Bemerkungen über die Division von Quadraten durch Primzahlen *

Leonhard Euler

Annahme

§1 *Wenn die Quadrate der Zahlen a, b, c, d, also a^2, b^2, c^2, d^2 etc., durch eine bestimmte Primzahl P dividiert werden, wollen wir die bei der Division zurückgelassenen Reste mit den gleichnamigen griechischen Buchstaben α, β, γ, δ etc. anzeigen.*

Korollar 1

§2 Weil also das Quadrat aa durch die Zahl P dividiert den Rest α zurücklässt, wird, nachdem der Quotient $= A$ gesetzt worden ist, $aa = AP + \alpha$ sein und daher wird $aa - \alpha$ durch P teilbar sein; und auf die gleiche Weise werden diese Ausdrücke $bb - \beta$, $cc - \gamma$, $dd - \delta$ etc. durch denselben Divisor P teilbar sein.

Korollar 2

§3 Die Quadrate $(a + P)^2$, $(a + 2P)^2$, $(a + 3P)^2$ und im im Allgemeinen $(a + nP)^2$ werden denselben Rest α zurücklassen, wenn sie durch die vorgelegte Zahl P dividiert werden. Daher tritt es klar zu tage, dass die Quadrate der Zahlen, die größer sind als der Teiler P, dieselben Reste liefern, welche aus den Quadraten der Zahlen, die kleiner als der Teiler P sind, entsprießen.

*Originaltitel: "Observationes circa divisionem quadratorum per numeros primos", erstmals publiziert in „*Opuscula varii argumenti 1* 1783, pp. 64-84", Nachdruck in „*Opera Omnia*: Series 1, Volume 3, pp. 497 - 512 ", Eneström-Nummer E552, übersetzt von: Alexander Aycock, Textsatz: Arseny Skryagin, im Rahmen des Projektes „Euler-Kreis Mainz"

KOROLLAR 3

§4 Weil des Weiteren das Quadrat $(P-a)^2$ durch P dividiert denselben Rest liefert wie das Quadrat a^2, tritt es klar zu tage, wenn $a > \frac{1}{2}P$ war, dass $P - a < \frac{1}{2}P$ sein wird. Daher ist es offenbar, dass aus den Quadraten der Zahlen alle verschiedenen Reste, die kleiner als die Hälfte des Teilers P sind, resultieren.

KOROLLAR 4

§5 Daher, wenn alle Reste verlangt werden, die aus der Division der Quadrate durch den gegebenen Teiler P hervorgehen, wird es genügen, nur die Quadrate betrachtet zu haben, deren Wurzel die Hälfte von P nicht überragen.

KOROLLAR 5

§6 Daher, wenn der Teiler $P = 2p + 1$ ist, wenn durch selbigen alle Quadratzahlen 1, 4, 9, 16, 25 etc. dividiert werden, können daher nicht mehr verschiedene Reste hervorgehen als Einheiten in der Zahl p enthalten sind, und diese resultieren aus den Quadraten $1, 2, 3, 4, \ldots p$; denn die Quadrate der folgenden Zahlen $p+1$, $p+2$, $p+3$ etc. erzeugen in umgekehrter Reihenfolge wieder dieselben Reste.

KOROLLAR 6

§7 Dies ist daher offenbar, weil diese zwei Quadrate p^2 und $(p+1)^2$ durch die Zahl $2p+1$ dividiert denselben Rest liefern, weil deren Differenz ja durch $2p+1$ teilbar ist. Denn allgemein, die Differenz $M - N$ welcher Zahlen auch immer durch $2p+1$ teilbar ist, ist es notwendig, dass jeder der beiden M und N einzeln dividiert denselben Rest zurücklässt. Daher muss auch, weil gilt

$$(p+2)^2 - (p-1)^2 = 3(2p+1),$$

jedes der beiden Quadrate einzeln, also $(p+2)^2$ und $(p-1)^2$, denselben Rest liefern und im Allgemeinen wird das Quadrat $(p+n+1)^2$ denselben Rest liefern wie das Quadrat $(p-n)^2$ geben. Nachdem dies also gezeigt worden ist, ist es klar, dass nicht mehr Reste resultieren können als Einheiten in der Zahl p enthalten sind; ob aber all diese Reste verschieden sind oder miteinander übereinstimmen, wird daher nicht bestimmt; und es kann sogar,

wenn irgendwelche Teiler zugelassen werden, jedes von beiden passieren. Wenn aber der Teiler $2p+1$ eine Primzahl war, werden all jene Reste einander verschieden sein, was ich auf die folgende Weise demonstriere.

