# Königliche Waisen- und Schulanstalt zu Bunzlau.

Gymnasium.

Über die

# pythagoreischen Zahlen.

Von

Professor **Friedr. Gauss.**

Beilage zum Jahresberichte des Gymnasiums der Königlichen Waisen- und Schulanstalt zu Bunzlau über das Schuljahr 1893/94.



**Bunzlau 1894.**
C. A. Voigt's Buchdruckerei (G. Wolf).

**Progr. No. 181.**

# Über die pythagoreischen Zahlen.

Die Buchstaben bedeuten ganze Zahlen, m und n ($m_1$ und $n_1$, $m_2$ und $n_2$, m′ und n′, . . .) zwei relative Primzahlen, von denen n gerade ist, und a ($a_1$, $a_2$, a′, . . .) und k positive Zahlen.

Eine Zahl heißt eine Primzahl, wenn sie nicht das Produkt zweier die Einheit übersteigenden Zahlen ist. Zwei Zahlen heißen relative Primzahlen, wenn sie keinen die Einheit übersteigenden Faktor gemein haben. Hiernach sind 1 und jede beliebige Zahl, auch 1 und 1, relative Primzahlen.

Zur Vermeidung von Wiederholungen seien folgende Sätze vorausgeschickt:

I. Die Summe und die Differenz zweier relativen Primzahlen, von denen die eine gerade ist, sind ungerade relative Primzahlen.

Denn hätten, wenn x und y relative Primzahlen sind, von denen die eine gerade ist, die ungeraden Zahlen $x+y$ und $x-y$ einen gemeinschaftlichen Faktor, der also ungerade sein müßte, so hätten auch ihre Summe und ihre Differenz, nämlich $2x$ und $2y$, folglich die Zahlen x und y diesen ungeraden Faktor gemein, was gegen die Voraussetzung verstößt.

II. Wenn sowohl die Zahlen $x_1$ und $y_1$ als auch die Zahlen $x_2$ und $y_2$ relative Primzahlen sind, so giebt es keine von 1 verschiedene Zahl, die zugleich in den Produkten $x_1x_2$, $y_1y_2$, $x_1y_2$, $x_2y_1$ enthalten ist.

Denn wäre die von 1 verschiedene Zahl $\gamma$, also auch irgend ein Grundfaktor $\delta$ von $\gamma$ in jedem der vier Produkte als Faktor enthalten, so müßte der Grundfaktor $\delta$, da er in $x_1x_2$ enthalten wäre, entweder in $x_1$ oder in $x_2$, etwa in $x_1$, enthalten sein. Alsdann müßte, da $x_1$ und $y_1$ relative Primzahlen sind, also $\delta$ kein Faktor von $y_1$ ist, wohl aber ein Faktor von $y_1y_2$ und $x_2y_1$ wäre, $\delta$ auch ein Grundfaktor von $x_2$ und $y_2$ sein, was gegen die Voraussetzung ist.

---

**§ 1.** Die Zahlen a, b, c heißen pythagoreische Zahlen, wenn sie keinen gemeinschaftlichen Faktor haben und

$$a^2 = b^2 + c^2$$

ist. a heißt die Hypotenuse, b und c heißen die Katheten.

**§ 2.** Aus der Definition geht hervor, daß je zwei von drei pythagoreischen Zahlen relative Primzahlen sind. Deshalb können nicht zwei gerade sein, also den gemeinschaftlichen Faktor 2 haben. Es können aber auch nicht alle drei Zahlen ungerade sein, weil dann auch ihre Quadrate ungerade wären, die Summe zweier ungeraden Zahlen aber gerade ist. Es müssen daher zwei Zahlen ungerade, die dritte gerade sein. Da sich jede ungerade Zahl unter der Form $2p-1$, also ihr Quadrat unter der Form $4p^2-4p+1$ darstellen läßt, so enthält der Summe der Quadrate zweier ungeraden Zahlen niemals den Faktor 4, woraus hervorgeht, daß die Hypotenuse niemals gerade ist.

Jede Hypotenuse ist ungerade; die Katheten sind relative Primzahlen, von denen die eine gerade ist.

§ 3. Nach der allgemeinen Voraussetzung sind m und n relative Primzahlen, von denen n gerade ist, also nach I. $m^2 + n^2$ und $m^2 - n^2$ ungerade relative Primzahlen. Folglich hat man wegen der Gleichung

$$(m^2 + n^2)^2 = (m^2 - n^2)^2 + (2mn)^2$$

den Satz:

Die Summe der Quadrate zweier relativen Primzahlen, von denen die eine gerade ist, ist eine Hypotenuse.

§ 4. Wenn b die ungerade Kathete ist, so kann man, da sowohl die Summe als auch die Differenz zweier ungeraden Zahlen gerade ist,

$$a + b = 2x,\ a - b = 2y$$

setzen. Alsdann ist

$$a = x + y,\ b = x - y.$$

Da hiernach jeder gemeinschaftliche Faktor von x und y auch ein Faktor von a und b ist, a und b aber nach der Voraussetzung relative Primzahlen sind, so sind auch x und y relative Primzahlen. Ferner ist

$$a^2 - b^2 = (x + y)^2 - (x - y)^2 = 4xy = c^2,$$

also

$$c = 2\sqrt{xy}.$$

Folglich ist xy ein Quadrat, was, weil x und y keinen gemeinschaftlichen Faktor haben, nur möglich ist, wenn sowohl x als auch y ein Quadrat ist. Setzt man

$$x = m^2,\ y = n^2,$$

so ist

$$a = m^2 + n^2.$$

Da a ungerade ist, so ist eine der beiden relativen Primzahlen $m^2$ und $n^2$ gerade. Hieraus ergiebt sich der Satz:

Jede Hypotenuse ist die Summe der Quadrate zweier relativen Primzahlen, von denen die eine gerade ist.

§ 5. Aus der Gleichung

$$a = m^2 + n^2 = \tfrac{1}{2}[(m + n)^2 + (m - n)^2]$$

folgt nach I.:

Jede Hypotenuse ist gleich der halben Summe der Quadrate zweier ungeraden relativen Primzahlen.

§ 6. Wenn x und y ungerade relative Primzahlen sind, so sind die Zahlen $\frac{1}{2}(x + y)$ und $\frac{1}{2}(x - y)$, weil ihre Summe und ihre Differenz die relativen Primzahlen x und y sind, ebenfalls relative Primzahlen, von denen die eine ungerade und die andere gerade ist, weil ihre Summe ungerade ist. Daher folgt aus der Gleichung

$$\tfrac{1}{2}(x^2 + y^2) = [\tfrac{1}{2}(x + y)]^2 + [\tfrac{1}{2}(x - y)]^2$$

der Satz:

Die halbe Summe der Quadrate je zweier ungeraden relativen Primzahlen ist eine Hypotenuse.

§ 7. Die Darstellung einer Hypotenuse als die Summe der Quadrate zweier relativen Primzahlen, von denen die eine gerade ist, und ebenso die Summe der Quadrate selbst heißt eine Zerlegung, die relativen Primzahlen heißen die Bestandteile der Zerlegung.

Eine Hypotenuse heißt einfach, wenn sie eine Primzahl oder eine Potenz einer Primzahl ist, zusammengesetzt, wenn sie mindestens zwei verschiedene Grundfaktoren (Primfaktoren) enthält. Einfache Hypotenusen heißen verschieden, wenn sie verschiedene Primzahlen oder Potenzen verschiedener Primzahlen sind. (Hypotenusen, die verschiedene Potenzen einer und derselben Primzahl sind, sehe ich darum nicht als verschieden an, weil die Anzahl ihrer Zerlegungen dieselbe ist und es sich hier nur um diese Anzahl, niemals aber um die Größe der Hypotenusen handelt).

Beispiele.

$5 = 1^2 + 2^2$, $13 = 3^2 + 2^2$, $17 = 1^2 + 4^2$, $29 = 5^2 + 2^2$, $37 = 1^2 + 6^2$, $41 = 5^2 + 4^2$, $53 = 7^2 + 2^2$, $61 = 5^2 + 6^2$, $73 = 3^2 + 8^2$, $89 = 5^2 + 8^2$, $97 = 9^2 + 4^2$, $101 = 1^2 + 10^2$, $109 = 3^2 + 10^2$, $113 = 7^2 + 8^2$, $137 = 11^2 + 4^2$, $149 = 7^2 + 10^2$; $25 = 3^2 + 4^2$, $625 = 7^2 + 24^2$, $169 = 5^2 + 12^2$, $289 = 15^2 + 8^2$; $85 = 9^2 + 2^2 = 7^2 + 6^2$, $221 = 11^2 + 10^2 = 5^2 + 14^2$, $325 = 1^2 + 18^2 = 17^2 + 6^2$, $1105 = 33^2 + 4^2 = 9^2 + 32^2 = 31^2 + 12^2 = 23^2 + 24^2$.

