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 $\operatorname{grad} r < \operatorname{grad} m$.

Diese Reste sind eindeutig: Haben wir $a = qm + r = \tilde{q}m + \tilde{r}$ mit $0 \leq r, \tilde{r}, |m|$. Dann ist $(q - \tilde{q})m = \tilde{r} - r \implies |m| \big| \tilde{r} - r$. 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 $\boldsymbol{R} = \mathbb{Z}$)
$m, a, b, \in R$

(1)

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

$$\iff a \mod m = b \mod m$$

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

(2) $\overline{a} := \{b \in R | b \equiv a \mod m\}$ heißt Restklasse modulo m.

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

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

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

(1) $\overline{0} + \overline{0} = \overline{0}$, „gerade + gerade = gerade"

(2) $\overline{0} + \overline{1} = \overline{1}$, „gerade + ungerade = ungerade"

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

Bemerkung:

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

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.

$(i) \implies (iii)$: $r = a \mod m = b \mod m \implies a = qm + r, b = q'm + r$ (Division mit Rest) $\implies a - b = (q - q')m \implies m|a - b$ ■

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 − 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 $a \mod m = b \mod m \iff a = b$, 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) $\overline{R}^\times = \{\overline{a} \in \overline{R} | \operatorname{ggT}(a, m) = 1\}$

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

Definition
$\overline{a} \in \overline{R}^{\times}$ heißt eine prime Restklasse modulo m, $\overline{R}^{\times}$ 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. $\overline{a}+\overline{b} = \overline{a+b} = \overline{b+a} = \overline{b}+\overline{a} \implies (\overline{R}, +)$ ist kommutativ. $0 := 0_{\overline{R}} = \overline{0}$, da $\overline{a}+\overline{0} = \overline{(}a+0) = \overline{a}$. $1_{\overline{R}} = \overline{1}$ ebenso.

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

(2) $\overline{a} \in \overline{R}^{\times} \overset{\text{Def.}}{\iff} \exists x \in R : \overline{x}\overline{a} = 1_{\overline{R}} = \overline{1} \iff 1 \equiv ax \mod m \iff \exists q \in R : 1 = ax + qm \implies \text{ggT}(a, m) = 1$, (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. $\implies \overline{1} = \overline{ax} + \overline{qm} = \overline{ax}$. Resultat: $\overline{a}^{-1} = \overline{x}$ 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 $R/mR = \{\overline{0}, \ldots, \overline{m-1}\}$ und $(R/mR)^{\times} = \{\overline{r} | 0 \leq r < m, \text{ggT}(r, m) = 1\}$, derer es $\varphi(m)$ gibt.

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

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 $K[X]/f \cdot K[X] = \overline{R}$ ein Körper.

Grund: m sei unzerlegbar. Dann $\overline{a} \in \overline{R}$, $\overline{a} \neq 0 = \overline{0} \iff m \not| a \implies \text{ggT}(m, a) = 1$ $(1, m$ sind die einzigen normierten Teiler von m!$) \implies a \in \overline{R}^{\times}$. Es gilt also $\overline{R}^{\times} = \overline{R} \setminus \{0\} \implies \overline{R}$ ist Körper.

$\overline{R} = R/mR \ni \overline{a} = a + Rm := \{a + qm \big| q \in R\}$ Restklasse von a.
Rechne in $\overline{R}$: **Idee**: Kodiere die Restklasse $\overline{a}$ durch den Vertreter $a \mod m$.

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

<u>R = $\mathbb{Z}$</u>:
$\text{Versys}_m = \{0, 1, ..., m-1\}$ „*System Betrag kleinster positiven Reste*" oder $\text{Versys}_m = \{v \in \mathbb{Z} \big| -\frac{m}{2} < r \leq \frac{m}{2}\}$ „*Symmetrisches Restsystem*"

$\underline{\mathrm{R} = K[X]}$:
$\mathrm{Versys}_m = \{f \in K[X] \big| \text{Grad } f < \text{ Grad } m\}$ (Grad $m > 0$)

Klar:

$$\begin{array}{rcl} \mathrm{Versys}_m & \longrightarrow & R/mR \text{ (Ist bijektiv)} \\ r & \longmapsto & \overline{r} \\ a & \longmapsto & \overline{a} \mod m \text{ (Umkehrung)} \end{array}$$

