Rechnen modulo n

1 Definition

$a \pmod n := a - \left\lfloor \frac{a}{n} \right\rfloor n \quad a \in \mathbb{Z}, n \in \mathbb{N}^+$

$a \equiv b \pmod n \;\leftrightarrow\; a \pmod n = b \pmod n$

$\mathbb{Z}_n := \{0, 1, \ldots, n-1\}$

$\underline{\mathbb{Z}_n} := (\mathbb{Z}_n, +, -, \cdot)$ (Restklassenring der ganzen Zahlen modulo n)

2 Sätze

Satz: $(\forall\, j \in \mathbb{N})(\exists\, k \in \mathbb{Z}_n)\;\; \mathrm{ggT}(j, n) = 1 \;\wedge\; j \cdot k = 1 \pmod n$

Man findet zu j und n das entsprechende k mit Hilfe des EUKLIDischen Algorithmus.

Satz: Die Abbildung $\mathbb{Z} \to \mathbb{Z}_n$ ist ein Ringhomomorphismus. Es gilt:

$$(a \circ b) \pmod n = \big(a \pmod n\big) \circ \big(b \pmod n\big) \quad \circ \in \{+, -, \cdot\}$$

Satz: Jeder endliche Körper ist **polynomvollständig**, d. h., jede Abbildung $f : GF(q)^n \to GF(q)$ kann durch ein Polynom aus $GF(q)[x_{n-1}, \ldots, x_1, x_0]$ dargestellt werden.

2.1 Chinesischer Restsatz

Formulierung 1: Sind $n_1, \ldots, n_s$ paarweise teilerfremde ganze Zahlen größer 1, und sind $r_1, \ldots, r_s$ ganze Zahlen mit $0 \le r_i < n_i \;\forall i \in \{1, \ldots, s\}$, dann hat das System linearer Kongruenzen

$$x \equiv r_1 \pmod{n_1} \quad \ldots \quad x \equiv r_s \pmod{n_s}$$

genau eine Lösung in $\mathbb{Z}_{n_1 \cdot n_2 \cdots n_s - 1}$.

Formulierung 2: Sind $n_1, \ldots, n_s$ paarweise teilerfremde ganze Zahlen größer 1, dann ist die Abbildung

$$f : \mathbb{Z}_{n_1 \cdot n_2 \cdots n_s} \to \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \ldots \times \mathbb{Z}_{n_s} \quad \text{mit} \quad f(z) = \big(z \pmod{n_1}, \ldots, z \pmod{n_s}\big)$$

ein Ringisomorphismus.

Bestimmung von $z = f^{-1}(z_1, \ldots, z_s)$: $n := n_1 \cdot n_2 \cdots n_s$; y_i sei diejenige Zahl aus $\in \mathbb{Z}_{n_i}$ mit $\frac{n}{n_i} y_i \equiv 1 \pmod n$. Dann gilt:

$$z = \sum_{i=1}^{s} \frac{n}{n_i} y_i z_i$$

3 Polynomauswertung und –interpolation im $GF(2)$

Das Wertetupel eines Polynoms aus $GF(2)[x_{n-1}, \ldots, x_0]$ erhält man, indem man das Koeffiziententupel mit der Matrix A_n (VANDERMONDE–Matrix dieser Abbildung) multipliziert.

$$A_0 = (1) \quad A_{n+1} = \begin{pmatrix} A_n & 0 \\ A_n & A_n \end{pmatrix} \qquad A_n^{-1} = A_n$$