1 Zahlentheorie

1.1 Kongruenzen

Der letzte Abschnitt zeigte, daß es sinnvoll ist, mit großen Zahlen möglichst einfach rechnen zu können. Oft kommt es nicht darauf, an eine Zahl im Detail zu kennen, sondern es genügt zu wissen, welchen Rest sie bei Division durch eine andere Zahl läßt. Das ist meistens wesentlich einfacher, als die Zahl oder den Quotienten explizit zu berechnen.
Jede ganze Zahl n läßt bei Division durch eine andere Zahl – etwa m – einen wohldefinierten Rest, der eine der m Zahlen 0, 1, ..., $m-1$ ist.

$$n = k \cdot m + r,\ 0 \leq r \leq m-1\ . \tag{1}$$

Alle ganzen Zahlen kann man in m Teilmengen (Restklassen) unterteilen in Abhängigkeit davon, welchen Rest sie bei Division durch m lassen. Interessiert man sich dafür, welchen Rest n bei Division durch m läßt, muß man weder die Zahl selbst noch den Quotienten (in (1) mit k bezeichnet) kennen. Es genügt zu wissen, in welche Restklasse die Zahl gehört. Ist z.B. $m = 7$, gibt es die 7 Reste 0, 1, 2, 3, 4, 5 und 6. Die Zahlen 1, 8, -6 und 2^{123456} lassen alle bei Division durch 7 den Rest 1. Für 1 und 8 ist das klar. Für -6 sieht man das, weil $-6 = (-1) \cdot 7 + 1$ gilt. Auch für 2^{123456} ist das leicht zu zeigen. Da $123456 = 3 \cdot 41152$, ist $2^{123456} - 1$ durch $2^3 - 1 = 7$ teilbar. Also läßt der Nachfolger von $2^{123456} - 1$, d.h. 2^{123456}, den Rest 1 bei Division durch 7.

1.1.1 Definition

Zwei ganze Zahlen a und b heißen restgleich bezüglich m, wenn $a - b$ durch m teilbar ist. Die beiden Zahlen gehören dann in die gleiche Restklasse bezüglich m. Das wird

$$a \equiv b \bmod m$$

geschrieben und

„a ist kongruent b modulo m“

gelesen. Die drei Ausdrücke

$$a \equiv b \bmod m \iff m \,|\, a-b \iff \exists k \in \mathbb{Z} :\ a - b = k \cdot m\ .$$

sind also äquivalent. Das Symbol $\exists$ bedeutet „es existiert“. Der letzte Ausdruck bedeutet

„Es existiert eine ganze Zahl k, so daß $a - b = k \cdot m$.“

1.1.2 Rechenregeln

Das besondere an diesen Kongruenzen ist, daß man mit ihnen fast wie mit ganzen Zahlen rechnen kann. Es sei $a \equiv b \bmod m$ und $c \equiv d \bmod m$. Dann gilt

$$\begin{aligned} a + c &\equiv b + d \bmod m \\ a - c &\equiv b - d \bmod m \\ a \cdot c &\equiv b \cdot d \bmod m \end{aligned}$$

Die Beweise sind einfach. Die letzte Zeile wird hier exemplarisch vorgeführt: Es ist zu zeigen, daß $a \cdot c - b \cdot d$ durch m teilbar ist, wenn $a - b$ und $c - d$ es sind. Nach Definition gibt es also ganze Zahlen k und j, so daß gilt:

$$\begin{aligned} a - b &= k \cdot m \\ c - d &= j \cdot m \end{aligned}$$

Das sind richtige Gleichungen. Man kann wie gewohnt mit ihnen rechnen. Multipliziert man die erste Gleichung mit c und die zweite mit b, folgt

$$\begin{aligned} a \cdot c - b \cdot c &= c \cdot k \cdot m \\ c \cdot b - d \cdot b &= b \cdot j \cdot m \end{aligned}$$

Addiert man diese beiden Gleichungen, erhält man

$$a \cdot c - d \cdot b = c \cdot k \cdot m + b \cdot j \cdot m = (c \cdot k + b \cdot j)m \ .$$

$a \cdot c - d \cdot b$ ist somit ein Vielfaches von m. Also sind $a \cdot c$ und $d \cdot b$ restgleich. ■

