Der Chinesische Restsatz

Satz (14.6)

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

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

mit

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

Lösbarkeit von Kongruenzsystemen

Satz (14.7)

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

$$x \equiv c_1 \bmod n_1 \quad , \quad x \equiv c_2 \bmod n_2 \quad , \quad ... \quad , \quad x \equiv c_r \bmod n_r$$

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

Anwendungsbeispiel zu Satz 14.7

ges.: Lösungsmenge des Systems

$x \equiv 0 \bmod 2,\ x \equiv 2 \bmod 3,\ x \equiv 3 \bmod 5$

Es ist $2 \cdot 3 \cdot 5 = 30$ (und 2, 3, 5 sind paarw. teilerfremd)

Bestimme zunächst eine Lösung $a \in \mathbb{Z}$ mit $0 \leq a < 30$.

Lösungen von $x \equiv 3 \bmod 5$: 3, 8, 13, 18, 23, 28

darunter Lösungen von $x \equiv 2 \bmod 3$: 8, 23

darunter einzige Lsg. von $x \equiv 0 \bmod 2$: 8

Nach Satz 14.7 ist die gesamte Lösungsmenge des Systems in $\mathbb{Z}$ geg. durch $L = 8 + 30\mathbb{Z}$

Berechnung einer Lösung eines Kongruenzsystems

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

(1) Bestimme mit Hilfe des Euklidischen Algorithmus Zahlen $u, v \in \mathbb{Z}$ mit $um + vn = \mathrm{ggT}(m, n) = 1$.

(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 $\mathcal{L} = a + mn\mathbb{Z}$.

Beispiel zum allgemein Lösungsverfahren

ges: Lösungsmenge von $x \equiv 15 \bmod 59$, $x \equiv 20 \bmod 73$

Es ist $ggT(59, 73) = 1$ (da 59, 73 Primzahlen sind)

und $59 \cdot 73 = 4307$

Bestimme mit dem Erw. Alg. Zahlen $u, v \in \mathbb{Z}$ mit $59u + 73v = 1$

q	a_n	x_n	y_n
–	73	1	0
–	59	0	1
1	14	1	-1
4	3	-4	5
4	2	17	-21
1	1	-21	26

Ergebnis: $u = 26$, $v = -21$

$a_1 - 59u = -1533$, $a_2 = 1 - a_1 = 1534$

$a = 15a_1 + 20a_2 = 7685$

$a \equiv 3378 \bmod 4307$

Die Lösungsmenge des Systems ist also $\mathcal{L} = 3378 + 4307\mathbb{Z}$

Lösungen im nicht-teilerfremden Fall

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 $\mathcal{L} \neq \varnothing$ genau dann, wenn $a \equiv b \bmod d$ erfüllt ist, mit $d = \mathrm{ggT}(m, n)$.

(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 $\mathcal{L} = a + dc + \mathrm{kgV}(m, n)\mathbb{Z}$.

Lösungen von Polynomgleichungen

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

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

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 zu Satz 14.9:

Bestimmung der Nullstellen von $f = x^2 - x \in \mathbb{Z}[x]$
im Restklassenring $\mathbb{Z}/35\mathbb{Z}$ $(35 = 5 \cdot 7)$

Da 5, 7 Primzahlen sind und $\operatorname{grad}(f) = 2$,
sind die Nullstellenmengen N_5, N_7 in $\mathbb{Z}/5\mathbb{Z}$
bzw. $\mathbb{Z}/7\mathbb{Z}$ zweielementig. Offenbar ist
$N_5 = \{0+5\mathbb{Z}, 1+5\mathbb{Z}\}$, $N_7 = \{0+7\mathbb{Z}, 1+7\mathbb{Z}\}$.
Nach Satz 14.9 sind die Elemente von N_{35}
die Urbilder von $(0+5\mathbb{Z}, 0+7\mathbb{Z})$, $(0+5\mathbb{Z}, 1+7\mathbb{Z})$,
$(1+5\mathbb{Z}, 0+7\mathbb{Z})$, $(1+5\mathbb{Z}, 1+7\mathbb{Z})$ unter der Abb.

