# DISKRETE MATHEMATIK

Zusammenfassung zur Vorlesung von
Prof. Dr. A. Steger

Lukas Cavigelli, Dezember 2010
lukasc@ee.ethz.ch

## BEWEISVERFAHREN

Gegenbeispiel
Gegenannahme zu Widerspruch führen.

### INDUKTION

**Verankerung**, dann Rekursion:
1. Induktionsanfang $n = 1$
zu zeigen: < hier steht $A(1)$ >
Beweis: < hier steht der Beweis von $A(1)$ >
2. Induktionsschritt $A(n) \Rightarrow A(n+1)$
**Annahme**: < hier steht $A(n)$ >
zu zeigen: < hier steht $A(n+1)$ >
**Beweis**: < hier wird $A(n+1)$ unter Verwendung von $A(n)$ bewiesen >

### PEANO-AXIOME

1. $0 \in \mathbb{N}$
2. $n \in \mathbb{N} \Rightarrow n' \in \mathbb{N}$
3. $n \in \mathbb{N} \Rightarrow n' \neq 0$
4. $m, n \in \mathbb{N} \Rightarrow (m' = n' \Rightarrow m = n)$
5. $0 \in \mathbb{X} \wedge \forall n \in \mathbb{N}: (n \in \mathbb{X} \Rightarrow n' \in \mathbb{X}) \Rightarrow \mathbb{N} \subseteq \mathbb{X}$ (Induktionsaxiom)

## IMPLIKATION

| A | B | $A \Rightarrow B$ |
|---|---|---|
| w | w | w |
| w | f | f |
| f | w | w |
| f | f | w |

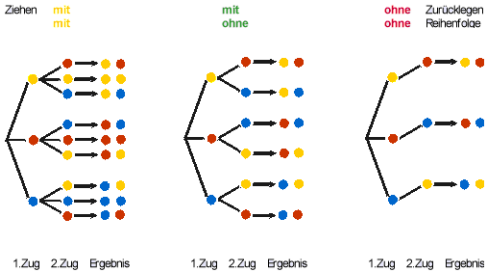
Kontrapunktion:
$(A \Rightarrow B) \Leftrightarrow (\neg B \Rightarrow \neg A)$
Disjunktion:
$(A \Rightarrow B) \Leftrightarrow (\neg A \vee B)$
Konjunktion:
$(A \Rightarrow B) \Leftrightarrow \neg(A \wedge \neg B)$

## SCHREIBWEISEN DIESER VORLESUNG

**Mengen**:
$\mathbb{N}$: natürliche Zahlen ohne 0
$\mathbb{N}_0$: natürliche Zahlen mit 0
$\mathbb{Z}$: ganze Zahlen
$\mathbb{Q}$: rationale Zahlen
$\mathbb{R}$: reelle Zahlen
$\mathbb{Z}_n$: $\{0,1,2,\dots,n-1\}$ mit $n \in \mathbb{N}$
$[n]$: $\{1,2,\dots,n\}$ mit $n \in \mathbb{N}$
**Zahlen**:
$\lfloor x \rfloor$: grösste Zahl $\in \mathbb{Z}$ kleiner gleich $x$, $\lfloor 1.6 \rfloor = 1, \lfloor -1.6 \rfloor = -2$
$\lceil x \rceil$: kleinste Zahl $\in \mathbb{Z}$ grösser gleich $x$, $\lceil 1.6 \rceil = 2, \lceil -1.6 \rceil = -1$
**Mengenoperationen**:
$A \setminus B$: Differenz von $A$ und $B$ $\{x | x \in A \wedge x \notin B\}$
$A \Delta B$: symmetrische Differenz $(A \setminus B) \cup (B \setminus A)$
$A \times B$: kartesisches Produkt $\{(a,b) | a \in A \wedge b \in B\}$
$A \uplus B$: Vereinigung von disjunkten Mengen
$\mathcal{P}(A), 2^A$: Potenzmenge von $A$ $\{M | M \subseteq A\}$

## KOMBINATORIK

| | Mit Repetition $\{a,a,b\}$ | Ohne Repetition $\{a,b,c\}$ |
|---|---|---|
| **Variation=geordnet** $(a,b) \neq (b,a)$ | $n^k$ | $n^{\underline{k}} = \binom{n}{k} k!$ |
| **Kombination=ungeord.** $\{a,b\} = \{b,a\}$ | $\binom{n+k-1}{k}$ | $\binom{n}{k}$ |
| **Permutation** $M = \{l_1 a, l_2 b, \dots, l_k x\}$ | $\frac{(\sum_{i=1}^k l_i)!}{\prod_{i=1}^k (l_i!)}$ | $n! = \lvert \mathfrak{S}_n \rvert$ |




### ANGEHENSWEISEN

Addieren, subtrahieren und multiplizieren von Möglichkeiten.
Prinzip der **Inklusion-Exklusion** (evtl. Mengen zeichen):
$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$

### BINOMIALKOEFFIZIENT

$$\binom{n}{k} := \frac{n!}{k!\,(n-k)!} = \frac{n^{\underline{k}}}{k!} = \prod_{j=1}^{k} \frac{n+1-j}{j}, \qquad k > n \Rightarrow \binom{n}{k} = 0$$

**Rechenregeln**:
$$\binom{n}{0} = \binom{n}{n} = 1, \quad \binom{n}{1} = n, \quad \binom{n}{k} = \binom{n}{n-k}$$
$$k\binom{n}{k} = n\binom{n-1}{k-1}, \quad \binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1}$$
$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}, \qquad 2^n = \sum_{k=0}^{n} \binom{n}{k}$$

Vandermonde'sche Identität:
$$\binom{n+m}{k} = \sum_{l=0}^{k} \binom{n}{l}\binom{m}{k-l}, \qquad k, m, n \in \mathbb{N}_0$$

