

## 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\_0177

**LOG Titel:** S. 158. Jede Classe des Hauptgeschlechtes entsteht durch Duplication

**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)

$-bc \equiv \mathfrak{A}^2 \pmod{a}$ ,  $-ca \equiv \mathfrak{B}^2 \pmod{b}$ ,  $-ab \equiv \mathfrak{C}^2 \pmod{c}$ ,  
 so ist die obige Gleichung in relativen Primzahlen  $x, y, z$  der Art  
 lösbar, dass

$\mathfrak{A}z \equiv by \pmod{a}$ ,  $\mathfrak{B}x \equiv cz \pmod{b}$ ,  $\mathfrak{C}y \equiv ax \pmod{c}$   
 wird.

### §. 158.

Mit Hülfe dieses Satzes lässt sich nun das oben (§. 155) erwähnte grosse Theorem von *Gauss* leicht beweisen:

*Jede Classe des Hauptgeschlechtes entsteht durch Duplication.*

Als Repräsentanten der dem Hauptgeschlechte der Determinante  $D$  angehörenden Classe wählen wir eine Form  $(A, B, C)$ , deren erster Coefficient  $A$  relative Primzahl zu  $2D$  ist (§. 93). Da die Zahl  $A$  durch diese Form darstellbar ist, und alle Einzel-Charaktere derselben den Werth  $+1$  haben, so ist  $A$  quadratischer Rest von jeder in  $D$  aufgehenden ungeraden Primzahl, und auch von 4 oder von 8, falls  $D$  durch 4 oder 8 theilbar ist (§. 122); mithin ist (nach §. 37)  $A$  quadratischer Rest von  $D$  selbst (umgekehrt ergibt sich leicht, zum Theil mit Hülfe des Reciprocitätssatzes, dass die Form  $(A, B, C)$  gewiss dem Hauptgeschlecht angehört, wenn  $A$  relative Primzahl zu  $2D$ , quadratischer Rest von  $D$ , und, falls  $D$  negativ sein sollte, positiv ist). Ja, man kann sogar voraussetzen, dass  $A$  quadratischer Rest von  $4D$  ist, d. h. dass  $A \equiv 1 \pmod{4}$ , oder  $A \equiv 1 \pmod{8}$  ist, je nachdem  $D$  ungerade oder gerade ist. Dies ist in der That von selbst der Fall, wenn  $D \equiv 3 \pmod{4}$ , oder  $D \equiv 0 \pmod{8}$  ist; sollte ferner  $A$  in den übrigen Fällen dieser Bedingung nicht genügen, wäre also  $A \equiv 3 \pmod{4}$ ,  $\equiv 7 \pmod{8}$ ,  $\equiv 3 \pmod{8}$ ,  $\equiv 5 \pmod{8}$ , je nachdem  $D \equiv 1 \pmod{4}$ ,  $\equiv 2 \pmod{8}$ ,  $\equiv 6 \pmod{8}$ ,  $\equiv 4 \pmod{8}$ , so kann man die Form  $(A, B, C)$  durch eine Substitution  $\begin{pmatrix} \alpha & -1 \\ 1 & 0 \end{pmatrix}$  in eine Form transformiren, deren erster Coefficient  $A' = A\alpha^2 + 2B\alpha + C$  relative Primzahl zu  $2D$  ist und zugleich die verlangte Eigenschaft besitzt; da nämlich  $AA' = (A\alpha + B)^2 - D$  ist, so braucht man  $\alpha$  nur so zu wählen, dass  $A\alpha + B$  im ersten Falle gerade, in den drei übrigen Fällen aber ungerade wird, was sich stets in der Art erreichen lässt, dass  $A\alpha + B$  zugleich relative Primzahl zu  $D$  wird.