

Diskrete Strukturen

für die Studiengänge

Angewandte Informatik & Technische Informatik

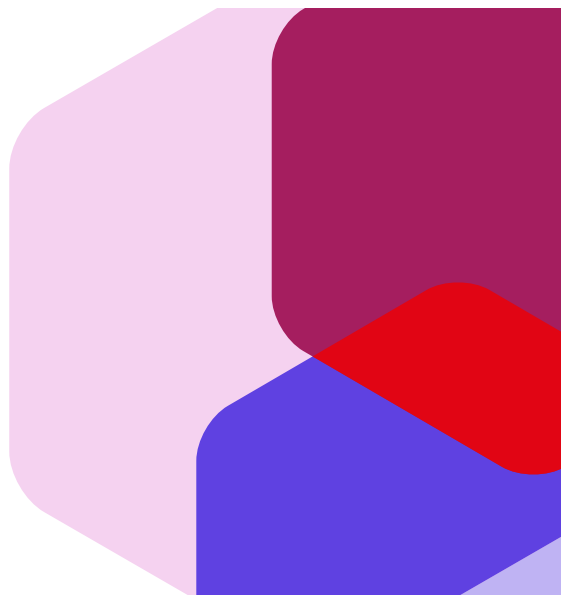
07 Algebraische Grundstrukturen

Prof. Dr. David Sabel

Wintersemester 2025/26

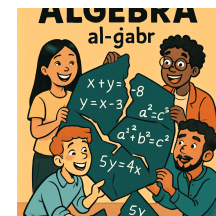
Stand der Folien: 24. Februar 2026

Bildnachweis: Alle Bilder sind selbst gezeichnet oder generiert mit KI von OpenAI unter <https://xt.tu-berlin.de>



Einleitung

- Algebra ist ein Teilgebiet der Mathematik.
- Sprachlich: Wort Algebra statt vom arabischen Wort „al-ğabr“ („Zusammenfügen gebrochener Teile“)
- Geschichtlich: Algebra = Lösen von Gleichungen mit Unbekannten
- Abstrakte Algebra = Eigenschaften von Mengen mit Operationen

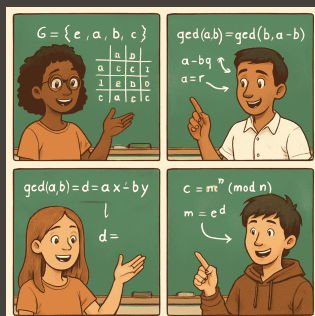


Inhalt:

- Gruppen
- Körper
- Anwendungen

GRUPPEN

- Definition
- Ganze Zahlen
- Endliche Gruppen
- Der Euklidische Algorithmus
- Der erweiterte Euklidische Algorithmus
- Anwendung: RSA-Verschlüsselung



Gruppe

Definition

Eine **Gruppe** $(G, \circ)$ besteht aus einer Menge G und einer binären Verknüpfung $\circ$, sodass die folgenden Gesetze (genannt Gruppenaxiome) erfüllt sind:

(G0) **Abgeschlossenheit**: Wenn $x, y \in G$, dann ist auch $x \circ y \in G$.

(G1) **Assoziativität**: Für alle $x, y, z \in G$: $(x \circ y) \circ z = x \circ (y \circ z)$.

(G2) **Existenz eines neutralen Elements**: Es gibt $e \in G$ mit $e \circ x = x \circ e = x$ für alle $x \in G$.

(G3) **Existenz inverser Elemente**: Für jedes $x \in G$ gibt es $x^{-1} \in G$ mit $x \circ x^{-1} = x^{-1} \circ x = e$.

Wenn zusätzlich gilt:

(G4) **Kommutativität**: Für alle $x, y \in G$: $x \circ y = y \circ x$.

dann ist G eine **abelsche Gruppe** (oder auch **kommutative Gruppe**).

Notationsvariationen: Neutrales Element 1 oder 0 statt e , Inverses $-x$ statt x^{-1}

Satz

Das Paar $(\mathbb{Z}, +)$, wobei $+$ die übliche Addition ist, ist eine abelsche Gruppe.

Beweis. Wir prüfen die Gruppenaxiome.

(G0): $\mathbb{Z}$ ist abgeschlossen bezüglich $+$.

(G1): $(x + y) + z = x + (y + z)$ gilt für die Addition auf ganzen Zahlen x, y und z .