**Veranschaulichung/Pascal'sches Dreieck**:
$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k, \qquad \text{(Pascal'sches Dreieck)}$$

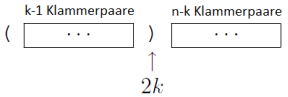
**Andere Operatoren**:
$$n^{\underline{k}} := n(n-1)(n-2)\dots(n-k+1) = \prod_{i=0}^{k-1}(n-i) = \frac{n!}{(n-k)!}$$
$$n! = n^{\underline{n}}, \qquad n^{\underline{0}} = 1, \qquad 0! = 1$$

### ZAHLENPARTITIONEN

blabla
**Diphantische Gleichungen**:

### CATALAN-ZAHLEN

**Anwendungen**:
Klammerausdrücke, Triangulierungen in $n$-Eck, Binärbäume
**Ausdruck**:
Für die Anzahl $C_n$ der korrekten Klammerausdrücke mit $n$ Klammerpaaren, $n \in \mathbb{N}_0$ gilt:
$$C_0 = 1, \qquad C_n = \sum_{k=1}^{n} C_{k-1} C_{n-k}, n \geq 1$$
**Überlegungsweise**: anhand von $n$ Klammerpaaren




**Direkte Berechnung**:
$$B_n = T_{n+2} = C_n = \frac{1}{n+1}\binom{2n}{n}, \qquad \forall n \in \mathbb{N}_0$$

### ASYMPTOTISCHE ABSCHÄTZUNGEN

**Arithmetisches & quadratisches Mittel**:
$$\underbrace{\frac{1}{n}\sum_{i=1}^{n} x_i}_{\text{arithmetisches Mittel}} \leq \underbrace{\sqrt{\frac{1}{n}\sum_{i=1}^{n} x_i^2}}_{\text{quadratisches Mittel}}$$
**Fakultätsfunktion**:
$$n^{n/2} \leq n! \leq \left(\frac{n+1}{2}\right)^n$$
Stirling-Formel: $n! = \sqrt{2\pi n}\left(\frac{n}{e}\right)^n \cdot \left(1 + \frac{1}{12n} + O\left(\frac{1}{n^2}\right)\right)$
**Binomialkoeffizienten**:
$$\left(\frac{n}{k}\right)^k \leq \binom{n}{k} \leq \left(\frac{en}{k}\right)^k$$

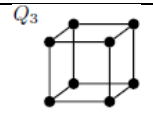
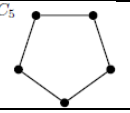
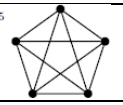
### UNTERE KOMPLEXITÄTSSCHRANKE

Jeder *vergleichsbasierte* Sortieralgorithmus benötigt zum Sortieren einer Folge von $n$ Zahlen im schlimmsten Fall mehr als $\frac{1}{2} n \log_2(n) - 1$ Vergleiche.
*Nicht vergleichsbasierter* Sortieralgorithmus: *Bucketsort*
Zahlen in Kübel einsortieren und am Ende Kübel sortiert leeren.

## GRAPHENTHEORIE

$$G = (V, E)$$
$V$: endliche, nicht-leere Menge von Knoten (Vetrices)
$E$: Edges, Teilmenge der zweielementigen Teilmengen von $V$
also $E \subseteq \binom{V}{2} := \{\{x,y\} | x, y \in V, x \neq y\}$

### SPEZIELLE GRAPHENKLASSEN

| | |
|---|---|
| **Hyperwürfel $Q_d$**:<br>ist $d$-regulär<br>$V(Q_d) = \{0,1\}^d$<br>$d = 3$: $V(Q_3) = \{000, 001, \dots, 111\}$<br>also $\lvert V(Q_3) \rvert = 8$ |  |
| **Vollständig bipartiter Graph $K_{n,n}$**:<br>ist $n$-regulär | |
| **$C_n$**:<br>ist 2-regulär |  |
| **$K_n$**:<br>ist $(n-1)$-regulär |  |

### BEGRIFFE

Nachbarschaft: $\Lambda(v) = \{u \in V | \{u,v\} \in E\}$
Grad: $\deg(v) = |\Lambda(v)|$
G heisst k-regulär, wenn: $\deg(v) = k \; \forall v \in V$
Sprechweise für $e = \{u,v\} \in E$:
- u und v sind adjazent
- u und e sind inzident
Für jeden Graphen $G = (V,E)$ gilt:
$$\sum_{v \in V} \deg(v) = 2|E|$$
In jedem Graphen $G = (V,E)$ ist die Anzahl der Knoten mit ungeradem Grad gerade.
**Korollar 2.6**: Für jeden Graphe $G = (V,E)$ gilt: Die Anzahl der Knoten mit ungeradem Grad ist gerade.
**Durchschnittsgrad**:
$$d = \frac{\sum_{v \in V} \deg(v)}{|V|} = \frac{2|E|}{|V|}$$

### WEGE, PFADE, KREISE

**Weg** in $G$ ist eine Folge $(v_0, \dots, v_n)$ mit $\{v_i, v_{i+1}\} \in E$
**Pfad**: Weg, bei dem alle Knoten verschieden sind
**Zyklus**: Pfad Weg mit identischem Start- und Endkonten
**Kreis**: Zyklus, bei dem alle Knoten verschieden sind.

