## 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

**LOG Id:** LOG_0029
**LOG Titel:** § 22. Congruenz ersten Grades mit einer Unbekannten; Kriterium ihrer Möglichkeit; erste Methode der Auflösung
**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

selben Congruenz; man sieht alle solche einander congruenten Wurzeln daher nur wie eine einzige Wurzel an, und das Problem der vollständigen Auflösung der Congruenz kommt daher darauf zurück, alle unter einander *incongruenten* Wurzeln derselben aufzufinden.

Ferner leuchtet ein, dass jede Wurzel der obigen Congruenz, sobald

$$a \equiv a',\ b \equiv b' \ldots g \equiv g',\ h \equiv h' \pmod{k}$$

ist, auch eine Wurzel der Congruenz

$$a'x^m + b'x^{m-1} + \cdots + g'x + h' \equiv 0 \pmod{k}$$

sein wird, und umgekehrt. Beide Congruenzen sind daher auch nur wie eine und dieselbe anzusehen; denn beide stellen an die Unbekannte $x$ genau dieselbe Forderung. Hieraus erhellt unmittelbar, dass man aus jeder Congruenz von der obigen Form ohne Weiteres alle diejenigen Glieder fortstreichen darf, deren Coefficienten durch den Modul theilbar sind; der Exponent der höchsten Potenz von $x$, welche nach dieser vorläufigen Ausscheidung zurückbleibt, heisst dann der *Grad* dieser Congruenz; ist z. B. in der obigen Congruenz der erste Coefficient $a$ nicht durch den Modul $k$ theilbar, so heisst dieselbe eine Congruenz $m$ten Grades.

Wenden wir diese Benennungen z. B. auf die Congruenz

$$x^{\varphi(k)} \equiv 1 \pmod{k}$$

an, so müssen wir sagen, dass dieselbe genau ebenso viele (incongruente) Wurzeln besitzt, als ihr Grad $\varphi(k)$ Einheiten enthält; denn erstens genügen alle relativen Primzahlen gegen den Modul der Congruenz, und diese zerfallen in $\varphi(k)$ Classen; und zweitens kann die Congruenz keine andern Wurzeln haben als diese; denn der grösste gemeinschaftliche Divisor $\delta$ einer Wurzel $x$ und des Modul $k$ ist auch gemeinschaftlicher Divisor der Zahlen $x^{\varphi(k)}$ und $k$, folglich auch (§. 18) der Zahlen 1 und $k$; folglich kann $\delta$ nur $= 1$ sein.

## §. 22.

Wir wenden uns nun nach den vorhergehenden allgemeinen Erörterungen zu dem einfachsten speciellen Fall, nämlich zu der Congruenz ersten Grades, welcher man offenbar durch Transposition des bekannten Gliedes stets die Form

$$ax \equiv b \pmod{k} \qquad (1)$$

geben kann. Betrachten wir auch hier zunächst nur den speciellen Fall, in welchem der Coefficient $a$ relative Primzahl gegen den Modul $k$ ist, so ergiebt sich unmittelbar, dass diese Congruenz stets eine, aber auch nur eine Wurzel hat. Denn wir haben früher (§. 18) gesehen, dass die Werthe des Ausdrucks $ax$, welche man erhält, wenn man für $x$ sämmtliche $k$ Individuen eines vollständigen Systems incongruenter Zahlen einsetzt, wieder ein solches System bilden; unter den Werthen dieses Ausdrucks wird sich daher auch einer und nur einer finden, welcher derselben Classe angehört wie $b$, d. h. welcher $\equiv b$ ist. Der verallgemeinerte Fermat'sche Satz giebt nun auch ein Mittel an die Hand, die Wurzel dieser Congruenz unmittelbar zu bestimmen; offenbar genügt jede Zahl

$$x \equiv b \cdot a^{\varphi(k)-1} \pmod{k}$$

der obigen Congruenz. So findet man z. B., dass alle Wurzeln der Congruenz

$$2x \equiv -3 \pmod{15}$$

durch die Formel

$$x \equiv -3 \cdot 2^7 \equiv 6 \pmod{15}$$

gegeben werden.

