Beweis des Fermat'schen Lehrsatzes, dass jede entweder ganze oder gebrochene Zahl die Summe von vier oder weniger Quadraten ist *

Leonhard Euler

§1 ***Lehrsatz 1***

Aus der Reihe der Quadrate

$$1, 4, 9, 16, 25, \quad etc.$$

sind keine Zahlen durch die Primmzahl p teilbar, wenn deren Wurzeln nicht durch dieselbe Zahl teilbar sind.

Beweis.
Wenn nämlich eine gewisse Quadratzahl aa durch die Primzahl p teilbar war, weil sie aus den Faktoren a und a besteht; ist es notwendig, dass der eine der beiden Faktoren durch p teilbar ist; daher kann die Quadratzahl aa durch die Primzahl p nicht teilbar sein, wenn nicht ihre Wurzel a durch p teilbar ist. □

§2 **Korollar 1**

*Originatitel: „Demonstratio theorematis Fermatiani omnem numerum sive integrum sive fractum esse summam quatuor pauciorumve quadratorum", erstmals publiziert in „*Novi Commentarii academiae scientiarum Petropolitanae* 5, 1760, pp. 13-58", Nachdruck in „*Opera Omnia*: Series 1, Volume 2, pp. 338 - 372", eine Version veröffentlicht in *Commentat. arithm.* 1, 1849, pp. 215-233 [E242a], Eneström-Nummer E 242, übersetzt von: Alexander Aycock, TEXtsatz: Matthias Gluth, im Rahmen des Hauptseminars „Euler", JGU Mainz

Durch die Primzahl p teilbare Quadratzahlen entsprießen also aus den Wurzeln $p, 2p, 3p, 4p$ etc. und es sind daher $pp, 4pp, 9pp, 16pp$, etc. und die übrigen Quadratzahlen werden alle durch die Primzahl p nicht teilbar sein.

§3 **Korollar 2**

Wenn also Quadratzahlen, deren Wurzeln in dieser arithmetischen Progression $p, 2p, 3p, 4p$, etc. nicht enthalten sind, durch die Primzahl p geteilt werden, wird in dieser Division immer ein Rest zurückbleiben, welcher weniger als die Zahl p sein wird.

§4 **Bemerkung**

Von welcher Art diese Reste sind, die aus der Division der einzelnen Quadratzahlen durch irgendeine Primzahl p entsprießen, habe ich beschlossen, in dieser Abhandlung sorgfältiger zu untersuchen. Es werden nämlich hier sehr viele hervorstechende Phänomene auftauchen, mit deren Betrachtung die Natur der Zahlen nicht unwesentlich erhellt wird. So außergewöhnliche tiefe Wahrheiten liegen aber noch in der Lehre der Zahlen im Verborgenen, auf das Entwickeln welcher die Mühe nicht vergebens verwendet zu werden scheint.

§5 ## *Lehrsatz 2*

Wenn die ins Unendliche fortgesetzte Reihe der Quadrate in Glieder aufgeteilt wird, deren einzelne aus p Termen bestehen, also auf diese Weise

$$1, 4 \ldots pp| \, (p+1)^2, \ldots, 4pp| \, (2p+1)^2, \ldots, 9pp| \, (3p+1)^2, \ldots, 16pp| \text{ etc.}$$

dann, wenn die einzelnen Terme irgendeines einzigen Gliedes durch die Primzahl p geteilt werden, werden dieselben Reste und in derselben Reihenfolge wiederkehren.

Beweis.

Wenn nämlich die ersten Terme der einzelnen Glieder $1, (p+1)^2, (2p+1), (3p+1)^2$, etc. durch p geteilt werden, werden sie denselben Rest $= 1$ geben. Und auf die gleiche Weise werden die zweiten Terme $4, (p+2)^2, (2p+2)^2, (3p+2)^2$, etc. durch p geteilt die gleichen Reste $= 4$ hervorbringen, wenn freilich $p > 4$ sei. Und auf dieselbe Weise tritt es klar zutage, dass die dritten Terme die gleichen Reste liefern und ebenso die vierten und fünften etc. Und im Allgemeinen, wenn der wie große Term auch immer des ersten Gliedes nun ist, werden die analogen Terme der übrigen Terme $(p+n)^2, (2p+n)^2, (3p+n)^2$, etc. sein, welche alle durch p geteilt denselben Rest zurücklassen, welcher der

Term nun ist. In den einzelnen Gliedern kehren also dieselben Reste zurück und in derselben Reihenfolge. □

§6 **Korollar 1**

Wenn wir also die Reste kennen, die aus Termen des ersten Gliedes entsprießen, werden wir zugleich die Reste haben, die aus der durch p durchgeführten Division aller übrigen Zahlen entsprungen.

§7 **Korollar 2**

Weil der letzte Term jedes Gliedes durch die Zahl p teilbar ist, wird der Rest $= 0$ sein, so wie der Rest des ersten Terms jedes Gliedes $= 1$ ist. Der Rest der zweiten Terme jedes Gliedes wird hingegen $= 4$ und der dritte $= 9$, der vierte $= 16$ etc. sein, wenn freilich $p > 4$ und $p > 9$ und $p > 16$ etc. ist.

§8 **Korollar 3**

So lange nämlich die Quadratzahlen $1, 4, 9, 16$, etc. kleiner sind als die Zahl p ist, werden jene selbst die Reste festlegen. Aus den folgenden größeren als jene Zahl p werden hingegen andere kleinere Reste als jene Zahl p ans Licht treten.

§9 **Bemerkung**

Aus der Natur der Division ist es bekannt, dass die Reste immer kleiner sind als der Teiler p, und wenn unter Umständen unbeabsichtigterweise ein größer Rest als der Teiler p zurückgelassen wird, wird er durch Subtraktion von p, sooft es geschehen kann, auf eine kleinere Zahl als p reduziert werden. So wird der Rest $p + a$ und im Allgemeinen $np + a$, welcher unter Umständen aus der Division durch p hervorgehen wird, dem Rest a gleichwertig sein; und weil über Reste, die aus der Teilung von Zahlen durch p entsprießen, gehandelt wird, können als diese Reste a, $p + a$, $2p + a$ und $np + a$ für äquivalent gehalten werden, alle gehen natürlich auf den Wert a zurück; weil diese Reduktion leicht ist, werden wir sie sicher missachten können oder als schon durchgeführt annehmen können. So , wenn die Quadratzahlen $1, 4, 9, 16, 25$, etc. durch die Zahl p geteilt werden, wird nichts im Wege stehen, dass wir sagen, dass die daher herstammenden Reste $1, 4, 9, 16, 25$, etc. sind, auch wenn hier größere Zahlen als der Teiler p auftauchen. Im Übrigen ist es anzunehmen, dass dieser Lehrsatz seine Gültigkeit beibehält, ob der Teiler p eine Primzahl ist oder nicht.

§10 **Korollar 4**

Weil der letzte Term pp des ersten Gliedes keinen Rest liefert, werden alle Reste, die freilich aus der ganzen Reihe der Quadrate entspringen können, aus diesen Termen $1, 4, 9, 16, \ldots, (p-1)^2$ entsprießen, deren Anzahl $= p - 1$ ist.

§11 **Korollar 5**

Es können also nicht mehr Reste entspringen als $p - 1$; dies ist freilich per se klar. Weil nämlich alle Reste kleiner sind als der Teiler p ist, aber die Anzahl aller Zahlen kleiner als p also $= p - 1$ ist, kann auch die Anzahl der übrigen Teiler nicht größer sein.

§12 ## *Lehrsatz 3*

Wenn alle Terme der Reihe der Quadrate

$$1, 4, 9, 16, \text{ etc.}$$

durch irgendeine Zahl p geteilt werden und die Reste notiert werden, werden unter diesen Resten nicht alle Zahlen kleiner als p auftreten.

Beweis.
Denn alle Reste, die freilich aus der Division aller Quadrate durch die Zahl p entspringen, resultieren aus diesen Termen

$$1, 4, 9, 16, \ldots, (p-4)^2, (p-3)^2, (p-2)^2, (p-1)^2$$

die Anzahl welcher Terme $= p - 1$ ist; und daher treten ebenso viele Reste hervor. Aber diese Reste sind nicht alle verschieden zueinander; denn der letzte Term $(p-1)^2 = pp - 2p + 1$ lässt durch p geteilt den Rest $= 1$ zurück, denselben natürlich, welchen der erste Term 1 zurücklässt. Auf die gleiche Weise liefert der vorletzte Term $(p-2)^2 = pp - 4p + 4$ denselben Rest, wie der zweite Term 4; und der vorvorletzte Term $(p-3)^2$ gibt denselben Rest, wie der dritte Term 9. Und im Allgemeinen gibt der Term der Ordnung n, der nn ist, denselben Rest, welchen der Term der Ordnung $p - n$ gibt, der $(p-n)^2$ ist. Weil also die Reste, die aus diesen Termen $1, 4, 9, \ldots, (p-1)^2$ entspringen und deren Anzahl $= p - 1$ ist, nicht alle voneinander verschieden sind, können in ihnen nicht alle kleineren Zahlen als p, deren Anzahl $= p - 1$ ist, auftauchen können. □

§13 **Korollar 1**

Weil also je zwei Reste immer gleich sind, geht die Anzahl der verschiedenen Reste auf die Hälfte $\frac{p-1}{2}$ zurück, wenn freilich $p-1$ eine gerade Zahl ist; aber wenn $p-1$ eine ungerade Zahl ist, oder p eine gerade, dann wird die Anzahl der verschieden Reste $= \frac{p}{2}$ sein; in diesem Fall wird nämlich ein mittlerer Rest gegeben sein, welcher keinen ihm gleichen hat.

§14 **Korollar 2**

Weil also die Anzahl aller Zahlen kleiner als $p = p-1$ ist, tritt es klar zutage, dass die Hälfte dieser Zahlen bei den Resten auftritt; und es werden daher Zahlen gegeben sein, die aus der Division von Quadratzahlen durch die Zahl p nie zurückgelassen werden, allein ausgenommen dem Fall, in dem $p = 2$ ist, weil $p - 1 = \frac{p}{2} = 1$ ist.

§15 **Korollar 3**

Welche Zahl auch immer also ferner p ist, durch welche die Quadratzahlen geteilt werden, von den kleineren Zahlen als p werden immer mindestens $\frac{p-1}{2}$ oder $\frac{p-2}{2}$ vorhanden sein, die unter den Resten nicht aufgefunden werden. Der erste Fall gilt, wenn p eine ungerade Zahl ist, der zweite, wenn p eine gerade.

