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_0144
LOG Titel: §. 130. Fall, wenn der Modulus eine Potenz der Zahl 2 ist; Indices
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

$$n^t \equiv g^{t\,\mathrm{Ind}.n} \pmod{p^\pi};$$

soll also $n^t \equiv 1$ sein, so muss t Ind. n durch c theilbar, und folglich t ein Multiplum von $c : \delta$ sein, wo δ den grössten gemeinschaftlichen Divisor von c und Ind. n bedeutet; die kleinste aller dieser Zahlen t, d. h. der Exponent, zu welchem n gehört, ist daher $= c : \delta$.

Hieraus folgt, dass n stets und nur dann eine primitive Wurzel von p^π ist, wenn Ind. n relative Primzahl zu c ist; die Anzahl aller nach dem Modul p^π incongruenten primitiven Wurzeln von p^π ist daher gleich der Anzahl derjenigen der Zahlen

$$0,\ 1,\ 2 \ldots c-1,$$

welche relative Primzahlen zu c sind, also gleich $\varphi(c) = \varphi\varphi(p^\pi)$. Dasselbe Resultat ist aber auch eine unmittelbare Folge aus dem Schlusssatze des vorigen Paragraphen.

§. 130.

Die Primzahl 2 verhält sich anders als die ungeraden Primzahlen, welche bisher ausschliesslich betrachtet wurden.

Für den Modul 2 kann jede ungerade Zahl als primitive Wurzel angesehen werden.

Für den Modul $2^2 = 4$ ist $3 \equiv -1$ eine primitive Wurzel; zu jeder ungeraden Zahl n giebt es einen entsprechenden Exponenten α von der Beschaffenheit, dass

$$n \equiv (-1)^\alpha \pmod{4}$$

ist; und zwar ist $\alpha \equiv 0 \pmod{2}$ oder $\equiv 1 \pmod{2}$, je nachdem $n \equiv 1$ oder $\equiv 3 \pmod{4}$ ist.

Bis hierher findet also noch völlige Analogie mit den ungeraden Primzahlen Statt; sobald aber ein Modul 2^λ betrachtet wird, in welchem der Exponent $\lambda \geqq 3$ ist, hört dieselbe auf. Es lässt sich nämlich zeigen, dass, wenn n irgend eine ungerade Zahl bedeutet, immer schon

$$n^{\frac{1}{2}\varphi(2^\lambda)} = n^{2^{\lambda-2}} \equiv 1 \pmod{2^\lambda}$$

ist. In der That ist dieser Satz richtig für $\lambda = 3$; denn das Quadrat jeder ungeraden Zahl n ist $\equiv 1 \pmod{8}$. Nehmen wir

ferner an, der Satz sei für einen beliebigen Exponenten $\lambda \geqq 3$ schon bewiesen, es sei also

$$n^{2^{\lambda-2}} = 1 + h\,2^{\lambda},$$

so folgt hieraus durch Quadriren

$$n^{2^{\lambda-1}} = 1 + h\,2^{\lambda+1} + h^2 2^{2\lambda} \equiv 1 \pmod{2^{\lambda+1}},$$

d. h. der Satz gilt auch für den nächstfolgenden Exponenten $\lambda + 1$. Er gilt mithin allgemein, da er für $\lambda = 3$ gilt.

Es fragt sich nun, ob es in diesen Fällen wenigstens Zahlen giebt, die zu dem Exponenten $\frac{1}{2}\varphi(2^{\lambda}) = 2^{\lambda-2}$ gehören; man überzeugt sich leicht, dass die Zahl 5 diese Eigenschaft für jeden Modul $2^{\lambda} \geqq 8$ besitzt. Es ist nämlich

$$5 \equiv 1 + 4 \pmod{8}$$
$$5^2 \equiv 1 + 8 \pmod{16}$$
$$5^4 \equiv 1 + 16 \pmod{32}$$
$$5^8 \equiv 1 + 32 \pmod{64}$$

allgemein

$$5^{2^{\lambda-3}} \equiv 1 + 2^{\lambda-1} \pmod{2^{\lambda}},$$

also

$$5^{2^{\lambda-3}} \text{ niemals} \equiv 1 \pmod{2^{\lambda}},$$

woraus unmittelbar folgt, dass der Exponent, zu welchem die Zahl 5 nach dem Modul 2^{λ} gehört, kein Divisor von $2^{\lambda-3}$ sein kann, und also, da er doch Divisor von $2^{\lambda-2}$ sein muss, nothwendig $= 2^{\lambda-2}$ ist.

Hieraus ergiebt sich nun, wenn man zur Abkürzung

$$\tfrac{1}{2}\varphi(2^{\lambda}) = 2^{\lambda-2} = b$$

setzt, dass die b Zahlen

$$5^0,\ 5^1,\ 5^2 \ldots 5^{b-1}$$

sämmtlich nach dem Modul 2^{λ} incongruent sind; dasselbe gilt von den Zahlen

$$-5^0,\ -5^1,\ -5^2 \ldots -5^{b-1}$$

da ferner die erstern sämmtlich $\equiv 1 \pmod 4$, die letztern sämmtlich $\equiv 3 \pmod 4$ sind, so bilden sie zusammengenommen ein System von $\varphi(2^{\lambda})$ nach dem Modul 2^{λ} incongruenten ungeraden Zahlen. Ist daher n irgend eine ungerade Zahl, so kann man stets