(G2): Das neutrale Element $e = 0$ erfüllt (G2), denn $0 + x = x = x + 0$ für alle $x \in \mathbb{Z}$.

(G3): Das Inverse zu $x \in \mathbb{Z}$ ist $x^{-1} = -x$, da $x + (-x) = (-x) + x = 0$ für alle $x \in \mathbb{Z}$.

(G4): Für alle $x, y \in \mathbb{Z}$ gilt: $x + y = y + x$.

- $(\mathbb{N}, +)$ ist keine Gruppe, da es z.B. kein neutrales Element gibt.
- $(\mathbb{N}_0, +)$ ist keine Gruppe, da es z.B. kein inverses Element zu 1 gibt.
- $(\mathbb{Z} \setminus \{0\}, \cdot)$ ist keine Gruppe, da es z.B. zu $3 \in \mathbb{Z}$ kein inverses Element in $\mathbb{Z}$ gibt.
- $(\{-2, -1, 0, 1, 2\}, +)$ (mit $+$ ist normale Addition auf $\mathbb{Z}$) ist keine Gruppe, da $+$ nicht abgeschlossen für die Menge $\{-2, -1, 0, 1, 2\}$ ist.

Satz

Das Paar $(\mathbb{R} \setminus \{0\}, \cdot)$ wobei $\cdot$ die übliche Multiplikation ist, ist eine abelsche Gruppe.

Beweis. Wir prüfen die Gruppenaxiome.

(G0): $\mathbb{R} \setminus \{0\}$ abgeschlossen bezüglich der Multiplikation.

(G1): $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ gilt für die Multiplikation auf reellen Zahlen.

(G2): Das neutrale Element $e = 1 \in \mathbb{R}$ erfüllt (G2), da $1 \cdot x = x = x \cdot 1$ für alle $x \in \mathbb{R} \setminus \{0\}$.

(G3): Das Inverse zu $x \in \mathbb{R} \setminus \{0\}$ ist: $x^{-1} = \frac{1}{x}$, da $x \cdot \frac{1}{x} = \frac{1}{x} \cdot x = 1$ für alle $x \in \mathbb{R} \setminus \{0\}$.

(G4): Für alle $x, y \in \mathbb{R} \setminus \{0\}$ gilt: $x \cdot y = y \cdot x$.

Bemerkung: $(\mathbb{R}, \cdot)$ ist keine Gruppe, da es zu 0 kein inverses Element gibt (es gibt keine reelle Zahl x mit $0 \cdot x = 1$!).

Wir betrachten nun endliche Strukturen, d.h. endliche Mengen mit Verknüpfung:

Definition (Restklassenmenge modulo n)

Wir definieren die Menge $\mathbb{Z}_n$ als Menge aller natürlichen Zahlen mit 0, die kleiner n sind:

$$\mathbb{Z}_n := \{0, 1, \dots, n-1\}$$

Die Addition $+$ auf $\mathbb{Z}_n$ sei die Addition modulo n , d.h. für $x, y \in \mathbb{Z}_n$ berechnen wir $(x + y) \bmod n$.

Beachte: Beim Rechnen modulo n , kann man in Zwischenschritten immer wieder den Rest bilden, um Zahlen klein zu halten.

Z.B. $(100 + 129 + 44) \bmod 3$ kann man durch

$((100 \bmod 3) + (129 \bmod 3) + (44 \bmod 3)) \bmod 3 = (1 + 0 + 2) \bmod 3 = 0$ berechnen

Additionstabeln

Wir betrachten $(\mathbb{Z}_n, +)$ für $n = 3, 4, 5$.

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Addition in $\mathbb{Z}_3$

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Addition in $\mathbb{Z}_4$

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Addition in $\mathbb{Z}_5$

$(\mathbb{Z}_n, +)$ ist eine Gruppe

Satz

Für alle $n \in \mathbb{N}$ gilt: $(\mathbb{Z}_n, +)$ ist eine Gruppe.

Beweis. Wir prüfen die Gruppenaxiome.

(G0): Da wir modulo n rechnen, ist der Rest zwischen 0 und $n - 1$ und damit in $\mathbb{Z}_n$.

(G1): Es gilt $(x + y) + z \equiv x + (y + z) \pmod{n}$, da
 $((a \bmod n) + b) \bmod n = (a + b) \bmod n$ für alle a, b, n .