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

$$r \oplus s := r + s \mod m \qquad r \odot s := rs \mod m$$

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

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

$r + s \mod m$ mit 1-Addition: Zahlen $< 2m$

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

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

Vorzug bei $R = K[X]$:

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

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

Versys_m enthält K als Teilkörper (konstante Polynome), da:
$\alpha, \beta \in K \subset K[X] \implies \alpha \odot \beta = \alpha\beta \mod m = \alpha\beta$

Folgerung 3.4
$\overline{R} = K[X]/mK[X]$ ist ein K-Vektorraum der dim $n =$ Grad m mit Basis $1, \overline{X}, \overline{X}^2, ..., \overline{X}^{n-1}$.
Identifiziert man $\alpha \in K$ mit der Restklasse $\overline{\alpha}$, so enthält $\overline{R}$ den Körper R.

Folgerung 3.5
Ist $m \in \mathbb{F}_p[X] = R$ irreduzibel, so ist $R/mR = \overline{R}$ ein Körper mit $q = p^n$ ($n =$ Grad m) Elementen!
Grund: $\mathbb{F}_p$-Basis ist $1, \overline{X}, \overline{X}^2, ..., \overline{X}^{n-1}$.
$\overline{R} = \{\alpha_0 \cdot 1 + \alpha_1 \overline{X} + ... + \alpha_{n-1}\overline{X}^{n-1} \big| \alpha_0, ..., \alpha_{n-1} \in \mathbb{F}_p\}$ mit $\#\overline{R} = p^n$

Zum Rechnen in $\overline{R}$ wird empfohlen $\overline{\alpha} \in \mathbb{F}_p$ durch $r = a \mod p$ zu ersetzen, mit $r \in \mathrm{Versys}_p$.
$f \in \mathrm{Versys}_p[X]$ hat die Form $f = \sum_{i=0}^n c_i X^i$, $c_i \in \mathrm{Versys}_p$.
Bei der Bestimmung von $f + g, f \cdot g$ ist bei allen Rechnungen mit Koeffizienten $c_1, ..., c_n$, $+$ 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 $\mod p$ nehmen.

Beispiel
$\mathbb{F}_3[X]$, $\mathbb{F}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$, $\mathrm{Versys}_3 = \{0, 1, 2\}$

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

Beispiel
$\mathbb{F}_4 = \{\underbrace{0,1}_{\mathbb{F}_2}, \underbrace{\overline{x}}_{=:\varrho}, \overline{x}+1\}$, wenn m irreduzibel in $\mathbb{F}_2[X]$, Grad $f = 2$
$X^2+1 = (X+1)^2$ $(= X^2 + \underbrace{\overline{2}}_{=0} X + 1 = X^2+1$ 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)
$\mathbb{F}_4 = \{0, 1, \varrho, \varrho+1\}$, $\varrho^2 = ?$
$(\overline{X})^2 = \underbrace{\overline{X^2 \mod m}}_{\in \text{Versys}_m} = \overline{X+1} = \overline{X} + 1 = \varrho + 1$
$X^2 - 1 \cdot (X^2+X+1) = -X-1 = X+1$ in $\mathbb{F}_2[X]$
Rechenregel: $\varrho^2 = \varrho + 1 \implies$ Multiplikationstafel

Bemerkung:

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

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

Beispiel
$\overline{R} = \mathbb{Z}/m\mathbb{Z}, z \in \mathbb{Z}$
$z\overline{a} = \overline{za}$ (leicht selbst nachzuweisen) $m \cdot 1_{\overline{R}} = m \cdot \overline{1} = \overline{m} = 0_{\overline{R}}$

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

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

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

$$(z_1z_2)\varrho = z_1(z_2\varrho)$$

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

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

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

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

3.1 Zyklische Gruppen

Aufgabe: Berechne $3^{10^{500}} \mod \underbrace{167}_{=:p}$ (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) $\operatorname{ord}(x) = \min\{n \in \mathbb{N}_+ \big| x^n = 1\}$ heißt „*Ordnung von x*“

(ii) $\#G$ heißt „*Ordnung von G*“

Bemerkung: $\operatorname{ord}(x)$ 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 $\{n \in \mathbb{N}_+ \big| x^n = 1\} = \emptyset$, dann schreibt man $\operatorname{ord}(x) = \infty$

