Über Zahlen, die aggregate zweier Quadrate sind *

Leonhard Euler

§1 Die Natur der Zahlen pflegen die Arithmetiker auf mehrere Arten zu erforschen, während sie deren Ursprung entweder durch Addition oder durch Multiplikation darstellen. Von der ersten Art ist ohne Zweifel die einfachste Zusammensetzung die aus Einheiten, nach welcher alle ganzen Zahlen durch die Aggregation von Einheiten zu entspringen aufgefasst werden. Dann können Zahlen auch so betrachtet werden, wie sie aus der zweier oder mehrerer ganzer Zahlen entstehen, worauf sich das Problem über die Partition von Zahlen bezieht, dessen Lösung ich vor nunmehr einigen Jahren dargelegt habe, in welchem gesucht wird, auf wie viele verschiedene Weisen jede beliebige vorgelegte Zahl durch Addition zweier oder mehrerer kleinerer Zahlen resultieren kann. Hier aber habe ich beschlossen, die Zusammensetzung von Zahlen zu betrachten, mit welcher sie durch Addition zweier Quadrate hervorgehen; und weil auf diese Weise nicht alle Zahlen entspringen, weil die Menge dieser riesig ist, die durch Addition zweier Quadrate nicht hervorgebracht werden können, möchte ich die Natur und Eigenschaften derer, die Summen zweier Quadrate sind, hier untersuchen. Auch wenn viele dieser Eigenschaften schon erkannt und quasi durch Induktion gefunden worden sind, sind sie dennoch zum größten Teil nicht mit strengen Beweisen untermauert; weil ein nicht zu verachtender Teil der Diophant'schen Analysis auf deren Gültigkeit gestützt

*Originaltitel: „De numeris, qui sunt aggregata duorum quadratorum", erstmals publizert in „Novi Commentarii academiae scientiarum Petropolitanae 4, 1758, pp. 3-40", Nachdruck in „Opera Omnia: Series 1, Volume 2, pp. 295 - 327" und „Commentat. arithm. 1, 1849, pp. 155-173 [E228b]", Eneström Nummer E228, übersetzt von: Alexander Aycock, Textsatz: Jens Becker, im Ramen des Hauptseminars „Euler" 2013/14

ist, werde ich in dieser Abhandlung den Beweis vieler dieser Eigenschaften, die bis jetzt ohne Beweise zugelassen worden sind, geben, zugleich werde ich aber auch mitteilen, was es mir freilich immer noch nicht zu beweisen möglich gewesen ist, auch wenn wir über deren Gültigkeit in keinster Weise zweifeln können.

§2 Zuerst wird es also, weil die Quadratzahlen sind:
$1, 4, 9, 16, 25, 36, 49, 64, 81, 100, 121, 144, 169, 196$ etc. förderlich sein, diese Zahlen, die aus der Kombination zweier Quadrate entspringen, angeschaut zu haben, welche ich deshalb bis hinzu 200 hier aufführe:
$0, 1, 2, 4, 5, 8, 9, 10, 13, 16, 17, 18, 20, 25, 26, 29, 32, 34, 36, 37, 40, 41, 45, 49, 50,$
$52, 53, 58, 61, 64, 65, 68, 72, 73, 74, 80, 81, 82, 85, 89, 90, 97, 98, 100, 101, 104, 106,$
$109, 113, 116, 117, 121, 122, 125, 128, 130, 136, 137, 144, 145, 146, 148, 149, 153,$
$157, 160, 162, 164, 169, 170, 173, 178, 180, 181, 185, 193, 194, 196, 197, 200$
Dies sind natürlich alle Zahlen bis hin zu 200, die aus der Addition zweier Quadrate hervorgehen, und diese Zahlen mit allen ins Unendliche folgenden werde ich als die Summen zweier Quadrate bezeichnen, welche deshalb in dieser allgemeinen Formal $xx + yy$ erfasst zu werden offenbar ist, während für x und y nacheinander alle ganzen Zahlen $0, 1, 2, 3, 4, 5, 6$ etc. eingesetzt werden. Welche Zahlen also in diesen nicht aufgefunden werden, die sind nicht Summen zweier Quadrate; diese sind also bis hin zu 200:
$3, 6, 7, 11, 12, 14, 15, 19, 21, 22, 23, 24, 27, 28, 30, 31, 33, 35, 38, 39, 42, 43, 44,$
$46, 47, 48, 51, 54, 55, 56, 57, 59, 60, 62, 63, 66, 67, 69, 70, 71, 75, 76, 77, 78, 79, 83,$
$84, 86, 87, 88, 91, 92, 93, 94, 95, 96, 99, 102, 103, 105, 107, 108, 110, 111, 112, 114,$
$115, 118, 119, 120, 123, 124, 126, 127, 129, 131, 132, 133, 134, 135, 138, 139, 140,$
$141, 142, 143, 147, 150, 151, 152, 154, 155, 156, 158, 159, 161, 163, 165, 166, 167,$
$168, 171, 172, 174, 175, 176, 177, 179, 182, 183, 184, 186, 187, 188, 189, 190, 191,$
$192, 195, 198, 199$
Daher tritt klar zutage, dass zumindest bis 200 die Menge der Zahlen, die nicht Summen zweier Quadrate sind, größer ist als die derer, die Summen zweier Quadrate sind. Im Übrigen wird dem Betrachtenden sofort klar werden, dass keine der beiden Reihen dieser Zahlen in einem bestimmten und angebbaren Gesetz enthalten sind und es deswegen selbst schwierig sein wird, die natürliche Beschaffenheit jeder der beiden zu untersuchen.

§3 Weil jede Quadratzahl entweder gerade und in diesem Fall durch 4 teilbar und in dieser Form $4a$ enthalten ist, oder ungerade und in diesem Fall in dieser

Form $8b + 1$ enthalten ist, wird jede aus zwei Quadraten zusammengesetzte Zahl sein:
Entweder erstens die Summe zweier gerader Quadrate und sich auf diese Form $4a + 4b$ beziehen und also durch 4 teilbar sein; oder zweitens die Summe zweier Quadrate, eines geraden und eines ungeraden, und deshalb in einer Form dieser Art $4a + 8b + 1$ oder in dieser $4a + 1$ enthalten sein; sie wird also ein Vielfaches von vier um die Einheit überschreiten; oder drittens die Summe zweier ungerader Quadrate und wird deshalb von dieser Form $8a + 1 + 8b + 1$ sein oder in dieser $8a + 2$ enthalten sein; sie wird natürlich eine verdoppelte ungerade Zahl sein und um zwei ein Vielfaches von acht übersteigen.
Weil also alle ungerade Zahlen entweder um die Einheit ein Vielfaches von vier übersteigen oder von dieser Form sind $4n + 1$, oder um die Einheit nach unten von einem Vielfachen von vier abweichen oder von dieser Form sind $4n - 1$, tritt es klar zutage, dass keine ungeraden Zahlen von dieser zweiten Form $4n - 1$ die Summen zweier Quadrate sind; oder aus der Reihe der Zahlen, die Summen zweier Quadrate sind, werden alle in dieser Form $4n - 1$ enthaltenen Zahlen ausgeschlossen.
Weil des Weiteren alle verdoppelten ungeraden Zahlen entweder um zwei ein Vielfaches von acht übersteigen, dass sie $8n + 2$ sind, oder um zwei von einem Vielfachen von acht nach unten abweichen, dass sie $8n - 2$ sind, tritt es klar zutage, dass keine Zahlen dieser letzten Form Summen zweier Quadrate sind; und so werden aus der Reihe der Zahlen, die Summen zweier Quadrate sind, die Zahlen von dieser Form ausgeschlossen $8n - 2$.
Dennoch ist indess sorgfältig zu bemerken, dass weder alle in dieser Form $4n + 1$ noch die in dieser $8n + 2$ enthaltenen die Summe zweier Quadrate sind. Von jener Form werden nämlich die Zahlen $21, 33, 48, 69, 77, 93, 105, 129$ etc. ausgeschlossen, von dieser hingegen diese $42, 66, 114, 138, 154$ etc. , deren Beschaffenheit später untersucht werden wird.

§4 Dennoch sind indess die Zahlen, die Summen zweier Quadrate sind, so mit einem gewissen Zusammenhang miteinander verbunden, dass aus einer einzigen Zahl von dieser natürlichen Beschaffenheit unendlich viele andere derselben Natur angegeben werden können. Damit dies leichter erkannt wird, möchte ich die folgenden Lemmata, die freilich für gewöhnlich hinreichend bekannt sind, hinzufügen.

- I.
  Wenn die Zahl p die Summe zweier Quadrate ist, werden auch die Zahlen $4p, 9p, 16p$ und allgemein nnp Summen zweier Quadrate sein. Weil nämlich $p = aa + bb$ ist, wird sein $4p = 4aa + 4bb$, $9p = 9aa + 9bb$, $16p = 16aa + 16bb$ und $nnp = nn(aa + bb)$ welche Formen gleichermaßen Summen zweier Quadrate sind.

