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_0084
LOG Titel: §. 76. Jede Form von positiver Determinante 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

Beispiel 3: Für $D = 35$ ist $\lambda = 5$; also bilden wir die Tabelle

$b = 1$; 34 giebt keine Zerlegung;
$b = 2$; 31 „ „ „
$b = 3$; 26 „ „ „
$b = 4$; 19 „ „ „
$b = 5$; $10 = 1 \cdot 10 = 2 \cdot 5$;

wir erhalten daher 8 reducirte Formen:

$(\pm 1, 5, \mp 10)$, $(\pm 2, 5, \mp 5)$;
$(\pm 10, 5, \mp 1)$, $(\pm 5, 5, \mp 2)$.

Beispiel 4: Für $D = 79$ ist $\lambda = 8$; wir bilden daher folgende Tabelle:

$b = 1$; 78 giebt keine Zerlegung;
$b = 2$; 75 „ „ „
$b = 3$; $70 = 7 \cdot 10$;
$b = 4$; $63 = 7 \cdot 9$;
$b = 5$; $54 = 6 \cdot 9$;
$b = 6$; 43 giebt keine Zerlegung;
$b = 7$; $30 = 2 \cdot 15 = 3 \cdot 10 = 5 \cdot 6$;
$b = 8$; $15 = 1 \cdot 15 = 3 \cdot 5$;

wir erhalten daher 32 reducirte Formen:

$(\pm 7, 3, \mp 10)$, $(\pm 7, 4, \mp 9)$, $(\pm 6, 5, \mp 9)$, $(\pm 2, 7, \mp 15)$,
$(\pm 3, 7, \mp 10)$, $(\pm 5, 7, \mp 6)$, $(\pm 1, 8, \mp 15)$, $(\pm 3, 8, \mp 5)$,

und

$(\pm 10, 3, \mp 7)$, $(\pm 9, 4, \mp 7)$, $(\pm 9, 5, \mp 6)$, $(\pm 15, 7, \mp 2)$,
$(\pm 10, 7, \mp 3)$, $(\pm 6, 7, \mp 5)$, $(\pm 15, 8, \mp 1)$, $(\pm 5, 8, \mp 3)$.

§. 76.

Aehnlich wie bei negativen Determinanten (§. 64) beweisen wir auch die Richtigkeit des folgenden Satzes*):

Jede Form von positiver Determinante ist einer reducirten Form äquivalent.

Bezeichnen wir die gegebene Form von positiver Determinante

*) *Gauss: D. A.* art. 183.

D mit (a, b, a'), so suchen wir eine ihr nach rechts benachbarte Form (a', b', a'') so zu bestimmen, dass

$$\sqrt{D} - (a') < b' < \sqrt{D}$$

wird. Da zufolge der Erklärung einer benachbarten Form der mittlere Coefficient b' jeden Werth erhalten kann, welcher $\equiv -b \pmod{a'}$ ist, und keinen andern, so fragt sich nur, ob zwischen den Grenzen $\sqrt{D} - (a')$ und $\sqrt{D}$ stets ein solcher Werth existirt; dies ist offenbar der Fall, da die sämmtlichen zwischen diesen beiden Grenzen enthaltenen ganzen Zahlen

$$\lambda + 1 - (a'), \quad \lambda + 2 - (a') \ldots \lambda - 1, \quad \lambda$$

ein vollständiges Restsystem in Bezug auf den Modulus a' bilden; aus demselben Grunde ergiebt sich, dass nur eine einzige solche Zahl b' existirt. Nachdem $b' = -b - a'\delta$ bestimmt ist, geht die Form (a, b, a') durch die Substitution $\left(\begin{smallmatrix} 0, & 1 \\ -1, & \delta \end{smallmatrix}\right)$ in die benachbarte Form (a', b', a'') über, deren Coefficienten a', b' der obigen Bedingung Genüge leisten. Findet sich nun, dass zu gleicher Zeit $(a'') \geqq (a')$ wird, so ist nach dem am Schlusse des §. 74 besonders hervorgehobenen speciellen Fall die gefundene Form (a', b', a'') eine reducirte. Ist dagegen

$$(a') > (a''),$$

so verfahre man mit der gefundenen Form (a', b', a'') genau so wie mit der gegebenen Form, d. h. man bilde die ihr nach rechts benachbarte Form (a'', b'', a'''), in welcher

