

# Diskrete Mathematik | DMI

## Zusammenfassung

---

## INHALTSVERZEICHNIS

<b>1. Aussagenlogik</b>	<b>2</b>
1.1. Glossar	2
1.2. Formeln	2
1.3. Rechenregeln	3
<b>2. Prädikatenlogik</b>	<b>3</b>
2.1. Glossar	3
<b>3. Beweisen</b>	<b>3</b>
3.1. Induktion	3
3.1.1. Techniken	4
<b>4. Direkte, iterative und rekursive Berechnungen</b>	<b>4</b>
4.1. Glossar	4
<b>5. Mengen</b>	<b>4</b>
5.1. Glossar	4
5.2. Rechenregeln	4
<b>6. Formeln, Abbildungen, Relationen</b>	<b>5</b>
6.1. Glossar	5
<b>7. Modulo-Rechnen</b>	<b>5</b>
7.1. Glossar	6
7.2. Rechenregeln	6
7.3. Primfaktorenzerlegung	6
7.4. Euklidischer Algorithmus	6
7.4.1. Beispiel	6
7.5. Erweiterter Euklidischer Algorithmus	7
7.5.1. Beispiel	7
7.6. Kleiner Fermat	7
7.7. Satz von Euler	7
7.7.1. Euler'sche $\varphi$ -Funktion (Totient)	7
7.7.1.1. Rechenregeln	8
7.8. RSA Verschlüsselung	8

# 1. AUSSAGENLOGIK

## 1.1. GLOSSAR

<i>Begriff</i>	<i>Bedeutung</i>
Aussage	<ul style="list-style-type: none"> <li>– Feststellender Satz, dem eindeutig «wahr» oder «falsch» zugeordnet werden kann</li> <li>– Symbole wie <b>A, B, C...</b> werden dafür verwendet</li> </ul>
Aussagenlogische Form	– Kombination von Aussagen, verknüpft durch Junktoren
Aussageform	– Aussagen verknüpft mit Variablen
Normalform	– Standardisierte Aussagenlogische Formen (Formeln)
Negationsnormalform	– $\neg$ steht ausschliesslich direkt vor Aussagen oder Konstanten
Verallgemeinerte Disjunktion	<ul style="list-style-type: none"> <li>– Einzelne Aussage oder Negation</li> <li>– wahr oder falsch</li> <li>– Disjunktion <math>A \vee B</math>, falls <b>A</b> und <b>B</b> selbst verallgemeinerte Disjunktionen sind</li> </ul>
Verallgemeinerte Konjunktion	<ul style="list-style-type: none"> <li>– Einzelne Aussage oder Negation</li> <li>– wahr oder falsch</li> <li>– Konjunktion <math>A \wedge B</math>, falls <b>A</b> und <b>B</b> selbst verallgemeinerte Konjunktionen sind</li> </ul>
Disjunktive Normalform	– Disjunktion von (oder eine einzelne) verallgemeinerten Konjunktionen
Konjunktive Normalform	– Konjunktion von (oder eine einzelne) verallgemeinerten Disjunktionen
Kontradiktion	– Immer falsch
Tautologie	– Immer wahr
Junktoren (/Konnektoren)	<ul style="list-style-type: none"> <li>– <math>\neg</math> Negation</li> <li>– <math>\wedge</math> Konjunktion</li> <li>– <math>\vee</math> Disjunktion (einschliessliches oder!)</li> <li>– <math>\Rightarrow</math> Implikation</li> <li>– <math>\Leftrightarrow</math> Äquivalenz</li> </ul>
Abtrennungsregel	– $(A \wedge (A \Rightarrow B)) \Rightarrow B$
Bindungsstärke	– $\neg$ vor $\wedge, \vee$ vor $\Rightarrow, \Leftrightarrow$

## 1.2. FORMELN

$$(A \Rightarrow B) \Leftrightarrow (\neg B \Rightarrow \neg A)$$

$$(A \Rightarrow B) \Leftrightarrow (\neg A \vee B)$$

$$(A \Leftrightarrow B) \Leftrightarrow (A \wedge B) \vee (\neg A \wedge \neg B)$$

