

LA1-Vorlesung 16.11.2009

In Zukunft: Meistens $K = \mathbb{R}, \mathbb{C}, \mathbb{F}_p$

Definition:

Eine Menge A mit Verknüpfungen $+$ und \cdot heißt Ring, wenn gilt:

(a) $(A, +)$ ist abelsche Gruppe

(b) (A, \cdot) ist Halbgruppe

(c) Distributivgesetze gelten:
$$\left. \begin{aligned} x(y+z) &= xy+xz \\ (x+y)z &= xz+yz \end{aligned} \right\} \forall x, y, z \in A.$$

Falls \cdot kommutativ ist, spricht man von einem kommutativen Ring. Falls ein Neutralelement 1 bezgl. \cdot existiert, spricht man von einem Ring mit 1 .

Eine Abb. $f: A \rightarrow B$ zweier Ringe $(A, +, \cdot)$ und $(B, +', \cdot')$ heißt (Ring-) Homomorphismus, wenn $f(x+y) = f(x) + f(y)$ und $f(x \cdot y) = f(x) \cdot f(y) \forall x, y \in A$ gilt.

Besitzen beide Ringe ein Neutralelement 1 bzw. $1'$, so fordert man zusätzlich, dass $f(1) = 1'$ gilt.

Beispiele:

(1) Jeder Körper K ist ein kommutativer Ring mit 1 .

(2) $(\mathbb{K}[A], \Delta, \cap)$ ist ein kommutativer Ring mit 1 .

(3) $\mathbb{Z}_m = \{ [0]_m, [1]_m, \dots, [m-1]_m \}$ ist ein kommutativer Ring mit 1 für $m \in \mathbb{N}$. Spezialfall: $\mathbb{Z}_1 = \{ [0]_1 \}$
 $[0]_m$ ist auch Einselement von \cdot . Ab jetzt: $m \geq 2$.

Neue Schreibweise: $\mathbb{Z}_m = \{ 0, 1, 2, \dots, m-1 \}$

Statt $x \sim y$ schreiben wir $x \equiv y \pmod{m}$.

Beispiel: Welche $x \in \mathbb{Z}$ erfüllen $4x = 3 \pmod{7}$?

\mathbb{Z}_7 ist Körper $\Rightarrow 4^{-1}$ ex. in \mathbb{Z}_7 und $4^{-1} = 2$ in \mathbb{Z}_7 .

Mit anderen Worten: $4^{-1} \equiv 2 \pmod{7} \Rightarrow 4^{-1} \cdot 4 \cdot x = 2 \cdot 3 \pmod{7}$,
 $\Rightarrow x \equiv 6 \pmod{7} \Rightarrow x = 7y + 6, y \in \mathbb{Z}$.

Wie sieht das bei $4x \equiv 3 \pmod{6}$ aus?

Hier ist diese Gleichung nicht lösbar.

Satz 22:

Sei $m \geq 2$ und $m \in \mathbb{N}$. Dann bezeichnen wir mit

$\varphi(m)$ die Anzahl der zu m teilerfremden Zahlen aus $\{1, 2, \dots, m-1\}$ (φ Euler'sche φ -Funktion).

Seien $x_1, \dots, x_{\varphi(m)} \in \{1, 2, \dots, m-1\}$ die zu m teilerfremden Zahlen in \mathbb{Z}_m . Dann ist $B = \{x_1, \dots, x_{\varphi(m)}\}$ bezüglich \cdot eine abelsche Gruppe.

Es gilt:

Seien $x, m \in \mathbb{N}$, dann gilt x, m teilerfremd $\Leftrightarrow \exists r, s \in \mathbb{Z}$ mit $x \cdot r + m \cdot s = 1$
(r, s findet man mit dem Euklidischen Algorithmus).