Satz 3.6 (Elementordnungssatz)
Sei G eine endliche Gruppe, $x \in G$, $m, n \in \mathbb{Z}$. Dann gelten:

(i) $x^m = x^n \iff m \equiv n \mod \operatorname{ord}(x)$
Insbesondere $x^m = x^{m \mod \operatorname{ord}(x)}$ und $\mod x^m = 1 \iff \operatorname{ord}(x) \big| m$

(ii) $x^{\#G} = 1$ (d.h. nach (i) $\operatorname{ord}(x) \big| \#G$)

(iii) $\operatorname{ord}(x^m) = \frac{\operatorname{ord}(x)}{\operatorname{ggT}(m, \operatorname{ord}(x))}$

Anwendung:

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

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

Zum Satz von Euler:
$G = (R/Rm)^\times, \#G = \varphi(m)$. $\overline{x} \in G \iff \operatorname{ggT}(x, m) = 1$. Elementordnungssatz (ii) $\implies \overline{1} = 1_g = \overline{x}^{\#G} = \overline{x}^{\varphi(m)} = x^{\varphi(m)} \iff 1 \equiv x^{\varphi(m)} \mod m$

Zum Satz von Fermat:
$\varphi(p) = p - 1$. Aussage klar, wenn $p \big| x (x \equiv 0 \equiv xp)$. $p \nmid x \implies \operatorname{ggT}(p, x) = 1 \implies \overline{x}^{p-1} = \overline{x}^{\#G} = \overline{1} \implies \overline{x}^p = \overline{x} \implies x^p \equiv x \mod p$

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

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

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

(2) $x^{\#G} = 1$. Dies wird in dieser Vorlesung nur für kommutative G benötigt und bewiesen. Betrachte die Abbildung $G \to G$, $x \mapsto y \cdot x$. 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): $\operatorname{ord}(x) \mid \#G$

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

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

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

Bemerkungen:

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

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

Beweis (Der Bemerkung (ii))

„$\implies$“: Klar

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

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 $n = (c_t, c_{t-1}, \ldots, c_0)_2$ 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 $\operatorname{ord}(\alpha)$ für ein $\alpha \in G$: 1,2,4, oder 8.

$$\begin{aligned}
\operatorname{ord}(\alpha) = 1 &\iff \alpha = 1 \\
\operatorname{ord}(\alpha) = 2 &\iff \alpha \neq 1, \alpha^2 = 1 \iff \alpha = -1_G = -1 \\
\operatorname{ord}(\alpha) = 4 &\iff \alpha^4 = 1, \alpha^2 \neq 1 \text{ (d.h. } \alpha \neq \pm 1) \\
\operatorname{ord}(\alpha) = 8 &\iff \alpha^4 \neq 1
\end{aligned}$$

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

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

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

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

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

Laut Ordnungsatz: $3^{10^{500}} \equiv 3^{10^{500} \mod \mathrm{ord}(\overline{3})}$.

Wir brauchen ord(3): $\overline{3}^2 = \overline{9} \neq 1_G \implies \mathrm{ord}(\overline{3}) \neq 1, 2$, $\mathrm{ord}(\overline{3}) = 83 \iff \overline{3}^{83} = 1_G = \overline{1}$. $83 = (1010011)_2 = 64 + 16 + 2 + 1$. 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: $\overline{3}^{83} = \overline{3} \cdot \overline{9} \cdot \overline{133} \cdot \overline{2} \cdot \overline{7182} \cdot \overline{1} = 1_G$. Ergebnis: $\mathrm{ord}(\overline{3}) = 83$.