(G2): Das Element $0 \in \mathbb{Z}_n$ erfüllt (G2), denn $x + 0 \equiv x \equiv 0 + x \pmod{n}$ für alle $x \in \mathbb{Z}_n$.

(G3): Das inverse Element zu $x \in \mathbb{Z}_n$ ist $x^{-1} = n - x$, denn

$$x + n - x \equiv n \equiv 0 \equiv n - x + x \pmod{n}.$$

Bemerkungen

- $(\mathbb{Z}_n, \cdot)$, wobei $\cdot$ die Multiplikation modulo n ist, ist keine Gruppe:
Denn $0 \in \mathbb{Z}_n$ hat kein multiplikativ inverses Element.
- Auch andere Elemente haben nicht immer ein multiplikatives Inverses:
Z.B. hat in $\mathbb{Z}_4$ das Element 2 kein multiplikativ inverses Element, denn es gibt kein 2^{-1} mit $2 \cdot 2^{-1} \equiv 1 \pmod{4}$: Probiere alle Zahlen aus $\mathbb{Z}_4$ aus:
 - $2 \cdot 0 \equiv 0 \pmod{4}$
 - $2 \cdot 1 \equiv 2 \pmod{4}$
 - $2 \cdot 2 \equiv 0 \pmod{4}$
 - $2 \cdot 3 \equiv 2 \pmod{4}$

Der ggT

Definition

Der **größte gemeinsame Teiler** zweier Ganzzahlen x, y , $\text{ggT}(x, y)$, ist die größte Zahl $a \in \mathbb{N}_0$, sodass es Zahlen $x', y' \in \mathbb{Z}$ gibt mit $x = a \cdot x'$ und $y = a \cdot y'$.

Für $\text{ggT}(0, 0)$ definieren wir $\text{ggT}(0, 0) = 0$.

Zwei natürliche Zahlen $x, y \in \mathbb{N}_0$ sind **teilerfremd**, wenn gilt: $\text{ggT}(x, y) = 1$.

Beachte, dass $\text{ggT}(0, x) = |x| = \text{ggT}(x, 0)$ für alle $x \in \mathbb{Z}$.

Die Menge $\mathbb{Z}_n^*$

Definition

Für $n \in \mathbb{N}$ definieren wir die Menge

$$\mathbb{Z}_n^* = \{x \in \mathbb{Z}_n \mid x \text{ und } n \text{ sind teilerfremd}\}.$$

Bemerkungen:

- $0 \notin \mathbb{Z}_n^*$ für $n > 1$ (da jede Zahl die 0 teilt).
- $\mathbb{Z}_4^* = \{1, 3\}$
- $\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$.
- Wenn p eine Primzahl ist, dann ist $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$.
- Wenn x teilerfremd zu n , dann $x \bmod n \in \mathbb{Z}_n^*$

Quiz 1

Welche Elemente liegen in $\mathbb{Z}_7^*$?

arsnova.hs-rm.de
3403 0558



Quiz 2

Welche Elemente liegen in $\mathbb{Z}_{16}^*$?

arsnova.hs-rm.de
3403 0558



Lemma von Bézout

Lemma von Bézout

Seien $x, y \in \mathbb{Z}$ und $d = \text{ggT}(x, y)$. Dann gibt es ganze Zahlen a, b mit $d = ax + by$.

Beweis: siehe Literatur

Beispiele:

- $\text{ggT}(15, 6) = 3$ und mit $a = 1$ und $b = -2$ ist das Lemma von Bézout für 15 und 6 erfüllt (denn $15 - 2 \cdot 6 = 3$).
- $\text{ggT}(132, 123) = 3$ und mit $a = 14$ und $b = -15$ ist das Lemma von Bézout für 132 und 123 erfüllt (denn $14 \cdot 132 - 15 \cdot 123 = 1848 - 1845 = 3$).

Satz

Das Paar $(\mathbb{Z}_n^*, \cdot)$, wobei $\cdot$ die Multiplikation modulo n ist, ist eine abelsche Gruppe.

Beweis. Wir prüfen die Gruppenaxiome:

- (G0): Seien $x, y \in \mathbb{Z}_n^*$. Dann sind x, y teilerfremd zu n . Auch $x \cdot y$ ist teilerfremd zu n (ein Teiler von $x \cdot y$ würde auch x oder y teilen) und damit $x \cdot y \bmod n \in \mathbb{Z}_n^*$.
- (G1): Da die Multiplikation assoziativ in $\mathbb{Z}_n$ ist, ist sie es auch in $\mathbb{Z}_n^*$.
- (G2): Das neutrale Element ist $1 \in \mathbb{Z}_n^*$, denn $1 \cdot x = x \cdot 1 = x$ für alle $x \in \mathbb{Z}_n$.
- ...

