Elementare Logik

Gesetze und Umformungen

Distributiv:

$$A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C)$$
$$A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C)$$

Assoziativ:

$$(A \wedge B) \wedge C = A \wedge (B \wedge C)$$
$$(A \vee B) \vee C = A \vee (B \vee C)$$

De Morgan: $\neg(A \wedge B) = \neg A \vee \neg B$

Kontraposition: $F \rightarrow G = \neg G \rightarrow \neg F$

Reihenfolge der Bindung:

$$\boldsymbol{Quantoren}, (,), \neg, \wedge, \vee, \Rightarrow, \Leftrightarrow$$

$\forall x \in M \left(P(x)\right) = \forall x \left(x \in M \rightarrow P(x)\right)$
$\exists x \in M \left(P(x)\right) = \exists x \left(x \in M \wedge P(x)\right)$
$\neg \forall x\, P(x) = \exists x\, \neg P(x)$
$\forall x\, \neg P(x) = \neg \exists x\, P(x)$

Begriffe

Gültig/Wahr: unter einer Belegung
Allgemeingültig: unter jeder Belegung
Erfüllbar: mind. Unter einer Belegung
Unerfüllbar: unter keiner Belegung
Widerlegbar: mind. 1 Belegung ist ungültig
Konsequenz: A ist eine Konsequenz von B, wenn die Formale A⟶B allgemeingültig ist.

Syntax		Semantik
Partitur	⟷	Musik (Schallwellen)
Java Code	⟷	Verhalten eines Computers
Terme einer math. Theorie	⟷	Math. Objekte
Aussagenlogische Formeln	⟷	Boolesche Funktionen
Peano-Axiome	⟷	Die Struktur $(\mathbb{N}, +, \cdot)$
Feynman-Diagramm	⟷	Wechselwirkungen

Normalformen

Negationsnormalform: Keine Implikationen & Negation die nicht direkt vor einem Buchstaben sind.
Konjunktive Normalform (KNF):
$(A \vee B) \wedge C \wedge (A \vee B \vee \neg C)$ oder $(A \wedge C \wedge B)$ / $(A \vee C \vee B)$
Disjunktive Normalform (DNF):
$(A \wedge B) \vee C \vee (A \wedge B \wedge \neg C)$ oder $(A \vee C \vee B)$ / $(A \wedge C \wedge B)$

Belegung

$\hat{B}$ ist eine Ausweitung der Belegung B auf grössere Formeln.
Bsp.: $p\ oder \neg p$
$B(p) = true = \hat{B}(p)$
$B(p \wedge \neg p)\ existiert\ nicht$
$\hat{B}(p \wedge \neg p) = true, falls\ \hat{B}(p) und\ \hat{B}(\neg p)$

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

Beweistechniken

Direkter Beweis: A → B
durch Widerspruch: Annahme A wäre falsch → Widerspruch
durch Kontraposition: A → B beweisen ¬B → ¬A
durch Gegenbeispiel: Beispiel wo nicht stimmt
durch Äquivalenz: A ⍰ B beweisen A=> B und B=> A

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

Wahrheitstabelle

Aufgabe: Bilde die Wahrheitstabelle von (A ∨ B) ⇒ (C ∧ A)

A	B	C	(A ∨ B)	⇒	(C ∧ A)
w	w	w	w	w	w
w	w	f	w	f	f
w	f	w	w	w	w
w	f	f	w	f	f
f	w	w	w	f	f
f	w	f	w	f	f
f	f	w	f	w	f
f	f	f	f	w	f

Symbole

Summe: $\sum_{i=1}^{5} x_i = x_1 + x_2 + x_3 + x_4 + x_5$
Produkt: $\prod_{i=1}^{5} x_1 \times x_2 \times x_3 \times x_4 \times x_5$

Mengen

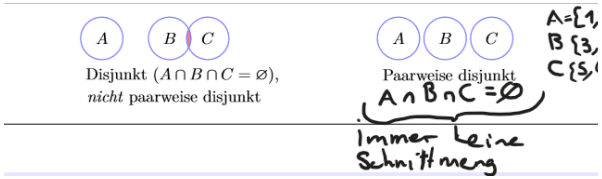
Zahlenmengen

Natürliche Zahlen: $\mathbb{N} = \{1; 2; 3\}$ oder $\mathbb{N}_0 = \{0; 1; 2; 3\}$
Ganze Zahlen: $\mathbb{Z} = \{-2; -1; 0; 1; 2; \}$
Rationale Zahlen: $\mathbb{Q}$ = Durch Bruch darstellbar
Reelle Zahlen: $\mathbb{R}$ =Alle Dezimalzahlen

