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_0033
LOG Titel: §. 26. Eine Congruenz mit einer Unbekannten, deren Modulus eine Primzahl ist, kann nicht mehr incongruente Wurzeln haben, als ihr Grad Einheiten enthält
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

$$\alpha' \equiv \alpha \pmod{a}, \quad \beta' \equiv \beta \pmod{b}, \quad \gamma' \equiv \gamma \pmod{c}$$

u. s. w. ist; da ferner $\alpha, \beta, \gamma \ldots$ resp. $a, b, c \ldots$ verschiedene Werthe durchlaufen, so ist die Anzahl aller verschiedenen Restsysteme, also auch die Anzahl der resultirenden nach dem Modul m incongruenten Werthe von x gleich $abc \ldots = m$; d. h. x durchläuft ein vollständiges Restsystem nach dem Modul m.

Ist ferner α relative Primzahl zu a, β zu b u. s. f., so ist x auch relative Primzahl zu m, und umgekehrt; hieraus folgt leicht ein neuer Beweis des Satzes, dass $\varphi(ab) = \varphi(a)\,\varphi(b)$ ist.

Endlich ergiebt sich, dass, wenn x irgend eine ganze Zahl bedeutet, stets

$$\frac{x}{m} = h + \frac{u}{a} + \frac{v}{b} + \frac{w}{c} + \cdots$$

gesetzt werden kann, wo $h, u, v, w \ldots$ ganze Zahlen bedeuten. Denn lässt x in Bezug auf die Moduln $a, b, c \ldots$ resp. die Reste $\alpha, \beta, \gamma \ldots$, so ist nach dem Obigen

$$x = hm + Aa'\alpha + Bb'\beta + Cc'\gamma + \cdots,$$

wo h eine ganze Zahl bedeutet, und folglich

$$\frac{x}{m} = h + \frac{a'\alpha}{a} + \frac{b'\beta}{b} + \frac{c'\gamma}{c} + \cdots$$

§. 26.

Wir wenden uns nun zu der Betrachtung der Congruenzen höherer Grade, beschränken uns aber dabei auf den einfachsten Fall, in welchem der Modul p eine *Primzahl* ist. Die allgemeinste Form einer Congruenz $n$ten Grades ist die folgende:

$$ax^n + bx^{n-1} + cx^{n-2} + \cdots + h \equiv 0 \pmod{p},$$

in welcher der höchste Coefficient a als nicht theilbar durch die Primzahl p vorausgesetzt wird. Ebenso wie man jede Gleichung leicht auf den Fall zurückführen kann, in welchem der höchste Coefficient $= 1$ ist, so erreicht man auch hier dasselbe, wenn man die Congruenz mit einer Zahl a' multiplicirt, welche der Bedingung $aa' \equiv 1 \pmod{p}$ genügt und also eine Wurzel der stets lösbaren Congruenz $ax \equiv 1 \pmod{p}$ ist. Doch hängt hiervon die Gültigkeit der folgenden Sätze nicht im Mindesten ab.

Wir bezeichnen der Einfachheit halber das auf der linken Seite der obigen Congruenz befindliche Polynom $n$ten Grades kurz mit $f(x)$. Hat nun eine solche Congruenz

$$f(x) \equiv 0 \pmod{p} \qquad (1)$$

eine Wurzel $x \equiv \alpha$ und dividirt man $f(x)$ durch $x - \alpha$, so wird der Divisionsrest r_1 eine durch p theilbare Zahl sein; denn bezeichnet man den Quotienten der Division, welcher eine ganze Function vom $(n-1)$ten Grade mit ganzzahligen Coefficienten ist, mit $f_1(x)$, so ist

$$f(x) = (x - \alpha) f_1(x) + r_1 \qquad (2)$$

und hierin ist $r_1 = f(\alpha)$ der Voraussetzung nach $\equiv 0 \pmod{p}$.