Satz

Das Paar $(\mathbb{Z}_n^*, \cdot)$, wobei $\cdot$ die Multiplikation modulo n ist, ist eine abelsche Gruppe.

...

- (G3): Sei $x \in \mathbb{Z}_n^*$. Da x und n teilerfremd, gilt $\text{ggT}(x, n) = 1$ und das Lemma von Bézout liefert a, b mit $ax + bn = 1$. Damit gilt
 $1 = (ax + bn) \bmod n = ((ax \bmod n) + (bn \bmod n)) \bmod n = ((a \bmod n)x) \bmod n$
 Setze $x^{-1} = a \bmod n$.
 Es bleibt zu zeigen $x^{-1} = (a \bmod n) \in \mathbb{Z}_n^*$:
 Aus $((a \bmod n)x) \bmod n = 1$ folgt: $((a \bmod n)x) - kn = 1$ für ein k .
 D.h. $\text{ggT}(((a \bmod n)x), kn) = 1$, denn jeder Teiler von $((a \bmod n)x)$ und kn muss die 1 teilen. Daher sind $a \bmod n$ und n teilerfremd und $a \bmod n \in \mathbb{Z}_n^*$.
- (G4): Die Multiplikation ist kommutativ, da sie kommutativ in $\mathbb{Z}_n$ ist. $\square$

Ziel: Berechnen von a, b mit $\text{ggT}(x, y) = ax + by$ für gegebene x und y :

- Hierfür kann der **erweiterte Euklidische Algorithmus** verwendet werden.
- Zunächst:
 Normaler Euklidischer Algorithmus, der $\text{ggT}(x, y)$ für $x, y \in \mathbb{N}_0$ berechnet

Satz (Euklidischer Algorithmus)

Seien $x, y \in \mathbb{N}_0$ und $y > 0$. Der $\text{ggT}(x, y)$ kann wie folgt rekursiv berechnet werden:

1. Setze $X := x$ und $Y := y$.
2. Dividiere X durch Y mit Rest, d.h. berechne q und $0 \leq r < Y$ mit: $X = q \cdot Y + r$
3. Wenn der Rest $r = 0$, dann stoppe mit Y als Ergebnis für den $\text{ggT}(x, y)$.
 Anderenfalls, setze $X := Y$ und $Y := r$ und mache weiter mit Schritt (2).

Beweis.

- Wenn der Algorithmus sofort in Schritt 3 stoppt, ist $\text{ggT}(x, y) = y$.
- Anderenfalls: Aus $X = q \cdot Y + r$ folgt, dass der $\text{ggT}(X, Y)$ auch r teilen muss, um ein Teiler von X zu sein. Daher kann man mit $\text{ggT}(X, r)$ weiter machen.
- Terminierung: Y wird in jeder Iteration kleiner, aber niemals < 1 gesetzt.
 (Wenn $Y > X$, dann ist $r = X$ und X und Y tauschen die Rollen (und Y wird kleiner).

Beispiel

1. Setze $X := x$ und $Y := y$.
2. Dividiere X durch Y mit Rest, d.h. berechne q und $0 \leq r < Y$ mit: $X = q \cdot Y + r$
3. Wenn Rest $r = 0$, dann stoppe mit $\text{ggT}(x, y) = Y$. Anderenfalls, setze $X := Y$ und $Y := r$ und gehe zu (2).

Wir berechnen $\text{ggT}(75, 48)$:

- Schritt 1: $X = 75, Y = 48$
- Schritt 2 ergibt $75 = 1 \cdot 48 + 27$, d.h. $q = 1$ und $r = 27$.
- Schritt 3 setzt $X = 48, Y = 27$ und weiter mit Schritt 2.
- Schritt 2 ergibt $48 = 1 \cdot 27 + 21$, d.h. $q = 1$ und $r = 21$.
- Schritt 3 setzt $X = 27, Y = 21$ und weiter mit Schritt 2.
- Schritt 2 ergibt $27 = 1 \cdot 21 + 6$, d.h. $q = 1$ und $r = 6$.
- Schritt 3 setzt $X = 21, Y = 6$ und weiter mit Schritt 2.
- Schritt 2 ergibt $21 = 3 \cdot 6 + 3$, d.h. $q = 3$ und $r = 3$.
- Schritt 3 setzt $X = 6, Y = 3$ und weiter mit Schritt 2.
- Schritt 2 ergibt $6 = 2 \cdot 3 + 0$, d.h. $q = 2$ und $r = 0$.
- Schritt 3 liefert 3 als Ergebnis für $\text{ggT}(75, 48)$.