$$\neg(A \Rightarrow B) \Leftrightarrow A \wedge \neg B$$

$$A \vee (\neg A \wedge B) \Leftrightarrow A \vee B$$

$$\text{Abtrennungsregel: } A \wedge (A \Rightarrow B) \Rightarrow B$$

### 1.3. RECHENREGELN

Begriff	Bedeutung
Kommutativität	$-(A \wedge B) \Leftrightarrow (B \wedge A)$ $-(A \vee B) \Leftrightarrow (B \vee A)$
Assoziativität	$-(A \wedge (B \wedge C) \Leftrightarrow (A \wedge B) \wedge C)$ $-(A \vee (B \vee C) \Leftrightarrow (A \vee B) \vee C)$
Distributivität	$-(A \wedge (B \vee C) \Leftrightarrow (A \wedge B) \vee (A \wedge C))$ $-(A \vee (B \wedge C) \Leftrightarrow (A \vee B) \wedge (A \vee C))$
Absorption	$-(A \vee (A \wedge B) \Leftrightarrow A)$ $-(A \wedge (A \vee B) \Leftrightarrow A)$
Idempotenz	$-(A \vee A = A)$ $-(A \wedge A = A)$
Doppelte Negation	$-(\neg(\neg A) \Leftrightarrow \neg\neg A \Leftrightarrow A)$
Konstanten	$-W=\text{wahr}$ $-F=\text{falsch}$
???	$-(A \Rightarrow B \Rightarrow C) \Leftrightarrow (A \Rightarrow B) \wedge (B \Rightarrow C)$
de Morgan	$-(\neg(A \wedge B) \Leftrightarrow \neg A \vee \neg B)$ $-(\neg(A \vee B) \Leftrightarrow \neg A \wedge \neg B)$

## 2. PRÄDIKATENLOGIK

### 2.1. GLOSSAR

Begriff	Bedeutung
Subjekt	«Konkretes Ding» / Stellvertreter einer Variable
Prädikat	$-(\text{«Eigenschaft»}, \text{zB «ist eine Primzahl»})$ $-(\text{Prädikate werden oft wie Funktionen geschrieben. Ist } P \text{ ein Prädikat, dann bedeutet } P(x), \text{ dass } x \text{ das Prädikat erfüllt. } P(x) \text{ ist eine Aussageform.})$
Quantor	$-(\forall \text{ Allquantor (Für alle)})$ $-(\exists \text{ Existenzquantor (Es existiert)})$

## 3. BEWEISEN

### TODO: MEHR BEWEISE

### 3.1. INDUKTION

$$A(1) \wedge (A(n) \Rightarrow A(n+1)) \Rightarrow A(m), m \in \mathbb{N}$$

Beispiel:  $2 \mid (6^n)$

- 1) Verankerung:  $n = 0$ 
  - $- 2 \mid (6^0)$
- 2) Induktionsschritt  $n \rightarrow n+1$ 
  - $- 2 \mid (6^{n+1})$ 
    - a) Induktionsannahme:  $2 \mid (6^n)$
    - b) Behauptung:  $2 \mid (6^{n+1})$

c) Beweis: Verwendung der Annahme, um Richtigkeit der Behauptung zu zeigen

### 3.1.1. Techniken

- 1) Direkter Beweis  $f(n) = f_1(n) = f_2(n) = \dots = f_m(n) = g(n)$
- 2) Differenz gleich Null  $f(n) - g(n) = 0 \Rightarrow f(n) = g(n)$
- 3) Äquivalenzumformung
- 4) Dritte Grösse (vereinfachen)  $g(n) = h(n) = f(n)$

## 4. DIREKTE, ITERATIVE UND REKURSIVE BERECHNUNGEN

### 4.1. GLOSSAR

Begriff	Bedeutung
Folge	– Nummerierte Liste von Objekten (Folgegliedern)
Reihe	– Summe von Folgegliedern einer Zahlenfolge

## 5. MENGEN

### 5.1. GLOSSAR

Begriff	Bedeutung
Aufzählend	– $\{1, 2, 3\}$
Beschreibend	– $\{x \in \mathbb{N}^+ \mid x < 4\}$
Mächtigkeit	– Anzahl Elemente einer Menge – $ M $
Potenzmenge	– Menge aller Teilmengen einer Menge – $P(M)$ – $ P(M)  = 2^{ M }$
Kartesisches Produkt	– $A \times B = \{(a, b) \mid a \in A, b \in B\}$

