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_0026
LOG Titel: §. 19. Beweis des verallgemeinerten Fermat'schen Satzes
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

§. 19.

Betrachten wir jetzt den Ausdruck ax, in welchem a wieder relative Primzahl gegen den Modul k ist, und setzen wir wieder für x der Reihe nach die Glieder eines vollständigen Systems incongruenter Zahlen ein, aber nicht alle, sondern nur diejenigen

$$a_1, a_2, a_3 \ldots,$$

welche relative Primzahlen gegen den Modul k sind, und deren Anzahl nach dem vorigen Paragraphen gleich $\varphi(k)$ ist, so leuchtet erstens ein, dass die Werthe des Ausdrucks ax, d. h. die Producte

$$aa_1, \quad aa_2, \quad aa_3 \ldots$$

sämmtlich incongruent sind, ferner, dass dieselben sämmtlich wieder relative Primzahlen gegen k sind; es wird daher jedes dieser Producte einem und nur einem Gliede der Reihe

$$a_1, a_2, a_3 \ldots$$

congruent sein. Wir können daher setzen

$$\left.\begin{aligned} aa_1 &\equiv b_1 \\ aa_2 &\equiv b_2 \\ aa_3 &\equiv b_3 \end{aligned}\right\} (\mathrm{mod.}\, k),$$

u. s. w.

wo nun die Zahlen

$$b_1, b_2, b_3 \ldots$$

vollständig, wenn auch in anderer Ordnung, mit den Zahlen

$$a_1, a_2, a_3 \ldots$$

übereinstimmen, so dass namentlich

$$a_1 a_2 a_3 \ldots a_{\varphi(k)} = b_1 b_2 b_3 \ldots b_{\varphi(k)}$$

sein wird. Bezeichnen wir zur Abkürzung dieses Product mit P, und multipliciren wir die vorstehenden $\varphi(k)$ Congruenzen mit einander, so erhalten wir daher

$$a^{\varphi(k)} \cdot P \equiv P \ (\mathrm{mod.}\, k).$$

Nun ist aber P ein Product von lauter Zahlen, die relative Primzahlen gegen den Modul sind, also selbst relative Primzahl gegen den Modul k; es ist daher nach §. 17, 6. gestattet, die vorstehende Congruenz durch den gemeinschaftlichen Factor P beider Seiten ohne Weiteres zu dividiren. Auf diese Weise erhalten wir die Congruenz

$$a^{\varphi(k)} \equiv 1 \pmod{k};$$

in Worten kann man diesen höchst wichtigen Satz folgendermaassen aussprechen:

Ist a relative Primzahl gegen die positive Zahl k, und erhebt man a zu einer Potenz, deren Exponent $\varphi(k)$ angiebt, wie viele der Zahlen

$$1, 2, 3 \ldots k$$

relative Primzahlen gegen k sind, so lässt diese Potenz, durch k dividirt, stets den Rest 1.

Nehmen wir z. B. $k = 15$, $a = 2$, so ist a wirklich relative Primzahl gegen k; nun ist $\varphi(k) = \varphi(15) = \varphi(3)\,\varphi(5) = 8$; es muss daher 2^8, durch 15 dividirt, den Rest 1 lassen; in der That ist

$$2^8 = 256 = 17 \cdot 15 + 1.$$

Es kann übrigens vorkommen, dass auch Potenzen von a mit niedrigerm Exponenten als $\varphi(k)$ denselben Rest 1 geben. Dies tritt wirklich in dem eben gewählten Beispiel ein, denn es ist auch

$$2^4 = 16 = 1 \cdot 15 + 1.$$

Specialisiren wir unsern Satz für den Fall, dass k nur durch eine einzige Primzahl p theilbar, also

$$k = p^\pi, \quad \varphi(k) = (p-1)p^{\pi-1}$$

ist, so erhalten wir den Satz:

Ist p eine Primzahl und a irgend eine durch p nicht theilbare Zahl, so ist

$$a^{(p-1)p^{\pi-1}} \equiv 1 \pmod{p^\pi}.$$

Nehmen wir ferner hierin $\pi = 1$, so erhalten wir einen berühmten Satz, der zuerst von *Fermat* aufgestellt ist und daher der Fermat'sche Satz heisst:

Ist p eine Primzahl und a irgend eine durch p nicht theilbare Zahl, so ist

$$a^{p-1} \equiv 1 \pmod{p}.$$

Man kann diesen Satz so umformen, dass er auch für den Fall gültig bleibt, wenn a durch p theilbar ist; zu diesem Zweck braucht man nur die vorstehende Congruenz mit a zu multipliciren, wodurch sie in die folgende

$$a^p \equiv a \pmod{p}$$

übergeht. Ist nämlich a theilbar durch p, so sind beide Seiten dieser Congruenz $\equiv 0 \pmod{p}$, also ist sie auch dann noch richtig. Umgekehrt kann man aus dieser Form des Satzes auch wieder die