

3 Kongruenzen und Restklassenringe

In diesem Kapitel betrachten wir entweder $R = \mathbb{Z}$ oder $R = K[X]$, wobei K ein Körper ist.

Grundbegriffe

In den betrachteten Ringen gibt es eine eindeutige Restwahl: In $R = \mathbb{Z}$ ist die Division mit Rest $a = qm + r$ mit $0 \leq r < |m|$. Andere Restwahl wäre etwa $a = qm + r'$ mit $-\frac{|m|}{2} < r' \leq \frac{|m|}{2}$. Es besteht folgender Zusammenhang:

$$r' = \begin{cases} r, & 0 \leq r \leq \frac{|m|}{2} \\ r - |m|, & \frac{|m|}{2} < r \leq |m| \end{cases}$$

In $R = K[X]$ haben wir $a = qm + r$ mit $\text{grad } r < \text{grad } m$.

Diese Reste sind eindeutig: Haben wir $a = qm + r = \tilde{q}m + \tilde{r}$ mit $0 \leq r, \tilde{r}, |m|$. Dann ist $(q - \tilde{q})m = \tilde{r} - r \implies |m| \mid \tilde{r} - r$. Annahme: $q - \tilde{q} \neq 0 \implies |\tilde{r} - r| \geq |m|$, Wid. Also ist $q = \tilde{q}$ und $r = \tilde{r}$. Der Beweis für $R = K[X]$ funktioniert ähnlich.

Definition (Gauß für $R = \mathbb{Z}$)

$m, a, b, \in R$

(1)

$$a \equiv b \pmod{m} \text{ (lies } a \text{ kongruent } b \text{ modulo } m)$$

$$\iff a \pmod{m} = b \pmod{m}$$

Gauß schreibt „Zwei Zahlen heißen kongruent mod m , wenn sie bei Division durch m den selben Rest lassen.“

(2) $\bar{a} := \{b \in R \mid b \equiv a \pmod{m}\}$ heißt Restklasse modulo m .

(3) $\bar{R} := R/mR := \{\bar{a} \mid a \in R\}$ heißt Restklassenring modulo m .

Warum ist Letzteres ein „Ring“? Der Dozent führt einen schönen Beweis durch Aufwickeln einer Schnur auf einer Tesa-Rolle durch.

Beispiel

$\mathbb{Z}/2\mathbb{Z} = \{\bar{0}, \bar{1}\}$ mit $\bar{0} = \{0, \pm 2, \pm 4, \dots\}$ (die geraden Zahlen) und $\bar{1} = \{\pm 1, \pm 3, \dots\}$ (die ungeraden Zahlen). Aus der Schule sind folgende Regeln bekannt:

(1) $\bar{0} + \bar{0} = \bar{0}$, „gerade + gerade = gerade“

(2) $\bar{0} + \bar{1} = \bar{1}$, „gerade + ungerade = ungerade“

$$(3) \quad \overline{1} + \overline{1} = \overline{0}, \text{ „ungerade} + \text{ungerade} = \text{gerade“}$$

Bemerkung:

$$(i) \ a \equiv b \pmod{m} \iff (ii) \ \overline{a} = \overline{b} \iff (iii) \ m|a - b$$

Merke: Kongruenz ist Gleichheit der Restklassen.

$\overline{qm} = \overline{0}$. Die Idee: In \overline{R} wird alles durch m teilbare als „unwesentlich“ angesehen und durch 0 ersetzt.

Beweis

(i) \iff (ii): Kongruenz mod m ist offensichtlich eine Äquivalenzrelation auf R . \overline{a} ist die Äquivalenzklasse von a . Lineare Algebra: Zwei Elemente sind genau dann äquivalent, wenn die zugehörigen Äquivalenzklassen überstimmen.

$$(i) \implies (iii): r = a \pmod{m} = b \pmod{m} \implies a = qm + r, b = q'm + r \text{ (Division mit Rest)} \\ \implies a - b = (q - q')m \implies m|a - b \quad \blacksquare$$

Um mit Restklassen zu rechnen, brauchen wir folgende Definitionen:

Definition

Jedes $b \in \overline{a}$ heißt Vertreter der Klasse $\overline{a} \in \overline{R}$. Die Idee ist, die Operationen $+$ und \cdot vertreterweise zu definieren. Wir haben also:

$$(\overline{R}, +, \cdot) \text{ mit } \overline{a} + \overline{b} := \overline{a + b}, \overline{a} \cdot \overline{b} = \overline{a \cdot b}$$

Zu zeigen: Die Definition ist vertreterunabhängig, also: $\overline{a} = \overline{a'} \implies \overline{a + b} = \overline{a' + b}$ und $\overline{a \cdot b} = \overline{a' \cdot b}$. Das ist klar:

$$\overline{a} = \overline{a'} \iff m|a - a' = a + b - (a' + b) \implies \overline{a + b} = \overline{a' + b} \\ m|a - a' \implies m|(a - a')b = ab - a'b \implies \overline{ab} = \overline{a'b}$$

Bemerkung: $e \in R^\times, m \in R \implies R/mR = R/emR$ (da $m|x \iff em|x$). Ohne Beschränkung der Allgemeinheit kann man m also normiert annehmen.

$m = 0$, dann $a \pmod{m} = b \pmod{m} \iff a = b$, also $\overline{a} = \{a\}$, „ a “. Also: $R/oR = R$ und $R/eR = R/R = \{\overline{0}\}$ („Nullring“)

Diese uninteressanten Fälle werden meist beiseite gelassen.

Satz 3.1 (Restklassenring-Satz)

Sei R ein euklidischer Ring, $m \in R$.

(1) $(\overline{R} = R/mR, +, \cdot)$ ist ein Ring

(2) $\overline{R}^\times = \{\overline{a} \in \overline{R} \mid \text{ggT}(a, m) = 1\}$

Zusatz: Zu $\overline{a} \in \overline{R}^\times$. Kann \overline{a}^{-1} effektiv mit Euklids Algorithmus berechnet werden.

Definition

$\bar{a} \in \bar{R}^\times$ heißt eine prime Restklasse modulo m , \bar{R}^\times heißt prime Restklassengruppe modulo m .
(Sprachlich besser wäre eigentlich: Gruppe der zu m relativ primen Restklassen)

Beweis

- (1) Alle Ringaxiome vererben sich von den Vertretern auf die Klassen. $\bar{a} + \bar{b} = \overline{a + b} = \overline{b + a} = \bar{b} + \bar{a} \implies (\bar{R}, +)$ ist kommutativ. $0 := 0_{\bar{R}} = \bar{0}$, da $\bar{a} + \bar{0} = \overline{a + 0} = \bar{a}$. $1_{\bar{R}} = \bar{1}$ ebenso.

Assoziativität der Addition: $(\bar{a} + \bar{b}) + \bar{c} = \overline{a + b + c} = \overline{(a + b) + c} = \overline{a + (b + c)} = \bar{a} + \overline{b + c} = \bar{a} + (\bar{b} + \bar{c})$, Assoziativität der Multiplikation und Distributivgesetz analog.

- (2) $\bar{a} \in \bar{R}^\times \xLeftrightarrow{\text{Def.}} \exists x \in R : \bar{x}\bar{a} = 1_{\bar{R}} = \bar{1} \iff 1 \equiv ax \pmod{m} \iff \exists q \in R : 1 = ax + qm \implies \text{ggT}(a, m) = 1$, (da normal).

Der LinKom-Satz 1.10 liefert: $d = \text{ggT}(a, m) \implies \exists x, y \in R : d = ax + by$. Diesen Satz dürfen wir anwenden, da R euklidisch ist. Wir wenden ihn mit $d = 1, q = y$ an und erhalten $1 = ax + qm$, wobei x durch Euklids Algorithmus geliefert wird. $\implies \bar{1} = \bar{a}\bar{x} + \bar{q}\bar{m} = \bar{a}\bar{x}$.
Resultat: $\bar{a}^{-1} = \bar{x}$ mit dem so berechnetem x . ■

Folgerung 3.2

Ist $m \in \mathbb{N}_+$, dann gilt für Eulers Funktion φ :

$$\varphi(m) = \#\{R/mR\}^\times$$

Der Grund ist dass $R/mR = \{\bar{0}, \dots, \overline{m-1}\}$ und $(R/mR)^\times = \{\bar{r} | 0 \leq r < m, \text{ggT}(r, m) = 1\}$, derer es $\varphi(m)$ gibt.

Im Allgemeinen ist \bar{R} nicht integer. Beispielsweise in $\mathbb{Z}/4\mathbb{Z} = \bar{R}$ gilt: $\bar{2} \cdot \bar{2} = \bar{4} = 0_{\bar{R}} = 0$, aber $\bar{2} \neq 0$

Folgerung 3.3

Falls m unzerlegbar (also m Primzahl oder -polynom). Dann gilt: R/mR ist ein Körper.

Speziell:

- (1) $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$, $p \in \mathbb{P}$ ist Körper mit p Elementen.
(2) Ist $f \in K[X]$, f irreduzibel, so ist $K[X]/f \cdot K[X] = \bar{R}$ ein Körper.

Grund: m sei unzerlegbar. Dann $\bar{a} \in \bar{R}$, $\bar{a} \neq 0 = \bar{0} \iff m \nmid a \implies \text{ggT}(m, a) = 1$ ($1, m$ sind die einzigen normierten Teiler von $m!$) $\implies a \in \bar{R}^\times$. Es gilt also $\bar{R}^\times = \bar{R} \setminus \{0\} \implies \bar{R}$ ist Körper.

$\bar{R} = R/mR \ni \bar{a} = a + Rm := \{a + qm | q \in R\}$ Restklasse von a .

Rechne in \bar{R} : **Idee:** Kodiere die Restklasse \bar{a} durch den Vertreter $a \pmod{m}$.