Begriffe und Beispiele

{} = Menge, Reihenfolge egal
() = Tupel, Reihenfolge wichtig

Disjunkt
Zwei Mengen sind disjunkt, wenn sie kein gemeinsames Element haben. Wenn es mehrere Mengen gibt, sind sie paarwise disjunkt, wenn man zwei beliebige, vergleichen kann und sie disjunkt sind.



Geben Sie folgende Mengen explizit an.

(a) $\{1,3\} \times \{0,2\}$
(b) $A \times \{1, A\}$ wobei $A = \{2\}$.
(c) $\mathcal{P}(\varnothing \times \{\varnothing\})$
(d) $\mathcal{P}(\mathcal{P}(\{1\}))$
(e) $\mathcal{P}(\{\varnothing\} \times \{a, b\})$

Lösung:

(a) $\{(1,0),(1,2),(3,0),(3,2)\}$
(b) $\{(2,1),(2,\{2\})\}$.
(c) $\{\varnothing\}$ weil $\varnothing \times \{\varnothing\} = \varnothing$
(d) $\mathcal{P}(\{\varnothing,\{1\}\}) = \{\varnothing,\{\varnothing\},\{\{1\}\},\{\varnothing,\{1\}\}\}$
(e) $\mathcal{P}(\{\varnothing\} \times \{a,b\}) = \{\varnothing,\{(\varnothing,a)\},\{(\varnothing,b)\},\{(\varnothing,a),(\varnothing,b)\}\}$

Mengen

Teilmenge: A = {1;2}, B = {1;2;3} $A \subseteq B$ Jeds Element von A ist auch in B. Echt($\subset$) = nicht die gleiche Menge. Im Beispiel ist sie echt.
Schnittmenge: A = {1;2}, B = {1;2;3} $A \cap B = \{2\}$
Vereinigungsmenge: A = {1;2}, B = {3;4} $A \cup B = \{1; 2; 3; 4\}$
Differenz: A = {1;2}, B = {2;3}, $A \setminus B = \{1\}$
Kartesisches Produkt: A = {1;2}, B = {3;4} $A \times B =$ {(1,3); (1,4); (2,3); (2,4); } , Mächtigkeit = |AxB| = |A|*|B|
Potenzmenge: $P(\{a,b,c\}) = \{\emptyset,\{a\},\{b\},\{c\},\{a,b\},\{a,c\},$ $\{b,c\},\{a,b,c\}\}$, Mächtigkeit $|\boldsymbol{P(A)}| = \mathbf{2\text{^}|A|}$

Partitionen und Blöcke

Eine Partition $P = \{P_i | i \in I\}$ Zerlegung in Teilmengen (Beliebige disjunkte.)

- Die Elemente von *P* sind nicht leer und paarweise disjunkt
- $\bigcup_{i \in I} P_i = A$
- Vereinigung ergibt ursprüngliche Menge
- Partition = Menge aller Äquivalenzklassen

Die Elemente einer Partition werden Blöcke genannt.

Beispiel: Natürliche Zahlen in Partition 1. Gerade und 2. Ungerade
Alle Partitionen von $A = \{\{(1,0)\},\{(2,0)\}\{(3,0)\}\}$
$P_1 = \{\{(1,0)\},\{(2,0)\},\{(3,0)\}\}$
$P_2 = \{\{(1,0),(2,0)\},\{(3,0)\}\}$
$P_3 = \{\{(1,0)\},\{(2,0),(3,0)\}\}$
$P_4 = \{\{(1,0),(3,0)\},\{(2,0)\}\}$
$P_5 = \{A\}$

Rechenregeln

Mächtigkeit/Kardinalität: |X| = Anz. Elemente ($|\emptyset| = |\{\}| = 0$ und $|\{\emptyset\}|=1$ (+ {})

Gelten für $\cap$ *und* $\cup$:

Kommutativität:
$$A \cup B = B \cup A \; und \; A \cap B = B \cap A$$
Assoziativ:
$$A \cup (B \cup C) = (A \cup B) \cup C$$
$$A \cap (B \cap C) = (A \cap B) \cap C$$
Distributiv:
$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$
Idempotenz Gesetz:
$$A \cap A = A \; und \; A \cup A = A$$
De Morgan:
$$(C \backslash A) \cap (C \backslash B) = C \backslash (A \cup B)$$
$$(C \backslash A) \cup (C \backslash B) = C \backslash (A \cap B)$$

$$\overline{A \cup B} = \bar{A} \cap \bar{B} \quad und \quad \overline{A \cap B} = \bar{A} \cup \bar{B}$$

Beweis der Mengen Vergleiche

$$(A \cup B) \setminus C \subseteq A \cup (B \setminus C).$$

$$\begin{aligned} x \in (A \cup B) \setminus C &\Rightarrow x \in A \cup B \wedge x \notin C \\ &\Rightarrow (x \in A \vee x \in B) \wedge x \notin C \\ &\Rightarrow x \in A \vee (x \in B \wedge x \notin C) \\ &\Rightarrow x \in A \vee x \in B \setminus C \\ &\Rightarrow x \in A \cup (B \setminus C). \end{aligned}$$

$$\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B).$$

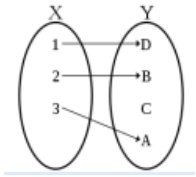
$$\begin{aligned} x \in \mathcal{P}(A \cap B) &\Leftrightarrow x \subseteq A \cap B \\ &\Leftrightarrow x \subseteq A \wedge x \subseteq B \\ &\Leftrightarrow x \in \mathcal{P}(A) \wedge x \in \mathcal{P}(B) \\ &\Leftrightarrow x \in \mathcal{P}(A) \cap \mathcal{P}(B). \end{aligned}$$

Relationen und Graphen

Eigenschaften zwischen Mengen

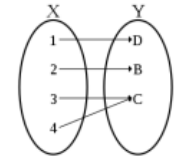
Injektiv (linkseundeutig)

Für jedes Element der Menge A gibt es genau eine Relation mit einem Element der Menge B. Es gibt kein Element der Menge B, welches Relationen mit mehreren Elementen A hat.



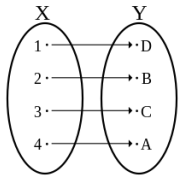
Surjektiv (rechtstotal)

Für jedes Element der Menge A gibt es mindestens eine Relation mit einem Element der Menge B. Es gibt kein Element der Menge B, welches keine Relation mit einem Element der Menge A hat.



Bijektiv

Für jedes Element der Menge A gibt genau eine Relation zur Menge B und jedes Element der Menge B hat genau eine Relation zur Menge A.



Eigenschaften von Relationen

Reflexivität:
Jedes Element steht zu sich selbst in Relation.
Beispiel: = Relation, 1 =1, 2 = 2
Gegen Beispiel < Relation, 1 < 1, 2 < 2 ist falsch

Transitivität:
~ ist eine Relation, a~b und b~c dann auch a~c
Beispiel: <= Relation 1 <= 2, 2 <=3 dann auch 1 <= 3
Gegen Beispiel: M alle Menschen, Sich kennen Relation: M1 kennt M2, M2 kennt M3, heisst nicht das M1 kennt M3

Symmetrisch: (Anti: a~b und b~a => a=b)
~ ist eine Relation, a~b dann auch b~a
Beispiel: = Relation 2 = 3 => 3 = 2
Gegen Beispiel: < Relation 2 < 3, 3 < 2 stimmt nicht

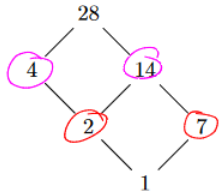
Totalität:
~ ist eine Relation, Es muss a~b oder b~a stimmen
Beispiel: < Relation, 2 < 3, 3 < 2 mindestens eines davon stimmt
Gegen Beispiel: Teiler Relation, 3~7, 7~3 beides stimmt nicht

