Neue Beweise über die Auflösung von Zahlen in Quadrate*

Leonhard Euler

§1 Nachdem ich oft und viel mit diesem Gegenstand beschäftigt war und mich dennoch der Beweis, den ich einst über die Auflösung aller Zahlen in vier oder weniger Quadrate gegeben hatte, nicht völlig zufrieden gestellt hatte, habe ich mit umso größerer Begeisterung den Beweis entwickelt, welcher der hochgeehrte Lagrange neulich im ersten Band der „NoVorum Actorum Acad. sc. Boruss." von diesem Lehrsatz angegeben hat, welchen ich natürlich dafür bewundert habe, die ganze Aufgabe vollendet zu haben, auch wenn seine wichtigsten Grundlagen allzu weit hergeholt und äußerst aufwendig scheinen.

§2 Ich glaube aber, dass es den Lesern nicht unangenehm sein wird, wenn ich die wesentlichen Grundzüge, auf welche dieser Beweis gestützt ist, hier kurz und knapp vorgelegt haben werde. Nachdem der hochgeehrter Autor dieses Lemma vorausgeschickt hatte, dass, wenn zwei Summen zweier Quadrate $pp + qq$ und $rr + ss$ den gemeinsamen Teiler ρ haben und dennoch die einzelnen Quadrate durch ihn nicht geteilt werden können, dann nicht nur dieser Teiler ρ selbst, sondern auch die beiden Quotienten $\frac{pp+qq}{\rho}$ und $\frac{rr+ss}{\rho}$ die Summe zweier Quadrate sein werden, schreitet er dazu voran, den Lehrsatz zu beweisen, dass, wenn eine Summe vierer Quadrate $P^2 + Q^2 + R^2 + S^2$ durch irgendeine Zahl A teilbar war und dennoch nicht die einzelnen Quadrate durch sie teilbar sind, dann diese Zahl A selbst eine Summe vierer Quadrate sein wird, dessen

*Originatitel: „Novae demonstrationes circa resolutionem numerorum in quadrata", erstmals publiziert in „*Acta Eruditorum* 1777, 1780, pp. 48-69", Nachdruck in „*Opera Omnia*: Series 1, Volume 3, pp. 218 - 238", eine Version veröffentlicht in *Commentat. arithm.* 1, 1849, pp. 538-548 [E445b], Eneström-Nummer E 445, übersetzt von: Alexander Aycock, TEXtsatz: Matthias Gluth, im Rahmen des Hauptseminars „Euler", JGU Mainz

Beweis in den folgenden Rechnungen enthalten ist.
I. Nachdem der aus jener Division herstammenden Quotient a gesetzt worden ist, dass ist

$$Aa = P^2 + Q^2 + R^2 + S^2$$

wenn es unter Umständen passiert, dass die zwei Formeln $P^2 + Q^2$ und $R^2 + S^2$ den gemeinsamen Teiler ρ haben, welchen also auch die Zahl a enthalten wird, setzt er $a = b\rho$, dass wird

$$Ab = \frac{P^2 + Q^2}{\rho} + \frac{R^2 + S^2}{\rho}$$

weil diese Formeln durch das vorausgeschickte Lemma Summen zweier Quadrate sind, wird man eine Gleichung dieser Art haben

$$Ab = pp + qq + rr + ss$$

wo die Formeln $pp + qq$ und $rr + ss$ nicht weiter einen gemeinsamen Faktor haben werden.
II. Dann setzt er aber $pp + qq = t$ und $rr + ss = u$, dass $Ab = t + u$ ist, in welche Gleichung er t einführt, indem er $Abt = tt + tu$ setzt; und weil tu auch eine Summe zweier Quadrate ist, beispielsweise $xx + yy$, indem natürlich $x = pr + qs$ und $y = ps - qr$ genommen wird, wird werden

$$Abt = tt + xx + yy$$

III. Nun bemerkt er, dass durch die Zahlen t und b, die natürlich einander prim sind, die beiden x und y so ausgedrückt werden können, dass $x = \alpha t + \gamma b$ und $y = \beta t + \delta b$; weil dort die Buchstaben $\alpha, \beta, \gamma, \delta$ auf unendlich viele Arten entweder negativ oder positiv angenommen werden können, werden unter deren Werte gewiss solche gegeben sein, dass $\alpha < \frac{1}{2}b$ und $\beta < \frac{1}{2}b$ ist.
IV. Nachdem nun diese Werte für x und y eingesetzt worden sind, wird diese Gleichung resultieren

$$Abt = tt\,(1 + \alpha\alpha + \beta\beta) + 2bt\,(\alpha\gamma + \beta\delta) + bb\,(\gamma\gamma + \delta\delta)$$

Weil dieser Ausdruck durch p teilbar sein muss und dennoch im ersten Glied tt diese Teilung nicht zulässt, ist es notwendig, dass dort die Formel $1 + \alpha\alpha + \beta\beta$ den Faktor b hat; auf dieselbe Weise ist es auch von Nöten, dass im letzten Glied der Faktor $\gamma\gamma + \delta\delta$ durch t teilbar ist. Es werde also $1 + \alpha\alpha + \beta\beta = ba'$

gesetzt, und weil jede der beiden Zahlen α und β kleiner als $\frac{1}{2}b$ ist, ist es offenbar, dass $a' < \frac{1}{2}b + \frac{1}{b}$ sein wird; nach Division durch b wird also sein

$$At = a'tt + 2t\,(\alpha\gamma + \beta\delta) + b\,(\gamma\gamma + \delta\delta)$$

V. Diese Gleichung werde nun mit a' multipliziert, dass hervorgeht

$$Aa't = a'^2tt + 2a't\,(\alpha\gamma + \beta\delta) + a'b\,(\gamma\gamma + \delta\delta)$$

und, indem in letzten Glied anstelle von $a'b$ von $1 + \alpha\alpha + \beta\beta$ geschrieben wird, wird werden

$$Aa't = a'^2tt + 2a't\,(\alpha\gamma + \beta\delta) + (\alpha\alpha + \beta\beta)\,(\gamma\gamma + \delta\delta) + \gamma\gamma + \delta\delta$$

welche Audruck in die folgenden vier Quadrate aufgelöst werden wird

$$Aa't = \left(a't + \alpha\gamma + \beta\delta\right)^2 + (\beta\gamma - \alpha\delta)^2 + \gamma^2 + \delta^2$$