Beliebige Vertretersysteme (ohne Einschränkung $m \in \mathbb{N}_+, m > 1$)

$\underline{R} = \mathbb{Z}$:

$\text{Versys}_m = \{0, 1, \dots, m-1\}$ „System Betrag kleinster positiven Reste“ oder $\text{Versys}_m = \{v \in \mathbb{Z} | -\frac{m}{2} < v \leq \frac{m}{2}\}$ „Symmetrisches Restsystem“

$$\begin{aligned} R &= K[X]: \\ \text{Versys}_m &= \{f \in K[X] \mid \text{Grad } f < \text{Grad } m\} \quad (\text{Grad } m > 0) \end{aligned}$$

Klar:

$$\begin{aligned} \text{Versys}_m &\longrightarrow R/mR \quad (\text{Ist bijektiv}) \\ r &\longmapsto \bar{r} \\ a &\longmapsto \bar{a} \quad \text{mod } m \quad (\text{Umkehrung}) \end{aligned}$$

Transportiere die Struktur $(\text{Versys}_m, \oplus, \odot)$, wobei gilt:

$$r \oplus s := r + s \quad \text{mod } m \quad r \odot s := rs \quad \text{mod } m$$

Klar, $r \mapsto \bar{r}$ ist ein Ringisomorphismus.

Vorzug bei $R = \mathbb{Z}$:

$r + s \quad \text{mod } m$ mit 1-Addition: Zahlen $< 2m$

$r \cdot s$: Zahlen $< m^2$

$(m \quad \text{mod } \frac{m^2}{4})$ bei symmetrischen Resten)

Vorzug bei $R = K[X]$:

Ist $n = \text{Grad } f$, so ist Versys_m ein K -Vektorraum der Dimension n (Basis z.B.: $1, X, X^2, \dots, X^{n-1}$)

$$\text{Grad } f < m, \text{Grad } g < m \implies \text{Grad } (f + g) < m \implies f \oplus g = f + g \implies \oplus = +$$

Versys_m enthält K als Teilkörper (konstante Polynome), da:

$$\alpha, \beta \in K \subset K[X] \implies \alpha \odot \beta = \alpha\beta \quad \text{mod } m = \alpha\beta$$

Folgerung 3.4

$\bar{R} = K[X]/mK[X]$ ist ein K -Vektorraum der $\dim n = \text{Grad } m$ mit Basis $1, \bar{X}, \bar{X}^2, \dots, \bar{X}^{n-1}$. Identifiziert man $\alpha \in K$ mit der Restklasse $\bar{\alpha}$, so enthält \bar{R} den Körper R .

Folgerung 3.5

Ist $m \in \mathbb{F}_p[X] = R$ irreduzibel, so ist $R/mR = \bar{R}$ ein Körper mit $q = p^n$ ($n = \text{Grad } m$) Elementen!

Grund: \mathbb{F}_p -Basis ist $1, \bar{X}, \bar{X}^2, \dots, \bar{X}^{n-1}$.

$$\bar{R} = \{\alpha_0 \cdot 1 + \alpha_1 \bar{X} + \dots + \alpha_{n-1} \bar{X}^{n-1} \mid \alpha_0, \dots, \alpha_{n-1} \in \mathbb{F}_p\} \quad \text{mit } \#\bar{R} = p^n$$

Zum Rechnen in \bar{R} wird empfohlen $\bar{\alpha} \in \mathbb{F}_p$ durch $r = a \quad \text{mod } p$ zu ersetzen, mit $r \in \text{Versys}_p$. $f \in \text{Versys}_p[X]$ hat die Form $f = \sum_{i=0}^n c_i X^i$, $c_i \in \text{Versys}_p$.

Bei der Bestimmung von $f + g$, $f \cdot g$ ist bei allen Rechnungen mit Koeffizienten c_1, \dots, c_n , $+$ durch \oplus und \cdot durch \odot zu ersetzen. Man kann auch $f + g$, $f \cdot g$ in $\mathbb{Z}[X]$ berechnen und dann zu allen Koeffizienten die Reste $\quad \text{mod } p$ nehmen.

Beispiel

$$\begin{aligned} \mathbb{F}_3[X], \mathbb{F}_3 &= \{\bar{0}, \bar{1}, \bar{2}\}, \text{Versys}_3 = \{0, 1, 2\} \\ \underbrace{(X^2 + 2X + 1) \cdot (2X + 1)}_{(= \bar{1} \cdot X^2 + \bar{2} \cdot X + \bar{1} \text{ in } \bar{R}[X])} &= 2X^3 + \underbrace{2 \odot 2}_{=1 \text{ in } \mathbb{Z}[X]} X^2 + 2X + X^2 + 2X + 1 \\ &= 2X^3 + 4X^2 + 2X + X^2 + 2X + 1 \\ &= 2X^3 + \underbrace{5}_{2 \text{ mod } 3} X^2 + \underbrace{4}_{1 \text{ mod } 3} X + 1 \\ &= 2X^3 + (1 \oplus 1)X^2 + (2 \oplus 2)X + 1 \\ &= 2X^3 + 2X^2 + X + 1 \end{aligned}$$

Beispiel

$\mathbb{F}_4 = \{0, 1, \underbrace{\bar{x}}_{\substack{\in \mathbb{F}_2 \\ =: \varrho}}, \bar{x} + 1\}$, wenn m irreduzibel in $\mathbb{F}_2[X]$, Grad $f = 2$

$$X^2 + 1 = (X + 1)^2 (= X^2 + \underbrace{2}_{=0}X + 1 = X^2 + 1 \text{ in } \mathbb{F}_2[X])$$

$X^2 + X + 1$ ist irreduzibel. (Alle Polynome vom Grad 1 sind $X, X + 1, X^2, X(X + 1), (X + 1)^2 = X^2 + 1$ sind von m verschieden \implies irreduzibel)

$\mathbb{F}_4 = \{0, 1, \varrho, \varrho + 1\}$, $\varrho^2 = ?$

$$(\bar{X})^2 = \underbrace{\bar{X}^2}_{\in \text{Versys}_m} \bmod m = \overline{X + 1} = \bar{X} + 1 = \varrho + 1$$

$$X^2 - 1 \cdot (X^2 + X + 1) = -X - 1 = X + 1 \text{ in } \mathbb{F}_2[X]$$

Rechenregel: $\varrho^2 = \varrho + 1 \implies$ Multiplikationstafel

Bemerkung:

- $R \rightarrow \bar{R} = R/mR$, $\kappa : a \mapsto \bar{a} = \kappa(a)$, so ist κ surjektiver Ringhomomorphismus. $\kappa(a + b) = \bar{a} + \bar{b} = \overline{a + b} = \kappa(a + b)$
- Ist R ein Ring und $z \in \mathbb{Z}$, so definiert man:

$$z \cdot \varrho := \text{sgn}(z) \underbrace{(\varrho + \varrho + \dots + \varrho)}_{|z|-\text{Stück}}$$

Beispiel

$$\bar{R} = \mathbb{Z}/m\mathbb{Z}, z \in \mathbb{Z}$$

$$z\bar{a} = \overline{za} \text{ (leicht selbst nachzuweisen)} \quad m \cdot 1_{\bar{R}} = m \cdot \bar{1} = \bar{m} = 0_{\bar{R}}$$

Rechenregeln: $z, z_1, z_2 \in \mathbb{Z}, \varrho, \varrho_1, \varrho_2 \in R$

$$(z_1 + z_2)\varrho = z_1\varrho + z_2\varrho$$

$$z(\varrho_1 + \varrho_2) = z\varrho_1 + z\varrho_2$$

$$(z_1 z_2)\varrho = z_1(z_2\varrho)$$

$$z(\varrho_1 \varrho_2) = (z\varrho_1)\varrho_2 = \varrho_1(z\varrho_2) \text{ (Beweis leicht)}$$

Für $f \in \mathbb{Z}[X]$, $\bar{a} \in \mathbb{Z}/m\mathbb{Z}$ ist definiert ($f = \sum_{i=0}^n z_i X^i$):

$$f(\bar{a}) = \sum_{i=0}^n z_i \bar{a}^i \in \bar{R} (= \sum_{i=0}^n \overline{z_i a^i} = \overline{f(a)})$$

Ergebnis: $f(\bar{a}) = \overline{f(a)}$

3.1 Zyklische Gruppen

Aufgabe: Berechne $3^{10^{500}} \bmod \underbrace{167}_{=:p}$ (Rechne in Versys_{167} !)

Mathematische Hilfsmittel: Ordnung eines Gruppenelements.

Definition

Sei G eine (ohne Einschränkung multiplikative) endliche Gruppe, $x \in G$. (Das neutrale Element werde mit $1 = 1_G$ bezeichnet)

- (i) $\text{ord}(x) = \min\{n \in \mathbb{N}_+ \mid x^n = 1\}$ heißt „*Ordnung von x* “
- (ii) $\#G$ heißt „*Ordnung von G* “

Bemerkung: $\text{ord}(x)$ existiert, da $n > m, n, m \in \mathbb{N}_+$ vorhanden sind mit $x^n = x^m$, da G endlich. $\implies x^{n-m} = 1$. In allgemeinen Gruppen kann sein $\{n \in \mathbb{N}_+ \mid x^n = 1\} = \emptyset$, dann schreibt man $\text{ord}(x) = \infty$

Satz 3.6 (Elementordnungssatz)

Sei G eine endliche Gruppe, $x \in G$, $m, n \in \mathbb{Z}$. Dann gelten:

- (i) $x^m = x^n \iff m \equiv n \pmod{\text{ord}(x)}$
Insbesondere $x^m = x^{m \bmod \text{ord}(x)}$ und $x^m = 1 \iff \text{ord}(x) \mid m$
- (ii) $x^{\#G} = 1$ (d.h. nach (i) $\text{ord}(x) \mid \#G$)
- (iii) $\text{ord}(x^m) = \frac{\text{ord}(x)}{\text{ggT}(m, \text{ord}(x))}$

Anwendung:

Satz von Euler: Sei $m, x \in \mathbb{Z}, m > 0, \text{ggT}(x, m) = 1$, φ sei die Eulersche Funktion. Dann gilt: $x^{\varphi(m)} \equiv 1 \pmod{m}$

(Kleine) Satz von Fermat: Sei $p \in \mathbb{P}, x \in \mathbb{Z}$. Dann gilt: $x^p \equiv x \pmod{p}$

Zum Satz von Euler:

$G = (R/Rm)^\times, \#G = \varphi(m)$. $\bar{x} \in G \iff \text{ggT}(x, m) = 1$. Elementordnungssatz (ii) $\implies \bar{1} = 1_g = \bar{x}^{\#G} = \bar{x}^{\varphi(m)} = x^{\varphi(m)} \iff 1 \equiv x^{\varphi(m)} \pmod{m}$

Zum Satz von Fermat:

$\varphi(p) = p - 1$. Aussage klar, wenn $p \mid x (x \equiv 0 \equiv xp)$. $p \nmid x \implies \text{ggT}(p, x) = 1 \implies \bar{x}^{p-1} = \bar{x}^{\#G} = \bar{1} \implies \bar{x}^p = \bar{x} \implies x^p \equiv x \pmod{p}$

Beweis (Elementordnungssatz)

Sei $x \in G, \text{ord}(X) =: l$.

