

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_0143

LOG Titel: S. 129. Theorie der Indices für solche Moduli

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

§. 129.

Nachdem im Vorhergehenden die Existenz von primitiven Wurzeln g für jeden Modul p^π nachgewiesen ist, der eine Potenz einer ungeraden Primzahl p ist, kann man leicht die übrigen elementaren Fragen über die Potenzreste beantworten. Setzt man zur Abkürzung

$$\varphi(p^\pi) = c,$$

so sind die Potenzen

$$g^0, g^1, g^2 \dots g^{c-1} \pmod{p^\pi}$$

sämmtlich incongruent, und bilden daher ein vollständiges System incongruenter Zahlen, mit Ausschuss der durch p theilbaren Zahlen. Ist daher n irgend eine durch p nicht theilbare Zahl, so existiren stets unendlich viele Exponenten γ , die aber nach dem Modul c sämmtlich einander congruent sind, von der Beschaffenheit, dass

$$n \equiv g^\gamma \pmod{p^\pi};$$

man nennt dann γ den *Index der Zahl n für die Basis g* , und drückt dies in Zeichen so aus

$$\text{Ind. } n \equiv \gamma \pmod{c};$$

durchläuft γ ein vollständiges Restsystem in Bezug auf den Modul c , so durchläuft n ein vollständiges System von Zahlen, die relative Primzahlen zu p^π und unter einander nach dem Modul p^π incongruent sind. Für die Rechnung mit diesen Indices gelten dieselben Gesetze, wie die (in §. 30 angegebenen) für den Fall $\pi = 1$. Wir heben hier besonders hervor, dass

$$\text{Ind. } (1) \equiv 0, \quad \text{Ind. } (-1) \equiv \frac{1}{2}c \pmod{c},$$

und ferner, dass n quadratischer Rest oder Nichtrest von p^π ist, je nachdem Ind. n gerade oder ungerade ist.

Aus dem Index einer Zahl n lässt sich leicht der Exponent t bestimmen, zu welchem n in Bezug auf den Modul p^π gehört; aus

$$n \equiv g^{\text{Ind. } n} \pmod{p^\pi}$$

folgt nämlich