- II.
  Wenn die Zahl p die Summe zweier Quadrate ist, wird auch $2p$ und allgemein $2nnp$ die Summe zweier Qudrate sein.
  Es sei nämlich $p = aa + bb$; es wird $2p = 2aa + 2bb$ sein. Aber es ist

$$2aa + 2bb = (a + b)^2 + (a - b)^2 \tag{1}$$

  Woher sein wird

$$2p = (a + b)^2 + (a - b)^2 \tag{2}$$

  und deshalb die Summe zweier Quadrate. Daher wird in der Tat weiter sein

$$2nnp = nn(a + b)^2 + nn(a - b)^2 \tag{3}$$

- III.
  Wenn die Zahl $2p$ die Summe zweier Quadrate war, wird auch ihre Hälfte p die Summe zweier Quadrate sein.
  Es sei nämlich $2p = aa + bb$; es wird jede der beiden Zahlen a und b entweder gerade oder ungerade sein, woher in jedem der beiden Fälle so $\frac{a+b}{2}$ wie $\frac{a-b}{2}$ eine ganze Zahl sein wird. Es ist in der Tat

$$aa + bb = 2(\frac{a + b}{2})^2 + 2(\frac{a - b}{2})^2 \tag{4}$$

  nach Einsetzen welches Wertes wird

$$p = (\frac{a + b}{2})^2 + (\frac{a - b}{2})^2 \tag{5}$$

Daher werden also alle geraden Zahlen, die Summen zweier Quadrate sind, durch wiederholte Zweiteilung schließlich auf ungerade Zahlen derselben

Gestalt zurückgeführt werden. Wenn umgekehrt allein ungerade Zahlen, die Summen zweier Quadrate sind, erkannt werden, werden aus ihnen auch alle geraden Zahlen durch wiederholte Verdopplung deriviert werden.

§5 Des Weiteren ist das folgende Theorem des Merkens würdig, mit welchem die Natur der Zahlen, die Summen zweier Quadrate sind, nicht unwesentlich ans Licht gebracht werden.

Theorem

Wenn p und q zwei Zahlen sind, von denen jede der beiden die Summe zweier Quadrate ist, wird auch deren Produkt pq die Summe zweier Quadrate sein.

Beweis

Es sei $p = aa + bb$ und $q = cc + dd$; es wird sein

$$pq = (aa + bb)(cc + dd) = aacc + aadd + bbcc + bbdd \tag{6}$$

welcher Ausdruck auf diese Weise dargestellt werden kann, dass ist

$$pq = aacc + 2abcd + bbdd + aadd - 2abcd + bbcc \tag{7}$$

und daher

$$pq = (ac + bd)^2 + (ad - bc)^2 \tag{8}$$

welcher das Produkt pq, die Summe zweier Quadrate sein wird

QED

Aus dieser Proposition folgt, auf welche Weise auch immer mehrere Zahlen, welche einzelnen die Summen zweier Quadrate seien, miteinander multipliziert werden, dass die Produkte immer die Summen zweier Quadrate sind. Und aus dieser angegebenen allgemeinen Form tritt es klar zutage, dass ein Produkt aus zwei Zahlen dieser Art auf zwei Weisen in zwei Quadrate aufgelöst werden kann. Wenn nämlich $p = aa + bb$ und $q = cc + dd$ ist, wird so

$$pq = (ac + bd)^2 + (ad - bc)^2 \tag{9}$$

wie sein

$$pq = (ac - bd)^2 + (ad + bc)^2 \tag{10}$$

welche Formeln verschieden sein werden, wenn nicht entweder $a = b$ oder $c = d$ ist. Weil so $5 = 1 + 4$ und $13 = 4 + 9$ ist, wird das Produkt auf zwei Arten die Summe zweier Quadrate sein, es wird natürlich sein

$$65 = (1 \cdot 3 + 2 \cdot 2)^2 + (2 \cdot 3 - 1 \cdot 2)^2 = 49 + 16 \tag{11}$$

und

$$65 = (2 \cdot 2 - 1 \cdot 3)^2 + (2 \cdot 3 + 1 \cdot 2)^2 = 1 + 64 \tag{12}$$

Und wenn man ein Produkte aus mehreren Zahlen hat, welche einzelnen die Summen zweier Quadrate seien, wird es auf mehrere Arten in zwei Quadrate aufgelöst werden können. Wie wenn die Zahl $1105 = 5 \cdot 13 \cdot 17$ vorgelegt wird, werden ihre Auflösungen in zwei Quadrate diese sein

$$1105 = 33^2 + 4^2 = 32^2 + 9^2 = 31^2 + 12^2 = 24^2 + 23^2 \tag{13}$$

Hier haben natürlich vier Auflösungen Geltung.

§6 Obwohl aber so dargetan worden ist, wenn die Faktoren p und q Summen zweier Quadrate sind, dass auch das Produkt pq die Summe zweier Quadrate sein wird, folgt dennoch die Umkehrung dieser Proposition nicht, dass, wenn das Produkt die Summe zweier Quadrate ist, auch ihre Faktoren Zahlen von derselben Natur sind; denn diese Schlussfolgerung würden weder die Regeln der Logik noch die Natur der Sache selbst billigen. Denn die Zahl $45 = 36 + 9$ ist die Summe zweier Quadrate, dennoch ist keiner von beiden dieser Faktoren von ihr $3, 15$ die Summe zweier Quadrate. Solider mag diese Schlussfolgerung scheinen: Wenn das Produkt pq und der eine der beiden ihrer Faktor p die Summen zweier Quadrate waren, dass dann auch der andere Faktor q die Summe zweier Quadrate sein wird. Obgleich aber diese Schlussfolgerung zufällig wahr ist, wird sie dennoch mit den Regeln das logischen Schließens nicht bestätigt, denn es kann nicht, weil bewiesen worden ist, wenn die beiden Faktoren p und q des Produktes pq Summen zweier Quadrate sind, dass

pq selbst eine Summe zweier Quadrate ist, daher die legitime Konsequenz gezogen werden: Wenn sowohl das Produkt pq als auch der eine Faktor p Summe zweier Quadrate sind, dass auch der andere Faktor q eine Summe zweier Quadrate sein wird. Dass nämlich eine logische Folgerung dieser Art nicht legitim ist, wird auch dieser Beispiel ersichtlich dartun: Es ist gewiss, wenn die zwei Faktoren p und q gerade Zahlen sind, dass auch das Produkt pq eine gerade Zahl sein wird; wenn jemand aber daher folgern will, wenn das Produkt pq und der eine Faktor gerade sind, dass auch der andere Faktor q gerade sein wird, würde er sich gewaltig täuschen.

§7 Wenn es daher wahr ist, dass, weil das Produkt pq und sein einer Faktor p Summe zweier Quadrate waren, auch der andere Faktor q eine Summe zweier Quadrate ist, kann diese Proposition nicht aus der zuvor bewiesenen vorgebracht werden, sondern muss mit einem eigenen Beweis gesichert werden. Aber dieser Beweis ist nicht so klar wie der vorhergehende und kann nur durch mehrere Umwege hindurch zustande gebracht werden; und dieser Beweis, den ich gefunden habe, erlangt freilich nicht geringe Rechenkraft. Dieser Sache wegen werde ich die Propositionen, aus denen schließlich nicht nur diese Wahrheit erschlossen wird, sondern auch andere hervorstehende Eigenschaften dieser Zahlen, die Summen zweier Quadrate sind, erkannt werden, mit ihren Beweisen hier der Reihe nach vorlegen und werde mir Mühe geben, dass nichts an der Strenge des Beweises vermisst werden kann. Wie die Dinge, die ich bisher über diese Zahlen voraus, trivial und allgemein bekannt sind, so werde ich sie als Lemma bei den folgenden Beweisen gebrauchen.

§8 Proposition 1
Wenn das Produkt pq die Summe zweier Quadrate und der eine Faktor p eine Primzahl und gleichermaßen eine Summe zweier Quadrate ist, wird auch der andere Faktor q die Summe zweier Quadrate sein.
Beweis
Es sei $pq = aa + bb$ und $p = cc + dd$; weil p eine Primzahl ist, werden c und d zueinander prime Zahlen sein. Es wird deshalb sein

$$q = \frac{aa + bb}{cc + dd} \tag{14}$$

und deshalb wird wegen der ganzen Zahl q der Zähler $aa + bb$ durch den Nenner $cc + dd$ teilbar sein. Daher wird durch $cc + dd$ auch diese Zahl teilbar

sein

$$cc(aa+bb) = aacc + bbcc \tag{15}$$

aber weil auch diese Zahl

$$aa(cc+dd) = aacc + aadd \tag{16}$$

durch $cc+dd$ teilbar ist, ist es von Nöten, dass die Differenz dieser Zahlen $aacc+bbcc-aacc-aadd$ oder $bbcc-aadd$ durch $cc+dd$ teilbar ist. Weil aber $cc+dd$ eine Primzahl ist und $bbcc-aadd$ die Faktoren $bc+ad$ und $bc-ad$ hat, wird der eine der beiden dieser Faktoren, natürlich $bc \pm ad$, durch $cc+dd$ teilbar sein. Es sei deshalb

$$bc \pm ad = mcc + mdd \tag{17}$$

Welche Zahlen auch immer a und b sind, die können so ausgedrückt werden, dass $b = mc + x$ und $a = \pm md + y$ ist, während x und y ganze, entweder positive oder negative Zahlen sind. Nachdem aber diese Werte für b und a eingesetzt worden sind, wird die Gleichung

$$bc \pm ad = mcc + mdd \tag{18}$$

diese Form annehmen

$$mcc + cx + mdd \pm dy = mcc + mdd \tag{19}$$

oder

$$cx \pm dy = 0 \tag{20}$$

Daher wird $\frac{x}{y} = \mp\frac{d}{c}$ sein, und weil d und c zueinander prime Zahlen sind, ist es von Nöten, dass $x = nd$ und $y = \mp nc$ ist, woher man haben wird

$$a = \pm md \mp nc \quad \text{und} \quad b = mc + nd \tag{21}$$

Werte von dieser Art werden natürlich die Zahlen a und b haben müssen, damit die Zahl $pq = aa + bb$ durch die Primzahl $p = cc + dd$ teilbar ist. Aber nach Einsetzen dieser Werte für a und b wird werden

$$pq = mmdd - 2mncd + nncc + mmcc + 2mncd + nndd \tag{22}$$

oder

$$pq = (mm + nn)(cc + dd) \tag{23}$$

und wird wegen $p = cc + dd$ sein

$$q = mm + nn \tag{24}$$

Und wenn daher das Produkt pq die Summe zweier Quadrate $aa + bb$ und der eine Faktor p eine Primzahl und gleichermaßen die Summe zweier Quadrate $cc + dd$ ist, folgt notwendigerweise, dass auch der andere Faktor q die Summe zweier Quadrate sein wird.
Q.E.D.