- (1) $x^m = x^n \iff x^{m-n} = 1 = 1_G \iff 1 = x^{ql+r} = (x^l)^q \cdot x^r = 1^q \cdot x^r = 1x^r = x^r$ (Falls $r \neq 0$, so haben wir einen Widerspruch zur Minimalwahl von l) $\iff r = 0 \iff l \mid m - n \iff m \equiv n \pmod{l}$.

Insbesondere: $x^m = 1 \iff l \mid m, x^n = x^{n \bmod l}$

- (2) $x^{\#G} = 1$. Dies wird in dieser Vorlesung nur für kommutative G benötigt und bewiesen. Betrachte die Abbildung $G \rightarrow G, x \mapsto y \cdot x$. Sie ist bijektiv (die Umkehrabbildung ist $y \mapsto yx^{-1}$), also $\{y \mid y \in G\} = G = \{yx \mid y \in G\}$.

$$\prod_{y \in G} y = \prod_{y, x \in G} (yx) = \prod_{y \in G} y \cdot x^{\#G} \implies x^{\#G} = 1$$

■

Also laut (1): $\text{ord}(x) \mid \#G$

(3) $\text{ord}(x^m) = k \implies 1 = (x^m)^k = x^{mk} \xrightarrow{(1)} l \mid mk$. Sei $d = \text{ggT}(m, l) \implies \frac{l}{d} \mid \frac{md}{d}k \implies \frac{l}{d} \mid k$. Warum sind $\frac{l}{d}$ und $\frac{m}{d}$ relativ prim? $d = \text{ggT}(m, l) = d \cdot \text{ggT}(\frac{m}{d}, \frac{l}{d}) \implies \text{ggT}(\frac{m}{d}, \frac{l}{d}) = 1$. Aber $k \mid \frac{l}{d}$ wegen $(x^m)^{\frac{l}{d}} = x^{l \cdot \frac{m}{d}} = 1^{\frac{m}{d}} = 1$, $k = \text{ord}(x^m)$ nach (1).

Ergebnis: $k = \frac{l}{d} = \frac{\text{ord}(x)}{\text{ggT}(\text{ord}(x), m)}$

Hilfestellungen zur Berechnung von $\text{ord}(x)$

Bemerkungen:

(i) $\text{ord}(a) \mid \#G$ (wirklich a ?)

(ii) Sei $x^d = 1$. Dann gilt: $d = \text{ord}(x) \iff \forall p \in \mathbb{P} \text{ mit } p \mid d: x^{\frac{d}{p}} \neq 1$.

Beweis (Der Bemerkung (ii))

„ \implies “: Klar

„ \impliedby “: Sei $x^d = 1$, $x \neq \text{ord}(x)$. Nach (1): $\text{ord}(x) \mid d \implies \exists p \in \mathbb{P} : \text{ord}(x) \mid \frac{d}{p} \implies x^{\frac{d}{p}} = 1$ ■

Zur Berechnung von x^n : Naive rekursive Berechnung: $x^{j+1} = x^j \cdot x$. Hier hätten wir n Produkte zu berechnen! Westentlich bessere Methode: Stelle n binär da: $n = \sum_{i=0}^t c_i \cdot 2^i$, $c_t \neq 0$, $c_i \in \{0, 1\}$. Bezeichnung $n = (c_t, c_{t-1}, \dots, c_0)_2$ mit den Binärziffern c_j .

$$x^n = x^{\sum_{i=0}^t c_i \cdot 2^i} = \prod_{i=0}^t \left(x^{2^i}\right)^{c_i} = \prod_{i=0, c_i \neq 0}^t x^{(2^i)}$$

Rekursiv: $x^{2^0} = x^1 = x$ und $x^{2^{i+1}} = (x^{2^i})^2$. t ist etwa $\log_2 n$, man hat ungefähr $2 \cdot \log_2 n$ Produkte zu berechnen.

Beispiel

$G = \mathbb{F}_9^\times$, $\#G = 9 - 1 = 8$. Mögliche $\text{ord}(\alpha)$ für ein $\alpha \in G$: 1, 2, 4, oder 8.

$$\text{ord}(\alpha) = 1 \iff \alpha = 1$$

$$\text{ord}(\alpha) = 2 \iff \alpha \neq 1, \alpha^2 = 1 \iff \alpha = -1_G = -1$$

$$\text{ord}(\alpha) = 4 \iff \alpha^4 = 1, \alpha^2 \neq 1 \text{ (d.h. } \alpha \neq \pm 1)$$

$$\text{ord}(\alpha) = 8 \iff \alpha^4 \neq 1$$

$\mathbb{F}_9 = \mathbb{F}_3[X]/m \cdot \mathbb{F}_3[X]$, $\text{ord}(m) = 2$, m irreduzibel. Beispielsweise ist $X^2 + 1$ in $R = \mathbb{F}_3[X]$ irreduzibel.

\mathbb{F}_9 hat \mathbb{F}_3 -Basis $1; \bar{x}$. $\mathbb{F}_9 = \underbrace{\{0, 1, -1, \dots\}}_{\mathbb{F}_3 = \text{Versys}_3} = \{a + b\bar{x} \mid a, b \in \mathbb{F}_3\}$

$$m = X^2 + 1 \equiv 0 \pmod{m} \implies X^2 \equiv -1 \pmod{m} \implies \bar{X}^2 = -1 = -1_{\mathbb{F}_9} = -1_{\mathbb{F}_3} \implies \bar{X}^4 = (-1)^2 = 1 \implies \text{ord}(\bar{X}) = 4.$$

$$(\bar{X} + 1)^2 = \bar{X}^2 + 2\bar{X} + 1 = -1 + 1 + 2\bar{X} = -\bar{X} \neq 1, (\bar{X} + 1)^4 = (-\bar{X})^2 = \bar{X}^2 = -1 \implies \text{ord}(\bar{X} + 1) = 8$$

Zurück zum Problem $3^{(10^{500})} \bmod 167$, $167 \in \mathbb{P}$. $G = \mathbb{F}_{167}$, $\#G = \varphi(167) = 166 = 2 \cdot 83$, also gilt $\text{ord}(n) \in \{1, 2, 83, 166\}$.

Laut Satzungssatz: $3^{10^{500}} \equiv 3^{10^{500} \bmod \text{ord}(\bar{3})}$.

Wir brauchen $\text{ord}(3)$: $\bar{3}^2 = \bar{9} \neq 1_G \implies \text{ord}(\bar{3}) \neq 1, 2$, $\text{ord}(\bar{3}) = 83 \iff \bar{3}^{83} = 1_G = \bar{1}$. $83 = (1010011)_2 = 64 + 16 + 2 + 1$. Tabelle: 3^{2^0} in \mathbb{F}_{167} ist 3, 3^{2^1} in \mathbb{F}_{167} ist $3^2 = 9$, 3^{2^2} in \mathbb{F}_{167} ist $9^2 = 81$, 3^{2^3} in \mathbb{F}_{167} ist $81^2 = 6651 = 30 \cdot 167 + 48 \equiv 48$, 3^{2^4} in \mathbb{F}_{167} ist $48^2 \equiv 133$, 3^{2^5} in \mathbb{F}_{167} ist $133^2 = 17629 \equiv 154$, 3^{2^6} in \mathbb{F}_{167} ist $154^2 \equiv 2$. Also: $\bar{3}^{83} = \bar{3} \cdot \bar{9} \cdot \bar{133} \cdot \bar{2} \cdot \bar{7182} \cdot \bar{1} = 1_G$. Ergebnis: $\text{ord}(\bar{3}) = 83$.

$3^{10^{500}} = 3^{10^{500} \bmod 83}$. Noch zu berechnen: $10^{500} \bmod 83$. Man kann $\bar{10}$ in \mathbb{F}_{83} berechnen. Reicht auch $\bar{10}^{500} = 10^{500 \bmod \varphi(83)}$. $\varphi(83) = 82$, $500 \equiv 8 \bmod 82 \implies 10^{500} \equiv 10^8 \equiv 23 \bmod 83$

Also: $\bar{3}^{10^{500}} = \bar{3}^{23} = \bar{124} = \bar{-33}$ und somit $3^{10^{500}} = 124 \bmod 167$

Satz 3.7 (Mersenne-Teiler-Satz)

Es seien $p, q \in \mathbb{P}$ mit $q \mid M_p = 2^p - 1$. Dann gilt: $q \equiv 1 \bmod p$

Beweis

$q \mid M_p \iff M_p = 2^p - 1 \equiv 0 \bmod q \iff \bar{2}^p = 1$ in $\mathbb{F}_q^\times = G \implies \text{ord}(\bar{2}) = p$, da 1 nicht geht und $\text{ord}(\bar{2}) \mid p$ nach dem Satzungssatz. $\text{ord}(\bar{2}) \mid \#G = \varphi(q) = q - 1 \implies q - 1 \equiv 0 \bmod p \implies q \equiv 1 \bmod p$ ■

Bezeichnungen:

(1) $\langle x \rangle = \{1, x, x^2, \dots, x^{l-1}\}$, ($l = \text{ord}(x)$), heißt die von x erzeugte zyklische Untergruppe von G .

