Security

- LV 4120 und 7240 -

Algebraische Strukturen und elementare Zahlentheorie

- Terminologie und Grundsätze der elementaren Zahlentheorie
- Herausstellung einer algebraischen Struktur
- Rechenregeln der modularen Arithmetik
- Zahlentheoretische Funktionen und Algorithmen
- Primzahlen und Primfaktorzerlegung
- Vertraulichkeitsschutz mittels einer Stromchiffre

Kap. 4: Algebraische Strukturen und elementare Zahlentheorie

Teil 1: Algebraische Strukturen und modulare Arithmetik

- Nomenklatur
- Algebraische Strukturen
  - Monoid
  - Gruppe
  - Ringe und Körper
- Modulare Arithmetik
  - Ganzzahlige Division (div und mod)
  - Teilbarkeit
  - Kongruenzen

N Menge der nichtnegativen ganzen Zahlen
$\mathbf{N} := \{0, 1, 2, 3, \cdots\}$

N+1 Menge der natürlichen (positiven ganzen) Zahlen
$\mathbf{N+1} := \{1, 2, 3, \cdots\} = \mathbf{N} \setminus \{0\}$

Z Menge der ganzen Zahlen
$\mathbf{Z} := \{0, \pm 1, \pm 2, \pm 3, \cdots\}$

P Menge der Primzahlen
$\mathbf{P} := \{2, 3, 5, 7, 11, 13, \cdots\}$

Q Menge der rationalen Zahlen (abb. oder period. nicht abb. Dezimalbrüche)
$\mathbf{Q} := \{a / b \mid a, b \in \mathbf{Z}, b \neq 0, ggT(a, b) = 1 \text{ (teilerfremd)}\}$

I Menge der irrationalen Zahlen (nicht-period. nicht abb. Dezimalbrüche)

$\mathbf{I} := \{\sqrt[n]{p} \mid p \in \mathbf{P};\ n = 2, 3, 4, \cdots ; \sin(\pi/4) ; e ; \pi ; \cdots\}$

R Menge der reellen Zahlen

$\mathbf{R} := \mathbf{Q} \cup \mathbf{I}$

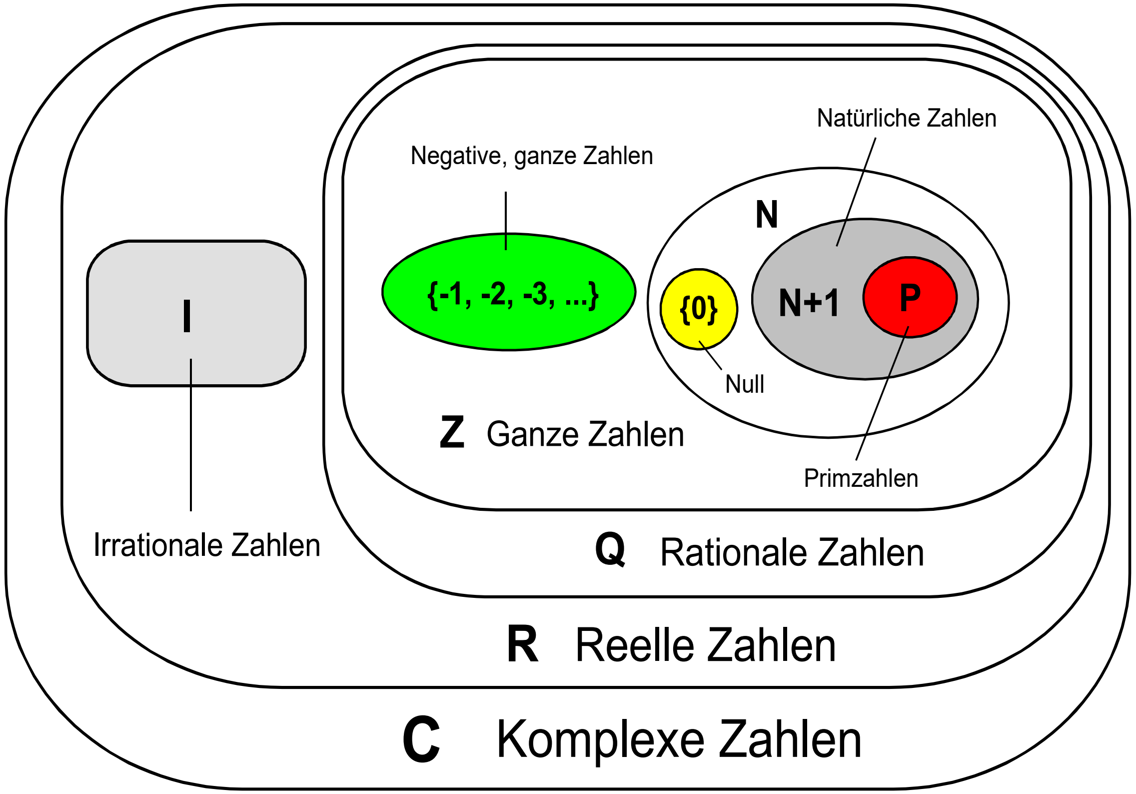
C Menge der komplexen Zahlen

$\mathbf{C} := \{a + j\, b \mid a, b \in \mathbf{R} ;\ j^2 = -1\}$

$\mathbf{Z_m}$ Restklassenring modulo m

$\mathbf{Z_m} := \{0, 1, 2, 3, \cdots, m - 1\}$

Es gelten die Zusammenhänge: $\mathbf{N} \subset \mathbf{Z} \subset \mathbf{Q} \subset \mathbf{R} \subset \mathbf{C}$ **und** $\mathbf{R} = \mathbf{Q} \cup \mathbf{I}$



$$[k{:}m] := \begin{cases} 0\ , & \text{falls } k > m \\ \{z \mid z \in \mathbf{Z}\ ,\ k \le z \le m\}\ , & \text{sonst} \end{cases} \qquad k,\ m \in \mathbf{Z}$$

n | k n teilt k

$\Rightarrow (\exists\ x \in \mathbf{Z})\ \ k = x \cdot n$

n ∤ k n teilt k nicht

$\Rightarrow (\forall\ x \in \mathbf{Z})\ \ k \neq x \cdot n$

ggT(n, k) der größte gemeinsame Teiler von n und k

kgV(n, k) das kleinste gemeinsame Vielfache von n und k

n mod d Divisionsrest, wenn man n durch d teilt

ϕ(m) EULERsche **ϕ**-Funktion
(gibt die Anzahl derjenigen natürlichen Zahlen $n < m$ an, die teilerfremd zu m sind; $m, n \in \mathbf{N}$)

a und b teilerfremd heißt: **ggT**(a, b) = 1

Anmerkungen zum Sprachgebrauch:

- Eine **Algebra** (Plural: Algebren) definiert Elemente und Operatoren sowie Regeln bzw. Eigenschaften (**Axiome**) in bezug auf deren Verknüpfung (abgeschlossene Arithmetik).
- Eigenschaften sind beispielsweise die Existenz eines **neutralen Elementes e** (0 oder 1) oder die Existenz von **inversen Elementen a′** (– a bzw. a^{-1}).
- Regeln betreffen die **Assoziativität** und die **Kommutativität** bzgl. eines Operators oder die **Distributivität** bzgl. zweier Operatoren.
- Wir benutzen im folgenden die Operatoren + (**Addition**) und • (**Multiplikation**) sowie die Quantoren ∃ (**Existenzquantor**) und ∀ (**Allquantor**).

