Algebra für Informationssystemtechniker

Prof. Dr. Ulrike Baumann

Fachrichtung Mathematik

Institut für Algebra

www.math.tu-dresden.de/∼baumann

Ulrike.Baumann@tu-dresden.de

10.1.2018

6. Vorlesung

Restklassenringe (2)

- Reste modulo n
- Rechnen modulo n – Homomorphieregeln
- Schnelles Potenzieren modulo n
  - Square & Multiply
  - Satz von Euler-Fermat
- Diffie-Hellman-Schlüsselaustausch

modulo n

- Sei $n \in \mathbb{N}$, $n > 1$ und $z \in \mathbb{Z}$.
  Mit z mod n wird diejenige Zahl in $\mathbb{Z}_n := \{0, 1, \ldots, n-1\}$ bezeichnet, um die z größer ist als eine durch n teilbare Zahl.

- $z \text{ mod } n := z - \lfloor \frac{z}{n} \rfloor \cdot n$ mit $\lfloor \frac{z}{n} \rfloor = max\{k \in \mathbb{Z} \mid k \leq \frac{z}{n}\}$

- $a \text{ mod } n = r \iff r$ ist der Rest von a bei Division durch n.

- Statt $a \text{ mod } n = r$ schreibt man auch $a \equiv r \pmod{n}$.
  (a ist kongruent zu r modulo n)

- $a \equiv b \pmod{n} \iff n | a - b$

  $\iff$ a und b lassen bei Division durch n den gleichen Rest.

Homomorphieregeln

- Homomorphieregeln:

$$\begin{aligned}(a+b) \bmod n &= (a \bmod n + b \bmod n) \bmod n \\ (a-b) \bmod n &= (a \bmod n - b \bmod n) \bmod n \\ (a \cdot b) \bmod n &= (a \bmod n \cdot b \bmod n) \bmod n\end{aligned}$$

- Man darf daher alle Zwischenergebnisse modulo n berechnen.

Square and Multiply

- effizientes Berechnungsverfahren für a^b mod n, das auf der Homomorphieregel beruht
- Beispiel: Zur Berechnung von 3^{201} mod 11 formt man wie folgt um:

$$\begin{aligned} 3^{201} &\equiv 3^{2^7} \cdot 3^{2^6} \cdot 3^{2^3} \cdot 3^{2^0} \\ &\equiv 3^{2\cdot2\cdot2\cdot2\cdot2\cdot2\cdot2} \cdot 3^{2\cdot2\cdot2\cdot2\cdot2\cdot2} \cdot 3^{2\cdot2\cdot2} \cdot 3 \\ &\equiv ((3^2 \cdot 3)^{2\cdot2\cdot2} \cdot 3)^{2\cdot2\cdot2} \cdot 3 \pmod{11} \end{aligned}$$

Satz von Euler-Fermat

- Satz: (von Euler)
  Sei $n \in \mathbb{N}$, $n > 1$, $a \in \mathbb{Z}$, $\text{ggT}(a, n) = 1$. Dann gilt:

$$a^{\varphi(n)} \bmod n = 1$$

- $\text{ggT}(a, n) = 1 \quad \Rightarrow \quad a^b \bmod n = a^{b \bmod \varphi(n)} \bmod n$

- Sonderfall: (Satz von Fermat)
  Sei p eine Primzahl, $a \in \mathbb{Z}$, $\text{ggT}(a, p) = 1$. Dann gilt:

$$a^{p-1} \bmod p = 1$$

Diffie-Hellman-Schlüsselaustausch

- Gegeben: große Zahl $n \in \mathbb{N}$, Basis $c \in \mathbb{N}$ (z.B. c=2)
- A erzeugt einen Exponenten a,
  berechnet $\alpha := 2^a \bmod n$ und sendet α an B.
- B erzeugt einen Exponenten b,
  berechnet $\beta := 2^b \bmod n$ und sendet β an B.
- A berechnet $\beta^a \bmod n = 2^{b \cdot a} \bmod n$.
- B berechnet $\alpha^b \bmod n = 2^{a \cdot b} \bmod n$.
- $K := \alpha^b \bmod n = \beta^a \bmod n$ ist der gemeinsame Schlüssel von A und B.