Kongruenz ist Äquivalenzrelation

Lemma Kongruenz ist Äquivalenzrelation

Die Kongruenz modulo n ist eine Äquivalenzrelation auf $\mathbb{Z}$. D.h. für alle $a, b, c \in \mathbb{Z}$ gilt

1. **Reflexivität:** $a \equiv a \bmod n$
2. **Symmetrie:** $a \equiv b \bmod n \Rightarrow b \equiv a \bmod n$.
3. **Transitivität:** $a \equiv b \bmod n$ und $b \equiv c \bmod n \Rightarrow a \equiv c \bmod n$.

Beweis:

(1) Es gilt $n \mid a - a$, da jede Zahl die Null teilt.

(2) Aus $n|a - b$ folgt $n| - (a - b)$ bzw $n|b - a$.

(3) Aus $n|a - b$ und $n|b - c$ folgt $n|(a - b) + (b - c)$ bzw. $n|a - c$.

Die Restklassen $\mathbb{Z}/n\mathbb{Z}$

Definition Restklassen $\mathbb{Z}/n\mathbb{Z}$

Die vorigen Äquivalenzklassen heißen *Restklassenklassen modulo n*.
Wir definieren $\bar{a} := a + n\mathbb{Z} := \{a + kn \in \mathbb{Z} \mid k \in \mathbb{Z}\}$ für $a \in \mathbb{Z}$.
Ein Element $b \in \bar{a}$ heißt *Repräsentant* der Restklasse $\bar{a}$.
Die Mengen aller Restklassen modulo n bezeichnen wir mit

$$\mathbb{Z}/n\mathbb{Z} := \{a + n\mathbb{Z} \mid a \in \mathbb{Z}\}.$$

Definition Vollständiges Repräsentantensystem

$R \subseteq \mathbb{Z}$ heißt *vollständiges Repräsentantensystem* für $\mathbb{Z}/n\mathbb{Z}$ falls gilt

1. $\mathbb{Z}/n\mathbb{Z} = \{r + n\mathbb{Z} \mid r \in R\}$,
2. $r_1 + n\mathbb{Z} \neq r_2 + n\mathbb{Z}$ für verschiedene $r_1, r_2 \in R$.

Repräsentantensystem für $\mathbb{Z}/n\mathbb{Z}$

Lemma Repräsentantensystem für $\mathbb{Z}/n\mathbb{Z}$

$R = \{0, 1, \ldots, n-1\}$ ist ein vollständiges Repräsentantensystem für $\mathbb{Z}/n\mathbb{Z}$. Insbesondere ist $|\mathbb{Z}/n\mathbb{Z}| = n$.

Beweis:

(1) Sei $\bar{a}$ eine beliebige Restklasse modulo n.

- Euklidische Division von a durch n liefert $a = qn + r$ mit $|r| < n$.
- Es gilt entweder $r \in R$ oder $r' := r + n \in R$. Ferner ist $\bar{a} = \bar{r} = \bar{r}'$.
- D.h. wir können $\bar{a}$ mittels eines Repräsentanten aus R darstellen.

(2) Annahme: $r_1 + n\mathbb{Z} = r_2 + n\mathbb{Z}$ für zwei verschiedene $r_1, r_2 \in R$.

- Dann gilt $r_1 - r_2 \equiv 0 \bmod n$. Es gilt aber $-n < r_1 - r_2 < n$.
- Damit folgt $r_1 - r_2 = 0 \cdot n = 0$ bzw $r_1 = r_2$. (Widerspruch)

Da R ein vollständiges Repräsentantensystem für $\mathbb{Z}/n\mathbb{Z}$ ist, gilt

$$|\mathbb{Z}/n\mathbb{Z}| = |R| = n.$$

$\mathbb{Z}/n\mathbb{Z}$ besitzt Ringstruktur.

Satz $\mathbb{Z}/n\mathbb{Z}$ besitzt Ringstruktur.

$\mathbb{Z}/n\mathbb{Z}$ ist mit den wie folgt definierten Operationen ein Ring

$$\bar{a} + \bar{b} := \overline{a+b} \text{ und } \bar{a} \cdot \bar{b} := \overline{a \cdot b} \text{ für alle } a, b \in \mathbb{Z}.$$

Beweis:

- Die Repräsentantenunabhängigkeit der Addition und Multiplikation modulo n haben wir bereits auf Folie 46 gezeigt.
- Die Ringeigenschaften – wie neutrale Elemente und Distributivität – vererben sich von $\mathbb{Z}$ auf $\mathbb{Z}/n\mathbb{Z}$.

