7. Vorlesung

- Kann man modulo *n* dividieren?
  - Multiplikative Inverse modulo *n*
  - Berechnung der multiplikativen Inversen mit dem erweiterten EUKLIDischen Algorithmus
- Eulersche φ-Funktion
  - Satz von Fermat
  - Satz von Euler
  - Anwendung zum schnellen Potenzieren modulo *n*

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 $a \cdot a^{-1} \equiv a^{-1} \cdot a \equiv 1 \pmod{n}$ gilt.

- Satz:

  $a \in \mathbb{Z}_n$ hat ein multiplikatives Inverses modulo n
  $\iff \mathrm{ggT}(a, n) = 1$

Berechnung des multiplikativen Inversen

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

1. ggT(a, n) mit dem euklidischen Algorithmus berechnen (Man erhält ggT$(a, n) = 1$.)

2. 1 mit Hilfe des erweiterten euklidischen Algorithmus als Linearkombination von a und n darstellen:

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

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

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

$\textsc{Euler}$sche φ-Funktion

- Sei $n \in \mathbb{N} \setminus \{0\}$.
  Die Anzahl der zu n teilerfremden Zahlen in $\{0, 1, \ldots, n-1\}$ wird
  mit $\varphi(n)$ bezeichnet.
  Man nennt die Funktion $n \mapsto \varphi(n)$ die ($\textsc{Euler}$sche) φ-Funktion.

- Hat die natürliche Zahl n die Darstellung
  $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$,
  dann gilt:

$$\varphi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right)$$

Satz von Euler

- Satz: (von Euler)

  Sei $n \in \mathbb{N}$, $n > 1$, $a \in \mathbb{Z}$, $\mathrm{ggT}(a, n) = 1$. Dann gilt:

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

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

- Sonderfall: (Satz von Fermat)

  Sei p eine Primzahl, $a \in \mathbb{Z}$, $\mathrm{ggT}(a, p) = 1$. Dann gilt:

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