$G$ enthält:
- keinen $P_1 \Rightarrow |E| = 0$
- keinen $P_2 \Rightarrow \deg(v) \leq 1 \; \forall v \in V \Rightarrow |E| \leq \frac{|V|}{2}$
- keinen $C_4 \Rightarrow |E| \leq$

**Herleitung** für $G$ enthält keinen $C_4$:
kein $C_4 \Leftrightarrow \forall x, y \in V$ mit $x \neq y$ gilt:
$x$ und $y$ haben keine zwei gemeinsame Nachbarn.
Kantenweise ausgehend von $G$ (der keinen $C_4$ enthält) einen neuen (bipartiten) Graphen $H$:
Knotenmenge von $H$ = Knotenmenge von $G \cup$ {allen zweielementigen Teilmengen der Knotenmenge von $G$}
Kantenmenge von $H$ = verbinde $x \in G$ genau dann, mit $\{y,z\} \in \binom{V}{2}$ wenn $\{x,y\}, \{x,z\} \in E_G$
$\Rightarrow$ Graph $H$ (wie oben konstruiert) hat die Eiganschaft:
$$\deg_H(\{x,y\}) \leq 1$$
Zähle Kanten in $H$: Da $H$ bipartit, gilt:
$\sum_{v \in V_G} \deg_H(v) = |E_H| = \sum_{\{x,y\} \in \binom{V_G}{2}} \deg_H(\{x,y\}) \leq \binom{|V_G|}{2} \cdot 1$
$= \sum_{v \in V_G} \binom{\deg_G(v)}{2} \rightarrow$ jedes Paar von Nahcbarn von $v$ in $G$
generiert eine Kante in $H$. Also:
$\sum_{v \in V_G} \binom{\deg_G(v)}{2} = \frac{(\deg_G(v))^2 - \deg_G(v)}{2} \leq \binom{|V_G|}{2}$
$\Leftrightarrow \underbrace{\sum_{v \in V_G} (\deg_G(v))^2}_{\geq \frac{1}{|V_G|}\left(\sum_{v \in V_G} \deg(v)\right)^2 = 2|E_G|} - \underbrace{\sum_{v \in V_G} \deg_G(v)}_{=2|E_G|} \leq |V_G|^2$

## TEILGRAPHEN

**Teilgraph**: Ein Graph $G_1 = (V_1, E_1)$ heisst Teilgraph, von $G_2 = (V_2, E_2)$ falls $V_1 \subseteq V_2$ und
-Bei einem Graphen ohne Mehrfachkanten: $E_1 \subseteq E_2$
-Bei ungerichtet. G. mit mehrf.-K.: $E_1(v) \subseteq E_2(v) \forall v \coloneqq \binom{|V_2|}{2}$
**Induzierter Teilgraph**: Teilgraph, bei dem gilt:
-Bei ein Graph ohne mehrf.-K.: $E_1 = E_2 \cap \binom{|V_1|}{2}$
- Bei unger. G. mit mehrf.-K.: $E_1(v) = E_2(v) \cap \binom{|V_1|}{2}$

## ZUSAMMENHÄNGENDE GRAPHEN

**Komponente**: Zusammenhängender Teilgraph
**Lemma**: Jeder Graph $G = (V, E)$ enthält mindestens $|V| - |E|$ viele Komponenten.
**Korollar**: Jeder zusammenhängende Graph $G = (V, E)$ enthält mindestens $|V| - 1$ viele Kanten
**Beweis**: Es muss gelten $|V| - |E| \leq 1$
**Definition zusammenhängend**:
$G$ ist zusammenhängend, wenn $\forall u, v \in V, u \neq v$ gilt: es gibt einen $u$-$v$-Pfad in $G$
**Lemma**: $G = (V, E)$ ein zusammenhängender Graph, $C$ ein Kreis in $G$. Dann gilt: $G_e = (V, E \backslash e)$ zusammenhängend $\forall e \in C$
**Lemma**: Sei $G = (V, E)$ und $v \in V$ beliebiger Knoten. Dann gilt: $G$ zusammenh. genau dann, wenn $\exists u$-$v$-Pfad in $G$ $\forall u \in V$
**Definition**: Sei $G = (V, E)$ ein Graph. $G$ heisst $k$-zusammenhängend, wenn: $|V| \geq k + 1$ und $\forall X \subseteq V$ mit $|X| < k$ gilt: $G[V \setminus X]$ ist zusammenhängend.
**Satz von Menger**: Sei $G = (V, E)$ ein Graph. Dann gilt: $G$ ist $k$-zusammenhängend genau dann, wenn $\forall u, v \in V, u \neq v$ existieren $k$-intern knotendisjunkte $u$-$v$-Pfade in $G$.

## HAMILTONKREISE & EULERTOUREN

**Hamiltonkreis**: Ein Hamiltonkreis ist ein Kreis, der jeden *Knoten* des Graphen genau einmal enthält.
#möglicher Hamiltonkreise: $\frac{n!}{2n}$
**Eulertour**: Eine Eulertour ist ein geschlossener Weg, der jede *Kante* des Graphen genau einmal enthält.
**Satz**: Ein $n \times m$ Gitter enthält genau dann einen Hamiltonkreis, wenn $n \cdot m$ gerade ist.
**Satz**: es gibt eine Eulertour ⇔ jeder Knoten hat eine gerade Anzahl Kanten (=der Grad aller Knoten ist gerade).

## MATRIXSCHREIBWEISE

**Adjazenzmatrix**: $A_G = (a_{ij})_{i,j=1}^{n},\ a_{i,j} = \begin{cases} 1, & \{i,j\} \in E \\ 0, & sonst \end{cases}$
$$A_G^1 = A_G, \qquad A_G^{k+1} = A_G A_G^k, k \geq 1$$
Satz: der Eintrag $a_{ij}^k$ der $i$-ten Zeile und $j$-ten Spalte in $A_G^k$ beschreibt die Anzahl der Wegen der Länge $k$ von $i$ nach $j$ in $G$.