§9 Korollar 1
Wenn also die Summe zweier Quadrate durch eine Primzahl teilbar ist, die selbst die Summe zweier Quadrate sei, wird auch der aus der Division resultierende Quotient die Summe zweier Quadrate sein. Wenn so die Summe zweier Quadrate durch eine gewisse aus diesen Primzahlen $2, 5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97$ etc. teilbar war, wird der Quotient immer die Summe zweier Quadrate sein.

§10 Korollar 2
Wenn also die Buchstaben $\alpha, \beta, \gamma, \delta$ etc. Primzahlen dieser Art bezeichnen, die Summen zweier Quadrate sind, tritt daher klar zutage, wenn das Produkt αq die Summe zweier Quadrate ist, dass auch der Faktor q eine Summe zweier Quadrate sein wird.

§11 Korollar 3
Daher wird aber weiter leicht erschlossen, wenn das Produkt $\alpha\beta q$ die Summe zweier Quadrate war, dass auch der Faktor q die Summe zweier Quadrate sein wird. Weil nämlich $\alpha\beta q$ die Summe zweier Quadrate ist, wird durch das vorhergehende Korollar auch βq die Summe zweier Quadrate sein und desselben Grundes wegen wird auch q die Summe zweier Quadrate sein.

§12 Korollar 4
Auf die gleiche Weise ist es ersichtlich, wenn das Produkt $\alpha\beta\gamma\delta\epsilon q$ die Summe zweier Quadrate war, dass dann auch q die Summe zweier Quadrate ist; wenn daher pq das Produkt der Summe zweier Quadrate und sein Faktor p das Produkt aus wie vielen Primzahlen auch immer ist, deren einzelne die Summen zweier Quadrate seien, dass dann auch der andere Faktor q die Summe zweier Quadrate sein wird.

§13 Bemerkung
Die Regeln der Logik erlauben es nicht, dass diese Proposition so umgekehrt wird, dass, sooft der eine Faktor q die Summe zweier Quadrate ist, auch der andere Faktor p entweder als Summe zweier Quadrate, wenn er prim ist, oder als Produkt aus Primzahlen, welche einzelnen Summen von zwei Quadraten sind, versprochen werden kann. Über diese selbst ist nämlich noch nicht bekannt, ob das Produkt aus einigen Primzahlen, die selbst nicht die Summen zweier Quadrate sind, nicht die Summe zweier Quadrate sein kann, ja wir haben sogar im Gegenteil den Fall, in dem das Produkt $45 = 3 \cdot 3 \cdot 5$ die Summe zweier Quadrate ist, obwohl dennoch ihre Faktoren 3 und 3 nicht von dieser Gestalt sind. Aber die Proposition des letzten Korollars kann so umgekehrt werden, dass von der Negation der Folge richtig auf die Negation des Vorhergehenden geschlossen wird, welche Umkehrung von natürlich größter Bedeutung ich in dieser Proposition erfassen möchte.

§14 Proposition 2
Wenn das Produkt pq die Summe zweier Quadrate ist, sein Faktor q aber nicht die Summe zweier Quadrate ist, dann wird der andere Faktor p, wenn er eine Primzahl ist, nicht die Summe zweier Quadrate sein, wenn er aber nicht prim ist, zumindest gewiss einen primen Faktor haben wird, der nicht die Summe zweier Quadrate ist.
Beweis

Weil der andere Faktor p entweder eine prime oder zusammengesetzte Zahl ist, ist es passend, jeden der beiden Fälle einzeln zu betrachten. Es sei zuerst p eine Primzahl; weil also, wenn er die Summe zweier Quadrate wäre, wäre auch der andere Faktor q die Summe zweier Quadrate, weil dies der Annahme widerspricht, folgt, dass der Faktor p nicht die Summe zweier Quadrate ist. Es sei zweitens p eine zusammengesetzte Zahl und aus dem vorhergehenden ist es klar, wenn all ihre Primfaktoren die Summen zweier Quadrate wären, dass auch der andere Faktor q von derselben Gestalt wäre. Daher, weil nach der Annahme q nicht die Summe zweier Quadrate ist, folgt, dass nicht alle Faktoren von p die Summen zweier Quadrate sind.
Q.E.D.

§15 Korollar 1
Wenn also das Produkt pq die Summe zweier Quadrate ist, sein einer Faktor q dennoch nicht in zwei Quadrate auflösbar ist, wird der andere Faktor p entweder selbst die Summe zweier Quadrate sein oder zumindest einen nicht in zwei Quadrate auflösbaren Primfaktor haben. Wie wenn $pq = 45$ und $q = 3$ ist, wird $p = 15$ sein und hat den Faktor 3, der nicht die Summe zweier Quadrate ist.

§16 Korollar 2
Daher ist aber nicht einmal möglich zu folgern, dass der andere Faktor p überhaupt nicht die Summe zweier Quadrate ist; obwohl dies nämlich in diesem Fall gewiss ist, in dem p eine Primzahl ist, ist das dennoch nicht einmal in dem Fall bekannt, in welchem p eine zusammengesetzte Zahl ist, weil p einen nicht in zwei Quadrate auflösbaren Faktor haben könnte, auch wenn p selbst die Summe zweier Quadrate wäre.

§17 Korollar 3
Aber dies lässt sich erschließen: Wenn p die Summe zweier Quadrate war, dass sie dann nicht nur einen, sondern mindestens zwei nicht in zwei Quadrate auflösbare Primfaktoren hat. Es sei nämlich $p = \alpha\beta\gamma\delta$ und δ jener in zwei Quadrate auflösbare Faktor; es ist klar, wenn p die Summe zweier Quadrate war, dass nach Streichen des Faktors δ darüber hinaus der Restfaktor $\alpha\beta\gamma$ einen in nicht in zwei Quadrate auflösbaren Faktor haben muss.

§18 Bemerkung

Weil die Frage über die Teiler der Zahlen, die Summen zweier Quadrate sind, gestellt wird, sind über die Summe von Quadrate $aa + bb$ diese Fälle sorgsam zu trennen, ob diese Quadrate aa und bb oder deren Wurzeln a und b zueinander prime Zahlen sind oder nicht. Wenn nämlich a und b nicht zueinander prime Zahlen sind, sondern den gemeinsamen Teiler n haben, dass $a = nc$ und $b = nd$ ist, wird die Summe der Quadrate $nncc + nndd = nn(cc + dd)$ sein und deshalb den Divisor n haben, das heißt, irgendeine Zahl. Wenn aber die Wurzeln a und b zueinander prime Zahlen waren, dann wird die Summe der Quadrate a und b nicht mehrere Zahlen für die Teiler zulassen; es ist nämlich ersichtlich, dass eine Summe zweier Quadrate von dieser Art $aa + bb$ nie durch 3 teilbar ist. Weil nach der Annahme jeder der beiden Quadrate einzeln nicht durch drei teilbar ist, weil sie andernfalls nicht zueinander prim wären, wenn die Summe $aa + bb$ durch 3 teilbar wäre, wäre keine der beiden durch 3 teilbar. Die Wurzeln jeder der beiden wären also entweder von dieser Form $3m + 1$ oder von dieser $3m - 1$ sein; aber eine Summe von zwei Quadraten dieser Art lässt durch 3 geteilt immer den Rest 2 zurück und ist daher durch 3 niemals teilbar. Auf dieselbe Weise wird eingesehen, dass die Summe zweier zueinander primer Quadrate $aa + bb$ nie durch 7 oder 11 oder 19 etc. teilbar ist. Was für Zahlen diese aber im Allgemeinen sind, dass nie Teiler der Summe zweier zueinander primer Quadrate existieren können, wird auf diese Weise nicht leicht bestimmt. Es ist also passend, dass die auf andere Weise hinreichend bekannte Proposition bewiesen wird, dass die Summe zweier zueinander primer Quadrate keine anderen Primleiter zulässt, außer die selbst Summen zweier Quadrate sind. Es muss aber die folgende Proposition vorausgeschickt werden.

