1 Grundbegriffe und elementare Logik

Aussage

Unter einer Aussage wollen wir ein «sprachliches Gebilde» verstehen, welchem zumindest im Prinzip ein Wahrheitswert «wahr» oder «falsch» zugeordnet werden kann.

Prädikat

Ein Prädikat ist im Wesentlichen eine Aussage, die freie Variablen enthält.
Aussagen sind 0-stellige Prädikate. Aussage mit N freien Variablen sind N-stellige Prädikate.

Junktoren

Zeichen	Prädikat	Bezeichnung
¬	$\neg A$	NICHT A
∧	$A \wedge B$	A UND B
∨	$A \vee B$	A ODER B
⇒	$A \Rightarrow B$	WENN A DANN B
⇔	$A \Leftrightarrow B$	A GLEICH B

Quantoren

Zeichen	Bezeichnung	Beispiel
∀	Allquantor	$\forall x\, A(x)$
∃	Existenzquantor	$\exists x\, A(x)$

Junktor Regeln

Doppelte Negation	$\neg\neg A$	$\Leftrightarrow A$
Kommutativität	$A \wedge B$ $A \vee B$	$\Leftrightarrow B \wedge A$ $\Leftrightarrow B \vee A$
Assoziativität	$(A \wedge B) \wedge C$ $(A \vee B) \vee C$	$\Leftrightarrow A \wedge (B \wedge C)$ $\Leftrightarrow A \vee (B \vee C)$
Distributivität	$A \wedge (B \vee C)$ $A \vee (B \wedge C)$	$\Leftrightarrow (A \wedge B) \vee (B \wedge C)$ $\Leftrightarrow (A \vee B) \wedge (B \vee C)$
De Morgan	$\neg(A \wedge B)$ $\neg(A \vee B)$	$\Leftrightarrow \neg A \vee \neg B$ $\Leftrightarrow \neg A \wedge \neg B$

Quantor Regeln

Vertauschungsregel	$\forall x\, A(x)$	$\Leftrightarrow \neg\exists x\, \neg A(x)$
Vertauschungsregel	$\forall x \in K\, A(x)$	$\Leftrightarrow \neg\exists x \in K\, \neg A(x)$
Allquantor	$\forall x \in K\, A(x)$	$\Leftrightarrow \forall x(x \in K \Rightarrow A(x))$
Existenzquantor	$\exists x \in K\, A(x)$	$\Leftrightarrow \exists x(x \in K \wedge A(x))$

Schlussfolgerungen

- $A \Rightarrow B \Leftrightarrow \neg A \vee B$
- $A \Rightarrow B \Leftrightarrow \neg B \Rightarrow \neg A$

Beispiele

- Existiert genau ein: $\exists!\, x(A(x)) = \underbrace{\exists x(A(x))}_{mind\ eins} \wedge \underbrace{\forall y, z(A(y) \wedge A(z) \Rightarrow y = z)}_{nicht\ zwei}$

2 Syntax und Semantik

Äquivalente Formeln werden folgendermassen geschrieben: $F \equiv G$

Literale sind atomare Formeln oder negierte atomare Formeln.

Negations Normalform (NNF)

- Alle Negationen kommen in Literalen vor
- Es gibt keine Implikationen

Disjunktiver Normalform (DNF)

- $(L_{1,1} \wedge L_{1,2} \wedge L_{1,3} \dots) \vee (L_{2,1} \wedge L_{2,2} \wedge L_{2,3} \dots) \vee (L_{3,1} \wedge L_{3,2} \wedge L_{3,3} \dots)$

Konjunktiver Normalform (KNF)

- $(L_{1,1} \vee L_{1,2} \vee L_{1,3} \dots) \wedge (L_{2,1} \vee L_{2,2} \vee L_{2,3} \dots) \wedge (L_{3,1} \vee L_{3,2} \vee L_{3,3} \dots)$

Wahrheitstabelle

- Der letzte Eintrag der ersten Zeile ist die Formel *F*.
- Wenn *A* in einer Spalte vor *B* erscheint, dann ist *A* eine Teilformel von *B*.