## GERICHTETE GRAPHEN (DIGRAPHEN)

**Digraph**: $D = (V, A),\ A \subseteq V \times V,\ u, v, \in V,\ (u, v) \neq (v, u)$
Keine Mehrfachkanten (Def. in dieser Vorlesung)
**Grad eines Knoten**:
Ausgrad: $\deg^-(v) \coloneqq |\{(x, y) \in A | x = v\}|$
Ingrad: $\deg^+(v) \coloneqq |\{(x, y) \in A | y = v\}|$
Es gilt immer: $\sum_{v \in V} \deg^-(v) = |A| = \sum_{v \in V} \deg^+(v)$
Für ungerichtete Graphen gilt somit: $|A| = 2|E|$

**Gerichteter Weg** der Länge $l$ in einem Digraphen $D = (V, A)$ und $w = (v_0, v_1, \dots, v_\ell) \in V^{\ell+1},\ (v_\ell, v_{\ell+1}) \in A \forall i = 0 \dots \ell - 1$
**Adjazenzmatrix**: $A_D = (a_{ij})^n,\ a_{ij} = \begin{cases} 1, & (i,j) \in A \\ 0, & sonst \end{cases}$
**Starker Zusammenhang**: $\forall u, v, \in V$: ∃ ger. Weg von $u$ nach $v$ und $v$ nach $u$

## BÄUME

**Baum**: Ein Baum ist zusammenhängender, kreisfreier Graph.
**Wald**: Ein Wald ist ein Graph, in dem alle Zusammenhangskomponenten Bäume sind.
**Blatt**: Ein Knoten $v$ in einem Baum heisst Blatt, wenn $\deg(v) = 1$
**Wurzel**: bla

**Lemma 2.42**: Jeder Baum $T = (V, E)$ mit $|V| \geq 2$ hat min. 2 Blätter.
**Lemma 2.44**: Ist $T = (V, E)$ ein Baum und $u \in V$ ein Blatt in $T$, dann ist $T' \coloneqq T[V \setminus \{u\}]$ ebenfalls ein Baum.
**Satz 2.45**: Ist $T = (V, E)$ ein Baum , so gilt: $|E| = |V| - 1$.
**Satz**: Ein Graph $G = (V, E)$ ist ein Baum (hat also keinen Kreis) genau dann, wenn $G$ zusammenhängend ist und $|E| = |V| - 1$.
**Satz 2.46**: Jeder zusammenhängende Graph $G = (V, E)$ enthält einen Spannbaum.
**Satz 2.47**: Für $n \geq 2$ Knoten gibt es genau $n^{n-2}$ markierte Spannbäume.
**Codierung** für Bäume: blabla

## MATCHINGS, HEIRATSSATZ

**Definition Matching**:
Eine Kantenmenge $M \subseteq E$ heisst Matching in einem Graphen $G = (V, E)$, falls kein Knoten des Graphen zu mehr als einer Kante aus $M$ inzident ist, oder formal augedrückt, wenn:
$$e \cap f = 0 \forall e, f \in M \; mit \; e \neq f$$
Man sagt ein Knoten $v$ wird von $M$ überdeckt, falls es eine Kante $e \in M$ gibt, die $v$ enthält. Ein Matching $M$ heisst perfektes Matching, wenn jeder Knoten durch genau eine Kante aus $M$ überdeckt wird, oder, anders ausgedrückt, wenn $|M| = \frac{|V|}{2}$.
**Satz 2.51**: Für einen bipartiten Graphen $G = (A \uplus B, E)$ gibt es genau dann ein Matching $M$ der Kardinalität $|M| = |A|$, wenn:
$$|\Gamma(X)| \geq |X| \; \forall X \subseteq A$$
**Defintion**: $X \subseteq V: \Gamma(X) \coloneqq \bigcup_{v \in X} \underbrace{\Gamma(x)}_{\text{Nachbarn von } x}$

## PLANARE GRAPHEN

**Planar**: Ein Graph ist planar, wenn er eine ebene Einbettung hat, d.h. wie Knoten und Kanten in der Ebene so zeichnen können, dass sich kein zwei Kanten kreuzen.
Jeden planaren Graphen kann man eben zeichnen.
**Satz (euler'sche Polyederformel)**: $G(V, E)$ zusammenhängend und eben eingebettet, dann gilt:
$$\#\text{Gebiete} = |E| - |V| + 2$$
*Aufpassen: Das Gebiet ausserhalb mitzählen!!*
*Achtung: Euler'sche Polyederformel gilt nur für kugelförmige Objekte, z.B. nicht für Reifen (mit einem Loch)*

**Satz**: $G = (V, E)$ planar, $|V| \geq 3$, dann $|E| \leq 3|V| - 6$
**Satz**: $G = (V, E)$, bipartit, dann $|E| \leq 2|V| - 4$

**Satz von Kuratowski**: Ein Graph $G$ ist genau dann planar,wenn er weder eine Unterteilung des $K_5$ noch des $K_{3,3}$ als Teilgraphen enthält.

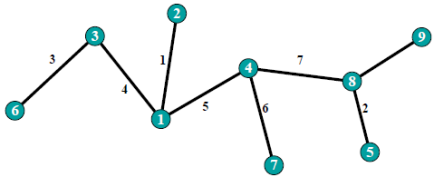
Ein planarer Graph $G = (V, E), |V| = n$ benötigt $O(n)$ Speicher bei Adjazenzlitenspeicherung.

Man kann einen bipartiten G. in $O(n)$ Zeit auf Planarität testen.

Prüfercode!

Jedes Gebiet hat ≥ 3 Kantenseiten. Jede Kante hat 2 Seiten.
→ $3|R| \leq 2|E|$

**NP-vollständigkeit**:
P: effizient entscheidbare Probleme, polynomial complexity
NP: (einseitig) effizient verifizierbare Probleme, non-polyn. c.
**Prüfer-Code**: Zur eindeutigen Codierung von Bäumen




Der Prüfercode ist (1,8,3,1,4,4,8).
Ein Knoten von Grad $d$ kommt $(d-1)$-mal im Code vor.
Ein Baum mit $n$ Elementen hat einen Code der Länge $n - 2$.

