

§ 14. Kongruenzrechnung und Chinesischer Restsatz

Erinnerung: Seien $a, b \in \mathbb{Z}$ und $n \in \mathbb{N}$.

$a \equiv b \bmod n$ bedeutet: $n \mid (b - a)$

Proposition (14.1)

Seien $m, n \in \mathbb{N}$, außerdem $a, b, c, d \in \mathbb{Z}$ und p eine Primzahl.

- (i) Aus $a \equiv c \bmod n$ und $b \equiv d \bmod n$ folgt
 $a + b \equiv c + d \bmod n$ und $ab \equiv cd \bmod n$.
- (ii) Gilt $a \equiv b \bmod n$ und ist m ein Teiler von n ,
dann folgt $a \equiv b \bmod m$.
- (iii) Es gilt $a \equiv b \bmod n$ genau dann, wenn $ma \equiv mb \bmod mn$
erfüllt ist.
- (iv) Es gilt $a^p \equiv a \bmod p$. Unter der zusätzlichen Voraussetzung
 $p \nmid a$ gilt darüber hinaus $a^p \equiv 1 \bmod p$.

Die Aussage (iv) ist auch als **Kleiner Satz von Fermat** bekannt.

Definition (14.2)

Sei R ein Ring. Zwei Ideale I, J in R werden **teilerfremd** genannt, wenn $I + J = (1)$ gilt, wobei (1) wie üblich das Einheitsideal in R bezeichnet.

Lemma (14.3)

Sei $R = \mathbb{Z}$, und seien $m, n \in \mathbb{N}$. Genau dann sind die Ideale $I = (m)$ und $J = (n)$ teilerfremd, wenn m, n als natürliche Zahlen teilerfremd sind.

Beweis von Lemma 14.3

geg $m, n \in \mathbb{N}$, Beh. m, n teilerfremd

Die Ideale $I = (m)$
und $J = (n)$ sind
teilerfremd, d.h.
 $I + J = (1)$.

" $\Rightarrow$ " Lemma von Bézout $\Rightarrow \exists u, v \in \mathbb{Z}$

mit $um + vn = \text{ggT}(m, n) = 1$

$um \in I, vn \in J \Rightarrow 1 = um + vn \in I + J$

$\Rightarrow I + J = (1)$

" $\Leftarrow$ " Sei $d \in \mathbb{N}$ ein gem. Teiler von m und n .

z.zg.: $d = 1$ $I + J = (1) \Rightarrow 1 \in I + J \Rightarrow \exists a \in I,$

$b \in J$ mit $1 = a + b$ $a \in I \Rightarrow \exists u \in \mathbb{Z}$ mit $a = um$

$$\exists \in J \Rightarrow \exists r \in \mathbb{Z} \text{ mit } f = rn \Rightarrow 1 = um + rn$$

$$d|m, d|n \Rightarrow d|um, d|rn \Rightarrow d|(um+rn) \Rightarrow d|1$$

$$\Rightarrow d = 1$$



Lemma (14.4)

Sei R ein Ring, und seien $I_1, \dots, I_m, J$ Ideale in R , wobei $I_1, \dots, I_m$ jeweils teilerfremd zu J sind. Dann ist auch das Produkt $I_1 \cdot \dots \cdot I_m$ teilerfremd zu J .

Lemma (14.5)

Sei R ein Ring, und seien $I_1, \dots, I_m$ Ideale in R , die paarweise teilerfremd sind. Dann gilt

$$I_1 \cdot \dots \cdot I_m = I_1 \cap \dots \cap I_m.$$

Beweis von Lemma 14.4

geg. Ring R Ideale $I_1, \dots, I_m, J$ von R
 $I_1, \dots, I_m$ jeweils teilerfremd zu J

z.zg. $I_1 \cdot \dots \cdot I_m$ ist teilerfremd zu J

Beweis für $m=2$: Nach Vr. gilt $I_1 + J = (1)$ und $I_2 + J = (1)$. z.zg. $I_1 I_2 + J = (1)$

$$\begin{aligned} \text{Es gilt } (1) &= (1)(1) = (I_1 + J)(I_2 + J) \\ &= (I_1 + J)I_2 + (I_1 + J)J = \end{aligned}$$

$$I_1 I_2 + \underbrace{J I_2}_{\subseteq J} + \underbrace{I_1 J}_{\subseteq J} + \underbrace{J^2}_{\subseteq J} \subseteq I_1 I_2 + J$$

$$\Rightarrow 1 \in I_1 I_2 + J \Rightarrow I_1 I_2 + J = (1)$$

Sei nun $m \geq 2$, setze die Aussage für m voraus.
geg: $m+1$ zu J teilerfremde Ideale $I_1, I_2, \dots, I_{m+1}$