Diese kleine Tabelle giebt Anlaß zu folgenden Bemerkungen:

Die ersten 16 Hypotenusen sind unter den Zahlen von 1 bis 156 die Primzahlen von der Form $4k + 1$ und lassen nur eine Zerlegung zu; alle übrigen Primzahlen sind von der Form $4k - 1$ und keine Hypotenusen. Die Hypotenusen 25, 625, 169, 289 sind Potenzen der primzahligen Hypotenusen 5, 13, 17 und haben ebenfalls nur eine Zerlegung. Die Hypotenusen 85, 221 mit je zwei und die Hypotenuse 1105 mit vier Zerlegungen sind Produkte primzahliger Hypotenusen, nämlich $5 \cdot 17$, $13 \cdot 17$, $5 \cdot 13 \cdot 17$. Die Hypotenuse 325 ist das Produkt der Hypotenusen 13 und 25, von denen die erste eine Primzahl, die zweite aber das Quadrat der Primzahl 5 ist; sie hat zwei Zerlegungen und läßt sich außerdem als die Quadratsumme $15^2 + 10^2$ darstellen, die aber keine Zerlegung im Sinne der Definition ist, da 15 und 10 keine relativen Primzahlen sind. Ebenso läßt sich $625 = 5^4$ als die Summe zweier Quadrate mit einem gemeinschaftlichen Faktor, nämlich als die Summe $15^2 + 20^2$, darstellen.

Die Anzahl der Paare von Katheten, die zu einer Hypotenuse gehören und relative Primzahlen sind, ist gleich der Anzahl der Zerlegungen, weil jede Zerlegung $m^2 + n^2$ die Katheten $m^2 - n^2$ und $2mn$ liefert. Außerdem gehören zu einer Hypotenuse, die nicht eine Primzahl ist, noch eine Anzahl von Kathetenpaaren, die einen gemeinschaftlichen Faktor haben. Es ist

$25^2 = 7^2 + 24^2 = 15^2 + 20^2$, $125^2 = 117^2 + 44^2 = 75^2 + 100^2 = 35^2 + 120^2$, $65^2 = 63^2 + 16^2 = 33^2 + 56^2 = 25^2 + 60^2 = 39^2 + 52^2$, $325^2 = 323^2 + 36^2 = 253^2 + 204^2 = 315^2 + 80^2 = 165^2 + 280^2 = 125^2 + 300^2 = 195^2 + 260^2 = 91^2 + 312^2$.

§ 8. Jede Hypotenuse läßt sich unter der Form $4k + 1$ darstellen; und es giebt keine Primzahl von der Form $4k - 1$, die eine Hypotenuse ist.

Denn da m ungerade, n gerade ist und alle ungeraden Zahlen sich unter der Form $4p \pm 1$ darstellen lassen, so kann man $m = 4p \pm 1$, $n = 2q$ setzen. Alsdann ist

$$a = m^2 + n^2 = 4(4p^2 \pm 2p + q^2) + 1.$$

Nun ist $4p^2 \pm 2p = 2p(2p \pm 1)$ gleich oder größer als Null, also $4p^2 \pm 2p + q^2$ positiv. Folglich ist für $4p^2 \pm 2p + q^2 = k$

$$a = 4k + 1.$$

§ 9. Jede durch 3 nicht teilbare Zahl läßt sich unter der Form $3p \pm 1$, ihr Quadrat also unter der Form $3(3p^2 \pm 2p) + 1$, also überhaupt unter Form $3k + 1$ darstellen. Folglich ist die Differenz zweier Quadrate, die nicht durch 3 teilbar sind, stets ein Vielfaches von 3. —

Jede Zahl, die nicht durch 5 teilbar ist, ist entweder von der Form $5p \pm 1$ oder von der Form $5p \pm 2$, ihr Quadrat also entweder von der Form $5(5p^2 \pm 2p) + 1$ oder von der Form $5(5p^2 \pm 4p) + 4 = 5(5p^2 \pm 4p + 1) - 1$, also allgemein von der Form $5k \pm 1$. Folglich ist stets entweder die Summe oder die Differenz zweier Quadrate, die nicht durch 5 teilbar sind, ein Vielfaches von 5.

Von den pythagoreischen Zahlen

$$a = m^2 + n^2,\ b = m^2 - n^2,\ c = 2mn$$

ist c stets durch 4 teilbar. Ist eine der Zahlen m und n durch 3 oder 5 teilbar, so ist auch c durch 3 oder 5 teilbar. Ist keine der Zahlen m und n durch 3 oder 5 teilbar, so ist stets $b = m^2 - n^2$ durch 3 und entweder $a = m^2 + n^2$ oder $b = m^2 - n^2$ durch 5 teilbar. Hiermit ist der Satz bewiesen:

Jede der drei Zahlen 3, 4, 5 ist ein Teiler einer von drei beliebigen pythagoreischen Zahlen und 60 ein Teiler des Produkts aller drei Zahlen. (Baltzer.)

**§ 10.** Es sei

$$a = m_1^2 + n_1^2 = m_2^2 + n_2^2.$$

Alsdann ist

$$\frac{m_1 + m_2}{n_2 - n_1} = \frac{n_2 + n_1}{m_1 - m_2},\quad \frac{m_1 + m_2}{n_2 + n_1} = \frac{n_2 - n_1}{m_1 - m_2}.$$

Setzt man

$$\frac{m_1 + m_2}{n_2 - n_1} = \frac{n_2 + n_1}{m_1 - m_2} = \frac{p_1}{q_1},\quad \frac{m_1 + m_2}{n_2 + n_1} = \frac{n_2 - n_1}{m_1 - m_2} = \frac{p_2}{q_2},$$

wo sowohl $p_1$ und $q_1$ als auch $p_2$ und $q_2$ relative Primzahlen sind, so ist

$$\frac{m_1 + m_2}{m_1 - m_2} = \frac{p_1 p_2}{q_1 q_2},\quad \frac{n_2 + n_1}{n_2 - n_1} = \frac{p_1 q_2}{p_2 q_1},$$

also

$$\frac{m_1}{m_2} = \frac{p_1 p_2 + q_1 q_2}{p_1 p_2 - q_1 q_2},\quad \frac{n_1}{n_2} = \frac{p_1 q_2 - p_2 q_1}{p_1 q_2 + p_2 q_1}.$$

Diese Gleichungen sind nur möglich, wenn

$$m_1 = \delta(p_1 p_2 + q_1 q_2),\quad m_2 = \delta(p_1 p_2 - q_1 q_2);$$
$$n_1 = \varepsilon(p_1 q_2 - p_2 q_1),\quad n_2 = \varepsilon(p_1 q_2 + p_2 q_1)$$

ist, wo $\delta$ und $\varepsilon$ ganze Zahlen oder Stammbrüche sind oder die eine eine ganze Zahl und die andere ein Stammbruch ist. Nun ist

$$m_1 + m_2 = 2\delta p_1 p_2,\quad n_2 - n_1 = 2\varepsilon p_2 q_1,$$

also

$$\frac{m_1 + m_2}{n_2 - n_1} = \frac{\delta}{\varepsilon} \cdot \frac{p_1}{q_1} = \frac{p_1}{q_1}.$$

Folglich ist $\delta = \varepsilon$. Ist $\delta$ eine ganze Zahl, so ist diese, weil $m_1 = \delta(p_1 p_2 + q_1 q_2)$, $n_1 = \delta(p_1 p_2 - p_2 q_1)$ ist und $m_1$ und $n_1$ relative Primzahlen sind, gleich 1. Ist dagegen $\delta$ ein Stammbruch und gleich $\frac{1}{\delta_1}$, so ist

$$p_1 p_2 + q_1 q_2 = \delta_1 m_1,\quad p_1 p_2 - q_1 q_2 = \delta_1 m_2;$$
$$p_1 q_2 - p_2 q_1 = \delta_1 n_1,\quad p_1 q_2 + p_2 q_1 = \delta_1 n_2,$$

also

$$p_1 p_2 = \tfrac{1}{2}\delta_1(m_1 + m_2),\quad q_1 q_2 = \tfrac{1}{2}\delta_1(m_1 - m_2);$$
$$p_1 q_2 = \tfrac{1}{2}\delta_1(n_2 + n_1),\quad p_2 q_1 = \tfrac{1}{2}\delta_1(n_2 - n_1).$$