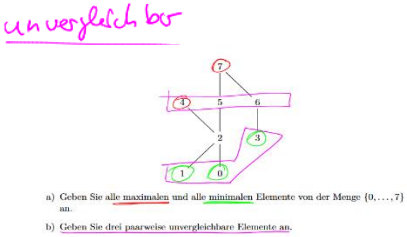
Ordnungen

Totalordnung: Reflexivität, Antisymmetrie, Transitivität, Totalität
Halbordnung: Reflexivität, Antisymmetrie, Transitivität
Wohlordnung: Ist eine Totalordnung, bei der jede nichtleere Teilmenge ein kleinstes Element besitzt
Wohldefinierte Funktion: Jedes Element aus Äquivalenzklasse hat gleichen Funktionswert

Hasse-Diagramm

Für Halbordnungen, anstatt Pfeile wird, die die Richtung nach oben verwendet.
Beispiel: Teilbarkeitsrelation auf der Menge Teilermenge von 28 ({1, 2, 4, 7, 14, 28})





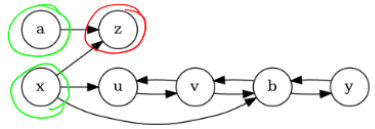
Begriffe

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. (Alle Pfeile zeigen weg davon)
- *R-maximal* in X, falls es kein anderes Element $y \in X$ mit *xRy* gibt. (Es zeigen nur Pfeile auf das Element)

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) $= z$



Linkstotal: Mindestens 1 Pfeil nach B für jedes Element von A
Rechtseindeutig: Maximal 1 Pfeil nach recht für jedes Element von A
Rechenregeln:
Falls X=> Y Injektiv und Y=>Z Injektiv dann ist auch X=>Z Injektiv
Falls X=> Y Surjektiv und Y=>Z Surjektiv dann ist auch X=>Z Surjektiv

Äquivalenzrelation/Klassen

Relation: reflexiv, symmetrisch und transitiv
Klasse: Sei ~ eine Äquivalenzrelation auf X. Für ein a aus X nennt man $[a] := \{x \in X \mid x \sim a\}$ die Äquivalenzklasse von a.

Beispiel: X = $\mathbb{Z}$ und $x_1 \sim x_2 : \Leftrightarrow 2 \mid (x_1 - x_2)$ (wenn die Differenz der beiden Zahlen gerade ist). Verschiedene Farben sind Klassen, ausser Grau
[0] = {0, 2, 4, ...}, [1] = 1, 3, 5, ...}, [10] = [0]
Zahl in der [] Klammer wird auch Representant gennent.

Binäre Relation

Binäre Relationen sind zweistellige Relationen, also Teilmengen des kartesischen Produkts $A \times B$ *der Mengen* A *und* B

Rekursive Strukturen und die natürlichen Zahlen

Induktion

Wird verwendet, um zu beweisen das A(n) für alle Natürlichen zahlen gilt: Wenn für A(n) folgendes gilt:

Induktionsverankerung: A (0) / Prüfung auf das kleinste Element

Induktionsannahme: $A(n)$

Induktionsschritt: $\forall n \in \mathbb{N}\big(A(n) \to A(n+1)\big)$,

folgt auch die Gültigkeit von $\forall n \in \mathbb{N}\big(A(n)\big)$

Beispiel: $0 + 1 + \cdots + n = \frac{n(n+1)}{2}$

Verankerung: $(n = 0)$: $A(0)$ *ist wahr weil*: $\frac{0\times1}{2} = 0$

Schritt:

$$\begin{aligned} 0+1+\cdots+n+(n+1) &= (0+1+\cdots+n)+(n+1) \\ &\overset{A(n)}{=} \frac{n(n+1)}{2}+(n+1) \\ &= \frac{n(n+1)+2(n+1)}{2} \\ &= \frac{(n+1)(n+2)}{2}. \end{aligned}$$

Bewiesen, weil bei beiden n + 1 gerechnet wurde und es immer noch stimmt; Ziel ist es in die n+1 Gleichung die I.A. einzufügen und die Gleichung stimmt weiterhin

Für jede Menge X von natürlichen Zahlen gilt:
Wenn X die Bedingungen:
- Induktionsverankerung: 0 ∈ X
- Induktionsschritt: ∀n (n ∈ X ⇒ n + 1 ∈ X)

erfüllt, dann ist bereits X = N.