Ind. - V. $\Rightarrow I = I_1 \cdot \dots \cdot I_m$ teilerfremd zu J

Fall $m=2 \Rightarrow I \cdot I_{m+1} = I_1 \cdot \dots \cdot I_{m+1}$ ist teilerfremd zu J . $\square$

Beweis von Lemma 14.5

geg. Ring R , paarweise teilerfremde Ideale
 $I_1, I_2, \dots, I_m$ in R ($m \geq 2$)

$$\text{z.zg. } I_1 \cap \dots \cap I_m = I_1 \cdot \dots \cdot I_m$$

$$\text{Fall } m=2 \quad \text{z.zg. } I_1 I_2 = I_1 \cap I_2$$

$$\text{"} \subseteq \text{" } I_1 I_2 \subseteq I_1 \text{ und } I_1 I_2 \subseteq I_2 \Rightarrow$$

$$I_1 I_2 \subseteq I_1 \cap I_2$$

$$\text{"} \supseteq \text{" Sei } a \in I_1 \cap I_2 \quad I_1 + I_2 = (1)$$

$$\Rightarrow \exists b_1 \in I_1, b_2 \in I_2 \text{ mit } b_1 + b_2 = 1$$

$$\Rightarrow a = a \cdot 1 = a(b_1 + b_2) = \underbrace{ab_1}_{\in I_2 I_1} + \underbrace{ab_2}_{\in I_1 I_2}$$

$$\Rightarrow a \in I_1 I_2$$

Sei nun $m \geq 2$, setze die Aussage für m voraus

Seien $I_1, \dots, I_{m+1}$ ^(paarweise) teilerfremde Ideale von R

Setze $I = I_1 \cdots I_m$. Lemma 14.4 $\Rightarrow$

I teilerfremd zu I_{m+1} . Fall $m=2 \Rightarrow$

$$I \cdot I_{m+1} = I \cap I_{m+1} \quad \text{Ind} - V. \Rightarrow$$

$$I = I_1 \cap \dots \cap I_m \Rightarrow I_i \cdot I_{m+1} =$$

$$I \cdot I_{m+1} = I \cap I_{m+1} = I_1 \cap \dots \cap I_m \cap I_{m+1}.$$

□

Satz (14.6)

Sei R ein Ring, $I_1, \dots, I_m$ paarweise teilerfremde Ideale in R und $I = I_1 \cdot \dots \cdot I_m$. Dann gibt es einen **Isomorphismus** von Ringen

$$\bar{\phi} : R/I \longrightarrow (R/I_1) \times \dots \times (R/I_m)$$

mit

$$\bar{\phi}(a + I) = (a + I_1, \dots, a + I_m) \quad \text{für alle } a \in R.$$

Anwendungsbeispiel für den Chinesischen Restsatz:

Betrachte $R = \mathbb{Z}$, $I_1 = (2) = 2\mathbb{Z}$, $I_2 = (3)$, $I_3 = (5)$

Lt. dem Satz gibt es einen Isom. von Ringen

$$\Phi: \mathbb{Z}/30\mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$$

$$a+30\mathbb{Z} \mapsto (a+2\mathbb{Z}, a+3\mathbb{Z}, a+5\mathbb{Z})$$

Jedes Element von $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ liegt im

Bild von Φ , zum Beispiel auch $(1+2\mathbb{Z}, 2+3\mathbb{Z}, 4+5\mathbb{Z})$

4, 9, 14, 19, 24, 29

$$\begin{aligned}\Phi(29+30\mathbb{Z}) &= (29+2\mathbb{Z}, 29+3\mathbb{Z}, 29+5\mathbb{Z}) \\ &= (1+2\mathbb{Z}, 2+3\mathbb{Z}, 4+5\mathbb{Z})\end{aligned}$$

