

1 Mengen

1.1 Konzept

Cantor: Naive Definition

Keine Beschränkung über x, A

Russel-Paradoxon: $R = \{A \mid A \notin A\} \in R? \rightarrow$ Axomatisierung (ZFC)

Leere Menge

$\forall A: \emptyset \subseteq A$: die Leere Menge ist in allen Mengen enthalten.

$:= \{x \in A \mid x \neq x\}$: sie ist eindeutig

1.2 Grundregeln der Mengenlehre

Idempotenz	$A \cap A = A, A \cup A = A$
Kommutativität	$A \cap B = B \cap A, A \cup B = B \cup A$
Assoziativität	$A \cap (B \cap C) = (A \cap B) \cap C$ $A \cup (B \cup C) = (A \cup B) \cup C$
Absorption	$A \cap (A \cup B) = A, A \cup (A \cap B) = A$
Distributivität	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
Komplement	$A \cap A' = \emptyset, A \cup A' = I$
Konsistenz	$A \cap B = A \Leftrightarrow A \subseteq B \Leftrightarrow A \cup B = B$

1.3 Operationen auf Mengen

Durchschnitt (\cap)

$$x \in (A \cap B) \Leftrightarrow (x \in A) \wedge (x \in B)$$

Vereinigung (\cup)

$$x \in (A \cup B) \Leftrightarrow (x \in A) \vee (x \in B)$$

Differenz (- oder \setminus)

$$x \in (A - B) \Leftrightarrow (x \in A) \wedge (x \notin B)$$

Symmetrische Differenz (\oplus oder Δ)

$$x \in (A \oplus B) \Leftrightarrow ((x \in A) \vee (x \in B)) \wedge \neg((x \in A) \wedge (x \in B))$$

Komplement

$$I: \text{Universum}, \bar{A} := I - A$$

Kartesisches Produkt

Menge aller geordneten Paare mit einem Element aus A und einem Element aus B.

$$A \times B := \{(x, y) \mid x \in A, y \in B\}$$

Potenzmenge

Die Potenzmenge $P(M)$ der Menge M ist die Menge aller Teilmengen von M: $P(M) := \{N \mid N \subseteq M\}$

Hat die Menge A n Elemente, dann hat ihre Potenzmenge 2^n Elemente, da jedes Element entweder enthalten sein kann oder nicht.

Beispiel:

$$\mathbb{P}(\{\}) = \{\emptyset, \{\}\}$$

$$\mathbb{P}(\{1, 2, 3\}) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$$

Teilmenge

Die Menge A ist eine Teilmenge der Menge B, $A \subseteq B$, wenn jedes Element von A ein Element von B ist:

$$A \subseteq B \Leftrightarrow (x \in A \rightarrow x \in B)$$

Gleichheit

$$A = B \Leftrightarrow (A \subseteq B) \wedge (B \subseteq A)$$

$$\forall x(x \in A \leftrightarrow x \in B)$$

Mengenbildung

$\{x \in A \mid P(x)\}$ oder durch Aufzählen $\{2, 3, \dots\}$

Geordnetes Paar: $(a, b) = (c, d) \rightarrow a = c \wedge b = d$

Definition: $(a, b) = \{\{a\}, \{a, b\}\}$

Ungeordnetes Paar $\{a, b\}$

1.4 Relationen

Eine Relation R von einer Menge A nach einer Menge B ist eine Menge von Paaren (a,b) mit $a \in A$ und $b \in B$, also $R \subseteq A \times B$.

Falls $A = B$, also $R \subseteq A^2$, so nennt man R eine Relation auf A.

Um auszudrücken, dass ein Paar (a,b) in der Relation enthalten ist, also $(a, b) \in R$, sagt man: "a steht in Relation zu b" und schreibt: $a R b$.

Mengendarstellung

Am Beispiel der \leq -Relation auf der Menge $W = \{1, 2, 3\}$:

$$\leq = \{(1, 1), (1, 2), (1, 3), (2, 2), (2, 3), (3, 3)\}$$

Matrixdarstellung

Eine Relation $R \subseteq A \times B$ kann als Matrix $M^R \in \{0, 1\}^{W \times |B|}$ dargestellt werden, wobei die Zeilen für die Elemente von A und die Kolonnen für die Elemente von B stehen. Ein Eintrag der Matrix ist 1 gdw. die entsprechenden Elemente in Relation stehen, und 0 sonst.

$$M^{\leq} = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$$

Darstellung als gerichteter Graph

Eine Relation $R \subseteq A \times B$ kann als bipartiter Graph dargestellt werden, wobei jedes Element aus A und jedes Element aus B durch seinen Knoten repräsentiert wird und von a nach b eine Kante existiert gdw. $a R b$

Im Falle einer Relation auf einer Menge A genügt A als Knotenmenge. Wir verwenden dann einen gerichteten Graphen und lassen darin Schleifen (Loops) zu für Reflexivität.

Kongruenzrelation

Eine Äquivalenzrelation auf einer algebraischen Struktur, die mit den Operationen dieser algebraischen Struktur verträglich ist.

Operationen auf Relationen

- üblicher Mengenoperationen: $\cap, \cup, \Delta, \neg, \dots$
- **Komposition:** $R \subseteq A \times B, Q \subseteq B \times C$, dann $R \circ Q \subseteq A \times C$
 $(a, c) \in R \circ Q \Leftrightarrow \exists b \in B : (a, b) \in R \wedge (b, c) \in Q$
 $(R \circ Q)_{ik} = \bigvee_j (R_{ij} \wedge Q_{jk})$

Eigenschaften von Relationen

Wir schreiben $a R b$ für $(a, b) \in R$

<p>reflexiv: $\forall a : (a, a) \in R$ <i>Bsp:</i> $\leq, =, \equiv_m$, <i>Geg-Bsp.</i> $<, \neq, \neq_m$ <i>Matrix:</i> Diagonale aus Einsen, <i>Graph:</i> Loops</p> <p>antireflexiv / irreflexiv: $\forall a : (a, a) \notin R$ <i>Matrix:</i> Diagonale aus Nullen.</p> <p>symmetrisch: $\forall a, b \in R : (a, b) \in R \leftrightarrow (b, a) \in R$ <i>Matrix:</i> symmetrisch $A^T = A$</p> <p>antisymmetrisch: $\forall a, b : (a, b) \in R \wedge (b, a) \in R \leftrightarrow (a = b)$ <i>Bsp:</i> $\leq, <$ <i>Geg. Bsp:</i> $\text{auf } \mathbb{Z} : -2 2; 2 -2$</p> <p>transitiv: $\forall a, b, c : (a, b) \in R \wedge (b, c) \in R \rightarrow (a, c) \in R$ <i>Bsp:</i> $=, \equiv_m, , <, \subseteq$, <i>Geg. Bps:</i> $\neq, \not\subseteq$</p> <p>Äquivalenzrelation: reflexiv, symmetrisch und transitiv</p> <p>Partielle Ordnung: reflexiv, antisymmetrisch und transitiv</p> <p>Transitiver Abschluss: R' heisst transitiver Abschluss von R, wenn: $(a, b) \in R' \leftrightarrow \exists c_1, \dots, c_n :$ $(a, c_1) \in R, (c_1, c_2) \in R, \dots, (c_n, b) \in R$ $R' = R \cup (R \circ R) \cup (R \circ R \circ R) \cup (\dots)$</p>
--

Beispielrelationen

- Reflexiv und transitiv aber nicht symmetrisch auf \mathbb{N} ist z.B. \leq

1.5 Äquivalenz- und Ordnungsrelationen

<p>Eine Äquivalenzrelation hat die folgenden drei Eigenschaften:</p> <ul style="list-style-type: none"> Reflexivität: $a \sim a$ Jedes Objekt ist zu sich selbst äquivalent. Symmetrie: $a \sim b \leftrightarrow b \sim a$ Wenn a zu b äquivalent ist, dann ist auch b äquivalent zu a (und umgekehrt). Transitivität: $a \sim b \wedge b \sim c \rightarrow a \sim c$ Wenn a zu b äquivalent und b zu c äquivalent ist, dann ist a äquivalent zu c. <p>Die Äquivalenzklasse eines Objektes a ist die Klasse der Objekte, die äquivalent zu a sind.</p>

