# 6. Vorlesung

- Reste modulo $n$
- Rechnen modulo $n$ – Homomorphieregeln
- Schnelles Potenzieren modulo $n$ – Square & Multiply
- Anwendungen
  - Diffie-Hellman-Schlüsselaustausch
  - Erzeugen von Pseudozufallszahlen

# 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.

- $z \bmod n := z - \lfloor \frac{z}{n} \rfloor \cdot n$ 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 $n$)

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

  $\iff$ $a$ 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 also auch alle Zwischenergebnisse modulo $n$ berechnen.

# Square and Multiply

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

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

# 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 $\alpha$ an B.
- B erzeugt einen Exponenten $b$,
  berechnet $\beta := 2^b \bmod n$ und sendet $\beta$ 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.

# Beispiel: Erzeugen von Pseudozufallszahlen

- $n \in \mathbb{N}$, $n > 1$

  $a, b, x_0 \in \mathbb{Z}_n$

  Rekursion: $x_{i+1} := ax_i + b \bmod n$

- Es entsteht eine Folge $x_0, x_1, x_2, \ldots$ von Zahlen (Pseudozufallszahlen)
  mit

$$x_k = a^k x_0 + (a^{k-1} + \cdots + a + 1) \cdot b \bmod n$$

- Die maximale Periodenlänge $n$ tritt genau dann auf, wenn
  (1) $\mathrm{ggT}(b, n) = 1$
  (2) $a \bmod p = 1$ für jeden Primteiler $p$ von $n$
  (3) $a \bmod 4 = 1$, falls $4|n$

  erfüllt sind.