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

Also: $\overline{3}^{10^{500}} = \overline{3}^{23} = \overline{124} = \overline{-33}$ und somit $3^{100^{500}} = 124 \mod 167$

Satz 3.7 (Mersenne-Teiler-Satz)
Es seien $p, q \in \mathbb{P}$ mit $q \mid M_p = 2^p - 1$. Dann gilt: $q \equiv 1 \mod p$

Beweis
$q \mid M_p \iff M_p = 2^p - 1 \equiv 0 \mod q \iff \overline{2}^p = 1$ in $\mathbb{F}_q^\times = G \implies \mathrm{ord}(\overline{2}) = p$, da 1 nicht geht und $\mathrm{ord}(\overline{2}) \mid p$ nach dem Ordnungsatz. $\mathrm{ord}(\overline{2}) \mid \#G = \varphi(q) = q - 1 \implies q - 1 \equiv 0 \mod p \implies q \equiv 1 \mod p$ ∎

Bezeichnungen:

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

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

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

3.2 Primitivwurzeln

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

Bemerkung: Sei $\alpha \in K$, $f \in R$, $\mathrm{ord}(f) > 0$. 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: $f = q \cdot (X - \alpha) + r$. $\mathrm{grad}\, r < \mathrm{grad}(X - \alpha) = 1 \implies r \in K$ (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)
$f \in K[X]$, $f \neq 0$, $n = \operatorname{grad} f$, so gilt: f hat höchstens n verschiedene Nullstellen in K.

Beweis
$\alpha_1, \ldots, \alpha_l$ 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: $l \leq \operatorname{grad} f$ ■

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

Satz 3.9 (Satz von Lagrange)
Sei $p \in \mathbb{P}$, $f = \sum_{i=0}^{n} c_i X^n \in \mathbb{Z}[X]$. Es gibt ein $j \in \{0, \ldots, n\}$ mit $c_j \not\equiv 0 \mod p$. Dann fallen die „Lösungen“ $x \in \mathbb{Z}$ der Kongruenz

$$f(x) \equiv 0 \mod p$$

in höchstens n verschiedene Restklassen modulo p.

Beweis
Der Satz ist eine Übersetzung des Nullstellenanzahls-Satzes auf Kongruenzen. Betrachte die $\overline{c_j} = \alpha_j \in \mathbb{F}_p \implies \exists j : \overline{c_j} \neq 0 \implies f = \sum_{i=0}^{n} \overline{c_j} X^j \neq 0$ in $\mathbb{F}_p[X]$, $\operatorname{ord}(f) \leq n$. $f(x) = 0 \mod p \iff \overline{f(x)} = f(\overline{x}) = 0_{\mathbb{F}_p}$. 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: $\#\{\alpha \in K \,|\, \operatorname{ord}(\alpha) = \#G\} = \varphi(\#G)$ (φ die Eulersche Funktion)

Bemerkung: Ist $\operatorname{ord}(\alpha) = \#G$, 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 $F_q^\times$ 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 $\alpha = \overline{w}$, $(0 \leq w < p-1)$. Solve w heißen Primitivwurzel modulo p.

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

Für die $d \mid l$, $d \in \mathbb{N}_+$, sei $\lambda(d) = \#\{\alpha \in G \mid \operatorname{ord}(\alpha) = d\}$. Laut Elementordnungssatz gilt: $l = \sum_{d|l} \lambda(d) = \sum_{d|l} \varphi(d)$ (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: $\sum_{d|l} \lambda(d) < \sum_{d|l} \varphi(d)$.

$(*)$ ist klar, wenn $\lambda(d) = 0$. Sei also $\lambda(d) \neq 0 \implies \exists \alpha \in G : \operatorname{ord}(\alpha) = d$. Sei $A = \langle\alpha\rangle = \{1, \alpha, \alpha^2, \ldots, \alpha d - 1\}$. 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. $B = \{\beta \in G \mid \operatorname{ord}(\beta) = d\}$, dann $\beta^d = 1 \implies \beta$ Nullstelle von $X^d - 1 \implies \beta \in A$. $B \subseteq A$.

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

Der folgende Satz ist eine Anwendung des Primitivwurzelsatzes:

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 $x^2 \equiv m \mod p \iff m^{\frac{p-1}{2}} \equiv 1 \mod p$. Solche $m \mod p$ heißen quadratische Reste.

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

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

Beweis
Sei ζ eine Primitivwurzel (Existenz folgt aus dem Primitivwurzelsatz).

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

„$\Longrightarrow$“: 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 $\operatorname{ord}(\zeta) = q - 1$

$\alpha^{\frac{q-1}{2}}$ 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“. $\operatorname{ggT}(m,p) = 1 \implies m^{\frac{p-1}{2}} \equiv -1 \mod p$

3.3 Zifferndarstellung nach Cantor

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

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

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

Satz 3.12 (Ziffernsatz)
Jedes $n \in \mathbb{N}_+$ bzw. $n \in K[X]$, $n \neq 0$ hat eine eindeutige Darstellung

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

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: $n = (z_r, z_{r-1}, \ldots, z_0)_\gamma$. Die Kommata dürfen bei Eindeutigkeit weggelassen werden.

