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_0035
LOG Titel: §. 28. Potenzreste; Exponent, zu welchem eine Zahl gehört
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

$$1 \cdot 2 \cdot 3 \ldots (p-1)+1$$

durch p theilbar, so muss p eine Primzahl sein; wäre nämlich p eine zusammengesetzte Zahl, also ausser durch 1 und durch sich selbst auch noch durch eine andere Zahl a theilbar, so würde a nothwendig eine der Zahlen 2, 3 . . $(p-1)$ sein müssen; da nun die obige Summe und ihr erstes Glied durch a theilbar ist, so müsste auch das zweite Glied 1 durch a theilbar sein, was nicht möglich ist.

Einen andern interessanten Satz erhält man durch Anwendung des dritten der vorhergehenden Sätze auf dasselbe Beispiel. Bezeichnet nämlich δ irgend einen Divisor von $p-1$, so ist bekanntlich

$$x^{p-1}-1 \doteq (x^{\delta}-1)\ \psi(x),$$

wo $\psi(x)$ ein Polynom mit ganzen Coefficienten bedeutet. Hieraus folgt also: *Die Congruenz*

$$x^{\delta} \equiv 1 \pmod{p},$$

deren Grad δ ein Divisor von $p-1$ ist, besitzt stets δ incongruente Wurzeln.

§. 28.

Der zuletzt abgeleitete Satz gehört seinem Inhalte nach eigentlich in eine allgemeinere Theorie, nämlich in die Theorie der *binomischen Congruenzen* von der Form

$$a x^n \equiv b \pmod{k}.$$

Dieselbe stützt sich auf die Betrachtung der sogenannten *Potenzreste*, d. h. der Reste der successiven Potenzen einer Zahl, und wir beschäftigen uns daher zunächst mit der Untersuchung der interessanten Gesetze, welche hier hervortreten.

Es sei also k ein beliebiger Modul, und a relative Primzahl gegen denselben; bilden wir nun die Reihe

$$1, a, a^2, a^3 \ldots$$

der successiven Potenzen von a und setzen dieselbe hinreichend weit fort, so muss es einmal geschehen, dass zwei verschiedene Glieder a^s und a^{s+n} einander nach dem Modul k congruent werden; denn es giebt ja nur eine endliche Anzahl incongruenter Zahlen. Aus der Congruenz

$$a^{s+n} = a^s \,.\, a^n \equiv a^s \pmod{k}$$

folgt aber, da a^s relative Primzahl gegen den Modul k ist, dass

$$a^n \equiv 1 \pmod{k}$$

ist. Es giebt daher, was wir auch schon durch den verallgemeinerten Fermat'schen Satz (§. 19) wussten, stets eine Potenz von a, welche durch k dividirt den Rest 1 lässt. Unter allen Potenzen von a, welche dieselbe Eigenschaft haben, ist aber besonders diejenige bemerkenswerth, welche den kleinsten Exponenten hat; doch versteht sich von selbst, dass der Exponent Null hier nicht in Betracht kommt, für welchen die entsprechende Potenz ja stets $\equiv 1$ sein würde. Bezeichnen wir mit δ diesen kleinsten positiven Exponenten, für welchen

$$a^\delta \equiv 1 \pmod{k}$$

wird, so wollen wir sagen, die Zahl a *gehöre* zu dem Exponenten δ oder zu der Zahl δ. Dann leuchtet zunächst ein, dass die ersten δ Glieder der obigen Potenzreihe, d. h. die Zahlen

$$1, \quad a, \quad a^2 \ldots a^{\delta-1}$$

sämmtlich incongruent unter einander sind; denn aus einer Congruenz von der Form $a^{s+n} \equiv a^s$, wo s und $s+n$ kleiner als δ sind, würde wieder $a^n \equiv 1$ folgen, was mit der Voraussetzung im Widerspruch steht, dass keine niedrigere Potenz als a^δ den Rest 1 lässt.

Die folgenden Glieder der Reihe geben nun genau dieselben Reste, und auch in derselben Reihenfolge, denn es ist

$$\begin{aligned}
&a^\delta \equiv 1, \quad a^{\delta+1} \equiv a, \quad a^{\delta+2} \equiv a^2 \ldots a^{2\delta-1} \equiv a^{\delta-1} \\
&a^{2\delta} \equiv 1, \quad a^{2\delta+1} \equiv a, \quad a^{2\delta+2} \equiv a^2 \ldots a^{3\delta-1} \equiv a^{\delta-1} \\
&a^{3\delta} \equiv 1, \quad a^{3\delta+1} \equiv a, \quad a^{3\delta+2} \equiv a^2 \ldots a^{4\delta-1} \equiv a^{\delta-1}
\end{aligned}$$

u. s. w.

Um daher zu erfahren, welchen Rest eine beliebige Potenz a^s lässt, dividire man den Exponenten s durch δ und bringe dadurch s in die Form $s = m\delta + r$, wo r eine der Zahlen $0, 1, 2 \ldots (\delta - 1)$ bezeichnet. Dann ist

$$a^s = a^{m\delta+r} \equiv a^r \pmod{k}.$$

Hieraus geht ferner hervor, dass zwei solche Potenzen wie a^s und $a^{s'}$ stets, aber auch nur dann congruent sein werden in Bezug auf den Modul k, wenn $s \equiv s' \pmod{\delta}$; denn ist r' der bei der Division von s' durch δ hervorgehende Rest, so ist $a^{s'} \equiv a^{r'} \pmod{k}$. Ist daher