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_0024
LOG Titel: §. 17. Erklärung der Congruenz zweier Zahlen in Bezug auf eine dritte. Einfachste Operationen mit Congruenz
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

Zweiter Abschnitt.

Von der Congruenz der Zahlen.

§. 17.

Bedeutet k irgend eine positive ganze Zahl, so lässt sich jede beliebige ganze Zahl a stets und nur auf eine einzige Weise in die Form

$$a = sk + r$$

bringen, in welcher s eine ganze Zahl und r eine der k Zahlen

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

bedeutet. Denn lässt man zunächst s alle ganzen Zahlwerthe von $-\infty$ bis $+\infty$ durchlaufen, so bilden die Zahlen sk die sämmtlichen Multipla von k, und von einem solchen Multiplum sk bis zum nächst grössern $(s+1)k$ excl. giebt es immer nur k Zahlen, nämlich

$$sk, sk+1, sk+2 \ldots sk+(k-1);$$

giebt man daher dem s alle denkbaren ganzen Zahlwerthe, und dem r jedesmal alle jene bestimmten k Werthe, so durchläuft der Ausdruck $sk+r$ wirklich alle ganzen Zahlwerthe a; dass ferner jede Zahl a auf diese Weise nur ein einziges Mal erzeugt wird, leuchtet auf folgende Weise ein. Wenn

$$s'k + r' = sk + r$$

ist, so folgt daraus

$$r' - r = (s - s')k;$$

wenn nun r' ebenfalls eine der k Zahlen $0, 1, 2 \ldots (k-1)$ ist, so ist der absolute Werth von $r'-r$ ebenfalls eine dieser Zahlen, also kleiner als k; da aber $r'-r$ ein Multiplum von k ist, so kann $r'-r$ nur $= 0$ sein, woraus $r' = r$ und $s' = s$ folgt.

Wir werden nun im Folgenden sagen, dass die Zahl r der *Rest* der Zahl a in Bezug auf den *Modulus* k ist; sobald ferner zwei Zahlen a und b in Bezug auf denselben Modulus k denselben Rest r lassen, sollen sie *gleichrestig* oder (nach *Gauss*) *congruent* in Bezug auf den Modulus k heissen; da in diesem Fall $a = sk+r$ und $b = s'k+r$ ist, so folgt, dass die Differenz $a-b = (s-s')k$ durch den Modulus k theilbar ist; und umgekehrt, ist $a-b$ durch k theilbar, so sind die Zahlen a und b auch congruent in Bezug auf den Modul k; denn ist r der Rest von a, r' der von b, also

$$a = sk+r, \quad b = s'k+r',$$

so ist

$$a-b = (s-s')k+(r-r');$$

da nun der Voraussetzung nach $a-b$ ein Multiplum von k ist, so muss auch $r'-r$ ein solches sein, was, wie wir vorher gesehen haben, nicht anders möglich ist, als wenn $r' = r$ ist. Man könnte daher congruente Zahlen auch als solche definiren, deren Differenz durch den Modul theilbar ist. (Aus diesem Grunde hat man die Bedeutung des Wortes Rest in der Weise erweitert, dass jede von zwei einander nach dem Modul k congruenten Zahlen a und b ein *Rest* der andern heisst.)

Da man sehr häufig die Congruenz zweier Zahlen a und b in Bezug auf eine dritte k als Modul auszudrücken hat, so ist von *Gauss**) für dieselbe folgende Bezeichnung eingeführt:

$$a \equiv b \pmod{k}.$$

So ist z. B.

$$3 \equiv -25 \pmod{4}, \quad 65 \equiv 16 \pmod{7}.$$

Da die beiden Zahlen a und b in dem Begriffe der Congruenz dieselbe Rolle spielen, so darf man offenbar die zur Linken und Rechten des Zeichens $\equiv$ stehenden Zahlen mit einander vertauschen. Ferner leuchten aus dem Begriffe der Congruenz leicht die folgenden Sätze ein:

1. Sind a und k zwei beliebige Zahlen, so ist stets

$$a \equiv a \pmod{k}.$$

*) *D. A.* art. 2.

2. Ist in Bezug auf denselben Modulus k eine erste Zahl a einer zweiten b, diese wieder einer dritten c congruent, so ist auch die erste a der dritten c in Bezug auf k congruent; in Zeichen: ist

$$a \equiv b \pmod{k}, \quad b \equiv c \pmod{k},$$

so ist auch

$$a \equiv c \pmod{k}.$$

Denn die Reste der drei Zahlen a, b, c sind einander gleich; oder auch, da $a-b$ und $b-c$ Multipla von k sind, so ist auch $(a-b)+(b-c)=a-c$ Multiplum von k.

