

Chinesischer Restesatz — einfachste Form

- $p, q \in \mathbb{Z}_{>0}$ mit $\text{ggT}(p, q) = 1$
- **Bézout-Koeffizienten** $u, v \in \mathbb{Z} : p \cdot u + q \cdot v = 1$
- **also** $p \cdot u \equiv 1 \pmod{q}$ und $q \cdot v \equiv 1 \pmod{p}$
- **für** $b, c \in \mathbb{Z}$ **sei** $x = c \cdot p \cdot u + b \cdot q \cdot v$, **dann gilt**

$$x \equiv b \pmod{p}$$

$$x \equiv c \pmod{q}$$

- **für** $y \in \mathbb{Z}$ **gilt**

$$\begin{cases} y \equiv b \pmod{p} \\ y \equiv c \pmod{q} \end{cases} \Leftrightarrow x \equiv y \pmod{p \cdot q}$$

d.h. es gibt in $\mathbb{Z}_{p \cdot q}$ genau eine Lösung y der simultanen Kongruenzen $y \equiv b \pmod{p}$ und $y \equiv c \pmod{q}$, nämlich $y = x \pmod{p \cdot q}$

1

Chinesischer Restesatz

• Theorem:

Zu paarweise teilerfremden natürlichen Zahlen

m_1, m_2, \dots, m_k **mit** $M = m_1 \cdot m_2 \cdot \dots \cdot m_k$

und Elementen $c_1 \in \mathbb{Z}_{m_1}, c_2 \in \mathbb{Z}_{m_2}, \dots, c_k \in \mathbb{Z}_{m_k}$

gibt es genau ein $c \in \mathbb{Z}_M$ **mit**

$$c \equiv c_i \pmod{m_i} \quad (1 \leq i \leq k)$$

3

Beispiel

- **bestimme** $x \in \mathbb{Z}$ **mit**

$$x \equiv 3 \pmod{5} \quad \text{und} \quad x \equiv 2 \pmod{7}$$

- **berechne mittels erweitertem euklidischen Algorithmus Bézout-Koeffizienten für** $(5, 7)$

$$3 \cdot 5 - 2 \cdot 7 = 1$$

- **es gilt also**

$$3 = 5^{-1} \text{ in } \mathbb{Z}_7 \quad \text{und} \quad -2 = 7^{-1} \text{ in } \mathbb{Z}_5$$

- **für**

$$x = 3 \cdot 7 \cdot (-2) + 2 \cdot 5 \cdot 3 = -42 + 30 = -12$$

gilt dann

$$x \equiv 3 \pmod{5} \quad \text{und} \quad x \equiv 2 \pmod{7}$$

und ebenso für jede Zahl y mit $y \equiv x \pmod{5 \cdot 7}$, also insbesondere auch für $y = 23 \in \mathbb{Z}_{35}$

2

Beweis

- **bestimme Bézout-Koeffizienten** $u_i, v_i \in \mathbb{Z}$ **für** m_i **und** M/m_i $(1 \leq i \leq k)$:

$$m_i \cdot u_i + (M/m_i) \cdot v_i = 1$$

- **für** $x = \sum_{1 \leq i \leq k} c_i \cdot (M/m_i) \cdot v_i$ **gilt**

$$x \equiv c_i \pmod{m_i} \quad (1 \leq i \leq k)$$

- **für** $y \in \mathbb{Z}$ **gilt**

$$y \equiv c_i \pmod{m_i} \quad (1 \leq i \leq k) \quad \Leftrightarrow \quad y \equiv x \pmod{M}$$

d.h. es gibt in \mathbb{Z}_M genau eine Lösung y der simultanen Kongruenzen $y \equiv c_i \pmod{m_i}$ $(1 \leq i \leq k)$, nämlich $y = x \pmod{M}$

