Werk

Titel: Vorlesungen über Zahlentheorie

Autor: Dirichlet, Peter

Verlag: Vieweg

Ort: Braunschweig

Jahr: 1871

Kollektion: Mathematica

Werk Id: PPN30976923X

PURL: http://resolver.sub.uni-goettingen.de/purl?PID=PPN30976923X|LOG_0043

OPAC: http://opac.sub.uni-goettingen.de/DB=1/PPN?PPN=30976923X

Contact

Niedersächsische Staats- und Universitätsbibliothek Göttingen
Georg-August-Universität Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen
Germany
Email: gdz@sub.uni-goettingen.de

langt, welche vorher aus der allgemeinen Theorie der binomischen Congruenzen abgeleitet waren.

§. 35.

Wir wenden uns jetzt zu der Untersuchung des Falls, in welchem der Modul k der quadratischen Congruenz

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

die Potenz einer Primzahl p ist; dabei müssen wir den Fall, in welchem $p = 2$, gesondert von den übrigen behandeln, in welchen p eine ungerade Primzahl ist*).

Ist zunächst p eine ungerade Primzahl, und $k = p^\pi$, wo π irgend eine positive ganze Zahl bedeutet, und nehmen wir an, die Congruenz

$$x^2 \equiv D \pmod{p^\pi} \qquad (1)$$

sei möglich, so überzeugt man sich leicht, dass sie im Ganzen zwei incongruente Wurzeln hat; denn ist α eine bestimmte, und x irgend eine Wurzel, so muss

$$x^2 - \alpha^2 = (x-\alpha)\ (x+\alpha) \equiv 0 \pmod{p^\pi}$$

sein; von den beiden Factoren $x-\alpha$ und $x+\alpha$ ist aber nur einer durch p theilbar; denn wären beide durch p theilbar, so wäre auch ihre Differenz 2α, und folglich auch α durch p theilbar, was nicht der Fall ist, da wir $D \equiv \alpha^2$ als nicht theilbar durch p vorausgesetzt haben. Da also einer der beiden Factoren relative Primzahl gegen p^π ist, so muss der andere für sich allein durch p^π theilbar sein. Es ist daher entweder

$$x \equiv \alpha \pmod{p^\pi}, \quad \text{oder} \quad x \equiv -\alpha \pmod{p^\pi};$$

also hat die Congruenz (1) entweder gar keine Wurzel, oder sie hat zwei incongruente Wurzeln α und $-\alpha$.

Es ist nun noch zu entscheiden, wann das Eine, wann das Andere Statt finden wird. Da nun jede Wurzel α der Congruenz (1) auch eine Wurzel der Congruenz

$$x^2 \equiv D \pmod{p} \qquad (2)$$

ist, so leuchtet ein, dass die Congruenz (1) nur dann möglich ist, wenn D quadratischer Rest von p ist; es fragt sich daher nur, ob

*) Die nachfolgenden Resultate lassen sich auch aus dem in §. 145 bewiesenen Satze ableiten.

auch umgekehrt, wenn D quadratischer Rest von p ist, hieraus die Möglichkeit der Congruenz (1) folgt. Um dies zu zeigen, brauchen wir nur nachzuweisen, dass, sobald die Congruenz (2) eine Wurzel α besitzt (also D quadratischer Rest von p ist), hieraus sich eine Wurzel der Congruenz (1) ableiten lässt, welche $\equiv \alpha \pmod{p}$ ist; und da Aehnliches von jeder Congruenz $x^2 \equiv D \pmod{k}$ gilt, wo D stets dieselbe Zahl, k aber irgend eine Potenz der Primzahl p ist, so braucht man nur zu zeigen, dass aus einer Wurzel α der Congruenz (1) sich eine Wurzel der Congruenz

$$x^2 \equiv D \pmod{p^{\pi+1}} \tag{3}$$

ableiten lässt, welche $\equiv \alpha \pmod{p^\pi}$ ist. Es sei daher

$$\alpha^2 \equiv D \pmod{p^\pi} \quad \text{oder} \quad \alpha^2 - D = hp^\pi,$$

so setzen wir

$$x = \alpha + p^\pi y,$$

woraus

$$x^2 - D = hp^\pi + 2\alpha p^\pi y + p^{2\pi} y^2 \equiv p^\pi (h + 2\alpha y) \pmod{p^{\pi+1}}$$

folgt; damit nun $x^2 \equiv D \pmod{p^{\pi+1}}$ werde, braucht y nur so bestimmt zu werden, dass

$$2\alpha y \equiv -h \pmod{p}$$

werde; da nun D, folglich auch α und also, da p ungerade ist, auch 2α eine durch p nicht theilbare Zahl ist, so lässt sich y stets so wählen, dass es dieser Congruenz ersten Grades genügt. Wir sehen also, dass aus der Möglichkeit der Congruenz (1) auch stets die Möglichkeit der Congruenz (3) folgt; durch dieselbe wiederholt angewendete Schlussweise ergiebt sich also auch, dass aus der Möglichkeit der Congruenz (2) stets die der Congruenz (1) folgt, und wir haben auch eine Methode gefunden, um aus einer Wurzel der Congruenz $x^2 \equiv D$ für den Modul p successive eine Wurzel derselben Congruenz für die Moduln p^2, $p^3 \ldots p^\pi$ zu gewinnen. Wir haben mithin folgendes Resultat:

Ist p eine ungerade Primzahl, und D eine durch p nicht theilbare Zahl, so ist für die Möglichkeit der Congruenz

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

erforderlich und hinreichend, dass

$$\left(\frac{D}{p}\right) = 1,$$

d. h. dass D quadratischer Rest von p sei; sobald diese Bedingung erfüllt ist, besitzt die vorgelegte Congruenz zwei incongruente Wur-