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_0025
LOG Titel: §. 18. Vollständiges Restsystem in Bezug auf einen Modulus
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

dass die Differenz $a - b$ durch k theilbar ist; offenbar behalten die vorstehenden Sätze auch nach dieser Erweiterung ihre volle Gültigkeit.

§. 18.

Da jede beliebige Zahl a ihrem Reste r in Bezug auf den (positiven) Modul k congruent ist, so ist jede Zahl a einer der k Zahlen

$$0, 1, 2 \ldots (k-1)$$

congruent; sie kann aber auch nur einer dieser Zahlen congruent sein, denn sonst müssten ja auch unter diesen k Resten mindestens zwei einander congruent sein, was offenbar nicht der Fall ist. Theilen wir daher sämmtliche Zahlen in *Classen* ein nach dem Princip, dass wir jedesmal zwei Zahlen in dieselbe oder in verschiedene Classen werfen, je nachdem sie in Bezug auf den Modulus k congruent sind oder nicht, so ist die *Anzahl* dieser Classen offenbar $= k$; die eine enthält sämmtliche Zahlen, welche $\equiv 0 \pmod{k}$, d. h. durch k theilbar sind; die folgende Classe enthält alle Zahlen, welche $\equiv 1 \pmod{k}$ sind, u. s. f.

Greift man nun aus jeder dieser Classen nach Belieben ein Individuum heraus, so hat das so gebildete System von k Zahlen die charakteristische Eigenschaft, dass jede beliebige ganze Zahl stets einer und auch nur einer von diesen k Zahlen congruent ist; ein solches System, wie es z. B. auch die Zahlen

$$0, 1, 2 \ldots (k-1)$$

bilden, nennt man ein *vollständiges System nicht congruenter* (oder *incongruenter*) *Zahlen* oder ein *vollständiges Restsystem* in Bezug auf den Modul k; offenbar bilden auch die Zahlen

$$1, 2, 3 \ldots k$$

und ebenso je k successive ganze Zahlen ein solches System.

Alle Zahlen, welche einer und derselben Classe angehören, haben nun mehrere allen gemeinschaftliche Eigenschaften, so dass sie in Bezug auf den Modul fast die Rolle einer einzigen Zahl spielen. Wir haben schon früher gesehen, dass jede Zahl, welche in einer Congruenz als Summand oder als Factor auftritt, unbeschadet der Richtigkeit der Congruenz durch jede andere ihr congruente, d. h. derselben Classe angehörige Zahl ersetzt werden

darf. Ein anderes Element, welches allen in einer Classe enthaltenen Individuen gemeinschaftlich ist, bildet der grösste Divisor, den sie mit dem Modul k gemeinschaftlich haben; denn sind a und b zwei congruente Zahlen, so ist

$$a = b + sk,$$

und folglich ist jeder gemeinschaftliche Divisor von a und k auch gemeinschaftlicher Divisor von b und k. Man kann daher nach diesem grössten gemeinschaftlichen Divisor die Classen wieder in Gruppen eintheilen, und da die Zahlen

$$1, 2 \ldots k$$

ein vollständiges System incongruenter Zahlen bilden, so ist (nach §. 13), wenn δ irgend einen Divisor von $k = n\delta$ bezeichnet, $\varphi(n)$ die Anzahl derjenigen Classen, welche solche Zahlen enthalten, die δ zum grössten gemeinschaftlichen Divisor mit dem Modul k haben. Speciell ist also $\varphi(k)$ die Anzahl derjenigen Classen, welche nur Zahlen enthalten, die relative Primzahlen gegen den Modulus k sind.

Von besonderer Wichtigkeit für spätere Untersuchungen ist auch noch folgender Satz:

Ist a relative Primzahl gegen den Modulus k, und setzt man in dem linearen Ausdruck $ax + b$ für x der Reihe nach alle k Glieder eines vollständigen Systems incongruenter Zahlen ein, so bilden die so entstehenden Werthe dieses Ausdrucks wieder ein vollständiges System incongruenter Zahlen.

Da nämlich aus

$$ax + b \equiv ay + b \pmod{k}$$

auch

$$ax \equiv ay \pmod{k}$$

und, da a relative Primzahl gegen k ist, nach §. 17, 6. auch

$$x \equiv y \pmod{k}$$

folgt, so ergiebt sich, dass alle Werthe des Ausdrucks $ax + b$, welche incongruenten Werthen von x entsprechen, ebenfalls incongruent sind; setzt man daher für x alle k incongruenten Zahlen ein, so erhält der Ausdruck $ax + b$ auch k incongruente Werthe, welche, da es überhaupt nur k Classen giebt, ein vollständiges System incongruenter Zahlen bilden.