Übung zu F25T1A2 : H22T2A2

Kongruenzrechnung

Def: Sei $n \in \mathbb{N}$, und seien $a, b \in \mathbb{Z}$.
$a \equiv b \bmod n$ bedeutet nach Def: $n \mid (b-a)$
Dies ist eine Äquivalenzrelation auf $\mathbb{Z}$, d.h.
für alle $a, b, c \in \mathbb{Z}$ gilt

(i) $a \equiv a \bmod n$ (ii) $a \equiv b \bmod n \Rightarrow b \equiv a \bmod n$

(iii) $a \equiv b \bmod n \wedge b \equiv c \bmod n \Rightarrow a \equiv c \bmod n$

(iii) $a \equiv b \bmod n \wedge b \equiv c \bmod n \Rightarrow a \equiv c \bmod n$

Darüber hinaus ist für alle $a, b \in \mathbb{Z}$ die Relation $a \equiv b \bmod n$ äquivalent zur Gleichung $a + n\mathbb{Z} = b + n\mathbb{Z}$ in $\mathbb{Z}/n\mathbb{Z}$.

Weitere Rechenregeln: Seien $a, b, c, d \in \mathbb{Z}$, $m, n \in \mathbb{N}$.

(i) $a \equiv b \bmod n,\ c \equiv d \bmod n \Rightarrow a + c \equiv b + d \bmod n$ und $ac \equiv bd \bmod n$

(ii) $a \equiv b \bmod n,\ m \mid n \Rightarrow a \equiv b \bmod m$

(iii) $am \equiv bm \bmod mn \iff a \equiv b \bmod n$

(z.B. $3x \equiv y \bmod 4 \Rightarrow 12x \equiv 4x \bmod 16$)

Beweis von (iii), nur „$\Rightarrow$": $am \equiv bm \bmod mn \Rightarrow$

$mn \mid (bm - am) \Rightarrow \exists k \in \mathbb{Z} : bm - am = k\,m\,n$

$\cdot m^{-1}$

$\Longrightarrow b - a = kn \Rightarrow n \mid (b-a) \rightarrow a \equiv b \bmod n$

Chinesischer Restsatz:

(1) allgemeine Fassung

Def.: Zwei Ideale I, J in einem Ring R heißen teilerfremd, wenn $I + J = (1_R)$ erfüllt ist.

Chinesischer Restsatz: Sei R ein Ring, und seien I, J teilerfremde Ideale in R. Dann gibt einen Ringisomorphismus $\phi : R/IJ \to R/I \times R/J$ mit $\phi(a + IJ) = (a + I, a + J)$ $\forall a \in R$. (Daraus folgt

$\phi: R/IJ \to R/I \times R/J$ mit
$\phi(a+IJ) = (a+I, a+J)$ $\forall a \in R$

insbesondere, dass für bel. $b, c \in R$ immer ein $a \in R$ existiert mit $(b+I, c+J) = \phi(a+IJ) = (a+I, a+J)$.

(2) Fassung für $\mathbb{Z}$: Seien $m, n \in \mathbb{N}$ teilerfremd. Dann existiert ein Ringisomorphismus

$\phi: \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ mit $\phi(a+mn\mathbb{Z}) = (a+m\mathbb{Z}, a+n\mathbb{Z})$ $\forall a \in \mathbb{Z}$.

häufiges Berechnungsproblem: Gegeben $b, c \in \mathbb{Z}$, wie findet man ein $a \in \mathbb{Z}$ mit $\phi(a+mn\mathbb{Z}) = (b+m\mathbb{Z}, c+n\mathbb{Z})$?

ii) Wegen $ggT(m,n)=1$ gibt es $x, y \in \mathbb{Z}$ mit

$xm + yn = 1$. Berechne solche x, y mit dem Euklidischen Algorithmus.

(ii) Berechne $u = 1 - xm = yn$ und
$v = 1 - yn = xm$. (Diese Elemente erfüllen $\phi(u + mn\mathbb{Z}) = (1 + m\mathbb{Z}, 0 + n\mathbb{Z})$ und $\phi(v + mn\mathbb{Z}) = (0 + m\mathbb{Z}, 1 + n\mathbb{Z})$.)