Eine Äquivalenzrelation \ominus auf einer Menge A induziert auf A eine Partition (=disjunkte Zerlegung in Teilmengen) in sogenannte Äquivalenzklassen:

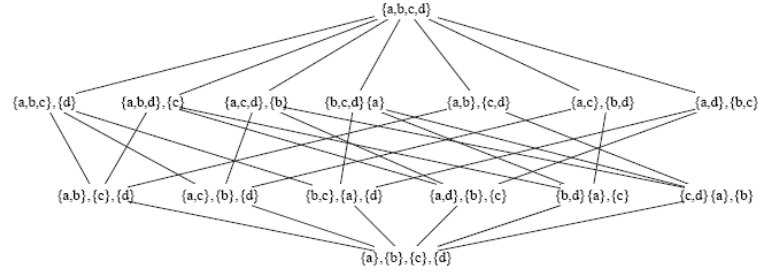
Die zum Element $a \in A$ gehörende Äquivalenzklasse ist definiert als $[a]_{\ominus} = [b]_{\ominus} \leftrightarrow (a \ominus b)$

1.6 Hasse Diagramme

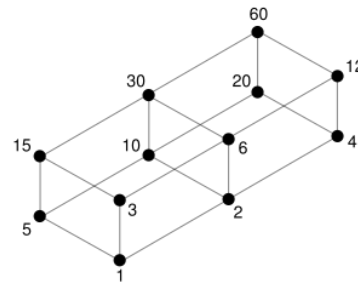
Eine graphische Darstellung von halbgeordneten Mengen. Das Hasse-Diagramm für eine Halbordnung (M, \leq) ist ein gerichteter Graph, wobei die Elemente von M die Knoten bilden. Zwei Knoten a und b werden durch eine Kante verbunden, wenn

$a < b$ gilt und es kein c mit $a < c < b$ gibt. Die Richtung der Kante wird dadurch zum Ausdruck gebracht, dass sich der Knoten b oberhalb von a befindet. Solch eine Anordnung lässt sich erreichen, da das Hasse Diagramm zyklensfrei ist. Schleifen bei Reflexivität werden weggelassen.

Man kann dies zum Beispiel auch für **Äquivalenzrelationen** tun. Nehmen wir z.B. alle möglichen Äquivalenzrelationen auf der Menge $M := \{a, b, c, d\}$.



Hasse-Diagramm der Teiler von der Natürlichen Zahl 60



<p>Grösstes Element $x: \leftrightarrow \forall y \in M : y \leq x$</p> <p>Kleinestes Element $x: \leftrightarrow \forall y \in M : x \leq y$</p> <p>Grösstes und kleinstes Element sind eindeutig bestimmt (falls vorhanden).</p> <p>Maximales Element $x: \leftrightarrow \forall y \in M : (y \geq x \rightarrow y = x)$</p> <p>Minimales Element $x: \leftrightarrow \forall y \in M : (y \leq x \rightarrow y = x)$</p> <p>Es kann mehrere maximale / minimale Elemente geben, wie aus der Definition hervorgeht.</p> <p>Für eine total geordnete Gruppe stimmen die Begriffe grösstes Element und maximales Element überein, nicht aber unbedingt in einer partiell geordneten Menge.</p>

Die Inklusions-Relation auf Menge $P(\{1, 2, 3, 4, 5\})$ und die Teilbarkeits-Relation auf der Menge aller Teiler von 2310 sind isomorph, da die Primfaktorenzerlegung von 2310 5 Elemente hat.

1.7 Funktionen

Eine Relation $f \subseteq A \times B$ heisst **funktionale Relation**, falls:

$$\forall a \exists! b : (a, b) \in f$$

$$(a, b) \in f \wedge (a, b') \in f \rightarrow b = b'$$

Wir schreiben für $(a, b) \in f : f(a) = b, f : a \rightarrow b$

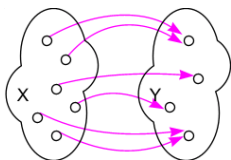
Komposition

$$f : A \rightarrow B, g : B \rightarrow C$$

$$g \circ f(a) = g(f(a))$$

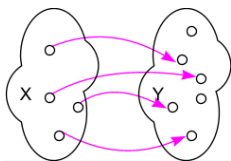
Surjektiv: Jedes Element der Zielmenge wird mindestens einmal als Funktionswert angenommen, hat also mindestens ein Urbild.

$$\forall y \in Y \exists x \in X : f(x) = y$$

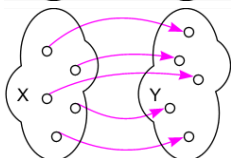


Injektiv: Jedes Element der Zielmenge wird höchstens einmal als Funktionswert angenommen.

$$\forall x_1, x_2 \in X : f(x_1) = f(x_2) \rightarrow x_1 = x_2$$



Bijektiv: Injektiv und Surjektiv. D.h. für alle $y \in Y$ existiert genau ein $x \in X$ mit $f(x) = y$



1.8 Kardinalität von Mengen

\preceq heisst "Weniger mächtig als".

$$A \preceq B \leftrightarrow \exists f : A \rightarrow B \text{ injektiv} \leftrightarrow \exists g : B \rightarrow A \text{ surjektiv}$$

\approx heisst "gleichmächtig wie".

$$A \approx B \leftrightarrow \exists f : A \rightarrow B \text{ bijektiv.}$$

Die Gleichmächtigkeit ist eine Äquivalenzrelation.

Wenn $[h = g \circ f]$, dann gilt:

$$A \underset{f}{\preceq} B \wedge B \underset{g}{\preceq} C \rightarrow A \underset{h}{\preceq} C$$

Cantor-Schröder-Bernstein

$$A \preceq B \wedge B \preceq A \rightarrow A \approx B$$

Totale Ordnungsrelation

$$A \preceq B \vee B \preceq A$$

Satz von Cantor:

$$P(A) \not\approx A$$

1.9 Abzählbarkeit

Abzählbar: Es existiert eine Bijektion zur Menge \mathbb{N} oder die Menge ist endlich.

Überabzählbar: Nicht abzählbar.

\mathbb{N}	Natürliche Zahlen	Per Definition abzählbar
\mathbb{P}	Primzahlen	Abzählbar
\mathbb{Z}	Ganze Zahlen	Abzählbar unendlich
\mathbb{Q}	Rationale Zahlen	Abzählbar unendlich
\mathbb{R}	Reelle Zahlen	Überabzählbar

2 Kombinatorik

2.1 Grundlagen

Auswahlprobleme

Man zieht k Elemente aus einer Urne mit n unterschiedlichen Elementen.

	Geordnet	Ungeordnet
mit Zurücklegen	n^k	$\binom{n+k-1}{k}$
ohne Zurücklegen	$\prod_{i=0}^{k-1} (n-i)$	$\binom{n}{k} = \frac{n!}{k!(n-k)!}$

2.2 Inklusions-Exklusions-Prinzip

Für zwei Mengen A und B gilt für die Kardinalität der Vereinigung:

$$|A \cup B| = |A| + |B| - |A \cap B|$$

Für drei Mengen A, B, C:

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$

Dieser Ansatz lässt sich auch auf eine endliche Anzahl Mengen verallgemeinern.

Prinzip der Inklusion und Exklusion

Für endliche Mengen A_1, \dots, A_n gilt:

$$|\bigcup_{i=1}^n A_i| = \sum_{r=1}^n (-1)^{r-1} \sum_{1 \leq i_1 < \dots < i_r \leq n} |\bigcap_{j=1}^r A_{i_j}|.$$

2.3 Fixpunktfreie Permutationen

Eine **Fixpunktfreie Permutation** ist eine Permutation, bei der kein Element an seinem ursprünglichen Platz bleibt.

