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_0037
LOG Titel: §. 30. Primitive Wurzeln einer Primzahl. Indices. Dritte Methode, Congruenzen ersten Grades aufzulösen
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

der incongruenten Zahlen, die zu δ gehören, entweder $= 0$, oder $= \varphi(\delta)$. Um nun über diese Alternative zu entscheiden, betrachten wir die Totalität aller $p-1$ nach dem Modul p incongruenten und durch p nicht theilbaren Zahlen; wir theilen dieselben in Gruppen ein, indem wir je zwei incongruente Zahlen in dieselbe oder in verschiedene Gruppen werfen, je nachdem sie zu demselben Divisor δ von $p-1$ gehören oder zu verschiedenen. Bezeichnen wir mit $\psi(\delta)$ die Anzahl der Individuen, welche in die dem Divisor δ entsprechende Gruppe gehören, so muss, da jede der $p-1$ vertheilten Zahlen in eine, aber auch nur in eine solche Gruppe gehört,

$$\Sigma \psi(\delta) = p-1$$

sein, wo sich das Summenzeichen auf sämmtliche Divisoren δ von $p-1$ bezieht; wir wissen ferner schon, dass

$$\psi(\delta) \text{ entweder } = 0, \text{ oder } = \varphi(\delta)$$

ist. Da nun früher bewiesen ist (§. 13), dass auch

$$\Sigma \varphi(\delta) = p-1$$

ist, so folgt hieraus mit Nothwendigkeit, dass

$$\psi(\delta) \text{ niemals } = 0, \text{ sondern stets } = \varphi(\delta)$$

ist. Denn da jedes Glied $\psi(\delta)$ der erstern Summe dem entsprechenden der letztern höchstens gleich sein, aber niemals dasselbe übertreffen kann, so würde, sobald nur ein einziges Mal oder öfter $\psi(\delta) = 0$ wäre, die erstere Summe nothwendig kleiner ausfallen müssen als die letztere, während sie in der That einander gleich sind. Wir haben so den wichtigen Satz*) gewonnen:

Die Anzahl der sämmtlichen incongruenten Zahlen, welche zu einem bestimmten Divisor δ von $p-1$ gehören ist stets $= \varphi(\delta)$.

Es genügt, einen Blick auf das obige Beispiel zu werfen, in welchem $p = 7$, um diesen Satz bestätigt zu sehen.

§. 30.

Am interessantesten und folgenreichsten ist der in diesem Resultat enthaltene specielle Fall, in welchem $\delta = p-1$ ist:

Es giebt stets $\varphi(p-1)$ incongruente Zahlen g, welche zu dem Exponenten $p-1$ gehören, welche also die charakteristische Eigenschaft haben, dass die $p-1$ Potenzen

*) *Gauss: D. A.* art. 54.

$$1,\ g,\ g^2,\ g^3 \ldots g^{p-2} \qquad (G)$$

sämmtlich incongruent (mod. p) sind.

Da es überhaupt nur $p-1$ incongruente und durch p nicht theilbare Zahlen c giebt, so folgt, dass jede solche Zahl c einer, und natürlich auch nur einer der Potenzen (G) congruent ist. Jede solche Zahl g, welche zum Exponenten $p-1$ gehört, heisst eine *primitive Wurzel der Primzahl p**), und man kann daher sagen: wenn g eine primitive Wurzel von p ist, und c irgend eine durch p nicht theilbare Zahl, so existirt stets eine Zahl γ in der Reihe $0, 1, 2 \ldots p-2$ und nur eine von der Beschaffenheit, dass

$$c \equiv g^{\gamma} \pmod{p}$$

ist. Wenn man in dieser Weise alle incongruenten und — was im Folgenden immer hinzuzudenken ist — durch p nicht theilbaren Zahlen als Potenzen einer Basis g darstellt, so heissen die Exponenten γ die *Indices* der zugehörigen Zahlen c in Bezug auf die *Basis g*, und man schreibt z. B.

$$\text{Ind. } c = \gamma,$$

indem man die Basis g, so lange sie unverändert bleibt, in der Bezeichnung unterdrückt.

Nehmen wir z. B. $p = 13$, so überzeugt man sich leicht, dass 2 eine primitive Wurzel ist; denn durch Potenziren erhält man

$$2^0 \equiv 1,\quad 2^1 \equiv 2,\quad 2^2 \equiv 4,\quad 2^3 \equiv 8,\quad 2^4 \equiv 3,\quad 2^5 \equiv 6,$$
$$2^6 \equiv 12,\quad 2^7 \equiv 11,\quad 2^8 \equiv 9,\quad 2^9 \equiv 5,\quad 2^{10} \equiv 10,\quad 2^{11} \equiv 7.$$

Nehmen wir daher 2 zur Basis eines Systems von Indices, so erhalten wir folgende Tabellen

c	1	2	3	4	5	6	7	8	9	10	11	12
Ind. c	0	1	4	2	9	5	11	3	8	10	7	6

und

Ind. c	0	1	2	3	4	5	6	7	8	9	10	11
c	1	2	4	8	3	6	12	11	9	5	10	7

deren erstere dazu dient, zu einer Zahl c den Index zu finden, während die zweite den entgegengesetzten Zweck hat**).

Offenbar hat dieses ganze Verfahren die grösste Analogie mit

*) *Euler*: *Demonstrationes circa residua ex divisione potestatum per numeros primos resultantia*, Nov. Comm. Petrop. XVIII, p. 85.

