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_0031
LOG Titel: §. 24. Zweite Methode der Auflösung der Congruenzen ersten Grades mit einer Unbekannt
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

und hieraus ergiebt sich mit Berücksichtigung des Satzes (5) die Gleichung (10). In der That ist aber

$$(\gamma, \delta) = \gamma + \frac{1}{\delta} = \frac{\gamma\delta + 1}{\delta} = \frac{[\gamma, \delta]}{[\delta]};$$

da also der Satz für zwei Grössen γ, δ richtig ist, so ist er auch für jede beliebige Anzahl der Grössen γ, $\delta \ldots \mu$, ν richtig.

Sind die Elemente γ, $\delta \ldots \mu$, ν ganze Zahlen, so gilt dasselbe von den Zählern und Nennern der Brüche

$$\frac{[\gamma]}{1}, \frac{[\gamma, \delta]}{[\delta]} \ldots \frac{[\gamma, \delta \ldots \mu, \nu]}{[\delta \ldots \mu, \nu]};$$

ferner ist jeder dieser Brüche irreductibel, d. h. durch die kleinsten Zahlen ausgedrückt; denn es folgt z. B. aus der Relation (9), dass Zähler und Nenner des letzten der obigen Brüche ohne gemeinschaftlichen Divisor sind.

§. 24.

Die vorstehenden Sätze, welche eigentlich in die Theorie der Differenzen-Gleichungen zweiter Ordnung*) gehören, sind deshalb gleich in solcher Vollständigkeit aufgestellt, damit wir bei einer spätern Untersuchung nicht nöthig haben, von Neuem auf denselben Algorithmus zurückzukommen; für unsern nächsten Bedarf, nämlich für die Lösung der unbestimmten Gleichung

$$ax - by = 1,$$

in welcher wir nun wieder a und b als zwei gegebene relative Primzahlen ansehen, genügt schon ein kleiner Theil der vorhergehenden Resultate. Zu dem Zweck verfahren wir nun, wie es bei der Aufsuchung des grössten gemeinschaftlichen Divisors der beiden Zahlen (oder bei der Verwandlung des Bruches $a:b$ in einen Kettenbruch) geschieht, indem wir das System der folgenden Gleichungen bilden

$$\begin{aligned} a &= \gamma b + c \\ b &= \delta c + d \\ &\cdots\cdots \\ l &= \nu m + 1 \end{aligned}$$

wobei zuletzt der Rest 1 auftreten muss (§. 5); diese Gleichungen können wir auch so schreiben

*) Vergl. *Jacobi: Allgemeine Theorie der kettenbruchähnlichen Algorithmen, in welchen jede Zahl aus Drei vorhergehenden gebildet wird*, Crelle's Journal Bd. LXIX.

$$c = (-\gamma)b + a$$
$$d = (-\delta)c + b$$
$$\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot$$
$$1 = (-\nu)m + l$$

und hieraus folgt, dass

$$1 = [-\delta, -\varepsilon \cdots -\mu, -\nu]a + [-\gamma, -\delta, -\varepsilon \cdots -\mu, -\nu]b$$

oder nach §. 23, (8)

$$1 = \mp[\delta, \varepsilon \ldots \mu, \nu]a \pm [\gamma, \delta, \varepsilon \ldots \mu, \nu]b$$

ist, worin das obere oder untere Zeichen zu nehmen ist, je nachdem die Anzahl der Grössen $\gamma, \delta \ldots \mu, \nu$ gerade oder ungerade ist. Wir erhalten daher folgende Auflösung der unbestimmten Gleichung:

$$x = \mp[\delta, \varepsilon \ldots \mu, \nu], \quad y = \mp[\gamma, \delta, \varepsilon \ldots \mu, \nu].$$

Hiermit ist also auch eine Wurzel x der Congruenz

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

gefunden, und dies genügt vollständig, da alle anderen dieser einen nach dem Modul b congruent sind*).

Wenden wir diese Methode auf unser Beispiel

$$2x \equiv 1 \pmod{15}$$

an, so erhalten wir

$$2 = 0 \cdot 15 + 2, \quad 15 = 7 \cdot 2 + 1$$

also

$$\gamma = 0, \ \delta = 7, \quad x \equiv -[\delta] \equiv -7 \equiv 8 \pmod{15}$$

und hieraus folgt, dass

$$x \equiv -7 \cdot (-3) \equiv 21 \equiv 6 \pmod{15}$$

die Wurzel der Congruenz

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

ist.

Als zweites Beispiel wählen wir die Congruenz

$$37x \equiv 1 \pmod{100};$$

indem wir ebenso verfahren, erhalten wir

$$37 = 0 \cdot 100 + 37; \quad 100 = 2 \cdot 37 + 26; \quad 37 = 1 \cdot 26 + 11;$$
$$26 = 2 \cdot 11 + 4; \quad 11 = 2 \cdot 4 + 3; \quad 4 = 1 \cdot 3 + 1$$

*) Man überzeugt sich leicht, dass aus einer Lösung x_0, y_0 alle anderen sich durch die Gleichungen $x = x_0 + bz$, $y = y_0 + az$ ableiten lassen, wo z eine willkürliche ganze Zahl bedeutet. Vergl. § 60.

und also

$$x \equiv - [2, 1, 2, 2, 1] \text{ (mod. } 100).$$

Nun ist, wenn wir von rechts nach links rechnen,

$$[1] = 1, [2, 1] = 3, [2, 2, 1] = 7, [1, 2, 2, 1] = 10,$$
$$[2, 1, 2, 2, 1] = 27,$$

also

$$x \equiv - 27 \equiv 73 \text{ (mod. } 100).$$

Da $\varphi(100) = \varphi(4)\,\varphi(25) = 2 \cdot 20 = 40$ ist, so hätten wir nach unserer früheren Methode die Auflösung

$$x \equiv 37^{39} \text{ (mod. } 100)$$

erhalten; die hierin angedeutete Rechnung würde sich zwar durch einige Kunstgriffe bedeutend abkürzen lassen, allein doch viel langwieriger sein als die nach der zweiten Methode ausgeführte Rechnung.

Kommt es darauf an, auch den Werth von

$$y = \mp [\gamma, \delta, \varepsilon \ldots \mu, \nu]$$

zu berechnen, so ist es vortheilhaft, die Berechnung des Werthes

$$x = \mp [\delta, \varepsilon \ldots \mu, \nu]$$

von rechts nach links vorzunehmen; man findet dann nach der Formel (5) des §. 23 aus

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

unmittelbar den Werth von y. So oft $\gamma = 0$, also $a < b$ ist, reducirt sich y auf

$$y = \mp [\varepsilon \ldots \mu, \nu].$$

Dies ist in unseren Beispielen der Fall; in dem zweiten erhält man auf diese Weise

$$y = - [0, 2, 1, 2, 2, 1] = - [1, 2, 2, 1] = - 10,$$

und in der That ist

$$37 \cdot (-27) - 100 \cdot (-10) = 1.$$

Bei dieser Lösung der unbestimmten Gleichung $ax - by = 1$ in ganzen Zahlen x, y war stillschweigend vorausgesetzt, dass die beiden gegebenen relativen Primzahlen a, b *positive* Zahlen sind; doch erkennt man leicht, dass hierdurch die Allgemeinheit der Lösung nicht beeinträchtigt wird.

Wir bemerken ferner, dass durch wiederholte Anwendung desselben Verfahrens folgende allgemeinere Aufgabe gelöst werden kann: *Sind a, b, c ... gegebene ganze Zahlen, deren grösster ge-*