  Beispiele: $\exists\ x \in B\ :\ p(x)$ ist wahr! $\forall\ x \in B\ :\ p(x)$ ist wahr!

$< \mathbf{M}, \circ >$:= algebraisches System (hier: **Monoid**)

$\mathbf{M}$ = Nichtleere Menge $\{a, b, c, ...\}$ der Operanden

$\circ$ = Operator (gebildet auf Elementpaare aus **M**)

hier: $\circ = \{+ , \bullet \}$

mit

1) $a, b \in \mathbf{M} \quad \Rightarrow \quad a \circ b \in \mathbf{M}$

2) $a, b, c \in \mathbf{M} \quad \Rightarrow \quad (a \circ b) \circ c = a \circ (b \circ c)$ **Assoziativ-Gesetz**

3) $a \in \mathbf{M} \quad \Rightarrow \quad \exists\, \mathbf{e}$ mit $a \circ \mathbf{e} = \mathbf{e} \circ a = a$

d. h. es existiert ein **neutrales Element e** (0 bzw. 1) in bezug auf die Operatoren + und $\bullet$.

$< \mathbf{G}, \circ >$:= algebraisches System (hier: **Gruppe**)

G = Nichtleere Menge {a, b, c, ...} der Operanden

$\circ$ = Operator (gebildet auf Elementpaare aus **G**)

hier: $\circ = \{+ , \bullet \}$

wenn

1) $< \mathbf{G}, \circ >$ ist ein **Monoid**, d. h. $\exists\ \mathbf{e} = 0$ bzw. 1

2) $a, b \in \mathbf{G} \quad \Rightarrow \quad a \circ b = b \circ a$ **Kommutativ-Gesetz**

(vgl. Abelsche Gruppe)

3) $a \in \mathbf{G} \quad \Rightarrow \quad \exists\ \mathbf{a'}$ mit $a \circ \mathbf{a'} = \mathbf{e}$

d. h. es existiert ein **inverses Element a′** = – a bezüglich der Addition und ein **inverses Element a′** = a^{-1} bezüglich der Multiplikation.

$< \mathbf{R}, +, \bullet >$:= algebraisches System (hier: **Ring**)

R = Nichtleere Menge $\{a, b, c, ...\}$ der Operanden

$+, \bullet$ = Operatoren (gebildet auf Elementpaare aus **R**)

wenn

1) $< \mathbf{R}, + >$ ist eine **kommutative Gruppe**, d. h. $\exists\ \mathbf{e} = 0$ & $\exists\ \mathbf{a'} = -a$

2) $a, b, c \in \mathbf{R} \Rightarrow a \bullet (b + c) = (a \bullet b) + (a \bullet c)$ **Distributiv-Gesetz**

3) $< \mathbf{R}, \bullet >$ ist ein **Monoid**, d. h. für $a \in \mathbf{R}$: $\exists\ \mathbf{e} = 1$ aber $\overline{\exists}\ \mathbf{a'} = a^{-1}$

d. h. es existiert zwar ein **inverses Element a′** = – a bezüglich der Addition aber <u>keine</u> **multiplikative Inverse**.

$< \mathbf{K}, +, \bullet >$:= algebraisches System (hier: **Körper**)

$\mathbf{K}$ = Nichtleere Menge $\{a, b, c, ...\}$ der Operanden

$+ , \bullet$ = Operatoren (gebildet auf Elementpaare aus **K**)

... ist ein **kommutativer Ring** mit Einselement, in dem jedes von Null verschiedene Element **invertierbar** ist, d. h. für

$$a \in \mathbf{K} \text{ mit } a \neq 0 \quad \Rightarrow \quad \exists\, \mathbf{a^{-1}} \in \mathbf{K} \text{ mit } a \bullet \mathbf{a^{-1}} = 1$$

Satz:

Jeder Körper $< \mathbf{K}, +, \bullet >$ und jeder Ring $< \mathbf{R}, +, \bullet >$ ist **nullteilerfrei** (Integritätsbereich), d. h. für $\forall\, x, y \in \mathbf{K} \setminus \{0\}$ bzw. $\forall\, x, y \in \mathbf{R} \setminus \{0\}$ gilt:

$$x \bullet y \neq 0$$

Satz:

$\mathbf{Z}_m := \{0, 1, ..., m - 1\}$ ist **ganau dann** ein Körper, wenn **m** eine Primzahl ist, d. h.: $\mathbf{Z}_p$ mit $p \in P$ ist ein Körper. (Beweis siehe Übung!)

Lemma:

Jeder Körper ist ein Ring. (Beweis siehe Übung!)

Definition:

Eine Algebra < **HG**, ○ > heißt **Halbgruppe**, wenn sie in Bezug auf die Operation ○ dem Assoziativgesetz genügt.

Sie wird **kommutative Halbgruppe** genannt, wenn die Operation ○ zusätzlich kommutativ ist.

Struktur					Bez.	Formel (Axiom)	A
Algebra (A, + ,•)		Algebra (A, +)					N+1 Z Q
Körper	Ring	abelsche Gruppe	additive Gruppe	HG	assoz.	a + (b + c) = (a + b) + c	x x x
					∃ 0	0 + a = a	- x x
					∃ - a	a + (- a) = 0	- x x
					komm.	a + b = b + a	x x x
					distri.	a (b + c) = a b + a c	x x x
		Algebra (A_o ,•)					
		abelsche Gruppe	multipl. Gruppe	HG	assoz.	a (b c) = (a b) c	x x x
	Einselem.				∃ 1	1 a = a	x x x
					∃ a -1	a a^{-1} = 1	- - x
					komm.	a b = b a	x x x

Restklassenring ist ein algebraisches System mit einer nichtleeren Menge von Elementen und **zwei** Operatoren ($\oplus$, $\otimes$), die auf die Elemente angewendet werden.

Anmerkung:

Wir sprechen oft nur von einem Ring $\mathbf{Z_m} := \{0, 1, 2, 3, \cdots, m - 1\}$, meinen aber den Restklassenring $< \mathbf{Z_m} , \oplus , \otimes >$, d. h. einen kommutativen Ring – auch „Ring von Integers modulo m“ genannt. Es ist heute bei weitem das wichtigste algebraische System der modernen Kryptographie.

Beispiel: $\mathbf{Z_2} := \{0, 1\}$; es gilt das Assoziativ-, Kommutativ- und Distributiv-Gesetz!

$0 \oplus 1 = 1$	$0 \otimes 1 = 0$
$1 \oplus 0 = 1$	$1 \otimes 0 = 0$
$0 \oplus 0 = 0$	$0 \otimes 0 = 0$
$1 \oplus 1 = 0$	$1 \otimes 1 = 1$

Ganzzahlige Division (Division mit Rest)

- Beim Dividieren einer natürlichen Zahl a durch eine natürliche Zahl b bleibt ein Rest $r \in \{0, 1, ..., b-1\}$.

  Beispiel: $17 : 3 = 5$ Rest **2** weil $17 = 5 \cdot 3 + \mathbf{2}$

  $12 : 3 = 4$ Rest **0** weil $12 = 4 \cdot 3 + \mathbf{0}$

- Der Divisionsrest ist immer eindeutig und es gilt:

  Satz:

  Seien $a, b \in \mathbf{N}$ und $b > 0$. Dann gibt es eindeutige natürliche Zahlen q und r mit

  $$a = q \cdot b + r \quad \text{sowie} \quad 0 \leq r < b.$$

  Man nennt q den Quotient, b den Divisor und r den Divisionsrest.

