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_0014
LOG Titel: §. 8. Primzahlen und zusammengesetzte Zahlen; Zerlegung der zusammengesetzten Zahlen in Primzahlen. Die Anzahl der Primzahlen ist unbegrenzt
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

Multipla der beiden Zahlen a, b übereinstimmen mit den sämmtlichen Vielfachen *einer* bestimmten Zahl

$$a'b'\delta = \frac{ab}{\delta} = \mu,$$

welche man deshalb das *kleinste gemeinschaftliche Vielfache* der beiden Zahlen a, b nennt.

Um diesen Satz für eine beliebige Anzahl gegebener Zahlen $a, b, c, d \ldots$ zu verallgemeinern, braucht man nur zu bemerken, dass jedes gemeinschaftliche Vielfache der Zahlen

$$a, b, c, d \ldots$$

nothwendig auch ein gemeinschaftliches Vielfaches der Zahlen

$$\mu, c, d \ldots$$

ist und umgekehrt. Man wird daher zunächst das kleinste gemeinschaftliche Multiplum ν der beiden Zahlen μ und c suchen, dann das kleinste gemeinschaftliche Vielfache ϱ von ν und d u. s. f. Auf diese Weise leuchtet ein, dass sämmtliche gemeinschaftliche Multipla der gegebenen Zahlen $a, b, c, d \ldots$ übereinstimmen mit den sämmtlichen Vielfachen einer einzigen vollständig bestimmten Zahl ω, welche man deshalb das *kleinste gemeinschaftliche Vielfache* der gegebenen Zahlen nennt.

Von besonderer Wichtigkeit ist der Fall, in welchem die Zahlen $a, b, c, d \ldots$ relative Primzahlen sind. In diesem Falle ist zunächst $\delta = 1$, also ist das kleinste gemeinschaftliche Vielfache der beiden relativen Primzahlen a und b ihr Product ab. Da nun c wieder relative Primzahl gegen a und gegen b, also (§. 5, 1.) auch gegen ab ist, so ist abc das kleinste gemeinschaftliche Multiplum der drei Zahlen a, b, c u. s. f. Kurz, man erhält das Resultat: *Sind $a, b, c, d \ldots$ relative Primzahlen, so ist jede Zahl, welche durch jede einzelne derselben theilbar ist, auch durch ihr Product $abcd \ldots$ theilbar.*

§. 8.

Da jede Zahl sowohl durch die Einheit, als auch durch sich selbst theilbar ist, so hat jede Zahl — die Einheit selbst ausgenommen — mindestens zwei (positive) Divisoren. Jede Zahl nun, welche keine anderen als diese beiden Divisoren besitzt, heisst eine *Primzahl (numerus primus)*; es ist zweckmässig, die Einheit nicht

zu den Primzahlen zu rechnen, weil manche Sätze über Primzahlen nicht für die Zahl 1 gültig bleiben.

Aus dieser Erklärung ergiebt sich der Satz: *Wenn p eine Primzahl und a irgend eine ganze Zahl ist, so geht entweder p in a auf, oder p ist relative Primzahl zu a.* Denn der grösste gemeinschaftliche Divisor von p und a ist entweder p selbst oder die Einheit.

Hieraus folgt weiter: *Wenn ein Product aus mehreren Zahlen $a, b, c, d \ldots$ durch eine Primzahl p theilbar ist, so geht p mindestens in einem der Factoren $a, b, c, d \ldots$ auf.* Denn wäre keine einzige dieser Zahlen durch p theilbar, so wäre p relative Primzahl gegen jede einzelne von ihnen und folglich auch gegen ihr Product, was gegen die Annahme streitet, dass dies Product durch p theilbar ist.

Jede Zahl, welche ausser sich selbst und der Einheit noch andere Divisoren hat, heisst *zusammengesetzt (numerus compositus).* Diese Benennung wird gerechtfertigt durch folgenden

Fundamentalsatz: Jede zusammengesetzte Zahl lässt sich stets und nur auf eine einzige Weise als Product aus einer endlichen Anzahl von Primzahlen darstellen.

Beweis. Da jede zusammengesetzte Zahl m ausser 1 und m noch andere Divisoren hat, so sei a ein solcher; ist nun a keine Primzahl, also eine zusammengesetzte Zahl, so besitzt a ausser 1 und a noch andere Divisoren, z. B. b; ist b noch keine Primzahl, also zusammengesetzt, so hat b wieder mindestens einen Divisor c, der von 1 und b verschieden ist. Fährt man so fort, so muss man endlich einmal zu einer Primzahl gelangen; denn die Reihe der Zahlen $m, a, b, c \ldots$ ist eine abnehmende, sie kann also, da es nur eine endliche Anzahl von Zahlen giebt, welche kleiner als m sind, nur eine endliche Anzahl von Gliedern enthalten; das letzte Glied derselben muss aber eine Primzahl sein, denn sonst könnte man ja die Reihe noch weiter fortsetzen. Bezeichnet man diese Primzahl mit p, so ist, da jedes Glied der Reihe ein Multiplum des folgenden ist, die erste Zahl m auch ein Multiplum von der letzten p. Man kann daher

$$m = pm'$$

setzen. Nun ist m' entweder eine Primzahl — dann ist m schon als Product von Primzahlen dargestellt — oder m' ist zusammengesetzt; im letztern Falle muss es wieder eine in m' aufgehende Primzahl p' geben, so dass

$$m' = p'm'', \quad \text{also} \quad m = pp'm''$$

wird. Ist nun m'' noch keine Primzahl, so kann man auf dieselbe Weise fortfahren, bis man m als Product von lauter Primzahlen dargestellt hat. Dass dies wirklich nach einer endlichen Anzahl von ähnlichen Zerlegungen geschehen muss, leuchtet daraus ein, dass die Reihe der Zahlen m, m', m'' ... ebenfalls eine abnehmende und folglich eine endliche ist.