weil dort die Summe der zwei letzten Quadrate $\gamma^2 + \delta^2$ durch die Zahl t teilbar ist, ist es von Nöten, dass die Summe der beiden ersten auch durch t teilbar ist, so dass hier zwei den gemeinsamen Teiler t habende Summen zweier Quadrate auftauchen; daher, wenn durch t geteilt werden, werden jene beiden Quotienten Summen zweier Quadrate sein.
VI. Wenn wir daher also festlegen

$$\frac{(a't + \alpha\gamma + \beta\delta)^2 + (\beta\gamma - \alpha\delta)^2}{t} = p'^2 + q'^2 \text{ und } \frac{\gamma^2 + \delta^2}{t} = r'^2 + s'^2$$

werden wir haben

$$Aa' = p'^2 + q'^2 + r'^2 + s'^2$$

In diesen Formeln Aa', wenn sie mit der ersten Aa verglichen wird, wird die Zahl a' um Vieles kleiner sein als a, weil ja $b < a$ und $a' < \frac{1}{2}b$ ist. Auf die gleiche Weise wird es also möglich sein, zu einer Formel Aa'' zu gelangen, wo a'' um vieles kleiner sein wir als a', und so ist es notwendig, dass schließlich zur Formel A einer gelangt wird, so dass die Zahl A selbst einer Summe vierer Quadrate gleich aufgefunden wird.

§3 Nachdem dieser Lehrsatz bewiesen worden ist, muss gezeigt werden, dass nach Vorlegen irgendeiner Primzahl immer eine durch sie teilbare Summe vierer Quadrate dargeboten werden kann, deren einzelne Quadrate dennoch

diese Division nicht zulassen. Und auf diese im höchsten Maße geniale Weise beweist es auch der hochgeehrte Lagrange, welche aber dermaßen schwer ergründbar und lang ist, dass seine wichtigsten Grundzüge hier niemals kurz und sorgfältig dargeboten werden können. Nun ist also jener berühmte Lehrsatz entweder von Bachet oder Fermat, dass jede Zahl in vier oder weniger Quadrate aufgelöst werden kann, für vollständig bewiesen zu halten. Weil nämlich für irgendeine Primzahl immer eine durch jene teilbare Summe vierer Quadrate gegeben werden kann, werden alle Primzahlen Summen vierer oder weniger Quadrate sein, und weil schon vor langer Zeit bewiesen worden ist, dass die Produkte aus zwei oder mehreren Zahlen, welche einzelnen Summen vierer oder weniger Quadrate sind, auch in vier Quadrate zerteilt werden können, ist es nun auf strengste Weise dargetan worden, dass gänzlich alle Zahlen Summen vierer oder weniger Quadrate sind.

§4 Obwohl es ganz und gar unrecht wäre, irgendwas gegen die Solidarität und die Strenge dieser Beweise zu entgegnen, wird dennoch niemand abstreiten, dass sie allzu weit hergeholt sind und die Fundamente selbst und die Begründungen der einzelnen Beweisschritte, aus denen diese Beweise zusammengesetzt worden sind, in nicht geringe Dunkelheiten gehüllt sind, so dass sich immer noch mit Recht klarere und leichter verständliche Beweise verlangen lassen. durch dieses Verlangen ist dem größten Lob, welchen diese Beweise verdienen, nichts abgesprochen zu werden anzusehen.

§5 Weil es mir also, nachdem ich diesen Gegenstand von Neuem gründlich betrachtet hatte, geglückt ist, auf neue und hinreichend klare Beweise derselben Lehrsätze zu stoßen, scheint es denen, die an diesen Studien Freude haben, die Mitteilung dieser neuen Beweise gewiss sehr belieben; deshalb werde ich sie an dieser Stelle, sofern es mir möglich sein wird, kurz und klar vorlegen. Und zuerst werde ich freilich von jenem allbekannten und zugleich in vollster Weise bewiesen Lehrsatz, nach welchem die Teiler jeder Summe zweier einander primer Quadrate der Summe zweier Quadrate gleich versichert werden, aus beginnen, sowohl weil dieser neuer Beweis sich durch seine Einfachheit im höchsten Maße empfiehlt, also auch weil; indem man denselben Spuren folgt, der Beweis in der Tat auch leicht auf vier Quadrate ausgedehnt werden kann.

§6 *Lemma 1*
Das Produkt aus zwei Summen zweier Quadrate ist ebenso eine Summe

zweier Quadrate.
Denn wenn jenes Produkt $(aa + bb)(\alpha\alpha + \beta\beta)$ war und genommen wird

$$A = a\alpha + b\beta \text{ und } B = \alpha\beta - ab$$

wird natürlich sein

$$(aa + bb)(\alpha\alpha + \beta\beta) = AA + BB$$

Lehrsatz 1

Wenn N ein Teiler einer Summe zweier einander primer Quadrate $P^2 + Q^2$ war, wird jene Zahl N selbst eine Summe zweier Quadrate sein.

Beweis.
Damit sich dieser Beweis leichter auch in Zahlen verfolgen lässt, wenn dies unter Umständen beliebt, bemerke ich, wie groß auch immer die Zahlen P und Q waren, dass aus ihnen immer eine andere Summe zweier Quadrate $pp + qq$ gebildet werden kann, deren Wurzel p und q die Hälfte der vorgelegten Zahl N nicht überragen. Denn wenn festgelegt wird

$$P = fN \pm p \text{ und } Q = gN \pm q$$

ist es bekannt, dass die Zahlen p und q so genommen werden können, dass sie die Hälfte $\frac{1}{2}N$ nicht überragen. weil also nun ist

$$PP + QQ = NN(ff + gg) + 2N(\pm fp \pm gq) + pp + qq$$

und dieser Ausdruck durch N teilbar ist, ist es ersichtlich, dass auch diese Summe zweier Quadrate durch N teilbar sein wird. Nachdem dies vorausgeschickt worden sind, möchte ich den Beweis selbst in den folgenden wesentlichen Grundzügen zusammenfassen.
I. Weil also diese Formel $pp + qq$ den Teiler N hat, werden wir durch Festlegen des Quotienten $= n$ haben

$$Nn = pp + qq$$

wo also n kleiner sein wird als $\frac{1}{2}N$, weil $p < \frac{1}{2}N$ und $q < \frac{1}{2}N$ ist.
II. Nun werden sich diese Zahlen p und q durch die Zahl n so ausdrücken lassen, dass gilt

$$p = a + \alpha n \text{ und } q = b + \beta n$$

wo, nachdem auch negative Zahlen für a und b zugelassen worden sind, sie sich unter $\frac{1}{2}n$ herabdrücken lassen werden, wie wir schon am Anfang beobachtet haben. Dann wird aber sein