§16 **Korollar 4**

Daher scheiden sich also die kleineren Zahlen der Teiler p, deren Menge $= p-1$ ist, von selbst in zwei Klassen, deren eine die in den Resten auftretenden enthält, die anderen hingegen die, die in der Klasse der Reste nicht auftauchen. Diese Zahlen werde ich hier „Nicht-Reste“ nennen.

§17 **Bemerkung**

Damit diese Dinge besser Begriffe werden wird es förderlich sein, einige Beispiele, in denen Reste und nicht-Reste unterschieden werden, angeschaut zuhaben.

Es sei	Reihe	Reste	Nicht-Reste
$p = 3$	1	1	2
	4	1	
4	1	1	2, 3
	4	0	
	9	1	
5	1	1	2, 3
	4	4	
	9	4	
	16	1	
6	1	1	2, 5
	4	4	
	9	3	
	16	4	
	25	1	
7	1	1	3, 5, 6
	4	4	
	9	2	
	16	2	
	25	4	
	36	1	
8	1	1	2, 3, 5, 6, 7
	4	4	
	9	1	
	16	0	
	25	1	
	36	0	
	49	1	

Es sei	Reihe	Reste	Nicht-Reste
$p = 9$	1	1	2, 3, 5, 6, 8
	4	4	
	9	0	
	16	7	
	25	7	
	36	0	
	49	4	
	64	1	
10	1	1	2, 3, 7, 8
	4	4	
	9	9	
	16	6	
	25	5	
	36	6	
	49	9	
	64	4	
	81	1	
11	1	1	2, 6, 7, 8, 10
	4	4	
	9	9	
	16	5	
	25	3	
	36	3	
	49	5	
	64	9	
	81	4	
	100	1	

Es sei	Reihe	Reste	Nicht-Reste
$p = 12$	1	1	
	4	4	
	9	9	
	16	4	
	25	1	
	36	0	$2, 3, 5, 6, 7, 8, 10, 11$
	49	1	
	64	4	
	81	9	
	100	4	
	121	1	

Daher wird erkannt, dass die Anzahl der Nicht-Reste zuweilen entweder $\frac{p-1}{2}$ oder $\frac{p-2}{2}$ ist, je nachdem ob p entweder eine ungerade Zahl war, manchmal sogar größer ist, niemals aber kleiner ist, ganz und gar wie es der Beweis des Lehrsatzes erfordert.

§18

Lehrsatz 4

Damit alle Reste, die aus der Teilung von Quadraten durch irgendeine Zahl p resultieren können, gefunden werden, ist es nur von Nöten, die Quadrate von der Einheit aus bis zum Term $\left(\frac{p-1}{2}\right)^2$ oder $\left(\frac{p}{2}\right)^2$, je nachdem ob p entweder eine ungerade oder eine gerade Zahl war, durch p zu teilen.

Beweis.
Zuvor haben wir schon bewiesen, dass alle Reste aus der Division dieser Terme hervortreten

$$1, 4, 9, 16, \ldots, (p-1)^2$$

des Weiteren haben wir aber gesehen, dass die Reihe der daher entsprießenden Reste reziprok ist oder in umgekehrter Reihenfolge geschrieben dieselbe bleibt. Daher werden alle Reste, sofern sie einander verschieden sind, aufgefunden werden, wenn von dieser Reihe die Terme nur bis hin zur Mitte genommen

werden, woher, wenn p eine ungerade und daher $p-1$ eine gerade Zahl ist, alle Zahlen, die unter den Resten auftauchen, aus diesen Termen hervorgehen werden

$$1, 4, 9, 16, \ldots, \left(\frac{p-1}{2}\right)^2$$

Wenn aber p eine gerade Zahl ist, weil die obere Progression einen mittleren Term hat, welcher beim Rückwärtsgehen sich selbst entspricht, werden alle Reste aus diesen Termen entspringen

$$1, 4, 9, 16, \ldots, \left(\frac{p}{2}\right)^2$$

□

§19 **Korollar 1**

Wenn also p eine ungerade Zahl ist, beispielsweise $p = 2q+1$, werden alle Reste nur aus diesen Quadraten $1, 4, 9, 16, \ldots, qq$ erkannt werden. Aber wenn p eine gerade Zahl ist, beispielsweise $p = 2q$, werden diese Quadrate $1, 4, 9, 16, \ldots, qq$ alle Reste hervorbringen.

§20 **Korollar 2**

Wenn alle diese Reste einander ungleich waren, weil deren Anzahl $= q$ ist, wird im ersten Fall, in dem $p = 2q+1$ und $p-1 = 2q$ ist, die Anzahl der Nicht-Reste $= q$ sein. Im zweiten Fall, in dem $p = 2q$ und $p-1 = 2q-1$ ist, wird die Anzahl aller Nicht-Reste $= q-1$ sein.

§21 **Korollar 3**

Wenn a irgendeine Zahl nicht größer als $\frac{p-1}{2}$ oder $\frac{p}{2}$ ist und der Rest bekannt ist, welcher aus der Division des Quadrates aa durch die Zahl p resultiert, werden alle in dieser allgemeinen Form $(np \pm a)^2$ enthaltenen Quadrate denselben Rest liefern. Aber es werden ganz und gar alle Zahlen in der Form $np \pm a$ eingeschlossen, so dass a weder $\frac{p-1}{2}$ noch $\frac{p}{2}$ überschneidet.

§22 **Bemerkung**

Damit sich die natürliche Beschaffenheit von Zahlen, die Reste sind, leichter erforschen lässt, wollen wir die Reihe der Reste mit diesen Buchstaben $1, \alpha, \beta, \gamma, \delta, \epsilon, \xi$, etc. für den Teiler p darstellen, so dass die Anzahl dieser Terme entweder $\frac{p-1}{2}$ oder $\frac{p}{2}$ ist, je nachdem ob p entweder eine ungerade oder gerade Zahl ist. Zuerst tritt es also klar zutage, dass in dieser Reihe $1, \alpha, \beta, \gamma, \delta, \epsilon$, etc.

der Reihe nach alle Quadratzahlen auftauchen, die freilich kleiner als die Zahl p seien, die übrigen aber die Reste sind, die in der Division größerer Quadrate durch dieselbe Zahl p zurückgelassen werden. Die übrigen Eigenschaften der Reste werden wir in den folgenden Lehrsätzen ausfindig machen.

§23

Lehrsatz 5

Wenn in der Reihe der Reste $1, \alpha, \beta, \gamma, \delta$, etc. irgendeine Zahl r auftaucht, werden ebendort auch alle Potenzen von r^2, r^3, r^4, r^5, etc. oder Reste aufgefunden werden, die aus der Division dieser Potenzen durch die vorgelegte Zahl p entsprießen.

Beweis.
Es treten also der Rest r aus dem Quadrat da ans Licht, so dass $aa = mp + r$ ist; und das Quadrat $a^4 = (mp + r)^2$ wird durch p geteilt denselben Rest ergeben, welcher aus rr entspringt, und aus dem Quadrat $a^6 = (mp + r)^3$ entspringt derselbe Rest wie aus r^3; und auf die gleiche Weise werden die Reste der Quadrate a^8, a^{10}, a^{12}, etc. mit den Resten der Terme r^4, r^5, r^6, etc. übereinstimmen. Aber die aus allen wie großen Quadraten auch immer herstammenden Reste treten schon aus den kleinsten Quadraten $1, 4, 9, 16, \ldots, \left(\frac{p-1}{2}\right)^2$ oder $\left(\frac{p}{2}\right)$ hervor und sind daher in der Reihe der Reste $1, \alpha, \beta, \gamma, \delta$, etc. enthalten. Wenn also in dieser Reihe die Zahl r auftaucht, werden ebendort auch die Terme r^2, r^3, r^4, r^5, etc. oder die Reste auftauchen, die aus deren Division durch den vorgelegten Teiler p zurückgelassen werden. □

§24 **Korollar 1**

Welche der Potenzen r^2, r^3, r^4, r^5, etc. also kleiner als p waren, die werden in der Reihe der Reste $1, \alpha, \beta, \gamma, \delta$, etc. aufgefunden werden. Aber die höheren Potenzen werden ihre Reste, die sie durch p geteilt zurücklassen, ebendort einführen.

§25 **Korollar 2**

Wenn $r = 1$ ist, weil alle seine Potenzen $= 1$ sind, entsprießen aus ihnen nur der eine einzige Terme 1 in der Reihe der Reste $1, \alpha, \beta, \gamma, \delta$, etc. Und daher wird aus diesem Fall kein neuer Term in der Reihe der Reste erkannt.

§26 **Korollar 3**

Weil in der Reihe der Reste nicht mehr Terme auftauchen als entweder

$\frac{p-1}{2}$ oder $\frac{p}{2}$, können auch nicht mehr verschiedene Reste aus den Potenzen r^2, r^3, r^4, r^5, etc., auch wenn sie ins Unendliche fortgesetzt werden, hervorgehen. Daher werden unendlich viele dieser Potenzen durch p geteilt die gleiche Reste liefern.

§27 **Korollar 4**

Es liefern also diese Potenzen r^m und r^n denselben Rest und deren Differenz $r^m - r^n$ oder $r^n \left(r^{m-n} - 1\right)$ wird durch die Zahl p teilbar sein. Daher, wenn der Faktor r^n zu p prim war, was passiert, wenn der Rest r zu p prim war, wird der andere Faktor $r^{m-n} - 1$ durch p geteilt die Einheit zurücklassen.

§28 **Korollar 5**

Es wird also eine Potenz r^λ gegeben sein, die durch p geteilt die Einheit zurücklässt, welche natürlich in der Reihe der Reste enthalten ist, wenn freilich r zur Zahl p prim ist. Dann wird aber die Potenz $r^{\lambda+1}$ den Rest r geben, die Potenz $r^{\lambda+2}$ den Rest r^2 und $r^{\lambda+3}$ den Rest r^3 etc. und so bringen diese höheren Potenzen dieselben Reste erneut hervor wie die niederen Potenzen r, r^2, r^3, etc.

§29 **Korollar 6**

Weil also nicht mehr verschiedene Reste hervor treten können als entweder $\frac{p-1}{2}$ oder $\frac{p}{2}$, tritt es klar zutage, dass eine Zahl λ nicht größer als $\frac{p-1}{2}$ oder $\frac{p}{2}$ gegeben ist, so dass die Potenz r^λ durch p geteilt die Einheit zurücklässt.

