Logik

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

Negation: $\neg A$ => kehrt den Wahrheitswert um => «Es trifft nicht zu, dass … »
Konjunktion: $A \wedge B$
Disjunktion: $A \vee B$
Äquivalenz: $A \leftrightarrow B$ => gleicher Wahrheitswert = $A \rightarrow B \wedge B \rightarrow A$

Implikation

A	B	$A \rightarrow B$
0	0	1
0	1	1
1	0	0
1	1	1

In jedem Fall, wo A wahr ist, muss auch B wahr sein.

1) Wenn A falsch ist, kann B wahr oder falsch sein.
2) Wenn A wahr ist, muss B auch wahr sein.

Junktorenregeln

Doppelte Negation	$\neg\neg A$	A
Assoziativität	$(A \wedge B) \wedge C$ $(A \vee B) \vee C$	$A \wedge (B \wedge C)$ $A \vee (B \vee C)$
Distributivität	$A \wedge (B \vee C)$ $A \vee (B \wedge C)$	$(A \wedge B) \vee (A \wedge C)$ $(A \vee B) \wedge (A \vee C)$
De Morgan	$\neg(A \wedge B)$ $\neg(A \vee B)$	$\neg A \vee \neg B$ $\neg A \wedge \neg B$
Implikation (Kontraposition)	$A \Rightarrow B$ $A \Rightarrow B$	$\neg A \vee B$ $\neg B \Rightarrow \neg A$
Äquivalenz	$A \leftrightarrow B$	$((A \Rightarrow B) \wedge (B \Rightarrow A))$ $(\neg A \vee B) \wedge (\neg B \vee A)$

Tautologie: immer wahr $A \vee A = T$
Widerspruch: immer falsch $A \wedge \neg A = W$

Quantoren

⇨ Quantoren binden Variablen

All-Quantor: $\forall x$ «für alle … »
Existenz-Quantor: $\exists$ «es gibt mindestens ein … »

Quantor-Regeln

1. keine Distributivität
2. Quantoren binden stärker als Junktoren

Vertauschungsregel	$\exists x A(x)$	$\neg\forall x \neg A(x)$
Negation	$\neg\exists x \in M A(x)$ $\neg\forall x \in M A(x)$	$\forall x \in M \neg A(x)$ $\exists x \in M \neg A(x)$

Beispiele

- Es gibt genau ein x mit P(X)

  $\exists x P(x) \wedge \forall y, z \quad P(y) \wedge P(z) \Rightarrow y = z$

- Es gibt mindestens zwei Dinge mit der Eigenschaft P(x)

  $\exists xy(p(x) \wedge p(y) \wedge x \neq y)$

- Es gibt höchstens ein x mit P(x)

  $\neg(\exists x, y(P(x) \wedge P(y) \wedge x \neq y))$

- Wenn P(x) und P(y) gilt, dann gilt stets auch Q(x,y).

  $\forall x, y(P(x) \wedge P(y) \Rightarrow Q(x, y))$

- Für kein x gilt Q(x, x)

  $(\neg\exists x Q(x, x)) \Leftrightarrow (\forall x(\neg Q(x, x)))$

Sei P die Menge aller Fachhochschul-Prüfungen und $E(x)$ das Prädikat "x ist einfach". Formalisieren Sie:

a) Alle Prüfungen sind einfach.
b) Eine Prüfung ist einfach.
c) Keine Prüfung ist einfach.
d) Alle Prüfungen sind nicht einfach.
e) Nur eine Prüfung ist einfach.
f) Nur eine Prüfung ist nicht einfach.
g) Nicht alle Prüfungen sind einfach.
h) Eine Prüfung ist nicht einfach.

Welche der Aussagen sagen dasselbe aus?

c) & d) äquivalent
g) & h)

a) $\forall x \in P \quad E(x)$
b) $\exists x \in P \; E(x)$
c) $\neg\exists x \in P \; E(x)$
d) $\forall x \in P \; \neg E(x)$
e) $(\exists x \in P \; E(x)) \wedge (\forall y, z \in P \; (E(y) \wedge E(z) \Rightarrow y = z))$
f) $(\exists x \in P \; \neg E(x)) \wedge (\forall y, z \in P \; (\neg E(y) \wedge \neg E(z) \Rightarrow y = z))$
g) $\neg\forall x \in P \; E(x)$
h) $\exists x \in P \; \neg E(x)$

Semantik

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

Wahrheitstabellen: jede Teilformel = eine Spalte in der Wahrheitstabelle

Semantische Eigenschafte

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 — $\exists \hat{B}(A) = false$

Konsequenz

F ist eine Konsequenz von G, falls F unter jeder Belegung wahr ist unter der G wahr ist.
⇒ Implikation "F folgt aus G"

