

Vorbemerkung: Homorphieprinzip für Ringe

Ringe $\langle R, +_R, *_R, 0_R, 1_R \rangle$ und $\langle S, +_S, *_S, 0_S, 1_S \rangle$
 Abbildung $\Phi : R \rightarrow S$ ist *Homomorphismus*, falls $\forall a, b \in R$

$$\begin{aligned} \Phi(a +_R b) &= \Phi(a) +_S \Phi(b) \\ \Phi(a *_R b) &= \Phi(a) *_S \Phi(b) \\ \Phi(0_R) &= 0_S \\ \Phi(1_R) &= 1_S \end{aligned}$$

Dann gilt

$$\Phi(f_R(a, b, \dots, c)) = f_S(\Phi(a), \Phi(b), \dots, \Phi(c))$$

für alle Funktionen f , die aus $+$, $*$ durch Komposition entstehen (Ringterme).

Φ ist *Isomorphismus*, falls bijektiv.



Schematische Darstellung (*kommutatives Diagramm*)
 für $+$, $*$ und zweistelliges f :

$$\begin{array}{ccc} R \times R & \xrightarrow{\Phi \times \Phi} & S \times S \\ \downarrow +_R, *_R, f_R & & \downarrow +_S, *_S, f_S \\ R & \xrightarrow{\Phi} & S \end{array}$$

Im Folgenden geht es um Homomorphismen

$$\Phi_N : \mathbb{Z} \rightarrow \mathbb{Z}_N : a \mapsto a \bmod N$$

bzw.

$$\Phi_{N,M} : \mathbb{Z}_N \rightarrow \mathbb{Z}_M : a \mapsto a \bmod M \quad (\text{falls } M|N)$$

Das sind die einzigen Homomorphismen, die die Ringe \mathbb{Z} bzw. \mathbb{Z}_N überhaupt zulassen!



Aus einem alten indischen Rechenbuch:

- ▶ Aus Früchten werden 63 gleich grosse Haufen gelegt, 7 Stück bleiben übrig. Es kommen 23 Reisende, unter denen die Früchte gleichässig verteilt werden, so dass keine übrig bleibt. Wieviele waren es?
- ▶ Gesucht ist eine (die kleinste?) natürliche Zahl x mit

$$\begin{aligned} x &\equiv 7 \pmod{63} \\ x &\equiv 0 \pmod{23} \end{aligned}$$

- ▶ Lösung: $x \equiv 322 \pmod{23 \cdot 63} \equiv 322 \pmod{1449}$



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

$$\begin{aligned} x &\equiv b \pmod{p} \\ x &\equiv c \pmod{q} \end{aligned}$$

- ▶ 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 $y = x \pmod{p \cdot q}$



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 $y = 23 \in \mathbb{Z}_{35}$

Aus einem alten chinesischen Rechenbuch:

- ▶ Eine Bande von 17 Räubern stahl einen Sack mit Goldstücken. Als sie ihre Beute teilen wollten, blieben 3 Goldstücke übrig. Beim Streit darüber, wer ein Goldstück mehr erhalten sollte, wurde ein Räuber erschlagen. Jetzt blieben bei der Verteilung 10 Goldstücke übrig. Erneut kam es zum Streit, und wieder verlor ein Räuber sein Leben. Jetzt liess sich endlich die Beute gleichmässig verteilen. Wieviele Goldstücke waren mindestens in dem Sack?
- ▶ Gesucht ist eine (die kleinste?) natürliche Zahl x mit

$$\begin{aligned} x &\equiv 3 \pmod{17} \\ x &\equiv 10 \pmod{16} \\ x &\equiv 0 \pmod{15} \end{aligned}$$

- ▶ Lösung: $x \equiv 3930 \pmod{15 \cdot 16 \cdot 17} \equiv 3930 \pmod{4080}$

Chinesischer Restesatz

- ▶ Theorem:

- ▶ m_1, m_2, \dots, m_k paarweise teilerfremden natürlichen Zahlen ("Moduln"), $M = m_1 \cdot m_2 \cdot \dots \cdot m_k$
- ▶ Elemente $c_1 \in \mathbb{Z}_{m_1}, c_2 \in \mathbb{Z}_{m_2}, \dots, c_k \in \mathbb{Z}_{m_k}$
- ▶ Dann gibt es *genau ein* $c \in \mathbb{Z}_M$ mit

$$\begin{aligned} c &\equiv c_1 \pmod{m_1} \\ c &\equiv c_2 \pmod{m_2} \\ &\vdots \\ c &\equiv c_k \pmod{m_k} \end{aligned}$$

d.h.

