

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_0034

LOG Titel: §.27. Ableitung des Wilson'schen Satzes aus dem Fermat'schen

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

§. 27.

Von diesen wichtigen Sätzen machen wir sogleich eine Anwendung. Zuzufolge des Fermat'schen Satzes genügt jede der $(p - 1)$ unter einander nach dem Modul p incongruenten Zahlen

$$1, 2, 3 \dots (p - 1)$$

der Congruenz

$$x^{p-1} - 1 \equiv 0 \pmod{p},$$

und diese Zahlen bilden auch ihre sämtlichen incongruenten Wurzeln. Es ist daher nach dem ersten der vorhergehenden drei Sätze

$$x^{p-1} - 1 = (x - 1)(x - 2)(x - 3) \dots (x - p + 1) + p\psi(x),$$

worin $\psi(x)$ ein Polynom mit ganzen Coefficienten bezeichnet. Entwickelt man daher das rechter Hand befindliche Product nach Potenzen von x , so muss der Coefficient einer jeden Potenz von x dem entsprechenden linker Hand in Bezug auf den Modul p congruent sein. Wir wollen hier nur den interessantesten Fall betrachten der sich durch die Vergleichung der Glieder ergibt, welche von x unabhängig sind. Ist zunächst p eine *ungerade* Primzahl, so ist dieses Glied rechter Hand, da die Anzahl $p - 1$ der negativen Factoren gerade ist,

$$= 1 \cdot 2 \cdot 3 \dots (p - 1),$$

linker Hand dagegen $= -1$, und hieraus ergibt sich der nach *Wilson* benannte Satz:

Wenn p eine Primzahl bedeutet, so ist das um eine Einheit vergrößerte Product aller kleineren Zahlen als p durch p theilbar in Zeichen

$$1 \cdot 2 \dots (p - 1) \equiv -1 \pmod{p}.$$

So ist z. B.

$$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 + 1 = 721$$

theilbar durch 7.

Der *Wilson'sche* Satz gilt aber auch für die Primzahl 2, da in diesem Fall $+1$ und -1 einander congruent sind.

Dieser Satz ist dadurch bemerkenswerth, dass er sich umkehren lässt und deshalb ein charakteristisches Merkmal für eine Primzahl abgibt. Denn nimmt man umgekehrt an, es sei