Beweis des Chinesischen Restsatzes

geg. $r \in \mathbb{N}$, $r \geq 2$, R Ring, $I_1, \dots, I_r$ paarweise teilerfremde Ideale, $I = I_1 \circ \dots \circ I_r$

z.zg.: Es existiert ein Isomorphismus von Ringen

$$\Phi: R/I \rightarrow R/I_1 \times \dots \times R/I_r \quad \text{mit} \quad \Phi(a+I) = (a+I_1, \dots, a+I_r) \\ \text{für alle } a \in R$$

Betrachte die Abbildung $\phi: R \rightarrow R/I_1 \times \dots \times R/I_r$,
 $a \mapsto (a+I_1, \dots, a+I_r)$. Um den Hom-Satz für Ringe anwenden zu können, müssen wir überprüfen

- (1) ϕ ist ein Ringhom (einfaches Nachrechnen)
- (2) $\ker(\phi) = I$
- (3) ϕ ist surjektiv

zu (2) Für jedes $a \in R$ gilt die Äquivalenz

$$\begin{aligned} a \in \ker(\phi) &\Leftrightarrow \phi(a) = (0+I_1, \dots, 0+I_r) \Leftrightarrow \\ (a+I_1, \dots, a+I_r) &= (0+I_1, \dots, 0+I_r) \Leftrightarrow a+I_k = I_k \\ \text{für } 1 \leq k \leq r &\Leftrightarrow a \in I_k \text{ für } 1 \leq k \leq r \Leftrightarrow \\ a \in I_1 \cap \dots \cap I_r &\stackrel{\text{Lemma 4.5}}{\Leftrightarrow} a \in I \end{aligned}$$

zu (3) Beweise die Surjektivität zunächst für $r=2$.

$$\begin{aligned} \text{Seien } a_1, a_2 \in R \text{ z.zg. } \exists a \in R : (a+I_1, a+I_2) &= \phi(a) = \\ (a_1+I_1, a_2+I_2). \quad I_1, I_2 \text{ teilerfremd} &\rightarrow 1 \in I_1 + I_2 \Rightarrow \\ \exists b_1 \in I_1, b_2 \in I_2 \text{ mit } b_1 + b_2 &= 1 \Leftrightarrow 1 - b_1 = b_2 \Leftrightarrow \\ 1 - b_2 = b_1 &\Rightarrow \phi(b_2) = (b_2+I_1, b_2+I_2) = (1-b_1+I_1, b_2+I_2) \end{aligned}$$

$$b_1 \in I_1 \\ \stackrel{=}{=} (1+I_1, 0+I_2) \quad \text{ebenso: } \phi(b_1) = \\ b_2 \in I_2$$

$$(b_1+I_1, b_1+I_2) = (b_1+I_1, 1-b_2+I_2) = (0+I_1, 1+I_2)$$

$$\text{Setze } a = a_1 \cdot b_2 + a_2 \cdot b_1 \Rightarrow \phi(a) =$$

$$\phi(a_1) \phi(b_2) + \phi(a_2) \phi(b_1) = (a_1+I_1, a_1+I_2) \cdot (1+I_1, 0+I_2) \\ + (a_2+I_1, a_2+I_2) \cdot (0+I_1, 1+I_2) = (a_1+I_1, 0+I_2) + \\ (0+I_1, a_2+I_2) = (a_1+I_1, a_2+I_2)$$

Zeige nun die Surjektivität durch vollständige Induktion für bel. $m \geq 2$. Der Induktionsanfang ist bereits erledigt. Sei $m \geq 2$, setze die Aussage für m voraus. Seien $I_1, \dots, I_{m+1}$ paarweise

$\mathbb{Z}$ teilerfremde Ideale von R und $a_1, \dots, a_{m+1} \in R$. z.zg:
 $\exists$ gibt ein $a \in R$ mit

$$(a + I_1, \dots, a + I_{m+1}) = (a_1 + I_1, \dots, a_{m+1} + I_{m+1})$$

$\mathbb{Z}$) Ind.-V. $\Rightarrow \exists$ gibt ein $a' \in R$ mit

$$(a' + I_1, \dots, a' + I_m) = (a_1 + I_1, \dots, a_m + I_m).$$

$\mathbb{Z}$ Sei $I' = I_1 \cdot \dots \cdot I_m$. Lemma 14.4 $\Rightarrow I'$ ist teilerfremd zu I_{m+1} . Fall $m=2 \Rightarrow \exists a \in R$ mit

$$(a + I', a + I_{m+1}) = (a' + I', a_{m+1} + I_{m+1})$$

$\dots, c_1 + n_1 \mathbb{Z}$) Beh.: $a + I_k = a_k + I_k$ für $1 \leq k \leq m$

$\dots, c_r + n_r \mathbb{Z}$) Sei $k \in \{1, \dots, m\}$ s.o. $\Rightarrow a + I_k = a_k + I_k$

außerdem: $a + I' = a' + I' \Rightarrow a - a' \in I' \subseteq I_k$
 $\Rightarrow a + I_k = a' + I_k = a_k + I_k$ $\square$