Multipliziert man die Kongruenz $a \equiv b \bmod m$ mit sich selbst, erhält man

$$a^2 \equiv b^2 \bmod m \ .$$

Das kann man n-mal ausführen und erhält

$$a^n \equiv b^n \bmod m \ .$$

Kongruenzen lassen sich daher auch potenzieren. Anders als mit ganzen Zahlen funktioniert die Division. Das sieht man an folgendem Beispiel:
Aus $22 \equiv -2 \bmod 8$ folgt $11 \not\equiv -1 \bmod 8$, aber aus $33 \equiv -3 \bmod 4$ folgt und $11 \equiv -1 \bmod 4$. Man kann also nicht in jedem Fall beide Seiten einer Kongruenz durch einen gemeinsamen Faktor teilen. Es gilt

$$ac \equiv bc \bmod m \implies a \equiv b \bmod m \text{ falls } ggt(m, c) = 1 \tag{2}$$

$$ac \equiv bc \bmod m \implies a\frac{c}{d} \equiv b\frac{c}{d} \bmod \frac{m}{d} \text{ falls } ggt(m, c) = d \tag{3}$$

$$ac \equiv bc \bmod m \implies a \equiv b \bmod \frac{m}{d} \text{ falls } ggt(m, c) = d \tag{4}$$

Das läßt sich leicht mit der Definition der Kongruenzen beweisen. $ac \equiv bc \bmod m$ bedeutet, es existiert eine ganze Zahl k mit

$$ac - bc = k \cdot m \tag{5}$$

oder

$$a - b = \frac{k \cdot m}{c} \ . \tag{6}$$

Es sei als erstes $ggt(m, c) = 1$ Die linke Seite von (6) ist eine ganze Zahl, die rechte Seite daher auch. Aber $ggt(m, c) = 1$, somit muß k durch c teilbar sein. Es ist folglich

$$a - b = \frac{k}{c} \cdot m$$

mit einer ganzen Zahl $\frac{k}{c}$. Das bedeutet aber gerade $a \equiv b \bmod m$. Damit ist (2) bewiesen.
Ist $ggt(m, c) = d$, so ist m und c durch d teilbar und aus (5) folgt

$$a\frac{c}{d} - b\frac{c}{d} = k \cdot \frac{m}{d} \ .$$

Damit ist (3) bewiesen.
(4) folgt aus (3) und (2), denn wenn $ggt(m, c) = d$, dann ist $ggt(\frac{m}{d}, \frac{c}{d}) = 1$ und man kann (3) durch den gemeinsamen Faktor $\frac{c}{d}$ teilen. ■

1.1.3 Beispielaufgaben

Aufgabe 1:
Für welche ganzzahligen n ist $4n^2+1$ durch 5 teilbar?

Wir stellen eine Restetabelle bezüglich der Division durch 5 auf:

$$\begin{array}{rcccccc} n & \equiv & 0 & 1 & 2 & 3 & 4 \mod 5 \\ n^2 & \equiv & 0 & 1 & 4 & 4 & 1 \mod 5 \\ 4n^2 & \equiv & 0 & 4 & 1 & 1 & 4 \mod 5 \\ 4n^2+1 & \equiv & 1 & 0 & 2 & 2 & 0 \mod 5 \end{array}$$

Durch 5 teilbar ist $4n^2+1$ also genau dann, wenn $n \equiv \pm 2 \mod 5$ ist. Das sind die Zahlen $n = 5k-2$ und $n = 5k+2$.
Aufgabe 2:
Beweise, daß $n^7 - n$ stets durch 42 teilbar ist!

Diese Aufgabe kann man auf verschiedene Weise lösen. Unter anderem sieht man, daß $f_n = \frac{n^7-n}{42}$ die Bildungsvorschrift für eine arithmetische Folge 7-ter Ordnung ist. Falls sie 7 aufeinanderfolgende ganzzahlige Glieder enthält, ist sie also ganzzahlig. Besonders einfach lassen sich die Glieder f_0, $f_{\pm 1}$, $f_{\pm 2}$ und $f_{\pm 3}$ berechnen. Eine Lösung mit Kongruenzen erhält man, wenn man $n^7 - n$ in Faktoren zerlegt. Es gilt

$$n^7 - n = (n-1)n(n+1)(n^2-n+1)(n^2+n+1) \; .$$

Hieran erkennt man sofort, daß $n^7 - n$ durch 2 und durch 3 – also durch 6 – teilbar ist (Produkt von drei aufeinanderfolgenden Zahlen). Es bleibt die Teilbarkeit durch 7 zu zeigen ($42 = 2 \cdot 3 \cdot 7$). Dazu stellen wir eine Restetabelle bezüglich der Division durch 7 auf:

n	$n-1$	$n+1$	n^2-n+1	n^2+n+1
0	6	1	1	1
1	0	2	1	3
2	1	3	3	0
3	2	4	0	6
4	3	5	6	0
5	4	6	0	3
6	5	0	3	1