$$Nn = aa + bb + 2n\,(a\alpha + b\beta) + nn\,(\alpha\alpha + \beta\beta)$$

und weil im vorausgeschickten Lemma $a\alpha + b\beta = A$ war, wird werden

$$Nn = aa + bb + 2nA + nn\,(\alpha\alpha + \beta\beta)$$

III. Das erste Glied dieses Ausdruckes $aa + bb$ hat also notwendigerweise den Faktor n, weil die übrigen Glieder schon per se den Teiler n zulassen. Wir wollen also festlegen

$$aa + bb = nn'$$

und weil $a < \frac{1}{2}n$ und $b < \frac{1}{2}n$ und daher $nn' < \frac{1}{2}nn$ ist, wird natürlich $n' < \frac{1}{2}n$ sein. Nachdem aber dieser Wert eingesetzt worden ist und eine Division durch n durchgeführt worden ist, geht hervor

$$N = n' + 2A + n\,(\alpha\alpha + \beta\beta)$$

IV. Diese Gleichung wollen wir mit n' multiplizieren, und weil $nn' = aa + bb$ ist, wird das letzte Glied durch das vorausgeschickte Lemma zurückgeführt auf

$$nn'\,(\alpha\alpha + \beta\beta) = (aa + bb)\,(\alpha\alpha + \beta\beta) = AA + BB$$

so dass wir nun haben

$$Nn' = n'n' + 2n'A + AA + BB$$

welcher Audruck offenbar die Summe zweier Quadrate ist, natürlich

$$Nn' = \left(n' + A\right)^2 + B^2$$

V. Weil also anfangs das Produkt Nn die Summe zweier Quadrate gewesen war und wir hier ein kleinere Produkt Nn' auch eine Summe zweier Quadrate gleich gefunden haben, wird sich auf dieselbe Weise zu immer kleineren solcher Produkten gelangen lassen, natürlich Nn'', Nn''' etc. Es ist also von Nöten, dass schließlich zu einem kleinsten Produkt, natürlich $N \cdot 1$, gelangt wird, und so wird die vorgelegte Zahl N auch selbst die Summe zweier Quadrate sein. □

Korollar

Es wird vielleicht wundersam scheinen, nachdem zu einer Zahl dieser Art $n' = 1$ gelangt worden ist, auf welche Weise sich die Folgenden gleichen Operationen verhalten werden; dies wird leicht klar werden, indem sofort $n = 1$ gesetzt wird; dann wird man nämlich $p = a + \alpha \cdot 1$ und $q = b + \beta \cdot 1$ haben, wo es offenbar möglich ist, $a = 0$ und $b = 0$ zu nehmen, auf welche Weise sie natürlich $< \frac{1}{2}$ werden; dann wird aber wegen $aa + bb = 0$ natürlich $n' = 0$ sein und hier wird das weiter Fortschreiten unserer Schlussweise von selbst aufgehalten.

§7 **Bemerkung** Auf dieselbe Weise kann bewiesen werden, dass alle Zahlen entweder von dieser Form $pp + 2qq$ oder $pp + 3qq$ keine anderen Teiler zulassen, welche selbst von derselben Form sind, wenn freilich die Zahlen p und q einander prim waren. Aber in der Tat kann diese Schlussweise nicht auf höhrer Formen, wie beispielsweise $pp + 5qq$, $pp + 6qq$ ausgedehnt werden, weil dann nicht weiter folgen würde, dass die Zahl n' notwendigerweise kleiner ist als n. Die Beweise jener ersten Fälle wollen wir also hier beifügen.

§8 *Lemma 2*

Ein Produkt aus zwei Zahlen dieser Form $pp + 2qq$ ist immer eine Zahl von derselben Form.

Wenn nämlich ein solches Produkt vorgelegt wird $(aa + 2bb)(\alpha\alpha + 2\beta\beta)$ und genommen wird

$$A = a\alpha + 2b\beta \quad \text{und} \quad B = a\beta - b\alpha$$

dann wird natürlich sein

$$AA + 2BB = (aa + 2bb)(\alpha\alpha + 2\beta\beta)$$

Lehrsatz 2

Wenn N ein Teiler der Zahl $pp + 2qq$ war und die Zahlen p und q einander prim sind, dann wird auch die Zahl N selbst in einer solchen Form erhalten sein.

Beweis.

Hier wird es wiederum möglich sein, die Zahlen p und q unter die Hälfte der Zahl N herabzusenken und unser Beweis wird auf die folgende Weise ablaufen.

I. Es sei

$$Nn = pp + 2qq$$

und weil $p < \frac{1}{2}N$ und $q < \frac{1}{2}N$ sind, wird $n < \frac{3}{4}N$ sein. Nun werde wie zuvor festgelegt

$$p = a + \alpha n \quad \text{und} \quad q = b + \beta n$$

wo die Zahlen a und b kleiner als $\frac{1}{2}n$ genommen werden können, und daher wird man haben

$$Nn = aa + 2bb + 2n\,(a\alpha + 2b\beta) + nn\,(\alpha\alpha + 2\beta\beta)$$

welche Form durch das vorausgeschickte Lemma zurückgeführt wird auf

$$Nn = aa + 2bb + 2nA + nn\,(\alpha\alpha + 2\beta\beta)$$

II. Hier wird also das erste Glied $aa + 2bb$ den Faktor n haben, woher nach Festlegen von

$$aa + 2bb = nn'$$

natürlich $n' < \frac{3}{4}$ sein wird. Nachdem nun dieser Wert eingesetzt und durch n geteilt worden ist, wird werden

$$N = n' + 2A + n\,(\alpha\alpha + 2\beta\beta)$$

III. Es werde mit n' multipliziert und durch das vorausgeschickte Lemma wird man haben

$$nn'\,(\alpha\alpha + 2\beta\beta) = (aa + 2bb)\,(\alpha\alpha + 2\beta\beta) = AA + 2BB$$

so dass man nun hat

$$Nn' = n'n' + 2n'A + AA + 2BB$$

welche Form offenbar auf diese zurückgeführt wird

$$Nn' = \left(n' + A\right)^2 + 2BB$$

und daher ebenso eine Zahl der form $pp + 2qq$ ist.
IV. Weil also $n' < n$ ist, wird es auf die gleiche Weise möglich sein, zu den folgenden Produkten Nn'', Nn''' etc. ununterbrochen abnehmen. Es ist also von Nöten, dass endlich zu der Form $N \cdot 1$ gelangt wird, so dass die Zahl N auch selbst in derselben Form $pp + 2qq$ enthalten ist. □

§9 *Lemma 3*

Das Produkt aus zwei Zahlen der Form $pp + 3qq$ kann immer auf die gleiche Form zurückgeführt werden.

