8.4 Der chinesische Restalgorithmus

Das chinesische Restproblem ist die Frage nach der Lösung simultaner Kongruenzen. Der einfachste erwähnenswerte Fall geht so:

Satz 5 (Chinesischer Restsatz) *Seien m und n teilerfremde natürliche Zahlen ≥ 1 und a, b beliebige ganze Zahlen. Dann gibt es genau eine ganze Zahl x, $0 \leq x < mn$, mit*

$$x \equiv a \pmod{m}, \; x \equiv b \pmod{n}.$$

Beweis. Die Eindeutigkeit folgt so: Ist auch y eine solche Zahl, so $y = x + km = x + ln$ mit ganzen Zahlen k und l, und $km = ln$. Da m und n teilerfremd sind, folgt $n|k$, $k = cn$,

$$y = x + cmn \equiv x \pmod{mn}.$$

Für den Existenzbeweis setzt man $x = a + tm$ an; dann ist $x \equiv a \pmod{m}$ erfüllt, und

$$x \equiv b \pmod{n} \Longleftrightarrow b - a \equiv x - a \equiv tm \pmod{n}.$$

Ein solches t existiert aber nach Satz 4. Die so gefundene Lösung x wird noch $\bmod(mn)$ reduziert. $\diamond$

Der Beweis ist konstruktiv und leicht in einen Algorithmus umzusetzen. Im allgemeinen Fall, für mehrfache Kongruenzen, lautet das chinesische Restproblem so:

- Gegeben sind q paarweise teilerfremde ganze Zahlen $n_1, \ldots, n_q \geq 1$ und q ganze Zahlen $a_1, \ldots, a_q$.
- Gesucht ist eine ganze Zahl x mit $x \equiv a_i \pmod{n_i}$ für $i = 1, \ldots q$.

Man kann Satz 5 entsprechend verallgemeinern. Interessanter ist aber eine abstrakte Formulierung, die auch die Interpolationsaufgabe für Polynome mit einschließt; auch in dieser allgemeinen Formulierung erkennt man Satz 5 samt Beweis leicht wieder, wenn man daran denkt, dass für ganze Zahlen m und n mit größtem gemeinsamen Teiler d gilt:

$$m, n \text{ teilerfremd} \Longleftrightarrow d = 1 \Longleftrightarrow \mathbb{Z}m + \mathbb{Z}n = \mathbb{Z}.$$

Satz 6 (Allgemeiner chinesischer Restsatz) *Sei R ein kommutativer Ring mit Einselement, $q \geq 1$, $\mathfrak{a}_1, \ldots, \mathfrak{a}_q \trianglelefteq R$ Ideale mit $\mathfrak{a}_i + \mathfrak{a}_j = R$ für $i \neq j$. Seien Elemente $a_1, \ldots, a_q \in R$ gegeben. Dann gibt es ein $x \in R$ mit $x - a_i \in \mathfrak{a}_i$ für $i = 1, \ldots, q$, und die Restklasse $x \bmod \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_q$ ist eindeutig bestimmt.*

Beweis. Die Eindeutigkeit ist auch hier einfach: Ist $x - a_i, y - a_i \in \mathfrak{a}_i$, so $x - y \in \mathfrak{a}_i$; gilt das für alle i, so $x - y \in \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_q$.

Die Existenz wird durch Induktion über q bewiesen. Im Fall $q = 1$ nimmt man $x = a_1$. Sei nun $q \geq 2$ und y mit $y - a_i \in \mathfrak{a}_i$ für $i = 1, \ldots, q-1$ schon gefunden. Idee: Zu y kann man ein $s \in \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_{q-1}$ addieren, ohne das bisher erreichte, nämlich die Lösung der ersten $q-1$ Kongruenzen, wieder aufzugeben. Benötigt wird dazu die Aussage: Zu jedem $r \in R$ gibt es ein $s \in \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_{q-1}$ mit $r - s \in \mathfrak{a}_q$, oder, anders ausgedrückt,

$$(\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_{q-1}) + \mathfrak{a}_q = R.$$

Zum Beweis dieser Zwischenbehauptung wählt man $c_i \in \mathfrak{a}_i$ für $i = 1, \ldots, q-1$ und $b_1, \ldots, b_{q-1} \in \mathfrak{a}_q$ mit $b_i + c_i = 1$. Dann ist

$$1 = (b_1 + c_1) \cdots (b_{q-1} + c_{q-1}) = c_1 \cdots c_{q-1} + b$$

mit $c_1 \cdots c_{q-1} \in \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_{q-1}$ und $b \in \mathfrak{a}_q$.