(2) G heißt zyklisch $\iff \exists x \in G : G = \langle x \rangle \iff \exists x \in G : \text{ord}(x) = \#G$

Bemerkung: Die Abbildung $(\mathbb{Z}/\mathbb{Z}l, +) \rightarrow (\langle x \rangle, \cdot)$ mit $\bar{m} \mapsto x^m$ ist ein Isomorphismus von Gruppen.

3.2 Primitivwurzeln

Vorbereitungen über $R = K[X]$, K ein Körper.

Bemerkung: Sei $\alpha \in K$, $f \in R$, $\text{ord}(f) > 0$. Dann gilt:

$$0 = f(\alpha) \iff X - \alpha \mid f \iff v_{X-\alpha}(f) > 0 \quad (X - \alpha \in \mathbb{P}_R)$$

$v_{X-\alpha}$ heißt Vielfachheit der Nullstelle α von f .

Beweis

Division mit Rest: $f = q \cdot (X - \alpha) + r$. $\text{grad } r < \text{grad}(X - \alpha) = 1 \implies r \in K$ (konstantes Polynom), insbesondere $r(\alpha) = r$. $f(\alpha) = q(\alpha)(\alpha - \alpha) + r(\alpha) = r$. Also: $r(\alpha) = 0 \iff r = 0 \iff X - \alpha \mid f$ ■

Satz 3.8 (Nullstellenanzahls-Satz)

$f \in K[X]$, $f \neq 0$, $n = \text{grad } f$, so gilt: f hat höchstens n verschiedene Nullstellen in K .

Beweis

$\alpha_1, \dots, \alpha_l$ seien l Nullstellen. $v_{X-\alpha_j}(f) > 0 \implies \prod_{j=1}^l (X-\alpha_j) \mid f$, wegen $v_{X-\alpha_i}(\prod_{j=1}^l (X-\alpha_j)) = 1$ und $v_m(\prod_{j=1}^l (X-\alpha_j)) = 0$ für alle anderen $m \in \mathbb{P}$ sowie $v_{X-\alpha_j}(f) \geq 1$. Daraus folgt: $l \leq \text{grad } f$ ■

Der Spezialfall $K = \mathbb{F}_p$ ergibt den

Satz 3.9 (Satz von Lagrange)

Sei $p \in \mathbb{P}$, $f = \sum_{i=0}^n c_i X^i \in \mathbb{Z}[X]$. Es gibt ein $j \in \{0, \dots, n\}$ mit $c_j \not\equiv 0 \pmod{p}$. Dann fallen die „Lösungen“ $x \in \mathbb{Z}$ der Kongruenz

$$f(x) \equiv 0 \pmod{p}$$

in höchstens n verschiedene Restklassen modulo p .

Beweis

Der Satz ist eine Übersetzung des Nullstellenanzahls-Satzes auf Kongruenzen. Betrachte die $\overline{c_j} = \alpha_j \in \mathbb{F}_p \implies \exists j : \overline{c_j} \neq 0 \implies f = \sum_{i=0}^n \overline{c_i} X^i \neq 0$ in $\mathbb{F}_p[X]$, $\text{ord}(f) \leq n$. $f(x) = 0 \pmod{p} \iff \overline{f(x)} = f(\overline{x}) = 0_{\mathbb{F}_p}$. Es gibt höchstens n Nullstellen \overline{x} , das heißt lösende Kongruenzklassen. ■

$p \in \mathbb{P}$ wird gebraucht, Aussage modulo m , $m \notin \mathbb{P}$, im Allgemeinen falsch. Beispiele: $m = 6$, $f = X^2 + X$ hat in $\mathbb{Z}/6\mathbb{Z}$ die Nullstellen $\overline{0}$, $\overline{2}$, $\overline{3}$, $\overline{5}$. $m = 9$, $f = X^2$ hat in $\mathbb{Z}/9\mathbb{Z}$ die Nullstellen $\overline{0}$, $\overline{3}$, $\overline{-3}$.

Satz 3.10 (Primitivwurzelsatz)

Sei K Körper, G eine endliche Untergruppe von K^\times . Dann ist G zyklisch. Genauer gilt: $\#\{\alpha \in K \mid \text{ord}(\alpha) = \#G\} = \varphi(\#G)$ (φ die Eulersche Funktion)

Bemerkung: Ist $\text{ord}(\alpha) = \#G$, so heißt α primitive $\#G$ -te Einheitswurzel, da $\alpha^{\#G} = 1$, sozusagen $\alpha = \sqrt[\#G]{1}$. primitiv, da $\alpha^m = 1$, wobei $\#G \mid m$.

Spezialfälle

- (1) $K = \mathbb{F}_q$, also ein Körper mit $q < \infty$ Elementen. $G = \mathbb{F}_q^\times = \mathbb{F}_q \setminus \{0\}$, $\#G = q - 1$. Nach dem Satz ist \mathbb{F}_q^\times zyklisch α mit $\langle \alpha \rangle = \mathbb{F}_q^\times$ heißt primitives Element.

- (2) Noch spezieller: $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ mit $p \in \mathbb{P}$ besitzt $\varphi(p-1)$ primitive Elemente $\alpha = \bar{w}$, ($0 \leq w < p-1$). Solve w heißen Primitivwurzel modulo p .

Beweis

Sei $l = \#G$, G wie im Satz.

Für die $d \mid l$, $d \in \mathbb{N}_+$, sei $\lambda(d) = \#\{\alpha \in G \mid \text{ord}(\alpha) = d\}$. Laut Elementordnungssatz gilt: $l = \sum_{d \mid l} \lambda(d) = \sum_{d \mid l} \varphi(d)$ (Lemma von Gauß). Man will zeigen: $\lambda(d) \leq \varphi(d)$ (*), denn dann muss gelten: $\forall d \mid l: \lambda(d) = \varphi(d)$, denn sonst würde gelten: $\sum_{d \mid l} \lambda(d) < \sum_{d \mid l} \varphi(d)$.

(*) ist klar, wenn $\lambda(d) = 0$. Sei also $\lambda(d) \neq 0 \implies \exists \alpha \in G: \text{ord}(\alpha) = d$. Sei $A = \langle \alpha \rangle = \{1, \alpha, \alpha^2, \dots, \alpha^{d-1}\}$. Klar: $(\alpha^d)^d = 1 \implies \alpha^j$ ist eine Nullstelle von $X^d - 1$. Wegen $\#A = d$ sind das d Nullstellen von $X^d - 1$, also alle solche. $B = \{\beta \in G \mid \text{ord}(\beta) = d\}$, dann $\beta^d = 1 \implies \beta$ Nullstelle von $X^d - 1 \implies \beta \in A$. $B \subseteq A$.

$\alpha^j \in B \iff \text{ord}(\alpha^j) = d \implies d = \text{ord}(\alpha^j) = \frac{\text{ord}(\alpha)}{\text{ggT}(d,j)} \text{ (Elementordnungssatz)} \implies \text{ggT}(d,j) = 1 \implies B \subseteq \{\alpha^j \mid \text{ggT}(d,j) = 1, 0 \leq j \leq d\}$. $\#B = \lambda(d) \leq \#\{\alpha^j \mid \text{ggT}(d,j) = 1, 0 \leq j \leq d\} = \varphi(d)$

Der folgende Satz ist eine Anwendung des Primitivwurzelatzes:

Satz 3.11 (Eulers Quadratkriterium)

Sei $\alpha \in \mathbb{F}_q^\times$ (\mathbb{F}_q ein Körper mit q Elementen, $2 \mid q$). Dann gilt:

$$\alpha \text{ ist ein Quadrat in } \mathbb{F}_q^\times \iff \alpha^{\frac{q-1}{2}} = 1$$

Anderenfalls gilt: $\alpha^{\frac{q-1}{2}} = -1$

Euler formuliert den Satz so: Sei $p \in \mathbb{P}$, $p > 2$, $n \in \mathbb{Z}$, $p \mid m$. Dann existiert ein $x \in \mathbb{Z}$ mit $x^2 \equiv m \pmod{p} \iff m^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Solche $m \pmod{p}$ heißen quadratische Reste.

Wenn Kongruenz als Gleichung in $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ gelesen wird, so gilt:

$$\alpha = \bar{x} \text{ Quadrat in } \mathbb{F}_p^\times \iff x \text{ quadratischer Rest modulo } p$$

Beweis

Sei ζ eine Primitivwurzel (Existenz folgt aus dem Primitivwurzelatz).

„ \Leftarrow “: Sei $\alpha^{\frac{q-1}{2}} = 1$ und $\alpha = \zeta^j$. $\zeta^{j \cdot \frac{q-1}{2}} = 1 \implies q-1 = \text{ord}(\zeta) \mid j \cdot \frac{q-1}{2} \implies \frac{j}{2} \in \mathbb{Z} \implies 2 \mid j \implies \beta = \zeta^{\frac{j}{2}}$ zeigt den Satz: $\beta^2 = \zeta^j = \alpha$

„ \Rightarrow “: α Quadrat $\iff \exists \beta \in \mathbb{F}_q: \alpha = \beta^2 \implies \exists k \in \mathbb{Z}: \beta = \zeta^k$. $\alpha = \zeta^{2k} \implies \alpha^{\frac{q-1}{2}} = \zeta^{(q-1)k} = 1$, da $\text{ord}(\zeta) = q-1$

$\alpha^{\frac{q-1}{2}}$ ist Nullstelle von $X^2 - 1$. Alle Nullstellen sind $\{1, -1\}$. 1 entfällt, also ist $\alpha^{\frac{q-1}{2}} = -1$ ■

Eulers Formulierung „ m nicht quadratischer Rest“, auch „quadratischer Nichtrest“. $\text{ggT}(m, p) = 1 \implies m^{\frac{p-1}{2}} \equiv -1 \pmod{p}$

3.3 Zifferndarstellung nach Cantor

In diesem Abschnitt seien $R = \mathbb{Z}$ oder $R = K[X]$, K ein Körper.

Ausgangspunkt ist die Folge $\gamma = (m_0, m_1, m_2, \dots)$, $m_j \in R$ mit $m_j > 1$ bei $R = \mathbb{Z}$ oder $\text{grad}(m_j) > 0$ bei $R = K[X]$.

