Über die Auflösung der unbestimmten Gleichung $x^n + y^n = z^n$ in rationalen Zahlen.

Von **Otto Schier.**

(Vorgelegt in der Sitzung am 4. März 1880.)

Einleitung.

Seitdem die besonderen Eigenschaften der ganzen Zahlen Gegenstand der wissenschaftlichen Forschung geworden sind, bildete die Frage, ob die Summe zweier n-ter Potenzen wieder eine n-te Potenz geben könne, einen Hauptpunkt zahlentheoretischer Untersuchungen.

Pythagoras schon gab eine Regel an, nach welcher Zahlen gefunden werden, deren Quadrate addirt, ein vollständiges Quadrat geben, und Diophant behandelt in seinem fünften und sechsten Buche Aufgaben, die sich auf die „pythagoräischen Zahlen" beziehen.

Fermat bemerkt in seinen Noten zu Diophant, dass die unbestimmte Gleichung

$$x^n + y^n = z^n$$

für $n > 2$ in rationalen Zahlen nicht lösbar sei, ohne jedoch den Ausspruch nachzuweisen.

Spätere Versuche, diesen Beweis zu erbringen, beschränkten sich auf besondere Fälle; so gab Euler den Beweis für $n = 3$, Lejeune-Dirichlet für $n = 5$, und in Klügel's mathematischem Wörterbuche findet sich ein solcher für $n = 4$ (Band 5, Seite 1143), welch letzterer jedoch durch seine unlogischen Schlüsse nicht geeignet ist, die behauptete Unmöglichkeit klar darzulegen.

Vorliegende Abhandlung nun hat den Zweck, die erwähnte Fermat'sche Äusserung allgemein nachzuweisen.

Nothwendige Zusammensetzung der Zahlen x, y und z für eine Primzahl n.

Soll die Gleichung

$$x^n + y^n = z^n$$

allgemein bestehen, so müssen x, y und z relative Primzahlen sein.

Würde in den drei Zahlen ein gemeinschaftlicher Theiler vorkommen, so könnte durch ihn gekürzt werden, und es ist ersichtlich, dass, wenn zwei von ihnen ein gemeinschaftliches Mass hätten, dies auch ein Mass für die dritte Zahl sein müsste, denn:

$$(r\,u)^n + y^n = (r\,v)^n \text{ gibt } y^n = r^n\,(v^n - u^n)$$

daher auch y ein Vielfaches von r.

Die Zahlen x, y und z werden demnach in der folgenden Untersuchung als prim gegeneinander vorausgesetzt.

Wird in der unbestimmten Gleichung

$$x^n + y^n = z^n \quad \ldots\ldots (\text{I}$$

n als absolute Primzahl angenommen, so besteht für jeden Werth der drei Zahlen, nach dem Fermat'schen Lehrsatze, die Relation:

$$\left.\begin{aligned} x^n &\equiv x \\ y^n &\equiv y \\ z^n &\equiv z \end{aligned}\right\} \pmod{n}$$

daher auch

$$x^n + y^n - z^n \equiv x + y - z \pmod{n}.$$

Da nun nach (I

$$x^n + y^n = z^n \text{ oder } x^n + y^n - z^n = o$$

daher auch $x^n + y^n - z^n \equiv o \pmod{n}$ ist, so muss auch $x+y-z \equiv o \pmod{n}$ sein.

Diese Congruenz kann nur bestehen für

$$x + y - z = o,$$

was jedoch mit Rücksicht auf (I nicht möglich ist, oder für

$$x + y - z = n\,k,$$

wobei k eine positive, ganze von o verschiedene Zahl bedeutet.

Daraus folgt:

$$x + y = z + n\,k \quad \ldots\ldots \text{(II.}$$

Diese Gleichung zeigt, dass

$$x^n + y^n = z^n$$

für Werthe von x, y und z, welche kleiner wären als n, ohneweiters nicht bestehen kann; denn da $z > x$ oder y, und $n > x$ oder y, so ist auch

$$z + n\,k > x + y$$

und (II ist nicht möglich.

Aus (II ist aber auch noch weiters ersichtlich, dass $x + y$ kein Multiplum von n sein könne; denn sonst wäre es auch z, und wird aus (II

$$x = z + n\,k - y$$

in die Gleichung (I gesetzt, und die n-te Potenz entwickelt, so zeigt sich, dass die Gleichung

$$(z + n\,k - y)^n + y^n = z^n$$

nur dann bestehen kann, wenn y ein Vielfaches von n ist, was auch eine Theilbarkeit von x durch n zur Folge hätte, wodurch der Annahme, dass x, y und z relative Primzahlen sind, widersprochen würde.