Es sei nämlich ein solches Produkt $(aa + 3bb)(\alpha\alpha + 3\beta\beta)$ und ees werde genommen

$$A = a\alpha + 3b\beta \quad \text{und} \quad B = a\beta - b\alpha$$

offenbar wird man haben

$$AA + 3BB = (aa + 3bb)(\alpha\alpha + 3\beta\beta)$$

Lehrsatz 3

Wenn N ein Teiler der Zahl $pp + 3qq$ war, wo p und q einander prime Zahlen seien, dann wird die Zahl N selbst auf dieselbe Form zurückgeführt werden können.

Beweis.

Weil sich wiederum $p < \frac{1}{2}$ und $q < \frac{1}{2}$ ansehen lässt, wird die Form $pp + 2qq$ selbst kleiner als N^2 sein. Also wird nach Festlegen von

$$pp + 3qq = Nn$$

der Faktor n kleiner sein als N, welche Reduktion freilich für den Beweis nicht notwendig ist, er wird nämlich gleichermaßen ablaufen, auch wenn $n > N$ war, wie folgt.

I. Nach Festlegen von

$$p = a + \alpha n \quad \text{und} \quad q = b + \beta n$$

ist es hier möglich, die Zahlen a und b kleiner als $\frac{1}{2}n$ festzusetzen, zumindest nicht größer; dann wird aber sein

$$Nn = aa + 3bb + 2n(a\alpha + 3b\beta) + nn(\alpha\alpha + 3\beta\beta)$$

welche durch das vorausgeschickte Lemma wird

$$Nn = aa + 3bb + 2nA + nn(\alpha\alpha + 3\beta\beta)$$

II. Es ist also von Nöten, dass das erste Glied $aa + 3bb$ den Faktor n hat; daher wird nach Setzen von

$$aa + 3bb = nn'$$

diese Zahl n' gewiss kleiner sein als n, zumindest nicht größer; dann wird aber nach Division durch n hervorgehen

$$N = n' + 2A + n\,(\alpha\alpha + 3\beta\beta)$$

III. wir wollen auch mit n' multiplizieren und das letzte Glied

$$nn'\,(\alpha\alpha + 3\beta\beta) = (aa + 3bb)\,(\alpha\alpha + 3\beta\beta)$$

wird durch das vorausgeschickte Lemma $AA + 3BB$ und so werden wir haben

$$Nn' = n'n' + 2n'A + AA + 3BB$$

welcher Ausdruck natürlich auf diesen zurückgeführt wird

$$Nn' = \left(n' + A\right)^2 + 3BB$$

IV. Weil also Nn' wiederum von der Form $pp + 3qq$ und $n' < n$ ist, wird sich auf dieselbe Weise zu immer kleiner Produkten Nn'', Nn''', etc. fortschreiten lassen, bis schließlich zum letzten $N \cdot 1$ gelangt wird; und daher ist es bewiesen, dass N selbst von der Form $pp + 3qq$ sein wird. □

Korollar 1

Das Fundament dieses Beweises wie auch das des vorhergehenden besteht darin, dass von jeder beliebigen Zahl n aus zu einer anderen um Vieles kleineren n' gelangt wird, was in den Fällen, in denen n eine hinreichend große Zahl ist, per se klar ist. Ja diese Begründung ist sogar in dem Fall anwendbar, in dem $n = 1$ ist; weil nämlich dann $a = 0$ und $b = 0$ genommen werden können wird, wird wegen $nn' = 0$ natürlich $n' = 0$ werden.
Dennoch tritt indes für diesen Lehrsatz ein völlig einzigartiger Fall auf, wann immer in der Progression der Zahlen n, n', n'' etc. schließlich zu zwei gelangt wird; dieser Fall verdient umso größere Aufmerksamkeit, weil er nirgendwo anders auftaucht.

Korollar 2

Für diesen Fall wollen wir also sofort $n = 2$ festlegen und es ist offenbar, dass in der Formel $pp + 3qq$ jede der beiden Zahlen p und q ungerade sein muss; jede der beiden gerade anzunehmen, ist nämlich nicht möglich, weil p und q einander prim festgelegt werden. Daher, weil $p = a + 2\alpha$ und $q = b + 2\beta$ werden muss, wird $a = 1$ und $b = 1$ und daher $aa + 3bb = 4 = nn'$ werden,

woher es klar zutage tritt, dass auch $n' = 2$ sein wird, so dass keine weitere Verminderung auftreten kann. Sooft dies also passiert wird dann nicht die Zahl n selbst, sondern ihr Doppeltes $2N$ eine Zahl der Form $pp + 3qq$ sein.

Korollar 3

Dies wird umso deutlicher gemacht werden, wenn wir gründlich erwägen, dass die Form $pp + 3qq$, wann immer die beiden Zahlen p und q ungerade sind, nicht nur gerade ist, sondern auch durch h teilbar ist, und dass daher eine ungerade gerade Zahl nie von der Form $pp + 3qq$ sein kann. Sooft es also, wie es in diesen Fällen passiert, die Zahl $2N$ in der Form $pp + 3qq$ enthalten ist, dann wird N immer eine gerade Zahl sein und ihre Hälfte $\frac{1}{2}N$ oder der vierte Teil von $2N$ wird immer in dieser Form $pp + 3qq$ enthalten sein. Sooft nämlich jede der beiden Zahlen p und q ungerade ist, dann wird auch $\frac{pp+3qq}{4}$ eine Zahl von derselben Form sein, und das sogar in ganzen Zahlen, was freilich nicht so leicht erkannt wird. Denn nach Festlegen von $p = 2r + 1$ und $q = 2s + 1$ geht diese Form hervor

$$\frac{pp + 3qq}{4} = 1 + r + rr + 3s + 3ss$$

die sich allgemein in keineswegs in ganzen Zahlen auf ein Quadrat zusammen mit einem dreifachen Quadrat zurückführen lässt. Auf die folgende Weise wird aber diese Auflösung im Allgemeinen durchgeführt werden können. Ich bemerke nämlich, dass alle ungeraden Quadrate in dieser Form $(4m + 1)^2$ enthalten sind, wenn freilich für m auch negative Zahlen zugelassen werden, denn wenn m positiv ist, resultieren die Quadrate der Zahlen $1, 5, 9, 13$, etc., deren Form $4i + 1$ ist; wenn aber m eine negative Zahl ist, dann entspringen die Quadrate der Zahlen $3, 7, 1, 15$, etc., deren Form $4i - 1$ ist. Nun wollen wir festlegen

$$pp = (4r + 1)^2 \text{ und } qq = (4s + 1)^2$$

und es wird sein

$$\frac{pp + 3qq}{4} = 1 + 2r + 4rr + 6s + 12ss$$

welche offenbar auf diese Form zurückgeht

$$(1 + r + 3s)^2 + 3(r - s)^2$$

Bemerkung

Nachdem diese Lehrsätze vorausgeschickt worden sind, wollen wir das, was

uns besonders vorgelegt ist, angehen und werden beweisen, dass die Summe von vier Quadraten keine anderen Teiler zulässt, außer welche selbst die Summen von vier Quadraten sind. In Ähnlichkeit zu den vorhergehenden Lehrsätzen muss aber auch ein Lemma vorausgeschickt werden.