§19 Proposition 3

Wenn die Summe zweier zueinander primer Quadrate $aa + bb$ durch die Zahl p teilbar ist, wird immer eine durch dieselbe Zahl p teilbare Summe zweier anderer Quadrate $cc + dd$ dargeboten werden können, so dass diese Summe $cc + dd$ nicht größer ist als $\frac{1}{2}pp$ ist.

Beweis

Es sei die Summe zweier zueinander primer Quadrate $aa + bb$ durch die Zahl p teilbar und a und b beliebig große Zahlen. Weil also weder a noch b einzeln durch p teilbar ist, werden die Zahlen a und b so ausgedrückt werden können, dass $a = mp \pm c$ und $b = np \pm d$ ist, wo es möglich ist, die Zahlen m und n so

zu bestimmen, dass c und d die Hälfte von p nicht übersteigen. Es wird also sein

$$aa + bb = mmpp \pm 2mcp + cc + nnpp \pm 2ndp + dd \tag{25}$$

weil sowohl diese ganze Formel durch p teilbar ist (nach der Annahme) und ihr Teil $mmpp \pm 2mcp + nnpp \pm 2ndp$ per se den Teiler p hat, ist es von Nöten, dass der andere Teil $cc + dd$, der die Summe zweier Quadrate ist, ebenso durch p teilbar ist. Aber weil die Wurzeln c und d die Hälfte von p nicht übersteigen, wird auch die Summe der Quadrate $cc + dd$ das Quadrat $\frac{1}{4}pp$ zweimal genommen nicht übersteigen; und daher kann eine Summe von Quadraten $cc + dd$ nicht größer als $\frac{1}{2}pp$ dargebeten werden, die dennoch durch p teilbar ist.
Q.E.D.

§20 Korollar 1
Wenn also eine durch die Zahl p nicht teilbare Summe zweier zueinander primer Quadrate nicht gegeben ist, die $\frac{1}{2}pp$ nicht übersteige, sind überhaupt keine Summen zweier zueinander primer Quadrate gegeben, die durch diese Zahl p teilbar wären.

§21 Korollar 2
Weil so keine Summe zweier zueinander primer Quadrate unter $\frac{1}{2} \cdot 3^2$ oder $4\frac{1}{2}$ gegeben ist, die durch 3 teilbar ist, folgt daher in klarer Weise, dass überhaupt keine Summe zweier zueinander primer Quadrate durch 3 teilbar ist. Und auf die gleiche Weise folgt für die Zahl 7, weil keine durch 7 teilbare Summe zweier Quadrate unter $\frac{1}{2} \cdot 7^2 = 24\frac{1}{2}$ gegeben ist, dass nicht einmal in den größten Zahlen durch 7 teilbare Summen zweier einander primer Quadrate gegeben sind. Weil so keine Summe zweier zueinander primer Quadrate unter $\frac{1}{2} \cdot 3^2$ oder $4\frac{1}{2}$ gegeben ist, die durch 3 teilbar ist, folgt daher in klarer Weise, dass überhaupt keine Summe zweier zueinander primer Quadrate durch 3 teilbar ist. Und auf die gleiche Weise folgt für die Zahl 7, weil keine durch 7 teilbare Summe zweier Quadrate unter $\frac{1}{2} \cdot 7^2 = 24\frac{1}{2}$ gegeben ist, dass nicht einmal in den größten Zahlen durch 7 teilbare Summen zweier einander primer Quadrate gegeben sind.

§22 Proposition 4
Die Summe zweier einander primer Quadrate kann nicht durch eine Zahl geteilt werden, die selbst nicht die Summe zweier Quadrate ist.
Beweis
Um dies zu beweisen, wollen wir festlegen, dass die Summe zweier zueinander primer Quadrate $aa + bb$ durch die Zahl p teilbar ist, die nicht Summe zweier Quadrate sei. Es könnte also eine andere Summe zweier einander primer Quadrate $cc + dd$ nicht größer als $\frac{1}{2}pp$ dargeboten werden, die durch p teilbar wäre. Es sei also $cc + dd = pq$, und weil p nicht Summe zweier Quadrate ist, wird entweder die Zahl q selbst nicht eine Summe solcher Art sein oder wird zumindest einen Faktor r haben, der nicht Summe zweier Quadrate sein wird. Weil also $pq < \frac{1}{2}pp$ ist, wird $q < \frac{1}{2}p$ und um vieles mehr $r < \frac{1}{2}p$sein. Daher, weil $cc + dd$ auch durch $r < \frac{1}{2}p$ teilbar ist, könnte durch die vorhergehende Proposition eine durch dieselbe Zahl r teilbare Summe zweier Quadrate $ee + ff$ dargeboten werden, die $\frac{1}{2}rr$ und um vieles mehr $\frac{1}{2}pp$ nicht überschreiten würde. Und weil r nicht die Summe zweier Quadrate ist, würde, indem auf die gleiche Weise fortgeschritten wird, ununterbrochen zu kleineren Summen zweier Quadrate gelangt werden, die dieselbe Zahl, nicht Summe zweier Quadrate, teilbar wäre. Deshalb, weil in kleinsten Zahlen keine Summe zweier einander primer gegeben ist, die durch eine Zahl teilbar wäre, die keine Summe zweier Quadrate sind, wird es nicht einmal größte Zahlen Summen zweier Quadrate solcher Art geben, die durch Zahlen teilbar sind, die selbst nicht die Summe zweier Quadrate wären.

§23 Korollar 1
Wenn also die Summe zweier einander primer Quadrate keine Primzahl war, werden alle ihre Primfaktoren auch Summen zweier Quadrate sein. Wie also das Produkt aus wie vielen Zahlen auch immer, die selbst Summen zweier Quadrate sind, gleichermaßen die Summe zweier Quadrate ist, so ist nun die Umkehrung dieser Proposition bewiesen worden, dass die Summe zweier (zueinander primer Quadrate) durch Multiplikation nicht entspringen kann, außer aus Zahlen, die selbst Summe zweier Quadrate sind.

§24 Korollar 2
Also sind alle Zahlen, die Summe zweier einander primer Quadrate sind, entweder selbst in dieser Reihe von Primzahlen enthalten
$2, 5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, 101, 109, 113, etc.$ oder aus zwei oder meh-

reren Zahlen dieser Reihe durch Multiplikation zusammengesetzt. Aber alle diese Primzahlen außer 2 überschreiten ein Vielfaches von vier um die Einheit oder sind in dieser Form $4n + 1$ enthalten.

§25 Korollar 3
Wenn also die Summe zweier Quadrate $aa + bb$ durch eine Zahl teilbar ist, die nicht die Summe zweier Quadrate war, wird daher eingesehen werden, dass jene Quadrate aa und bb einander nicht prim sind und daher auch nicht deren Wurzeln a und b.

§26 Korollar 4
Weil aber, wenn $a = nc$ und $b = nd$ ist, die Summe zweier Quadrate $aa + bb = nn(cc + dd)$ durch jede Zahl n, die keine Summe zweier Quadrate ist, geteilt werden kann, weil sie ja nicht nur durch n, sondern auch durch nn teilbar ist, ist es ersichtlich, wenn die Summe zweier Quadrate durch eine gewisse Zahl teilbar ist, die keine Summe zweier Quadrate ist, dass sie dann auch durch das Quadrat dieser Zahl teilbar sein wird. weil so $45 = 36 + 9$ durch 3 teilbar ist, ist sie zugleich auch durch 9 teilbar ist.

§27 Korollar 5
Weil keine der in dieser Form $4n - 1$ enthaltenen Zahlen die Summe zweier Quadrate ist, ist es auch offenbar, dass keine Summe zweier einander primer Quadrate durch eine in dieser Form $4n - 1$ enthaltenen Primzahlen geteilt werden kann, welche Primzahlen sind

$$3, 7, 11, 19, 23, 31, 43, 47, 59, 67, 71, 79, 83, 103, 107, etc \tag{26}$$

§28 Bemerkung
Weil alle Primzahlen, die Summe zweier Quadrate sind, nachdem die zwei ausgenommen worden ist, diese Reihe bestimmen

$$5, 13, 17, 29, 37, 41, 53, 61, 63, 73, 89, 97, 101, 109, 113, 137, 149, etc \tag{27}$$

die nicht mehr in dieser Form $4n + 1$ enthalten sind, sondern auch, wie weit auch immer sie fortgesetzt wird, wir werden auch entdecken, dass in ihr ganz und gar alle Primzahlen dieser Form $4n + 1$ gegeben sind, die nicht zugleich

die Summe zweier Quadrate sind. Weil dennoch indess eine beliebig weite Induktion nicht den Platz eines Beweises annehmen kann, lässt sich diese Wahrheit, dass jede Primzahl der Form $4n + 1$ die Summe zweier Quadrate ist, auch wenn niemand zweifelt sie anzuerkennen, dennoch noch nicht zu den bewiesenen Wahrheiten der Mathematik zählen. Fermat hat sich freilich öffentlich bekannt, dass er einen Beweis ihrer gefunden hat, obwohl er ihn aber nie veröffentlich hat, schenken wir dem Versicherten dieses tiefgründigsten Herren freilich mit recht Vertrauen und glauben diese Eigenschaft der Zahlen; und diese unsere Erkenntnis ist lediglich auf Vertrauen ohne Wissen gestützt. Obwohl ich mich aber im Finden dieses Beweises viel vergeblich bemüht habe, habe ich dennoch ein anderes Argument für das Hinzufügen dieser Wahrheit gefunden, welches, auch wenn es nicht vollkommen streng ist, dennoch mit der Induktion zusammen einem beinahe strengen Beweis gleichwertig scheint.

