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_0030
LOG Titel: §. 23. Digression über den Euler'schen Algorithmus
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

$$8x \equiv -12 \pmod{60};$$

der grösste gemeinschaftliche Divisor des Coefficienten 8 und des Modul 60 ist hier $= 4$; da die rechte Seite -12 durch denselben theilbar ist, so ist sie möglich und wird 4 nach dem Modul 60 incongruente Wurzeln haben. Wir finden dieselben, indem wir zunächst die Wurzeln der entsprechenden Congruenz

$$2x \equiv -3 \pmod{15}$$

suchen; wir haben oben gesehen, dass dieselben in der Form

$$x \equiv 6 \pmod{15}$$

enthalten sind, und schliessen daraus, dass

$$x \equiv 6, \equiv 21, \equiv 36, \equiv 51 \pmod{60}$$

die vier Wurzeln der ursprünglichen Congruenz sind.

§. 23.

Obgleich im Vorhergehenden das Problem, zu entscheiden, ob eine vorgelegte Congruenz ersten Grades Wurzeln hat oder nicht, und im erstern Fall dieselben aufzufinden, eine vollständige Lösung gefunden hat, so ist dieselbe, sobald der Modul k eine grosse Zahl ist, wegen der erforderlichen Potenzirung für praktische Zwecke nicht wohl anwendbar; wir wollen daher im Folgenden eine einfachere Methode angeben. Offenbar können wir uns auf den Fall beschränken, in welchem der Coefficient der Unbekannten relative Primzahl gegen den Modul ist; ausserdem können wir annehmen, dass die rechte Seite $= 1$ ist; denn um aus der Wurzel einer solchen Congruenz diejenige einer andern zu finden, in welcher die rechte Seite eine andere Zahl ist, genügt es offenbar, dieselbe mit dieser Zahl zu multipliciren. Nennen wir der Bequemlichkeit halber den Modul nicht k, sondern b, so reducirt sich also unsere Aufgabe auf die Auflösung der Congruenz

$$ax \equiv 1 \pmod{b}$$

oder, was dasselbe ist, auf die Auflösung der unbestimmten Gleichung ersten Grades*)

$$ax - by = 1.$$

---

*) Die erste Lösung dieser Aufgabe findet sich bei *Bachet de Meziriac: Problèmes plaisans et délectables qui se font par les nombres.* 2e éd. 1624.

Wir schicken derselben einige Sätze über einen Algorithmus voraus, der zuerst von *Euler**) behandelt und für die Theorie der Kettenbrüche, sowie auch für unsere spätern Untersuchungen von Wichtigkeit ist. Es seien

$$a, b \tag{1}$$

irgend zwei unbestimmte Grössen, und ebenso

$$\gamma, \delta, \varepsilon \ldots \lambda, \mu, \nu \tag{2}$$

eine Reihe von beliebig vielen unbestimmten Grössen. Aus diesen bilden wir nun successive eine neue Reihe $c, d, e \ldots l, m, n$ nach folgendem Gesetz:

$$\left.\begin{aligned} c &= \gamma b + a \\ d &= \delta c + b \\ e &= \varepsilon d + c \\ &\cdots\cdots \\ n &= \nu m + l \end{aligned}\right\} \tag{3}$$

Substituirt man den Ausdruck für c in den für d, so wird der letztere eine ähnliche Form annehmen wie der erstere, nämlich

$$d = \delta a + (\gamma\delta + 1)b;$$

er besteht also aus einem Gliede, welches den Factor a, und aus einem zweiten, welches den Factor b enthält. Substituirt man nun diesen Ausdruck für d, und den ersten für c in den Ausdruck für e, so nimmt auch dieser letztere dieselbe Form an. So kann man fortfahren, und aus dem Ausdruck für n erkennt man, dass dieses Gesetz allgemein ist; denn sobald l und m schon diese Form erhalten haben, so nimmt auch n dieselbe an. Wir können daher

$$n = Ga + Hb$$

setzen, wo nun G und H unabhängig von a und b sein werden. Man bezeichnet den Coefficienten H, der nur von den in der Reihe (2) befindlichen Grössen abhängt, durch das Zeichen**)

$$[\gamma, \delta, \varepsilon \ldots \lambda, \mu, \nu], \tag{4}$$

und wir werden im Folgenden einige interessante Sätze beweisen, die sich auf dasselbe beziehen.

---

*) *Solutio problematis arithmetici de inveniendo numero, qui per datos numeros divisus, relinquat data residua*, Comm. Ac. Petrop. VII, p. 46. — *De usu novi algorithmi in problemate Pelliano solvendo*, Nov. Comm. Petrop. XI, p. 28. — Vergl. *Gauss: D. A.* art. 27.