Wir sehen, daß es stets einen Faktor gibt, der durch 7 teilbar ist, gleichgültig, welchen Rest n läßt. Damit ist die Teilbarkeit des Produkts gesichert und die Aufgabe gelöst.
Aufgabe 3:
Bestimme alle ganzzahligen Lösungen x, y und z der Gleichung $2^x + 7y = z^3 - 1$

Wir lösen die Gleichung nach y auf

$$y = \frac{2^x - z^3 + 1}{7}$$

und stellen fest, daß es nur eine ganzzahlige Lösung geben kann, wenn $2^x - z^3 + 1$ durch 7 teilbar ist.

Wir sehen, daß die Reste von 2^x bei Division durch 7

$$\begin{aligned} 2^0 &\equiv 1 \bmod 7 \\ 2^1 &\equiv 2 \bmod 7 \\ 2^3 &\equiv 4 \bmod 7 \\ 2^4 &\equiv 1 \bmod 7 \\ 2^5 &\equiv 2 \bmod 7 \\ 2^6 &\equiv 4 \bmod 7 \\ &... \end{aligned}$$

periodisch die Werte 1, 2 und 4 annehmen und an der Restetabelle

$$\begin{array}{rcccccccc} z & \equiv & 0 & 1 & 2 & 3 & 4 & 5 & 6 & \bmod 7 \\ 1-z^3 & \equiv & 1 & 0 & 0 & 2 & 0 & 2 & 2 & \bmod 7 \end{array}$$

daß $1-z^3$ nur die Reste 0, 1 und 2 annehmen kann. Die Summe 2^x+1-z^3 kann also nie durch 7 teilbar sein. Folglich kann die gegebene Gleichung keine Lösung haben.

1.1.4 Neunerprobe

Die Teilbarkeitsregel für die 9 (siehe Punkt 3.2.1) lautet: Eine Zahl n ist genau dann durch 9 teilbar, wenn ihre Quersumme $Q(n)$ durch 9 teilbar ist. Tatsächlich gilt mehr: n läßt bei Division durch 9 den gleichen Rest wie $Q(n)$. Das kann man mit Kongruenzen leicht beweisen: Es sei

$$n = a_0 + 10a_1 + 100a_2 + ... + 10^k a_k = \sum_{j=0}^{k} 10^j a_j$$

die Dezimaldarstellung von n. $10^j - 1$ besteht für jedes j nur aus Neunen, ist offensichtlich durch 9 teilbar. Also ist $10^j \equiv 1 \bmod 9$ und folglich $10^j a_j \equiv a_j \bmod 9$ für jedes $j = 0, 1, 2, ...$ Summation über alle j ergibt

$$n = \sum_{j=0}^{k} 10^j a_j \equiv \sum_{j=0}^{k} a_j = Q(n) \bmod 9 \qquad \blacksquare$$

Diese Regel kann man zum Testen von komplizierten Aufgaben verwenden. Angenommen man hat das Ergebnis der Aufgabe $9854758739 \cdot 8457498579485 + 677910847 \cdot 825734979856$ als 83906383735851598767447 diktiert bekommen und möchte feststellen, ob man sich verhört hat, ohne die Aufgabe nachrechnen zu können. Man bildet die Quersummen der Faktoren und erhält

$$65 \cdot 83 + 49 \cdot 73 \equiv 2 \cdot 2 + 4 \cdot 1 = 8 \bmod 9$$

Aber für das Ergenbis erhalten wir

$$83906383735851598767447 \equiv 126 \equiv 0 \bmod 9$$

Man sollte also noch einmal nachfragen.

