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_0142

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

Repräsentanten von δ Zahl-Classen in Bezug auf den Modul k angesehen werden können. Gesetzt nun, es findet sich eine und dieselbe Zahlclasse in jedem der beiden Complexe A' und A'' vertreten, so giebt es zwei Exponenten μ', μ'' von der Beschaffenheit, dass

$$a' \cdot a^{\mu'} \equiv a'' \cdot a^{\mu''} \pmod{k}$$

ist; nehmen wir an, was der Symmetrie wegen erlaubt ist, dass $\mu'' \geqq \mu'$, so erhält man durch Division mit $a^{\mu'}$ die Congruenz

$$a' \equiv a'' \cdot a^{\mu''-\mu'} \pmod{k};$$

und hieraus folgt sogleich, dass *jede* in A' enthaltene Zahl $a' \cdot a^m$ auch einer Zahl von der Form $a'' \cdot a^n$, d. h. einer in A'' enthaltenen Zahl congruent ist. Wir können hieraus schliessen, dass entweder zwei solche Complexe A', A'' dieselben δ Zahlclassen enthalten, oder dass keine einzige Classe in beiden gleichzeitig vertreten ist.

Bildet man nun der Reihe nach alle solche aus δ Zahlclassen bestehenden Complexe von der Form A', A'' . . ., und zwar nur solche, welche von einander verschieden sind, so muss endlich jede der $\varphi(k)$ Zahlclassen, welche relative Primzahlen zu k enthalten, in einem dieser Complexe, und auch nur in einem, vertreten sein; ist daher ε die Anzahl dieser von einander verschiedenen Complexe, so muss $\varphi(k) = \varepsilon\delta$, also $\varphi(k)$ theilbar durch δ sein, was zu beweisen war.

Hieraus ergiebt sich nun der Fermat'sche Satz als Folgerung; denn erhebt man die Congruenz

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

zur εten Potenz, so erhält man

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

§. 128.

Für den Fall, dass der Modul k eine Primzahl p ist, wurde ferner in §. 29 bewiesen, dass zu jedem Divisor δ von $\varphi(p) = p-1$ genau $\varphi(\delta)$ Zahlen gehören, die nach dem Modul p incongruent sind; und in §. 30 sind die Eigenschaften der sogenannten primi-

tiven Wurzeln von p betrachtet, d. h. derjenigen $\varphi(p-1)$ incongruenten Zahlen g, welche zum Exponenten $p-1$ selbst gehören. Wir wollen nun untersuchen, ob ähnliche Gesetze auch für zusammengesetzte Moduln gelten.

Zunächst beschränken wir uns auf den Fall, in welchem der Modul k eine *Potenz von einer ungeraden Primzahl* p ist, und wir werden der Analogie nach unter einer *primitiven Wurzel* von k jede Zahl g verstehen, welche zum Exponenten $\varphi(k)$ gehört. Dem Beweise der wirklichen Existenz solcher primitiven Wurzeln schicken wir folgenden Hülfssatz voraus:

Ist h irgend eine ganze Zahl und $\pi \geqq 1$ eine positive ganze Zahl, so ist stets

$$(1 + hp^{\pi})^p \equiv 1 + hp^{\pi+1} \pmod{p^{\pi+2}}.$$

Man überzeugt sich hiervon leicht durch die Entwicklung der linken Seite nach dem binomischen Satze; man findet nämlich zunächst, indem man sich auf die drei ersten Glieder beschränkt,

$$(1 + hp^{\pi})^p \equiv 1 + hp^{\pi+1} + \tfrac{1}{2}(p-1)h^2p^{2\pi+1} \pmod{p^{3\pi}},$$

und hieraus ergiebt sich die obige Congruenz, wenn man bedenkt, dass p ungerade, also $\frac{1}{2}(p-1)$ eine ganze Zahl, und ferner, dass sowohl $p^{2\pi+1}$ als auch $p^{3\pi}$ durch $p^{\pi+2}$ theilbar ist.

Nach dieser Vorbemerkung gehen wir an unsere Untersuchung und nehmen zunächst einmal an, es existire für den Modul $p^{\pi+1}$, wo $\pi \geqq 1$ ist, wirklich eine primitive Wurzel g; dann liegt es nahe zu fragen: zu welchem Exponenten gehört eine solche Zahl g in Bezug auf den Modul p^{π}? Es sei δ dieser Exponent, also

$$g^{\delta} = 1 + hp^{\pi},$$

so erhält man mit Hülfe des soeben bewiesenen Satzes

$$g^{\delta p} \equiv 1 \pmod{p^{\pi+1}};$$

da nun g primitive Wurzel von $p^{\pi+1}$ ist, so muss δp durch $\varphi(p^{\pi+1}) = (p-1)p^{\pi}$, und folglich δ durch $(p-1)\,p^{\pi-1}$ theilbar sein; andererseits muss aber, da g zum Exponenten δ in Bezug auf den Modul p^{π} gehört, nothwendig $\varphi(p^{\pi}) = (p-1)\,p^{\pi-1}$ durch δ theilbar sein; mithin ist $\delta = \varphi(p^{\pi})$, d. h. g ist auch primitive Wurzel von p^{π}. Zugleich leuchtet ein, dass die in der Gleichung

$$g^{(p-1)p^{\pi-1}} = 1 + hp^{\pi}$$

vorkommende Zahl h nicht durch p theilbar sein kann; denn sonst wäre

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

also g keine primitive Wurzel von $p^{\pi+1}$.