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

- ▶ Beweis

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

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

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

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

- ▶ für $y \in \mathbb{Z}$ gilt

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

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 $y = x \pmod{M}$

▶ 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

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

Warum funktioniert das?

- ▶ die Zahlen $e_i = v_i \cdot (M/m_i)$ ($1 \leq i \leq k$) 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

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

Dieses Konstruktionsprinzip ist weit verbreitet. Andere Instanzen sind:

- ▶ Interpolationsformel von LAGRANGE

- ▶ Zu vorgegebenen (paarweise verschiedenen) Stellen $m_1, m_2, \dots, m_k \in \mathbb{C}$
- ▶ und vorgegebenen Werten $c_1, c_2, \dots, c_k \in \mathbb{C}$
- ▶ gibt es genau ein Polynom

$$p(X) = \sum_{0 \leq i < k} p_i X^i \quad \text{mit Grad } \deg p(X) < k,$$

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

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

- ▶ Für die Polynome

$$e_i(X) = \frac{\prod_{j \neq i} (X - m_j)}{\prod_{j \neq i} (m_i - m_j)}$$

gilt die Indikatoreigenschaft

$$e_i(m_j) = \delta_{i,j} = \begin{cases} 1 & \text{für } i = j \\ 0 & \text{für } i \neq j \end{cases}$$

- ▶ Darstellung BOOLEscher Funktionen in disjunktiver Normalform
 - ▶ $\mathbb{B} = \{0, 1\}^n$: BOOLEsche Algebra mit \neg, \vee, \wedge
 - ▶ Jede BOOLEsche Funktion $f : \mathbb{B}^n \rightarrow \mathbb{B}$ kann als BOOLEsches Polynom

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

dargestellt werden.

- ▶ Dabei sind für $\mathbf{b} = (b_1, b_2, \dots, b_n) \in \mathbb{B}^n$ 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

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

für $\mathbf{a} = (a_1, a_2, \dots, a_n) \in \mathbb{B}^n$

Algebraische Version des Chinesischen Restesatzes:

- ▶ Die Abbildung

$$\begin{aligned} \Psi : \mathbb{Z}_M &\rightarrow \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \dots \times \mathbb{Z}_{m_k} \\ a &\mapsto (a \bmod m_1, a \bmod m_2, \dots, a \bmod m_k) \end{aligned}$$

ist ein Isomorphismus von Ringen

- ▶ Insbesondere gilt 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

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: Lösung einer linearen Kongruenz

- ▶ Bestimme die Lösung von $1193 \cdot x \equiv 367 \pmod{31500}$
- ▶ $31500 = 2^2 \cdot 3^2 \cdot 5^3 \cdot 7$
- ▶ Wähle Moduln $m_1 = 4, m_2 = 9, m_3 = 125, m_4 = 7$
- ▶ Die gegebene Kongruenz ist äquivalent zu

$$\begin{aligned} 1 \cdot x &\equiv 3 \pmod{4} \\ 5 \cdot x &\equiv 7 \pmod{9} \\ 68 \cdot x &\equiv 117 \pmod{125} \\ 3 \cdot x &\equiv 3 \pmod{7} \end{aligned}$$

- ▶ Wegen $5^{-1} = 2 \in \mathbb{Z}_4$ und $68^{-1} \equiv 57 \in \mathbb{Z}_{125}$:

$$\begin{aligned} x &\equiv 3 \pmod{4} \\ x &\equiv 2 \cdot 7 \equiv 2 \pmod{9} \\ x &\equiv 57 \cdot 117 \equiv 44 \pmod{125} \\ x &\equiv 1 \pmod{7} \end{aligned}$$