$$\sqrt{D} - (a'') < b'' < \sqrt{D}$$

ist, und welche gewiss eine reducirte ist, wenn $(a''') \geqq (a'')$ ist. Sollte aber wieder

$$(a'') > (a''')$$

sein, so setze man denselben Process in derselben Weise fort; da unter einer gegebenen positiven Zahl (a') nur eine endliche Anzahl von ganzen positiven Zahlen liegt, so muss man nach einer endlichen Anzahl von Transformationen durchaus zu einer Form $(a^{(n)}, b^{(n)}, a^{(n+1)})$, in welcher sowohl

$$\sqrt{D} - (a^{(n)}) < b^{(n)} < \sqrt{D}$$

als auch

$$(a^{(n+1)}) \geqq (a^{(n)})$$

ist, also zu einer reducirten Form gelangen, was zu beweisen war.

Es verdient bemerkt zu werden, dass bei diesem Process nicht gerade erst die letzte Form eine reducirte zu sein braucht, denn

es giebt reducirte Formen, in welchen die Bedingungen des besondern hier benutzten speciellen Falles nicht erfüllt sind. Von grösserer Wichtigkeit ist es aber, besonders darauf aufmerksam zu machen, dass durch den angegebenen Process auch jedes Mal eine Substitution gefunden wird, durch welche die gegebene Form in die reducirte Form übergeht, und zwar erhält man diese Substitution durch Composition der successiven Substitutionen, welche in dem Processe auftreten. Der Algorithmus selbst ist durchaus nicht beschwerlich (vergl. §. 64), wie folgende Beispiele zeigen.

Beispiel 1: Die Form (4, 6, 7) hat die Determinante $D = 8$; es ist also $\lambda = 2$. Unter den Zahlen

$$-4, -3, -2, -1, 0, 1, 2$$

ist $b' = 1 \equiv -6 \pmod 7$; dies giebt die benachbarte Form $(7, 1, -1)$, welche noch nicht reducirt ist. Da $(a'') = 1$ ist, so ist $b'' = \lambda = 2$, und folglich erhält man die benachbarte Form $(-1, 2, 4)$, welche wirklich reducirt ist. Durch die Substitution $\left(\begin{smallmatrix} 0, & +1 \\ -1, & -1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0, & 1 \\ -1, & 3 \end{smallmatrix}\right) = \left(\begin{smallmatrix} -1, & +3 \\ +1, & -4 \end{smallmatrix}\right)$ geht die gegebene Form in die gefundene über.

Beispiel 2: Die Form (713, 60, 5) hat die Determinante $D = 35$; man findet nach der angegebenen Methode die nach rechts benachbarte Form (5, 5, −2), und zu dieser wieder die Form (−2, 5, 5), in welcher der letzte Coefficient in der That grösser ist als der erste. In diesem Beispiel ist aber auch schon die vorhergehende Form (5, 5, −2) reducirt. Die gegebene Form geht durch die Substitution $\left(\begin{smallmatrix} 0, & +1 \\ -1, & -13 \end{smallmatrix}\right)$ in (5, 5, −2) und durch die Substitution $\left(\begin{smallmatrix} 0, & +1 \\ -1, & -13 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0, & 1 \\ -1, & 5 \end{smallmatrix}\right) = \left(\begin{smallmatrix} -1, & +5 \\ 13, & -66 \end{smallmatrix}\right)$ in (−2, 5, 5) über.

Beispiel 3: Die Form (62, 95, 145), deren Determinante $D = 35$, geht durch die folgenden successiven Substitutionen

$$\left(\begin{smallmatrix} 0, & 1 \\ -1, & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0, & 1 \\ -1, & 2 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0, & 1 \\ -1, & 2 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0, & 1 \\ -1, & 4 \end{smallmatrix}\right)$$

successive in die Formen

$$(145, -95, 62), \quad (62, -29, 13), \quad (13, 3, -2), \quad (-2, 5, 5)$$

über, von denen erst die letzte reducirt ist; die Zusammensetzung dieser Substitutionen giebt die Substitution $\left(\begin{smallmatrix} -3, & +10 \\ +2, & -7 \end{smallmatrix}\right)$, durch welche (62, 95, 145) in (−2, 5, 5) übergeht.