Setzt man diese Schlüsse weiter fort, so erhält man zunächst das Resultat:

Jede primitive Wurzel g von einer höhern Potenz einer ungeraden Primzahl p ist nothwendig eine primitive Wurzel der Zahl p selbst, und zwar von der Beschaffenheit, dass $g^{p-1} - 1$ nicht durch p^2 theilbar ist.

Wir wollen nun umgekehrt annehmen, es sei g eine primitive Wurzel von p^π, und zwar von der Beschaffenheit, dass die in der Gleichung

$$g^{(p-1)p^{\pi-1}} = 1 + hp^\pi$$

vorkommende Zahl h nicht durch p theilbar ist; und wir fragen jetzt: zu welchem Exponenten gehört diese Zahl g in Bezug auf den Modul $p^{\pi+1}$? Ist δ dieser Exponent, also

$$g^\delta \equiv 1 \pmod{p^{\pi+1}},$$

so ist auch

$$g^\delta \equiv 1 \pmod{p^\pi},$$

und folglich δ theilbar durch $\varphi(p^\pi)$; da aber andererseits δ ein Divisor von $\varphi(p^{\pi+1}) = p\varphi(p^\pi)$ sein muss, so ist δ entweder $= \varphi(p^\pi)$, oder $= \varphi(p^{\pi+1})$; das Erstere ist aber nicht der Fall, weil unserer Voraussetzung zufolge die Zahl h nicht durch p theilbar ist; also ist $\delta = \varphi(p^{\pi+1})$, d. h. die Zahl g ist primitive Wurzel von $p^{\pi+1}$. Zugleich leuchtet aus der Congruenz

$$g^{(p-1)p^\pi} = (1 + hp^\pi)^p \equiv 1 + hp^{\pi+1} \pmod{p^{\pi+2}}$$

ein, dass die in der Gleichung

$$g^{(p-1)p^\pi} = 1 + h'p^{\pi+1}$$

vorkommende Zahl h' nicht durch p theilbar ist.

Durch Fortsetzung dieser Schlussweise erhalten wir das zweite Resultat:

Jede primitive Wurzel g einer ungeraden Primzahl p, für welche die Differenz $g^{p-1} - 1$ nicht durch p^2 theilbar ist, ist auch eine primitive Wurzel aller höheren Potenzen von p.

Um also die Existenz von primitiven Wurzeln g für höhere Potenzen von p nachzuweisen, und um alle diese Zahlen g zu finden, haben wir nur noch zu zeigen, dass in der That primitive Wurzeln g von p existiren, für welche $g^{p-1} - 1$, oder, was dasselbe sagt, für welche $g^p - g$ nicht durch p^2 theilbar ist. Dies geschieht leicht auf folgende Weise. Ist f irgend eine primitive Wurzel von p, so sind alle in der Form

$$g = f + px$$

enthaltenen Zahlen g ebenfalls primitive Wurzeln von p; dann ist nach dem binomischen Satze

$$g^p \equiv f^p \pmod{p^2};$$

setzen wir daher

$$f^p \equiv f + f'p \pmod{p^2},$$

so wird

$$g^p - g \equiv p(f' - x) \pmod{p^2},$$

und folglich ist $g = f + px$ jedesmal eine primitive Wurzel aller Potenzen von p, ausgenommen, wenn $x \equiv f' \pmod{p}$, also

$$g \equiv f^p \pmod{p^2}$$

ist. Da nun $\varphi(p-1)$ nach dem Modul p incongruente Zahlen f existiren, und aus jeder Zahl f genau $(p-1)$ in Bezug auf den Modul p^2 incongruente Zahlen $g = f + px$ von der Beschaffenheit abgeleitet werden können, dass $g^{p-1} - 1$ nicht durch p^2 theilbar wird, so erhalten wir das Resultat:

Die sämmtlichen primitiven Wurzeln von höheren Potenzen einer ungeraden Primzahl p sind die sämmtlichen Individuen von $(p-1)\,\varphi(p-1)$ verschiedenen Zahlclassen in Bezug auf den Modul p^2.

Beispiel: Sämmtliche primitive Wurzeln der Primzahl $p = 7$ sind in den beiden Reihen $7x + 3$, $7x + 5$ enthalten; da nun

$$3^7 \equiv 31, \quad 5^7 \equiv 19 \pmod{49}$$

ist, so sind alle in den arithmetischen Reihen $7x + 3$, $7x + 5$ enthaltenen Zahlen, mit Ausnahme derer, welche $\equiv 31$ oder $\equiv 19 \pmod{49}$ sind, auch primitive Wurzeln von allen höheren Potenzen von 7.