### 5.2. RECHENREGELN

Für die Mengen A und B in der Obermenge M gelten die folgenden Aussagen:

$$\overline{\overline{A}} = A$$

$$A \cap \overline{A} = \emptyset$$

$$A \cup \overline{A} = M$$

$$\overline{A \cap B} = \overline{A} \cup \overline{B}$$

$$\overline{A \cup B} = \overline{A} \cap \overline{B}$$

## 6. FORMELN, ABBILDUNGEN, RELATIONEN

### 6.1. GLOSSAR

Begriff	Bedeutung
Funktion/Abbildung	<ul style="list-style-type: none"> <li>– Zuordnung, die jedem Element der Definitionsmenge <math>D</math> genau ein Element einer Zielmenge <math>Z</math> zuordnet.</li> <li>– Injektive Relation</li> <li>– <math>f : D \rightarrow Z</math></li> <li>– Abbildungen mit mehreren Argumenten: <math>f : A \times B \rightarrow Z, f(a, b) = y</math></li> </ul>
Graph	<ul style="list-style-type: none"> <li>– Menge von Paaren <math>(x, f(x))</math></li> <li>– <math>G \in D \times Z</math></li> </ul>
Relation	<ul style="list-style-type: none"> <li>– Teilmenge des Kartesischen Produktes mehrerer Mengen</li> <li>– <math display="block">A = \prod_{i=1}^n A_i,  A_i  = n_i \Rightarrow  A  = \prod_{i=1}^n n_i</math></li> <li>– Kleiner-Relation: <math>R_{&lt;} = \{(a, b) \mid a \in A, b \in B, a &lt; b\}</math></li> <li>– Gleich-Relation: <math>R_{=} = \{(a, b) \mid a \in A, b \in B, a = b\}</math></li> <li>– Kleiner-Gleich-Relation: <math>R_{\leq} = R_{=} \cup R_{&lt;} = \{(a, b) \mid a \in A, b \in B, a \leq b\}</math></li> </ul>
Surjektiv	– Alle Elemente der Definitions- und Zielmenge sind «verknüpft» / jedes Element der Bildmenge kommt als Bild vor
Injektiv	<ul style="list-style-type: none"> <li>– Alle Inputs haben eindeutige Outputs</li> <li>– <math>a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2)</math></li> </ul>
Bijektiv	– Surjektiv und Injektiv
Reflexiv	<ul style="list-style-type: none"> <li>– Alle Elemente von <math>A</math> stehen zu sich selbst in Beziehung</li> <li>– <math>a \in A \Rightarrow (a, a) \in R</math></li> <li>– <math>A \Leftrightarrow A</math></li> </ul>
Symmetrisch	<ul style="list-style-type: none"> <li>– <math>(a, b) \in R \wedge (b, a) \in R</math></li> <li>– <math>(A \Leftrightarrow B) \Leftrightarrow (B \Leftrightarrow A)</math></li> </ul>
Transitiv	<ul style="list-style-type: none"> <li>– <math>(a, b) \in R \wedge (b, c) \in R \Rightarrow (a, c) \in R</math></li> <li>– <math>(A \Leftrightarrow B) \wedge (B \Leftrightarrow C) \Rightarrow (A \Leftrightarrow C)</math></li> </ul>
Äquivalenzrelation	<ul style="list-style-type: none"> <li>– reflexiv, symmetrisch und transitiv</li> <li>– <math>\Leftrightarrow, =</math></li> </ul>
Irreflexiv	– $a \in A \Rightarrow \neg(a, a) \in R$
Asymmetrisch	– $(a, b) \in R \Rightarrow \neg(b, a) \in R$
Antisymmetrisch	– $((a, b) \in R) \wedge ((b, a) \in R) \Rightarrow a = b$
Ordnungsrelation	<ul style="list-style-type: none"> <li>– reflexiv, antisymmetrisch und transitiv</li> <li>– <math>\leq</math></li> </ul>
Symmetrische Differenz	<ul style="list-style-type: none"> <li>– <math>A \Delta B = \{x \in G \mid (x \in A \cup B) \wedge \neg(x \in A \cap B)\}</math></li> <li>– <math>A \Delta B = (A \cup B) \setminus (A \cap B)</math></li> <li>– <math>(A \Delta B) \Delta C = A \Delta (B \Delta C)</math></li> </ul>

## 7. MODULO-RECHNEN

Die Modulo-Relation ist eine **Äquivalenzrelation** auf  $\mathbb{Z}$ .

