Kongruenzrechnung

Def: Sei $n \in \mathbb{N}$, und seien $a, b \in \mathbb{Z}$.
Man bezeichnet a, b als kongruent modulo n (Notation: $a \equiv b \bmod n$) wenn $n \mid (b-a)$ gilt, also $b - a = kn$ für ein $k \in \mathbb{Z}$ erfüllt ist.
(äquivalent: Dividiert man a und b durch n, dann bleibt derselbe Rest übrig.)

Satz: Seien $a, b, c, d \in \mathbb{Z}$, $m, n \in \mathbb{N}$
(i) Die Kongruenz modulo n ist eine Äquivalenzrelation auf $\mathbb{Z}$ (reflexiv, symm., transitiv)

$a \equiv b \bmod n$ und $b \equiv c \bmod n \Rightarrow a \equiv c \bmod n$

(kürzer: $a \equiv b \equiv c \bmod n$)

(ii) Die Äquivalenzklassen dieser Äquivalenzrelation sind genau die Elemente von $\mathbb{Z}/n\mathbb{Z}$. Es gilt

$a \equiv b \bmod n \iff a + n\mathbb{Z} = b + n\mathbb{Z}$.

[falsch: $\frac{1}{2} \equiv 3 \bmod 5$ (obwohl $(2+5\mathbb{Z})^{-1} = 3+5\mathbb{Z}$) Die Kongruenz modulo n ist eine Relation auf $\mathbb{Z}$, nicht auf $\mathbb{Q}$.)]

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

$a+c \equiv b+d \bmod n$, $ac \equiv bd \bmod n$

$a \equiv c \bmod n$

Äquiva-

Elemente

$+ n\mathbb{Z}$.

wohl

orgrenz

$\mathbb{Z}_i$ nicht

$\to$

$\bmod n$

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

(iv) Für alle $d \in \mathbb{N}$ gilt

$$a \equiv b \bmod n \iff da \equiv db \bmod dn$$

(z.B. $a \equiv b \bmod 2 \iff 2a \equiv 2b \bmod 4$)

Chinesischer Restsatz

(i) für beliebige Ringe:

Ist R ein Ring, $r \geq 2$, $I_1, \dots, I_r$ paarweise teilerfremde Ideale von R (d.h. $I_j + I_k = (1_R)$ für $j \neq k$), dann existiert ein eindeutig bestimmter Ringisomorphismus $\bar{\Phi}: R/I \to R/I_1 \times \dots \times R/I_r$ mit $\bar{\Phi}(a+I) = (a+I_1, \dots, a+I_r)$ $\forall a \in R$, wobei $I = I_1 \cdot \dots \cdot I_r$.

(ii) f

Ist

teile

exist

morp

mit

$\forall a \in$

(iii) für

Ist

frem

dann

mit

(ii) für den Ring $\mathbb{Z}$:

Ist $r \geq 2$ und sind $m_1, \dots, m_r \in \mathbb{N}$ paarweise teilerfremde natürliche Zahlen, dann existiert ein eindeutig bestimmter Ringisomorphismus $\Phi : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m_1\mathbb{Z} \times \dots \times \mathbb{Z}/m_r\mathbb{Z}$ mit $\Phi(a + m\mathbb{Z}) = (a + m_1\mathbb{Z}, \dots, a + m_r\mathbb{Z})$ $\forall a \in \mathbb{Z}$, wobei $m = m_1 \cdot \dots \cdot m_r$.

(iii) für Kongruenzen:

Ist $r \geq 2$, $m_1, \dots, m_r \in \mathbb{N}$ paarweise teilerfremd, $m = m_1 \cdot \dots \cdot m_r$ und $a_1, \dots, a_r \in \mathbb{Z}$, dann existiert ein eind. bestimmtes $a \in \{0, 1, \dots, m-1\}$ mit $a \equiv a_j \bmod m_j$ für $1 \leq j \leq r$.

(Das $a+m\mathbb{Z} \in \mathbb{Z}/m\mathbb{Z}$ ist das eindeutig bestimmte Urbild von $(a_1+m_1\mathbb{Z}, \dots, a_r+m_r\mathbb{Z}) \in \mathbb{Z}/m_1\mathbb{Z} \times \dots \times \mathbb{Z}/m_r\mathbb{Z}$ unter dem Isomorphismus Φ aus (ii).)

Beispiel:

Gesucht wird die Menge aller $a \in \mathbb{Z}$ mit $a \equiv 3 \bmod 23$, $a \equiv 7 \bmod 31$.