§30 **Bemerkung**

Daher wird also eingesehen, auf welche Weise es geschehen kann, dass, auch wenn die Potenzen r^2, r^3, r^4, r^5, etc. ins Unendliche fortschreiten, dennoch aus ihnen in Bezug auf die Anzahl endliche Reste entspringen, wenn sie durch den Teiler p geteilt werden. Ich habe aber freilich in der oberen Abhandlung bewiesen, wenn r eine zu p prime Zahl ist, dass immer eine Potenz λ solcher Art gegeben ist, die durch p geteilt die Einheit zurücklässt, wenn r schon in der Reihe der aus den Quadraten entstandenen Reste enthalten ist, dass dann der Exponent λ sogar kleiner wird als $\frac{p}{2}$.

§31

Lehrsatz 6

Wenn in der Reihe der Reste $1, \alpha, \beta, \gamma, \delta$, etc., die aus der Division der Quadratzahlen durch die Zahl p entspringen, die Zahlen r und s entspringen, wird ebendort auch das Produkt dieser Zahlen rs der der Rest auftauchen, welcher

aus seiner Teilung durch die Zahl p entsteht.

Beweis.
Es trete der Rest r aus dem Quadrat aa und der Rest s aus dem Quadrat bb hervor; es wird $aa = mp + r$ und $bb = np + s$ sein; daher wird das Quadrat werden

$$aabb = mnpp + msp + nrp + rs$$

welches also durch p geteilt den Rest rs zurücklassen wird, oder wenn $rs > p$ ist, wird es denselben Rest zurücklassen, welcher aus rs entspringt. Daher, weil der aus dem Quadrat $aabb$ entsprossene Rest in der Reihe der Reste enthalten ist, wird dort auch rs oder der daher entspringende Rest aufgefunden werden. □

§32 **Korollar 1**
Wenn also in der Reihe der Reste $1, \alpha, \beta, \gamma, \delta$, etc. die zwei Zahlen r und s auftauchen, werden ebendort auch nicht nur die Potenzen r, r^2, r^3, r^4, etc. und s^2, s^3, s^4, etc. auftauchen, sondern auch die Produkte aus irgendwelchen zwei Termen $rs, r^2s, r^3s, r^2s^2, rs^3$, etc.

§33 **Korollar 2**
Daher tritt es also klar zutage, wenn die Formel $\frac{1}{(1-r)(1-s)}$ in eine Reihe aufgelöst wird

$$1 + r + s + rr + rs + ss + r^3 + rrs + rss + s^3 \text{ etc.}$$

dass die einzelnen Terme dieser Reihe in der Reihe der Reste oder auch die aus diesen Termen durch Teilung durch p entspringenden Reste auftauchen.

§34 **Korollar 3**
Aber auch wenn die Anzahl dieser Terme unendlich ist, steht dennoch fest, dass aus ihnen nicht mehr Reste als entweder $\frac{p-1}{2}$ oder $\frac{p}{2}$ hervorgebracht werden können, je nachdem ob p entweder eine ungerade oder gerade Zahl war.

§35 **Bemerkung**
Damit es besser klar wird, auf welche Weise aus diesen von der Anzahl unendlichen Termen dennoch eine endliche Anzahl der verschiedenen Reste und zwar weder größer als $\frac{p-1}{2}$ noch als $\frac{p}{2}$ entspringt, wollen wir ein konkretes

Beispiel entwickeln und es sei $p = 19$, es wird $\frac{p-1}{2} = 9$ sein, woher aus diesen Quadraten

$$1, 4, 9, 16, 25, 36, 49, 64, 81$$

diese Reste entspringen werden

$$1, 4, 9, 16, 6, 17, 11, 7, 5$$

Aus dieser Reihe der Reste wollen wir diese zwei Zahlen 5 und 6 betrachten, aus denen wir zuerst die Reihe der Potenzen bilden wollen

$$5, 25, 125, 625, 3125, 15625, 78125, \text{ etc.}$$
$$6, 36, 216, 1296, 7776, 4656, 279936, \text{ etc.}$$

Aus jener Reihe gehen durch $p = 19$ geteilt diese Reste hervor

$$5, 6, 11, 17, 9, 7, 16, 4, 1$$

der folgende Rest wird natürlich immer gefunden, wenn der vorhergehende mit 5 multipliziert wird und das Produkt, wenn es > 19 ist, unter 19 herabgedrückt wird. Auf die gleiche Weise werden aus den Potenzen der Zahl 6 diese Reste hervorgehen

$$6, 17, 7, 4, 5, 11, 9, 16, 1$$

Wenn weiter diese einzelnen Reste mit den einzelnen oberen multipliziert werden und die Produkte unter 19 herabgesenkt werden, gehen dieselben Zahlen hervor; es werden nämlich die untere Reihe zuerst mit 5, dann mit $6, 11, 17$, etc. multipliziert wie folgt

$$\begin{aligned}
\text{mit } 5: &\quad 11, 9, 16, 1, 6, 17, 7, 4, 5 \\
\text{mit } 6: &\quad 17, 7, 4, 5, 11, 9, 16, 1, 6 \\
\text{mit } 11: &\quad 9, 16, 1, 6, 17, 7, 4, 5, 11 \\
\text{mit } 17: &\quad 7, 4, 5, 11, 9, 16, 1, 6, 17 \\
\text{mit } 9: &\quad 16, 1, 6, 17, 7, 4, 5, 11, 9 \\
\text{mit } 7: &\quad 4, 5, 11, 9, 16, 1, 6, 17, 7 \\
\text{mit } 16: &\quad 1, 6, 17, 7, 4, 5, 11, 9, 16 \\
\text{mit } 4: &\quad 5, 11, 9, 16, 1, 6, 17, 7, 4
\end{aligned}$$

Es wird also erkannt, auf welche Weise auch immer diese die Reihe der Reste festgelegten Zahlen $1, 4, 9, 16, 6, 17, 11, 7, 5$ miteinander durch Multiplikation verbunden werden, wenn sie freilich nach der Division durch 19 unter 19 herabgesenkt werden, dass immer dieselben Zahlen wiederkehren und wie eine Zahl derer, die keine Reste sind, natürlich $2, 3, 8, 10, 12, 13, 14, 15, 18$, etc. hervorgehen.

§36 **Korollar 4**

Wenn also $1, \alpha, \beta, \gamma, \delta$, etc. die Reihe der Reste ist, die aus der Teilung der Quadrate durch die Zahl p resultiere, werden in der selben Reihe auch die Produkte aus je zweien oder mehreren der Zahlen $\alpha, \beta, \gamma, \delta$, etc. auftauchen. Wenn daher also dieser Ausdruck $\left(\frac{1}{(1-\alpha)(1-\beta)(1-\gamma)(1-\delta)\text{ etc.}}\right)$ in eine Reihe entwickelt wird, werden all ihre Terme in der Reihe der Reste auftauchen.

§37

Lehrsatz 7

Wenn in der Reihe der Reste $\alpha, \beta, \gamma, \delta$, etc., die aus der Teilung der Quadrate durch die Zahl p hervorgehen, die Zahlen r und rs aufgefunden werden, die zu p prim seien, von welchen jener ein Faktor dieser ist, dann wird in derselben Reihe der Reste auch die Zahl s enthalten sein.

Beweis.

Es trete der Rest r aus dem Quadrat aa und rs aus bb hervor; es wird $aa = mp + r$ und $bb = np + rs$ sein; daher wird $bb - aas = np - mps$ und so wird $bb - aas$ durch p teilbar sein. Aber weil r und rs zu p prime Zahlen sind, wenn auch die Quadrate aa und bb zu p prim sein; daher, wenn diese Quadrate aa und bb nicht zueinander prim sind, werden sie durch den gemeinsamen quadratischen Teiler auf prime zurückgeführt werden können, so dass $bb - aas$ durch p teilbar bleibt. Es seien b und a zueinander prime Zahlen, und weil auch diese Form $(mp \pm b)^2 - aas$ durch p teilbar ist, kann immer für m eine Zahl solcher Art angegeben werden, dass $mp \pm b$ ein Vielfaches von a ist. Es sei also $mp \pm b = ac$; es wird $aacc - aas$ durch p teilbar sein; weil dies $= aa(cc - s)$ und der eine Faktor aa zu p prim ist, ist es notwendig, dass der andere Faktor durch $cc - s$ durch p teilbar ist, woher das Quadrat cc durch p geteilt s zurücklassen wird, woher die Zahl s in der Reihe der Reste $1, \alpha, \beta, \gamma, \delta$, etc. aufgefunden werden ist, wenn freilich dort die Zahlen r und rs auftauchen und sie zu p prim sind. □

§38 **Korollar 1**

Damit also die Gültigkeit des Lehrsatzes bestehen bleibt, ist es notwendig, dass die Zahl r und rs oder r und s zum Teiler p prim sind. Oben haben wir nämlich gesehen, wenn $p = 12$ ist, dass in den Resten die Zahlen 4 und 0 oder 4 und 12 aufgefunden werden; daher folgt aber nach Festlegen von $r = 4$ und $rs = 12$ nicht, dass die Zahl $s = 3$ in den Resten aufgefunden wird, weil r und s nicht zueinander prim sind; und in der Tat ist sogar die Zahl 3 unter den Nicht-Resten enthalten.

§39 **Korollar 2**

Wenn aber der Teiler p eine Primzahl ist, weil dann alle Reste $\alpha, \beta, \gamma, \delta$, etc. zu ihr prim sind, wenn in ihnen die Zahlen r und rs auftauchen, dann wird auch gewiss in Ihnen die Zahl s auftauchen.

§40 **Korollar 3**

Wenn unter den Resten die zu p primen Zahlen r und s auftauchen, weil dem Rest r die Reste $p + r$, $2p + r$ und im Allgemeinen $np + r$ gleichwertig anzusehen sind, wenn $np + r = ts$ war, dann wird auch die Zahl t unter den Resten aufgefunden werden.

§41 **Bemerkung**

Damit wir nicht verpflichtet sind, auf Ausnahmen von dieser Art, wann immer die Reste nicht zu p prime Zahlen sind, zu achten, wollen wir im Folgenden festlegen, dass der Teiler p immer eine Primzahl ist; und weil die aus zwei entspringenden Reste offensichtlich wird, sei der Teiler p zugleich eine ungerade Zahl oder $p = 2q + 1$; dann wird also die Reihe der Reste aus diesen Termen gebildet werden

$$1, 4, 9, 16, \ldots, qq$$

so dass deren Anzahl, sofern sie einander verschieden sind, nicht größer sein kann als q. Wenn also die Reste aus diesem primen Teiler $p = 2q + 1$ $1, \alpha, \beta, \gamma, \delta$, etc sind, werden in dieser Reihe nur die Produkte aus je zweien oder mehreren der Terme $\alpha, \beta, \gamma, \delta$, etc. auftauchen, aber weil alle diese Reste zu p prim sind, wenn unter ihnen r und rs auftauchen, so dass einer durch einen anderen teilbar ist, dann wird der daher entsprießende Quotient s in derselben Reihe der Reste enthalten sein.