Definiere $M_0 = 1$, $M_k = m_0 \cdot \dots \cdot m_{k-1}$.

Satz 3.12 (Ziffersatz)

Jedes $n \in \mathbb{N}_+$ bzw. $n \in K[X]$, $n \neq 0$ hat eine eindeutige Darstellung

$$n = z_r M_r + z_{r-1} M_{r-1} + \dots + z_1 M_1 + z_0 \quad (*)$$

wobei $r \in \mathbb{N}$ und $0 \leq z_j < m_j$ bzw. $\text{grad}(z_j) < \text{grad}(m_j)$

Bezeichnungen: Die z_j heißen γ -adische Ziffern und $(*)$ Zifferndarstellung (vorlesungs-spezifisch). Kurzbezeichnung: $n = (z_r, z_{r-1}, \dots, z_0)_\gamma$. Die Kommata dürfen bei Eindeutigkeit weggelassen werden.

Spezialfall: $m_0 = m_1 = m_2 = \dots =: m$ gibt Zifferndarstellung $n = z_r m^r + z_{r-1} m^{r-1} + \dots + z_0 = (z_r, \dots, z_0)_m$ heißt m -adische Darstellung von n .

Spezialbenennungen:

m	Zifferndarstellung	Ziffern	
10	Dezimaldarstellung	0,1,...,9	bei Menschen beliebt (10 Finger)
2	Binär oder dyadisch	0,1	bei Computern beliebt (0,1 gut realisierbar)
8	Oktalдарstellung	0,...,7	
16	Hexadezimal	0,...,9,A,B,C,D,E,F	Speicherverwaltung im Rechner

Beispiel

$$\begin{aligned}
 (A8C)_{16} &= 10 \cdot 16^2 + 8 \cdot 16 + 12 \cdot 1 \\
 &= 2700 := (2700)_{10} \\
 &= (10101001100)_2 \\
 &= (5214)_8
 \end{aligned}$$

$\gamma = (m_0, m_1, \dots)$, $m_j \in \mathbb{Z}$ (bzw. $K[X]$), $m_j > 1$ bzw. $\text{Grad } m_j > 0$
 $M_0 = 1$, $M_k = m_0 \cdot \dots \cdot m_{k-1}$

γ -adische Entwicklung von $n \in \mathbb{N}_+$ bzw. $n \in K[X]$, $n \neq 0$:

$$n = z_r M_r + z_{r-1} M_{r-1} + \dots + z_1 M_1 + z_0 \cdot 1 \quad (3.1)$$

γ -adische Darstellung, wenn $0 \leq z_j < m_j$ (bzw. $\text{Grad } z_j < \text{Grad } m_j$)

Beweis (Ziffersatz)

Fall (3.1) vorliegt: Wegen $M_k | M_{k+1} | M_{k+2} | \dots$:
 $n \equiv z_{k-1}M_{k-1} + z_{k-2}M_{k-2} + \dots + z_0 \pmod{M_k}$

Speziell: $n \equiv z_0 \pmod{M_1 = m_0} \implies n - z_0 = n'm_0, n' \in \mathbb{Z}$ bzw. $K[X]$

Beweisidee: Induktion nach n bzw. Grad n (hier nur $\mathbb{Z}, K[X]$ fast genau so)

Behauptung: Sei $n \in \mathbb{Z}_+$. Dann existiert für alle γ 's dieser Art die γ -dische Darstellung (3.1).

Induktion nach n :

Falls $n < m_0$, dann $z_0 = n, n = z_0M_0$ ist (\star)

Falls $n \geq m_0$, $z_0 = (n \bmod m_0), n'$ aus $n - z_0 = n'm_0 (n' = \frac{n-z_0}{m_0})$. Klar $0 \leq z_0 < m_0 \leq n \implies 0 < n' < n$.

Induktionshypothese anwendbar auf n' mit $\gamma' = (m'_1, m'_2, \dots), m'_j = m_{j+1} (j \geq 0)$.

$\exists \gamma'$ -adische Darstellung von n' :

$n' = z'_{r'}M'_{r'} + z'_{r'-1}M'_{r'-1} + \dots + z'_1M'_1 + z'_0 (r' \in \mathbb{N}, z'_{r'} \neq 0)$

$n \leq z'_j < m'_j = m_{j+1} \implies n = n'm_0 + z_0 = z'_{r'}M_{r'+1} + \dots + z'_1M_1 + z_0$

Das ist die gesuchte γ' -adische Darstellung von n mit $r := r' + 1, z'_j = z_j + 1 (j = 0, \dots, r')$ also $0 \leq z_{j+1} = z_j < m'_j = m_{j+1}$

Dies ist ein Algorithmus, wenn die Abbildung $j \mapsto m_j$ berechenbar ist.

Eindeutigkeit: Ebenfalls Induktion. z_0 muss $n \bmod m_0$ sein. Induktionshypothese n' eindeutig dargestellt \implies Darstellung von n eindeutig (Details: selbst!) ■

Bemerkung: Zur Berechnung von $(n_1 + / \cdot n_2)_\gamma$ aus $(n_1)_\gamma$ und $(n_2)_\gamma$ ähnliche Algorithmen wie für $()_{10}$.

3.4 Simultane Kongruenzen

3.4.1 Prinzip des Parallelen Rechnens

$R_j (j = 1, \dots, l)$ seien algebraische Strukturen gleicher Art mit gleichbezeichneten Verknüpfungen $*$, zum Beispiel:

Gruppen $* \in \{\cdot\}$

Abelsche Gruppen $* \in \{+\}$

Ringe $* \in \{+, \cdot\}$

Vektorräume $* \in \{+, \text{Skalarmultiplikation}\}$

Dann ist auch $S = \prod_{i=1}^l R_j = R_1 \times \dots \times R_l$ eine algebraische Struktur mit Verknüpfungen (komponentenweise):

$S \ni (a_1, \dots, a_l), (b_1, \dots, b_l), a_j, b_j \in R_j$

$(a_1, \dots, a_l) * (b_1, \dots, b_l) := (a_1 * b_1, \dots, a_l * b_l)$

$\alpha(a_1, \dots, a_l) := (\alpha a_1, \dots, \alpha a_l)$ bei K-Vektorräumen.

Sind j Ringe/Gruppen/Abelsche Gruppen/Vektorräume, so auch S .

Grund: Alles vererbt sich von den Komponenten!

Zum Beispiel Ringe: $0_S = (0_{R_1}, \dots, 0_{R_l}), 1_S = (1_{R_1}, \dots, 1_{R_l})$, kurz: $0 = (0, \dots, 0), 1 = (1, \dots, 1)$,
 $-(a_1, \dots, a_l) = (-a_1, \dots, -a_l)$

Zum Beispiel Assoziativität:

$$((a_1, \dots, a_l) * (b_1, \dots, b_l)) * (c_1, \dots, c_l) = ((a_1 * b_1) * c_1, \dots, (a_l * b_l) * c_l) = (a_1, \dots, a_l) * ((b_1, \dots, b_l) * (c_1, \dots, c_l))$$

Warnung! Sind die R_j Körper, so ist für $l > 1$, S kein Körper.

Zum Beispiel: $\underbrace{(1, 0)}_{\neq 0} \cdot \underbrace{(0, 1)}_{\neq 0} = (1 \cdot 0, 0 \cdot 1) = (0, 0) = 0$

Lemma 3.13

Sind die R_j Ringe, so $S^\times = \prod_{j=1}^l R_j^\times$

Grund: Muss sein $(a_1, \dots, a_l)^{-1} = (a_1^{-1}, \dots, a_l^{-1})$

Falls ein Isomorphismus $\psi : R \rightarrow S = \prod_{j=1}^l R_j$ vorliegt, so wird das Rechnen in R zurückgeführt auf das gleichzeitig („parallele“) Rechnen in dem R_j wie folgt:

$$\psi(a) = (a_1, \dots, a_l), \psi(b) = (b_1, \dots, b_l)$$

$$a * b = \psi^{-1}(\psi(a * b)) = \psi^{-1}(\psi(a) * \psi(b)) = \psi^{-1}((a_1 * b_1, \dots, a_l * b_l))$$

Praxis: Berechne die $a_j * b_j$ gleichzeitig auf verschiedenen Prozessoren. Wende ψ, ψ^{-1} wie oben an. Nützt nur, wenn ψ, ψ^{-1} gut und schnell berechenbar sind.

3.4.2 Der Chinesische Restsatz

Frage: Morgen ist Freitag, der 2. Juni. Nach wievielen ($x = ?$) Tagen fällt frühestens der Dienstag auf einen 17. des Monats?

Vorraussetzung: Chinesische Kalender vor ca. 2000 Jahren: Alle Monate haben 20 Tage.

Wochentag	Fr	Sa	So	Mo	Di	Mi	Do	Fr	Sa	So
Wochentagsnr.	0	1	2	3	4	5	6	0	1	2
Monatstagnr.	2	3	4	5	6	7	8	9	10	11

(Wochentagsnummer modulo 7, Monatstagnummer modulo 30)

Gesucht ist also die kleinste positive Lösung x der Kongruenzen:

$$x \equiv 4 \pmod{7}$$

$$x \equiv 17 - 2 \pmod{30}$$

R sei euklidischer Ring, $a_1, \dots, a_l, m_1, \dots, m_l \in R$

$$x \equiv a_j \pmod{m_j}, (j = 1, \dots, l) \quad (3.2)$$

heißt *System simultaner Kongruenzen* (mit gesuchter Lösung $x \in R$).

