8.3 Kongruenzdivision

Der erweiterte Euklidische Algorithmus liefert nun eine Lösung des nicht ganz trivialen Problems, im Ring $\mathbb{Z}/n\mathbb{Z}$ der ganzen Zahlen $\bmod n$ effizient zu dividieren.

Satz 4 *Gegeben seien $n \in \mathbb{N}, n \geq 2$, und $a, b \in \mathbb{Z}$ mit $\mathrm{ggT}(b, n) = d$. Genau dann ist a in $\mathbb{Z}/n\mathbb{Z}$ durch b teilbar, wenn $d|a$. Ist dies der Fall, so gibt es genau d Lösungen z von $zb \equiv a \pmod{n}$ mit $0 \leq z < n$, und je zwei solche unterscheiden sich um ein Vielfaches von n/d. Ist $d = xn + yb$ und $a = td$, so ist $z = yt$ Lösung.*

Beweis. Ist a durch b teilbar, $a \equiv bz \pmod{n}$, so $a = bz + kn$, also $d|a$. Ungekehrt sei $a = td$. Nach Satz 1 findet man x, y mit $nx + by = d$; also ist $nxt+byt = a$ und $byt \equiv a \pmod{n}$. Ist auch $a \equiv bw \pmod{n}$, so $b(z-w) \equiv 0 \pmod{n}$, also $z - w$ Vielfaches von n/d. $\diamond$

Ein expliziter Algorithmus für die Division ist dem Beweis von Satz 4 direkt zu entnehmen. Wichtig – und wesentlich einfacher zu formulieren – ist der Spezialfall $d = 1$:

Korollar 1 *Ist b zu n teilerfremd, so ist jedes a in $\mathbb{Z}/n\mathbb{Z}$ eindeutig durch b teilbar.*

Die Berechnung des Inversen y zu b folgt dann, da $d = 1$, sofort aus der Formel $1 = nx + by$; es ist nämlich $by \equiv 1 \pmod{n}$.

Korollar 2 $(\mathbb{Z}/n\mathbb{Z})^\times = \{b \bmod n \mid \mathrm{ggT}(b, n) = 1\}$.

Die invertierbaren Elemente im Ring $\mathbb{Z}/n\mathbb{Z}$ sind also genau die Restklassen der zu n teilerfremden ganzen Zahlen. Der wichtigste Fall ist: $n = p$ Primzahl. Dann gilt

Korollar 3 *$\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ ist ein Körper.*

Beweis. Ist $b \in \mathbb{F}_p, b \neq 0$, so gibt es genau ein $c \in \mathbb{F}_p$ mit $bc = 1$. $\diamond$

Korollar 4 (Kleiner Satz von Fermat) *$a^p \equiv a \pmod{p}$ für alle $a \in \mathbb{Z}$.*

Beweis. Die Elemente $\neq 0$ von $\mathbb{F}_p$ bilden die multiplikative Gruppe $\mathbb{F}_p^\times$. Da die Ordnung eines Elements stets Teiler der Gruppenordnung ist, gilt $a^{p-1} \equiv 1 \pmod{p}$ wenn a zu p teilerfremd ist. Andernfalls gilt $p|a$, also $a \equiv 0 \equiv a^p \pmod{p}$. $\diamond$