Die folgende Permutation hat an der Stelle i einen Fixpunkt und ist somit keine fixpunktfreie Permutation.

$$\begin{pmatrix} 1 & 2 & 3 & \dots & i & \dots & n \\ 13 & 23 & 1 & \dots & i & \dots & 42 \end{pmatrix}$$

Anzahl fixpunktfreier Permutationen einer Menge mit n Elementen

$$!n = n! \sum_{j=0}^n \frac{(-1)^j}{j!}$$

Man nennt $!n$ **Subfakultät**.

Eine Annäherung ist:

$$\approx \frac{n!}{e}$$

Eulersche φ -Funktion

Anzahl Zahlen k, die kleiner als n sind für die $\text{ggT}(n, k) = 1$

$$\varphi(n) := |\{k \in \{0, \dots, n-1\} : \text{ggT}(k, n) = 1\}|$$

$$\varphi(5) = 4, \varphi(6) = 2, \varphi(p) = p - 1 \text{ (für p prim)}$$

Bei zwei Primzahlen p, q mit $p \cdot q = n$

$$\varphi(p \cdot q) = n - q - p + 1 = (p-1)(q-1)$$

2.4 Doppeltes Abzählen

Frage: Ein Team von 4 Programmierern bearbeitet gemeinsam eine unbekannte Zahl n von Projekten. Programmierer A ist in 3 Projekten involviert, B in 5, C in 2 und D in 4. Wenn jedes Projekt genau zwei Programmierer braucht, wie gross ist dann

n?

Antwort: Es gibt $3 + 5 + 2 + 4 = 14$ Paare in der Relation $\rho \subseteq \{\text{Programmierer}\} \times \{\text{Projekte}\}$ mit der Bedeutung $a\rho P$ gdw. Programmierer a bei Projekt P mitarbeitet. Jedes Projekt muss in genau 2 Paaren enthalten sein, somit gibt es $14 : 2 = 7$ Projekte.

2.5 Schubfachprinzip

Auch Pigeonhole principle genannt.

Schubfachprinzip: Wenn man n Objekte auf m Mengen verteilt und n grösser als m ist, dann gibt es mindestens eine Menge, in der mehr als ein Objekt landet.

2.6 Binomialkoeffizienten

$$\binom{n}{k} = \binom{n}{n-k}$$

x, y komplexe Zahlen. Für Zahlen $n \geq 0$ gilt:

$$(x + y)^n = \sum_{k=0}^n \binom{n}{k} x^{n-k} y^k$$

Pascals Identität

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k} \text{ wenn } n > 0$$

$m, n \geq 0$ ganze Zahlen und $m + n > 0$ und k irgendeine ganze Zahl:

$$\binom{n+m}{k} = \sum_{i=0}^k \binom{n}{i} \binom{m}{k-i}$$

$n \geq 0$ und ganze Zahl, $0 < k \leq n$:

$$\left(\frac{n}{k}\right)^k \leq \binom{n}{k} < \left(\frac{e \cdot n}{k}\right)^k$$

Beispiel:

Anzahl binärer Strings der Länge n , in denen der Teilstring 01 genau einmal vorkommt. Es gibt genau $n + 1$ Position um einen Marker zu setzen. Für den Teilstring 01 benötigen wir 3 Marker, da ein passender String folgende Form hat $11 \dots 1|0 \dots 0|11 \dots 1|00 \dots 0$. Somit gibt es $\binom{n+1}{3}$ derartiger Strings.

2.7 Permutationen

Permutation π von n -Elementen:

$$\pi : \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\} \text{ bijektiv}$$

Schreibweise:

$$\begin{pmatrix} 1 & \dots & n \\ \pi(1) & \dots & \pi(n) \end{pmatrix}$$

Identität

$$\Pi = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$$

Involution: Eine Permutation π ist eine Involution (=selbst-invers), wenn gilt: $\pi \circ \pi = \Pi$

Komposition \circ Die Komposition ist assoziativ, aber nicht kommutativ.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix}$$

Zyklendarstellung

Jede Permutation lässt sich eindeutig in disjunkte **Zyklen** zerlegen. Dadurch entsteht die Zyklendarstellung.

$$\pi = (6) \circ \underbrace{(3, 8)}_{=(8,3)} \circ (1, 5, 7) \circ (2, 9, 4, 9)$$

Die Reihenfolge darf dabei vertauscht werden, da die Teile disjunkt sind.

Zyklusstruktur

$\delta \cdot \pi \cdot \delta^{-1}$ hat die selbe Zyklusstruktur wie π .

Stirling Zahlen 1. Art: Wieviele Permutationen einer n -Menge gibt es mit genau k Zyklen?

$$s_{n,k} = s_{n-1,k-1} + (n-1) \cdot s_{n-1,k}$$

Stirling-Dreieck 1. Art für $n = 0, \dots, 6$.

$s_{0,0} = 1; s_{n,0} = 0, n > 0, k = 0; s_{n,k} = 0, k > n$.

						1
					0	1
				0	1	1
			0	2	3	1
		0	6	11	6	1
	0	24	50	35	10	1
0	120	274	225	85	15	1

Stirling Zahlen 2. Art: Wieviele Partitionen der n -Menge in k Mengen?

$$S_{n,k} = S_{n-1,k-1} + k \cdot S_{n-1,k}$$

Stirling-Dreieck 2. Art für $n = 0, \dots, 6$.

$S_{0,0} = 1; S_{n,0}, n > 0, k = 0; S_{n,k} = 0, k > n$.

						1
					0	1
				0	1	1
			0	1	3	1
		0	1	7	6	1
	0	1	15	25	10	1
0	1	31	90	65	15	1

Bell-Zahlen beschreiben die Anzahl Äquivalenzrelationen auf n -Menge:

$$B_n := \sum_{k=0}^n S_{n,k}$$

Partition von Zahlen

Auf wieviele Arten kann $n \in \mathbb{N}$ als Summen:

$$n = n_1 + n_2 + \dots + n_k$$

von $n_i \in \mathbb{N}, n_i > 0$ geschrieben werden?

Geordnet: $n = 1+1+1+1+\dots+1+1$. Wir können nun zwischen allen Einsen ein + habe oder nicht. Somit gibt es

$$2^{n-1}$$

verschiedene geordnete Summendarstellungen mit den obigen Anforderungen.

Für die Anzahl der **geordneten k -Partitionen** von n , für alle $k, n \in \mathbb{N}$ mit $n \geq k$, gilt:

$$\binom{n-1}{k-1}$$

Ungeordnet:

Für die Anzahl **ungeordneter k -Partitionen** $P_{n,k}$ einer Zahl n gilt für alle $k, n \in \mathbb{N}$ mit $n \geq k$:

$$P_{n+k,k} = \sum_{j=1}^n P_{n,j}$$

$$P_{n,k} = \begin{cases} 1, & \text{falls } n = 0 \text{ und } k = 1 \\ 0, & \text{falls } n < k \\ \sum_{i=1}^k P_{n-k,i}, & \text{andernfalls.} \end{cases}$$

$P_{n,k}$ (n)	1	2	3	4	5	6	7	8	9	10	(k)
1	1										
2	1	1									
3	1	1	1								
4	1	2	1	1							
5	1	2	2	1	1						
6	1	3	3	2	1	1					
7	1	3	4	3	2	1	1				
8	1	4	5	5	3	2	1	1			
9	1	4	7	6	5	3	2	1	1		
10	1	5	8	9	7	5	3	2	1	1	

2.8 Lösen einfacher Rekursionsgleichungen

Eine Gleichung der Form

$$a_{n+1} = u \cdot a_n + v \cdot a_{n-1}$$

nennt man **lineare Rekursionsgleichung 2. Ordnung mit konstanten Koeffizienten**.