Beispiel: $F = A \vee \neg(B \wedge C)$

A	B	C	$B \wedge C$	$\neg(B \wedge C)$	$A \vee \neg(B \wedge C)$
0	0	0	False	True	True
0	0	1	False	True	True
0	1	0	False	True	True
0	1	1	True	False	False
1	0	0	False	True	True
1	0	1	False	True	True
1	1	0	False	True	True
1	1	1	True	False	True

Belegung

Die Funktion $\hat{B}$ ordnet jeder aussagenlogischen Formel ihren Wahrheitswert bezüglich dessen Belegung B zu. $\hat{B}: \mathbb{F} \to \{false, true\}$

- $\hat{B}(F \wedge G) = and\left(\hat{B}(F), \hat{B}(G)\right)$
- $\hat{B}(F \vee G) = or\left(\hat{B}(F), \hat{B}(G)\right)$
- $\hat{B}(\neg G) = not\left(\hat{B}(F), \hat{B}(G)\right)$

Beispiel: Bestimmen Sie $\hat{B}$ der Formel $(u \to r) \wedge s$

- $B(p) = B(q) = B(r) = B(s) = true$
- $B(u) = B(v) = false$

$$\hat{B}\big((u \to r) \wedge s\big) = and\left(\hat{B}(u \to r), \underbrace{\hat{B}(s)}_{true}\right) = \hat{B}(u \to r) = or\left(\neg\hat{B}(u), \underbrace{\hat{B}(r)}_{true}\right) = \boldsymbol{true}$$

Eine aussagenlogische Formel *A* heisst

• Allgemeingültig	Alle Belegungen	$\forall \hat{B}(A) = true$
• Unerfüllbar	Alle Belegungen	$\forall \hat{B}(A) = false$
• Erfüllbar	Min. Eine Belegung	$\exists \hat{B}(A) = true$
• Widerlegbar	Min. Eine Belegung	$\exists \hat{B}(A) = false$

3 Mengen, Relationen und Graphen

Notationen

- $y \in X$
- Explizite Schreibweise: {1, 2, 3, 4, …}

Zahlenmengen

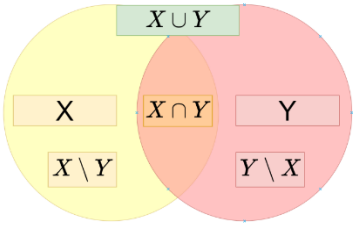
- $\mathbb{Z}$ = Ganze Zahlen = {…, -2, -1, 0, 1, 2, …}
- $\mathbb{N}$ = Natürliche Zahlen = {0, 1, 2, 3, …}

Teilmengen

- X ist eine *Teilmenge* von Y: $\boldsymbol{X \subseteq Y}$
- X ist eine echte *Teilmenge* ($X \neq Y$) von Y: $X \subset Y$

Operationen

- Vereinigung $X \cup Y \coloneqq \{x | x \in X \vee x \in Y\}$
- Schnittmenge $X \cap Y \coloneqq \{x | x \in X \wedge x \in Y\}$
- Differenz $X \setminus Y \coloneqq \{x | (x \in X) \wedge (x \notin Y)\}$



Partitionen und Blöcke

Eine Partition $P = \{P_i | i \in I\}$ einer Menge A, ist eine Menge von Teilmengen von A, die folgende beiden Voraussetzungen erfüllt:

- Die Elemente von *P* sind nicht leer und paarweise disjunkt
- $\bigcup_{i \in I} P_i = A$

Die Elemente einer Partition werden Blöcke genannt.

Rechenregeln

Kommutativität der Vereinigung und des Schnittes:
$A \cup B = B \cup A \; und \; A \cap B = B \cap A$

Assoziativgestze von Schnitt und Vereinigung:
$A \cup (B \cup C) = (A \cup B) \cup C \; und \; A \cap (B \cap C) = (A \cap B) \cap C$

Distributivgesetze von $\cap \; und \; \cup$:
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \; und \; A \cup (B \cap / C) = (A \cup B) \cap (A \cup C)$

Idempotenzgesetz:
$A \cap A = A \; und \; A \cup A = A$

Regeln von De Morgan:
$(C \backslash A) \cap (C \backslash B) = C(A \cup B) \; und \; (C \backslash A) \cup (C \backslash B) = C \backslash (A \cap B)$

Potenzmenge

Ist A eine beliebige Menge, dann bezeichnen wir mit $\boldsymbol{P(A) \coloneqq \{x | x \subseteq A\}}$ die Potenzmenge von A, die genau die Teilmengen von A als Element enthält.

- $\emptyset \in P(A)$ Jede Potenzmenge enthält die leere Menge

Beispiel

- $P(\{0,1\}) = \{\emptyset, \{0\}, \{1\}, \{0,1\}\}$

Kartesisches Produkt = Kreuzprodukt

Das *kartesische Produkt* von $A_1, \ldots, A_n$, ist die Menge aller n-Tupel mit Einträgen aus den Mengen $A_1, \ldots A_n$.