LEHRSATZ 1

§8 *Wenn der Teiler* $P = 2p+1$ *eine Primzahl war und durch diese alle Quadrate* 1, 4, 9, 16, ... *bis hin zu* p^2 *dividiert werden, werden alle daraus resultierenden Reste einander verschieden sein und deren Menge wird daher* $= p$ *sein.*

BEWEIS

Es seien a und b irgendwelche Zahlen, die kleiner als p oder zumindest nicht größer als selbige sind, und es ist zu beweisen, wenn deren Quadrate a^2 und b^2 durch die Primzahl $2p+1$ dividiert werden, dass die Reste gewiss als verschiedene hervorgehen werden. Wenn sie nämlich denselben Rest lieferten, wäre deren Differenz $aa - bb$ durch $2p+1$ teilbar und daher müsste wegen der Primzahl $2p+1$ und $aa - bb = (a-b)(a+b)$ der eine dieser Faktoren durch $2p+1$ teilbar sein. Weil aber so $a - p$ wie $b > p$, zumindest nicht $a < p$ ist, ist die Summe $a+b$ um vieles mehr die Differenz $a-b$ kleiner als der Teiler $2p+1$; und daher kann keine der beiden durch $2p+1$ teilbar sein. Daher folgt offenbar, dass alle Quadrate, deren Wurzeln nicht größer als p sind, durch die Primzahl $2p+1$ dividiert gewiss verschiedene Reste zurücklassen werden.

KOROLLAR 1

§9 Wenn daher also alle Quadrate 1, 4, 9, 16 etc. durch die Primzahl $2p+1$ dividiert werden und alle verschiedenen Reste notiert werden, wird deren Anzahl weder größer noch kleiner sein als p, sondern dieser Zahl p genau gleich sein.

KOROLLAR 2

§10 Aber all diese an der Zahl p verschiedenen Reste entspringen aus ebenso vielen in der natürlichen Reihe zuerst auftretenden Zahlen, natürlich 1, 4, 9, 16, ... pp, und aus den folgenden größeren werden auch keine neuen Reste gefunden.

KOROLLAR 3

§11 Es werden also nicht alle Zahlen, die kleiner sind als der Teiler $2p+1$, unter den Resten auftreten, sondern nur so viele derer, wie Einheiten in der kleineren Hälfte des Teilers P enthalten sind. Daher, weil die Menge der Zahlen, die kleiner als der Teiler $2p+1$ sind, $= 2p$ ist, wird nur die eine Hälfte dieser in der Reihe der Reste aufgefunden werden, die andere wird dahingegen davon vollkommen ausgeschlossen.

BEMERKUNG

§12 Ich werde diese Zahlen, die kleiner als der Primteiler $2p+1$ sind und die aus der Reihe der Reste ausgeschlossen werden, mit dem Namen der Nicht-Reste bezeichnen, deren Menge also immer der Anzahl der Reste gleich ist. Diesen Unterschied zwischen den Resten und Nicht-Resten sittsam und gründlich angemerkt zu haben wird förderlich sein, weshalb ich auch für einige kleinere Primteiler so die Reste wie die Nicht-Reste hier darbieten werde.

Teiler 3, $p=1$	
Quadrat	1
Rest	1
Nicht-Rest	2

Teiler 5, $p=2$	
Quadrate	1, 4
Reste	1, 4
Nicht-Reste	2, 3

Teiler 7, $p=3$	
Quadrate	1, 4, 9
Reste	1, 4, 2
Nicht-Reste	3, 5, 6

Teiler 11, $p=5$	
Quadrate	1, 4, 9, 5, 3
Reste	1, 4, 9, 5, 3
Nicht-Reste	2, 6, 7, 8, 10

Teiler 13, $p=6$	
Quadrate	1, 4, 9, 16, 25, 36
Reste	1, 4, 9, 3, 12, 10
Nicht-Reste	2, 5, 6, 7, 8, 11

Teiler 17, $p=8$	
Quadrate	1, 4, 9, 16, 25, 36, 49, 64
Reste	1, 4, 9, 16, 8, 2, 15, 13
Nicht-Reste	3, 5, 6, 7, 10, 11, 12, 14

Teiler 19, $p=9$	
Quadrate	1, 4, 9, 16, 25, 36, 49, 64, 81
Reste	1, 4, 9, 16, 6, 17, 11, 7, 5
Nicht-Reste	2, 3, 8, 10, 12, 13, 14, 15, 18

Über diese Reste und Nicht-Reste für jeden Primteiler wird eine so bemerkenswerte Eigenschaft bemerkt, welche es der Mühe wert ist, sie mit umso größerem Eifer betrachtet zu haben, weil sich daher nicht zu verachtende Zuwächse auf die Zahlentheorie zu ergießen scheinen.

