

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_0050

LOG Titel: S. 42. Inhalt des Reciprocitätssatzes

LOG Typ: chapter

Terms and Conditions

The Goettingen State and University Library provides access to digitized documents strictly for noncommercial educational, research and private purposes and makes no warranty with regard to their use for other purposes. Some of our collections are protected by copyright. Publication and/or broadcast in any form (including electronic) requires prior written permission from the Goettingen State- and University Library.

Each copy of any part of this document must contain these Terms and Conditions. With the usage of the library's online system to access or download a digitized document you accept the Terms and Conditions.

Reproductions of material on the web site may not be made for or donated to other repositories, nor may be further reproduced without written permission from the Goettingen State- and University Library.

For reproduction requests and permissions, please contact us. If citing materials, please give proper attribution of the source.

Contact

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

d. h. dass

$$\left(\frac{2}{p}\right) = -1 \text{ für } p = 8n + 5$$

$$\left(\frac{2}{p}\right) = +1 \text{ für } p = 8n + 7$$

ist.

Es bleibt jetzt nur noch zu beweisen übrig, dass 2 quadratischer Rest von allen Primzahlen p von der Form $8n + 1$ ist; hierauf ist die vorhergehende Methode aus dem Grunde nicht anwendbar, weil die Annahme des Gegentheils sich nicht in Form einer Congruenz darstellen lässt, die dann zur Auffindung des Widerspruchs benutzt werden könnte. Allein in diesem Falle kann man direct, wie folgt, verfahren; da $p = 8n + 1$ ist, so hat die Function $x^{p-1} - 1$ den Divisor $x^8 - 1$, also auch den Factor $x^4 + 1$, und hieraus folgt nach einem frühern Satze (§. 26), dass die Congruenz

$$x^4 + 1 \equiv 0 \pmod{p}$$

Wurzeln hat; ist nun x eine solche, so ist

$$x^4 + 1 = (x^2 \pm 1)^2 \mp 2x^2 \equiv 0 \pmod{p},$$

also

$$(x^2 \pm 1)^2 \equiv \pm 2x^2 \pmod{p};$$

es ist daher $\pm 2x^2$ und folglich auch ± 2 quadratischer Rest von p ; in Zeichen

$$\left(\frac{\pm 2}{p}\right) = 1, \text{ wenn } p = 8n + 1.$$

Hiermit ist der Satz in allen seinen Theilen bewiesen; wir können denselben in der einen Gleichung

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

zusammenfassen; denn je nachdem $p = 8n \pm 1$, oder $p = 8n \pm 3$ ist, wird $\frac{1}{8}(p^2 - 1)$ eine gerade oder ungerade Zahl.

§. 42.

Wir kommen nun zu der Untersuchung der dritten Frage: *von welchen ungeraden Primzahlen p ist die gegebene ungerade*

Primzahl q quadratischer Rest? Die vollständige Antwort hierauf wird durch einen der wichtigsten und interessantesten Sätze der Zahlentheorie gegeben, welcher seines eigenthümlichen Charakters wegen den Namen des *Reciprocitäts-Satzes* erhalten hat. Man kann ihn folgendermaassen aussprechen:

Sind p und q zwei positive ungerade Primzahlen, von denen mindestens eine die Form $4n + 1$ hat, so ist q quadratischer Rest oder Nichtrest von p , je nachdem p quadratischer Rest oder Nichtrest von q ist; haben aber beide Primzahlen p und q die Form $4n + 3$, so ist q quadratischer Rest oder Nichtrest von p , je nachdem p quadratischer Nichtrest oder quadratischer Rest von q ist.

Offenbar lässt sich dieser Satz durch die für beide Fälle gültige Gleichung

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

ausdrücken; denn sobald mindestens eine der beiden Primzahlen p oder q die Form $4n + 1$ hat, so ist die entsprechende der beiden Zahlen $\frac{1}{2}(p-1)$ oder $\frac{1}{2}(q-1)$, und folglich auch ihr Product $\frac{1}{2}(p-1) \cdot \frac{1}{2}(q-1)$ eine gerade Zahl, so dass

$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = 1, \text{ d. h. } \left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$$

ist, worin der erste Fall seinen Ausdruck findet; sind dagegen beide Primzahlen p und q von der Form $4n + 3$, so sind auch beide Zahlen $\frac{1}{2}(p-1)$ und $\frac{1}{2}(q-1)$, und folglich auch ihr Product $\frac{1}{2}(p-1) \cdot \frac{1}{2}(q-1)$ ungerade, so dass

$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = -1, \text{ d. h. } \left(\frac{q}{p}\right) = - \left(\frac{p}{q}\right)$$

wird, worin der zweite Theil des Satzes ausgedrückt ist.

Ist z. B. $p = 3$, $q = 5$, so ist p quadratischer Nichtrest von q und gleichzeitig q quadratischer Nichtrest von p , in Zeichen

$$\left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = -1.$$

Ist ferner $p = 3$, $q = 13$, so ist p quadratischer Rest von q und gleichzeitig q quadratischer Rest von p , in Zeichen

$$\left(\frac{3}{13}\right) = \left(\frac{13}{3}\right) = +1.$$

Ist dagegen $p = 3$, $q = 7$, so ist p quadratischer Nichtrest von q und gleichzeitig q quadratischer Rest von p , in Zeichen