Diskrete Mathematik

Dipl.-Math. Christian Kratochwil

Duale Hochschule Baden-Württemberg

8. März 2024

Über den Dozenten (Christian Kratochwil)

Meine Heimatstadt:

Über den Dozenten (Christian Kratochwil)

Studium der Mathematik und Informatik:

Über den Dozenten (Christian Kratochwil)

Kontakt per Mail:

lehre@kratochwil-it.com

Mein Kanal auf YouTube:

www.youtube.com/user/ChristianKratochwil

Neuer Kanal ab September 2014 (speziell für das Studium):

www.youtube.com/user/MathematikFH

Leistungsfeststellung

Am Ende des Semesters kann ein verkürzte Hausarbeit geschrieben werden.
Die Modulnote ergibt sich zu 100% aus der Hausarbeit.

Es wird eine Übungsklausur geben.

- Gruppen zu zwei maximal drei Personen.
- Umfang 4 Seiten pro Person.
- Eine Themenliste gibt es in der Vorlesung.

Einleitung

Die Aufteilung der Vorlesung erfolgt in folgende Kapitel:

- Die Konstruktion der ganzen Zahlen
- Der Ring der ganzen Zahlen
- Primzahlen
- Etwas Gruppentheorie
- RSA-Verschlüsselung
- Polynomringe und endliche Körper
- Graphentheorie
- Kombinatorik

Inhaltsverzeichnis I

Die Konstruktion der ganzen Zahlen

- Grundlagen der Mengenlehre
- Relationen
- Die natürlichen Zahlen
- Die ganzen Zahlen

Der Ring der ganzen Zahlen

- Teibarkeit und Division mit Rest
- Restklassen
- Kongruenzen
- Anwendung: Hashfunktionen
  - Entwurf einer Hashfunktion
  - Kollisionen
  - Lineares Sondieren
  - Quadratisches Sondieren
- Der euklidische Algorithmus

Primzahlen

- Grundlagen

Inhaltsverzeichnis II

Der kleine Satz von Fermat. Euler'sche Phi-funktion

Etwas Gruppentheorie

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

Untergruppen. Zyklische Gruppen

Anwendung: Diffie-Hellman-Schlüsselvereinbarung

Anwendung:RSA-Verschlüsselung

Grundprinzip

Generierung des Schlüssels

Ver- und Entschlüsselung

Polynomringe und endliche Körper

Der Polynomring $\mathbb{K}[x]$

Der Restklassenring $\mathbb{K}[x]_{m(x)}$

Endliche Körper

Anwendung: Der Advanced Encryption Standard (AES)

Anwendung: Reed-Solomon-Code

Graphentheorie

Inhaltsverzeichnis III

Grundlegende Definitionen
Adjazenzmatrix
Traversieren von Graphen
Gerichtete und bewertete Graphen
Topologisches Sortierung
Kürzeste Wege und Dijkstra-Algorithmus

Kombinatorik
Endliche Mengen
Disjunkte Vereiningungen und Mengenprodukte
Permutationen
Inklusion und Exklusion bei Vereinigungen von Mengen
Anzahl von Teilmengen
Eigenschaften von Permutationen
Verschiedene Darstellungsarten von Permutationen
Komposition von Permutationen
Transpositionen
Zusammenhang zwischen Kombinatorik,Geometrie und Gruppentheorie
Matrixgruppen

Was ist diskrete Mathematik?

Die diskrete Mathematik beschäftigt sich mit den natürlichen und ganzen Zahlen. Es werden endliche oder abzählbar unendliche Mengen betrachtet. Wichtige Teilgebiete sind die Zahlentheorie und die Graphentheorie.

Wikipedia

Mengenlehre

Die Mengenlehre wurde von Georg Cantor (1845 - 1918) begründet.
Er gab für den Begriff der Menge folgende Definition.

Definition 1.1 (Menge)

Unter einer Menge versteht man die Zusammenfassung bestimmter, verschiedener Objekte des Denkens oder der Anschauung
zu einem Ganzen.

Beispiel

$A = \{1; 2; 3; 4\}$
$B = \{rot; blau; gelb\}$
$C = \{x \mid x \leq 5\}$
$D = \{x \mid x$ ist Teilnehmer*in der Vorlesung Diskrete Mathematik $\}$

Mengenlehre

Definition 1.2 (leere Menge)

Die Menge, die keine Elemente enthält nennt man leere Menge und schreibt $\{\}$ *oder* $\emptyset$
Sie ist definiert durch $\emptyset = \{x \mid x \neq x\}$

Definition 1.3 (Teilmenge)

Ist jedes Element der Menge A auch ein Element der Menge B, so sagt man. Die Menge A ist eine Teilmenge von B und schreibt: $A \subseteq B$. *Ist A keine Teilmenge von B, so schreibt man:* $A \not\subseteq B$.

Definition 1.4 (Differenzmenge)

Die Differenzmenge zweier Mengen A und B, ist die Menge derjeniger Elemente von A, die nicht zu B gehören. Man schreibt: $A \setminus B = \{x \mid x \in A \wedge x \notin B\}$

Mengenlehre

Beispiel

$A = \{1; 2; 3; 4; 5\} \quad B = \{1; 2\} \quad A \setminus B = \{3; 4; 5\}$

Definition 1.5 (Vereinigungsmenge)

Die Vereinigungsmenge zweier Mengen A und B besteht aus allen Elementen, die zu A oder B gehören. Man schreibt:
$A \cup B = \{x \mid x \in A \vee x \in B\}$

Beispiel

$A = \{1; 2; 3\} \quad B = \{1; 2; 4; 5\} \quad A \cup B = \{1; 2; 3; 4; 5\}$

Mengenlehre

Definition 1.6 (Schnittmenge)

Die Schnittmenge zweier Mengen A und B
besteht aus allen Elementen, die gleichzeitig zu A und B gehören.
Man schreibt: $A \cap B = \{x \mid x \in A \wedge x \in B\}$

Beispiel

$A = \{1; 2; 3\} \quad B = \{2; 4; 6\} \quad A \cap B = \{2\}$

Mengenlehre

In der Mathematik werden bestimmte Mengen sehr oft gebraucht, die wir nun besprechen wollen. Es sind die Mengen:
$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$

1.Die Menge der natürlichen Zahlen: $\mathbb{N}$

$$\mathbb{N} = \{0; 1; 2; 3; ....\}$$

$$\mathbb{N}^* = \{1; 2; 3; ....\}$$

2.Die Menge der ganzen Zahlen: $\mathbb{Z}$

$$\mathbb{Z} = \{... - 3; -2; -1; 0; 1; 2; 3; ....\}$$

$$\mathbb{Z}_- = \{x \in \mathbb{Z} \mid x \leq 0\}$$

$$\mathbb{Z}_+ = \{x \in \mathbb{Z} \mid x \geq 0\}$$

$$\mathbb{Z}_-^* = \{x \in \mathbb{Z} \mid x < 0\}$$

$$\mathbb{Z}_+^* = \{x \in \mathbb{Z} \mid x > 0\}$$

Mengenlehre

3.Die Menge der rationalen Zahlen: $\mathbb{Q}$

$\mathbb{Q} = \{x \mid x = \frac{p}{q}; p \in \mathbb{Z}; q \in \mathbb{N}^*\}$

$\mathbb{Q}_- = \{x \in \mathbb{Q} \mid x \leq 0\}$

$\mathbb{Q}_+ = \{x \in \mathbb{Q} \mid x \geq 0\}$

$\mathbb{Q}_-^* = \{x \in \mathbb{Q} \mid x < 0\}$

$\mathbb{Q}_+^* = \{x \in \mathbb{Q} \mid x > 0\}$

4.Die Menge der reellen Zahlen: $\mathbb{R}$

$\mathbb{R} = \mathbb{Q} \cup \{x | x$ ist irrational $\}$ Irrationale Zahlen sind z.B. $\sqrt{2}$ oder π.

5.Die Menge der komplexen Zahlen: $\mathbb{C}$

Es gilt: $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$

Relationen

Definition 1.7 (kartesisches Produkt)

Unter dem Kartesischen Produkt zweier Mengen A und B versteht man die Menge aller Zahlenpaare (x, y) *mit* $x \in A$ *und* $y \in B$ *und schreibt:*

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

Beispiel

$A = \{1; 2\}, B = \{3; 4\}, AxB = \{(1, 3); (1, 4); (2, 3); (2, 4)\}$

Definition 1.8 (Relation)

Unter einer Relation R verstehen wir eine Teilmenge von A x B. Anstatt $(x, y) \in R$ *schreibt man auch xRy.*

Relationen

Beispiel

- Ordnungsrelation $\leq$
- Gleichheitsrelation $=$
- $A = \{\text{Wien,Berlin,Paris,Stuttgart}\}$ und $B = \{\text{D,A,F}\}$ und $a\ R\ b =$ Ist Hauptstadt von. Dann ist z.B. Wien R A.

Bei einer Relation werden jedem Element aus A nach einer Vorschrift Elemente aus B zugeordnet.

Übung 1.1

Seien $A = \{2, 3, 4, 5, 6\}$ und $B = \{3, 4, 6\}$ und $R = a$ ist Teiler von b aber verschieden von b.
Geben Sie alle Paare an, die zur Relation R gehören.

Relationen

Definition 1.9 (Eigenschaften von Relationen)

Sei R eine Relation in $A \times A$ dann definieren wir die folgenden Eigenschaften:

(RLR)	$\forall a \in A:$	$a \; R \; a$	*Reflexivität*
(RLS)	$\forall a, b \in A$	$a \, R \, b \Rightarrow b \, R \, a$	*Symmetrie*
(RLA)	$\forall a, b \in A:$	$a \, R \, b \wedge b \, R \, a \Rightarrow a = b$	*Antisymmetrie*
(RLT)	$\forall a, b, c \in A:$	$a \, R \, b \wedge b \, R \, c \Rightarrow a \, R \, c$	*Transitivität*

Relationen

Definition 1.10 (Äquivalenzrelation)

Eine reflexive, symmetrische und transitive Relation wird Äquivalenzrelation genannt.
Anstelle von $a\,R\,b$ schreiben wir $a \sim b$ und sagen: a ist äquivalent zu b.

Beispiel

- Gleichheitsrelation $=$
- Sei $a \sim b \Leftrightarrow b - a$ ist durch 5 teilbar.

Übung 1.2

Beweisen Sie, dass die Relation $a \sim b \Leftrightarrow b - a$ ist durch 5 teilbar eine Äquivalenzrelation ist.

Die natürlichen Zahlen

Giuseppe Peano (1858-1932): Axiomatische Beschreibung der natürlichen Zahlen.

Peano-Axiome

1. $0 \in \mathbb{N}$
2. Jede natürliche Zahl n hat einen Nachfolger n'
3. $\forall n \in \mathbb{N} : n' \neq 0$
4. $\forall n, m \in \mathbb{N} : n' = m' \Rightarrow n = m$
5. $(0 \in M \wedge (n \in M \Rightarrow n + 1 \in M)) \Rightarrow M = \mathbb{N}$ Induktionsaxiom

Verknüpfung

Definition 1.11

Eine (innere) Verknüpfung $\circ$ auf einer Menge A ist eine Zuordnung, die jedem Paar aus $A \times A$ wieder eindeutig ein Element von A zuordnet.

Beispiel

Auf der Menge $\mathbb{N}$ ist die Addition eine Verknüpfung.

Rechenregeln auf den natürlichen Zahlen

Definition 1.12

Für die Menge der natürlichen Zahlen führen wir die innere Verknüpfung $+$ ein. Für x, y heißen $x + y$ Summe
Es gelten die folgenden Axiome:

(A1)	$\forall x, y, z \in \mathbb{N} : x + (y + z) = (x + y) + z$	*Assoziativgesetz*
(A2)	$\forall x \in \mathbb{N} : x + 0 = 0 + x = x$	*Neutrales Element*
(A3)	$\forall x, y \in \mathbb{N} : x + y = y + x$	*Kommutativgesetz*

Damit haben wir eine erste algebraische Struktur einen sogenannten (kommutativen) Monoid.

Definition 1.13

Eine Menge A mit einer Verknüpfung $+$ heißt Halbgruppe, falls die Verknüpfung das Rechengesetz (A1) erfüllt.
Ist (A1) und (A2) erfüllt, so nennen wir A einen Monoid. Ist zusätzlich (A3) erfüllt, so sprechen wir von einem kommutativen Monoid.

Die ganzen Zahlen

Definition 1.14

Die Menge $\mathbb{N} \times \mathbb{N}$ *kürzen wir nun mit* $\mathbb{N}^2$ *ab.*
Wir definieren eine Relation in $\mathbb{N}^2 \times \mathbb{N}^2$ *durch*

$$(a, b) \sim (c, d) \Leftrightarrow a + d = b + c$$

Übung 1.3

Beweisen Sie, dass die oben definierte Relation eine Äquivalenzrelation ist.

Die ganzen Zahlen

Definition 1.15

Gegeben sei eine eine Äquivalenzrelation $\sim$ in A. Dann definieren wir die Menge

$$\bar{a} = \{b \in A \mid b \sim a\}$$

und nennen diese Menge die Äquivalenzklasse von a und a einen Repräsentanten dieser Äquivalenzklasse.

Übung 1.4

Geben Sie alle Äquivalenzklassen der Relation $a \sim b \Leftrightarrow b - a$ ist durch 5 teilbar an.

Die ganzen Zahlen

Definition 1.16

Gegeben sei eine eine Äquivalenzrelation $\sim$ in A. Dann definieren wir die Menge

$$A / \sim = \{\bar{a} \mid \bar{a} \text{ ist Äquivalenzklasse von } A\}$$

und nennen diese die Faktormenge oder Quotientenmenge der Äquivalenzklasse.

Satz 1.17

$A / \sim$ ist eine Partition von A, das heißt A ist die disjunkte Vereinigung der Äquivalenzklassen bezüglich der Äquivalenzrelation $\sim$

Die ganzen Zahlen

Nun weiter mit der Konstruktion der ganzen Zahlen. Wir betrachten nun die Äquivalenzklassen, die wir auf $\mathbb{N}^2$ bilden können und bilden die ganzen Zahlen $\mathbb{Z}$ über die Faktormenge dieser Relation.

Definition 1.18 (ganze Zahlen)

Für jedes Paar $(a, b) \in \mathbb{N}^2$ *definieren wir*

$$\overline{(a,b)} = \{(x,y) \in \mathbb{N}^2 : (x,y) \sim (a,b)\}$$

und weiterhin definieren wir

$$\mathbb{Z} = \mathbb{N}^2 \,/\sim\; = \{\overline{(a,b)} : a \in \mathbb{N} \wedge b \in \mathbb{N}\}$$

Die ganzen Zahlen

Nun benötigen wir eine Addition für die ganzen Zahlen, die wir wie folgt definieren.

Definition 1.19 (Addition in den ganzen Zahlen)

$$\overline{(a,b)} + \overline{(c,d)} = \overline{(a+c, b+d)}$$

Es existiert ein neutrales Element nämlich $\overline{(0,0)}$, denn es gilt:

$$\overline{(a,b)} + \overline{(0,0)} = \overline{(a+0, b+0)} = \overline{(a,b)}$$

Damit ist $(\mathbb{Z}, +)$ ein kommutativer Monoid, wie es schon die natürlichen Zahlen sind.

Die ganzen Zahlen

Wir haben hier aber auch ein inverses Element, denn

$$\overline{(a,b)} + \overline{(b,a)} = \overline{(a+b, a+b)} = \overline{(0,0)}$$

Es gelten die folgenden Rechenregeln:

(G1)	$\forall x, y, z \in \mathbb{Z} : x + (y + z) = (x + y) + z$	Assoziativgesetz
(G2)	$\exists 0 \in \mathbb{Z} : \forall x \in \mathbb{Z} : x + 0 = 0 + x = x$	Neutrales Element
(G3)	$\forall x \in \mathbb{Z} : \exists -x \in \mathbb{Z} : x + (-x) = 0$	Inverses Element
(G4)	$\forall x, y \in \mathbb{Z} : x + y = y + x$	Kommutativgesetz

Die ganzen Zahlen

Definition 1.20

Eine Menge A mit einer Verknüpfung $+$, die die Rechenregeln (G1)-(G3) erfüllt heißt Gruppe. Gilt zusätzlich noch (G4), so sprechen wir von einer kommutativen Gruppe oder Abelschen Gruppe.

Benannt nach dem norwegischen Mathematiker Niels Henrik Abel (1802-1829).

Satz 1.21

$(\mathbb{Z}, +)$ *ist eine Kommutative Gruppe.*

Die ganzen Zahlen

Definition 1.22 (Einbettung der natürlichen Zahlen)

Wir definieren die Abbildung

$$\alpha : \mathbb{N} \to \mathbb{Z}, \qquad n \mapsto \overline{(n, 0)}$$

Die obige Abbildung ist verträglich mit der Addition. Es gilt:

$$\alpha(n + m) = \alpha(n) + \alpha(m)$$

Definition 1.23

Seien A,B Gruppen, dann heißt eine Abbildung α *Monomorphismus, falls*

$$\alpha(a + a') = \alpha(a) + \alpha(a')$$

gilt.

Die ganzen Zahlen

Es gilt: $\mathbb{Z} = \mathbb{N} \cup \{\overline{(0,1)}, \overline{(0,2)}, \overline{(0,3)}, \dots\}$

Mit der Abkürzung $-n = \overline{(0,n)}$ erhalten wir

$$\mathbb{Z} = \mathbb{N} \cup \{-1, -2, -3, \dots\}$$

Außerdem definieren wir $m - n = m + (n)$

Die ganzen Zahlen

Wir benötigen nun noch eine Multiplikation.

Definition 1.24 (Multiplikation ganzer Zahlen)

$$\overline{(a,b)} \cdot \overline{(c,d)} = \overline{(ac+bd, ad+bc)}$$

Beispiel

1. $3 \cdot 4 = \overline{(3,0)} \cdot \overline{(4,0)} = \overline{(3 \cdot 4 + 0 \cdot 0, 3 \cdot 0 + 0 \cdot 4)} = \overline{(12,0)} = 12.$
2. $\overline{(-3)} \cdot \overline{(-4)} = \overline{(0,3)} \cdot \overline{(0,4)} = \overline{(0 \cdot 0 + 3 \cdot 4, 0 \cdot 4 + 3 \cdot 0)} = \overline{(12,0)} = 12.$

Hier sehen wir die Regel Minus x Minus = Plus.

Die ganzen Zahlen

Satz 1.25

$(\mathbb{Z}, \cdot)$ *ist ein kommutativer Monoid.*

Definition 1.26 (Distributivgesetze)

Die Distributivgesetze auf einer Menge A sind definiert durch:

(D1) $\forall x, y, z \in A : (x + y)z = xz + yz$ *Distributivgesetz*

(D2) $\forall x, y, z \in A : z(x + y) = zx + zy$ *Distributivgesetz*

Die ganzen Zahlen

Definition 1.27 (Ring)

Gegeben sei eine Menge R mit zwei Verknüpfungen $+$ und $\cdot$. Ist $(R, +)$ eine kommutative Gruppe und $(R, \cdot)$ eine Halbgruppe und gelten die Distributivgesetze, dann nennt man $(R, +, \cdot)$ einen Ring.