§10 *Lemma 4*

Das Produkt aus zwei oder mehr Zahlen, welche einzeln die Summen vierer Quadrate sind, kann auch immer durch eine Summe vierer Quadrate ausgedrückt werden.
Es sei ein solches Produkt

$$(aa + bb + cc + dd)\,(\alpha\alpha + \beta\beta + \gamma\gamma + \delta\delta)$$

und es werde genommmen

$$\begin{aligned} A &= a\alpha + b\beta + c\gamma + d\delta \\ B &= a\beta - b\alpha - c\delta + d\gamma \\ C &= a\gamma + b\delta - c\alpha - d\beta \\ D &= a\delta - b\gamma + c\beta - d\alpha \end{aligned}$$

und die Summe dieser Quadrate wird sein

$$A^2 + B^2 + C^2 + D^2 = \left(a^2 + b^2 + c^2 + d^2\right)\left(\alpha^2 + \beta^2 + \gamma^2 + \delta^2\right)$$

es ist offenbar, dass sich die einzelnen Produkte aus je zwei Anteilen gegenseitig aufheben und die einzelnen Quadrate der lateinischen Buchstaben mit den einzelnen der griechischen multipliziert werden.

Lehrsatz 4

Wenn N ein Teiler einer gewissen Summe vierer Quadrate oder der Form $pp + qq + rr + ss$ war, welche einzeln freilich durch N nicht teilbar sein, dann wird N gewiss eine Summe vierer Quadrate sein.

Beweis.
Es wird nicht wenig förderlich sein, angemerkt zu haben, dass jene vier Wurzeln p, q, r, s unter die Hälfte der vorgelegten Zahl N herabgesenkt werden können; der Beweis wird aber auf folgende Weise vonstatten gehen.
I. Während n den aus jener Division resultierenden Quotienten bezeichnet, dass ist

$$Nn = pp + qq + rr + ss$$

wo die Buchstaben p, q, r, s so zu n gerechnet werden, dass ist

$$p = a + n\alpha, q = b + n\beta, r = c + n\gamma, s = d + n\delta$$

ist es ersichtlich, dass ganz und gar alle Buchstaben a, b, c, d so genommen werden können, dass sie $\frac{1}{2}n$ nicht überragen, weil ja negative Werte davon nicht ausgeschlossen werden. Und so wird die Formel $aa + bb + cc + dd$ gewiss kleiner sein als nn.

II. Nachdem aber diese Werte eingesetzt worden sind, wird unsere Gleichung sein

$$Nn = aa + bb + cc + dd + 2n\,(a\alpha + b\beta + c\gamma + d\delta) + nn\,(\alpha\alpha + \beta\beta + \gamma\gamma + \delta\delta)$$

welche aus dem vorausgeschickten Lemma, wo wir festgelegt haben

$$A = a\alpha + b\beta + c\gamma + d\delta$$

so zusammengezogen wird

$$Nn = aa + bb + cc + dd + 2nA + nn\,(\alpha\alpha + \beta\beta + \gamma\gamma + \delta\delta)$$

weil also hier der erste Teil $aa + bb + cc + dd$ den Faktor n haben muss, werde festgelegt

$$aa + bb + cc + dd = nn'$$

und es wird insgesammt $n' < n$ sein, wie wir gerade gezeigt haben. Nach Division durch n werden wir also erhalten

$$N = n' + 2A + n\,(\alpha\alpha + \beta\beta + \gamma\gamma + \delta\delta)$$

III. Wir wollen nun mit n' multiplizieren, und weil $nn' = aa + bb + cc + dd$ ist, werden wir aus dem vorausgeschickten Lemma haben

$$nn'\,(\alpha\alpha + \beta\beta + \gamma\gamma + \delta\delta) = A^2 + B^2 + C^2 + D^2$$

nach Einführen welcher Form unsere Gleichung sein wird

$$Nn' = n'n' + 2n'A + A^2 + B^2 + C^2 + D^2$$

welche natürlich auf diese vier Quadrate zurückgeführt wird

$$Nn' = \left(n' + A\right)^2 + B^2 + C^2 + D^2$$

IV. Sofern also hier $n' < n$ ist, wird es auf dieselbe Weise möglich sein, zu immer kleineren Formen Nn'', Nn''', etc. zu gelangen, bis schließlich bei der Form $N \cdot 1$ angekommen wird und daher die vorausgeschickte Zahl N vier Quadraten gleich wird. □

Korollar 1

Diese Schlussweise ist wiederum einer kleinen Ausnahme unterworfen, wann immer natürlich $n = 2$ war und alle Zahlen p, q, r, s ungerade waren; dann wird nämlich $a = 1, b = 1, c = 1$ und $d = 1$ und daher $nn' = 4$ werden, so dass auch $n' = 2$ und so wohl kleiner als n ward. Aber weil daher die Zahl $2N$ einer Summe vierer Quadrate gleich wird, ist es anders woher klar, dass die Hälfte N eine Summe vierer Quadrate sein, so dass diese Ausnahme überhaupt nichts zu stören anzusehen ist.

Korollar 2

Damit dies besser erkannt wird, seien die Zahlen p, q, r, s ungerade und n gerade; dann, weil $Nn = pp + qq + rr + ss$ ist, wird sein

$$\frac{1}{2}Nn = \left(\frac{p+q}{2}\right)^2 + \left(\frac{p-q}{2}\right)^2 + \left(\frac{r+s}{2}\right)^2 + \left(\frac{r-s}{2}\right)^2$$

welche vier Quadrate ebenso ganzzahlig sein werden; diese Reduktion wird sich gebrauchen lassen, solange alle vier Wurzeln der Quadrate ungerade waren; dann entfällt die zuvor erwähnte Ausnahme von selbst.