1. Schritt: Bestimme $k, l \in \mathbb{Z}$ mit $23k + 31l = 1$ mit dem Euklidischen Algorithmus.

q	a_n	x_n	y_n
–	31	1	0
–	23	0	1
1	8	1	-1
2	7	-2	3
1	1	3	-4
	=	=	=

Ergebnis:
$k = 4$, $l = 3$

ndeutig

..., $a_r + m_r\mathbb{Z}$)

dem Isomor-

$\in \mathbb{Z}$

d 31.

lidusklas

y_n
0
1
-1
3
-1
-4
=

2. Schritt: Betrachte den Isom

$$\Phi: \mathbb{Z}/_{7132\mathbb{Z}} \to \mathbb{Z}/_{232\mathbb{Z}} \times \mathbb{Z}/_{312\mathbb{Z}},$$

aus dem Chin. Restsatz, bestimme Urbilder von $(\bar{1},\bar{0})$, $(\bar{0},\bar{1})$.

$1 - 23k = 31l = 93 \Rightarrow \phi(\overline{93}) = (\bar{1},\bar{0})$

$23k = 1 - 31l = -92 \Rightarrow \phi(\overline{-92}) = (\bar{0},\bar{1})$

3. Schritt: Bestimme das Urbild von $(\bar{3},\bar{7})$.

$\phi^{-1}(\bar{3},\bar{7}) = \bar{3}\cdot\phi^{-1}(\bar{1},\bar{0}) + \bar{7}\cdot\phi^{-1}(\bar{0},\bar{1})$

$= \bar{3}\cdot\overline{93} + \bar{7}(\overline{-92}) = \overline{279} - \overline{644}$

$= -\overline{365} = \overline{348}$

...ffern von n
...aldarstel-
...g?. dann
...≡ 10^k mod 1000.
...od 1000
...3
)

...7, 2^3 5^3) = 1
... von (ℤ/1000ℤ)^×
... = a + 1000ℤ.

...3) = φ(2^3) φ(5^3)
└ 2^3, 5^3 teilerfremd

...ahl von 400,

wichtige Folgerung aus dem Chin. Restsatz:
Sind m, n ∈ ℕ teilerfremd, dann gilt
$(\mathbb{Z}/mn\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$

Erinnerung:
(i) $(\mathbb{Z}/p^e\mathbb{Z})^\times \cong \mathbb{Z}/p^{e-1}(p-1)\mathbb{Z}$ falls p ungerade Primzahl und $e \in \mathbb{N}$
(ii) $(\mathbb{Z}/2^r\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{r-2}\mathbb{Z}$ für $r \geq 2$

F22T1A2 Lösung: F20T3A2
H20T1A1

(a) Bestimmen Sie die letzten drei Ziffern von 7^{404404}

Sei n die angegebene Zahl. Es genügt, die eindeutig bestimmte Zahl $a \in \{0, \ldots, 9997\}$ mit $n \equiv a \bmod 1000$ zu bestimmen.

(denn: Ist $r \in \mathbb{N}$ die Anzahl der Ziffern von n und $a_r a_{r-1} \dots a_1 a_0$ die Dezimaldarstellung von n, mit $a_k \in \{0, 1, \dots, 9\}$, dann gilt $n = \sum_{k=0}^{r} a_k 10^k \equiv \sum_{k=0}^{2} a_k 10^k \bmod 1000$.
$\llcorner 10^k \equiv 0 \bmod 1000$ für $k \geq 3$

$\Rightarrow n = a_2 \cdot 100 + a_1 \cdot 10 + a_0$)

Wegen $ggT(7, 1000) = ggT(7, 2^3 5^3) = 1$
ist $\overline{7} = 7 + 1000\mathbb{Z}$ ein Element von $(\mathbb{Z}/1000\mathbb{Z})^\times$.
außerdem: $\overline{7}^{404404} = n + 1000\mathbb{Z} = a + 1000\mathbb{Z}$.

$|(\mathbb{Z}/1000\mathbb{Z})^\times| = \varphi(1000) = \varphi(2^3 5^3) = \varphi(2^3)\varphi(5^3)$
$= 2^2 \cdot 5^2 \, 4 = 25 \cdot 16 = 400$ $\llcorner 2^3, 5^3$ teilerfremd

$\Rightarrow$ Die Ordnung von $\overline{7}$ ist ein Teiler von 400,
also gilt $\overline{7}^{400} = \overline{1}$.

$404404 \equiv 4 \mod 400 \Rightarrow \exists k \in \mathbb{Z}$

mit $404404 = 400k + 4 \Rightarrow$

$$\bar{7}^{404404} = \bar{7}^{400k+4} = (\bar{7}^{400})^k \cdot \bar{7}^4 =$$

$$\bar{1}^k \bar{7}^4 = \bar{7}^4 = \overline{49}^2 = \overline{2401} = \overline{401}$$

$\Rightarrow a_2 \cdot 100 + a_1 10 + a_0 = a = 401$

$\Rightarrow$ Die letzten drei Ziffern sind $a_2 = 4$, $a_1 = 0$, $a_0 = 1$.