Da nun $m_1 + m_2$, $m_1 - m_2$, $n_2 + n_1$, $n_2 - n_1$ gerade Zahlen sind, so ist $\delta_1$ ein Teiler der vier Zahlen $p_1p_2$, $q_1q_2$, $p_1q_2$, $p_2q_1$, was nach II. nur möglich ist, wenn auch $\delta_1 = 1$ ist. Folglich ist

$$m_1 = p_1p_2 + q_1q_2, \quad n_1 = p_1q_2 - p_2q_1,$$
$$a = m_1^2 + n_1^2 = p_1^2p_2^2 + p_1^2q_2^2 + p_2^2q_1^2 + q_1^2q_2^2,$$

also

$$a = (p_1^2 + q_1^2)(p_2^2 + q_2^2).$$

Aus dieser Gleichung zu folgern, daß jede Hypotenuse, die mehr als eine Zerlegung zuläßt, zusammengesetzt sei (vergl. § 28) wäre übereilt, da sehr wohl $p_1^2 + q_1^2$ und $p_2^2 + q_2^2$, wie $1^2 + 8^2$ und $7^2 + 4^2$, einander gleich oder, wie $11^2 + 2^2$ und $3^2 + 4^2$, Potenzen einer und derselben Primzahl sein können. Wohl aber berechtigt die Gleichung zu dem Schlusse, daß a keine Primzahl ist, woraus sich der Satz ergiebt:

Jede primzahlige Hypotenuse hat nur eine Zerlegung.

**§ 11.** Es ist allgemein

$$(x_1^2 + y_1^2)(x_2^2 + y_2^2) = x_1^2x_2^2 \pm 2x_1x_2 \cdot y_1y_2 + y_1^2y_2^2 + x_1^2y_2^2 \mp 2x_1y_2 \cdot x_2y_1 + x_2^2y_1^2,$$
$$= (x_1x_2 + y_1y_2)^2 + (x_1y_2 - x_2y_1)^2$$
$$= (x_1x_2 - y_1y_2)^2 + (x_1y_2 + x_2y_1)^2.$$

Hiernach ist

$$(m_1^2 + n_1^2)\ (m_2^2 + n_2^2) = (m_1m_2 + n_1n_2)^2 + (m_1n_2 - m_2n_1)^2$$
$$= (m_1m_2 - n_1n_2)^2 + (m_1n_2 + m_2n_1)^2.$$

Da $m_1$ und $m_2$ ungerade, $n_1$ und $n_2$ gerade sind, so sind auch $m_1m_2 + n_1n_2$ und $m_1m_2 - n_1n_2$ ungerade, $m_1n_2 - m_2n_1$ und $m_1n_2 + m_2n_1$ gerade. Hieraus ergiebt sich der Satz:

Das Produkt zweier Hypotenusen läßt sich auf mindestens zweifache Weise als die Summe der Quadrate zweier Zahlen, von denen die eine ungerade, die andere gerade ist, darstellen.

Anmerkung. Ob die Quadratsummen $(m_1m_2 + n_1n_2)^2 + (m_1n_2 - m_2n_1)^2$ und $(m_1m_2 - n_1n_2)^2 + (m_1n_2 + m_2n_1)^2$ Zerlegungen im Sinne der Definition sind, bedarf in jedem Falle einer besonderen Untersuchung; es ist möglich, daß keine, eine oder beide Summen Zerlegungen sind. Es ist z. B.

$$(1^2 + 18^2)(1^2 + 8^2) = 145^2 + 10^2 = 143^2 + 26^2$$
$$(1^2 + 18^2)(7^2 + 4^2) = 79^2 + 122^2 = 65^2 + 130^2$$
$$(11^2 + 2^2)(5^2 + 12^2) = 79^2 + 122^2 = 31^2 + 142^2.$$

Das erste Produkt giebt keine, das zweite eine, das dritte zwei Zerlegungen. In den beiden ersten Fällen haben die Hypotenusen, nämlich 325 und 65, zwei Grundfaktoren gemein, im dritten sind sie, nämlich 125 und 169, relative Primzahlen.

**§ 12.** Nach Euler*). Es sei die Hypotenuse $a_1 = p^2 + q^2$ eine Primzahl und

$$a = m^2 + n^2 = a_1a_2.$$

Da p und q relative Primzahlen sind, so lassen sich durch Verwandlung des Bruches $\frac{p}{q}$ in einen Kettenbruch die Zahlen $\alpha$ und $\beta$ so bestimmen, daß

$$p\alpha - q\beta = 1, \quad p(n\alpha) + q(-m\beta) = m$$

oder, wenn man $m\alpha = x$, $-m\beta = y$ setzt,

$$m = px + qy, \quad n = py - qx + z$$

*) Leonhardi Euleri commentationes arithmeticae collectae. Petropoli 1849. Tomus posterior. pag. 570, 571. (Opera arithmetica hucusque inedita.)

ist. Alsdann ist

$$\begin{aligned} m^2+n^2 &= (px+qy)^2+(py-qx+z)^2 \\ &= (px+qy)^2+(py-qx)^2+2(py-qx)z+z^2 \\ &= (p^2+q^2)(x^2+y^2)+[2(py-qx)+z]z. \end{aligned}$$

Da $m^2+n^2$ durch die Primzahl $p^2+q^2$ teilbar ist, so ist entweder $2(py-qx)+z$ oder $z$ ebenfalls durch $p^2+q^2$ teilbar. Im ersten Falle setzt man

$$2(py-qx)+z=(p^2+q^2)t, \quad z=(p^2+q^2)t-2(py-qx)$$

und erhält

$$\begin{aligned} m^2+n^2=(p^2+q^2)a_2 &= (p^2+q^2)(x^2+y^2)+(p^2+q^2)t[(p^2+q^2)t-2(py-qx)], \\ a_2 &= x^2+y^2+(p^2+q^2)t^2-2(py-qx)t \\ &= (x+qt)^2+(y-pt)^2. \end{aligned}$$

Im zweiten Falle setzt man

$$z=(p^2+q^2)u, \quad 2(py-qx)+z=2(py-qx)+(p^2+q^2)u$$

und findet

$$\begin{aligned} a_2 &= x^2+y^2+[2(py-qx)+(p^2+q^2)u]u \\ &= x^2+y^2+2(py-qx)u+(p^2+q^2)u^2 \\ &= (x-qu)^2+(y+pu)^2. \end{aligned}$$

Folglich ist in jedem Falle $a_2$ eine Summe zweier Quadrate.

Wenn ein Grundfaktor einer zusammengesetzten Hypotenuse eine Hypotenuse ist, so ist das Produkt der übrigen Grundfaktoren eine Summe zweier Quadrate.

**§ 13.** Nach Legendre*). Es seien x und y relative Primzahlen und A ein Faktor von $x^2+y^2$. Setzt man

$$p=x-vA, \quad q=y-wA,$$

so ist auch $p^2+q^2$ durch A teilbar, also

$$AA_1=p^2+q^2.$$

Die Zahlen v und w lassen sich so bestimmen, daß die absoluten Werte von p und q kleiner als $\frac{1}{2}A$ sind. Ist nämlich $z<\frac{x}{A}<z+1$, so ist $zA<x<(z+1)A$, $o<x-zA<A$. Ist $x-zA<\frac{1}{2}A$, so ist $v=z$. Ist $x-zA>\frac{1}{2}A$, so ist $A-(x-zA)<\frac{1}{2}A$, also $-[x-(z+1)A]<\frac{1}{2}A$. Ebenso läßt sich w derart bestimmen, daß der absolute Wert von q kleiner als $\frac{1}{2}A$ ist. Hiernach ist $p^2<\frac{1}{4}A^2$, $q^2<\frac{1}{4}A^2$, also

$$AA_1<\tfrac{1}{2}A^2, \quad A_1<\tfrac{1}{2}A.$$

Ist $A_1>1$, so bestimmt man r und s so, daß die absoluten Werte von $p-rA_1$ und $q-sA_1$ kleiner als $\frac{1}{2}A_1$ sind. Da $A_1$ ein Teiler von $p^2+q^2$, also auch von $(p-rA_1)^2+(q-sA_1)^2$ ist, so kann man

$$A_1A_2=(p-rA_1)^2+(q-sA_1)^2$$

setzen, wo $A_2<\frac{1}{2}A_1$ ist. Multipliziert man diese Gleichung mit der Gleichung $AA_1=p^2+q^2$, so erhält man

$$\begin{aligned} AA_1^2A_2 &= p^4-2rp^3A_1+r^2p^2A_1^2+p^2q^2-2sp^2qA_1+s^2p^2A_1^2+p^2q^2-2rpq^2A_1+r^2q^2A_1^2 \\ &\quad +q^4-2sq^3A_1+s^2q^2A_1^2 \\ &= (p^2+q^2)^2+(rp+sq)^2A_1^2+(rq-sp)^2A_1^2-2(p^2+q^2)rpA_1-2(p^2+q^2)sqA_1 \\ &= [(p^2+q^2)-(rp+sq)A_1]^2+(rq-sp)^2A_1^2. \end{aligned}$$

*) Legendre, Théorie des nombres, 3. Édit. Paris 1830. Tome I. pag. 203.