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

Speziallbenennungen:

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

Beispiel

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

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

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

$$n = z_r M_r + z_{r-1} M_{r-1} + ... + z_1 M_1 + z_0 \cdot 1 \tag{3.1}$$

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

Beweis (Ziffernsatz)
Fall (3.1) vorliegt: Wegen $M_k | M_{k+1} | M_{k+2} | ...$:
$n \equiv z_{k-1} M_{k-1} + z_{k-2} M_{k-2} + ... + z_0 \mod M_k$

Speziell: $n \equiv z_0 \mod M_1 = m_0 \implies n - z_0 = n' m_0, n' \in \mathbb{Z}$ 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 $z_0 = n, n = z_0 M_0$ ist $(\star)$
Falls $n \geq m_0, z_0 = (n \mod m_0), n'$ 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 $\gamma' = (m_1', m_2', ...), m_j' = m_{j+1} (j \geq 0)$.

$\exists \gamma'$-adische Darstellung von n':
$n' = z_{r'}' M_{r'}' + z_{r'-1} M_{r'-1}' + ... + z_1' M_1' + z_0' (r' \in \mathbb{N}, z_{r'}' \neq 0)$
$n \leq z_j' < m_j' = m_{j+1} \implies n = n' m_0 + z_0 = z_{r'}' M_{r'+1} + ... + z_1' M_1 + z_0$
Das ist die gesuchte γ'-adische Darstellung von n mit $r := r' + 1, z_j' = z_j + 1 (j = 0, ..., r')$ 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 $n \mod m_0$ 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

$R_j (j = 1, ..., l)$ 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 $S = \prod_{i=1}^{l} R_j = R_1 \times ... \times R_l$ eine algebraische Struktur mit Verknüpfungen (komponentenweise):
$S \ni (a_1, ..., a_l), (b_1, ..., b_l), a_j, b_j \in R_j$
$(a_1, ..., a_l) * (b_1, ..., b_l) := (a_1 * b_1, ..., a_l * b_l)$
$\alpha(a_1, ..., a_l) := (\alpha a_1, ..., \alpha a_l)$ bei K-Vektorräumen.
Sind $_j$ Ringe/Gruppen/Abelsche Gruppen/Vektorräume, so auch S.

Grund: Alles vererbt sich von den Komponenten!
Zum Beispiel Ringe: $0_S = (0_{R_1}, ..., 0_{R_l}), 1_S = (1_{R_1}, ..., 1_{R_l})$, kurz: $0 = (0, ..., 0), 1 = (1, ..., 1)$, $-(a_1, ..., a_l) = (-a_1, ..., -a_l)$
Zum Beispiel Assoziativität:
$((a_1, ..., a_l) * (b_1, ..., b_l)) * (c_1, ..., c_l) = ((a_1 * b_1) * c_1, ..., (a_l * b_l) * c_l) = (a_1, ..., a_l) * ((b_1, ..., b_l) * (c_1, ..., c_l))$

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

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

Falls ein Isomorphismus $\psi : R \to S = \prod_{j=1}^{l} R_j$ vorliegt, so wird das Rechnen in R zurückgeführt auf das gleichzeitig („*parallele*“) Rechnen in dem R_j wie folgt:
$\psi(a) = (a_1, ..., a_l), \psi(b) = (b_1, ..., b_l)$
$a * b = \psi^{-1}(\psi(a * b)) = \psi^{-1}(\psi(a) * \psi(b)) = \psi^{-1}((a_1 * b_1, ..., a_l * b_l))$

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:

$$\begin{aligned} x &\equiv 4 && \bmod 7 \\ x &\equiv 17 - 2 && \bmod 30 \end{aligned}$$

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

$$x \equiv a_j \mod m_j, \ (j = 1, \ldots, l) \tag{3.2}$$

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

Bemerkung: Im Allgemeinen gibt es *keine* Lösung.
$x \equiv a \mod m \implies x \equiv a \mod m$, falls $d \mid m$
System: $x \equiv 1 \mod 4, x \equiv 0 \mod 6 \implies x \equiv 1 \mod 2, x \equiv 0 \mod 2 \implies 1 \equiv 0 \mod 2 \implies$ Widerspruch!