Beweistechniken

Methode	Vorgehensweise	Beispiel
Direkter Beweis	Basierend auf der Annahme, dass A wahr ist, gibt man zwingende Argumente für die Richtigkeit von B.	
Beweis durch Widerspruch	Man geht davon aus das die initiale Aussage falsch ist und findet dann einen Wiederspruch. ⇨ Aussage negieren ⇨ Bewiesen wenn Widerspruch gefunden wird ⇨ Evtl. Fallunterscheidung (Mengen beachten / Teilbarkeit)	«Es gibt keine grösste natürliche Zahl». => Annahme es gibt eine grösste natürliche Zahl. Jedoch (Widerspruch) gilt für alle natürliche Zahlen es gibt «n + 1» und «n < n + 1». Das steht also im Widerspruch
Beweis durch Kontraposition	Statt «A ⇒ B» beweist man «¬ B ⇒ ¬ A»	Im Halbfinale gewinnen => Finale **Nicht** im Finale sein => Halbfinale **nicht** gewonnen
Beweis einer Äquivalenz (A ⇔ B	Beweis von $A \Rightarrow B$ und B ⇒ A	

⇨ Lange Verkettung von Junktoren als Aussage extrahieren
⇨ Aussage «verdeutschen»

Benötigte Beweistechnik

Aussage	Beweis
∀ - wahr • falsch	Für alle aus der Grundmenge zeigen => Variablen verwenden! Gegenbeispiel => 1 konkreter Wert, für den es nicht zustimmt!
∃ - wahr • falsch	Beispiel => 1 konkreter Wert Für alle aus der Grundmenge zeigen

Kleinster Verbrecher

Will man zeigen, dass alle natürlichen Zahlen eine Eigenschaft E haben, dann geht man davon aus, dass wenn dies nicht der Fall wäre, es eine kleinste natürliche Zahl n0 (den kleinsten Verbrecher) gäbe, die nicht die Eigenschaft E hat. Führt man diese Annahme zu einem Widerspruch, so hat man die ursprüngliche Behauptung bewiesen. => Widerspruchsbeweis (Eigenschaft gilt auch für den kleinsten Verbrecher)

Aufgabe 10. Beweisen Sie mit der Methode des „kleinsten Verbrechers" die folgende Aussage:
$\forall n \in \mathbb{N}: \quad n^3 + 2n$ ist durch 3 teilbar.

Annahme: n_0 kleinste nat. Zahl, für die $n_0^3 + 2n_0$ nicht durch 3 teilbar existiert
weil $n_0 \neq 0$, da $0^3 + 20$ durch 3 teilbar ist
n_0 sicher Nachfolger einer nat. Zahl $n_0 = k+1$
Da $k < n_0$, muss gelten $k^3 + 2k = 3j$, $j \in \mathbb{N}$
$\Rightarrow n_0^3 + 2n_0 = (k+1)^3 + 2(k+1) = k^3 + 3k^2 + 3k + 2k + 3$
$= \underbrace{k^3 + 2k}_{\text{durch 3 teilbar}} + \underbrace{3(k^2 + k + 1)}_{\text{durch 3 teilbar}} = 3\ell, \ \ell \in \mathbb{N}$
$\Rightarrow n_0$ ist nicht kleinster Verbrecher
$\Rightarrow$ es gibt keinen kleinsten Verbrecher
$\Rightarrow$ Eigenschaft gilt für alle nat. Zahlen

Normalformen (NNF, KNF, DNF)

⇨ Syntaktisch, einfache Formeln: ∧,∨, ¬

NNF

alle Negationen in Literalen und keine Implikationen →

DNF

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

KNF

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

In Normalformen umformen

NNF:

1. Implikationen eliminieren mit $F \to G = \neg F \vee G$
2. Negationen, die nicht zu einem Literal gehören werden sukzessive durch Anwenden der De Morganschen Regeln und der Regel der doppelten Negation eliminiert.

KNF/DNF:

1. Jede Formel in NNF kann durch sukzessives Anwenden der Distributivgesetze wahlweise in KNF oder DNF gebracht werden.

Beispiel

Wir eliminieren zuerst alle Implikationen und doppelten Negationen:

$$\begin{aligned}(\neg p \to q) \to ((p \wedge p_1) \vee (p_2 \wedge p_3)) &\equiv \neg(\neg p \to q) \vee ((p \wedge p_1) \vee (p_2 \wedge p_3)) \\ &\equiv \neg(\neg\neg p \vee q) \vee ((p \wedge p_1) \vee (p_2 \wedge p_3)) \\ &\equiv \neg(p \vee q) \vee ((p \wedge p_1) \vee (p_2 \wedge p_3)).\end{aligned}$$

Als Nächstes eliminieren wir alle Negationen, die nicht in Literalen vorkommen (De Morgan):

$$\neg(p \vee q) \vee ((p \wedge p_1) \vee (p_2 \wedge p_3)) \equiv (\neg p \wedge \neg q) \vee ((p \wedge p_1) \vee (p_2 \wedge p_3)).$$

Diese Formel ist nun in NNF und DNF. Mit der Distributivität («Ausmultiplizierung» der verknüpfenden ∨) erhält man dann noch die KNF.