- ▶ Lösung: $x \equiv 22919 \pmod{31500}$



- ▶ Beispiel: Berechnung einer Determinanten

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

- ▶ Homomorphieprinzip: Determinanten sind 'Ringterme', deshalb gilt

$$(\det_{\mathbb{Z}} A) \pmod{m} = \det_{\mathbb{Z}_m}(A \pmod{m})$$

und für $M = m_1 \cdot m_2 \cdot \dots \cdot m_k$

$$(\det_{\mathbb{Z}_M}(A \pmod{M})) \pmod{m_i} = \det_{\mathbb{Z}_{m_i}}(A \pmod{m_i}) \quad (1 \leq i \leq k)$$



Homomorphieprinzip: Determinanten sind Ringterme!

- ▶ $\mathbb{Z} \rightarrow \mathbb{Z}_m : a \mapsto a \pmod{m}$

$$\begin{array}{ccc} \det_{\mathbb{Z}} & \begin{array}{c} A \\ \downarrow \\ \det(A) \end{array} & \xrightarrow{\pmod{m}} \begin{array}{c} A \pmod{m} \\ \downarrow \\ \det(A \pmod{m}) \end{array} \\ & & \det_{\mathbb{Z}_m} \end{array}$$

- ▶ $\mathbb{Z}_M \rightarrow \mathbb{Z}_{m_i} : a \mapsto a \pmod{m_i} \quad (M = m_1 \cdot \dots \cdot m_k)$

$$\begin{array}{ccc} \det_{\mathbb{Z}_M} & \begin{array}{c} A \\ \downarrow \\ \det(A) \end{array} & \xrightarrow{\pmod{m_i}} \begin{array}{c} A \pmod{m_i} \\ \downarrow \\ \det(A \pmod{m_i}) \end{array} \\ & & \det_{\mathbb{Z}_{m_i}} \end{array}$$



- ▶ Moduln :

$$\begin{aligned} m_1 &= 29, m_2 = 31, m_3 = 37, m_4 = 41 \\ M &= m_1 \cdot m_2 \cdot m_3 \cdot m_4 = 1363783 \end{aligned}$$

- ▶ Berechnungen in den einzelnen $\mathbb{Z}_{m_i} \quad (1 \leq i \leq 4)$

- ▶ $m_1 = 29$

$$A \pmod{29} = \begin{bmatrix} 5 & 10 & 18 \\ 9 & 22 & 0 \\ 22 & 19 & 14 \end{bmatrix}$$

$$\det(A \pmod{29}) = (\det A) \pmod{29} = 11$$

- ▶ $m_2 = 31$

$$A \pmod{31} = \begin{bmatrix} 11 & 14 & 20 \\ 7 & 24 & 27 \\ 30 & 25 & 14 \end{bmatrix}$$

$$\det(A \pmod{31}) = (\det A) \pmod{31} = 20$$



- ▶ $m_3 = 37$

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

$$\det(A \bmod 37) = (\det A) \bmod 37 = 11$$

- ▶ $m_4 = 41$

$$A \bmod 41 = \begin{bmatrix} 0 & 34 & 30 \\ 38 & 34 & 17 \\ 29 & 14 & 14 \end{bmatrix}$$

$$\det(A \bmod 41) = (\det A) \bmod 41 = 19$$

Eine andere Sicht der modularen Arithmetik:

- ▶ Gegeben teilerfremde Moduln m_1, m_2, \dots, m_k ,
 $M := m_1 \cdot m_2 \cdot \dots \cdot m_k$
- ▶ Aus den Bézout-Beziehungen

$$u_i \cdot m_i + v_i \cdot \frac{M}{m_i} = 1 \quad (1 \leq i \leq k)$$

hat man $v_i = (M/m_i)^{-1} \in \mathbb{Z}_{m_i}$ und $e_i \equiv v_i \cdot (M/m_i) \in \mathbb{Z}_M$.

