

Werk

Titel: Vorlesungen über Zahlentheorie

Autor: Dirichlet, Peter

Verlag: Vieweg

Ort: Braunschweig

Jahr: 1871

Kollektion: Mathematica

Digitalisiert: Niedersächsische Staats- und Universitätsbibliothek Göttingen

Werk Id: PPN30976923X

PURL: <http://resolver.sub.uni-goettingen.de/purl?PPN30976923X>

OPAC: <http://opac.sub.uni-goettingen.de/DB=1/PPN?PPN=30976923X>

LOG Id: LOG_0176

LOG Titel: S. 157. Hauptsatz über die Lösbarkeit dieser Gleichung

LOG Typ: chapter

Terms and Conditions

The Goettingen State and University Library provides access to digitized documents strictly for noncommercial educational, research and private purposes and makes no warranty with regard to their use for other purposes. Some of our collections are protected by copyright. Publication and/or broadcast in any form (including electronic) requires prior written permission from the Goettingen State- and University Library.

Each copy of any part of this document must contain these Terms and Conditions. With the usage of the library's online system to access or download a digitized document you accept the Terms and Conditions.

Reproductions of material on the web site may not be made for or donated to other repositories, nor may be further reproduced without written permission from the Goettingen State- and University Library.

For reproduction requests and permissions, please contact us. If citing materials, please give proper attribution of the source.

Contact

Niedersächsische Staats- und Universitätsbibliothek Göttingen
Georg-August-Universität Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen
Germany
Email: gdz@sub.uni-goettingen.de

§. 157.

Durch den zuletzt bewiesenen Satz ist offenbar die Frage nach der eigentlichen Lösbarkeit der Gleichung

$$ax^2 + by^2 + cz^2 = 0 \quad (1)$$

auf den Fall zurückgeführt, in welchem keine der relativen Primzahlen a, b, c durch ein Quadrat theilbar ist; als eine erforderliche Bedingung für die Lösbarkeit ist ferner im vorigen Paragraphen (II) erkannt, dass die Zahlen $-bc, -ca, -ab$ resp. quadratische Reste von den Zahlen a, b, c sein müssen, und ausserdem leuchtet ein, dass die letzteren unmöglich alle dasselbe Vorzeichen haben können. Mit Hülfe einer Reductionsmethode, welche im Wesentlichen von *Lagrange**) herrührt, lässt sich nun wirklich beweisen, dass diese Bedingungen auch die hinreichenden sind, dass also folgender Satz**) besteht:

Sind a, b, c drei von Null verschiedene und durch kein Quadrat theilbare relative Primzahlen, welche nicht alle dasselbe Vorzeichen haben, und sind die Zahlen $-bc, -ca, -ab$ resp. quadratische Reste der Zahlen a, b, c ; so ist die Gleichung (1) eigentlich lösbar.

Zunächst bemerken wir, dass der Satz in dem speciellen Falle richtig ist, wenn einer der Coefficienten, z. B. $a = +1$, ein anderer, z. B. $b = -1$ ist; denn man genügt der Gleichung (1) durch die relativen Primzahlen $x = y = 1, z = 0$.

Um uns nun bequemer ausdrücken zu können, nennen wir, indem wir den absoluten Werth einer Grösse k mit (k) bezeichnen, dasjenige der drei Producte $(bc), (ca), (ab)$, welches der Grösse nach zwischen den beiden anderen liegt, den *Index* der Gleichung (1), und wenn etwa zwei dieser Producte oder alle drei einander gleich sein sollten, so soll unter dem Index der gemeinschaftliche

*) *Sur la solution des problèmes indéterminés du second degré.* Mém. de l'Acad. de Berlin. T. XXIII. 1769. (Œuvres de L. T. II. 1868. p. 375.) — *Additions aux Éléments d'Algèbre par L. Euler.* §. V.

**) *Legendre: Théorie des Nombres*, 3^{me} éd. T. I. §§. III, IV. — *Gauss: D. A.* artt. 294, 295. — Der nachfolgende Beweis lässt sich auf den Fall ausdehnen, dass a, b, c quadratische Divisoren besitzen.