Mathematica

- In dem Computeralgebrasystem Mathematica gibt es die Funktionen

  Mod[a, b] und Quotient[a, b]

  mit der Eigenschaft

  $$a = \text{Quotient}[a, b] \cdot b + \text{Mod}[a, b].$$

- Quotient[a, b] $\in$ **Z** ist der ganzzahlige Anteil von a / b. a und b dürfen beliebige reelle Zahlen sein mit $b \neq 0$.
- Zahlenbeispiel:

  Quotient[12345678, 3456] = 3572

  Mod[12345678, 3456] = 846

Definition: Seien a, b $\in$ **Z** und sei $a = q \cdot b + r$ mit $0 \leq r < b$.

Dann schreibt man $r = a \bmod b$.

Zwei Zahlen a, b $\in$ **Z** heißen **restgleich**, wenn $a \bmod n = b \bmod n$.

Man schreibt: $a \equiv b \bmod n$

und sagt: a ist **kongruent** zu b modulo n.

Beispiele:

$19 \equiv 12 \bmod 7 = 5$

2, 5, 8, 11, ... sind paarweise kongruent modulo 3

Definition: Sei n $\in$ **N**. Dann ist: $\mathbf{Z_n} := \mathbf{Z} / n\mathbf{Z} := \{0, 1, ..., n - 1\}$

Man spricht bei $\mathbf{Z_n}$ von einem **kommutativen Ring**.

Teilbarkeit

Es seien n, d $\in \mathbf{Z}$; $d \neq 0$.

- n heißt durch d teilbar $\Leftrightarrow$ $(\exists\, q \in \mathbf{Z})\;\; n = q \cdot d$
  Schreibweise: $\mathbf{d \mid n}$ (in Worten: d teilt n)
- Ist n nicht durch d teilbar, so schreiben wir $\mathbf{d \nmid n}$.
  $d = 0$ ist als Teiler nie zugelassen.

Satz:

$$0 \mid a \;\Leftrightarrow\; a = 0$$

$$a \mid b \text{ und } b \mid a \;\Rightarrow\; a = \pm\, b$$

$$(t \mid a \wedge t \mid b) \;\Rightarrow\; (\forall\, x, y \in \mathbf{Z})\;\; t \mid (a \cdot x + b \cdot y)$$

Euklidische Divisions-Theorem

Es seien $n, d \in \mathbf{Z}$; $d \neq 0$.

$\Rightarrow$ $(\exists\, q, r \in \mathbf{Z})$ $n = q \cdot d + r$; $0 \leq r < |d|$

q und r sind dabei eindeutig bestimmt.

Man nennt: d = Divisor; n = Divident; q = Quotient; r = Divisionsrest.

Notation: $r = R_d(n) = n \bmod d$

Sätze: $R_{-d}(n) = R_d(n)$

$\mathbf{R_d(n + i \cdot d) = R_d(n)}$ **Fundamental Property of Remainders!** $(i \in \mathbf{Z})$

Größte gemeinsame Teiler

Definition: Der größte gemeinsame Teiler der Integerzahlen n_1 und n_2 (nicht beide gleich Null) ist der größte Integerwert t, der sowohl n_1 als auch n_2 teilt.

t heißt größter gemeinsamer Teiler von n_1 und n_2 .

$\Rightarrow \; (\exists\, t = \max\{\tau\}) \;\Big|\; (\tau \mid n_1 \wedge \tau \mid n_2)$

Notation: $\mathbf{t := ggT(n_1, n_2)}$

Sätze: $1 \leq ggT(n_1, n_2) \leq \min\{|n_1|, |n_2|\}$

$ggT(n_1, 0) = |n_1|$

Weitere Sätze:

Ist $ggT(a, b) = 1$, so werden a und b auch <u>teilerfremd</u> oder <u>relativ prim</u> bezeichnet.

$$ggT(n_1, n_2) = ggT(n_1 + i \cdot n_2, n_2)$$

Fundamental Property of Greatest Common Divisors!

$$ggT(n_1, n_2) = ggT(n_2, R_{n2}(n_1))$$

Euklid´s gcd Recursion!

Trickreich und nützlich sind noch folgende Sätze, bei denen $a, b, c \in Z$ gilt:

- $a \mid c$ und $b \mid c \;\Rightarrow\; a \cdot b \mid c \cdot \mathrm{ggT}(a, b)$
- $a \mid b \;\Leftrightarrow\; \mathrm{ggT}(a, b) = \mid a \mid$
- $\mathrm{ggT}(a \cdot c, b \cdot c) = \mid c \mid \cdot \mathrm{ggT}(a, b)$
- $a \mid b \cdot c$ und $\mathrm{ggT}(a, b) = 1 \;\Rightarrow\; a \mid c$

(Zugehörige Beweise siehe Übungen!)

Kleinste gemeinsame Vielfache

Lösungsverfahren:

Das kleinste gemeinsame Vielfache von zwei ganzen Zahlen a und b können wir vereinfacht so bestimmen:

1. Wähle die größere der beiden Zahlen aus.
2. Bilde das 1fache, 2fache, 3fache, ... dieser Zahl. Prüfe jeweils, ob es auch ein Vielfaches der anderen Zahl ist.
3. Das erste gemeinsame Vielfache ist das sogenannte kleinste gemeinsame Vielfache **kgV** der beiden Zahlen.

Satz: $\mathrm{kgV}(a, b) \cdot \mathrm{ggT}(a, b) = a \cdot b$

Beispiel:

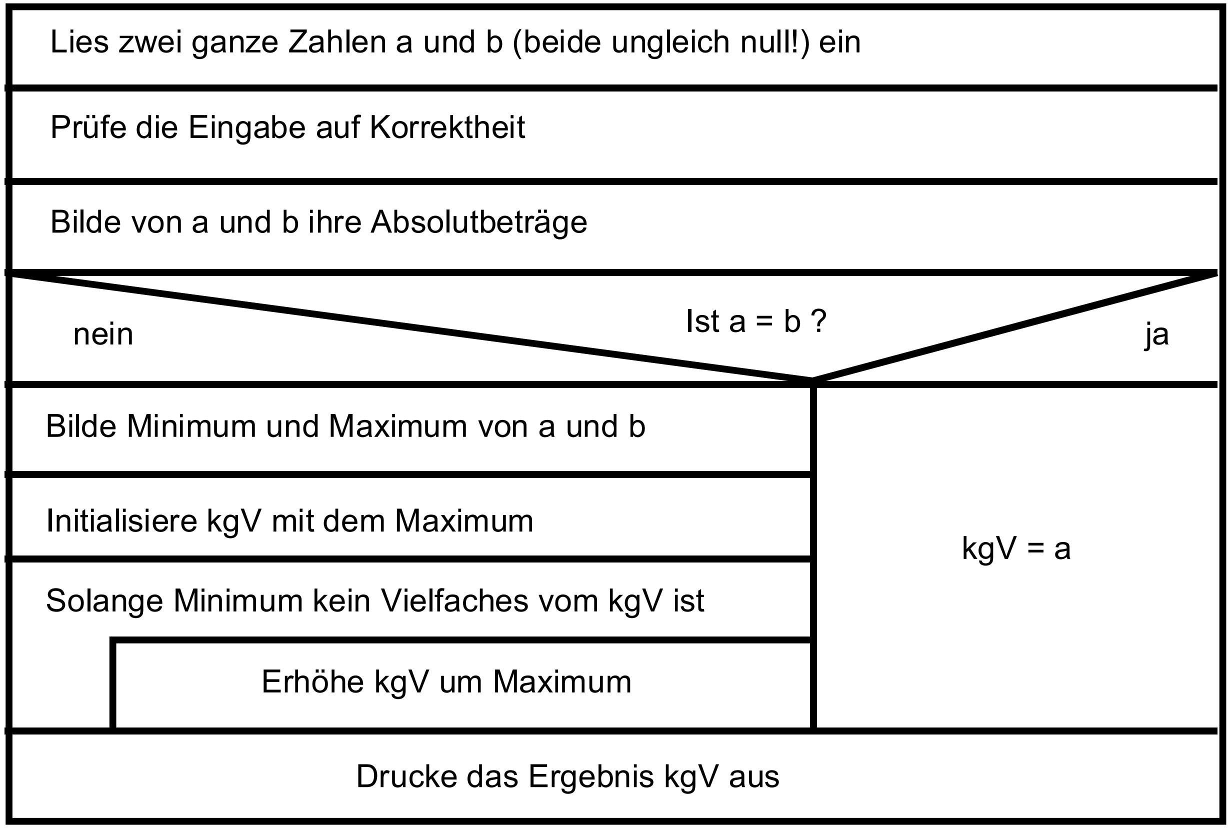
Berechnung von kgV(10, 8)