Satz 3.14 (Chinesischer Restsatz, rechnerische Form)
Sei R ein euklidischer Ring, $m_1, ..., m_l \in R$, $a_1, ..., a_l \in R$ derartig, dass $\forall i, j \in \mathbb{Z}$ mit $1 \leq i < j \leq l$ gilt:

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

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

Beweis
$l = 1$: $x = a_1$ oder $x = (a_1 \mod m_1) \iff (x \equiv a_1) \mod m_1$ und $0 \leq x \leq m_1$

$l = 2$: $x \equiv a_1 \mod m_1$. x muss in der Form $x = a_1 + um_1, u \in R$ angesetzt werden.
Idee: Bestimme u so, dass $x \equiv a_2 \mod m_2$. Also in $\overline{R} = R/m_2R$ soll werden:
$\overline{a}_1 + \overline{um}_1 = \overline{a_1 + um_1} = \overline{a}_2$, daher tut es: $\overline{u} = (\overline{a}_2 - \overline{a}_1)\overline{m}_1^{-1}$
Geht, da $\overline{m}_1^{-1}$ existiert und da $\overline{m}_1 \in (R/m_2R)^\times$. Nach dem Restklassensatz: $\overline{m}_1 \in (R/m_2R)^\times \iff \mathrm{ggT}(m_1, m_2) = 1$
Algorithmisch $\overline{u} = \overline{m}_1^{-1}$, u kann mit LinKom-Satz, also euklidischem Algorithmus, bestimmt werden. *Erinnerung*: $\mathrm{ggT}(m_1, m_2) = um_1 + vm_2$, u, v berechnet der Algorithmus.
$1 = \overline{um}_1, \overline{m}_2 = 0, \overline{u} = \overline{m}_1^{-1}$
Für dieses $u \in R$ ist $x = a_1 + um_1$ (eventuell $\mod m, m_2$) die gesuchte Lösung.

$l > 2$: Induktionshypothese löst $x' \equiv a_j \mod m_j (j = 1, ..., l-1)$.
Löse dann $x \equiv x' \mod m_1 \cdot ... \cdot m_{l-1}$ ($\implies x \equiv x' \equiv a_j \mod m_j, j = 1, ..., l-1) \implies x \equiv a_l \mod m_l \implies x$ ist die gesuchte Lösung. ∎

Beispiel
Gegeben sind die Kongruenzen:

$$\begin{aligned} x &\equiv 4 && \mod 7 \\ x &\equiv 19 && \mod 30 \end{aligned}$$

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

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

$$\begin{aligned} x &\equiv 109 && \mod 30 \\ x &\equiv 1 && \mod 11 \end{aligned}$$

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

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

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 $x = (z_{l-1}, \ldots, z_0)_\gamma$

Zum paralellen Rechnen: Seien $R, m_1, \ldots, m_l$ wie im chinesischen Restsatz. Betrachte die Abbildung

$$\begin{gathered} R/mR \to \prod_{j=1}^{l} (R/m_jR) \\ \psi : x + mR \mapsto (\ldots, x + m_jR, \ldots) \end{gathered}$$

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

Wir beobachten: Ist $\psi : A \to B$ 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: $b = (\ldots, a_j + m_jR, \ldots)$. $\psi(x + m_jR) = b$: $(\ldots, x + m_jR, \ldots) = (\ldots, a_j + m_jR, \ldots) = b$. $x + mR$ Urbild von $b \iff \forall j : x + m_jR_j = a_j + m_jR \iff \forall j : x \equiv a_j \mod m_j$. Also:

- ψ surjektiv $\iff \forall b \exists$Lösung $x \equiv a_j \mod m_j$
- ψ injektiv $\iff$ Lösung x 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, $m_1, \ldots, m_l \in R$, $\mathrm{ggT}(m_i, m_j) = 1$ für $i \neq j$. Dann hat man den Ringisomorphismus:

$$\begin{gathered} R/mR \to \prod_{j=1}^{l} (R/m_jR) \\ \psi : x + mR \mapsto (\ldots, x + m_jR, \ldots) \end{gathered}$$

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_jR“

Bemerkung (Theoretische Anwendung): Voraussetzungen wie im Satz. Die Einheitengruppe $(R/mR)^\times$ ist isomorph durch ψ zu $\prod_{j=1}^{l}(R/m_jR)^\times$. 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 eine „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 $f \in \mathbb{Z}[X1, \dots, X_n]$ entscheidet, ob $\mathcal{V}_f(\mathbb{Z}) = \emptyset$ oder $\mathcal{V}_f(\mathbb{Z}) \neq \emptyset$ ist.