Hiermit ist der eine Haupttheil des Satzes erwiesen, welcher die Möglichkeit der Zerlegung behauptet; offenbar ist aber diese successive Ablösung von Primzahl-Factoren in mancher Beziehung willkürlich, und es bleibt daher noch nachzuweisen übrig, dass, auf welche Weise dieselbe auch ausgeführt sein mag, das Endresultat doch stets dasselbe sein muss. Nehmen wir daher an, man habe durch zwei verschiedene Anordnungen einmal

$$m = pp'p'' \ldots$$

ein anderes Mal

$$m = qq'q'' \ldots$$

gefunden, wo p, p', p'' ... und q, q', q'' ... sämmtlich Primzahlen bedeuten. Da nun das Product $pp'p''$ ... durch die Primzahl q theilbar ist, so muss mindestens einer der Factoren, z. B. p, durch q theilbar sein; p besitzt aber als Primzahl nur die beiden Divisoren 1 und p, und folglich muss $q = p$ sein, da q nicht $= 1$ ist. Hieraus folgt nun

$$p'p'' \ldots = q'q'' \ldots$$

und man kann auf dieselbe Weise zeigen, dass q' mit einer der Primzahlen p', p'' ..., z. B. mit p', identisch sein muss, woraus dann wieder

$$p'' \ldots = q'' \ldots$$

folgt. Auf diese Weise überzeugt man sich davon, dass jede Primzahl, welche bei der zweiten Art der Zerlegung ein oder mehrere Male als Factor auftritt, mindestens ebenso oft auch bei der ersten Zerlegung vorkommt; da aber ferner auf dieselbe Weise gezeigt werden kann, dass sie bei der zweiten Zerlegung mindestens ebenso oft vorkommt wie bei der ersten, so muss jede Primzahl in beiden Zerlegungen gleich oft als Factor vorkommen, und folglich stimmt der Complex aller Primzahlen bei der einen Zerlegung vollständig mit dem bei der andern überein.

Nachdem so der Satz in allen seinen Theilen bewiesen ist,

können wir die Darstellung der zusammengesetzten Zahl m noch dadurch vereinfachen, dass wir jedesmal alle unter einander identischen Primzahl-Factoren zu einer Potenz vereinigen. Es sei nämlich a eine von den in m aufgehenden Primzahlen, und zwar mag dieselbe genau αmal als Factor in der Zerlegung vorkommen, so vereinigen wir diese α Factoren zu der Potenz a^α; sind hierdurch noch nicht alle Factoren erschöpft, und ist b eine der übrigen Primzahlen, so bilden wir, wenn sie genau βmal vorkommt, die Potenz b^β, und in derselben Weise fahren wir fort, wenn hierdurch noch nicht alle Primzahl-Factoren von m erschöpft sind. Auf diese Weise überzeugt man sich, dass man jeder zusammengesetzten Zahl m die Form

$$m = a^\alpha b^\beta c^\gamma \ldots$$

geben kann, in welcher a, b, c die sämmtlichen unter einander verschiedenen, in m aufgehenden Primzahlen, und α, β, γ . . . ganze positive Zahlen bedeuten. Dass aber in dieser Form nicht nur alle zusammengesetzten, sondern auch alle Primzahlen enthalten sind, leuchtet unmittelbar ein.

Die Primzahlen bilden daher gewissermaassen das Material, aus welchem alle anderen Zahlen sich zusammensetzen lassen. *Dass es unendlich viele Primzahlen giebt*, hat schon *Euclid**) bewiesen, und zwar in folgender Art. Gesetzt es gäbe nur eine endliche Anzahl von Primzahlen, so würde eine von ihnen, die wir mit p bezeichnen wollen, die letzte, d. h. die grösste sein. Denken wir uns nun alle diese Primzahlen aufgeschrieben

$$2, 3, 5, 7, 11 \ldots p,$$

so müsste jede Zahl, welche grösser als p ist, zusammengesetzt und folglich durch mindestens eine dieser Primzahlen theilbar sein. Allein es ist sehr leicht, eine Zahl zu bilden, welche erstens grösser als p und zweitens durch keine jener Primzahlen theilbar ist; dazu bilden wir das Product aller Primzahlen von 2 bis p und vergrössern dasselbe um eine Einheit. Diese Zahl

$$z = 2.\,3.\,5 \ldots p + 1$$

ist in der That grösser als p, da ja schon $2p$ grösser als p ist; sie ist aber durch keine der Primzahlen theilbar, da z, durch jede derselben dividirt, immer den Rest 1 lässt. Damit ist also unsere

*) *Elemente*, Buch IX, Satz 20.