Beispiel $A = \{0,1\}, B = \{2,3\}$

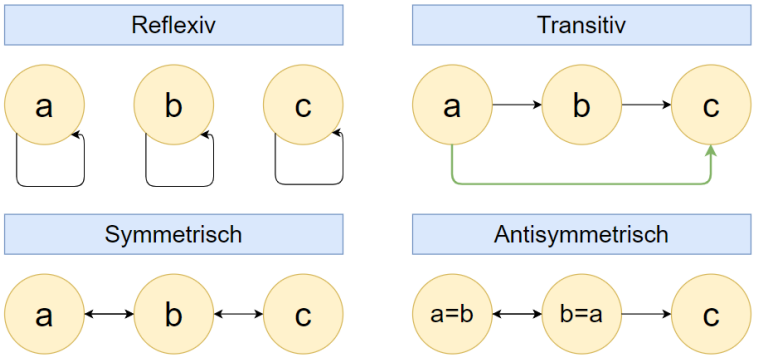
- $A \times B = \{(0,2), (0,3), (1,2), (1,3)\}$
- $A^2 \quad = \{(0,0), (0,1), (1,0), (1,1)\}$

Relationen

Binäre Relation R mit $(x, y) \in R$, dann schreiben wir auch xRy.

Eine binäre Relation R auf eine Menge X heisst

- Reflexiv — wenn für alle $\boldsymbol{x \in X}$ — gilt $\boldsymbol{xRx}$
- Symmetrisch — wenn für alle $\boldsymbol{x, y \in X}$ — gilt $\boldsymbol{xRy \Rightarrow yRx}$
- Antisymmetrisch — wenn für alle $\boldsymbol{x, y \in X}$ — gilt $\boldsymbol{xRy \wedge yRx \Rightarrow x = y}$
- Transitiv — wenn für alle $\boldsymbol{x, y, z \in X}$ — gilt $\boldsymbol{xRy \wedge yRz \Rightarrow xRz}$



Ordnungstypen

Es sei *R* eine binäre Relation auf der Menge *M*.

- Totale Ordnung — Kein unvergleichbares Element — (+ Halbordnung)
- Wohlordnung — mind. 1 min. Element pro Teilmenge — (+ Totale Ordnung)

	Reflexiv	Symmetrisch	Antisymmetrisch	Transitiv
Äquivalenzrelation	X	X		X
Prä-Ordnung	X			X
Halb-Ordnung	X		X	X
Totale Ordnung	X		X	X
Wohl-Ordnung	X		X	X

Unvergleichbar

Zwei Elemente $x, y \in M$ heissen R-unvergleichbar, falls weder xRy noch yRx gilt.

Minimal / Maximal

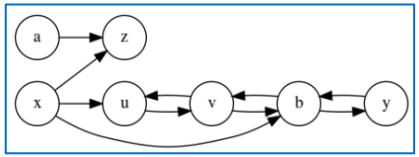
Ein Element $x \in X$ einer Teilmenge $X \subseteq M$ von *M* heisst

- *R-minimal* in X, falls es kein anderes Element $y \in X$ mit *yRx* gibt.
- *R-maximal* in X, falls es kein anderes Element $y \in X$ mit *xRy* gibt.

Graphen

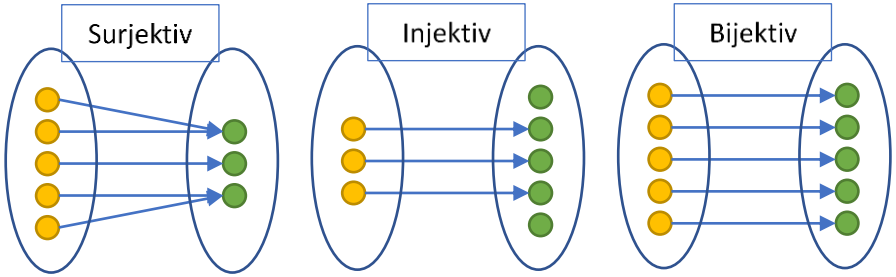
Die Relation R auf $M = \{a, b, u, b, x, y, z\}$ sei durch den Graph (M, R) gegeben.

Minimal (Nur ausgehende Pfeile) = a, x
Maximal (Nur eingehende Pfeile) = z



Surjektiv, Injektiv und Bijektiv

Surjektiv — Elemente der Zielmenge werden *mindestens* einmal getroffen.
Injektiv — Elemente der Zielmenge werden *höchstens* einmal getroffen.
Bijektiv — Surjektiv + Injektiv



Hasse-Diagramm

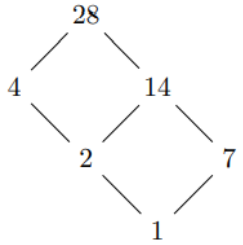
Das Hasse-Diagramm bietet eine Vereinfachte Darstellung einer Halbordnungs-Relation.