Werden nun in (II beide Theile zur n-ten Potenz erhoben, und nach dem binomischen Lehrsatze entwickelt, so ist:

$$(x + y)^n = z + n\,k)^n$$

$$x^n + \binom{n}{1} x^{n-1} y + \qquad + \binom{n}{1} x\, y^{n-1} + y^n =$$

$$= z^n + \binom{n}{1} x^{n-1}\, n\,k + \qquad + \binom{n}{1} z\, n^{n-1}\, k^{n-1} + n^n\, k^n$$

dabei heben sich x^n, y^n und z^n nach (I auf.

Da ferner x als Primzahl angenommen wurde, so enthalten sämmtliche Binominalcoëfficienten den Faktor n, durch den also gekürzt werden kann, und es ist:

$$x^{n-1}\, y + \frac{n-1}{2} x^{n-2}\, y^2 + \qquad + \frac{n-1}{2} x^2\, y^{n-2} + x\, y^{n-1} =$$

$$= z^{n-1}\, n\,k + \frac{n-1}{2} z^{n-2}\, n^2\, k^2 + \qquad +$$

$$+ \frac{n-1}{2} z^2\, n^{n-2}\, k^{n-2} + z\, n^{n-1}\, k^{n-1} + n^{n-1}\, k^n$$

Die rechte Seite der Gleichung hat noch immer den gemeinschaftlichen Theiler n, und muss daher auch die linke Seite durch n theilbar sein. Werden auf der linken Seite die Glieder mit gleichen Coëfficienten vereinigt

$$x\,y\,(x^{n-2}+y^{n-2})+\frac{n-1}{2}\,x^2\,y^2\,(x^{n-4}+y^{n-4})+$$

$$+\frac{n-1}{2}\cdot\frac{n-2}{3}\,x^3\,y^3\,(x^{n-6}+y^{n-6})+$$

so ist die Theilbarkeit der ganzen Summe abhängig von der Theilbarkeit der in allen Summanden vorkommenden Faktoren $x\,y$ und $x+y$.

Da nun, wie früher gezeigt wurde, $x+y$ kein Vielfaches von x sein kann, so muss diese Zahl in $x\,y$ enthalten sein, und da diese prim gegen einander sind, so kann nur eine von ihnen, z. B. y den Faktor n haben, während wegen

$$x^n+y^n=z^n$$

x und y gleiche Reste nach n geben müssen.

Die drei Zahlen x, y und z bekommen demnach folgende Form:

$$\begin{aligned} x &= n\,h+r \\ y &= n\,l \\ z &= n\,p+r \end{aligned} \qquad \text{(III}$$

Ist n eine Primzahl >2, so kann die Gleichung $x^n+y^n=z^n$ nicht bestehen.

Wird in der ursprünglichen Gleichung

$$x^n+y^n=z^n$$

gesetzt $z=x+u$, so ist

$$x^n+y^n=x^n+\binom{n}{1}x^{n-1}\,u+\qquad+\binom{n}{1}x\,u^{n-1}+u^n$$

oder

$$\frac{y^n-u^n}{u}=\binom{n}{1}x^{n-1}+\qquad+\binom{n}{1}x\,u^{n-2}$$

Statt u wieder $z - x$ substituirt

$$\frac{y^n - (z-x)^n}{z-x} = \binom{n}{1} x^{n-1} + \binom{n}{2} x^{n-2}(z-x) + \\ + \binom{n}{1} x (z-x)^{n-2}$$

Werden nun die in (III gefundenen Werthe in diese Gleichung gesetzt, so bekommt sie die Form:

$$\frac{n^n l^n - n^n (p-h)^n}{n(p-h)} = n^{n-1} \cdot \frac{l^n - (p-h)^n}{p-h} =$$

$$= \binom{n}{1}(nh+r)^{n-1} + \binom{n}{2}(nh+r)^{n-2} n(p-h) + \\ + \qquad + \binom{n}{1}(nh+r) n^{n-2}(p-h)^{n-2}.$$

Jedes Glied dieser Gleichung lässt sich durch die Primzahl n kürzen, und man erhält:

$$n^{n-2} \cdot \frac{l^n - (p-h)^n}{ph} = (nh+r)^{n-1} + \frac{n-1}{2}(nh+r)^{n-2} n(p-h) \\ + \cdot \qquad + (nh+r) n^{n-2}(p-h)^{n-2} \cdot \qquad \text{(IV.}$$

In dieser Schlussgleichung enthalten, ausser $(nh+r)^{n-1}$, alle Glieder nochmals den Faktor n.