$$X = 75, Y = 48$$

$$75 = 1 \cdot 48 + 27, \text{ d.h. } q = 1 \text{ und } r = 2748 = 1 \cdot 27 + 21$$

$$X = 48 \text{ und } Y = 27 \quad X = 27 \text{ und } Y = 21 \quad X = 21 \text{ und } Y = 21$$

Quiz 3

Bringe die Werte für (X, Y) bei der Berechnung von $\text{ggT}(140, 128)$ in die Reihenfolge, wie sie beim Euklidischen Algorithmus auftreten.

- (8,4)
- (128,12)
- (12,8)
- (140,128)

arsnova.hs-rm.de
3403 0558



Zahlen a und b aus dem Lemma von Bézout

- Verwende die Gleichungen des Euklidischen Algorithmus $X = q \cdot Y + r$, nummeriert nach Iteration, Start mit $i = 2$ ($X_2 = q_2 \cdot Y_2 + r_2$ mit $X_2 = x, Y_2 = y$)

$$X_i = q_i \cdot Y_i + r_i$$

- Löse Gleichungen nach r_i auf:

$$r_i = X_i - q_i \cdot Y_i$$

- Das Setzen der X - und Y -Werte in Schritt 3 zeigt:

$$Y_i = r_{i-1} \text{ und } X_i = Y_{i-1} = r_{i-2}$$

(für alle i , wenn wir noch $r_0 = x$ und $r_1 = y$ definieren), d.h.

$$r_i = r_{i-2} - q_i \cdot r_{i-1}$$

- Sei die vorletzte Gleichung die n -te Gleichung. Deren r_n ist der ggT , d.h.

$$\text{ggT}(x, y) = r_n = r_{n-2} - q_n \cdot r_{n-1}$$

- Setze sukzessive die r_i davor ein, bis nur noch q_i 's und x und y vorkommen.
- Vereinfache die Gleichung bis sie von der Form $r_n = ax + by$ ist

Beispiel

Gleichungen aus dem Eukl. Algorithmus	nach r_i aufgelöst	entspricht
		$r_0 = x = 75$
		$r_1 = y = 48$
$75 = 1 \cdot 48 + 27$, d.h. $q = 1$ und $r = 27$	$27 = 75 - 1 \cdot 48$	$r_2 = r_0 - 1 \cdot r_1$
$48 = 1 \cdot 27 + 21$, d.h. $q = 1$ und $r = 21$	$21 = 48 - 1 \cdot 27$	$r_3 = r_1 - 1 \cdot r_2$
$27 = 1 \cdot 21 + 6$, d.h. $q = 1$ und $r = 6$	$6 = 27 - 1 \cdot 21$	$r_4 = r_2 - 1 \cdot r_3$
$21 = 3 \cdot 6 + 3$, d.h. $q = 3$ und $r = 3$	$3 = 21 - 3 \cdot 6$	$r_5 = r_3 - 3 \cdot r_4$
Einsetzen und vereinfachen:		
	$3 = r_5 = r_3 - 3 \cdot r_4$	
	$= r_3 - 3 \cdot (r_2 - 1 \cdot r_3)$	
	$= (r_1 - 1 \cdot (r_0 - 1 \cdot r_1)) - 3 \cdot ((r_0 - 1 \cdot r_1) - 1 \cdot (r_1 - 1 \cdot (r_0 - 1 \cdot r_1)))$	
	$= (48 - 1 \cdot (75 - 1 \cdot 48)) - 3 \cdot ((75 - 1 \cdot 48) - 1 \cdot (48 - 1 \cdot (75 - 1 \cdot 48)))$	
	$= (-7 \cdot 75) + (11 \cdot 48)$	

Erweiterter Euklidischer Algorithmus

Der erweiterte Euklidische Algorithmus macht genau diese Berechnung, nur er merkt sich die Faktoren direkt, sodass man nicht rückwärts rechnen muss.