Bemerkung: Im Allgemeinen gibt es *keine* Lösung.

$$x \equiv a \pmod{m} \implies x \equiv a \pmod{m}, \text{ falls } d \mid m$$

$$\text{System: } x \equiv 1 \pmod{4}, x \equiv 0 \pmod{6} \implies x \equiv 1 \pmod{2}, x \equiv 0 \pmod{2} \implies 1 \equiv 0 \pmod{2} \implies \text{Widerspruch!}$$

Satz 3.14 (Chinesischer Restsatz, rechnerische Form)

Sei R ein euklidischer Ring, $m_1, \dots, m_l \in R$, $a_1, \dots, a_l \in R$ derartig, dass $\forall i, j \in \mathbb{Z}$ mit $1 \leq i < j \leq l$ gilt:

$$\text{ggT}(m_i, m_j) = 1 \text{ („paarweise relativ prime } m_j\text{“)}$$

Dann hat das System simultaner Kongruenzen (3.2) eine Lösung. Sämtliche Lösungen bilden eine Restklasse modulo m mit $m = m_1 \cdot \dots \cdot m_l$

Beweis

$$l = 1: x = a_1 \text{ oder } x = (a_1 \pmod{m_1}) \iff (x \equiv a_1) \pmod{m_1} \text{ und } 0 \leq x \leq m_1$$

$$l = 2: x \equiv a_1 \pmod{m_1}. x \text{ muss in der Form } x = a_1 + um_1, u \in R \text{ angesetzt werden.}$$

Idee: Bestimme u so, dass $x \equiv a_2 \pmod{m_2}$. Also in $\bar{R} = R/m_2R$ soll werden:

$$\bar{a}_1 + \bar{u}\bar{m}_1 = \bar{a}_1 + \bar{u}\bar{m}_1 = \bar{a}_2, \text{ daher tut es: } \bar{u} = (\bar{a}_2 - \bar{a}_1)\bar{m}_1^{-1}$$

Geht, da \bar{m}_1^{-1} existiert und da $\bar{m}_1 \in (R/m_2R)^\times$. Nach dem Restklassensatz: $\bar{m}_1 \in (R/m_2R)^\times \iff \text{ggT}(m_1, m_2) = 1$

Algorithmisch $\bar{u} = \bar{m}_1^{-1}$, u kann mit LinKom-Satz, also euklidischem Algorithmus, bestimmt werden. *Erinnerung:* $\text{ggT}(m_1, m_2) = um_1 + vm_2$, u, v berechnet der Algorithmus.

$$1 = \bar{u}\bar{m}_1, \bar{m}_2 = 0, \bar{u} = \bar{m}_1^{-1}$$

Für dieses $u \in R$ ist $x = a_1 + um_1$ (eventuell $\pmod{m, m_2}$) die gesuchte Lösung.

$$l > 2: \text{Induktionshypothese löst } x' \equiv a_j \pmod{m_j} (j = 1, \dots, l-1).$$

$$\text{Löse dann } x \equiv x' \pmod{m_1 \cdot \dots \cdot m_{l-1}} \implies x \equiv x' \equiv a_j \pmod{m_j}, j = 1, \dots, l-1 \implies x \equiv a_l \pmod{m_l} \implies x \text{ ist die gesuchte Lösung.} \blacksquare$$

Beispiel

Gegeben sind die Kongruenzen:

$$x \equiv 4 \pmod{7}$$

$$x \equiv 19 \pmod{30}$$

Ansatz: $x = 4 + u \cdot 7 \equiv 19 \pmod{30}$. Im $\mathbb{Z}/30\mathbb{Z}$: $\bar{4} + \bar{u} \cdot \bar{7} = \bar{19} \implies \bar{u} = (\bar{19} - \bar{4})^{-1} \cdot \bar{7}^{-1}$. Es ist $\bar{7}^{-1} = \bar{13}$, also $u \equiv 13 \cdot 15$, etwa $x = 4 + 13 \cdot 15 \cdot 7 \equiv 109 \pmod{210}$.

Wir fügen eine Bedingung hinzu: $x \equiv 1 \pmod{77}$. So ist nun zu lösen:

$$x \equiv 109 \pmod{30}$$

$$x \equiv 1 \pmod{11}$$

Es ist $\bar{210}^{-1} = \bar{1}$ im \mathbb{F}_{11} , also $x = 109 + 2 \cdot 210 \equiv 529 \pmod{11 \cdot 3 \cdot 7}$

Bemerkung (zur Praxis): Das System $x \equiv x_i \pmod{m_i}$, $(i = 0, \dots, l)$. Der Beweis liefert eine γ -adische Darstellung von x und $m = y \gamma = (m_0, \dots, m_l)$ wie folgt: $y = z_{l-1}M_{l-1} + \dots + z_0$. Die z_i sind rekursiv aus $z_0 = x_0 \pmod{m_0}$, $y' \equiv x'_i \pmod{m_j}$, $(i = 1, \dots, l)$. Also $y' = \frac{x-z_0}{m_0}$, $x'_i = (x_i - z_0)u_{i0} \pmod{m_j}$. $\overline{u_{i0}} = \overline{m_0^{-1}}$ in $\mathbb{Z}/m_i\mathbb{Z}$. x'_i in γ' -adischer Darstellung nach Induktions-Voraussetzung ($\gamma' = (m_1, \dots, m_l)$).

Empfehlung zur Praxis, vor allem wenn viele Kongruenzen zu den selben m_i zu lösen sind:

- (1) Berechne die u_{ij} nur einmal.
- (2) Belasse die Ergebnisse m in der Form $x = (z_{l-1}, \dots, z_0)_\gamma$

Zum parallelen Rechnen: Seien R, m_1, \dots, m_l wie im chinesischen Restsatz. Betrachte die Abbildung

$$R/mR \rightarrow \prod_{j=1}^l (R/m_j R)$$

$$\psi : x + mR \mapsto (\dots, x + m_j R, \dots)$$

ψ ist wohldefiniert: $x + mR = x' + mR \iff x \equiv x' \pmod{m} \iff x \equiv x' \pmod{m_j}$ und ein Ringhomomorphismus (leicht zu sehen).

Wir beobachten: Ist $\psi : A \rightarrow B$ eine Abbildung, so gilt, dass ψ injektiv genau dann ist wenn die Gleichung $\psi(x) = b$ höchstens eine Lösung x hat. Surjektivität heißt analog, dass jede Gleichung $\psi(x) = b$ mindestens eine Lösung x hat. ψ bijektiv ist dann gleichbedeutend damit, dass $\psi(x) = b$ genau eine Lösung hat.

Für obiges ψ gilt: $b = (\dots, a_j + m_j R, \dots)$. $\psi(x + m_j R) = b$: $(\dots, x + m_j R, \dots) = (\dots, a_j + m_j R, \dots) = b$. $x + mR$ Urbild von $b \iff \forall j : x + m_j R = a_j + m_j R \iff \forall j : x \equiv a_j \pmod{m_j}$. Also:

- ψ surjektiv $\iff \forall b \exists \text{Lösung } x \equiv a_j \pmod{m_j}$
- ψ injektiv $\iff \text{Lösung } x \text{ ist eindeutig modulo } m$

Ergebnis: Der chinesische Restsatz wie oben ist gleichbedeutend mit:

Satz 3.15 (Theorem B, Chinesischer Restsatz, theoretische Form)

R ein euklidischer Ring, $m_1, \dots, m_l \in R$, $\text{ggT}(m_i, m_j) = 1$ für $i \neq j$. Dann hat man den Ringisomorphismus:

$$R/mR \rightarrow \prod_{j=1}^l (R/m_j R)$$

$$\psi : x + mR \mapsto (\dots, x + m_j R, \dots)$$

Bemerkung (Zur Praxis): ψ^{-1} wird gegeben durch lösen simultaner Kongruenzen. „Komponentenweises Rechnen: Rechnen im R/mR ersetzt durch paralleles Rechnen in den $R/m_j R$ “

Bemerkung (Theoretische Anwendung): Voraussetzungen wie im Satz. Die Einheitengruppe $(R/mR)^\times$ ist isomorph durch ψ zu $\prod_{j=1}^l (R/m_j R)^\times$. Ist $R = \mathbb{Z}$, so gilt $\varphi(m) = \prod_{j=1}^l \varphi(m_j)$, also ein neuer Beweis für die Multiplikativität von φ .

3.5 Ausgewählte Anwendungen von Kongruenzen

3.5.1 Diophantische Gleichungen

Sei $0 \neq f \in \mathbb{Z}[X_1, \dots, X_n]$ (Polynom mit n Unbekannten und Koeffizienten aus \mathbb{Z}), $x = (x_1, \dots, x_n) \in \mathbb{Z}^n$.

Eine diophantische Gleichung ist eine Gleichung der Form $f(x) = 0$, f wie oben, mit einer „Lösung x “.

Der Wunsch hier ist: Man finde möglichst viel Informationen über die Menge $\mathcal{V}_f(\mathbb{Z}) := \{x \in \mathbb{N}^n \mid f(x) = 0\}$ aller ganzzahligen Lösungen.

Das Problem ist oft extrem schwierig. Zum Beispiel die diophantischen Gleichungen $x^n + y^n + z^n = 0$, $x = (x, y, z)$, auch bekannt als das Fermatproblem.

Information für Logik-Freunde: Das 10. Hilbertsche Problem (Paris 1900):

Man finde einen Algorithmus, der zu gegebenem $f \in \mathbb{Z}[X_1, \dots, X_n]$ entscheidet, ob $\mathcal{V}_f(\mathbb{Z}) = \emptyset$ oder $\mathcal{V}_f(\mathbb{Z}) \neq \emptyset$ ist.

Satz von Julia Robinson (1910-85), J. Matjasevič: Es gibt keinen solchen Algorithmus!

Triviale, aber wichtige Methode: $f(x) = 0$ hat Lösung $x \in \mathbb{Z}^n \implies f(x) = 0$ hat Lösung $x \in \mathbb{R}^n$ (Analysis) und $\forall m \in \mathbb{Z} : f(x) \equiv 0 \pmod m$ lösbar $\iff \forall t \in \mathbb{N}_+ \forall p \in \mathbb{P} : f(x) \equiv 0 \pmod{p^t}$ lösbar. Die Folgerung ist, dass falls für ein $m \in \mathbb{N}_+$ gilt, dass für alle $(x_1, \dots, x_n) \in \mathbb{Z}^n$, $0 \leq x_j < m_j$ gilt: $f(x) \not\equiv 0 \pmod m$, so gilt $\mathcal{V}_f(\mathbb{Z}) = \emptyset$, es gibt also keine Lösung.

