Neue Beweise über die Teiler von Zahlen der Form $xx + nyy$*

Leonhard Euler

Nachdem ich neulich die Entdeckungen des illustren Lagrange über die Teiler von Zahlen der Form $xx + nyy$ durchdacht hatte und mit meinen Beobachtungen, welche ich einst zumeist mit Induktion gefunden hatte, zusammengeführt hatte, welche natürlich daher eine nicht unwesentliche Bestätigung erhalten haben, habe ich nicht bezweifelt, dass sie bald auch vollkommene Beweise, die noch vermisst werden, verheißen. Ich vertraute natürlich auf den Scharfsinn des sehr geistreichen Herrn Lagrange, mit welchem er schon viele Beweise von dieser Art mit so glücklichem Erfolg erbracht hat. Nachdem ich aber alle Umstände, auf welche bei dieser Untersuchung zu achten ist, genauer betrachtet hatte, ist es mir auch gelungen, die wesentlichen Bausteine, auf welche diese ersehnten Beweise gestützt sind, zu erkennen, welche ich also hier darzulegen beschlossen habe.

Theorem 1

§1 *Wenn alle Quadratzahlen durch irgendeine Primzahl P (außer zwei, deren Natur natürlich per se offensichtlich ist) geteilt werden, ist die Anzahl aller Teilerreste, die daraus resultieren können, immer* $= \frac{1}{2}(P-1)$.

*Originaltitel: "Novae demonstrationes circa divisores numerorum formae $xx + nyy$", zuerst publiziert in: *Nova Acta Academiae Scientiarum Imperialis Petropolitanae, Band 1* (1787, geschrieben 1775): pp. 47 – 74, Nachdruck in: Opera Omnia: Serie 1, Band 4, pp. 197 – 220, Eneström Nummer E610, übersetzt von: Alexander Aycock für den "Euler-Kreis Mainz".

BEWEIS

Alle durch die vorgelegte Primzahl P nicht teilbaren Zahlen sind in einer dieser Formeln enthalten: $\lambda P \pm 1$, $\lambda P \pm 2$, $\lambda P \pm 3$, $\lambda P \pm 4$, $\cdots$, $\lambda P \pm \omega$, in der letzten derer $\omega = \frac{1}{2}(P-1)$ ist, die Anzahl welcher Formeln also $\frac{1}{2}(P-1)$ ist. Aber nun, wenn die Quadrate jeder dieser Formeln, wie beispielsweise $(\lambda P \pm a)^2$, durch die Zahl P geteilt werden, wird derselbe Rest zurückbleiben wie der, der aus dem Quadrat aa resultiert, woher, weil a die Zahl $\omega = \frac{1}{2}(P-1)$ nicht übersteigt, es offenkundig ist, dass die Anzahl der Reste, die aus der Teilung durch die Primzahl P entspringen können, nicht größer sein kann als $\frac{1}{2}(P-1)$. Und all diese Reste entstehen aus den Quadraten 1, 4, 9, 16, $\cdots$, $\omega\omega$, während $\omega = \frac{1}{2}(P-1)$ ist, welche, solange sie kleiner sind als P, selbst die Reste sein werden; wenn sie aber größere Waren, können sie durch Teilung unter P herabgesenkt werden, sodass alle kleiner werden als P, wie aus der Natur der Teilung ja offensichtlich ist. Es ist also übrig, dass bewiesen wird, dass die Anzahl dieser Reste nicht kleiner sein kann als $\frac{1}{2}(P-1)$, was daher klar werden wird, wenn wir gezeigt haben werden, dass alle Quadrate keine verschiedenen Reste größer als $\omega\omega$ erzeugen. Zu diesem Zweck seien aa und bb zwei Quadrate von dieser Art, wenn welche durch P geteilt denselben Rest lieferten, wäre deren Differenz $bb - aa$ durch P teilbar; weil also P eine Primzahl ist, müsste entweder $b + a$ oder $b - a$ durch P teilbar sein, weil aber so a wie b nicht $\omega = \frac{1}{2}(P-1)$ übersteigen, ist es offenkundig, dass so $b + a$ wie $b - a$ Zahlen kleiner als P sind, und daher gewiss nicht durch P geteilt werden können; daher ist es ersichtlich, dass die Anzahl der verschiedenen Reste auch nicht kleiner sein kann als $\frac{1}{2}(P-1)$. Und so ist bewiesen, dass die Anzahl aller Teilungsreste $= \frac{1}{2}(P-1)$ ist.

KOROLLAR 1

§2 Wenn daher also die lateinischen Buchstaben a, b, c, d etc. alle Reste bezeichnen, die aus der Teilung der Quadratzahlen durch die Primzahl P resultieren können, wird deren Menge immer $\frac{1}{2}(P-1)$ sein, und in ihnen werden immer die Quadrate 1, 4, 9, 16 etc. auftreten, sofern sie kleiner sind als die Zahl P, die übrigen entstehen hingegen aus den Quadraten größer als P.

Korollar 2

§3 Weil alle Reste a, b, c, d etc. kleiner sind als der Teiler P und deren Anzahl nur $\frac{1}{2}(P-1)$ ist, während die Menge aller Zahlen kleiner als P natürlich $P-1$ ist, bildet nur die Hälfte dieser Reste eine Klasse, die übrigen Zahlen hingegen, deren Menge auch $\frac{1}{2}(P-1)$ ist, werden aus dieser Klasse vollkommen ausgeschlossen, welche wir also mit den griechischen Buchstaben α, β, γ, δ etc. bezeichnen und *Nicht-Reste* nennen, sodass für jedwede Primzahl alle Zahlen kleiner als selbige zu zwei Klassen zu rechnen sind, von denen die eine alle Reste a, b, c, d etc. enthält, die andere hingegen die Nicht-Reste α, β, γ, δ etc. Aber in jeder der beiden Klassen wird immer dieselbe Anzahl an Zahlen enthalten sein, deren Menge $\frac{1}{2}(P-1)$ ist.

Korollar 3

§3 Wenn also a irgendeinen Rest bezeichnet, werden alle Quadratzahlen in dieser Formel enthalten sein: $\lambda P + a$, und immer wird sich der Koeffizient λ so annehmen lassen, dass diese Formel ein Quadrat wird, andernfalls, wenn α irgendeinen Nicht-Rest bezeichnet, wird diese Formel $\lambda P + \alpha$ niemals ein Quadrat werden können, welche Zahlen auch immer anstelle von λ angenommen werden.

Scholion

§5 Nun habe ich vor einiger Zeit viele außerordentliche Eigenschaften so der Reste wie der Nicht-Reste bewiesen, welche sie alle hier zu wiederholen überflüssig wäre; aber es wird förderlich sein, sich hier zumindest der folgenden erinnert zu haben:

1. Dass die Produkte aus zwei Resten, wie beispielsweise ab, immer auch in der Klasse der Reste auftreten, nachdem sie natürlich durch Teilung durch P auf kleinste Werte reduziert worden sind, woher klar ist, dass alle Potenzen eines jeden Restes in derselben Klasse gefunden werden müssen.

2. Wenn aber die Reste mit einem Nicht-Rest multipliziert werden, werden die Produkte immer in der Klasse der Nicht-Reste gefunden werden;

daher ist klar, dass aus einem einzigen Nicht-Rest α alle übrigen gefunden werden können, während natürlich die Reste a, b, c, d etc. mit α multipliziert werden.

3. Wenn aber zwei Nicht-Reste, wie α und β, miteinander multipliziert werden, fallen die Produkte $\alpha\beta$ in die Klasse der Nicht-Reste, die Produkte aus drei Nicht-Resten hingegen werden wiederum Nicht-Reste, aus vieren aber erneut Reste, und so weiter.