4

Beispiel

– bestimme $x \in \mathbb{Z}_{5 \cdot 7 \cdot 11}$ mit

$$x \equiv 3 \pmod{5}, \quad x \equiv 1 \pmod{7}, \quad x \equiv 7 \pmod{11}$$

– eeA liefert Bézout-Koeffizienten

$$31 \cdot 5 - 2 \cdot 77 = 1 \quad \text{also} \quad (-2) \cdot 77 \equiv \begin{cases} 1 \pmod{5} \\ 0 \pmod{7} \\ 0 \pmod{11} \end{cases}$$

$$8 \cdot 7 - 1 \cdot 55 = 1 \quad \text{also} \quad (-1) \cdot 55 \equiv \begin{cases} 0 \pmod{5} \\ 1 \pmod{7} \\ 0 \pmod{11} \end{cases}$$

$$16 \cdot 11 - 5 \cdot 35 = 1 \quad \text{also} \quad (-5) \cdot 35 \equiv \begin{cases} 0 \pmod{5} \\ 0 \pmod{7} \\ 1 \pmod{11} \end{cases}$$

– Lösung

$$x = 3 \cdot (-2) \cdot 77 + 1 \cdot (-1) \cdot 55 + 7 \cdot (-5) \cdot 35 = -1742 \equiv 183 \pmod{5 \cdot 7 \cdot 11}$$

5

Dieses Konstruktionsprinzip ist weit verbreitet. Andere Instanzen sind:

• die Interpolationsformel von LAGRANGE

Zu vorgegebenen (paarweise verschiedenen) Stellen $m_1, m_2, \dots, m_k \in \mathbb{C}$

und Werten $c_1, c_2, \dots, c_k \in \mathbb{C}$

gibt es genau ein Polynom $p(X) = \sum_{0 \leq i < k} p_i X^i$ mit Grad $< k$,

das an den Stellen m_i die vorgegebenen Werte c_i annimmt:

$$p(m_i) = c_i \quad (1 \leq i \leq k)$$

Dieses $p(X)$ kann man angeben

$$p(X) = \sum_{1 \leq i \leq k} c_i \cdot \frac{\prod_{j \neq i} (X - m_j)}{\prod_{j \neq i} (m_i - m_j)}$$

Dabei gilt für die Polynome

$$e_i(X) = \frac{\prod_{j \neq i} (X - m_j)}{\prod_{j \neq i} (m_i - m_j)} \quad \text{die Indikatoreigenschaft } e_i(m_j) = \begin{cases} 1 & \text{für } i = j \\ 0 & \text{für } i \neq j \end{cases}$$

7

Warum funktioniert das?

• die Zahlen $e_i = (M/m_i) \cdot v_i$ ($1 \leq i \leq k$) haben die “Indikatoreigenschaft”

$$e_i \equiv \begin{cases} 1 \pmod{m_i} \\ 0 \pmod{m_j} \text{ für } j \neq i \end{cases} \quad (1 \leq i \leq k)$$

Damit kann man Zahlen mit vorgegebenen Kongruenzeigenschaften (= Werten an den Stellen m_i) mittels Linearkombination konstruieren

• für $x = \sum_{1 \leq i \leq k} c_i \cdot e_i$ gilt

$$x \equiv c_i \pmod{m_i} \quad (1 \leq i \leq k)$$

6

• die Darstellung BOOLEscher Funktionen in disjunktiver Normalform

$\mathcal{B} = \{0, 1\}^n$: BOOLEsche Algebra mit \neg, \vee, \wedge

Jede BOOLEsche Funktion $f : \mathcal{B}^n \rightarrow \mathcal{B}$ kann als BOOLEsches Polynom

$$f(X_1, \dots, X_n) = \bigvee_{\mathbf{b} \in \mathcal{B}^n} f(\mathbf{b}) \cdot e_{\mathbf{b}}(X_1, \dots, X_n)$$

dargestellt werden. Dabei sind für $\mathbf{b} = (b_1, b_2, \dots, b_n) \in \mathcal{B}^n$ die “Minterme”

$$e_{\mathbf{b}}(X_1, \dots, X_n) = \bigwedge_{b_i=1} X_i \wedge \bigwedge_{b_i=0} (\neg X_i)$$

Funktionen mit

$$e_{\mathbf{b}}(a_1, \dots, a_n) = \begin{cases} 1 & \text{für } (b_1, \dots, b_n) = (a_1, \dots, a_n) \\ 0 & \text{für } (b_1, \dots, b_n) \neq (a_1, \dots, a_n) \end{cases}$$

8

Algebraische Version des Chinesischen Restesatzes:

• **Die Abbildung**

$$\Psi : \mathbb{Z}_M \rightarrow \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \dots \times \mathbb{Z}_{m_k}$$

$$a \mapsto (a \bmod m_1, a \bmod m_2, \dots, a \bmod m_k)$$

ist ein Isomorphismus von Ringen, insbesondere auch für die invertierbaren Elemente (Einheiten)

$$\Psi(\mathbb{Z}_M^*) = \mathbb{Z}_{m_1}^* \times \mathbb{Z}_{m_2}^* \times \dots \times \mathbb{Z}_{m_k}^*$$

(Isomorphismus von Gruppen)

• **Bemerkung:** aus der Isomorphie der Einheitengruppen folgt

$$\varphi(M) = \varphi(m_1) \cdot \varphi(m_2) \cdot \dots \cdot \varphi(m_k)$$

d.h. die Multiplikativität der EULERSchen φ -Funktion

Schema der modularen Arithmetik

$$\begin{array}{ccccccc} \mathbb{Z}_M & \xrightarrow{\Psi} & \mathbb{Z}_{m_1} & \times & \mathbb{Z}_{m_2} & \times & \dots & \times & \mathbb{Z}_{m_k} \\ \downarrow_{\text{op}} & & \downarrow_{\text{op}} & & \downarrow_{\text{op}} & & \dots & & \downarrow_{\text{op}} \\ \mathbb{Z}_M & \xleftarrow{\Psi^{-1}} & \mathbb{Z}_{m_1} & \times & \mathbb{Z}_{m_2} & \times & \dots & \times & \mathbb{Z}_{m_k} \end{array}$$

wobei $\text{op} \in \{+, *, \text{inverse}\}$

- Ψ ist eine "Auswertungsabbildung", ihre Umkehrung Ψ^{-1} ist eine "Interpolationsabbildung"

Beispiel

Isomorphismus der Ringe: $\mathbb{Z}_4 \times \mathbb{Z}_9 \simeq \mathbb{Z}_{36}$

	0	1	2	3	4	5	6	7	8	\mathbb{Z}_9
0	0	28	20	12	4	32	24	16	8	
1	9	1	29	21	13	5	33	25	17	
2	18	10	2	30	22	14	6	34	26	
3	27	19	11	3	31	23	15	7	35	
\mathbb{Z}_4										\mathbb{Z}_{36}

Isomorphismus der Einheitengruppen: $\mathbb{Z}_4^* \times \mathbb{Z}_9^* \simeq \mathbb{Z}_{36}^*$

	1	2	4	5	7	8	\mathbb{Z}_9^*
1	1	29	13	5	25	17	
3	19	11	31	23	7	35	
\mathbb{Z}_4^*							\mathbb{Z}_{36}^*

Beispiel: Addition in $\mathbb{Z}_{36} \simeq \mathbb{Z}_4 \times \mathbb{Z}_9$

$$\begin{array}{ccc} \mathbb{Z}_{36} & & \mathbb{Z}_4 \quad \mathbb{Z}_9 \\ (22, 25) & \xrightarrow{\Psi} & (2, 1) \quad (4, 7) \\ \downarrow_{+_{36}} & & \downarrow_{+_4} \quad \downarrow_{+_9} \\ 11 & \xleftarrow{\Psi^{-1}} & 3 \quad 2 \end{array}$$

Beispiel: Multiplikation in $\mathbb{Z}_{36} \simeq \mathbb{Z}_4 \times \mathbb{Z}_9$

$$\begin{array}{ccc} \mathbb{Z}_{36} & & \mathbb{Z}_4 \quad \mathbb{Z}_9 \\ (22, 25) & \xrightarrow{\Psi} & (2, 1) \quad (4, 7) \\ \downarrow_{*_{36}} & & \downarrow_{*_4} \quad \downarrow_{*_9} \\ 10 & \xleftarrow{\Psi^{-1}} & 2 \quad 1 \end{array}$$

Das Schema der modularen Arithmetik

$$\begin{array}{ccccccc} \mathbb{Z}_M & \xrightarrow{\Psi} & \mathbb{Z}_{m_1} & \times & \mathbb{Z}_{m_2} & \times & \dots & \times & \mathbb{Z}_{m_k} \\ \downarrow \mathfrak{f} & & \downarrow \mathfrak{f} & & \downarrow \mathfrak{f} & & \dots & & \downarrow \mathfrak{f} \\ \mathbb{Z}_M & \xleftarrow{\Psi^{-1}} & \mathbb{Z}_{m_1} & \times & \mathbb{Z}_{m_2} & \times & \dots & \times & \mathbb{Z}_{m_k} \end{array}$$

gilt für alle Funktionen \mathfrak{f} , die mit den Ringoperationen verträglich sind ("Homomorphismen"), d.h. aus $\{+, *, \text{inverse}\}$ mittels Komposition entstehen.

