius in hac $\frac{ff+gg}{2fg}$ contentas.

35. Haec autem fractio $\frac{ff+gg}{2fg}$ pro numeratore habet hypotenusam trianguli rectanguli rationalis, pro .....

.....

49. Huic problemati affine est istud:

Invenire triangulum, in quo rectae ex singulis angulis ita ductae, ut latera opposita bifariam secent, per numeros rationales exprimantur[1]),

quod autem illo ideo difficilius est iudicandum, quoniam non generaliter solvi patitur. Positis a, b, c lateribus trianguli, negotium huc redit, ut tres istae formulae

$$2aa + 2bb - cc, \quad 2aa + 2cc - bb, \quad 2bb + 2cc - aa$$

reddantur quadrata.

50. Si in hunc finem ponatur

$$a = (m+n)p - (m-n)q, \; b = (m-n)p + (m+n)q, \; c = 2mp - 2nq,$$

ut formula prima quadrata evadat, pro reliquis ad quadratum revocari debent hae formulae

$$(3m+n)^2pp - 2(3mm + 8mn - 3nn)pq + (3n-m)^2qq$$

et

$$(3m-n)^2pp - 2(3nn + 8mn - 3mm)pq + (3n+m)^2qq,$$

1) Vide Commentationes 451, 713, 732 et 754 indicis ENESTROEMIANI, ubi idem problema tractatum est; *LEONHARDI EULERI Opera omnia*, vol. 3 seriei I, p. 282, vol. 4 seriei I, p. 290 et 399, hoc vol., p. 28. R. F.

quorum productum sufficiet quadrato coaequasse. Est vero productum

$$(9mm-nn)^2p^4-8mn(27mm+13nn)p^3q-6(3m^4-94mmnn+3n^4)ppqq$$
$$-8mn(27nn+13mm)pq^3+(9nn-mm)^2q^4 .$$

51. Si radix statuatur

$$(9mm-nn)\,pp-\frac{4mn(27mm+13nn)}{9mm-nn}\,pq+(9nn-mm)\,qq ,$$

elicerentur hi valores:

$$p=(mm+nn)(9mm-nn) \quad \text{et} \quad q=2mn(9mm+nn),$$

ex quibus sequentia triangula simpliciora concluduntur[1])

$a=87$,	$a=127$,	$a=207$,	$a=881$,	$a=463$
$b=85$,	$b=131$,	$b=328$,	$b=640$,	$b=142$
$c=68$,	$c=158$,	$c=145$,	$c=569$,	$c=529$.

52. Cum hic invenienda sint tria quadrata, ut binorum summa duplicata, tertio minuta fiat quadratum, simili modo facile solvitur quaestio de tribus quadratis, quorum binorum summa ipsa tertio minuta fiat quadratum[2]). Quo in genere facillima videtur quaestio haec:

Invenire tria quadrata, quorum binorum summa sit quadratum.

Verum tentanti mox patebit huius solutionem multo maioribus difficultatibus implicari. Si enim positis his quadratis aa, bb et cc statuatur

$$b=\frac{2mn}{mm-nn}a \quad \text{et} \quad c=\frac{2pq}{pp-qq}a,$$

ut tam $aa+bb$ quam $aa+cc$ fiant quadrata, superest, ut haec formula

$$mmnn(pp-qq)^2+ppqq(mm-nn)^2$$

aequetur quadrato, cuius tractatio frustra suscipitur.

53. Commodissima autem methodus hoc problema solvendi videtur statuendo $aa=4mnpq$, $b=mp-nq$ et $c=np-mq$, ut fiat

$$aa+bb=(mp+nq)^2 \quad \text{et} \quad aa+cc=(np+mq)^2 .$$

1) Vide exempla p. 34 huius voluminis. R. F.
2) Vide Commentationem 796, hoc volumen, p. 303. R. F.

