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_0059
LOG Titel: §. 51. Zweiter Theil des Beweises für den Reciprocitätssatz
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

$$M = 1 \cdot 2 \cdot 3 \cdot 4 \ldots\ldots (2m)\ (2m+1);$$

es giebt daher positive Zahlen k von der Beschaffenheit, dass

$$q \equiv k^2 \pmod{M}$$

ist, und zwar muss k relative Primzahl zu M sein, weil $2m+1 < q$ und also auch q relative Primzahl zu M ist. Aus dieser Congruenz folgt nun weiter, dass in Bezug auf den Modul M

$$k(q-1^2)\ (q-2^2)\ (q-3^2) \ldots (q-m^2)$$
$$\equiv k(k^2-1^2)\ (k^2-2^2)\ (k^2-3^2) \ldots (k^2-m^2)$$
$$\equiv (k+m)\ (k+m-1) \ldots (k+1)\ k(k-1) \ldots (k-m+1)\ (k-m)$$

ist; da nun nach einem frühern Satze (§. 15) jedes Product von $(2m+1)$ successiven ganzen Zahlen durch M theilbar, und ausserdem k relative Primzahl zu M ist, so ist das Product

$$(q-1^2)\ (q-2^2)\ (q-3^2) \ldots (q-m^2)$$

theilbar durch das Product

$$M = (m+1)\ ((m+1)^2-1^2)\ ((m+1)^2-2^2) \ldots ((m+1)^2-m^2)$$

d. h. das Product

$$\frac{1}{m+1} \cdot \frac{q-1^2}{(m+1)^2-1^2} \cdot \frac{q-2^2}{(m+1)^2-2^2} \cdots \frac{q-m^2}{(m+1)^2-m^2}$$

ist nothwendig eine ganze Zahl.

Andererseits leuchtet ein, dass dies Product gewiss keine ganze Zahl ist, sobald für m die grösste ganze Zahl unterhalb $\sqrt{q}$ genommen wird; denn, wenn $m < \sqrt{q} < m+1$ ist, so sind alle Factoren dieses Productes echte Brüche. Da nun ausserdem $2m+1 < 2\sqrt{q}+1 < q$ ist, so kann für diese Zahl m die Annahme nicht zulässig sein, und wir haben daher folgenden Satz gewonnen:

Ist q eine Primzahl von der Form $8n+1$, so giebt es unterhalb $2\sqrt{q}+1$ und folglich auch unterhalb q mindestens eine ungerade Primzahl p', von welcher q quadratischer Nichtrest ist.

§. 51.

Nachdem für jede Primzahl q von der Form $4n+1$ die Existenz einer Primzahl $p' < q$ nachgewiesen ist, von welcher q quadratischer Nichtrest ist, gehen wir zum Beweise unseres zweiten Theiles über. Jede solche Primzahl p' muss Nichtrest von q sein;

denn wäre p' Rest von q, so würde aus dem schon von uns bewiesenen Theil (§. 49)

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

folgen, was mit der Voraussetzung streitet. Mithin gilt für diese Primzahl p' das Reciprocitätsgesetz. Giebt es nun *ausser* p' noch *andere* ungerade Primzahlen $p < q$, welche Nichtreste von q sind, so ist nur zu beweisen, dass

$$\left(\frac{q}{pp'}\right) = +1$$

ist, weil hieraus sogleich folgt, dass q Nichtrest von p ist. Da nun der Voraussetzung nach p' und p quadratische Nichtreste von q sind, so ist pp' quadratischer Rest von q, und es giebt daher wieder eine gerade Zahl $e < q$ von der Beschaffenheit, dass

$$e^2 - pp' = q\varphi$$

und φ eine ganze Zahl ist; und weil die linke Seite dieser Gleichung eine ungerade Zahl darstellt, welche ihrem absoluten Werthe nach $< q^2$ ist, so ist φ ebenfalls eine ungerade Zahl und zwar $< q$. Je nach der Beschaffenheit dieser Zahl φ zerfällt nun der Beweis in drei Theile.

1. Ist φ weder durch p noch durch p' theilbar, so ist

$$\left(\frac{pp'}{\varphi}\right) = +1,$$

und da $q\varphi$ quadratischer Rest von pp' ist, auch

$$\left(\frac{q\varphi}{pp'}\right) = 1, \text{ also } \left(\frac{q}{pp'}\right) = \left(\frac{\varphi}{pp'}\right);$$

da ferner die beiden ungeraden relativen Primzahlen φ und pp' (von denen die letztere positiv ist) nur solche Primfactoren enthalten, welche $< q$ sind, so gilt für diese beiden Zahlen auch das verallgemeinerte Reciprocitätsgesetz, d. h. es ist

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

und folglich, mit Berücksichtigung der beiden vorhergehenden Gleichungen

$$\left(\frac{q}{pp'}\right) = (-1)^{\frac{1}{2}(\varphi-1)\cdot\frac{1}{2}(pp'-1)}.$$

Da aber e eine gerade Zahl, so ist $q\varphi \equiv -pp' \pmod 4$, also, da $q \equiv 1 \pmod 4$ ist,

$$\varphi \equiv -pp' \pmod 4$$

$$\frac{\varphi-1}{2} \equiv -\frac{pp'+1}{2} \pmod 2$$

also

$$\frac{\varphi-1}{2} \cdot \frac{pp'-1}{2} \equiv 0 \pmod 2$$

und folglich

$$\left(\frac{q}{pp'}\right) = 1,$$

was zu beweisen war.

