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_0057
LOG Titel: §. 49. Erster Theil des Beweises
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

Primzahlen 3 und 5 wirklich richtig ist, folgt dann unmittelbar seine Allgemeingültigkeit

Von besonderer Wichtigkeit für diesen Nachweis ist nun die vorläufige Bemerkung, dass aus der angenommenen Richtigkeit des Reciprocitätssatzes für je zwei Primzahlen p, p', welche kleiner als die Primzahl q sind, mit Nothwendigkeit auch die Gültigkeit des verallgemeinerten Satzes (§. 46, 7.)

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}$$

folgt, sobald die beiden ungeraden relativen Primzahlen P und Q (die nicht gleichzeitig negativ sein dürfen) nur solche Primzahlfactoren enthalten, die kleiner als q sind; denn der Beweis dieses verallgemeinerten Satzes gründete sich ausschliesslich auf die Richtigkeit des einfachen Satzes für alle die Paare von zwei Primzahlen, von denen die eine in P, die andere in Q aufgeht.

Bei dem Beweise nun, dass der Reciprocitätssatz für jede Combination von q mit einer Primzahl p gilt, welche kleiner als q ist, haben wir zwei Fälle zu unterscheiden. Der eine Fall und zwar der schwierigere findet Statt, wenn q die Form $4n+1$ hat, und zugleich p quadratischer Nichtrest von q ist; dann ist zu beweisen, dass auch q quadratischer Nichtrest von p ist. In irgend einem der andern Fälle, nämlich wenn q von der Form $4n+3$ ist, oder auch, wenn q zwar die Form $4n+1$ hat, dann aber p quadratischer Rest von q ist, kann man offenbar der Primzahl p immer ein solches Vorzeichen geben, dass, wenn man $\omega = \pm p$ setzt, wenigstens für eins der beiden Vorzeichen ω quadratischer Rest von q wird; dann ist also zu beweisen, dass

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

ist; dieser letztere Fall ist deshalb leichter zu behandeln, weil die Annahme sogleich einen Ansatz giebt, welcher nur ausgebeutet zu werden braucht. Wir beginnen daher mit diesem Theile des Satzes.

§. 49.

Es sei also $\omega = \pm p$ quadratischer Rest von q, so hat die Congruenz $x^2 \equiv \omega \pmod{q}$ zwischen 0 und q immer zwei Wurzeln x

deren Summe $= q$, und von denen folglich die eine, welche wir mit e bezeichnen wollen, eine gerade Zahl ist. Dann wird

$$e^2 - \omega = qf$$

sein, wo f eine ganze Zahl bedeutet, welche jedenfalls nicht $= 0$ ist, weil sonst die Primzahl ω eine Quadratzahl sein müsste. Diese Zahl f kann aber auch nicht negativ sein; denn sonst wäre ω positiv $= p$, und $p - e^2$ eine positive durch q theilbare Zahl, was aber unmöglich ist, da $p - e^2 < p$, und der Voraussetzung nach $p < q$ ist. Diese positive Zahl f muss ferner ungerade sein; denn da e gerade ist, so ist $e^2 - \omega$ ungerade, und folglich auch jeder Divisor von $e^2 - \omega$, also auch f ungerade. Endlich ist diese positive ungerade Zahl f nothwendig $< q - 1$; denn da $e \leqq q - 1$, und $p < q - 1$, so ist $qf = e^2 - \omega < (q-1)^2 + (q-1)$, d. h. $qf < q(q-1)$, also wirklich $f < q - 1$.

Nun sind zwei Fälle möglich:

1. Ist f nicht durch p theilbar, so folgt aus der Gleichung $e^2 - \omega = qf$, dass

$$\left(\frac{\omega}{f}\right) = +1,$$

und ferner, weil qf quadratischer Rest von p ist, dass

$$\left(\frac{q}{\omega}\right) = \left(\frac{f}{\omega}\right)$$

sein muss; da nun die beiden ungeraden Zahlen f und ω relative Primzahlen zu einander, beide kleiner als q, und endlich nicht beide negativ sind, so gilt für sie der verallgemeinerte Reciprocitätssatz, d. h. es ist

$$\left(\frac{f}{\omega}\right)\left(\frac{\omega}{f}\right) = (-1)^{\frac{1}{2}(\omega-1)\cdot\frac{1}{2}(f-1)}$$

und hieraus ergiebt sich unter Berücksichtigung der beiden vorhergehenden Gleichungen

$$\left(\frac{q}{\omega}\right) = (-1)^{\frac{1}{2}(\omega-1)\cdot\frac{1}{2}(f-1)}.$$

Da ferner e eine gerade Zahl ist, so ist auch $-\omega \equiv qf \pmod 4$, also (nach dem ersten Lemma 4. in §. 46)

$$-\frac{\omega+1}{2} \equiv \frac{qf-1}{2} \equiv \frac{q-1}{2} + \frac{f-1}{2} \pmod 2;$$

multiplicirt man diese Congruenz mit $\frac{1}{2}(\omega - 1)$, so erhält man auf

der linken Seite ein Product aus zwei successiven ganzen Zahlen, also gewiss eine gerade Zahl, und hieraus folgt unmittelbar

$$\frac{\omega-1}{2}\frac{f-1}{2} \equiv \frac{\omega-1}{2}\frac{q-1}{2} \pmod 2$$

und also

$$\left(\frac{q}{\omega}\right) = (-1)^{\frac{1}{2}(\omega-1)\cdot\frac{1}{2}(q-1)},$$

was zu beweisen war.

2. Ist dagegen f theilbar durch p, so kann man $f = \omega\varphi$ setzen, wo φ eine ungerade Zahl bedeutet, die dasselbe Zeichen wie ω hat und ihrem absoluten Werthe nach $< q$ ist. Da nun $e^2 - \omega = q\omega\varphi$, so ist auch e theilbar durch ω und also $e = \varepsilon\omega$, wo ε wieder eine gerade Zahl ist. Hieraus ergiebt sich nun

$$\varepsilon^2\omega - 1 = q\varphi,$$

und es kann daher φ nicht durch ω theilbar sein. Nun war ω quadratischer Rest von $f = \omega\varphi$, und folglich auch von φ, also ist

$$\left(\frac{\omega}{\varphi}\right) = \left(\frac{\omega}{-\varphi}\right) = +1;$$

ausserdem folgt aus der vorhergehenden Gleichung, dass $-q\varphi$ quadratischer Rest von ω, dass also

$$\left(\frac{q}{\omega}\right) = \left(\frac{-\varphi}{\omega}\right)$$

ist; da endlich von den beiden ungeraden Zahlen $-\varphi$ und ω die eine positiv ist, und da sie relative Primzahlen zu einander und ausserdem beide $< q$ sind, so ist nach dem verallgemeinerten Reciprocitätssatze

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

und folglich unter Berücksichtigung der beiden vorhergehenden Gleichungen

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

Da nun ε eine gerade Zahl und folglich $q\varphi \equiv -1 \pmod 4$ ist, so muss die eine der beiden Zahlen φ und q von der Form $4n+1$, die andere aber von der Form $4n+3$ sein, woraus folgt, dass