Wahrheitstabellen

DNF ∨: Bildung einer Konjunktion aus jeder Zeile die true liefert = Minterm $(a \wedge b \wedge c) \vee \dots$

KNF ∧: Bildung einer Disjunktion ∨ aus jeder Zeile die false liefert = Maxterm $(a \vee b \vee c) \wedge \dots$

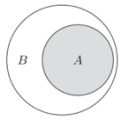
Mengen

Menge = Zusammenfassung unterscheidbarer Objekte ohne innere Ordnung

Teilmenge

$X \subseteq Y$ bedeutet, dass X eine Teilmenge von Y ist ⇒ jedes Element von X ist auch ein Element von Y

$X \subsetneq Y$ = echte Teilmenge, falls X eine von Y verschiedene Teilmenge von Y ist =



Identische Mengen

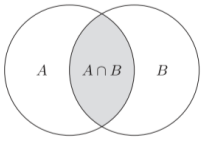
Zwei Mengen X und Y sind gleich, wenn $X \subset Y$ und $Y \subset X$ gilt.

Schnittmenge

Definition 1.27 Die Menge

$$A \cap B = \{x \mid x \in A \text{ und } x \in B\}$$

nennt man den **Durchschnitt** von A und B.



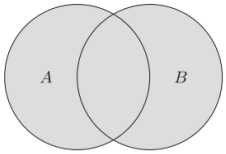
Schnittmenge mehrerer Mengen: $\bigcap_{j=1}^{n} A_j = A_1 \cap \dots \cap A_n$

Vereinigung

Definition 1.29 Die Menge

$$A \cup B = \{x \mid x \in A \text{ oder } x \in B\}$$

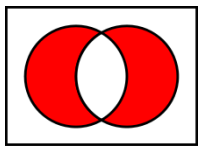
nennt man **Vereinigung** von A und B.



Vereinigung mehrerer Mengen: $\bigcup_{j=1}^{n} A_j = A_1 \cup \ldots \cup A_n$

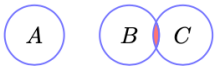
Symmetrische Differenz

$A \triangle B := (A \setminus B) \cup (B \setminus A)$
$= \{x \in A \cup B \mid (x \in A \wedge x \notin B) \vee (x \notin A \wedge x \in B)\}$
$= \{x \in A \cup B \mid x \in A \dot{\vee} x \in B\}$

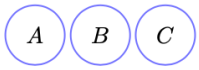


Disjunkt

$X \cap Y = \emptyset$ bedeutet, dass die Mengen keine gemeinsamen Elemente haben = disjunkt



Disjunkt $(A \cap B \cap C = \varnothing)$,
nicht paarweise disjunkt



Paarweise disjunkt

Differenz und Komplement

$A \setminus B = A \cap \bar{B}$
=> «nicht» = ausserhalb von B z.B.
$A = (A \setminus B) \cup B$

Mächtigkeit

Vereinigung	$\lvert \boldsymbol{A} \cup \boldsymbol{B} \rvert$	$\lvert \boldsymbol{A} \rvert + \lvert \boldsymbol{B} \rvert - \lvert \boldsymbol{A} \cap \boldsymbol{B} \rvert$
Disjunkte Mengen	$\lvert A \cup B \rvert$	$\lvert A \rvert + \lvert B \rvert$
3 Mengen	$\lvert A \cup B \cup C \rvert$	$\lvert A \rvert + \lvert B \rvert + \lvert C \rvert - \lvert A \cap B \rvert - \lvert B \cap C \rvert - \lvert A \cap C \rvert + \lvert A \cap B \cap C \rvert$

Rechenregeln

De Morgan	$\overline{\boldsymbol{A} \cup \boldsymbol{B}} = \bar{\boldsymbol{A}} \cap \bar{\boldsymbol{B}}$	$\overline{\boldsymbol{A} \cap \boldsymbol{B}} = \bar{\boldsymbol{A}} \cup \bar{\boldsymbol{B}}$
Komplement	$A \cup \bar{A} = G$	$A \cap \bar{A} = \emptyset$
	$\bar{G} = \emptyset$	$\bar{\emptyset} = G$