§42 ## *Lehrsatz 8*

Wenn aus dem primen Teiler $p = 2q + 1$, durch welchen alle Quadratzahlen geteilt werden, die Reihe der Reste $1, \alpha, \beta, \gamma, \delta, \epsilon$, etc. entsprießt, deren Anzahl $= q$ ist, werden all diese Reste einander ungleich sein.

Beweis.
Zuerst tritt es klar zutage, dass kein Rest in dieser Reihe $= 0$ sein kann; weil sie nämlich aus den nicht größeren Quadraten qq entsprießen, ist keine dieser Quadrate durch die Primzahl $p = 2q + 1$ teilbar; also wird die Null unter diesen Resten um vieles weniger zweimal auftauchen können. Wir wollen aber festlegen, dass die zwei Reste, die aus den Quadraten aa und bb entspringen, gleich sind und die Differenz dieser Quadrate $aa - bb$ wird durch den Teiler $p = 2q + 1$ teilbar sind. Aber weil all diese Reste $1, \alpha, \beta, \gamma, \delta$, etc. aus den kleinsten Quadraten, die qq nicht über Augen, entspringen, werden jene Quadrate aa und bb qq nicht überragen und es wird deshalb weder $a > q$ noch $b > q$ und deshalb auch nicht $a + b > 2q$ sein, woher gewiss $a + b < p$ sein wird. Weil also die Differenz der Quadrate $aa - bb$ durch p teilbar ist, wenn freilich die daher entsprießenden Reste gleich wären und p eine Primzahl ist, werde entweder die Summe $a + b$ oder die Differenz $a - b$ durch p teilbar; jedes von beiden kann aber so wegen $a - b < p$ wie wegen $a + b < p$ nicht geschehen. Also sind alle Reste, die aus der Division der Quadrate $1, 4, 9, 16, \ldots, qq$ durch die Primzahl $p = 2q + 1$ resultieren, einander ungleich. □

§43 **Korollar 1**
Also die Anzahl aller verschiedenen Reste, die aus der Teilung der Quadrate durch die Primzahl $p = 2q + 1$ entspringen, ist gewiss $= q$, zuvor ist nämlich gezeigt worden, dass sie nicht größer als q, hier haben wir aber dargetan, dass sie nicht kleiner ist als q.

§44 **Korollar 2**
Weil die Anzahl aller kleineren Zahlen als der Teiler $p = 2q + 1$ kleiner $= p - 1 = 2q$ ist, tritt es klar zutage, dass nur die Hälfte dieser Zahlen in der Reihe der Reste $1, \alpha, \beta, \gamma, \delta$, etc. auftaucht und sie festlegt, die andere Hälfte hingegen die Reihe der Nicht-Reste festlegt und daher, wenn p eine Primzahl ist, die Reihe der Nicht-Reste auch aus q Zahlen besteht.

§45 **Korollar 3**
Wenn also x irgendeine Zahl aus der Reihe der dem Teiler p entsprechenden

Nicht-Reste, können wir sicher bestätigen, was auch immer n ist, dass keine Zahl in dieser Form $np + x$ ein Quadrat sein kann.

§46 **Bemerkung**

Weil wir nun unsere Untersuchung nur auf prime Teiler richtet, wird es zuträglich sein, so die Reste wie die Nicht-Reste, die kleineren Primzahlen entsprechen, hier darzubieten. Im Allgemeinen natürlich, wenn der Teiler p ist, wollen wir die Reihe der Reste durch $1, \alpha, \beta, \gamma, \delta$, etc. und die Reihe der Nicht-Reste darstellen; und damit leichter zusammen so die Reste wie die Nicht-Reste gezeigt werden, wollen wir sie auf diese Weise darlegen:

$$p \left\{ \begin{matrix} 1, & \alpha, & \beta, & \gamma, & \delta, & \epsilon, & \xi, & \text{etc.} \\ & a, & b, & c, & d, & e, & f, & \text{etc.} \end{matrix} \right\}$$

Wir werden natürlich in jedem Fall zwei Reihen von Zahlen schreiben, deren obere die Reste, die untere die Nicht-Reste enthält, und jeder der beiden werden wir den Teiler p, auf welchen sie sich beziehen, voranstellen. Auf diese Weise werden die Reste und Nicht-Reste, die aus den einfacheren Primteilern resultieren, so angezeigt werden:

$$3 \left\{ \begin{matrix} 1 \\ 2 \end{matrix} \right\} \quad 5 \left\{ \begin{matrix} 1, & 4 \\ 2, & 3 \end{matrix} \right\} \quad 7 \left\{ \begin{matrix} 1, & 4, & 2 \\ 3, & 5, & 6 \end{matrix} \right\} \quad 11 \left\{ \begin{matrix} 1, & 4, & 9, & 5, & 3 \\ 2, & 6, & 7, & 8, & 10 \end{matrix} \right\}$$

$$13 \left\{ \begin{matrix} 1, & 4, & 9, & 3, & 12, & 10 \\ 2, & 5, & 6, & 7, & 8, & 11 \end{matrix} \right\} \quad 17 \left\{ \begin{matrix} 1, & 4, & 9, & 16, & 8, & 2, & 15, & 13 \\ 3, & 5, & 6, & 7, & 10, & 11, & 12, & 14 \end{matrix} \right\}$$

$$19 \left\{ \begin{matrix} 1, & 4, & 9, & 16, & 6, & 17, & 11, & 7, & 5 \\ 2, & 3, & 8, & 10, & 12, & 13, & 14, & 15, & 18 \end{matrix} \right\}$$

$$23 \left\{ \begin{matrix} 1, & 4, & 9, & 16, & 2, & 13, & 3, & 18, & 12, & 8, & 6 \\ 5, & 7, & 10, & 11, & 14, & 15, & 17, & 19, & 20, & 21, & 22 \end{matrix} \right\}$$

$$29 \left\{ \begin{matrix} 1, & 4, & 9, & 16, & 25, & 7, & 20, & 6, & 23, & 13, & 5, & 28, & 24, & 22 \\ 2, & 3, & 8, & 10, & 11, & 12, & 14, & 15, & 17, & 18, & 19, & 21, & 26, & 27 \end{matrix} \right\}$$

Die Reste sind hier in der Reihenfolge, in welcher sie aus den Quadraten entsprießen, festgelegt worden, die Nicht-Reste, weil sie durch keine Struktur

verbunden werden, haben wir durch Fortschreiten von den kleinsten zu größeren zusammengestellt. Diese Beispiele werden auch zu dem Zweck dienen können, dass in ihnen die zuvor bewiesenen Eigenschaften der Reste erforscht werden.

§47

Lehrsatz 9

Wenn aus der Teilung der Quadrate durch die Primzahl $p = 2q + 1$ die Reihe von Resten $1, \alpha, \beta, \gamma, \delta$, etc. und diese Reihe von Nicht-Resten a, b, c, d, e, etc. entsprießt und in dieser Reihe der Nicht-Reste die Zahl r auftaucht, werden in derselben auch alle diese Zahlen $\alpha r, \beta r, \gamma r, \delta r$, etc. oder deren durch die Teilung durch p zurückgelassenen Reste auftauchen.

Beweis.
Denn irgendeine dieser Zahlen, wie αr, ist entweder in der Reihe der Reste oder der Nicht-Reste enthalten. Aber weil α in der Reihe der Reste enthalten ist, wenn αr ebendort enthalten wäre, befände sich notwendigerweise auch r in der Reihe der Reste. Daher, weil nach der Annahme r aus der Reihe der nicht-Reste ist, wird die Zahl αn nicht in der Reihe der Reste sein; es wird also αr in der Reihe der nicht-Reste auftreten, welches selbe über die Zahlen $\beta r, \gamma r, \delta r$, etc. gilt. Was wir aber über diese Produkte $\beta r, \gamma r, \delta r$, etc. bewiesen haben, wenn sie größer als p, ist auch über die Reste zu verstehen, die diese Produkte durch p geteilt zurücklassen. □

§48 **Korollar 1**

Weil alle Zahlen $1, \alpha, \beta, \gamma, \delta$, etc., deren Anzahl $= q$ ist, einander verschieden sind, folgt, dass auch alle diese Zahlen $r, \alpha r, \beta r, \gamma r, \delta r$, etc. einander verschieden sind; daher, wenn man alle Reste hat, werden aus einem einzigen bekannten Nicht-Rest alle übrigen Nicht-Reste definiert.

§49 **Korollar 2**

Es wird also die Reihe $r, \alpha r, \beta r, \gamma r, \delta r$, etc. gänzlich alle Nicht-Reste geben; sie enthält nämlich q verschiedene Zahlen und ebenso viele und nicht mehr Nicht-Reste existieren, wenn freilich der Teiler p eine Primzahl ist.

§50 **Korollar 3**

Wenn also aus der Reihe der Nicht-Reste eine beliebige andere Zahl s genommen wird, liefern ihre Produkte $\alpha s, \beta s, \gamma s$, etc. keine andere Zahlen für die

nicht-Reste, außer welche aus jeglicher anderen r auf diese Weise aufgefunden worden sind.

§51

Lehrsatz 10

Die Produkte aus zwei Zahlen der Reihe der Nicht-Reste ist in der Reihe der Reste enthalten, wenn freilich diese Reste aus der Division von Quadratzahlen durch gewisse Primzahl entsprießen.

Beweis.
Es sei nämlich $p = 2q + 1$ der prime Teiler und die Reihe der Reste sei $1, \alpha, \beta, \gamma, \delta$, etc., die Reihe der Nicht-Reste sei aber a, b, c, d, e, etc. Wir haben aber gesehen, wenn r irgendein Nicht-Rest ist, dass die Reihe der Nicht-Reste auch auf diese Weise dargeboten wird

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

Nun besteht das Produkt aus irgendwelchen zweien dieser Terme $\alpha\beta r^2$ aus den zwei Faktoren $\alpha\beta$ und rr, von welchen jeder von beiden in der Reihe der Reste enthalten ist, weil alle Quadrate und deshalb auch rr dort auftreten; daher ist es klar, dass das Produkt aus jeglichen zwei Nicht-Resten in der Reihe der Reste enthalten ist. □

§52 **Korollar 1**

Wie also das Produkt aus zwei Resten einen Rest gibt, so wird auch das Produkt aus zwei Nicht-Resten einen Rest geben. Aber das Produkt aus einem Rest und einem Nicht-Rest erzeugt immer einen Nicht-Rest.