Ersetzt man hierin $p^2 + q^2$ durch $AA_1$, so ergiebt sich nach Division durch $A_1^2$

$$AA_2 = [A - (rp + sq)]^2 + (rq - sp)^2.$$

Ist $A_2 > 1$, so läßt sich aus dem Produkte $AA_2$ in derselben Weise ein Produkt $AA_3$ gleich einer Summe zweier Quadrate herleiten, in dem $A_3 < \frac{1}{2}A_2$ ist, u. s. w. Da in der Reihe der ganzen positiven Zahlen

$$A,\ A_1,\ A_2,\ A_3,\ \ldots$$

jede kleiner als die Hälfte der vorhergehenden Zahl ist, so gelangt man notwendig zu einer Gleichung von der Form

$$AA_k = t^2 + u^2,$$

in der $A_k = 1$ ist. Folglich ist A eine Summe zweier Quadrate.

Jeder Teiler einer Summe der Quadrate zweier relativen Primzahlen ist eine Summe zweier Quadrate.

Anmerkung. In dem vorstehend wiedergegebenen Legendreschen Beweise wird vorausgesetzt, daß x und y relative Primzahlen sind. Daraus folgt, daß keine der Zahlen $p = x - vA$ und $q = y - wA$ gleich Null sein kann. Die Voraussetzung ist aber auch notwendig, weil man, wenn x und y einen gemeinschaftlichen Faktor hätten, als A diesen Faktor wählen könnte. Dann aber wäre die Bestimmung von p und q derart, daß sie kleiner als $\frac{1}{2}A$ sind, nur möglich, wenn $x = vA$, $y = wA$ gesetzt würde, folglich sowohl p als auch q gleich Null wäre, wodurch die weitere Entwickelung unmöglich würde.

Es kann die Frage aufgeworfen werden, ob sich r und s stets den Erfordernissen des Beweises gemäß bestimmen lassen. Von den Zahlen p und q muß mindestens eine größer als $\frac{1}{2}A_1$ sein. Denn wären beide kleiner als $\frac{1}{2}A_1$ oder die eine kleiner als $\frac{1}{2}A_1$ und die andere gleich $\frac{1}{2}A_1$ oder beide gleich $\frac{1}{2}A_1$, so wäre wegen der Gleichung $AA_1 = p^2 + q^2$, $AA_1 \leq \frac{1}{2}A_1^2$, $A \leq \frac{1}{2}A_1$. Also ist eine der Zahlen r und s stets größer als Null, während die andere gleich Null sein kann.

Da t und u Differenzen sind, so ist der Fall nicht ausgeschlossen, daß die eine dieser Zahlen verschwindet, A also gleich einem Quadrate $B^2$ ist. Alsdann ist auch B ein Teiler von $x^2 + y^2$, läßt sich daher unter der Form einer Summe zweier Quadrate darstellen, wo aber ebenfalls das eine Quadrat verschwinden, B also gleich einem Quadrat $B_1^2$ sein kann. Es ist daher denkbar, daß man zu dem Ergebnisse gelangt, daß

$$A = B^2,\ B = B_1^2,\ B_1 = B_2^2,\ \ldots.$$

ist. Da in der Reihe der Zahlen

$$A,\ B,\ B_1,\ B_2,\ \ldots.$$

jede die Quadratwurzel aus der vorhergehenden, also kleiner als die vorhergehende ist, so muß man zu einer Zahl $B_k$ gelangen, die gleich $t^2 + u^2$ ist, wo aber keins der Quadrate verschwindet. Aus § 6 geht hervor, daß $x^2 + y^2$ nur einen geraden Faktor haben kann, nämlich 2. Ist $A = 2$, so ist $A = 1^2 + 1^2$. In jedem anderen Falle ist A, also auch $B_k$ ungerade, folglich die eine der Zahlen t und u ungerade, die andere gerade. Ferner ist

$$B_{k-1} = B_k^2 = (t^2 + u^2)^2 = (t^2 - u^2)^2 + (2tu)^2 = t_1^2 + u_1^2,$$

wo $t_1$ ungerade, $u_1$ gerade ist, und ebenso

$$B_{k-2} = B_{k-1}^2 = t_2^2 + u_2^2,\quad B_{k-3} = B_{k-2}^2 = t_3^2 + u_3^2,\ \ldots$$
$$B_1 = B_2^2 = t_{k-1}^2 + u_{k-1}^2,\quad A = B^2 = t_k^2 + u_k^2.$$

Legendre giebt a. a. O. einen auf ganz anderen Prinzipien beruhenden Beweis des Satzes: „Tout diviseur de la formule $t^2 + u^2$, composée de deux carrés premiers entre eux, est également la somme de deux carrés premiers entre eux". Den vorstehend mitgeteilten Beweis schließt er mit den Worten: „ ... on parviendra donc nécessairement à un terme égal à l'unité, et alors le nombre A sera égal à la somme de deux carrés." Wie man sieht, läßt er hier am Schlusse die Worte „premiers entre eux" weg. Aus dem hier mitgeteilten Beweise geht auch in der Tat nicht hervor, daß A eine Summe der Quadrate zweier relativen Primzahlen ist.

Euler giebt a. a. O. folgenden Beweis:

Aus dem im § 12 wiedergegebenen Satze folgert Euler zunächst, daß, wenn das Produkt der beiden Zahlen A und B eine Summe $x^2 + y^2$ der Quadrate zweier relativen Primzahlen und A nicht eine Summe zweier Quadrate ist, von den Grundfaktoren von B mindestens einer ebenfalls nicht eine Summe zweier Quadrate

ist. Denn wäre jeder Grundfaktor von B eine Summe zweier Quadrate, so würde man durch auf einander folgende Divisionen durch die einzelnen Grundfaktoren zur Zahl A gelangen, die nach dem bewiesenen Satze eine Summe zweier Quadrate sein müßte. Dann fährt er fort:

557. Nunc igitur investigemus, an summa duorum quadratorum $pp + qq$ inter se primorum per ullum numerum $\mathfrak{A}$, qui non sit summa duorum quadratorum, divisibilis esse queat. Ad hoc sumamus $pp + qq$ divisibile esse per talem numerum $\mathfrak{A}$, atque etiam $(p - m\mathfrak{A})^2 + (q - n\mathfrak{A})^2$ divisibilis erit per $\mathfrak{A}$.*)

558. Poterit ergo talis summa duorum quadratorum $pp + qq$ exhiberi, quorum radices p et q minores sint quam $\mathfrak{A}$, quin etiam minores quam $\frac{1}{2}\mathfrak{A}$; cum etiam $(\mathfrak{A} - p)^2 + (\mathfrak{A} - q)^2$ divisionem admittere debeat, quorum quadratorum radices minores erint quam $\frac{1}{2}\mathfrak{A}$, si p et q eo essent majores.

559. Dabitur ergo summa duorum quadratorum $pp + qq$ minor qnam $\frac{1}{2}\mathfrak{A}\mathfrak{A}$ (cum sit $p < \frac{1}{2}\mathfrak{A}$ et $q < \frac{1}{2}\mathfrak{A}$) per numerum $\mathfrak{A}$ divisibilis; ponatur quotus $= \mathfrak{B}$, qui etiam vel ipse non erit summa duorum quadratorum, vel factorem talem habebit, eritque $\mathfrak{B} < \frac{1}{2}\mathfrak{A}$.

560. Cum jam $pp + qq$ divisibile sit per $\mathfrak{B}$, exhiberi poterit summa duorum quadratorum $rr + ss$ minor quam $\frac{1}{2}\mathfrak{B}\mathfrak{B}$, divisibilis per $\mathfrak{B}$, et quotus $\mathfrak{C}$, qui erit minor quam $\frac{1}{2}\mathfrak{B}$, pariter non erit summa duorum quadratorum, per quem cum divisibilis sit $rr + ss$, dabitur $tt + uu < \frac{1}{2}\mathfrak{C}\mathfrak{C}$ divisibilis per $\mathfrak{C}$, et quotus $\mathfrak{D} < \frac{1}{2}\mathfrak{C}$ itidem non erit summa duorum quadratorum.