1. Wähle 10.
2. Prüfe:

   Ist 10 Vielfaches von 8? → nein
   Ist 20 Vielfaches von 8? → nein
   Ist 30 Vielfaches von 8? → nein
   Ist 40 Vielfaches von 8? → ja
3. Ergebnis: **kgV(10, 8) = 40**

Überprüfung: Weil ggT(10, 8) = 2 $\Rightarrow$ $\text{kgV}(a, b) \cdot \text{ggT}(a, b) = 80 = a \cdot b$

Struktogramm:



Kongruenzen

Es seien n, r, d $\in$ **Z**; $d \neq 0$.

Dann heißen n und r kongruent modulo d $\Leftrightarrow d \mid (n - r)$

$\Leftrightarrow (\exists\, x \in \mathbf{Z})\;\; n = x \cdot d + r$

Schreibweise: $\mathbf{n \equiv r \ (mod\ d)}$

Ist n – r <u>nicht</u> durch d teilbar, so heißen n und r inkongruent modulo d.

Schreibweise: $\mathbf{n \not\equiv r \ (mod\ d)}$

Sätze: $a \equiv b \pmod m \;\Leftrightarrow\; b \equiv a \pmod m \;\Leftrightarrow\; a - b \equiv 0 \pmod m$

$a \equiv b \pmod m \;\Rightarrow\; ggT(a, m) = ggT(b, m)$

Restsystem

Definition: y heißt ein Rest von x modulo m $\Leftrightarrow x \equiv y \pmod{m}$.
Eine Menge von Zahlen $x_1, x_2, \ldots, x_m$ heißt vollständiges Restsystem modulo m, falls für alle $y \in \mathbf{Z}$ genau ein x_j $(j \in [1:m])$ mit

$$\mathbf{y \equiv x_j \ (mod\ m)}$$

existiert.

Satz: Es gibt unendlich viele vollständige Restsysteme modulo m.
$\mathbf{Z_m} := \{0, 1, 2, \ldots, m-1\}$ bilden ein vollständiges Restsystem.

Sätze von Fermat und Euler

Es sei $p \in \mathbf{P}$ und $a \in \mathbf{Z}$.

$$\mathrm{ggT}(a, p) = 1 \quad \Rightarrow \quad a^{p-1} \equiv 1 \pmod{p}$$

Für $\forall\, b \in \mathbf{Z}$ gilt: $\quad b^{p} \equiv b \pmod{p}$

$$\phi(p) = p - 1$$

$$\boldsymbol{\phi(p \cdot q) = (p - 1)(q - 1)}$$

für $p \neq q$ und $p, q \in \mathbf{P}$

<u>Eulersche Verallgemeinerung</u>:

Es sei $a \in \mathbf{Z} \setminus \{\mathbf{0}\}$ und $m \in \mathbf{N} + \mathbf{1}$.

$$\mathrm{ggT}(a, m) = 1 \quad \Rightarrow \quad a^{\phi(m)} \equiv 1 \pmod{m}$$

Quadratische Reste

Es sei a, m $\in$ **N + 1** mit ggT(a, m) = 1 .

a heißt quadratischer Rest modulo m, falls:

$$\mathbf{x^2 \equiv a \ (mod\ m)}$$ lösbar ist.

a heißt quadratischer Nichtrest modulo m, falls:

$$\mathbf{x^2 \equiv a \ (mod\ m)}$$ nicht lösbar ist.

Satz: Es sei p $\in$ **P**; a $\in$ **Z** mit ggT(a, p) = 1 und

$$\mathbf{x^2 \equiv a \ (mod\ p)} \qquad (*)$$

Wenn $a^{(p-1)/2} \equiv 1 \pmod p$ $\Leftrightarrow$ (*) hat 2 Lösungen x_1 und x_2.

$a^{(p-1)/2} \equiv -1 \pmod p$ $\Leftrightarrow$ (*) hat keine Lösung.

Der diskrete Logarithmus

Gegeben seien $g, \alpha \in \mathbf{Z}$ und $p \in \mathbf{P}$.

Gesucht ist x, so daß

$$\mathbf{g^x = \alpha \bmod p}$$

- Das Problem ist äußerst schwierig zu lösen, falls p mindestens 100 Dezimalstellen hat.
- Der Sicherheitswert vieler Algorithmen beruht auf der Schwierigkeit des diskreten Logarithmus.

Anwendungen des diskreten Logarithmus

- Schlüsselaustausch (Diffie-Hellmann)
- Verschlüsselung (El Gamal, Massey-Omura) und
- Digitale Signatur (El Gamal, DSS)

Nicht nur diskreter Logarithmus „modulo p“, sondern auch

- In beliebigen endlichen Körpern
  (mit p oder 2^n Elementen)
- Auf „elliptischen Kurven“
- Allgemein in „Gruppen“

Satz 1:

Die „Diskrete Exponentialfunktion“ ist eine Einwegfunktion.

Satz 2:

Mit den besten bekannten Algorithmen braucht man i. a. exponentiellen Aufwand, um aus **y** ein **x** mit

$$\mathbf{y = g^x \bmod p}$$

zu berechnen.

Beispiel:

$g = 2$
$p = 37$

x	5	10	20	30
y	32	25	33	11

Wir suchen eine Lösung x der **quadratischen Gleichung**

$$x^2 \equiv a \pmod{p} \qquad (1)$$

in der Ringstruktur $\mathbf{Z_p}$ mit $p \in \mathbf{P}$.

Eine solche Lösung bezeichnen wir als **modulare Quadratwurzel** und schreiben sie als:

$$x \equiv \sqrt{a} \pmod{p} \qquad (2)$$

Zahlen $a \in \mathbf{Z_p}$, welche eine modulare Quadratwurzel besitzen, nennen wir quadratische Reste (sonst quadratische Nichtreste).

