4. Dezember 2018

Kongruenzen und Restklassenringe

Kongruenzen und Restklassenringe

Setup

- $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K
- $m \in R \setminus \{0\}$

(m steht für *modulus*, lat. Maß.)

Kongruenzen

Definition

$a, b \in R$

$a \equiv_m b :\Leftrightarrow m \mid a - b$

Wir lesen $a \equiv_m b$ als „a kongruent b modulo m“.

Beispiele

- in $\mathbb{Z}$:
  - $7 \equiv_7 0$
  - $1 \equiv_7 8$
  - $1 \equiv_7 -6$
  - $3 \equiv_7 10$
  - $2 \equiv_7 9$
  - $2 \equiv_7 16$
  - $2 \equiv_7 -5$
  - $16 \equiv_7 -5$
- in $\mathbb{Q}[X]$:
  - $X^2 - 1 \equiv_{X^2-1} 0$
  - $X^2 \equiv_{X^2-1} 1$
  - $X^4 - X^2 + 1 \equiv_{X^2-1} 1$

Kongruenzen (Forts.)

Proposition

$\equiv_m$ ist Äquivalenzrelation auf R.

Notation

- Äquivalenzklasse von $a \in R$ wird mit $\overline{a}$ bezeichnet.
- $R/(m) := \{\overline{a} \mid a \in R\}$ Menge der Äquivalenzklassen.
- Für $R = \mathbb{Z}$ schreiben wir auch $\mathbb{Z}_m := \mathbb{Z}/(m)$.

Kongruenzen (Forts.)

Beispiele

- in $\mathbb{Z}_7$:
  - $\overline{7} = \overline{0}$
  - $\overline{1} = \overline{8} = \overline{-6}$
  - $\overline{3} = \overline{10}$
  - $\overline{2} = \overline{9} = \overline{16} = \overline{-5}$
- in $\mathbb{Q}[X]/(X^2 - 1)$:
  - $\overline{X^2 - 1} = \overline{0}$
  - $\overline{X^2} = \overline{X^4 - X^2 + 1} = \overline{1}$

Kongruenzen und Division mit Rest

Definition

Es sei $a \in R$. Dividiere a durch m mit Rest:

$$a = qm + r$$

mit

$$\begin{cases} 0 \leq r < m, & \text{im Fall } R = \mathbb{Z}, \\ \deg r < \deg m, & \text{im Fall } R = K[X]. \end{cases}$$

Wir setzen

$$a \bmod m := r.$$

Beispiele

- $101 \bmod 7 = 3$;
- $1001 \bmod 13 = 0$;
- $X^3 - 2X^2 + 5 \bmod (X^2 + X + 1) = 2X + 8$.

Kongruenzen und Division mit Rest (Forts.)

Proposition

- Für alle $a \in R$ gilt: $a \equiv_m a \bmod m$.

- Es seien $a, b \in R$.

  Dann sind äquivalent:

  - $a \equiv_m b$
  - $a \bmod m = b \bmod m$

Kongruenzen und Division mit Rest (Forts.)

Bemerkung

Für $a \in R$ ist

$$\overline{a} = a + Rm$$

mit $a + Rm = \{a + xm \mid x \in R\}$.

Kongruenzen und Division mit Rest (Forts.)

Definition

Es sei $n \in \mathbb{N}_0$. Wir setzen

$$\begin{aligned} K[X]_{<n} &:= \{f \in K[X] \mid \deg f < n\} \\ &= \{\sum_{i=0}^{n-1} a_i X^i \mid a_0, a_1, \ldots, a_{n-1} \in K\}. \end{aligned}$$

Beipiele

- $K[X]_{<0} = \{0\}$.
- $K[X]_{<1} = \{f \in K[X] \mid f \text{ ist konstant}\} = K$.
- $K[X]_{<2} = \{aX + b \mid a, b \in K\}$: Menge der linearen Polynome.

Kongruenzen und Division mit Rest (Forts.)

Korollar

- Es sei $n \in \mathbb{N}$.

  $\{0, 1, \ldots, n-1\}$ ist Repräsentantensystem von $\mathbb{Z}/(n)$; insbesondere:

  $$\mathbb{Z}/(n) = \{\overline{r} \mid r \in \{0, 1, \ldots, n-1\}\}.$$

- Es sei $g \in K[X] \setminus \{0\}$, $n := \deg g$.

  $K[X]_{<n}$ ist Repräsentantensystem von $K[X]/(g)$; insbesondere:

  $$K[X]/(g) = \{\overline{r} \mid r \in K[X]_{<n}\}.$$

Kongruenzen und Division mit Rest (Forts.)

Beispiel

- $\mathbb{Z}/(7) =$
- $\mathbb{Q}[X]/(X^2 - 1) =$

Restklassenringe

Proposition

Es seien $a, a', b, b' \in R$ mit $a \equiv_m a'$, $b \equiv_m b'$. Dann gilt:

- $a + b \equiv_m a' + b'$;
- $ab \equiv_m a'b'$.

Restklassenringe (Forts.)

Beispiel

In $\mathbb{Q}[X]$:

$f := X^5 - 3X^4 + 2X^3 - X^2 + 2, h := X^4 - X^3 + 2.$

$$\begin{aligned} f &\equiv_{X^2-1} 3X - 2 \\ h &\equiv_{X^2-1} -X + 3 \end{aligned}$$

$$\begin{aligned} f + g &\equiv_{X^2-1} 2X + 1 \\ f \cdot g &\equiv_{X^2-1} -3X^2 + 11X - 6 \end{aligned}$$

Wegen $-3X^2 + 11X - 6 \bmod X^2 - 1 = 11X - 9$ gilt auch

$$f \cdot g \equiv_{X^2-1} 11X - 9.$$

Restklassenringe (Forts.)