Abzählbarkeit

Abzählbar: Hat gleiche Mächtigkeit wie Natürliche Zahlen. Sie können durchnummeriert werden. Es kann eine lehre Menge sein. Eine abzählbare Menge A hat:

- E eine surjektive Funktion $F: \mathbb{N} \to A$
- Eine injektive Funktion $F: A \to \mathbb{N}$
- Eine bijektive Funktion $F: A \to \mathbb{N}$
- Eine bijektive Funktion $F: \mathbb{N} \to A$

Überabzählbar: Beispiel Irrationale Zahlen. Zwischen 1 und 2 gibt es schon gleich viele Zahlen wie in $\mathbb{N}$, davon gibt es dann unendlich viele (2-3,4-5,…).

Der kleinste Verbrecher

Wenn nicht alle natürlichen Zahlen A(n) erfüllen, müsste es einen kleinsten Verbrecher **n** geben der A(n) nicht erfüllt. Führt diese Annahme zu einem Wiederspruch **erfüllen alle n. Zahlen A(n).**

Beispiel: jede n. Zahl die min. 2 Teiler hat, hat auch min. einen Primfaktor = A(n)

Wenn nicht gibt es eine Zahl und Menge: $\neg A(n), V = \{n \in N | \neg A(n)\} \neq \emptyset$

Behauptung: Jede nat. Zahl n > 1 hat PF

Beweis: Wenn nicht, dann sei $n_0 = \min(k \in N \mid 1 < k \wedge$ »k *hat keine PF*«

$n_0 \notin \mathbb{P}(Primzahlen) \Longrightarrow n_0 hat\ min.\ 3\ Teiler$

$\Longrightarrow \exists k(1 < k < n_0) \wedge$ k teilt $n_0 \Longrightarrow k \notin V \Longrightarrow k\ hat\ PF$

$sei\ p \in \mathbb{P}\ mit\ p\ teilt\ k \wedge k\ teilt\ n_0$

$\Longrightarrow p\ teilt\ n_0, die\ ist\ ein\ wiederspruch\ mit\ n_0 \in V$

$somit\ hat\ V\ kein\ min. Element\ und\ A\ ist\ als\ wahr\ bewiesen$

Rekursion

Explizit: Wert der Funktion direkt erkennbar Bsp: $a_n = n * 5$

Rekursiv: Wert muss zuerst ausgerechnet werden Bsp: $a_{n+1} = a_n + a_{n-1}$

Peano-Axiome

n' = Nachfolger von n

1. $\forall n(n \in \mathbb{N} \longrightarrow n' \in \mathbb{N})$ Jede natürliche Zahle hat einen Nachfolger (NF)
2. $\forall n(n \in \mathbb{N} \longrightarrow n' \neq 0)$ 0 ist kein NF
3. $\forall n, m(n, m \in \mathbb{N} \longrightarrow (n' = m' \longrightarrow n = m))$ Zahlen mit gleichem NF sind gleich

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

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

$$ggT(45,25) \overset{Satz\ 24}{=} ggT(25,20) \overset{Satz\ 24}{=} ggT(20,5) \overset{Satz\ 24}{=} ggT(5,15) \overset{Satz\ 24}{=} ggT(5,10) \overset{Satz\ 24}{=} ggT(5,5) = 5.$$

Erweitert, Beispiel Bézout:

$$a = q_1 \cdot b + r_0$$
$$b = q_2 \cdot r_0 + r_1$$
$$r_0 = q_3 \cdot r_1 + r_2$$

Verknüpfungstabelle

Für Z/6

·	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

1 kommt nicht vor ⇒ $\bar{2}^{-1}$ existiert nicht.

$\bar{5} \cdot \bar{5} = \bar{1} \Rightarrow \bar{5}^{-1} = \bar{5}$

kgV und ggT Formeln

n*m = kgV(n,m)*ggT(n,m)

falls n, m teilerfremd: ggT(n,m) = 1

ggT(n, m)= ggT(m, n)

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

ggT(n, m) = ggT(n, m-k*n)

Bézout Koeffizienten/Erweiterter Euklidischer Algo.

sind $x, y \in \mathbb{Z}$ *mit* $x, y \neq 0$; *dann gibt es* $ggT(x,y) = ax + by$

Beispiel: ggT(132,28)

		a=3	b=-14
1.	$132 = 4 \times 28 + 20$	3	$-2 - 4 \times 3 = -14$
2.	$28 = 1 \times 20 + 8$	-2	$1 - 1 \times -2 = 3$
3.	$20 = 2 \times 8 + 4$	1	$0 - 2 \times 1 = -2$
4.	$8 = 2 \times 4 + 0$	0	1
5.	ggT(132,28)=4	Immer minus die gelbe Zahl Schritt 4.	