Satz von Julia Robison (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 $\forall m \in \mathbb{Z} : f(x) \equiv 0 \mod m$ lösbar $\iff \forall t \in \mathbb{N}_+ \forall p \in \mathbb{P} : f(x) \equiv 0 \mod p^t$ 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: $f(x) \not\equiv 0 \mod m$, so gilt $\mathcal{V}_j(\mathbb{Z}) = \emptyset$, es gibt also keine Lösung.

Beispiel
$f = X_1^2 + X_2^2 - k$, $k \in \mathbb{Z}$, diophanischsche 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 $k \equiv 3 \mod 4$ 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 $p \equiv 1 \mod 4$ 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:

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

Ergebnis: Für $k<0$ oder $k \equiv 7 \mod 8$ 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: $9^x\equiv 0 \mod 9$. $0^3=0$, $(\pm1)^3=\pm1$, $(\pm2)^3=\mp1$, $(\pm3)^3=0$, $(\pm4)^3=\pm1 \implies x^x+x^3\equiv 0,\pm1 \mod 9$. Ergebnis: Für $k\equiv 2,3,4,5,6,7 \mod 9$ hat die Gleichung keine Lösung in $x\in\mathbb{Z}$.

3.5.2 Interpolation

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

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

Das Sytem $f\equiv\beta_j \mod (X-\alpha_j)$ $(j=0,\dots,n) \iff \forall j=0,\dots,n: f(\alpha_j)=\beta_j$ (Vorraussetzung $\alpha_i\neq\alpha_j$ für $i\neq j$, d.h $\mathrm{ggT}(X-\alpha_i,X-\alpha_j)\neq 0$).

Der Chinesische Restsatz ergib 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 $\mathrm{ord}(f)\le n$ 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 (Hermitesche 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 $z:j<\mathrm{grad}(X-\alpha)=1$, 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 $\frac{f^{(j)}(\alpha)}{j!}$.

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

$g_{\alpha,d}$ 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: Gleicheit in $\mathbb{Z}$ entspricht Kongruenz und einer passender Abschätzung.

Bemerkung: $m \in \mathbb{N},\ m > 1$, etwa $2 \nmid m$. Ist $u \equiv v \mod m$ 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 $f(x), f \in \mathbb{Z}[X_1, \ldots, X_n],\ x = (x_1, x_2, \ldots, x_n) \in \mathbb{Z}^n$. Kennt man eine Schranke $|f(x)| < \frac{m}{2}$, so genügt es, $f(x) \mod m$ auszurechnen. $f(x) \mod m$ kann für $m = m_1 \cdot \cdots \cdot m_l$ durch Berechnen von $y_j = f(x) \mod m_j\ (j = 1, \ldots, l)$ ersetzt werden, das ergibt simultane Kongruenz $y = y_j \mod m_j$, 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: $(R/mR)^\times \cong \prod_{j=1}^{l} (R/p_j^{t_j} R)$ (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 zyklich, es existiert eine Primitivwurzel $w \mod p$.

Frage: Wie ist der Fall für $t > 1$?

Für $p > 2$ existiert eine Primitivwurzel!

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

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

Ebenso: $\operatorname{ord} \overline{v}_2 = p^{t-1}$ (Nachrechnen). Aus Übungsaufgabe 3 (a) Blatt 7 folgt mit $u := v_1 v_2 \mod p^t,\ \operatorname{ord} \overline{u} = (p-1)p^{t-1}$. 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: $(1 + up)^{p^{r-1}} \equiv 1 + up^r \mod p^{r+1}$.

Beweis
Beweis via Induktion nach r.

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

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

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

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

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

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

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

$\implies$ Behauptung. ∎

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

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

(2) $\operatorname{ord}(\overline{1+p}) = p^{t-1}$ ($v_2 = 1+p$ *wählbar*).

