Der Chinesische Restsatz

Wir formulieren den Chinesischen Restsatz als Struktursatz über Restklassenringe der Form $\mathbb{Z}/n\mathbb{Z}$:

Satz: Für teilerfremde Zahlen m, n ist die Abbildung

$$\begin{aligned} \mathbb{Z}/mn\mathbb{Z} &\to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ x + mn\mathbb{Z} &\mapsto (x + m\mathbb{Z}, x + n\mathbb{Z}) \end{aligned}$$

ein Isomorphismus von Ringen.

Beweis: Die Homomorphie-Eigenschaften bzgl. Addition und Multiplikation sind leicht zu überprüfen.

Die Bijektivität der Abbildung wurde im Lemma bewiesen.

Gleichzeitige Kongruenzen

Die Standardanwendung des Chinesischen Restsatzes:

Gegeben seien paarweise teilerfremde Zahlen $m_1, \ldots, m_n$.
Das Produkt dieser n Zahlen sei m.
Für jedes n-Tupel ganzer Zahlen $x_1, \ldots, x_n$ existiert genau ein $x \in \{0, \ldots, m-1\}$, für das die Kongruenzen

$$x \equiv x_i \mod m_i$$

für alle i erfüllt sind.

Wie findet man die Lösung?

Suche y mit $y \equiv x_n \mod m_n$ und $y \equiv x_{n-1} \mod m_{n-1}$.
Nun die letzten zwei Kongruenzen durch $x \equiv y \mod m_{n-1}m_n$ ersetzen.
Sukzessive so weitermachen. Lösung sei x.

Wie sieht die Lösungsmenge in $\mathbb{Z}$ aus?

Antwort: $x + m\mathbb{Z}$

Verallgemeinerung und Folgerung

Den Chin. Restsatz kann man auf n Komponenten erweitern:

Korollar: Für paarweise teilerfremde Zahlen $m_1, \ldots, m_n$ mit $m = m_1 \cdot \cdots \cdot m_n$ ist die Abbildung

$$\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_n\mathbb{Z}$$
$$x + m\mathbb{Z} \mapsto (x + m_1\mathbb{Z}, \ldots, x + m_n\mathbb{Z})$$

ein Isomorphismus von Ringen.

Als Anwendung zeigen wir, dass es unendlich viele Primzahlen gibt.

Denn angenommen, es gäbe nur endlich viele. Dann könnte man mit dem Chinesischen Restsatz eine Zahl finden, für die $n \equiv p - 1 \bmod p$ für alle Primzahlen p erfüllt ist. Die Zahl n wäre größer als 1, würde aber von keiner Primzahl geteilt. Das widerspricht dem Satz von der Existenz einer eindeutig bestimmten Primfaktorzerlegung.

Der kleine Satz von Fermat

Der kleine Satz von Fermat bildet die Grundlage für viele Primzahltests, und darüberhinaus wird er in Beweisen oft als nützlicher Baustein verwendet:

Satz: Für alle Primzahlen p und alle $a \in \mathbb{Z}$ gilt:

$$a^p \equiv a \mod p$$

Falls a und p teilerfremd sind, gilt sogar:

$$a^{p-1} \equiv 1 \mod p$$

Bevor wir den Beweis geben, prüfen wir die Aussage am Beispiel $a = 6$ und $p = 13$:

$$6^{13-1} = 6^{12} = (6^3)^4 = 216^4 \equiv (221-5)^4 = (13 \cdot 17 - 5)^4 \equiv (-5)^4 \equiv 8^4 = 64^2 = (5 \cdot 13 - 1)^2 \equiv (-1)^2 = 1 \mod 13$$

Beweis des Satzes

Wenn p ein Teiler von a ist, ist die erste Aussage trivial, und die zweite ist für diesen Fall irrelevant, da $ggT(a, p) = p > 1$ gilt.

Von jetzt an können wir also $ggT(a, p) = 1$ voraussetzen.
Dann ist nach Teil c) des Satzes von Folie 26.3 die Abbildung $x \mapsto ax$ zunächst auf $\mathbb{Z}/p\mathbb{Z}$ bijektiv. Aber daraus folgt sofort, dass diese Abbildung auch auf $(\mathbb{Z}/p\mathbb{Z})^*$ bijektiv ist.

Also gilt

$$(p-1)! \equiv \prod_i i \equiv \prod_i ai \equiv a^{p-1} \cdot \prod_i i \equiv a^{p-1}(p-1)!$$

wobei das Produkt jeweils über alle $i \in (\mathbb{Z}/p\mathbb{Z})^*$ geht.
Da $(p-1)!$ invertierbar ist, können wir die Gleichung durch diesen Wert teilen und erhalten $a^{p-1} \equiv 1$, sowie $a^p \equiv a$.

Primzahltest nach Fermat

Die folgende Prozedur nennt man den *Fermat-Test:*

Eingabe sei die natürliche Zahl n.

Frage: Ist n eine Primzahl?

Wähle $a \in \{1, \ldots, n-1\}$ zufällig.

Berechne $x := a^{n-1} \bmod n$

Falls $x \not\equiv 1 \bmod n$:

AUSGABE: n ist keine Primzahl.

Sonst keine Aussage.