## 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_0048
**LOG Titel:** §. 40. Die Zahl 2 ist quadratischer Rest aller Primzahlen von der Form .... und Nichtrest aller Primzahlen von der Form ....
**LOG Typ:** chapter



## Contact

Niedersächsische Staats- und Universitätsbibliothek Göttingen
Georg-August-Universität Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen
Germany
Email: gdz@sub.uni-goettingen.de

*Alle ungeraden Primzahlen $p$ zu finden, für welche irgend eine der drei Congruenzen*

$$x^2 \equiv -1, \quad x^2 \equiv 2, \quad x^2 \equiv q \pmod{p}$$

*möglich ist, wo $q$ irgend eine gegebene positive ungerade Primzahl bedeutet.*

## §. 40.

Die Auffindung aller ungeraden Primzahlen $p$, für welche die Congruenz

$$x^2 \equiv -1 \pmod{p}$$

möglich ist, bietet keine Schwierigkeit mehr dar. Denn da (nach §. 33) allgemein

$$\left(\frac{D}{p}\right) \equiv D^{\frac{p-1}{2}} \pmod{p}$$

ist, so erhält man speciell

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$$

und folglich auch

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

In Worten lautet dieser wichtige Satz*) folgendermaassen:

*Die Zahl $-1$ ist quadratischer Rest aller Primzahlen von der Form $4n+1$, dagegen quadratischer Nichtrest aller Primzahlen von der Form $4n+3$.*

Dasselbe Resultat erhält man auch auf folgendem Wege. Ist die Congruenz $x^2 \equiv -1 \pmod{p}$ möglich, und $x$ eine Wurzel derselben, so folgt hieraus durch Potenzirung

$$x^{p-1} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$$

und hieraus (nach dem Fermat'schen Satze §. 19) $(-1)^{\frac{p-1}{2}} = 1$ also $p = 4n+1$; d. h. die Zahl $-1$ ist quadratischer Nichtrest von allen Primzahlen von der Form $4n+3$. Ist umgekehrt $p$ von der Form $4n+1$, so ist $x^{p-1}-1$ algebraisch theilbar durch $x^4-1$, also auch durch $x^2+1$; es ist folglich

$$x^{p-1} - 1 = (x^2+1)\,\psi(x),$$

*) *Euler: Demonstratio theorematis Fermatiani, omnem numerum primum formae $4n+1$ esse summam duorum quadratorum*, Nov. Comm. Petrop. V, p. 3.