Beweis

(1) Sei $l=\operatorname{ord}\overline{w}$, also $\overline{w}^l=1$, das heißt $w^l\equiv 1 \mod p^t$. $t\geq 1 \implies w^l\equiv 1 \mod p^1 \implies$ in $\mathbb{F}_p$ ist $\overline{w}^l=1$, $\operatorname{ord}\overline{w}=p-1 \implies p\cdot a\mid l$ (Elementar-Ordnungssatz).

(2) Folgt aus Lemma 3.16

$(1+p)^{p^{t-1}}\equiv 1+1\cdot p^t \mod p^{t-1} \implies (1+p)^{p^{t-1}}\equiv 1 \mod p^t \implies \overline{1+p}^{p^{t-1}} \implies \operatorname{ord}\overline{1+p}\mid p^{t-1}$. Für $t\geq 2$ ist noch zu zeigen: $(1+p)^{p^{t-2}}\neq 1$. $(1+p)^{p^{t-2}}\equiv 1+p^{t-1} \mod p^t$ (nach Lemma 3.16). $\overline{1+p}^{p^{t-2}} = \overline{1}+\underbrace{\overline{p^{t-1}}}_{\neq 0}\neq\overline{1}=1$. ∎

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 $u \mod p^t$, also $(\mathbb{Z}/p^t\mathbb{Z})^\times = \{1,\overline{u},\dots,\overline{u}^{p^{t-1}(p-1)-1}\}$

(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 $\overline{a}\in(\mathbb{Z}/2^t\mathbb{Z})^\times$ lässt sich eindeutig in der Form $\overline{a}=\overline{(-1)}^\varepsilon\cdot\overline{5}^s$ schreiben, mit $\varepsilon\in\{0,1\}, s \mod 2^{t-2}$ (eindeutig). $(\mathbb{Z}/2^t\mathbb{Z})^\times$ ist sozusagen bis auf das Vorzeichen $(-1)^\varepsilon$ zyklisch.

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 $m = p_1^{t_1} \cdot \ldots \cdot p_l^{t_l}$ $t_j \in \mathbb{N}_+$
Kodiere $a + m\mathbb{Z} = \overline{a}$ wie folgt:
Berechne vorab PW u_j mod $p_j^{t_j}$

$$\begin{array}{rcl} (\mathbb{Z}/m\mathbb{Z})^x & \to & \prod_{j=1}^{l} (\mathbb{Z}/p^j\mathbb{Z})^x \\ \alpha = a + m\mathbb{Z} & \mapsto & (\dots, a + p_j, \dots) \end{array}$$

$$\begin{array}{lrcl} \text{Bijektiv:} & \alpha & \leftrightarrow & (\dots, r(\alpha, j), \dots) \\ & \alpha \cdot \beta & \leftrightarrow & (\dots, r(\alpha, j) + r(\beta, j) \bmod p_j^{t_j - 1}(p_j - 1), \dots) \end{array}$$

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 $u \equiv v$ mod 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 $f(x)$ mod m auszurechnen.
$f(x)$ mod m kann für $m = m_1 \cdot \ldots \cdot m_l$ durch Berechnen von $f(x)$ mod $m_j =: y_j$ $(j = 1, \dots, l)$ ersetzt werden + 1x chinesischer Restsatz: $y \equiv y_j$ mod 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 $|\det A| \leq s^n \cdot n!$ $(n! = \#S_n)$
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 $S \leq p_1 \cdot \ldots \cdot p_t$. Dann $|\det A| \leq \frac{p_1 \cdot \ldots \cdot p_t}{2} = \frac{m}{2}$, $m = p_1 \cdot \ldots \cdot p_t$
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 $\det \overline{A}$, $\overline{A} = (\overline{a_{ij}})$ in $\mathbb{F}_{p_j}^{n \times n}$ kann durch Herstellen von Dreiecksform von $\overline{A}$ 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 $\det A \mod p_j = y_j$. Es ist dann $y \equiv y_j$ mod p_j zu lösen (simultane Kongruenz $m = p_1 \cdot \ldots \cdot p_t$). Daher für $y \in \text{Versys}_m$ (symm.) ist $\det A = m$. 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.