**) *Gauss: D. A.* art. 27.

Zunächst leuchtet ein, dass, wenn man mit den Anfangsgliedern

$$b,\ c = \gamma b + a \tag{1'}$$

und der Reihe

$$\delta,\ \varepsilon \ldots \lambda,\ \mu,\ \nu \tag{2'}$$

in derselben Weise verfährt wie oben, man genau dieselben Glieder $d, e \ldots l, m, n$ erhalten wird. Wir können daher gleichzeitig

$$n = Ga + [\gamma, \delta, \varepsilon \ldots \mu, \nu]b$$

und

$$n = G'b + [\delta, \varepsilon \ldots \mu, \nu]c$$

setzen; ersetzen wir hierin c durch $\gamma b + a$, so erhalten wir

$$n = [\delta, \varepsilon \ldots \mu, \nu]\ a + (\gamma[\delta, \varepsilon \ldots \mu, \nu] + G')b,$$

woraus, durch Vergleichung der Coefficienten von a in den beiden Formen für n, zunächst

$$G = [\delta, \varepsilon \ldots \mu, \nu]$$

folgt. Der Coefficient G lässt sich daher durch dasselbe Zeichen ausdrücken wie H. Wir können also von jetzt an schreiben

$$n = [\delta \ldots \mu, \nu]a + [\gamma, \delta \ldots \mu, \nu]b;$$

da nun auch

$$G' = [\varepsilon \ldots \mu, \nu]$$

sein muss, so erhalten wir durch Vergleichung der Coefficienten von b in den beiden Formen für n den Satz

$$[\gamma, \delta, \varepsilon \ldots \nu] = \gamma[\delta, \varepsilon \ldots \nu] + [\varepsilon \ldots \nu], \tag{5}$$

in welchem das Gesetz ausgedrückt ist, nach welchem die Fortbildung der Ausdrücke von der Form (4) nach links hin geschieht.

Einen ganz analogen Satz für die Fortbildung nach rechts hin erhält man durch die einfache Bemerkung, dass durch die Annahme $a = 0$, $b = 1$ die drei Grössen l, m, n resp. in

$$[\gamma \ldots \lambda],\ [\gamma \ldots \lambda, \mu],\ [\gamma \ldots \lambda, \mu, \nu]$$

übergehen, so dass zwischen diesen drei consecutiven Ausdrücken die Relation

$$[\gamma \ldots \lambda, \mu, \nu] = [\gamma \ldots \lambda, \mu]\nu + [\gamma \ldots \lambda] \tag{6}$$

besteht.

Verbindet man diese beiden Sätze mit einander, so überzeugt man sich leicht von der Richtigkeit des folgenden:

$$[\nu, \mu \ldots \delta, \gamma] = [\gamma, \delta \ldots \mu, \nu]. \tag{7}$$

Nimmt man nämlich an, dieser Satz sei für alle Ausdrücke dieser Art bewiesen, welche eine kleinere Anzahl von Grössen enthalten, so dass also z. B.

$$[\delta, \varepsilon \ldots \nu] = [\nu \ldots \varepsilon, \delta] \text{ und } [\varepsilon \ldots \nu] = [\nu \ldots \varepsilon],$$

so folgt aus (5):

$$[\gamma, \delta, \varepsilon \ldots \nu] = [\nu \ldots \varepsilon, \delta]\gamma + [\nu \ldots \varepsilon];$$

verbindet man dies mit dem Satz (6), so ergiebt sich unmittelbar die Richtigkeit der Gleichung (7). In der That gilt aber der Satz wirklich für die ersten Fälle; enthält nämlich der Ausdruck nur eine einzige Grösse γ, so versteht sich dies von selbst; und ausserdem ist

$$[\gamma, \delta] = \gamma\delta + 1 = [\delta, \gamma].$$

Hieraus folgt also, dass der Satz auch für jede beliebige Anzahl der Grössen $\gamma, \delta \ldots \mu, \nu$ gilt.