Potenzmenge

- ⇨ Menge aller Teilmengen

$\mathcal{P}(\{\emptyset\}) = \{\emptyset\} \neq \emptyset$ $\mathcal{P}(\{0,1\}) = \{\emptyset, \{0\}, \{1\}, \{0,1\}\}$ $\mathcal{P}(\{\{a,\{c\}\}) = \{\phi, \{a\}, \{\{c\}\}, \{a_1\{c\}\}\}$

Mächtigkeit: $|P(A)| = 2^{|A|}$

Partition

- ⇨ Zerlegung einer Menge in **Teilmengen der Potenzmenge**
- ⇨ Nichtleer & paarweise disjunkt
- ⇨ Vereinigung der Teilmengen ergibt die Menge

Kartesisches Produkt

Wichtig: $A \times B \neq B \times A$
=> Tupel haben eine innere Ordnung!
$|A \times B| = |A| \cdot |B|$

$\{1,3\} \times \{0,2\} = \{(1,0), (1,2), (3,0), (3,2)\}$
$\emptyset \times \{\emptyset\} = \{\emptyset\}$ $\{\emptyset\} \times \emptyset = \emptyset$

Grössenvergleich

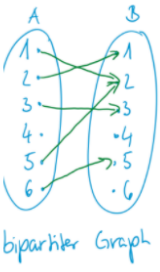
Abzählbar unendlich	gleichmächtig wie N (bijektive Funktion «**Zuordnung existiert**»)	N, Z, Q, N x N, Z x Z, Z x N
Überabzählbar unendlich	**grösser als die Mächtigkeit von N**	(0, 1) = alle unendlichen Binärsequenzen (2. Cantor) R, P(N), R x N, R \ N

Vereinigung von abzählbaren Mengen: abzählbar
Schubfachprinzip: keine injektive Zuordnung = überabzählbar unendlich

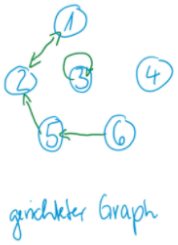
Relationen

⇨ Menge von Tupeln aus dem Kreuzprodukt

Graphen



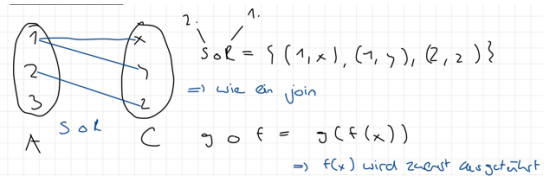
bipartiter Graph



gerichteter Graph

Komposition

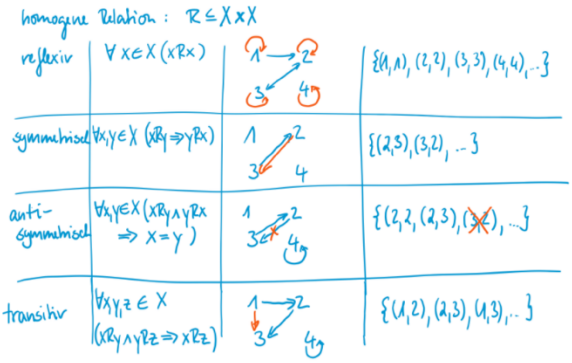
=> Hintereinanderausführung

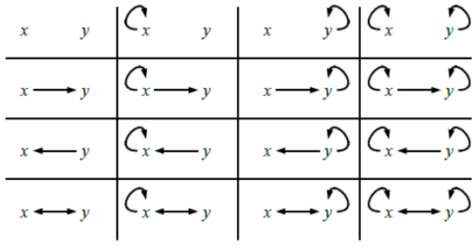


Inverses Element: $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$

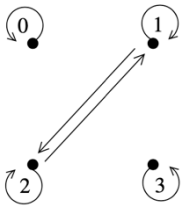
Äquivalenzrelationen

⇨ Ähnliche Objekte miteinander zu identifizieren
⇨ **Reflexiv, symmetrisch, transitiv**





SAIT	SIT	SIT	RSIT
AITK	ITK	ITK	RITK
AITK	ITK	ITK	RITK
SK	SK	SK	RSTK



Äquivalenzklassen
paarweise disjunkt, nichtleer & Vereinigung ergibt A
Faktormenge: Menge der Äquivalenzklassen (Beispiel: { [0]R, [1]R, [3]R } für den obigen Graph einer Äquivalenzrelation)

Ordnungsrelationen

Minimale Elemente: kein Pfeil auf das Element
Maximale Elemente: kein Pfeil weg vom Element

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)