1.2 Lineare Diophantische Gleichungen und Kongruenzen

1.2.1 Lineare Kongruenzen

Die einfachste lineare Gleichung ist $ax = 1$. Sie hat die Lösung $x = \frac{1}{a}$. Analog hierzu kann man die Frage stellen, welche Lösungen x die Kongruenz

$$a \cdot x \equiv 1 \bmod b \tag{7}$$

besitzt. Das heißt, welche Zahl – mit a multipliziert – läßt bei Division durch b Rest 1? Ein Beispiel ist

$$6x \equiv 1 \bmod 13$$

Mit ein wenig Probieren findet man als Lösung die Zahlen, die bei Division durch 13 Rest 11 lassen, also $x \equiv 11 \bmod 13$. Es gibt modulo 13 genau diese eine Lösung.
Für die allgemeine Gleichung (7) stellt man fest, daß sie keine Lösung hat, falls a und b gemeinsame Teiler haben. Z.B. gibt es keine ganze Zahl x, die die Kongruenz $6x \equiv 1 \bmod 14$ löst, da alle Reste von $6x$ bezüglich 14 durch den gemeinsamen Teiler von 6 und 14 – also 2 – teilbar sein müssen. Es genügt somit Aufgaben

$$a \cdot x \equiv 1 \bmod b\ , \quad ggT(a,b) = 1 \tag{8}$$

zu untersuchen. Ist z.B. $b = 15$, gibt es 8 teilerfremde a, nämlich 1, 2, 4, 7, 8, 11, 13 und 14. In einer Tabelle kann man die möglichen Produkte dieser Zahlen untereinander (modulo 15) darstellen:

	1	2	4	7	8	11	13	14
1	1	2	4	7	8	11	13	14
2	2	4	8	14	1	7	11	13
4	4	8	1	13	2	14	7	11
7	7	14	13	4	11	2	1	8
8	8	1	2	11	4	13	14	7
11	11	7	14	2	13	1	8	4
13	13	11	7	1	14	8	4	2
14	14	13	11	8	7	4	2	1

Es fällt auf, daß jede der 8 Zahlen in jeder Spalte und jeder Reihe genau einmal vorkommt. Ist a einer der Faktoren, läßt sich stets ein x finden, so daß $a \cdot x \equiv 1 \bmod 15$ ist.
Diese Eigenschaft gilt für beliebige Kongruenzen:

Satz 9:
Für $ggT(a,b) = 1$ gibt es genau ein x modulo b, das die Kongruenz $a \cdot x \equiv 1 \bmod b$ löst.

Beweis: Als erstes beweisen wir indirekt, daß eine Lösung der Aufgabe existiert. Dazu betrachten wir die zu b teilerfremden Zahlen modulo b. Das seien die Zahlen x_1, x_2, ..., x_k, die modulo b natürlich verschieden sein sollen. Weiter seien b_i die Reste von $a \cdot x_i$ bei Division durch b, also

$$a \cdot x_i \equiv b_i \bmod b\ , \quad i = 1, ...,\ k\ .$$

Da nach Voraussetzung die $a \cdot x_i$ zu b teilerfremd sind, sind auch die b_i teilerfremd. Wir nehmen nun an, daß es kein x mit $a \cdot x \equiv 1 \bmod b$ gibt. Dann müssen natürlich auch alle b_i ungleich

1 sein. Da 1 zu b teilerfremd ist, es aber nur k zu b teilerfremde Zahlen gibt, müssen zwei der b_i gleich sein. O.B.d.A. sei $b_p = b_q = c$. Es gilt also $a \cdot x_p \equiv c \bmod b$ und $a \cdot x_q \equiv c \bmod b$. Subtrahiert man beide Kongruenzen, erhält man $a \cdot (x_p - x_q) \equiv 0 \bmod b$. Wegen $ggT(a, b) = 1$ muß somit $x_p - x_q$ durch b teilbar sein, das heißt, es gilt $x_p \equiv x_q \bmod b$ im Gegensatz zur Annahme, daß x_p und x_q nicht restgleich sind.
Als nächstes beweisen wir die Eindeutigkeit ebenfalls indirekt. Das verläuft exakt so wie eben. Wir nehmen an, es gibt zwei bezüglich b nicht restgleiche Lösungen x und y mit $a \cdot x \equiv 1 \bmod b$ und $a \cdot y \equiv 1 \bmod b$. Subtrahiert man beide Kongruenzen, erhält man $a \cdot (x - y) \equiv 0 \bmod b$. Wegen $ggT(a, b) = 1$ muß also $x - y$ durch b teilbar sein, das heißt, es gilt $x \equiv y \bmod b$ im Gegensatz zur Annahme, daß x und y nicht restgleich sind. ■
Der eben bewiesene Satz ist der Schlüssel für viele andere Aufgaben, zum Beispiel für