Wir können die Gleichungen (3), durch welche das Bildungsgesetz der Grössen $c, d \ldots n$ ausgedrückt wird, auch in folgender Weise schreiben:

$$\begin{aligned} -c &= (-\gamma)b + (-a) \\ +d &= (-\delta)\,(-c) + b \\ -e &= (-\varepsilon)d + (-c) \\ &\cdots\cdots\cdots \\ \pm n &= (-\nu)\,(\mp m) + (\pm l) \end{aligned}$$

wo in der letzten Gleichung das obere oder untere Zeichen zu nehmen ist, je nachdem die Anzahl der Grössen $\gamma, \delta \ldots \mu, \nu$ gerade oder ungerade ist. Hieraus geht hervor, dass aus den Anfangsgliedern

$$-a, b \qquad (1'')$$

und der Reihe

$$-\gamma, -\delta, -\varepsilon \ldots -\lambda, -\mu, -\nu \qquad (2'')$$

durch dasselbe frühere Verfahren die Reihe

$$-c, +d, -e \ldots \pm n$$

entsteht. Es wird daher auch

$$\pm n = [-\delta, -\varepsilon \ldots -\nu]\,(-a) + [-\gamma, -\delta, -\varepsilon \ldots -\nu]b$$

und folglich

$$[-\gamma, -\delta \ldots -\nu] = \pm[\gamma, \delta \ldots \nu] \qquad (8)$$

sein, worin wieder das obere oder untere Zeichen zu nehmen ist, je nachdem die Anzahl der Grössen $\gamma, \delta \ldots \nu$ gerade oder ungerade ist.

Endlich kann man die Gleichungen (3) auch in umgekehrter Folge so schreiben:

$$l = (-\nu)m + n$$
$$k = (-\mu)l + m$$
$$\cdots\cdots\cdots$$
$$b = (-\delta)c + d$$
$$a = (-\gamma)b + c$$

Es wird daher

$$a = [-\mu \ldots -\gamma]n + [-\nu, -\mu \ldots -\gamma]m$$

oder mit Hülfe des Satzes (8):

$$\pm a = -[\mu \ldots \gamma]n + [\nu, \mu \ldots \gamma]m$$

oder mit Berücksichtigung des Satzes (7):

$$\pm a = -[\gamma, \delta \ldots \mu]n + [\gamma, \delta \ldots \mu, \nu]m.$$

Wenn man nun $a = 1$, $b = 0$ setzt, so gehen m, n resp. in

$$[\delta \ldots \mu], \quad [\delta \ldots \mu, \nu]$$

über, und man erhält das Resultat:

$$[\delta \ldots \mu]\,[\gamma, \delta \ldots \mu, \nu] - [\delta \ldots \mu, \nu]\,[\gamma, \delta \ldots \mu] = \pm 1, \qquad (9)$$

wo wieder das obere oder untere Zeichen zu nehmen ist, je nachdem die Anzahl der Grössen $\gamma, \delta \ldots \mu, \nu$ gerade oder ungerade ist.

Zum Schluss wollen wir bemerken, dass diese Ausdrücke in der Theorie der Kettenbrüche von der grössten Wichtigkeit sind; bezeichnen wir nämlich einen gewöhnlichen Kettenbruch, in welchem die Zähler sämmtlich $= 1$, und dessen sogenannte Quotienten $\gamma, \delta \ldots \mu, \nu$ sind, kurz durch das Symbol $(\gamma, \delta \ldots \mu, \nu)$, so dass also

$$(\gamma, \delta \ldots \lambda, \mu, \nu) = \gamma + \frac{1}{(\delta \ldots \lambda, \mu, \nu)} = \left(\gamma, \delta \ldots \lambda, \mu + \frac{1}{\nu}\right)$$

ist, so ergiebt sich allgemein durch Reduction desselben

$$(\gamma, \delta \ldots \mu, \nu) = \frac{[\gamma, \delta \ldots \mu, \nu]}{[\delta \ldots \mu, \nu]}. \qquad (10)$$

Denn gesetzt, dieser Satz sei schon für jede kleinere Anzahl der Grössen $\gamma, \delta, \varepsilon \ldots \mu', \nu$ bewiesen, so dass also namentlich

$$(\delta, \varepsilon \ldots \mu, \nu) = \frac{[\delta, \varepsilon \ldots \mu, \nu]}{[\varepsilon \ldots \mu, \nu]}$$

ist, so folgt hieraus

$$(\gamma, \delta, \varepsilon \ldots \mu, \nu) = \gamma + \frac{1}{(\delta, \varepsilon \ldots \mu, \nu)}$$
$$= \gamma + \frac{[\varepsilon \ldots \mu, \nu]}{[\delta, \varepsilon \ldots \mu, \nu]} = \frac{\gamma\,[\delta, \varepsilon \ldots \mu, \nu] + [\varepsilon \ldots \mu, \nu]}{[\delta, \varepsilon \ldots \mu, \nu]}$$