Das Neutrale Element in $(R, +)$ heißt Nullelement.

Ist $(R, \cdot)$ sogar ein Monoid, d.h. es gibt ein neutrales Element bezüglich der Multiplikation (Einselement genannt), so sprechen wir von einem Ring mit Einselement oder von einem unitären Ring. Gilt für $(R, \cdot)$ das Kommutativgesetz so sprechen wir von einem kommutativen Ring.

Satz 1.28

$(\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring mit Einselement.

Der Ring der ganzen Zahlen

Definition 2.1

Seien $a, b \in \mathbb{Z}$ dann heißt b durch a teilbar wenn es eine ganze Zahl q gibt, so dass $b = q \cdot a$ gilt. Wir führen dafür das Symbol $a \mid b$ („a teilt b“) ein, also

$$a \mid b \Leftrightarrow \exists\, q \in \mathbb{Z} : b = q \cdot a$$

Beispiele

- $5 \mid 25$
- $13 \mid 65$

Der Ring der ganzen Zahlen

Satz 2.2 (Rechenregeln)

Seien $a, b, c, d \in \mathbb{Z}$ *dann gelten:*

- $a \mid b \Rightarrow -a \mid b$ *und* $a \mid -b$
- $a \mid b \ \wedge \ b \mid c \Rightarrow a \mid c$
- $a \mid b \ \wedge \ r \in \mathbb{Z}^* \Rightarrow ar \mid br$
- $a \mid b \ \wedge \ c \mid d \Rightarrow ac \mid bd$
- $a \mid b \ \wedge \ a \mid c \ \wedge \ r, s \in \mathbb{Z} \Rightarrow a \mid rb + sc$
- $a \mid b \ \wedge \ b \mid a \Rightarrow a = b \ \vee \ a = -b$

Der Ring der ganzen Zahlen

Satz 2.3 (Division mit Rest)

Seien $a, b \in \mathbb{Z}$ *und* $b > 0$, *so gibt es eindeutige ganze Zahlen* $q, r \in \mathbb{Z}$ *mit* $0 \leq r < b$, *so dass die folgende Gleichung erfüllt ist:*

$$a = q \cdot b + r$$

Wir betrachten nun eine besondere Teilmenge von $\mathbb{Z}$

Definition 2.4

$$m\mathbb{Z} = \{z \in \mathbb{Z} : \exists\, x \in \mathbb{Z} :\ z = x \cdot m\}$$

Der Ring der ganzen Zahlen

Beispiele

- $5\mathbb{Z} = \{\ldots, -10, -5, 0, 5, 10, 15, \ldots\}$
- $2\mathbb{Z} = \{\ldots, -6, -4, -2, 0, 2, 4, 6, \ldots\}$

Addiert oder multipliziert man zwei Zahlen aus $m\mathbb{Z}$ miteinander, so bleibt man in der Menge. Es ist leicht nachzurechnen, das diese Mengen wieder Ringe bilden. Sie sind also Unterringe von $\mathbb{Z}$

Definition 2.5

Sei R ein Ring, dann heißt eine Teilmenge $A \subseteq R$ Unterring von R, wenn A selbst ein Ring ist, also mit $x, y \in A$ sind $x + y \in A$ und $x \cdot y \in A$

Der Ring der ganzen Zahlen

Die Unterringe $m\mathbb{Z}$ haben aber eine weitere interessante Eigenschaft. Multipliziert man ein Element von $m\mathbb{Z}$ mit einer beliebigen Zahl $z \in \mathbb{Z}$, so erhält man wieder ein Element aus $m\mathbb{Z}$

Definition 2.6

Sei R ein Ring, dann heißt eine Teilmenge $I \subseteq R$ Ideal, wenn I ein Unterring von R ist und

$$\forall\, r \in R, a \in I : r \cdot a \in I$$

Nun definieren wir Äquivalenzklassen, mit dem Ziel den Ring der ganzen Zahlen zu verkleinern:

Definition 2.7

$$a \sim b \Leftrightarrow b - a \in m\mathbb{Z}$$

Der Ring der ganzen Zahlen

Wie sehen die Äquivalenzklassen bezüglich dieser Menge aus? Es sind alle Reste, die bei der Division durch m anfallen. also $\bar{0}, \bar{1}, \ldots, \overline{m-1}$

Definition 2.8

Die Faktormenge bezüglich der obigen Äquivalenzrelation wird abgekürzt mit

$$\mathbb{Z}_m = \mathbb{Z} \,/\, m\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, \overline{m-1}\}$$

Die Zahl m wird in diesem Zusammenhang Modul genannt und die Äquivalenzklassen sind die Divisionsreste modulo m und diese Äquivalenzklassen werden auch Restklassen genannt.

Der Ring der ganzen Zahlen

Auf der Menge $\mathbb{Z}_m$ ist eine Rechenstruktur durch die folgenden Definitionen gegeben:

Definition 2.9 (Rechenoperationen)

- $\bar{a} + \bar{b} = \overline{a + b}$
- $\bar{a} \cdot \bar{b} = \overline{a \cdot b}$

Mit diesen Rechenoperationen wird die Menge $\mathbb{Z}_m$ zu einem kommutativen Ring mit Einselement $\bar{1}$

Der Ring der ganzen Zahlen

Wollen wir uns $\mathbb{Z}_6$ näher ansehen. $\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$ Wir erstellen nun eine Additionstabelle und eine Multiplikationstabelle für $\mathbb{Z}_6$ und kürzen dabei $\bar{a}$ mit a ab.

Additionstabelle:

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Der Ring der ganzen Zahlen

Multiplikationstabelle:

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Verkürzte Form:

1	2	3	4	5
2	4	0	2	4
3	0	3	0	3
4	2	0	4	2
5	4	3	2	1

Der Ring der ganzen Zahlen

Übung 2.1

Stellen Sie sie verkürzte Multiplikationstafel für $\mathbb{Z}_5$ auf.

Der Ring der ganzen Zahlen

Definition 2.10 (Kongruenz)

Wir sagen a ist kongruent zu b modulo m, wenn $m|(b-a)$ gilt und schreiben
$a \equiv b \mod m$. *Wir nennen m den Modul dieser Kongruenz.*
Zwei Zahlen a, b sind genau dann kongruent modulo m, wenn sie bei der Division durch m den gleichen Rest haben.

Beispiele

Das Rechnen mit Uhrzeiten bedeutet Rechnen mit Restklassen modulo 24 oder modulo 12. Wir rechnen mal mit Modulo 12.
Wieviel Uhr ist es 7 Stunden nach 9 Uhr? $9 + 7 \mod 12 = 16 \mod 12 = 4$

Der Ring der ganzen Zahlen

Satz 2.11

Es seien $a, b, c, d, m \in \mathbb{Z}$ *und* $m > 0$ *mit* $a \equiv b \mod m$ *und* $c \equiv d \mod m$ *Dann ist*

- $a + c \equiv b + d \mod m$
- $a - c \equiv b - d \mod m$
- $a \cdot c \equiv b \cdot d \mod m$

Der Ring der ganzen Zahlen

Satz 2.12

Es seien $a, b, m \in \mathbb{Z}$ *und* $m > 0$ *und* $k \geq 1$*. Dann gilt*

$$a \equiv b \mod m \Rightarrow a^k \equiv b^k \mod m$$

Beispiel

Gesucht ist $7^{52} \mod 53$

Lösung:

$7^{52} \equiv 7^{32} \cdot 7^{16} \cdot 7^4 \mod 53 \equiv (7^{16})^2 \cdot (7^4)^2 \cdot (7^2)^2 \mod 53$

$7^2 = 49 \equiv -4 \mod 53$

Der Ring der ganzen Zahlen

Übung 2.2

Berechnen Sie die folgenden Divisionsreste:

1. $5^{12} \mod 13$
2. $3^{132} \mod 11$

Hash-Funktion

Definition 2.13 (Hash-Funktion)

Eine Hash-Funktion ordnet einer Zeichenkette bzw. Bitfolge (eher groß) eine (möglichst eindeutige) kleinere Ausgabe mit fester Länge, den sogenannten Hashwert zu.
to hash (engl.) = zerhacken.

Anwendungen

- Prüfsummen
- Digitale Signaturen
- Verifikation von Downloads
- WLAN-Router
- Passwortverschlüsselung
- Datenzugriff (dictionary operations)
- Kryptologie

Hash-Funktion

Dictionary Operationen

- Suchen nach einem Datensatz mit einem gegebenen Schlüssel x search(x)
- Löschen eines Datensatzes mit einem gegebenen Schlüssel x delete(x)
- Einfügen eines Datensatzes d mit Schlüssel x insert(d,x)

Hash-Funktion

Dictionary Operationen

- Die Menge U (= Universum) potentieller Schlüssel ist normalerweiser sehr groß.
- Die aktuelle Schlüsselmenge K (= Teilmenge von U) ist normalerweise nicht bekannt.
- Grundidee: durch Berechnung festzustellen, an welcher Adresse der Datensatz gespeichert ist.
- Dazu dient eine Hashtabelle bestehend aus einem Array $\{0, 1, \ldots, m-1\}$
- Die Hashfunktion h liefert für jeden Schlüssel $x \in U$ eine Adresse in der Hashtabelle.

Entwurf einer Hash-Funktion

Definition 2.14 (Kongruenzmethode)

Sei K die Menge der Schlüssel und $|K|$ die Anzahl der Elemente von K und $m > |K|$ eine Primzahl, dann definieren wir die Kongruenzmethode als

$$h(k) = f(k) \mod m$$

Hierbei ist f(k) eine injektive Funktion auf K. sollten die Schlüssel Zeichenketten sein, so muss eine Umwandlung in eine numerischen Wert erfolgen.

Entwurf einer Hash-Funktion

Definition 2.15 (Belegungsfaktor)

Sei K die Menge der Schlüssel und die Hashtabelle $T = \{0, \ldots, m-1\}$ gegeben. Dann heißt

$$\beta = |K|/m$$

Belegungsfaktor der Hashtabelle.

Entwurf einer Hash-Funktion

Beispiel

Sei $m = 11$ und $K = \{49, 22, 6, 52, 76, 34, 13, 29\}$ Es ergeben sich die folgenden Hashwerte:

k	$h(k)$
49	5
22	0
6	6
52	8
76	10
34	1
13	2
29	7

Entwurf einer Hash-Funktion

Beispiel

Sei K = {Jan, Feb, Mar, ..., Dez} und $m = 17 > |K|$ Sei b(k,n) die Funktion, die von einem Key k den n-ten Buchstaben liefert. Es ist also zum Beispiel b(Jan,1)=J oder b(Feb,3)=b. Nun definieren wir die Funktion α(Buchstabe) = Position des Buchstaben im Alphabet. Hierbei ist Groß- und Kleinschreibung nicht relevant.

Nun sei $f(k) = 11 \cdot \alpha(b(k,1)) + 5 \cdot \alpha(b(k,2)) + 3 \cdot \alpha(b(k,3))$

und $h(k) = f(k) \mod 17$

Entwurf einer Hash-Funktion

Beispiel

Die Hashfunktion liefert folgende Werte:

k	h(k)
Jan	4
Feb	12
Mar	15
Apr	9
Mai	5
Jun	2
Jul	13
Aug	1
Sep	10
Okt	8
Nov	6
Dez	11

Entwurf einer Hash-Funktion

Die Hashfunktion wird nicht immer injektiv sein. Es kann also vorkommen, dass mehrere Schlüssel auf den gleichen Hashwert abgebildet werden, was Kollision genannt wird.

Wie wahrscheinlich sind Kollisionen?

Geburtstagsparadoxon

Nehmen wir an, dass sich 23 Personen in einem Raum befinden. Wie wahrscheinlich ist es, dass zwei Personen am gleichen Tag und Monat Geburtstag haben? Das Jahr darf hierbei unterschiedlich sein.

Wir gehen von 365 Tagen aus und berücksichtigen nicht, dass es ein Schaltjahr sein kann. Die Lösung gewinnt man durch das sogenannte Gegenereignis:
$\bar{A}$ = Alle 23 Personen haben an verschiedenen Tagen Geburtstag.
Für die erste Person gibt es nun 365 Möglichkeiten und alle sind möglich, aber für die nächste Person gibt es nur noch 364 Möglichkeiten usw. also ergibt sich

$$P(\bar{A}) = \frac{365}{365} \cdot \frac{364}{365} \cdot \frac{363}{365} \cdot \ldots \cdot \frac{343}{365} = 0,4927$$

Damit ist die Wahrscheinlichkeit bei 23 Personen 0,5073 also größer als 50%, dass zwei Personen am gleichen Tag Geburtstag haben.

Kollisionen

Was lernen wir aus dem Geburtstagsparadoxon?

Ist die Größe der Hashtabelle $m = 365$, so ist die Wahrscheinlichkeit, dass wir keine Kollision bekommen etwa 49%.

Da wir mit Kollisionen leben müssen, brauchen wir Strategien zur Kollisionsbehandlung.

Folgende Strategien werden unterschieden:

- verkettete Liste (chaining). Die Hashtabelle enthält Zeiger auf eine Liste
- offene Adressierung (open hashing). Suche nach einem freien Platz in der Hashtabelle.

Kollisionen

Beispiel mit Kollision

Sei K $= \{$Jan, Feb, Mar, $\ldots$, Dez$\}$ und $m = 17 > |K|$ Nun seien:

$f_1(k) = \alpha(b(k,1)) + \alpha(b(k,2))$

$f_2(k) = 13 \cdot \alpha(b(k,1)) + 5 \cdot \alpha(b(k,2))$

und $h_i(k) = f_i(k) \mod 17$ für $i = 1, 2$

Kollisionen

Beispiel mit Kollision

Die Hashfunktion liefert folgende Werte:

k	$h_1(k)$	$h_2(k)$
Jan	6	1
Feb	11	1
Mar	14	4
Apr	0	8
Mai	14	4
Jun	14	14
Jul	14	14
Aug	5	16
Sep	7	0
Okt	9	12
Nov	12	2
Dez	9	9
Kollisionen	3	3

Kollisionen

Übung 2.3

In eine Hashtabelle der Größe 13 (Kongruenzmethode und chaining) werden folgende Schlüssel eingetragen:

34, 23, 67, 41, 45, 112, 4, 17, 9, 54, 80

Wie lautet die Belegung der Hashtabelle?

Index	*Eintrag / Einträge*
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	

Kollisionen

Einfaches Open Hashing: Lineares Sondieren

Ist der Platz k bereits belegt, so wird versucht den Schlüssel auf der Position $(k+1) \mod m$, $(k+2) \mod m$ usw. zu speichern.

Kollisionen

Beispiel: Lineares Sondieren

Eingetragen wurden bereits 34,23 und 67

0	1	2	3	4	5	6	7	8	9	10	11	12
		67						34		23		

Nun soll 41 eingetragen werden und es ergibt sich $41 \equiv 2 \mod 13$ also ist eine Kollision vorhanden.
Es wird deshalb der nächste frei Speicherplatz gewählt, nämlich die 3.

0	1	2	3	4	5	6	7	8	9	10	11	12
		67	41					34		23		

Kollisionen

Beispiel: Lineares Sondieren

Eingetragen wurden bereits 34,23,67 und 41

0	1	2	3	4	5	6	7	8	9	10	11	12
		67	41					34		23		

Nun soll 2 eingetragen werden und es ergibt sich $2 \equiv 2 \mod 13$
also ist eine Kollision vorhanden.
Es wird deshalb der nächste frei Speicherplatz gewählt, nämlich die 4.

0	1	2	3	4	5	6	7	8	9	10	11	12
		67	41	2				34		23		

Kollisionen

Übung 2.4

In eine Hashtabelle der Größe 13 (Kongruenzmethode mit linearem Sondieren) werden folgende Schlüssel eingetragen:

34, 23, 67, 41, 45, 112, 4, 17, 9, 54, 80

Wie lautet die Belegung der Hashtabelle?

Kollisionen

Übung 2.5

Die Monatsnamen sollen in eine Hashtabelle der Größe 17 eingetragen werden. Dazu werden Umlaute als zwei Zeichen dargestellt, also a = ae. Wir verwenden dann die Funktion $f(k) = \alpha(b(k,1)) + \alpha(b(k,2)) + \alpha(b(k,3))$ *und* $h(k) = f(k) \mod 17$

Wie lautet die Belegung der Hashtabelle, wenn die Kollisionen mit linearem Sondieren aufgelöst werden?

Kollisionen

Nachteile vom linearen Sondieren:

- Es entstehen immer längere zusammenhängende, belegte Abschnitte in der Hashtabelle (Clusterbildung)
- erhöhte Suchzeiten
- Löschen eines Elements schwierig, da Suchketten unterbrochen werden.

Kollisionen

Quadratisches Sondieren

Ist der Platz $k = h(s)$ belegt, so versucht das quadratische Sondieren der Reihe nach mit der Folge
$(k + 1) \mod m$, $(k + 4) \mod m$, $(k + 9) \mod m$ usw. einen freien Platz zu finden.

Quadratisches Sondieren vermindert Clusterbildung.

Kollisionen

Übung 2.6

Die Monatsnamen sollen in eine Hashtabelle der Größe 17 eingetragen werden. Dazu werden Umlaute als zwei Zeichen dargestellt, also a = ae. Wir verwenden dann die Funktion $f(k) = \alpha(b(k,1)) + \alpha(b(k,2)) + \alpha(b(k,3))$ *und* $h(k) = f(k) \mod 17$

Wie lautet die Belegung der Hashtabelle, wenn die Kollisionen mit quadratischem Sondieren aufgelöst werden?

Größter gemeinsamer Teiler

Moderner Euklidischer Algorithmus

Wie lautet ggT$(84, 231)$?

Lösung: Euklidischer Algorithmus

a	b	a/b	Rest
84	231	0	84
231	84	2	63
84	63	1	21
63	21	3	0
21	0		

Der moderne euklidische Algorithmus

Rekursive Variante (Pseudo-Code)

EUKLID(a,b)

1. **if** (b == 0)
2. **return** a
3. **else**
4. **return** EUKLID(b, Divisionsrest(a durch b))

Der moderne euklidische Algorithmus

Iterative Variante (Pseudo-Code)

EUKLID(a,b)

1. **while** (b ! = 0)
2. {
3. h = Divisionsrest(a durch b)
4. a = b
5. b = h
6. }
7. **return** a

Diophantische Gleichungen

Der euklidische Algorithmus ist mit sehr interessanten Gleichungen verbunden, den sogenannten linearen diophantischen Gleichungen.

Definition 2.16

Eine Gleichung der Form

$$ax + by = c \text{ mit } a, b, c \in \mathbb{Z}$$

für die ganzzahlige Lösungen x,y gesucht werden, heißt lineare diophantische Gleichung

Benannt sind diese Gleichungen nach **Diophantos von Alexandria**. Die genauen Angaben wann er gelebt hat, sind nicht bekannt, aber es wird vermutet, dass er etwa um 250 n.Chr. gelebt hat.