Quo igitur et $bb + cc$ fiat quadratum, fiat

$$mp - nq = 2(mm - nn)rs = b, \quad np - mq = (mm - nn)(rr - ss) = c$$

eritque

$$bb + cc = (mm - nn)^2 (rr + ss)^2 .$$

Cum autem hinc prodeat

$$p = 2mrs - n(rr - ss) \quad \text{et} \quad q = 2nrs - m(rr - ss),$$

habebitur

$$\frac{aa}{4} = mmnnr^4 - 2mn(mm + nn)r^3 s + 2mmnnrrss + 2mn(mm + nn)rs^3 + mmnns^4 .$$

54. Ad hanc speciali saltem modo resolvendam fingatur:

$$\frac{a}{2} = mnrr - (mm + nn)rs + mnss$$

elicieturque $r = 4mn$ et $s = mm + nn$, unde numeris m et n arbitrio nostro relictis consequimur sequentes numerorum a, b, c valores

$$a = 2mn(3mm - nn)(3nn - mm),$$

$$b = 8mn(mm - nn)(mm + nn),$$

$$c = (mm - nn)(mm - 4mn + nn)(mm + 4mn + nn).$$

55. Hinc simplicissima solutio eruitur sumendo $m = 2$ et $n = 1$, unde resultant hi numeri:

$a = 44$,	$aa = 1936$,	$aa + bb = 59536 = 244^2$,
$b = 240$,	$bb = 57600$,	$aa + cc = 15625 = 125^2$,
$c = 117$,	$cc = 13689$,	$bb + cc = 71289 = 267^2$.

INDEX NOMINUM

QUAE IN TOMIS 2, 3, 4, 5 INSUNT

ADAM, CH. 2 60
AHRENS, W., 2 192, 241, 338
3 472
D'ALEMBERT, J. le R., 2 192, 242
BACHET, C. G., 2 51, 70, 224, 301, 310, 359, 370, 404, 423, 431
3 144, 145, 148, 200, 282, 339, 351, 356
4 65
BÉGUELIN, N. DE, 3 418, 421
4 65, 66, 71, 245, 269, 271
BERNOULLI, DAN., 2 192
3 487
BERNOULLI, JAC., 2 192
BERNOULLI, JOH. I., 3 335
II., 3 335
III., 3 335
BERNOULLI, NIC., 2 192, 249
BHASKARA, 2 600
BILLY, J. DE, 2 431, 434
BRAHMEGUPTA, 2 600
BRANCKER, TH., 2 104
BROUNCKER, 2 432
3 77
BURCKHARDT, J. CHR., 3 398
CAJORI, F., 2 70
CANTOR, M., 2 404, 600
3 147, 488
CARCAVI, 2 38, 310, 359
CARTESIUS, R., 2 59, 60, 86, 98
5 354, 358, 361
CAUCHY, A. L., 3 145
CAYLEY, 2 104
CENTURIO PRUSSICUS, 3 150
COLEBROOKE, H. TH., 2 600
CULLEN, J., 3 420
CUNNINGHAM, A., 3 420
DIGBY, K., 2 2, 310, 359, 432, 466, 486, 558
DIOPHANTEA, arithmetica 3 73
DIOPHANTEA, Analysis 2 297, 359, 372, 400, 404, 414, 427, 429, 454
3 148, 149, 182, 297, 298, 309, 429
4 101, 221, 235, 244
5 28, 48, 61, 82, 95, 102, 116, 148, 157, 284, 303
DIOPHANTEA, methodus 2 70, 223, 224, 399, 428, 522, 576
3 172, 174, 405, 430
4 222
DIOPHANTEUM, problema 2 6, 404, 428, 429, 521
3 172, 173, 180, 405, 416, 429
4 256, 399, 406
DIOPHANTUS, 2 51, 70, 295, 301, 310, 316, 359, 400, 402, 404, 413, 423, 426, 429, 430, 431, 460, 533, 574
3 144, 148, 180, 200, 282, 339, 351, 356
4 96
5 19, 64, 354
EISENSTEIN, G., 5, 250
ENESTROEM, G., 2 12, 38, 104, 192, 258, 377, 558
3 77, 147
ENESTROEMIANUS, index Commentationum Euleri, passim
EUKLID 2 39, 295, 494, 533
3 3, 441
EULER, J. ALBR., 3 46, 61, 173, 458, 463
EULER, L., 2 1, 3 (*Commentatio indicis Enestroemiani* 134), 4 (*Commentationes* 54, 134, 262, 271), 5 (134, 164, 262), 14 (*Algebra*), 33 (26, 134, 262), 59 (152, 798), 64 (54), 67 (54, 262), 69 (242), 73