§28[a] Proposition 5
Jede Primzahl, die ein Vielfaches von vier um die Einheit übersteigt, ist die Summe zweier Quadrate.
Versuch eines Beweises
Die Primzahlen, über die hier die Rede ist, sind in dieser Form $4n + 1$ enthalten. Wenn daher also $4n + 1$ eine Primzahl war, habe ich bewiesen, dass durch sie diese Form $a^{4n} - b^{4n}$ immer teilbar ist, welche Zahlen auch immer für a und b eingesetzt werden, solange keine von diesen einzeln durch $4n + 1$ teilbar war. Weil aber $a^{4n} - b^{4n} = (a^{2n} - b^{2n})(a^{2n} + b^{2n})$ ist, ist es notwendig, dass der eine der beiden Faktoren, natürlich entweder $a^{2n} - b^{2n}$ oder $a^{2n} + b^{2n}$, durch die Primzahl $4n + 1$ teilbar ist. Je nachdem wie aber für a und b die einen Zahlen und die anderen Zahlen dort angenommen werden, wird in den einen Fällen die Formel $a^{2n} - b^{2n}$, in den anderen hingegen die Formel $a^{2n} + b^{2n}$ durch $4n + 1$ teilbar sein, woher sich annehmen lässt, auch wenn ich dies freilich noch nicht durch einen strengen Beweis dartun kann, dass immer Zahlen solcher Art für a und b angenommen werden können, dass die Formel $a^{2n} - b^{2n}$ nicht durch $4n + 1$ teilbar ist; in diesen Fällen wird also die andere Formel $a^{2n} + b^{2n}$ notwendigerweise durch $4n + 1$ teilbar sein. Es sei $a^n = p$ und $b^n = q$ und man wird eine durch $4n + 1$ teilbare Summe zweier Quadrate $pp + qq$ haben, so dass keine der beiden Quadrate pp oder qq einzeln den Teiler $4n + 1$ hat. Und daher, auch wenn zufällig pp und qq einen gemeinsamen Teiler mm haben, dass $pp + qq = mm(rr + ss)$ ist, weil der gemeinsame Faktor mm nicht den Teiler $4n + 1$ hat, ist es von Nöten, dass

die Summe der zwei einander primen Quadrate $rr + ss$ den Teiler $4n + 1$ hat. Als logische Konsequenz, weil eine Summe zweier Quadrate dieser Art keine anderen Werte zulässt, außer die selbst Summen zweier Quadrate sind, ist es von Nöten, dass die Primzahl $4n + 1$ die Summe zweier Quadrate ist.

§29 Korollar 1
Dieser Beweis wäre also vollkommen, wenn nur bewiesen werden könnte, da es immer für a und b einzusetzende Werte solcher Art existieren, mit welchen die Formel $a^{2n} - b^{2n}$ nicht durch die Primzahl $4n + 1$ teilbar wird, in denselben Fällen wird nämlich die Formel $a^{2n} + b^{2n}$ notwendigerweise durch $4n + 1$ teilbar.

§30 Korollar 2
Wenn aber daher jemand diese Sache durch Rechnung ausprobiert, wird er nicht nur immer mehrere Fälle, ja sogar unendlich viele, der Formel $a^{2n} - b^{2n}$ auffinden, in denen sie nicht durch die Primzahl $4n + 1$ teilbar ist, sonden es ist auch möglich für b die Einheit festzulegen, so dass auch diese einfachere Formel $a^{2n} - 1$ oftmals nicht durch $4n + 1$ teilbar ist.

§31 Bemerkung
Die Fälle oder die Werte von a, in denen die Formel $a^{2n} - 1$ gewiss durch die Primzahl $4n + 1$ teilbar wird, können leicht angegeben werden. Wenn nämlich zuerst $a = pp$ ist, ist die Formel $a^{2n} - 1 = p^{4n} - 1$ immer durch $4n + 1$ teilbar, solange p nicht $= 4n + 1$ oder ein Vielfaches davon ist. Wenn darauf $a = pp \pm (4n + 1)q$ ist, hat die Formel $a^{2n} - 1$ auch den Teiler $4n + 1$; es wird nämlich

$$a^{2n} = (pp \pm (4n + 1)q)^{2n} \tag{28}$$

in einer Reihe von Termen aufgelöst, deren erster p^{4n} ist, die folgenden hingegen alle von selbst durch $4n + 1$ teilbar sein. Daher tritt es klar zutage, dass die geeigneten Werte für a alle Reste sind, die zurückbleiben, wenn die Quadratzahlen p^2 durch $4n + 1$ geteilt werden. Aber diese Reste, ob für $a \cdot r$ oder $4n + 1 + r$ oder $(4n + 1)q + r$ festgelegt wird, gehen als dieselben hervor, woher alle möglichen Reste erhalten werden, wenn für p nacheinander die Zahlen $1, 2, 3, 4, ...$ bis hin zu $4n$ eingesetzt werden; aber der Wert $4n$ gibt für p festgelegt denselben Rest wie der Wert 1, und auf die gleiche Weise geben

die Werte 2 und $4n-1$ ebenso wie 3 und $4n-1$, genauso 4 und $4n-1$ etc. denselben Rest. Weil daher immer je zwei Reste, die aus den für die Wurzeln der Quadrate gekommenen Zahlen $1, 2, 3...$ bis hin zu $4n$ hervorgehen, gleich sind, wird die Anzahl verschiedener resultierender Reste nur $2n$ sein und daher werden genauso viele kleinere Zahlen als $4n+1$ selbst gegeben sein, die keine aus der Teilung von Quadratzahlen durch $4n+1$ ans Licht tretende Reste sein können; und diese Zahlen werden für a eingesetzt die Formel $a^{2n}-1$ immer nicht durch $4n+1$ teilbar machen. Dieser kann freilich folgendermaßen nicht bewiesen werden; aber denn, weil beim Unternehmen des Versuches, wie viele Zahlen auch immer auf diese Weise erforscht werden, nicht einmal ein einziger Fall auftauchen wird, in dem diese Regel falsch ist, muss ihre Gültigkeit anerkannt werden.
Damit diese Dinge deutlicher erkannt werden, möchte ich einige Beispiele anfügen. Es sei zuerst $4n+1=5$ und die Fälle, in denen die Formel a^2-1 durch 5 teilbar sein wird, wird man haben, wenn für a aus der Division durch 5 herstammende Reste festgelegt werden, welche Reste $1, 4$ sind. Aber wenn für a entweder 2 oder 3 festgelegt wird, wird die Formel a^2-1 nicht durch 5 teilbar sein; in diesen Fällen wird also die Formel a^2+1 den Teiler 5 haben. Wenn darauf $4n+1=13$ oder $n=3$ ist, sind die Reste, die aus der Division der Quadratzahlen durch 13 zurückbleiben, $1, 4, 9, 3, 12, 10$; daher, wenn eine der übrigen Zahlen $2, 5, 6, 7, 8, 11$ für a eingesetzt wird, wird nicht die Formel a^6-1, sondern a^6+1 teilbar sein. Wenn weiter $4n+1=17$ oder $n=4$ ist, weil die Reste der durch 17 geteilten Quadrate $1, 4, 9, 16, 8, 2, 15, 13$ sind, wenn für a eine bestimmte aus den übrigen Zahlen $3, 5, 6, 7, 10, 11, 12, 14$ festgesetzt wird, wird nicht diese Formel a^8-1, sondern diese a^8+1 durch 17 teilbar sein. Weil also dieses Gesetz immer beobachtet wird, wird diese Induktion anzusehen, fast die Mächtigkeit eines Beweises anzunehmen; und daher scheint diese Proposition dermaßen bestätigt, dass sich ihre Gültigkeit nicht weiter in Zweifel ziehen lässt. Dennoch wäre es indess umso größerer Mühe wert, wenn jemand einen strengen Beweis dieser Proposition darbieten könnte damit wir über deren Gültigkeit noch mehr gewiss sind; es besteht nämlich kein Zweifel, dass ein lange vergeblich gesuchter Beweis zu sehr vielen anderen hervorstechenden Eigenschaften von Zahlen führen wird. Obwohl aber die Gültigkeit dieser Proposition außer Zweifel gestellt worden ist, werde ich dennoch die Folgerungen, die auf selbige gestützt sind, sorgfältig anmerken und von denen, die mit strengen Beweisen untermauert sind, trennen; aber aus dieser noch nicht bewiesenen Proposition folgen diese Korollare, welche ich mit diesem Namen auch bezeichnen will.

§32 Korollar 3
Wenn also eine Zahl der Form $4n+1$ auf keine Weise in zwei Quadrate aufgelöst werden kann, wird dies ein sicheres Zeichen sein, dass die Zahl nicht prim ist, wenn nämlich diese Zahl $4n+1$ prim wäre, könnte sie gewiss in zwei Quadrate aufgelöst werden. Weil so die Zahlen $21, 33, 57, 69, 77, 93$ etc., die in der Form $4n+1$ enthalten sind, nicht die Summen zweier Quadrate sind, tritt aus diesem selbst klar zutage, dass sie keine Primzahlen sind.

