

8. Vorlesung

- Restklassenringe modulo n
 - Rechenregeln
 - Einheiten

- Anwendung: RSA-Kryptosystem
 - Idee für ein asymmetrisches Kryptosystem
 - Verschlüsselung / Entschlüsselung

Restklassenringe modulo n

- Definition:

Sei $n \in \mathbb{N}$, $n > 0$, $\mathbb{Z}_n := \{0, 1, \dots, n-1\}$.

$\underline{\mathbb{Z}}_n := (\mathbb{Z}_n; +_{\text{mod } n}, -_{\text{mod } n}, \cdot_{\text{mod } n}; 0, 1)$

heißt Restklassenring modulo n .

- $(\mathbb{Z}_n; +_{\text{mod } n}, -_{\text{mod } n}; 0)$ ist eine abelsche Gruppe.
- $(\underline{\mathbb{Z}}_n; +_{\text{mod } n}, -_{\text{mod } n}, \cdot_{\text{mod } n}; 0, 1)$ ist ein kommutativer Ring mit Eins.

Rechenregeln in Restklassenringen (1)

Die Addition ist

- assoziativ:

es gilt $(a + b) + c = a + (b + c)$ für alle a, b, c

- kommutativ:

es gilt $a + b = b + a$ für alle a, b

- hat 0 als neutrales Element:

es gilt $0 + a = a + 0$ für alle a

- hat inverse Elemente:

zu jedem a ist $-a := 0 - a$ ein Element mit

$$a + (-a) = (-a) + a = 0$$

Rechenregeln in Restklassenringen (2)

Die Multiplikation ist

- assoziativ:
es gilt $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ für alle a, b, c
- kommutativ:
es gilt $a \cdot b = b \cdot a$ für alle a, b
- hat 1 als neutrales Element:
es gilt $1 \cdot a = a \cdot 1$ für alle a
- ist über der Addition distributiv:
es gilt $a \cdot (b + c) = a \cdot b + a \cdot c$ für alle a, b, c

Einheiten in Restklassenringen

- Definition:

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

$a^{-1} \in \mathbb{Z}_n$ heißt multiplikatives Inverses von a in \mathbb{Z}_n ,
wenn $a \cdot a^{-1} = a^{-1} \cdot a = 1$ gilt.

- Definition:

$a \in \mathbb{Z}_n$ heißt Einheit im Restklassenring \mathbb{Z}_n ,
wenn a ein multiplikatives Inverses besitzt.

- Satz:

$a \in \mathbb{Z}_n$ ist Einheit im Restklassenring $\mathbb{Z}_n \iff \text{ggT}(a, n) = 1$

RSA-Kryptosystem

Sei $n = pq$ (p, q ungerade Primzahlen, $p \neq q$).

$$\mathbb{M} = \mathbb{C} = \mathbb{Z}_n$$

$$\mathbb{K} = \{ (n, p, q, e, d) \mid ed \equiv 1 \pmod{\varphi(n)} \}$$

Für $k = (n, p, q, e, d) \in \mathbb{K}$ sei

$$E_k(m) = m^e \quad \text{und} \quad D_k(c) = c^d$$

für alle $m, c \in \mathbb{Z}_n$.

Die Werte n, e bilden den **öffentlichen Schlüssel**,
die Werte p, q, d bilden den **geheimen Schlüssel**
des Empfängers der Nachricht.