## 7.1. GLOSSAR

Begriff	Bedeutung
Teiler-Relation	<ul style="list-style-type: none"> <li>Für <math>a, b \in \mathbb{Z}</math> ist die Teiler-Relation <math>b \mid a \Leftrightarrow T(b, a) \Leftrightarrow \exists q \in \mathbb{Z} : bq = a</math></li> <li><math>b \mid a \Leftrightarrow -b \mid a</math></li> <li><math>b \mid a \Leftrightarrow b \mid -a</math></li> <li>Ordnungsrelation auf <math>\mathbb{N}</math></li> </ul>
Modulo-Relation	Für $a, q, r \in \mathbb{Z}$ ist die Modulo-Relation $R_q(a, r) \Leftrightarrow q \mid a - r \Leftrightarrow a \equiv r \pmod{q}$
$\sim$	<ul style="list-style-type: none"> <li>«relates to»</li> <li><math>a \sim b \Leftrightarrow (a, b) \in R</math></li> </ul>
Quotient, Rest	Zu jeder Zahl $a \in \mathbb{Z}$ und jeder Zahl $b \in \mathbb{Z}$ gibt es eindeutig bestimmte Zahlen $q, r \in \mathbb{Z}$ mit $a = q * b + r, 0 \leq r < b$ Bsp: $7 = 2 * 3 + 1$ $q$ heisst <b>Quotient</b> $r$ heisst <b>Rest</b>
Restklassen	<ul style="list-style-type: none"> <li><math>[b]_q = \{a \in \mathbb{Z} \mid a \equiv b \pmod{q}, q &gt; 0\}</math></li> <li><math>\mathbb{Z}_q = \{[0]_q, [1]_q, [2]_q, \dots, [q-1]_q\} = \underbrace{\{0, 1, 2, 3, \dots, q-1\}}_{\text{Vereinfachung}}</math></li> </ul>
Multiplikatives Inverses	Für $a \in \mathbb{Z}_q$ ist $b \in \mathbb{Z}_q$ das <b>multiplikative inverse</b> von $a$ , wenn $a * b \equiv 1 \pmod{q}$
Nullteiler	Wenn für $a, b \in \mathbb{Z}_q : ab \equiv 0 \pmod{q}$ und $a \not\equiv 0 \pmod{q} \wedge b \not\equiv 0 \pmod{q}$ , heissen $a, b$ <b>Nullteiler</b>

## 7.2. RECHENREGELN

- $(a + b) \pmod{n} = ((a \pmod{n}) + (b \pmod{n})) \pmod{n}$
- $(a - b) \pmod{n} = ((a \pmod{n}) - (b \pmod{n})) \pmod{n}$
- $(a * b) \pmod{n} = ((a \pmod{n}) * (b \pmod{n})) \pmod{n}$
- $a^d \pmod{n} = (a^{d-x} * a^x) \pmod{n} = ((a^{d-x} \pmod{n}) * (a^x \pmod{n})) \pmod{n}$

## 7.3. PRIMFAKTORENZERLEGUNG

Begriff	Bedeutung
$\text{ggT}(a, b)$	$\max\{d \in \mathbb{N} \mid d \mid a \wedge d \mid b\}$
$\text{kgV}(a, b)$	<ul style="list-style-type: none"> <li><math>\min\{m \in \mathbb{N} \mid a \mid m \wedge b \mid m\}</math></li> <li><math>\frac{ab}{\text{ggT}(a, b)}</math></li> </ul>
Teilerfremd	<ul style="list-style-type: none"> <li>Zwei Zahlen <math>a, b \in \mathbb{N}</math> heissen <b>Teilerfremd</b>, wenn <math>\text{ggT}(a, b) = 1</math></li> <li>Sei <math>p \in \mathbb{N}</math> eine Primzahl und <math>q \in \mathbb{N}, q &lt; p, q \neq 0</math> dann ist <math>\text{ggT}(p, q) = 1</math></li> </ul>

## 7.4. EUKLIDISCHER ALGORITHMUS

Seien  $a, b \in \mathbb{N}, a \neq b, a \neq 0, b \neq 0$

Initialisierung: Setze  $x := a, y := b$  und  $q := x, r := x - q * y$  (d.h. bestimme  $q$  und  $r$  so, dass  $x = q * y + r$  ist)

Wiederhole bis  $r = 0$  ist

Ergebnis:  $y = \text{ggT}(a, b)$

### 7.4.1. Beispiel

$\text{ggT}(122, 72), a = 122, b = 72$

– Init:  $x_0 = a = 122, y_0 = b = 72$

– Iteration:

	$x_i = y_{i-1}$	$y_i = r_{i-1}$	$q_i = x_i \text{ div } y_i$	$r_i = x_i \bmod y_i = x_i - q_i * y_i$
$i = 0$	122	72	1	50
$i = 1$	72	50	1	22 Muster: $r_{i+1} < r_i$
$i = 2$	50	22	2	6
$i = 3$	22	6	3	4
$i = 4$	6	4	1	2
$i = 5$	4	$2 = \text{ggT}(122, 72)$	2	0 (immer 0 am Schluss)