Diophantische Gleichungen

Satz 2.17

Die lineare diophantische Gleichung $ax + by = c$ *ist genau dann lösbar, wenn* $ggT(a, b)|c$ *gilt. Eine Lösung kann dadurch gefunden werden, indem man die Gleichung* $ax + by = ggT(a, b)$ *löst und die Lösungen mit* $c/ggT(a, b)$ *multipliziert. Dazu bedienen wir uns dem erweiterten euklidischen Algorithmus.*

Diophantische Gleichungen

Beispiel

Wir berechnen $ggT(294, 201)$

a	b	a/b	Rest
294	201	1	93
201	93	2	15
93	15	6	3
15	3	5	0
3	0		

Also ist $ggt(294, 201) = 3$. Rückwärtsrechnen ergibt folgendes:

$$\begin{aligned} 3 &= 93 - 6 \cdot 15 & &= 93 - 6 \cdot (201 - 2 \cdot 93) \\ &= 13 \cdot 93 - 201 & &= 13 \cdot (294 - 201) - 6 \cdot 201 \\ &= 13 \cdot 294 - 19 \cdot 201 = 3 \end{aligned}$$

Damit hat die diophantische Gleichung $294x + 201y = 3$ die Lösung $x = 13, y = -19$

Diophantische Gleichungen

Mit einer Tabelle kann dies leicht gelöst werden.

$x_i = y_{i+1}$ und $y_i = x_{i+1} - q_i \cdot y_{i+1}$

a	b	q	r	x	y
294	201	1	93		
201	93	2	15		
93	15	6	3		
15	3	5	0	0	1

a	b	q	r	x	y
294	201	1	93		
201	93	2	15		
93	15	6	3	1	-6
15	3	5	0	0	1

Diophantische Gleichungen

a	b	q	r	x	y
294	201	1	93		
201	93	2	15	-6	13
93	15	6	3	1	-6
15	3	5	0	0	1

a	b	q	r	x	y
294	201	1	93	13	-19
201	93	2	15	-6	13
93	15	6	3	1	-6
15	3	5	0	0	1

Diophantische Gleichungen

Übung 2.7

Finden Sie eine Lösung der diophantischen Gleichung
$73685x + 25513y = 10$

Diophantische Gleichungen

Übung 2.8

Finden Sie Lösung der diophantischen Gleichungen, falls möglich

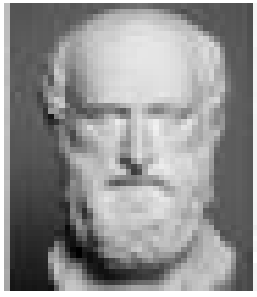
1. $12x + 56y = 32$
2. $12x + 8y = 16$
3. $-28x + 42y = -56$

Primzahlen

Definition 3.1

Eine natürliche Zahl $p > 1$ heißt Primzahl, wenn p nur die positiven Teiler 1 und p besitzt.

Der Sieb des Eratosthenes



Eratosthenes (276 v.Chr. - 194 v.Chr.)

Sieb des Eratosthenes

	2	3	4	5	6	7	8	9	10	11	12	13	14	15
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40	41	42	43	44	45
46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70	71	72	73	74	75
76	77	78	79	80	81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99						

Der Sieb des Eratosthenes

Sieb des Eratosthenes

	2	3	4	5	6	7	8	9	10	11	12	13	14	15
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40	41	42	43	44	45
46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70	71	72	73	74	75
76	77	78	79	80	81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99						

Der Sieb des Eratosthenes

Sieb des Eratosthenes

	2	3	4	5	6	7	8	9	10	11	12	13	14	15
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40	41	42	43	44	45
46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70	71	72	73	74	75
76	77	78	79	80	81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99						

Der Sieb des Eratosthenes

Sieb des Eratosthenes

	2	3	4	5	6	7	8	9	10	11	12	13	14	15
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40	41	42	43	44	45
46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70	71	72	73	74	75
76	77	78	79	80	81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99						

Der Sieb des Eratosthenes

Sieb des Eratosthenes

	2	3	4	5	6	7	8	9	10	11	12	13	14	15
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40	41	42	43	44	45
46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70	71	72	73	74	75
76	77	78	79	80	81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99						

Der Sieb des Eratosthenes

Sieb des Eratosthenes

	2	3	4	5	6	7	8	9	10	11	12	13	14	15
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40	41	42	43	44	45
46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70	71	72	73	74	75
76	77	78	79	80	81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99						

Der Sieb des Eratosthenes

Sieb des Eratosthenes

	2	3	4	5	6	7	8	9	10	11	12	13	14	15
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40	41	42	43	44	45
46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70	71	72	73	74	75
76	77	78	79	80	81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99						

Primzahlen

Satz 3.2

Jede Zahl $n \in \mathbb{N}$ mit $n > 1$ besitzt einen kleinsten Teiler $k > 1$ und dieser ist eine Primzahl.

Beweis.

Sei $M = \{m \in \mathbb{N} | m > 1 \wedge m \mid n\}$. Da $n \in M$ gilt, ist diese Menge nicht leer. Jede nichtleere Teilmenge der natürlichen Zahlen, besitzt ein kleinstes Element. (Dies folgt aus dem Peano-Axiom 5, dem Induktionsprinzip). Angenommen k wäre keine Primzahl, so hätte diese einen weiteren Teiler k_1 mit $k_1 \neq 1 \wedge k_1 \neq k$. Es ist aber $k_1 < k$ und $k_1 \in M$ und damit widerspricht dies der Minimalität von M. □

Primzahlen

Satz 3.3

Jede Zahl $n \in \mathbb{N}$ mit $n > 1$ kann als Produkt von Primzahlen dargestellt werden. Also $n = \prod_{i=1}^{k} p_i$ wobei alle p_i Primzahlen sind.

Beweis.

Annahme: $\exists\, n \in \mathbb{N}$: n ist nicht als Produkt lauter Primzahlen darstellbar.

Sei $M = \{m \in \mathbb{N} \mid$ m ist nicht als Produkt von Primzahlen darstellbar$\}$. Laut Annahme ist $M \subset \mathbb{N} \wedge M \neq \{\}$. Also enthält diese Menge ein kleinstes Element, welches wir m_0 nennen. Dieses ist entweder eine Primzahl oder durch eine Primzahl p teilbar, also $\exists\, \ell \in \mathbb{N} : p \cdot \ell = m_0$. Da $\ell < m_0$ gilt, ist $\ell \notin M$ also lässt sich ℓ als Produkt von Primzahlen darstellen, also $\ell = \prod_{i=1}^{k} p_i$ und damit gilt

$m_0 = p \cdot \prod_{i=1}^{k} p_i$ im Widerspruch zur Annahme. □

Primzahlen

Satz 3.4 (Fundamentalsatz der elementaren Zahlentheorie)

Für jede natürliche Zahl > 1 *gibt es eine bis auf die Reihenfolge der Faktoren eindeutige Zerlegung in ein Produkt aus Primfaktoren.*

Primzahlen

Satz 3.5 (Euklid)

Es gibt unendlich viele Primzahlen.

Beweis durch Widerspruch.

Annahme: Es gibt nur endlich viele Primzahlen.

Nehmen wir an diese heißen $p_1, \ldots, p_n$ so betrachten wir $q = \prod_{i=1}^{n} p_i + 1$.

q hat eine Zerlegung in Primfaktoren und wird deshalb von mindestens einer der p_i geteilt. Nennen wir die Zahl p_1. Wegen $p_1 \mid q \wedge p_1 \mid \prod_{i=1}^{n} p_i$ gilt $p_1 \mid q - \prod_{i=1}^{n} p_i$ also $p_1 \mid 1$. Dann muss aber $p_1 = 1$ gelten, was einen Widerspruch darstellt. □

Primzahlen

Satz 3.6 (Kleiner Satz von Fermat)

Es sei p eine Primzahl und $a \in \mathbb{Z}$ mit $ggT(p, a) = 1$ dann gilt

$$a^p \equiv a \mod p$$

Beweis durch vollständige Induktion.

Induktionsanfang: $0^p - 0$ ist durch p teilbar.

Induktionsschritt: Die Behauptung sei für ein gewisses a wahr.

$(a+1)^p - (a+1) = a^p + \binom{p}{1} a^{p-1} + \ldots + \binom{p}{p-1} a + 1 - (a+1)$

Im Binomialkoeffizienten $\binom{p}{k} = \frac{p \cdot (p-1) \cdot \ldots \cdot (p-k+1)}{k!}$ taucht p für $1 \leq k \leq p-1$ nur im Zähler auf. Daher sind alle Binomialkoeffizienten durch p teilbar. Daher folgt

$(a+1)^p - (a+1) \equiv a^p + 1 - (a+1) \mod p \equiv a^p - a \mod p.$

Nach Induktionsvoraussetzung ist $a^p - a$ durch p teilbar. □

Primzahlen

Definition 3.7

Die Phi-Funktion ist definiert durch $\varphi : \mathbb{N}^* \to \mathbb{N}^*$ *mit*

$$\varphi(n) = |\{a \in \mathbb{N}^* \mid 1 \leq a \leq n \wedge ggT(a, n) = 1\}|$$

Also die Anzahl aller zu n teilerfremden Zahlen, die kleiner oder gleich n sind.

Primzahlen

Satz 3.8 (Euler)

Für alle $a, n \in \mathbb{N}^*$ *mit* $ggT(a, n) = 1$ *dann gilt*

$$a^{\varphi(n)} \equiv 1 \mod n$$

Primzahlen

Satz 3.9

- *Für natürliche Zahlen a,b gilt:* $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$
- *Für eine Primzahl p gilt* $\varphi(p) = p - 1$

Gruppentheorie

Definition 4.1

Wir definieren die Menge $\mathbb{Z}_n^*$ als die Menge aller der Elemente von $\mathbb{Z}_n$, die zu n teilerfremd sind.

Übung 4.1

Ermitteln Sie die Mengen $\mathbb{Z}_8^*, \mathbb{Z}_{10}^*, \mathbb{Z}_{12}^*$ samt Multiplikationstafeln.

Gruppentheorie

Satz 4.2

Die Menge $\mathbb{Z}_n^*$ bildet mit der Multiplikation einer Gruppe. Diese nennen wir auch prime Restklassengruppe von n

Definition 4.3

Sei $(G, \cdot)$ eine Gruppe, dann definieren wir die Ordnung eines Elementes a dieser Gruppe, als die kleinste Zahl k, für die $a^k = 1$ gilt und schreiben dann $ord(a) = k$.
Unter der Ordnung einer Gruppe verstehen wir die Anzahl der Elemente der Gruppe, also $ord(G) = |G|$

Übung 4.2

Ermitteln Sie die Gruppe $G = \mathbb{Z}_{14}^*$ *die folgenden Ordnungen:*

- *ord(3),ord(5)*
- *ord(9),ord(11)*
- *ord(G)*

Satz 4.4 (Element- und Gruppenordnung)

Sei G eine multiplikative Gruppe.

1. $\forall\, a \in G : a^{ord(G)} = 1$
2. $\forall\, a \in G : ord(a) \mid ord(G)$

Gruppentheorie

Bestimmung der Inversen

Gesucht ist das inverse Element von 47 in der Gruppe $\mathbb{Z}_{60}^*$.

Dazu verwenden wir den erweiterten euklidischen Algorithmus an:

a	b	q	r	x	y
60	47	1	13		
47	13	3	8		
13	8	1	5		
8	5	1	3		
5	3	1	2		
3	2	1	1		
2	1	2	0		

Gruppentheorie

Bestimmung der Inversen

a	b	q	r	x	y
60	47	1	13	-18	23
47	13	3	8	5	-18
13	8	1	5	-3	5
8	5	1	3	2	-3
5	3	1	2	-1	2
3	2	1	1	1	-1
2	1	2	0	0	1

Also gilt $-18 \cdot 60 + 23 \cdot 47 = 1 \Rightarrow 23 \cdot 47 \equiv 1 \mod 60$

Untergruppen

Definition 4.5

Sei G eine Gruppe. Dann heißt eine Teilmenge $U \subseteq G$ Untergruppe von G, wenn U selbst wieder eine Gruppe ist. Wir schreiben dann $U \triangleleft G$

Beispiel

Die Menge $5\mathbb{Z}$ mit der Addition ist eine Untergruppe von $(\mathbb{Z}, +)$

Übung 4.3

Beweisen Sie das Untergruppenkriterium:
U ist Untergruppe von $G \Leftrightarrow \forall\, a, b \in U : a \cdot b^{-1} \in U$

Untergruppen

Übung 4.4

Sei $H := \{ \begin{pmatrix} 1 & a & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \mid a \in \mathbb{R} \}$

Zeigen Sie, dass H eine Untergruppe der Gruppe $GL_3(\mathbb{R})$ *der invertierbaren 3x3-Matrizen ist.*

Untergruppen

Definition 4.6

Sei G eine Gruppe und $M \subseteq G$.

Wir definieren nun die von M erzeugte Untergruppe von G als die kleinste Untergruppe von G, die die Menge M enthält und schreiben für diese Untergruppe $< M >$. Ist M eine einelementige Menge $M = \{g\}$, so schreiben wir für die von M erzeugte Gruppe $< g >$

Beispiel

Sei $M = \{9, 15\}$, so gilt: $< M >= 3\mathbb{Z}$

Untergruppen

Definition 4.7

Eine Gruppe heißt zyklisch, wenn sie von einem einzigen Element g erzeugt wird, also $G =< g >$ gilt. Das Element g heißt dann erzeugendes Element

Beispiel

Sei $M = \{9, 15\}$, so gilt: $< M >= 3\mathbb{Z}$

Diffie-Hellman-Protokoll

In der Kryptographie wird immer die (geheime) Kommunikation zweier fiktiver Personen betrachtet, die wir in der Folge Alice und Bob nennen wollen.

Alice und Bob einigen sich auf eine Primzahl p und eine Zahl g, die zwischen 2 und $p-1$ liegt. Der gemeinsame Schlüssel k wird wie folgt erzeugt:

Alice wählt eine geheime Zahl s und Bob eine geheime Zahl r. Diese Zahlen werden Exponenten genannt.

- Alice rechnet $a \equiv g^s \mod p$ und sendet a an Bob.
- Bob rechnet $b \equiv g^r \mod p$ und sendet b an Bob.
- Alice rechnet $k_{\text{Alice}} \equiv b^s \mod p$
- Bob rechnet $k_{\text{Bob}} \equiv a^r \mod p$

Diffie-Hellman-Protokoll

Satz 4.8

Es gilt: $k_{Alice} = k_{Bob}$

Beweis.

$k_{\text{Alice}} \equiv b^s \mod p \equiv (g^r)^s \mod p \equiv g^{r \cdot s} \mod p \equiv (g^s)^r \mod p$

$\equiv a^r \mod p \equiv k_{\text{Bob}} \mod p$ □

RSA

Das RSA-Verfahren ist nach den Mathematikern Ronald Rivest, Adi Shamir und Leonard Adleman benannt, die dieses Verfahren 1977 am MIT entwickelten.
Das Verfahren hat folgende Eigenschaften:

- Keine feste Zuordnung von Buchstaben im Originaltext und im Chiffrat
- nicht symmetrisch
- Der Schlüssel besteht aus zwei Teilen (public-key, private-key)
- Entschlüsseln ist nur mit dem privaten Schlüssel möglich
- Aus dem öffentlichen Schlüssel kann der private Schlüssel nur mit großem Zeitaufwand (Jahre) ermittelt werden.

RSA

Definition 5.1

Eine Falltürfunktion ist eine Abbildung f einer Menge X in eine Menge Y, ist eine Funktion für die $f(x)$ leicht zu berechnen ist, aber es schwierig (oder sehr zeitaufwändig) ist, aus $y = f(x)$ das Urbild x zu berechnen.

Beispiel (Briefkasten)

In einen Briefkasten kann man leicht etwas einwerfen, aber zum herausholen benötigt man den Schlüssel oder müsste ihn aufbrechen.

RSA

Schlüsselgenerierung (Public-Key)

- Alice wählt zwei Primzahlen p und q aus und multipliziert diese miteinander und erhält $n = p \cdot q$
- Danach ermittelt sie $m = \varphi(p) \cdot \varphi(q) = (p-1) \cdot (q-1)$
- Sie wählt eine Zahl e aus mit $ggT(e, m) = 1$
- Der öffentliche Schlüssel ist nun das Paar (n,e) wobei n Modul und e Exponent genannt wird.

RSA

Beispiel zum Public-Key

$p = 19, q = 23$
$n = 437, m = (19 - 1) \cdot (23 - 1) = 18 \cdot 22 = 396$
Wähle $e = 281$ und erhalte damit den Schlüssel (437,281)

Übung 5.1

Zeigen Sie mit dem euklidischen Algorithmus, dass $ggT(396, 281) = 1$ *gilt.*

RSA

Schlüsselgenerierung (Private-Key)

- Alice hat den öffentlichen Schlüssel (n,e) gewählt
- Danach ermittelt sie das Inverse Element d von e in $\mathbb{Z}^*_{\varphi(n)}$
- Sie wählt d als privaten Schlüssel

RSA

Verschlüsselung und Entschlüsselung

- Bob möchte eine Nachricht x an Alice senden.
- Bob verschafft sich den öffentlichen Schlüssel (n,e) von Alice
- Bob verschlüsselt x mit $y = x^e \mod n$
- Alice entschlüsselt y und rechnet $x = y^d \mod n$

Übung 5.2

Ermitteln Sie das Inverse Element d von $e = 281$ *in* $\mathbb{Z}^*_{396}$

RSA

Beispiel zur Ver- und Entschlüsselung

- $(n, e) = (437, 281)$, $d = 365$
- Nachricht von Bob an Alice $x = 401$
- $y = 401^{281} \mod 437 = 224$
- Alice entschlüsselt: $x = 224^{365} \mod 437 = 401$

RSA

Warum funktioniert das RSA?

Beweis von RSA (Fall 1).

Sei $1 \leq x < n$:

Fall 1: $ggT(x, n) = 1$

$y^d \equiv (x^e)^d \mod n \equiv x^{e \cdot d} \mod n$

Wegen $d \cdot e \equiv 1 \mod m$ (EULER) existiert ein

$k \in \mathbb{Z} : d \cdot e = k \cdot m + 1$ also

$x^{e \cdot d} \equiv x^{km+1} \mod n \equiv x^{km} \cdot x \mod n \equiv (x^m)^k \cdot x \mod n \equiv 1^k x$

$\mod n \equiv x \mod n$

RSA

Warum funktioniert das RSA?

Beweis von RSA (Fall 2).

Fall 2: x und n sind nicht teilerfremd.

Die kleinste positive natürliche Zahl s mit
$ggT(s,p) > 1 \wedge ggT(s,q) > 1$ ist $s = p \cdot q = n$
Wegen $x < n$ und $ggT(x,n) > 1$ gibt es zwei Möglichkeiten:
a) $ggT(x,q) = 1 \wedge p \mid x$ oder b) $ggT(x,p) = 1 \wedge q \mid x$
o.B.d.A nehmen wir a) an. Dann gilt $p \mid x \Rightarrow x \cdot x^{k \cdot \varphi(n)} \equiv x$ mod $p \Rightarrow x^{km+1} \equiv x \mod p \Rightarrow x^{e \cdot d} \equiv x \mod p \Rightarrow x^{e \cdot d} \equiv 1$ mod n □

Übung 5.3

Berechnen Sie den Public-Key und Private-Key für gegebenes p und q und verschlüsseln x.