4. Aber dann, wenn ein gewisser Rest a durch einen anderen Rest b geteilt wird, wird auch der Quotient in der Klasse der Reste gefunden werden, wenn freilich a durch b geteilt werden kann; wenn er aber nicht geteilt werden kann, wird immer ein solches Vielfaches von P gegeben sein, welches μP sei, dass die Formel $\mu P + a$ eine Teilung durch b zulässt; und aus in diesem Fall wird der Quotient immer in der Klasse der Reste gefunden werden.

THEOREM 2

§6 *Während a irgendeinen Rest bezeichnet, welcher aus der Teilung der Quadrate durch eine Primzahl P entspringen kann, wenn die Zahl n in der Formel $\lambda P - a$ enthalten ist, werden immer solche Zahlen x und y angegeben werden können, dass die Form $xx + nyy$ eine Teilung durch die Primzahl P zulässt.*

BEWEIS

Wir wollen festlegen, dass die Primzahl P ein Teiler einer in der Form $xx + nyy$ enthaltenen Zahl ist, sodass $\mu P = xx + nyy$ ist; also wird $nyy = \mu P - xx$ sein. Aber das Quadrat xx ist in der Form $\lambda P + a$ enthalten, nach Einsetzen von welchem $nyy = (\mu - \lambda)P - a = \nu P - a$ und daher

$$n = \frac{\nu P - a}{yy}$$

werden wird. Weil aber yy ein Quadrat ist, ist es in der Klasse der Reste enthalten, als logische Konsequenz wird auch $\frac{a}{yy}$ ein Rest sein, und kann daher in a erfasst werden, woher wir in ganzen Zahlen $n = \lambda P - a$ haben werden. Daher folgt also umgekehrt, sooft n eine in der Form $\lambda P - a$ enthaltene Zahl war, dass dann immer eine Zahl der Form $xx + nyy$ dargeboten werden kann, die durch die Primzahl P teilbar ist.

Korollar 1

§7 Daher wird also auch eingesehen, wenn α irgendeinen Nicht-Rest bezüglich der Primzahl P bezeichnet, und n eine in dieser Form $\mu P - \alpha$ enthaltene Zahl war, dass dann diese Primzahl P in keiner Weise ein Teiler einer in der Form $xx + nyy$ enthaltenen Zahl sein kann.

Korollar 2

§8 Weil also gänzlich alle Zahlen entweder in der Form $\mu P - a$ oder $\mu P - \alpha$ enthalten sind, lernen wir daraus, dass für jedwede Primzahl P alle Zahlen in zwei Klassen aufgeteilt werden, von welchen beide gleich viele Zahlen enthalten, weil die Menge der Werte von a dieselbe ist wie die der Werte von α, die eine welcher Klassen alle Zahlen n enthalten wird, woher die Formel $xx + nyy$ den Teiler P erhalten kann; aber die andere Klasse wird die übrigen Teiler beinhalten, wenn welche für n angenommen werden, kann die Formel $xx + nyy$ in keiner Weise durch P teilbar sein.

Scholion 1

§9 Damit diese Dinge in einem Beispiel deutlicher werden, wollen wir die Primzahl 13 betrachten, für welche diese Reste gefunden werden: 1, 4, 9, 3, 12, 10, die Nicht-Reste sind hingegen: 2, 5, 6, 7, 8, 11; und damit die Form $xx + nyy$ durch 13 teilbar sein kann, muss die Zahl n in einer der sechs folgenden Formeln enthalten sein:

$$13\lambda - 1, \quad 13\lambda - 4, \quad 13\lambda - 9, \quad 13\lambda - 3, \quad 13\lambda - 12, \quad 13\lambda - 10$$

enthalten sein, und so werden die geeigneten Werte für diese Zahl n in natürlichen Zahlen aufsteigend angeordnet die folgenden sein:

$$1,\ 3,\ 4,\ 9,\ 10,\ 12,\ 14,\ 16,\ 17,\ 22,\ 23,\ 25,\ 27,\ 29,\ 30,\ 35,\ 36,\ 38,\ 40$$

$$42,\ 43,\ 48,\ 49,\ 51,\ 53,\ 55,\ 56,\ 61,\ 62,\ 64,\ 66,\ 68,\ 69,\ 74,\ 75,\ 77,\ 79,$$

$$81,\ 82,\ 87,\ 88,\ 90,\ 92,\ 94,\ 95,\ 100,$$

deren Anzahl bis hin zur Zahl 100 hier 46 ist. Also werden die übrigen Zahlen, die den Teiler 13 von der Formel $xx + nyy$ vollkommen auszuschließen, nach

Streichen derjenigen, die selbst durch 13 teilbar sind, der Reihe nach diese sein:

$$2, 5, 6, 7, 8, 11, 15, 18, 19, 20, 21, 24, 28, 31, 32, 33, 34, 37, 41, 44, 45,$$
$$46, 47, 50, 54, 57, 58, 59, 60, 63, 67, 70, 71, 72, 73, 76, 80, 83, 84, 85, 86,$$
$$89, 93, 96, 97, 98, 99,$$

deren Anzahl 47 ist, und daher der ersten nicht ganz gleich. Aber der Grund, warum wir die Vielfachen von 13 ausgeschlossen haben, ist, dass über die Formel $xx + 13vyy$ die Frage, ob die den Teiler 13 erhält, überhaupt nicht bestehen kann, weil offensichtlich die Zahl x durch 13 teilbar sein müsste.

SCHOLION 2

§10 Weil das Wesen unseres Beweises deutlicher in Beispielen erkannt wird, wollen wir eine andere Primzahl 19 betrachten, für welche die neun Reste sind: 1, 4, 9, 16, 6, 17, 11, 7, 5, die neun Nicht-Reste sind hingegen: 2, 3, 8, 10, 12, 13, 14, 15, 18. Daher wird also die Formel $xx + nyy$ den Teiler 19 erhalten können, wenn die Zahl n in der folgenden Formel enthalten ist:

$$n = 19\lambda - (1, 4, 9, 16, 6, 17, 11, 7, 5);$$

wenn aber n in der folgenden Formel enthalten ist:

$$n = 19\lambda - (2, 3, 8, 10, 12, 13, 14, 15, 18),$$

dann wird keine Zahl der Form $xx + nyy$ durch 19 geteilt werden können. Also werden die geeigneten Werte für n bis hin zu hundert der Reihe nach sein:

$$2, 3, 8, 10, 12, 13, 14, 15, 18, 21, 22, 27, 29, 31, 32, 33, 34, 37, 40,$$
$$41, 46, 48, 50, 51, 52, 53, 56, 59, 60, 65, 67, 69, 70, 71, 72, 75, 78,$$
$$79, 84, 86, 88, 89, 90, 91, 94, 97, 98,$$

deren Menge 47 ist. Also werden die Zahlen für dieses Ziel geeigneten Zahlen, nach Ausschluss der Vielfachen von 19, diese an der Zahl 48 sein:

$$1,\ 4,\ 5,\ 6,\ 7,\ 9,\ 11,\ 16,\ 17,\ 20,\ 23,\ 24,\ 25,\ 26,\ 28,\ 30,\ 35,\ 36,\ 39,\ 42,$$
$$43,\ 44,\ 45,\ 47,\ 49,\ 54,\ 55,\ 58,\ 61,\ 61,\ 62,\ 63,\ 64,\ 66,\ 68,\ 73,\ 74,\ 77,\ 80,$$
$$81,\ 82,\ 83,\ 85,\ 87,\ 92,\ 93,\ 96,\ 99, 100.$$