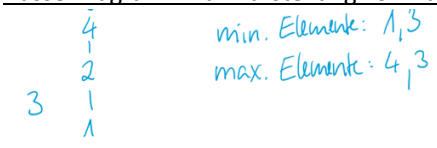
	Reflexiv	Symmetrisch	Antisymmetrisch	Transitiv
Äquivalenzrelation	X	X		X
Prä-Ordnung	X			X
Halb-Ordnung	X		X	X
Totale Ordnung	X		X	X
Wohl-Ordnung	X		X	X

Notationen:
R^+ : transitiver Abschluss = {(1,1), (1,2), (2,3), (1,3)} R^*: reflexiv-transitiver Abschluss

DAG:

- gerichteter, zyklenfreier Graph => z.B. Hasse Diagramm
- topologische Sortierungen = alle möglichen Pfade

Hasse-Diagramm zur Darstellung von Halbordnungen



Funktionen

- ⇨ Jedem Wert aus der Definitionsmenge wird genau ein Element aus der Bildmenge zugeordnet.
- ⇨ Rechtseindeutig + linkstotal

Linkseindeutig (injektiv)	zu jedem y gibt es höchstens ein x
Linkstotal	jedes x hat mindestens ein y Wert
Rechtstotal (surjektiv)	zu jedem y gibt es mindestens ein x
Rechtseindeutig	es gibt zu jedem x maximal ein y Wert

Rekursion

Rekursive Darstellung

F(0)
F(n+1) in Abhängigkeit von n

z.B. rekursiv
$F(0) = 0$
$F(n+1) = F(n) + (n+1)$

explizit
$F(n) = \sum_{k=0}^{n} k = \frac{n(n+1)}{2}$

$F(0) = 0$ +1
$F(1) = 1$ +2
$F(2) = 3$ +3
$F(3) = 6$

Beweis einer rekursiven Funktion

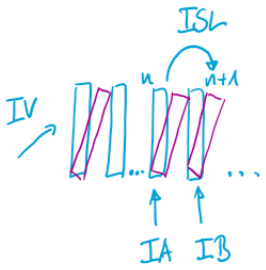
1. IV: $E(0)$: wahr?
$F(0) = \frac{0 \cdot (0+1)}{2} = 0$ explizit
$F(0) = 0$ rekursiv

2.1. IA: $E(n)$: wahr
$F(n) = \frac{n(n+1)}{2}$

2.2. IB: $E(n+1)$: wahr?
$F(n+1) = \frac{(n+1)(n+2)}{2}$

2.3. ISL: $E(n) \Rightarrow E(n+1)$: wahr?
$F(n+1) = F(n) + n+1$
$= \frac{n \cdot (n+1)}{2} + n+1$
$= \frac{n \cdot (n+1)}{2} + \frac{2(n+1)}{2}$
$= \frac{(n+1)(n+2)}{2}$ ✓ s. Behauptung

Induktion



Vollständige Induktion (Induktionsprinzip)

Sei $A(n)$ eine Aussage für beliebiges $n \in \mathbb{N}$, sodass gilt:

1. **Induktionsanfang** (Induktionsverankerung):
   $A(1)$ ist richtig bzw. $A(0)$ ist richtig. (Muss nicht bei 1 oder 0 beginnen, je nach Vorgabe.)
2. **Induktionsvoraussetzung** (Induktionsannahme):
   2.1 Induktionsannahme A(n): wahr
   2.2 Induktionsbehauptung A(n+1): wahr
   2.3 **Induktionsschluss** A(n) => A(n+1): wahr

Dann ist $A(n)$ für alle $n \in \mathbb{N}$ richtig.

Beispiel Induktionsbeweis:
Wir betrachten die Eigenschaft A(n), die besagt, dass die Summe aller natürlichen bis n halb so gross wie die Zahl n(n + 1) ist.

$$\sum_{i=0}^{n} i = 0 + 1 + \cdots + n = \frac{n(n+1)}{2}.$$

1. IV A(0): wahr n=0
$0 = \frac{0 \cdot (0+1)}{2} = 0$ ✓

2. IS A(n) ⇒ A(n+1): wahr

2.1. Induktionsannahme: A(n): wahr (IA)
$\sum_{i=0}^{n} i = 0+1+..+n = \frac{n(n+1)}{2}$ Annahme, dass A(n): wahr

2.2 Induktionsbehauptung: A(n+1): wahr (IB)
$\sum_{i=0}^{n+1} i = 0+1+..+n+n+1 = \frac{(n+1)((n+1)+1)}{2} = \frac{(n+1)(n+2)}{2}$ Behauptung, dass A(n+1): wahr