Starte mit

$$r_0 = x, r_1 = y$$

$$s_0 = 1, s_1 = 0$$

$$t_0 = 0, t_1 = 1$$

Berechne für $i = 2, 3, \dots$ (wobei q_i der ganzzahlige Anteil der Division von r_{i-2} durch r_{i-1} ist)

$$r_i = r_{i-2} - q_i \cdot r_{i-1}$$

$$s_i = s_{i-2} - q_i \cdot s_{i-1}$$

$$t_i = t_{i-2} - q_i \cdot t_{i-1}$$

Stoppe sobald $r_i = 0$. Dann gilt $\text{ggT}(x, y) = r_{i-1} = s_{i-1} \cdot x + t_{i-1} \cdot y$

Beispiel

i		r_i	s_i	t_i
0		75	1	0
1		48	0	1
i	$q_i = \lfloor r_{i-2}/r_{i-1} \rfloor$	$r_i = r_{i-2} - q_i \cdot r_{i-1}$	$s_i = s_{i-2} - q_i \cdot s_{i-1}$	$t_i = t_{i-2} - q_i \cdot t_{i-1}$
2	$1 = \lfloor 75/48 \rfloor$	$27 = 75 - 1 \cdot 48$	$1 = 1 - 1 \cdot 0$	$-1 = 0 - 1 \cdot 1$
3	$1 = \lfloor 48/27 \rfloor$	$21 = 48 - 1 \cdot 27$	$-1 = 0 - 1 \cdot 1$	$2 = 1 - 1 \cdot (-1)$
4	$1 = \lfloor 27/21 \rfloor$	$6 = 27 - 1 \cdot 21$	$2 = 1 - 1 \cdot (-1)$	$-3 = -1 - 1 \cdot 2$
5	$3 = \lfloor 21/6 \rfloor$	$3 = 21 - 3 \cdot 6$	$-7 = -1 - 3 \cdot 2$	$11 = 2 - 3 \cdot (-3)$
6	$2 = \lfloor 6/3 \rfloor$	$0 = 6 - 2 \cdot 3$	Stop!	

$$\text{ggT}(75, 48) = 3 = -7 \cdot 75 + 11 \cdot 48$$

Eulersche Funktion

Definition

Die Eulersche Funktion $\phi : \mathbb{N} \rightarrow \mathbb{N}$ ist definiert als $\phi(n) = |\mathbb{Z}_n^*|$.

Für alle Primzahlen $p \neq q$ gilt $\phi(p \cdot q) = \phi(p) \cdot \phi(q) = (p-1) \cdot (q-1)$.

Satz von Euler

Für alle $x \in \mathbb{Z}_n^*$ gilt:

$$x^{\phi(n)} \equiv 1 \pmod{n}$$

Beweis: Siehe Literatur.

Anwendung: Die RSA-Verschlüsselung

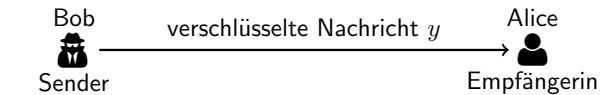
- benannt nach Ron Rivest, Adi Shamir und Leonard Adleman
- Asymmetrisches Verschlüsselungsverfahren: Kein gemeinsamer geheimer Schlüssel, sondern Sender und Empfänger haben öffentliche und private Schlüssel.
- Empfänger gibt seinen öffentlichen Schlüssel öffentlich bekannt, der Sender verwendet diesen Schlüssel zum Verschlüsseln.
- Empfänger kennt seinen privaten Schlüssel und entschlüsselt damit

Annahme: Nachricht x sei eine kleine Zahl
(insbesondere x viel kleiner als n im folgenden)

Annahme kann eingehalten werden, indem Nachricht stückweise geschickt wird,
oder die Nachricht selbst nur ein symmetrischer Schlüssel ist.