§53 **Korollar 2**

Daher liegt sogar, wie ein Rest durch einen Rest geteilt einen Rest gibt, dass so auch ein Nicht-Rest durch einen Nicht-Rest geteilt einen Rest gibt. Aber ein Rest durch einen Nicht-Rest oder umgekehrt ein Nicht-Rest durch einen Rest geteilt liefert einen Nicht-Rest.

§54 **Korollar 3**

So wie zwei nicht-Rest miteinander multipliziert einen Rest hervorbringen, so werden drei nicht-Reste miteinander multipliziert einen Nicht-Rest liefern; vier Nicht-Reste bringen hingegen wiederum einen Rest hervor, aber fünf einen Nicht-Rest und so weiter.

§55 **Definition**

Das Komplement eines Restes ist seine Abweichung vom Teiler, aus welchem er entsprungen ist; so, wenn der Teiler $= p$ und der Rest $= r$ ist, wird das Komplement des Restes $= p - r$ sein.

§56 **Korollar 1**

Weil in Bezug auf die Reste alle diese Zahlen $r, p + r, 2p + r$ und im Allgemeinen $np + r$ für dieselben gehalten werden, welche Zahl auch immer für n genommen wird, wird deren Komplement $= p - np - r$ sein; daher, wenn $n = 1$ genommen wird, wird das Komplement des Restes $r = -r$ sein.

§57 **Korollar 2**

Wenn $n = -1$ genommen wird, kann der Rest r auch durch $r - p$ ausgedrückt werden, so dass er negativ ist. Wenn nämlich in der Division der Quotient zu groß angenommen wird, wird zu negativen Resten gelangt. So wird der positive Rest r dem negativen Rest $r - p$ gleichwertig sein.

§58 **Korollar 3**

Wenn $r > \frac{1}{2}p$ ist, dann wird dieser Rest negativ durch $r - p$ ausgedrückt werden können, welcher kleiner als $\frac{1}{2}p$ sein wird. So, wenn die negativen Ausdrücke benutzt werden, werden alle Reste durch Zahlen nicht größer als die Hälfte des Teilers $\frac{1}{2}p$ dargeboten werden können. So wird man für den Teiler $p = 23$ diese durch nicht größere Zahllen als $\frac{23}{2}$ ausgedrückten Reste haben

$$1, 4, 9, -7, 2, -10, 3, -5, -11, 8, 6$$

Korollar 4

§59

Und auf die gleiche Weise werden auch die Nicht-Reste durch nicht größere Zahlen als $\frac{1}{2}p$ dargeboten werden können und es werden für den Teiler die Nicht-Reste diese sein

$$5, 7, 10, 11, -9, -8, -6, -3, -2, -1$$

Daher, wenn $p = 2q + 1$ ist, wird die Anzahl so der Reste wie der nicht-Reste $= q$ sein und in keiner der beiden Reihen tauchen größere Zahlen als q auf.

§60 **Korollar 5**

Wenn auf diese Weise die Reste ausgedrückt werden, tritt es sofort klar zutage, ob das Komplement eines gewissen Restes in derselben Reihe der Reste

enthalten ist oder nicht. Denn wenn $r4$ ein Rest ist, wird $-r$ sein Komplement sein, und umgekehrt, wenn $-r$ ein Rest ist, wird $+r$ sein Komplement sein. Daher, wenn in der Reihe der Reste nicht dieselbe Zahl zweimal auftaucht, positiv und negativ natürlich, ist ihr Komplement nicht in der Reihe der Rest enthalten.

§61 ## *Lehrsatz 11*

Wenn in der Reihe der Reste $1, \alpha, \beta, \gamma, \delta$, etc., die aus der Teilung der Quadrate durch die Primzahl $p = 2q + 1$ erzeugt werden, das Komplement eines einzigen Termes auftaucht, dann werden zugleich die Komplemente aller Terme in derselben Reihe auftauchen.

Beweis.
Es sei r der Rest, dessen Komplement $-r$ auch in der Reihe $1, \alpha, \beta, \gamma, \delta$, etc. auftauche. Weil also $-r$ durch r geteilt $-r$ gibt, wird in derselben Reihe auch die Zahl $-q$ auftauchen oder der Wert eines bestimmten der Buchstaben $\alpha, \beta, \gamma, \delta$, etc. wird $= -1$ sein. Weil ja also in derselben Reihe die Produkte aus zwei Termen zugleich aufgefunden werden, werden ebendort die Terme $-\alpha, -\beta, -\gamma, -\delta$, etc. auftauchen. Also wird das Komplement jedes Restes zugleich in der Reihe der Reste aufgefunden werden, wenn freilich das Komplement eines einzigen Termes in ihr auftaucht. □

§62 **Korollar 1**

Wenn also das Komplement eines Termes r also $-r$ in der Reihe der Reste enthalten ist, dann wird jede beliebige Zahl dieser Reihe zweimal auftauchen, zuerst natürlich positiv, dann aber auch negativ. Denn in der Reihe der Reste $1, \alpha, \beta, \gamma, \delta$, etc. werden auch die Terme $-1, -\alpha, -\beta, -\gamma, -\delta$, etc. enthalten sein.

§63 **Korollar 2**

Weil also in diesem Fall in der Reihe der Reste jeder beliebige Term zweimal auftaucht, wird die Anzahl aller Terme notwendig gerade sein. Aber die Anzahl aller Terme $= q$; wenn also q keine gerade Zahl ist, kann es nicht geschehen, dass die Komplemente der Reste zugleich in der Reihe der Reste enthalten sind.

§64 **Korollar 3**

Wenn also q eine ungerade Zahl ist, beispielsweise $q = 2n + 1$, so dass $p = 4n + 3$ ist, taucht in der Reihe der Reste überhaupt keine Zahl auf,

deren Komplement zugleich in der Reihe enthalten ist. Also werden alle Komplemente in diesem Fall in die Reihe der Nicht-Reste eingehen und es wird bei jeder der beiden die Anzahl der Terme ungerade $= q = 2n + 1$ sein.

§65 **Bemerkung**

Daher wird also der größte Unterschied erkannt, welcher zwischen Primzahlen der Form $p = 2q + 1$ besteht, je nachdem ob q eine gerade oder ungerade war, weil im zweiten Fall sicher wissen, dass das Komplement keines Restes in der Reihe der Reste enthalten ist. Wenn wir daher also im ersten Fall $q = 2n$, im zweiten $q = 2n - 1$ setzen, wird in jenem Fall die Primzahl $p = 4n + 1$, in diesem hingegen $p = 4n - 1$ sein; daher tritt es klar zutage, dass alle Primzahlen, zwei ausgenommen, entweder um die Einheit ein Vielfaches von vier überragen oder um die Einheit von selbigem nach unten abweichen und so erhalten wir zwei Klassen von Zahlen, deren eine in der Form $4n + 1$, die andere in der Form $4n - 1$ enthalten ist. Primzahlen der ersten Klasse $4n + 1$ sind also $5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97$, etc., von der zweiten Klasse $4n - 1$ hingegen diese $3, 7, 11, 19, 23, 31, 43, 47, 59, 67, 71, 79, 83$, etc. Über die Primzahlen der ersten Klasse hat Fermat einst ausgesprochen, dass die einzelnen die Aggregate zweier Quadrate sind, die Gültigkeit welches Lehrsatz ich nämlich schließlich nach vielen Versuchen bewiesen habe. Über die Zahlen der anderen Klasse wird aber leicht gezeigt, dass keine derer die Summe zweier Quadrate ist; ja ich werde sogar bald beweisen, dass nicht einmal eine Summe zweier Quadrate $aa + bb$ dargeboten werden kann, die durch eine Primzahl $p = 4n - 1$ solcher Art teilbar ist, wenn nicht jedes der beiden Quadrate aa und bb einzeln durch sie teilbar ist. Über diese Zahlen hat Fermat dennoch bekräftigt, dass die einzelnen die Aggregate entweder dreier oder vierer Quadrate sind; so sehen wir, da es $3 = 1 + 1 + 1$, $7 = 1 + 1 + 1 + 4$, $11 = 1 + 1 + 9$, $19 = 1 + 9 + 9$, $23 = 1 + 4 + 9 + 9$, $31 = 4 + 9 + 9 + 9 = 1 + 1 + 4 + 25$, aber keine Zahl dieser Art existiert, die nicht zumindest in vier Quadrate aufgelöst werden kann. Auch wenn Fermat sich offensichtlich bekannt hat, einen Beweis dessen gefunden zu haben, hat er ihn dennoch nie veröffentlicht, so dass er nach seinem Tod verloren gegangen scheint, und darauf folgend ist auch niemand gefunden worden, der diesen Beweis, der in der Diophant'schen Analysis und der ganzen Wissenschaft der Zahlen von größter Bedeutung ist, hat wieder finden können. Ich für meine Person werde beweisen, dass nach Vorlegen irgendeiner Primzahl $4n - 1$ immer eine Summe vierer Quadrate, ja sogar dreier, dargeboten werden kann, die durch sie teilbar ist. Weil also sogar bewiesen werden kann, dass das Produkt aus zwei Zahlen, von welche jeder

der beiden die Summe vierer Quadrate ist, auch ein Aggregat vierer Quadrate ist, scheinen wir nicht weit vom vermissten Beweis entfernt zu sein. Es bleibt nämlich übrig, dass bewiesen wird, wenn die Summe vierer Quadrate durch eine Zahl teilbar war, die auch die Summe vierer Quadrate sei, dass auch der Quotient gewiss die Summe vierer Quadrate sein wird.

§66 ***Lehrsatz 12***

Wenn alle Quadrate durch eine Primzahl $= 4n - 1$ geteilt werden und daher die Reihe der Reste $1, \alpha, \beta, \gamma, \delta$, etc. entspringt, dann wird das Komplement keines Restes zugleich in dieser Reihe der Reste enthalten sein.