Man kann Berechnungen in \mathbb{Z} "modularisiert" ausführen, wenn man M gross genug macht (d.h. genügend viele "kleine" Moduln m_i , z.B. Primzahlen in Maschinenwortgrösse)

Vorteil: Exaktes Rechnen in Bereichen kontrollierter Grösse, Parallelisierung

Beispiel: Inverse in $\mathbb{Z}_{36}^* \simeq \mathbb{Z}_4^* \times \mathbb{Z}_9^*$

$$\begin{array}{ccc} \mathbb{Z}_{36}^* & & \mathbb{Z}_4^* & \mathbb{Z}_9^* \\ 25 & \xrightarrow{\Psi} & 1 & 7 \\ \downarrow \text{inv}_{36} & & \downarrow \text{inv}_4 & \downarrow \text{inv}_9 \\ 13 & \xleftarrow{\Psi^{-1}} & 1 & 4 \end{array}$$

13

Beispiel: Berechnung einer Determinanten

$$A = \begin{bmatrix} -82 & -48 & -11 \\ 38 & -7 & 58 \\ -94 & -68 & 14 \end{bmatrix} \quad \det A = ?$$

Beachte: Determinanten sind "Ringterme", deshalb

$$\det A \equiv \det(A \bmod m) \pmod m$$

und

$$\det(A \bmod m_1 \cdot m_2 \cdot \dots \cdot m_k) \equiv \det(A \bmod m_i) \pmod{m_i} \quad (1 \leq i \leq k)$$

15

Moduln

$$m_1 = 29, m_2 = 31, m_3 = 37, m_4 = 41$$

$$M = m_1 \cdot m_2 \cdot m_3 \cdot m_4 = 1363783$$

Berechnen in den einzelnen \mathbb{Z}_{m_i} ($1 \leq i \leq 4$)

$$A \bmod 29 = \begin{bmatrix} 5 & 10 & 18 \\ 9 & 22 & 0 \\ 22 & 19 & 14 \end{bmatrix} \quad \det(A \bmod 29) = (\det A) \bmod 29 = 11$$

$$A \bmod 31 = \begin{bmatrix} 11 & 14 & 20 \\ 7 & 24 & 27 \\ 30 & 25 & 14 \end{bmatrix} \quad \det(A \bmod 31) = (\det A) \bmod 31 = 20$$

16

$$A \bmod 37 = \begin{bmatrix} 29 & 26 & 26 \\ 1 & 30 & 21 \\ 17 & 6 & 14 \end{bmatrix} \quad \det(A \bmod 37) = (\det A) \bmod 37 = 11$$

$$A \bmod 41 = \begin{bmatrix} 0 & 34 & 30 \\ 38 & 34 & 17 \\ 29 & 14 & 14 \end{bmatrix} \quad \det(A \bmod 41) = (\det A) \bmod 41 = 19$$

17

- Modulare Arithmetik lässt sich sehr effizient z.B. für die exakte Lösung von ganzzahligen Gleichungssystemen mit sehr grossen Koeffizienten einsetzen
- Literaturhinweise
 - J. D. LIPSON,
Elements of Algebra and Algebraic Computing,
Addison-Wesley, Kapitel 8.
 - D. E. KNUTH,
The Art of Computer Programming, vol. 2, (Seminumerical Algorithms),
Addison-Wesley, Abschnitt 4.3.2.
 - J. V.Z. GATHEN, J. GERHARD,
Modern Computer Algebra,
Cambridge University Press, Kap. 5.