2. Ist φ durch p' theilbar, durch p nicht theilbar, so setze man $\varphi = p'\psi$, und, da auch e durch p' theilbar sein muss, $e = p'\varepsilon$; dann ist $\psi < q$ eine durch p nicht theilbare ungerade, und ε eine gerade Zahl, und es wird

$$p'\varepsilon^2 - p = q\psi.$$

Hieraus folgt nun zunächst wieder (da ψ relative Primzahl zu pp' ist)

$$\left(\frac{pp'}{\psi}\right) = +1,$$

ferner

$$\left(\frac{q\psi}{p}\right) = \left(\frac{p'}{p}\right), \quad \text{also} \quad \left(\frac{q}{p}\right) = \left(\frac{p'}{p}\right)\left(\frac{\psi}{p}\right)$$

und

$$\left(\frac{q\psi}{p'}\right) = \left(\frac{-p}{p'}\right), \quad \text{also} \quad \left(\frac{q}{p'}\right) = \left(\frac{-p}{p'}\right)\left(\frac{\psi}{p'}\right)$$

und folglich

$$\left(\frac{q}{pp'}\right) = \left(\frac{p'}{-p}\right)\left(\frac{-p}{p'}\right)\left(\frac{\psi}{pp'}\right) = (-1)^{\frac{1}{2}(p+1)\cdot\frac{1}{2}(p'-1)}\left(\frac{\psi}{pp'}\right);$$

da endlich ψ und pp' nur solche Primfactoren enthalten, die $< q$ sind, so ist nach dem verallgemeinerten Reciprocitätssatz

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

und hieraus in Verbindung mit zwei vorhergehenden Gleichungen

$$\left(\frac{q}{pp'}\right) = (-1)^{\frac{1}{2}(p+1)\cdot\frac{1}{2}(p'-1)+\frac{1}{2}(\psi-1)\cdot\frac{1}{2}(pp'-1)}.$$

Da nun $\varepsilon^2 \equiv 0 \pmod 4$ und $q \equiv 1 \pmod 4$, so ist $\psi \equiv -p \pmod 4$, folglich

$$\tfrac{1}{2}(\psi-1) \equiv \tfrac{1}{2}(p+1) \pmod 2,$$

also

$$\tfrac{1}{2}(p+1)\cdot\tfrac{1}{2}(p'-1)+\tfrac{1}{2}(\psi-1)\cdot\tfrac{1}{2}(pp'-1)$$
$$\equiv \tfrac{1}{2}(p+1)\,[\tfrac{1}{2}(p'-1)+\tfrac{1}{2}(pp'-1)] \pmod 2,$$

und da ferner (nach dem ersten Lemma 4. in §. 46)

$$\tfrac{1}{2}(pp'-1) \equiv \tfrac{1}{2}(p-1)+\tfrac{1}{2}(p'-1) \pmod 2$$

ist, so ergiebt sich

$$\tfrac{1}{2}(p+1)\cdot\tfrac{1}{2}(p'-1)+\tfrac{1}{2}(\psi-1)\cdot\tfrac{1}{2}(pp'-1)$$
$$\equiv \tfrac{1}{2}(p+1)\cdot\tfrac{1}{2}(p-1) \equiv 0 \pmod 2$$

und folglich

$$\left(\frac{q}{pp'}\right)=1,$$

was zu beweisen war.

Da bei diesem Beweise die Annahme, dass q Nichtrest von p' ist, gar nicht zur Anwendung gekommen ist, so wird durch einfache Vertauschung von p mit p' der Beweis für den Fall entstehen, dass φ durch p theilbar, durch p' nicht theilbar ist; denn im Uebrigen sind sowohl die Voraussetzungen als auch das zu beweisende Resultat vollständig symmetrisch in Bezug auf beide Primzahlen p und p'.

3. Ist φ sowohl durch p als auch durch p' und folglich (da p und p' verschiedene Primzahlen sind) auch durch pp' theilbar, so setze man $\varphi = pp'\psi$, und, da e dann ebenfalls durch pp' theilbar ist, $e = pp'\varepsilon$; dann bedeutet ψ eine ungerade Zahl $< q$, und ε eine gerade Zahl, und es wird

$$pp'\varepsilon^2-1 = q\psi.$$

Hieraus folgt, dass pp' relative Primzahl zu ψ und ausserdem quadratischer Rest von ψ, also

$$\left(\frac{pp'}{\psi}\right)=+1$$

ist; ebenso ergiebt sich aber, dass $-q\psi$ quadratischer Rest von pp', dass also

$$\left(\frac{q}{pp'}\right)=\left(\frac{-\psi}{pp'}\right)$$

ist; nach dem verallgemeinerten Reciprocitätssatze, welcher offenbar für die beiden Zahlen $-\psi$ und pp' gilt, ist ferner

$$\left(\frac{-\psi}{pp'}\right)\left(\frac{pp'}{-\psi}\right)=(-1)^{\frac{1}{2}(pp'-1)\cdot\frac{1}{2}(\psi+1)},$$