LEHRSATZ 2

§13 *Wenn in der Reihe der aus dem Teiler P entspringenden Reste die Zahlen α und β auftreten, wird ebendort deren Produkt $\alpha\beta$ auftreten, wenn es freilich kleiner als der Teiler P war; wenn es aber größer war, muss an seiner Stelle entweder $\alpha\beta - P$ oder $\alpha\beta - 2P$ oder allgemein $\alpha\beta - nP$ genommen werden, bis es schließlich unter P herabgesenkt wird.*

BEWEIS

Die Reste α und β mögen aus der Division der Quadrate aa und bb durch den Teiler P entspringen, so dass gilt

$$aa = AP + \alpha \quad \text{und} \quad bb = BP + \beta.$$

Daher wird sein

$$aabb = ABP^2 + (A\beta + B\alpha)P + \alpha\beta.$$

Daher, wenn das Quadrat $aabb$ durch den Teiler P dividiert wird, wird der Rest $\alpha\beta$ zurückgelassen werden, oder wenn $\alpha\beta$ den Teiler P überragt, muss an seiner Stelle der Rest genommen werden, welcher aus der Division von $\alpha\beta$ durch P zurückgelassen wird, welcher daher entweder $\alpha\beta - P$ oder $\alpha\beta - 2P$ oder $\alpha\beta - 3P$ oder allgemein $\alpha\beta - nP$ sein wird, so dass $\alpha\beta - nP < P$ ist.

KOROLLAR 1

§14 Wenn also unter den Resten die Zahl α auftaucht, werden ebendort auch $\alpha\alpha$ und ebenso α^3, α^4 und sogar all ihre Potenzen auftreten, wenn freilich von den einzelnen ein Vielfaches des Teilers P solcher Art subtrahiert wird, dass der Rest kleiner als der Teiler P wird.

KOROLLAR 2

§15 Weil also, während der Teiler P die Primzahl $2p+1$ ist, die Anzahl der Reste $= p$ ist, wenn alle Potenzen eines bestimmten Restes α, also α^0, α^1, α^2, α^3, α^4 etc. durch denselben Teiler P dividiert werden, können daher nicht mehr als p verschiedene Reste resultieren.

KOROLLAR 3

§16 Daher folgt, dass die Potenz a^p durch $P = 2p+1$ dividiert denselben Rest liefert wie $\alpha^0 = 1$ oder der Rest die Einheit sein wird, wie ich anderen Ortes gezeigt habe, wenn freilich der Teiler $2p+1$ eine Primzahl war.

BEMERKUNG

§17 Mit dem weiteren Entwickeln der außerordentlichen Eigenschaften, die daher abgeleitet werden können, halte ich mich hier nicht auf, weil dies von mir schon einst getan worden ist. Ich habe beschlossen, nur die Prinzipien hier kurz zu wiederholen, die ich brauche, um gewisse neue Beschaffenheiten der Reste zu erklären, woher es möglich ist, einige vorzügliche Eigenschaften um vieles bequemer zu beweisen. Für dieses Ziel bemerke ich, was freilich per se klar ist, dass, wie dem Rest $\alpha\beta$ die Zahlen $\alpha\beta - P$, $\alpha\beta - 2P$ und im Allgemeinen $\alpha\beta - nP$, wobei P der Teiler ist, gleichwertig sind, so auch alle durch P dividierten denselben Rest zurücklassenden Zahlen bei dieser Aufgabe als dieser Rest selbst angesehen werden können. So sind in der Reihe der Reste für irgendeinen Teiler P gänzlich alle Quadratzahlen selbst zweimal aufzutreten zu verstehen, weil jedes beliebige *aa* mit einer Form von dieser Art $AP + \alpha$ dargeboten werden kann und daher dem wahren Rest α äquivalent anzusehen ist. Daher werden negative Zahlen unter den Resten zugelassen werden können, weil $\alpha - P$ dem Rest α gleichwertig ist, und auf diese Weise wird es möglich sein, alle Reste auf Zahlen zurückzuführen, die kleiner als die Hälfte des Teilers P sind.

LEHRSATZ 3

§18 *Wenn in der Reihe der aus dem Teiler P entspringenden Reste die zwei Reste α und β auftreten, wird in ihr auch der Rest* $\frac{\alpha+nP}{\beta}$ *auftreten, nachdem die Zahl n so*

angenommen worden ist, dass $\frac{\alpha+nP}{\beta}$ *eine ganze Zahl wird, was sich freilich immer machen lässt.*

BEWEIS

Es seien aa und bb die Quadrate, die durch P dividiert die Reste α und β zurücklassen, dass ist

$$aa = AP + \alpha \quad \text{und} \quad bb = BP + \beta.$$

Nun werde ein c gesucht, dass $c = \frac{a+mP}{b}$ eine ganze Zahl ist, und es wird sein

$$cc = \frac{aa + 2amP + mmPP}{bb} = \frac{\alpha + (A + 2am + mmP)P}{\beta + BP} = \text{einer ganzen Zahl.}$$