Lösen von linearen Rekursionsgleichungen

Beispiel: Fibonacci-Reihe

1. Rekursionsgleichung

$$f_n = f_{n-1} + f_{n-2} \text{ mit Anfangsbedingungen: } f_0 = 0 \\ f_1 = 1$$

2. Charakteristisches Polynom

Ansatz: $f_n = \lambda^n$ (für mehrfache NST wird der Ansatz mit n multipliziert, bis ein einzigartiger Term entsteht)

$$\lambda^2 - \lambda - 1 = 0 \\ \lambda_{1,2} = \frac{1 \pm \sqrt{5}}{2}$$

3. Linearkombinationen

Somit gibt es zwei Lösungen: A_1^n, A_2^n , deren Linearkombinationen alle auch Lösungen sind.

4. partikuläre Lösung

Anfangsbedingungen einsetzen:

$$f(0) = 0 = a + b \rightarrow a = -b \\ f(1) = \dots$$

3 Graphentheorie

3.1 Grundbegriffe

Ein Graph lässt sich schreiben als **Graph** $G = (\underbrace{V}_{\text{Vertices}}, \underbrace{E}_{\text{Edges}})$

V : Menge mit $0 < |V| < \infty$

$E \subseteq V \times V$

G heisst **ungerichtet**, falls $(u, v) \in E \leftrightarrow (v, u) \in E$ oder alternativ $E \subseteq \{\{u, v\} | u \neq v\}$

Ein **einfacher Graph** enthält keine Mehrfachkanten.

Die **Nachbarschaft** eines Knoten ist definiert mit:

$$\Gamma(v) := \{w | (v, w) \in E\}$$

Der **Eingangs-** bzw. **Ausgangsgrad** eines Knotens v ist definiert als Anzahl der eingehenden, bzw. von v weggehenden Kanten:

$deg^-(v)$: Eingangsgrad

$deg^+(v)$: Ausgangsgrad

Ist G **ungerichtet**, so gilt:

$$deg(v) = deg^-(v) = deg^+(v) \\ \sum_{v \in V} deg(v) = 2 \cdot |E|$$

Ist G **gerichtet**, so gilt:

$$\sum_{v \in V} deg^-(v) = \sum_{v \in V} deg^+(v) = |E|$$

3.2 Grundbegriffe für einfache ungerichtete Graphen

Weg: Ein Weg ist eine Liste von aufeinander folgenden Knoten, die jeweils durch eine Kante verbunden sind.

$$W = (v_0, v_1, \dots, v_l)$$

Pfad: Weg, bei dem alle Knoten paarweise verschieden sind.

zusammenhängend: Graph G heisst zusammenhängend, falls für alle $u, v \in V$ ein u - v -Pfad existiert.

Zyklus: Weg, bei dem Start- und Endknoten identisch sind, d.h. $v_1 = v_n$

Kreis: Weg, bei dem *nur* Start- und Endknoten von W identisch sind. D.h. $C = (v_1, \dots, v_l)$ sind paarweise verschieden.

Teilgraph: $H = (V', E')$ heisst Teilgraph von $G = (V, E)$, falls $v' \subseteq V, E' \subseteq E, E' \subseteq V' \times V$

Induzierter Teilgraph: H' von V' induzierter Teilgraph wenn $(u, v) \in V' : (u, v) \in E \rightarrow (u, v) \in E'$

Zusammenhangskomponente: Die $G[V_i]$ sind Zusammenhangskomponente von G , wenn $(V_i)_i$ Partitionen von V sind, so dass gilt $\exists u - v$ -Pfad $\leftrightarrow \exists i : u, v \in V_i$. D.h. gibt es eine Verbindung zwischen zwei Knoten, so sind sie in der selben Partition.

Brücke: $G = (V, E), e \in E$ heisst Brücke, falls $G' = (V, E \setminus \{e\})$ eine Zusammenhangskomponente mehr hat als G .

$G = (V, E)$ hat mindestens $|V| - |E|$ Zusammenhangskomponenten.

G zusammenhängend $\rightarrow |V| - |E| \leq 1$

Gilt zudem $|V| - |E| = 1 \rightarrow G$ ist ein Baum

3.3 Bäume

Wald: Ein ungerichteter einfacher Graph ohne Kreis.

Baum: Ein zusammenhängender Wald.

Blatt: Ein $v \in V$ mit $deg(v) = 1$.

Spannbaum: Es sei $G = (V, E)$ zusammenhängend. $H = (V, E')$ ist ein Spannbaum von G , falls:

$$\begin{aligned} H \text{ ist ein Baum} \\ E' \subseteq E \end{aligned}$$

Minimaler Spannbaum: Kruskal, Prim

Jeder Baum mit mindestens 2 Knoten hat mindestens 2 Blätter.

Für die Anzahl a der verschiedenen Spannäume des vollständigen Graphen K_n gilt:

$$a = n^{n-2}$$

Satz von Cayley:

Es gibt genau n^{n-2} markierte Bäume mit n Knoten.

Zwei Graphen $G = (V, E)$ und $G' = (V', E')$ sind **isomorph** ($G \cong G'$), falls $\exists f : V \rightarrow V'$ bijektiv so, dass $\forall v, w \in V : (v, w) \in E \leftrightarrow (f(v), f(w)) \in E'$

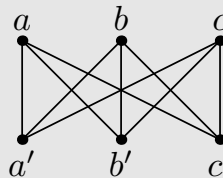
3.4 Einige spezielle ungerichtete Graphen

K_n : **Vollständiger Graph** mit n Knoten, d.h. alle Knotenpaare sind verbunden. Auch: Clique.

C_n : **Kreis** mit n Kanten.

$M_{m,n}$: **Gittergraph** ist ein Gitter der Breite n und Höhe m . Auch: Mesh.

$K_{m,n}$: **Kompletter bipartiter Graph**



Q_d : **d-dimensionaler Hyperkubus** Verbinde alle Knoten, die sich nur in einem Bit unterscheiden ($d = 0 \rightarrow$ Punkt, $d = 1 \rightarrow$ Strecke)

$$V = \{0, 1\}^d \text{ (d-Bit Strings), } |V| = 2^d$$

$$u, v \in E \leftrightarrow \underbrace{d_H(u, v)}_{\text{Hemming-Distanz}} = 1$$

$d_H(0101, 0110) = 2$ (Hemming-Distanz: Anzahl differierende Bits)

$$|E| = \sum_v \frac{deg(v)}{2} = d * 2^{d-1}$$

3.5 Eulertouren

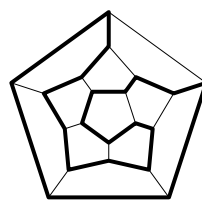
Eine **Eulertour** ist ein Kantenzug, der jede Kante genau einmal enthält. Sie heisst **geschlossen**, wenn sie zum Schluss wieder den ersten Knoten erreicht und **offen**, wenn nicht.

Ein zusammenhängender Graph (oder Multigraph) hat genau dann eine geschlossene Eulertour, wenn alle Knotengrade gerade sind. Diese kann in linearer Zeit gefunden werden.

K_n hat Eulertour $\leftrightarrow n$ ungerade

Q_d hat Eulertour $\leftrightarrow d$ gerade

3.6 Hamiltonsche Kreise



Ein **Hamiltonscher Kreis** ist ein Kreis, der jeden Knoten eines Graphen genau einmal besucht. Ein Graph, der einen Hamiltonkreis besitzt, heisst **hamiltonsch**. *Beispiel:* Das Dodekaeder ist hamiltonsch

$M_{m,n}$ hamiltonsch $\leftrightarrow m \cdot n$ gerade

Q_d hamiltonsch für alle $d \geq 2$

$$G = (V, E) \text{ mit } deg(v) \geq \frac{|V|}{2} \text{ für alle } v \in V$$

ist **hamiltonsch**

K_n , der vollständige Graph mit n Knoten, besitzt $\frac{(n-1)!}{2}$ verschiedene Hamiltonkreise.

Folgende Graphen sind **nicht hamiltonsch**:

- Stern
- Baum mit ≥ 3 Knoten

3.7 Planare Graphen

Ein Graph $G = (V, E)$ ist ein **planarer Graph**, wenn er so gezeichnet (in die Ebene eingebettet) werden kann, dass sich keine Kanten kreuzen. Dabei müssen Kanten keine Geradenstücke sein.

