

6. Vorlesung

- Reste modulo n
- Rechnen modulo n – Homomorphieregeln
- Schnelles Potenzieren modulo n – Square & Multiply
Anwendung: Diffie-Hellman-Schlüsselaustausch
- Kann man modulo n dividieren?
 - Multiplikative Inverse modulo n
 - Berechnung der multiplikativen Inversen
mit dem erweiterten EUKLIDischen Algorithmus

modulo n

- Sei $n \in \mathbb{N}$, $n > 1$ und $z \in \mathbb{Z}$.
Mit $z \bmod n$ wird diejenige Zahl in $\mathbb{Z}_n := \{0, 1, \dots, n-1\}$ bezeichnet,
um die z größer ist als eine durch n teilbare Zahl.
- $z \bmod n := z - \lfloor \frac{z}{n} \rfloor \cdot n$ mit $\lfloor \frac{z}{n} \rfloor = \max\{k \in \mathbb{Z} \mid k \leq \frac{z}{n}\}$
- $a \bmod n = r \iff r$ ist der Rest von a bei Division durch n .
- Statt $a \bmod n = r$ schreibt man auch $a \equiv r \pmod{n}$.
(a ist kongruent zu r modulo n)
- $a \equiv b \pmod{n} \iff n \mid a - b$
 $\iff a$ und b lassen bei Division durch n den gleichen Rest.

Homomorphieregeln

- Homomorphieregeln:

$$(a + b) \bmod n = (a \bmod n + b \bmod n) \bmod n$$

$$(a - b) \bmod n = (a \bmod n - b \bmod n) \bmod n$$

$$(a \cdot b) \bmod n = (a \bmod n \cdot b \bmod n) \bmod n$$

- Man darf also auch alle Zwischenergebnisse modulo n berechnen.

Square and Multiply

- effizientes Berechnungsverfahren für $a^b \bmod n$, das auf der Homomorphieregel beruht
-

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

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.

Multiplikative Inverse modulo n

- Definition:

Sei $a \in \mathbb{Z}_n$.

$a^{-1} \in \mathbb{Z}_n$ heißt multiplikatives Inverses von a modulo n ,
wenn $a \cdot a^{-1} \equiv \overline{a^{-1} \cdot a} \equiv 1 \pmod{n}$ gilt.

- Satz:

$a \in \mathbb{Z}_n$ hat ein multiplikatives Inverses modulo n

$$\iff \text{ggT}(a, n) = 1$$

Berechnung des multiplikativen Inversen

Sei $a \in \mathbb{Z}_n$ und $\text{ggT}(a, n) = 1$.

- ① $\text{ggT}(a, n)$ mit dem euklidischen Algorithmus berechnen (Man erhält $\text{ggT}(a, n) = 1$.)
- ② 1 mit Hilfe des erweiterten euklidischen Algorithmus als Linearkombination von a und n darstellen:

$$1 = \text{ggT}(a, n) = \alpha \cdot a + \beta \cdot n$$

- ③ $\alpha \bmod n$ ist das multiplikative Inverse von a in modulo n :

$$a^{-1} = \alpha \bmod n$$