$\varphi: \mathbb{Z}/35\mathbb{Z} \to \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}, \; a+35\mathbb{Z} \mapsto (a+5\mathbb{Z}, a+7\mathbb{Z})$

Dies sind $0+35\mathbb{Z}, 15+35\mathbb{Z}, 21+35\mathbb{Z}, 1+35\mathbb{Z}$.

(72) Beweis von Satz 14.9

geg: $m, n \in \mathbb{N}$ teilerfremd. $f = \sum_{k=0}^{r} a_k x^k \in \mathbb{Z}[x]$
mit $r \in \mathbb{N}_0$. $a_0, a_1, \ldots, a_r \in \mathbb{Z}$.

N_a = Nullstellenmenge von f in $\mathbb{Z}/a\mathbb{Z}$
für $a \in \{m, n, mn\}$

Sei $\varphi: \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ der Ringhom. aus dem Chin. Restsatz.

Beh: $\varphi | N_{mn}$ liefert eine Bij. $N_{mn} \to N_m \times N_n$.

Sei $a \in \mathbb{Z}$ mit $a + mn\mathbb{Z} \in N_{mn}$, und seien
$b, c \in \mathbb{Z}$ mit $\varphi(a + mn\mathbb{Z}) = (b + m\mathbb{Z}, c + n\mathbb{Z})$
Es gilt $f(b + m\mathbb{Z}, c + n\mathbb{Z}) = f(\varphi(a + mn\mathbb{Z}))$

$$= \sum_{k=0}^{r} \underbrace{(a_k + m\mathbb{Z}, a_k + n\mathbb{Z})}_{\text{Bild von } a_k \text{ in } \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}} \psi(a + mn\mathbb{Z})$$

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

$$= \sum_{k=0}^{r} \varphi(a_k a^k + mn\mathbb{Z}) = \varphi\left(\sum_{k=0}^{r} a_k a^k + mn\mathbb{Z}\right)$$

$$= \varphi(f(a + mn\mathbb{Z})) = \varphi(0 + mn\mathbb{Z}) = (0 + m\mathbb{Z}, 0 + n\mathbb{Z})$$

$\uparrow\ a + mn\mathbb{Z} \in V_{mn}$

$(f(b + m\mathbb{Z}), f(c + mn\mathbb{Z})) = f(b + m\mathbb{Z}, c + n\mathbb{Z}) =$

$(0 + m\mathbb{Z}, 0 + n\mathbb{Z}) \Rightarrow b + m\mathbb{Z} \in V_m,\ c + n\mathbb{Z} \in V_n$

$\Rightarrow \varphi(V_{mn}) \subseteq V_m \times V_n.$

noch zzg: $\varphi|_{\mathbb{N}_{mn}} : \mathbb{N}_{mn} \to \mathbb{N}_m \times \mathbb{N}_n$ ist Bijektiv

(1) Injektivität: klar, da die Einschränkung einer injektiven Abbildung injektiv ist

(2) Surjektivität: Sei $(b+m\mathbb{Z}, c+n\mathbb{Z}) \in \mathbb{N}_m \times \mathbb{N}_n$.

Chin. Restsatz $\Rightarrow \exists a \in \mathbb{Z}$ mit $\varphi(a+mn\mathbb{Z}) = (b+m\mathbb{Z}, c+n\mathbb{Z})$.

$\varphi(f(a+mn\mathbb{Z})) = f(b+m\mathbb{Z}, c+n\mathbb{Z}) = (f(b+m\mathbb{Z}), f(c+n\mathbb{Z}))$

$= (0+m\mathbb{Z}, 0+n\mathbb{Z}) = \varphi(0+mn\mathbb{Z})$ ($\leftarrow$ siehe oben; φ injektiv $\Rightarrow$)

$f(a+mn\mathbb{Z}) = 0+mn\mathbb{Z} \Rightarrow a+mn\mathbb{Z} \in \mathbb{N}_{mn}$ Also wird $(b+m\mathbb{Z}, c+n\mathbb{Z})$ durch $\varphi|_{\mathbb{N}_{mn}}$ getroffen. □

Ringisomorphismen und Einheiten

Lemma (14.10)

Seien R und S Ringe. Dann gilt

(i) $(R \times S)^\times = R^\times \times S^\times$

(ii) Ist $\phi : R \to S$ ein Isomorphismus von Ringen, dann gilt $\phi(R^\times) = S^\times$. Insbesondere sind die Einheitengruppen $R^\times$ und $S^\times$ also isomorph.