Bemerkung

Mit diesem Beweis wird jener Fermat'sche Lehrsatz zum größten Teil erledigt, weil ja der andere Teil, der noch übrig ist, dass natürlich nach Vorlegen irgendeiner Primzahl immer durch jene Teilbare Summen vierer Quadrate dargeboten werden können, von mir schon vor langer Zeit klar dargetan und sogar neulich vom hochgeehrten Lagrange mit einem sehr gründlichen Beweis gesichert worden ist. Damit ich dennoch dieses Argument ganz zu Ende führe, mochte ich den folgenden sehr leichten Beweis beifügen.

§11

Lehrsatz 5

Nach Vorlegen irgendeiner Primzahl N können nicht nur vier Quadrate, sondern sogar drei Quadrate auf unendlich viele Arten dargeboten werden, deren Summe durch diese Zahl N teilbar ist und deren einzelne dennoch nicht durch sie geteilt werden können.

Beweis.

In Bezug auf die Zahl N sind gänzlich alle Zahlen in einer der folgenden

Formen enthalten

$$\lambda N, \lambda N + 1, \lambda N + 2, \lambda N + 3, \ldots, \lambda N + N - 1$$

deren Anzahl N ist. Nachdem aber die erste Form beiseite gelegt worden ist, die Vielfachen von N enthält, ist über die übrigen, deren Anzahl $N - 1$ ist, anzumerken, dass die Quadrate der erste Form $\lambda N + 1$ und der letzten $\lambda N + N - 1$ auf dieselbe Form $\lambda N + 1$ zurückgehen, die Quadrate der zweiten Form $\lambda N + 2$ und der vorletzten $\lambda N + N - 2$ hingegen auf die Form $\lambda N + 4$, der dritten und der vorletzten aber auf $\lambda N + 9$, und so weiter, so dass nur diese Formen

$$\lambda N + 1, \lambda N + 4, \lambda N + 9, \text{ etc.}$$

deren Anzahl $\frac{1}{2}(N - 1)$ ist, Quadrate in sich umfassen können, welche wir Formeln der ersten Klasse nennen und so bezeichnen wollen

$$\lambda N + a, \lambda N + b, \lambda N + c, \lambda N + d, \text{ etc.}$$

so dass die Buchstaben a, b, c, d, etc. entweder die Quadrate $1, 4, 9, 16$, etc. selbst oder, wenn sie die Zahl N überschreiten, die aus der Division resultierenden Reste. Aber die übrigen Formen, deren Anzahl ebenso $\frac{1}{2}(N - 1)$ sein wird, werden hingegen auf diese Weise dargestellt

$$\lambda N + \alpha, \lambda N + \beta, \lambda N + \gamma, \lambda N + \delta, \text{ etc.}$$

welche wir Formen der zweiten Klasse nennen werden. Über diese zwei Klassen seien aber die drei folgenden Eigenschaften angemerkt, welche sich freilich leicht beweisen lassen.

I. Das Produkt aus zwei Zahlen der ersten Klasse ist ebenso in der ersten Klasse enthalten, natürlich wird die Form $\lambda N + ab$ in der ersten Klasse aufgefunden werden; wenn nämlich ab größer als N war, ist an ihrer Stelle der aus der Division durch N zurückgelassenen Rest genommen zu werden zu verstehen.

II. Die Zahlen der erste Klasse a, b, c, d, etc. werden mit irgendeiner Zahl der zweiten Klasse $\alpha, \beta, \gamma, \delta$, etc. multipliziert in die zweite Klasse fallen.

III. Schließlich werden die Produkte aus zwei Zahlen der zweiten Klasse, wie beispielsweise $\alpha\beta$, in die erste Klasse übertragen werden.

Nachdem diese Dinge vorausgeschickt worden sind, werde ich beweisen: Wenn keine drei Quadrate gegeben wären, deren Summe durch N teilbar wäre, dass dann daher etwas höchst Absurdes folgen würde. Dafür wollen

wir solange im Gegenteil annehmen, dass keine drei Quadrate gegeben sind, deren Summe durch N teilbar ist; um Vieles weniger werden also zwei solche Quadrate gegeben sein. Daher folgt sofort, dass die Form $\lambda N - a$, oder was auf dasselbe zurückgeht, $\lambda N + (N - a)$ nicht in der ersten Klasse auftaucht; wenn nämlich ein Quadrat der Form $\lambda N - a$ gegeben wäre, würde dieses zum Quadrate der Form $\lambda N + a$ eine durch N teilbare Summe liefern, entgegen der Annahme. Also ist es notwendig, dass die Form $\lambda N - a$ in der zweiten Klasse enthalten ist und so werden unter den Buchstaben $\alpha, \beta, \gamma, \delta$, etc. die Zahlen $-1, -4, -9$, etc. aufgefunden werden. Es sei f irgendeine Zahl der ersten Klasse, so dass Quadrate der Form $\lambda N + f$ gegeben sind; wenn zu diesen Quadrate der Form $\lambda N + 1$ addiert werden, wird die Summe zweier Quadrate die Form $\lambda N + f + 1$ haben. Wenn nur ein Quadrat der Form $\lambda N - f - 1$ gegeben wäre, hätte man eine durch N teilbare Summe dreier Quadrate; weil dies verneint wird, wird die Form $\lambda N - f - 1$ nicht in der ersten Klasse und daher in der zweiten enthalten sein; weil also in dieser die Zahlen -1 und $-f - 1$ aufgefunden werden, ist es notwendig, dass deren Produkt $+f + 1$ in der ersten Klasse auftaucht. Auf die gleiche Weise wird gezeigt werden, dass in der ersten Klasse auch diese Zahlen auftauchen müssen

$$f + 2, f + 3, f + 4, \text{ etc.}$$

daher würden nach Nehmen von $f = 1$ in der ersten Klasse gänzlich alle Formen auftauchen

$$\lambda N + 1, \lambda N + 2, \lambda N + 3, \text{ etc.}$$

und es würden überhaupt keine für die zweite Klasse übrig gelassen werden. Dennoch haben wir indes auch gesehen, dass in der zweiten Klasse diese Zahlen auftauchen

$$-1, -f - 1, -f - 2, \text{ etc.}$$

und daher auch gänzlich alle Formen; weil dies im höchsten Maße absurd ist, folgt, dass es falsch ist, dass keine drei Quadrate gegeben sind, deren Summe durch die vorgelegte Zahl N teilbar ist. Es sind also insgesamt drei und um Vieles mehr vier Quadrate dieser Art geben, deren Summe durch N teilbar sein wird. □

Korollar

Aus diesem Lehrsatz mit dem vorhergehenden verbunden folgt offenbar, dass

gänzlich alle Primzahlen Summen vierer oder weniger Quadrate sind. Und weil die Produkte aus zwei oder mehreren Zahlen dieser Art derselben Natur folgen, ist es sehr solide dargetan, dass gänzlich alle Zahlen Summen vierer oder sogar weniger Quadrate sind.