Weil im der Zähler als der Rest α, der Nenner hingegen als Rest β angesehen werden kann, tritt es klar zu tage, wenn cc durch P dividiert wird, dass der Rest auf die vorgelegte Form reduziert werden wird. Nachdem nämlich der Kürze wegen $A + 2am + mmP = D$ gesetzt worden ist, dass $cc = \frac{\alpha+DP}{\beta+BP}$, dann aber $\frac{\alpha+nP}{\beta} = \gamma$ ist, muss gezeigt werden, dass $cc = CP + \gamma$ sein wird, dass der aus der Division des Quadrates cc durch die Zahl P entstandene Rest als $= \gamma$ hervorgeht. Weil aber $\alpha = \beta\gamma - nP$ gilt, wird natürlich werden können

$$cc = \frac{\beta\gamma + (D - n)P}{\beta + BP} = CP + \gamma,$$

weil daher folgt

$$(D - n)P = (\beta C + \gamma B + BCP)P \quad \text{oder} \quad D - n = \beta C + \gamma B + BCP,$$

eine Relation von welcher Art zwischen den Koeffizienten von P ganz und gar notwendig ist, dass ganze Zahlen hervorgehen.

ANDERS

Anstelle des Restes α werde ein anderer gleichwertiger $\alpha + nP$ angenommen, dass $\alpha + nP = \beta\gamma$ ist; und weil alle Quadrate dieser Form $(a + mP)^2$ denselben Rest α liefern, welcher angenommen wird, aus dem Quadrat aa zu entsprießen, werde m so angenommen, dass $a + mP = bc$ wird; und weil das Quadrat $bbcc$

durch P dividiert den Rest α oder $\beta\gamma$, das Quadrat bb hingegen den Rest β zurücklässt, ist es notwendig, dass das Quadrat cc den Rest $\gamma = \frac{\alpha+nP}{\beta}$ zurücklässt. Es sei nämlich $bbcc = EP + \beta\gamma$ und $bb = BP + \beta$; wenn man dann aber verneint, dass das Quadrat cc den Rest γ liefern wird, liefere es den davon verschiedenen x, dass $cc = CP + x$; es wird also sein

$$bbcc = EP + \beta\gamma = (BP + \beta)(CP + x) = \beta x + (\beta C + Bx + BCP)P.$$

Nachdem nun auf beiden Seiten die Vielfachen des Teilers P weggelassen worden sind wie es bei der Bewertung der Reste getan zu werden pflegt, wenn sie freilich in der kleinsten Form verlangt werden, wird man $\beta x = \beta\gamma$ und daher $x = \gamma$ haben.

KOROLLAR 1

§19 Weil die Einheit also immer ein Rest ist, dann wird auch, wenn für den Teiler P auch irgendein Rest α war, $\frac{1+nP}{\alpha}$ unter den Resten auftauchen; wenn dieser β genannt wird, wird $\alpha\beta = 1 + nP$ sein, oder das Produkt $\alpha\beta$ wird unter den Resten der Einheit gleichwertig sein.

KOROLLAR 2

§20 Für jeden beliebigen Rest α kann also quasi einem selbigem reziproker β angegeben werden, dass $\alpha\beta$ der Einheit gleichwertig ist, natürlich indem $\beta = \frac{1+nP}{\alpha}$ angenommen wird; und diese zwei reziproken Reste α und β werden einander verschieden sein, wenn die beiden nicht $+1$ oder -1 waren. Wenn nämlich $\beta = \alpha$ ist und gilt

$$\alpha\alpha = 1 + NP = 1 + 2mP + mmPP,$$

wird auch gelten

$$\alpha = \pm(1 + mP)$$

und wird ein Vielfaches des Teilers mP sein, indem $\alpha = \pm 1$ weggelassen wird.

KOROLLAR 3

§21 Während also in der Reihe der Reste jedem beliebigen Rest sein Reziprokes hinzugefügt wird, werden auf diese Weise je zwei zusammengebracht

werden; die Einheit wird aber immer alleine zurückgelassen werden, dann aber auch der Rest -1 oder $P-1$, sooft er freilich unter den Resten auftritt.

BEMERKUNG

§22 Diese Idee der je zwei reziproken Reste ist von größter Bedeutung und wird zu einem leichten Beweis des wunderschönen Lehrsatzes führen, welchen ich an anderer Stelle über ziemlich viele Umwege beweisen hatte, natürlich dass eine Primzahl der Form $4q+1$ immer eine Summe zweier Quadrate ist. Im Übrigen wird es förderlich sein sich hier daran zu erinnern, wenn für einen gewissen Teiler P die Reste α, β, γ, δ etc., die Nicht-Reste hingegen $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D}$ etc. sind, dass dann alle gegenseitigen Produkte der Reste, also $\alpha\beta$, $\alpha\gamma$ etc., auch unter den Resten aufgefunden werden [§ 13], aber deren Produkte mit einem gewissen Nicht-Rest, wie beispielsweise $\alpha\mathfrak{A}$, zu den Nicht-Resten zu rechnen sind. Aber die Produkte aus je zwei Nicht-Resten, wie beispielsweise $\mathfrak{AB}$, gehen in die Reihe der Reste über.

