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_0027
LOG Titel: §. 20. Anderer Beweis desselben 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

frühere ableiten; denn sobald a nicht theilbar durch p, also relative Primzahl gegen p ist, darf man beide Seiten dieser Congruenz auch wieder durch a dividiren, ohne den Modul zu ändern.

Kehren wir zu dem allgemeinen Satz zurück, der zuerst von *Euler**) bewiesen ist und den Namen des verallgemeinerten Fermat'schen Satzes führt, so können wir denselben auch in folgender Weise aussprechen: Sind p, r, s . . . von einander verschiedene absolute Primzahlen, und ist a durch keine dieser Primzahlen theilbar, so ist stets

$$a^{(p-1)p^{\pi-1}\cdot(r-1)r^{\varrho-1}\cdot(s-1)s^{\sigma-1}\cdots} \equiv 1 \pmod{p^\pi r^\varrho s^\sigma \ldots},$$

wo π, ϱ, σ . . . irgend welche ganze positive Zahlen bedeuten.

§. 20.

Es ist wohl nicht überflüssig, dem vorhergehenden Beweise dieses wichtigen Satzes einen zweiten hinzuzufügen, der gradatim zu Werke geht und sich zunächst auf den binomischen Satz stützt. Ist p irgend eine ganze positive Zahl, so ist zufolge dieses Satzes bekanntlich

$$(a+b)^p =$$

$$a^p + \frac{p}{1}a^{p-1}b + \cdots + \frac{p!}{r!(p-r)!}a^{p-r}b^r + \cdots + b^p;$$

hierin sind (nach §. 15) alle Coefficienten ganze Zahlen. Ist aber p eine Primzahl, so können wir hinzufügen, dass alle Coefficienten mit Ausnahme des ersten und letzten, welche $= 1$ sind, durch p theilbar sind; denn der Zähler des Bruches

$$\frac{p!}{r!(p-r)!},$$

in welchem r eine der Zahlen 1, 2, 3 . . . $(p-1)$ bedeutet, enthält den Factor p, der Nenner dagegen nicht; der Bruch ist also von der Form $pm:n$, wo n nicht theilbar durch p, also auch relative Primzahl gegen p ist; da wir aber ferner wissen, dass dieser Bruch eine ganze Zahl, dass also pm durch n theilbar ist, so muss m durch n theilbar sein; der Bruch hat daher die Form ps, wo der zweite Factor s eine ganze Zahl ist; und folglich ist jeder dieser $(p-1)$ Coefficienten $\equiv 0 \pmod{p}$. Sind daher a und b irgend welche ganze Zahlen, so erhalten wir die folgende Congruenz

$$(a+b)^p \equiv a^p + b^p \pmod{p},$$

*) *Theorematа arithm. nova meth. demonstr.*, Comm. nov. Ac. Petrop. VIII. p. 74.

wobei also vorausgesetzt ist, dass p eine Primzahl ist. Offenbar folgt hieraus weiter

$$(a+b+c)^p \equiv (a+b)^p + c^p \equiv a^p + b^p + c^p \pmod{p}$$

und allgemein für eine beliebige Reihe von n ganzen Zahlen a, $b \ldots h$:

$$(a+b+\cdots+h)^p \equiv a^p + b^p + \cdots + h^p \pmod{p}.$$

Setzen wir hierin $a = 1$, $b = 1 \ldots h = 1$, so erhalten wir für jede beliebige positive ganze Zahl n den Satz:

$$n^p \equiv n \pmod{p}.$$

Da ferner für jede ungerade Primzahl $(-1)^p \equiv -1$, und für die einzige gerade Primzahl $p = 2$ ebenfalls $(-1)^p = 1 \equiv -1 \pmod{p}$ ist, so erhalten wir durch Multiplication der vorstehenden Congruenz mit der andern

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

die neue

$$(-n)^p \equiv -n \pmod{p}.$$

Also ist der Fermat'sche Satz

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

für jede positive und negative Zahl a bewiesen, während er für $a = 0$ unmittelbar evident ist. Wenn nun a nicht durch p theilbar ist, was wir von jetzt annehmen wollen, so folgt hieraus, dass

$$a^{p-1} \equiv 1 \pmod{p}, \text{ d. h. } a^{p-1} = 1 + hp$$

ist, wo h eine ganze Zahl bedeutet. Erheben wir diese Gleichung zur $p$ten Potenz und entwickeln die rechte Seite wieder nach dem binomischen Satze, so zeigt sich, dass alle Glieder mit Ausnahme des ersten Multipla von p^2 sind; wir erhalten daher

$$a^{(p-1)p} = 1 + h'p^2 \text{ oder } a^{(p-1)p} \equiv 1 \pmod{p^2},$$

wo wieder h' eine ganze Zahl bedeutet. So kann man fortfahren, indem man jedesmal wieder zur $p$ten Potenz erhebt, und gelangt auf diese Weise zu der Congruenz

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

deren Allgemeingültigkeit sich in derselben Weise durch den Schluss von π auf $\pi + 1$ nachweisen lässt.

Sind nun r, s . . . ebenfalls Primzahlen, welche nicht in a aufgehen, so ist nach demselben Satze

$$a^{(r-1)r^{\varrho-1}} \equiv 1 \pmod{r^\varrho}, \quad a^{(s-1)s^{\sigma-1}} \equiv 1 \pmod{s^\sigma} \ldots$$

Setzen wir ferner zur Abkürzung