561. Hoc modo tandem pervenietur ad summam duorum quadratorum quantumvis parvam, quae foret divisibilis per numerum non-summam duorum quadratorum, quod cum sit absurdum, necessario sequitur, summam duorum quadratorum inter se primorum non esse divisibilem per ullum numerum, qui ipse non sit summa duorum quadratorum."

Abgesehen von der Unrichtigkeit der am Fuße des Textes mitgeteilten Randbemerkung (denn ist z. B. $p = 37$, $q = 16$, $\mathfrak{A} = 65$, so ist $p - 1 \cdot \mathfrak{A} = -28$, $q - 0 \cdot \mathfrak{A} = 16$) sind Eulers Schlußfolgerungen nicht unbedenklich. Er hat bewiesen, daß $\mathfrak{B}$ entweder nicht eine Summe zweier Quadrate ist oder eine Nicht-Summe zweier Quadrate als Faktor enthält, also nicht bewiesen, daß $\mathfrak{B}$ eine Nicht-Summe zweier Quadrate ist. Der Schluß in § 560 beruht aber auf der Voraussetzung, daß $\mathfrak{B}$ nicht eine Summe zweier Quadrate ist, weil, wenn $\mathfrak{B}$ eine Summe zweier Quadrate wäre, alle Grundfaktoren von $\mathfrak{C}$ Summen zweier Quadrate sein könnten.

**§ 14.** Nach Euler**). Nach der Lehre von den quadratischen Resten läßt sich, wenn $4k + 1$ eine Primzahl ist, ein Quadrat $x^2$ so bestimmen, daß

$$r(4k + 1) - 1 = x^2$$

ist. Folglich ist

$$1^2 + x^2 = r(4k + 1),$$

also $4k + 1$ ein Teiler von $1^2 + x^2$. Nach dem vor. § ist aber jeder Teiler einer Summe der Quadrate zweier relativen Primzahlen, auch wenn diese ungerade sind, die Summe ihrer Quadrate also nicht eine Hypotenuse ist, ebenfalls eine Summe zweier Quadrate. Folglich ist auch $4k + 1$ eine Summe der Quadrate zweier Zahlen, die, weil $4k + 1$ eine Primzahl ist, relative Primzahlen sind, und von denen, da $4k + 1$ ungerade ist, die eine gerade sein muß. Mithin ist $4k + 1$ eine Hypotenuse. Beispiel:

$$\text{Für } k = 3 \text{ ist } 1^2 + 8^2 = 65 = 5 \cdot 13 = (1^2 + 2^2)(3^2 + 2^2).$$
$$\text{Für } k = 10 \text{ ist } 1^2 + 9^2 = 82 = 2 \cdot 41 = (1^2 + 1^2)(5^2 + 4^2).$$

Hiermit ist die Umkehrung des in § 8 in Verbindung mit § 10 enthaltenen Satzes: Jede primzahlige Hypotenuse ist von der Form $4k + 1$ und läßt nur eine Zerlegung zu, nämlich der Fermatsche Satz bewiesen:

Jede Primzahl von der Form $4k + 1$ ist eine Hypotenuse mit nur einer Zerlegung.

---

*) Script. ad marg. Quorum radices, si p et q sint primi inter se, etiam erunt primae inter se.

**) A. a. O. pag. 572.

**§ 15.** Aus § 13 folgt:

Jeder Grundfaktor einer Hypotenuse ist eine Hypotenuse.

Wenn eine Potenz einer Primzahl eine Hypotenuse ist, so ist es auch ihre Grundzahl.

**§ 16.** Nach § 12 ist, wenn $a = a_1 a_2 = m^2 + n^2$ und $a_1 = p^2 + q^2$ eine Primzahl ist, $a_2 = r^2 + s^2$, wo entweder $r = x + qt$, $s = y - pt$ oder $r = x - qu$, $s = y + pu$ und $m = px + qy$ ist. Also ist

$$m^2 + n^2 = (p^2 + q^2)(r^2 + s^2) = (pr + qs)^2 + (ps - qr)^2.$$

Da nun in beiden Fällen $pr + qs = px + qy$ ist, so ist

$$m = pr + qs, \text{ also } n = ps - qr.$$

Hiernach sind, da m und n relative Primzahlen sind, auch r und s relative Primzahlen. Also hat man den Satz:

Wenn ein Grundfaktor einer Hypotenuse eine Hypotenuse ist, so ist das Produkt der übrigen Grundfaktoren ebenfalls eine Hypotenuse.

**§ 17.** Haben die Hypotenusen

$$a_1 = m_1^2 + n_1^2, \quad a_2 = m_2^2 + n_2^2$$

einen gemeinschaftlichen Grundfaktor $\gamma$, so ist dieser nach § 15 eine Hypotenuse. Ist ferner

$$m_1^2 + n_1^2 = a_1'\gamma, \; m_2^2 + n_2^2 = a_2'\gamma,$$

so sind nach § 16 auch $a_1'$ und $a_2'$ Hypotenusen. Ist $\delta^2 + \varepsilon^2$ die nach § 10 eindeutig bestimmte Zerlegung von $\gamma$, so muß es unter den möglichen Zerlegungen von $a_1'$ eine, $p_1^2 + q_1^2$, geben, die mit $\delta^2 + \varepsilon^2$ zusammengesetzt die Zerlegung $m_1^2 + n_1^2$ der Hypotenuse $a_1$ liefert. Ebenso sei unter den möglichen Zerlegungen der Hypotenuse $a_2'$ $p_2^2 + q_2^2$ diejenige, deren Zusammensetzung mit $\delta^2 + \varepsilon^2$ die Zerlegung $m_2^2 + n_2^2$ der Hypotenuse $a_2$ liefert. Alsdann ist

$$\begin{aligned} m_1^2 + n_1^2 = (p_1^2 + q_1^2)(\delta^2 + \varepsilon^2) &= (p_1\delta + q_1\varepsilon)^2 + (p_1\varepsilon - q_1\delta)^2 \\ &= (p_1\delta - q_1\varepsilon)^2 + (p_1\varepsilon + q_1\delta)^2, \\ m_2^2 + n_2^2 = (p_2^2 + q_2^2)(\delta^2 + \varepsilon^2) &= (p_2\delta + q_2\varepsilon)^2 + (p_2\varepsilon - q_2\delta)^2 \\ &= (p_2\delta - q_2\varepsilon)^2 + (p_2\varepsilon + q_2\delta)^2. \end{aligned}$$

Hiernach ist entweder

$$m_1 = \pm(p_1\delta + q_1\varepsilon), \quad n_1 = \pm(p_1\varepsilon - q_1\delta)$$

oder

$$m_1 = \pm(p_1\delta - q_1\varepsilon), \quad n_1 = \pm(p_1\varepsilon + q_1\delta)$$

und ebenso entweder

$$m_2 = \pm(p_2\delta + q_2\varepsilon), \quad n_2 = \pm(p_2\varepsilon - q_2\delta)$$

oder

$$m_2 = \pm(p_2\delta - q_2\varepsilon), \quad n_2 = \pm(p_2\varepsilon + q_2\delta).$$

Ist eine der beiden Zahlen $a_1$ und $a_2$, etwa $a_2$, eine Primzahl, so ist überall $p_2 = 1$, $q_2 = 0$ zu setzen. Bildet man aus diesen Gleichungen die Zahlenpaare $m_1m_2 + n_1n_2$, $m_1n_2 - m_2n_1$ und $m_1m_2 - n_1n_2$, $m_1n_2 + m_2n_1$, so wird sich, wie man auch die Vorzeichen für $m_1$, $n_1$, $m_2$, $n_2$ wählen mag, in den Zahlen des einen Zahlenpaars stets der gemeinschaftliche Faktor $\gamma$ vorfinden. Wählt man z. B.

$$\begin{aligned} m_1 &= -(p_1\delta - q_1\varepsilon), \quad n_1 = +(p_1\varepsilon + q_1\delta), \\ m_2 &= -(p_2\delta + q_2\varepsilon), \quad n_2 = -(p_2\varepsilon - q_2\delta), \end{aligned}$$

so ist

$$m_1m_2 - n_1n_2 = (p_1p_2 - q_1q_2)\gamma, \quad m_1n_2 + m_2n_1 = -(p_1q_2 + p_2q_1)\gamma;$$

oder ist

$$m_1 = +(p_1\delta + q_1\varepsilon), \quad n_1 = -(p_1\varepsilon - q_1\delta)$$
$$m_2 = -(p_2\delta - q_2\varepsilon), \quad n_2 = +(p_2\varepsilon + q_2\delta),$$

so ist

$$m_1m_2 + n_1n_2 = -(p_1p_2 - q_1q_2)\gamma, \; m_1n_2 - m_2n_1 = +(p_1q_2 + p_2q_1)\gamma.$$