Eulersche Polyederformel

Sei $G = (V, E)$ ein Graph der **zusammenhängend** und **planar** ist und die Ebene in f Gebiete teilt. Dann gilt:

$$|V| + f - |E| = 2$$

Satz von Kuratowski

Ein endlicher Graph ist genau dann planar, wenn er durch Reduktion nicht auf K_5 oder $K_{3,3}$ zurückgeführt werden kann:

Erlaubte Schritte beim Reduzieren sind:

- i) Eine Kante streichen
- ii) Zwei verbundene Knoten v und w "vereinigen": Die Kante $\{v, w\}$ streichen, die beiden Knoten identifizieren und den Knoten v^* mit allen Knoten verbinden, die mit v oder w (oder beiden) verbunden waren.

$G = (V, E)$ planar, $|V| \geq 3$, dann gilt:

$$|E| \leq 3|V| - 6$$

Ist G zudem **dreiecksfrei** (enthält nicht C_3):

$$|E| \leq 2|V| - 4$$

3.8 Färbung von Graphen

(Knoten-)Färbung von $G = (V, E)$ mit k Farben:

$c : V \rightarrow \{1, 2, \dots, k\}$ so, dass

$(u, v) \in E \rightarrow c(u) \neq c(v)$

$\chi(G)$: minimales k , so dass k -Färbung von G existiert

Beispiele:

$\chi(K_n) = n, \chi(M_{m,n}) = 2, \chi(K_{m,n}) = 2$

$\chi(C_n) = \begin{cases} 2 & \text{für } n \text{ gerade,} \\ 3 & \text{sonst.} \end{cases}$

Wenn G planar: $\chi(G) \leq 4$

3.9 Breiten- / Tiefensuche

Breitensuche

Die Breitensuche hat lineare Laufzeit und liefert kürzeste Wege.

Bipartit: $G = (V, E), |V| \geq 2, G$ ist bipartit (zweifärbbar) $\leftrightarrow \chi(G) = 2$ genau dann, wenn er keinen Kreis ungerader Länge enthält.

G planar:

$$\chi(G) \leq 4$$

Algorithmische Entscheidung, ob $\chi(G) = 2$: lineare Zeit. Finden der Färbung: BFS: lineare Färbung.

3.10 Matchings

$G = (V, E)$

Matching: $M \subseteq E$ so, dass kein Knoten von G Endpunkt von mehr als einer Kante in M ist.

M heisst **perfektes Matching**, falls jeder Knoten Endpunkt genau einer Kante in M ist, d.h.

$$|M| = \frac{|V|}{2}$$

Für bipartite Graphen

$|A| \leq |B|$ In einem bipartiten Graphen mit den Mengen A und B gibt es genau dann ein **perfektes Matching**, wenn für jede beliebige Teilmenge X von A gilt: die Kanten, die in X beginnen, haben in der Menge B mindestens so viele Enden, wie X Elemente hat.

Satz von Hall:

$$G = (A \cup B, E)$$

$|A| \leq |B|$, dann existiert Matching M mit $|M| = |A|$ genau dann, wenn $|\Gamma(X)| \geq |X|$ für alle $X \subseteq A$

4 Zahlentheorie

Gewisse Grundtatsachen werden als wahr angenommen:

- $0 \neq 1$
- $a \cdot b = 0 \rightarrow a = 0 \vee b = 0$
- $a \geq b \rightarrow -a \leq -b$
- $(-a) \cdot b = -(a \cdot b)$
- $a^2 \geq 0$

p ist eine **Primzahl**, wenn:

$$\forall a : a|p \rightarrow a = \pm p \vee a = \pm 1$$

4.1 Teilrelation

Die Teilrelation $a|b : \leftrightarrow \exists c \in \mathbb{Z} : a \cdot c = b$ hat folgende Eigenschaften.

- Sie ist transitiv.
- $a|b \wedge b|a \leftrightarrow a = b \vee a = -b$
- Nur 1 und -1 haben Inverse bzgl. Multiplikationen \rightarrow Einheiten (Elemente mit Inversen)
- $a|b \vee a|c \rightarrow a|b \cdot c$
Der Umkehrschluss ist i.A. falsch (Bsp: $4|2 \cdot 2$)

4.2 Teilbarkeit

$a, b \in \mathbb{Z}, a \neq 0$

$a|b : \leftrightarrow \exists c \in \mathbb{Z} : a \cdot c = b$

Rest

Für alle $a, d \in \mathbb{Z}, d \neq 0$, gibt es eindeutige q, r mit $a = d \cdot q + r, 0 \leq r < d$

Wir schreiben $R_d(a) := r$

4.3 Ideale

Idee: Welche Distanzen lassen sich mit unendlich vielen Linearen der Länge 35, 55 und 77 messen?

$\{u \cdot 35 + v \cdot 37 + w \cdot 77 | u, v, w \in \mathbb{Z}\}$ ein Ideal $= (35, 55, 77) \subseteq \mathbb{Z}$
 $(35, 55, 77) = (1) = \mathbb{Z}$

Ideal: Das von a_1, \dots, a_n erzeugte Ideal ist $(a_1, a_2, \dots, a_n) = \{\sum_{i=1}^n u_i \cdot a_i | u_i \in \mathbb{Z}\} \subseteq \mathbb{Z}$. Für alle $a_i \in \mathbb{Z}, i = 1, \dots, n$ gibt es $d \in \mathbb{Z}$ mit $(a_1, \dots, a_n) = (d) = \{vd | v \in \mathbb{Z}\}$

4.4 ggT

$a, b \in \mathbb{Z}, (a, b) \neq (0, 0)$ mit $|a| + |b| \neq 0$

Dann heisst d **ggT** von a und b , falls

$d|a, d|b, c|a \wedge c|b \rightarrow c|d$

Für den Positiven schreiben wir als Funktion: $ggT(a, b) = \underbrace{(a, b)}_{\text{Ideal}}$

Für $a \neq 0 : ggT(a, 0) = |a|$

Satz von Bézou $ggT(a, b) = u \cdot a + v \cdot b$
Rechenregeln $ggT(a, b) = ggT(b, a - b)$

4.5 Erweiterter Euklidischer Algorithmus

Beispiel: EEA(132, 27)

s	t	$s \cdot A + t \cdot B$	
1	0	132	
0	1	27	-4
1	-4	24	-1
-1	5	3	-8
9	-44	0	□

$ggT(132, 27) = s \cdot A + t \cdot B = 9 \cdot 132 - 44 \cdot 27 = 3$

4.6 Primfaktorenzerlegung

Prim: $p \in \mathbb{N}, p > 1$ ist prim, falls p als positive Teiler nur 1 und p hat.

Satz

Ist $a, b \in \mathbb{Z}, p$ prim, so gilt
 $p|a \cdot b \rightarrow p|a \vee p|b$

Fundamentalsatz der Arithmetik

Jede Zahl $n \in \mathbb{N}, n \geq 1$, besitzt eine **eindeutige Primfaktorenzerlegung**. Die Zahl 1 hat null Primfaktoren.

4.7 Modulare Arithmetik

$a \equiv b \pmod{m} :\Leftrightarrow m|(a - b)$

Äquivalent: $a = b + z \cdot m, z \in \mathbb{Z}$

$a \equiv b \pmod{m} \leftrightarrow R_m(a) = R_m(b)$

$\equiv \pmod{m}$ ist eine **Äquivalenzrelation** auf \mathbb{Z} :

$m|(a - a) \rightarrow$ reflexiv

$m|(a - b) \leftrightarrow m|(b - a) \rightarrow$ symmetrisch

$m|(a - b) \wedge m|(b - c) \rightarrow m|(a - c) \rightarrow$ transitiv

Klassen:

$\mathbb{Z}_m \setminus \{0\} = \{[0], [1], \dots, [m - 1]\}$, somit $|\mathbb{Z}_m| = m$

Regeln:

$R_m(a \pm b) = R_m(R_m(a) \pm R_m(b))$

$R_m(a \cdot b) = R_m(R_m(a) \cdot R_m(b))$

$R_m(a^b) = R_m(R_m(a)^b)$

Inversen

	Kommutativ	Assoziativ	Neutralement	Inverse
+	✓	✓	[0]	✓
*	✓	✓	[1]	?