1.2.2 Lineare Diophantische Gleichungen

Wir wollen die Diophantische Gleichung

$$a \cdot x - b \cdot y = 1 \tag{9}$$

lösen. Natürlich geht es – wie immer bei Diophantischen Gleichungen – um ganzzahlige Lösungen. Stellt man (9) nach y um erhält man

$$y = \frac{a \cdot x - 1}{b} \ ,$$

das heißt, für ganzzahliges y muß $a \cdot x - 1$ durch b teilbar sein. Das ist offensichtlich genau dann der Fall, wenn x die Kongruenz $a \cdot x \equiv 1 \bmod b$ löst. Wie man das macht, haben wir gerade gelernt. Es gibt genau eine Lösung x modulo b, falls a und b teilerfremd sind. Das sieht man auch Gleichung (9) an. Ist nämlich $ggT(a, b) = r > 1$, dann ist die linke Seite von (9) durch r teilbar, die rechte aber nicht. Es sei x_0 die Lösung von $a \cdot x_0 \equiv 1 \bmod b$ und

$$y_0 = \frac{a \cdot x_0 - 1}{b}$$

dann gilt $a \cdot x_0 - b \cdot y_0 = 1$. Aber das ist nicht die einzige Lösung von Gleichung (9), denn wir haben nur Lösungen der Kongruenz $a \cdot x \equiv 1 \bmod b$ modulo b gesucht. Tatsächlich lösen alle Zahlen der Form $x = x_0 + b \cdot k$ diese Kongruenz und nur diese. Damit erhalten wir alle Lösungen von Gleichung (9) wegen

$$y = \frac{a \cdot x - 1}{b} = \frac{a \cdot (x_0 + b \cdot k) - 1}{b} = \frac{a \cdot x_0 - 1}{b} + \frac{a \cdot b \cdot k}{b} = y_0 + a \cdot k$$

in der Form

$$x = x_0 + b \cdot k \ , \quad y = y_0 + a \cdot k \ ,$$

wobei k eine beliebige ganze Zahl ist. Es gibt folglich unendlich viele Lösungen von Gleichung (9), die sich aus einer speziellen Lösung (x_0, y_0) und einer Verschiebung um $b \cdot k$ bzw. $a \cdot k$ zusammensetzen. Die Richtigkeit dieser Verschiebung läßt sich auch direkt aus der Gleichung ablesen. Ist (x_0, y_0) Lösung, daß heißt, gilt $a \cdot x_0 - b \cdot y_0 = 1$, dann folgt

$$a \cdot (x_0 + b \cdot k) - b \cdot (y_0 + a \cdot k) = a \cdot x_0 + a \cdot b \cdot k - b \cdot y_0 - b \cdot a \cdot k = a \cdot x_0 - b \cdot y_0 = 1 \ .$$

Aufgabe 5:
Löse die Diophantische Gleichung $9x - 7y = 1$*!*

9 und 7 sind teilerfremd, also hat die Kongruenz $9 \cdot x_0 \equiv 2 \cdot x_0 \equiv 1 \bmod 7$ genau eine Lösung. Sie läßt sich mit $x_0 = 4$ leicht erraten. Dann folgt

$$y_0 = \frac{9x_0 - 1}{7} = \frac{9 \cdot 4 - 1}{7} = \frac{35}{7} = 5 \ .$$

Die allgemeine Lösung ist somit

$$x = 4 + 7k \ , \quad y = 5 + 9k \ .$$

Wir wollen jetzt die allgemeinere Diophantische Gleichung

$$a \cdot x - b \cdot y = c \tag{10}$$

lösen. Sind a und b nicht teilerfremd, ist etwa $ggT(a, b) = r > 1$, so ist die linke Seite von (10) durch r teilbar. Eine Lösung ist nur möglich, wenn auch die rechte Seite durch r teilbar ist. Dann kann aber die ganze Gleichung durch r geteilt werden. Deshalb wird o.B.d.A. $ggT(a, b) = 1$ angenommen.
Die Lösung der Gleichung (10) folgt sofort aus der Lösung von (9): Ist (x_0, y_0) Lösung von (9), dann gilt $a \cdot x_0 - b \cdot y_0 = 1$ und nach Multiplikation dieser Gleichung mit c folgt $a \cdot (x_0 c) - b \cdot (y_0 c) = c$. Die allgemeine Lösung dieser Gleichung ist also