Bsp: Verknüpfungstafel für $\mathbb{Z}/4\mathbb{Z}$:

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

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

Ringhomomorphismen

Lemma $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$

Die Abbildung $f : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, x \mapsto x + n\mathbb{Z}$ ist ein Ringhomomorphismus.

Beweis:

- Es gilt $f(a+b) = \overline{a+b} = \bar{a} + \bar{b} = f(a) + f(b)$.
- Analog folgt $f(a \cdot b) = \overline{a \cdot b} = \bar{a} \cdot \bar{b} = f(a) \cdot f(b)$.
- Ferner ist $f(1) = 1 + n\mathbb{Z} = \bar{1}$ das neutrale Element in $\mathbb{Z}/n\mathbb{Z}$.

Lemma $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$

Seien $n, m \in \mathbb{N}$ mit $m|n$. Die Abbildung
$f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}, x + n\mathbb{Z} \mapsto x + m\mathbb{Z}$ ist ein Ringhomomorphismus.

Beweis: Folgt aus dem Lemma auf Folie 51.

CRT reloaded

Satz Chinesischer Restsatz (Version 2)

Seien $m, n \in \mathbb{N}$ teilerfremd. Dann ist die Abbildung

$$\begin{array}{rccc} \Phi: & \mathbb{Z}/nm\mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \\ & x + nm\mathbb{Z} & \mapsto & (x + n\mathbb{Z}, x + m\mathbb{Z}) \end{array}$$

ein Isomorphismus. Sei $xn + ym = 1$ für $x, y \in \mathbb{Z}$. Dann gilt

$$\begin{array}{rccc} \Phi^{-1}: & \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} & \to & \mathbb{Z}/nm\mathbb{Z} \\ & (\bar{a}, \bar{b}) & \mapsto & \overline{a(1 - xn) + b(1 - ym)}. \end{array}$$

Beweis:

- Dass Φ ein Homomorphismus ist, folgt aus dem vorigen Lemma.
- Bleibt zu zeigen, dass Φ bijektiv ist. Es gilt
$$|\mathbb{Z}/nm\mathbb{Z}| = nm = |\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}|.$$
- Daher genügt es zu zeigen, dass Φ injektiv ist.
- Die 1.Version des CRT liefert aber gerade, dass jedes $(\bar{a}, \bar{b}) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ genau eine Lösung $\bar{x} \in \mathbb{Z}/nm\mathbb{Z}$ besitzt.

2. Variante des CRT

Beweis: (Fortsetzung)

- Wir wollen noch die explizite Formel für Φ^{-1} herleiten.
- Nach Lemma von Bézout existieren $x, y \in \mathbb{Z}$ mit $xn + ym = 1$.
- Es gilt

$$\Phi(\overline{1 - xn}) = (\overline{1 - xn}, \overline{1 - xn}) = (\bar{1}, \overline{ym}) = (\bar{1}, \bar{0}) \text{ und}$$

$$\Phi(\overline{1 - ym}) = (\overline{1 - ym}, \overline{1 - ym}) = (\overline{xn}, \bar{1}) = (\bar{0}, \bar{1}).$$

- Aus der Linearität des Ringhomomorphismus folgt
  $\Phi(\overline{a(1 - xn) + b(1 - ym)}) = \bar{a}(\Phi(\overline{1 - xn})) + \bar{b}(\Phi(\overline{1 - ym})) = (\bar{a}, \bar{b})$.
- Anwendung von Φ^{-1} auf beide Seiten liefert die Formel.

Korollar

Seien $n_1, \ldots, n_k \in \mathbb{N}$ paarweise teilerfremd. Dann gilt

$$\mathbb{Z}/n_1 \ldots n_k\mathbb{Z} \simeq \mathbb{Z}/n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/n_k\mathbb{Z}.$$

Beweis: Folgt induktiv aus vorigem Satz für $n = n_1 \ldots n_{k-1}$, $m = n_k$.

Die Einheitengruppe U_n

Definition Einheitengruppe U_n

Wir bezeichnen die Einheiten von $\mathbb{Z}/n\mathbb{Z}$ als

$$U_n := (\mathbb{Z}/n\mathbb{Z})^* = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} \mid \bar{a}|\bar{1}\}.$$

Satz Struktur der Einheitengruppe U_n

Es gilt $U_n = \{a + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z} \mid \mathrm{ggT}(a,n) = 1\}$. Ferner ist $(U_n, \cdot)$ eine Gruppe.