2.3 Induktionsschluss: A(n) ⇒ A(n+1): wahr (ISL)

$0+1+..+n+n+1 = \frac{n(n+1)}{2} + n+1$
$= \frac{n(n+1) + 2(n+1)}{2}$
$= \frac{(n+1)(n+2)}{2}$

aus der Annahme A(n): wahr folgt die Behauptung A(n+1): wahr
⇒ ∀n∈ℕ A(n): wahr

Elementare Zahlentheorie

kgV $(m,n) \cdot ggT(m,n) = m \cdot n$

Teilbarkeit

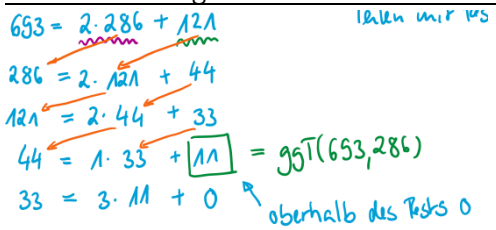
Eine ganze Zahl a heißt durch eine natürliche Zahl b teilbar, wenn es eine ganze Zahl n gibt, sodass $a = n \cdot b$ ist. Die Zahl b heißt in diesem Fall Teiler von a. Man schreibt dafür $b|a$, gelesen: «b teilt a».

Teilermenge: $T(y) = \{x \in \mathbb{N} | x|y\}$
Teilerfremd: Zwei ganze Zahlen x, y heissen teilerfremd, wenn ggT (x, y) = 1 gilt

ggT

ggT $(n,m) =$ ggT $(n, m-n)$
$ggT(n,m) = ggT(n, m-k \cdot n). \quad k \cdot n \leqslant m$

Euklidischer Algorithmus zur Bestimmung von ggT(n, m)



kgV(x, y): (x * y) / ggT(x, y)

Erweiterter Euklidischer Algorithmus

Lemma von Bézout:
$ggT(x,y) = ax + by$ *falls x, y teilerfremd*

x steht immer bei der grösseren Zahl! Eine solche Gleichung bezeichnet man auch als **diophantische Gleichung**.

x0 = 1 x1 = 0; y0 = 0 y1 = 1

$x_k = x_{k-2} - q_k \cdot x_{k-1}$

$y_k = y_{k-2} - q_k \cdot y_{k-1}$

Beispiel

$ax + by = c \rightarrow 75x + 38y = 10'000$
$ax + by = ggT(a,b) \rightarrow 75x + 38y = 1$

Es gibt hier eine ganzzahlige Lösung, da $c = 10000$ ein Vielfaches von $ggT(75,38) = 1$ ist.

$75 = 1 \cdot 38 + 37, \quad x_2 = 1 - 1 \cdot 0 = 1, \quad y_2 = 0 - 1 \cdot 1 = -1$
$38 = 1 \cdot 37 + 1, \quad x_3 = 0 - 1 \cdot 1 = -1, \quad y_3 = 1 - 1 \cdot (-1) = 2$
$37 = 37 \cdot 1 + 0$

Primzahlen

Primzahl: Eine natürliche Zahl $p > 1$, die nur durch sich selbst und durch 1 teilbar ist.
Primfaktorzerlegung: $60 = 2 \cdot 2 \cdot 3 \cdot 5 = 2^2 \cdot 3 \cdot 5$

Modulare Arithmetik

Kongruent modulo m: Wenn zwei ganze Zahlen a und b bei Division durch $m \in \mathbb{N}$ denselben Rest haben, so sagt man, a und b sind kongruent modulo m.
Man schreibt dafür $\boldsymbol{a \equiv b \ (mod\ m)}$. Die Zahl m heisst Modul. → $17 \equiv 22 \ (mod\ 5)$
Zwei Zahlen sind also genau dann kongruent modulo m, wenn sie sich um ein Vielfaches von m unterscheiden.

Rechnen mit kongruenten Zahlen

Satz 3.4 Wenn $a = b \pmod m$ und $c = d \pmod m$ gilt, dann folgt

$$\begin{aligned} a + c &= b + d \pmod m \\ a \cdot c &= b \cdot d \pmod m. \end{aligned}$$

Beispiel: $(38 + 22 \cdot 17)\ (mod\ 4) = (2 + 2 \cdot 1)\ (mod\ 4) = 4\ (mod\ 4) = 0\ (mod\ 4)$

$$[a]_n + [b]_n = [a + b]_n$$
$$[a]_n \cdot [b]_n = [a \cdot b]_n$$

Restklassen

⇨ Klassen mit demselben Rest bei der Division durch eine Zahl

$[z]_n := \{x \in \mathbb{Z} \mid x \equiv_n z\}$

Menge aller Restklassen:
$\mathbb{Z}/n = \{[z]_n \mid z \in \mathbb{Z}\} = \{[0]_n, [1]_n, [2]_{n,\dots,}[n-1]_n\}$

