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_0045
LOG Titel: §. 37. Fall, in welchem der Modulus eine beliebige Zahl ist
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

sein. Da nun die Differenz der beiden Factoren $\frac{1}{2}(x-\alpha)$ und $\frac{1}{2}(x+\alpha)$ eine ungerade Zahl ist, so muss einer von ihnen ungerade, und der andere folglich theilbar durch $2^{\pi-2}$ sein. Dies giebt folgende Fälle:

$$x \equiv \alpha \pmod{2^{\pi-1}} \quad \text{oder} \quad x \equiv -\alpha \pmod{2^{\pi-1}}$$

und diese liefern wieder folgende vier Fälle:

$$x \equiv \alpha \pmod{2^{\pi}}; \qquad x \equiv \alpha + 2^{\pi-1} \pmod{2^{\pi}};$$
$$x \equiv -\alpha \pmod{2^{\pi}}; \quad x \equiv -\alpha - 2^{\pi-1} \pmod{2^{\pi}}.$$

Und umgekehrt überzeugt man sich leicht, dass jede dieser vier in Bezug auf den Modul 2^{π} incongruenten Zahlen der Congruenz genügt.

Wir fassen die ganze Untersuchung in folgendem Satze zusammen:

Die Congruenz

$$x^2 \equiv D \pmod{2^{\pi}}$$

ist stets möglich, wenn $\pi = 1$, *und hat dann eine Wurzel; sie ist, wenn* $\pi = 2$, *stets und nur dann möglich, wenn* $D \equiv 1 \pmod{4}$ *und sie hat dann zwei Wurzeln; sie ist, wenn* $\pi \geqq 3$, *stets und nur dann möglich, wenn* $D \equiv 1 \pmod{8}$ *ist, und zwar hat sie dann vier Wurzeln.*

§. 37.

Es ist jetzt leicht, die Möglichkeit und die Anzahl der Wurzeln der Congruenz $x^2 \equiv D$ für einen beliebigen Modulus zu beurtheilen, der relative Primzahl zu D ist. Wir führen diese Untersuchung ganz allgemein in folgender Weise.

Es seien $a, b, c \ldots$ relative Primzahlen zu einander, und

$$f(x) \equiv 0 \pmod{abc \ldots} \tag{1}$$

eine beliebige zur Auflösung vorgelegte Congruenz, so lässt dieselbe sich stets auf die vollständige Auflösung der Congruenzen

$$\left.\begin{aligned} f(x) &\equiv 0 \pmod{a} \\ f(x) &\equiv 0 \pmod{b} \\ f(x) &\equiv 0 \pmod{c} \end{aligned}\right\} \tag{2}$$

u. s. w.

zurückführen. Zunächst leuchtet ein, dass jede Wurzel x der Congruenz (1) auch allen Congruenzen (2) genügen muss; es wird daher die Congruenz (1) unmöglich sein, wenn dies mit irgend einer der Congruenzen (2) der Fall ist. Umgekehrt, ist α irgend eine Wurzel der Congruenz $f(x) \equiv 0 \pmod{a}$, ebenso β irgend eine Wurzel der Congruenz $f(x) \equiv 0 \pmod{b}$, γ eine Wurzel der Congruenz $f(x) \equiv 0 \pmod{c}$ u. s. w., so bestimme man (nach §. 25) eine Zahl x durch das System von Congruenzen

$$\left.\begin{aligned} x &\equiv \alpha \pmod{a} \\ x &\equiv \beta \pmod{b} \\ x &\equiv \gamma \pmod{c} \end{aligned}\right\} \quad (3)$$

u. s. w.,

so wird

$$\begin{aligned} f(x) &\equiv f(\alpha) \equiv 0 \pmod{a} \\ f(x) &\equiv f(\beta) \equiv 0 \pmod{b} \\ f(x) &\equiv f(\gamma) \equiv 0 \pmod{c} \end{aligned}$$

u. s. w.

und folglich, da $a, b, c \ldots$ relative Primzahlen zu einander sind, auch

$$f(x) \equiv 0 \pmod{abc \ldots},$$

d. h. jede dem System (3) genügende Zahl x ist eine Wurzel der vorgelegten Congruenz (1). Da nun (nach §. 25) dem System (3) unendlich viele Zahlen x genügen, welche aber alle nach dem Modul $abc \ldots$ einander congruent sind, so liefert das System (3), eine und nur eine Wurzel x der Congruenz (1). Ist nun

λ die Anzahl aller incongruenten Wurzeln $\alpha \pmod{a}$
μ „ „ „ „ „ $\beta \pmod{b}$
ν „ „ „ „ „ $\gamma \pmod{c}$

u. s. w.

so kann man im Ganzen $\lambda\mu\nu \ldots$ verschiedene Systeme (3) bilden, welchen (nach §. 25) ebensoviele verschiedene Wurzeln x der Congruenz (1) entsprechen; und andere Wurzeln kann diese letztere nicht besitzen, weil, wie schon oben bemerkt ist, jede bestimmte Wurzel x der Congruenz (1) auch Wurzel aller Congruenzen (2) und folglich einem bestimmten $\alpha \pmod{a}$, einem bestimmten $\beta \pmod{b}$, einem bestimmten $\gamma \pmod{c}$ u. s. f. congruent sein muss. Mithin ist die Anzahl aller nach dem Modul $abc \ldots$ incongruenten Wurzeln der vorgelegten Congruenz $= \lambda\mu\nu \ldots$