1. $p = 7, q = 13, e = 5, x = 12$
2. $p = 3, q = 17, e = 5, x = 15$

Polynomringe

Definition 6.1 (Polynom)

Die Menge $\mathbb{K}$ *steht für einen Körper z.B.* $\mathbb{R}$
Eine Funktion $p : \mathbb{K} \to \mathbb{K}$ *mit*

$$p(x) = \sum_{k=0}^{n} a_k x^k$$

heißt Polynom. Die Zahlen $a_0, a_1, \ldots, a_n$ *heißen Koeffizienten. Sei* $a_n \neq 0$ *dann heißt* n *Grad des Polynoms und wir schreiben* $\deg(p) = n$. *Im Falle von* $a_n = 1$ *nennen wir das Polynom normiert.*

Polynomringe

Beispiele

1. $\mathbb{R}[x]$ enthält alle Polynome mit reellen Koeffizienten,z.B. $p(x) = x^3 - 2x^2 + \sqrt{3}$
2. $\mathbb{C}[x]$ enthält alle Polynome mit komplexen Koeffizienten, z.B. $p(x) = x^4 + \mathrm{i} \cdot x^2 + 1$
3. $\mathbb{Z}_2[x]$ besteht aus allen Polynomen mit den Koeffizienten $0, 1$ z.B. $p(x) = x^2 + x + 1$

Polynomringe

Definition 6.2 (Rechenoperationen)

Wir führen nun zwei Rechenoperationen (Addition, Multiplikation) ein.

Seien $p, q \in \mathbb{K}[x]$ *mit* $p(x) = \sum_{k=0}^{n} a_k x^k, q(x) = \sum_{k=0}^{m} b_k x^k$ *dann ist*

$$(p+q)(x) = \sum_{k=0}^{\max(m,n)} (a_k + b_k) x^k$$

$$(p \cdot q)(x) = \sum_{k=0}^{m+n} \sum_{i+j=k} (a_i \cdot b_j) x^k$$

Mit diesen Rechenoperation bildet $\mathbb{K}[x]$ einen kommutativen Ring mit Einselement.

Polynomringe

Übung 6.1

Rechnen in $\mathbb{Z}_p[x]$

1. *Berechnen Sie für*
   $p(x) = x^3 + x$, $q(x) = x + 1 \in \mathbb{Z}_2[x] : p + q$, $q + q$, $p \cdot q$
2. *Berechnen Sie für*
   $p(x) = x^2 + 2x + 1$, $q(x) = x + 2 \in \mathbb{Z}_3[x] : p + q$, $p \cdot q$

Beachten Sie, dass in $\mathbb{Z}_p$ alle Rechenoperationen Modulo p ausgeführt werden.

Polynomringe

Satz 6.3 (Polynomdivision)

sind $p(x)$ *und* $q(x)$ *Polynome mit* $\deg(q) \leq \deg(p)$, *dann gibt es Polynome* $s(x), r(x)$ *mit*

$$p(x) = s(x)q(x) + r(x)$$

Es gelten außerdem: $\deg(s) = \deg(p) - \deg(q)$ *und* $\deg(r) < \deg(q)$

Polynomringe

Hornerschema

a) $(x^3 - 3x^2 - x + 3) : (x - 1)$

b) $(x^3 - 4x^2 + 3x + 2) : (x - 2)$

Übung 6.2

Finden Sie die Lösungen der folgenden Gleichungen:

1. $x^3 - 4x^2 + x + 6 = 0$
2. $x^4 + 2x^3 - 8x^2 - 16x = 0$

Polynomringe

Doppeltes Hornerschema

$\frac{3x^4+3x^3-5x^2+x-1}{x^2+x-2} = ?$

Übung 6.3

Berechnen Sie die folgenden Polynome:

1. $(3x^4 + x^3 - 2x) : (x^2 + 1)$
2. $(x^2 + x + 2) : (x - 1)$

Polynomringe

Definition 6.4 (Teiler)

Verschwindet bei der Polynomdivision der Polynome $p(x) : q(x)$ der Rest, gilt also

$$p(x) = s(x)q(x)$$

so nennen wir die Polynome $s(x)$ und $q(x)$ Teiler von $p(x)$. Ist ein Teiler ein normiertes Polynom so sprechen wir von einem normierten Teiler.

Übung 6.4

Geben Sie die normierten Teiler der folgenden Polynome an:

1. $x^2 - 8x + 15$
2. $(2x - 1)(x - 5)^2$

Polynomringe

Definition 6.5 (Größter gemeinsamer Teiler)

Wir definieren den größten gemeinsamen Teiler zweier Polynome p,q ($ggT(p,q)$) ist das normierte Polynom maximalen Grades, welches sowohl p als auch q teilt. Falls $ggT(p,q) = 1$ gilt, so nennt man die Polynome teilerfremd.

Der ggT kann mit dem euklidischen Algorithmus errechnet werden. Der letzte nicht verschwindende Rest ist ggf. zu normieren.

Übung 6.5

Berechnen Sie den ggT der folgenden Polynome:

1. $p(x) = 4(x-1)^2$, $q(x) = 8(x-1)$
2. $p(x) = (3x-1)(x+2)^4$, $q(x) = (x-\frac{1}{3})(5x+2)$
3. $p(x) = 5(x-1)$, $q(x) = 5(x+1)$

Polynomringe

Satz 6.6 (Erweiterter euklidischer Algorithmus)

Für beliebige Polynome $p(x)$ und $q(x)$ gibt es Polynome $s(x)$ und $r(x)$ mit

$$s(x)p(x) + r(x)q(x) = ggT(p(x), q(x))$$

Diese können mit dem erweiterten euklidischen Algorithmus berechnet werden.

Übung 6.6

Es sei $p(x) = x^3 - 2x + 1$ und $q(x) = x^2 - 1$.
Finden Sie Polynome $s(x), r(x)$ mit
$s(x)P(x) + r(x)q(x) = ggT(p(x), q(x))$

Restklassenringe

Definition 6.7 (Kongruenz von Polynomen)

Zwei Polynome $p(x), q(x) \in \mathbb{K}[x]$ *heißen kongruent modulo* $m(x)$ ($p(x) \equiv q(x) \mod m(x)$)*, falls Sie bei der Division durch* $m(x)$ *den gleichen Rest haben, bzw. wenn* $p(x) - q(x) \mid m(x)$ *gilt.*

Übung 6.7

Sind die folgenden Polynome kongruent modulo m(x)?

1. $p(x) = x^3 + 1,\ q(x) = x + 1,\ m(x) = x^2 - 1$
2. $p(x) = x^5 + 2x^3 + 7,\ q(x) = x^3 + 3x - 9,\ m(x) = x^3 + x + 1$

Restklassenringe

Definition 6.8 (Restklassenring von Polynomen)

Die Menge aller Polynome $p(x) \in \mathbb{K}[x]$, *die kongruent modulo* $m(x)$ *sind bilden den Restklassenring* $\mathbb{K}[x]_{m(x)}$

Restklassenringe

Übung 6.8

Berechnen Sie in $\mathbb{Z}_2[x]$ *den Rest modulo* $m(x) = x^2 + 1$

1. $f(x) = x^3 + 1$
2. $g(x) = x + 1$
3. *Geben Sie alle Reste an, die bei der Division durch* $m(x)$ *in* $\mathbb{Z}_2[x]$ *auftreten können.*

Restklassenringe

Übung 6.9

Geben Sie die Menge $\mathbb{R}[x]_{m(x)}$ *an für:*

1. $m(x) = x^2 + 1$
2. $m(x) = x^4 + x^3 + 1$

Übung 6.10

Geben Sie die Additions- und Multiplikationstabelle für $\mathbb{Z}_2[x]_{x^2+x+1} = \{0, 1, x, x+1\}$ *an.*

Wenn man die Koeffizienten eines Polynomas aus $\mathbb{Z}_2[x]_{x^2+x+1}$ als Dualzahl auffasst, bekommt man die folgende Additionstabelle:

$+$	00	01	10	11
00	00	01	10	11
01	01	00	11	10
10	10	11	00	01
11	11	10	01	00

Dies entspricht der XOR - Verknüpfung

Restklassenringe

Übung 6.11

Geben Sie die Additions- und Multiplikationstabelle für $\mathbb{Z}_2[x]_{x^2+1} = \{0, 1, x, x+1\}$ *an.*

$\mathbb{Z}_2[x]_{x^2+x+1}$ ist ein Körper, aber
$\mathbb{Z}_2[x]_{x^2+1}$ ist nur ein Ring.

Satz 6.9

Für ein Polynom $p(x) \in \mathbb{K}_[x]_{m(x)}$ *gibt es genau dann ein multiplikatives Inverses, wenn* $ggT(p(x), m(x)) = 1$ *gilt.*

Endliche Körper

Definition 6.10

Ein Polynom $p(x)$ vom Grad > 1 heißt über $\mathbb{K}$ irreduzibel, falls es kein Polynom $q(x)$ mit $0 < deg(q) < deg(p)$ gibt, welches $p(x)$ teilt. Ansonsten nennen wir $p(x)$ reduzibel.

Satz 6.11

Sei $p(x) \in \mathbb{K}[x]$ ein normiertes Polynom vom Grad > 1, dann lässt sich $p(x)$ in der Form

$$\prod_{i=1}^{n} q_i(x)$$

darstellen, wobei $q_i(x)$ irreduzible Polynome mit höchstem Koeffizienten $= 1$ sind. Bis auf die Reihenfolge ist die Zerlegung eindeutig.

Endliche Körper

Übung 6.12

Ist $p(x)$ reduzibel oder irreduzibel über $\mathbb{K}$?

1. $p(x) = x^2 + 1$, $\mathbb{K} = \mathbb{R}$
2. $p(x) = x^2 + 1$, $\mathbb{K} = \mathbb{C}$
3. $p(x) = x^2 + 1$, $\mathbb{K} = \mathbb{Z}_2$
4. $p(x) = x^3 + x + 1$, $\mathbb{K} = \mathbb{Z}_2$
5. $p(x) = x^4 + x^2 + 1$, $\mathbb{K} = \mathbb{Z}_2$

Endliche Körper

Satz 6.12

$\mathbb{K}[x]_{m(x)}$ *ist genau dann ein Körper, wenn* $m(x)$ *irreduzibel über* $\mathbb{K}$ *ist.*

Beispiel

$\mathbb{R}[x]_{x^2+1}$ ist ein Körper, da $x^2 + 1$ in $\mathbb{R}$ irreduzibel ist.
Die Elemente sind der Form $p(x) = a_0 + a_1 x$

Addition:

$$a(x) + b(x) = (a_0 + a_1 x) + (b_0 + b_1 x) = (a_0 + b_0) + (a_1 + b_1)x$$

Multiplikation:

$$a(x) \cdot b(x) = (a_0 + a_1 x) \cdot (b_0 + b_1 x) =$$
$$a_0 b_0 + a_0 b_1 x + a_1 b_0 x + a_1 b_1 x^2 = (a_0 b_0 - a_1 b_1) + (a_0 b_1 + a_1 b_0)x$$

Endliche Körper

Satz 6.13

Sei $m(x)$ ein Polynom vom Grad k, welches über $\mathbb{Z}_p$ irreduzibel ist. Dann ist $\mathbb{Z}_p[x]_{m(x)}$ ein Körper mit p^k Elementen.

Definition 6.14

Ein Körper mit p^k Elementen wird Galois-Körper genannt und mit $GF(p^k)$ abgekürzt.

Endliche Körper

Satz 6.15

Für jede Primzahlpotenz p^k gibt es einen zugehörgigen Galois-Körper, der bis auf die Bezeichnung der Elemente eindeutig ist.

AES

Ein wichtiger Körper ist $GF(2^8) = \mathbb{Z}_2[x]_{x^8+x^4+x^3+x+1}$

Der Rijndael-Verschlüsselungsalgorithmus berechnet das multiplikative Inverse in $GF(2^8)$. Er berechnet also das Inverse modulo $m(x) = x^8 + x^4 + x^3 + x + 1$ in $\mathbb{Z}_2[x]$.

Der Algorithmus wurde von den Belgiern Vincent Rijmen und Joan Daeman entwickelt und wurde als Verschlüsselungsstandard AES im Jahre 2001 als Nachfolger von DES festgelegt.

Reed-Solomon-Code

Der Körper $GF(2^8)$ wird beim sogenannten Reed-Solomon-Code verwendet, mit dessen Hilfe Daten auf CDs und DVDs gespeichert werden.
Der Code ist nach den amerikanischen Mathematikern Irving S. Reed und Gustave Solomon benannt.

Graphentheorie

Wo kommt die Graphentheorie zum Einsatz?

- Routenplanung
- Frequenzplanung im Mobilfunk
- Netzwerk (Router)
- Wegplanung für Roboter
- Optimierung von Ampelschaltungen
- Suchmaschinen

Graphentheorie

Definition 7.1 (Graph)

Ein ungerichteter Graph $G = (V, E)$ besteht aus einer Menge V von Knoten (vertex) und einer Menge E von Kanten (edge). Hierbei sind jeder Kante zwei Knoten, die auch gleich sein können, zugeordnet. Ist $v \in V$ ein Endknoten der Kante $e \in E$, so nennen wir v inzident zu e. Sind zwei Knoten $u, v \in V$ durch eine Kante $e = \{u, v\}$ verbunden, so nennen wir sie adjazent. Eine Kante der Form $e = \{v, v\}$ heißt Schlinge. Zwei Kanten $e = \{u, v\}$ und $f = \{u, v\}$zwischen denselben Endknoten heißen parallel.
Ein Graph ohne Schlingen und parallele Kanten, heißt schlichter Graph

Graphentheorie

$G = (\{1, 2, 3, 4, 5\}, \{a, b, c, d, e, f\})$

mit $a = \{1.2\}$, $b = \{1, 5\}$, $c = \{1, 3\}$, $d = \{1, 3\}$, $e = \{2, 4\}$, $f = \{5, 5\}$

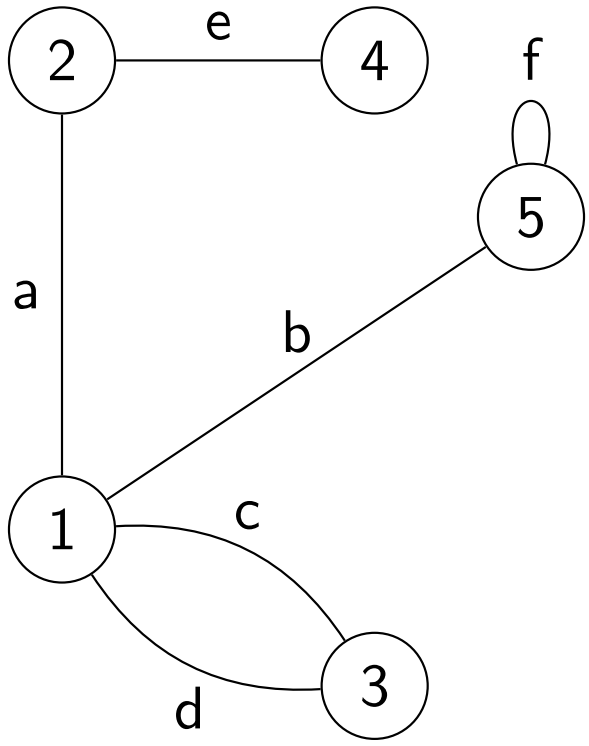


Abbildung: 7.1

Beispiel ungerichteter Graph

Das Ergebnis lässt sich in folgender Tabelle festhalten:

Kante	a	b	c	d	e	f
Endknoten	1	1	1	1	2	5
	2	5	3	3	4	5

Definition 7.2

Der Grad (deg v) eines Knotens $v \in V$ ist die Anzahl der zu v inzidenten Kanten von G. Schlingen werden hierbei doppelt gezählt.

Übung 7.1

Ermitteln Sie die Knotengrade des Graphen 178.

Graphentheorie

Satz 7.3

In einem Graphen mit m Kanten gilt stets

$$\sum_{v \in V} deg\ v = 2m$$

Definition 7.4 (Adjazenzmatrix)

Sei G ein ungerichteter Graph mit n Knoten. Die Knoten von G werden mit den Zahlen der Menge $\{1, \ldots, n\}$ *bezeichnet. Wir definieren die Adjazenzmatrix A als n x n - Matrix mit den Werten*

a_{ij} = *Anzahl der Kanten zwischen i und j.*

Anmerkung: Ist der Graph G ein schlichter Graph, so ist $a_{ij} \in \{0, 1\}$.

Übung 7.2

Stellen Sie für den Graph 178 die Adjazenzmatrix auf.

Definition 7.5 (Kantenfolge,Weg)

Die Kantenfolge eines Graphen G, dann ist eine Kantenfolge eine Folge

$$v_1, e_1, v_2, e_2, \ldots, v_{k-1}, e_{k-1}, v_k$$

von Knoten und Kanten, so dass die Kante e_i jeweils die Endknoten v_i und v_{i+1} besitzt ($i = 1, \ldots, k-1$). Die Länge der Kantenfolge ist die Anzahl der Kanten der Kantenfolge. Ein Weg ist eine Kantenfolge, in dem jeder Knoten nur einmal vorkommt.

Adjazenzmatrix

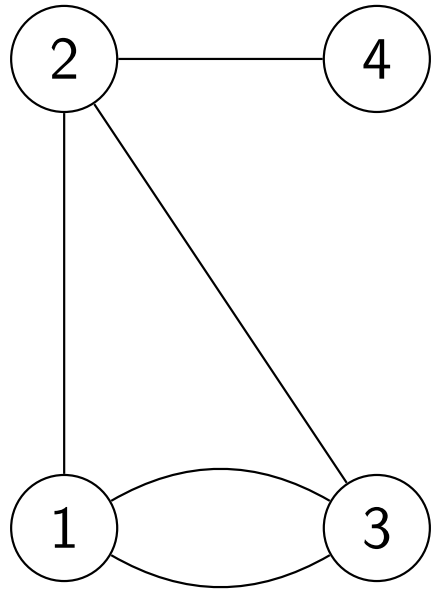


Abbildung: 7.2

Übung 7.3

Stellen Sie die Adjazenzmatrix A auf und errechnen Sie die Matrix A^2.

Adjazenzmatrix

Satz 7.6

Sei A die Adjazenzmatrix eines Graphen. Die Matrix A^p (mit $p \geq 1$) liefert die Anzahl der Kantenfolgen eines Knoten i zum Knoten j der Länge p.

Übung 7.4

Verifizieren Sie dies für $p = 2$ und $p = 3$ für den Graphen 2

Adjazenzliste

Neben der Adjazenzmatrix besteht noch eine weitere Möglichkeit einen Graphen abzuspeichern, die sogenannte Adjazenzliste.
Hierbei speichert man alle Knoten eines Graphen in einem Array.
Jedes Arrayelement enthält eine verkettete Liste der benachbarten Knoten.

Adjazenzliste

Vor- und Nachteile von Adjazenzmatrix und Adjazenzliste

1. Adjazenzmatrix
   - Vorteile:
     - Feststellen, ob eine Kante von i nach j existiert $\in O(1)$
     - Haben die Kanten Markierungen oder Gewichte, so können diese in die Matrix eingetragen werden. Existiert keine Kante, so trägt man ∞ ein (siehe TSP).
   - Nachteile:
     - Hoher Platzbedarf bei großen Graphen $O(n^2)$. Insbesondere bei vielen Knoten aber wenig Kanten.
     - Auffinden aller Nachfolger eines Knotens $\in O(n)$.