Multiplikatives Inverse

$[a]^{-1}$ in \mathbb{Z}_m existiert genau dann, wenn $ggT(a, m) = 1$, d.h. a, m teilerfremd. Das Inverse kann effizient mit EEA berechnet werden. Es gilt:

$a^{-1} \cdot a \equiv 1 \pmod{m}$

4.8 Chinesischer Restsatz

Eine simultane Kongruenz ganzer Zahlen ist ein System von linearen Kongruenzen.

$x \equiv a_1 \pmod{m_1}$

$x \equiv a_2 \pmod{m_2}$

...

$x \equiv a_n \pmod{m_n}$

Existiert eine Lösung x , so sind mit $M := \text{kgV}(m_1, m_2, \dots, m_n)$ alle Zahlen $x + kM$ mit $k \in \mathbb{Z}$ genau alle Lösungen. Es kann auch sein, dass keine Lösung existiert.

Teilerfremde Modulo

Seien m_1, \dots, m_n paarweise teilerfremde ganze Zahlen, dann existiert für jedes Tupel ganzer Zahlen a_1, \dots, a_n eine ganze Zahl x , die folgende simultane Kongruenz erfüllt:

$x \equiv a_i \pmod{m_i}$ für $i = 1, \dots, n$

Alle Lösungen dieser Kongruenz sind kongruent modulo

$M := m_1 m_2 m_3 \dots m_n$

Finden einer Lösung

Für jedes i sind die Zahlen m_1 und $M_i = M/m_i$ teilerfremd, also kann man mit dem EEA zwei Zahlen r_i und s_i , so dass

$r_i \cdot m_i + s_i \cdot M_i = 1$

Setzen wir $e_i := s_i \cdot M_i$, dann gilt

$e_i \equiv 1 \pmod{m_i}$

$e_i \equiv 0 \pmod{m_j}, j \neq i$

Die Zahl

$x := \sum_{i=1}^n a_i \cdot e_i$

ist dann eine Lösung der simultanen Kongruenz.

Beispiel: Chinesischer Restsatz

$$\begin{aligned} x &\equiv 2 \pmod{3} \\ x &\equiv 3 \pmod{4} \\ x &\equiv 2 \pmod{5} \end{aligned}$$

$$M = 3 \cdot 4 \cdot 5 = 60, M_1 = M/3 = 20, M_2 = M/4 = 15, M_3 = M/5 = 12$$

ss Mit EEA berechnet man:

$$(-13) \cdot 3 + 2 \cdot 20 = 1 \rightarrow e_1 = 40$$

$$(-11) \cdot 4 + 3 \cdot 15 = 1 \rightarrow e_2 = 45$$

$$5 \cdot 5 + (-2) \cdot 12 = 1 \rightarrow e_3 = -24$$

Eine Lösung ist dann $x = 2 \cdot 40 + 3 \cdot 45 + 2 \cdot (-24) = 167$. Wegen $167 \equiv 47 \pmod{60}$ sind alle anderen Lösungen also kongruent zu 47 modulo 60.

5 Algebra

5.1 Gruppen

$\langle G; * \rangle$ heisst **Gruppe**, falls folgendes gegeben ist

- **Assoziativität**

$$\forall a, b, c : (a * b) * c = a * (b * c)$$

- **Neutralement**

$$\forall a \exists e : a * e = e * a = a$$

- **Inverse**

$$\forall a \exists b : a * b = b * a = e$$

G: Menge (endlich oder unendlich)

* : $G \times G \rightarrow G$ Operation

Eine Gruppe heisst **abelsche Gruppe** oder **kommutative Gruppe** wenn gilt:

$$\forall a, b : a * b = b * a$$

Die multiplikative Gruppe $G = \langle \mathbb{Z}_n^*, * \rangle$ enthält alle $a \in \mathbb{Z}$ für die gilt $a < n$ und $\text{ggT}(a, n) = 1$

Beispiele von Gruppen

$(\mathbb{Z}, +), (\mathbb{Z}, \bullet)$

$(\mathbb{Z}_m, +), (\mathbb{Z}_m^*, \bullet), (\mathbb{Z}_m, \bullet)$

$(\mathbb{Q}_m, +), (\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}, \bullet), \mathbb{R}, \mathbb{C}$

$(\mathbb{R}, \text{Vektoraddition})$

Symmetriegruppen

Endliche Gruppen: Systematisch

Triviale Gruppe: $G = \{e\}, e * e = e$

Gruppe mit 2 Elementen

\oplus	0	1
0	0	1
1	1	0

$(\mathbb{Z}_2, +)$

Gruppen mit 3 Elementen

Es gibt genau eine Gruppe mit 3 Elementen. Dabei ist $e = 0, a = 1, b = 2$

*	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

$(\mathbb{Z}_3, +)$

Gruppen mit 4 Elementen

Es gibt genau zwei Gruppen mit 4 Elementen: $(\mathbb{Z}_4, +)$ und $(\mathbb{Z}_2 \times \mathbb{Z}_2)$.

Neuformulierung des Chinesischen Restsatzes

$$n = p \cdot q; p, q \text{ prim}, p \neq q$$

$$\mathbb{Z}_n^* \equiv \mathbb{Z}_p^* \times \mathbb{Z}_q^*$$

Gruppenisomorphismus

Ordnung: $|G|$ ist die Ordnung von G. Die Ordnung von $a \in G$, $\text{ord}(a)$, ist die kleinste Zahl $m \geq 1$, so dass $a^m = e$, falls m existiert und $\text{ord}(a) = \infty$ sonst.

Falls die Ordnung von $a \in G$ endlich ist, dann gilt $a^m = a^{R_{\text{ord}(a)}(m)}$ und die Menge

$$\langle a \rangle = \{e, a, a^2, \dots, a^{\text{ord}(a)-1}\}$$

bildet die kleinste Untergruppe von G, die a enthält.

5.2 Untergruppen

Sei $(G, *)$ eine Gruppe. $H \subseteq G$ mit $H \neq \emptyset$ heisst **Untergruppe von G**, falls H selbst eine Gruppe ist bezüglich *.

- $e \in H$
- $\forall a, b \in H : a * b \in H$
- $\forall a \in H : a^{-1} \in H$

Die Ordnung der Untergruppen teilt die Ordnung der Gruppe.

$$|H| \text{ teilt } |G|$$

5.3 Satz von Lagrange II

Sei G endlich und $a \in G$. Dann gilt:

$$a^{|G|} = e$$

5.4 Kleiner Satz von Fermat

Sei p prim und $p \neq a$. Dann gilt:

$$a^{p-1} \equiv 1 \pmod{p}$$

Eine (endliche) Gruppe G heisst **zyklische Gruppe** und g heisst **Generator** falls es $g \in G$ gibt mit

$$\text{ord}(g) = |G|$$

Man schreibt

$$G = \langle g \rangle$$

Zyklische Gruppen sind stets kommutativ / abelsch. Die Umkehrung gilt i.A. nicht.

$$|G| \text{ prim} \rightarrow G \text{ zyklisch}$$

Jedes $g \neq e$ ist Generator

Ist g ein Generator für \mathbb{Z}_n^* und $ggT(a, |G|) = 1$, dann ist g^a auch ein Generator. Für die Gruppe \mathbb{Z}_n^* gibt es $\varphi(n)$ Generatoren (siehe 2.3)

Beispiel: Gegeben: Für alle $i = 1, 2, \dots, n$ gilt für die Primfaktoren $p_i: g^{|G|/p_i} \neq e$

Zeige: g ist Generator von G

Sei $\text{ord}(g) = y$, d.h. $g^y = e$. Wir wissen y teilt $|G|$. Nehmen wir nun an, dass $y < |G|$. Wir können dann schreiben $y = \prod_{i=1}^n p_i^{f_i}$ mit $0 \leq f_i \leq e_i$ und $f_j < e_j$ für mindestens ein j . Dann teilt aber y sicher $|G|/p_j$, d.h. $|G|/p_j$, d.h. $|G|/p_j = n \cdot y$ und für dieses gilt dann $g^{|G|/p_j} = g^{n \cdot y} = (g^y)^n = e^n = e$. Da dies nicht der Fall ist, wissen wir, dass $y \nmid |G|$. Da aber $y \mid |G|$ teilt, muss gelten $y = |G|$, muss gelten $y = |G|$. Also $\text{ord}(g) = |G|$: g ist ein Generator.