Satz (14.7)

Seien $r \in \mathbb{N}$ mit $r \geq 2$, außerdem $n_1, \dots, n_r \in \mathbb{N}$ paarweise teilerfremde natürliche Zahlen und $n = \prod_{j=1}^r n_j$. Seien $c_1, \dots, c_r \in \mathbb{Z}$. Dann ist die Lösungsmenge $\mathcal{L} \subseteq \mathbb{Z}$ des Kongruenzsystems

$$x \equiv c_1 \pmod{n_1} \quad , \quad x \equiv c_2 \pmod{n_2} \quad , \quad \dots \quad , \quad x \equiv c_r \pmod{n_r}$$

nicht leer. Ist $a \in \mathcal{L}$ beliebig gewählt, dann gilt $\mathcal{L} = a + n\mathbb{Z}$.

Beweis von Satz 14.7

geg. $r \geq 2$, $n_1, \dots, n_r \in \mathbb{N}$ paarweise teilerfremd, $c_1, \dots, c_r \in \mathbb{Z}$

Sei $L \subseteq \mathbb{Z}$ die Lösungsmenge des Kongruenzsystems

$$x \equiv c_1 \pmod{n_1}, \dots, x \equiv c_r \pmod{n_r}$$

z.zg. (i) $L \neq \emptyset$ (ii) $a \in L \Rightarrow L = a + n\mathbb{Z}$
wobei $n = n_1 \cdot \dots \cdot n_r$

Sei $\bar{\cdot} : \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_r\mathbb{Z}$

der Isomorphismus aus dem Chin. Restsatz.

zu li) Da $\bar{\phi}$ surjektiv ist, gibt es ein $a \in \mathbb{Z}$
mit $\bar{\phi}(a+n\mathbb{Z}) = (c_1+n_1\mathbb{Z}, \dots, c_r+n_r\mathbb{Z})$

$$\Rightarrow (a+n_1\mathbb{Z}, \dots, a+n_r\mathbb{Z}) = (c_1+n_1\mathbb{Z}, \dots, c_r+n_r\mathbb{Z})$$

$$\Rightarrow a+n_k\mathbb{Z} = c_k+n_k\mathbb{Z} \text{ für } 1 \leq k \leq r$$

$$\Rightarrow a \equiv c_k \pmod{n_k} \text{ für } 1 \leq k \leq r \Rightarrow a \in \mathcal{L}$$

$$\Rightarrow \mathcal{L} \neq \emptyset$$

zu lii) Sei $a \in \mathcal{L}$ beliebig, z.zg. $\mathcal{L} = a+n\mathbb{Z}$

" $\subseteq$ " Sei $a' \in \mathcal{L}$, z.zg. $a' \in a+n\mathbb{Z}$

$$\text{s.o. } a' \in \mathcal{L} \Rightarrow \bar{\phi}(a'+n\mathbb{Z}) = (c_1+n_1\mathbb{Z}, \dots, c_r+n_r\mathbb{Z})$$

$$\text{ebenso: } a \in \mathcal{L} \Rightarrow \bar{\phi}(a+n\mathbb{Z}) = (c_1+n_1\mathbb{Z}, \dots, c_r+n_r\mathbb{Z})$$

$$\Rightarrow \bar{\phi}(a'+n\mathbb{Z}) = \bar{\phi}(a+n\mathbb{Z}) \xrightarrow[\text{injektiv}]{\text{Chin. RS}} \bar{\phi}$$

$$a'+n\mathbb{Z} = a+n\mathbb{Z} \Rightarrow a' \in a+n\mathbb{Z}$$

" $\supseteq$ " Sei $a' \in a + n\mathbb{Z}$. $\Rightarrow a' + n\mathbb{Z} = a + n\mathbb{Z} \Rightarrow$

$$\bar{\phi}(a' + n\mathbb{Z}) = \phi(a + n\mathbb{Z}) \stackrel{a \in L}{=} (c_1 + n_1\mathbb{Z}, \dots, c_r + n_r\mathbb{Z})$$

$$\Rightarrow a' \in L$$

□

Berechnung einer Lösung eines Kongruenzsystems

Seien $m, n \in \mathbb{N}$ teilerfremd und $c, d \in \mathbb{Z}$. Gesucht wird eine Lösung des Systems $x \equiv c \pmod{m}$, $x \equiv d \pmod{n}$.