$$x = x_0 c + b \cdot k \ , \quad y = y_0 c + a \cdot k \ ,$$

wobei k eine beliebige ganze Zahl ist.
Auch die Lösung der Gleichung

$$a \cdot x + b \cdot y = 1 \tag{11}$$

folgt aus der von Gleichung (9). Ist (x_0, y_0) Lösung von (9), dann ist offensichtlich $(x_0, -y_0)$ Lösung von (11). Allgemein gilt: Lösung von Gleichung

$$a \cdot x + b \cdot y = c$$

ist

$$x = x_0 c + b \cdot k \ , \quad y = -y_0 c - a \cdot k \ ,$$

wobei (x_0, y_0) Lösung von Gleichung $a \cdot x_0 - b \cdot y_0 = 1$ ist.

1.2.3 Euklidischer Algorithmus

Der letzte Punkt hat gezeigt, daß für die Lösung einer allgemeinen Linearen Diophantischen Gleichungen die Lösung der Gleichung

$$a \cdot x - b \cdot y = 1 \tag{12}$$

oder der äquivalenten Kongruenz

$$a \cdot x \equiv 1 \bmod b \tag{13}$$

Ausgangspunkt ist. Hat man hierfür eine spezielle Lösung gefunden, läßt sich die allgemeine Lösung leicht bestimmen. Die Lösung von (12) oder (13) kann man für kleine a und b leicht erraten. Im allgemeinen ist das aber schwierig. Mit dem Euklidischen Algorithmus läßt sie sich aber auch in komplizierten Fällen mit wenig Aufwand finden. Dazu betrachten wir die

Aufgabe 6:
Löse die Diophantische Gleichung

$$263x - 128y = 1 \; ! \tag{14}$$

Da 263 und 128 teilerfremd sind, existiert eine Lösung dieser Aufgabe, die man aber nicht mehr schnell erraten kann.
Wir schreiben für die beiden Zahlen 263 und 128 den Euklidischen Algorithmus auf:

$$\begin{array}{rcrcrcl} 263 & = & 2 & \cdot & 128 & + & 7 \\ 128 & = & 18 & \cdot & 7 & + & 2 \\ 7 & = & 3 & \cdot & 2 & + & 1 \\ 2 & = & 2 & \cdot & 1 & + & 0 \end{array}$$

Die letzte Gleichung betrachten wir nicht mehr, aber aus der vorletzten folgt

$$7 - 3 \cdot 2 = 1 \; .$$

Hätten wir die Gleichung $7x - 2y = 1$ zu lösen, wären wir fertig. Wir setzen anstelle der 2 hier den nach 2 umgeformten Ausdruck aus der zweiten Gleichung $2 = 128 - 18 \cdot 7$ des Euklidischen Algorithmus ein:

$$\begin{array}{rcl} 7 - 3 \cdot (128 - 18 \cdot 7) & = & 1 \\ (1 + 3 \cdot 18)7 - 3 \cdot 128 & = & 1 \\ 55 \cdot 7 - 3 \cdot 128 & = & 1 \end{array}$$

Hätten wir die Gleichung $7x - 128y = 1$ zu lösen, wären wir fertig. Die 7 stört, wir ersetzen sie durch den nach 7 umgeformten Ausdruck aus der ersten Gleichung $7 = 263 - 2 \cdot 128$ des Euklidischen Algorithmus:

$$\begin{array}{rcl} 55 \cdot (263 - 2 \cdot 128) - 3 \cdot 128 & = & 1 \\ 55 \cdot 263 - (55 \cdot 2 + 3) \cdot 128 & = & 1 \\ 55 \cdot 263 - 113 \cdot 128 & = & 1 \; . \end{array}$$