Beispiel

$f = X_1^2 + X_2^2 - k$, $k \in \mathbb{Z}$, diophantische Gleichung $x_1^2 + x_2^2 = k$. Unlösbar für $k < 0$ (da keine Lösung in \mathbb{R}^2). Nur interessant: $k > 0$.

Betrachtung modulo 4:

$$0^2 = 0, (\pm 1)^2 = 1, (\pm 2)^2 = 0 \implies (x_1^2 + x_2^2) \bmod 4 = \begin{cases} 0 + 0 \\ 0 + 1 \\ 1 + 1 \end{cases} \in \{0, 1, 2\}.$$

Für $k \equiv 3 \pmod 4$ hat $x_1^2 + x_2^2 = k$ also keine ganzzahlige Lösung!

Es kann eine Primzahl $p \neq 2$ nur dann Summe zweier Quadrate sein, wenn $p \equiv 1 \pmod 4$ ist. Hier gilt auch die Umkehrung, Beweis folgt eventuell später.

Beispiel

$f = X_1^2 + X_2^2 + X_3^2 - k$, also $x^2 + y^2 + z^2 = k$. Modulo 4 führt hier zu keiner Aussage. Wie betrachten modulo 8: $0^2 = 0, (\pm 1)^2 = 1, (\pm 2)^2 = 4, (\pm 3)^2 = 1, (\pm 4)^2 = 0$. Also gilt:

$$(x_1^2 + x_2^2 + x_3^2) \bmod 8 = \begin{cases} 0 + 0 + 0 \\ 0 + 1 + 0 \\ 1 + 1 + 1 \\ 1 + 1 + 1 \\ 0 + 4 + 0 \\ \vdots \end{cases} \in \{0, 1, 2, 3, 4, 5, 6\}.$$

Ergebnis: Für $k < 0$ oder $k \equiv 7 \pmod{8}$ hat die Diophantische Gleichung $x_1^2 + x_2^2 + x_3^2 = k$ keine Lösung.

Zur Information, nach Gauß: Die Umkehrung gilt auch für ungerade k .

Satz von Lagrange: $x_1^2 + x_2^2 + x_3^2 + x_4^2 = k$ ($k \in \mathbb{N}$) hat immer Lösungen.

Gelegentlich erlangt man Ergebnisse auch über andere Gleichungen:

Beispiel

Gesucht sind Lösungen von $9^x + x^3 = k$ mit $x \in \mathbb{N}_+$.

Betrachtung modulo 9: $9^x \equiv 0 \pmod{9}$. $0^3 = 0$, $(\pm 1)^3 = \pm 1$, $(\pm 2)^3 = \mp 1$, $(\pm 3)^3 = 0$, $(\pm 4)^3 = \pm 1 \implies x^3 \equiv 0, \pm 1 \pmod{9}$. Ergebnis: Für $k \equiv 2, 3, 4, 5, 6, 7 \pmod{9}$ hat die Gleichung keine Lösung in $x \in \mathbb{Z}$.

3.5.2 Interpolation

Hier sei $R = K[X] \ni f, \alpha, \beta \in K$:

$$\begin{aligned} f(\alpha) = \beta &\iff (f - \beta)(\alpha) = 0 \\ &\iff (X - \alpha) \mid f - \beta \\ &\iff f \equiv \beta \pmod{(X - \alpha)} \end{aligned}$$

Das System $f \equiv \beta_j \pmod{(X - \alpha_j)}$ ($j = 0, \dots, n$) $\iff \forall j = 0, \dots, n : f(\alpha_j) = \beta_j$ (Voraussetzung $\alpha_i \neq \alpha_j$ für $i \neq j$, d.h. $\text{ggT}(X - \alpha_i, X - \alpha_j) \neq 0$).

Der Chinesische Restsatz ergibt nun: Zu gegebenen $n + 1$ Punkten $\alpha_0, \dots, \alpha_n \in K$ ($\alpha_i \neq \alpha_j$) und Punkten $\beta_0, \dots, \beta_n \in K$ gibt es genau ein $f \bmod (X - \alpha_0) \cdots (X - \alpha_n)$, also $\text{ord}(f) \leq n$ mit $f(\alpha_j) = \beta_j$. Damit ist das Interpolationsproblem gelöst.

Frage: Kann man bei Interpolation die Tangentensteigung (allgemein $f^{(j)}(\alpha_k)$) auch vorschreiben (Hermite'sche Interpolationsaufgabe)? Ja für $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ (Übung).

$f \in K[X]$, $(X - \alpha)$ -adische Darstellung. Ziffern $z_j \in K[X]$ haben Grad $z : j < \text{grad}(X - \alpha) = 1$, das heißt $z_j \in K$. $f = \sum_{j=0}^n z_j (X - \alpha)^j$, das ist die Taylor-Entwicklung in α . z_j gegeben durch $\frac{f^{(j)}(\alpha)}{j!}$.

$$f \equiv g_{\alpha,d} \pmod{(X - \alpha)^{\alpha+1}}, \quad g_{\alpha,d} := \sum_{j=0}^d z_j (X - \alpha)^j \quad (3.3)$$

$g_{\alpha,d}$ ist gegeben durch $f(\alpha), f'(\alpha), \dots, f^{(d)}(\alpha)$.

System (3.3) entspricht der Vorgabe der $f^{(j)}(\alpha)$, Interpolation mit $m_{j,k} = (X - \alpha_k)^{d_j}$ ist lösbar mit dem Restsatz.

3.5.3 Rechnen im Computer mit großen ganzen Zahlen

Prinzip: Gleichheit in \mathbb{Z} entspricht Kongruenz und einer passender Abschätzung.

Bemerkung: $m \in \mathbb{N}$, $m > 1$, etwa $2 \nmid m$. Ist $u \equiv v \pmod{m}$ und $|u|, |v| \leq \frac{m}{2}$, so ist $u = v$, weil u, v sind im symmetrischen Versys $_m$.

Wende dies an auf die Berechnung von $f(x)$, $f \in \mathbb{Z}[X_1, \dots, X_n]$, $x = (x_1, x_2, \dots, x_n) \in \mathbb{Z}^n$. Kennt man eine Schranke $|f(x)| < \frac{m}{2}$, so genügt es, $f(x) \pmod{m}$ auszurechnen. $f(x) \pmod{m}$ kann für $m = m_1 \cdot \dots \cdot m_l$ durch Berechnen von $y_j = f(x) \pmod{m_j}$ ($j = 1, \dots, l$) ersetzt werden, das ergibt simultane Kongruenz $y = y_j \pmod{m_j}$, die mit dem chinesischen Restsatz gelöst werden kann.

3.6 Struktur der Primrestklassengruppe mod m

R euklidisch, $m = \prod_{i=1}^l p_i^{t_i}$ Primzerlegung, $t_j \in \mathbb{N}_+$. Aus dem Chinesischen Restsatz: $(R/mR)^\times \cong \prod_{j=1}^l (R/p_j^{t_j} R)^\times$ (beachte: $\text{ggT}(p_i^{t_i}, p_j^{t_j}) = 1$ für $i \neq j$). Es genügt also $G := R/p^t R$ mit $p \in P$, $t \in \mathbb{N}_+$ zu betrachten. Hier nur der Fall $R = \mathbb{Z}$ ($R = \mathbb{F}_p[X]$ geht ähnlich).

Erinnerung: $t = 1$, $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$, \mathbb{F}_p^\times ist zyklisch, es existiert eine Primitivwurzel $w \pmod{p}$.

Frage: Wie ist der Fall für $t > 1$?

Für $p > 2$ existiert eine Primitivwurzel!

Gesucht ist also eine Primitivwurzel u , das heißt $\text{ord } \bar{u} = \varphi(p^t) = (p-1)p^{t-1}$ in G . Es genügt $u_1, u_2 \in \mathbb{Z}$ mit $p-1 \mid \text{ord } \bar{u}_1$ und $p^{t-1} \mid \text{ord } \bar{u}_2$ zu finden. Wegen $\text{ord } \bar{u}_j \mid \#G = (p-1)p^{t-1}$ gilt $s \mid p-1$. Daraus folgt, für $v_1 := u_1^{p^{t-1}}$, $v_2 := u_2^{p-1}$ ist

$$\text{ord } \bar{v}_1 = \text{ord } \bar{u}_1^{p^{t-1}} = \frac{\text{ord } \bar{u}_1}{\text{ggT}(\text{ord } \bar{u}_1, p^{t-1})} = \frac{(p-1)p^r}{p^r} = p-1.$$

Ebenso: $\text{ord } \bar{v}_2 = p^{t-1}$ (Nachrechnen). Aus Übungsaufgabe 3 (a) Blatt 7 folgt mit $u := v_1 v_2 \pmod{p^t}$, $\text{ord } \bar{u} = (p-1)p^{t-1}$. Bevor wir fortfahren, benötigen wir noch ein Lemma, das wir zum Beweis eines Hilfssatzes benötigen.

Lemma 3.16 ((1 + p)–Lemma)

$p \in \mathbb{P}$, $p > 2$, $r \in \mathbb{N}_+$, $u \in \mathbb{Z}$. Dann gilt: $(1 + up)^{p^{r-1}} \equiv 1 + up^r \pmod{p^{r+1}}$.