Proposition (14.11)

Sind m, n teilerfremd und $m, n \geq 2$. Dann gilt für die Eulersche φ-Funktion die Rechenregel $\varphi(mn) = \varphi(m)\varphi(n)$.

Der Exponent einer Gruppe

Der Exponent $\exp(G)$ einer Gruppe G ist die kleinste Zahl $n \in \mathbb{N}$ mit der Eigenschaft $g^n = e$ für alle $g \in G$. Existiert keine natürliche Zahl mit dieser Eigenschaft, dann setzt man $\exp(G) = +\infty$.

Proposition (14.12)

Sei G eine endliche abelsche Gruppe vom Exponenten n. Dann existiert in G ein Element der Ordnung n.

Beweis von Proposition 14.12.

geg: $n \in \mathbb{N}$, G endliche abelsche Gruppe, $d = \exp(G)$

Beh: Es gibt in G ein Element der Ordnung d.

Hauptsatz über endl. abelsche Gruppen $\Rightarrow$

o.B.d.A. $G = \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_r\mathbb{Z}$, wobei $r \in \mathbb{N}_0$ und $n_1, \dots, n_r \in \mathbb{N}$. Sei $l = \mathrm{kgV}(n_1, \dots, n_r)$.

Beh. $l = d$ zzg: l ist minimal mit $l(a_1 + n_1\mathbb{Z}, \dots, a_r + n_r\mathbb{Z}) \overset{(*)}{=} (0 + n_1\mathbb{Z}, \dots, 0 + n_r\mathbb{Z})$ $\forall a_1, \dots, a_r \in \mathbb{Z}$ (*)

Offenbar erfüllt l diese Gleichung für beliebig vorgeg. $a_1, \dots, a_r \in \mathbb{Z}$, wegen $l(a_j + n_j\mathbb{Z}) = la_j + n_j\mathbb{Z} \overset{n_j \mid l}{=}$

$\overset{(*)}{=} (0+n_1\mathbb{Z}, \ldots, 0+n_r\mathbb{Z}) \quad \forall a_1, \ldots, a_r \in \mathbb{Z}. \quad (*)$

Also erfüllt l diese Gleichung für beliebig vorgeg.

$0+n_j\mathbb{Z}$ für $1 \leq j \leq r$. Sei nun $m \in \mathbb{N}$ beliebig vorgeg.

mit $(*)$. $\Rightarrow$ insb. $m(1+n_1\mathbb{Z}, \ldots, 1+n_r\mathbb{Z}) = (0+n_1\mathbb{Z}, \ldots, 0+n_r\mathbb{Z})$

$\Rightarrow m+n_j\mathbb{Z} = 0+n_j\mathbb{Z}$ für $1 \leq j \leq r \Rightarrow m \in n_j\mathbb{Z}$ für $1 \leq j \leq r$

$\Rightarrow n_j \mid m$ für $1 \leq j \leq r \Rightarrow l = \operatorname{kgV}(n_1, \ldots, n_r)$ teilt m

Also ist l minimal mit der Eigenschaft $(*)$.

Außerdem zeigt die Rechnung, dass $(1+n_1\mathbb{Z}, \ldots, 1+n_r\mathbb{Z})$ in G ein Element der Ordnung l ist. $\square$

Existenz von Primitivwurzeln

Satz (14.13)

Sei K ein Körper und U eine endliche Untergruppe der multiplikativen Gruppe $K^\times$. Dann ist U zyklisch. Insbesondere ist die multiplikative Gruppe eines endlichen Körpers immer eine zyklische Gruppe.

