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_0076
LOG Titel: §. 68. Zerlegung der Zahlen in zwei Quadratzahlen
LOG Typ: chapter

(8, $\pm$ 4, 8) aus je zwei äquivalenten Formen; also bleiben nur *acht* nicht äquivalente Formen

$$(1, 0, 48),\quad (2, 0, 24),\quad (3, 0, 16),\quad (4, 0, 12),$$
$$(6, 0, 8),\quad (7, 1, 7),\quad (4, 2, 13),\quad (8, 4, 8).$$

Ursprünglich von der ersten Art sind die folgenden vier:

$$(1, 0, 48),\quad (3, 0, 16),\quad (7, 1, 7),\quad (4, 2, 13),$$

die anderen vier sind derivirte Formen.

§. 68.

Um schon jetzt einen Begriff von der Fruchtbarkeit dieser Untersuchungen zu geben, verbinden wir in einigen Beispielen die gewonnenen Resultate mit der in §. 60 vorausgeschickten Theorie der Darstellung der Zahlen durch bestimmte quadratische Formen, bemerken jedoch gleich, dass die folgenden Sätze nur specielle Fälle eines grossen allgemeinen Satzes sind.

Die Formen der Determinante $D = -1$ bilden nur eine einzige Classe, denn es giebt für diese Determinante, wie man leicht erkennt, nur die einzige reducirte Form

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

Wir fragen nun nach dem System der durch diese Form darstellbaren, d. h. also in zwei Quadrate zerlegbaren Zahlen m; um aber die frühere Theorie unmittelbar anwenden zu können, lassen wir nur *eigentliche* Darstellungen (x, y) gelten, in denen die beiden darstellenden Zahlen x, y relative Primzahlen sind; ferner wollen wir uns der Einfachheit halber auf *ungerade* darstellbare Zahlen m beschränken. Es sei also m eine solche darstellbare ungerade Zahl, so ist zunächst m positiv. Da ferner die Determinante -1 quadratischer Rest von m ist, so müssen alle in m aufgehenden Primzahlen von der Form $4h+1$ sein. Umgekehrt, ist diese Bedingung erfüllt, so ist die Determinante -1 quadratischer Rest von m, und die Congruenz

$$z^2 \equiv -1 \pmod{m}$$

hat im Ganzen (nach §. 37) 2^μ incongruente Wurzeln, wenn μ die Anzahl dieser von einander verschiedenen in m aufgehenden Primzahlen bedeutet (dies gilt selbst für den Fall, in welchem $\mu = 0$,

$m = 1$ ist). Es sei n ein bestimmter Repräsentant einer bestimmten dieser Wurzeln, und $n^2 + 1 = ml$, so bilde man die quadratische Form (m, n, l) von der Determinante -1; da nur eine einzige Formenclasse existirt, so ist diese Form der reducirten Form $(1, 0, 1)$ nothwendig äquivalent, und man wird durch die in §. 66 angegebene Methode eine, und hieraus nach §§. 61, 62 alle Transformationen finden, durch welche $(1, 0, 1)$ in (m, n, l) übergeht. Die Anzahl dieser von einander verschiedenen Transformationen $\binom{x,\ \xi}{y,\ \eta}$ ist (nach §§. 61, 62) stets $= 4$; ebenso viele Darstellungen (x, y) der Zahl m existiren daher, welche zu derjenigen Wurzel gehören, deren Repräsentant n ist. Und da dasselbe Raisonnement auf jede der 2^μ Wurzeln der obigen Congruenz passt, so existiren im Ganzen

$$4 \,.\, 2^\mu = 2^{\mu+2}$$

verschiedene Darstellungen der Zahl m.

Stellt man aber die Frage, auf wie viele verschiedene Arten eine solche Zahl m in zwei Quadrate zerlegt werden kann, ohne Rücksicht auf die Ordnung der beiden Quadrate und auf die Vorzeichen ihrer Wurzeln, so liefern je acht verschiedene Darstellungen von der Form

$$(\pm x, \pm y) \quad \text{und} \quad (\pm y, \pm x)$$

nur eine einzige Zerlegung $m = x^2 + y^2$ (von diesen acht Darstellungen gehören vier, nämlich

$$(x, y), (-x, -y), (-y, x), (y, -x)$$

zu einer, und die anderen vier

$$(x, -y), (-x, y), (-y, -x), (y, x)$$

zu der ihr entgegengesetzten Wurzel); folglich ist die Anzahl dieser verschiedenen Zerlegungen

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

mit einziger Ausnahme des Falles $m = 1$, weil dann nicht acht, sondern nur vier verschiedene Darstellungen

$$(\pm 1, 0) \quad \text{und} \quad (0, \pm 1)$$

existiren, die sich zu der einzigen Zerlegung $1 = 1^2 + 0^2$ vereinigen.

In diesem allgemeinen Resultat ist als specieller Fall der