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_0126

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

§. 116.

Für den Fall, dass p eine ungerade Primzahl, und h irgend eine durch p nicht theilbare ganze Zahl ist, haben wir im vorigen Paragraphen folgende Gleichung erhalten

$$\Sigma \left(\frac{s}{p}\right) e^{s \frac{2h\pi i}{p}} = \left(\frac{h}{p}\right) \varphi(1, p),$$

welche, wenn man den für $\varphi(1, p)$ gefundenen Werth einsetzt, in die folgende übergeht:

$$\Sigma \left(\frac{s}{p}\right) e^{s \frac{2h\pi i}{p}} = \left(\frac{h}{p}\right) i^{\frac{1}{4}(p-1)^2} \sqrt{p}; \tag{1}$$

soll dieselbe auch für den vorher ausgeschlossenen Fall, in welchem $h \equiv 0 \pmod{p}$ ist, ihre Gültigkeit behalten, so müssen wir übereinkommen, immer

$$\left(\frac{h}{p}\right) = 0$$

zu setzen, wenn h durch p theilbar ist; denn die linke Seite der Gleichung wird

$$\Sigma \left(\frac{s}{p}\right) = 0,$$

weil die Anzahl der quadratischen Reste genau gleich ist der Anzahl der quadratischen Nichtreste. Nach dieser Erweiterung des von Legendre eingeführten Zeichens wird ferner, wenn man an der in §. 46 gegebenen Erklärung des Jacobi'schen Symbols festhält, stets

$$\left(\frac{m}{P}\right) = 0,$$

wenn m keine relative Primzahl zu P ist.

Die Gleichung (1) gilt jetzt allgemein für jede positive ungerade Primzahl p, wenn h irgend eine ganze Zahl bedeutet, und die Summation linker Hand darf auch auf die Zahlclasse $s \equiv 0 \pmod{p}$ ausgedehnt werden. Wir wollen nun zeigen, dass dieser Satz über ungerade positive Primzahlen p sich genau in derselben Fassung auch auf jede positive ungerade zusammengesetzte Zahl P übertragen lässt, welche durch keine Quadratzahl (ausser 1) theilbar ist. Wir setzen also

$$P = pp'p'' \ldots$$

wo $p, p', p'' \ldots$ lauter positive ungerade und von einander verschiedene Primzahlen bedeuten, und führen der Bequemlichkeit halber folgende Bezeichnung ein:

$$\frac{P}{p} = Q, \quad \frac{P}{p'} = Q', \quad \frac{P}{p''} = Q'' \ldots$$

Schreiben wir nun für jede der Primzahlen $p, p', p'' \ldots$ die obige Gleichung (1) auf:

$$\Sigma \left(\frac{s}{p}\right) e^{s \frac{2h\pi i}{p}} = \left(\frac{h}{p}\right) i^{1/4(p-1)^2} \sqrt{p}$$

$$\Sigma \left(\frac{s'}{p'}\right) e^{s' \frac{2h\pi i}{p'}} = \left(\frac{h}{p'}\right) i^{1/4(p'-1)^2} \sqrt{p'}$$

$$\Sigma \left(\frac{s''}{p''}\right) e^{s'' \frac{2h\pi i}{p''}} = \left(\frac{h}{p''}\right) i^{1/4(p''-1)^2} \sqrt{p''}$$

$$\cdots\cdots\cdots\cdots\cdots$$

und setzen wir zur Abkürzung

$$s\,Q + s'\,Q' + s''\,Q'' + \cdots = m,$$

so ergiebt, da auch nach der neuen Erweiterung des Legendre'schen Symbols stets

$$\left(\frac{h}{p}\right)\left(\frac{h}{p'}\right)\left(\frac{h}{p''}\right) \cdots = \left(\frac{h}{P}\right)$$

ist, die Multiplication aller dieser Gleichungen folgendes Resultat

$$\begin{aligned} &\Sigma \left(\frac{s}{p}\right)\left(\frac{s'}{p'}\right)\left(\frac{s''}{p''}\right) \ldots e^{m \frac{2h\pi i}{P}} \\ &= \left(\frac{h}{p}\right) i^{1/4(p-1)^2 + 1/4(p'-1)^2 + 1/4(p''-1)^2 + \cdots} \sqrt{P}, \end{aligned} \qquad (2)$$

wo $\sqrt{P}$ wieder positiv zu nehmen ist, und das Summenzeichen linker Hand sich auf alle $pp'p'' \ldots = P$ Combinationen aller Werthe von $s, s', s'' \ldots$ bezieht. Zunächst leuchtet nun ein, dass je zwei verschiedenen dieser Combinationen auch zwei nach dem Modulus P incongruente Werthe von m entsprechen; denn aus

$$sQ + s'Q' + s''Q'' + \cdots \equiv tQ + t'Q' + t''Q'' + \cdots \pmod{P}$$

würde, da Q', Q'' ... sämmtlich $\equiv 0 \pmod{p}$ sind, folgen, dass

$$sQ \equiv tQ \pmod{p},$$

und, da Q relative Primzahl zu p ist, auch

$$s \equiv t \pmod{p}$$

wäre; ähnlich würde aus derselben Annahme gleichzeitig

$$s' \equiv t' \pmod{p'};\quad s'' \equiv t'' \pmod{p''} \ldots$$

folgen, so dass also die beiden Combinationen $s, s', s'' \ldots$ und $t, t', t'' \ldots$ identisch wären. In der That durchläuft also m ein vollständiges Restsystem in Bezug auf den Modulus P. Ferner ist nun