Adjazenzliste

Vor- und Nachteile von Adjazenzmatrix und Adjazenzliste

2. Adjazenzliste
   - Vorteile:
     - geringer Platzbedarf, nämlich $O(|V| + |E|)$
     - k Nachfolger eines Knotens werden in $O(k)$ erreicht.
   - Nachteile:
     - Feststellen, ob zwei Knoten benachbart sind ist nicht in konstanter Zeit möglich.

Graphen durchsuchen

Eine wichtige Aufgabe ist das systematische Durchsuchen eines Graphen.
Folgende Strategien werden am häufigsten verwendet:

- Breitensuche
- Tiefensuche

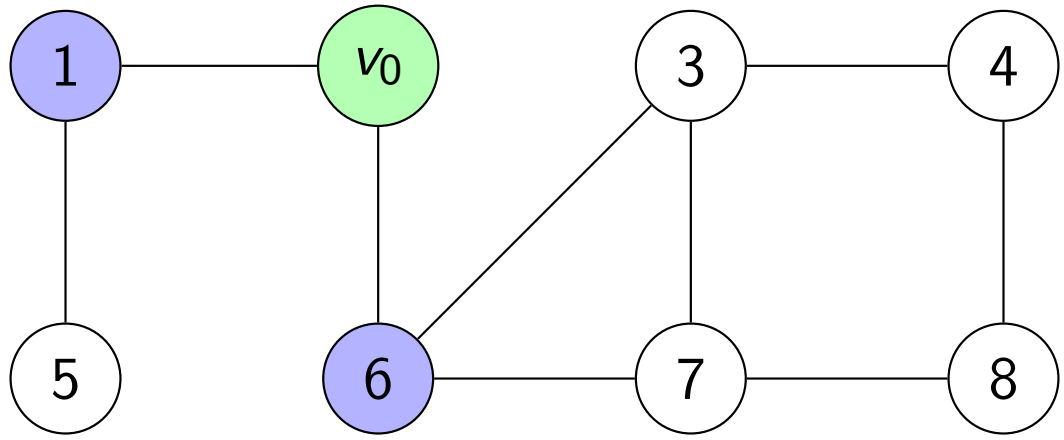
Graphen durchsuchen

Für die Breitensuche benötigen wir eine Queue. In dieser sollen Knoten gespeichert werden.
Wir beginnen mit einem Startknoten v_0

Breitensuche(G)
Input: Startknoten v_0.

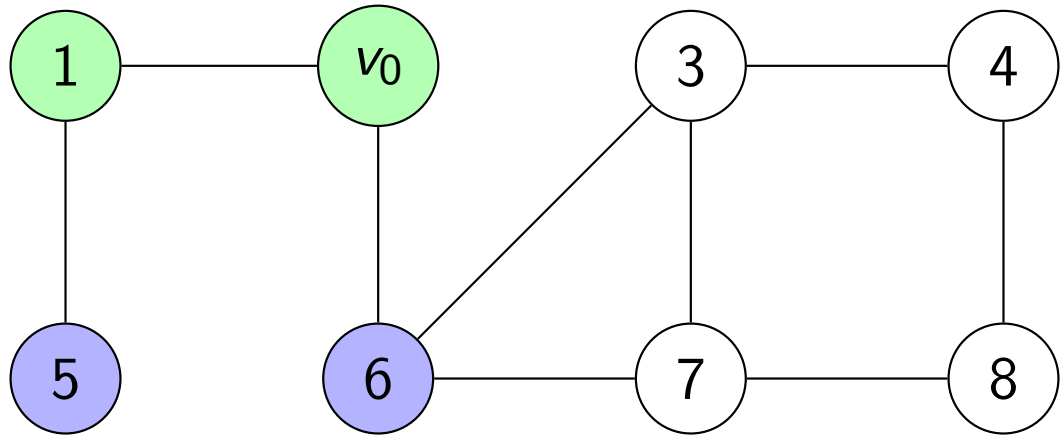
1. Queue = q
2. Füge v_0 in q ein.
3. **solange** q ! = leer
4. u = erstes Element von q
5. **solange** Nachbarknoten n von u gefunden
6. **wenn** n noch nicht besucht
7. Markiere n als besucht
8. Entferne n aus q
9. **solange ende**
10. **solange ende**

Breitensuche



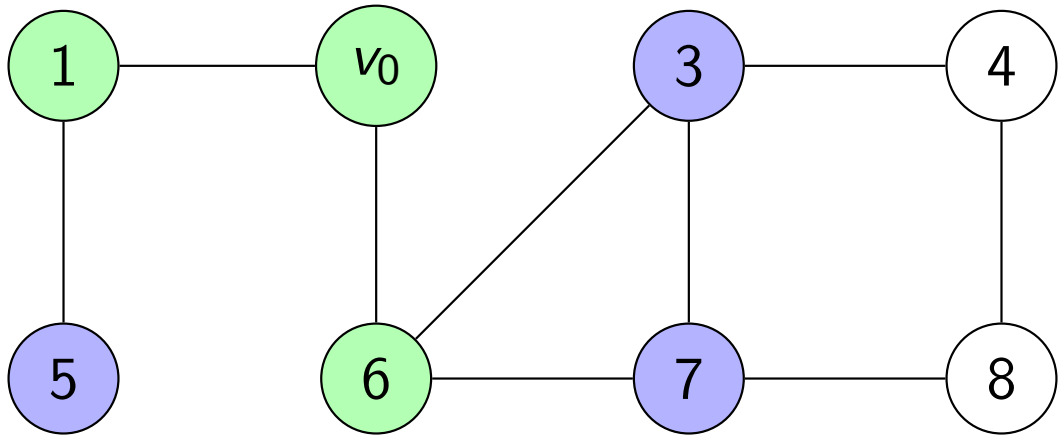
Schritt 1: v_0 wurde besucht. Queue: $\{1, 6\}$

Breitensuche



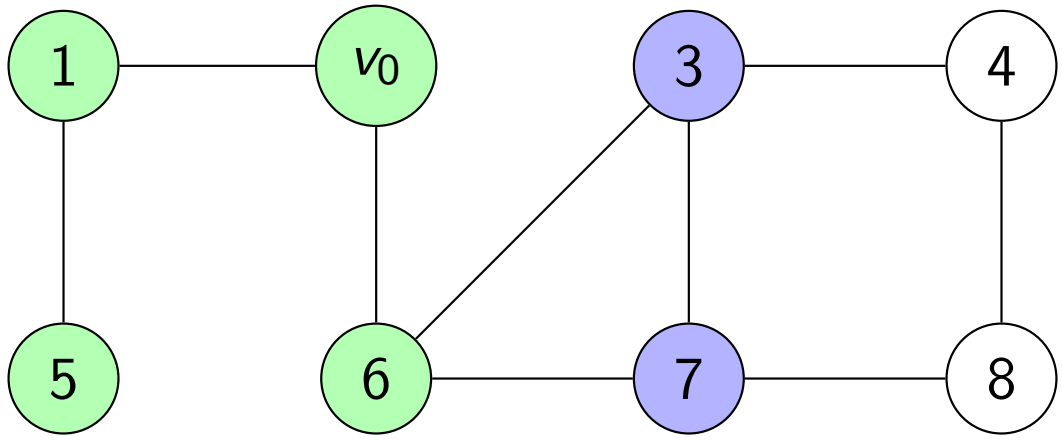
Schritt 2: v_0 und 1 wurden besucht. Queue: $\{6, 5\}$

Breitensuche



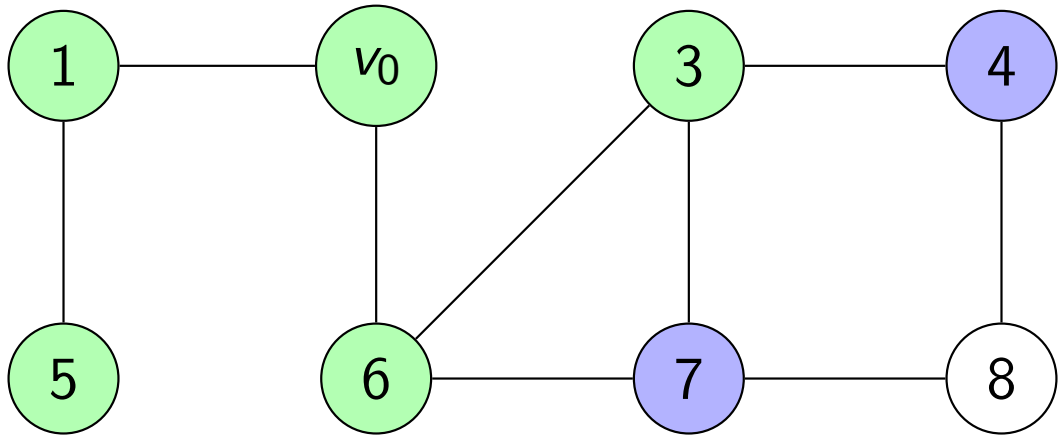
Schritt 3: v_0,1,6 wurden besucht. Queue: $\{5, 3, 7\}$

Breitensuche



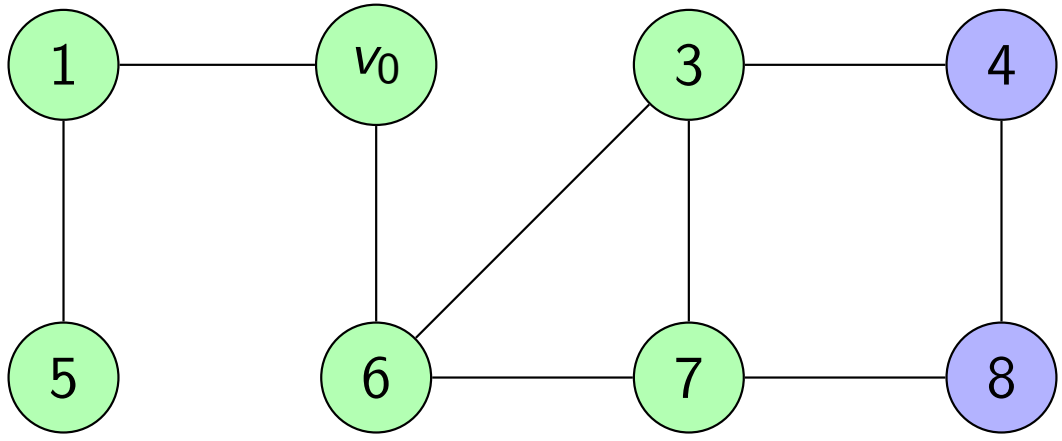
Schritt 4: v_0,1,6,5 wurden besucht. Queue: $\{3, 7\}$

Breitensuche



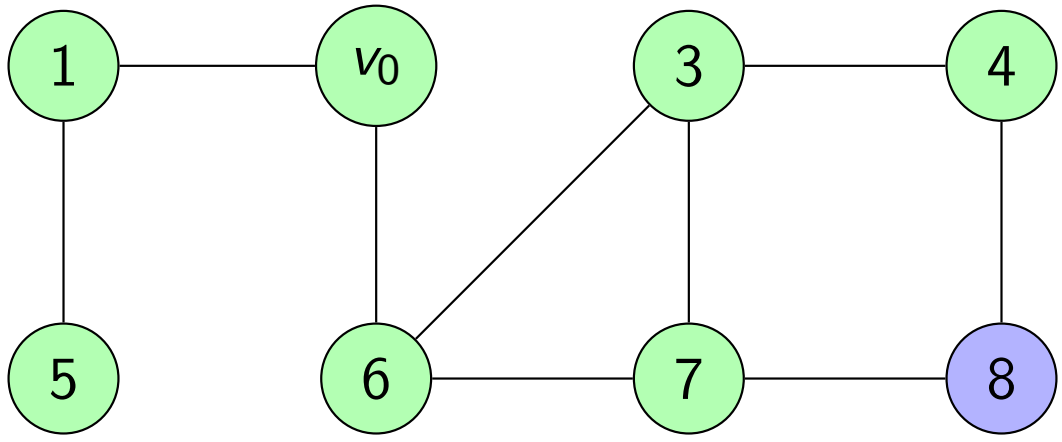
Schritt 5: v_0,1,6,5,3 wurden besucht. Queue: $\{7, 4\}$

Breitensuche



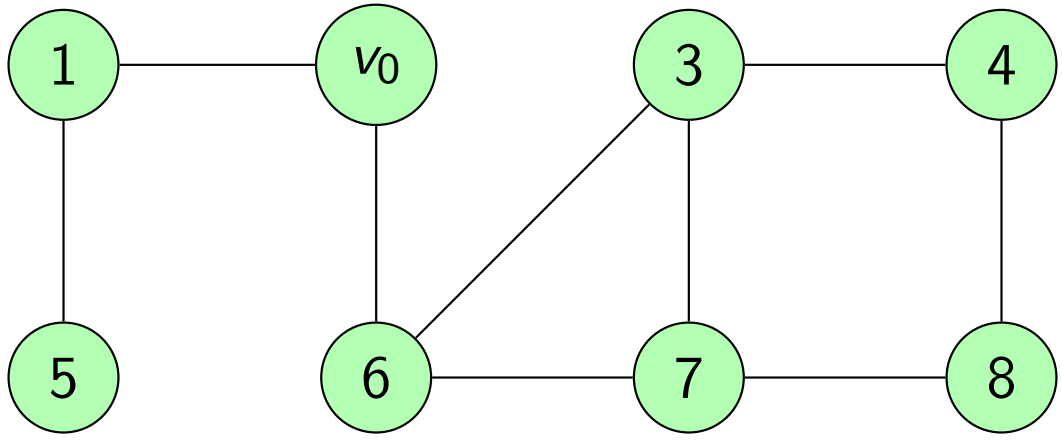
Schritt 6: v_0,1,6,5,3,7 wurden besucht. Queue: $\{4, 8\}$

Breitensuche



Schritt 7: v_0,1,6,5,3,7,4 wurden besucht. Queue: $\{8\}$

Breitensuche

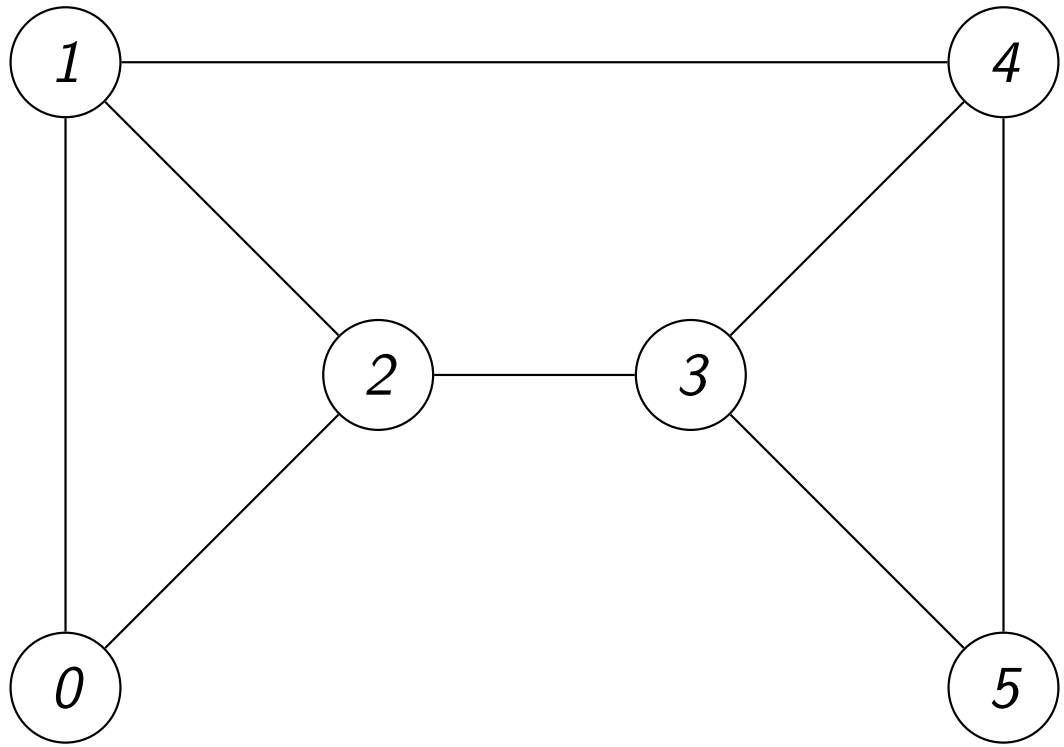


Schritt 8: v_0,1,6,5,3,7,4,8 wurden besucht. Queue: $\{\}$

Breitensuche

Übung 7.5

Geben Sie für die Breitensuche die Reihenfolge der besuchten Knoten aus. Startknoten ist der Knoten 0.



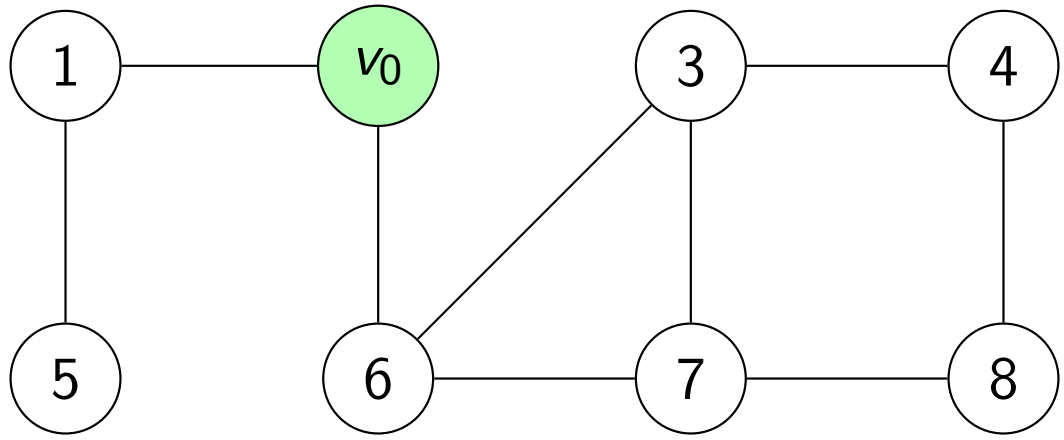
Tiefensuche

Für die Tiefensuche wird eine rekursive Prozedur mit dem Startknoten v_0 aufgerufen.

