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_0042

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

die positive oder negative Einheit, je nachdem die durch die Primzahl p nicht theilbare Zahl m quadratischer Rest oder Nichtrest von p ist; es ist daher stets

$$\left(\frac{m}{p}\right)\left(\frac{m}{p}\right) = +1 \quad \text{und} \quad m^{\frac{p-1}{2}} \equiv \left(\frac{m}{p}\right) \pmod{p}.$$

Den Satz über den Charakter eines Productes kann man dann offenbar durch die folgende Gleichung ausdrücken:

$$\left(\frac{mnl\ldots}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{n}{p}\right)\left(\frac{l}{p}\right)\cdots$$

Es leuchtet ferner ein, dass, sobald $m \equiv n \pmod{p}$, auch

$$\left(\frac{m}{p}\right) = \left(\frac{n}{p}\right)$$

sein wird.

§. 34.

Es ist nun interessant zu sehen, dass die soeben gewonnenen Sätze, welche zum Theil als Resultate einer ausgedehnten Theorie, wie der der binomischen Congruenzen, erscheinen, sich aus den ersten Principien auf einem ganz elementaren Wege ableiten lassen, der zugleich einen neuen Beweis des Wilson'schen und Fermat'schen Satzes liefern wird.

Es sei D irgend eine durch die (ungerade) Primzahl p nicht theilbare Zahl, und r irgend eine der Zahlen

$$1, 2, 3 \ldots (p-1); \tag{1}$$

dann existirt in derselben Reihe stets eine und nur eine Zahl s von der Beschaffenheit, dass

$$rs \equiv D \pmod{p}$$

ist; denn diese Zahl s ist ja die Wurzel der Congruenz ersten Grades $rx \equiv D \pmod{p}$; je zwei solche Zahlen r und s der Reihe (1), deren Product $\equiv D$ ist, wollen wir *zusammengehörige* Zahlen nennen; offenbar ist durch eine dieser beiden Zahlen die andere ebenfalls bestimmt. Identisch können diese beiden Zahlen nur dann werden, wenn die Congruenz

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

möglich ist. Danach theilen wir unsere Untersuchung in zwei Fälle ein.

Erstens: Die Congruenz (2) ist unmöglich. — Dann sind also je zwei zusammengehörige Zahlen von einander verschieden, und da zwei solche Paare stets identisch sind, sobald sie nur eine gemeinschaftliche Zahl haben, so zerfallen die sämmtlichen $p-1$ Zahlen (1) in $\frac{1}{2}(p-1)$ solche Paare zusammengehöriger Zahlen, und folglich ist ihr Product

$$1 \cdot 2 \cdot 3 \ldots (p-1) \equiv D^{\frac{p-1}{2}} \pmod{p}. \qquad (3)$$

Zweitens: Die Congruenz (2) ist möglich. — Dann existirt also auch in der Reihe (1) mindestens eine Zahl ϱ von der Beschaffenheit, dass $\varrho^2 \equiv D$; sehen wir zu, ob ausser ϱ in der Reihe (1) noch eine solche Zahl σ existirt; dann muss $\sigma^2 \equiv \varrho^2$, folglich $(\sigma-\varrho)(\sigma+\varrho)$ durch p theilbar sein; da wir σ verschieden von ϱ voraussetzen, so ist $\sigma-\varrho$ nicht theilbar durch p, folglich muss $\sigma+\varrho$ theilbar durch p, also $\sigma = p-\varrho$ sein; und in der That ist wirklich $(p-\varrho)^2 \equiv D$. Trennen wir nun diese beiden (wirklich ungleichen) Zahlen ϱ und $\sigma = p-\varrho$, deren Product $\varrho\sigma \equiv -\varrho^2 \equiv -D$ ist, von den übrigen der Reihe (1), so zerfallen die letztern in $\frac{1}{2}(p-3)$ Paare zusammengehöriger Zahlen von der Beschaffenheit, dass jedes Paar aus zwei verschiedenen Zahlen besteht. Demnach ist in diesem Fall das Product aller Zahlen der Reihe (1):

$$1 \cdot 2 \cdot 3 \ldots (p-1) \equiv -D^{\frac{p-1}{2}} \pmod{p}. \qquad (4)$$

Nun giebt es aber einen Fall, in welchem die Congruenz (2) stets möglich ist, nämlich den, in welchem $D = 1 = 1^2$; wir erhalten daher zunächst aus (4) den Satz von *Wilson:*

$$1 \cdot 2 \cdot 3 \ldots (p-1) \equiv -1 \pmod{p}, \qquad (5)$$

und substituiren wir dies in die Congruenzen (3) und (4), so erhalten wir das Resultat, dass

$$D^{\frac{p-1}{2}} \equiv +1 \quad \text{oder} \quad \equiv -1 \pmod{p}$$

ist, je nachdem die Congruenz (2) möglich oder nicht möglich ist. Da endlich ein dritter Fall nicht existiren kann, so erhalten wir allgemein

$$D^{p-1} = (D^{\frac{p-1}{2}})^2 \equiv (\pm 1)^2 \equiv +1 \pmod{p},$$

also den Satz von *Fermat.*

Durch diese einfache Betrachtung sind wir also sogleich bis zu denselben Sätzen in der Theorie der quadratischen Reste ge-