- (1) Bestimme mit Hilfe des Euklidischen Algorithmus Zahlen $u, v \in \mathbb{Z}$ mit $um + vn = \text{ggT}(m, n) = 1$.
- (2) Berechne $a_1 = 1 - um = vn$ und $a_2 = 1 - a_1$.
- (3) Setze $a = ca_1 + da_2$. Dies ist eine Lösung des Systems. Die gesamte Lösungsmenge ist gegeben durch $\mathcal{L} = a + mn\mathbb{Z}$.

Satz (14.8)

Seien $m, n \in \mathbb{N}$ und $a, b \in \mathbb{Z}$. Wir betrachten die Lösungsmenge $\mathcal{L} \subseteq \mathbb{Z}$ des Kongruenzsystems

$$x \equiv a \bmod m \quad , \quad x \equiv b \bmod n.$$

- (i) Es gilt $\mathcal{L} \neq \emptyset$ genau dann, wenn $a \equiv b \bmod d$ erfüllt ist, mit $d = \text{ggT}(m, n)$.
- (ii) Sei $\ell \in \mathbb{Z}$ mit $b = a + \ell d$, außerdem $m' = \frac{m}{d}$ und $n' = \frac{n}{d}$. Sei c eine Lösung des Systems $x \equiv 0 \bmod m'$, $x \equiv \ell \bmod n'$. Dann ist die Lösungsmenge des ursprünglichen Systems gegeben durch $\mathcal{L} = a + dc + \text{kgV}(m, n)\mathbb{Z}$.

Satz (14.9)

Seien $m, n \in \mathbb{N}$ teilerfremd und $f \in \mathbb{Z}[x]$. Es bezeichne $\mathcal{N}$ die Menge der Nullstellen von f in $\mathbb{Z}/(mn)\mathbb{Z}$, und $\mathcal{N}_m$ bzw. $\mathcal{N}_n$ die Menge der Nullstellen von f in $\mathbb{Z}/m\mathbb{Z}$ bzw. $\mathbb{Z}/n\mathbb{Z}$. Dann existiert eine **Bijektion**

$$\psi : \mathcal{N} \rightarrow \mathcal{N}_m \times \mathcal{N}_n$$

mit $\psi(a + mn\mathbb{Z}) = (a + m\mathbb{Z}, a + n\mathbb{Z})$ für alle $a \in \mathbb{Z}$ mit $a + mn\mathbb{Z} \in \mathcal{N}$.

Anwendungsbeispiel: Bestimmung der Lösungen von
 $x^2 - x = \bar{0}$ in $\mathbb{Z}/35\mathbb{Z}$

1. Bestimmung der Lösungsmengen N_5, N_7 in $\mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z}$
und $\mathbb{F}_7 = \mathbb{Z}/7\mathbb{Z}$. Da $\mathbb{F}_5, \mathbb{F}_7$ Körper sind, sind
 N_5, N_7 jeweils höchstens zweielementig. Wegen $x^2 - x = x(x-1)$
gilt $N_5 = \{\bar{0}, \bar{1}\} \subseteq \mathbb{F}_5, N_7 = \{\bar{0}, \bar{1}\} \subseteq \mathbb{F}_7. \Rightarrow$
 $N_5 \times N_7 = \{(\bar{0}, \bar{0}), (\bar{1}, \bar{0}), (\bar{0}, \bar{1}), (\bar{1}, \bar{1})\}.$

2. Bestimmung der vzer Urbilder unter dem Isom. $\psi: \mathbb{Z}/35\mathbb{Z} \Rightarrow$
 $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}, (a+35\mathbb{Z}) \mapsto (a+5\mathbb{Z}, a+7\mathbb{Z}).$

Satz 14.9 $\Rightarrow N_{35} = \{\bar{0}, \bar{21}, \bar{15}, \bar{1}\}$