- Pfeile werden weggelassen. Der Graph geht nach «oben».
- Verbindungen zwischen zwei Punkten werden weggelassen, wenn es bereits eine «indirekte Verbindung» gibt.
- Verbindungen von einem Punkt zu sich selbst werden weggelassen.

Beispiel

Teilbarkeitsrelation auf der Menge $\{1, 2, 4, 7, 14, 28\}$

- Minimale Elemente $= \{1\}$
- Maximale Elemente $= \{28\}$



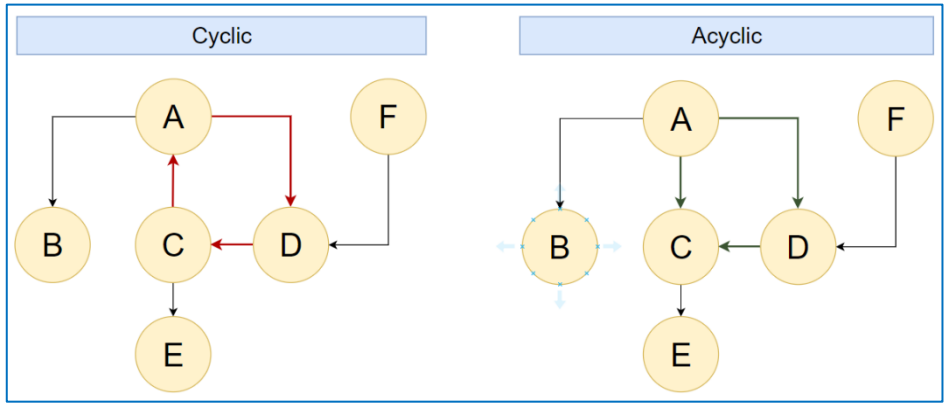
DAG (Directed Acyclic Graph)

Jeder endliche DAG besitzt (mindestens) eine topologische Sortierung.

Topologische Sortierung

Es sei *M* eine endliche Menge und $G = (M, E)$ ein DAG. Eine lineare Ordnung $\preccurlyeq \subseteq M \times M$ ist eine *topologische Sortierung* von G, wenn für alle $a, b \in M$ gilt:

$$aE^*b \Rightarrow a \preccurlyeq b$$



Abzählbar

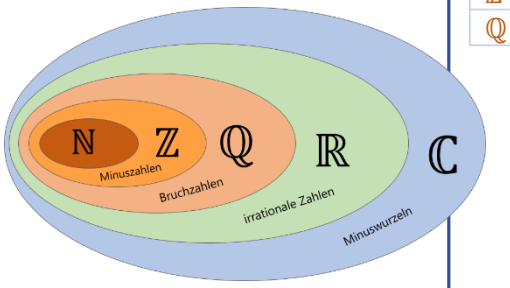
Eine Menge X heisst *abzählbar*, wenn … (oder) … .

- Surjektive Funktion $F: \mathbb{N} \to X$
- $X = \emptyset$

Überabzählbar

Eine Menge X heisst *überabzählbare* sie…

- Nicht abzählbar ist



Abzählbar	Überabzählbar
$\{1, 2, 3\}$	$\mathbb{I}$ $= irrationale\ Zahlen$
$\mathbb{P}$	$\mathbb{R}$ $= reelle\ Zahlen$
$\mathbb{N}$	$\mathbb{C}$ $= komplexe\ Zahlen$
$\mathbb{Z}$	$B(\infty)$ $= alle\ unendlichen\ Binärsequenzen$
$\mathbb{Q}$	$P(\mathbb{N})$ $= Potenzmenge\ von\ \mathbb{N}$

4 Rekursive Strukturen und die natürlichen Zahlen

Induktion

Es sei $A(n)$ eine Eigenschaft von natürlichen Zahlen

- Verankerung $A(n)$
- Schritt $\forall n \in \mathbb{N}(\underbrace{A(n)}_{Induktions-Annahme} \Rightarrow A(n+1))$

Induktions-**A**nnahme *IA*

$$\sum_{i=1}^{n}\left(\frac{1}{i(i+1)}\right) = \frac{n}{n+1}$$

Induktions-**V**erankerung IV $(n = 0)$

$$\sum_{i=1}^{0}\left(\frac{1}{i(i+1)}\right) = \frac{0}{0+1} = 0$$

Zu zeigen

$$\sum_{i=1}^{n+1}\left(\frac{1}{i(i+1)}\right) = \frac{\boldsymbol{n+1}}{\boldsymbol{n+2}}$$