$$\left(\frac{m}{p}\right) = \left(\frac{sQ + s'Q' + s''Q'' + \cdots}{p}\right) = \left(\frac{sQ}{p}\right) = \left(\frac{s}{p}\right)\left(\frac{Q}{p}\right),$$

und ebenso

$$\left(\frac{m}{p'}\right) = \left(\frac{s'}{p'}\right)\left(\frac{Q'}{p'}\right),\quad \left(\frac{m}{p''}\right) = \left(\frac{s''}{p''}\right)\left(\frac{Q''}{p''}\right)\cdots,$$

folglich auch, wenn man alle diese Gleichungen multiplicirt,

$$\left(\frac{m}{P}\right) = \left(\frac{s}{p}\right)\left(\frac{s'}{p'}\right)\left(\frac{s''}{p''}\right)\cdots\left(\frac{Q}{p}\right)\left(\frac{Q'}{p'}\right)\left(\frac{Q''}{p''}\right)\cdots$$

Multiplicirt man daher beide Seiten der obigen Gleichung (2) mit

$$\left(\frac{Q}{p}\right)\left(\frac{Q'}{p'}\right)\left(\frac{Q''}{p''}\right)\cdots,$$

so erhält man

$$\Sigma\left(\frac{m}{P}\right)e^{m\frac{2h\pi i}{P}} = \left(\frac{Q}{p}\right)\left(\frac{Q'}{p'}\right)\left(\frac{Q''}{p''}\right)\cdots\left(\frac{h}{P}\right)i^{\Sigma 1/4(p-1)^2}\sqrt{P},$$

wo rechts zur Abkürzung

$$\left(\frac{p-1}{2}\right)^2 + \left(\frac{p'-1}{2}\right)^2 + \left(\frac{p''-1}{2}\right)^2 + \cdots = \Sigma\left(\frac{p-1}{2}\right)^2$$

gesetzt ist. Da nun ferner

$$\left(\frac{Q}{p}\right) = \left(\frac{p'}{p}\right)\left(\frac{p''}{p}\right)\cdots$$

$$\left(\frac{Q'}{p'}\right) = \left(\frac{p}{p'}\right)\left(\frac{p''}{p'}\right)\cdots$$

$$\left(\frac{Q''}{p''}\right) = \left(\frac{p}{p''}\right)\left(\frac{p'}{p''}\right)\cdots$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

ist, so erhält man durch Multiplication

$$\left(\frac{Q}{p}\right)\left(\frac{Q'}{p'}\right)\left(\frac{Q''}{p''}\right)\cdots = \Pi\left(\frac{p}{p'}\right)\left(\frac{p'}{p}\right),$$

wo das Productzeichen Π sich auf alle möglichen Paare von je zwei verschiedenen Primzahlen p, p' bezieht. Da nun nach dem Reciprocitätssatze

$$\left(\frac{p}{p'}\right)\left(\frac{p'}{p}\right) = (-1)^{\frac{1}{2}(p-1)\cdot\frac{1}{2}(p'-1)} = i^{\frac{1}{2}(p-1)(p'-1)}$$

ist, so erhält man

$$\left(\frac{Q}{p}\right)\left(\frac{Q'}{p'}\right)\left(\frac{Q''}{p''}\right)\cdots = i^{2\Sigma\frac{1}{2}(p-1)\cdot\frac{1}{2}(p'-1)},$$

wo das Summenzeichen rechter Hand sich wieder auf alle Combinationen von je zwei verschiedenen Primzahlen p, p' bezieht; es ist ferner

$$\Sigma\left(\frac{p-1}{2}\right)^2 + 2\,\Sigma\,\frac{p-1}{2}\,\frac{p'-1}{2}$$
$$= \left(\frac{p-1}{2} + \frac{p'-1}{2} + \frac{p''-1}{2} + \cdots\right)^2,$$

folglich

$$\Sigma\left(\frac{m}{P}\right)e^{m\frac{2h\pi i}{P}} = \left(\frac{h}{P}\right)i^{[\frac{1}{2}(p-1)+\frac{1}{2}(p'-1)+\cdots]^2}\sqrt{P}.$$

Da endlich (vergl. §. 46)

$$P = (1+(p-1))(1+(p'-1))(1+(p''-1))\ldots$$
$$\equiv 1 + (p-1) + (p'-1) + (p''-1) + \cdots \pmod{4}$$

und folglich

$$\frac{P-1}{2} \equiv \frac{p-1}{2} + \frac{p'-1}{2} + \frac{p''-1}{2} + \cdots \pmod{2}$$

und hieraus

$$\left(\frac{P-1}{2}\right)^2 \equiv \left(\frac{p-1}{2} + \frac{p'-1}{2} + \frac{p''-1}{2}\cdots\right)^2 \pmod{4}$$

ist, so ergiebt sich schliesslich

$$\Sigma\left(\frac{m}{P}\right)e^{m\frac{2h\pi i}{P}} = \left(\frac{h}{P}\right)i^{\frac{1}{4}(P-1)^2}\sqrt{P},$$

worin der zu beweisende Satz besteht. Nimmt man $h \equiv 0 \pmod{P}$, so erhält man wieder den (in §. 52. I. bewiesenen) Satz

$$\Sigma\left(\frac{m}{P}\right) = 0.$$