SCHOLION 3

§11 Damit aber leichter verstanden wird, wie in jedem Fall, wo die Zahl einen geeigneten Wert hat, die Formel $xx+nyy$ durch die Primzahl P teilbar gemacht wird, bemerke man, dass es immer passieren kann, während für x und y Zahlen nicht größer als $\frac{1}{2}(P-1)$ angenommen werden, und daher die einer dieser Zahlen y nach Belieben angenommen werden kann. Es sei also $y=1$, sodass man diese Formel hat: $xx+n$, und als Rest der Zahl n entstehe r; dann suche man also für xx das Quadrat, welchem der Rest $P-r$ zukomme, und offenkundig wird die Summe $xx+n$ durch P teilbar sein. Es ist aber ersichtlich, dass dies immer geschehen kann, weil $n=\lambda P-a$ ist, woher der Rest $r=P-a$ wird, und daher $P-r=a$, und so muss für xx das Quadrat genommen werden, welchem der Rest a zukomme. So nehme man nach Setzen von $P=13$ für n nach Belieben einen geeigneten Wert aus den oben gefundenen, wie beispielsweise $n=82$, und man suche x so, dass die Form $xx+82$ durch 13 teilbar wird. Hier sei aber der Rest $r=4$, und daher $P-r=9$; es wird also $x=3$ und die Formel 3^2+82 kann durch 13 geteilt werden. Wenn man für den Teiler 19 in gleicher Weise $n=88$ nimmt, entspringt daraus der Rest $r=12$, und daher $P-r=7$; aber das Quadrat, welches durch 19 geteilt 7 zurücklässt, ist 64, und so geht die Formel 8^2+88 durch 19 teilbar hervor. Und daher kann leichter und gefälliger der Beweis unseres Lehrsatzes abgeleitet werden.

EIN ANDERER BEWEIS VON THEOREM 2

§12 Natürlich kann gezeigt werden, wenn $n=\lambda P-a$ war, dass dann immer eine Zahl x gegeben ist, dass die Formel $xx+n$ eine Teilung zulässt: Denn man nehme für xx nur das Quadrat, welches durch P geteilt a zurücklässt, welches also von der Form $\mu P+a$ sein wird; daher wird wegen $n=\lambda P-a$ die Formel $xx+n=(\mu+\lambda)P$ sein, und daher natürlich durch die Zahl P teilbar.

SCHOLION 1

§13 Weil also für jede beliebige Primzahl P leicht alle Zahlen n dargeboten werden können, für welche die Form $xx + nyy$ eine Teilung durch P zulassen kann, weil wir ja, während a alle aus der Teilung der Quadrate durch P zu entspringenden Reste bezeichnet, $n = \lambda P - a$ gefunden haben, ist es offensichtlich, dass für n auch unendlich viele negative Werte gegeben sind, die entspringen, wenn für λ auch negative Zahlen angenommen werden. Deswegen wird es nicht unnütz sein, für Primzahlen einfachere Formeln darzubieten, die alle geeigneten Werte der Zahl n enthalten, für welche die Form $xx + nyy$ durch die Primzahl P teilbar gemacht werden kann, welche wir also hier beifügen wollen.

P	n		
3	3λ	$-$	1
5	5λ	$-$	$(1,4)$
7	7λ	$-$	$(1,4,2)$
11	11λ	$-$	$(1,4,9,5,3)$
13	13λ	$-$	$(1,4,9,3,12,10)$
17	17λ	$-$	$(1,4,9,16,8,8,2,15,13)$
19	19λ	$-$	$(1,4,9,16,6,17,11,7,5)$
23	23λ	$-$	$(1,4,9,16,2,13,3,18,12,8,6)$
29	29λ	$-$	$(1,4,9,16,25,7,20,6,23,13,5,28,24,22)$
31	31λ	$-$	$(1,4,9,16,25,5,18,2,19,7,28,20,14,10,8)$
37	37λ	$-$	$(1,4,9,16,25,36,12,27,7,26,10,33,21,11,3,34,30,28)$
41	41λ	$-$	$(1,4,9,16,25,36,8,23,40,18,39,21,5,32,20,10,2,37,33,31)$
43	43λ	$-$	$(1,4,9,16,25,36,6,21,38,14,35,15,40,24,10,41,31,23,17,13,11)$
47	47λ	$-$	$(1,4,9,16,25,36,2,17,34,6,27,3,28,8,37,21,7,42,32,24,18,14,12)$

KOROLLAR

§14 Wenn also n eine negative Zahl war, wie etwa $n = -m$, wird für negativ genommenes λ auch $m = \lambda P + a$ sein, weil welche Form alle Quadratzahlen enthält, welche Primzahl auch immer für P angenommen wird, ist es klar, wenn m eine Quadratzahl war, natürlich $m = k^2$, dass die Zahlen der Form $xx - kkyy$ durch gänzlich alle Primzahlen teilbar sein können, in welchem Fall also keine Primzahlen ausgeschlossen werden, was per se offenkundig ist, weil ja die Formel $xx - kkyy$ im Allgemeinen die Faktoren $x + ky$ und $x - ky$

hat, von welchen beide durch alle Primzahlen teilbar gemacht werden können, was sich in keinem anderen Fall bewerkstelligen lässt.

SCHOLION 2

§15 So wie bezüglich jedweder Primzahl P alle Zahlen in zwei Klassen aufgeteilt werden, von denen die eine die geeigneten Werte des Buchstaben n enthält, dass die Formel $xx + nyy$ durch die Primzahl P teilbar gemacht werden kann, die andere hingegen die Zahlen, welche eine solche Teilung verweigern, und außerdem die Menge der in jeder der beiden Klassen enthaltenen Zahlen als dieselbe entdeckt wird, so müssen umgekehrt für jede beliebige Zahl n alle Primzahlen auch in zwei Klassen aufgeteilt werden, von denen die eine diejenigen enthalten wird, welche Teiler der Form $xx + nyy$ sein können, die andere hingegen die übrigen, welche in keiner Weise Teiler dieser Form sein können. Aber für jede der beiden Klassen habe ich schon vor einiger Zeit allgemeine Formeln angegeben, ähnlich jenen, mit denen ich hier für jede beliebige Primzahl die geeigneten Werte der Zahl n von den ungeeigneten unterschieden habe: Nur mit diesem Unterschied, dass, während hier die Formeln den Teiler P erhalten, dort die Zahl $4n$ den Platz des Teilers einnimmt. Natürlich habe ich für die Primteiler der Zahlen der Form $xx + nyy$ eine solche Form angegeben: $4ni + A$, aber für die, die in keiner Weise Teiler sein können, eine solche: $4ni + \mathfrak{A}$, wo die Buchstaben A und $\mathfrak{A}$ zugleich alle zu $4n$ primen und kleineren Zahlen als selbige erfassen, aus welchen der Buchstabe A die enthält, die zur Teilung geeignet sind, der Buchstabe $\mathfrak{A}$ hingegen die, die ausgeschlossen werden. Nachdem ich also diese Formeln einst mit Induktion gefunden hatte, kann nun kein Zweifel mehr vorhanden sein, dass die erste Formel $4ni + A$ alle Primzahlen umfasst, durch welche sich die Formel $xx + nyy$ teilen lässt, während die andere $4ni + \mathfrak{A}$ die beinhaltet, die in keiner Weise Teiler sein können. Dennoch werden sich indes die beiden Formeln auf die folgende Weise aus den aufgestellten Prinzipien ableiten lassen.

PROBLEM

Nach Vorlage einer beliebigen positiven Zahl n alle Primzahlen anzugeben, durch welche Zahlen der Form $xx + nyy$ eine Teilung zulassen können.