Wenden wir uns nun dem allgemeinen Fall zu und nehmen wir an, es sei $\delta$ der grösste gemeinschaftliche Divisor des Coefficienten $a$ und des Modul $k$, so leuchtet zunächst ein, dass, wenn die Congruenz überhaupt eine Wurzel $x$ besitzt, auch $b$ durch $\delta$ theilbar sein muss; denn da $ax$ mit dem Modul $k$ den gemeinschaftlichen Divisor $\delta$ hat, so muss auch $b \equiv ax$ durch $\delta$ theilbar sein. Dies ist also eine unerlässliche Bedingung für die Möglichkeit der Congruenz; dass sie auch hinreichend für dieselbe ist, wird sich sogleich zeigen.

Gesetzt nun, es sei $x$ eine Wurzel der Congruenz, also

$$ax = b + mk,$$

wo $m$ irgend eine ganze Zahl, so folgt hieraus, wenn $a = a'\delta$, $b = b'\delta$, $k = k'\delta$ gesetzt wird, $a'x = b' + mk'$, d. h. jede Wurzel der ursprünglichen Congruenz ist auch Wurzel der Congruenz

$$a'x \equiv b' \pmod{k'} \qquad (2)$$

und umgekehrt überzeugt man sich sogleich, dass jede Wurzel dieser letztern Congruenz auch eine Wurzel der erstern sein wird.

Die beiden Congruenzen (1) und (2) stimmen daher hinsichtlich ihrer Wurzeln vollständig mit einander überein; da nun in der letztern der Coefficient $a'$ relative Primzahl gegen den Modul $k'$ ist, so haben wir wieder den frühern Fall: diese Congruenz ist stets lösbar, und alle ihr genügenden Zahlen bilden in Bezug auf ihren Modul $k'$ nur eine einzige Classe, in der Weise, dass, wenn $\alpha$ eine bestimmte derselben ist, alle andern in der Form

$$x = \alpha + zk' \qquad (3)$$

enthalten sind, wo $z$ jede beliebige ganze Zahl bedeutet. Da nun alle diese Zahlen auch die sämmtlichen Wurzeln der Congruenz (1) bilden, so fragt es sich nur noch, wie viele in Bezug auf den Modul $k$ incongruente Zahlen unter ihnen sich vorfinden. Irgend zwei in der Reihe (3) enthaltene Zahlen $\alpha + zk'$ und $\alpha + z'k'$ werden offenbar stets und auch nur dann congruent in Bezug auf den Modulus $k$ sein, sobald $(z' - z)k'$ durch $k = k'\delta$, und also $z' - z$ durch $\delta$ theilbar ist; diese beiden Zahlen werden also einer und derselben Classe, oder verschiedenen Classen in Bezug auf den Modul $k$ angehören, je nachdem die beiden Zahlen $z$ und $z'$ einer und derselben Classe, oder verschiedenen Classen in Bezug auf den Modulus $\delta$ angehören; woraus unmittelbar folgt, dass die Reihe (3) sämmtliche Individuen von $\delta$ verschiedenen Classen in Bezug auf den Modul $k$ enthält, und es leuchtet ein, dass die folgenden $\delta$ Zahlen

$$\alpha,\ \alpha + k',\ \alpha + 2k' \ \ldots\ \alpha + (\delta - 1)k'$$

aus jeder dieser $\delta$ Classen einen Repräsentanten enthalten. Wir haben mithin folgendes allgemeine Resultat gewonnen:

*Damit die Congruenz*

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

*überhaupt Wurzeln besitze, ist erforderlich, dass b durch den grössten gemeinschaftlichen Divisor $\delta$ der beiden Zahlen a und k theilbar sei; ist diese Bedingung erfüllt, so hat die Congruenz genau $\delta$ incongruente Wurzeln.*

Es ist zu bemerken, dass in dem früher behandelten Fall, in welchem $\delta = 1$ ist, die erforderliche Bedingung stets erfüllt ist, ferner, dass dieser Satz auch noch für den Fall $\delta = k$, in welchem also $a \equiv 0 \pmod{k}$ ist, seine Gültigkeit behält, indem, sobald $b$ ebenfalls $\equiv 0 \pmod{k}$ ist, jede beliebige Zahl $x$ dieser identischen Congruenz Genüge leistet.

Um auch ein Beispiel für den allgemeinen Fall zu behandeln, nehmen wir die Congruenz