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_0077
LOG Titel: §. 69. Zerlegung der Zahlen in eine einfache und eine doppelte Quadratzahl
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

berühmte von *Fermat* aufgestellte, zuerst von *Euler**) bewiesene Satz enthalten:

Jede (positive) Primzahl von der Form $4h+1$ *lässt sich stets, und zwar nur auf eine einzige Weise in zwei Quadrate zerfällen.*

Die Bedingung, dass die Quadrate keinen gemeinschaftlichen Factor haben, fällt hier fort, da sie sich von selbst versteht.

Beispiel 1: Die Zahl 37 ist eine Primzahl von der Form $4h+1$; die beiden Wurzeln der Congruenz $z^2 \equiv -1 \pmod{37}$ findet man (z. B. mit Hülfe des Wilson'schen Satzes) $\equiv \pm 6$; nimmt man $n = 6$, so hat man die Form (37, 6, 1) zu betrachten, welche durch die Substitution $\left(\begin{smallmatrix} 0, & +1 \\ -1, & -6 \end{smallmatrix}\right)$ in die reducirte Form (1, 0, 1) übergeht; umgekehrt geht also (1, 0, 1) durch die inverse Substitution $\left(\begin{smallmatrix} -6, & -1 \\ +1, & 0 \end{smallmatrix}\right)$ in (37, 6, 1) über. Also ist die gesuchte Zerlegung folgende: $37 = 6^2 + 1^2$; es ist nicht nöthig, die vier zu dieser Wurzel $+6$, und die anderen vier zu der entgegengesetzten Wurzel -6 gehörenden Darstellungen hier einzeln aufzuschreiben.

Beispiel 2: Die Zahl $m = 65 = 5 \cdot 13$ ist das Product aus den beiden Primzahlen 5 und 13, welche beide die Form $4h+1$ haben. Mithin giebt es $2^4 = 16$ verschiedene Darstellungen, also nur zwei verschiedene Zerlegungen der Zahl 65. Die vier Wurzeln der Congruenz $z^2 \equiv -1 \pmod{65}$ sind ± 8 und ± 18; wir bilden daher die beiden Formen (65, 8, 1) und (65, 18, 5), welche durch die Substitutionen $\left(\begin{smallmatrix} 0, & +1 \\ -1, & -8 \end{smallmatrix}\right)$ und $\left(\begin{smallmatrix} -1, & -2 \\ +4, & +7 \end{smallmatrix}\right)$ in die reducirte Form (1, 0, 1) übergehen; die inversen Substitutionen sind $\left(\begin{smallmatrix} -8, & -1 \\ +1, & 0 \end{smallmatrix}\right)$ und $\left(\begin{smallmatrix} +7, & +2 \\ -4, & -1 \end{smallmatrix}\right)$, und folglich sind die beiden gesuchten Zerlegungen folgende:

$$65 = 8^2 + 1^2 = 7^2 + 4^2.$$

§. 69.

Alle Formen der Determinante $D = -2$ bilden ebenfalls nur eine einzige Classe, da nur eine einzige reducirte Form

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

vorhanden ist. Wir fragen auch hier wieder nach allen durch

*) *Demonstratio theorematis Fermatiani, omnem numerum primum formae* $4n+1$ *esse summam duorum quadratorum*, Nov. Comm. Petrop. V. p. 3.

diese Form darstellbaren *ungeraden* Zahlen m; die erste Bedingung ist die, dass -2 quadratischer Rest von m sein muss; dazu ist erforderlich und hinreichend, dass für jede in m aufgehende (also ungerade) Primzahl p

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

also p von einer der beiden Formen $8h+1$ oder $8h+3$ sei. Umgekehrt: sind die sämmtlichen μ in m aufgehenden Primzahlen p alle von der Form $8h+1$ oder $8h+3$, so hat die Congruenz

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

stets 2^μ incongruente Wurzeln. Ist n ein bestimmter Repräsentant einer solchen Wurzel, und $n^2+2 = ml$, so ist die Form (m, n, l) nothwendig der Form $(1, 0, 2)$ äquivalent; man findet daher (nach §. 66) eine Substitution $\left(\begin{smallmatrix} x, & \xi \\ y, & \eta \end{smallmatrix}\right)$, durch welche die letztere in die erstere übergeht; ausser dieser existirt (nach §. 62) nur noch die andere $\left(\begin{smallmatrix} -x, & -\xi \\ -y, & -\eta \end{smallmatrix}\right)$, welche dieselbe Eigenschaft hat; es giebt daher zwei verschiedene Darstellungen (x, y) und $(-x, -y)$ der Zahl m, die zu dieser Wurzel gehören. Im Ganzen giebt es daher

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

verschiedene Darstellungen der Zahl m durch die Form $(1, 0, 2)$.

Man erkennt ferner leicht, dass, wenn die beiden Darstellungen $\pm(x, y)$ zu der Wurzel n gehören, entsprechend die beiden Darstellungen $\pm(x, -y)$ zu der entgegengesetzten Wurzel $-n$ gehören. Je vier solche Darstellungen geben eine und dieselbe Zerlegung der Zahl m in ein Quadrat und ein doppeltes Quadrat; mithin ist die Anzahl aller verschiedenen Zerlegungen

$$= 2^{\mu-1};$$

die einzige Ausnahme bildet wieder der Fall, in welchem $\mu = 0$, also $m = 1$ ist; denn dann vereinigen sich die zwei verschiedenen Darstellungen ($+n$ ist $\equiv -n \pmod{1}$) zu der einzigen Zerlegung $1 = 1^2 + 2 \cdot 0^2$. Der interessanteste specielle Fall ist wieder der, in welchem $\mu = 1$ ist:

Jede Primzahl p von einer der beiden Formen $8h+1$ oder $8h+3$ lässt sich stets und nur auf eine einzige Weise in ein Quadrat und ein doppeltes Quadrat zerlegen.

Beispiel 1: Ist $m = 41$, so ist die Bedingung erfüllt; μ ist $= 1$; die beiden Wurzeln der Congruenz $z^2 \equiv -2 \pmod{41}$ sind ± 11; die Form $(41, 11, 3)$ geht durch die Substitution $\left(\begin{smallmatrix} -1, & -1 \\ +4, & +3 \end{smallmatrix}\right)$ in