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_0072
LOG Titel: §. 64. Negative Determinanten. Positive Formen Reduoirte Formen. Jede Form ist einer reducirten Form äquivalent.
LOG Typ: chapter

Contact

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

in eine neue Form über, deren erste beide Coefficienten a', b' mit denen der Form φ' übereinstimmen; und da die neue Form jedenfalls der Form φ äquivalent ist, also auch dieselbe Determinante wie φ und folglich auch wie φ' hat, so muss sie mit φ' identisch sein *).

§. 64.

Wir wenden uns nun zu der Untersuchung, ob zwei gegebene Formen von gleicher *negativer* Determinante $D = -\Delta$ äquivalent sind oder nicht. Zunächst ist zu bemerken, dass die beiden äusseren Coefficienten a und c einer solchen Form

$$\varphi = ax^2 + 2bxy + cy^2$$

nothwendig gleiche Vorzeichen haben, da $ac = b^2 + \Delta$ positiv ist; da ferner

$$a\varphi = (ax + by)^2 + \Delta y^2$$

ist, so zeigt sich, dass alle durch die Form φ darstellbaren Zahlen dasselbe Vorzeichen haben wie a und c. Sind daher (a, b, c) und (a', b', c') äquivalente Formen, so haben die äusseren Coefficienten a', c' der letztern Form dasselbe Zeichen wie die der erstern. Da ferner aus der Aequivalenz dieser beiden Formen auch die der beiden Formen $(-a, -b, -c)$ und $(-a', -b', -c')$ folgt, so können wir uns im Folgenden auf die Betrachtung der sogenannten *positiven* Formen beschränken, in welchen die beiden äusseren Coefficienten das *positive* Vorzeichen haben.

Um nun über die Aequivalenz zweier Formen dieser Art zu entscheiden, vergleicht man sie nicht direct mit einander, sondern

*) Der letzte Grund, weshalb die Substitutionen von der Form $\left(\begin{smallmatrix} 0, & 1 \\ -1, & \delta \end{smallmatrix}\right)$ eine so wichtige Rolle spielen, besteht darin, dass aus ihnen alle anderen sich zusammensetzen lassen; man kann die Coefficienten δ in ihrer Aufeinanderfolge noch gewissen Beschränkungen, namentlich in Bezug auf ihre Vorzeichen, unterwerfen, in der Art, dass jede beliebige Substitution sich auch nur auf eine einzige Weise aus solchen einfachen Substitutionen zusammensetzen lässt. Eine wichtige Anwendung findet diese Bemerkung z. B. in der Theorie der unendlich vielen Formen der ϑ-Functionen. Man erkennt ferner leicht, dass auch der in §. 23 behandelte Algorithmus in der Theorie dieser Substitutionen und ihrer Zusammensetzung enthalten ist. Man vergleiche ferner §. 81.

mit sogenannten *reducirten**) Formen. Man nennt eine Form (A, B, C) von negativer Determinante (und positiven äusseren Coefficienten) eine reducirte, wenn der letzte Coefficient C nicht kleiner ist als der erste A, und der erste A wieder nicht kleiner als der absolute Werth des doppelten mittlern Coefficienten $2B$, in Zeichen, wenn

$$C \geqq A \geqq 2(B)$$

ist, wo (B) den absoluten Werth von B bedeuten soll. Wir beweisen nun zunächst folgenden Satz:

Jede Form von negativer Determinante ist einer reducirten Form äquivalent.

Zu dem Zweck betrachte man die der gegebenen Form (a, b, a') nach rechts benachbarten Formen (a', b', a''); unter diesen wird es immer eine (bisweilen auch zwei) geben, in welchen wenigstens die eine Bedingung $a' \geqq 2(b')$ erfüllt ist. Denn unter allen mit $-b$ nach dem Modul a' congruenten Zahlen giebt es eine b', deren absoluter Werth am kleinsten, und zwar kleiner oder wenigstens nicht grösser als $\frac{1}{2}a'$ ist (falls a' gerade und $b \equiv \frac{1}{2}a'$ (mod. a') ist, würde es zwei solche Zahlen b' geben, nämlich $\pm \frac{1}{2}a'$), so dass jedenfalls $b' \equiv -b$ (mod. a') und ausserdem $2(b') \leqq a'$ ist. Ist b' auf diese Weise gefunden, und $b + b' = -a'\delta$, so geht die Form (a, b, a') durch die Substitution