RSA-Verfahren



Nachricht x

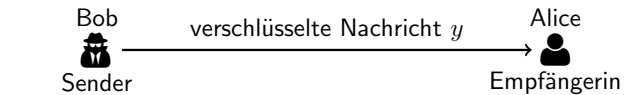
- wählt große Primzahlen p und q und bildet $n = p \cdot q$
- wählt Zahl a , teilerfremd zu $\phi(n) = (p-1) \cdot (q-1)$
- sei b das multiplikative Inverse zu a modulo $\phi(n)$
- der öffentliche Schlüssel von Alice ist (n, a)

Verschlüsseln: berechne $y = x^a \mod n$

- der private Schlüssel ist $\phi(n)$
(b kann Alice aus a und $\phi(n)$ berechnen)

Entschlüsseln: berechne $y^b \mod n$

Beispiel



Nachricht $x = 2$

Alice wählt $p = 3, q = 11, n = p \cdot q = 33$

$\phi(n) = (3-1) \cdot (11-1) = 2 \cdot 10 = 20$ wähle $a = 9$

Gesucht: $9 \cdot b = 1 \mod 20$

Öffentlicher Schlüssel $(n, a) = (33, 9)$

Verschlüsseln: $y = 2^9 \mod 33 = 512 \mod 33 = 17$

Privater Schlüssel $\phi(n) = 20$.

Erw. Eukl. Alg. für $(\phi(n), a) = (20, 9)$ liefert $k = -4, l = 9$ mit
 $\text{ggT}(\phi(n), a) = 1 = k \cdot 20 + l \cdot 9$ daher $b = 9$

Entschlüsseln $17^9 \mod 33 = 2$

Bemerkung: Signieren

Zum Signieren einer Nachricht von Alice and Bob:

- Alice verschlüsselt die Signatur x mit b aus ihrem privaten Schlüssel als $x^b \mod n$
- Bob verifiziert, indem er Alice öffentlichen Schlüssel anwendet und $(x^b)^a \mod n$ berechnet und prüft, ob x die erwartete Signatur x ist.

Das funktioniert, da $x^{ab} \equiv x^{a \cdot b} \equiv x^{b^a} \mod n$

Bemerkung: Die unverschlüsselte Signatur kann z.B. ein Hash-Wert der Nachricht sein, der sich leicht berechnen lässt.

Korrektheit des RSA-Verfahrens

Satz

Das RSA-Verfahren ist korrekt, d.h. $(x^a)^b \equiv x \mod n$.

Beweis.

- da b das multiplikative Inverse zu a ist (in $\mathbb{Z}_{\phi(n)}^*$), folgt $a \cdot b \equiv 1 \mod \phi(n)$
- damit gibt es k mit $a \cdot b = k \cdot \phi(n) + 1$.
- $y^b \mod n = x$ durch Umformen:

$$\begin{aligned} y^b \mod n &= (x^a \mod n)^b \mod n = x^{a \cdot b} \mod n = x^{k \cdot \phi(n) + 1} \mod n \\ &= (((x^{\phi(n)}) \mod n)^k \mod n) \cdot x \mod n \stackrel{(1)}{=} ((1^k \mod n) \cdot x) \mod n = x \mod n \end{aligned}$$

(1) folgt mit dem Satz von Euler, wenn n und x teilerfremd sind.

Für alle anderen Fälle beweisen wir $x^{ab} \equiv x \mod n$ direkt (nächste Folie)

Korrektheit des RSA-Verfahrens (2)

Wir zeigen $x^{ab} \equiv x \pmod n$ für x und $n = p \cdot q$ nicht teilerfremd. 3 Fälle:

- ❶ x ist durch n teilbar: Dann gibt es k'' mit $x = n \cdot k''$ und daher

$$x^{ab} \equiv (n \cdot k'')^{ab} \equiv 0 \equiv n \cdot k'' \equiv x \pmod n$$

- ❷ x ist durch q , aber nicht durch p teilbar

Dann folgt mit dem Satz von Euler $x^{\phi(p)} \equiv x^{p-1} \equiv 1 \pmod p$ und auch:

$$x^{\phi(n)} \equiv 1 \pmod p \text{ (da } x^{\phi(n)} \equiv x^{(p-1) \cdot (q-1)} \equiv (x^{p-1})^{(q-1)} \equiv 1^{(q-1)} \equiv 1 \pmod p)$$

D.h. es gibt ℓ mit $x^{p-1} = 1 + \ell \cdot p$. Damit können wir schließen

$$x^{a \cdot b} \equiv x^{k \cdot \phi(n) + 1} \equiv x \cdot x^{(p-1)(q-1)k} \equiv x(1 + \ell \cdot p)^{(q-1)k} \stackrel{(2)}{\equiv} x(1 + p \cdot t) \equiv x + xpt \stackrel{(3)}{\equiv} x \pmod n$$

wobei (2) folgt, da Ausmultiplizieren von $(1 + \ell \cdot p)^{(q-1)k}$ zeigt, dass jeder Summand $\ell \cdot p$ als Faktor enthält außer der erste (der nur Einsen multipliziert).

