Werk

Titel: Vorlesungen über Zahlentheorie

Autor: Dirichlet, Peter

Verlag: Vieweg

Ort: Braunschweig

Jahr: 1871

Kollektion: Mathematica

Werk Id: PPN30976923X

PURL: http://resolver.sub.uni-goettingen.de/purl?PID=PPN30976923X|LOG_0036

OPAC: http://opac.sub.uni-goettingen.de/DB=1/PPN?PPN=30976923X

Contact

Niedersächsische Staats- und Universitätsbibliothek Göttingen
Georg-August-Universität Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen
Germany
Email: gdz@sub.uni-goettingen.de

$$a^s \equiv a^{s'} \pmod{k}$$

so muss auch

$$a^r \equiv a^{r'} \pmod{k}$$

sein; da aber r und r' kleiner als δ sind, so ist dies nur dann möglich, wenn $r = r'$ ist, woraus $s \equiv s' \pmod{\delta}$ folgt; und umgekehrt leuchtet ein, dass, sobald $s \equiv s' \pmod{\delta}$, also $r = r'$ ist, auch $a^s \equiv a^{s'} \pmod{k}$ sein muss.

Ein specieller Fall ist der, dass, sobald $a^s \equiv 1$, also $a^s \equiv a^0$ ist, nothwendig $s \equiv 0 \pmod{\delta}$, d. h. dass s theilbar durch δ sein muss. Nun wissen wir schon aus dem verallgemeinerten Fermat'schen Satz, dass stets

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

ist; hieraus folgt also, dass die Zahl δ, zu welcher eine Zahl a gehört, stets ein Divisor von $\varphi(k)$ sein muss*).

§. 29.

Beschränken wir uns jetzt wieder auf den Fall, in welchem der Modul eine Primzahl p und also a irgend eine durch p nicht theilbare Zahl ist, so folgt aus der letzten Bemerkung, dass die Zahl δ, zu welcher a gehört, jedenfalls ein Divisor von $\varphi(p) = p - 1$ sein muss. Man kann nun umgekehrt fragen: wenn δ irgend ein Divisor von $p - 1$ ist, giebt es dann jedesmal auch Zahlen a, welche zu δ gehören? und wie viele? Nehmen wir zunächst einmal ein Beispiel, indem wir $p = 7$ setzen. Da aus $a \equiv a' \pmod{p}$ auch stets $a^s \equiv a'^s \pmod{p}$ folgt, so gehören je zwei congruente Zahlen auch stets zu demselben Exponenten, und wir brauchen daher in unserm Beispiel nur die Zahlen $a = 1, 2, 3, 4, 5, 6$ zu betrachten; durch wirkliches Potenziren, welches man dadurch abkürzt, dass man statt jeder Potenz immer ihren kleinsten Rest substituirt, findet man nun das in der folgenden Tabelle ausgedrückte Resultat:

a	1	2	3	4	5	6
δ	1	3	6	3	6	2

Es gehört daher zu dem Divisor $\delta = 1$ nur die einzige Zahl 1, zu $\delta = 2$ nur die einzige Zahl 6; zu $\delta = 3$ gehören zwei Zah-

*) Ein anderer Beweis dieses Satzes findet sich in den Supplementen V. §. 127.

len, nämlich 2 und 4, und zu $\delta = 6$ gehören die beiden Zahlen 3 und 5.

Nehmen wir nun vorläufig einmal an, dass *mindestens eine* Zahl a existirt, welche zu dem Exponenten δ gehört, so sind die δ Zahlen

$$1,\ a,\ a^2 \ldots a^{\delta-1} \qquad (A)$$

nach dem Vorhergehenden sämmtlich incongruent; da ferner $a^\delta \equiv 1$, so ist auch

$$(a^r)^\delta = (a^\delta)^r \equiv 1 \pmod{p},$$

d. h. die δ Zahlen (A) sind Wurzeln der Congruenz

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

und da sie unter einander incongruent sind, und der Modulus eine Primzahl ist, so bilden sie auch die sämmtlichen Wurzeln dieser Congruenz vom Grade δ. Jede Zahl aber, welche zum Exponenten δ gehört, muss vor Allem eine Wurzel dieser Congruenz sein, und wir haben daher alle etwa existirenden Zahlen, die zu δ gehören, unter den Zahlen (A) zu suchen. Wir fragen daher: zu welchem Exponenten h gehört irgend eine dieser Zahlen, z. B. a^r? d. h. welches ist die kleinste positive Zahl h, für welche

$$(a^r)^h = a^{rh} \equiv 1 \pmod{p}$$

ist? Offenbar muss rh (da a zum Exponenten δ gehört) durch δ theilbar sein; ist daher ε der grösste gemeinschaftliche Divisor von r und $\delta = \varepsilon\delta'$, so muss h durch δ' theilbar sein; die kleinste Zahl h, welche diese Bedingung erfüllt, ist offenbar δ' selbst, und dann ist auch wirklich

$$(a^r)^h = (a^\delta)^{\frac{r}{\varepsilon}} \equiv 1 \pmod{p};$$

also ist δ' die Zahl, zu welcher a^r gehört. Soll also a^r zum Exponenten δ gehören, so muss $\varepsilon = 1$, also r relative Primzahl gegen δ sein; und umgekehrt, sobald dies der Fall, also $\varepsilon = 1$ ist, gehört auch a^r wirklich zum Exponenten δ. Wir erhalten so das Resultat, dass unter den Zahlen (A) genau ebenso viele zu dem Exponenten δ gehören, als es unter den Exponenten

$$0,\ 1,\ 2 \ldots (\delta - 1)$$

relative Primzahlen zu δ giebt; es giebt daher $\varphi(\delta)$ solche Zahlen.

Da wir angenommen hatten, dass *mindestens eine* solche Zahl a existirte, so können wir das Bisherige so zusammenfassen: Ist p eine Primzahl und δ ein Divisor von $p-1$, so ist die Anzahl