$$\begin{pmatrix} 0, & 1 \\ -1, & \delta \end{pmatrix}$$

in die nach rechts benachbarte Form (a', b', a'') über, in welcher $2(b') \leqq a'$ ist. Wenn nun gleichzeitig sich herausstellt, dass $a' \leqq a''$ ist, so ist (a', b', a'') eine reducirte Form und der Process geschlossen. Findet sich aber, dass das Gegentheil

$$a' > a''$$

Statt findet, so ist (a', b', a'') noch keine reducirte Form. Mit dieser verfahre man ebenso wie mit (a, b, a'), d. h. man transformire sie in eine nach rechts benachbarte Form (a'', b'', a'''), in welcher $2(b'') \leqq a''$ ist; sobald dann gleichzeitig $a'' \leqq a'''$ ist, so ist (a'', b'', a''') reducirt, folglich der Process geschlossen; ist dies aber nicht der Fall, also

$$a'' > a''',$$

---

*) *Gauss: D. A.* art. 171. Die Bedingung $A \leqq \sqrt{\frac{4}{3}D}$ ist schon eine Folge der beiden anderen (vergl. §. 65).

so setze man den Process in derselben Weise fort. Immer aber wird er nach einer *endlichen* Anzahl von Operationen schliessen; denn wäre dies nicht der Fall, so hätte man eine nie abbrechende Reihe von positiven ganzen Zahlen

$$a', a'', a''' \ldots a^{(n)}, a^{(n+1)} \ldots,$$

in welcher jede folgende mindestens um eine Einheit kleiner wäre, als die unmittelbar vorausgehende, was unmöglich ist, da es immer nur eine endliche Anzahl ganzer positiver Zahlen giebt, welche kleiner sind als eine gegebene.

Auf diese Weise ist bewiesen, dass man endlich zu einer Form $(a^{(n)}, b^{(n)}, a^{(n+1)})$ gelangen muss, in welcher nicht nur $2(b^{(n)}) \leqq a^{(n)}$, sondern auch $a^{(n)} \leqq a^{(n+1)}$ ist.

Zugleich ergiebt sich jedesmal durch die wirkliche Ausführung der Operationen eine Substitution, welche aus den successiven Substitutionen von der Form

$$\begin{pmatrix} 0, & 1 \\ -1, & \delta \end{pmatrix}$$

zusammengesetzt ist, und durch welche die gegebene Form (a, b, a') in die ihr äquivalente reducirte Form $(a^{(n)}, b^{(n)}, a^{(n+1)})$ übergeht.

Nehmen wir als Beispiel die Form (200, 100, 51), deren Determinante $D = -200$ ist, so haben wir $b' \equiv -100 \pmod{51}$ zu setzen und finden hieraus $b' = 2$ und $\delta = -2$; die Substitution, durch welche die gegebene Form (200, 100, 51) transformirt werden muss, ist daher gefunden; da wir aber den ersten und zweiten Coefficienten a' und b' und die Determinante D kennen, so brauchen wir diese Transformation nicht wirklich auszuführen, sondern wir berechnen den letzten Coefficienten a'' durch die Formel

$$a'' = \frac{b'^2 - D}{a'} = a + (b - b')\delta;$$

in unserm Fall finden wir also $a'' = 4$. Die benachbarte Form ist daher (51, 2, 4); sie ist nicht reducirt, weil der letzte Coefficient kleiner ist als der erste. Wir wiederholen daher dieselbe Operation, indem wir $b'' \equiv -2 \pmod{4}$ und folglich $b'' = \pm 2$ setzen, wo beide Zeichen zulässig sind; dann ergiebt sich $\delta' = -1$ oder $= 0$, je nachdem das obere oder untere Zeichen genommen wird, und ausserdem $a''' = 51$; also ist die neue Form $(4, \pm 2, 51)$, und diese ist, mag man das obere oder das untere Zeichen wählen, reducirt. Ferner geht die gegebene Form (200, 100, 51) durch die Substitution