LÖSUNG

§16 Es bezeichne P irgendeinen Primteiler der vorgelegten Form $xx + nyy$, und es sei λ der aus dieser Teilung zu entspringende Quotient, und wir werden diese Gleichung haben: $\lambda P = xx + nyy$, welchen Ausdruck wir transformieren wollen, indem wir $x = 2nr + s$ und $y = 2t + u$ setzen, und es wird diese Gleichung hervorgehen:

$$\lambda P = 4n(nrr + rs + tu + tt) + ss + nuu,$$

an deren Stelle, weil $nrr + rs + tu + tt$ alle Zahlen bedeuten kann, wir der Kürze wegen λi schreiben wollen, dass natürlich das erste Glied durch λ geteilt werden kann, und wir werden diese Gleichheit haben: $P = 4ni + \frac{ss+nuu}{\lambda}$.

§17 Auf diese Weise haben wir also nun die oben erwähnte Form erhalten: $4ni + A$, und zugleich ist klar, dass anstelle von A alle aus der Formel $\frac{ss+nuu}{\lambda}$ resultierenden Zahlen genommen werden müssen, wo, weil λ irgendeine Zahl bezeichnen kann, der Buchstabe A so alle in der Form $ss + nuu$ enthaltenen Zahlen wie all deren Teiler in sich erfassen wird. Weil ja aber unsere Form Primzahlen darbieten muss, werden sich anstelle von A keine anderen Zahlen annehmen lassen, außer denen, die zu $4n$ prim waren, welche also ungerade und zugleich zur Zahl n selbst prim sein müssen, oder mit n keinen gemeinsamen Teiler haben dürfen.

§18 Zuerst werden also unter den Werten des Buchstaben A, indem man $u = 0$ und $\lambda = 1$ nimmt, alle ungeraden und zu n primen Quadratzahlen ss auftauchen, entweder als sie selbst oder durch Teilung durch $4n$ vermindert. Weiter werden durch Nehmen von $u = 1$, während $\lambda = 1$ bleibt, auch alle in der Form $ss + n$ enthaltenen Zahlen auftauchen, sofern sie natürlich zu $4n$ prim waren; hier wird es freilich förderlich sein bemerkt zu haben, dass, nachdem schon einige geeignete Zahlen für A gefunden worden sind, welche a, b, c, d, e etc. seien, auch alle Produkte aus zweien, also ab, ac, bc etc., ebenso auftreten müssen, der Grund für welche Tatsache der ist, dass das Produkt aus mehreren Zahlen der Form $ss + nuu$ immer auf dieselbe Form reduziert werden kann.

§19 Was aber die Werte von A betrifft, die entspringen, wenn λ nicht die Einheit war, oder welche nur Teiler der Form $ss + nuu$ sind, deren Menge unbestimmt erscheinen könnte, so müssen wir zum Theorem des illustren LAGRANGE zurückkehren, in welchem er bewiesen hat, dass alle Teiler der Zahlen der Form $ss + nuu$ immer in dieser Formel enthalten sind: $fpp \pm 2gpq + hqq$, während $fh = gg + n$ ist, und dass es nicht nötig ist, weiter fortzuschreiten als $2g < f$ oder $2g < h$, die Anzahl welcher Formen immer hinreichend gemäßigt ist. Daher wird sich für A also immer entweder f oder h annehmen lassen, wenn sie nicht zufällig nicht prim zu $4n$ waren. In diesem Fall wird es ratsam sein, dass für A entweder $f \pm 2g + h$ oder $4f \pm 4g + h$ oder $4 \pm 4g + 4h$ etc. genommen wird, sofern diese natürlich prim zu $4n$ waren. Sobald aber ein einziger solcher Wert gefunden worden ist, wird er mit denen, die schon zuvor gefunden worden sind, multipliziert ebenso viele neue geeignete Werte für A geben.

§20 Aber auf diese Weise werden wir bald alle geeigneten Werte für A erhalten, weil deren Anzahl immer der Hälfte aller Zahlen kleiner als $4n$, die zugleich zu ihr prim sind, gleich ist. Wenn also die Menge all dieser Zahlen $= 2k$ war (es ist nämlich anderswoher bekannt, dass deren Anzahl immer gerade ist), wird die Menge der Werte des Buchstaben A immer $= k$ sein, einzig ausgenommen in dem Fall, in dem n eine negative Quadratzahl ist, in welchem Fall gänzlich alle diese Zahlen einen Platz finden; aber in allen übrigen Fällen wird die Menge der ausgeschlossenen Zahlen ebenso $= k$ sein, wenn welche mit den griechischen Buchstaben α, β, γ, δ etc. bezeichnet werden, werden sie alle diese Werte des Buchstabens $\mathfrak{A}$ für die Formel $4ni + \mathfrak{A}$ geben, welche alle Primzahlen enthält, die auf keine Weise Teiler einer in der Form $xx + nyy$ enthaltenen Zahl sein können.

§21 Was aber die Werte von A selbst angeht, welche aus der Form $fpp \pm 2gpq + hqq$ entspringen, weil diese Form, ob sie mit f oder mit h multipliziert wird, wegen $fh = gg + n$ auf $xx + nyy$ reduziert wird, wird in diesen Fällen entweder $\lambda = f$ oder $\lambda = h$ sein, so dass dann für die daraus entstehenden Primzahlen so fP wie hP immer eine Zahl der Form $xx + nyy$ sein wird, wo es also genügen wird, die kleinere dieser zwei Zahlen f und h genommen zu haben, so dass sich verlauten lässt: Sooft eine Primzahl P ein Teiler einer gewissen Zahl der Form $xx + nyy$ war, so wird dann entweder diese Zahl P selbst oder ihr Vielfaches fP auch eine Zahl derselben Form $xx + nyy$ sein.

§22 Weil also die Form $4ni + \mathfrak{A}$ gewiss alle Zahlen enthält, die in keiner Weise Teiler der Form $xx + nyy$ sein können, ist es notwendig, dass alle in der Form $4ni + A$ enthaltenen Primzahlen zugleich Teiler einer bestimmten Form $xx + nyy$ sind.

KOROLLAR 1

§23 Dass die Menge der Werte des Buchstaben $\mathfrak{A}$ immer der Menge der Werte von A gleich ist, welche wir a, b, c, d, e etc. setzen, ist daher klar, dass, wenn eine einzige bekannt geworden ist, wie beispielsweise α, die zu $\mathfrak{A}$ zu zählen ist, dann auch αa, αb, αc, αd etc. zur selben Klasse gehören, wovon dennoch der eine Fall ausgenommen werden muss, in welchem $n = -mm$ ist, weil ja in diesem Fall überhaupt keine Werte für $\mathfrak{A}$ gegeben sind.

KOROLLAR 2

§24 Weil ja für jedwede Zahl n die LAGRANGE'sche Form der Teiler $fpp \pm 2gpq + hqq$ eine kleine Veränderung erfährt, weil sie immer so reduziert werden kann, dass $2g$ kleiner wird als f oder h, wenn diese kleineren Werte mit dem Buchstaben f bezeichnet werden, dann werden alle Primteiler der Form $xx + nyy$ entweder von derselben Form sein oder zusätzlich mit f multipliziert, woher, wenn f keine anderen Werte hat als die Einheit, was in den Fällen $n = 1$, $n = \pm 2$ und $n = \pm 3$ passiert, dann alle Primteiler in diesen Fällen auch dieselben Form haben werden.

0.1 KOROLLAR 3

§25 Weil ja alle Werte für den Buchstaben A ungerade Zahlen sein müssen, sind daher alle Formen $fpp \pm 2gpq + hqq$ auszuschließen, in denen die beiden Zahlen f und h gerade sind. Daher, weil $fh = gg + n$ ist, ist es ratsam, die Zahl $gg + n$ so in zwei Faktoren aufzulösen, dass zumindest der eine ungerade wird, woher, wenn $gg + n$ mehrere gerade Faktoren hat, mehrere Auflösungen als unnütz zu verwerfen sein werden.