§33 Korollar 4
Also sind in dieser Reihe, die die Summe zweier Quadrate ist, zuerst alle Primzahlen dieser Form $4n+1$ enthalten, des Weiteren alle Produkte aus zwei oder mehreren Primzahlen dieser Art, dann die Produkte aus diesen Zahlen mit zwei und jeglichen Quadratzahlen.

§34 Korollar 5
Alle Zahlen n, aus denen die Formel $4n+1$ eine Primzahl wird, sind die Summen zweier Trigonalzahlen. Weil nämlich $4n+1$ die Summe zweier Quadrate ist, wird ihr Doppeltes $8n+2$ die Summe zweier ungerader Quadrate sein [§4]. Es sei also

$$8n+2 = (2x+1)^2 + (2y+1)^2 \tag{29}$$

es wird werden

$$n = \frac{xx+x}{2} + \frac{yy+y}{2} \tag{30}$$

Daher, wenn n keine Summe zweier Dreieckszahlen ist, wird gewiss die Zahl $4n+1$ keine Primzahl sein.

§35 Proposition 6
Wenn eine Zahl der Form $4n+1$ auf eine einzige Weise in zwei einander prime Quadrate aufgelöst werden kann, dann ist sie gewiss eine Primzahl.
Beweis
Weil ja nämlich diese Zahl die Summe zweier zueinander primer Quadrate ist, wenn sie nicht prim ist, werden ihre einzelnen Faktoren die Summen zweier Quadrate sein [§22]. Daher, wenn diese Zahl nicht prim wäre, könnte

sie zumindest in zwei Faktoren dieser Art aufgelöst werden, dass $4n + 1 = (aa + bb)(cc + dd)$ wäre; in diesem Fall haben aber zwei Auflösungen in zwei Quadrate Geltung [§5], natürlich

I. $4n + 1 = (ac + bd)^2 + (ad - bc)^2$

II. $4n + 1 = (ad + bc)^2 + (ac - bd)^2$

Und diese Auflösungen sind einander immer verschieden, wenn nicht entweder $ac + bd = ad + bc$ oder $ac + bd = ac - bd$ ist. Im ersten Fall wäre aber $ac + bd - ad - bc = 0$ oder $(a - b)(c - d) = 0$ und daher entweder $a = b$ oder $c = d$, und daher entweder $aa + bb$ oder $cc + dd$ eine gerade Zahl, von denen natürlich keiner von beiden Teilern eine ungerade Zahl sein kann. Im zweiten Fall wäre hingegen entweder $b = 0$ oder $d = 0$ und daher $4n + 1$ entweder $= aa(cc + dd)$ oder $= cc(aa + bb)$; daher wären diese zwei Quadrate entgegen der Annahme einander nicht prim. Nachdem diese Fälle angemerkt worden sind, folgt, dass dieselbe zusammengesetzte Zahl $4n + 1$, wenn sie in zwei zueinander prime Quadrate auflösbar war, mindestens auf zwei Arten in zwei Quadrate auflösbar ist. Deshalb, wenn die Zahl $4n + 1$ nur auf eine einzige Weise die Summe zweier Quadrate ist, wird sie gewiss nicht zusammengesetzt sein und als Konsequenz prim sein.
Q.E.D.

§36 Korollar 1

Wenn also, nachdem eine gewisse Zahl der Form $4n + 1$ vorgelegt worden ist, nach unternommener Untersuchung in Erfahrung gebracht wird, dass sie auf eine einzige Weise in zwei einander prime Quadrate aufgelöst werden kann, werden wir daher sicher erschließen, dass sie eine Primzahl ist, auch wenn wir ihre Teilbarkeit durch Primzahlen auf die übliche Weise nicht ausprobiert haben. Weil so die Zahl 73 auf eine einzige Weise Summe zweier Quadrate ist, nämlich $64 + 9$, wissen wir sicher, dass sie prim ist.

§37 Korollar 2

Wenn man also eine bequeme Methode hätte, mit deren Hilfe es einfach möglich wäre zu untersuchen, ob und auf wie viele Arten eine vorgelegte in der Form $4n + 1$ enthaltene Zahl in zwei Quadrate aufgelöst werden kann, werden wir daher leicht beurteilen können, ob sie prim ist; wenn sie nämlich auf eine einzige Weise in zwei Quadrate auflösbar ist und die Quadrate einander prim sind, wird sie gewiss für prim zu halten sein.

§38 Korollar 3
Es ist aber offenbar, wenn die zwei Quadrate in welche eine gewisse Zahl aufgelöst wird, einander nicht prim waren, dass sie keine Primzahl sein wird. Wenn nämlich die vorgelegte Zahl gefunden wird $= nnaa + nnbb$ zu sein, dann wird sie die Teiler n und nn haben; dieses selbe ist zu verstehen, wenn die vorgelegte Zahl selbst ein Quadrat oder $= aa + 0$ ist; dann wird sie den Teiler a haben.

§39 Bemerkung
Diese Regel Primzahlen zu erforschen ist nur auf ungerade Zahlen der Form $4n + 1$ beschränkt; denn gerade Zahlen können auch manchmal auf eine einzige Weise in zwei Quadrate aufgelöst werden, obwohl sie dennoch nicht prim sind; so ist 10 auf eine einzige Weise Summe zweier Quadrate, auch wenn sie nicht prim ist, die Begründung welcher Sache die ist, dass im Produkt $(aa + bb)(cc + dd)$, welchem Zahlen dieser Art gleich werden, entweder $a = b$ oder $c = d$ ist, in welchem Fall die zwei Auflösungen, die allgemein angedeutet zu werden scheint, auf eine einzige zurückgehen, wie im Beweis bemerkt worden ist. Und in der Tat wird mit dieser Ausnahme die gegebene Regel nicht gebrochen, weil die Beurteilung gerader Zahlen per se einfach ist. Aber die ungeraden Zahlen der anderen Form $4n + 1$ werden daher von selbst ausgeschlossen, weil sie ja überhaupt nicht in zwei Quadrate auflösbar sind. Über das Übrige, wenn die Zahl $4n + 1$ entweder überhaupt nicht in zwei Quadrate auflösbar ist oder auf mehrere Weisen diese Auflösung gelingt, haben wir für den ersten Fall schon angemerkt, dass die Zahl gewiss nicht prim ist, auch wenn dies auf die nicht hinreichend streng bewiesene vorhergehende Proposition gestützt ist. Für den zweiten Fall wird hingegen in der folgenden Proposition ein Beurteilungskriterium angeführt werden.

§40 Proposition 7
Weil die Zahl auf zwei oder mehrere verschiedene Arten in zwei Quadrate aufgelöst werden kann, ist sie nicht prim, sondern mindestens aus zwei Faktoren zusammengesetzt.
Beweis
Es sei die vorgelegte Zahl N, die auf zwei Weisen in Quadrate auflösbar sei, natürlich

$$N = aa + bb = cc + dd \tag{31}$$

Weil ja diese Quadrate nicht gleich sind, andernfalls wäre nämlich die Zahl N per se nicht prim, sei $a > b$ und $c > d$, und weil diese zwei Auflösungen verschieden sind, wird weder $a = c$ noch $b = d$ sein. Es sei also $a > c$; es wird $b < d$ sein; daher werde $a = c + x$ und $d = b + y$ festgelegt. Daher wird wegen $aa + bb = cc + dd \quad 2cx + xx = 2by + yy$ werden. Es sei jede der beiden Formen $= xyz$, weil die eine durch x, die andere durch y teilbar ist; es wird werden

$$a = \frac{yz - x}{2}, b = \frac{xz - y}{2}, c = \frac{yz + e}{2}, d = \frac{xz + y}{2} \tag{32}$$

und daher wird sein

$$N = aa + bb = \frac{xxzz + yy + yyzz + xx}{4} \quad oder \quad N = \frac{(yy + xx)(1 + zz)}{4} \tag{33}$$

Wenn also $xx + yy$ nicht durch vier teilbar ist, wird $xx + yy$ ein Teiler von N sein, wenn aber $xx + yy$ durch 4 oder irgendeine zusammengesetzte Zahl teilbar ist, wird ein gewisser Faktor von ihr gewiss ein Teiler von N sein. Weil also $x = a - c$ und $y = d - b$ ist, wird die vorgelegte Zahl $N = aa + bb = cc + dd$ als Teiler entweder die Zahl $(a - c)^2 + (d - b)^2$ selbst oder ihre Hälfte oder ihr Viertel haben, und weil sich die Zahlen a, b und c, d miteinander auf irgendeine Weise vertauschen lassen, werden auch $(a - d)^2 + (c - b)^2$ Faktoren von N sein oder auch, weil sich die Wurzeln a, b, c, d negativ annehmen lassen, $(a \pm c)^2 + (d \pm b)^2$ oder $(a \pm d)^2 + (c \pm b)^2$ oder die Hälften oder andere aliquote Teile dieser Formeln. Daher, weil sogar die Faktoren der mehr auf eine einzige Weise in zwei Quadrate auflösbaren Zahl angegeben werden können, wird jene Zahl gewiss nicht prim sein, sondern zusammengesetzt
Q.E.D

§41 Korollar 1
Weil also die Zahl $N = aa + bb = cc + dd$ zusammengesetzt ist, wird sie von dieser Art sein $N = (pp + qq)(rr + ss)$. Daher resultieren aber umgekehrt zwei Auflösungen in zwei Quadrate; es wird natürlich sein

$$a = pr + qs, b = ps - qr \tag{34}$$

und

$$c = ps + qr, d = pr - qs \tag{35}$$

Und daher wird weiter $a - d = 2qs$ und $c - b = 2qr$ erhalten, woher $\frac{r}{s} = \frac{c-b}{a-d}$ wird. Daher, wenn der Bruch $\frac{c-b}{a-d}$ auf kleinste Terme zurückgeführt wird, dass $\frac{c-b}{a-d} = \frac{r}{s}$ ist, wird aus diesem Bruch $\frac{r}{s}$ ein Teiler $= rr + ss$ der Zahl N entspringen, wenn er nicht gerade ist; denn wenn er gerade war, muss seine Hälfte genommen werden.