Hieraus kann sofort die spezielle Lösung $x_0 = 55$ und $y_0 = 113$ abgelesen werden.
Im allgmeinen sieht der Euklidische Algorithmus zwischen den Zahlen b_0 und b_1 so aus:

$$\begin{array}{rcrcrcl} b_0 & = & a_1 & \cdot & b_1 & + & b_2 \\ b_1 & = & a_2 & \cdot & b_2 & + & b_3 \\ b_2 & = & a_3 & \cdot & b_3 & + & b_4 \\ \ldots & & & & & & \\ b_{k-2} & = & a_{k-1} & \cdot & b_{k-1} & + & b_k \\ b_{k-1} & = & a_k & \cdot & b_k & + & b_{k+1} \end{array}$$

b_{i+1} ist jeweils der Rest einer Zahl bei Division durch b_i. Deshalb ist $b_i < b_{i+1}$. Es gilt also

$$b_1 > b_2 > b_3 > ... > b_{k+1} \geq 0$$

Daher bricht der Euklidische Algorithmus nach endlich vielen Schritten ab. Wir nehmen an, daß das nach k Schritten der Fall ist, daß $b_{k+1} = 0$ ist. Dann ist

$$b_k = ggT(b_0, b_1) \ .$$

Im Falle, daß b_0 und b_1 teilerfremd sind, ist also $b_k = 1$ und die letzte (k-te) Zeile hat die Form

$$b_{k-1} = a_k \cdot 1 + 0 \ .$$

Besonders bequem wird der Euklidische Algorithmus durch seine Darstellung als

1.2.4 Kettenbrüche

Wir formen den Euklidischen Algorithmus für die beiden Zahlen 263 und 128 aus dem letzten Punkt um:

$$\begin{aligned}
\frac{263}{128} &= 2 + \frac{7}{128} \quad \Longrightarrow \quad \frac{263}{128} = 2 + \frac{1}{\frac{128}{7}} \\
\frac{128}{7} &= 18 + \frac{2}{7} \quad \Longrightarrow \quad \frac{128}{7} = 18 + \frac{1}{\frac{7}{2}} \\
\frac{7}{2} &= 3 + \frac{1}{2} \quad \Longrightarrow \quad \frac{7}{2} = 3 + \frac{1}{\frac{2}{1}} \\
\frac{2}{1} &= 2 + 0
\end{aligned}$$

Jetzt kann man die Gleichungen der Reihe nach ineinander einsetzen und erhält

$$\frac{263}{128} = 2 + \frac{1}{18 + \frac{1}{3 + \frac{1}{2}}}$$

einen Kettenbruch. Im allgemeinen Fall gilt

$$\frac{b_0}{b_1} = a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \ddots \frac{1}{a_{k-1} + \frac{1}{a_k}}}}$$

Zum Lösen der Gleichung (14) setzten wir die Zeilen im Euklidischen Algorithmus von unten nach oben – beginnend mit der vorletzten – ineinander ein. Diesem Vorgehen entspricht die Berechnung des Kettenbruchs ohne den letzten Eintrag:

$$2 + \frac{1}{18 + \frac{1}{3}} = 2 + \frac{1}{\frac{55}{3}} = 2 + \frac{3}{55} = \frac{113}{55}$$

Mit dieser Methode lösen wir

Aufgabe 7:
Löse die Diophantische Gleichung

$$71x - 41y = 1 \; ! \tag{15}$$

Die Zahl $\frac{71}{41}$ – entwickelt in einen Kettenbruch – ergibt

$$\frac{71}{41} = 1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \frac{1}{2}}}}}}$$

Die Berechnung diese Kettenbruchs – ohne den letzten Eintrag – ergibt

$$1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{2 + \frac{1}{1}}}}} = 1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{\frac{4}{3}}}} = 1 + \cfrac{1}{1 + \cfrac{1}{2 + \frac{3}{4}}} = 1 + \cfrac{1}{1 + \frac{4}{11}} = 1 + \frac{11}{15} = \frac{21}{15} \; .$$

Die spezielle Lösung von Gleichung (15) müßte $x = 15$ und $y = 26$ sein. In die Gleichung eingesetzt, ergibt das

$$71 \cdot 15 - 41 \cdot 26 = 1065 - 1066 = -1 \; .$$

Tatsächlich ist eine spezielle Lösung von Gleichung (15) also $x = -15$ und $y = -26$. Das hängt mit der Länge des Kettenbruchs zusammen. Es gilt folgender