SCHOLION 1

§26 Wie die Werte des Buchstaben A für die Form $4ni + A$ kleiner als $4n$ sind, wenn wir negative einführen wollen, werden sie sich unter $2n$ senken lassen, Ich habe aber weiter für alle Fälle, in denen n eine positive Zahl ist, beobachtet, dass die Menge dieser Werte von A auf die Hälfte reduziert werden kann, sodass die einzelnen nicht die Zahl n übersteigen, wenn sie natürlich nicht auf die Form $4ni$ bezogen werden, sondern nur auf ihre Hälfte $2ni$. Hier müssen aber zwei Fälle sorgsam voneinander unterschieden werden, je nachdem ob n in der einer dieser beiden Formeln: $4k$ und $4k-1$ oder in einer dieser beiden anderen: $4k+1$ und $4k+2$ enthalten ist. Denn im zweiten Fall muss den einzelnen Werten von A das doppeldeutige Vorzeichen $\pm$ oder $\mp$ vorangestellt werden, von welchen Zeichen die oberen gelten, sooft i eine gerade Zahl war, die unteren aber, wenn eine ungerade. Auf diese Weise ist also die folgende drei Spalten umfassende Tabelle konstruiert worden, deren erste die Werte der Zahl n in natürlicher Reihenfolge darbietet, die zweite die Formeln für die Teiler P, die dritte hingegen die oben mit dem Buchstaben f bezeichneten Indizes, welche so zu deuten sind, dass, sooft P eine Primzahl war, ihr Produkt mit einer bestimmten Index f eine Zahl der Form $xx+nyy$ wird.

TABELLE, WELCHE ALLE PRIMTEILER FÜR ZAHLEN DER FORM $xx + nny$ ZUSAMMEN MIT DEN INDIZES f ZEIGT.

Hier ist bezüglich der mehrdeutigen Vorzeichen zu bemerken, dass die oberen gelten, sooft i eine gerade Zahl war, die unteren hingegen, sooft i eine ungerade Zahl war.

n		Teiler P	f
1	$2i$	± 1	1
2	$4i$	± 1	1
3	$6i$	$+1$	1
4	$8i$	$+1, -3$	1
5	$10i$	$\pm 1, \pm 3$	$1, 2$
6	$12i$	$\pm 1, \pm 5$	$1, 2$
7	$14i$	$+1, -3, -5$	1
8	$16i$	$+1, +3, -5, -7$	$1, 3$
9	$18i$	$\pm 1, \pm 5, \mp 7$	$1, 2$
10	$20i$	$\pm 1, \mp 3, \pm 7, \pm 9$	$1, 2$
11	$22i$	$+1, +3, +5, -7, +9$	$1, 3$
12	$24i$	$+1, -5, +7, -11$	$1, 3$
13	$26i$	$\pm 1, \mp 3, \mp 5, \pm 7, \pm 9, \mp 11$	$1, 2$
14	$28i$	$\pm 1, \pm 3, \pm 5, \pm 9, \mp 11, \pm 13$	$1, 2, 3$
15	$30i$	$+1, -7, -11, -13$	$1, 3$
16	$32i$	$+1, -3, +5, -7, +9, -11, +13, -15$	$1, 4$
17	$34i$	$\pm 1, \pm 3, \mp 5, \pm 7, \pm 9, \pm 11, \pm 13, \mp 15$	$1, 2, 3$
18	$36i$	$\pm 1, \mp 5, \mp 7, \pm 11, \mp 13, \pm 17$	$1, 2, 3$
19	$38i$	$+1, -3, +5, +7, +9, +11, -13, -15, +17$	$1, 4$
20	$40i$	$+1, +3, +7, +9, -11, -13, -17, -19$	$1, 3, 4$
21	$42i$	$\pm 1, \pm 5, \pm 11, \mp 13, \pm 17, \pm 19$	$1, 2, 3, 5$
22	$44i$	$\pm 1, \mp 3, \mp 5, \mp 7, \pm 9, \pm 13, \pm 15, \mp 17, \pm 19, \pm 21$	$1, 2$
23	$46i$	$+1, +3, -5, -7, +9, -11, +13, -15, -17,$ $-19, -21$	$1, 3$
24	$48i$	$+1, +5, +7, +11, -13, -17, -19, -23$	$1, 3, 4$
25	$50i$	$\pm 1, \mp 3, \mp 7, \pm 9, \mp 11, \pm 13, \pm 17, \mp 19, \pm 21$ ± 23	$1, 2$

n		Teiler P	f
26	$52i$	$\pm1, \pm3, \pm5, \pm7, \pm9, \mp11, \pm15, \pm17, \mp19,$ $\pm21, \mp23, \pm25$	$1, 4$
27	$54i$	$+1, -5, +7, -11, +13, -17, +19, -23, +25$	$1, 4$
28	$56i$	$+1, -3, -5, +9, +11, -13, +15, -17, -19,$ $+23, +25, -27$	$1, 4$
29	$58i$	$\pm1, \pm3, \pm5, \mp7, \pm9, \pm11, \pm13, \pm15, \mp17,$ $\pm19, \mp21, \mp23, \pm25, \pm27$	$1, 2, 3, 5$
30	$60i$	$\pm1, \mp7, \pm11, \pm13, \pm17, \mp19, \pm23, \pm29$	$1, 2, 3, 5$
31	$62i$	$+1, -3, +5, +7, +9, -11, -13, -15, -17,$ $+19, -21, -23, +25, -27, -29$	$1, 5$
32	$64i$	$+1, +3, -5, -7, +9, +11, -13, -15, +17,$ $+19, -21, -23, +25, +27, -29, -31$	$1, 3, 4$
33	$66i$	$\pm1, \mp5, \pm7, \mp13, \pm17, \pm19, \pm23, \pm25, \pm29$ ∓31	$1, 2, 3, 6$
34	$68i$	$\pm1, \mp3, \pm5, \pm7, \pm9, \mp11, \mp13, \mp15, \mp19,$ $\pm21, \pm23, \pm25, \mp27, \pm29, \pm31, \pm33$	$1, 2, 5$
35	$70i$	$+1, +3, +9, +11, +13, +17, -19, -23, +27$ $+29, -31, +33$	$1, 3, 4, 5$
36	$72i$	$+1, +5, -7, -11, +13, +17, -19, -23, +25$ $+29, -31, -35$	$1, 3, 4, 5$
37	$74i$	$\pm1, \mp3, \mp5, \pm7, \pm9, \mp11, \mp13, \pm15, \mp17, \pm19$ $\pm21, \pm23, \pm25, \mp27, \mp29, \pm31, \pm33, \pm35$	$1, 2$
38	$76i$	$\pm1, \mp3, \mp5, \pm7, \pm9, \mp11, \pm13, \mp15, \mp17,$ $\pm21, \pm23, \pm25, \pm27, \pm29, \mp31, \mp33, \mp35$	$1, 2, 3, 6$
39	$78i$	$+1, +5, -7, +11 - 17, -19, -23, +25, -29$ $-31, -35, -37$	$1, 3, 5$
40	$80i$	$+1, -3, +7, +9, +11, +13, -17, +19, -21,$ $+23, -27, -29, -31, -33, +37, -39$	$1, 4, 5, 7$
$41i$	$82i$	$\pm1, \pm3, \pm5, \pm7, \pm9, \pm11, \mp13, \pm15, \mp17,$ $\pm19, \pm21, \mp23, \pm25, \pm27, \mp29, \mp31, \pm33$ $\pm35, \pm37, \mp39$	$1, 2, 3, 5, 6$