- ▶ Seien nun $a \in \mathbb{Z}$ sowie $a_i \in \mathbb{Z}_{m_i} (1 \leq i \leq k)$ mit

$$a \equiv a_1 \cdot e_1 + a_2 \cdot e_2 + \dots + a_k \cdot e_k \pmod{M}$$

- ▶ Anders formuliert: es gibt ein $a_0 \in \mathbb{Z}$ mit

$$a = a_0 \cdot M + a_1 \cdot v_1 \cdot \frac{M}{m_1} + a_2 \cdot v_2 \cdot \frac{M}{m_2} + \dots + a_k \cdot v_k \cdot \frac{M}{m_k}$$

▶ 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)

- ▶ Division durch M ergibt

$$\frac{a}{M} = a_0 + \frac{a_1 \cdot v_1}{m_1} + \frac{a_2 \cdot v_2}{m_2} + \dots + \frac{a_k \cdot v_k}{m_k}$$

- ▶ Indem man jetzt noch Division mit Rest in den Brüchen macht, erhält man eine Darstellung

$$\frac{a}{M} = \alpha_0 + \frac{\alpha_1}{m_1} + \frac{\alpha_2}{m_2} + \dots + \frac{\alpha_k}{m_k}$$

mit $\alpha_0 \in \mathbb{Z}$ und $\alpha_i \in \mathbb{Z}_{m_i} (1 \leq i \leq k)$

- ▶ Diese "modulare" Darstellung (*Partialbruchdarstellung*) der rationalen Zahl a/M ist eindeutig!
- ▶ Solche modularen Darstellungen verwendet man vorteilhaft beim exakten Rechnen mit rationalen Zahlen, die grosse Nenner haben.

Beispiel:

- ▶ $a = 20853, M = 5544 = 7 \cdot 8 \cdot 9 \cdot 11$
- ▶ Mit $m_1 = 7, m_2 = 8, m_3 = 9, m_4 = 11$ ergibt sich

$$\begin{aligned} v_1 &= (8 \cdot 9 \cdot 11)^{-1} \pmod{7} = 1 & a \pmod{7} &= 1 & a \cdot v_1 \pmod{7} &= 1 \\ v_2 &= (7 \cdot 9 \cdot 11)^{-1} \pmod{8} = 5 & a \pmod{8} &= 5 & a \cdot v_2 \pmod{8} &= 1 \\ v_3 &= (7 \cdot 8 \cdot 11)^{-1} \pmod{9} = 7 & a \pmod{9} &= 8 & a \cdot v_3 \pmod{9} &= 2 \\ v_4 &= (7 \cdot 8 \cdot 9)^{-1} \pmod{11} = 5 & a \pmod{11} &= 9 & a \cdot v_4 \pmod{11} &= 1 \end{aligned}$$

- ▶ Darstellung

$$\frac{a}{M} = \frac{20853}{5544} = 3 + \frac{3221}{5544} = 3 + \frac{1}{7} + \frac{1}{8} + \frac{2}{9} + \frac{1}{11}$$



Partialbruchzerlegung für Polynome

- ▶ Betrachten Polynome in der Variablen X über einem Körper k
- ▶ $M(X) \in k[X]$ ein normiertes Polynom
- ▶ $M(X) = m_1(X) \cdot m_2(X) \cdots m_k(X)$
Zerlegung von $M(X)$ in normierte teilerfremde Faktoren
- ▶ Für jedes Polynom $a(X) \in k[X]$ hat die rationale Funktion $a(X)/M(X)$ genau eine Darstellung

$$\frac{a(X)}{M(X)} = \alpha_0(X) + \frac{\alpha_1(X)}{m_1(X)} + \frac{\alpha_2(X)}{m_2(X)} + \cdots + \frac{\alpha_k(X)}{m_k(X)}$$

mit $\alpha_0(X), \dots, \alpha_k(X) \in k[X]$ und $\deg \alpha_i(X) < \deg m_i(X) \ (1 \leq i \leq k)$



- ▶ Modulare Arithmetik lässt sich sehr effizient z.B. für die exakte Lösung von ganzzahligen Gleichungssystemen mit sehr grossen Koeffizienten einsetzen
- ▶ Modulare Arithmetik lässt sich sehr effizient für das exakte Rechnen mit "grossen" rationalen Zahlen einsetzen
- ▶ Die Prinzipien der modularen Arithmetik für \mathbb{Z} übertragen sich wörtlich auf Polynomringe $k[X]$.
- ▶ 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.