(b) Zeigen Sie: Für alle $n \in \mathbb{N}$ gilt

$$\varphi(n^2) = n\,\varphi(n)$$

bekannt: Ist p eine Primzahl und $e \in \mathbb{N}$, dann gilt $\varphi(p^e) = p^{e-1}(p-1)$. Sei nun $n \in \mathbb{N}$ und $n = \prod_{j=1}^{r} p_j^{e_j}$ die Primfaktorzerlegung von n ($p_1, \dots, p_r$

verschiedene Primzahlen, $e_1, \dots, e_r \in \mathbb{N}$)

$$\Rightarrow \varphi(n) = \prod_{j=1}^{r} \varphi(p_j^{e_j}) = \prod_{j=1}^{r} p_j^{e_j-1}(p_j-1)$$

$$n^2 = \prod_{j=1}^{r} p_j^{2e_j} \Rightarrow \varphi(n^2) = \prod_{j=1}^{r} p_j^{2e_j-1}\cdot(p_j-1)$$

$$= \prod_{j=1}^{r} p_j^{e_j} \; p_j^{e_j-1}(p_j-1) =$$

$$\prod_{j=1}^{r} p_j^{e_j} \cdot \prod_{j=1}^{r} p_j^{e_j-1}(p_j-1) = n\,\varphi(n)$$

zu (c) Sei p eine Primzahl, wobei $p \notin \{2,5\}$.
Zeigen Sie, dass p eine der Zahlen $9, 99, 999, \dots$ teilt.

Die Folge der angegebenen Zahlen ist gegeben durch $(10^k-1)_{k\in\mathbb{N}}$ zu zeigen:

$10^k \equiv 1 \bmod p$

$\mathbb{Z}/p\mathbb{Z}$

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

Gruppe ist
der Ordnung
$k \in \mathbb{N}$ mit

□

$\exists k \in \mathbb{N} : p \mid (10^k - 1)$

äquivalent dazu: $\exists k \in \mathbb{N} : 10^k \equiv 1 \bmod p$

$\Leftrightarrow \exists k \in \mathbb{N} : \overline{10}^k = \overline{1}$ in $\mathbb{Z}/p\mathbb{Z}$

$p \notin \{2, 5\}$

$\Leftrightarrow \exists k \in \mathbb{N} : \overline{10}^k = \overline{1}$ in $(\mathbb{Z}/p\mathbb{Z})^\times$

ggT(10, p) = 1

d.h. $\overline{10} \in (\mathbb{Z}/p\mathbb{Z})^\times$

Da $(\mathbb{Z}/p\mathbb{Z})^\times$ eine endliche Gruppe ist, ist $\overline{10}$ ein Element endlicher Ordnung, d.h. es gibt tatsächlich ein $k \in \mathbb{N}$ mit $\overline{10}^k = \overline{1}$ in $(\mathbb{Z}/p\mathbb{Z})^\times$. □

H25T2A4

Sei $f \in \mathbb{Z}[x]$ ein Polynom mit $f(1) = 1$ und $f(2) = 2$.

(a) Zeigen Sie: $f(a) \equiv 1 \bmod (a-1)$ und $f(a) \equiv 2 \bmod (a-2)$ für alle $a \in \mathbb{Z}$ mit $a \geq 2$.

(b) Es gelte zusätzlich $f(10) > 10$. Zeigen Sie: $f(10) \geq 82$

zu (a) Sei $a \in \mathbb{Z}$ mit $a \geq 3$.

Es gilt $a \equiv 1 \bmod (a-1)$, $a \equiv 2 \bmod (a-2)$ (wegen $(a-1) \mid (a-1)$, $(a-2) \mid (a-2)$).

Allgemein gilt: Ist $g \in \mathbb{Z}[x]$, $n \in \mathbb{N}$, mod

Sind $a, b \in \mathbb{Z}$ mit $a \equiv b \bmod n$, dann gilt $g(a) \equiv g(b) \bmod n$.

denn: Sei $\bar{g}$ das Bild von g in $(\mathbb{Z}/n\mathbb{Z})[x]$. Dann gilt:

$a \equiv b \bmod n \Rightarrow \bar{a} = \bar{b}$ (wobei $\bar{a}, \bar{b}$ Bilder von a, b in $\mathbb{Z}/n\mathbb{Z}$) $\Rightarrow \bar{g}(\bar{a}) = \bar{g}(\bar{b}) \Rightarrow g(a) \equiv g(b) \bmod n$.

Anwendung hier:

$a \equiv 1 \bmod (a-1) \Rightarrow f(a) \equiv f(1) \equiv 1 \bmod (a-1)$

$a \equiv 2 \bmod (a-2) \Rightarrow f(a) \equiv f(2) \equiv 2 \bmod (a-2)$