Beweis (zu Satz 22):

Seien $x, y \in B \Rightarrow x, y$ teilerfremd zu m

$\Rightarrow \overset{\text{in } \mathbb{Z}}{x \cdot y}$ teilerfremd zu m . Sei z der Rest von $x \cdot y \pmod{m} \Rightarrow z = x \cdot y \pmod{m} \overset{\text{zt. fr.}}{\Rightarrow} z \in B$.

Ist $x \in B$, so ~~ex.~~ ex. $r, s \in \mathbb{Z}$ mit $x \cdot r + m \cdot s = 1$ (in \mathbb{Z})

$\Rightarrow \overset{\text{in } \mathbb{Z}}{x \cdot r} = 1 \pmod{m} \Rightarrow \overset{\text{in } \mathbb{Z}_m}{x \cdot r} = 1 \Rightarrow r$ ist das Inverse v. x .

Wegen $1 \in B$ folgt somit die Behauptung.

Korollar 23: (Fermat-Euler)

Seien $a, m \in \mathbb{N}$ teilerfremd $\Rightarrow a^{\varphi(m)} = 1 \pmod{m}$

Beweis:

Nach Satz 22 sind $\bar{a} \cdot x_1, \bar{a} \cdot x_2, \dots, \bar{a} \cdot x_{\varphi(m)}$, \forall

$\bar{a} \in \{1, \dots, m-1\}$, $\bar{a} = a \pmod{m}$, alle verschieden. $\in \mathbb{B}$

$$\Rightarrow \underbrace{\bar{a} x_1 \cdot \dots \cdot \bar{a} x_{\varphi(m)}}_{\equiv x_1 \cdot \dots \cdot x_{\varphi(m)}} \equiv a \cdot \dots \cdot a \cdot x_1 \cdot \dots \cdot x_{\varphi(m)} = a^{\varphi(m)} \cdot \underbrace{x_1 \cdot \dots \cdot x_{\varphi(m)}}_{\equiv 1 \pmod{m}}$$

$$\Rightarrow a^{\varphi(m)} = 1 \pmod{m}$$

Beispiel:

Welchen Rest lässt 4^{10259} bei Division durch 15?

$\text{ggT}(4, 15) = 1$ (also 4, 15 teilerfremd) \Rightarrow Korollar ist anwendbar.

$$\varphi(15) = 8$$

$$\Rightarrow 4^{10259} = (4^8)^{1282} \cdot 4^3$$

$$\stackrel{\text{kor. 23}}{\equiv} 4^3$$

$$\equiv 16 \cdot 4$$

$$\equiv 4 \pmod{15}$$

Formel: Wenn m die Primteiler p_1, \dots, p_k

hat, dann $\varphi(m) = m \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_k}\right)$.

Wenn $m = p_1 \cdot p_2 \Rightarrow \varphi(m) = m - p_1 - p_2 + 1$

Kryptographie:

Teilnehmer T_1, T_2
(z.B. Kunde, Bank)

T_1 $\xrightarrow{\text{verschl. Nachricht}}$ T_2

Schlüssel
(öffentlich)

(n_1, σ_1)

(n_2, σ_2)

Schlüssel
(geheim)

σ_1^{-1}

σ_2^{-1}

1. Fall: Nur T_2 kann die Nachricht lesen. $\sigma_2(x)$ gesendet
2. Fall: Nur T_1 kann die Nachricht abschicken.
3. Fall: Nur T_1 und T_2 können kommunizieren.

Schlüssel: Wähle $n \in \mathbb{N}$ als Produkt von zwei großen^(*) Primzahlen.

Die Nachricht wird in Zahlen aus $\{0, \dots, n-1\}$ zerlegt.

Gesendet wird eine Permutation $\sigma(x), x \in \{0, \dots, n-1\}$
 σ Permutation von $0, \dots, n-1$.

(n, σ) macht man öffentlich $\overleftrightarrow{\sigma}$

$$\left[\begin{array}{l} (*) \\ 1992 \sim 10^{227832} \\ 2001 \sim 10^{2098960} \end{array} \right.$$