`Tiefensuche(v : Knoten)`

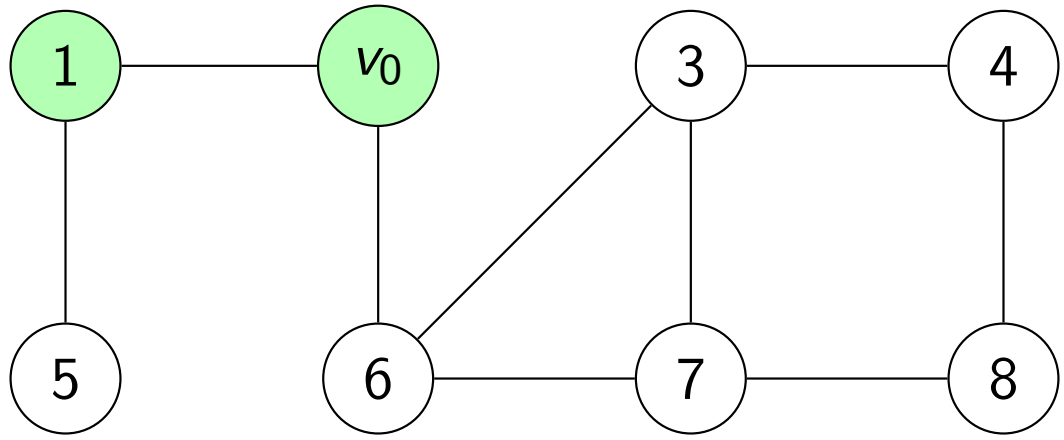
1. Markiere v als besucht
2. N = Array mit allen Nachbarknoten von v
3. n = Anzahl Elemente von N
4. i = 0
5. **solange** $i < n$
6. **wenn** N[i] noch nicht besucht
7. Tiefensuche(N[i])
8. $i = i + 1$
9. **solange ende**

Tiefensuche



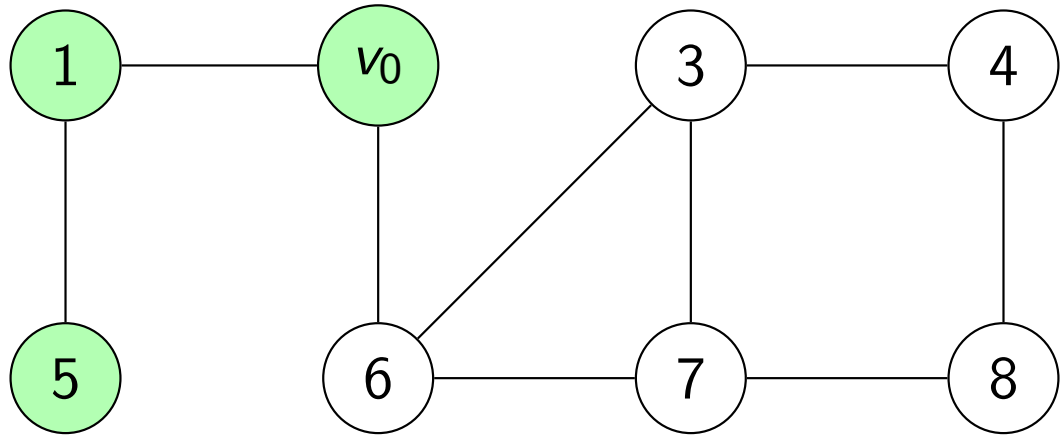
Schritt 1: Tiefensuche(v_0).

Tiefensuche



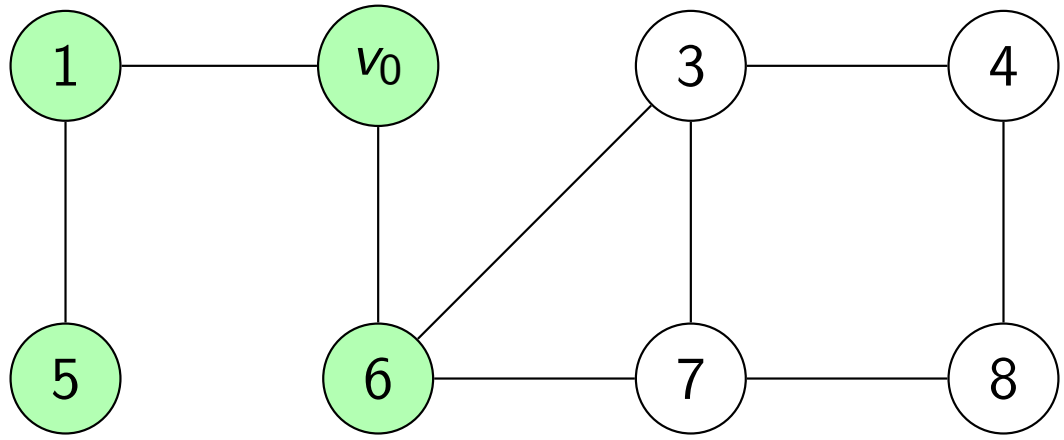
Schritt 2: Tiefensuche(v_0), Tiefensuche(1)

Tiefensuche



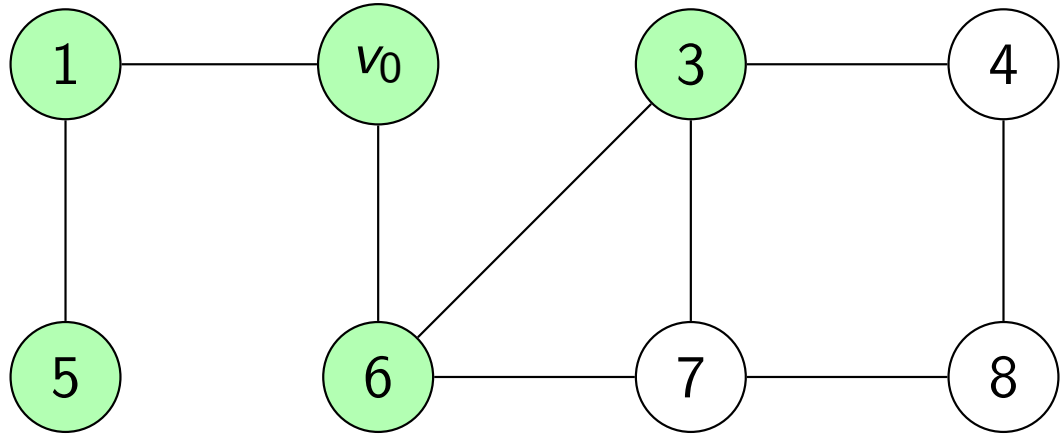
Schritt 3: Tiefensuche(v_0), Tiefensuche(1), Tiefensuche(5)
Da der Knoten 5 keine Nachbarknoten mehr hat, geht es mit dem nächsten Nachbarknoten von v_0 weiter.

Tiefensuche



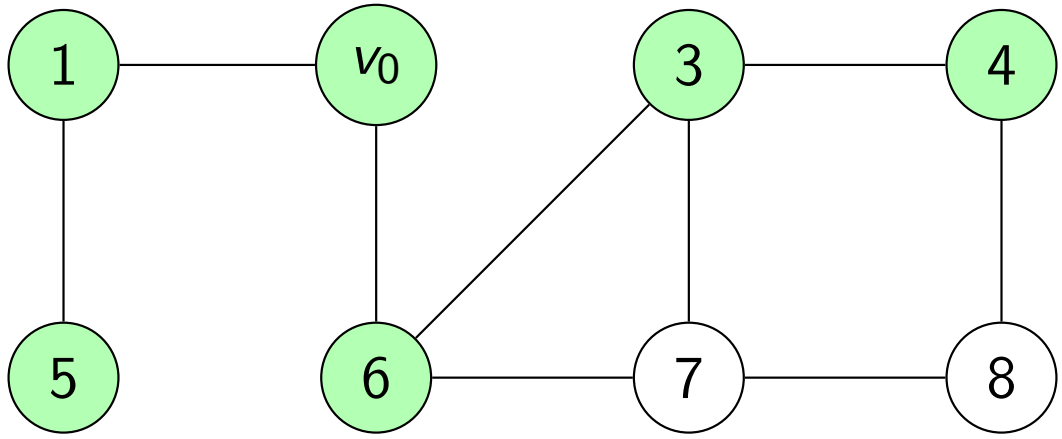
Schritt 4: Tiefensuche(v_0), Tiefensuche(6)

Tiefensuche



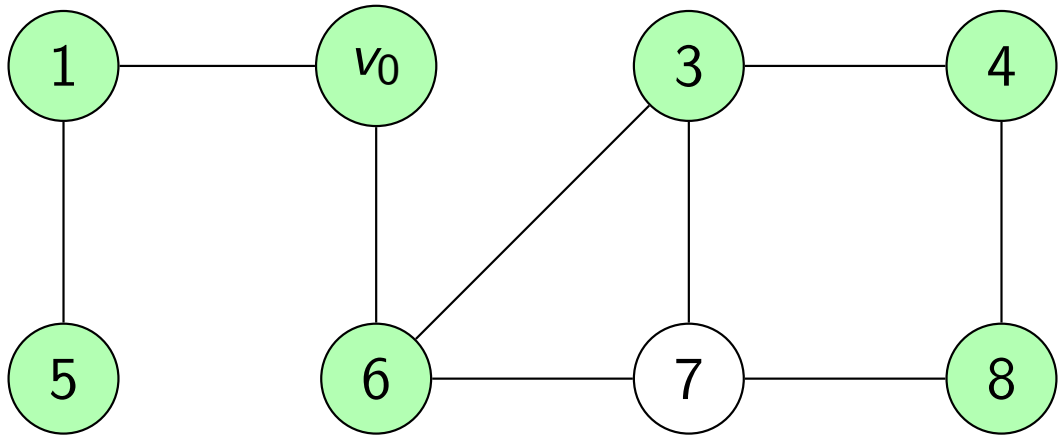
Schritt 5: Tiefensuche(v_0), Tiefensuche(6), Tiefensuche(3)
Es hätte auch Knoten 7 gewählt werden können.

Tiefensuche



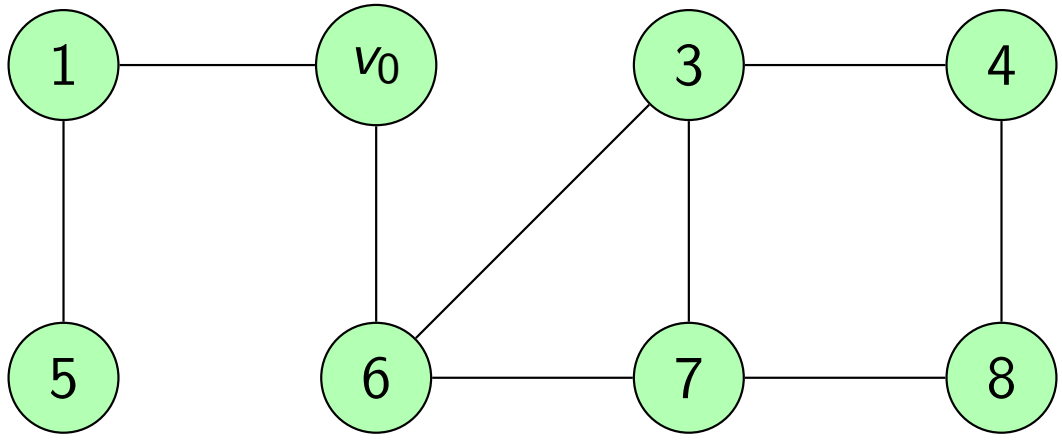
Schritt 6: Tiefensuche(v_0), Tiefensuche(6), Tiefensuche(3), Tiefensuche(4)

Tiefensuche



Schritt 7: Tiefensuche(v_0), Tiefensuche(6), Tiefensuche(3), Tiefensuche(4), Tiefensuche(8)

Tiefensuche



Schritt 8: Tiefensuche(v_0), Tiefensuche(6), Tiefensuche(3), Tiefensuche(4), Tiefensuche(8), Tiefensuche(7)
Alle Knoten wurden besucht. Die Rekursion ist beendet.

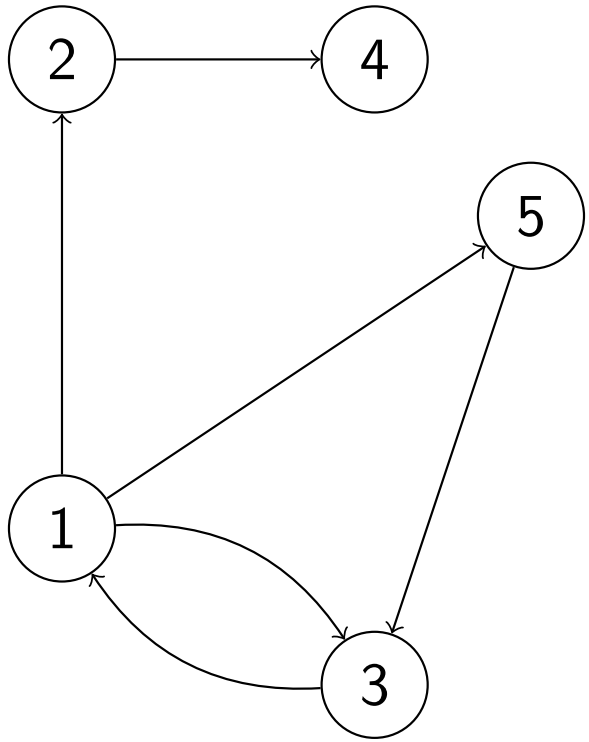
Gerichtete Graphen

Definition 7.7 (Graph)

Ein gerichteter Graph $G = (V, E)$ besteht aus einer Menge V von Knoten und einer Menge E von Kanten, die hier Pfeile genannt werden. Hierbei besteht die Menge E aus geordneten Paaren.

Gerichtete Graphen

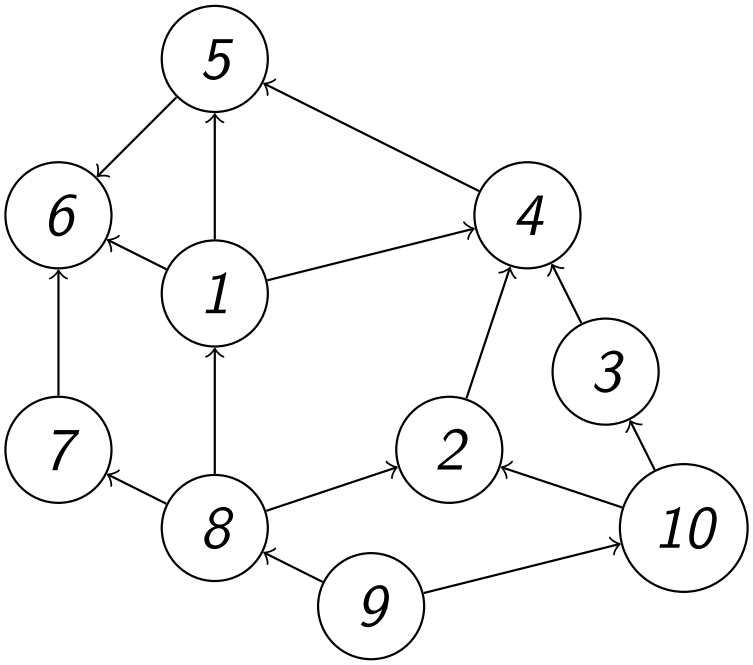
$$G = (\{1, 2, 3, 4, 5\}, \{(1, 2); (1, 5); (2, 4); (5, 3), (1, 3), (3, 1)\})$$



Gerichtete Graphen

Übung 7.6

Gegen Sie an, in welcher Reihenfolge die Knoten bei Breiten- oder Tiefensuche durchlaufen werden. Startknoten ist der Knoten 9.



Bewertete Graphen

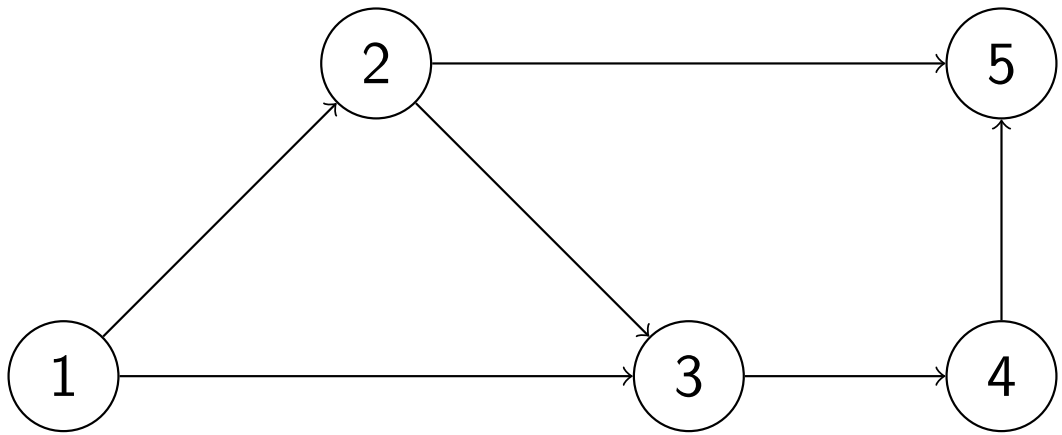
Definition 7.8 (Bewerteter Graph)

Ein bewerteter Graph $G = (V, E, c)$ besteht zusätzlich zur Knoten und Kantenmenge aus einer Matrix c, die jeder Kante eine Bewertung zuordnet.

Topologisches Sortierung

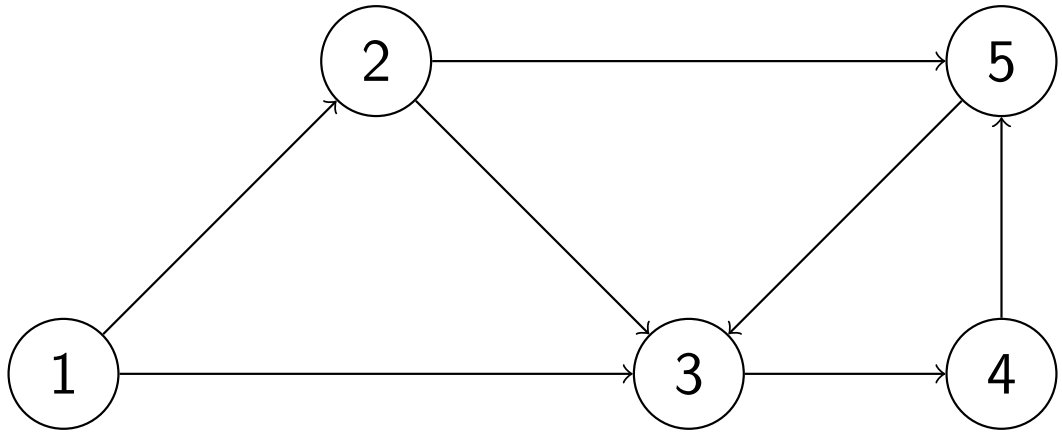
Definition 7.9 (kreisfreier Graph)

Ein gerichteter Graph heißt kreisfrei(azyklisch), falls er keinen geschlossenen Weg enthält



kreisfreier Graph

Topologisches Sortierung



Graph mit Kreis

Mit der Tiefensuche lässt sich leicht feststellen, ob ein Graph kreisfrei ist. Wird bei der Tiefensuche eine Rückwärtskante gefunden, so liegt ein geschlossener Weg vor.

Topologisches Sortierung

Liegt ein kreisfreier gerichteter Graph vor, so lassen sich damit hierarchische Strukturen beschreiben.