Proposition

$R/(m)$ wird kommutativer Ring mit:

- Addition:
- Null:
- Negative:
- Multiplikation:
- Eins:

Restklassenringe (Forts.)

Beispiele

- In $\mathbb{Z}/(7)$:
  - $\overline{5} + \overline{4} \quad =$
  - $\overline{3} \cdot \overline{4} \quad =$
  - $\overline{13} \cdot \overline{13} \quad =$
- In $\mathbb{Q}[X]/(X^2 - 1)$:
  - $\overline{X^5 - X^3 - 3} \cdot \overline{X^4 - X^2 + 2} \quad =$
  - $\overline{X - 1} \cdot \overline{X + 1} \quad =$

Restklassenringe (Forts.)

Bemerkung (Rechnen in $\mathbb{Z}_n$)

Es seien $i, j \in \mathbb{Z}$ mit $0 \leq i, j < n$.

- Zur Addition von $\bar{i}$ und $\bar{j}$, addiere i und j in $\mathbb{Z}$ und dividiere das Ergebnis mit Rest durch n:

$$\bar{i} + \bar{j} = \overline{(i + j) \bmod n}.$$

- Zur Multiplikation von $\bar{i}$ und $\bar{j}$, multipliziere i und j in $\mathbb{Z}$ und dividiere das Ergebnis mit Rest durch n:

$$\bar{i} \cdot \bar{j} = \overline{(i \cdot j) \bmod n}.$$

Analoge Regeln gelten für das Rechnen im Restklassenring $K[X]/(g)$ für ein $g \in K[X] \setminus \{0\}$.

Restklassenringe (Forts.)

Beispiel

Addition und Multiplikation von $\mathbb{Z}/(4) = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$				
$\overline{1}$				
$\overline{2}$				
$\overline{3}$				

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$				
$\overline{1}$				
$\overline{2}$				
$\overline{3}$				

Lineare Kongruenzgleichungen in einer Unbekannten

Lösbarkeitskriterium für lineare Kongruenzgleichungen

Es seien $a, b \in R$. Dann gilt:

Es gibt $x \in R$ mit $xa \equiv_m b \Leftrightarrow \mathrm{ggT}(a, m) \mid b$.

Korollar

Es sei $a \in R$. Dann gilt: $\overline{a} \in (R/(m))^\times \Leftrightarrow \mathrm{ggT}(a, m) = 1$.

Lin. Kongruenzgleichungen in einer Unbekannten (Forts.)

Lösungsmenge linearer Kongruenzgleichungen

Es seien $a, b \in R$ mit $\mathrm{ggT}(a, m) \mid b$.

Gesucht: $\{x \in R \mid xa \equiv_m b\}$.

Verfahren

Berechne $u, v, w, x', y' \in R$ mit

- $m = u \cdot \mathrm{ggT}(a, m)$,
- $a = v \cdot \mathrm{ggT}(a, m)$,
- $b = w \cdot \mathrm{ggT}(a, m)$,
- $x'a + y'm = \mathrm{ggT}(a, m)$.

Dann ist $\{x \in R \mid xa \equiv_m b\} = \{wx' + uz \mid z \in R\}$.

Lin. Kongruenzgleichungen in einer Unbekannten (Forts.)

Beispiel

$\{x \in \mathbb{Z} \mid x \cdot 168 \equiv_{91} 21\} =$

Einheiten (Forts.)

Korollar
Es sei $a \in R$. Dann gilt: $\overline{a} \in (R/(m))^\times \Leftrightarrow \mathrm{ggT}(a, m) = 1$.

Bemerkung
Es sei $a \in R$ mit $\mathrm{ggT}(a, m) = 1$.

Frage: Wie findet man $\overline{a}^{-1} \in R/(m)$?

Antwort: Bestimme $x, y \in R$ mit $xa + ym = 1$.

Dann ist $\overline{a}^{-1} = \overline{x}$.

Einheiten (Forts.)

Beispiele

- $\overline{17} \in (\mathbb{Z}/(30))^\times$ mit

$$\overline{17}^{-1} = \overline{23}$$

- $\overline{X+2} \in (\mathbb{Q}[X]/(X^2-1))^\times$ mit

$$(\overline{X+2})^{-1} = \overline{-X/3+2/3}$$

- $(\mathbb{Z}_8)^\times =$

Einheiten (Forts.)

Definition

- Ein Element $p \in \mathbb{N}$ heißt *Primzahl*, wenn $p > 1$ ist und 1 und p die einzigen Teiler von p in $\mathbb{N}$ sind.

- Ein Element $g \in K[X]$ heißt *irreduzibel*, wenn $g \neq 0$ ist, $\deg g \geq 1$ ist und es gilt: die einzigen Teiler von g sind Einheiten oder assoziiert zu g.

  Mit anderen Worten: Ist $g = fh$ mit $f, h \in K[X]$, dann ist $f \in K^\times$ oder $h \in K^\times$.

Einheiten (Forts.)

Satz

Es sei $m \in R, m \neq 0$. Dann sind äquivalent:

- R/m ist Körper
- $\begin{cases} m \text{ ist Primzahl} & (\text{im Fall } R = \mathbb{Z}) \\ m \text{ ist irreduzibel} & (\text{im Fall } R = K[X]) \end{cases}$

Endliche Primkörper

Definition

$p \in \mathbb{P}$

Primkörper zu p: $\mathbb{F}_p := \mathbb{Z}/(p)$

Beispiel

- $\mathbb{F}_2 = \mathbb{Z}/(2) = \{\overline{0}, \overline{1}\}$

$+$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

$\cdot$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$