LEHRSATZ 4

§23 *Wenn der Teiler P eine Primzahl der Form $4q+3$ war, dann wird -1 oder $P-1$ gewiss in der Reihe der Nicht-Reste aufgefunden.*

BEWEIS

Weil, nachdem der Teiler $P = 2p+1$ gesetzt worden ist, hier $p = 2q+1$ und daher eine ungerade Zahl ist, wird die Anzahl aller Reste ungerade sein. Aber wenn -1 in der Reihe der Nicht-Reste auftauchte, entspräche jedem beliebigen Rest α ein anderer Rest $-\alpha$, woher sich die Reihe der Reste so verhielte

$$\begin{array}{lllll} +1, & +\alpha, & +\beta, & +\gamma, & +\delta \quad \text{etc.} \\ -1, & -\alpha, & -\beta, & -\gamma, & -\delta \quad \text{etc.} \end{array}$$

und die Anzahl der Reste daher gerade wäre. Weil die Anzahl der Reste also gewiss ungerade ist, kann es nicht geschehen, dass in der Reihe der Reste -1 oder $P-1$ auftritt; als logische Konsequenz muss sie notwendigerweise in der Reihe der Nicht-Reste aufgefunden werden.

KOROLLAR 1

§24 Wenn daher also für den Primteiler $P = 4q + 3$ unter den Resten die Zahl α auftaucht, dann wird die Zahl $-\alpha$ oder $P - \alpha$ gewiss unter den Nicht-Resten aufgefunden werden; und auf die gleiche Weise, wenn $-\beta$ ein Rest war, wird dann $+\beta$ ein Nicht-Rest sein.

KOROLLAR 2

§25 Wenn das Quadrat aa durch den Teiler $P = 4q + 3$ geteilt den Rest α zurücklässt, kann, weil kein Quadrat xx gegeben ist, was den Rest $-\alpha$ liefert, es überhaupt nicht geschehen, dass jene Summe der zwei Quadrate $aa + xx$ durch jene Zahl $4q + 3$ teilbar ist.

KOROLLAR 3

§26 Zusätzlich entspringe der Rest β aus dem Quadrat bb, und weil die Form βaa den Rest $\beta\alpha$, die Form αbb den Rest $\alpha\beta$ gibt, wird diese Form $\beta aa - \alpha bb$ durch den Teiler $P = 4q + 3$ teilbar sein.

KOROLLAR 4

§27 Weil aber kein Quadrat xx gegeben ist, welches den Rest $-\beta$ liefert, ist keine Form αxx gegeben, die den Rest $-\alpha\beta$ liefert; also wird keine Form dieser Art $\beta aa + \alpha xx$ durch die Zahl $P = 4q + 3$ teilbar sein, wenn freilich α und β Reste sind und α der dem Quadrat aa entsprechende Rest ist.

KOROLLAR 5

§28 Weil aber auch diese Form $\beta aacc + \alpha ccxx$ nur durch den Teiler $P = 4q + 3$ teilbar ist, wenn das Quadrat cc eine Division zulässt, welcher Fall von selbst ausgeschlossen wird, kann dem Quadrat $aacc$ irgendein anderer Rest außer α entsprechen; daher kann, indem dd und yy anstelle von $aacc$ und $ccxx$ geschrieben wird, keine Form dieser Art

$$\beta dd + \alpha yy$$

dargeboten werden, die durch die Zahl $P = 4q + 3$ teilbar ist, während α und β Reste sind.

BEMERKUNG

§29 Damit diese Dinge besser verstanden werden, wollen wir gewisse Primzahlen der Form $4q+3$ durchgehen und die Reste, die größer sind als deren Hälfte, indem davon $4q+3$ subtrahiert wird, negativ darstellen, dass sie unter die Hälfte herabgesenkt werden und es daher klar zu tage tritt, dass das Negative $-\alpha$ des Restes α nicht zugleich in der Reihe der Reste auftritt. In nachstehender Tabelle sind in der linken Spate die Teiler aufgeführt, in der rechten hingen die jeweiligen Reste:

3	1
7	1, -3, $+2$
11	1, $+4$, -2, $+5$, $+3$
19	1, $+4$, $+9$, -3, $+6$, -2, -8, $+7$, $+5$
23	1, $+4$, $+9$, -7, $+2$, -10, $+3$, -5, -11, $+8$, $+6$
31	1, $+4$, $+9$, -15, -6, -5, -13, $+2$, -12, $+7$, -3, -11, $+14$, $+10$, $+8$.

Hier ist es ersichtlich, dass unter den Resten alle mit dem Vorzeichen $+$ oder $-$ versehenen Zahlen, die nicht größer sind als die Hälfte des Teilers sind, auftreten, aber keine mit zweimal mit demselben Vorzeichen behaftet auftaucht. Daher, wenn die Vorzeichen dieser einzelnen Reste verändert werden, wird die Reihe der Nicht-Reste vervollständigt werden. Daher können für den Teiler 31 die folgenden niemals durch die Zahl 31 teilbaren Zahlen dargeboten werden:

$$aa+bb, \quad aa-15bb, \quad aa-6bb, \quad aa+5bb, \quad aa-13bb, \quad aa+2bb, \quad aa+7bb,$$

$$aa-3bb, \quad aa-11bb, \quad aa+14bb, \quad aa+10bb.$$

Und im Allgemeinen, wenn α und β irgendwelche zwei Reste sind, wird keine Form dieser Art

$$\alpha aa+\beta bb$$

eine Division durch die Zahl 31 zulassen.