Satz 10: *Es sei*

$$\frac{b_0}{b_1} = a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots \cfrac{1}{a_{k-1} + \frac{1}{a_k}}}} \qquad \textit{und} \qquad a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots \cfrac{1}{a_{k-1}}}} = \frac{y}{x} \; ,$$

dann gilt

$$b_0 \cdot x - b_1 \cdot y = \begin{cases} 1 & \textit{falls} \quad k \quad \textit{gerade} \\ -1 & \textit{falls} \quad k \quad \textit{ungerade} \end{cases}$$

oder – zusammengefaßt –

$$b_0 \cdot x - b_1 \cdot y = (-1)^k$$

1.2.5 Simultane Kongruenzen

Aufgabe 8:
Gesucht sind alle Zahlen x, die bei Division durch 5 und 7 jeweils den Rest 2 lassen, das heißt, alle Zahlen x, die die beiden Kongruenzen

$$\begin{aligned} x &\equiv 2 \bmod 5 \\ x &\equiv 2 \bmod 7 \end{aligned}$$

gleichzeitig (simultan) erfüllen.

Diese Aufgabe ist einfach, denn sie bedeutet, daß $x-2$ durch 5 und durch 7 teilbar sein soll. Also muß $x-2$ durch 35 teilbar sein. Alle Lösungen sind folglich $x = 35k+2$ oder $x \equiv 2 \bmod 35$. Die Aufgabe war einfach, weil der Rest bezüglich jedes Moduls gleich war. Allgemein gilt: Erfüllt x gleichzeitig die Kongruenzen

$$\begin{aligned} x &\equiv r \bmod m_1 \\ x &\equiv r \bmod m_2 \\ &... \\ x &\equiv r \bmod m_k \ , \end{aligned}$$

so ist die Lösung

$$x \equiv r \bmod kgV(m_1, m_2, ..., m_k) \ .$$

Schwieriger ist
Aufgabe 9:
Gesucht sind alle Zahlen x, die bei Division durch 5 den Rest 1 und bei Division durch 7 den Rest 2 lassen, das heißt, alle Zahlen x, die die beiden Kongruenzen

$$\begin{aligned} x &\equiv 1 \bmod 5 \\ x &\equiv 2 \bmod 7 \end{aligned}$$

simultan erfüllen.

Die beiden Kongruenzen bedeuten, daß es ganze Zahlen i und j gibt mit

$$\begin{aligned} x &= 5i + 1 \ , \\ x &= 7j + 2 \ . \end{aligned}$$

i und j müssen also die Gleichung

$$5i - 7j = 1$$

erfüllen. Die allgemeine Lösung dieser Gleichung ist

$$\begin{aligned} i &= 7k + 3 \\ j &= 5k + 2 \end{aligned}$$

und – in einen der beiden Ausdrücke für x eingesetzt – $x = 5i + 1 = 5(7k + 3) + 1 = 35k + 16$ oder $x \equiv 16 \bmod 35$.

Auf diese Weise können beliebig viele Kongruenzen simultan gelöst werden. Sind z.B. die drei Kongruenzen

$$\begin{aligned} x &\equiv 1 \bmod 5 \\ x &\equiv 2 \bmod 7 \\ x &\equiv 4 \bmod 11 \end{aligned}$$

zu lösen, dann betrachtet man als erstes zwei davon – z.B. die beiden ersten – deren Lösung wir eben gefunden haben, und setzt diese Lösung anstelle der beiden Kongruenzen. Man erhält

$$\begin{aligned} x &\equiv 16 \bmod 35 \\ x &\equiv 4 \bmod 11 \end{aligned}$$

eine Aufgabe mit zwei Kongruenzen. Man findet die Lösung, indem man schrittweise die Zahl der Kongruenzen reduziert. Im allgemeinen gilt folgender

Satz 11: *Es seien k Kongruenzen*

$$\begin{aligned} x &\equiv r_1 \bmod m_1 \\ x &\equiv r_2 \bmod m_2 \\ &... \\ x &\equiv r_k \bmod m_k \ , \end{aligned}$$

dann existiert genau eine Lösung

$$x \bmod kgV(m_1, m_2, ..., m_k) \ .$$

Dieser Satz wird auch chinesischer Restsatz genannt.