Primzahltest-Beispiel

- ▶ \mathbb{Z}_N ist ein Körper $\Leftrightarrow N$ ist Primzahl
- ▶ Allgemein gilt: ein Polynom k -ten Grades hat in einem Körper höchstens k Nullstellen.
- ▶ Die Gleichung $X^2 = 1$ hat in einem Körper genau zwei Nullstellen, nämlich ± 1
 - ▶ Sonderfall: im Körper \mathbb{Z}_2 hat $X^2 = 1$ nur die Nullstelle 1, aber die zählt doppelt (wegen $+1 = -1$)
- ▶ Beobachtet man in einem \mathbb{Z}_N eine Zahl $1 < a < N - 1$ mit $a^2 = 1$, so ist N keine Primzahl!
- ▶ Beispiele:
 - ▶ $N = 8$: in \mathbb{Z}_8 gilt $3^2 = 5^2 = 1$, die Gleichung $X^2 = 1$ hat 4 Lösungen.
 - ▶ $N = 21$: in \mathbb{Z}_{21} gilt $8^2 = 13^2 = 1$, die Gleichung $X^2 = 1$ hat 4 Lösungen.



$$N = 1105 = 5 \cdot 13 \cdot 17$$

EEA:

$$1 \cdot 13 \cdot 17 - 44 \cdot 5 = 1 \Rightarrow e_5 = 221 \equiv \begin{cases} 1 & \text{mod } 5 \\ 0 & \text{mod } 13 \\ 0 & \text{mod } 17 \end{cases}$$

$$2 \cdot 5 \cdot 17 - 13 \cdot 13 = 1 \Rightarrow e_{13} = 170 \equiv \begin{cases} 0 & \text{mod } 5 \\ 1 & \text{mod } 13 \\ 0 & \text{mod } 17 \end{cases}$$

$$(-6) \cdot 5 \cdot 13 + 23 \cdot 17 = 1 \Rightarrow e_{17} = 715 \equiv \begin{cases} 0 & \text{mod } 5 \\ 0 & \text{mod } 13 \\ 1 & \text{mod } 17 \end{cases}$$

Die Gleichung $X^2 = 1$ hat in $\mathbb{Z}_{1105} \cong \mathbb{Z}_5 \times \mathbb{Z}_{13} \times \mathbb{Z}_{17}$ insgesamt $2^3 = 8$ Lösungen ($\mathbb{Z}_5, \mathbb{Z}_{13}, \mathbb{Z}_{17}$ sind Körper).

$\mathbb{Z}_5 \times \mathbb{Z}_{13} \times \mathbb{Z}_{17}$	\leftrightarrow	\mathbb{Z}_{1105}
$(+1, +1, +1) = (1, 1, 1)$	\leftrightarrow	$e_5 + e_{13} + e_{17} = 1$
$(+1, +1, -1) = (1, 1, 16)$	\leftrightarrow	$e_5 + e_{13} - e_{17} = 781$
$(+1, -1, +1) = (4, 12, 1)$	\leftrightarrow	$e_5 - e_{13} + e_{17} = 766$
$(-1, +1, +1) = (4, 1, 1)$	\leftrightarrow	$-e_5 + e_{13} + e_{17} = 664$
$(+1, -1, -1) = (1, 12, 16)$	\leftrightarrow	$e_5 - e_{13} - e_{17} = 441$
$(-1, +1, -1) = (4, 1, 16)$	\leftrightarrow	$-e_5 + e_{13} - e_{17} = 339$
$(-1, -1, +1) = (4, 12, 1)$	\leftrightarrow	$-e_5 - e_{13} + e_{17} = 324$
$(-1, -1, -1) = (4, 12, 16)$	\leftrightarrow	$-e_5 - e_{13} - e_{17} = 1104$