**) Im *Canon Arithmeticus* von *Jacobi* (1839) findet man solche Tabellen für alle dem ersten Tausend angehörenden Primzahlen.

der Construction von Logarithmentafeln, die ja auf dem ähnlichen Gedanken beruhen, alle positiven Zahlen als Potenzen einer einzigen Basis darzustellen; und es zeigt sich nun auch, dass in der Zahlentheorie die Indices ähnliche Gesetze befolgen und für praktische Zwecke ebenso brauchbar sind, wie die Logarithmen. Zunächst leuchtet ein, dass zwei congruente Zahlen auch stets denselben Index haben, in Zeichen: wenn $a \equiv b \pmod{p}$, so ist auch $\text{Ind. } a = \text{Ind. } b$. Ist ferner $c \equiv ab \pmod{p}$, so ist $\text{Ind. } c \equiv \text{Ind. } a + \text{Ind. } b \pmod{p-1}$, oder kürzer, es ist stets

$$\text{Ind. } (ab) \equiv \text{Ind. } a + \text{Ind. } b \pmod{p-1}.$$

Denn es ist ja

$$a \equiv g^{\text{Ind.}a} \pmod{p}; \quad b \equiv g^{\text{Ind.}b} \pmod{p},$$

also

$$ab \equiv g^{\text{Ind.}a + \text{Ind.}b} \pmod{p};$$

nun ist aber auch

$$ab \equiv g^{\text{Ind.}(ab)} \pmod{p},$$

folglich

$$g^{\text{Ind.}(ab)} \equiv g^{\text{Ind.}a + \text{Ind.}b} \pmod{p}.$$

Da nun g eine primitive Wurzel von p, also eine zum Exponenten $\delta = (p-1)$ gehörende Zahl ist, so folgt aus §. 28 die Richtigkeit der zu beweisenden Congruenz nach dem Modul $p-1$. Nehmen wir unser obiges Beispiel, in welchem $p = 13$, so ist z. B.

$$\text{Ind. } (7) = 11, \quad \text{Ind. } (9) = 8,$$

folglich

$$\text{Ind. } (63) \equiv 19 \pmod{12}$$

oder

$$\text{Ind. } (63) = 7.$$

In der That ist aber $63 \equiv 11 \pmod{13}$, und $\text{Ind. } (11) = 7$. Man sieht aus diesem Beispiel, wie eine solche Doppeltafel der Indices dazu benutzt werden kann, mit Leichtigkeit die Classe (11) zu finden, welcher das Product (63) aus zwei Zahlen (7 und 9) angehört.

Natürlich lässt sich der vorstehende Satz auf ein Product aus beliebig vielen Factoren in folgender Weise ausdehnen:

$$\text{Ind. } (abc \ldots) \equiv \text{Ind. } a + \text{Ind. } b + \text{Ind. } c + \cdots \pmod{p-1}.$$

Nimmt man hierin alle Factoren einander congruent, so erhält man:

$$\text{Ind. } (a^n) \equiv n \text{ Ind. } a \pmod{p-1},$$

wo n irgend eine positive ganze Zahl bedeutet.

Es liesse sich hieraus auch leicht nachweisen, dass der Uebergang von einem System von Indices zu einem andern, dessen Basis eine andere der $\varphi(p-1)$ primitiven Wurzeln ist, ganz ähnlichen Gesetzen unterliegt, wie der Uebergang von einem Logarithmensystem zu einem andern; wir beschränken uns indessen auf folgende einfache Bemerkungen. Wie auch die Basis g gewählt sein mag, der Index von 1 ist stets $= 0$; denn es ist immer $g^0 = 1$. Ferner ist (den Fall $p = 2$ ausgenommen) der Index von -1 stets $= \frac{1}{2}(p-1)$; denn da nach §. 19

$$g^{p-1} - 1 = (g^{\frac{p-1}{2}} - 1)(g^{\frac{p-1}{2}} + 1) \equiv 0 \pmod{p}$$

ist, so muss mindestens eine der beiden Zahlen

$$g^{\frac{p-1}{2}} - 1, \quad g^{\frac{p-1}{2}} + 1$$

durch p theilbar sein; die erstere ist es aber nicht, denn sonst wäre

$$g^{\frac{p-1}{2}} \equiv 1 \pmod{p},$$

was mit der Voraussetzung im Widerspruch ist, dass g zum Exponenten $p-1$ gehört; es ist daher stets

$$g^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

und folglich

$$\text{Ind. } (-1) = \frac{p-1}{2}.$$

Es verdient endlich noch bemerkt zu werden, dass man die Indices, statt aus den Zahlen $0, 1, 2 \ldots (p-2)$, ebenso gut aus jedem andern vollständigen System incongruenter Zahlen in Bezug auf den Modul $p-1$ wählen kann; die so eben bewiesenen Fundamentalsätze erleiden dadurch nicht die geringste Aenderung.

Man kann nun die Indices benutzen, um eine Congruenz ersten Grades

$$ax \equiv b \pmod{p},$$

die hier die Stelle eines Divisionsproblems vertritt, mit Leichtigkeit aufzulösen; denn es muss offenbar

$$\text{Ind. } x \equiv \text{Ind. } b - \text{Ind. } a \pmod{p-1}$$

sein. Ist also z. B. die Congruenz

$$5x \equiv 6 \pmod{13}$$