(26), 82 (262), 86 (100, 798), 98 (100), 103 (100), 104, 115 (256), 141 (243), 163 (191, 394, *Introd.*), 191 (158, 175, 191, 243, 244, *Introd.*), 192 (*Epistola ad Goldbachium et N. Bernoulli*), 194 (134, 228, 241, 242, 256, 262, 271, 272, 598, 610), 206 (242, 598), 207 (271), 217 (552), 224 (98), 241 (243), 242 (152, 243, 244, *Epistola ad Goldbachium*), 249 (*Epistola ad Goldbachium et N. Bernoulli*), 253 (244), 254 (158, 394, *Introd.*), 255 (*Introd.*), 289 (*Algebra*), 295 (*Epistola ad Goldbachium*), 296 (241), 297 (158, 191), 307 (134), 310 (134), 311 (134, 241), 312 (134, 242), 328 (228, *Epistola ad Goldbachium*), 330 (228), 331 (134), 334 (*Inst. calc. diff.*), 347 (54, 134, 242, 262), 358 (134, 228, 241) 360 (*Epistola ad Goldbachium*), 363 (134), 370 (445), 373 (152, 175, 244), 390 (175, 243), 399 (*Algebra*), 423 (*Algebra*), 428 (*Algebra*), 439 (272), 460 (228, 241, 242), 461 (586), 462 (228), 483 (228), 485 (228, 241), 486 (134, 228, 241, 164), 498 (242), 510 (54, 134), 513 (134), 514 (134, 242), 518 (134, 228, 241), 519 (427), 520 (*Epistola ad G. F. Müller*), 531 (564), 532 (270), 534 (54, 134, 262), 545 (262), 554 (26), 558 (*Algebra*, 164, 255, 256), 566 (228), 573 (134), 574 (241, 262), 575 (256, 241, 164), 576 (29), 577 (29), 582 (29), 584 (*Introd.*, 453), 585 (29), 601 (164)

3 1 (369, 461, 467, 498, 708a), 3 (26), 4, (72, *Epistola ad Goldbachium*), 6 (134, 228, 241), 7 (*Epistola ad Goldbachium*, 71, 228, *Introd.*), 22 (*Epistola ad Goldbachium*), 73 (*Epistola ad Goldbachium*, 29, 279, 452, 454, 559, *Algebra*), 75 (29, 279), 76 (279, 452), 77 (29, 281), 78 (71), 90 (71), 92 (281), 101 (281), 110 (29, *Algebra*), 112 (283, 461, 467, 498, 708a), 114 (228, 241), 115 (228, 256), 132 (158, 191, *Introd.*), 144 (*Epistola ad Goldbachium*), 145 (242), 146 (*Algebra*), 157 (*Algebra*), 173 (270, 523), 183 (164, 256), 184 (134), 185 (*Algebra*), 189 (228), 198 (*Algebra*), 212 (98), 217 (776), 218 (242), 221 (242), 222 (228), 224 (256, 272), 228 (272), 229 (242), 232 (242), 233 (242), 234 (242), 235 (242), 237 (271), 239 (242, 464, 475), 240 (262, 271), 246 (54, 134, 262, 271), 248 (262), 252 (271), 255 (242), 261 (242), 262 (242, 552), 263 (242), 265 (228, 445), 266 (134, 241, 242), 271 (272), 272 (272), 274 (256, 445), 277 (164), 282 (167, 713, 732, 748, 754, 799), 287 (*Algebra*), 297 (29, 279, 323, 454, 559), 298 (*Algebra*), 302 (*Introd.*), 306 (323), 309 (29, 279, 323, *Algebra*), 310 (323), 312 (452), 319 (323), 324 (452), 327 (452), 334 (323), 336 (134, 26), 342 (*Algebra*), 351 (167), 359 (283, 369, 461, 498, 708a), 403 (498, 699), 408 (*Algebra*), 418 (228, 283, 369, 461, 467, 708a), 420 (467, 719, 725), 421 (283, 369, 461, 467, 498, 708, 715, 718, 719, 725), 422 (228), 429 (253), 440 (98), 453 (270, 427), 455 (*Algebra*), 458 (270), 463 (523), 472 (244), 480 (*Algebra*), 481 (175, 243, 244), 483 (244, 541), 484 (*Algebra*), 485 (*Introd.*), 486 (153), 497 (242), 500 (242), 501 (134), 502 (134, 242, 262), 504 (228, 241, 242), 507 (242, 449), 508 (228, 241, 242), 512 (164), 513 (552), 520 (242), 521 (242, 552), 522 (262), 525 (552), 526 (228, 241), 534 (134, 262), 540 (449), 543 (271, 449).