n		Teiler P	f
42	$84i$	$\pm 1, \mp 5, \mp 11, \pm 13, \pm 17, \mp 19, \pm 23, \pm 25, \pm 29,$	
		$\pm 31, \mp 37, \pm 41$	$1, 2, 3, 6$
43	$86i$	$+1, -3, -5, -7, +9, +11, +13, +15, +17$	
		$-19, +21, +23, +25, -27, -29, +31, -33,$	
		$+35, -37, -39, +41$	$1, 4$
44	$88i$	$+1, +3, +5, -7, +9, -13, +15, -17, -19,$	
		$-21, +23, +25, +27, -29, +31, -35, +37,$	
		$-39, -41, -43$	$1, 3, 4, 5$
45	$90i$	$\pm 1, \pm 7, \mp 11, \mp 13, \mp 17, \mp 19, \pm 23, \pm 29, \mp 31,$	
		$\pm 37, \pm 41, \mp 43$	$1, 2, 3, 5, 7$
46	$92i$	$\pm 1, \mp 3, \pm 5, \mp 7, \pm 9, \pm 11, \mp 13, \mp 15, \mp 17,$	
		$\pm 19, \pm 21, \pm 25, \mp 27, \mp 29, \pm 31, \mp 33, \mp 35,$	
		$\pm 37, \pm 39, \pm 41, \pm 43, \pm 45$	$1, 2, 5$
47	$94i$	$+1, +3, -5, +7, +9, -11, -13, -15, +17,$	
		$-19, +21, -23, +25, +27, -29, -31, -33,$	
		$-35, +37, -39, -41, -43, -45$	$1, 3, 7$
48	$96i$	$+1, -5, +7, -11, +13, -17, +19, -23, +25$	
		$-29, +31, -35, +37, -41, +43, -47$	$1, 3, 4, 7$
49	$98i$	$\pm 1, \mp 3, \pm 5, \pm 9, \mp 11, \pm 13, \mp 15, \pm 17, \mp 19,$	
		$\mp 23, \pm 25, \mp 27, \pm 29, \mp 31, \pm 33, \pm 37, \mp 39,$	
		$\pm 41, \mp 43, \pm 45, \mp 47$	$1, 2, 5$
50	$100i$	$\pm 1, \pm 3, \mp 7, \pm 9, \pm 11, \mp 13, \pm 17, \pm 19, \mp 21,$	
		$\mp 23, \pm 27, \mp 29, \mp 31, \pm 33, \mp 37, \mp 39, \pm 41,$	
		$\pm 43, \mp 47, \pm 49$	$1, 2, 3, 6$

SCHOLION 2

§27 Diese Tabelle kann ohne Mühe beliebig weit fortgesetzt werden. Nachdem nämlich irgendeine Zahl n vorgelegt worden ist, suche man für die Formel $2ni + A$ zuerst alle Primzahlen kleiner als n, die zugleich zu n teilerfremd sind, denen man das Vorzeichen $+$ zuteile, wenn n eine Zahl der Form $4k$ oder $4k-1$ war; aber in den Fällen, in denen n von der Form $4k+1$ oder $4k+2$ ist, ist das mehrdeutige Vorzeichen $\pm$ voranzustellen; den übrigen Primzahlen stelle man entweder das Zeichen $-$ voran oder das zweideutige $\mp$. Wenn also n ungerade Teiler hat, müssen sie alle von den Werten von A ausgeschlossen werden, die übrigen Primzahlen nehme man hingegen aus den Teilern der in dieser Form $n+xx$ enthaltenen Zahlen, während anstelle von n nacheinander die Zahlen 1, 2, 3, 4, 5 etc. geschrieben werden, welche aber nicht weiter als $\frac{1}{2}n$ fortgesetzt werden müssen. Wenn nämlich p eine Primzahl größer als n bezeichnet, wenn sie kein Teiler der Form $n+xx$ war, wird für $x<\frac{1}{2}p$ diese gewiss kein Teiler sein, wie große Zahlen auch immer geschrieben werden. Auf diese Weise werden leicht alle anstelle von A zu schreibenden Zahlen entdeckt, nach Finden von welchen die zusammengesetzten Zahlen leicht aus der Zusammensetzung selbst berechnet werden, während das Vorzeichen jedes Produkts aus den Vorzeichen der Faktoren in gewohnter Weise gebildet wird. Es wird der Mühe Wert sein, diese ganze Operationen an einigen Beispielen zu illustrieren. Es sei also zuerst $n=40$, und daher von der Form $4k$, woher alle Werte von A mit einfachen Vorzeichen behaftet sein werden. Weil nun 37 die größte Primzahl unter 40 ist, wird es genügen, die Zahlen x bis hin zu 18 fortgesetzt zu haben. Wir wollen also diese Werte der Form $40+xx$ hier zusammen mit den einzelnen Primteilern unter 40, außer 5, beifügen:

$n+xx$	Teiler	$n+xx$	Teiler
41	$--$	140	7
44	11	161	7, 23
49	7	184	23
56	7	209	11, 19
65	13	236	$--$
76	19	265	$--$
89	$--$	296	37
104	13	329	7
121	11	364	7, 13

Daher sind also die mit dem Vorzeichen $+$ zu markierenden Primzahlen $+1$, $+7$, $+11$, $+13$, $+19$, $+23$, $+37$, die übrigen Primzahlen kleiner als 40 werden hingegen das Vorzeichen $-$ haben, und sie werden -3, -17, -29, -31 sein, und aus diesen werden die Zahlen $+9$, -21, -27, -33, -39 zusammengesetzt sein, weshalb die Formel für die Primteiler P die folgende sein wird:

$$80i+1, \quad -3, \quad +7, \quad +9, \quad +11, \quad +13, \quad -17, \quad +19, \quad -21,$$
$$+23, \quad -27, \quad -29, \quad -31, \quad -33, \quad +37, \quad -39.$$

Für ein anderes Beispiel nehme man $n = 41$, weil welche Zahl von der Form $4k+1$ ist, werden die mehrdeutigen Zeichen zu nehmen sein. Man suche also zuerst alle Primteiler der Zahlen der Form $41 + xx$, welche nicht weiter als $x = 18$ fortgesetzt werden müssen, weil die größte Primzahl unterhalb von 41 ja 37 ist, deren Hälfte 18 ist; diese Operation führe man also wie zuvor durch.

$n+xx$	Teiler	$n+xx$	Teiler
42	$3,7$	141	$3,--$
45	$3,5$	162	3
50	5	185	$5,37$
57	$3,19$	210	$3,5,7$
66	$3,11$	237	$3,--$
77	$7,11$	266	$7,19$
90	$3,5$	297	$3,11$
105	$3,5,7$	330	$3,5,11$
122	$--$	365	$5,--$

Also sind die mit dem Zeichen $\pm$ zu versehenden Primzahlen ±1, ±3, ±5, ±7, ±11, ±19, ±37, die übrigen mit dem Zeichen $\mp$ zu versehenden sind hingegen ∓13, ∓17, ∓23, ∓29, ∓31, woher die zusammengesetzten Zahlen ±9, ±15, ±21, ±25, ±27, ±33, ±35, ∓39, weshalb sich die Formel für die Primteiler P so verhalten wird:

$$82i \pm 1, \quad \pm3, \quad \pm5, \quad \pm7, \quad \pm9, \quad \pm11, \quad \mp13, \quad \pm15, \quad \mp17, \quad \pm19, \quad \pm21,$$
$$\mp23, \quad \pm25, \quad \pm27, \quad \mp29, \quad \pm31, \quad \pm33, \quad \pm35, \quad \pm37, \quad \mp39.$$

