Diskrete Mathematik

Logik

Junktoren

Zeichen	Prädikat	Bezeichnung
$\neg$	$\neg A$	NICHT A
$\wedge$	$A \wedge B$	A UND B
$\vee$	$A \vee B$	A ODER B
$\Rightarrow$	$A \Rightarrow B$	WENN A DANN B
$\Leftrightarrow$	$A \Leftrightarrow B$	A GLEICH B

Negation: $\neg A$ => kehrt den Wahrheitswert um

Konjunktion: $A \wedge B$

Disjunktion: $A \vee B$

Äquivalenz: $A \leftrightarrow B$ => gleicher Wahrheitswert

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 $A \wedge \neg A = W$

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

💡 *Wenn xyz , dann abc :* Falls xyz falsch, dann alles WAHR.

Quantoren

- Allquantor : ∀x "für alle.."
- Existenzquantor: $\exists x$

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 Logik

Mindestens 3 mit G(x):

$$\exists x, y, z(G(x) \wedge G(y) \wedge G(z) \wedge x \neq y \wedge x \neq z \wedge y \neq z)$$

Höchstens 2 mit G(x):

$\neg(\exists x, y, z(G(x) \wedge G(y) \wedge G(z) \wedge x \neq y \wedge x \neq z \wedge y \neq z))$

Es gibt genau ein x mit P(x) ⇔ ∃x (P(x)) ∧ ∀y, z (P(y) ∧ P(z) ⇒ y = z)
Es gibt mindestens zwei Dinge mit der Eigenschaft P ⇔ ∃x, y (P(x) ∧ P(y) ∧ x ≠ y)
Es gibt höchstens ein x mit P(x) ⇔ ¬∃x, y (P(x) ∧ P(y) ∧ x ≠ y)
Wenn P(x) und P(y) gilt, dann gilt stets auch Q(x, y) ⇔ ∀x, y (P(x) ∧ P(y) ⇒ Q(x, y))
Für kein x gilt Q(x, x) ⇔ ∀x¬Q(x, x)

Umformungsregeln:

Vertauschungsregel für unbeschränkte Quantoren: ∀xA(x) ⇔ ¬∃x¬A(x)

Beschränkter und unbeschränkter Allquantor: ∀x ∈ K A(x) ⇔ ∀x(x ∈ K ⇒ A(x))

Beschränkter und unbeschränkter Existenzquantor: ∃x ∈ K A(x) ⇔ ∃x(x ∈ K ∧ A(x))

Semantik

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

Beispiele:

Gegeben sei eine Belegung $B : V \rightarrow \{false, true\}$

$B(p) = B(q) = B(r) = B(s) = true$

$B(u) = B(v) = false$

$\hat{B}$ von folgendem ist:

1. $p \rightarrow s$

   $\hat{B}(p \rightarrow s) = \hat{B}(\neg p \vee s) = OR(\hat{B}(\neg p), \hat{B}(s))$

   → B hat von (s) im OR statement ist true, somit ist der Ausdruck TRUE.

2. $(u \rightarrow r) \wedge s$

   $AND(\hat{B}(u \rightarrow r), \hat{B}(s))$

   B hat von s ist false, also kann gestrichen werden.

   ⇒ $\hat{B}(u \rightarrow r) = \hat{B}(\neg u \vee r) = OR(\hat{B}(\neg u), \hat{B}(r))$

   $\hat{B}(r)$ im OR statement ist TRUE, somit ist der Ausdruck TRUE.

Teilformen:

p_0	q	p_1	$q \lor p_1$	$p_0 \to (q \lor p_1)$
0	0	0	0	1
0	0	1	1	1
0	1	0	1	1
0	1	1	1	1
1	0	0	0	0
1	0	1	1	1
1	1	0	1	1
1	1	1	1	1

- Allgemeingültig
  - wenn unter jeder Belegung true
  - Wahrheitstabelle (ganz rechts) alles 1
- Wiederlegbar
  - Wahrheitstabelle ganz rechts mindestens ein 0

- *Gesetz der doppelten Negation:* $\neg\neg F \equiv F$
- *Absorption:* $F \land F \equiv F$ *und* $F \lor F \equiv F$
- *Kommutativität:* $F \land G \equiv G \land F$ *und* $F \lor G \equiv G \lor F$
- *Assoziativität:* $F \land (G \land H) \equiv (F \land G) \land H$
- *Assoziativität:* $F \lor (G \lor H) \equiv (F \lor G) \lor H$
- *Distributivität:* $F \land (G \lor H) \equiv (F \land G) \lor (F \land H)$
- *Distributivität:* $F \lor (G \land H) \equiv (F \lor G) \land (F \lor H)$
- *De Morgan:* $\neg(F \land G) \equiv \neg F \lor \neg G$
- *De Morgan:* $\neg(F \lor G) \equiv \neg F \land \neg G$
- *Kontraposition:* $F \to G \equiv \neg G \to \neg F$

p	q	$\neg p$	$\neg q$	$p \to q$	$\neg q \to \neg p$	$(p \to q) \to (\neg q \to \neg p)$
0	0	1	1	1	1	1
0	1	1	0	1	1	1
1	0	0	1	0	0	1
1	1	0	0	1	1	1