Hat nun die Congruenz (1) noch eine zweite von α verschiedene, d. h. nicht mit α congruente Wurzel β, so folgt aus (2), dass

$$(\beta - \alpha) f_1(\beta) \equiv 0 \pmod{p}$$

und also, da $\beta - \alpha$ nicht durch p theilbar ist, dass $f_1(\beta) \equiv 0$, d. h. dass β eine Wurzel der Congruenz $f_1(x) \equiv 0 \pmod{p}$ sein muss. Man kann daher wieder

$$f_1(x) = (x - \beta) f_2(x) + r_2$$

setzen, wo der Rest r_2 wieder eine durch p theilbare Zahl, und der Quotient $f_2(x)$ eine ganze Function $(n-2)$ten Grades mit ganzzahligen Coefficienten ist. Setzt man aber diesen Ausdruck für $f_1(x)$ in die Gleichung (2) ein, so nimmt dieselbe die Form

$$f(x) = (x - \alpha)(x - \beta) f_2(x) + r_2 (x - \alpha) + r_1$$

oder, da r_1 und r_2 durch p theilbar sind, die Form

$$f(x) = (x - \alpha)(x - \beta) f_2(x) + p(lx + m)$$

an, in welcher l und m ganze Zahlen sind.

Besitzt nun die Congruenz (1) noch eine dritte von α und β verschiedene Wurzel γ, so ergiebt sich, da weder $(\gamma - \alpha)$ noch $(\gamma - \beta)$ durch p theilbar ist, dass γ eine Wurzel der Congruenz $f_2(x) \equiv 0$ ist; verfährt man daher wie früher, so erhält man eine Gleichung von der Form

$$f(x) = (x - \alpha)(x - \beta)(x - \gamma) f_3(x) + p(rx^2 + sx + t),$$

wo r, s, t ganze Zahlen bedeuten. Setzt man diese Schlussweise fort, so gelangt man offenbar zu folgendem Satze: ***Besitzt die Congruenz $n$ten Grades***

$$f(x) \equiv 0 \pmod{p},$$

deren Modulus p eine Primzahl ist, n incongruente Wurzeln $\alpha, \beta, \gamma \ldots \lambda$, so ist ihre linke Seite von der Form

$$f(x) = a(x - \alpha)(x - \beta)(x - \gamma) \ldots (x - \lambda) + p\psi(x), \qquad (3)$$

wo a den höchsten Coefficienten von $f(x)$, und $\psi(x)$ ein Polynom bedeutet, dessen Coefficienten ganze Zahlen sind.

Und aus diesem ersten Satze folgt sogleich der zweite*): *Eine Congruenz vom Grade n, deren Modulus eine Primzahl ist, kann niemals mehr als n incongruente Wurzeln haben.* Denn hätte die Congruenz (1) ausser den n Wurzeln $\alpha, \beta \ldots \lambda$ noch mindestens eine solche μ, die mit keiner der vorhergehenden congruent ist, so würde aus der Gleichung (3) folgen, dass das Product

$$a(\mu-\alpha)(\mu-\beta)(\mu-\gamma)\ldots(\mu-\lambda)$$

durch p theilbar wäre, was unmöglich ist, da der Voraussetzung nach keiner der Factoren durch p theilbar ist.

Man hätte diese beiden Sätze, welche für die Folge von der grössten Wichtigkeit sind, auch in umgekehrter Folge aus dem in der Gleichung (2) ausgesprochenen Resultat schliessen können. Da nämlich jede von α verschiedene Wurzel β der Congruenz (1) eine Wurzel der Congruenz nächst niedrigern Grades

$$f_1(x) \equiv 0 \pmod{p}$$

ist, so folgt hieraus unmittelbar, dass die erstere Congruenz höchstens eine Wurzel mehr besitzt, als die letztere; da nun eine Congruenz ersten Grades (sobald der Modulus eine Primzahl ist) nur eine Wurzel besitzt, so kann eine Congruenz vom zweiten Grade höchstens 2, folglich eine Congruenz dritten Grades höchstens 3 u. s. f., allgemein eine Congruenz $n$ten Grades höchstens n incongruente Wurzeln besitzen. Und nachdem so der zweite Satz bewiesen ist, ergiebt sich auch der erste leicht auf folgende Weise. Gesetzt, die Congruenz (1) vom $n$ten Grade hat wirklich n incongruente Wurzeln $\alpha, \beta, \gamma \ldots \lambda$, so bilde man die Differenz