19

Modulares Schema

$$\begin{array}{cccccc} \mathbb{Z}_{29 \cdot 31 \cdot 37 \cdot 41} & & \mathbb{Z}_{29} & \mathbb{Z}_{31} & \mathbb{Z}_{37} & \mathbb{Z}_{41} \\ A & \xrightarrow{\Psi} & A \bmod 29 & A \bmod 31 & A \bmod 37 & A \bmod 41 \\ \downarrow \det_M & & \downarrow \det_{29} & \downarrow \det_{31} & \downarrow \det_{37} & \downarrow \det_{41} \\ 7522 & \xleftarrow{\Psi^{-1}} & 11 & 20 & 11 & 19 \end{array}$$

Dieses Schema zeigt

$$\det A \equiv 7522 \pmod{M}$$

Tatsächlich gilt sogar

$$\det A = 7522$$

Das kann man folgern, wenn man weiss, dass $0 \leq \det A < M$ oder $-(M/2) \leq \det A \leq M/2$ ist

(z.B. mittels der Ungleichung von HADAMARD für Determinanten)

18

Was tun, wenn die Moduln nicht teilerfremd sind?

Wegen

$$n \mid (x - a) \wedge d \mid n \Rightarrow d \mid (x - a)$$

gilt

$$x \equiv a \pmod{n} \wedge d \mid n \Rightarrow x \equiv a \pmod{d}$$

und somit gilt

$$\left\{ \begin{array}{l} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{array} \right\} \text{ lösbar} \Leftrightarrow \text{ggT}(m, n) \mid a - b$$

und allgemein für beliebige Moduln m_i ($1 \leq i \leq k$)

$$x \equiv a_i \pmod{m_i} \quad (1 \leq i \leq k) \text{ lösbar} \Leftrightarrow \text{ggT}(m_i, m_j) \mid a_i - a_j \quad (1 \leq i < j \leq k)$$

Die Lösung ist eindeutig modulo $\text{kgV}(m_1, m_2, \dots, m_k)$.

20

Beispiel

- Lösung von

$$\begin{cases} x \equiv 3 \pmod{6} \\ x \equiv 7 \pmod{8} \end{cases}$$

existiert wegen $\text{ggT}(6, 8) = 2 \mid (3 - 7)$.

$$\begin{cases} x \equiv 3 \pmod{6} \\ x \equiv 7 \pmod{8} \end{cases} \Leftrightarrow \begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 0 \pmod{3} \\ x \equiv 7 \pmod{8} \end{cases} \Leftrightarrow \begin{cases} x \equiv 0 \pmod{3} \\ x \equiv 7 \pmod{8} \end{cases} \Leftrightarrow x \equiv 15 \pmod{24}$$

- Lösung von

$$\begin{cases} x \equiv 7 \pmod{9} \\ x \equiv 2 \pmod{12} \end{cases}$$

existiert nicht wegen $\text{ggT}(9, 12) = 3 \nmid (7 - 2)$.

Genauer:

$$\begin{aligned} x \equiv 7 \pmod{9} &\Rightarrow x \equiv 1 \pmod{3} \\ x \equiv 2 \pmod{12} &\Rightarrow x \equiv 2 \pmod{3} \end{aligned}$$

Ergänzende Bemerkung zur Algebra:

- sind $p, q \in \mathbb{Z}_{>0}$ beliebig, so gibt es einen Isomorphismus von Ringen

$$\mathbb{Z}_p \times \mathbb{Z}_q \simeq \mathbb{Z}_{\text{ggT}(p,q)} \times \mathbb{Z}_{\text{kgV}(p,q)}$$

- jede endliche kommutative Gruppe $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \dots \times \mathbb{Z}_{m_k}$ ist isomorph zu genau einer Gruppe

$$\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \dots \times \mathbb{Z}_{d_\ell} \quad \text{mit} \quad 2 \leq d_1 \mid d_2 \mid \dots \mid d_\ell$$

(Elementarteilersatz)

- Isomorphie von endlichen kommutativen Gruppen

$$\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \dots \times \mathbb{Z}_{m_k} \stackrel{?}{\simeq} \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \dots \times \mathbb{Z}_{n_\ell}$$

kann man mittels lokaler Transformationen $(p, q) \mapsto (\text{ggT}(p, q), \text{kgV}(p, q))$ effizient entscheiden, indem man die Indexfolgen (m_1, \dots, m_k) und (n_1, \dots, n_ℓ) in Elementarteilerform transformiert.