Kongruenzrechnung

Def.: Sei $n \in \mathbb{N}$. Dann ist die **Kongruenz modulo n** auf $\mathbb{Z}$ definiert durch $a \equiv b \bmod n \iff n \mid (b-a)$.

Lemma: Beziehung zu Restklassenringen

$\forall n \in \mathbb{N}, a, b \in \mathbb{Z}$:

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

wichtige Rechenregeln für Kongruenzen:

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

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

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

(iv) $a \equiv b \bmod m \Leftrightarrow na \equiv nb \bmod nm$

für alle $a, b, c, d \in \mathbb{Z}$ und $m, n \in \mathbb{N}$

Bem. zur Notation: $a_1 \equiv a_2 \bmod n$, $a_2 \equiv a_3 \bmod n$, $\dots$, $a_{r-1} \equiv a_r \bmod n$ kann abgekürzt werden durch die Schreibweise $a_1 \equiv a_2 \equiv a_3 \equiv \dots \equiv a_r \bmod n$

[~~$7 \bmod 4 = 3$~~]

drei Fassungen des Chinesischen Restsatzes:

(1) allgemeine Fassung für Ringe

Sei R ein Ring, $r \in \mathbb{N}$ mit $r \geq 2$, und seien $I_1, \dots, I_r$ paarweise teilerfremde Ideale (d.h. $I_j + I_k = (1_R)$ für $j \neq k$)

Sei $I = I_1 \cdot \dots \cdot I_r$. Dann existiert ein Ringisomorphismus $\overline{\Phi} : R/I \to R/I_1 \times \dots \times R/I_r$ mit

$\overline{\Phi}(a+I) = (a+I_1, \dots, a+I_r) \quad \forall a \in R$

(2) Fassung für $R = \mathbb{Z}$.

Seien $r \in \mathbb{N}$ mit $r \geq 2$, $m_1, \dots, m_r \in \mathbb{N}$ paarweise teilerfremd (d.h. $ggT(m_j, m_k) = 1$ für $j \neq k$), und $m = m_1 \cdot \dots \cdot m_r$.

Seien $r \in \mathbb{N}$ mit $r \geq 2$, $m_1, \dots, m_r \in \mathbb{N}$ paarweise teilerfremd (d.h. $\operatorname{ggT}(m_j, m_k) = 1$ für $j \neq k$), und $m = m_1 \cdot \dots \cdot m_r$.

Dann existiert ein Ringisom. $\phi : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m_1\mathbb{Z} \times \dots \times \mathbb{Z}/m_r\mathbb{Z}$ mit $\phi(a + m\mathbb{Z}) = (a + m_1\mathbb{Z}, \dots, a + m_r\mathbb{Z})$ $\forall a \in \mathbb{Z}$.

(3) Fassung für Kongruenzen:

Seien $r \in \mathbb{N}$ mit $r \geq 2$, $m_1, \dots, m_r \in \mathbb{N}$ paarw. teilerfr. ($m = m_1 \cdot \dots \cdot m_r$).
Dann existiert für bel. vorgeg. $a_1, \dots, a_r \in \mathbb{Z}$ ein eindeutig bestimmtes $a \in \{0, 1, \dots, m-1\}$ mit $a \equiv a_j \bmod m_j$ für $1 \leq j \leq r$.

Erinnerung: Multiplikation von Idealen

Sei R ein Ring, und seien I, J Ideale in R. Dann ist das Produktideal IJ das von $S = \{ab \mid a \in I, b \in J\}$ erzeugte Ideal, d.h. $IJ = (S)$.

wichtige Regel für Produktideale:

$$(a_1, \dots, a_r) \cdot (b_1, \dots, b_s) = \left(\{ a_i b_j \mid \begin{matrix} 1 \le i \le r \\ 1 \le j \le s \end{matrix} \} \right)$$

Bsp: in $R = \mathbb{Z}[\sqrt{-5}]$

$p = (3, 1+2\sqrt{-5})$, $q = (3, 1-2\sqrt{-5})$

$\Rightarrow pq = (3 \cdot 3, 3 \cdot (1-2\sqrt{-5}), (1+2\sqrt{-5}) \cdot 3,$

$(1+2\sqrt{-5})(1-2\sqrt{-5}) = (9, 3-6\sqrt{-5}, 3+6\sqrt{-5}, 21)$

$= (3, 3-6\sqrt{-5}, 3+6\sqrt{-5}) = (3)$

„$\subseteq$" $9 = 3 \cdot 3$, $21 = 7 \cdot 3$

„$\supseteq$" $3 = 1 \cdot 21 + (-2) \cdot 9$

wichtiger Spezialfall: $(a) \cdot (b) = (ab)$

H23T1A1

(a) Sei $n \in \mathbb{N}$, p eine Primzahl mit $p \neq 2$

Zeigen Sie: $p \mid (1+2+\dots+n) \Leftrightarrow p \mid n$ oder $p \mid (n+1)$

bekannt: $1+2+\dots+n = \frac{1}{2}n(n+1)$

Zzg. also: $p \mid \frac{1}{2}n(n+1) \Leftrightarrow p \mid n$ oder $p \mid (n+1)$