Beweis.
Alle Reste

$$1, \alpha, \beta, \gamma, \delta, \ldots, \nu$$

resultieren aus der Teilung dieser Quadrate

$$1, 4, 9, 16, 25, \ldots, (2n-1)^2$$

die Anzahl dieser Reste ist also $= 2n - 1$ und daher ungerade. Aber wenn das Komplement eines Einzigen Reste α also $p - \alpha$ oder $-\alpha$ in derselben Reihe existieren würde, dann müssten zugleich die Komplemente aller Reste ebendort auftauchen und so, weil jeder einzelne Rest zweimal, nämlich mit dem Vorzeichen $+$ und mit dem Vorzeichen $-$ da wäre, wäre die Anzahl der Reste gerade. Daher, weil sie ungerade ist, kann es nicht geschehen, dass auch nur das Komplement eines Einzigen Restes zugleich in derselben Reihe der Reste enthalten ist. □

§67 **Korollar 1**

Wenn der letzte Term der Reihe der Reste $= \nu$ gesetzt wird, weil aus dem durch $4n - 1$ geteilten Quadrat $(2n-1)^2 = 4nn - 4n + 1$ entspringt, wird der Rest $\nu = -3n - 1$ oder $= n$ sein, nachdem der Quotient $n - 1$ genommen worden ist. Also wird sein Komplement $-n$ oder $3n - 1$ in der Reihe nicht aufgefunden. Also wird die Zahl $-n$ oder $3n - 1$ gewiss in der Reihe der Nicht-Reste sein.

§68 **Korollar 2**

Weil $mp - n$ oder $m(4n-1) - n$ alle Zahlen umfasst, die durch $4n - 1$ geteilt

den Rest $-n$ geben, tritt es klar zutage, dass keine dieser Zahlen $m\,(4n-1)-n$ oder $4mn-m-n$ jemals ein Quadrat sein kann.

§69 **Korollar 3**

Weil in der Reihe der Reste die Quadratzahlen $1, 4, 9, 16$, etc. auftauchen, werden in derselben gewiss nicht deren Komplemente $-1, -4, -9, -16$, etc. auftauchen. Also werden die mit dem Vorzeichen $-$ behafteten Quadratzahlen in die Reihe der Nicht-Reste eingehen.

§70 ***Lehrsatz 13***

Es ist keine Summe zweier Quadrate gegeben, die durch eine Primzahl der Form $4n-1$ teilbar ist, wenn nicht jedes der beiden Quadrate einzelnen durch dieselbe teilbar ist, oder es ist keine durch die Primzahl $4n-1$ teilbare Summe zweier einander primer Quadrate gegeben.

Beweis.
Wir werden nämlich festlegen, dass die Summe zweier Quadrate $aa+bb$ durch die Primzahl $4n-1$ teilbar ist und dennoch weder aa noch bb einzeln durch $4n-1$ teilbar ist. Es sei also r der Rest, welcher in der Teilung des Quadrates aa durch $4n-1$ zurückgelassen wird, und s der aus der Teilung des Quadrates bb entspringende Rest; und so wie s wird in der Reihe der Reste $1, \alpha, \beta, \gamma, \delta$, etc. auftauchen. Nun wird die Summe der Quadrate $aa+bb$ durch $4n-1$ geteilt den Rest $r+s$ zurücklassen, weil dieser nach der Annahme $=$ dem Teiler $4n-1$ sein muss, wird $s=4n-1-r$ oder $s=-r$ sein und daher wird s das Komplement des Restes r sein. Daher, wenn r in der Reihe der Reste enthalten ist, wird sein Komplement des Restes r sein. Daher, wenn r in der Reihe der Reste enthalten ist, wird sein Komplement s in ihr gewiss nicht auftaucht; daher ist nach Nehmen irgendeines Quadrates aa kein anderes Quadrat bb solcher Art gegeben ist, dass die Summe $aa+bb$ durch die Primzahl $4n-1$ teilbar wird, wenn nicht das Quadrat aa selbst per se durch $4n-1$ teilbar ist, in welchem Fall auch bb durch $4n-1$ teilbar sein muss. Es ist also keine Summe zweier einander primer Quadrate gegeben, die durch die Primzahl $4n-1$ teilbar ist. □

§71 **Korollar 1**

Es ist also keine Zahl einer Form dieser Art $aa+1$ gegeben, die durch die Primzahl $4n-1$ teilbar ist. Dafür wäre es nämlich von Nöten, dass der aus

dem Quadrat aa entspringende Rest $= -1$ wäre, welcher aber in der Reihe der Reihe der Reste nicht existiert.

§72 **Korollar 2**

Weil die Summe zweier Quadrate $aa + bb$ durch keine Primzahl der Form $4n - 1$ teilbar, wird sie auch durch keine zusammengesetzte Zahl p, die einen Primfaktor der Form $4n - 1$ hat, teilbar sein; wenn sie nämlich durch diese Zahl p teilbar wäre, würde sie auch durch ihren Faktor $4n - 1$ teilbar sein.

§73

Lehrsatz 14

Ob die Zahl $4n - 1$ prim oder zusammengesetzt ist, es ist keine durch die Zahl $4n - 1$ teilbare Summe zweier einander primer Quadrate gegeben.

Beweis.
Wenn nämlich die Zahl $4n - 1$ prim ist, ist die Gültigkeit des Lehrsatzes schon bewiesen worden. Aber wenn $4n - 1$ keine Primzahl ist, wird sie ein Produkt aus einigen Primzahlen und zwar ungeraden sein, weil die Zahl $4n - 1$ selbst ungerade ist. Aber alle Primzahlen sind entweder von der Form $4m + 1$ oder $4m - 1$; aber nicht alle Faktoren der Zahl $4n - 1$ können von der Form $4m + 1$ sein; wie viele Zahlen dieser Form $4m + 1$ nämlich auch immer miteinander multipliziert werden, das Produkt wird immer eine Zahl der Form $4n + 1$ sein oder um eine Einheit ein Vielfaches von vier übertragen. Daher ist es von Nöten, dass die Zahl $4n - 1$ mindestens einen Primfaktor der Form $4m - 1$ hat, und weil durch eine solche Primzahl keine Summe zweier einander primer Quadrate teilbar ist, ist auch keine gegeben, die durch die zusammengesetzte Zahl $4n - 1$ teilbar wäre. □

§74 **Korollar 1**

Weil keine durch die Zahl $4n - 1$, ob sie prim oder zusammengesetzt ist, teilbare Summe zweier zueinander primer Quadrate gegeben ist, wird um Vieles weniger die Zahl $4n - 1$ selbst die Summe zweier Quadrate sein. Wenn nämlich $4n - 1 = aa + bb$ wäre, müsste jedes der beiden Quadrate aa und bb einzeln durch die Zahl $4n - 1$ teilbar sein, was, weil jeder der beiden kleiner als $4n - 1$ ist, nicht geschehen kann.

§75 **Bemerkung**

Dass keine Zahl der Form $4n - 1$ die Summe zweier Quadrate sein kann, wird auch sehr leicht auf diese Weise gezeigt. Wenn nämlich die Zahl $4n - 1$ die

Summe zweier Quadrate wäre, müsste die eine gerade, die andere ungerade. Aber alle geraden Quadrate sind Zahlen der Form $4f$ und alle ungeraden Quadrate sind Zahlen dieser Form $4g + 1$. Also wird die Summe zweier Quadrate, deren eines gerade, das andere hingegen ungerade ist, eine Zahl der Form $4f + 4g + 1$ oder $4n + 1$ sein; also kann eine Zahl der Form $4n - 1$ nicht die Summe zweier Quadrate sein.

§76 **Korollar 2**

Auch kann keine Zahl, die einen Faktor der Form $4n - 1$ hat, ein Teiler einer Summe zweier einander primer Quadrate sein; wenn sie nämlich ein Teiler wäre, würde auch ihr Faktor $4n - 1$ ein Teiler sein, was nicht geschehen kann.

§77 **Korollar 3**

Um Vieles weniger kann also eine Zahl dieser Art, die den Faktor $4n - 1$, die Summe zweier einander primer Quadrate sein. So ist es unmöglich, dass $m\,(4n - 1) = aa + bb$ ist, wenn freilich a und b zueinander prime Zahlen sind.

§78

Lehrsatz 15

Keine in dieser Form $4mn - m - n$ enthaltene Zahl, welche Zahlen auch immer für m und n genommen werden, kann jemals ein Quadrat sein.

Beweis.

Weil keine Zahl, die einen Faktor $4n - 1$ hat, die Summe zweier einander primer Quadrate sein kann, oder die außer der Einheit keinen gemeinsamen Teiler haben, folgt, dass es nicht geschehen kann, dass ist

$$(4m - 1)\,(4n - 1) = 1 + aa$$

Also wird nicht sein

$$16mn - 4m - 4n = aa$$

daher kann nicht einmal ihr Viertel $4mn - m - n$ jemals ein Quadrat sein. □

§79

Lehrsatz 16

Wenn in der Reihe der Reste $1, \alpha, \beta, \gamma, \delta$, etc., die aus der Teilung der Quadrate durch irgendeine Zahl p resultieren, das Komplement eines gewissen Restes in derselben Reihe der Reste auftaucht, dann werden zwei Quadrate dargeboten werden können, deren Summe durch dieselbe Zahl p teilbar ist, auch wenn keine der beiden einzeln durch p teilbar ist.

Beweis.
Es liefere das Quadrat aa einen Rest $= r$, das Quadrat bb aber einen Rest $= -r$ oder $p - r$, welcher das Komplement von jenem ist, so dass r der Rest ist, dessen Komplement zugleich in der Reihe der Reste enthalten ist. Nun ist es offenbar, dass die Summe dieser Quadrate $aa + bb$ durch die Zahl p teilbar sein wird. □

§80 **Korollar 1**
Wenn p eine Primzahl ist, sofort wie das Komplement eines einzigen Restes in der Reihe der Reste auftaucht, werden auch die Komplemente der einzelnen Reste ebendort enthalten sein. Nachdem also irgendein Quadrat aa genommen worden ist, dessen Rest $= r$ sei, wird ein anderes xx gegeben sein, dessen Rest $= -r$ sein wird, so dass x nicht größer als $\frac{p}{2}$ ist, und die Summe $aa + xx$ wird durch p teilbar sein.

§81 **Korollar 2**
Wenn also eine durch die Primzahl p teilbare Summe zweier Quadrate $aa + bb$ gegeben ist, weil der eine der aus aa und bb entspringenden Reste das Komplement des anderen ist, wird auch das Komplement des aus irgendeinem anderen Quadrat cc entspringenden Restes in der Reihe der Reste aufgefunden werden. Es wird also eine durch die Zahl p teilbare Summe zweier Quadrate $cc + xx$ gegeben sein.

