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_0032
LOG Titel: §. 25. Auflösung der Aufgabe, alle Zahlen zu finden, welche in Bezug auf gegebene Divisoren vorgeschriebene Reste lassen
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

meinschaftlicher Divisor m ist, so sollen ebensoviele ganze Zahlen $x, y, z \ldots$ gefunden werden, welche der Gleichung

$$ax + by + cz + \cdots = m$$

genügen. Denn gesetzt, man habe für die Zahlen $b, c \ldots$, deren grösster gemeinschaftlicher Divisor m' nothwendig ein Multiplum von m ist, schon ganze Zahlen $y', z' \ldots$ gefunden, welche der Bedingung

$$by' + cz' + \cdots = m'$$

genügen, so löse man, da m der grösste gemeinschaftliche Divisor von a und m' ist, nach der obigen Methode die Gleichung

$$ax + m'x' = m$$

in ganzen Zahlen x, x', so wird die vorgelegte Gleichung durch die Zahlen $x, y = x'y', z = x'z' \ldots$ befriedigt.

§. 25.

Auf das im Vorhergehenden behandelte Problem der Auflösung der Congruenzen ersten Grades lässt sich das folgende zurückführen:

Alle Zahlen x zu finden, welche in Bezug auf zwei gegebene Moduln a, b gegebenen Zahlen resp. α, β congruent sind, d. h. welche den beiden Forderungen

$$x \equiv \alpha \pmod{a}, \quad x \equiv \beta \pmod{b}$$

genügen.

Da nämlich alle Zahlen x, welche die erste dieser beiden Forderungen erfüllen, in der Form $x = \alpha + at$ enthalten sind, wo t jede beliebige ganze Zahl bedeutet, so kommt es nur noch darauf an, dieses t näher so zu bestimmen, dass

$$at \equiv \beta - \alpha \pmod{b} \qquad (1)$$

wird. Bezeichnet man nun mit δ den grössten gemeinschaftlichen Divisor der beiden Moduln a und b, so muss, wenn diese Congruenz möglich sein soll, $\beta - \alpha$ durch δ theilbar, d. h. es muss

$$\alpha \equiv \beta \pmod{\delta} \qquad (2)$$

sein. Ist diese Bedingung nicht erfüllt, so existirt keine Zahl, welche der Aufgabe genügt; ist sie aber erfüllt, so sind sämmtliche der Congruenz (1) genügende Zahlen t in der Form

$$t \equiv \gamma \left(\text{mod. } \frac{b}{\delta}\right) \text{ oder } t = \gamma + \frac{b}{\delta} u$$

enthalten, wo γ eine bestimmte von ihnen, und u jede beliebige ganze Zahl bedeutet. Hieraus folgt, dass die gesuchten Zahlen durch die Formel

$$x = \alpha + \gamma a + \frac{ab}{\delta} u \text{ oder } x \equiv x_0 \left(\text{mod. } \frac{ab}{\delta}\right)$$

gegeben werden, wo $x_0 = \alpha + \gamma a$ selbst eine der gesuchten Zahlen, und der Modulus offenbar das kleinste gemeinschaftliche Multiplum der beiden gegebenen Moduln a, b ist.

Werden z. B. die Zahlen gesucht, welche durch 12 dividirt den Rest 7, durch 15 dividirt den Rest 4 lassen, so hat man die Congruenzen

$$x \equiv 7 \text{ (mod. 12)}, \quad x \equiv 4 \text{ (mod. 15)}.$$

Man setzt also $x = 7 + 12t$, und erhält für t die Congruenz

$$12t \equiv -3 \text{ (mod. 15)},$$

welche (da hier die Bedingung (2) erfüllt ist) sich auf

$$4t \equiv -1 \text{ (mod. 5)}$$

reducirt. Hieraus folgt

$$t \equiv 1 \text{ (mod. 5)}$$

und also

$$x = 7 + 12t \equiv 19 \text{ (mod. 60)}.$$

Besonders bemerkenswerth ist der besondere Fall, in welchem die beiden gegebenen Moduln a, b relative Primzahlen sind; da gleichzeitig $\delta = 1$ wird, so fällt die Bedingung (2) ganz fort; die Auflösung ist stets möglich und liefert ein Resultat von der Form