Beweis

Beweis via Induktion nach r .

$$r = 1: (1 + up)^{p^{1-1}} = 1 + up \equiv 1 + up^1 \pmod{p^2} \quad \checkmark.$$

$r > 1$: Induktionshypothese (für $r-1$):

$$(1 + up)^{p^{r-2}} \equiv 1 + up^{r-1} \pmod{p^r}.$$

$$\begin{aligned} \implies (1+up)^{p^{r-2}} &= 1 + up^{r-1} + zp^r \text{ mit } z \in \mathbb{Z} \implies (1+up)^{p^{r-1}} = \left((1+up)^{p^{r-2}}\right)^p = \\ &= (1 + (up^{r-1} + zp^r))^p = 1 + \sum_{i=1}^p \underbrace{\binom{p}{i}}_{\in \mathbb{Z}} \underbrace{(up^{r-1} + zp^r)^i}_{=(p^{r-1}(u+zp))^i =: c_i}. \end{aligned}$$

$$\begin{aligned} r \geq 2, i > 2: v_p(c_i) &= v_p\left(\binom{p}{i}\right) + v_p(p^{(r-1)i}) + \underbrace{v_p(u+zp)^i}_{\geq 0} \geq (r-1)i \geq (r-1)r > r+1 \implies \\ p^{r+1} \mid c_1 &\implies c_i \equiv 0 \pmod{p^{r+1}}. \end{aligned}$$

$$\begin{aligned} i = 2: v_p(c_2) &= v_p\left(\frac{p(p-1)}{2}\right) + \underbrace{v_p(p^{2(r-1)})}_{=2(r-1)} + \underbrace{v_p(u+zp)^2}_{\geq 0} \geq 2r-2+1 = 2r-1 \geq r+1 \implies \\ c_2 &\equiv 0 \pmod{p^{r+1}}. \end{aligned}$$

$$i = 1: c_1 = p \cdot p^{r-1}(u+zp) = up^r + zp^{r+1} \equiv up^r \pmod{p^{r+1}}.$$

\implies Behauptung. ■

Hilfssatz

Sei $p \in \mathbb{P}$, $p > 2$, $t \in \mathbb{N}_+$.

- (1) Ist w eine Primitivwurzel mod p , so gilt in $G = (\mathbb{Z}/p^t\mathbb{Z})^\times : p-1 \mid \text{ord } \bar{w}$, $\bar{w} = w + p^t\mathbb{Z}$.
($u_1 = w$ wählbar).
- (2) $\text{ord}(\overline{1+p}) = p^{t-1}$ ($v_2 = 1+p$ wählbar).

Beweis

- (1) Sei $l = \text{ord } \bar{w}$, also $\bar{w}^l = 1$, das heißt $w^l \equiv 1 \pmod{p^t}$. $t \geq 1 \implies w^l \equiv 1 \pmod{p^1} \implies$ in \mathbb{F}_p ist $\bar{w}^l = 1$, $\text{ord } \bar{w} = p-1 \implies p \cdot a \mid l$ (Elementar-Ordnungssatz).
- (2) Folgt aus Lemma 3.16

$(1+p)^{p^{t-1}} \equiv 1 + 1 \cdot p^t \pmod{p^{t-1}} \implies (1+p)^{p^{t-1}} \equiv 1 \pmod{p^t} \implies \overline{1+p^{p^{t-1}}} \implies \text{ord } \overline{1+p} \mid p^{t-1}$. Für $t \geq 2$ ist noch zu zeigen: $(1+p)^{p^{t-2}} \not\equiv 1 \pmod{p^t}$. $(1+p)^{p^{t-2}} \equiv 1 + p^{t-1} \pmod{p^t}$ (nach Lemma 3.16). $\overline{1+p^{p^{t-2}}} = \overline{1 + \underbrace{p^{t-1}}_{\neq 0}} \neq \overline{1} = 1$. ■

Gezeigt (für $p > 2$):

Satz 3.17 (Struktursatz für $(\mathbb{Z}/p^t\mathbb{Z})^\times$, eigentlich ein Theorem)

Sei $p \in \mathbb{P}$, $t \in \mathbb{N}_+$. Dann gilt:

- (1) Falls $p > 2$, so ist $(\mathbb{Z}/p^t\mathbb{Z})^\times$ zyklisch (das heißt, es gibt eine Primitivwurzel $u \pmod{p^t}$, also $(\mathbb{Z}/p^t\mathbb{Z})^\times = \{1, \bar{u}, \dots, \bar{u}^{p^{t-1}(p-1)-1}\}$).
- (2) Falls $p = 2$: $(\mathbb{Z}/2\mathbb{Z})^\times$, $(\mathbb{Z}/4\mathbb{Z})^\times$ zyklisch. Für $t > 2$ ist $(\mathbb{Z}/2^t\mathbb{Z})^\times$ *nicht* zyklisch, doch es gilt: Jedes $\bar{a} \in (\mathbb{Z}/2^t\mathbb{Z})^\times$ lässt sich eindeutig in der Form $\bar{a} = \overline{(-1)}^\varepsilon \cdot \bar{5}^s$ schreiben, mit $\varepsilon \in \{0, 1\}$, $s \pmod{2^{t-2}}$ (eindeutig). $(\mathbb{Z}/2^t\mathbb{Z})^\times$ ist sozusagen bis auf das Vorzeichen $(-1)^\varepsilon$ zyklisch.

3 Kongruenzen und Restklassenringe

Info:

Man kann sagen: Ist $u \in \mathbb{Z}$ Primitivwurzel mod p^2 , so auch mod $p^t \forall t \in \mathbb{N}_+$

Es gibt viele Arbeiten über Primitivwurzeln, z. B. analytische Zahlentheorie (sehr schwierig) gibt Schranken $s(p)$ so, dass in $\{2, \dots, s(p)\}$ PW mod p zu finden.

Artins Vermutung: 2 (oder jedes $n \in \mathbb{N}_+, n \neq 1$) ist Primitivwurzel für ∞ -viele $p \in \mathbb{P}$.

Rechnen in $(\mathbb{Z}/m\mathbb{Z})^x$ auf dem Computer, falls viele Produkte zu berechnen sind.

Primzerlegung $m = p_1^{t_1} \cdot \dots \cdot p_l^{t_l} \quad t_j \in \mathbb{N}_+$

Kodierte $a + m\mathbb{Z} = \bar{a}$ wie folgt:

Berechne vorab PW u_j mod $p_j^{t_j}$

$$\begin{aligned} (\mathbb{Z}/m\mathbb{Z})^x &\rightarrow \prod_{j=1}^l (\mathbb{Z}/p_j^{t_j}\mathbb{Z})^x \\ \alpha = a + m\mathbb{Z} &\mapsto (\dots, a + p_j, \dots) \end{aligned}$$

$$\text{Bijektiv:} \quad \alpha \leftrightarrow (\dots, r(\alpha, j), \dots)$$

$$\alpha \cdot \beta \leftrightarrow (\dots, r(\alpha, j) + r(\beta, j) \bmod p_j^{t_j-1}(p_j - 1), \dots)$$

α^{-1} ähnlich

Zum Rechnen mit großen ganzen Zahlen (Skizze)

Prinzip: Gleichheit in \mathbb{Z} = Kongruenz + passende Abschätzung

Bemerkung: $m \in \mathbb{N}, m > 1$, etwa $2 \nmid m$. Ist $u \equiv v \bmod m$ und $|u| \leq \frac{m}{2}, |v| \leq \frac{m}{2}$, so ist $u = v$.

Grund: u, v sind in Versys_m (symm. Vertretersystem der Reste mod m), also $u = v$.

Wende dies an auf die Berechnung von $f(x), f \in \mathbb{Z}[X_1, \dots, X_n], x = (x_1, \dots, x_n) \in \mathbb{Z}$. Kennt man Schranke $|f(x)| < \frac{m}{2}$ so genügt es $f(x) \bmod m$ auszurechnen.

$f(x) \bmod m$ kann für $m = m_1 \cdot \dots \cdot m_l$ durch Berechnen von $f(x) \bmod m_j =: y_j \quad (j = 1, \dots, l)$ ersetzt werden + 1x chinesischer Restsatz: $y \equiv y_j \bmod m_j$.

Aufgabe:

Berechne mit dem Computer $\det A$ (exakt), $A \in \mathbb{Z}^{n \times n}$

Soll sein n mäßig groß, $A = (a_{ij})$, die a_{ij} mäßig groß.

Naives Verfahren: Gauß-Algorithmus in \mathbb{Q} :

Ärger: Sehr große Integer-Zahlen als Zähler und Nenner entstehen während der Rechnung unkontrolliert. Mögliche bessere Vorgehensweise, etwa $|a_{ij}| \leq s$ (Schranke)

Leibnitzformel: $\det A = \sum_{\pi \in S_n} \text{sgn}(\pi) \prod_{i=1}^n a_{i, \pi(i)}$ liefert Abschätzung $|\det A| \leq s^n \cdot n! \quad (n! = \#S_n)$

Schranke $S = 2 \cdot |\det A| = 2 \cdot s^n \cdot n!$ kann sehr groß sein. Wähle Primzahlen ($\neq 2$) p_1, \dots, p_t (t verschieden) mit $S \leq p_1 \cdot \dots \cdot p_t$. Dann $|\det A| \leq \frac{p_1 \cdot \dots \cdot p_t}{2} = \frac{m}{2}, m = p_1 \cdot \dots \cdot p_t$

Kann oft sein: t mäßig groß, alle p_j mäßig groß. (z. B.: $s = 100, n = 100 \Rightarrow S = 100^{100} \cdot 2 \cdot 100! \leq 2 \cdot 100^{120}$ Es reichen also 130 p_j 's mit $p_j > 100$, diese können < 1000 gewählt werden \Rightarrow in \mathbb{F}_{p_j} kann sehr gut und schnell gerechnet werden!

\Rightarrow Berechnung von $\det \bar{A}, \bar{A} = (\bar{a}_{ij})$ in $\mathbb{F}_{p_j}^{n \times n}$ kann durch Herstellen von Dreiecksform von \bar{A} für mäßig große n schnell berechnet werden. (Durch Arbeiten in Versys_p entstehen niemals große Zahlen!) Das ergibt $y_j \in \text{Versys}_p$ mit $\det A \bmod p_j = y_j$. Es ist dann $y \equiv y_j \bmod p_j$ zu lösen (simultane Kongruenz $m = p_1 \cdot \dots \cdot p_t$). Daher für $y \in \text{Versys}_m$ (symm.) ist $\det A = m \cdot y$ kann sehr groß sein, aber die Kongruenz ergibt sehr große Zahlen nur kontrolliert! (Mäßig große Zahlen, falls man mit γ -adischer Darstellung von $y = \det A, \gamma = (p_1, \dots, p_t, \dots)$ zufrieden ist.