Induktions-**S**chritt IS $(n \to n+1)$

$$\begin{aligned}
\textstyle\sum_{i=1}^{n}\left(\frac{1}{i(i+1)}\right) + \frac{1}{n+1(n+1+1)} &= \frac{n}{n+1} &&+ \frac{1}{n+1(n+1+1)} \\
&= \frac{n}{n+1} &&+ \frac{1}{(n+1)(n+2)} \\
&= \frac{n\cdot(n+2)}{(n+1)(n+2)} &&+ \frac{1}{(n+1)(n+2)} \\
&= \frac{n^2+2n+1}{(n+1)(n+2)} \\
&= \frac{(n+1)^2}{(n+1)(n+2)} \\
&= \frac{\boldsymbol{n+1}}{\boldsymbol{n+2}}
\end{aligned}$$

Rekursionsgleichung

- Verankerung $F(0) = c$
- Schritt $F(k+1) = G\left(\underbrace{F(k)}_{Selbstbezug}, k\right)$

<u>Beispiel Exponentiation von $\mathbb{N}$</u>

$$\begin{aligned}
F(n) &= x^n \\
F(0) &= x^0 = 1 \\
F(n+1) &= G(F(n), n) \\
x^{n+1} &= F(n) \cdot n \\
x^{n+1} &= x^n \cdot n
\end{aligned}$$

Peano Axiome

- Jede Natürliche Zahl k hat genau einen Nachfolger $k+1$
- Die Zahl 0 ist die einzige natürliche Zahl, die kein Nachfolger ist
  $\forall n \in \mathbb{N}(\forall k \in \mathbb{N}(n \neq k+1) \Leftrightarrow n = 0)$
- Jede natürliche Zahl ist Nachfolger von höchstens einer natürlichen Zahl
  $\forall n, m \in \mathbb{N}(n+1 = m+1 \Rightarrow n = m)$
- *Prinzip der (vollständigen) Induktion*

5 Elementare Zahlentheorie

Teilbarkeit

Sind $x, y \in \mathbb{Z} \rightarrow x\ Teiler\ von\ y$, falls es kein $k \in \mathbb{Z}$ gibt mit $xk = y$.

$$x\ teilt\ y \Leftrightarrow x|y: \Leftrightarrow \exists k \in \mathbb{Z}(y = xk)$$

Euklidischer Algorithmus

Für $n, m \in \mathbb{N}$ mit 0 < n < m gilt

$$ggT(n, m) = ggT(n, m - n) = ggT(m, m - n)$$

Definition kgV und ggT

Seien $n, m \in \mathbb{Z}$. *Kleinstes gemeinsames Vielfaches* von n und m:

$$kgV(n, m) \coloneqq \min\{k \in \mathbb{N} \mid n|k \wedge m|k\}$$

Ist $n \neq 0$ oder $m \neq 0$. *Grösster gemeinsamen Teiler* von n und m:

$$ggT(n, m) \coloneqq \max\{k \in \mathbb{N} \mid k|n \wedge k|m\}$$

Primzahlen

Eine natürliche Zahl $p \in \mathbb{N}$ ist eine *Primzahl* $\mathbb{P}$, wenn $|T(p)| = 2$ gilt.

1. Jede Primzahl p hat genau zwei unterschiedliche Teiler $\mathbb{T} = \{1, p\}$
   - $1 \in \mathbb{T}$
   - $p \in \mathbb{T}$
2. Jede ganze Zahl z besitzt mind. einen Primfaktor $p \in \mathbb{P}$
3. Es gibt unendlich viele Primzahlen

Lemma von Euklid

Folgende Aussagen sind für $p \in \mathbb{N}$ mit $p \neq 1$ äquivalent

- $\forall n, m \in \mathbb{N}(p|nm \rightarrow p|n \vee p|m)$
- $p \in \mathbb{P}$

Lemma von Bézout

Sind $x, y \in \mathbb{Z}$ mit $x, y \neq 0$, dann gibt es Zahlen a, b so dass folgendes gilt

$$ggT(x, y) = ax + by$$

Beispiel

$$a \cdot 128 + b \cdot 34 = ggT(128, 34)$$

1. Sukzessive Teilen mit Rest

$x / y = q$	Rest r	$a = q \cdot b + r$
$128 / 34 = 3$	Rest 26	$128 = 3 \cdot 34 + 26$
$34 / 26 = 1$	Rest 8	$34 = 1 \cdot 26 + 8$
$26 / 8 = 3$	Rest 2	$26 = 3 \cdot 8 + \mathbf{2} \rightarrow \mathbf{2} = \boldsymbol{ggT}$
$8 / 2 = 4$	Rest 0	$8 = 4 \cdot \mathbf{2} + 0$