Hiernach ist also $\gamma$ ein gemeinschaftlicher Faktor der Zahlen des einen der Zahlenpaare $m_1m_2 + n_1n_2$, $m_1n_2 - m_2n_1$ und $m_1m_2 - n_1n_2$, $m_1n_2 + m_2n_1$. Wäre nun $\gamma$ auch ein gemeinschaftlicher Faktor der Zahlen des anderen Zahlenpaares, so würde sich durch Addition und Subtraktion ergeben, daß $\gamma$ ein gemeinschaftlicher Faktor der vier Zahlen $2m_1m_2$, $2n_1n_2$, $2m_1n_2$, $2m_2n_1$, also, da $\gamma$ als Hypotenuse ungerade ist, der vier Zahlen $m_1m_2$, $n_1n_2$, $m_1n_2$, $m_2n_1$ ist, was dem Satze II. widerspricht. Hiermit ist bewiesen:

Wenn die Hypotenusen $m_1^2 + n_1^2$ und $m_2^2 + n_2^2$ nicht relative Primzahlen sind, so ist jeder beiden gemeinschaftliche Grundfaktor ein gemeinschaftlicher Faktor der Zahlen des einen, aber auch nur des einen der Zahlenpaare

$$m_1m_2 + n_1n_2, \; m_1n_2 - m_2n_1 \text{ und } m_1m_2 - n_1n_2, \; m_1n_2 + m_2n_1.$$

Eine aus einer Hypotenuse durch Wiederholung eines Grundfaktors neu gebildete Hypotenuse läßt nicht mehr Zerlegungen zu als die Hypotenuse, aus der sie gebildet woren ist.

Anmerkung. Zur Erläuterung der Beweisführung diene das Produkt der Hypotenusen $a_1 = 325$ und $a_2 = 65$; beide haben die Grundfaktoren $5 = 1^2 + 2^2$ und $13 = 3^2 + 2^2$ gemein. Handelt es sich um den Grundfaktor 5, so ist $a_1' = 65 = 7^2 + 4^2 = 1^2 + 8^2$, $a_2' = 13 = 3^2 + 2^2$. Es sei nun $m_1^2 = 1^2$, $n_1^2 = 18^2$; $m_2^2 = 1^2$, $n_2^2 = 8^2$. Da $\delta^2 + \varepsilon^2 = 1^2 + 2^2$ eindeutig bestimmt ist, so muß, da die Zerlegung $1^2 + 18^2$ von $a_1$ faktisch existirt, die eine der beiden Zerlegungen von $a_1'$ mit $1^2 + 2^2$ zusammengesetzt $m_1^2 = 1^2$, $n_1^2 = 18^2$ geben, und das ist die Zerlegung $7^2 + 4^2$. Ebenso muß, da $3^2 + 2^2$ die einzige Zerlegung von $a_2'$ ist, $(3^2 + 2^2)(1^2 + 2^2)$ die Zerlegung $m_2^2 + n_2^2$ liefern. In der Tat gelangt man zu diesem Resultate, wenn man in den Gleichungen
$m_1 = p_1\delta + q_1\varepsilon$, $n_1 = p_1\varepsilon - q_1\delta$, $m_2 = p_2\delta + q_2\varepsilon$, $n_2 = p_2\varepsilon - q_2\delta$ $p_1 = 7$, $q_1 = -4$, $p_2 = 3$, $q_2 = -2$, $\delta = 1$, $\varepsilon = 2$ setzt, nämlich zu den Gleichungen $m_1 = -1$, $n_1 = 18$, $m_2 = -1$, $n_2 = 8$.

Handelt es sich um den gemeinschaftlichen Grundfaktor $13 = 3^2 + 2^2$, so ist $a_1' = 25 = 3^2 + 4^2$, $a_2' = 5 = 1^2 + 2^2$, und man erhält für $p_1 = 3$, $q_1 = -4$, $p_2 = 1$, $q_2 = -2$, $\delta = 3$, $\varepsilon = 2$ das Ergebnis $m_1 = 1$, $n_1 = 18$, $m_2 = -1$, $n_2 = 8$. Das Produkt $(1^2 + 18^2)(1^2 + 8^2)$ selbst liefert die beiden Quadratsummen $145^2 + 10^2$ und $143^2 + 26^2$; die Summanden der einen haben den Grundfaktor 5, die der anderen den Grundfaktor 13 gemein.

Die Zahlen 325 und 65 haben aber auch noch die zusammengesetzte Hypotenuse 65 als Faktor gemein. Sollen nun die Zahlen eines der Zahlenpaare $m_1m_2 + n_1n_2$, $m_1n_2 - m_2n_1$ und $m_1m_2 - n_1n_2$, $m_1n_2 + m_2n_1$ diesen Faktor gemein haben, so muß $a_1' = 5 = 1^2 + 2^2$ mit $\gamma = 1^2 + 8^2$ zusammengesetzt die Zerlegung $1^2 + 18^2$ liefern, was nicht der Fall ist. Man sieht also, daß der Satz für einen gemeinschaftlichen zusammengesetzten Faktor keine Giltigkeit hat, was auch natürlich ist, da dieser Faktor zwei Zerlegungen zuläßt und diejenige, die $m_2^2 + n_2^2$ liefert, hier $m_2^2 + n_2^2$ selbst, nämlich $1^2 + 8^2$, nicht mit einer der Zerlegungen von $a_1'$, hier mit der einzigen $1^2 + 2^2$, die Werte $m_1^2 = 1^2$, $n_1^2 = 18^2$ zu liefern braucht. Daraus folgt aber nicht, daß es keine Zerlegungen von $a_1$ und $a_2$ gäbe, deren Zusammensetzung die Summe der Quadrate zweier Zahlen liefert, die eine zusammengesetzte Zahl als gemeinschaftlichen Faktor enthalten. Wäre $m_1^2 + n_1^2 = 1^2 + 18^2$, aber $m_2^2 + n_2^2$ nicht gleich $1^2 + 8^2$ sondern gleich $7^2 + 4^2$, so würde man in der Tat zu einer Summe von Quadraten zweier Zahlen, die den Faktor 65 gemein haben, gelangen; es ist nämlich $(1^2 + 18^2)(7^2 + 4^2) = 65^2 + 130^2 = 79^2 + 122^2$.

Wie man aber auch 325 und 65 zerlegen (von 325 giebt es noch die Zerlegung $17^2 + 6^2$) und die Zerlegungen kombiniren mag, stets wird sich sowohl 5 als auch 13 in den Summanden der einen der beiden sich ergebenden Quadratsummen vorfinden, in denen der anderen nicht, sei es, daß die Summanden einer und derselben Quadratsumme beide Grundfaktoren gemein haben, dann sind die der anderen relative Primzahlen, geben also eine Zerlegung, oder daß 5 in den Summanden der einen, 13 in denen der anderen enthalten ist.

**§ 18.** Aus § 17 erhält man durch Umkehrung den Satz:

Wenn sowohl die Zahlen $m_1m_2 + n_1n_2$ und $m_1n_2 - m_2n_1$ als auch die Zahlen $m_1m_2 - n_1n_2$ und $m_1n_2 + m_2n_1$ relative Primzahlen sind, so sind auch die Zahlen $m_1^2 + n_1^2$ und $m_1^2 + n_1^2$ relative Primzahlen.

**§ 19.** Da die Seiten der Gleichung

$$(m_1^2 + n_2^2)(m_2^2 + n_1^2) = (m_1m_2 + n_1n_2)^2 + (m_1n_2 - m_2n_1)^2$$

weder ihren Inhalt noch ihre Form ändern, wenn man $m_1$ mit $m_2$ und $n_1$ mit $n_2$ vertauscht, oder mit andern Worten: da die Bestandteile der Zerlegungen $m_1^2 + n_1^2$ und $m_2^2 + n_2^2$ in gleicher Weise an der Bildung der Quadratsumme $(m_1m_2 + n_1n_2)^2 + (m_1n_2 - m_2n_1)^2$, beteiligt sind, so muß, wenn $m_1m_2 + n_1n_2$ und $m_1n_2 - m_2n_1$ einen Faktor $\delta$ gemein haben, nach dem Satze vom zureichenden Grunde $\delta$ ein Faktor sowohl von $m_1^2 + n_1^2$ als auch von $m_2^2 + n_2^2$ sein. Dasselbe gilt, wenn die Zahlen $m_1m_2 - n_1n_2$ und $m_1n_2 + m_2n_1$ einen Faktor $\varepsilon$ gemein haben. Also hat man den Satz:

Wenn die Zahlen eines der Zahlenpaare $m_1m_2 + n_1n_2$, $m_1n_2 - m_2n_1$ und $m_1m_2 - n_1n_2$, $m_1n_2 + m_2n_1$ einen Faktor gemein haben, so ist dieser auch ein Faktor sowohl von $m_1^2 + n_1^2$ als auch von $m_2^2 + n_2^2$.