Beweis:

- $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ ist eine Einheit falls $\bar{a}\bar{x} = \bar{1}$ für ein $\bar{x} \in \mathbb{Z}/n\mathbb{Z}$.
- Dies ist äquivalent mit $ax \equiv 1 \bmod n$. Nach Folie 52 existiert eine Lösung für x gdw $\mathrm{ggT}(a,n)|1$, d.h. $\mathrm{ggT}(a,n) = 1$.
- $(U_n, \cdot)$ ist abgeschlossen bezüglich Multiplikation, denn für $\overline{ab}$, $\bar{a}, \bar{b} \in U_n$ existiert das Inverse $(\overline{ab})^{-1} = \bar{b}^{-1}\bar{a}^{-1}$. D.h. $\overline{ab} \in U_n$.
- Nach Definition von U_n besitzen alle Elemente ein Inverses.

Die Eulersche φ-Funktion

Bsp: $U_{12} = \{\bar{1}, \bar{5}, \bar{7}, \overline{11}\}$ und $U_p = \mathbb{Z}/p\mathbb{Z} \setminus \{\bar{0}\}$ für $p \in \mathbb{P}$.

Definition Eulersche φ-Funktion

Die *Eulersche φ-Funktion* ist definiert als

$$\varphi : \mathbb{N} \to \mathbb{N} \text{ mit } n \mapsto |U_n|.$$

Bsp: $\varphi(12) = 4$ und $\varphi(p) = p - 1$ für $p \in \mathbb{P}$.

Eulersche φ-Funktion für Primpotenzen

Lemma Eulersche φ-Funktion für Primpotenzen

Sei $p \in \mathbb{P}$ und $r \in \mathbb{N}$. Dann gilt

$$\varphi(p^r) = p^{r-1}(p-1).$$

Beweis:

- Es gilt $U_{p^r} = \{a + p^r\mathbb{Z} \in \mathbb{Z}/p^r\mathbb{Z} \mid \mathrm{ggT}(a, p^r) = 1\}$
  $= \mathbb{Z}/p^r\mathbb{Z} \setminus \{a + p^r\mathbb{Z} \in \mathbb{Z}/p^r\mathbb{Z} \mid \mathrm{ggT}(a, p^r) > 1\}.$
- Wir stellen $\mathbb{Z}/p^r\mathbb{Z}$ mittels der Repräsentanten $0, 1, \ldots, p^r - 1$ dar.
- Folgende p^{r-1} Repräsentanten besitzen nicht-triviale ggTs mit p^r:
  $$0, p, 2p, \ldots, (p^{r-1} - 1)p\ .$$
- Damit gilt
  $$\begin{aligned}\varphi(p^r) = |U_{p^r}| &= |\mathbb{Z}/p^r\mathbb{Z}| - |\{a + p^r\mathbb{Z} \in \mathbb{Z}/p^r\mathbb{Z} \mid \mathrm{ggT}(a, p^r) > 1\}| \\ &= p^r - p^{r-1} = p^{r-1}(p-1).\end{aligned}$$

Eulersche φ-Funktion

Lemma Eulersche φ-Funktion für teilerfremde Zahlen

Seien $n, m \in \mathbb{N}$ teilerfremd. Dann gilt

$$U_{nm} \cong U_n \times U_m \text{ und } \varphi(nm) = \varphi(n) \cdot \varphi(m).$$

Beweis: Nach Chinesischem Restsatz gilt

$$\begin{aligned} U_{nm} = (\mathbb{Z}/nm\mathbb{Z})^* &\cong (\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z})^* \\ &= (\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^* = U_n \times U_m. \end{aligned}$$

Es folgt $\varphi(nm) = |U_{nm}| = |U_n \times U_m| = |U_n| \cdot |U_m| = \varphi(n) \cdot \varphi(m)$.

Satz Eulersche φ-Funktion

Sei $n \in \mathbb{N}$ mit Primfaktorzerlegung $n = \prod_{i=1}^{s} p_i^{r_i}$. Dann gilt

$$\varphi(n) = \prod_{i=1}^{s} p_i^{r_i - 1}(p_i - 1).$$

Beweis: Nach den vorigen beiden Lemmata gilt

$$\varphi(n) = \prod_{i=1}^{s} \varphi(p_i^{r_i}) = \prod_{i=1}^{s} p_i^{r_i - 1}(p_i - 1).$$