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_0079
LOG Titel: §. 71. 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

§. 71.

Als letztes Beispiel wählen wir die Determinante $D = -5$; es giebt *zwei* nicht äquivalente reducirte Formen

$$(1, 0, 5) \text{ und } (2, 1, 3),$$

beide sind ursprünglich und von der ersten Art. Wir suchen wieder das System aller ungeraden und durch 5 nicht theilbaren Zahlen m zu bestimmen, welche durch diese Formen darstellbar sind. Die dazu erforderliche Bedingung besteht darin, dass für jede in m aufgehende Primzahl p die Gleichung

$$\left(\frac{-5}{p}\right) = (-1)^{\frac{1}{2}(p-1)}\left(\frac{p}{5}\right) = +1$$

Statt finden muss; hieraus folgt (§. 52, II), dass jede solche Primzahl von einer der vier Formen

$$20h+1,\quad 20h+9,\quad 20h+3,\quad 20h+7$$

sein muss. Ist diese Bedingung erfüllt, und μ die Anzahl der verschiedenen Primzahlen p, so hat die Congruenz

$$z^2 \equiv -5 \pmod{m}$$

wieder 2^μ incongruente Wurzeln; ist n ein bestimmter Repräsentant einer solchen, und $n^2+5 = ml$, so ist die Form (m, n, l) nothwendig einer und nur einer der beiden obigen reducirten Formen äquivalent; es giebt dann jedesmal (nach §. 62) zwei Substitutionen, durch welche diese reducirte Form in (m, n, l) übergeht, also auch zwei zu der Wurzel n gehörige Darstellungen der Zahl m durch diese reducirte Form. Im Ganzen giebt es also

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

Darstellungen einer solchen Zahl durch die obigen reducirten Formen. Allein es bleibt noch zweifelhaft, durch welche der beiden reducirten Formen die zu einer bestimmten Wurzel n gehörigen beiden Darstellungen erfolgen; und eine ähnliche Frage wird jedesmal da auftreten, wo es mehrere nicht äquivalente Formen derselben Art giebt. In unserm Fall ist es nicht schwierig, diesen Zweifel zu heben.

Ist nämlich die Zahl m darstellbar durch die Form $(1, 0, 5)$, also z. B. $m = x^2 + 5y^2$, so folgt hieraus $m \equiv x^2 \pmod{5}$, d. h.

m ist quadratischer Rest von 5; ist dagegen die Zahl m darstellbar durch die zweite Form (2, 1, 3), also z. B. $m = 2x^2 + 2xy + 3y^2$, so ist $2m = (2x + y)^2 + 5y^2 \equiv (2x + y)^2 \pmod 5$, und, da 2 quadratischer Nichtrest von 5 ist, so ist m ebenfalls quadratischer Nichtrest von 5. Es tritt also hier die besonders einfache Erscheinung auf, dass alle Darstellungen einer Zahl entweder nur durch die Form (1, 0, 5) oder nur durch die Form (2, 1, 3) geschehen, je nachdem m quadratischer Rest oder Nichtrest von 5, d. h. je nachdem $m \equiv \pm 1$, oder $\equiv \pm 2 \pmod 5$ ist. Hieraus folgen die speciellen Sätze:

Jede Primzahl von einer der beiden Formen $20h + 1$, $20h + 9$ *ist auf vier Arten durch die Form* (1, 0, 5) *darstellbar (welche wesentlich nur eine einzige Zerlegung in ein einfaches und ein fünffaches Quadrat bilden); jede Primzahl von einer der beiden Formen* $20h + 3$, $20h + 7$ *ist auf vier Arten durch die Form* (2, 1, 3) *darstellbar.*

Beispiel 1: Ist $m = 29$, so sind $n = \pm 13$ die beiden Wurzeln der Congruenz $z^2 \equiv -5 \pmod{29}$; die hieraus gebildete Form (29, 13, 6) geht durch die Substitution

$$\begin{pmatrix} -1, & +1 \\ +2, & -3 \end{pmatrix}$$

in die reducirte Form (1, 0, 5) über; durch Umkehrung dieser Substitution erhält man die Zerlegung

$$29 = 3^2 + 5 \cdot 2^2.$$

Beispiel 2: Für $m = 27$ findet man $n = \pm 7$; die beiden entsprechenden Formen (27, 7, 2) und (27, −7, 2) gehen bezüglich durch die Substitutionen

$$\begin{pmatrix} 0, & +1 \\ -1, & -4 \end{pmatrix} \text{ und } \begin{pmatrix} 0, & 1 \\ -1, & 3 \end{pmatrix}$$

in die reducirte Form (2, 1, 3) über; durch Umkehrung derselben erhält man daher die vier Darstellungen

$$27 = 2(\mp 4)^2 + 2(\mp 4)(\pm 1) + 3(\pm 1)^2$$
$$27 = 2(\pm 3)^2 + 2(\pm 3)(\pm 1) + 3(\pm 1)^2$$

von denen die beiden ersteren zu der Wurzel $+7$, die beiden letzteren zu der Wurzel -7 gehören.