Beispiele

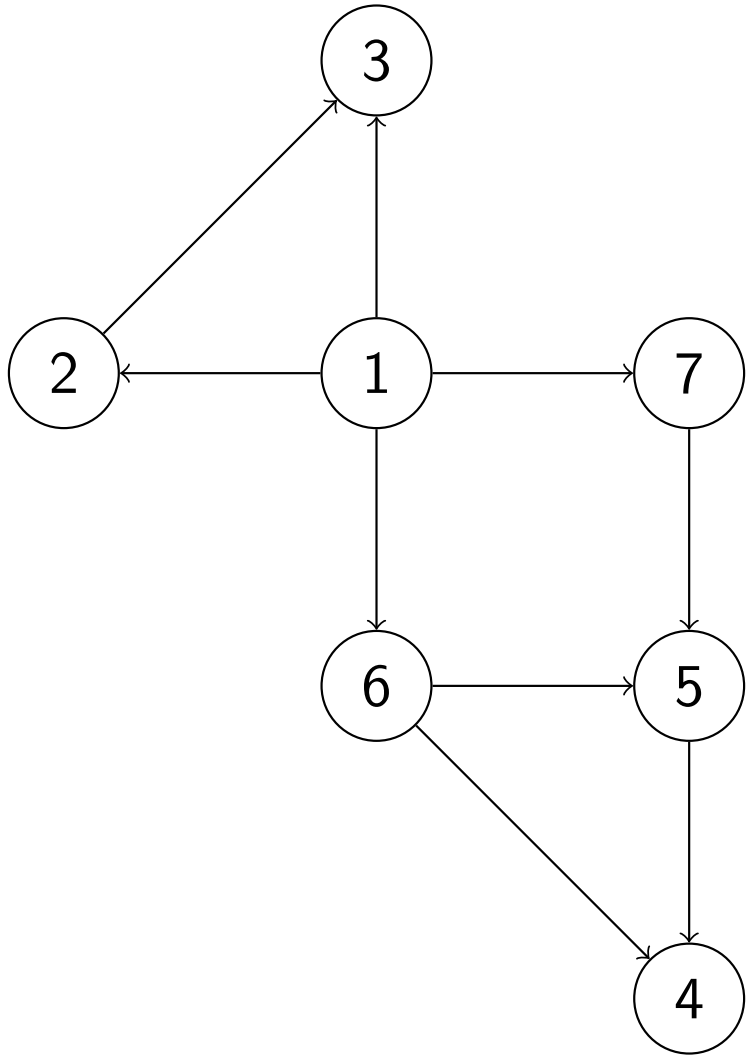
- Fertigung eines Werkstücks. Arbeitsgang v_i kommt vor v_j
- Vorlesungen. Vorlesung v_i ist Voraussetzung für v_j

Topologisches Sortierung

Algorithmus topologische Sortierung.

1. solange der Graph G nicht leer ist.
2. Wähle Quelle (= Knoten ohne Vorgänger) $v \in V$ und füge ihn an die bisherige Knotenfolge an.
3. Entferne v und alle davon ausgehenden Kanten aus G.
4. Fahre fort bei (2) bis alle Knoten aus G entfernt wurden.
5. Falls keine Quellen mehr vorhanden sind und Knotenmenge = leer dann fertig, ansonsten liegt ein Zyklus vor.

Topologisches Sortierung



Topologisches Sortierung

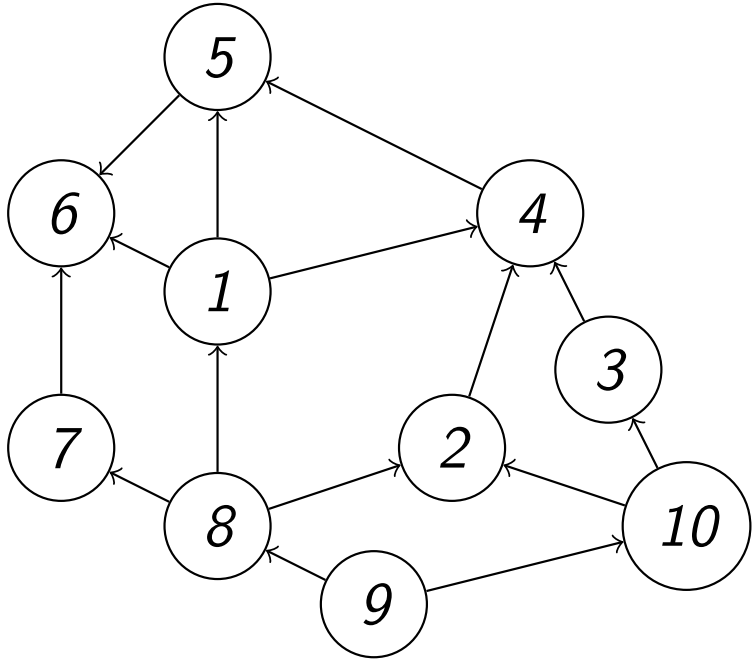
Schritt	vorhandene Quellen	gewählte Quellen
1	{1}	1
2	{2,6,7}	2
3	{6,7,3}	6
4	{7,3}	3
5	{7}	7
6	{5}	5
7	{4}	4

Eine mögliche topologische Sortierung ist 1, 2, 6, 3, 7, 5, 4

Gerichtete Graphen

Übung 7.7

Gegen Sie eine topologische Sortierung an. Geben Sie zu jedem Schritt die vorhandenen Quellen und jeweils die gewählte Quelle



an.

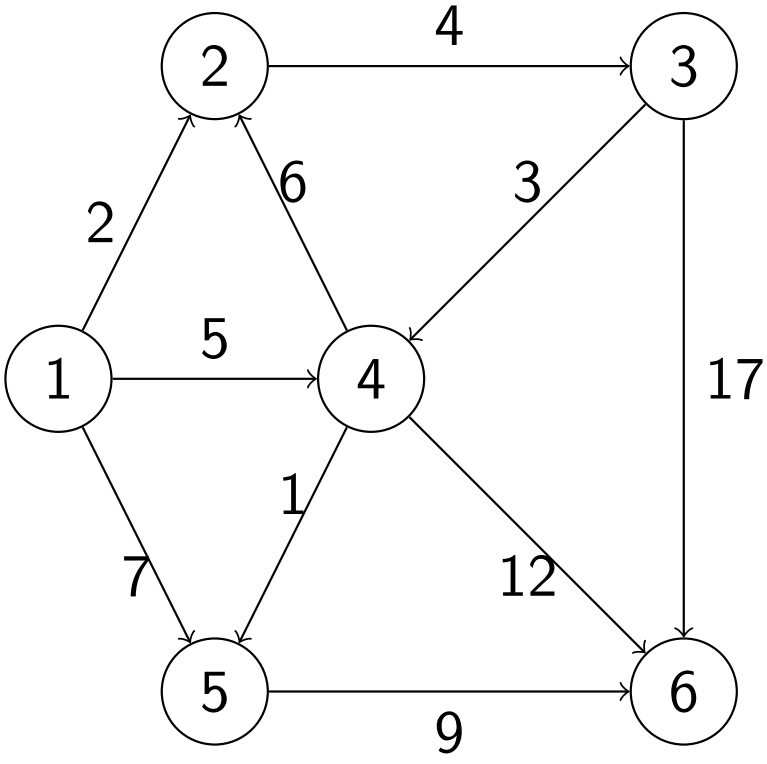
Übung 7.8

Gegeben ist die Adjazenzmatrix eines gerichteten Graphen mit den Knoten 0 bis 5. Geben Sie eine topologische Sortierung der Knoten an.

	0	*1*	*2*	*3*	*4*	*5*
0	*0*	*1*	*1*	*0*	*0*	*0*
1	*0*	*0*	*0*	*0*	*0*	*0*
2	*0*	*1*	*0*	*0*	*0*	*0*
3	*0*	*0*	*0*	*0*	*1*	*0*
4	*0*	*1*	*0*	*0*	*0*	*0*
5	*0*	*0*	*0*	*1*	*1*	*0*

Kürzeste Wege und Dijkstra-Algorithmus

Gesucht sind die kürzesten Wege von einem Startknoten s zu allen anderen Knoten, d.h. die Summe der gewichteten Kanten soll minimal sein.



Der kürzeste Weg von 1 nach 5 ist hier nicht der direkte Weg, sondern der Umweg über den Knoten 4.

Kürzeste Wege

Der Algorithmus von Dijkstra.

Seien nun MK = Menge der markierten Knoten, $D[1, \ldots, n]$ und $R[1, \ldots, n]$ Arrays zur Speicherung kürzester Entfernungen und Wege.

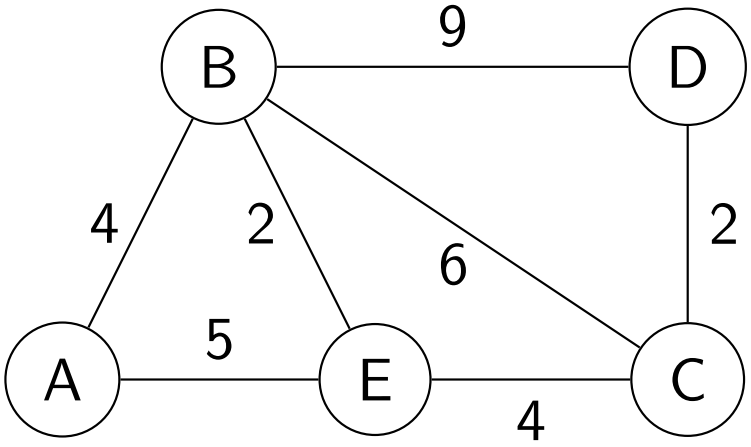
Start:

Setze $MK = \{s\}$ (Startknoten), $D[s] = 0$ und $D[i] = \infty$ für alle Knoten außer s.

Iteration $(1, 2, \ldots)$

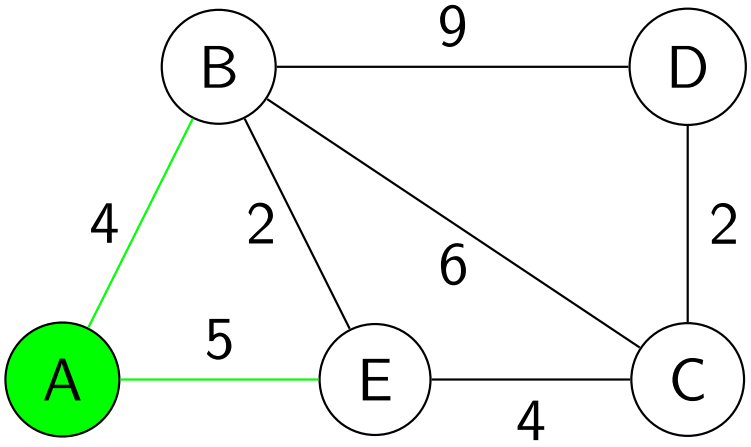
1. Wähle den Knoten h aus MK mit $D[h] = min\{D[i] | i \in MK\}$
2. Für alle erreichbaren Nachbarknoten j: Falls $D[j] > D[h] + c_{hj}$ dann $D[j] = D[h] + c_{hj}$; $R[j] = h$; $MK = MK \cup \{j\}$
3. Eliminiere h aus MK

Kürzeste Wege und Dijkstra-Algorithmus



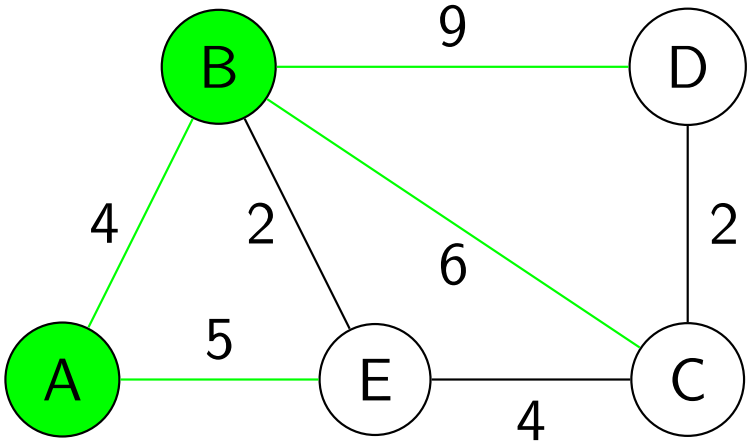
Schritt	Knoten	Knotenmenge	Kosten (B)	Kosten (C)	Kosten (D)	Kosten (E)
Initial	A	{A}				
1						
2						
3						
4						

Kürzeste Wege und Dijkstra-Algorithmus



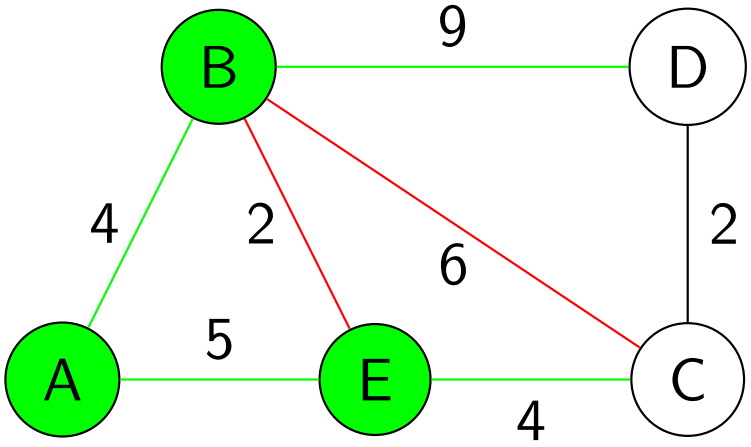
Schritt	Knoten	Knotenmenge	Kosten (B)	Kosten (C)	Kosten (D)	Kosten (E)
Initial	A	{A}	4	-	-	5
1						
2						
3						
4						

Kürzeste Wege und Dijkstra-Algorithmus



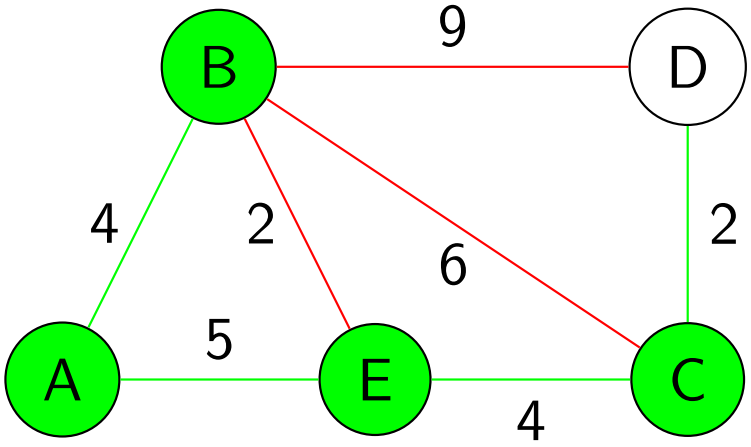
Schritt	Knoten	Knotenmenge	Kosten (B)	Kosten (C)	Kosten (D)	Kosten (E)
Initial	A	{A}	4	-	-	5
1	B	{A,B}	4	10	13	5
2						
3						
4						

Kürzeste Wege und Dijkstra-Algorithmus



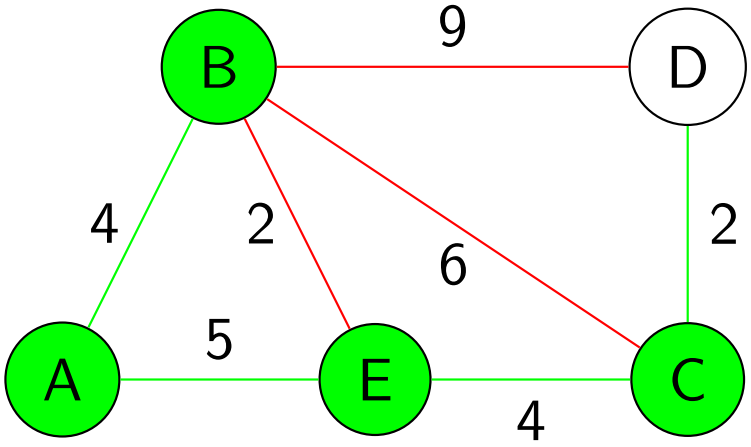
Schritt	Knoten	Knotenmenge	Kosten (B)	Kosten (C)	Kosten (D)	Kosten (E)
Initial	A	{A}	4	-	-	5
1	B	{A,B}	4	10	13	5
2	E	{A,B,E}	4	9	13	5
3						
4						

Kürzeste Wege und Dijkstra-Algorithmus



Schritt	Knoten	Knotenmenge	Kosten (B)	Kosten (C)	Kosten (D)	Kosten (E)
Initial	A	{A}	4	-	-	5
1	B	{A,B}	4	10	13	5
2	E	{A,B,E}	4	9	13	5
3	C	{A,B,E,C}	4	9	11	5
4						

Kürzeste Wege und Dijkstra-Algorithmus

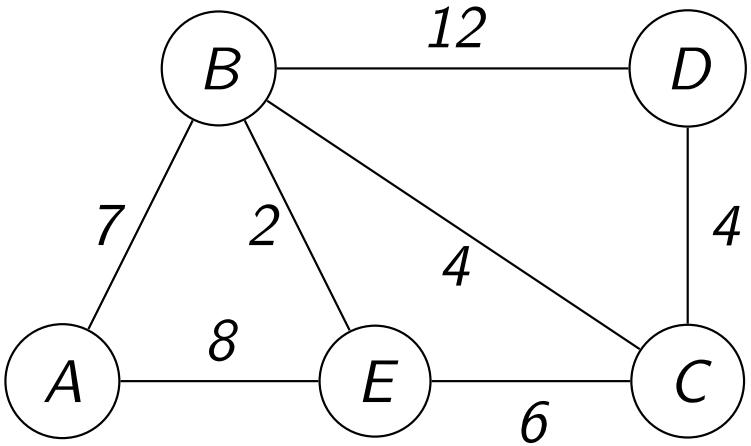


Schritt	Knoten	Knotenmenge	Kosten (B)	Kosten (C)	Kosten (D)	Kosten (E)
Initial	A	{A}	4	-	-	5
1	B	{A,B}	4	10	13	5
2	E	{A,B,E}	4	9	13	5
3	C	{A,B,E,C}	4	9	11	5
4	D	{A,B,E,C,D}	4	9	11	5

Kürzeste Wege und Dijkstra-Algorithmus

Übung 7.9

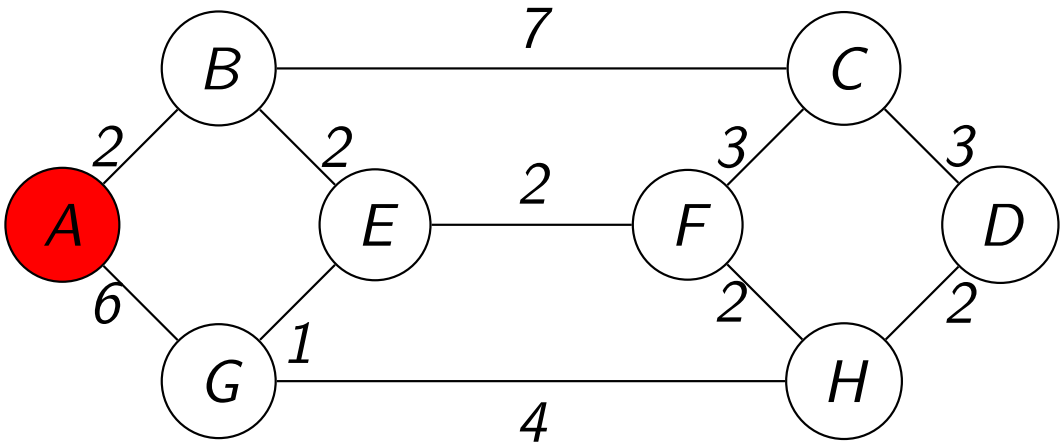
Geben Sie die kürzesten Pfade vom Knoten A zu allen anderen Knoten an.