LEHRSATZ 5

§30 *Wenn der Teiler P eine Primzahl der Form $4q+1$ war, dann wird die Zahl -1 oder $P-1$ gewiss in der Reihe der Reste aufgefunden.*

BEWEIS

Es sei α irgendein Rest und auch sein Reziprokes $\frac{1}{\alpha}$ oder $\frac{1+nP}{\alpha}$ wird ein Rest sein (§ 19) sein, welcher, wenn nicht entweder $\alpha = +1$ oder $\alpha = -1$ ist, von α verschieden sein wird, so dass unter Ausnahme dieser zwei Fälle jedem beliebigen Rest α sein von α verschiedenes Reziprokes, welches α' sei, entspricht, Daher, wenn -1 nicht unter den Resten aufgefunden wird, könnten alle Reste, indem je zwei reziproke verbunden werden, so dargestellt werden

$$\begin{array}{llllll} 1, & \alpha, & \beta, & \gamma, & \delta & \text{etc.} \\ & \alpha', & \beta', & \gamma', & \delta' & \text{etc.} \end{array}$$

und so, weil sie alle verschieden sind, wäre die Anzahl aller Reste ungerade. Weil aber der Teiler eine Primzahl der Form $4q+1$ ist, ist die Anzahl aller Reste $2q$ und daher gerade; daher folgt notwendigerweise, dass unter den Resten auch die Zahl -1 oder $P-1$ auftritt, weil andernfalls die Anzahl der Reste ungerade wäre.

KOROLLAR 1

§31 Weil also für den Primteiler $P = 4q+1$ die Zahl -1 gewiss unter den Resten aufgefunden wird, wenn irgendein anderer Rest α war, wird unter den Resten auch $-\alpha$ auftreten.

KOROLLAR 2

§32 Wenn also das Quadrat aa durch den Primteiler $4q+1$ dividiert den Rest α zurücklässt, wird ein anderer Rest bb gegeben sein, welcher den Rest $-\alpha$ liefern wird, woher die Summe dieser Quadrate $aa+bb$ gewiss durch die Primzahl $4q+1$ teilbar sein wird.

KOROLLAR 3

§33 Weil ja alle Reste aus Quadraten, deren Wurzel die Hälfte des Teilers nicht übersteigen, entspießen, kann, nachdem irgendein Quadrat aa vorgelegt worden ist, immer ein anderes bb, das nicht größer ist als $4qq$, dargeboten werden, dass die Summe $aa + bb$ durch $4q + 1$ teilbar hervorgeht.

KOROLLAR 4

§34 Wenn $1 + aa$ die Division durch $4q + 1$ zulässt, dann wird auch $bb + aabb$ und daher auch

$$bb + (ab - (4q + 1)n)^2$$

eine Division zulassen; und so wird, nachdem das eine Quadrat bb nach Belieben angenommen worden ist, dass andere $(ab - (4q + 1)n)^2$ leicht aufgefunden.

KOROLLAR 5

§35 Wenn diese Summe der zwei Quadrate $aa + bb$ durch den Teiler $4q + 1$ teilbar war, dann wird auch $aaxx + bbxx$ und daher auch diese Form

$$(ax - (4q + 1)m)^2 + (bx - (4q + 1)n)^2$$

eine Division zulassen. Immer ist es aber möglich x so anzunehmen, dass die Wurzel des einen Summanden, $ax - (4q + 1)m$, einer gegebenen Zahl c gleich wird, indem $x = \frac{c+(4q+1)m}{a}$ genommen wird, was immer in ganzen Zahlen geschehen kann.

BEMERKUNG 1

§36 Für jeglichen Primteiler, ob er von der Form $4q + 1$ oder $4q + 3$ ist, verdient die Betrachtung der Reziproken die ganze Aufmerksamkeit, weil wir daher leicht diese vorzügliche Wahrheit gefunden haben, dass, nachdem irgendeine Primzahl der Form $4q + 1$ vorgelegt worden ist, immer durch jene teilbare Summen zweier Quadrate dargeboten werden können. Weil also zusätzlich bewiesen werden kann, dass die Summe nur Teiler zulässt, die selbst Summen zweier Quadrate sind, wird auf diese Weise der Beweis des FERMAT'schen Lehrsatzes, dass alle Primzahlen der Form $4q + 1$ die Aggregate

von zwei Quadraten sind, bequemer geführt als es freilich einst von mir getan worden ist. Wie sich aber die reziproken Zahlen für einen gewissen Teiler P verhalten, während die $\frac{1+nP}{\alpha}$ die reziproke Zahl zu einer bestimmten Zahl α ist, wird aus den beigefügten Beispielen besser verstanden werden. In der nachstehenden Tabelle enthält die linke Spalte die Divisoren, die rechte die Paare der Reziproken:

3													
5	2												
	3												
7	2,	3											
	4,	5											
11	2,	3,	5,	7									
	6,	4,	9,	8									
13	2,	3,	4,	5,	6								
	7,	9,	10,	8,	11								
17	2,	3,	4,	5,	8,	10,	11						
	9,	6,	13,	7,	15,	12,	14						
19	2,	3,	4,	6,	7,	8,	9,	14					
	10,	13,	5,	16,	11,	12,	17,	15					
23	2,	3,	4,	5,	7,	9,	11,	13,	15,	17			
	12,	8,	6,	14,	10,	18,	21,	16,	20,	19			
29	2,	3,	4,	5,	7,	8,	9,	12,	14,	16,	18,	19,	23
	15,	10,	22,	6,	25,	11,	13,	17,	27,	20,	21,	26,	24

Diese einzelnen reziproken Paare sind so miteinander verbunden, dass jede beliebige Zahl nur einen einzigen reziproken Wert erhält, der natürlich kleiner als der Teiler ist, genauso wie wir im Lehrsatz angenommen haben.

BEMERKUNG 2

§37 Wenn daher also der Primteiler von der Form $4q+1$ war, wollen wir sehen, auf welche Weise sich die nach dem Gesetz der Reziproken angeordneten Reste verhalten werden. In nachstehender Tabelle sind in der linken Spalte wieder die Teiler aufgeführt, in der rechten hingegen die Reste:

5	1,	4																												
	1,	−1																												
13	1,	4,	9,	12,	10																									
	1,	4,	9,	12																										
		10,	3,	−1																										
17	1,	4,	9,	16,	8,	2,	15,	13																						
	1,	4,	9,	8,	16																									
		13,	2,	15,	−1																									
29	1,	4,	9,	16,	25,	7,	20,	6,	23,	13,	5,	28,	24,	22																
	1,	4,	9,	16,	25,	6,	23,	28																						
		22,	13,	20,	7,	5,	24,	−1																						
37	1,	4,	9,	16,	25,	26,	12,	27,	7,	26,	10,	33,	21,	11,	3,	34,	30,	28												
	1,	4,	9,	16,	25,	12,	27,	26,	21,	36																				
		28,	33,	7,	3,	34,	11,	10,	30,	−1																				

Aus diesen Beispielen ist es klar, weil die Einheit allein gestellt ist und von den übrigen Resten jedem sein reziproker beigefügt ist, dass die Anzahl der Reste ungerade sein wird, wenn nicht ein anderer allein gestellter Rest hinzukäme, der sich selbst reziprok wäre. Weil ja also in diesen Fällen, in denen der Teiler eine Primzahl der Form $4q+1$ ist, die Anzahl der Reste gewiss gerade und $= 2q$ ist, ist es notwendig, dass außer der Einheit der Rest $4q$ oder -1 auftritt, dessen Reziprokes natürlich selbigem gleich ist. Daher wird die Gültigkeit dieses wunderschönen Lehrsatzes, dessen Beweis auf anderem Wege höchst schwierig war, sehr klar, natürlich dass, sooft der Teiler eine Primzahl der Form $4q+1$ war, unter den Resten immer die Zahl $4q$ oder -1 auftaucht.

BEMERKUNG 3

§38 Wie aber daher klar zu tage tritt, dass die Zahl -1 unter den Resten aufgefunden wird, sooft der Teiler eine Primzahl der Form $4q + 1$ war, so kann für jegliche andere Primzahl s die Form der Primzahl angegeben, aber noch nicht bewiesen werden, dass die Zahl s in den Resten aufgefunden wird. Von dieser Art ist dieser Lehrsatz:

Wenn der Primteiler von Form $4ns + (2x + 1)^2$ war, während s eine Primzahl ist, dann werden in den Resten die Zahlen $+s$ und $-s$ auftreten;

und ein anderer diesem ähnliche:

Wenn der Primteiler von der Form $4ns - (2x + 1)^2$ war, während s eine Primzahl ist, dann wird in deren Resten die Zahl $+s$ auftreten, aber $-s$ wird in den Nicht-Resten zu finden sein.