## FLÜSSE IN NETZWERKEN

**Netzwerk**: bedeutet für diese Vorlesung gerichteter Graph.
$$N = (V, A, s, t, c)$$
$(V, A)$: gerichteter Graph
$s \in V$ **Quelle**, $t \in V, t \neq s$ **Senke**, $c: A \to \mathbb{R}_0^+$ **Kapazitätsfunkt**.
**Fluss**: $f: A \to \mathbb{R}_0^+$, falls
1. $0 \leq f(e) \leq c(e)\ \forall e \in A$.
2. $\forall v \in V \setminus \{s, t\}: \sum_{(u,v) \in A} f(v, u) = \sum_{(v,u) \in A} f(v, u)$
3. Der Wert des Flusses $f$ ist $\text{val}(f) \coloneqq \text{netoutflow}(s) \coloneqq \sum_{(s,u) \in A} f(s, u) - \sum_{(s,u) \in A} f(u, s)$
Lemma: $\text{netinflow}(t) \coloneqq \sum_{(u,t) \in A} f(u, t) - \sum_{(t,u) \in A} f(t, u) = \text{val}(f)$
**Berechnung des maximalen Flusses**:
Ein $(s,t)$-schnitt in einem Netzwerk $N = (V, A, s, t, c)$ ist eine Partition $(S, T)$ von $V$ mit $s \in S$ und $t \in T$.
**Kapazität**: $\text{cap}(S, T) \coloneqq \sum_{(u,w) \in (S \times T) \cap A} c(u, w)$
also die Summe der Kapazitäten der Pfeile, die von S nach T gehen. (die entgegengesetzten Pfeile NICHT abziehen)
Lemma: $f$ Fluss, $(S, T)$ ein $s$-$t$-Schnitt in $N$: $\text{val}(f) \leq \text{cap}(S, T)$
**Bew**: Für eine Partition $(U, W)$ von $V$:
$f(U, W) = \sum_{(u,w) \in (U \times W) \cap A} f(u, w)$.
$$\text{vol}(f) = f(S, T) - f(T, S) \leq f(S, T) \leq \text{cap}(S, T)$$
**Maxflow-Mincut Theorem**:
$$\underbrace{\max \text{val}(f)}_{f \text{ Fluss in } N} = \underbrace{\min \text{cap}(S, T)}_{(S,T) \text{ s-t-Schnitt in } N}$$
**Proposition**: Kapazitäten ganzzahlig, ≤ 0.
max. Fluss $m$ in $O(mn(1 + \log(N)))$ Zeit berechnen mit $n = |V|, m = |A|$.
**Proposition**: allgemein $O(mn \log(n))$
Algorithmus!!!
**Bipartites Matching** als Fluss berechnen:
Zusätzlichen $s$ und $t$-Knoten einführen. $s$ mit allen Knoten der einen Seite des bipartiten Graphen verbinden, $t$ mit den anderen. Dann: maximaler Fluss = bestes Matching.

## BILDSEGMENTIERUNG

(Unterscheidung Vorder- vs. Hintergrund, Objekterkennung)
Pixel $p, \alpha_p \in \mathbb{R}$(je grösser desto mehr im Vordergrund), $\beta_p \in \mathbb{R}$ (...Hintergrund).
Vordergrund: $A = \{p \in P, \alpha_p > \beta_p\}$
Das ist viel zu granuliert (instabil). Deshalb führen wir ein:
Kante $e = \{p, p'\}$ und
$\gamma_e \in \mathbb{R}$je grössere, desto mehr ist $p$ und $p'$ im gleichen Teil.
Für eine Auflösung $(A, B),\ P = A \cup B$
Qualitätsmass: $q(A, B) = \sum_{p \in A} \alpha_p + \sum_{p \in B} \beta_p - \sum_{|e \cap A| = 1} \gamma_e$
Dies gilt es zu maximieren. Äquivalente Aussage:
$$Q \coloneqq \sum_{p \in P} (\alpha_p - \beta_p)$$
$$q(A, B) = Q - \sum_{p \in A} \beta_p - \sum_{p \in B} \alpha_p - \sum_{|e \cap A| = 1} \gamma_e \to max$$
$$\Leftrightarrow q'(A, B) = \sum_{p \in A} \beta_p + \sum_{p \in B} \alpha_p + \sum_{|e \cap A| = 1} \gamma_e \to min$$
$(S, T)$ ein $s$-$t$-Schnitt in $N$ und
$$A \coloneqq S \setminus \{s\}, \qquad B \coloneqq T \setminus \{t\}$$
Betrachte die Kanten im Schnitt $(S, T)$, d.h. in $S \times T$.
= Kanten $(s, p)$ mit $p \in B$. Ihr Beitrag zu $\text{cap}(S, T)$ ist $\sum_{p \in B} \alpha_p$.
Kanten $(p, t)$ mit $p \in A$ ... Betrag $\sum_{p \in A} \beta_p$
Kanten $(p, p')$ in $A \times B$. Beitrag: $\sum_{(p,p') \in A \times B} \gamma(p, p') = \sum_{|e \cap A| = 1} \gamma_e$.
$$\text{cap}(S, T) = \sum_{p \in B} \alpha_p + \sum_{p \in A} \beta_p + \sum_{|e \cap A| = 1} \gamma_e$$