**§ 20.** Hieraus folgt umgekehrt:

Wenn die Zahlen $m_1^2 + n_1^2$ und $m_2^2 + n_2^2$ relative Primzahlen sind, so sind sowohl die Zahlen des Zahlenpaars $m_1m_2 + n_1n_2$, $m_1n_2 - m_2n_1$, als auch die des Zahlenpaars $m_1m_2 - n_1n_2$, $m_1n_2 + m_2n_1$ ebenfalls relative Primzahlen.

**§ 21.** Obschon die Zahlen

$$a_1 = m_1^2 + n_1^2, \quad a_2 = m_2^2 + n_2^2$$

Hypotenusen sind, so folgt aus der Gleichung

$$a = a_1a_2 = (m_1m_2 + n_1n_2)^2 + (m_1n_2 - m_2n_1)^2 = (m_1m_2 - n_1n_2)^2 + (m_1n_2 + m_2n_1)^2,$$

z. B. aus der Gleichung

$$a = (1^2 + 18^2)\ (1^2 + 8^2) = 145^2 + 10^2 = 143^2 + 26^2$$

noch nicht, daß a eine Hypotenuse ist, weil die Summanden der Quadratsummen nicht relative Primzahlen sind. So ist $245 = 7^2 + 14^2$ in der That keine Hypotenuse. Darum kann man vorläufig noch nicht behaupten, daß das Produkt zweier Hypotenusen ebenfalls eine Hypotenuse sei, wohl aber auf Grund der Sätze § 17 und § 20 Folgendes:

Das Produkt zweier Hypotenusen, die keinen oder nur einen Grundfaktor gemein haben, ist ebenfalls eine Hypotenuse.

**§ 22.** Sind die Zahlen $a_1$, $a_2$, $a_3$, . . . beliebige Hypotenusen, so kann man sie, soweit sie nicht schon Primzahlen sind, in Produkte von Primzahlen, also $a = a_1a_2a_3 \ldots$ in ein Produkt der Primzahlen $\alpha_1$, $\alpha_2$, $\alpha_3$, $\alpha_4$, . . . . zerlegen, die nach § 15 sämtlich Hypotenusen sind, aber nicht alle verschieden zu sein brauchen. Wendet man alsdann wiederholt den vorigen Satz [auf $\alpha_1\alpha_2$, $(\alpha_1\alpha_2)\alpha_3$, $(\alpha_1\alpha_2\alpha_3)\alpha_4$ . . . . ] an, so gelangt man zu dem Ergebnisse:

Jedes Produkt beliebiger Hypotenusen ist ebenfalls eine Hypotenuse.

**§ 23.** Jetzt läßt sich der Satz § 15 dahin erweitern:

Jeder Teiler einer Hypotenuse ist ebenfalls eine Hypotenuse.

**§ 24.** Sind alle Hypotenusen $a_1$, $a_2$, $a_3$, . . . gleich, so ergiebt sich der Satz:

Jede Potenz einer Hypotenuse ist ebenfalls eine Hypotenuse.

§ 25. Ist die Hypotenuse a eine Primzahl, so läßt sie nach § 10 nur eine Zerlegung zu. Folglich haben nach § 17 auch die Hypotenusen $aa = a^2$, $a^2a = a^3$, . . . $a^{k-1}a = a^k$, also jede Potenz von a nur eine Zerlegung. Daher kann man den Satz in § 10 mit Rücksicht auf die Erklärung der einfachen Hypotenuse dahin erweitern:

Jede einfache Hypotenuse läßt nur eine Zerlegung zu.

§ 26. Der vorige Satz läßt sich umkehren:

Jede Hypotenuse, die nur eine Zerlegung zuläßt, ist einfach.

Denn wäre sie zusammengesetzt, so hätte sie, da sie sich als ein Produkt zweier relativen Primzahlen darstellen ließe, die nach § 23 Hypotenusen wären, nach § 20 zwei Zerlegungen.

§ 27. Jede zusammengesetzte Hypotenuse läßt mindestens zwei Zerlegungen zu.

Denn ließe die Hypotenuse nur eine Zerlegung zu, so wäre sie nach § 26 einfach.

§ 28. Jede Hypotenuse mit mehr als einer Zerlegung ist zusammengesetzt.

Denn wäre eine solche Hypotenuse einfach, so ließe sie nach § 25 nur eine Zerlegung zu.

§ 29. Sind

$$a_1 = m_1^2 + n_1^2, \quad a_2 = m_2^2 + n_2^2$$

verschiedene einfache Hypotenusen, so haben sie keinen Faktor gemein. Folglich liefert das Produkt $(m_1^2 + n_1^2)(m_2^2 + n_2^2)$ nach § 20 zwei verschiedene Zerlegungen. Diese sind aber auch die einzigen, weil die Zerlegungen $m_1^2 + n_1^2$ und $m_2^2 + n_2^2$ von $a_1$ und $a_2$ nach § 25 eindeutig bestimmt sind.

Das Produkt zweier verschiedenen einfachen Hypotenusen ist eine Hypotennse, die zwei, aber auch nur zwei Zerlegungen zuläßt.

§ 30. Es seien

$$a_1 = m_1^2 + n_1^2, \quad a_2 = m_2^2 + n_2^2, \quad a_3 = m_3^2 + n_3^2, \ldots a_k = m_k^2 + n_k^2$$

verschiedene einfache Hypotenusen und

$$a = a_1 a_2 a_3 \ldots . a_k.$$

Die Anzahl der Zerlegungen von $a_1$ ist gleich $1 = 2^0$, die der Zerlegungen der Hypotenuse $a_1 a_2$ ist gleich $2 = 2^1$. Angenommen die Anzahl der möglichen verschiedenen Zerlegungen der Hypotenuse $a_1 a_2 a_3 \ldots . a_p$ ist gleich $2^{p-1}$, so ist, da jede dieser Zerlegungen mit $a_{p+1} = m_{p+1}^2 + n_{p+1}^2$ zusammengesetzt zwei verschiedene Zerlegungen liefert, die Anzahl der möglichen verschiedenen Zerlegungen der Hypotenuse $a_1 a_2 a_3 \ldots a_p a_{p+1}$ gleich $2^{p-1} \cdot 2 = 2^p$. Also ist die Anzahl der verschiedenen möglichen Zerlegungen von a gleich $2^{k-1}$.

Eine Hypotenuse, die aus k verschiedenen einfachen Hypotenusen zusammengesetzt ist, läßt $2^{k-1}$ verschiedene Zerlegungen zu.

§ 31. Da die beliebige Zerlegung $m_x^2 + n_x^2$ die zur Hypotenuse gehörigen Katheten $m_x^2 - n_x^2$ und $2m_x n_x$, die keinen gemeinschaftlichen Faktor haben, liefert, so hat man nach § 30 den Satz:

Wenn eine Hypotenuse aus k einfachen verschiedenen Hypotenusen zusammengesetzt ist, so ist die Anzahl der zur Hypotenuse gehörigen Paare von Katheten, die relative Primzahlen sind, gleich $2^{k-1}$.

**§ 32.** Ist a′ ein Teiler der Hypotenuse a, also nach § 23 ebenfalls eine Hypotenuse, und

$$a = a'a'', \quad a' = m'^2 + n'^2, \quad a'^2 = (m'^2 - n'^2)^2 + (2m'n')^2,$$

so ist

$$a^2 = (a'a'')^2 = [(m'^2 - n'^2)a'']^2 + [(2m'n')a'']^2.$$

Jeder Teiler einer Hypotenuse liefert ein zur Hypotenuse gehöriges Paar von Katheten, die einen Faktor gemein haben.

