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_0078
LOG Titel: §. 70. Darstellung der Zahlen durch die Formen .... und .....
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

die Form (1, 0, 2) über, diese also rückwärts in jene durch die Substitution $\left(\begin{smallmatrix}+3, & +1\\ -4, & -1\end{smallmatrix}\right)$; also ist $x = 3$, $y = -4$, und folglich

$$41 = 3^2 + 2 \cdot 4^2.$$

Beispiel 2: Ist $m = 33 = 3 \cdot 11$, so ist die Bedingung erfüllt; μ ist $= 2$, und folglich muss es zwei verschiedene Zerlegungen geben. Die Wurzeln der Congruenz $z^2 \equiv -2 \pmod{33}$ sind ± 8 und ± 14: wir bilden daher die beiden Formen (33, 8, 2) und (33, 14, 6), welche resp. durch die Substitutionen

$$\begin{pmatrix}-1, & 0\\ +4, & -1\end{pmatrix} \text{ und } \begin{pmatrix}-1, & +2\\ +2, & -5\end{pmatrix}$$

in die Form (1, 0, 2) übergehen; die inversen Substitutionen sind

$$\begin{pmatrix}-1, & 0\\ -4, & -1\end{pmatrix} \text{ und } \begin{pmatrix}-5, & -2\\ -2, & -1\end{pmatrix}$$

und folglich ist

$$33 = 1^2 + 2 \cdot 4^2 = 5^2 + 2 \cdot 2^2.$$

§. 70.

Alle Formen der Determinante $D = -3$ bilden *zwei* Classen, als deren Repräsentanten man die reducirten Formen

$$(1, 0, 3) = x^2 + 3y^2$$

und

$$(2, 1, 2) = 2x^2 + 2xy + 2y^2$$

annehmen kann; sie sind resp. von der ersten und zweiten Art. Ungerade Zahlen können offenbar nur durch die erstere dargestellt werden; es sei daher m eine ungerade und der Einfachheit wegen durch 3 nicht theilbare Zahl; damit sie durch die Form (1, 0, 3) darstellbar sei, ist erforderlich, dass, wenn p irgend eine in ihr aufgehende Primzahl ist,

$$\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right) = +1,$$

folglich p von der Form $3h + 1$ sei. Umgekehrt, sobald diese Bedingung für alle μ in m aufgehenden Primzahlen p erfüllt ist, so hat die Congurenz

$$z^2 \equiv -3 \pmod{m}$$

stets 2^μ incongruente Wurzeln; ist n ein bestimmter Repräsentant

einer solchen, und $n^2 + 3 = ml$, so ist die Form (m, n, l) von der ersten Art (da m ungerade ist) und folglich der Form $(1, 0, 3)$ äquivalent. Es giebt also (nach §. 62) zwei Substitutionen

$$\begin{pmatrix} x, & \xi \\ y, & \eta \end{pmatrix} \text{ und } \begin{pmatrix} -x, & -\xi \\ -y, & -\eta \end{pmatrix}$$

durch welche die Form $(1, 0, 3)$ in die Form (m, n, l) übergeht, und folglich auch zwei Darstellungen (x, y) und $(-x, -y)$ der Zahl m, welche zu dieser Wurzel gehören. Im Ganzen giebt es daher

$$2 \cdot 2^{\mu} = 2^{\mu+1}$$

verschiedene Darstellungen einer solchen Zahl m durch die Form $(1, 0, 3)$, die sich aber wieder auf nur

$$\tfrac{1}{4} \cdot 2^{\mu+1} = 2^{\mu-1}$$

verschiedene Zerlegungen der Zahl m in ein einfaches und ein dreifaches Quadrat reduciren (nur auf den Fall $\mu = 0$, also $m = 1$ passt die letztere Formel wieder nicht). Besonders bemerkenswerth ist der specielle Fall:

Jede Primzahl von der Form $3h + 1$ *ist stets und nur auf eine einzige Weise in ein einfaches und ein dreifaches Quadrat zerlegbar.*