wird hier übersprungen, weil Rest 0, koef, wird für Rest 4 berechnet

Primzahlen

Ist p eine Primzahl gilt: $T(p) = \{1, p\}\ und\ |T(p)| = 2$

Jede Zahl in $\mathbb{Z}$ besitzt mindestens einen Primfaktor

Es gibt unendlich Primzahlen

Primfaktorzerlegung

$24 = 2 \cdot 2 \cdot 2 \cdot 3 = 2^3 \cdot 3^1$

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

Modulare Arithmetik

$$r = s\ mod\ n \Rightarrow r \equiv_n s \Rightarrow s = q \times n + r$$

Äquivalenzklasse/Restklasse:

Äquivalenzklasse z von $\equiv_n$ heisst Restklassenmenge von z, geschrieben:

$$[z]_n\ oder\ \{x \in \mathbb{Z}\ |x \equiv_n z\}\ oder\ \bar{k} = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\}$$

Damit kann auch man rechnen:

Multiplikation: $[x]_n \times [y]_n = [x \times y]_n$

Addition: $[x]_n + [y]_n = [x + y]_n$

Primes Restklassen: $\mathbb{Z} *\!/n$ nur Restklassen die zu n teilerfremd sind

Multiplikatives Inverse

Theorem 8. *Es sei* $n \in \mathbb{N}\backslash\{1\}$ *beliebig. Folgende Aussagen sind äquivalent:*

1. *n ist eine Primzahl.*
2. *Für jedes* $\bar{k} \in \mathbb{Z}/n$ *mit* $\bar{k} \neq \bar{0}$ *gibt es genau ein* $r \in \{0, .., n-1\}$ *mit* $\bar{k} \cdot \bar{r} = \bar{1}$.

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

Übung 42. Es sei $n \in \mathbb{N}$ beliebig, dann heisst $k \in \mathbb{Z}/n$ invertierbar, falls es zu k inverse Elemente in $\mathbb{Z}/n$ gibt.

$\mathbb{Z}/3 = \{\bar{0}, \bar{1}, \bar{2}\}$ $\mathbb{Z}/4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ $\mathbb{Z}/5 = \{\bar{0}, \bar{1}, \dots \bar{4}\}$

a) Geben Sie alle invertierbaren Elemente von $\mathbb{Z}/n$ für $n = 1, 3, 4, 5$ an.

b) Lösen Sie $\bar{3}x = \bar{4}$ in $\mathbb{Z}/7$. $\bar{3}^{-1} = \bar{5} \Rightarrow x = \bar{6}$

$\mathbb{Z}/1 = \{\bar{0}\} = \{\bar{1}\} = \{100\}$

c) Geben Sie das bezüglich · zu $\bar{3}$ inverse Element in $\mathbb{Z}/11$ an. $\bar{4}$

Invertierbar: Kann man die Zahl mit etwas multiplizieren zum im Modulo Rest 1 zu bekommen?

Berechnung: Mit Erweiterter Euklidischer Algo. Muss als Rest +1 geben da ggT von den Zahlen auch 1 sein muss. $[5^{-1}]_7 = ggT(5,7) = a5 + b7 = 1 \Rightarrow 3 \times 5 + 2 \times 7 = 1$. Damit ist die Lösung 3

Berechnung Multiplikatives Inverse

Erweiterter Euklidischer Algo.:$[7^{-1}]_{20} = ggT(20,7)$

i	a	b	q	r	x	y
1	20	7	2	6	-1	$1 - 2 \times -1 = 3$
2	7	6	1	1	1	$0 - 1 \times 1 = -1$
3	6	1	6	0	0	1

Hier ist in Spalte 3b der ggT = 1 zu finden. Jetzt ist $1 = 20 \times x + 7y$ gesucht.

$1 = 20 \times -1 + 7 \times 3$ Die Lösung ist also 3

Wenn das Ergebnis negativ ist, muss man das Modulo – das Ergebnis Rechnen.