§82 **Korollar 3**
Aus dem Vorhergehenden tritt es aber klar zutage, dass dieser Fall keine Geltung haben kann, weder wenn p eine Primzahl der Form $4n - 1$ ist, noch wenn p zumindest einen Faktor dieser Form hat, weil in keinem der beiden Fälle eine durch die Zahl p teilbare Summe zweier Quadrate gegeben ist, welche Quadrate freilich einander prim sind.

§83 **Korollar 4**
Es werden also keine anderen Primzahlen zurückgelassen, auf welche dieser Lehrsatz angewendet werden kann, außer die in dieser Form $4n + 1$ enthalten sind.

§84 **Bemerkung**
Ob aber alle Primzahlen der Form $4n + 1$ diese Eigenschaft haben, dass in den daher entspringenden Reihen der Reste das Komplement jedes Termes

zugleich enthalten ist, ist hier noch nicht bewiesen werden und erscheint auch nicht zu bezweifeln, dass aus diesen selben Prinzipien ein Beweis gefunden werden kann, auch wenn es mir freilich noch nicht möglich war, dorthin zu gelangen. Aber die aus einfacheren Primzahlen dieser Form entspringenden Reihen der Reste verhalten sich auf die folgende Weise, wo es freilich ratsam erscheint, die größeren Reste als die Hälfte jeder Zahl durch negative Zahlen darzubieten, damit leichter, welche die Komplemente von anderen sind, klar wird:

$$5\,(1,-1)\,,13\,(1,4,-4,3,-1,-3)\,,17\,(1,4,-8,-1,8,2,-2,-4)\,,$$
$$29\,(1,4,9,-13,-4,7,-9,6,-6,13,5,-1,-5,-7)\,,$$
$$37\,(1,4,9,16,-12,-1,12,-10,7,-11,10,-4,-16,11,3,-3,-7,-9)$$

In diesen Reihen ist es also offenkundig, dass das Komplement jedes Termes zugleich in ihnen auftaucht. Dass dies aber notwendig passiert, wenn der Teiler eine Primzahl der Form $4n+1$ ist, ein direkter Beweis dessen wird noch vermisst, der auf diese Weise geführt werden zu müssen scheint. Es geht also aus der Primzahl $4n+1$ diese Reihe an Resten hervor $1, \alpha, \beta, \gamma, \delta$, etc., die Anzahl welcher Terme $2n$ ist; wenn nun jemand verneint, dass die Komplemente dieser Terme zugleich in derselben Reihe enthalten sind, so muss er sagen, dass alle Komplemente $-1, -\alpha, -\beta, -\gamma, -\delta$, etc. die Reihe der Nicht-Reste festlegen; weil die Anzahl dieser Terme $= 2n$ ist, würde folgen, dass zusätzlich keine Nicht-Reste gegeben sind; daher, wenn eine gewisse in der Reihe der Nicht-Reste enthaltene Zahl angegeben werden könnte, die kein Komplement eines gewissen in der Reihe der Reste enthaltenen Terme wäre, würde zugleich folgen, dass überhaupt kein Komplement der Reihe der Reste in der Reihe der Nicht-Reste enthalten wäre. Wenn dies also bewiesen werden könnte, hätte man den gewünschten und freilich direkten Beweis. Denn ein indirekter Beweis ist schon daher gegeben, weil ich bewiesen habe, dass jede Primzahl der Form $4n+1$ die Summe zweier Quadrate ist; daher, wenn $4n+1 = aa+bb$ ist, wird das eine der aus diesen Quadraten aa und bb entspringenden Reste das Komplement des anderen sein und daher wird weiter richtig gefolgert, dass das Komplement jedes Restes zugleich in der Reihe der Quadrate enthalten ist.

§85

Lehrsatz 17

Wenn in der Reihe der Reste $1, \alpha, \beta, \gamma, \delta$, etc., die aus der Division der Quadrate durch irgendeine Zahl p entspringen, ein Term auftaucht, der das Komplement

der Summe zweier anderer Terme ist, dann kann eine durch die Zahl p teilbare Summe dreier Quadrate dargeboten werden, so dass die Wurzel keines Quadrates größer ist als $\frac{p}{2}$.

Beweis.
Es seien r und s die aus den zwei Quadraten aa und bb herstammenden Reste, deren Summe $= r + s$ und deren Komplement daher $= p - r - s$ oder $-r - s$ ist. Wenn nun dieses Komplement in der Reihe der Reste $1, \alpha, \beta, \gamma, \delta$, etc. aufgefunden wird, wird ein Quadrat $cc < \frac{1}{4}pp$ gegeben sein, welches durch p geteilt $-r - s$ zurücklassen wird; und so wird es offenbar sein, dass die Summe der drei Quadrate $aa + bb + cc$ durch die Zahl p teilbar ist und keines dieses Quadrate größer als $\frac{1}{4}pp$ ist. □

§86 **Korollar 1**
Wenn also in der Reihe der Reste $1, \alpha, \beta, \gamma, \delta$, etc. eine aus diesen Zahlen -2, -1, $-\alpha$, -2α, $-1-\beta$, $-\alpha-\beta$, -2β, $-1-\gamma$, $-\alpha-\gamma$, $-\beta-\gamma$, -2γ, $-1-\delta$, $-\alpha-\delta$ etc. auftaucht, kann immer eine durch die Zahl p teilbare Summe dreier Quadrate dargeboten werden.

§87 **Korollar 2**
Und wenn p eine Primzahl ist, werden die Wurzeln dieser einzelnen Quadrate a, b, c, weil sie kleiner als $\frac{p}{2}$ sind, zu p prime Zahlen und daher auch selbst Quadrate sind; und wenn nicht diese drei Quadrate selbst zueinander prim war, sondern einen gemeinsamen quadratischen Teiler haben, weil dieser notwendigerweise zu p prim ist, werden durch ihn jene Quadrate auf kleinere und einander prime zurückgeführt werden, deren Summe in gleicher Weise durch p teilbar sein wird.

§88 **Korollar 3**
Wenn in der Reihe der Reste die Komplemente der einzelnen Terme zugleich enthalten sind, dann kann auch eine durch die Zahl p teilbare Summe zweier Quadrate angegeben werden. Wann immer aber eine Summe zweier Quadrate gegeben ist, wird um Vieles mehr eine Summe dreier Quadrate gegeben sein, wie die Form $aa + bb$ in der Form $aa + bb + cc$ enthalten ist.

§89 **Bemerkung**
Auf die gleiche Weise wird bewiesen, wenn in der Reihe der Reste eine Zahl auftaucht, die das Komplement der Summe dreier Reste ist, dass dann eine

Summe vierer Quadrate dargeboten werden kann, die durch die Zahl p teilbar ist. Aber wenn Summen zweier oder dreier Reste genommen werden, gehen so viele verschiedene Zahlen hervor, dass es hinreichend offenbar scheint, dass all deren Komplemente nicht in der Reihe der Nicht-Reste enthalten sein können.

§90

Lehrsatz 18

Wenn nach Vorlegen irgendeiner Primzahl p ein durch sie teilbare Summe zwei einander nicht primer Quadrate nicht dargeboten werden kann, kann gewiss immer eine durch sie teilbare Summe dreier Quadrate angegeben werden, so dass die einzelnen jeweils nicht durch p teilbar sind.

Beweis.
Es sei $1, \alpha, \beta, \gamma, \delta, \epsilon$, etc. die aus der Teilung der Quadrate durch die vorgelegte Primzahl p entspringende Reihe. Nun taucht in dieser Reihe entweder -1 auf oder -1 nicht auf. Wenn -1 dort auftaucht, tauchen die Komplemente der einzelnen Reste zugleich dort auf und daher ist auf mehrere Arten eine durch p teilbare Summe zweier Quadrate gegeben. Wenn aber -1 nicht in der Reihe der Reste enthalten ist, wird sie in der Reihe der Nicht-Reste aufgefunden werden, wo zugleich die Komplemente aller Reste auftauchen werden; in diesem Fall wird also keine durch die Zahl p teilbare Summe zweier Quadrate gegeben sein, wenn nicht jedes der beiden einzeln eine Division zulässt. Dass aber in diesen Fällen und durch die Primzahl p teilbare Summe dreier Quadrate gegeben ist, zeige ich so.
Zuerst sei es angemerkt, wenn eine gewisse Zahl r in der Reihe der Reste auftaucht, dass ihr Komplement $-r$ gewiss in der Reihe der Nicht-Reste ist, und umgekehrt wenn r ein Nicht-Rest ist, dass gewiss $-r$ ein Rest sein wird. Wir wollen nun festlegen, dass es verneint wird, dass eine durch p teilbare Summe dreier Quadrate gegeben ist; und weil in der Reihe zuerst die Zahl 1 vorhanden ist, wird ebendort die Zahl -2 nicht auftauchen (andernfalls wäre nämlich entgegen der Annahme eine durch die Zahl p teilbare Summe dreier Quadrate gegeben). Es wird also die Zahl -2 in der Reihe der Nicht-Reste und deshalb die Zahl $+2$ in der Reihe der Reste auftauchen. Weil man nun in der Reihe der Reste die Zahlen 1 und 2 hat, wird das Komplement der Summe derer -3 ein Nicht-Rest und daher $+3$ ein Rest sein. Auf dieselbe Weise wird aus den Resten 1 und 3 geschlossen, dass -4 ein Nicht-Rest und daher $+4$ ein Rest sein wird. Und im Allgemeinen, wenn irgendein Rest r ist, wird $-r-1$ ein Nicht-Rest sein müssen und daher wäre $1+r$ ein Rest.

Aus dieser Annahme folgt also, dass gänzlich alle Zahlen $1, 2, 3, 4, 5, 6$, etc. in der Reihe der Reste enthalten sind und daher überhaupt keine Zahlen für die Reihe der Nicht-Reste übrig gelassen werden; weil dies absurd ist, müssen wir schließen, dass natürlich eine durch die Primzahl p teilbare Summe dreier Quadrate gegeben ist, von denen freilich keines einzeln durch p teilbar ist. Wenn diese unter Umständen einander nicht prim waren, werden sie durch deren größten gemeinsamen Teiler zu primen herabgesenkt werden können, weil der größte gemeinsame Teiler gewiss quadratisch ist. □

§91 **Korollar 1**

Mit der gleichen Schlussweise wird dargetan, dass es um Vieles mehr im Widerspruch steht, wenn jemand verneinte, dass eine durch eine Primzahl teilbare Summe vierer Quadrate gegeben ist. Also wird nach Vorlegen irgendeiner Primzahl p immer eine durch sie teilbare Summe vierer Quadrate gegeben sein.