Scholion 3

§28 Was die Indizes f für jedwede Zahl n betrifft, muss die allgemeine Form, welche der illustre Lagrange für die Teiler der Form $xx + nyy$ gegeben hat, welche $fpp + 2gpq + hqq$ war, während $fh = n + gg$ ist, betrachtet werden, wo man bemerke, dass es nicht vonnöten ist, in einem gewissen Fall mehr Formeln dieser Art zu bilden, als bis dahin, wo $2g$ die Zahl f übersteigt; außerdem nehmen wir hier aber für f den kleineren Faktor der Formel $n + gg$; dann ist aber außerdem notwendig, dass die eine der Zahlen f und h gerade ist, und auf diese Weise wird es leicht sein, alle Indizes f anzugeben. So nehme man für den ersten oben erwähnten Fall, wo $n = 40$ ist, zuerst $g = 0$, und es wird $fh = 40 = 5 \cdot 8$ sein, und so wird $f = 5$ sein; dann wird für $g = 1$ gesetzt $fh = 41$ werden, und daher $f = 1$; weiter wird für $g = 2$ gesetzt $fh = 44$ werden, und daher $f = 4$; aber für $g = 3$ gesetzt wird wegen $fh = 49$ dann $f = 7$ sein können, woher alle Werte von f entsprechend 1, 4, 5, 7 sein werden. Aber für das andere Beispiel, in welchem $n = 41$ ist, gibt der Wert $g = 0$ nur $f = 1$; der Wert $g = 1$ liefert $fh = 42$, und daher entweder $f = 2$ oder $f = 3$ oder $f = 6$; weiter liefert der Wert $g = 2$ zunächst $fh = 45$, woher man $f = 5$ berechnet, und so sind alle Werte für f dann 1, 2, 3, 4, 5, 6. Daher folgern wir also, sooft für die Formel $xx + 41yy$ die Zahl P als Primzahl hervorgeht, dass dann immer entweder P oder $2P$ oder $3P$ oder $5P$ oder $6P$ gewiss eine Zahl der Form $xx + 41yy$ sein wird. Wie wenn beispielsweise $i = 1$ genommen wird, weil $82 - 3 = 79$ ist, und daher eine Primzahl, ist sofort klar, dass die Zahl 79 selbst zwar nicht in der Form $xx + 41yy$ enthalten ist, auch nicht ihr Doppeltes 158; aber ihr Dreifaches 237 ist $14^2 + 41 \cdot 1^2$. In gleicher Weise findet man für P auch die Primzahl 73, welche weder selbst noch ihr Doppeltes und auch nicht ihr Dreifaches in der vorgelegten Form enthalten ist, aber ihr Fünffaches 365 dahingegen $= 18^2 + 41 \cdot 1^2$.

Problem

Wenn n eine negative Zahl war, also $n = -m$, eine allgemeine Formel für alle Primzahlen zu finden, die Teiler einer gewissen Zahl der Form $xx - myy$ oder auch $myy - xx$ sein können.

Lösung

§29 Diese Lösung von diesem Problem gehe man an wie die des vorhergehenden, indem man natürlich $-m$ anstelle von n schreibe, dann aber, wenn P einen Primteiler der vorgelegten Form bezeichnet, weil er ja notwendig positiv sein muss, ist es ratsam auch die Zahl i negativ anzunehmen, woher die oben gefundene Form

$$P = 4mi + \frac{ss - muu}{\lambda}$$

oder auch

$$P = 4mi - \frac{ss - muu}{\lambda}$$

werden wird, woher klar ist, dass alle dem ersten Term $4mi$ beizufügenden Zahlen so positiv wie negativ angenommen werden können, sodass wir allgemein $P = 4mi \pm A$ haben, wo A alle Teiler bezeichnet, entweder von der Form $ss - m$ oder von der Form $m - ss$, welche freilich zu $4m$ prim sind, woher von diesen Teilern zuerst alle geraden Zahlen ausgeschlossen werden, dann auch die ungeraden, die einen gemeinsamen Teiler mit der Zahl m haben.

§30 Wenn also die Menge aller zu $4m$ primen Zahlen, die kleiner als selbige sind, $= 4k$ ist, wird die Anzahl der Werte von A nur $= k$ sein, welche aber wegen der mehrdeutigen Vorzeichen als $= 2k$ anzusehen ist, sodass die Anzahl der ausgeschlossenen ebenso $= 2k$ ist. Nachdem dies bemerkt worden ist, wenn a ein Teiler der Form $m - ss$ oder $ss - m$ war, dann, sooft $4mi \pm a$ eine Primzahl war, wird sie immer ein Teiler einer gewissen Zahl der vorgelegten Form sein; andernfalls aber, wenn α eine davon ausgeschlossene Zahl war, dann lässt sich mit Gewissheit sagen, dass keine Zahl der Form $4mi \pm \alpha$ jemals ein Teiler der vorgelegten Form sein kann.

§31 Aber aus dem Lehrsatz des illustren Lagrange sind alle Teiler der vorgelegten Form in dieser allgemeinen Form enthalten: $fpp \pm 2gpq - hgg$, während $fh = m - gg$ ist, welche Formeln nur bis dorthin fortzusetzen sind, bis $2g$ schließlich f überragt; denn für uns bezeichne f immer den kleineren der beiden Faktoren, in welche die Zahl $m - gg$ aufgelöst wird. Aber außerdem, wie im vorhergehenden Fall, muss die eine der beiden Zahlen f und h als ungerade angenommen werden; daher sieht man ein, dass in jedwedem Fall die Menge der Werte von f hinreichend gemäßigt ist, nach

Finden von welchen alle Primteiler P entweder selbst oder mit einem gewissen Vielfachen von f multipliziert in der vorgelegten Form enthalten sein werden, und das nicht auf eine einzige Weise, wie es im vorhergehenden Fall passiert ist, sondern sogar auf unendlich viele Arten.

§32 Davon schließen wir aber mit Recht die Fälle aus, in denen m eine Quadratzahl ist, weil dann gänzlich alle Primzahlen, ohne Ausnahme, Teiler der vorgelegten Form werden können, was auch daher klar ist, dass für A alle Teiler der Formel $ss - m$ genommen werden müssen; denn daher, wenn $m = ll$ war und $s = l$ genommen wird, wird diese Formel 0, aber die Null ist durch vollkommen alle Zahlen teilbar.

KOROLLAR 1

§33 Wenn daher also a ein Teiler einer gewissen Zahl der Form $xx - myy$ war, dann werden alle Primzahlen so in dieser Form $4mi + a$ wie in dieser $4mi - a$ gewiss Teiler einer gewissen Zahl der vorgelegten Form sein; aber dann werden auch entweder sie selbst oder sie mit einem gewissen Wert von f multipliziert in derselben Form enthalten sein.

KOROLLAR 2

§34 Weil ja alle Werte von A so positiv wie negativ angenommen werden, ist es nicht notwendig, sie über die Grenze $2m$ hinaus fortzusetzen, und daher, wenn die Zahlen $m - ss$ oder $ss - m$ der Reihe nach geschrieben werden, müssen die Werte des Buchstaben nicht über $\frac{1}{2}p$ hinaus fortgesetzt werden, wenn freilich p die größte Primzahl kleiner als $2m$ bezeichnet.

KOROLLAR 3

§35 Weil die Werte des Produkts fh ja m, $m-1$, $m-4$, $m-9$, $m-16$, $m-25$ etc. sind, welche von Anfang an schrumpfen, wenn aus einem bestimmten größeren fh genommen wird, in den kleineren hingegen fk oder kk auftauchen, sodass $k < f$ ist, dann muss in den Indizes k anstelle von f geschrieben werden; daher, wenn $k = 1$ war, wird die Menge der Indizes daher nicht vergrößert werden; wenn nämlich fP von der Form $xx - myy$ oder $myy - xx$ war, dann wird auch hP immer dieselbe Form haben, und daher wird auch kP dieselbe Form haben.