Nach heutigem Kenntnisstand ist die Berechnung der modulare Quadratwurzel (mod p) ein **recht schwieriges** mathematisches Problem.

<u>Satz:</u>

Modulare Quadratwurzeln (mod p) treten immer **paarweise** auf.
Beweis hierzu siehe im folgenden.

<u>Satz:</u>

Damit Gl(1) eine Lösung $x \in \mathbf{Z_p}$ besitzt, muss gelten:

$$p \equiv 3 \pmod 4 \qquad (3)$$

oder

$$a^{\frac{p-1}{2}} \bmod p = +1 \qquad (4)$$

Ansonsten existiert <u>keine</u> Lösung.

Satz:

Unter der Voraussetzung von Gl(3) bzw. Gl(4) ergibt sich für Gl(1) als eine Quadratwurzel die Lösung:

$$x_1 = a^{\frac{p+1}{4}} \bmod p \qquad (5)$$

Eine weitere Lösung (zweite Quadratwurzel) von Gl(1) ist dann auch gegeben durch:

$$x_2 = p - x_1 \qquad (6)$$

Vorstehende Sätze sollen im folgenden bewiesen werden. Dazu benötigen wir lediglich den Satz von Fermat.

Beweis für x_1:

Aus dem Satz von Fermat

$$a^{p-1} \bmod p = 1$$

folgt nach Multiplikation mit a^2:

$$a^{p+1} \bmod p = a^2 \qquad \Big| \qquad (\ )^{1/4}$$

$$\Rightarrow a^{\frac{p+1}{4}} \bmod p = a^{\frac{1}{2}} = \sqrt{a}$$

bzw.

$$x_1 := \sqrt{a} = a^{\frac{p+1}{4}} \bmod p \qquad\qquad q.e.d.$$

Beweis für x_2:

Aus Gl(1) ergibt sich:

$$x \equiv \pm\sqrt{a} \pmod{p}$$

Ist $x = x_1$ eine Lösung von Gl(1), d. h. $x_1 = +\sqrt{a} \bmod p$, dann ist auch $x_2 = -\sqrt{a} \bmod p = -x_1$ eine Lösung.

Und somit:

$$x_2 \equiv -x_1 \bmod p = (p - x_1) \bmod p \qquad q.e.d.$$

Beweis für die $\exists$ von $x_{1,2}$:

Eine Lösung nach Gl(5) ist nur **berechenbar**, falls der Exponent (p + 1)/4 eine ganze Zahl ist.

$$\Rightarrow \quad p+1 \;\; \textit{ist ein Vielfaches von } 4$$

$$\Rightarrow \quad 4 \;\big|\; (p+1)$$

$$\Rightarrow \quad p+1 = 4 \cdot k \quad (k = 1, 2, \dots)$$

$$\Rightarrow \quad p = 4 \cdot k - 1$$

$$\Rightarrow \quad p = \{3, 7, 11, 19, 23, 31, \dots\}$$

$$\Rightarrow \quad p \equiv 3 \pmod 4 \qquad q.e.d.$$

Wir suchen eine Lösung x für die modulare Quadratwurzel

$$x^2 \equiv a \pmod{n} \qquad (7)$$

in der Ringstruktur $\mathbf{Z_n}$ mit **$\mathbf{n = p \cdot q}$** und p, q $\in$ **P**.

Satz:

Genügen p und q den Bedingungen

$$p \equiv 3 \pmod 4 \quad bzw. \quad q \equiv 3 \pmod 4,$$

so besitzt die Gl(7) dann insgesamt **vier** Quadratwurzeln der Form **± r** und **± s** in der Menge {0, 1, 2, …, n - 1}, also mod n.

Beweis siehe Übungsaufgaben!

Kap. 2: Algebraische Strukturen und elementare Zahlentheorie

Teil 2: Zahlentheorie und kryptologische Anwendungen

- Zahlentheoretische Funktionen und Algorithmen
  - Euklidischer und erweiterter Euklidischer Algorithmus
  - Sätze von Fermat und Euler
  - Modulare Inverse und modulare Exponentiation
- Generierung von Schlüsselparametern
  - Sieb von Eratosthenes
  - Rückgekoppelte Schieberegister
  - Blum-Micali-Generator
- Bitstromverschlüsselung

<u>Definition</u>: Für a, b ∈ **N** sei g = ggT(a, b) der größte gemeinsame Teiler von a und b, d. h. die größte ganze Zahl, die a und b ohne Rest teilt.

<u>Pseudocode</u>:

```
repeat
    r := a mod b
    if r == 0 then
        g := b
    else
    {   a = b
        b = r   }
until r == 0
```

<u>Satz</u>: Zwei natürliche Zahlen a und b heißen **relativ prim** oder **teilerfremd**, wenn ggT(a, b) = 1 ist.

Berechnungsbeispiel:

Der ggT von 531 und 93 lässt sich wie folgt durch wiederholte Division berechnen:

$$
\begin{aligned}
531 &= 5 \cdot 93 + 66 \\
93 &= 1 \cdot 66 + 27 \\
66 &= 2 \cdot 27 + 12 \\
27 &= 2 \cdot 12 + 3 \\
12 &= 4 \cdot 3
\end{aligned}
$$

$$\Rightarrow \quad \underline{\underline{\mathrm{ggt}(531, 93) = 3}}$$

Kurz:

a	b	g
531	93	66
93	66	27
66	27	12
27	12	3
12	$\underline{\underline{3}}$	0

<u>Satz</u> (Lineare diophantische Gleichung):

Sei a, b, d $\in$ **Z** und $d = ggT(a, b) > 0$. Dann gibt es ganze Zahlen **x** und **y** mit:

$$d = a \cdot \mathbf{x} + b \cdot \mathbf{y} \,,$$

wobei: $|\mathbf{x}| \leq b / (2 \cdot d)$ und $|\mathbf{y}| \leq a / (2 \cdot d)$.

<u>Pseudocode</u> (Berlekamp-Algorithmus):

```
ErwEuklid(a, b)
if b == 0 then return (a, 1, 0)
(d, x, y) = ErwEuklid(b, Mod(a, b))
return (d, y, x - Div(a, b) * y)
```

<u>Hilfsfunktionen:</u>

```
Mod(a, n)            Div(a, n)
return (a % n)       return ((a - Mod(a, n)) / n)
```

Berechnungsbeispiel:

Gesucht sei die Lösung der Gleichung

$$3 = 531 \cdot x + 93 \cdot y \quad (*)$$

Durch schrittweises Rückwärts-einsetzen ergibt sich aus

$$\begin{aligned} 531 &= 5 \cdot 93 + 66 && (1)\\ 93 &= 1 \cdot 66 + 27 && (2)\\ 66 &= 2 \cdot 27 + 12 && (3)\\ 27 &= 2 \cdot 12 + 3 && (4) \end{aligned}$$

folgende Gleichungskette:

$$\begin{aligned} 3 &\overset{(4)}{=} 27 - 2 \cdot 12\\ &\overset{(3)}{=} 27 - 2 \cdot (66 - 2 \cdot 27) = -2 \cdot 66 + 5 \cdot 27\\ &\overset{(2)}{=} -2 \cdot 66 + 5 \cdot (93 - 1 \cdot 66) = 5 \cdot 93 - 7 \cdot 66\\ &\overset{(1)}{=} 5 \cdot 93 - 7 \cdot (531 - 5 \cdot 93) = -7 \cdot 531 + 40 \cdot 93 \end{aligned}$$

$\Rightarrow$ Zahl 3 darstellbar als Linear-kombination von 531 und 93.