Prime Restklassen

Diejenigen Restklassen, die teilerfremd zu n sind => Notation: $\mathbb{Z}^*_{/n}$

Beispiele:

$\mathbb{Z}^*_{17} = \{1, 2, 3, 4, 5, 6\}$

$\mathbb{Z}^*_{16} = \{1, 5\}$

$\mathbb{Z}^*_{/8} = \{1, 3, 5, 7\}$

Mächtigkeit von $\mathbb{Z}^*/n$: *Eulersche φ − Funktion*

1. $\varphi(n \cdot m) = \varphi(n) \cdot \varphi(m)$, $ggT(n, m) = 1$
2. $\varphi(p) = p - 1$, $p \in \mathbb{P}$
3. $\varphi(p^k) = p^k - p^{k-1}$, $k \in \mathbb{N}_{>0}$

$|\mathbb{Z}^*_8| = \varphi(8) = \varphi(2^3) = 2^3 - 2^{3-1} = 8 - 4 = 4$
$|\mathbb{Z}^*_{15}| = \varphi(15) = \varphi(3 \cdot 5) = \varphi(3) \cdot \varphi(5) = 2 \cdot 4 = 8$
$|\mathbb{Z}^*_{240}| = \varphi(240) = \varphi(2^4 \cdot 3 \cdot 5) = \varphi(2^4) \cdot \varphi(3) \cdot \varphi(5) = (2^4 - 2^3) \cdot 2 \cdot 4 = 64$

Verknüpfungstabelle

Die Verknüpfungstabellen für $\mathbb{Z}/6$ sind wie folgt:

+	[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]	
[3]	[3]			[0]		
[4]	[4]		[0]			
[5]	[5]	[0]				

neutrales Element: $[0]_n$, da $[0]_n + [a]_n = [a]_n$
inverse Elemente: $[-a]_n$, da $[a]_n + [-a]_n = [a]_n + [n-a]_n = [0]_n$

·	[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]

mult. Inverse
hier $[1^{-1}]_6 = [1]_6$
$[5^{-1}]_6 = [5]_6$

neutrales Element: $[1]_n$, da $[a]_n \cdot [1]_n = [a]_n$
inverse Elemente $[a^{-1}]_n$, da $[a]_n \cdot [a^{-1}]_n = [1]_n$

Multiplikative Inverse

$[a]_n \cdot [a^{-1}]_n = [1]_n$

⇨ Multiplikatives Inverse **existiert nur falls ggT(a, n) = 1 = teilerfremd**

Berechnen

1. Pröbeln 2. Erweiterter Eukl. Algorithmus

Lemma von Bézout für Teilerfremde Zahlen $ggT(a,n) = 1$
$ax + ny = 1$
Gleichung mod n:
$ax + ny \equiv_n 1$ (wegen $\equiv_n 0$) $\quad ax \equiv_n 1$
x: mult. Inverses zu a

- x ist mult. Inverses zu a in $\mathbb{Z}_{/n}$, falls $a > n$
- y ist mult. Inverses zu a in $\mathbb{Z}_{/n}$, falls $a < n$

Bsp.: $[5^{-1}]$ in $\mathbb{Z}_{/32}$ $\quad 32x + 5y = 1$ $\quad [y]_{32} = [5^{-1}]_{32}$

$32 = 6 \cdot 5 + 2$
$5 = 2 \cdot 2 + 1$

$y_0 = 0, y_1 = 1$
$y_2 = 0 - 6 \cdot 1 = -6$
$y_3 = 1 - 2 \cdot (-6) = 13$

$[y]_{32} = [5^{-1}]_{32} = [13]_{32}$

Kongruenzgleichungen

Wir betrachten die Gleichung in $\mathbb{Z}/5$

$$\bar{2} \cdot x = \bar{3}$$

$\bar{2} \cdot x = \bar{3} \quad | \cdot \bar{2}^{-1}$

$\bar{2}^{-1} \cdot \bar{2} \cdot x = \bar{2}^{-1} \cdot \bar{3}$

$\bar{3} \cdot \bar{2} \cdot x = \bar{3} \cdot \bar{3}$

$\bar{1} \cdot x = \bar{9}$

$x = \bar{4}$

"normal" in $\mathbb{Q}$

$2 \cdot x = 3 \quad | \cdot \frac{1}{2}$

$\frac{1}{2} \cdot 2 \cdot x = \frac{1}{2} \cdot 3$

$1 \cdot x = \frac{3}{2}$

$x = \frac{3}{2}$

Wichtig: Sind a und m nicht teilerfremd, so kann es keine oder auch mehrere Lösungen geben (aber nicht genau eine). Es gibt genau $t = ggT(a, m)$ Lösungen, falls t auch b teilt; ansonsten existiert keine Lösung. Beispiel:

$\bar{2} \cdot x = \bar{3}$ in $\mathbb{Z}/4$

$\bar{2}$ hat kein mult. Inverses

$\Rightarrow$ Gleichung ist nicht lösbar

Fermat

Satz 3.43 (Fermat) Sei p eine Primzahl. Für jede Zahl x, die teilerfremd zu p ist, gilt

$$x^{p-1} = 1 \pmod{p}.$$

Bsp.: $26^{123} \bmod 7$ $\quad ggT(26,7) = 1$ ✓

$26^{7-1} \equiv_7 26^6 \equiv_7 1$ (aus kleinem Fermat)

$26^{123} \equiv_7 (26^6)^{20} \cdot 26^3 \equiv_7 1^{20} \cdot 26^3 \equiv_7 26^3 \equiv_7 5^3 \equiv_7 (-2)^3$

$\equiv_7 -8 \equiv_7 6$

Satz von Euler

$ggT(a, m) = 1 \Rightarrow a^{\varphi(m)} \equiv 1 \bmod m$

Bsp.: $111^{182} \equiv_{19} ?$ $\quad ggT(111, 19) = 1$ ✓

$111^{\varphi(19)} \equiv_{19} 1$ (aus Satz von Euler) $\quad \varphi(19) = 18$

$111^{18} \equiv_{19} 1$

$111^{182} \equiv_{19} (111^{18})^{10} \cdot 111^2 \equiv_{19} 1^{10} \cdot 111^2$

$\equiv_{19} 111^2 \equiv_{19} 16^2 \equiv_{19} 256$

Chinesischer Restsatz

Mit dem chinesischen Restsatz kann man Systeme von Kongruenzen eindeutig lösen, bei denen die **Module m paarweise teilerfremd** sind.

Vorgehensweise für 2 Kongruenzen

Bsp.: $x \equiv 2 \bmod 3$ $\quad a_1 = 2$ $\quad m_1 = 3$

$x \equiv 5 \bmod 7$ $\quad a_2 = 5$ $\quad m_2 = 7$

Vorgehensweise für 2 Kongruenzen:

1. Inverse der Module gegenseitig:

$M_1 = 7$: $7 \cdot N_1 \equiv_3 1$ $\quad [N_1]_3 = [1]_3$ $\quad N_1 = 1$

$M_2 = 3$: $3 \cdot N_2 \equiv_7 1$ $\quad [N_2]_7 = [5]_7$ $\quad N_2 = 5$

2. Kongruenz zusammengefasst:

$x \equiv 2 \cdot 7 \cdot 1 + 5 \cdot 3 \cdot 5 \bmod (3 \cdot 7)$

$\equiv (14 + 75) \equiv 89 \equiv 5 \bmod 21$

Eine Lösung der simultanen Kongruenz existiert genau dann, wenn für alle $i \neq j$ gilt:

$$a_i \equiv a_j \mod \text{ggT}(m_i, m_j).$$

Alle Lösungen sind dann kongruent modulo dem kgV der m_i.

Mehrere Kongruenzen

Bsp.: $x \equiv 2 \bmod 3$ $\quad a_1 = 2$ $\quad m_1 = 3$

$x \equiv 3 \bmod 5$ $\quad a_2 = 3$ $\quad m_2 = 5$

$x \equiv 2 \bmod 7$ $\quad a_3 = 2$ $\quad m_3 = 7$

$m = m_1 \cdot m_2 \cdot m_3 = 3 \cdot 5 \cdot 7 = 105$

1. M_k bestimmen:

$M_1 = \frac{m}{m_1} = \frac{m_1 \cdot m_2 \cdot m_3}{m_1} = m_2 \cdot m_3 = 5 \cdot 7 = 35$

$M_2 = m_1 \cdot m_3 = 3 \cdot 7 = 21$

$M_3 = m_1 \cdot m_2 = 3 \cdot 5 = 15$

2. N_k bestimmen: Mult. Inverse $[N_k]_{m_k} = [M_k^{-1}]_{m_k}$

N_1: $[N_1]_3 = [35^{-1}]_3 = [2^{-1}]_3 = [2]_3$ $\quad N_1 = 2$

N_2: $[N_2]_5 = [21^{-1}]_5 = [1^{-1}]_5 = [1]_5$ $\quad N_2 = 1$

N_3: $[N_3]_7 = [15^{-1}]_7 = [1^{-1}]_7 = [1]_7$ $\quad N_3 = 1$

3. Kongruenz

$x \equiv (2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1) \bmod 105$

$\equiv 233 \bmod 105 \equiv 23 \bmod 105$

$\mathbb{L} = [23]_{105}$