Nun wird zu $a_q - y \in R$ ein $s \in \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_{q-1}$ gewählt mit $a_q - y - s \in \mathfrak{a}_q$ und dann $x = y + s$ gesetzt. Dann ist $x \equiv y \equiv a_i \pmod{\mathfrak{a}_i}$ für $i = 1, \ldots, q-1$ und $x \equiv y + s \equiv a_q \pmod{\mathfrak{a}_q}$. $\diamond$

Bemerkungen und Beispiele

1. Ist $R = \mathbb{Z}$ oder sonst ein Hauptidealring und $\mathfrak{a}_i = Rn_i$, so ist $\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_q = R(n_1 \cdots n_q)$. Daraus erhält man die übliche Formulierung des chinesischen Restsatzes.

2. Ist R ein Hauptidealring, so ist läuft die Konstruktion der Lösung wie folgt: Ist $\mathfrak{a}_i = Rn_i$, so wird s in der Zwischenbehauptung so gewählt, dass $s = tn_1 \cdots n_{q-1}$ mit

   $$r - tn_1 \cdots n_{q-1} \in Rn_q$$

   (Kongruenzdivision mod n_q). Ein expliziter Algorithmus für das chinesische Restproblem existiert also, wenn einer für die Kongruenzdivision existiert, auf jeden Fall also für $R = \mathbb{Z}$.

3. Im Fall $R = \mathbb{Z}$ berechnet man iterativ

   $$\begin{aligned} x_1 = a_1 \bmod n_1, &\qquad s_1 = n_1, \\ t_i \text{ mit } 0 \leq t_i \leq n_i - 1 &\quad \text{und } a_i - x_{i-1} - t_i s_{i-1} \in Rn_i, \\ x_i = x_{i-1} + t_i s_{i-1}, &\qquad s_i = s_{i-1} n_i. \end{aligned}$$

   Insbesondere ist $s_k = n_1 \cdots n_k$. Durch Induktion beweist man sofort $0 \leq x_i \leq s_i - 1$ für alle i. Am Ende erhält man die Lösung $x = x_q$. Die

eben durchgeführte Überlegung garantiert, dass kein Zwischenergebnis einen Überlauf erzeugt. Der Aufwand besteht im wesentlichen aus $q-1$ Kongruenzdivisionen und $2\cdot(q-1)$ gewöhnlichen Ganzzahlmultiplikationen. Der Gesamtaufwand ist also ungefähr $cq\times$ dem Aufwand für eine Langzahl-Multiplikation mit einer kleinen Konstanten c.

4. Die allgemeine Gestalt der Lösungsformel ist

$$x = x_1 + t_1 n_1 + \cdots + t_{q-1} n_1 \cdots n_{q-1}.$$

5. Als Beispiel wird die Aufgabe von Sun-Tsu aus dem 1. Jahrhundert behandelt, die in unserer Schreibweise so heißt: Finde x mit

$$x \equiv 2 \pmod 3,\ x \equiv 3 \pmod 5,\ x \equiv 2 \pmod 7.$$

   Der Algorithmus liefert der Reihe nach:

$$\begin{aligned} x_1 = 2, &\quad s_1 = 3, \\ 1 - 3t_2 \in 5\mathbb{Z}, &\quad t_2 = 2, \\ x_2 = 2 + 2\cdot 3 = 8, &\quad s_2 = 15, \\ -6 - 15t_3 \in 7\mathbb{Z}, &\quad t_3 = 1, \\ x = x_3 = 8 + 1\cdot 15 = 23. & \end{aligned}$$

6. Für den Polynomring $K[T]$ über einem Körper K erhält man die Lösung des Interpolationsproblems. Der Algorithmus ist dabei gerade das Interpolationsverfahren von Newton.