Beispiel 10 mod 11. Ergebnis ist -1 heisst das Inverse ist 11-1 = 10. Oder

Beispiel -2083 mod 665 ist 2083/665 = 3.13.. dann – volle Zahl + 1, also hier -4 = 0.867.. dann * den Modulo also hier 0.867 * 665 = 577

Chinesischer Restsatz

Wenn die Zahlen paarweise teilerfremd sind.

$$x \equiv 3\ mod\ 7$$
$$x \equiv 2\ mod\ 5$$
$$x \equiv 6\ mod\ 9$$

Zuerst lösen:

$$x \equiv 3\ mod\ 7$$
$$x \equiv 2\ mod\ 5$$

Erweiterter Euklidischer Algo.

$$7 = 1 \times 5 + 2$$
$$5 = 2 \times 2 + 1$$

Bézout Koeffizient:

$a_0 = 1, a_1 = 0$ $\quad$ $b_0 = 0, b_1 = 1$

$1 - 1 \times 0 = 1$ $\quad$ $0 - 1 \times 1 = -1$

$0 - 2 \times 1 = -2 = a$ $\quad$ $1 - 2 \times -1 = 3 = b$

Erste Lösung: vor grössere x/y das kleinere von a/b

$$x \times a \times (rest\ von\ y) + y \times b \times (rest\ von\ x)$$
$$x = 5 \times 3 \times 3 + 7 \times -2 \times 2 = 17$$

Wiederholen mit:

$$x \equiv 17\ mod\ (7 \times 5)$$
$$x \equiv 6\ mod\ 9$$

lösen. Wir teilen sukzessive mit Rest:

$$35 = 3 \cdot 9 + 8$$
$$9 = 1 \cdot 8 + 1.$$

Wir erhalten damit:

$$1 = 9 - 8$$
$$= 9 - (35 - 3 \cdot 9)$$
$$= 4 \cdot 9 + (-1) \cdot 35.$$

Eine Lösung ergibt sich erneut durch

$$x := 17 \cdot 4 \cdot 9 + 6 \cdot (-1) \cdot 35 = 402.$$

Die Lösungsmenge des ganzen Systems ist also $[402]_{35\text{-}9} = [87]_{315}$.

Chinesischer Restsatz 2

$x \equiv 3\ mod\ 7$ $\quad$ $a_1 = 3$ $\quad$ $m_1 = 7$ $\quad$ $m = m_1 \times m_2 \times m_3 \times m_4 = 3465$

$x \equiv 2\ mod\ 5$ $\quad$ $a_2 = 2$ $\quad$ $m_2 = 5$

$x \equiv 6\ mod\ 9$ $\quad$ $a_3 = 6$ $\quad$ $m_3 = 9$

$x \equiv 6\ mod\ 11$ $\quad$ $a_4 = 6$ $\quad$ $m_4 = 11$

Bestimmen von M_k:

$$M_1 = \frac{m}{m_1} = \frac{m_1 \times m_2 \times m_3 \times m_4}{m_1} = m_2 \times m_3 \times m_4 = 495$$
$$M_2 = \frac{m}{m_2} = m_1 \times m_3 \times m_4 = 693$$
$$M_3 = \frac{m}{m_3} = m_1 \times m_2 \times m_4 = 385$$
$$M_4 = \frac{m}{m_4} = m_1 \times m_2 \times m_3 = 315$$

Bestimmen von N_k:

$$N_1 = \left[{M_1}^{-1}\right]_{m_1} = [495^{-1}]_7 = [5^{-1}]_7 = [3]_7 = 3$$
$$N_2 = \left[{M_2}^{-1}\right]_{m_2} = [693^{-1}]_5 = [3^{-1}]_5 = [2]_5 = 2$$
$$N_3 = \left[{M_3}^{-1}\right]_{m_3} = [385^{-1}]_9 = [7^{-1}]_9 = [4]_9 = 4$$
$$N_4 = [{M_4}^{-1}]_{m_4} = [315^{-1}]_{11} = [7^{-1}]_{11} = [8]_{11} = 8$$

Bestimmen von Kongruenzen:

$$x \equiv a_1 \times M_1 \times N_1 + a_2 \times M_2 \times N_2 + \cdots\ mod\ m$$
$$x \equiv (3 \times 495 \times 3 + 2772 + 9240 + 15120) mod\ 3465$$
$$x \equiv 31587\ mod\ 3465$$
$$x \equiv 402\ mod\ 3465$$