

## 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\_0044

**LOG Titel:** §. 36. Fall, in welchem der Modulus eine Potenz der Zahl 2 ist

**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)

zeln  $\alpha$  und  $-\alpha$ , welche gefunden werden können, sobald man eine Wurzel der Congruenz

$$x^2 \equiv D \pmod{p}$$

gefunden hat.

### §. 36.

Wir gehen nun zu dem besondern Fall über, in welchem der Modul  $k$  eine Potenz der Primzahl 2 ist, so dass also  $D$  irgend eine ungerade Zahl bedeutet. Betrachten wir zunächst die Congruenz

$$x^2 \equiv D \pmod{4},$$

so erkennt man leicht, dass dieselbe stets und nur dann möglich ist, wenn

$$D \equiv 1 \pmod{4}$$

ist. Denn ist die Congruenz möglich, so ist  $x$  jedenfalls ungerade, und das Quadrat von  $x = 2n + 1$  ist  $4n^2 + 4n + 1 \equiv 1 \pmod{4}$ ; umgekehrt, ist  $D \equiv 1 \pmod{4}$ , so hat die Congruenz offenbar die beiden incongruenten Wurzeln  $x \equiv 1$  und  $x \equiv -1 \pmod{4}$ .

Gehen wir nun zu der Congruenz

$$x^2 \equiv D \pmod{8}$$

über, so leuchtet ein, da das Quadrat einer jeden ungeraden Zahl  $4n \pm 1$  gleich  $16n^2 \pm 8n + 1 \equiv 1 \pmod{8}$  ist, dass diese Congruenz nur dann möglich ist, wenn

$$D \equiv 1 \pmod{8}$$

ist; und umgekehrt, sobald diese Bedingung erfüllt ist, hat die Congruenz die vier incongruenten Wurzeln  $x \equiv 1$ ,  $x \equiv 3$ ,  $x \equiv 5$ ,  $x \equiv 7$ .

Betrachten wir jetzt die Congruenz

$$x^2 \equiv D \pmod{2^\pi},$$

wo  $\pi \geq 3$  ist, so kann diese Congruenz nur dann möglich sein, wenn die Congruenz

$$x^2 \equiv D \pmod{8}$$

möglich ist; es ist daher erforderlich, dass

$$D \equiv 1 \pmod{8}$$

sei. Wir wollen nun umgekehrt zeigen, dass diese Bedingung

auch hinreicht, und dass dann die Congruenz stets 4 incongruente Wurzeln hat. Nehmen wir nämlich an, dies sei für den Modul  $2^\pi$  schon bewiesen, so können wir zeigen, dass dasselbe auch für den Modul  $2^{\pi+1}$  gilt. Es sei nämlich  $\alpha$  eine Wurzel der Congruenz

$$x^2 \equiv D \pmod{2^\pi}$$

also

$$\alpha^2 - D = h \cdot 2^\pi,$$

so setzen wir

$$x = \alpha + 2^{\pi-1} \cdot y;$$

dann wird

$$x^2 - D = h \cdot 2^\pi + 2^\pi \cdot \alpha y + 2^{2\pi-2} y^2.$$

Da nun  $\pi \geq 3$ , so ist  $2\pi - 2 \geq \pi + 1$ , folglich

$$x^2 - D \equiv 2^\pi (h + \alpha y) \pmod{2^{\pi+1}}.$$

Damit also  $x^2 - D$  durch  $2^{\pi+1}$  theilbar werde, braucht man nur  $y$  so zu wählen, dass

$$\alpha y \equiv -h \pmod{2}$$

werde. Dies ist aber stets möglich, da  $\alpha$  eine ungerade Zahl ist; also folgt aus der Möglichkeit der Congruenz

$$x^2 \equiv D \pmod{2^\pi},$$

wo  $\pi \geq 3$  ist, stets die Möglichkeit der Congruenz

$$x^2 \equiv D \pmod{2^{\pi+1}}.$$

Wir schliessen hieraus zunächst das folgende Resultat:

*Damit die Congruenz*

$$x^2 \equiv D \pmod{2^\pi},$$

*in welcher  $\pi \geq 3$  ist, Wurzeln habe, ist erforderlich und hinreichend, dass*

$$D \equiv 1 \pmod{8}$$

*sei.*

Ist nun  $\alpha$  eine Wurzel dieser Congruenz — und eine solche kann immer nach der obigen Methode gefunden werden —, so muss, wenn  $x$  irgend eine Wurzel derselben Congruenz bezeichnet,

$$x^2 - \alpha^2 = (x - \alpha)(x + \alpha) \equiv 0 \pmod{2^\pi}$$

sein. Da ferner  $\alpha$  sowohl wie  $x$  ungerade Zahlen sein müssen, so sind die beiden Factoren  $x - \alpha$  und  $x + \alpha$  gerade Zahlen, und dann muss

$$\frac{x - \alpha}{2} \cdot \frac{x + \alpha}{2} \equiv 0 \pmod{2^{\pi-2}}$$