Werth dieser beiden oder aller Producte verstanden werden. Aus dieser Erklärung ergibt sich unmittelbar die Richtigkeit des Satzes für den Fall, dass ihr Index = 1 ist; denn dann muss, wie man leicht erkennt, $(a) = (b) = (c) = 1$ sein, und da die Coefficienten nicht alle dasselbe Vorzeichen haben, so ergibt sich die Lösbarkeit der Gleichung aus der vorausgeschickten Bemerkung.

Um nun den Beweis allgemein zu führen, nehmen wir an, er sei schon geleistet für alle Gleichungen, deren Index kleiner als eine bestimmte positive ganze Zahl J ist, und zeigen, dass der Satz dann auch für alle Gleichungen gelten muss, deren Index = J ist. Gelingt dies, so gilt der Satz allgemein, weil er für $J = 1$ richtig ist.

Es sei daher $J \geq 2$ der Index der Gleichung (1). Nehmen wir an, was der Symmetrie wegen erlaubt ist, es sei $(a) \leq (b) \leq (c)$, also auch $(ab) \leq (ac) \leq (bc)$, so ist $J = (ac)$; wäre nun $(b) = (c)$, so müsste, weil b und c relative Primzahlen sind, $(b) = (c) = 1$ sein, woraus auch $J = 1$ folgen würde, was mit unserer Annahme streitet; mithin ist

$$(a) \leq (b) < (c), (ab) < (ac) = J \leq (bc). \quad (2)$$

Der Annahme nach ist nun $-ab$ quadratischer Rest von c , und folglich kann man eine Zahl r so bestimmen, dass $ar^2 \equiv -b \pmod{c}$, und zugleich $(r) \leq \frac{1}{2}(c)$ wird; setzt man dann

$$ar^2 + b = cC, \quad (3)$$

so wird C eine ganze Zahl, deren absoluter Werth

$$(C) \leq \frac{(a)r^2 + (b)}{(c)} < \frac{1}{4}J + 1 < J \quad (4)$$

ist, weil $(r) \leq \frac{1}{2}(c)$, $(ac) = J \geq 2$, und $(b) < (c)$ ist.

Ist nun $C = 0$, so folgt $b = -ar^2$, also, da b relative Primzahl zu a und durch kein Quadrat theilbar ist, $(r) = 1$ und $b = -a = \pm 1$, und mithin besitzt die Gleichung (1) in diesem Fall wieder die eigentliche Lösung $x = y = 1, z = 0$.

Ist aber C von Null verschieden, so führen wir die Gleichung (1) folgendermaassen auf eine andere von kleinerem Index zurück. Es sei a' der grösste gemeinschaftliche Divisor der drei in der Gleichung (3) vorkommenden Glieder ar^2, b, cC , so ist a' zugleich der grösste gemeinschaftliche Divisor von je zweien dieser Zahlen, so dass die drei Glieder der Gleichung

$$\frac{ar^2}{a'} + \frac{b}{a'} = \frac{cC}{a'}$$

gewiss relative Primzahlen sind. Da nun a' in b aufgeht, also relative Primzahl zu c und zu a ist, so muss a' in C und in r^2 , also auch in r selbst aufgehen, weil a' als Divisor von b durch kein Quadrat theilbar ist. Man kann daher

$$r = a'\alpha, \quad b = a'\beta, \quad C = a'C' = a'c'\gamma^2 \quad (5)$$

setzen, wo γ^2 das grösste in $C' = c'\gamma^2$ aufgehende Quadrat bedeutet; hierdurch geht die Gleichung (3) in die folgende über

$$aa'\alpha^2 + \beta = cc'\gamma^2, \quad (6)$$

deren drei Glieder also relative Primzahlen sind; setzen wir endlich noch

$$b' = a\beta, \quad (7)$$

so sind hierdurch drei Zahlen a', b', c' definirt, welche, wie wir beweisen wollen, dieselben Eigenschaften besitzen, wie die gegebenen Zahlen a, b, c .

Dass erstens keine der Zahlen $a', b', c' = 0$ ist, leuchtet ein, weil $a'b' = a'a\beta = ab$ ist, und c' in C aufgeht. Aus $a'b' = ab$ folgt ferner, dass a', b' relative Primzahlen und durch kein Quadrat theilbar sind, weil a, b dieselben Eigenschaften haben; da ferner γ^2 das grösste in $C' = c'\gamma^2$ aufgehende Quadrat ist, so kann c' durch kein Quadrat theilbar sein; und da die Glieder der Gleichung (6) relative Primzahlen sind, so ist c' auch relative Primzahl zu $aa'\beta = a'b'$.