Scholion 1

§36 Nachdem alle Primzahlen größer als $4m$, die zugleich zu ihr teilerfremd sind, notiert worden sind, welche a, b, c, d etc. seien, notiere man auch die übrigen, welche α, β, γ, δ etc. seien, und die zusammengesetzten Zahlen werden entweder die Produkte aus den Zahlen a, b, c, d etc. sein oder Produkte aus je zwei ausgeschlossenen α, β, γ, δ etc. Wenn also P alle Primteiler der Zahlen der Form $xx - myy$ bezeichnet, wollen wir Π für das Bezeichnen der davon ausgeschlossenen Zahlen nehmen, es wird dann

$$P = 4mi \pm (a, b, c, d, e \text{ etc.}),$$
$$\Pi = 4mi \pm (\alpha, \beta, \gamma, \delta, \varepsilon \text{ etc.}),$$

sein, woher für jedwede Zahl m diese zwei Formeln leicht konstruiert werden; aber die beiden werden immer aus der gleichen Anzahl an Termen bestehen. Wie wenn beispielsweise $m = 21$ war, sodass aus den Teilern die Zahlen 3 und 7 zusammen mit ihren Vielfachen ausgeschlossen werden müssen, entwickle man die aus der Form $21 - ss$ zu entspringenden Zahlen, ohne dabei zu berücksichtigen, ob sie positiv oder negativ sind, und für jede notiere man die Primteiler, außer 3 und 7, die $2m = 42$ nicht übersteigen, welche Operation auf diese Weise durchgeführt werde.

$21 - ss$	Teiler	$21 - ss$	Teiler
21	$--$	79	$--$
20	5	100	5
17	17	123	41
12	$--$	148	37
5	5	175	5
4	$--$	204	17
15	5	235	$--$
28	$--$	268	$--$
43	$--$	303	$--$
60	5	340	$17, 5$

Daher sind die Werte für die Buchstaben a, b, c, d also 5, 17, 37, 41, die ausgeschlossenen hingegen, mit den Buchstaben α, β, γ, δ etc. bezeichneten, sind 11, 13, 19, 23, 29, 31; zu diesem kommt also diese zusammengesetzte 25 hinzu, sodass unsere beiden Formeln sein werden:

$$P = 84i \pm (1, 5, 17, 25, 37, 41),$$
$$\Pi = 84i \pm (11, 13, 19, 23, 29, 31).$$

Und so besteht jede der beiden Formen aus derselben Anzahl an Termen, was immer notwendigerweise passieren muss. Aber für die Produkte fk, je nachdem wie sie aus den schrumpfenden Termen entspringen, werden wir die folgenden haben: $3 \cdot 7$, $4 \cdot 5$, $3 \cdot 4$, $1 \cdot 5$, $1 \cdot 4$, aus den kleinsten 5 und 4 klar ist, dass die nur die Einheit zu den Indizes zu zählen ist. Daher wird aus $3 \cdot 4$ auch 3 auf die Einheit reduziert, woher man folgert, dass ein einziger Index 1 gegeben ist. Hier war es gefällig, auch die Formeln für die Zahlen beizufügen, die in keiner Weise Teiler sein können, welche ohne Gewinn in der obigen Tabelle hinzugefügt worden wären, weil ja, wenn in den für P gegebenen Formeln die einzelnen Vorzeichen in die entgegengesetzten verwandelt werden, dann werden sie alle Zahlen liefern.

TABELLE, WELCHE ALLE PRIMTEILER FÜR DIE ZAHLEN DER FORM $xx - myy$ ODER $myy - xx$ ZUSAMMEN MIT DEN INDIZES f DARBIETEN

Hier haben immer die mehrdeutigen zugleich Geltung.

m	P und Π		f
2	$8i$	± 1	1
	$8i$	± 3	
3	$12i$	± 1	1
	$12i$	± 5	
5	$20i$	$\pm(1,9)$	1
	$20i$	$\pm(3,7)$	1
6	$24i$	$\pm(1,5)$	1
	$24i$	$\pm(7,11)$	
7	$28i$	$\pm(1,3,9)$	1
	$28i$	$\pm(5,11,13)$	
8	$32i$	$\pm(1,7,9,15)$	1
	$32i$	$\pm(3,5,11,13)$	
10	$40i$	$\pm(1,3,9,13)$	1, 2
	$40i$	$\pm(7,11,17,19)$	
11	$44i$	$\pm(1,5,7,9,19)$	1
	$44i$	$\pm(3,13,15,17,21)$	
12	$48i$	$\pm(1,11,13,23)$	1
	$48i$	$\pm(5,7,17,19)$	
13	$52i$	$\pm(1,3,9,17,23,25)$	1
	$52i$	$\pm(5,7,11,15,19,21)$	
14	$56i$	$\pm(1,5,9,11,13,25)$	1
	$56i$	$\pm(3,15,17,19,23,27)$	
15	$60i$	$\pm(1,7,11,17)$	1, 2
	$60i$	$\pm(13,19,23,29)$	
17	$68i$	$\pm(1,9,13,15,19,21,25,33)$	1
	$68i$	$\pm(3,5,7,11,23,27,29,31)$	
18	$72i$	$\pm(1,7,17,23,25,31)$	1
	$72i$	$\pm(5,11,13,19,25,35)$	
19	$76i$	$\pm(1,3,5,9,15,17,25,27,31)$	1
	$76i$	$\pm(7,11,13,21,23,29,33,35,37)$	

m		P und Π	f
20	$80i$	$\pm(1, 9, 11, 19, 21, 31, 39)$	1
	$80i$	$\pm(3, 7, 13, 17, 23, 27, 33, 37)$	
21	$84i$	$\pm(1, 5, 17, 25, 37, 41)$	1
	$84i$	$\pm(11, 13, 19, 23, 29, 31)$	
22	$88i$	$\pm(1, 3, 7, 9, 13, 21, 25, 27, 29, 39)$	1
	$88i$	$\pm(5, 15, 17, 19, 23, 31, 35, 37, 41, 43)$	
23	$92i$	$\pm(1, 7, 9, 11, 13, 15, 19, 25, 29, 41, 43)$	1
	$92i$	$\pm(3, 5, 17, 21, 27, 31, 33, 35, 37, 39, 45)$	
24	$96i$	$\pm(1, 5, 19, 23, 25, 29, 43, 47)$	1
	$96i$	$\pm(7, 11, 13, 17, 31, 35, 37, 41)$	

SCHOLION

§37 Es hier offensichtlich, dass die Formeln P und Π für den Fall $m = 24$ nicht von denen abweichen, die für den Fall $m = 6$ gegeben worden sind, wie es die Natur der Sache erfordert, weil ja die Form $xx - 6yy$ auf die Form $xx - 24yy$ reduziert wird, während in der ersten $2y$ anstelle von y geschrieben wird, welcher Umstand im Allgemeinen Geltung haben muss, wenn die Zahl m mit 4 oder einer anderen Quadratzahl multipliziert wird. Dieselbe Harmonie wird auch in den Formeln des ersten Problems gefunden; dennoch kann indes ein Unterschied in Bezug auf die Indizes bestehen, welches Grundes wegen wir solche Fälle voneinander unterschieden haben. Nachdem diese Dinge also abgehandelt worden sind, möchte ich anstelle des Schlussschnörkels zwei Theoreme erwähnen, mit welchen in den Fällen des erstes Problems die Formeln P auf das Glied $2ni$ reduziert worden sind, und deren Gültigkeit sich aus dem bisher behandelten ohne Mühe erkennen lassen wird.

THEOREM 3

§38 *Wenn $n = 4k + 1$ oder $n = 4k + 2$ war, sooft $4ni + 2n - 1$ eine Primzahl war, wird der Teiler von der Form $xx + nyy$ sein.*

THEOREM 4

Wenn entweder $n = 4k$ *oder* $n = 4k - 1$ *war, dann wird, sooft* $4ni - 2n + 1$ *eine Primzahl war, sie ein Teiler der Form* $xx + nyy$ *sein.*