Durch Vergleich mit (*) erhält man

$$\underline{\underline{x = -7}} \quad \text{und} \quad \underline{\underline{y = 40}}$$

Modulare Inversion:

Wir nehmen an, dass ggT(a, n) = 1 ist. Dann gibt es ganze Zahlen x und y mit $1 = a \cdot x + n \cdot y$ und es folgt:

$$x = a^{-1} \bmod n \,.$$

Mit dem erweiterten Euklidischen Algorithmus (Berlekamp-Algorithmus) haben wir also ein Verfahren zur Berechnung der Inversen $a^{-1} \bmod n$.

<u>Beispiel:</u>

Gesucht ist die Inverse von 11 in $\mathbf{Z}_{26}$.

$\Rightarrow 11^{-1} \bmod 26 = 19$ weil $19 \cdot 11 \bmod 26 = 1$

Herleitung:

$$\mathrm{ggT}(a,b) = a \cdot x + b \cdot y \Rightarrow x, y$$

1. Setze: $b = n$
2. Annahme: $\mathrm{ggt}(a,n) = 1$

$$\Rightarrow \quad 1 = a \cdot x + n \cdot y$$

3. Bilde: mod n auf beiden Seiten

$$\underbrace{1 \bmod n}_{=1} = a \cdot x \bmod n + \underbrace{n \cdot y \bmod n}_{=0}$$

Also $1 = a \cdot x \bmod n$

$$\Leftrightarrow \quad x = a^{-1} \bmod n$$

Berechnungsbeispiel:

gesucht : Inverse von 11 in $\mathbf{Z}_{26}$ = ?

(falls sie existiert)

a	b	g
11	26	11
26	11	4
11	4	3
4	3	1

$a = 11 \quad b = n = 26$

$$26 = 2 \cdot 11 + 4 \quad (1)$$
$$11 = 2 \cdot 4 + 3 \quad (2)$$
$$4 = 1 \cdot 3 + 1 \quad (3)$$

Da ggt(11,26) = 1 ist 11 invertierbar.
Nun wird schrittweise rückwärts eingesetzt:

$$1 \overset{(3)}{=} 4 - 1 \cdot 3$$
$$\overset{(2)}{=} 4 - 1 \cdot (11 - 2 \cdot 4) = -11 + 3 \cdot 4$$
$$\overset{(1)}{=} -11 + 3 \cdot (26 - 2 \cdot 11)$$
$$= \underbrace{3}_{y} \cdot 26 \underbrace{- 7}_{x} \cdot 11$$

Also ist

$$a^{-1} \bmod n = 11^{-1} \bmod 26$$
$$= -7 \bmod 26$$
$$= \underline{\underline{19}}$$

Probe: $11 \cdot 19 \bmod 26$
$= 209 \bmod 26 = 1$

Definition: Für jede natürliche Zahl n gibt die Eulersche ϕ-Funktion $\phi(n)$ die Anzahl der natürlichen Zahlen kleiner als n an, die zu n **teilerfremd** sind, d. h.

$$\phi(n) = \left| \; 0 \leq k < n \mid ggT(k, n) = 1 \; \right|$$

Beispiel:

$\phi(15) = 8$, denn die Zahlen 1, 2, 4, 7, 8, 11, 13 und 14 sind teilerfremd zu 15.

Spezialfälle:

- $p \in \mathbf{P} \quad \Rightarrow \quad \phi(p) = p - 1$
- $k \in \mathbf{N+1} \quad \Rightarrow \quad \phi(p^k) = p^{k-1} \cdot (p - 1)$
- $p, q \in \mathbf{P} \quad \Rightarrow \quad \phi(p \cdot q) = (p - 1) \cdot (q - 1)$
  $(p \neq q) \qquad\qquad = \phi(p) \cdot \phi(q)$

Berechnungsbeispiel:

gesucht : $\Phi(15) = ?$

			# ↓ abzählen :
Berechne :	$ggT(0,15)$	$\neq 1$	
	$ggT(1,15)$	$= 1$	1
	$ggT(2,15)$	$= 1$	2
	$ggT(3,15)$	$\neq 1$	
	$ggT(4,15)$	$= 1$	3
	$ggT(5,15)$	$\neq 1$	
	$ggT(6,15)$	$\neq 1$	
	$ggT(7,15)$	$= 1$	4
	$ggT(8,15)$	$= 1$	5
	$ggT(9,15)$	$\neq 1$	
	$ggT(10,15)$	$\neq 1$	
	$ggT(11,15)$	$= 1$	6
	$ggT(12,15)$	$\neq 1$	
	$ggT(13,15)$	$= 1$	7
	$ggT(14,15)$	$= 1$	8

ggt = 1 ist 8

$\Rightarrow \quad \underline{\underline{\Phi(15) = 8}}$

Spezialfall : $\quad \underline{\underline{\Phi(p) = p-1}}$

$p \in P$

<u>Satz</u>: Wenn ggT(a, n) = 1 ist, dann gilt:

$$a^{\phi(n)} \bmod n = 1$$

Ist $n = p \in \mathbf{P}$ eine Primzahl, so ergibt sich der Fermatsche Satz:

$$a^{p-1} \bmod p = 1\ ;\ (a \neq 0)$$

und damit auch für die modulare Inverse:

$$a^{-1} \bmod p = a^{p-2} \bmod p\ ;\ (a \neq 0)$$

<u>Beispiel</u>: $6^{-1} \bmod 23 = 6^{21} \bmod 23 = \underline{\underline{4}}$

Berechnungsbeispiel:

gesucht : $6^{-1} = ? \quad (\bmod 23)$

Satz von Fermat:

$$a^{p-1} \bmod p = 1 \quad ; \quad (a \neq 0 \; p \in P)$$

$$\underbrace{a \cdot a^{-1}}_{1} \cdot a^{p-1} \bmod p = 1 \qquad a^{-1} \cdot a^{p-1} = a^{p-2}$$

also

$$a \cdot a^{p-2} \bmod p = 1$$

Auf der anderen Seite gilt :

$$a \cdot a^{-1} \bmod p = 1$$

also

$$a^{-1} \bmod p = a^{p-2} \bmod p$$

d.h.

$$6^{-1} \bmod 23 = \underbrace{6^{21} \bmod 23}_{=4}$$

$$6^{-1} \bmod 23 = 4$$

Probe: $6 \cdot 4 = 24 \equiv 1 \; (\bmod 23)$

q.e.d.

Satz: Wenn ggT(a, n) = 1 ist, dann gilt:

$$a^b \bmod n = a^{b \bmod \phi(n)} \bmod n$$

Beweis:

Entwickle b als Quotient von $\phi(n)$, d. h.

$$b = q \cdot \phi(n) + r \quad \text{mit} \quad r = b \bmod \phi(n) < \phi(n).$$

Also

$$\begin{aligned} a^b \bmod n &= a^{q \cdot \phi(n)} \bmod n \cdot a^r \bmod n \\ &= \underbrace{a^{\phi(n)} \bmod n \cdot a^{\phi(n)} \bmod n \cdot \ldots \cdot a^{\phi(n)} \bmod n}_{q \text{ mal}} \cdot a^r \bmod n \\ &= 1 \cdot 1 \cdot \ldots \cdot 1 \cdot a^r \bmod n \\ &= a^r \bmod n = \underline{\underline{a^{b \bmod \phi(n)} \bmod n}} \end{aligned}$$

q.e.d.