Bemerkung

Anstelle dieser Proposition hat der hochgeehrte Lagrange einen sich um Vieles weiter erstreckenden Lehrsatz angeführt und mit einem zwar äußerst geistreichen, aber dermaßen schwer ergründbaren und schwer verständlichen, dass er nur unter Aufbringung höchster Aufmerksamkeit begriffen werden kann, Beweis gesichert. Er hat natürlich bewiesen, dass nach Vorlegen irgendeiner Primzahl A immer zwei zu jener prime Quadrate pp und qq gegeben werden können, so dass die Formel $pp - Bqq - C$ durch die Primzahl A teilbar wird, welche Zahlen auch immer für die Buchstaben B und C angenommen werden, solange sie in Bezug auf A prim waren. Denselben Lehrsatz ein wenig weiter erstreckt möchte ich also hier mit einem weit leichteren und klareren Beweis beifügen.

§12

Lehrsatz 6

Nach Vorlegen irgendeiner Primzahl N ist es immer möglich, drei zu selbiger prime Quadrate xx, yy und zz darzubieten, dass die Formel

$$\lambda xx + \mu yy + \nu zz$$

durch jene Primzahl N teilbar wird, solange diese Koeffizienten λ, μ und ν zu N prim waren, das heißt, dass keine derer weder verschwindet noch N selbst oder einem bestimmten Vielfachen von ihr gleich war.

Beweis.
Es bezeichnen die Buchstaben

$$a, b, c, d, \text{ etc.}$$

alle Reste, die aus der Division von Quadraten durch jene Primzahl N zurückgelassen werden, welche Zahlen wir zuvor zur ersten Klasse gerechnet haben, deren Menge $\frac{1}{2}(N-1)$ ist; in ihnen tauchen natürlich alle kleineren Quadratzahlen $1, 4, 9, 16$, etc. als N auf, die aus jener Division durch N resultierenden Reste der größeren Kommen aber auch hinzu. Zu derselben Klasse

sind aber auch dieselben Zahlen a, b, c, d, etc. um ein gewisses Vielfaches der Zahl N vermehrt zu rechnen. Aber alle übrigen Zahlen kleineren Zahlen als N, deren Anzahl ebenso $\frac{1}{2}(N-1)$ ist und welche sich Nicht-Reste nennen lassen, sind zur zweiten Klasse gezählt worden und werden mit den griechischen Buchstaben

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

bezeichnet. Über diese Zahlen der zwei Geschlechter haben wir schon zuvor [§10] angemerkt, dass die Produkte aus zwei Resten oder der ersten Klasse wiederum in dieselbe Klasse fallen, wie beispielsweise ab, ac, bc, etc., sofern sie natürlich durch Division unter N herabgesenkt werden, aber das Produkt aus einem Rest mit einem Nicht-Rest in der zweiten Klasse der Nicht-Reste aufgefunden wird und schließlich Produkte aus zwei Nicht-Resten wiederum Reste sein werden. Nachdem diese Dinge bemerkt worden sind, werden wir den Beweis so führen, dass wir zeigen, dass etwas vollkommen absurdes folgen wird, wenn keine durch die Zahl N teilbare Formel $\lambda xx, \mu yy + \nu zz$ gegeben wäre. Der Beweis wird aber auf die folgen Weise vonstatten gehen.
I. Weil alle Quadrate einem gewissen Reste a oder b oder c um ein gewisses Vielfaches der Zahl N vermehrt gleich werden, wenn eine solche durch die Zahl N teilbare Formel $\lambda xx + \mu yy + \nu zz$ gegeben wäre, wäre wegen $xx = \zeta N + a, yy = \eta N + b$ und $zz = \vartheta N + c$ natürlich die Formel $\lambda a + \mu b + \nu c$ durch N teilbar. Wer unser daher unseren Lehrsatz verneinen wird, muss festlegen, dass keine durch N teilbare Formeln dieser Art $\lambda a + \mu b + \nu c$ gegeben ist.
II. Weil also keine durch N teilbare Form dieser Art gegeben ist, wird sie um vieles weniger $= 0$ werden können und daher wird diese Gleichung $\lambda a = -\mu b - \nu c$ genauso wie eine solche Gleichung unmöglich sein

$$\lambda a = (\zeta N - \mu)\, b + (\eta N - \nu)\, c$$

Aber weil λ, μ und ν zu N prim sind, lassen sich die Koeffizienten ζ und η immer so annehmen, dass die Formeln $\zeta N - \mu$ und $\eta N - \nu$ durch λ teilbar werden. Wir wollen also festlegen

$$\zeta N - \mu = \lambda m \quad \text{und} \quad \eta N - \nu = \lambda n$$

und es wird auch diese Gleichung unmöglich sein

$$a = mb + nc$$

III. Weil also diese Formel $mb + nc$ nicht gleich a ist und daher nicht in der Klasse der Reste aufgefunden wird (natürlich in Annahme des Gegenteils,

was unser Lehrsatz negiert) wird sie notwendigerweise; ebendort wird also auch (weil c die Einheit bezeichnen kann) $mb + n$ auftauchen und daher sogar all diese Formeln

$$ma + n, mb + n, mc + n, md + n, \text{ etc.}$$

weil diese alle voneinander verschieden und an der Zahl $\frac{1}{2}(N-1)$ sind, wird mit diesen die ganze Klasse der Nicht-Reste ausgeschöpft werden, sofern natürlich die durch N geteilten unter N herabgestuft werden.
IV. In derselben Klasse müssen aber auch alle Produkte dieser Zahlen mit jeder beliebigen Zahl der ersten Klasse, wie beispielsweise d, multipliziert auftauchen, welche also sein werden

$$mad + nd, mbd + nd, mcd + nd, \text{ etc.}$$

Aber die Produkte ad, bd, cd, etc. fallen in die erste Klasse und werden unter den Zahlen a, b, c, d, etc. selbst aufgefunden werden; und so werden in der anderen Klasse der Nicht-Reste auch alle diese Formeln auftauchen