$$f(x) - a(x-\alpha)(x-\beta)(x-\gamma)\ldots(x-\lambda) = \varphi(x)$$

wo a den höchsten Coefficienten in $f(x)$ bezeichnet, und denke sich dieselbe nach Potenzen von x geordnet; dann ist zu zeigen, dass alle Coefficienten dieses Polynoms $\varphi(x)$, dessen Grad höchstens $= n-1$, also jedenfalls kleiner als n ist, durch p theilbar sind. Gesetzt, dies wäre nicht der Fall, und es wäre x^r die höchste in $\varphi(x)$ vorkommende Potenz von x, deren Coefficient nicht durch p theilbar wäre, so wäre

$$\varphi(x) \equiv 0 \pmod{p}$$

---

*) ***Lagrange:*** *Nouvelle méthode pour résoudre les problèmes indéterminés en nombres entiers,* Mém. de l'Ac. de Berlin. T. XXIV.

eine Congruenz vom $r$ten Grade, welche, wie man unmittelbar einsieht, die n incongruenten Zahlen $\alpha, \beta \ldots \lambda$ zu Wurzeln hätte, also, da $r < n$ ist, mehr Wurzeln besässe, als ihr Grad Einheiten enthält. Da dies gegen den schon bewiesenen Satz streitet, so müssen wirklich alle Coefficienten von $\varphi(x)$ durch p theilbar sein, d. h. es muss

$$\varphi(x) = p\,\psi(x)$$

sein, wo sämmtliche Coefficienten des Polynoms $\psi(x)$ ganze Zahlen sind. Dies war aber der Inhalt des ersten Satzes.

Wir können zu diesen beiden Sätzen noch den folgenden dritten hinzufügen: *Wenn*

$$f(x) = \varphi(x)\ \psi(x)$$

ist, wo die Coefficienten der Polynome $\varphi(x)$ und $\psi(x)$ sämmtlich ganze Zahlen sind, und wenn die Congruenz

$$f(x) \equiv 0 \pmod{p}, \tag{4}$$

(wo p wieder eine Primzahl bedeutet) ebenso viele incongruente Wurzeln besitzt, als ihr Grad Einheiten enthält, so gilt dasselbe von jeder der beiden Congruenzen

$$\varphi(x) \equiv 0 \pmod{p}, \quad \psi(x) \equiv 0 \pmod{p}. \tag{5}$$

Zunächst leuchtet nämlich ein, dass jede Wurzel α der Congruenz (4) auch eine Wurzel von mindestens einer der beiden Congruenzen (5) sein muss; denn aus

$$\varphi(\alpha)\ \psi(\alpha) = f(\alpha) \equiv 0 \pmod{p}$$

folgt, dass mindestens eine der beiden Zahlen $\varphi(\alpha)$, $\psi(\alpha)$ durch p tbeilbar sein muss. Hätte nun eine der beiden Congruenzen (5) weniger incongruente Wurzeln als ihr Grad Einheiten enthält, so müsste nothwendig die Anzahl der Wurzeln der andern Congruenz d. h. der übrigen Wurzeln der Congruenz (4) ihren Grad übersteigen, da die Summe der Grade der beiden Polynome $\varphi(x)$ und $\psi(x)$ genau dem Grade des Polynoms $f(x)$ gleich ist. Da dies gegen den zweiten Satz verstossen würde, so muss die Anzahl der incongruenten Wurzeln einer jeden der beiden Congruenzen (5) genau ihrem Grade gleich sein *).

*) Eine weitere Entwicklung dieses Gegenstandes findet man in des Herausgebers Abhandlung: *Abriss einer Theorie der höheren Congruenzen in Bezug auf einen reellen Primzahl-Modulus*, Crelle's Journal Bd. LIV. — Vergl. die nachgelassene Abhandlung von *Gauss: Analysis Residuorum*, Gauss' Werke Bd. II. 1863.