Kürzeste Wege und Dijkstra-Algorithmus

Übung 7.10

Wenden Sie den Dijkstra-Algorithmus, um die kürzesten Wege von Router A zu allen anderen zu erhalten.



Endliche Mengen

Satz 8.1

Seien M und N zwei endliche Mengen. Dann gilt:

1. $M \cap N = \{\} \Rightarrow |M \cup N| = |M| + |N|$
2. $|M \times N| = |M| \cdot |N|$

Korollar 8.2

Seien $M_1, M_2, ..., M_n$ paarweise disjunkte endliche Mengen. Dann gilt:

1. $|\bigcup_{i=1}^{n} M_i| = \sum_{i=1}^{n} |M_i|$
2. $|M_1 \times M_2 \times \cdots \times M_n| = \prod_{i=1}^{n} |M_i|$

Endliche Mengen

Satz 8.3

Seien M eine Menge mit n Elementen. Dann gilt: $|M^k| = n^k$

Urnenexperimente

Definition 8.4 (Variation)

Zieht man aus einer Urne eine geordnete Stichprobe, spielt also die Reihenfolge in der gezogen wird eine Rolle, so spricht man von einer Variation

Beispiel (Hotelsafe)

Ein Hotelsafe hat eine Zahlenschloss, dass eine 4-stelligen Zahlencode mit den Ziffern 0..9 zulässt. Leider haben Sie Ihren Code vergessen. Wie oft müssen Sie im ungünstigsten Fall probieren, bis der Safe offen ist?

Urnenexperimente

Lösung

Es gibt 10 Ziffern, also $10 \cdot 10 \cdot 10 \cdot 10 = 10^4$ Möglichkeiten.

Man kann dies als Urnenexperiment auffassen. Es werden 4 Kugeln mit den Ziffern 0-9 mit Zurücklegen gezogen. Die Reihenfolge ist relevant, da der Code 1234 nicht gleich dem Code 4321 ist.

Anzahl der Variationen mit Wiederholung

Bei n Kugeln und k Zügen ergibt sich für die Anzahl der Variationen mit Wiederholung
$V_w(n; k) = n^k$

Urnenexperimente

Übung 8.1

Wie viel Zeichen kann man mit acht Bit codieren? Ein Bit kann nur die Werte 0 oder 1 annehmen.

Urnenexperimente

Übung 8.2

Wie viele 5-stellige Zahlen, die nur aus den Ziffern 0,1,2 oder 3 bestehen, können gebildet werden?

Permutationen

Beispiel (Stühle in einem Hörsaal)

In einem Hörsaal hat es 100 Plätze. Wie viele Möglichkeiten gibt es 100 Studenten auf diese 100 Plätze zu verteilen?

Zunächst wollen wir dies mal mit 4 Stühlen ausprobieren.
Die erste Person hat 4 Möglichkeiten auszuwählen, danach die zweite Person 3 Möglichkeiten, die dritte Person zwei Möglichkeiten und zum Schluss die letzte Person nur noch eine Möglichkeit. Insgesamt sind es also $4 \cdot 3 \cdot 2 \cdot 1 = 24$ Möglichkeiten.

Permutationen

Definition 8.5 (Permutation)

Eine Anordnung von n verschiedenen Elementen in einer bestimmten Reihenfolge heißt Permutation der Elemente.

Definition 8.6 (Fakultät (rekursiv))

Wir definieren nun

$$n! = \begin{cases} 1 & n = 0 \\ 1 & n = 1 \\ n \cdot (n-1)! & n > 1 \end{cases} \quad (\text{„Sprich: n Fakultät“})$$

Permutationen

Satz 8.7 (Anzahl der Permutationen)

Die Anzahl der Permutationen von n verschiedenen Elementen beträgt
$P(n) = n!$
Sind von n Elementen jeweils $n_1, n_2, \cdots, n_k$ *einander gleiche, so gilt*
$P(n; n_1, n_2, \cdots, n_k) = \frac{n!}{n_1! \cdot n_2! \cdots n_k!}$

Beispiel (Stühle in einem Hörsaal)

In einem Hörsaal hat es 100 Plätze. 100 Studenten können auf 100! verschiedene Möglichkeiten im Hörsaal Platz nehmen.

Permutationen

Beispiel (Farbige Kugeln)

Man hat 6 Kugeln, davon sind 3 Kugeln blau, 2 sind rot und eine Kugel ist weiß. Wie viele mögliche Anordnungen gibt es?

Lösung:

Es gibt $P(6;3,2,1) = \frac{6!}{3!2!1!} = 60$ mögliche Anordnungen.

Übung 8.3

Wie viele 5-stellige Zahlen kann man aus den Ziffern der Zahl 20132 bilden?

Inklusion und Exklusion

Satz 8.8

Seien M und N zwei beliebige endliche Mengen. Dann gilt

$$|M \cup N| = |M| + |N| - |M \cap N|$$

Satz 8.9

Seien M_1, M_2, M_3 drei beliebige endliche Mengen. Dann gilt

$$|M_1 \cup M_2 \cup M_3| =$$
$$|M_1|+|M_2|+|M_3|-|M_1 \cap M_2|-|M_1 \cap M_3|-|M_2 \cap M_3|+|M_1 \cap M_2 \cap M_3|$$

Inklusion und Exklusion

Beispiel

Man bestimme die Anzahl der natürlichen Zahlen zwischen 1 und 100, die durch 2,3 oder 5 teilbar sind.

Lösung:

$M_2 = \{2, 4, \ldots, 100\}, M_3 = \{3, 6, \ldots, 99\}, M_5 = \{5, 10, \ldots, 100\}.$
$|M_2| = 50, |M_3| = 33, |M_5| = 20, |M_2 \cap M_3| = 16, |M_2 \cap M_5| = 10, |M_3 \cap M_5| = 6, |M_2 \cap M_3 \cap M_5| = 3$

Also gilt: $|M_2 \cup M_3 \cup M_5| = 50 + 33 + 20 - 16 - 10 - 6 + 3 = 74$

Inklusion und Exklusion

Satz 8.10 (Prinzip der Inklusion und Exklusion, Siebformel)

Seien $M_1, M_2, \ldots M_n$ beliebige endliche Mengen. Dann gilt:

$$|\bigcup_{i=1}^{n} M_i| = \sum_{i=1}^{n} |M_i| - \sum_{1 \le i < j \le n} |M_i \cap M_j| + \sum_{1 \le i < j < k \le n} |M_i \cap M_j \cap M_k|$$

$$+ \cdots + (-1)^{n+1} |\bigcap_{i=1}^{n} M_i|$$

Inklusion und Exklusion

Übung 8.4

Wie viele durch 2,3,9 oder 11 teilbare Zahlen zwischen 1 und 200 gibt es?

Anzahl von Teilmengen

Satz 8.11 (Potenzmenge)

Die Potenzmenge einer n-elementigen Menge M hat 2^n Teilmengen.

Satz 8.12

Sei M eine Menge mit n Elementen. Dann beträgt die Anzahl der k-Tupel ($k \leq n$) aus verschiedenen Elementen dieser Menge

$$\prod_{i=1}^{n}(n-i+1) = n \cdot (n-1) \cdot \dots \cdot (n-k+1) = \frac{n!}{(n-k)!}$$

Anzahl von Teilmengen

Beispiel (Stühle)

Jetzt gibt es fünf Stühle, aber es kommen nur drei Personen. Wie viele Möglichkeiten gibt es für diese drei Personen auf den Stühlen Platz zu nehmen?

Lösung:

Die erste Person hat 5 Möglichkeiten, die zweite Person hat 4 Möglichkeiten und die dritte Person hat 3 Möglichkeiten. Also gibt es insgesamt $5 \cdot 4 \cdot 3 = 60$ Möglichkeiten.

Wie könnte man dies durch Fakultäten ausdrücken ?

$5 \cdot 4 \cdot 3 = \frac{5 \cdot 4 \cdot 3 \cdot 2 \cdot 1}{2 \cdot 1} = \frac{5!}{2!} = \frac{5!}{(5-3)!}$

Anzahl von Teilmengen

Anzahl der Variationen ohne Wiederholung

Bei n Kugeln und k Zügen ergibt sich für die Anzahl der Variationen ohne Wiederholung

$V(n;k) = \frac{n!}{(n-k)!}$

Übung 8.5

Beim Pferderennen sollen von acht Pferden der Einlauf der ersten drei Pferde in der richtigen Reihenfolge getippt werden. Wie viele Wettmöglichkeiten gibt es?

Anzahl von Teilmengen

Satz 8.13

Sei M eine Menge mit n Elementen. Dann beträgt die Anzahl der k-elementigen Teilmengen mit $(k \leq n)$

$$\frac{\prod_{i=1}^{n}(n-i+1)}{k!} = \frac{n!}{k!(n-k)!}$$

Definition 8.14 (Binomialkoeffizient)

Wir definieren den Binomialkoeffizient (n über k) durch

$$\binom{n}{k} = \frac{n!}{k! \cdot (n-k)!}$$

Anzahl von Teilmengen

Anzahl der Kombinationen ohne Wiederholung

Bei n Kugeln und k Zügen ergibt sich für die Anzahl der Kombinationen ohne Wiederholung
$C(n;k) = \binom{n}{k}$

Eigenschaften des Binomialkoeffizienten

$$\binom{n}{0} = \binom{n}{n} = 1 \tag{1}$$

$$\binom{n}{n-1} = n \tag{2}$$

$$\binom{n}{k} = \binom{n}{n-k} \tag{3}$$

Anzahl von Teilmengen

Übung 8.6

Wie viele natürliche Zahlen kleiner 3000 gibt es, bei denen jede Ziffer nur einmal vorkommen darf?

(A) 1008
(B) 1747
(C) 1512
(D) 1939

Anzahl von Teilmengen

Übung 8.7

Gegeben sei die Menge $\{a, b, c, d, e, f\}$. Bilde alle 4-elementige Teilmengen und vergleiche mit dem Binomialkoeffizienten.

Anzahl von Teilmengen

Übung 8.8

Beweise die folgende Formel:

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

Anzahl von Teilmengen

Satz 8.15 (Binomischer Lehrsatz)

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

Anzahl von Teilmengen

Satz 8.16 (Sterlingsche Formel)

Für alle natürlichen Zahlen n gilt:

$$\sqrt{2\pi n} \cdot \left(\frac{n}{e}\right)^n \leq n! \leq \sqrt{2\pi n} \cdot \left(\frac{n}{e}\right)^{n+\frac{1}{12\pi}}$$

Satz 8.17

Für alle natürlichen Zahlen n, mit $1 \leq k \leq n$ gilt:

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

Permutationen

Definition 8.18

Sei $M = \{1, \ldots, n\}$ für eine natürlichen Zahl $n \geq 1$.
Eine bijektive Abbildung $f : M \to M$ heißt Permutation.

Die Abbbildungstabelle lautet:

$$f = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ f(1) & f(2) & f(3) & \ldots & f(n) \end{pmatrix}$$

Wir nennen dies Permutationstabelle

Permutationen

Beispiel einer Permutation

Permutation einer 8-elementigen Menge

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 6 & 4 & 7 & 2 & 8 & 1 & 5 \end{pmatrix}$$

Bei kleinen Mengen kann auch die Anordnungsschreibeweise verwendet werden, indem man auf die Indizes verzichtet. Es ergibt sich damit:

$f = 3\ 6\ 4\ 7\ 2\ 8\ 1\ 5$

Permutationen

Definition 8.19 (Zyklus)

Ein Zyklus beginnt mit einem beliebigen Zahl. Das nächste Element ist immer Bild des vorangegangenen Elements und wird geschlossen, wenn das erste Element wieder als Bild auftaucht.

Bei dem obenstehenden Beispiel lassen sich zwei Zyklen erkennen. Diese werden immer in Klammern geschrieben:
$f = (1\ 3\ 4\ 7)\,(2\ 6\ 8\ 5)$

Permutationen

Übung 8.9

Finden Sie die Zyklenschreibweise für die folgende Permutation.

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 6 & 5 & 4 & 1 & 2 & 3 & 5 \end{pmatrix}$$

Permutationen

Beispiel einer Komposition

$$f_3 = f_1 \circ f_2 =$$
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 6 & 5 & 4 & 1 & 2 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 5 & 7 & 1 & 2 & 6 \end{pmatrix}$$
$$= (1\,7\,3\,5)\,(2\,6) \circ (1\,3\,5)\,(2\,4\,7\,6)$$
$$= (1\,5\,7\;\;2\,4\,3) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 4 & 1 & 3 & 7 & 6 & 2 \end{pmatrix}$$

Permutationen

Definition 8.20 (Transposition)

Ein Transposition ist ein Zyklus, der aus zwei Elementen besteht.

Satz 8.21

Jede Permutation kann in eine Hintereinanderschaltung von Transpositionen zerlegt werden.
Es gelten die folgenden Punkte

1. *Die Zerlegung ist nicht eindeutig*
2. *Die Anzahl der Transpositionen ist nicht eindeutig festgelegt*
3. *Jede Anzahl von Transpositionen hat immer den gleichen Rest (modulo 2)*

Permutationen

Beispiel einer Transposition

$f = (1; 3\ 5)\,(2\ 4\ 7\ 6) = (1\ 5)\,(1\ 3)\,(2\ 6)\,(2\ 7)\,(2\ 4)$

Definition 8.22

Eine Permutation heißt gearde, wenn sie in eine gearde Anzahl von Transpositionen zerlegt werden kann,andernfalls heißt sie ungerade.

Permutationen

Satz 8.23

1. *Ein Zyklus ist genau dann gerade, wenn er aus einer ungeraden Anzahl von Elementen besteht.*
2. *Eine Permutation ist genau dann gerade, wenn sie aus einer geraden Anzahl von ungeraden Zyklen besteht.*

Beispiel

Die Permutation

$f = (1\ 7\ 3\ 5)\,(2\ 6) \circ (1\ 3\ 5)\,(2\ 4\ 7\ 6)$

besteht aus 3 ungeraden Zyklen und einem geradem Zyklus, ist also insgesamt ungerade.

Permutationen

Übung 8.10

Gegeben sei die Permutation $f = (2\ 5\ 4\ 3)\,(9\ 7)(1\ 6\ 8)$

1. *Ermitteln Sie die Permutationstabelle.*
2. *Geben Sie eine Zerlegung in Transpositionen an.*
3. *Ist die Permutation gerade oder ungerade?*

Permutationen

Übung 8.11

Gegeben sei die Permutation
$f = (20\ 2\ 5\ 4)\,(12\ 10\ 13)\,(19\ 3\ 9\ 7\ 15)\,(11\ 14\ 17)\,(1\ 16\ 6\ 8\ 18)$

Ist diese Permutation gerade?

Permutationen

Satz 8.24

Die Menge S_n der Permutationen einer n-elementigen Menge bildet mit der Komposition als Verknüpfung eine Gruppe $(S_n, \circ)$. Sie wird die symmetrische Gruppe genannt.

Übung 8.12

Geben Sie alle Elemente der Gruppe $(S_3, \circ)$ an und erstellen die Verknüpfungstabelle.

Permutationen

Satz 8.25

- *Die Gruppe $(S_n, \circ)$ enthält die Gruppe aller Symmetrien eines regelmäßigen n-Ecks, ist aber nur für $n = 3$ zu dieser isomorph.*
- *Die Gruppe $(S_n, \circ)$ ist für $n > 2$ nicht kommutativ.*
- *Die Menge der geraden Permutationen bildet eine Untergruppe $(A_n \circ)$. welche genau aus der Hälfte aller Elemente von $(S_n . \circ)$ besteht. Sie heißt die alternierende Gruppe*

Permutationen

Übung 8.13

Untersuchen Sie die Gruppe S_4

1. *Schreiben Sie alle Elemente in Zyklendarstellung auf und markieren die Elemente von* A_n.
2. *Die Gruppe* $(S_n, \circ)$ *ist für* $n > 2$ *nicht kommutativ.*
3. *Geben Sie zu den Elementen* $(1\ 3\ 2\ 4)$ *und* $(1\ 3)\,(2\ 4)$ *die Inversen an.*
4. *Zeigen Sie an den Elementen von 2, dass in* S_4 *das Kommutativgesetz nicht gilt.*

Permutationen

Übung 8.14

Untersuchen Sie die Gruppe S_5

1. *Geben Sie an, wie viele Elemente diese Gruppe hat.*
2. *Geben Sie ein Element maximaler Ordnung an, Weisen Sie die Ordnung explizit nach.*

Permutationen

Satz 8.26 (Satz von Cayley)

Jede endliche Gruppe ist zu einer Untergruppe von $(S_n, \circ)$ *isomorph.*

Permutationen

Definition 8.27 (GL=general linear group)

Sei K ein Körper, dann bildet die Menge der invertierbaren n x n - Matrizen

$$GL_n(K) = \{A \in Mat_n(K) | det(A) \neq 0\}$$

eine Gruppe, wenn man die Matrizenmultiplikation als Verknüpfung verwendet.

Permutationen

Übung 8.15

Zeigen Sie, dass $SL_2(K) = \{A \in GL_n(K) | det(A) = 1\}$ *eine Untergruppe von* $GL_n(K)$ *ist.*

Übung 8.16

Bestimmen Sie $|GL_2(\mathbb{Z}_2)|$ *indem Sie alle Elemente aufzählen. Geben Sie auch die Ordnung aller Elemente an.*

Summenzeichen

Das Summenzeichen ist definiert durch:

$$\sum_{i=1}^{n} x_i = x_1 + x_2 + \cdots + x_n$$

Distributivgesetz

$$\sum_{i=1}^{n} r \cdot x_i = r \cdot \sum_{i=1}^{n} x_i$$

Konstanten

$$\sum_{i=1}^{n} c = n \cdot c$$

Summenzeichen

Addition

$$\sum_{i=1}^{n} x_i + y_i = \sum_{i=1}^{n} x_i + \sum_{i=1}^{n} y_i$$

LÖSUNGSTEIL

Lösung

Lösung zu Übung 1.1

$R = \{(2,4);(2,6);(3;6)\}$

Lösung

Lösung zu Übung 1.2

1.reflexiv:

$a - a = 0$ ist durch 5 teilbar, also $a \sim a$

2.symmetrisch

$a \sim b \Leftrightarrow \exists\, r \in \mathbb{Z} : b - a = 5 \cdot r \Leftrightarrow 5 \cdot (-r) = a - b \Leftrightarrow b \sim a$

3. transitiv:

$a \sim b \wedge b \sim c \Leftrightarrow \exists\, r, s \in \mathbb{Z} : b - a = 5 \cdot r \wedge c - b = 5 \cdot s \Leftrightarrow$
$c - a = r(r + s) \Leftrightarrow c \sim a$

Lösung Übung 1.4

- einstellige Zahlen (Ziffern): 10
- zweistellige Zahlen: $9 \cdot 9 = 81$
- dreistellige Zahlen: $9 \cdot 9 \cdot 8 = 648$
- vierstellige Zahlen: $2 \cdot 9 \cdot 8 \cdot 7 = 1008$

Es ergeben sich also 1747 mögliche Zahlen.