Semantische Eigenschaften

- Erfüllbar
  - wenn mindestens eine Belegung true
  - Wahrheitstabelle ganz rechts mindestens ein 1.
- Unerfüllbar
  - wenn unter keiner Belegung true
  - Wahrheitstabelle alle werte ganz rechts auf 0

Beweisen:

$\neg\neg F \equiv F$

$\hat{B}(\neg\neg F) \equiv \hat{B}(F)$

$\hat{B}(\neg\neg F) \equiv NOT(\hat{B}(\neg F)) \equiv NOT(NOT(\hat{B}(F)) = \hat{B}(F)$

Normalformen

NNF (Negationsnormalform)

- keine Implikation $\rightarrow$
- negationen nur direkt beim Literal ($\neg p$)

KNF (konjuktive Normalform)

Literale: $L_{i,j}$

$(L_{1,1} \lor L_{1,2} \lor ...) \land (L_{2,1} \lor L_{2,2} \lor ...) \land (...)$

DNF (disjunktive Normalform)

Literale: $L_{i,j}$

$(L_{1,1} \land L_{1,2} \land ...) \lor (L_{2,1} \land L_{2,2} \land ...) \lor (...)$

💡 DNF und KNF sind auch immer NNF

Formel in Normalform bringen:

Beispiel 14. Wir bringen die Formel

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

in DNF. 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:

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

Die Formel, die wir erhalten haben, ist sowohl in NNF als auch in DNF. Wir k

$$(p \wedge p_1) \vee (p_2 \wedge p_3)$$

äquivalente Formel in KNF. Wir wenden sukzessive die Distributivgesetze an:

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

Wahrheitstabellen

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

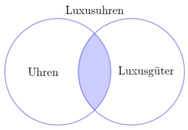
KNF $\wedge$**:** Bildung einer Disjunktion $\vee$ aus jeder Zeile die false liefert = Maxterm $(a \vee b \vee c) \wedge$ ...

Mengen

$y \in X$: y ist ein Element von X.

$y \notin X$: y ist kein Elment von X.

Schnittmenge

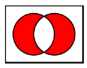


Veranschaulichung der Mengenbildung durch Schnitt von zwei Mengen.

$X \cap Y$

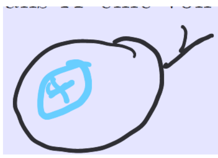
Symmetrische Differenz

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



$X \subset Y$: X ist eine Teilmente von Y.

$X \subsetneq Y$: X ist eine echte Teilmenge von Y.

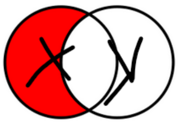


Disjunkt

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

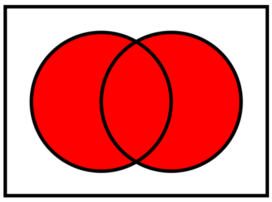
Disjunkt ($A \cap B \cap C = \emptyset$), *nicht* paarweise disjunkt

Paarweise disjunkt



$X \setminus Y$:= Menge aller Elemente von X die NICHT zu Y gehören.

Vereinigung



$X \cup Y$

Potzenzmenge

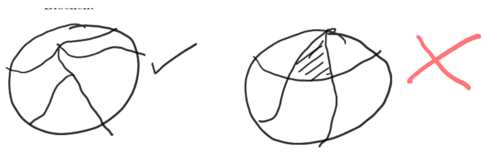
A ist ein beliebige Menge, $\mathcal{P}(A)$ ist die Potenzmenge von A. Bedeutet genau die Teilmengen A als Elemente.

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

💡 Immer folgendes Schema: {leer}, {alle} {kombinationen}, {ganze menge}

Partitionen

b)Eine Partition P={P_i|$i \in I$} einer Menge A, ist eine Menge von Teilmengen wiederrum von A. Ein Element von P wird Block (Blöcke) genannt.



- Die elemente von P sind nichtleer und paarweise diskjunkt.