(iii) Setze $a = bu + cv$. (Dann gilt $\phi(a + mn\mathbb{Z}) = (a + m\mathbb{Z}, b + n\mathbb{Z})$, wie gewünscht.)

(Übung dazu: H12T1A5 (G))

(3) Formulierung des Chin. Restsatzes für Kongruenzsysteme: Sind $m, n \in \mathbb{N}$ teilerfremd und $b, c \in \mathbb{Z}$, dann gibt es ein eindeutig bestimmtes $a \in \{0, 1, \ldots, mn-1\}$ mit $a \equiv b \bmod m$ und $a \equiv c \bmod n$.

alternativ: Die Lösungsmenge $\mathcal{L} \subseteq \mathbb{Z}$ des Kongruenzsystems $x \equiv b \bmod m$, $x \equiv c \bmod n$ ist gegeben durch $\mathcal{L} = a + mn\mathbb{Z}$, falls a eine Lösung des Systems ist, und es ist $\mathcal{L} = \emptyset$.

es für
N teile-
in einen-
] mit

⊆ ℤ des
-c mod n
lls a eine
st $\mathcal{L} \neq \emptyset$.

F22T3A2

(a) Bestimmen Sie $a, b \in \mathbb{Z}$ mit

$(1+2\mathbb{Z}) \cap (2+3\mathbb{Z}) \cap (3+5\mathbb{Z}) = a+b\mathbb{Z}$,

mit Nachweis.

Für jedes $a \in \mathbb{Z}$ gilt die Äquivalenz

$a \in 1+2\mathbb{Z} \iff \exists k \in \mathbb{Z} : a = 1+2k$

$\iff 2 \mid (a-1) \iff a \equiv 1 \bmod 2$, ebenso:

$a \in 2+3\mathbb{Z} \iff a \equiv 2 \bmod 3$ und

$a \in 3+5\mathbb{Z} \iff a \equiv 3 \bmod 5$.

Insgesamt gilt also:

$a \in (1+2\mathbb{Z}) \cap (2+3\mathbb{Z}) \cap (3+5\mathbb{Z}) \iff$

a ist Lösung des Systems

$x \equiv 1 \bmod 2 \wedge x \equiv 2 \bmod 3 \wedge x \equiv 3 \bmod 5$

Da die Zahlen 2, 3 und 5 paarweise teilerfremd sind und $2 \cdot 3 \cdot 5 = 30$ ist, existiert nach dem Chin. Restsatz (für drei statt zwei Faktoren) ein eindeutig bestimmtes $a \in \{0, 1, \ldots, 29\}$, das das System löst, und die Lösungsmenge $\mathbb{L}$ des Systems ist dann gegeben durch

$$\mathbb{L} = a + 30\mathbb{Z}.$$

Lösungen von $x \equiv 3 \bmod 5$ in $\{0, \ldots, 29\}$:

3, 8, 13, 18, 23, 28

Davon lösen zusätzlich $x \equiv 2 \bmod 3$:

8, 23

Die einzige Zahl, die zusätzlich $x \equiv 1 \bmod 2$ löst, ist 23 $\Rightarrow \mathbb{L} = 23 + 30\mathbb{Z} \Rightarrow a = 23, b = 30$

(6) Bestimmen Sie alle $(x,y) \in \mathbb{Z}^2$ mit $221x + 39y = 26$.