5.5 RSA

Ingredienzen

- **Effizienz:** Modulare Arithmetik, EEA
- **Korrektheit:** Fermat, Chinesischer Restsatz
- **Sicherheit:** $n = p \cdot q \xrightarrow{?} p, q$ schwierig. Nicht bewiesen!

Ablauf von RSA

Alle Rechenoperationen werden in der Gruppe $\mathbb{Z}_{p \cdot q}^*$ durchgeführt.

Bob

Wählt Primzahlen p, q

$$n = p \cdot q$$

$$e \in \mathbb{Z} \text{ mit}$$

$$\text{ggT}(e, (p-1)(q-1)) = 1$$

$$\text{publicKey} = (n, e)$$

publicKey



Alice

Meldung $m (\leq n)$

Verschlüsselung:

$$R_n(m^e) = c$$

Kryptogramm c



Bob

$$\text{EEA: } d = e^{-1}(\text{mod}((p-1)(q-1)))$$

$$R_n(c^d) \stackrel{?}{=} m$$

Effizientere Entschlüsselung

$$c^{p-1} \equiv 1 \pmod{p}$$

RSA: Digitale Signaturen

Alice

verificationKey = (u, e)

signatureKey = $(n = p \cdot q, d)$

$v =$ "Ich schulde Bob CHF 100.-"

Signatur $S = R_n(v^d)$

Signature S



Bob

Verifikation:

$$s^e \equiv v \pmod{u}$$

Problem: Bob kann beliebige (v,s) erzeugen, v ist zufällig.

Lösung: In der Praxis wird Redundanz hinzugefügt, d.h. der Hash des Vertrages.

Für Unterschriften, die oft verifiziert werden sollen, kann $e = 3, 5, \dots$ gewählt werden. Diese Wahl ist nicht unsicher!

Sicherheit von RSA: Faktorisierungsproblem

Es ist kein effizienter Faktorisierungsalgorithmus bekannt.

- **Trial division:**
Zeit $\sim \sqrt{u} = e^{\frac{1}{2} \log(u)}$
- **Number field sieve**
Der effizienteste bekannte Algorithmus.
Zeit $\sim e^{(\log n)^{\frac{1}{3}}} = e^{\sqrt[3]{\log n}}$

5.6 Faktorisieren

5.7 Diskreter Logarithmus

Wir nehmen als Beispiel das Rechnen modulo n . Der diskrete Logarithmus ist hier die kleinste Lösung für x , so dass $a^x \equiv m \pmod{p}$ bei gegebenen natürlichen Zahlen m, a und der Primzahl p .

Die diskrete Exponentiation lässt sich leicht berechnen, während für die Umkehrfunktion, der diskrete Logarithmus, nur schwere Algorithmen bekannt sind.

$$\text{Laufzeit} \sim \sqrt{G} = e^{\frac{1}{2} \log |G|}$$

5.8 Diffie-Hellman

Der **Diffie-Hellmann-Schlüsselaustausch** ist ein Protokoll mit dem zwei Kommunikationspartner einen geheimen Schlüssel, den nur diese beiden kennen, erzeugen können. Beide Partner schicken dem anderen über einen unsicheren Kanal eine Nachricht zu. Aus diesen beiden Schlüsseln den geheimen Schlüssel zu berechnen ist praktisch nicht lösbar.

Prinzip von Diffie-Hellmann

1. Die Kommunikationspartner einigen sich auf eine Primzahl p und eine Primitivwurzel $g \pmod p$ mit $2 \leq g \leq p - 2$. Diese Parameter müssen nicht geheim sein.
2. Beide Kommunikationspartner erzeugen eine geheim zu haltende Zufallszahl a , bzw. b aus der Menge $\{1, \dots, p - 2\}$. a und b werden nicht übertragen, bleiben also dem jeweiligen Kommunikationspartner aber auch potenziellen Lauschern unbekannt.
3. Die Kommunikationspartner berechnen $A = g^a \pmod p$, bzw. $B = g^b \pmod p$. Nun werden A und B übertragen.
4. Die Partner berechnen nun $K = B^a \pmod p$ bzw. $K = A^b \pmod p$. Das Ergebnis K ist für beide Partner gleich und kann als Schlüssel für die weitere Kommunikation verwendet werden.

Beweis

Das beide Partner den selben Wert für K berechnen, sieht man an den folgenden Umformungen:

$$K = B^a \pmod p = (g^b \pmod p)^a \pmod p = g^{ba} \pmod p = g^{ab} \pmod p$$

$$K = A^b \pmod p = (g^a \pmod p)^b \pmod p = g^{ab} \pmod p$$

5.9 Körper

$(K, +, \bullet)$ ist ein **Körper**, falls K Menge und $+$ und \bullet Operationen: $K \times K \rightarrow K$ wenn gilt:

- $(K, +)$ ist abelsche Gruppe (Neutralelement 0)
- $(\underbrace{K \setminus \{0\}}_{K^*}, \bullet)$ ist abelsche Gruppe (Neutralelement $1 \neq 0$)
- $\forall a, b, c \in K : a(b + c) = ab + ac$

Beispiele: $\mathbb{Q}, \mathbb{R}, \mathbb{C}, (\underbrace{\mathbb{Z}_p, +, \bullet}_{GF(p)})$ mit p prim

Ein **endlicher Körper** oder **Galoiskörper** ist ein Körper mit nur endlich vielen Elementen.

$$GF(p) = (\mathbb{Z}_p, +, \bullet)$$

Ein **Ring** ist eine algebraische Struktur $(M, +, \cdot)$ mit folgenden Eigenschaften:

- $(M, +)$ ist eine kommutative Gruppe mit Neutralelement 0
- Für alle $a, b, c \in M$ gilt das Assoziativgesetz:
 $a \cdot b = b \cdot a$
- Für alle $a, b, c \in M$ gilt das Distributivgesetz:
 $(a + b) \cdot c = a \cdot c + b \cdot c$
 $c \cdot (a + b) = c \cdot a + c \cdot b$

Ein **Integritätsbereich** ist ein Ring, bei dem für alle $a, b \in M$ gilt:
 $a \cdot b = 0, a \neq 0 \rightarrow b = 0$

Die **Charakteristik** ist eine Kennzahl eines Körpers, die angibt, wie oft man die im Körper enthaltene Zahl 1 aufaddieren muss, um als Ergebnis 0 zu erhalten.

Beispiel: Der unendliche Körper $GF(2)$ hat Charakteristik 2:

$$1(x) + 1(x) = 0$$

Rechenregeln in GF(2)

$$1+ = -1$$

$$1 + 1 = 0, 2 = 0, a = -a$$

$$(a + b)^2 = a^2 + \underbrace{2ab}_{ab+ab=ab(1+1)=0} + b^2 = a^2 + b^2$$

Polynome über Körpern (z.B. über GF(p))

Beispiel: $GF(2)$ Arithmetik mit Koeffizienten $\in \{0, 1\}$

Beispiel: $GF(9) = GF(3^2)$. Arithmetik modulo ein irreduzibles Polynom über $GF(3)$ vom Grad 2. Dabei gibt es für $n \in \mathbb{N}$ genau dann einen Körper mit n Elementen, wenn $n = p^k$ für eine Primzahl p und ein $k \in \mathbb{N}$. Sind K_1 und K_2 zwei endliche Körper mit $|K_1| = |K_2|$, so gilt $K_1 \cong K_2$.