Gehen wir nun zu den durch die zweite Form $(2, 1, 2)$ darstellbaren, nothwendig geraden Zahlen über; wir beschränken uns auf diejenigen von der Form $2m$, wo m wieder eine ungerade und durch 3 nicht theilbare Zahl bedeutet. Dann erkennen wir leicht, dass der Complex dieser Zahlen m mit dem eben behandelten vollständig identisch ist. Denn aus der Möglichkeit der Congruenz $z^2 \equiv -3 \pmod{m}$ folgt auch die der Congruenz $z^2 \equiv -3 \pmod{2m}$, und umgekehrt (§. 37), und ausserdem ist die Anzahl der Wurzeln wieder $= 2^{\mu}$. Ist ferner n' ein bestimmter Repräsentant einer solchen, und $n'^2 + 3 = 2ml$, so ist die Form $(2m, n', l)$ nothwendig von der zweiten Art (denn der mittlere Coefficient n' ist ungerade, folglich l gerade) und also gewiss der Form $(2, 1, 2)$ äquivalent; man kann daher (nach §. 62) sechs verschiedene Transformationen der letztern Form in die erstere finden, aus welchen folgende sechs Darstellungen

$$\pm (x, y), \pm (y, -x-y), \pm (x+y, -x)$$

entspringen, die alle zu derselben Wurzel n' gehören (die sechs zu der entgegengesetzten Wurzel $-n'$ gehörenden Darstellungen

entstehen aus diesen durch Vertauschung der ersten darstellenden Zahl mit der zweiten)*). Im Ganzen existiren daher

$$6 \cdot 2^{\mu} = 3 \cdot 2^{\mu+1}$$

verschiedene Darstellungen der Zahl $2m$ durch die Form (2, 1, 2), oder, was dasselbe ist, der Zahl m durch die Form $x^2 + xy + y^2$. Sieht man je vier zusammengehörige Darstellungen von der Form

$$(x, y), \quad (-x, -y), \quad (y, x), \quad (-y, -x)$$

als nicht wesentlich verschieden an, so ist die Anzahl der wesentlich verschiedenen Darstellungen nur noch

$$= 3 \cdot 2^{\mu-1}.$$

Für eine Primzahl p von der Form $3h + 1$ giebt es daher immer drei wesentlich verschiedene Darstellungen durch die Form $x^2 + xy + y^2$.

Beispiel: Ist $m = 13$, so sind $n = \pm 7$ die Wurzeln der Congruenz $z^2 \equiv -3 \pmod{26}$ und also auch der Congruenz $z^2 \equiv -3 \pmod{13}$. Wir bilden daher die beiden Formen (13, 7, 4) und (26, 7, 2). Sie gehen resp. durch die Substitutionen

$$\begin{pmatrix} -1, & -1 \\ +2, & +1 \end{pmatrix} \text{ und } \begin{pmatrix} 0, & +1 \\ -1, & -4 \end{pmatrix}$$

in die Formen (1, 0, 3) und (2, 1, 2) über. Die beiden inversen Substitutionen sind

$$\begin{pmatrix} +1, & +1 \\ -2, & -1 \end{pmatrix} \text{ und } \begin{pmatrix} -4, & -1 \\ +1, & 0 \end{pmatrix}$$

und folglich ist

$$13 = 1^2 + 3\,(-2)^2 = (-4)^2 + (-4) \cdot 1 + 1^2;$$

hieraus findet man leicht die beiden anderen Darstellungen

$$\begin{aligned} 13 &= 4^2 + 4 \cdot (-3) + (-3)^2 \\ &= 3^2 + 3 \cdot 1 + 1^2 \end{aligned}$$

---

*) Da von den Zahlen x, y, $x+y$ stets eine und nur eine gerade ist, so giebt es unter den sechs zu der Wurzel n' gehörenden Darstellungen der Zahl $2m$ immer zwei $\pm (x', y')$, in welchen y' gerade ist $= 2u$; setzt man ferner $x' + u = t$, so geht die Gleichung $x'x' + x'y' + y'y' = m$ über in $tt + 3uu = m$, d. h. man erhält eine Darstellung (t, u) der Zahl m durch die Form (1, 0, 3), und zwar gehört diese Darstellung zu derselben Wurzel n'. Hierin besteht der Zusammenhang zwischen den Darstellungen der Zahlen m und $2m$ resp. durch die Formen (1, 0, 3) und (2, 1, 2).