„$\Leftarrow$" Sowohl aus $p \mid n$ als auch aus $p \mid (n+1)$ folgt $p \mid n(n+1)$

1. Fall: n gerade $\Rightarrow n = 2m$ für ein $m \in \mathbb{N}$

$p \mid 2m(n+1)$, $p \neq 2$ (da $p \neq 2$), p Primzahl

$\rightarrow p \mid m(n+1) \overset{m=\frac{1}{2}n}{\Rightarrow} p \mid \frac{1}{2}n(n+1)$

2. Fall: n ungerade $\Rightarrow$ $n+1$ gerade $\Rightarrow$

$\exists m \in \mathbb{N}: n+1 = 2m \rightarrow p \mid n(2m)$ $\overset{p \neq 2}{\Rightarrow}$ p Primz.

$p \mid nm \overset{\frac{1}{2}(n+1)=m}{\Rightarrow} p \mid \frac{1}{2}n(n+1)$

" $\Leftarrow$ " $p \mid \frac{1}{2}n(n+1) \rightarrow p \mid n(n+1) \overset{p \text{ Primz.}}{\Rightarrow} p \mid n$ oder $p \mid (n+1)$

(6) Bestimmen Sie die Anzahl der Elemente in $(\mathbb{Z}[x]/(2, x^3+x^2+x))^*$.

Beh.: $\mathbb{Z}[x]/(2, x^3+x^2+x) \cong \mathbb{F}_2[x]/(x^3+x^2+x)$

Sei $\phi: \mathbb{Z}[x] \rightarrow \mathbb{F}_2[x]$, $P \mapsto \bar{P}$ geg. durch koeffizientenweise Reduktion modulo 2 und $\pi: \mathbb{F}_2[x] \rightarrow \mathbb{F}_2[x]/(x^3+x^2+x)$ der kanonische Epimorphismus. Dann ist $\psi = \pi \circ \phi: \mathbb{Z}[x] \rightarrow \mathbb{F}_2[x]/(x^3+x^2+x)$

als Komposition von zwei Ringepimorphismen wiederum ein Ringepimorphismus.

Beh.: $\ker(\varphi) = (2, x^3+x^2+x)$ (Nachweis als Übung)

Insgesamt sind damit für φ die Voraussetzungen des Hom.-satzes für Ringe erfüllt, und dieser liefert die Behauptung.

$$\text{Beh} \Rightarrow \left(\mathbb{Z}[x]/(x^3+x^2+x)\right)^\times \cong \left(\mathbb{F}_2[x]/(x^3+x^2+x)\right)^\times$$

In $\mathbb{F}_2[x]$ gilt $x^3+x^2+x = x(x^2+x+\bar{1})$, und die beiden Faktoren sind teilerfremd (da x irred. und $x \nmid (x^2+x+1)$). Damit sind (x) und (x^2+x+1) teilerfremde Ideale in $\mathbb{F}_2[x]$. Chin. Restsatz $\Rightarrow$

$$\left(\mathbb{F}_2[x]/(x^3+x^2+x)\right)^\times \cong \left(\mathbb{F}_2[x]/(x)\right)^\times \times \left(\mathbb{F}_2[x]/(x^2+x+\bar{1})\right)^\times$$

Allgemein gilt: Ist $q > 1$ eine Primzahlpotenz und $f \in \mathbb{F}_q[x]$ ein Polynom vom Grad n, dann enthält der Ring $\mathbb{F}_q[x]/(f)$ genau q^n Elemente, weil durch $\{a_0 + a_1 x + \dots + a_{n-1}x^{n-1} \mid a_0, \dots, a_{n-1} \in \mathbb{F}_q\}$ ein Repräsentantensystem der Nebenkl. geg. ist.

$\Rightarrow |\mathbb{F}_2[x]/(x)| = 2, \quad |\mathbb{F}_2[x]/(x^2+x+\bar{1})| = 4$ (a)

Das Pol. x ist wg. $\operatorname{grad}(x) = 1$, ebenso $x^2+x+\bar{1}$ als nullstellenfreies Pol. vom Grad 2 $\Rightarrow$ (*)

(x), $(x^2+x+\bar{1})$ sind max. Ideale in $\mathbb{F}_2[x]$

$\Rightarrow \mathbb{F}_2[x]/(x)$, $\mathbb{F}_2[x]/(x^2+x+\bar{1})$ sind Körper.