Die Zahlen a', b', c' können auch nicht alle dasselbe Vorzeichen haben; ist nämlich $ab = a'b'$ negativ, so haben a', b' entgegengesetzte Zeichen; ist aber ab positiv, folglich ca und bc negativ, so ergibt sich aus der Gleichung $ar^2 + b = ca'c'\gamma^2$, dass $a'c'$ negativ ist, dass also a', c' entgegengesetzte Vorzeichen haben.

Da ferner zufolge der Gleichung (6), deren drei Glieder relative Primzahlen sind, die drei Zahlen $\beta cc', ac'a'c', -aa'\beta = -a'b'$ resp. quadratische Reste der drei Zahlen aa', β, c' sein müssen, und da nach Voraussetzung die beiden Zahlen $-bc = -\beta a'c', -ca$ resp. Reste von den beiden Zahlen $a, b = a'\beta$ sind, so ergibt sich hieraus leicht, dass die drei Zahlen $-b'c', -c'a', -a'b'$ resp. Reste der drei Zahlen a', b', c' sind.

Endlich ist $(a'b') = (ab) < J$ zufolge (2), und $(c'a') \leq (c'a')\gamma^2 = (C) < J$ zufolge (4); mithin ist der Index der Gleichung

$$a'x'^2 + b'y'^2 + c'z'^2 = 0$$

gewiss kleiner als J , und folglich ist sie nach unserer obigen Voraussetzung lösbar in relativen Primzahlen x', y', z' ; da nun die Zahlen $a' \alpha x' - \beta y', x' + a \alpha y'$ nicht beide verschwinden, weil sonst auch $x' = y' = 0$ wäre, so kann man

$$mx = a' \alpha x' - \beta y'; \quad my = x' + a \alpha y'; \quad mz = c' \gamma z'$$

setzen, wo m den grössten gemeinschaftlichen Theiler der drei Zahlen rechter Hand bedeutet; hieraus folgt aber mit Beachtung von (5), (6), (7)

$$m^2(ax^2 + by^2 + cz^2) = cc' \gamma^2 (a' x'^2 + b' y'^2 + c' z'^2) = 0,$$

also, da m nicht $= 0$ ist, auch

$$ax^2 + by^2 + cz^2 = 0;$$

da endlich die Zahlen x, y, z keinen gemeinschaftlichen Theiler haben, und keine der Zahlen a, b, c durch ein Quadrat theilbar ist, so sind x, y, z auch relative Primzahlen und bilden folglich eine eigentliche Lösung der Gleichung (1).

Hiermit ist der Schluss vollständig durchgeführt, und also auch der obige Satz allgemein bewiesen. Es leuchtet ferner ein, dass in der successiven Zurückführung der Gleichung (1) auf ähnliche Gleichungen von immer kleinerem Index und endlich auf eine Gleichung, in welcher ein Coefficient $= +1$, ein anderer $= -1$ ist, auch eine Methode liegt, eine Lösung derselben zu finden.

Nachdem für diejenigen Gleichungen, deren Coefficienten durch kein Quadrat theilbar sind, die oben genannten *erforderlichen* Bedingungen zugleich als *hinreichend* für die Existenz eigentlicher Lösungen erkannt sind, so geht aus dem Schlussätze des vorigen Paragraphen hervor, dass genau Dasselbe Statt findet für alle Gleichungen (1), deren Coefficienten von Null verschieden und relative Primzahlen sind. Wir können daher das Gesamtergebn unserer Untersuchungen in dem folgenden wichtigen Satze niederlegen:

Sind die Zahlen a, b, c relative Primzahlen und von Null verschieden, so ist die Gleichung

$$ax^2 + by^2 + cz^2 = 0$$

stets und nur dann in relativen Primzahlen x, y, z lösbar, wenn die Zahlen $-bc, -ca, -ab$ resp. quadratische Reste von den Zahlen a, b, c sind, und diese letzteren nicht alle dasselbe Vorzeichen haben; ist ferner