## 7.5. ERWEITERTER EUKLIDISCHER ALGORITHMUS

Seien  $a, b \in \mathbb{N}, a \neq b, a \neq 0, b \neq 0$

Initialisierung: Setze  $x := a, y := b, q := x \div y, r := x - q * y, (u, s, v, t) = (1, 0, 0, 1)$  (d.h. bestimme  $q$  und  $r$  so, dass  $x = q * y + r$  ist)

Wiederhole bis  $r = 0$  ist

Ergebnis:  $y = \text{ggT}(a, b) = s * a + t * b$

Wenn  $\text{ggT}(a, b) = 1$  ist, dann folgt:  $t * v \equiv 1 \bmod a$

### 7.5.1. Beispiel

$\text{ggT}(99, 79)$

$i$	$x = y_{-1}$	$y = r_{-1}$	$q = x \div y$	$r = x_i - q_i * y_i$	$u = s_{-1}$	$s = u_{-1} - q_{-1} * s_{-1}$	$v = t_{-1}$	$t = v_{-1} - q_{-1} * t_{-1}$
$i = 0$	99	79	1	20	1	0	0	1
$i = 1$	79	20	3	19	0	1	1	-1
$i = 2$	20	19	1	1	1	-3	-1	4
$i = 3$	19	1	19	0	-3	4	4	-5

Daraus folgend:

- $\text{ggT}(99, 79) + 1 + 4 * 99 + (-5) * 79 \Leftrightarrow 396 - 395 = 1$
- $-5$  ist mult. Inv. von  $79$  in  $\mathbb{Z}_{99}$
- $4$  ist mult. Inv. von  $99$  in  $\mathbb{Z}_{79}$

## 7.6. KLEINER FERMAT

Sei  $p \in \mathbb{N}$  eine Primzahl und  $x \in \mathbb{Z} \setminus \{0\}$  mit  $\text{ggT}(x, p) = 1$

Dann ist:  $x^{p-1} \equiv 1 \bmod p$

Daraus folgend:

$$\begin{aligned}
 x^{p-1} &\equiv 1 \bmod p & | \quad ()^n \\
 \Leftrightarrow x^{n(p-1)} &\equiv 1 \bmod p & | \quad * x \\
 \Leftrightarrow x^{1+n(p-1)} &\equiv x \bmod p \\
 \Leftrightarrow x^{1 \bmod (p-1)} &\equiv x \bmod p
 \end{aligned}$$

## 7.7. SATZ VON EULER

Sei  $n \in \mathbb{N} \setminus \{0\}$  und  $z \in \mathbb{Z}$  mit  $\text{ggT}(z, n) = 1$ . Dann ist  $z^{\varphi(n)} \equiv 1 \bmod n$ .

### 7.7.1. Euler'sche $\varphi$ -Funktion (Totient)

Sei  $n \in \mathbb{N} \setminus \{0\}$  und  $\mathbb{Z}_n^* = \{x \in \mathbb{Z}_n \mid x \text{ hat ein multiplikatives Inverses in } \mathbb{Z}_n\}$ . Dann heisst  $\varphi(n)$ :

$$\begin{aligned}
 \varphi(n) &= \text{Anz. Elemente in } \mathbb{Z}_n \text{ mit mult. Inversen} \\
 &= \text{Anz. Zahlen } 1 \leq q \leq n \text{ mit } \text{ggT}(q, n) = 1 \\
 &= |\mathbb{Z}_n^*|
 \end{aligned}$$

Falls  $p$  Primzahl ist, dann ist  $\varphi(p) = p - 1$

#### 7.7.1.1. Rechenregeln

- 1) Sei  $n \in \mathbb{N}$  eine Primzahl, dann  $\varphi(n) = n - 1$
- 2) Sei  $n \in \mathbb{N}$  eine Primzahl und  $p \in \mathbb{N} \setminus \{0\}$ , dann  $\varphi(n^p) = n^{p-1} * (n - 1)$
- 3) Seien  $m, n \in \mathbb{N} \setminus \{0\}$  und  $\text{ggT}(m, n) = 1$ , dann  $\varphi(n * m) = \varphi(n) * \varphi(m)$

#### 7.8. RSA VERSCHLÜSSELUNG

- 1) Wähle 2 Primzahlen  $p, q$
- 2) Berechne  $n = p * q$
- 3) Berechne  $\varphi(n) = (p - 1)(q - 1)$
- 4) Wähle  $a, b$  so, dass  $a * b \equiv 1 \pmod{\varphi(n)}$
- 5) Vergesse  $p, q, \varphi(p * q)$ . Brauchen wir nicht und riskieren nur, dass uns jemand hackt

Public key ist nun  $n, b$ , Private key ist  $n, a$

Sidenote: Fürs Alphabet muss  $n$  grösser sein als 26