Wann immer aber umgekehrt $-s$ in den Resten, aber $+s$ in den Nicht-Resten auftritt, kann so im Allgemeinen nicht bestimmt werden. Für Spezialfälle wird die Sache aber entdeckt, sich so zu verhalten:

Damit		muss der Primteiler sein
$\left\{\begin{matrix} - & 2 \\ + & 2 \end{matrix}\right.$	$\left.\begin{matrix} \text{ein Rest ist} \\ \text{ein Nicht-Rest ist} \end{matrix}\right\}$	$P = \quad 8n + 3$
$\left\{\begin{matrix} - & 3 \\ + & 3 \end{matrix}\right.$	$\left.\begin{matrix} \text{ein Rest ist} \\ \text{ein Nicht-Rest ist} \end{matrix}\right\}$	$P = 12n + 7$
$\left\{\begin{matrix} - & 5 \\ + & 5 \end{matrix}\right.$	$\left.\begin{matrix} \text{ein Rest ist} \\ \text{ein Nicht-Rest ist} \end{matrix}\right\}$	$P = 20n + 3,\ 7$
$\left\{\begin{matrix} - & 7 \\ + & 7 \end{matrix}\right.$	$\left.\begin{matrix} \text{ein Rest ist} \\ \text{ein Nicht-Rest ist} \end{matrix}\right\}$	$P = 28n + 11,\ 15,\ 23$
$\left\{\begin{matrix} -11 \\ +11 \end{matrix}\right.$	$\left.\begin{matrix} \text{ein Rest ist} \\ \text{ein Nicht-Rest ist} \end{matrix}\right\}$	$P = 44n + 3,\ 15,\ 23,\ 27,\ 31$
$\left\{\begin{matrix} -13 \\ +13 \end{matrix}\right.$	$\left.\begin{matrix} \text{ein Rest ist} \\ \text{ein Nicht-Rest ist} \end{matrix}\right\}$	$P = 52n + 7,\ 11,\ 19,\ 25,\ 31,\ 47$
$\left\{\begin{matrix} -17 \\ +17 \end{matrix}\right.$	$\left.\begin{matrix} \text{ein Rest ist} \\ \text{ein Nicht-Rest ist} \end{matrix}\right\}$	$P = 68n + 3,\ 7,\ 11,\ 23,\ 27,\ 31,\ 39,\ 63$
$\left\{\begin{matrix} -19 \\ +19 \end{matrix}\right.$	$\left.\begin{matrix} \text{ein Rest ist} \\ \text{ein Nicht-Rest ist} \end{matrix}\right\}$	$P = 76n + 7,\ 11,\ 19,\ 23,\ 35,\ 39,\ 43,\ 47,\ 55,\ 63$
$\left\{\begin{matrix} -23 \\ +23 \end{matrix}\right.$	$\left.\begin{matrix} \text{ein Rest ist} \\ \text{ein Nicht-Rest ist} \end{matrix}\right\}$	$P = 92n + 3,\ 23,\ 27,\ 31,\ 35,\ 39,\ 47,\ 55,\ 59,\ 71,\ 75,\ 87$

Die Betrachtung dieser Fälle gibt diesen Lehrsatz an die Hand:

Wenn der Primteiler von der Form $4ns - 4z - 1$ *war, indem alle in der Form* $4ns - (2x + 1)^2$ *enthaltene Zahlen ausgeschlossen werden, während s eine Primzahl ist, dann wird in den Resten* $-s$ *auftauchen, aber* $+s$ *wird ein Nicht-Rest sein.*

Diesen Lehrsätzen kann darüber hinaus dieser hinzugefügt werden:

Wenn der Primteiler der Form $4ns + 4z + 1$, *indem alle in der Form* $4ns + (2x + 1)^2$ *enthaltenen Werte ausgeschlossen werden, während s eine Primzahl ist, dann wird so* $+s$ *wie* $-s$ *in den Nicht-Resten auftreten.*

Diese Lehrsätze füge ich daher an, damit diejenigen, die an Betrachtungen

von dieser Art Freunde haben, nach deren Beweis suchen, weil kein Zweifel besteht, dass die Zahlentheorie daher riesige Zuwächse erfahren wird.

KONKLUSION

§39 Diese letzten vier Lehrsätze, deren Beweis noch aussteht, können gefälliger auf die folgende Weise dargeboten werden:

Während s irgendeinene Primzahl ist, werden nur die ungeraden Quadrate 1, 9, 25, 49 *etc. durch den Teiler* 4s *dividiert und die Reste notiert, welche alle von der Form* $4q + 1$ *sind, von welchen ein bestimmter mit dem Buchstaben* α *bezeichnet werde, von den übrigen Zahlen der Form* $4q + 1$*, die nicht unter den Resten auftreten, werde ein beliebiger aber mit dem Buchstaben* $\mathfrak{A}$ *angezeigt; wenn danach*

der Primteiler von nachstehender Form war	*dann ist*			
$4ns + \alpha$	$+s$	*ein Rest und*	$-s$	*ein Rest*
$4ns - \alpha$	$+s$	*ein Rest und*	$-s$	*ein Nicht-Rest*
$4ns + \mathfrak{A}$	$+s$	*ein Nicht-Rest und*	$-s$	*ein Nicht-Rest*
$4ns - \mathfrak{A}$	$+s$	*ein Nicht-Rest und*	$-s$	*ein Rest*