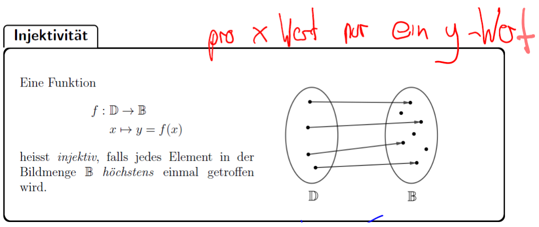
Kartesisches Produkt

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

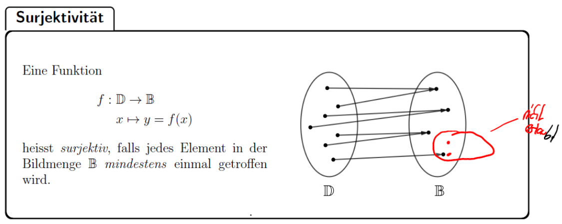
$\{1,3\} \times \{0,2\} = \{(1,0),(1,2),(3,0),(3,2)\}$
$\emptyset \times \{\emptyset\} = \emptyset$

Unendlichkeit

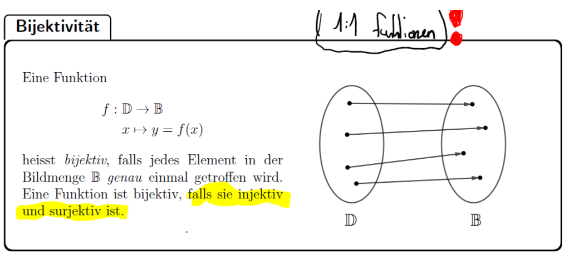
Injektiv



Surjektiv



Bijektiv



Grössenvergleich

Definition 33.

- Eine Menge X heisst *endlich*, wenn es eine natürliche Zahl n und eine Darstellung der Form $X = \{x_1, x_2, \ldots, x_n\}$ gibt. Wenn $X = \{x_1, \ldots, x_n\}$ gilt, und die Elemente x_i paarweise verschieden sind (d.h. es gilt $i \neq j \Rightarrow x_i \neq x_j$), dann hat die Menge X genau n viele Elemente und wir schreiben $|X| = n$.
- Nicht endliche Mengen nennen wir *unendlich*.
- Eine Menge X heisst *abzählbar*, wenn eine surjektive Funktion $F : \mathbb{N} \to X$ existiert oder wenn $X = \varnothing$ gilt.
- Die Menge X heisst *abzählbar unendlich*, wenn X abzählbar und unendlich ist.
- Eine *überabzählbare* Menge ist eine Menge, die nicht abzählbar ist.

Abzählbar unendlich	gleichmächtig wie N (bijektive Funktion «Zuordnung existiert»)	N, Z, Q, N x N, Z x Z
Überabzählbar unendlich	grösser als N	(0, 1) = alle unendlichen Binärsequenzen

Relationen

Binäre Relationen R auf einer Menge X :

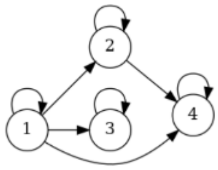
gilt immer für ALLE $x \in X$

Reflexion

xRx

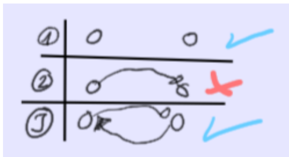
Äquivalenzrelationen

💡 sind relfexiv, symetrische und transitive Relationen

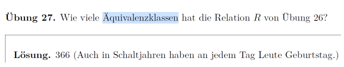


Symetrisch

$xRy \to yRx$



Äquivalenzklassen

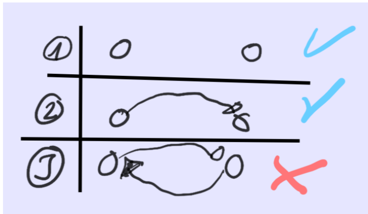


Übung 27. Wie viele Äquivalenzklassen hat die Relation R von Übung 26?

Lösung. 366 (Auch in Schaltjahren haben an jedem Tag Leute Geburtstag.)

Antisymetrisch

$xRy \wedge yRx \to x = y$



Transitiv

$xRy \wedge yRz \to xRz$

Ordnungsrelationen

R-unvergleichbar

falls weder xRy noch yRx gilt

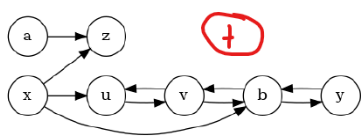
R-maximal

kein anderes Element $y \in X$ mit xRy

R-minmal

kein anderes Element $y \in X$ mit yRx

Beispiel:



minimalen Elemente: a,x

maximalen Elemente: z

unvergleichbar: t

	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

Präordnung

R reflexiv und transitiv

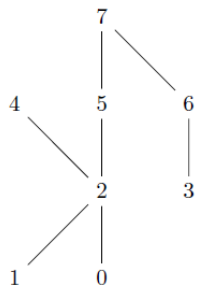
Total / lineare Ordnung

Halbordnung & keine R-unvergleichbaren Elemente

DAG

gerichteter, zyklenfreier Graph => z.B. Hasse Diagramm

Hasse-Diagramm



Paarweise unvergleichbar:
Im Hasse Diag. auf einer Linie!