Folgerung (14.14)

Ist p eine Primzahl, dann gilt $(\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$.

Eine Zahl $a \in \mathbb{Z}$ mit der Eigenschaft $(\mathbb{Z}/p\mathbb{Z})^\times = \langle a + p\mathbb{Z} \rangle$ wird Primitivwurzel modulo p genannt.

Beweis von Satz 14.13:

geg.: Körper K, endl. Untergr. $U \leq K^\times$

Sei $d = \exp(U)$ und $n = |U|$.

Es genügt z.zg., dass $d = n$ ist, denn

nach Prop. 14.12 existiert dann in U ein

Element der Ordnung n. und ein solches

Element a erfüllt dann $\langle a \rangle = U$.

Da die Ordnungen der Gruppenelemente

stets die Gruppenordn. teilen, gilt

$u^n = 1 \quad \forall u \in U \quad \Rightarrow \quad d \leq n$

Sei $f = x^d - 1 \in K[x]$. $u^d = 1 \ \forall u \in U$

$\Rightarrow$ Jedes $u \in U$ ist Nullstelle von f. Da f (als Pol. vom Grad d über einem Körper höchstens d Nullstellen hat, folgt $n = |U| \leq d$.

Insgesamt gilt also $d = n$.

□

Anwendungsbeispiel: Struktur von $(\mathbb{Z}/15\mathbb{Z})^\times$

Es gilt $(\mathbb{Z}/15\mathbb{Z})^\times \overset{\text{Chin. RS}}{\cong} (\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/5\mathbb{Z})^\times$

$\overset{3,5 \text{ prim}}{=}$ $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ (nicht zyklisch)

Folgerung 14.14

$\text{ggT}(3,5) = 1$

Beispiel: Bestimmung einer Primitivwurzel mod 43

Folgerung 14.14 $\Rightarrow$ $\exists\, \bar{a} \in (\mathbb{Z}/43\mathbb{Z})^\times$ von Ordnung 42,

d.h. eine Primitivwurzel modulo 43 existiert

Teste $\bar{a} = 2 + 43\mathbb{Z} \in (\mathbb{Z}/43\mathbb{Z})^\times$

Erinnerung: Gilt $\bar{a}^{42} = \bar{1}$ und $\bar{a}^{42/p} \neq \bar{1}$ für jeden

teste $a = 2 + 43\mathbb{Z} \in (\mathbb{Z}/43\mathbb{Z})^*$

Primitivwurzel $p = 43$, $42 = 2 \cdot 3 \cdot 7$, dann folgt $\operatorname{ord}(\bar{a}) = 42$

zu überprüfen also: $\bar{a}^{42} = \bar{1}$, $\bar{a}^{21}, \bar{a}^{14}, \bar{a}^{6} \neq \bar{1}$

$\bar{a}^{42} = \bar{1}$ ist immer erfüllt, da $|(\mathbb{Z}/43\mathbb{Z})^*| = 42$

aber: $\bar{a}^1 = \bar{2}$, $\bar{a}^2 = \bar{4}$, $\bar{a}^4 = \bar{16}$, $\bar{a}^8 = (\bar{a}^4)^2 = \overline{256} = \overline{41} = -\bar{2}$

$\Rightarrow \bar{a}^{14} = \bar{a}^{8+4+2} = \bar{a}^8 \cdot \bar{a}^4 \cdot \bar{a}^2 = (-\bar{2}) \cdot \bar{16} \cdot \bar{4}$

$= (-\bar{32}) \cdot \bar{4} = \bar{11} \cdot 4 = \bar{44} = \bar{1}$

$\rightarrow$ 2 ist keine Primitivwurzel modulo 43

aber: $\bar{3}^{21} = \bar{42} \neq \bar{1}$, $\bar{3}^{14} = \bar{36} \neq \bar{1}$, $\bar{3}^{6} = \bar{41} \neq \bar{1}$

$\Rightarrow$ 3 ist Primitivwurzel modulo 43