§92 **Korollar 2**

Wenn die Primzahl p kein Teiler einer Summe zweier Quadrate ist, werden jene drei einzelnen Quadrate, deren Summe $aa + bb + cc$ durch P teilbar ist, kleiner als $\frac{1}{4}pp$ sein. Daher wird also $aa + bb + cc < \frac{3}{4}pp$ sein, woher der Quotient, der aus der Teilung dieses Aggregats $aa + bb + cc$ durch p entspringt, $< \frac{3}{4}p$ sein.

§93

Lehrsatz 19

Wenn eine Summe vierer Quadrate durch eine Summe vierer Quadrate geteilt wird, wird der Quotient auch eine Summe vierer Quadrate, zumindest in gebrochenen Zahlen, sein.

Beweis.
Es sei $aa + bb + cc + dd$ eine Summe vierer Quadrate, die durch diese Summe vierer Quadrate $pp + qq + rr + ss$ zerteilt sei; der Quotient wird sein

$$= \frac{aa + bb + cc + dd}{pp + qq + rr + ss}$$

welcher, ob er eine ganze oder gebrochene Zahl ist, immer in, zumindest in gebrochenen Zahlen, vier Quadrate aufgelöst werden kann. Wir wollen mit $pp + qq + rr + ss$ erweitern, damit der Nenner ein Quadrat wird; es wird der

Quotient dieser sein

$$= \frac{(aa+bb+cc+dd)\,(pp+qq+rr+ss)}{(pp+qq+rr+ss)^2}$$

wenn daher nun der Zähler in vier Quadrate aufgelöst werden kann, wird der Bruch selbst einem Aggregat vierer Quadrate gleich werden. Aber der Zähler kann auf mehrere Weisen in vier Quadrate aufgehört werden; wenn nämlich festgelegt wird

$$(aa+bb+cc+dd)\,(pp+qq+rr+ss) = xx+yy+zz+vv$$

wird sein

$$\begin{aligned} x &= ap+bq+cr+ds \\ y &= aq-bp \pm cs \mp dr \\ z &= ar \mp bs - cp \pm dq \\ v &= as \pm br \mp cq - dp \end{aligned}$$

welche vier Zahlen, wenn die einzelnen durch den gemeinsamen Teiler $pp+qq+rr+ss$ geteilt werden, die Wurzeln der Quadrate geben werden, deren Summe dem vorgelegten Quotienten gleich wird. Wenn also diese Zahlen x, y, z und v nicht durch $pp+qq+rr+ss$ teilbar sind, können zumindest in gebrochenen Zahlen vier Quadrate angegeben werden, deren Summe dem Quotienten $\frac{aa+bb+cc+dd}{pp+qq+rr+ss}$ gleich ist. □

§94 **Korollar 1**

Was hier über die Summen vierer Quadrate bewiesen worden ist, bezieht sich auch auf die Summen dreier oder sogar zweier, weil nichts verhindert, dass eine oder zwei aus den zahlen a, b, c, d und p, q, r, s gleich Null ist.

§94[a] **Korollar 2**

Wenn also eine Summe dreier Quadrate durch eine Summe vierer oder auch dreier Quadrate geteilt wird, wird der Quotient gewiss die Summe vierer Quadrate sein.

§95 **Korollar 3**

Weil das Produkt aus zwei Summen vierer Quadrate auch die Summe vierer Quadrate ist, tritt es klar zutage, wenn alle Primzahlzahlen Summe vierer

oder auch weniger Quadrate sind, dass dann auch ganz und gar alle Zahlen Summen vierer oder auch weniger Quadrate sind.

§96 **Bemerkung**

Wenn eine Summe vierer Quadrate $aa + bb + cc + dd$ durch eine andere Summe vierer Quadrate $pp + qq + rr + ss$ teilbar war, dass dann der Quotient nicht nur in gebrochenen Zahlen, sondern auch in ganzen Zahlen eine Summe vierer Quadrate ist, ist ein sehr eleganter Lehrsatz von Fermat, dessen Beweis uns mit selbigem entrissen worden ist. Ich gestehe, dass ich diesen Beweise bis jetzt nicht habe finden können, aber dennoch wird daher ein Weg eröffnet, um den folgenden Lehrsatz zu beweisen, in welchem jede beliebige Zahl die Summe vierer oder weniger Quadrate zu sein versichert wird, natürlich in dem Fall, in welchem gebrochene Quadrate nicht ausgeschlossen werden; auch wenn nämlich dieser Lehrsatz in ganze Zahlen auch immer wahr ist, glaube ich dennoch nicht wenig geleistet zu haben, dadurch dass ich diesen nach Herausnehmen der Bedingung ganzzahlige Quadrate bewiesen haben. Weil nämlich ein Beweis nach Fermat bis jetzt vergebens gesucht worden ist, meine ich, sehr nahe an dieses Ziel herangekommen zu sein.

§97

Lehrsatz 20

Jede Zahl ist die Summe vierer oder auch weniger Quadrate, wenn freilich gebrochene Quadrate nicht ausgeschlossen werden.

Beweis.

Dieser Lehrsatz ist freilich wahr, auch wenn gebrochene Quadrate ausgeschlossen werden; Fermat versichert nämlich, dass jede ganze Zahl das Aggregat aus vier oder auch weniger ganzen Quadraten ist, ich aber gestehe, dass ich diesen Beweis noch nicht habe finden können; ich werde also einen Beweis für den Fall geben, in welchem gebrochene Quadrate nicht ausgeschlossen werden. Nun habe ich angemerkt, dass dieser Beweis nur auf Primzahlen zurückgeführt wird, über welche es also ausreicht, den Lehrsatz bewiesen zu haben. Weil wir ja also wissen, dass die kleineren Primzahlen, wie $2, 3, 5, 7, 11, 13$, etc., alle in vier oder weniger Quadrate aufgelöst werden können, wenn jemand das über die folgenden negiert, muss er sagen, dass eine bestimmte kleinste Primzahl gegeben ist, die nicht die Summe vierer oder weniger Quadrate ist. Es sei p diese Primzahl, so dass alle kleineren Primzahlen als selbige und daher auch alle zusammengesetzten gewiss Summen vierer oder weniger Quadrate sind. Nun ist durch den vorhergehenden Lehrsatz eine durch diese

Zahl p teilbare Summe dreier Quadrate gegeben, die $aa + bb + cc$ sei, so dass diese einzelnen Quadrate kleiner als $\frac{1}{4}pp$ sind; daher wird sein

$$aa + bb + cc < \frac{3}{4}pp$$

Also wird der Quotient

$$\frac{aa + bb + cc}{p}$$

kleiner sein also $\frac{3}{4}p$; weil dieser deshalb kleiner als p ist, wird er gewiss die Summe vierer oder weniger Quadrate sein: es sei $xx + yy + zz + vv$ dieser Quotient; es wird sein

$$p = \frac{aa + bb + cc}{xx + yy + zz + vv}$$

und daher wird die Zahl p selbst die Summe vierer oder weniger Quadrate sein, die auch in Brüchen angegeben werden können. Weil also unter den Primzahlen keine kleinste gegeben ist, die nicht in vier oder weniger Quadrate aufgeteilt werden kann, ist überhaupt keine Primzahl gegeben, die kein Aggregat vierer oder weniger Quadrate wäre; weil die über Primzahlen gewiss ist, wird es auch für alle zusammengesetzten Zahlen und dafür ganz und gar alle Zahlen gelten, so dass überhaupt keine Zahl gegeben ist, die nicht die Summe vierer oder weniger Quadrate ist. □

§98 **Korollar 1**

Weil jede ganze Zahl die Summe vierer oder weniger Quadrate ist, erstreckt sich dieselbe Eigenschaft auch auf alle gebrochenen Zahlen. Es sei nämlich irgendein Bruch $\frac{m}{n}$ vorgelegt, der in $\frac{mn}{nn}$ transformiert werde. Nun sei $mn = \frac{aa}{pp} + \frac{bb}{qq} + \frac{cc}{rr} + \frac{dd}{ss}$ und es wird sein

$$\frac{mn}{nn} = \frac{m}{n} = \frac{aa}{nnpp} + \frac{bb}{nnqq} + \frac{cc}{nnrr} + \frac{dd}{nnss}$$

und daher wird jede gebrochene Zahl die Summe vierer oder weniger Quadrate sein.

§99 **Korollar 2**

Weil ja, wenn über die Auflösung von gebrochenen Zahlen in Quadrate die Rede ist, jene Bedingung von ganzzahligen Quadraten von selbst verschwindet, habe ich den Lehrsatz im Weiteren Sinne so aufgefasst, dass gänzlich alle

Zahlen, ob ganze oder gebrochene, in vier oder weniger Quadrate auflösbar bezeichnen, ohne jegliche Einschränkung streng bewiesen.

§100 **Bemerkung**

Nachdem also Fermat versichert hatte, dass jede ganze Zahl die Summe entweder vierer oder weniger ganzzahliger Quadrate ist, ist nun freilich diese über im Allgemeinen betrachtete Quadrate bewiesen worden, weil gebrochene nicht ausgeschlossen worden sind. Daher, damit Fermat Genüge geleistet wird, ist es übrig, dass wir beweisen, welche ganze Zahl in vier gebrochene Quadrate aufgelöst werden kann, dass dieselbe auch in vier oder weniger ganze Quadrate aufgelöst werden kann. In der Diophant'schen Analysis pflegt es freilich als gewiss angenommen zu werden, dass keine ganze Zahl in vier gebrochene Quadrate zerteilt werden kann, wenn nicht ihre Auflösung in vier oder weniger ganzzahlige Quadrate bekannt ist; wenn dies also mit einem Beweis gesichert wäre, wäre nichts weiter zu wünschen. Aber bis jetzt habe ich nie einen Beweis solcher Art gefunden. Was aber den sich sehr weit erstreckenden mit diesen Worten zusammengefassten Lehrsatz betrifft:

Jede entweder ganze oder gebrochene Zahl ist die Summe vierer oder weniger Quadrate

habe ich hier einen so strengen Beweis von diesem angegeben, dass in ihm überhaupt nichts vermisst werden kann; und dadurch selbst glaube ich für meine Person einen nicht zu verachtenden Anteil der verloren gegangenen Fermat'schen Beweise wiederhergestellt zu haben.