

## 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\_0173

**LOG Titel:** S. 154. Vierter Beweis 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](mailto:gdz@sub.uni-goettingen.de)

ist, was nur bei den Formen des zweiten Typus eintreten kann, so ist  $A = 2B$ , und  $(B) < \sqrt{D}$ , folglich  $B' = (B)$ , weil dieser Werth allen an  $B'$  gestellten Forderungen genügt, und also wieder  $(A) < \sqrt{D} + B'$ . Endlich behaupten wir, dass jede ambige reducirte Form  $(a, b, c)$ , welche zugleich ursprünglich von erster Art ist, nothwendig mit einer dieser  $2\tau$  Formen  $(A, B', C')$  identisch sein muss; ist nämlich  $b$  theilbar durch  $a$ , so muss  $(a) < \sqrt{D}$  sein, weil in einer reducirten Form  $0 < b < \sqrt{D}$  ist, und die mit  $(a, b, c)$  äquivalente Form  $(a, 0, a')$  ist eine der  $2\tau$  Formen  $(A, B, C)$ , woraus folgt, dass  $(a, b, c)$  selbst mit der entsprechenden Form  $(A, B', C')$  identisch sein muss, weil  $b$  als mittlerer Coefficient einer reducirten Form denselben charakteristischen Bedingungen genügt, wie  $B'$ ; ist aber  $b$  nicht theilbar durch  $a$ , so ist wenigstens  $(a) < 2\sqrt{D}$ , und folglich die mit  $(a, b, c)$  äquivalente Form  $(a, \frac{1}{2}a, c')$  eine der Formen  $(A, B, C)$ , woraus wieder folgt, dass  $(a, b, c)$  mit der entsprechenden Form  $(A, B', C')$  identisch ist. Wir müssen aus dem Vorhergehenden schliessen, dass die Anzahl aller ambigen ursprünglichen Formen erster Art, welche zugleich reducirt sind, genau  $= 2\tau$  ist; da nun in jeder ambigen Classe sich stets zwei und nur zwei solche Formen finden (§§. 78, 82), so erhalten wir dasselbe Resultat, wie für negative Determinanten: *Die Anzahl  $\alpha$  aller ambigen ursprünglichen Classen erster Art von positiver Determinante  $D$  ist genau halb so gross wie die Anzahl  $2\tau$  aller angebbaren Totalcharaktere.*

Verbinden wir diese Resultate mit dem des vorigen Paragraphen, so ergibt sich folgender Satz\*):

*Die Anzahl der wirklich existirenden verschiedenen Geschlechter ist höchstens halb so gross wie die Anzahl der angebbaren Totalcharaktere.*

### §. 154.

Das soeben erhaltene Resultat führt nun zu einem neuen Beweise des Reciprocitätssatzes, sowie der Ergänzungssätze über den Charakter der Zahlen — 1 und 2. Wir machen zunächst die Be-

\*) Vergl. §. 123.

merkung, dass in den Fällen  $D = -1, \pm 2$ , und wenn  $D \equiv 1 \pmod{4}$  eine positive oder negative Primzahl ist, nur ein einziger Charakter  $C$  (§. 122), und folglich (§. 153) nur ein einziges Geschlecht vorhanden ist, welches kein anderes, als das durch die Form  $(1, 0, -D)$  vertretene Hauptgeschlecht ( $C = +1$ ) sein kann. Wir bezeichnen nun mit  $p, q$  immer positive, ungerade (von einander verschiedene) Primzahlen, und wenden uns zum Beweise der drei Sätze:

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

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

1. Ist zunächst  $p \equiv 1 \pmod{4}$ , so ist  $(-1, 0, p)$  eine ursprüngliche Form erster Art von der Determinante  $D = p \equiv 1 \pmod{4}$ , für welche nur Formen existiren, die dem Hauptgeschlecht angehören; mithin muss der Coefficient  $-1$  quadratischer Rest von  $p$  sein. Ist aber  $p \equiv 3 \pmod{4}$ , so ist  $-1$  Nichtrest von  $p$ ; wäre nämlich  $-1 = b^2 - cp$ , so wäre  $(p, b, c)$  eine (positive) Form der Determinante  $D = -1$ , welche zufolge ihres Coefficienten  $p$  den Charakter  $C = -1$  besäße, was unmöglich ist.

2. Ist  $p \equiv 1 \pmod{8}$ , so ist  $(8, 1, \frac{1}{8}(1-p))$  oder  $(8, 3, \frac{1}{8}(9-p))$ , je nachdem  $p \equiv 9$  oder  $\equiv 1 \pmod{16}$  ist, eine ursprüngliche Form erster Art von der Determinante  $D = p \equiv 1 \pmod{4}$ , und muss deshalb dem Hauptgeschlecht angehören, woraus folgt, dass 8 und also auch 2 quadratischer Rest von  $p$  ist.

Ist ferner  $p \equiv 7 \pmod{8}$ , so ist 2 ebenfalls quadratischer Rest von  $p$ ; denn im entgegengesetzten Fall wäre (zufolge 1. und §. 33, III.) die Zahl  $-2$  Rest von  $p$ , also  $-2 = b^2 - cp$ , und es existirte eine (positive) Form  $(p, b, c)$  der Determinante  $D = -2$ , für welche  $C = -1$  wäre, was unmöglich ist.

Ist endlich  $p \equiv 3$  oder  $5 \pmod{8}$ , so ist 2 Nichtrest von  $p$ ; wäre nämlich  $2 = b^2 - cp$ , so wäre  $(p, b, c)$  eine Form der Determinante  $D = 2$ , für welche  $C = -1$  wäre, was unmöglich ist.

3. Ist wenigstens eine der beiden Primzahlen  $p, q$ , z. B.  $p \equiv 1 \pmod{4}$ , so ist

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right).$$