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

Contact

§. 27.

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

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

der Congruenz

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

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

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

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 ergiebt, 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,

$$= 1 . 2 . 3 \ldots (p-1),$$

linker Hand dagegen $= -1$, und hieraus ergiebt 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

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

So ist z. B.

$$1 . 2 . 3 . 4 . 5 . 6 + 1 = 721$$

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 abgiebt. Denn nimmt man umgekehrt an, es sei