# ALGEBRA

## MODULARE ARITHMETIK

**Definition 5.1 (Algebra, Operator)**: Ein Algebra $\langle S, f_1, \dots, f_t \rangle$ besteht aus einer nichtleeren Trägermenge $S$ und Operatoren $f_1, \dots, f_t$ auf $S$. Ein Operator ist eine Abb. $f: S^m \to S$. Die Konstante $m \in \mathbb{N}$ nennt man die Stelligkeit des Operators. Zweistellige Operatoren nenn man auch Verknüpfungen.
**Definition 5.6 (neutrale Elemente)**: Sei $\langle S, \circ \rangle$ eine Algebra mit einem zweistelligen Operator $\circ$. Ein Element $e \in S$ heisst *linksneutrales Element* für den Operator $\circ$, falls: $e \circ a = a\ \forall a \in S$. Rechtsneutralen Element analog.
Ein neutrales Element ist rechts- und linksneutral.
**Lemma 5.8**: Sei $\langle S, \circ \rangle$ eine Algebra mit einer zweistelligen Verknüpfung $\circ$. Dann gilt: Ist $c$ ein linksneutrales Element und $d$ ein rechtsneutrales Element, so ist $c = d$. Insbesondere: Jede

Algebra $\langle S,\circ\rangle$ mit einer zweistelligen Verknüpfung $\circ$ enthält höchstens ein neutrales Element.
**Definition 5.10**: Sei $\langle S,\circ\rangle$ eine Algebra mit einem zweistelligen Operator $\circ$ und einem neutralen Element $e$. Ein Element $x \in S$ heisst linksinverses Element von $a \in S$, falls $x \circ a = e$.
Gilt stattdessen $a \circ x = e$, so nennt man $x$ ein rechtsinverses Element von $a$. Ein Element $x \in S$ heisst inverses Element, oder auch kurz Inverses von $a$, falls $x$ sowohl ein linksinverses als auch ein rechtsinverses Element von $a$ ist.
**Lemma 5.11**:

**Lemma**: $a,b,m \in \mathbb{Z}, m \geq 2$
$$(a+b) \bmod m = \big((a \bmod m) + (b \bmod m)\big) \bmod m$$
$$ab \bmod m = \big((a \bmod m)(b \bmod m)\big) \bmod m$$
**Lemma**: $a,b,c,d,m \in \mathbb{Z},\ m \geq 2$
$$a \equiv b\ (mod\ m), \qquad c \equiv d\ (mod\ m)$$
$$a+c \equiv b+d\ (mod\ m), \qquad ac \equiv bd\ (mod\ m)$$
ABER: $ac = bc\ (mod\ m) \Rightarrow a = b\ (mod\ m)$ gilt nur, wenn $ggT(c,m) = 1$
**Euklidischer Algorithmus zur ggT-Bestimmung**:
func Euklid(m,n):
if ($m$ teilt $n$) then {return $m$;} else {return Euklid($n \bmod m, m$);}
**Satz von Fermat**:
$$n\ Primzahl \Leftrightarrow a^{n-1} \equiv 1(mod\ n)\ \forall a \in \mathbb{Z}_n \setminus \{0\}$$
**Satz von Euler**: Für alle $n \in \mathbb{N}$ mit $n \geq 2$ gilt:
$$a^{\varphi(n)} \equiv 1(mod\ n), \qquad \varphi(n) = |\mathbb{Z}_n^*| = n-1$$

## GRUPPEN

**Def. Gruppe**:
Bestandteile: 1. Trägermenge $G$, 2. Verknüpfung $\circ: G \times G \to G$
Eigenschaften:
1. $\circ$ ist *assoziativ*, d.h. $(a \circ b) \circ c = a \circ (b \circ c),\ \forall a,b,c \in G$
2. $\exists$ *neutrales Elem.*: $e \in G$ mit $x \circ e = e \circ x = x\ \forall x \in G$
3. $\forall x \in G \exists$ ein *inverses Elem.* $y \in G$ mit $x \circ y = y \circ x = e$
Bsp.: Addition $(\mathbb{R},+)$ neutr. Elem: 0, inv. Elem: $-x$
Bsp.: Multipikation $(\mathbb{R} \setminus \{0\},\cdot)$ neutr. Elem: 1, inv. Elem: $1/x$
**Satz**: $\forall n \in \mathbb{N}, n \geq 2$ ist $\mathbb{Z}_n^*$ bzgl. Multipl. mod $n$ eine Gruppe
**Gesetze**:
Involution: $a = (a^{-1})^{-1}$
Kürzungsregel: $a \circ b = c \circ b \Rightarrow a = c$
Eindeutigkeit: $a \circ x = b \Leftrightarrow x = a^{-1} \circ b$
$x \circ a = b \Leftrightarrow x = b \circ x^{-1}$
Injektivität: $a \neq b \Leftrightarrow a \circ c \neq b \circ c \Leftrightarrow c \circ a \neq c \circ b$
Surjektivität: $\exists x: a \circ x = b$ und $\exists y: y \circ a = b$
**Ordnung**:
Sei $G$ eine Gruppe. Die Ordnung $ord(a)$ eines Elementes $a \in G$ ist das minimale $r \in \mathbb{N}$, so dass $a^r = e$. Existiert es nicht $\to \infty$.
**Lemma**: $G$ eine endliche Gruppe, so hat jedes Elem. endl. Ord.
**Lemma**: $G$ eine Gruppe, $a \in G$ ein Elem. mit endl. Ord., dann:
$$a^k = e \Leftrightarrow ord(a) | k$$

## UNTERGRUPPEN

**Def. Untergruppe**:
$\langle G,\circ\rangle$ eine Gruppe und $H \subseteq G$, dann heisst $\langle H,\circ\rangle$ Untergruppe von $G$, falls $\langle H,\circ\rangle$ eine Gruppe ist.
**Lemma**: $G$ eine Gruppe, $H$ eine Untergruppe von $G$, so sind die neutralen Elemente von $G$ und $H$ identisch.
**Lemma**:
Sei $G$ eine Gruppe und $a \in G$ ein Elem. endl. Ordnung, so ist:
$$S_a := \{e, a, a^2, \dots, a^{ord(a)-1}\}$$
die kleinste Untergruppe, die $a$ enthält.