Anwendungsbeispiel:

$$a^{1234} \bmod 31 = a^{4} \bmod 31$$

Nebenrechnung:

$$1234 \bmod \Phi(31)$$
$$= 1234 \bmod 30 = 4$$

Berechnungsbeispiel:

$$a^b \bmod n = a^{b \bmod \Phi(n)} \bmod n$$

$a = 1234$ $n = p = 163$

$b = 5678$

$n = 163$

$1234^{5678} \bmod 163 = \boxed{?}$

$\Phi(n) = \Phi(163) = 162$

$b \bmod \Phi(n) = 5678 \bmod 162 = \mathbf{8}$

$\rightarrow 1234^{5678} \bmod 163 =$

$1234^{8} \bmod 163 =$

$((1234^2)^2)^2 \bmod 163 = \boxed{57}$

$1234 \bmod 163 = 93$

$93^2 \bmod 163 = 10$

$10^2 \bmod 163 = 100$

$100^2 \bmod 163 = 57$

Beispiel: Wir betrachten ($\mathbb{Z}_4$, +, •) und erstellen die Verknüpfungstabelle für die Multiplikation:

•	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	**0**	2
3	0	3	2	1

- $\mathbb{Z}_4$ ist nicht nullteilerfrei und es gibt zu 2 kein multiplikatives Inverses.
- Die Zahl 3 ist zu sich selbst invers, denn $3 \cdot 3 = 1$.

<u>Beispiel</u>: Wir betrachten ($\mathbf{Z}_3$, +, •) und erstellen ebenfalls die Verknüpfungstabelle für die Multiplikation:

•	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

- Die Zahl 2 ist invers zu sich selbst, denn $2 \cdot 2 = 1$, d. h. $2^{-1} = 2$.
- Wegen $2 \cdot ½ = 1$ folgt in $\mathbf{Z}_3$ auch: $½ = 2$
  (mit ½ ist <u>nicht</u> die Zahl 0.5 gemeint, die es in $\mathbf{Z}_3$ <u>nicht</u> gibt!)

Zur effizienten Berechnung von a^b mod n wird bei binärer Repräsentation des (k+1)-Bit-Exponenten b = (b_k, ..., b_1, b_0) die Funktion ModExpo(a, b, n) benutzt.

Pseudocode (Square-and-Multiply-Algorithmus):

```
d := 1
  for i := k to 0 do
  {  d := (d * d) mod n
     if bi == 1 then
        d := (d * a) mod n  }
return d
```

Ausgabe: $d = a^b \bmod n$

(maximal *size(Exponent)* Quadrierungen und Multiplikationen!)

Berechnungsbeispiel:

gesucht : 6^{21} mod 23 = ?

$\Rightarrow$ a = 6 und b = 21 = 16 + 4 + 1

$= (1\ 0\ 1\ 0\ 1)_d$

$\underset{b_4}{\|}$ $\underset{b_2}{\|}$ $\underset{b_0}{\|}$

$\Rightarrow$ 8 Multiplikationen

d · d oder d · a

d = 1

for i = 4 to 0

d = d · d mod n = 1

if b_4 == 1 then d:= d·a = a (weil b_4 = 1)

d = d · d mod n = a^2 mod n

if b_3 == 1 $\Rightarrow$ nein

d = d · d mod n = $a^2 \cdot a^2$ mod n = a^4 mod n

if b_2 == 1 then d:= d·a = a^5 (weil b_2 = 1)

d = d · d mod n = $a^5 \cdot a^5$ mod n = a^{10}

if b_1 == 1 $\Rightarrow$ nein

d = d · d mod n = $a^{10} \cdot a^{10}$ mod n = a^{20}

if b_0 == 1 then d:= d·a = a^{21} (weil b_0 = 1)

Berechnungsbeispiel:

gesucht : 6^{21} mod 23 = ?

$\Rightarrow$ a = 6 und b = 21 = 16 + 4 + 1

$= (1\ 0\ 1\ 0\ 1)_d$

$\underset{b_4}{/\!/}\quad \underset{b_2}{/\!/}\quad \underset{b_0}{/\!/}$

$\Rightarrow$ $\underline{\underline{6^{21} \equiv 4 \bmod 23}}$

(erzielt nach 8 Multiplikationen)

d = 1
for i = 4 to 0

- d = 1 · 1 mod 23 = 1
- if b_4 == 1 then d:= 1·6 = 6 (weil b_4 = 1)
- d = 6 · 6 mod 23 = 6^2 mod 23 = 13
- if b_3 == 1 $\Rightarrow$ nein
- d = 13 · 13 mod n = 13^2 mod 23 = 8
- if b_2 == 1 then d:= 8·6 = 2 (weil b_2 = 1)
- d = 2 · 2 mod 23 = 4
- if b_1 == 1 $\Rightarrow$ nein
- d = 4 · 4 mod 23 = 16
- if b_0 == 1 then d:= 16·6 = 4 (weil b_0 = 1)

Problemstellung:

$x \equiv a_i \bmod m_i \quad ; \quad i = 1, 2, \ldots$

Beispiel :

$x \bmod 4 = 2$

$x \bmod 3 = 1$

$x \bmod 5 = 0$

gesucht : $x = ?$

(kleinste natürliche Zahl)

Antwort / Lösung : $\underline{\underline{x = 10}}$

Fragestellungen :

1. Wie findet man x ?
2. Lässt sich x eindeutig benennen ?
3. Effiziente Berechnung möglich ?

$\Rightarrow$ Lösungsalgorithmus

Lösungsmethode:

Seien $m_1, m_2, \ldots, m_n \in \mathbf{N+1}$ und paarweise teilerfremd
sowie $a_1, a_2, \ldots, a_n \in \mathbf{Z}$.

Simultane Kongruenz:

$$x \equiv a_1 \bmod m_1 \; ; \;\; x \equiv a_2 \bmod m_2 \; ; \;\; \ldots \; ; \;\; x \equiv a_n \bmod m_n \qquad (1)$$

Lösung:

1. Setze: $m = \prod_{i=1}^{n} m_i \; ;$ $\quad M_i = m / m_i \quad (1 \le i \le n)$

   d. h., in M_i ist kein m_i enthalten!