4 6 (241, 467), 16 (134, 262), 25 (54, 134, 262), 26 (26), 38 (449), 42 (242), 55 (552), 60 (271), 65 (242), 76 (323), 78 (241), 80 (256), 91 (449), 93 (*Algebra*), 98 (158), 109 (271), 116 (242), 117 (445), 141 (71), 144 (*Inst. calc. diff.*), 157 (*Inst. calc. diff*), 161 (*Introd.*), 170 (557), 173 (241), 174 (256), 177 (164), 191 (164), 195 (164), 197 (164, 228, 256, 272, 598), 199 (242), 200 (242), 235 (98, 755), 238 (323), 245

(467, 498), 248 (228), 256 (*Algebra*), 269 (498), 271 (708a), 274 (699), 277 (498), 278 (715), 303 (708), 321 (699, 719), 329 (428), 331 (428), 352 (715), 353 (715), 360 (708, 715, 718), 364 (715), 395 (708, 719), 396 (708, 715), 399 (713), 406 (29, 279).
5 28 (451, 713, 732), 35 (696), 48 (*Algebra*, 702), 53 (702), 61 (560), 73 (279), 77 (763), 82 (769), 86 (769), 96 (515), 116 (773), 117 (405), 128 (405), 135 (428, 716), 136 (716), 164 (98), 165 (560, 763), 193 (152, 175), 196 (175), 202 (271), 207 (271), 214 (271), 220 (134, 262), 222 (241), 225 (134, 164), 228 (242), 241 (598, 610), 258 (134), 274 (228), 279 (164, 256), 285 (255), 300 (405), 301 (774), 302 (405), 353 (100, 152), 355 (100), 361 (152), 368 (451, 713, 732, 754), 369 (796).

FERMAT, P. DE, **2** 1, 2, 11, 12, 33, 34, 38, 51, 60, 62, 63, 64, 70, 74, 223, 224, 295, 296, 310, 328, 329, 330, 339, 358, 359, 370, 373, 431, 460, 461, 466, 486, 510, 533, 557, 558, 574, 580
3 1, 3, 5, 6, 112, 114, 132, 144, 145, 180, 221, 238, 275, 336, 351, 356, 425
4 26, 65, 96, 116, 125, 127, 173, 330
5 64, 354

FERMATIANA, aequatio, **2** 11, 580

FERMATIANUM, problema **3** 5, 77
4 390
5 77, 86

FERMATIANUM, theorema **2** 4, 34, 39, 63, 328, 373, 518, 534, 554, 555, 557
3 218, 231, 246, 265, 266, 275, 336, 337, 497, 508
4 25, 26, 117, 124, 125, 127, 128, 130, 133, 135
5 214, 310

FERMAT, S., **3** 144, 351

FRÉNICLE, B., DE B., **2** 34, 38, 310, 432
3 212, 336, 440
5 354

FROBENIUS, G., **3** 337

FUSS, N., **2** 89, 241
3 13, 421
4 2, 14, 17, 271

FUSS, P. H., **2** 89, 162, 192, 241, 242, 249, 295, 328, 338, 358, 360, 369, 530, 600
3 4, 7, 13, 22, 73, 144, 472
4 2, 14, 17