Die Lösungsmenge stimmt überein mit der Lösungsmenge der Gleichung $17x + 3y = 2$ (Division durch 13)

Für $(x,y) \in \mathbb{Z}^2$ gilt jeweils

$$17x + 3y = 2 \iff y = \tfrac{2}{3} - \tfrac{17}{3}x \text{ und } x, y \in \mathbb{Z}$$

$$\iff y = \tfrac{2}{3} - \tfrac{17}{3}x \wedge x \in \mathbb{Z} \wedge \tfrac{2}{3} - \tfrac{17}{3}x \in \mathbb{Z}$$

$$\iff y = \tfrac{2}{3} - \tfrac{17}{3}x \wedge x \in \mathbb{Z} \wedge \exists k \in \mathbb{Z} : \tfrac{2}{3} - \tfrac{17}{3}x = k$$

$$\iff y = \tfrac{2}{3} - \tfrac{17}{3}x \wedge x \in \mathbb{Z} \wedge \exists k \in \mathbb{Z} : 2 - 17x = 3k$$

$$\iff x \in \mathbb{Z} \wedge 2 \equiv 17x \bmod 3 \wedge y = \tfrac{2}{3} - \tfrac{17}{3}x$$

$$\iff x \in \mathbb{Z} \wedge 2 \equiv 2x \bmod 3 \wedge y = \tfrac{2}{3} - \tfrac{17}{3}x$$

$\Leftrightarrow y = \frac{2}{3} - \frac{17}{3}x \wedge x \in \mathbb{Z} \wedge \frac{2}{3} - \frac{17}{3}x \in \mathbb{Z}$

außerdem $\forall x \in \mathbb{Z}: 2 \equiv 2x \bmod 3 \Leftrightarrow 4 \equiv 4x \bmod 3$

$\Leftrightarrow x \equiv 4 \bmod 3 \Leftrightarrow x \equiv 1 \bmod 3 \Leftrightarrow x \in 1 + 3\mathbb{Z}$

Die Lösungsmenge der Gleichung ist also gegeben durch

$$\mathcal{L} = \{(x, \tfrac{2}{3} - \tfrac{17}{3}x) \mid x \in 1+3\mathbb{Z}\}$$
$$= \{(1+3k, \tfrac{2}{3} - \tfrac{17}{3}(1+3k)) \mid k \in \mathbb{Z}\}$$
$$= \{(1+3k, -5-17k) \mid k \in \mathbb{Z}\}$$

(z.B. liefern $k = 0, 1$ die Lösungen $(1, -5)$ bzw $(4, -22)$

$17 \cdot 1 + 3 \cdot (-5) = 2$, $17 \cdot 4 + 3 \cdot (-22) = 2$.)

Übung: Bestimmen Sie $\{(x,y) \in \mathbb{Z}^2 \mid 11x + 7y = 32\}$

Körper $\Rightarrow$ $b + p\mathbb{Z} \in (\mathbb{Z}/p\mathbb{Z})^\times$

(c) Sei $n \in \mathbb{N}$ mit $n \geq 2$. Sei $a \in \mathbb{Z}$.
Wir setzen voraus, dass $p = 2^n + 1$ eine Primzahl ist. Zeigen Sie: Genau dann ist $a + p\mathbb{Z}$ ein Erzeuger von $(\mathbb{Z}/p\mathbb{Z})^\times$, wenn a in $\mathbb{Z}/p\mathbb{Z}$ kein Quadrat ist.

„$\Rightarrow$" durch Kontraposition

Voraussetzung: $\exists b \in \mathbb{Z} : a + p\mathbb{Z} = (b + p\mathbb{Z})^2$

z.zg.: $a + p\mathbb{Z}$ ist kein Erzeuger von $(\mathbb{Z}/p\mathbb{Z})^\times$

1. Fall: $p \mid a$ Dann gilt $a + p\mathbb{Z} = 0 + p\mathbb{Z}$ und somit $a + p\mathbb{Z} \notin (\mathbb{Z}/p\mathbb{Z})^\times$. Damit kann $a + p\mathbb{Z}$

erst recht kein Erzeuger von $(\mathbb{Z}/p\mathbb{Z})^*$ sein.

2. Fall: $p \nmid a$ Dann gilt $a+p\mathbb{Z} \neq 0+p\mathbb{Z}$, und weil p eine Primzahl ist, folgt daraus, dass $(\mathbb{Z}/p\mathbb{Z})^* = \mathbb{Z}/p\mathbb{Z} \setminus \{0+p\mathbb{Z}\}$ und $a+p\mathbb{Z} \in (\mathbb{Z}/p\mathbb{Z})^*$ gilt.