Weil jedes Element ungleich null in einem Körper eine Einheit ist, gilt $|(\mathbb{F}_2[x]/(x))^\times| = 2-1 = 1$

und $|(\mathbb{F}_2[x]/(x^2+x+1))^\times| = 4-1 = 3$

$$\Rightarrow |(\mathbb{Z}[x]/(x^3+x+1))^\times| = |(\mathbb{F}_2[x]/(x))^\times| \cdot |(\mathbb{F}_2[x]/(x^2+x+\bar{1}))^\times|$$

$$= 1 \cdot 3 = 3$$

(c) Bestimmen Sie (mit Nachweis) das kleinste $n \in \mathbb{N}$ mit $n \equiv 1 \bmod 3$, $n \equiv 2 \bmod 5$, $n \equiv 0 \bmod 8$.

Da 3, 5 und 8 paarweise teilerfremd sind, kann der Chin. Restsatz angewendet werden. Demnach existiert ein eindeutig bestimmtes

$n \in \{0, 1, \ldots, 119\}$ mit $n \equiv 1 \bmod 3$, $n \equiv 2 \bmod 5$, $n \equiv 0 \bmod 8$.

Die einzigen Zahlen in $M = \{0, \ldots, 119\}$, die die dritte Kongruenz erfüllen, sind $\{8k \mid 0 \leq k \leq 14\}$.

Für alle $k \in \{0, \ldots, 14\}$ gilt die Äquivalenz $8k \equiv 2 \bmod 5$

$\Leftrightarrow 3k \equiv 2 \bmod 5 \Leftrightarrow (3+5\mathbb{Z})\cdot(k+5\mathbb{Z}) = 2+5\mathbb{Z}$

$\Leftrightarrow (2+5\mathbb{Z})(3+5\mathbb{Z})(k+5\mathbb{Z}) = 4+5\mathbb{Z} \Leftrightarrow k+5\mathbb{Z} = 4+5\mathbb{Z}$

$\uparrow 2+5\mathbb{Z} \in (\mathbb{Z}/5\mathbb{Z})^\times$ $\quad (2+5\mathbb{Z})(3+5\mathbb{Z}) = 1+5\mathbb{Z}$

$\Leftrightarrow k \equiv 4 \bmod 5 \Leftrightarrow k \in \{4, 9, 14\}$

einzige Zahlen, die die beiden letzten Kongr. erf.: $8\cdot 4 = 32$, $8\cdot 9 = 72$, $8\cdot 14 = 112$

$32 \equiv 2 \bmod 3$, $72 \equiv 0 \bmod 3$, $112 \equiv 1 \bmod 3$

$\Rightarrow$ 112 ist die einzige Zahl in $10, \dots, 1997$, die alle Kongruenzen erfüllt. Also ist dies die kleinste nat. Zahl mit dieser Eigenschaft. □

H25T2A4 Sei $f \in \mathbb{Z}[x]$ ein Polynom mit $f(1) = 1$, $f(2) = 2$.

(a) Zeigen Sie, dass für alle $a \in \mathbb{Z}$ mit $a \geq 3$ jeweils $f(a) \equiv 1 \bmod (a-1)$ $f(a) \equiv 2 \bmod (a-2)$ gilt

(*) Sei zusätzlich $f(10) > 10$ angenommen.
Zeigen Sie, dass $f(10) \geq 82$ gilt.

zu (a) $(a-1) \mid (a-1) \Rightarrow a \equiv 1 \bmod (a-1)$

ebenso: $(a-2) \mid (a-2) \Rightarrow a \equiv 2 \bmod (a-2)$

Allgemein gilt: Sind $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$ und ist $f \in \mathbb{Z}[x]$, dann folgt aus $a \equiv b \bmod n$ jeweils $f(a) \equiv f(b) \bmod n$. denn: Sei $\bar{f}$ das Bild von f in $(\mathbb{Z}/n\mathbb{Z})[x]$. $a \equiv b \bmod n$