MILLER-RABIN-Test

- ▶ $N - 1 = 2^t \cdot u$ mit $t \geq 1$ und u ungerade
- ▶ Wähle $a \in \mathbb{Z}_N$ mit $\text{ggT}(a, N) = 1$
- ▶ Berechne durch fortgesetztes Quadrieren in \mathbb{Z}_N :

$$a^u \mapsto a^{2 \cdot u} \mapsto a^{4 \cdot u} \mapsto \dots \mapsto a^{2^t \cdot u} = a^{N-1}$$
- ▶ Falls in dieser Folge die 1 nicht auftaucht, ist N keine Primzahl (FERMAT!)
- ▶ Falls die 1 auftaucht mit Vorgänger $\neq -1$, ist N keine Primzahl (\mathbb{Z}_N ist kein Körper)
- ▶ Im Erfolgsfalle: a ist "Zeuge" für die Nicht-Primheit von N
- ▶ MILLER-RABIN: falls N nicht prim, sind solche Zeugen häufig!

Beispiel: $N = 1105, a = 2$

- ▶ $N - 1 = 1104 = 2^4 \cdot 69$, also $t = 4, u = 69$
- ▶ Ordnungen

$$\begin{aligned} \text{ord}_5(2) &= 4 = \phi(5) \\ \text{ord}_{13}(2) &= 12 = \phi(13) \\ \text{ord}_{17}(2) &= 8 \mid 16 = \phi(17) \end{aligned} \Rightarrow \text{ord}_{1105}(2) = \text{kgV}(4, 12, 8) = 24$$
- ▶ Berechnung von 2^{69} in \mathbb{Z}_{1105} bei Kenntnis der Faktorisierung (!)

$$\begin{aligned} \mathbb{Z}_5 &: 2^{69} = 2^1 = 2 \\ \mathbb{Z}_{13} &: 2^{69} = 2^9 = 5 \\ \mathbb{Z}_{17} &: 2^{69} = 2^5 = 15 \end{aligned} \Rightarrow 2^{69} = 2 \cdot e_5 + 5 \cdot e_{13} - 2 \cdot e_{17} = -138 = 967 \in \mathbb{Z}_{1005}$$

▶ Test durch Quadrieren

$$\begin{array}{l} \mathbb{Z}_5 \times \mathbb{Z}_{13} \times \mathbb{Z}_{17} \\ (2^{69}, 2^{69}, 2^{69}) = (2, 5, 15) \leftrightarrow 2 \cdot e_5 + 5 \cdot e_{13} - 2 \cdot e_{17} = 967 \\ (2^2, 5^2, 5^2) = (4, 12, 4) \leftrightarrow 4 \cdot e_5 - e_{13} + 4 \cdot e_{17} = 259 \\ (4^2, 12^2, 4^2) = (1, 1, 16) \leftrightarrow e_5 + e_{13} - e_{17} = 781 \\ (1^2, 1^2, 16^2) = (1, 1, 1) \leftrightarrow e_5 + e_{13} + e_{17} = 1 \end{array}$$

▶ Fazit: $a = 2$ bezeugt, dass $N = 1105$ keine Primzahl ist, denn

$$2^{4 \cdot 69} = 781 \neq 1 \quad \text{und} \quad 2^{8 \cdot 69} = (2^{4 \cdot 69})^2 = 1 \quad \text{in} \quad \mathbb{Z}_{1105}$$



▶ Aus einem alten indischen Lehrbuch der Astronomie und Mathematik:

- ▶ Man bestimme die kleinste positive Zahl, die bei Division durch 3,4,5 und 6 die Reste 2,3,4, bzw. 5 lässt.
- ▶ Lösung: $x = 59$

▶ Aus FIBONACCIS *Liber abbaci*:

- ▶ Man bestimme die kleinste positive Zahl, die bei Division durch 2,3,4,5,6 jeweils den Rest 1 lässt und durch 7 teilbar ist
- ▶ Lösung: $x = 301$

▶ Die Moduln sind nicht mehr teilerfremd!



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:

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

▶ Allgemein für beliebige Moduln m_i ($1 \leq i \leq k$)

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

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



Beispiele

▶ Lösung von

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

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

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

▶ 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.