3. Ist

$$a \equiv b \pmod{k} \text{ und } m \equiv n \pmod{k},$$

so ist auch

$$a+m \equiv b+n \pmod{k} \text{ und } a-m \equiv b-n \pmod{k}.$$

Denn da $a-b$ und $m-n$ Multipla von k sind, so sind auch $(a-b)+(m-n)=(a+m)-(b+n)$ und $(a-b)-(m-n)=(a-m)-(b-n)$ Multipla von k.

Dies lässt sich für eine beliebige Anzahl von Congruenzen erweitern, die sich auf denselben Modulus beziehen; man kann sie addiren und subtrahiren wie Gleichungen.

4. Ist wieder

$$a \equiv b \pmod{k} \text{ und } m \equiv n \pmod{k},$$

so ist auch

$$am \equiv bn \pmod{k}.$$

Denn da $a-b$ ein Vielfaches von k ist, so ist zunächst auch $(a-b)\,m=am-bm$ ein solches, also

$$am \equiv bm \pmod{k};$$

da ferner $m-n$ ein Vielfaches von k ist, so ist auch $b(m-n)=bm-bn$ ein solches, also

$$bm \equiv bn \pmod{k};$$

die beiden Zahlen am und bn sind daher derselben Zahl bm congruent, folglich sind sie auch unter einander congruent.

Auch dieser Satz lässt sich dahin verallgemeinern, dass man eine ganze Reihe von Congruenzen, die sich auf denselben Modul beziehen, mit einander multipliciren kann wie Gleichungen; und hieraus folgt wieder, dass gleich hohe Potenzen zweier congruenten Zahlen wieder congruent sind in Bezug auf denselben Modulus.

5. Die bisherigen Sätze kann man folgendermaassen zusammenfassen. Ist $f(x, y, z \ldots)$ eine ganze rationale Function der

Unbestimmten $x, y, z \ldots$, deren Coefficienten ganze Zahlen sind, und ist in Bezug auf einen und denselben Modulus k

$$a \equiv a',\ b \equiv b',\ c \equiv c' \ldots,$$

so ist auch

$$f(a,b,c \ldots) \equiv f(a',b',c' \ldots) \pmod{k}.$$

6. Etwas anders verhält es sich bei der Division. Ist nämlich

$$am \equiv bm \pmod{k},$$

so kann man hieraus im Allgemeinen nicht mit Sicherheit schliessen, dass auch $a \equiv b \pmod{k}$ sein muss; bezeichnen wir mit δ den grössten gemeinschaftlichen Divisor der beiden Zahlen $m = m'\delta$ und $k = k'\delta$, so folgt aus der obigen Congruenz nur, dass

$$a \equiv b \left(\mathrm{mod.}\frac{k}{\delta}\right)$$

sein muss. Denn da $m(a-b)$ durch k, also $m'(a-b)$ durch k' theilbar, und m' relative Primzahl gegen k' ist, so muss $(a-b)$ durch k' theilbar sein.

7. Ist

$$a \equiv b \pmod{k}$$

und m irgend ein Divisor von k, so ist auch

$$a \equiv b \pmod{m}.$$

Denn $a-b$ ist ein Multiplum von k, und k ein Multiplum von m; also ist $a-b$ auch ein Multiplum von m.

8. Ist

$a \equiv b \pmod{k}$ und $a \equiv b \pmod{l}$ und $a \equiv b \pmod{m}$ u. s. w., so ist auch

$$a \equiv b \pmod{h},$$

wo h das kleinste gemeinschaftliche Multiplum von $k, l, m \ldots$ bezeichnet. Denn $a-b$ ist ein gemeinschaftliches Multiplum aller dieser Zahlen, also auch Multiplum von h.

Hieraus folgt auch noch als ein besonders bemerkenswerther specieller Fall, dass, wenn eine Congruenz richtig ist in Bezug auf eine Reihe von Moduln, die sämmlich unter einander relative Primzahlen sind, dieselbe auch in Bezug auf einen Modul gilt, welcher das Product aus allen jenen Moduln ist.

Wir bemerken schliesslich, dass auch *negative* Moduln k zugelassen werden; das Zeichen $a \equiv b \pmod{k}$ bedeutet auch dann,