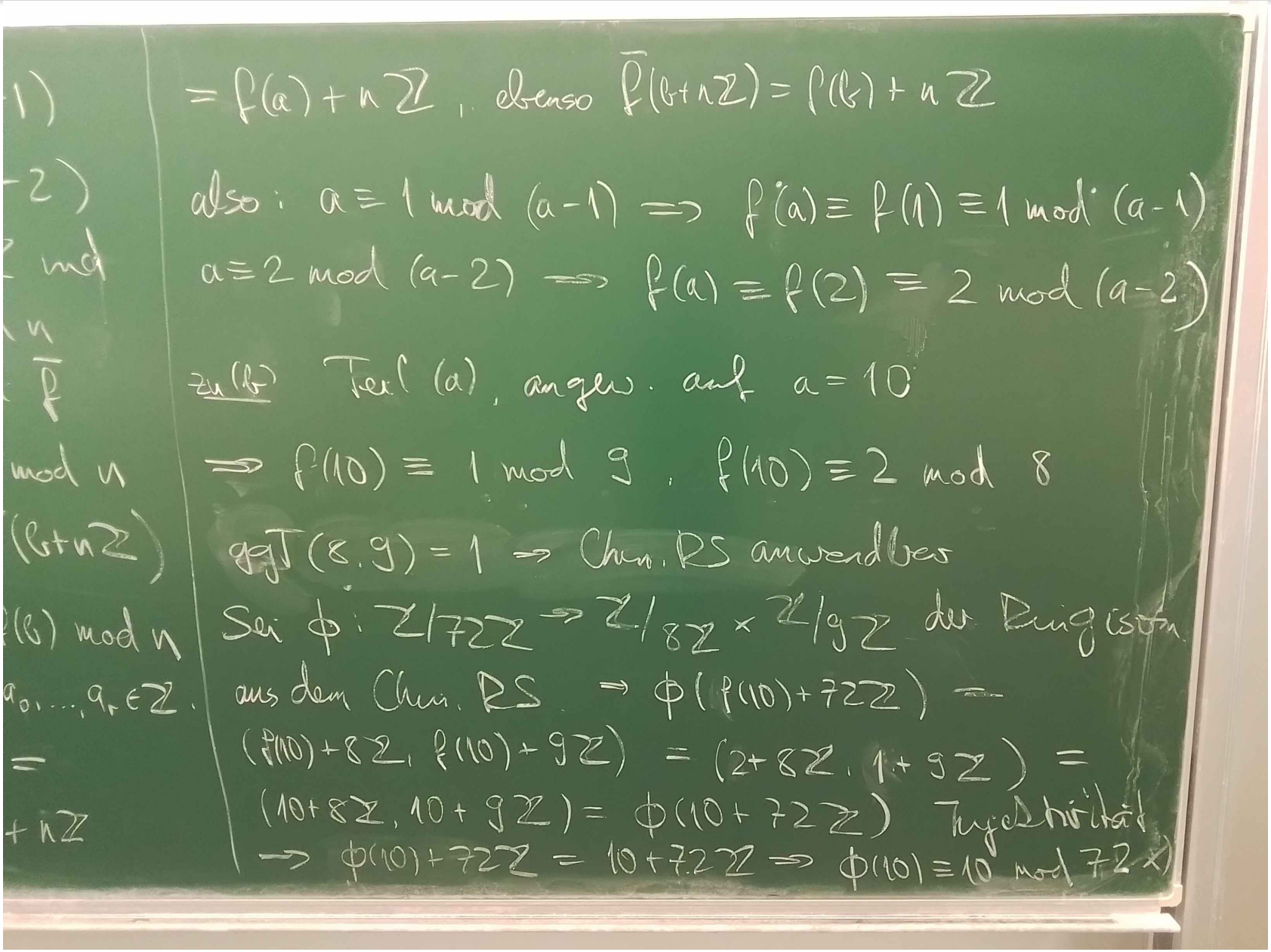
$\Rightarrow a + n\mathbb{Z} = b + n\mathbb{Z} \Rightarrow \bar{f}(a+n\mathbb{Z}) = \bar{f}(b+n\mathbb{Z})$

$\overset{(*)}{\Rightarrow} f(a) + n\mathbb{Z} = f(b) + n\mathbb{Z} \Rightarrow f(a) \equiv f(b) \bmod n$

(*) Sei $f = \sum_{k=0}^{r} a_k x^k$, mit $r \in \mathbb{N}_0$, $a_0, \dots, a_r \in \mathbb{Z}$.

$\Rightarrow \bar{f} = \sum_{k=0}^{r} (a_k + n\mathbb{Z}) x^k \Rightarrow \bar{f}(a+n\mathbb{Z}) =$

$\sum_{k=0}^{r} (a_k + n\mathbb{Z})(a+n\mathbb{Z})^k = \sum_{k=0}^{r} a_k a^k + n\mathbb{Z}$



Korrektur letzte Zeile:

$f(10) + 72\mathbb{Z} = 10 + 72\mathbb{Z} \;\Rightarrow\; f(10) \equiv 10 \mod 72.$

Es gibt also ein $m \in \mathbb{Z}$ mit $f(10) = 10 + 72m$. Wegen $f(10) > 10$ ist $m \geq 1$ und somit $f(10) \geq 10 + 72 \cdot 1 = 82$.