§42 Korollar 2
Auf die gleiche Weise, weil es möglich ist, die Zahlen a, b und c, d miteinander zu vertauschen und sogar negativ festlegen lassen, wenn der eine dieser Brüche $\frac{a \pm c}{b \pm d}$ oder $\frac{a \pm d}{b \pm c}$ auf kleinste Terme zurückgeführt wird, dass $= \frac{r}{s}$ ist, wird $rr + ss$ immer ein Teiler der vorgelegten Zahl N sein.

§43 Korollar 3
Obwohl aber daher mehr als zwei Teiler zu entstehen scheinen, führen dennoch die verschiedenen Formeln so auf denselben Teiler, dass nicht mehr als zwei gefunden werden, wenn freilich die vorgelegte Zahl nur auf zwei Weisen in zwei Quadrate auflösbar war. Wenn so $N = 85 = 9^2 + 2^2 = 7^2 + 6^2$ ist, verschaffen die Formel $\frac{9 \pm 7}{6 \pm 2}$, $\frac{9 \pm 6}{7 \pm 2}$ diese vier Brüche in kleinsten Termen, natürlich $\frac{2}{1}, \frac{4}{1}, \frac{5}{3}, \frac{3}{1}$, von denen die zwei letzten für die Formel $rr + ss$ nur den doppelten Wert von dem darbieten, der aus der ersten entspringt; daher wird es klar zutage treten, dass die zwei Faktoren $2^2 + 1 = 5$ und $4^2 + 1 = 17$ sind. Auf die kürzeste Weise werden also diese Faktoren gefunden, wenn nur die geraden und ungeraden Wurzeln der Quadrate einzeln miteinander kombiniert werden und die Kombination der geraden mit den ungeraden völlig weggelassen wird, weil daher Brüche entspringen werden, die einen ungeraden Zähler und Nenner haben.

§44 Problem
Nachdem irgendeine Zahl der Form $4n + 1$ vorgelegt worden ist, zu untersuchen, ob sie prim ist oder nicht.
Lösung

Durch die darauf folgend zu erklärende Operation werde die vorgelegte Zahl untersucht, ob sie in zwei Quadrate aufgelöst werden kann oder nicht, und wenn sie kann, ob sie auf mehr als auf eine Weise eine Auflösung zulässt. Wenn sie nämlich eine Auflösung in zwei Quadrate überhaupt nicht zulässt, wird es durch §32 ein sicheres Zeichen sein, dass die vorgelegte Zahl nicht prim ist, auch wenn dieser Schluss aus der nicht hinreichend bewiesenen Proposition 5 folgt. In diesem Fall ist freilich über ihre Teiler nichts bekannt; denn erschließen wir indess sicher, dass sie Primteiler von der Form $4m - 1$ hat, weil, wenn alle ihre Teiler von der Form $4m + 1$ wären, sie gewiss in zwei Quadrate auflösbar wäre. Aber wenn die vorgelegte Zahl auf eine einzige Weise in zwei Quadrate auflösbar ist, dann wird sie unfehlbar für eine prime zu halten sein. Wenn aber die Auflösung auf mehr als eine einzige Weise gelingt, dann wird nicht feststehen, dass sie nicht prim ist, sondern es werden auch durch §43 ihre Teiler angegeben werden können. Nachdem diese Dinge gründlich untersucht worden sind, möchte ich eine Regel angeben, mit deren Hilfe die Auflösbarkeit in zwei Quadrate nicht schwer erkundet werden können wird. Die vorgelegte Zahl endigt entweder auf 1 oder auf 3 oder auf 7 oder auf 9; der Fall, in dem sie auf 5 endigt, lasse ich hier weg, weil b der Teiler 5 dann offenbar ist und anzeigt, dass die Zahl nicht prim ist. Darauf werden Quadratzahlen, indem von der größten kleiner als die vorgelegte Zahl selbst aus begonnen wird, nacheinander von ihr subtrahiert, damit klar zutage tritt, ob irgendwann eine Quadratzahl zurückbleibt; sooft dies nämlich passiert, sooft gelingt die Auflösung in zwei Quadrate. Aber weil die Quadratzahlen auf keiner dieser Zahlen $2, 3, 7, 8$ endigen können, wird die Subtraktion derer Quadrate, die auf diesen Zahlen endigende Reste geben, weggelassen werden können. Daher ist es nur von Nöten, dass von der vorgelegten Zahl die Quadrate subtrahiert werden, die auf $0, 1, 4, 5, 6, 9$ endigende Reste liefern; natürlich

Wenn die vorgelegte Zahl endigt auf	endigen die zu subtrahierenden Quadrate auf	und die Wurzeln dieser Quadrate endigen auf
1	0,1,5,6	0,1,4,5,6,9
3	4,9	2,3,7,8
7	1,6	1,4,6,9
9	0,4,5,9	0,2,3,5,7,8

Für jede beliebige Zahl $4n + 1 = N$ werden also so viele Operationen ein-

zeln ausgeführt, wie es geeignete Endungen der Wurzeln gibt. Es sei also pp das größte Quadrat von dieser Gestalt, welches von der vorgelegten Zahl N subtrahiert werden muss, und dann werden nacheinander die Quadrate $(p-10)^2, (p-20)^2, (p-30)^2, (p-40)^2$ etc. subtrahiert. Aber die daher ans Licht tretenden Reste werden bequem durch wiederholte Addition auf diese Weise gefunden werden können:

Die vorgelegte Zahl	N
von welcher subtrahiert werden	pp
	N-pp
Es werde addiert	20p-100
	$N-(p-10)^2$
Es werde addiert	20p-300
	$N-(p-20)^2$
Es werde addiert	20p-500
	$N-(p-30)^2$

Die nacheinander zu addierenden Zahlen sind also $20p-100, 20p-300, 20p-500, 20p-700, etc.$ die in einer arithmetischen Progression nach der Differenz $=200$ wachsen. Eine Operation von dieser Art werde also für die einzelnen Zahlen p, deren Quadrate nur ein wenig kleiner als die vorgelegte Zahl sind und die auf einer der oben angegebenen Stellen endigen, durchgeführt und nicht weiter fortgesetzt, als bis zur Hälfte der vorgelegten Zahl N gelangt wird. Wenn nämlich die Zahl N die Summe zweier Quadrate war, ist es nämlich gewiss von Nöten, dass der eine Summand kleiner als die Hälfte selbiger ist. Nachdem dies bemerkt worden ist, wird auf so viele, wie mit dieser Operation Quadrate hervorgehen werden, Weisen die vorgelegte Zahl in zwei Quadrate auflösbar sein.
Dass aber diese Operation nicht völlig unangenehm ist und allen anderen Methoden, Primzahlen zu erforschen, weit vorzuziehen ist, werden die folgenden Beispiele aufzeigen.

§45 Beispiel 1
zu untersuchen, ob diese Zahl 82421 prim ist oder nicht.
Die Operation wird durch die folgenden sechs Spalten hindurch durchgeführt werden

p 82421	p 82421	p 82421	p 82421	p 82421	p 82421
286 81796	285 81225	284 80656	281 78961	280 78400	279 77841
625	1196	1765	3460	4021	4580
5620	5600	5580	5520	5500	5480
6245	6796	7345	8980	9521	10060
5420	5400	5380	5320	5300	5280
11665	12196	12725	14300	14821	15340
5220	5200	5180	5120	5100	5080
16885	17396	17905	19420	19921	20420
5020	5000	4980	4920	4900	4880
21905	22396	22885	24340	24821	25300
4820	4800	4780	4720	4700	4680
26725	27196	27665	29060	29521	29980
4620	4600	4580	4520	4500	4480
31345	31796	32245	33580	34021	34460
4420	4400	4380	4320	4300	4280
35765	36196	36625	37900	38321	38740
4220	4200	4180	4120	4100	4080
39985	40396	40805	42020	42421	42820

Weil also hier das eine einzige Quadrat 625 auftaucht und daher die vorgelegte Zahl 82421 auf eine einzige Art in zwei Quadrate auflösbar ist, sie ist natürlich $= 25^2 + 286^2$, wird sie prim sein.

