

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_0145

LOG Titel: S. 131. Fall, wenn der Modulus eine beliebig zusammengesetzte Zahl ist; Indices

LOG Typ: chapter

Terms and Conditions

The Goettingen State and University Library provides access to digitized documents strictly for noncommercial educational, research and private purposes and makes no warranty with regard to their use for other purposes. Some of our collections are protected by copyright. Publication and/or broadcast in any form (including electronic) requires prior written permission from the Goettingen State- and University Library.

Each copy of any part of this document must contain these Terms and Conditions. With the usage of the library's online system to access or download a digitized document you accept the Terms and Conditions.

Reproductions of material on the web site may not be made for or donated to other repositories, nor may be further reproduced without written permission from the Goettingen State- and University Library.

For reproduction requests and permissions, please contact us. If citing materials, please give proper attribution of the source.

Contact

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

$$n \equiv (-1)^\alpha 5^\beta \pmod{2^\lambda}$$

setzen, wo α nach dem Modul 2, und β nach dem Modul b vollständig bestimmt ist. Durchläuft α ein vollständiges Restsystem in Bezug auf den Modul 2, und β unabhängig von α ein vollständiges Restsystem in Bezug auf den Modul b , so durchläuft n ein vollständiges System von Zahlen, die in Bezug auf den Modul 2^λ incongruent und relative Primzahlen zu 2^λ , d. h. ungerade sind. Diese beiden Zahlen α und β kann man die *Indices* der Zahl n nennen; sie befolgen ganz ähnliche Gesetze, wie die Indices für die früher betrachteten Moduli. Wir heben noch besonders hervor, dass $n \equiv \pm 1$ oder $\equiv \pm 3 \pmod{8}$ ist, je nachdem β gerade oder ungerade.

Es verdient bemerkt zu werden, dass die vorstehende Form, in welche jede ungerade Zahl n gebracht werden kann, auch noch für den Fall $\lambda = 2$ gilt; die Anzahl b der Werthe von β reducirt sich nämlich auf 1, und da $5 \equiv 1 \pmod{4}$, so geht die obige Form in die frühere $n \equiv (-1)^\alpha \pmod{4}$ über. Für eine spätere Untersuchung ist es sogar zweckmässig, dieselbe Form der Darstellung aller relativen Primzahlen zu einem Modul von der Form 2^λ auf die Fälle $\lambda = 0$ und $\lambda = 1$ auszudehnen; da in denselben nur eine einzige Zahlclasse darzustellen ist, so wird man α und β auch nur einen einzigen Werth beizulegen haben; setzen wir daher $a = b = 1$, wenn $\lambda = 0$ oder $\lambda = 1$ ist, in allen anderen Fällen ($\lambda \geq 2$) aber $a = 2$, $b = \frac{1}{2}\varphi(2^\lambda)$, so können wir sagen, dass der Ausdruck

$$n \equiv (-1)^\alpha 5^\beta \pmod{2^\lambda}$$

alle incongruenten relativen Primzahlen zum Modul durchläuft, wenn α und β resp. vollständige Restsysteme in Bezug auf a und b durchlaufen.

§. 131.

Es sei nun der Modul eine beliebige zusammengesetzte Zahl

$$k = 2^\lambda p^\pi p'^{\pi'} \dots,$$

wo p, p' von einander verschiedene ungerade Primzahlen, und $\lambda, \pi, \pi' \dots$ ganze positive Exponenten bedeuten, deren erster, λ ,

auch $= 0$ sein kann. Ist n irgend eine relative Primzahl zu k , so kann man stets

$$n \equiv (-1)^\alpha 5^\beta \pmod{2^\lambda}$$

$$n \equiv g^\gamma \pmod{p^\pi}$$

$$n \equiv g' \gamma' \pmod{p'^{\pi'}}$$

.....

setzen, wo $g, g' \dots$ primitive Wurzeln resp. von $p^2, p'^2 \dots$ bedeuten. Geben wir den Zahlen a, b die im vorigen Paragraphen festgesetzte Bedeutung und setzen wir zur Abkürzung

$$\varphi(p^\pi) = c, \quad \varphi(p'^{\pi'}) = c' \dots,$$

so sind die Exponenten oder Indices

$$\alpha, \beta, \gamma, \gamma' \dots$$

vollständig bestimmt in Bezug auf die entsprechenden Moduli

$$a, b, c, c' \dots,$$

und umgekehrt entspricht jedem solchen Systeme von Indices (nach §. 25) eine bestimmte Classe von Zahlen n nach dem Modul k , die relative Primzahlen zu k sind. Durchlaufen die Indices $\alpha, \beta, \gamma, \gamma' \dots$ unabhängig von einander ihre $a, b, c, c' \dots$ Werthe, so durchläuft n sämmtliche

$$abc c' \dots = \varphi(k)$$

Zahlclassen in Bezug auf den Modul k , welche relative Primzahlen zu k enthalten.

Sind die Indices $\alpha, \beta, \gamma, \gamma' \dots$ einer Zahl n bekannt, so ist es leicht, den Exponenten δ zu bestimmen, zu welchem die Zahl n gehört; denn offenbar ist δ das kleinste gemeinschaftliche Multipulum aller derjenigen Exponenten, zu welchen die Zahl n in Bezug auf die einzelnen Moduli $2^\lambda, p^\pi, p'^{\pi'} \dots$ gehört. Dieser Exponent δ ist daher immer ein Divisor von dem kleinsten gemeinschaftlichen Vielfachen μ der Zahlen $a, b, c, c' \dots$. Es können daher primitive Wurzeln von k , d. h. Zahlen, die zum Exponenten $\varphi(k)$ gehören, nur dann existiren, wenn $\mu = \varphi(k)$ ist; man überzeugt sich leicht, dass dies nur dann der Fall ist, wenn der Modul $k = 1$, oder $= 2$, oder $= 4$, oder eine Potenz einer ungeraden Primzahl, oder das Doppelte einer solchen Potenz ist; und umgekehrt leuchtet ein, dass in diesen Fällen immer primitive Wurzeln existiren.

Da ferner die Möglichkeit einer binomischen Congruenz von der Form

$$x^m \equiv n \pmod{k}$$

und die Anzahl ihrer Wurzeln nur von der Möglichkeit derselben Congruenz in Bezug auf die einzelnen Moduli $2^\lambda, p^\pi, p'^{\pi'}$. . . abhängt (nach §. 37), so überzeugt man sich leicht, dass zur Beurtheilung dieser Frage und zur Auffindung der Wurzeln der Congruenz die Kenntniss der Indices der Zahl n vollständig ausreicht. Die wirkliche Ausführung dieser Untersuchung unterdrücken wir hier, weil sie sich ganz ebenso gestaltet wie in §. 31. Der Fall $m = 2$ würde auf diese Weise behandelt auf das in §. 37 gewonnene Resultat zurückführen. Ebenso leicht ist es, den verallgemeinerten Wilson'schen Satz (§. 38) von Neuem zu beweisen.