2. Weil die m_i paarweise teilerfremd sind, gilt:
   $ggT(m_i, M_i) = 1$ für $1 \le i \le n$.

3. Nutze den erweiterten Euklidischen Algorithmus, um Zahlen $y_i \in \mathbf{Z}$ für $1 \leq i \leq n$ zu berechnen:

$$y_i \cdot M_i \equiv 1 \pmod{m_i} \;\Leftrightarrow\; y_i \cdot M_i + n_i \cdot m_i = 1 \quad \text{für} \quad (1 \leq i \leq n) \tag{2}$$

Behauptung: Eindeutige Lösung der simultanen Kongruenz (1) ist:

$$x = \left(\sum_{i=1}^{n} a_i \cdot y_i \cdot M_i\right) \bmod m \tag{3}$$

Beweis: Aus (2) folgt:

$$a_i \cdot y_i \cdot M_i \equiv a_i \pmod{m_i} \quad \text{für} \quad (1 \leq i \leq n) \tag{4}$$

und weil für $j \neq i$ die Zahl m_i ein Teiler von M_j ist, gilt:

$$(a_j \cdot y_j \cdot m_1 \cdot m_2 \cdot m_i \cdot \cancel{m_j} \cdot m_n \,/\, \cancel{m_j}) \bmod m_i = 0 \qquad \Leftrightarrow$$

$$a_j \cdot y_j \cdot M_j \equiv 0 \; (\mathrm{mod}\; m_i) \quad \text{für} \quad (1 \le \{i, j\} \le n \;\; \text{sowie} \;\; i \ne j) \qquad (5)$$

Aus dem Lösungsansatz gemäß (3) folgt:

$$x = \left(\sum_{i=1}^{n} a_i \cdot y_i \cdot M_i\right) \mathrm{mod}\; m$$

$$= (a_i \cdot y_i \cdot M_i) \;\mathrm{mod}\; m + \left(\sum_{\substack{j=1 \\ j \ne i}}^{n} a_j \cdot y_j \cdot M_j\right) \mathrm{mod}\; m\,,$$

wobei wir die Summe in zwei Terme geschrieben haben!

Nun wenden wir auf der rechten und linken Seite die Operation **mod m_i** an:

$$x \ \mathbf{mod}\ \mathbf{m_i} = \Big(\big(\sum_{i=1}^{n} a_i \cdot y_i \cdot M_i\big) \bmod m \Big)\ \mathbf{mod}\ \mathbf{m_i}$$

$$= \big(\sum_{i=1}^{n} a_i \cdot y_i \cdot M_i\big)\ \mathbf{mod}\ \mathbf{m_i}$$

$$= \underbrace{(a_i \cdot y_i \cdot M_i)\ \mathbf{mod}\ \mathbf{m_i}}_{=\ a_i \text{ wegen } (4)} + \underbrace{\big(\sum_{\substack{j=1 \\ j \neq i}}^{n} a_j \cdot y_j \cdot M_j\big)\ \mathbf{mod}\ \mathbf{m_i}}_{=\ 0 \text{ wegen } (5)}$$

$\rightarrow \quad x \equiv a_i \;(\bmod\; m_i) \;$ für $\;(1 \leq i \leq n) \qquad$ **q.e.d.**

Also löst x nach (3) die Kongruenz (1)!

Rechenbeispiel:

$\mathbf{x} \equiv 2 \bmod 4$; $\mathbf{x} \equiv 1 \bmod 3$ und $\mathbf{x} \equiv 0 \bmod 5$; gesucht: $\mathbf{x} = ?$

$$\leftrightarrow \quad \begin{matrix} a_1 = 2 & & m_1 = 4 \\ a_2 = 1 & \text{und} & m_2 = 3 \\ a_3 = 0 & & m_3 = 5 \end{matrix} \quad \rightarrow \; m = m_1 \cdot m_2 \cdot m_3 = 60 \; \rightarrow$$

$M_1 = 60 / 4 = 15$;

$M_2 = 60 / 3 = 20$ und

$M_3 = 60 / 5 = 12$.

Wir lösen:

1) $y_1 \cdot M_1 \equiv 1 \bmod m_1 \;\rightarrow\; y_1 \cdot 15 \equiv 1 \bmod 4 \;\rightarrow\; \mathbf{y_1 = 3}$

2) $y_2 \cdot M_2 \equiv 1 \bmod m_2 \;\rightarrow\; y_2 \cdot 20 \equiv 1 \bmod 3 \;\rightarrow\; \mathbf{y_2 = 2}$

3) $y_3 \cdot M_3 \equiv 1 \bmod m_3 \;\rightarrow\; y_3 \cdot 12 \equiv 1 \bmod 5 \;\rightarrow\; \mathbf{y_3 = 3}$

Mit (3) erhalten wir die Lösung:

$$\underline{\underline{\mathbf{x}}} = \left(\sum_{i=1}^{3} a_i \cdot y_i \cdot M_i\right) \bmod m$$

$$= (2 \cdot \mathbf{3} \cdot 15 + 1 \cdot \mathbf{2} \cdot 20 + 0 \cdot \mathbf{3} \cdot 12) \bmod 60 = \underline{\underline{\mathbf{10}}}$$

Algorithmus:

Pseudocode (Chinesischer Restalgorithmus):

```
CRT(int koeff[], int moduli[], int number)
{   int multi[number], result = 0, modulus, i
    CRTPre(moduli[], number, modulus, multi[])
    for i := 1 to number do
        result = (result + koeff[i] * multi[i]) % modulus;
return result
}
```

Benutzt wird die Hilfsfunktion `CRTPre`, die mittels `ErwEuklid` die Werte y_i und anschließend die Produkte $y_i \cdot M_i$ berechnet und in der Variable $multi_i$ übergibt.

<u>Pseudocode</u> (Hilfsfunktion):

```
CRTPre(moduli[], number, modulus, multi[])
{   int i, m, M, x, y, ggT, modulus = 1
    for i := 1 to number do
        modulus = modulus * moduli[i]
    for i := 1 to number do
        {   m = moduli[i]
            M = modulus / m
            (ggT, x, y) = ErwEuklid(M, m)
            multi[i] = (x * M) % modulus   }
return (modulus, multi[])   }
```

Für die Implementierung des erweiterten Euklidischen Algorithmus `ErwEuklid` (Berlekamp-Algorithmus) siehe Kap. IV Seite 38.

Seien $m_1, m_2, \ldots, m_n \in \mathbf{N+1}$ und paarweise teilerfremd sowie $a_1, a_2, \ldots, a_n \in \mathbf{Z}$.

Behauptung:

Dann hat die simultane Kongruenz gemäß (1)

$$x \equiv a_i \bmod m_i \quad (1 \leq i \leq n)$$

eine Lösung gemäß (3), die eindeutig ist mod m mit: $m = \prod_{i=1}^{n} m_i$.

Satz:

Der Algorithmus zur Lösung der simultanen Kongruenz erfordert mit $k := \mathrm{size}(m)$ folgende Aufwände:

Zeit-Aufwand: $o(k^2)$

Speicherplatz-Aufwand: $o(k)$

Zusammenfassung

- Gegenstand der elementaren Zahlentheorie sind die natürlichen Zahlen **N** und deren Erweiterungen **Z** (ganze Zahlen), sowie der Körper **Q** der rationalen Zahlen.
- Der Gebrauch der Zahlentheorie setzt an manchen Stellen auch grundlegende Kenntnisse der Algebra (Gruppen- und Ringtheorie) sowie der linearen Algebra voraus.
- Das Material zur Lehrveranstaltung ist so ausführlich wie nötig und so knapp wie möglich zusammengestellt, um hier sämtliche Grundlagen der folgenden Praktikumsaufgaben zu legen und doch das erste Verständnis nicht zu erschweren.
- In einer Krypto-Library wurden die für unsere Zwecke effizientesten Algorithmen (erweiterter Euklidischer Algorithmus, modulare Inverse, Square & Multiply Algorithmus, Chinesischer Restalgorithmus etc.) implementiert.
- Damit werden die Teilnehmer in die Lage versetzt, praktische Kryptoverfahren nachprogrammieren und den Aufwand von insbesondere asymmetrischen Verschlüsselungs-, Signatur- und Authentifikationssystemen abschätzen zu können.