5.10 Polynome

+	0	1	x	$x + 1$
0	0	1	x	$x + 1$
1	1	0	$x + 1$	x
x	x	$x + 1$	0	1
$x + 1$	$x + 1$	x	1	0

$$x + (x + 1) = \underbrace{2x}_0 + 1 = 1$$

•	0	1	x	$x + 1$
0	0	0	0	0
1	0	1	1	$x + 1$
x	0	x	$x + 1$	1
$x + 1$	0	$x + 1$	1	x

$$x^2 \equiv x + 1 \pmod{x^2 + x + 1}$$

$$(x^2) = (x + 1 + 1 * (x^2 + x + 1))$$

$$(x + 1)^2 = x^2 + 1 \equiv x$$

Sei K ein Körper, dann ist $K[x]$ **Polynomring**:

$$K[x] := \left\{ \sum_{i=0}^n a_i \cdot x^i \mid a_i \in K, a_n \neq 0 \right\}$$

$$\deg\left(\sum_{i=0}^n a_i x^i\right) = n, \text{ falls } a_n \neq 0.$$

K Körper, $a(x), b(x) \in K[x]$ und

$$b(x) \neq \underbrace{0(x)}_{\text{Nullpolynom}}$$

dann gibt es eindeutige $q(x), r(x)$, so dass gilt:

$$a(x) = q(x) \cdot b(x) + r(x)$$

mit $\deg(r(x)) < \deg(b(x))$

Polynomdivision

Wir schreiben:

$$r(x) = R_{b(x)}(a(x))$$

Teilbarkeit und irreduzible Polynome

Teilbarkeit der Polynome:

Sei $a(x), b(x) \in K[x], b \neq 0$

Dann gilt:

$$b(x) | a(x) : \leftrightarrow \exists c(x) \in K[x] b(x) \cdot c(x) \equiv a(x).$$

Ein nichtkonstantes Polynom $p(x)$ heisst **irreduzibles Polynom**, wenn es sich nicht als Produkt zweier nichtkonstanter Polynome schreiben lässt

- $\deg(p(x)) \geq 1$
- $p(x) = s(x) \cdot t(x) \rightarrow (\deg(s) = 0 \vee \deg(t) = 0)$
- Alle **linearen Polynome** sind irreduzibel.
- Ein Polynom von Grad 2 oder 3 ist genau dann irreduzibel, wenn es keine Nullstelle hat

Nullstellen und lineare Faktoren

$a(x) \in K[x], c \in K$ mit $a(c) = 0$ (c heisst Nullstelle)

Genau dann gilt: $(x-c) \mid a(x)$

Folgerung: Ein Polynom mit $\deg \geq 2$ mit mindestens einer Nullstelle ist nicht irreduzibel. (Bemerkung: Umkehrung falsch i.A., Umkehrung richtig, falls $\deg = 2,3$)

Beispiel: Irreduzible Polynome in $K = GF(2)$

- $x \mid x^2$
x ist irreduzibel
 x^2 ist nicht irreduzibel
- $(x+1) \mid (x^2+1) = (x+1)^2$

Euklidischer Algorithmus

Beispiel: EEA($x^3 + 2x + 1, 2x^2 + x + 2$) über $K = GF(3)$

$x^3 + 2x + 1$	1	0
$2x^2 + x + 2$	0	1
$2x$	1	$x + 1$
2	$2x + 1$	$2x^2 + 1$
1	$x + 2$	$x^2 + 1$

5.11 Shamir's Secret Sharing

Ein Geheimnis (eine Zahl) wird in mehrere Teile zerlegt, wobei jeder Teilnehmer einen einzigartigen Teil erhält, wobei eine bestimmte Anzahl der Teile benötigt wird, um das Geheimnis zu rekonstruieren.

Wir zerteilen ein Geheimnis D in n Teile D_1, \dots, D_n , so dass gilt:

- Das Wissen über k oder mehr D_i -Stücke macht D einfach berechenbar

- Das Wissen über $k - 1$ oder weniger D_i -Stücke lässt D komplett unbestimmt (alle seine möglichen Werte sind gleich wahrscheinlich)
- Dieses Schema heisst „ (k, n) threshold scheme“

Idee von Adi Shamir

Es braucht 2 Punkte zur Definition einer Linie, 3 für eine Parabel, etc. Es braucht also $n + 1$ Punkte um ein Polynom des Grades n eindeutig zu bestimmen. Verwenden wir das (k, n) threshold scheme, um das Geheimnis S zu teilen.

Wähle zufällige $(k - 1)$ Koeffizienten a_1, \dots, a_{k-1} und sei $a_0 = S$. Dies ergibt nun ein Polynom $f(x) = a_0 + a_1x + \dots + a_{k-1}x^{k-1}$. Wähle n beliebige Punkte i und erzeuge Paare $(i, f(i))$ für jeden der Punkte. Jeder Mitwisser erhält ein solches Paar. Mit beliebigen k Paaren können wir durch Interpolation das Polynom und somit das Geheimnis a_0 bestimmen (den konstanten Teil des Polynoms).

Rekonstruktion mit Lagrange

Es seien folgende Stützstellen gegeben:

- $(x_0, y_0) = (2, 1942);$
- $(x_1, y_1) = (4, 3402);$
- $(x_2, y_2) = (5, 4414);$

Wir berechnen die Lagrange-Polynome:

$$\begin{aligned} \ell_0 &= \frac{x-x_1}{x_0-x_1} \cdot \frac{x-x_2}{x_0-x_2} = \frac{x-4}{2-4} \cdot \frac{x-5}{2-5} = \frac{1}{6}x^2 - 1\frac{1}{2}x + 3\frac{1}{3} \\ \ell_1 &= \frac{x-x_0}{x_1-x_0} \cdot \frac{x-x_2}{x_1-x_2} = \frac{x-2}{4-2} \cdot \frac{x-5}{4-5} = -\frac{1}{2}x^2 + 3\frac{1}{2}x - 5 \\ \ell_2 &= \frac{x-x_0}{x_2-x_0} \cdot \frac{x-x_1}{x_2-x_1} = \frac{x-2}{5-2} \cdot \frac{x-4}{5-4} = \frac{1}{3}x^2 - 2x + 2\frac{2}{3} \end{aligned}$$

Somit:

$$\begin{aligned} f(x) &= \sum_{j=0}^2 y_j \cdot \ell_j(x) \\ &= 1942 \cdot \left(\frac{1}{6}x^2 - 1\frac{1}{2}x + 3\frac{1}{3}\right) + 3402 \cdot \left(-\frac{1}{2}x^2 + 3\frac{1}{2}x - 5\right) + 4414 \cdot \left(\frac{1}{3}x^2 - 2x + 2\frac{2}{3}\right) \\ &= 1234 + 166x + 94x^2 \end{aligned}$$

Das Geheimnis ist nun der freie Koeffizient, das heisst $S = 1234$.

Geheimnis ausrechnen

Gegeben seien n Stützstellen (x_i, y_i) , aus denen der konstante Koeffizient des Polynoms von Grad $n - 1$ berechnet werden soll. Für jedes i wird nun ein l_i berechnet:

$$l_i = \prod_{j=1, j \neq i}^n \frac{-x_j}{x_i - x_j}$$

Der konstante Koeffizient a berechnet sich nun aus:

$$a = \sum_{j=1}^n y_j \cdot l_j$$

Beispiel: Zwei-aus-vier Secret-Sharing

Es wurde der kleinstmögliche Körper $GF(5)$ gewählt. Folgende Stellen sind von $f(x) = a + bx$ bekannt:

$$f(1) = 3, f(2) = 0$$

Somit:

$$\begin{aligned} f(1) &= a + b = 3 \\ f(2) &= a + 2b = 0 \end{aligned}$$

Es folgt $a = -2b$ und dadurch $b = -3 \equiv 2$ und $a = 6 \equiv 1$.