$$ma + nd, mb + nd, mc + nd, \text{ etc.}$$

welches die einzelnen vorhergehenden um die Größe $n(d-1)$ überragen. Dieser Unterschied werde der Kürze wegen $= \omega$ gesetzt, welcher natürlich zum Teiler N selbst prim sein wird, wenn nur für d nicht Einheit angenommen wird, weil $d - 1 < N$ und n eine zu N prime Zahl ist.
V. Wenn daher also in der Klasse der Nicht-Reste die Zahl α enthalten ist, wird ebendort auch $\alpha + \omega$ auftauchen und desselben Grundes wegen ist es von Nöten, dass diese Zahl wiederum den Zuwachs ω erhaltend, natürlich $\alpha + 2\omega$, dort aufgefunden wird und desselben Grundes wegen auch die Zahlen $\alpha + 3\omega, \alpha + 4\omega$, etc. Also werden alle Terme dieser arithmetischen Progression

$$\alpha, \alpha + \omega, \alpha + 2\omega, \alpha + 3\omega, \text{ etc.}$$

sofern sie natürlich durch N geteilt unter N herabgesenkt werden, unter den Nicht-Resten auftauchen müssen.
VI. Weil die Differenz dieser Progression ω ist, eine natürlich zu N prime Zahl, tauchen in dieser Progression nicht nur durch N teilbare Terme auf, sondern darüber hinaus alle, die durch N geteilt für die Reste gänzlich alle Zahlen $1, 2, 3, 4$, etc., die Null nicht ausgeschlossen, liefern. Deshalb würden in der Annahme des Gegenteils in der Klasse der Nicht-Reste gänzlich alle

Zahlen $1, 2, 3, 4$, etc. auftauchen; weil dies absurd ist, ist die Annahme des Gegenteils gewiss falsch. Natürlich ist es falsch, dass keine Zahlen dieser Form gegeben und

$$\lambda xx + \mu yy + \nu zz$$

die durch N teilbar sind. Also werden natürlich solche Zahlen gegeben sein; und dies ist das selbst, was wir zu zeigen unternommen haben. □

Korollar 1

Nicht nur aber ist es möglich, immer diese Quadrate dieser Art xx, yy und zz aufzufinden, sondern lässt sich auch einer derer, wie beispielsweise zz, nach Belieben annehmen, solange es nicht durch N teilbar ist. So, wenn f eine nach Belieben gegebene durch N nicht teilbare Zahl bezeichnet, wird es immer möglich sein, zwei Quadrate xx und yy anzugeben, dass die Formel

$$\lambda xx + \mu yy + \nu ff$$

durch N teilbar wird. Um dies zu bewiesen, welche Zahl auch immer z ist, wird immer eine Zahl ν solcher Art gegeben sein, dass das Produkt νz durch N geteilt den gegebenen Rest f zurücklässt. Es sei nämlich $\nu z = \vartheta N + f$ und unsere Formeln wird mit $\nu\nu$ multipliziert, welche natürlich noch durch N teilbar sein wird, werden

$$\lambda\nu\nu xx + \mu\nu\nu yy + \nu\left(\vartheta\vartheta NN + 2\vartheta Nf + ff\right)$$

wo, weil die Glieder $\vartheta\vartheta NN + 2\vartheta Nf$ durch N von selbst teilbar sind, auch die übrige Form

$$\lambda\nu\nu xx + \mu\nu\nu yy + \nu ff$$

durch N teilbar sein wird.

Korollar 2

Welche Zahlen nämlich auch immer λ, μ, ν waren, für eine von diesen lässt sich immer die Einheit oder eine andere Zahl nach Belieben annehmen. Weil nämlich durch Multiplizieren mit ϑ diese Formel

$$\vartheta\lambda xx + \vartheta\mu yy + \vartheta\nu zz$$

eine Division durch N zulässt, wird es möglich sein, anstelle von ϑ eine Zahl solcher Art anzunehmen, dass das Produkt $\vartheta\lambda$ durch N geteilt die Einheit zurücklässt; dann aber wird dise Formel

$$xx + \vartheta\mu yy + \vartheta\nu zz$$

immer noch durch N teilbar sein. Ja es lassen sich sogar Zwei anstelle von $\vartheta\mu$ und $\vartheta\nu$ aus der Division durch N herstammende Reste schreiben und auf diese Weise erreichen wir eine jener, welche der hochgeehrte Lagrange betrachtet hat, ganz und gar gleiche Form.

Bemerkung

Betrachte und staune also, wir haben diesen für alle Zahlen geführt Beweis jenes allbekannten Lehrsatzes erhalten, dass gänzlich alle Zahlen Summen vierer oder weniger Quadrate sind, welchen freilich schon einst Fermat selbigen gefunden zu haben sich öffentlich bekannt hat, aber dennoch ist es immer noch äußerst zu bedauern, dass er unglücklicherweise mit der Zeit verloren gegangen ist. Denn es besteht überhaupt kein Zweifel, dass dieser Fermat'sche Beweis um Vieles einfacher und allgemeiner war als diese, die nun erst das Licht der Welt erblickt haben. Sofern es sich nämlich aus seinen Monumenten vermuten lässt, scheint er seinen Beweis und ganz verschiedenen Prinzipien hergeholt zu haben, weil er ja versichert hatte, dass er ihn aus derselben Quelle bewiesen hat, dass gänzlich alle Zahlen die Summen entweder dreier oder weniger Dreieckszahlen, dann auch die Summen von für fünf oder weniger Pentagonalzahlen und auch die Summen von sechs Hexagonalzahlen sind, und so weiter, von welcher Allgemeinheit dieser Beweis noch sehr weit entfernt ist. Und immer noch kennen wir keinen Beweis, dass jede Zahl die Summe dreier oder weniger Trigonalzahlen ist. Dennoch ist es indes passend, dass über diesen Lehrsatz bemerkt wird, dass er nur in ganzen Zahlen wahr ist, während der andere, welchen wir hier bewiesen haben, auch in gebrochenen erfüllt wird; denn alle diese Brüche $\frac{1}{2}, \frac{3}{2}, \frac{5}{2}, \frac{7}{2}, \frac{9}{2}$ lassen es sich auf keine Weise zu, in drei Dreieckszahlen aufgelöst zu werden und es lassen sich keine natürlichen Werte anstelle von x, y, z finden, dass wird

$$\frac{1}{2} = \frac{xx + x}{2} + \frac{yy + y}{2} + \frac{zz + z}{2}$$

daher, was im höchsten Maße zu verwundern scheint, ist diese Gleichung

$$1 = xx + x + yy + y + zz + z$$

unmöglich, welche gebrochenen Zahlen auch immer für x, y, z angenommen werden.