2. In Tabelle einsetzen

i	x_i	y_i	q_i	r_i	a_i	b_i	Linearkombination
1	128	34	3	26	b_{i+1}	$a_{i+1} - (q \cdot b_{i+1})$	$ggT = a_i \cdot x_i + b_i \cdot y_i$
2	34	26	1	8	b_{i+1}	$a_{i+1} - (q \cdot b_{i+1})$	$ggT = \cdots$
3	26	8	3	**2**	b_{i+1}	$a_{i+1} - (q \cdot b_{i+1})$	$ggT = \cdots$
4	8	**2**	4	0	a_n	b_n	$ggT = a_i \cdot x_i + b_i \cdot y_i$

3. a, b ermitteln
   - $a_i = b_{i+1}$
   - $b_i = a_{i+1} - (q \cdot b_{i+1})$

i	x_i	y_i	q_i	r_i	a_i	b_i	Linearkombination
1	128	34	3	26	4	$-3 - (3 \cdot 4) = -15$	$2 = 4 \cdot 128 + (-15 \cdot 34)$
2	34	26	1	8	-3	$1 - (1 \cdot -3) = 4$	$2 = -3 \cdot 34 + 4 \cdot 26$
3	26	8	3	**2**	1	$0 - (3 \cdot 1) \quad = -3$	$2 = 1 \cdot 26 + (-3 \cdot 8)$
4	8	**2**	4	0	0	1	$2 = 0 \cdot 8 + 1 \cdot 2$

Restklassen

Es sei $n \in \mathbb{N}$ beliebig. Wir definieren eine Relation $\equiv_n$ auf $\mathbb{Z}$ wie folgt $(r, z \in \mathbb{Z})$

$$r \equiv_n z \qquad \Leftrightarrow n|(r-z)$$

$$r = z \; mod \; n \quad \Leftrightarrow r \equiv_n z$$

Es sei $n \in \mathbb{N}$ beliebig. Für jede ganze Zahl z bezeichnen wir mit

$$[z]_n \coloneqq \{r \in \mathbb{Z} | r \equiv_n z\}$$

Die Äquivalenzklasse von z der Relation $\equiv_n$ heisst *Restklasse* von z.

$$\mathbb{Z}/n = [z]_n = \overline{k}$$

$$\mathbb{Z}/n = \{\overline{k} | 0 \leq k < n-1 \wedge z \equiv_n k\} = \{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{n-1}\}$$

Beispiel

- $\overline{3} + x = \overline{2} \; (\mathbb{Z}/5)$ $\quad \overline{2} - \overline{3} = \; x = \overline{-1} \; = \overline{4}$
- $3 + x \equiv_5 2$ $\quad 2 - 3 \equiv_5 x \equiv_5 -1 \equiv_5 4$
- $3 + x = 2 \; mod \; 5$ $\quad (2-3) \; mod \; 5 = -1 = 4$

Rechenregeln

Wir definieren die Verknüpfungen $\cdot = Multiplikation$ und $+ = Addition$

- $\cdot = Multiplikation$ $\quad (\mathbb{Z}/n)^2 \to \mathbb{Z}/n$ $\quad [x]_n + [y]_n \coloneqq [x+y]_n$
- $+= Addition$ $\quad (\mathbb{Z}/n)^2 \to \mathbb{Z}/n$ $\quad [x]_n \cdot [y]_n \coloneqq [x \cdot y]_n$

Restklasse $(\mathbb{Z}/12)$

- $\overline{7} \cdot \overline{3} = \overline{21} = \overline{9}$

Restklasse $\mathbb{Z}/3221$

- $\overline{2}x = \overline{3}$ $\quad \overline{3221} = \overline{0}$
  $\overline{2}x = \overline{3}$ $\quad \overline{3221} + \overline{3} = \overline{3224}$
  $\overline{2}x = \overline{3}$ $\quad \overline{2} \cdot \overline{1612} = \overline{3224} = \overline{3}$ $\quad x = \overline{1612}$

Anwendung Primzahlen / Restklassen

Beweise oder widerlege

$$b^e + x = \underbrace{3^{71071}}_{ungerade} + \underbrace{4}_{gerade} = \underbrace{p \in \mathbb{P}}_{ungerade}$$