$a+p\mathbb{Z} = (b+p\mathbb{Z})^2$, $a+p\mathbb{Z} \neq 0+p\mathbb{Z}$, $\mathbb{Z}/p\mathbb{Z}$ Körper $\Rightarrow b+p\mathbb{Z} \in (\mathbb{Z}/p\mathbb{Z})^*$

$b+p\mathbb{Z} \in (\mathbb{Z}/p\mathbb{Z})^*$, $|(\mathbb{Z}/p\mathbb{Z})^*| = p-1 = 2^n$

$\Rightarrow \operatorname{ord}(b+p\mathbb{Z})$ teilt 2^n

$2 \mid 2^n \Rightarrow \operatorname{ord}(a+p\mathbb{Z}) = \operatorname{ord}((b+p\mathbb{Z})^2) = \frac{\operatorname{ord}(b+\mathbb{Z})}{2}$

$\Rightarrow \operatorname{ord}(a+p\mathbb{Z}) \leq \frac{2^n}{2} = 2^{n-1} \Longrightarrow$

und $\phi(rt \text{ mn } \mathbb{Z}) = (0+n\mathbb{Z}, 1+n\mathbb{Z})$

$\text{ord}(a+p\mathbb{Z}) < |(\mathbb{Z}/p\mathbb{Z})^\times| \Rightarrow a+p\mathbb{Z}$ ist kein Erzeuger von $(\mathbb{Z}/p\mathbb{Z})^\times$.

„$\Leftarrow$" durch Kontraposition

Vor.: $a+p\mathbb{Z}$ ist kein Erzeuger von $(\mathbb{Z}/p\mathbb{Z})^\times$

z.zg.: $\exists b \in \mathbb{Z}: a+p\mathbb{Z} = (b+p\mathbb{Z})^2$

1. Fall: $p \mid a \Rightarrow a+p\mathbb{Z} = 0+p\mathbb{Z} = (0+p\mathbb{Z})^2$

2. Fall: $p \nmid a$ s.o. $\Rightarrow a+p\mathbb{Z} \in (\mathbb{Z}/p\mathbb{Z})^\times$

Da $\mathbb{Z}/p\mathbb{Z}$ ein endl. Körper ist, ist $(\mathbb{Z}/p\mathbb{Z})^\times$ eine zyklische Gruppe, d.h. $\exists c \in \mathbb{Z}$ mit $(\mathbb{Z}/p\mathbb{Z})^\times = \langle c+p\mathbb{Z} \rangle$. $\Rightarrow a+p\mathbb{Z} \in \langle c+p\mathbb{Z} \rangle \Rightarrow$ $\exists l \in \mathbb{Z}$ mit $a+p\mathbb{Z} = (c+p\mathbb{Z})^l$

Fall 2.1: l ist ungerade. Dann ist l teiler-

2 ist

$\mathbb{Z})^\times$

$p\mathbb{Z})^2$

$\mathbb{Z})^\times$

$p\mathbb{Z})^\times$ ein

$\mathbb{Z}/p\mathbb{Z})^\times$

$\rangle \Rightarrow$

ist l teilen -

Rest zu $|(\mathbb{Z}/p\mathbb{Z})^\times| = p-1 = 2^n \Rightarrow$

$\operatorname{ord}(a+p\mathbb{Z}) = \operatorname{ord}((c+p\mathbb{Z})^l) = \operatorname{ord}(c+p\mathbb{Z})$

$= p-1 \Rightarrow \langle a+p\mathbb{Z}\rangle = (\mathbb{Z}/p\mathbb{Z})^\times$ ↯

Fall 2.2: l ist gerade, d.h. $l = 2k$

für ein $k \in \mathbb{Z} \Rightarrow a+p\mathbb{Z} = (c+p\mathbb{Z})^l$

$= (c+p\mathbb{Z})^{2k} = (c^k+p\mathbb{Z})^2 \Rightarrow$

$a+p\mathbb{Z} = (b+p\mathbb{Z})^2$ ist für $b = c^k$ erfüllt.

□