§46 Bemerkung

In dieser Richtung können die vier Spalten, wo die Rest der Zahl entweder auf 5 oder auf 0 endigen, merklich zusammengezogen werden, indem all die weggelassen werden, die nicht entweder auf 25 oder auf 100 endigen, zuerst das nächste Quadrat subtrahiert, welches einen entweder auf 25 oder auf 00 endigen Rest liefert, und dieses Quadrat werde pp genannt, dass der Rest $= N - pp$ ist; dann werden die Quadrate, woher die auf die gleiche Weise

endigenden Reste entspringen, $(p-50)^2, (p-100)^2, (p-150)^2$ etc. sein und daher werden diese Reste erhalten werden, wenn zu $N - pp$ ununterbrochen diese Zahlen addiert werden $100p - 2500, 100p - 7500, 100p - 12500$, welche arithmetisch gemäß der konstanten Differenz schrumpfen; daher werden diese Spalten bald zum Ende geführt werden, während es nicht von Nöten ist, dass sie über die Hälfte der vorgelegten Zahl hinaus fortgesetzt werden. Dieser Vorteil wird also bei entweder auf 1 oder auf 9 endigenden Zahlen zugute kommen, die deshalb, auch wenn sie sechs Spalten verlangen, während für die übrigen vier genügen, leichter erledigt werden.

§47 Beispiel 2

Zu untersuchen, ob diese Zahl 100981 prim ist oder nicht

p 100981	p 100981	p 100981	p 100981
316 99856	315 99225	309 95481	310 96100
1125	1756	5500	4881
29100	6200	28400	6100
30225	7956	33900	10981
24100	6000	23400	5900
54325	13956	57300	16881
	5800		5700
p 100981	19756	p 100981	22581
284 80656	5600	291 84681	5500
20325	25356	16300	28081
25900	5400	26600	5300
$215^2 = 46625$	30756	42900	33381
	5200	21600	5100
	35956	64500	38481
	5000		4900
	40956		43381
	4800		4700
	45756		48081
	4600		
	50356		

Weil also ein einziges Quadrat $46225 = 215^2$ auftaucht, woher $100981 = 215^2 + 234^2$ wird, wird diese Zahl prim sein.

48 Beispiel 3

Zu untersuchen, ob die Zahl 1000009 prim ist oder nicht.

p 1000009 1000 1000000	continuation of column 1	p 1000009 978 956484	p 1000009 994009	p 1000009 995 990025	continuation of column 5
3^2=9	277509	43525	6000	9984	285984
19900	1900	95300	97200	19800	16800
19909	294409	138825	103200	29784	302784
19700	16700	90300	92200	19600	16600
39609	311109	229125	195400	49384	319384
19500	16500	85300	87200	19400	16400
59109	327609	31425	282600	68784	835784
18300	16300	80300	82200	19200	16200
78409	343909	394725	364800	87984	351984
19100	16100	75300	77200	19000	16000
97509	360009	470025	442000	106984	367984
18900	15900			18800	15800
116409	375909	p 1000009	9 1000009	125784	383784
18700	15700	972 944784	953 908209	18600	15600
135109	391609	635^2=55225	91800	144384	399384
18500	15500	94700	92800	18400	15400
153609	407109	149925	184600	162784	414784
18300	15300	89700	87800	18200	15200
171909	422409	239625	272400	180984	429984
18100	15100	84700	82800	18000	15000
190009	437509	324325	355200	198984	444984
17900	14900	79700	77800	17800	14800
207909	457509	404025	433000	216784	459784
17700	14700	74700		17600	14600
225609	467109	478725		234384	474384
17500	14500			17400	14400
243109	481609			251784	488784
17300	14300			17200	
260409	495909			268984	
17100				17000	

Diese Zahl 1000009 ist also auf zwei Arten in zwei Quadrate auflösbar, es ist natürlich $= 1000^2 + 3^2 = 235^2 + 972^2$, woher sie nicht prim sein wird; aber ihre Faktoren werden aus dieser auf kleinste Terme zurückgeführten Formel $\frac{1000 \pm 972}{235 \pm 3}$ aufgefunden werden, welcher entspringt:
$\frac{1000+972}{235+3} = \frac{1972}{238} = \frac{986}{119} = \frac{58}{7}$ also ist der Faktor 3413
$\frac{1000+972}{235-3} = \frac{1972}{232} = \frac{493}{58} = \frac{17}{2}$ also ist der Faktor 293
diese Faktoren werden lichter aus dieser Formel gefunden werden
$\frac{1000-972}{235 \pm 3} = \frac{28}{238} = \frac{14}{119} = \frac{2}{17}$ und $\frac{28}{232} = \frac{7}{58}$
Wir wissen also, dass $1000009 = 293 \cdot 3413$ ist, welche Faktoren mit keiner anderen Methode so leicht aufgefunden werden gekonnt hätten.

49 Beispiel 4

233033	233033	233033	233033
482^2=232324	477^2=227529	473^2=223729	478^2=228484
709	5504	9304	4549
9540	9440	9360	9460
10249	14944	19664	14009
9340	9240	9160	9260
19589	24184	27824	23269
9140	9040	8960	9060
28729	33224	36784	32329
8940	8840	8760	8860
37669	42064	45544	41189
8740	8640	8560	8660
46409	50704	54104	49849
8540	8440	8360	8460
54949	59144	62464	58309
8340	8240	8160	8260
63289	67384	70624	66569
8140	8040	7960	8060
71429	75424	78584	74629
7940	7840	7760	7860
79369	83264	86344	82489
7740	7640	7560	7660
87109	90904	93904	90149
7540	7440	7360	7460
94649	98344	101264	97609
7340	7240	7160	7260
101989	105584	108424	104869
7140	7040	6960	7060
109129	112624	115384	11929
6940	6840	6760	6860
116069	119464	122144	118789

Weil also die Zahl, auch wenn sie von der Form $4n + 1$ ist, nicht die Summe zweier Quadrate ist, erschließen wir vermöge von Proposition 5, dass sie keine Primzahl ist. Es ist freilich nicht möglich, daher ihre Faktoren anzugeben, denn folgern wir indess, dass sie zumindest zwei Faktoren der Form $4m - 1$ hat nach Unternehmen einer Untersuchung wird $467 \cdot 499$ aufgefunden werden.

§50 Beispiel 5
Zu untersuchen, ob diese Zahl 262657 prim ist oder nicht.

262657	262657	262657	262657
511^2=261121	509^2=259081	506^2=256036	504^2=254016
1536	3576	6621	8641
10120	10080	10020	9980
11656	13656	129^2=16641	18621
9920	9880	9820	9780
21576	23536	26461	28401
9720	9680	9620	9580
31296	33216	36081	37981
9520	9480	9420	9380
40816	42696	45501	47361
9320	9280	9220	9180
50136	51976	54721	56541
9120	9080	0920	8980
59256	61056	63741	65521
8920	8880	8820	8780
68176	69936	72561	74301
8720	8680	8620	8580
76896	78616	81181	82881
8520	8480	8420	8380
85416	87096	98601	91261
8320	8280	8220	8180
93736	95376	97821	99441
8120	8080	8020	7980
101856	103456	105841	107421
7920	7880	7820	7780
109776	111336	113661	115201
7720	7680	7620	7580
117496	119016	121281	122781
7520	7480	7420	7380
125016	126496	128701	130161
7320	7280	7220	7180
132336	133776	135921	137341

Weil also hier ein einziges Quadrat $16641 = 129^2$ auftaucht, so dass auf eine einzige Weise $262657 = 129^2 + 496^2$ ist, und diese Zahlen 129 und 496 zueinander prim sind, ist es gewiss, dass die Zahl 262657 prim ist.

§51 Beispiel 6

Zu untersuchen, ob diese Zahl 32129 prim ist oder nicht.

32129	32129	32129	32129
152^2=23104	177^2=31329	175^2=30625	170^2=28900
95^2=9025	800	1504	3229
12700	15200	3400	3300
21725	16000	4904	6529
		3200	3100
32129	32129	8104	9629
148^2=21904	173^2=29929	3000	2900
10225	2200	11104	12529
12300	14800	2800	2700
22525	17000	13904	15229
		2600	2500
		16504	17729

Diese Zahl ist also auch auf eine einzige Weise in zwei Quadrate $= 95^2 + 152^2$ ist, aber weil diese Zahlen 95 und 152 nicht zueinander prim sind, sondern den gemeinsamen Teiler 19 haben, wird die vorgelegte Zahl nicht prim sein, sondern sie hat den Faktor $19^2 = 361$ und es ist $32129 = 19^2 \cdot 89$.

§52 Bemerkung

Obwohl diese Methode, Zahlen zu untersuchen, ob sie prim sind oder nicht, nur auf in dieser Form $4n + 1$ enthaltenen Zahlen erstreckt wird, kann sie dennoch beim Beurteilen von Zahlen eine große Hilfe verschaffen. Wie sehr sie aber andere Regeln, dieses selbe zu leisten, übertrifft, wird jeder beliebige, der einen Versuch dieser Sache unternehmen will, leicht erfahren. Wer nämlich eine Zahl nicht kleiner als eine Million auf dem üblichem Weg untersuchen wollte, muss ihre Teilung durch alle Primzahlen bis hin zu eintausend aus-

probieren, welche Arbeit er nicht unter mehreren Stunden ausführen wird, während mit Hilfe dieser Regel für selbiges kaum eine halbe Stunde von Nöten sein wird.