Da dies aber ungereimt ist, so kann die Gleichung (IV nur dann bestehen, wenn nach der Abkürzung durch n alle n als Coëfficienten verschwinden, insbesondere wenn $n^{n-2} = 1$ ist, was nur für $n = 1$ oder 2 möglich is; für alle Zahlen > 2 enthält die Gleichung (IV und mit ihr (I einen Widerspruch, ist somit unmöglich.

Nachweis für zusammengesetzte Zahlen.

Für Exponenten, welche durch Multiplication von Primfaktoren > 2 entstanden sind, ist ein specieller Nachweis überflüssig, denn

$$x^{mn} + y^{mn} = z^{mn} \text{ ist } (x^m)^n + (y^m)^n = (z^m)^n,$$

und wurde für $n > 2$ die Unmöglichkeit bereits dargethan.

Anders verhält es sich mit

$$x^{2n} + y^{2n} = z^{2n}$$

welche Gleichung auch

$$(x^n)^2 + (y^n)^2 = (z^n)^2$$

geschrieben werden kann.

In jeder unbestimmten quadratischen Gleichung

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

müssen die Zahlen die Zusammensetzung haben:

$$a = u^2 - v^2$$
$$b = 2\,u\,v$$
$$c = u^2 + v^2,$$

daher in vorliegendem Falle

$$x^n = u^2 - v^2 = (u + v)\,(u - v)$$
$$y^n = (2u)\,v$$
$$z^n = u^2 + v^2$$

Da nun $u + v$ gegen $u - v$, und $2u$ gegen v relativ prim sind, so muss jede dieser Zahlen selbst eine n-te Potenz sein, wenn ihr Produkt eine sein soll, daher

$$u + v = r^n \qquad 2u = \rho^n. \qquad \text{(V}$$
$$u - v = s^n \qquad v = \sigma^n$$

woraus $\rho^n = r^n + s^n$ folgt, eine Gleichung, welche für $n > 2$ nicht bestehen kann.

Nachweis für Exponenten, die Potenzen von 2 sind.

Wird in den Gleichungen (V $n = 2$ gesetzt, so folgt durch Substitution von ρ^2 und σ^2

$$\frac{\rho^2}{2} - \sigma^2 = s^2, \text{ oder } \rho^2 = 2s^2 + 2\sigma^2.$$

Wird ferner $\sigma > s$ angenommen, so ist auch $\rho > 2s$, und man kann setzen:

$$(2\,s + \psi)^2 = 2\,s^2 + 2\,(s + \varphi)^2$$
$$4\,s^2 + 4\,s\,\psi + \psi^2 = 4\,s^2 + 4\,s\,\varphi + 2\varphi^2$$
$$4\,s\,\psi + \psi^2 = 4\,s\,\varphi + 2\,\varphi^2$$
$$2\,s\,\psi + \frac{\varphi^2}{2} = 2\,s\,\psi + \varphi^2$$

daher

$$\varphi = -s \pm \sqrt{s^2 + 2s\psi + \frac{\psi^2}{2}}.$$

Da jedoch der Ausdruck unter dem Wurzelzeichen kein vollständiges Quadrat ist, so kann auch φ keine rationale Zahl sein, und die Gleichung

$$x^4 + y^4 = z^4 \qquad \text{(VI}$$

ist in ganzen Zahlen nicht lösbar.

Kann jedoch (VI nicht bestehen, so ist die Gleichung auch für die höheren Potenzen von 2 nicht möglich.

Schlussbemerkung.

Nachdem also gezeigt wurde, dass die Gleichung

$$x^n + y^n = z^n$$

nur für die Zahlen $n = 1$ oder 2 in rationalen Zahlen lösbar ist, bei allen grösseren Primzahlen, zusammengesetzten Exponenten und Potenzen von 2 sich jedoch Widersprüche ergeben, welche das Bestehen der Gleichung unmöglich machen, so ist die Induction eine vollständige, und der Beweis allgemein geführt.