GAUSS, G. FR., **2** 192, 194
3 145, 238, 250, 252, 276, 313, 512
4 91, 186, 193, 214, 277
5 258

GERHARDT, C. J., **4** 96

GLAISHER, J. W. L., **2** 104

GOLDBACH, CHR., **2** 192, 242, 245, 249, 295, 328, 358, 360, 369, 390, 530, 558, 600
3 4, 7, 16, 22, 23, 73, 144

GRUBE, F., **4** 269

HANKEL, H., **2** 404, 600

HEATH, T. L., **2** 404, 432
3 180

HEIBERG, J. L., **2** 39, 494
3 3, 441

HENRY, CH., **2** 2
3 336

HUNRATH, K., **2** 61

JACOBI, C. G. J., **2** 192, 241, 338
3 52, 472
4 129

JAMBLICHUS, **2** 60

KONEN, H., **3** 73, 77

KRAFFT, G. W., **2** 86

KRONECKER, L., **2** 217

KRÜGER, J. G., **2** 104
3 5

LAGRANGE, J. L., **2** 194, 370, 485, 603
3 145, 218, 221, 232, 234, 238, 276, 421
4 65, 91, 116, 125, 163, 168, 189, 191, 195, 197, 198, 207, 214
5 61, 64, 77

LAHIRE, PH. DE, **2** 18

LAMBERT, J. H., **3** 252

LEGENDRE, A. M., 3 109, 130, 337
LEHMER, D. N., 3 398
LEIBNIZ, G., 2 34, 257
4 96
LEIBNIZIANA, series, 3 488
4 148, 153, 156
LUCAS, E., 3 336
LUTHER, M., 5 354
MAHNKE, D., 2 34, 257
MERSENNE, M., 2 60, 310
3 336
MÜLLER, G. F., 2 520
NAUDÉ, PH. minor, 2 178, 183, 188, 254, 255, 256, 272
NESSELMANN, G. H. F., 2 404
NEWTON, I., 2 510
NIKOMACHUS, 2 60
OLDENBURG, H., 4 96
PASCAL, BL., 2 310
PELL, J., 2 12, 104
3 1, 74, 77, 306, 311, 313
PELLIANA, aequatio, 2 11, 12
PELLIANA, formula, 4 238
PELLIANUM, problema, 3 73, 77, 97, 98, 99, 102, 103, 325, 334
4 76, 90, 410
PISANO, LEONARDO, 2 258
PISTELLI, H., 2 60
PYTHAGOREI, 2 60
RAHN, J. H., 2 104
ROBERVAL, G. P. DE, 2 70
ROLLE, M., 2 70
RUDOLFF, CHR., 2 28, 258
SAUVEUR, J., 2 18
SCHAEWEN, P. v., 2 432, 434
3 282
SCHLESINGER, L., 2 192
SCHOOTEN, F. v., 2 59, 60, 87, 98, 258, 377, 431
3 416
5 354, 358, 361
SERRET, J. A., 2 194, 370
3 218
4 91, 163
SMITH, J., 2 104
STÄCKEL, P., 2 192, 241, 242, 338
3 472
STIFEL, M., 2 28, 86, 258
5 354
STOKES, 2 104
TANNERY, P., 2 2, 60, 70, 301, 310, 402, 404, 413, 423, 426, 431
3 148, 200, 336, 339, 351, 356
THOMSON, 2 104
VACCA, G., 2 34
VIETA, FR., 2 431, 434
WALLIS, J., 2 2, 13, 104, 310, 377, 432, 466
3 1, 3, 7, 77, 78, 316
4 136
5 354
WARING, E., 4 91
WERTHEIM, G., 2 38, 70, 104, 404
WILBRECHT, A., 5 303, 330, 337, 340
WILSONIANUM, theorema, 4 91
WOLF, CHR., 2 3