## NEBENKLASSEN, SATZ VON LAGRANGE

**Def.:** Sei $H$ eine Untergruppe von $G$ und $b \in G$, dann heisst:
$H \circ b = \{h \circ b | h \in H\}$ *eine* rechte Nebenklasse von $H$ in $G$.
und $b \circ H = \{b \circ h | h \in H\}$ *eine* linke Nebenklasse von $H$ in $G$.
Falls $H \circ b = b \circ H$ gilt, so heisst $H \circ b$ auch Nebenkl. v. $H$ in $G$.
Bsp: $\langle \mathbb{Z}_{12},+_{12}\rangle,\ H = \{0,3,6,9\}$ ist Untergruppe.
$H = \{0,3,6,9\} = H+_{12}0 = H+_{12}3 = H+_{12}6 = H+_{12}9$
**Lemma**: Sei $H$ Untergruppe von $G$. Dann gilt:
1. $H \circ h = H\ \forall h \in H$
2. Für $b,c \in G$ sind Nebenkl. $H \circ b$ und $H \circ c$ ident. od. disjunkt
3. Ist $H$ endlich, so ist $|H \circ b| = |H|\ \forall b \in G$
Für linke Nebenklassen gelten analoge Aussagen.
**Korollar**: Sei $H$ eine Untergruppe $G$. Dann bildet die Menge der rechten (und ebenfalls der linken) Nebenklassen von $H$ eine Partition in $G$.
**Def.:** Die Anzahl verschiedener Nebenklassen von $H$ in $G$ heisst der Index von $H$ in $G$ und wird abgekürzt mit $ind_G(H)$.
**Satz (Lagrange)**: $G$ eine endl. Gruppe und $H$ eine Untergruppe von $G$. Dann gilt $|G| = |H| ind_G(H)$. Insbesondere teilt die Kardinalität von $H$ also diejenige von $G$.

## KÖRPER

**Def Körper**:
Ein Körper $\langle K,\oplus,\otimes\rangle$ besteht aus einer Trägermenge $K$ und zwei zweistelligen Operatoren $\oplus,\otimes: T \times T \to T$, so dass:
1. $\langle K,\oplus\rangle$ ist eine abelsches Gruppemit neutr. Elem $0 \in K$.
2. $\langle K \setminus \{0\},\otimes\rangle$ ist eine abelsche Grp. mit neutr. Elem. $1 \in K$.
3. $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)\ \forall a,b,c \in K$
**Eigenschaften**:
Lemma: Für jeden Körper $K$ gilt: $0 \cdot a = a \cdot 0 = 0\ \forall a \in K$
Lemma: Für jeden Körper $K$ gilt: $ab = 0 \Rightarrow a = 0$ oder $b = 0$
Satz: $\langle \mathbb{Z}_n,+_n \cdot_n\rangle$ ist ein Körper $\Leftrightarrow n$ ist Primzahl.
Satz: In jedem endl. Körper $K$ ist die multiplikative Gruppe $K^*$ zyklisch, d.h. $\exists a \in K^*$ mit $K^* = \{1, a, a^2, \dots a^{|K|-2}\}$.
**Def primitives Element**:
$K$ endl. Körper. Einen Generator der multiplikativen Gruppe $K^* = K \setminus \{0\}$ nennt man primitves Element.
Satz: blabla

## RSA-VERSCHLÜSSELUNG

**Initialisierung**:
Wahl von zwei Primzahlen $p,q$(zufällig)
Wahl von k: Zufällig Zahlen wählen, durchtesten bis $ggT(k,\varphi(n)) = 1$ wobei $n = pq$ (Euklid erw.) also $\varphi(n) = (p-1)(q-1)$
Wahl von $\ell$ so dass $k \cdot \ell = 1\ mod\ \varphi(n)$ (Euklid erw.)
**Verschlüsselung**:
Verschlüsseln: $s := m^k\ mod\ n$
Gesendete Nachricht: $s$
Entschlüsseln: $m := s^\ell\ mod\ n$

Def.: $\mathbb{Z}_n^* := \{x \in \mathbb{Z}_n \setminus \{0\} | ggT(x,n) = 1\}$

Beweis: $g^{n-1} \equiv 1(mod\ n)$, also $g^{n-1} - 1 = kn$
abelsch $\Leftrightarrow$ kommutativ

## ALLGEMEINE FORMELN

## SUMMENFORMELN

- $\sum_{k=1}^{n} \prod_{j=1}^{m} (k+j-1) = \frac{1}{m+1} \prod_{j=1}^{m+1} (n+j-1) \Rightarrow$
  $\sum_{k=1}^{n} k, \sum_{k=1}^{n} k^2, \dots$
- $\sum_{k=1}^{n} k = 1+2+3+4+5+6+7+8+\dots+n = \frac{n(n+1)}{2}$
- $\sum_{k=1}^{n} k^2 = 1^2+2^2+3^2+4^2+5^2+\dots+n^2 = \frac{n(n+1)(2n+1)}{6}$
- $\sum_{k=0}^{n} \frac{(-1)^k}{k!} = \frac{1}{e}$

## AUS DEN ÜBUNGEN

# **Derangement** (= fixpunktfrei Permutation) = Subfakultät:
$$!n = n! \sum_{i=0}^{n} \frac{(-1)^i}{i!}$$

## TIPPS

$F_{\{1,2\}}$: Funktionen, die 1 auf 1 und 2 auf 2 abbilden.
$$F_{\{1\}} \cap F_{\{2\}} = F_{\{1,2\}}$$
Anteil = #spezielle/#total. Hier: total=n!, Anteil=D_n/n!