**§ 33.** Es seien $a_1, a_2, a_3, \ldots a_k$ einfache Hypotenusen, $\alpha_1, \alpha_2, \alpha_3, \ldots \alpha_k$ Primzahlen und

$$a_1 = \alpha_1^{p_1}, \quad a_2 = \alpha_2^{p_2}, \quad a_3 = \alpha_3^{p_3}, \quad \ldots \; a_k = \alpha_k^{p_k},$$

$$a = \alpha_1^{p_1} . \alpha_2^{p_2} . \alpha_3^{p_3} . \ldots . \alpha_k^{p_k}.$$

Die Teiler von a, die einfache Hypotenusen sind, sind die verschiedenen Potenzen der Primzahlen $\alpha_1, \alpha_2, \alpha_3 \ldots . \alpha_k$, nämlich $\alpha_1, \alpha_1^2, \alpha_1^3, \ldots \alpha_1^{p_1}$; $\alpha_2, \alpha_2^2, \alpha_2^3, \ldots \alpha_2^{p_2}$ u. s. w., ihre Anzahl also gleich

$$p_1 + p_2 + p_3 + \ldots . + p_k = \Sigma \binom{k}{1},$$

wenn man allgemein die Summe der Produkte, die man erhält, wenn man die xte Klasse der Kombinationen (ohne Wiederholung) der Exponenten bildet, durch $\Sigma \binom{k}{x}$ bezeichnet. Angenommen die Anzahl der Teiler der Hypotenuse, die q verschiedene Grundfaktoren enthalten, sei gleich $\Sigma \binom{k}{q}$. Die Teiler, die $q+1$ verschiedene Grundfaktoren enthalten, erhält man, wenn man die Teiler mit q verschiedenen Grundfaktoren mit den verschiedenen Potenzen der Grundfaktoren, die sie nicht enthalten, multipliziert, nämlich den Teiler, der die $k-q$ letzten Grundfaktoren nicht enthält, mit den $p_{q+1}$ verschiedenen Potenzen von $\alpha_{q+1}$, die Teiler, die die $k-q-1$ letzten Grundfaktoren nicht enthalten, mit den $p_{q+2}$ verschiedenen Potenzen von $\alpha_{q+2}$, die Teiler, die die $k-q-2$ letzten Grundfaktoren nicht enthalten, mit den $p_{q+3}$ verschiedenen Potenzen von $\alpha_{q+3}$ u. s. w., die Teiler, die die beiden letzten Grundfaktoren nicht enthalten, mit den $p_{k-1}$ verschiedenen Potenzen von $\alpha_{k-1}$ und schließlich die Teiler, die den letzten Grundfaktor nicht enthalten, mit den $p_k$ verschiedenen Potenzen von $\alpha_k$. Folglich ist die Anzahl der Teiler mit $q+1$ verschiedenen Grundfaktoren gleich der Summe

$$[\Sigma \tbinom{q}{q}]\, p_{q+1} + [\Sigma \tbinom{q+1}{q}]\, p_{q+2} + [\Sigma \tbinom{q+2}{q}]\, p_{q+3} + \ldots + [\Sigma \tbinom{k-2}{q}]\, p_{k-1} + [\Sigma \tbinom{k-1}{q}]\, p_k.$$

Diese Summe ist aber die Summe der Produkte, die man erhält, wenn man die $(q+1)$ste Klasse der Kombinationen der Exponenten bildet, ist also gleich $\Sigma \binom{k}{q+1}$. Folglich ist allgemein die Anzahl der Teiler, die x verschiedene Grundfaktoren enthalten, gleich $\Sigma \binom{k}{x}$. Da nach § 32 jeder dieser Teiler $2^{x-1}$ verschiedene Zerlegungen zuläßt, so liefern alle Teiler mit x verschiedenen Grundfaktoren $2^{x-1} \Sigma \binom{k}{x}$ Paare von Katheten. Hieraus ergiebt sich der Satz:

Zu jeder aus k verschiedenen einfachen Hypotenusen zusammengesetzten Hypotenuse gehören

$$2^0 \Sigma \tbinom{k}{1} + 2^1 \Sigma \tbinom{k}{2} + 2^2 \Sigma \tbinom{k}{3} + 2^3 \Sigma \tbinom{k}{4} + \ldots + 2^{k-1} \Sigma \tbinom{k}{k}$$

verschiedene Paare von Katheten. Die Katheten von $2^{k-1}$ Paaren sind relative Primzahlen, die der übrigen nicht.

Beispiele. Es sei a eine Hypotenuse und

$$a = \alpha_1^{p_1} . \alpha_2^{p_2} . \alpha_3^{p_3} . \alpha_4^{p_4} . \alpha_5^{p_5}.$$

$p_1 + p_2 + p_3 + p_4 + p_5 = \Sigma \binom{5}{1}$,

$p_1p_2 + (p_1 + p_2)p_3 + (p_1 + p_2 + p_3)p_4 + (p_1 + p_2 + p_3 + p_4)p_5 = \Sigma \binom{5}{2}$,

$p_1p_2p_3 + (p_1p_2 + p_1p_3 + p_2p_3)p_4 + (p_1p_2 + p_1p_3 + p_1p_4 + p_2p_3 + p_2p_4 + p_3p_4)p_5 = \Sigma \binom{5}{3}$,

$p_1p_2p_3p_4 + (p_1p_2p_3 + p_1p_2p_4 + p_1p_3p_4 + p_2p_3p_4)p_5 = \Sigma \binom{5}{4}$,

$p_1p_2p_3p_4p_5 = \Sigma \binom{5}{5}$.

Die Anzahl der Teiler, die einfache Hypotenusen sind, ist $\Sigma\binom{5}{1}$, die Anzahl der Teiler mit zwei einfachen Hypotenusen $\Sigma\binom{5}{2}$, die Anzahl der Teiler mit drei einfachen Hypotenusen $\Sigma\binom{5}{3}$, die Anzahl der Teiler mit vier einfachen Hypotenusen $\Sigma\binom{5}{4}$ und die Anzahl der Teiler mit fünf einfachen Hypotenusen $\Sigma\binom{5}{5}$. Also ist die Anzahl der Kathetenpaare

$$2^0\cdot\Sigma\binom{5}{1}+2^1\cdot\Sigma\binom{5}{2}+2^2\cdot\Sigma\binom{5}{3}+2^3\cdot\Sigma\binom{5}{4}+2^4\cdot\Sigma\binom{5}{5}$$

Zur Hypotenuse $5^3\cdot13^2\cdot17^2$ gehören

$$1\cdot(3+2+2)+2\cdot(3\cdot2+3\cdot2+2\cdot2)+4\cdot3\cdot2\cdot2,$$

also 87 Kathetenpaare; nur die Katheten von 4 Paaren sind relative Primzahlen.

**§ 34.** Sind die Hypotenusen des vor. Satzes, aus denen die Hypotenuse a zusammengesetzt ist, Primzahlen, so hat man sämtliche Exponenten gleich 1 zu setzen. Dadurch werden auch sämtliche Produkte in $\Sigma\binom{k}{x}$ gleich 1, ihre Summen als gleich ihrer Anzahl $\binom{k}{x}$. Oder: Die Teiler der Hypotenuse a, die x verschiedene Grundfaktoren enthalten, bilden die xte Klasse der der Kombinationen der Grundfaktoren selbst (nicht ihrer Exponenten), deren Anzahl $\binom{k}{x}$ ist; die letzte Klasse dieser Kombinationen liefert die Paare von Katheten, die relative Primzahlen sind. Also hat man den Satz:

Zu jeder aus k verschiedenen Primzahlen zusammengesetzten Hypotenuse gehören

$$2^0\binom{k}{1}+2^1\binom{k}{2}+2^2\binom{k}{3}+2^3\binom{k}{4}+\ldots.+2^{k-1}\binom{k}{k}$$

verschiedene Paare von Katheten. Die Katheten von $2^{k-1}\binom{k}{k}$ Paaren sind relative Primzahlen, die der übrigen nicht.

Die Anzahl der Te… ($\binom{5}{1}$), die Anzahl der Teiler mit zwei einfachen Hypotenusen …fachen Hypotenusen $\Sigma\binom{5}{3}$, die Anzahl der Teiler mit vier …zahl der Teiler mit fünf ein-fachen Hypotenusen $\Sigma\binom{5}{5}$.

$2^0 \cdot \Sigma($… $2^4 \cdot \Sigma\binom{5}{5}$

Zur Hypotenuse 5…

$1 \cdot (3$… $\cdot 3 \cdot 2 \cdot 2$,

also 87 Kathetenpaare; nur … Primzahlen.

**§ 34.** Sind die … die Hypotenuse a zusammengesetzt ist, Primzahlen, so …zu setzen. Dadurch werden auch sämtliche Produkte in …ch ihrer Anzahl $\binom{k}{x}$. Oder: Die Teiler der Hypotenuse …lten, bilden die xte Klasse der der Kombinationen der Gru…uten), deren Anzahl $\binom{k}{x}$ ist; die letzte Klasse dieser Kombinati…elative Primzahlen sind. Also hat man den Satz:

Zu jeder aus k …mengesetzten Hypotenuse gehören

$2^0\binom{k}{1}$… $2^{k-1}\binom{k}{k}$

verschiedene Paare von …$^1\binom{k}{k}$ Paaren sind relative Primzahlen, die der üb…