1. *Gerade Restklassen $(z \; mod \; 2 = 0)$ ausschliessen*
2. *Zyklen finden $(z \in \mathbb{P})$ $(Länge = L)$*

n	3^n	$\mathbb{Z}/4$	$\mathbb{Z}/5$	$\mathbb{Z}/6$	$\mathbb{Z}/7$	$\mathbb{Z}/8$
0	$3^0 = 1$	1	1	1	1	1
1	$3^1 = 3$	3	3	3	3	3
2	$3^2 = 9$	1	4	3	2	0
3	$3^3 = 27$	3	2	3	6	0
4	$3^4 = 81$	1	1	3	4	0
5	$3^5 = 243$	3	3	3	5	0
6	$3^6 = 729$	1	4	3	1	0

3. *Teilbarenkeit von e durch L prüfen*
   - $F(k, L) \coloneqq k \; \% \; L == 0 \to true \; (k \in \mathbb{N} \mid k \leq e \wedge k > e - L)$

k	n		$L = 4$	$L = 6$
71071	0	$k \; \% \; L$	$71071\%4 = 3$	$71071\%6 = 1$
71070	1	$k \; \% \; L$	$71070\%4 = 2$	$71070\%6 = 0$
71069	2	$k \; \% \; L$	$71069\%4 = 1$	…
71068	3	$k \; \% \; L$	$71068\%4 = 0$	…
…		…	…	…

4. *Ursprüngliche Gleichung prüfen (durch z teilen)*
   - $\mathbb{Z}/5$ $\quad 3^{71068} = 3^0 = 1 \to 3^{71068+3} = 3^{0+3} = 2$
     $3^{71071} + x = 2 + 4 \qquad (2 + 4 = 5) \to false$
   - $\mathbb{Z}/7$ $\quad 3^{71070} = 3^0 = 1 \to 3^{71071} = 3^{71070+1} = 3^{0+1} = 3$
     $3^{71071} + x = 3 + 4 \qquad (\mathbf{3 + 4 = 7}) \to (\mathbf{b^e + x}) \notin \mathbb{P}$

Multiplikatives Inverse

Sind $\overline{k}, \overline{r} \in \mathbb{Z}/n$ mit $\overline{k} \cdot \overline{r} = \overline{1}$, so sagen wir $\overline{r}$ sei invers zu $\overline{k}$ und schreiben auch $(\overline{k})^{-1}$ für $\overline{r}$.
Bei Restklassen von Primzahlen ist jedes $\overline{r}$ invers zu $\overline{k}$.

- $\overline{k} \cdot \overline{r} = \overline{1}$ $\quad ggT(\overline{k}, \overline{n}) = \overline{z}$ $\quad \overline{z} = \overline{1} \rightarrow \overline{k}$ hat EIN Inverses in $\mathbb{Z}/n$

Beispiel

Restklasse $\mathbb{Z}/n$ $(n = 12)$

1. ggT Bestimmen
   - $ggT = 1 \rightarrow Inverses\ ermitteln$
   - $ggT \neq 1 \rightarrow Kein\ Inverses$

k	$\overline{k} \cdot \overline{x} = \overline{1}$	$ggT(k,n) = \overline{z}$	$\overline{x} = (\overline{k})^{-1}$
1	$\overline{1} \cdot \overline{x} = \overline{1}$	$ggT(1,12) = \overline{1}$	$\overline{1}$
2	$\overline{2} \cdot \overline{x} = \overline{1}$	$ggT(2,12) = \overline{2}$	
3	$\overline{3} \cdot \overline{x} = \overline{1}$	$ggT(3,12) = \overline{3}$	
4	$\overline{4} \cdot \overline{x} = \overline{1}$	$ggT(4,12) = \overline{4}$	
5	$\overline{5} \cdot \overline{x} = \overline{1}$	$ggT(5,12) = \overline{1}$	$\overline{5}$
6	$\overline{6} \cdot \overline{x} = \overline{1}$	$ggT(6,12) = \overline{3}$	
7	$\overline{7} \cdot \overline{x} = \overline{1}$	$ggT(7,12) = \overline{1}$	$\overline{7}$
8	$\overline{8} \cdot \overline{x} = \overline{1}$	$ggT(8,12) = \overline{4}$	
9	$\overline{9} \cdot \overline{x} = \overline{1}$	$ggT(9,12) = \overline{3}$	
10	$\overline{10} \cdot \overline{x} = \overline{1}$	$ggT(10,12) = \overline{2}$	
11	$\overline{11} \cdot \overline{x} = \overline{1}$	$ggT(11,12) = \overline{1}$	$\overline{11}$

Verknüpfungstabelle

Die Verknüpfungstabelle der Multiplikation in $\mathbb{Z}/4$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Multiplikatives Inverses bestimmen