## SERIE 3

**A1**: Petersen-Graph
$$V(G) = \{x,y\} \subseteq \{a,b,c,d,e\}$$
Kante zwischen Mengen, die kein gleiches Element haben.
Beweis: falls es ein Dreieck (oben z.B. $\{a,b\}$ gibt, dann kann keine Wahl für die übrigen Ecken getroffen werden, so dass ale Menge disjunkt sind.
**A2**: Gegeben: 2 längste Pfade. Behauptung: 1 Knoten gemeinsam.
Methode: Annahme es stimme nicht, dann Widerspruch zeigen. Zwei gleichlange Pfade, Verbindung einfügen -> Widerspruch
**A3**: Gegeben: Graph G. $\exists$ 2 disjunkte Kreise. Zeigen: es gibt einen Pfad so lange wie die Kreise zusammen - 1.
Bsp: Party-Organisation: 8 Bands, Organisator wählt 3 aus. Es hat n Gäste. Nach einer Umfrage merkt er: Für jedes Tripel von Bands mögen min. 4/5 der Gäste alle 3.
Beh: Min. 1 Gast hat alle 8 gewählt
Trick: zähle alle $\left(\underbrace{(i,j,h)}_{=S}, g\right)$, so dass Gast g $(i,j,h)$ gewählt hat. S: Summe aller gewählten Tripel.
$S = \sum_{g \in S} \binom{\#Bands\ gewählt}{3} \leq \binom{7}{3}$.
$S \geq \sum_{\{i,j,k\} \in Bands} \frac{4}{5} n = \binom{8}{3} \cdot \frac{4}{5} n$
$n\binom{7}{3} \geq S \geq \binom{8}{3} \cdot \frac{4}{5} n, \qquad 35n \geq \frac{4}{5} 56n \Rightarrow Widerspruch$
**A4**: Hamiltonkreise zählen in $Q_3$: (Tipp: <=10)
Vollst. bipartiter Graph: auf beiden Seiten n Knoten, dann alle miteinander verbinden.
**A5**: 5 Tickets. gültig in beide Richtungen, aber nur 1mal
Tickets z.B.: {Basel,Bern},
{Basel,Locarno},{Bern,Locarno},{Bern,Zürich},{Locarno,Zürich}
Gibt es eine Rundreise bei der jedes Ticket verwendet wird? (= euler-Tour) -> Graph
Euler-Tour vs. Euler-Spaziergang: Bei zweitem köenn start und ende frei gewählt werden.

## SERIE 4

**A2**: „topologische Sortierung“: Nummerierung der Knoten, so dass alle Pfeile sortiert sind, also dass alle Pfeile von einer kleineren zu einer grösseren Zahl zeigen (wenn die Knoten nummeriert sind).

## SERIE 5

**A1**: a) Entfernen von Kanten
**A3**: einmal gibt es einen, einmal nicht

## SERIE 6

**Erweiterter Euklidischer Algorithmus**:

| m | n | q | s | t |
|---|---|---|---|---|
| 99 | 78 | 1 | | |
| 78 | 21 | 3 | | |
| 21 | 15 | 1 | | |
| 15 | 6 | 2 | | |
| 6 | 3 | 2 | | |
| 3 | 0 | | 1 | 0 |

| m | n | q | s | t |
|---|---|---|---|---|
| 99 | 78 | 1 | -11 | 14 |
| 78 | 21 | 3 | 3 | -11 |
| 21 | 15 | 1 | -2 | 3 |
| 15 | 6 | 2 | 1 | -2 |
| 6 | 3 | 2 | 0 | 1 |
| 3 | 0 | | 1 | 0 |

$$q_k = \lfloor m/n \rfloor, \qquad m_{k+1} = n_k, \qquad n_{k+1} = m_k - n_k \cdot q_k$$
$$t_k = s_{k+1} - q_k \cdot t_{k+1}, \qquad s_k = t_{k+1}$$
Dabei ist das unterste $m$ der ggT der ursprünglichen $m$ und $n$
Der erweiterte Euklid löst die Gleichung $m\tilde{x} + n\tilde{y} = ggT(\tilde{x},\tilde{y})$ mit $\tilde{x} = s_0,\ \tilde{y} = t_0$ als *eine* Lösung davon.
Verallgemeinerte Version:
$$mx + ny = r$$
Gleichung genau dann lösbar, wenn $ggT(m,n)$ teilt $r$.
Alle Lösungen: $(x,y) = \frac{(r\tilde{x}+kn, r\tilde{y}-km)}{ggT(m,n)}$
Falls Gleichung der Form $mx + ny + pz = r$ selbes Verfahren anwenden für $mx + ny = r - pz$.
Falls Gleichung der Form $mx = 1\ mod\ n$ dann selbes Verfahren für $mx + ny = 1$.
**Allgemeine Vereinfachungen**:
Wenn $e$ teilt $a,b,m$, dann $a = b\ mod\ m \Leftrightarrow \frac{a}{e} = \frac{b}{e}\ mod \frac{m}{e}$
Wenn $ggT(k,m) = 1$, dann $ak = bk\ mod\ m \Leftrightarrow a = b\ mod\ m$
**Satz von Euler bzw. Kleiner Satz von Fermat**:
$a^{\varphi(n)} = 1\ mod\ n$ mit $ggT(a,n) = 1$
mit $\varphi(n)$ die Euler'sche $\varphi$-Funktion.
$\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$ mit $ggT(m,n) = 1$.
$\varphi(p^k) = p^k - p^{k-1}$ mit $p$ prim.
Sonderfall (Kl. Satz von Fermat): $\varphi(p) = p-1$ wenn $p$ prim.
Daraus folgt: $a^b = a^{b\ mod\ \varphi(n)}\ mod\ n$ mit $ggT(a,n) = 1$

Ordnung ist immer Teiler von $\varphi(n)$ (nicht $\varphi(n)$ direkt)
→ via Primfaktorzerlegung, dann probieren