$$x \equiv \mu x_0 \text{ (mod. } ab).$$

Die ursprüngliche Aufgabe lässt sich auch leicht für den Fall verallgemeinern, in welchem eine Reihe von beliebig vielen Moduln und eine Reihe ihnen entsprechender Reste gegeben ist; für uns ist indessen nur der Fall von Wichtigkeit, in welchem die gegebenen Moduln a, b, c . . . relative Primzahlen sind; wir beschränken uns daher auf denselben, und stellen uns unter dieser Voraussetzung die Aufgabe, alle Zahlen x zu finden, welche dem System von Congruenzen

$$x \equiv \alpha \text{ (mod. } a), \quad x \equiv \beta \text{ (mod. } b), \quad x \equiv \gamma \text{ (mod. } c) \ldots$$

genügen. Da wir nun schon wissen, dass alle Zahlen, welche die beiden ersten dieser Forderungen erfüllen, in der Form $x \equiv \beta_1$ (mod. ab)

enthalten sind, wo die Zahl β_1 nach dem Vorhergehenden gefunden werden kann, so kommt unsere Aufgabe offenbar auf die einfachere zurück, alle Zahlen x zu finden, welche dem folgenden System von Congruenzen genügen:

$$x \equiv \beta_1 \pmod{ab}, \quad x \equiv \gamma \pmod{c} \ldots$$

Da nun der Modul ab der ersten dieser Congruenzen wieder relative Primzahl gegen jeden folgenden Modul $c \ldots$ ist, so kann man in derselben Weise fortfahren und gelangt so zu dem Resultat, dass sämmtliche Zahlen x in der Form

$$x \equiv x_0 \pmod{m}$$

enthalten sind, wo x_0 eine bestimmte von ihnen, und m das Product $abc \ldots$ aus allen gegebenen Moduln bedeutet.

Statt eine solche Zahl x_0 in der eben angegebenen Weise durch successive Auflösung einer Reihe von Congruenzen ersten Grades in Bezug auf die Moduln $b, c \ldots$ zu suchen, kann man auch auf folgende Art symmetrisch verfahren.

Man setze $m = aA = bB = cC \ldots$ und bestimme (nach §. 24) zunächst Zahlen $a', b', c' \ldots$, welche den Congruenzen

$$Aa' \equiv 1 \pmod{a}, \quad Bb' \equiv 1 \pmod{b}, \quad Cc' \equiv 1 \pmod{c} \ldots$$

genügen; so wird

$$x \equiv Aa'\alpha + Bb'\beta + Cc'\gamma + \cdots \pmod{m};$$

denn da $B, C \ldots$ durch a theilbar sind, so ist $x \equiv Aa'\alpha \equiv \alpha \pmod{a}$, und ebenso $\equiv \beta \pmod{b}$, $\equiv \gamma \pmod{c}$ u. s. w.

Ein besonderer Vortheil dieser Methode besteht darin, dass die Hülfszahlen $a', b', c' \ldots$ ganz unabhängig von $\alpha, \beta, \gamma \ldots$ sind, und daher stets dieselben bleiben, wie auch die letzteren variiren mögen, vorausgesetzt natürlich, dass das System der Moduln $a, b, c \ldots$ unverändert bleibt.

Es folgt ferner hieraus, dass x ein vollständiges Restsystem nach dem Modul m durchläuft, sobald die Reste $\alpha, \beta, \gamma \ldots$ vollständige Restsysteme resp. in Bezug auf die Moduln $a, b, c \ldots$ durchlaufen; denn wenn $\alpha', \beta', \gamma' \ldots$ irgend ein zweites System gegebener Reste ist, so wird

$$Aa'\alpha' + Bb'\beta' + Cc'\gamma' + \cdots$$

stets und nur dann

$$\equiv Aa'\alpha + Bb'\beta + Cc'\gamma + \cdots$$

nach dem Modulus m sein, wenn gleichzeitig