Daher muss es ein t geben mit $(1 + \ell \cdot p)^{(q-1)k} = 1 + p \cdot t$.

(3) ist richtig, da x durch q teilbar und damit xpt durch $n = p \cdot q$ teilbar ist.

- ❸ x ist durch p aber nicht durch q teilbar: Analog zum vorherigen.

Warum ist das RSA-Verfahren sicher?

Es gibt bisher kein schnelles Verfahren, um aus der Zahl n die Zahl $\phi(n)$ bzw. die Primzahlen p und q zu berechnen (dies nennt man **Faktorisierung von n**).

Da ein solches Verfahren bisher nicht entdeckt wurde und man p und q mit steigender Rechenkraft immer größer wählen kann, ist es schwierig den privaten Schlüssel zu knacken.

BSI empfiehlt Schlüssellänge von 3000 Bit $\approx$ 900 Dezimalstellen

Mit **Quantencomputern** ist die schnelle Faktorisierung theoretisch möglich, daher könnte es sein, dass RSA mit der Skalierung von Quantencomputern geknackt wird.

Spätestens dann muss man auf andere Verschlüsselungsverfahren umstellen.

KÖRPER

- Definition
- Endliche Körper



Körper

Struktur mit Verknüpfungen für Addition und Multiplikation sodass man „normal“ in dieser Struktur rechnen kann.

Definition

Eine Menge K mit Verknüpfungen $+$ und $\circ$ ist ein **Körper**, wenn

- ❶ $+$ und $\circ$ sind abgeschlossen auf K .
- ❷ $+$ und $\circ$ sind assoziativ und kommutativ.
- ❸ Es gibt ein neutrales Element 0 bezüglich $+$ und ein neutrales Element $1 \neq 0$ bezüglich $\circ$.
- ❹ Jedes Element $x \in K$ hat ein additives Inverses $-x \in K$ und jedes Element $x \neq 0$ hat ein multiplikatives Inverses $x^{-1} \in K$.
- ❺ Das Distributivgesetz gilt: $x \circ (y + z) = x \circ y + x \circ z$ und $(x + y) \circ z = (x \circ z) + (y \circ z)$ für alle $x, y, z \in K$

Körper (2)

Alternativ kann man auch sagen: $(K, +, \circ)$ ist ein Körper, wenn

- $(K, +)$ eine abelsche Gruppe mit neutralem Element 0 und
- $(K \setminus \{0\}, \cdot)$ eine abelsche Gruppe ist
- und das Distributivgesetz gilt.

Beispiele:

- $(\mathbb{Q}, +, \cdot)$ ist ein Körper
- $(\mathbb{R}, +, \cdot)$ ist ein Körper
- die komplexen Zahlen sind ein Körper

Endliche Körper

- $\mathbb{Z}_2 = \{0, 1\}$ mit Addition und Multiplikation modulo 2 ist ein Körper
- $\mathbb{Z}_3 = \{0, 1, 2\}$ mit Addition und Multiplikation modulo 3 ist ein Körper.

Satz

$\mathbb{Z}_p$ mit der Addition und Multiplikation modulo p ist genau dann ein Körper, wenn p eine Primzahl ist.

„ $\leftarrow$ “: Wenn p prim, dann ist $\mathbb{Z}_p^*$ eine multiplikative Gruppe und $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$.

„ $\rightarrow$ “: Ist p keine Primzahl, dann ist $\mathbb{Z}_p$ nicht null-teilerfrei, d.h. wenn $p = q_1 \cdot q_2$, dann ist $q_1 \cdot q_2 \equiv 0 \pmod{p}$.

Aber Körper sind null-teilerfrei (Beweis siehe Literatur), also kann $\mathbb{Z}_p$ kein Körper sein.

Endliche Körper (2)

Trotzdem gibt es Körper mit $n - 1$ Elementen, wobei n keine Primzahl ist:

- Man muss Multiplikation und Addition anders definieren.
- Allgemein gilt der folgende Satz:

Satz

Es gibt genau dann einen endlichen Körper mit q Elementen wenn $q = p^n$ mit p eine Primzahl und $n \in \mathbb{N}$.