1. $a \cdot \overline{k} + b \cdot \overline{n} = \overline{1}$
2. Erweiterter Euklidischer Algorithmus
3. $(\overline{k})^{-1} = \overline{a}$

Beispiel

Inverses von $\overline{6111}$ in $\mathbb{Z}/6211$

1. $a \cdot 6111 + b \cdot 6211 = 1$
2. Erweiterter Euklidischer Algorithmus

i	x_i	y_i	q_i	r_i	b_i	a_i
1	6211	6111	1	100	550	$-559 = -9 - (1 \cdot 550)$
2	6111	100	61	11	-9	$550 = 1 - (61 \cdot -9)$
3	100	11	9	**1**	1	$-9 = 0 - (9 \cdot 1)$
4	11	**1**	11	0	0	1

3. $(\overline{6111})^{-1} = \overline{-559}$

Primfaktorzerlegung

Es sei p_i jeweils die *i-te* Primzahl. Für $n \in \mathbb{N} > 1$ gibt es eine eindeutig bestimmte, endliche Folge $\{a_1, \dots, a_k\} \in \mathbb{N}$ mit $a_k \neq 0$, so dass

$$n = \prod_{i=1}^{k} p_i^{a_i}$$

Beispiel

- $24 = 2 \cdot 2 \cdot 2 \cdot 3 = 2^3 \cdot 3^1$
- $520 = 2 \cdot 2 \cdot 2 \cdot 5 \cdot 13 = 2^3 \cdot 5^1 \cdot 13^1$

Chinesischer Restsatz ($KgV\ 2.0$)

Simultane Kongruenz ($\mathbb{Z}/(n_1, \dots, n_k)$)

$$x \equiv_{n_1} y_1$$

$$x \equiv_{n_2} y_2$$

$$\dots$$

$$x \equiv_{n_k} y_k$$

<u>Vorgehen</u>

1. Lösen zweier Gleichungen
   - $a \cdot n_1 + b \cdot n_2 = 1$
2. Restklasse $\mathbb{Z}/(n_{new})$ der neuen Gleichung
   - $\mathbb{Z}/(n_1 \cdot n_2) = \mathbb{Z}/(n_{new})$
3. Lösung $z = y_{new}$ der neuen Gleichung
   - $z \coloneqq y_1 \cdot b \cdot n_2 + y_2 \cdot a \cdot n_1$

<u>Beispiel – Teil 1</u>

$$x \equiv_7 3$$

$$x \equiv_5 2$$

$$x \equiv_9 6$$

Vorgehen

1. Lösen zweier Gleichungen
   - 1. Gleichung: $x \equiv_7 3$ $(n_1 = 7, y_1 = 3)$
   - 2. Gleichung: $x \equiv_5 2$ $(n_2 = 5, y_2 = 2)$

n_1	n_2	q	r	a	b
7	5	1	2	-2	3
5	2	2	**1**	1	-2
2	**1**	2	0	0	1

2. Restklasse $\mathbb{Z}/(n_{new})$ der neuen Gleichung
   - $n_{new} = n_1 \cdot n_2 = 7 \cdot 5 = 35$
3. Lösung $z = y_{new}$ der neuen Gleichung
   - $z \coloneqq 3 \cdot 3 \cdot 5 + \cdot\, 2 \cdot -2 \cdot 7 = 17$

Neue Gleichung

- $x \equiv_{n_{new}} z \equiv_{35} 17$

<u>Beispiel – Teil 2</u>

$$x \equiv_{35} 17$$

$$x \equiv_9 6$$

Vorgehen

1. Lösen zweier Gleichungen
   - 1. Gleichung: $x \equiv_{35} 17$ $(n_1 = 35, y_1 = 17)$
   - 2. Gleichung: $x \equiv_9 6$ $(n_2 = 9,\ y_2 = 6)$

n_1	n_2	q	r	a	b
35	9	3	8	-1	4
9	8	1	**1**	1	-1
8	**1**	8	0	0	1

2. Restklasse $\mathbb{Z}/(n_{new})$ der neuen Gleichung
   - $n_{new} = n_1 \cdot n_2 = 35 \cdot 9 = 315$
3. Lösung $z = y_{new}$ der neuen Gleichung
   - $z \coloneqq 17 \cdot 4 \cdot 9 + \cdot\, 6 \cdot -1 \cdot 35 = 402$

Neue Gleichung

- $x \equiv_{n_{new}} z \equiv_{315} 402 \equiv_{315} 87$

Lösungsmenge

- $[87]_{315} = \{87 + 315z \mid z \in \mathbb{Z}\}$