

## 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\_0144

**LOG Titel:** S. 130. Fall, wenn der Modulus eine Potenz der Zahl 2 ist; Indices

**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)

$$n' \equiv g^{t \text{Ind. } n} \pmod{p^n};$$

soll also  $n' \equiv 1$  sein, so muss  $t$  Ind.  $n$  durch  $c$  theilbar, und folglich  $t$  ein Multiplum von  $c : \delta$  sein, wo  $\delta$  den grössten gemeinschaftlichen Divisor von  $c$  und Ind.  $n$  bedeutet; die kleinste aller dieser Zahlen  $t$ , d. h. der Exponent, zu welchem  $n$  gehört, ist daher  $= c : \delta$ .

Hieraus folgt, dass  $n$  stets und nur dann eine primitive Wurzel von  $p^n$  ist, wenn Ind.  $n$  relative Primzahl zu  $c$  ist; die Anzahl aller nach dem Modul  $p^n$  incongruenten primitiven Wurzeln von  $p^n$  ist daher gleich der Anzahl derjenigen der Zahlen

$$0, 1, 2 \dots c - 1,$$

welche relative Primzahlen zu  $c$  sind, also gleich  $\varphi(c) = \varphi \varphi(p^n)$ . Dasselbe Resultat ist aber auch eine unmittelbare Folge aus dem Schlussätze des vorigen Paragraphen.

### §. 130.

Die Primzahl 2 verhält sich anders als die ungeraden Primzahlen, welche bisher ausschliesslich betrachtet wurden.

Für den Modul 2 kann jede ungerade Zahl als primitive Wurzel angesehen werden.

Für den Modul  $2^2 = 4$  ist  $3 \equiv -1$  eine primitive Wurzel; zu jeder ungeraden Zahl  $n$  giebt es einen entsprechenden Exponenten  $\alpha$  von der Beschaffenheit, dass

$$n \equiv (-1)^\alpha \pmod{4}$$

ist; und zwar ist  $\alpha \equiv 0 \pmod{2}$  oder  $\equiv 1 \pmod{2}$ , je nachdem  $n \equiv 1$  oder  $\equiv 3 \pmod{4}$  ist.

Bis hierher findet also noch völlige Analogie mit den ungeraden Primzahlen Statt; sobald aber ein Modul  $2^\lambda$  betrachtet wird, in welchem der Exponent  $\lambda \geq 3$  ist, hört dieselbe auf. Es lässt sich nämlich zeigen, dass, wenn  $n$  irgend eine ungerade Zahl bedeutet, immer schon

$$n^{1/2 \varphi(2^\lambda)} = n^{2^{\lambda-2}} \equiv 1 \pmod{2^\lambda}$$

ist. In der That ist dieser Satz richtig für  $\lambda = 3$ ; denn das Quadrat jeder ungeraden Zahl  $n$  ist  $\equiv 1 \pmod{8}$ . Nehmen wir

ferner an, der Satz sei für einen beliebigen Exponenten  $\lambda \geq 3$  schon bewiesen, es sei also

$$n^{2^{\lambda-2}} = 1 + h 2^\lambda,$$

so folgt hieraus durch Quadriren

$$n^{2^{\lambda-1}} = 1 + h 2^{\lambda+1} + h^2 2^{2\lambda} \equiv 1 \pmod{2^{\lambda+1}},$$

d. h. der Satz gilt auch für den nächstfolgenden Exponenten  $\lambda + 1$ . Er gilt mithin allgemein, da er für  $\lambda = 3$  gilt.

Es fragt sich nun, ob es in diesen Fällen wenigstens Zahlen giebt, die zu dem Exponenten  $\frac{1}{2}\varphi(2^\lambda) = 2^{\lambda-2}$  gehören; man überzeugt sich leicht, dass die Zahl 5 diese Eigenschaft für jeden Modul  $2^\lambda \geq 8$  besitzt. Es ist nämlich

$$5 \equiv 1 + 4 \pmod{8}$$

$$5^2 \equiv 1 + 8 \pmod{16}$$

$$5^4 \equiv 1 + 16 \pmod{32}$$

$$5^8 \equiv 1 + 32 \pmod{64}$$

allgemein

$$5^{2^{\lambda-3}} \equiv 1 + 2^{\lambda-1} \pmod{2^\lambda},$$

also

$$5^{2^{\lambda-3}} \text{ niemals } \equiv 1 \pmod{2^\lambda},$$

woraus unmittelbar folgt, dass der Exponent, zu welchem die Zahl 5 nach dem Modul  $2^\lambda$  gehört, kein Divisor von  $2^{\lambda-3}$  sein kann, und also, da er doch Divisor von  $2^{\lambda-2}$  sein muss, nothwendig  $= 2^{\lambda-2}$  ist.

Hieraus ergibt sich nun, wenn man zur Abkürzung

$$\frac{1}{2}\varphi(2^\lambda) = 2^{\lambda-2} = b$$

setzt, dass die  $b$  Zahlen

$$5^0, 5^1, 5^2 \dots 5^{b-1}$$

sämmtlich nach dem Modul  $2^\lambda$  incongruent sind; dasselbe gilt von den Zahlen

$$-5^0, -5^1, -5^2 \dots -5^{b-1}$$

da ferner die erstern sämmtlich  $\equiv 1 \pmod{4}$ , die letztern sämmtlich  $\equiv 3 \pmod{4}$  sind, so bilden sie zusammengenommen ein System von  $\varphi(2^\lambda)$  nach dem Modul  $2^\lambda$  incongruenten ungeraden Zahlen. Ist daher  $n$  irgend eine ungerade Zahl, so kann man stets