Halbordnung

reflexiv, antisymmetrisch und transitiv

Wohlordnung

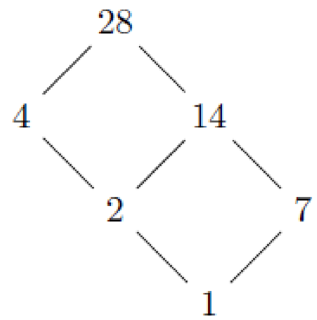
wenn R eine totale Ordnung ist so, dass jede Teilmenge von M (mindestens) ein R-minimales Element enthält

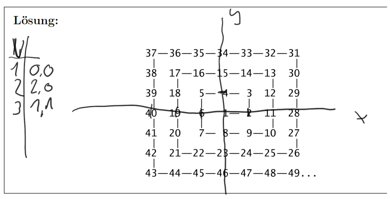
R^+

transitiver Abschluss = {(1,1), (1,2), (2,3), (1,3)}

R^*

reflexiv-transitiver Abschluss





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

Induktion & Rekursion

Induktion

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

1 . IA: $n = 0$

links:

$$\sum_{k=1}^{n} k = \sum_{k=1}^{0} = 0$$

rechts:

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

2 . IV: $\exists\, n \in \mathbb{N} : \sum_{k=1}^{n} k = \frac{n(n+1)}{2}$

3 . IS: $n \to n+1$

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

ZZ: $\sum_{k=1}^{n+1} k = \frac{(n+1)(n+2)}{2}$

$$\sum_{i=1}^{0} a_i = 0$$

$$\sum_{i=1}^{n+1} a_i = (\sum_{i=0}^{n} a_i) + a_{n+1}$$

Für $n = 0$ ist $0^5 - 0 = 0$. Da 0 durch jede Zahl teilbar ist, ist sie auch durch 5 Induktionsanfang bewiesen.

2. Induktionsschritt:

2a. Induktionsvoraussetzung:

$n^5 - n$ ist durch 5 teilbar.

2b. Induktionsbehauptung:

$(n+1)^5 - (n+1)$ ist durch 5 teilbar.

2c. Beweis des Induktionsschritts:

Es gilt:

$$(n+1)^5 - (n+1) = n^5 + 5n^4 + 10n^3 + 10n^2 + 5n + 1 - n - 1$$
$$= \underbrace{(n^5 - n)}_{\text{durch 5 teilbar (IV)}} + \underbrace{5(n^4 + 2n^3 + 2n^2 + n)}_{\text{durch 5 teilbar}}$$

links: “auseinander nehmen”: $\sum_{k=1}^{n+1} k = \sum_{k=0}^{n} k + (n+1) \overset{IV}{=} \frac{n(n+1)}{2} + (n+1)$ = $\frac{(n+1)(n+2)}{2}$ qed

Elementare Zahlentheorie

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

Teilbarkeit

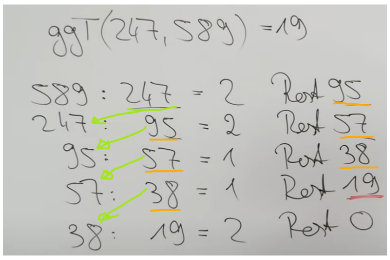
Eine ganze Zahl a heißt durch eine natürliche Zahl b teilbar, wenn es eine ganze Zahl n gibt, sodass $a = n \cdot b$ ist. Die Zahl b heißt in diesem Fall Teiler von a. Man schreibt dafür $b|a$, gelesen: «b teilt a».

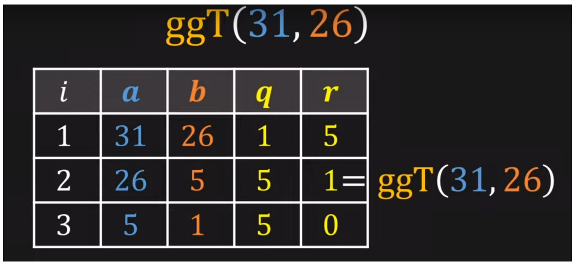
Teilermenge: $T(y) = \{x \in \mathbb{N} | x|y\}$
Teilerfremd: Zwei ganze Zahlen x, y heissen teilerfremd, wenn ggT (x, y) = 1 gilt

ggT

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

Euklidischer Algorithmus zur Bestimmung von ggT(a,b)

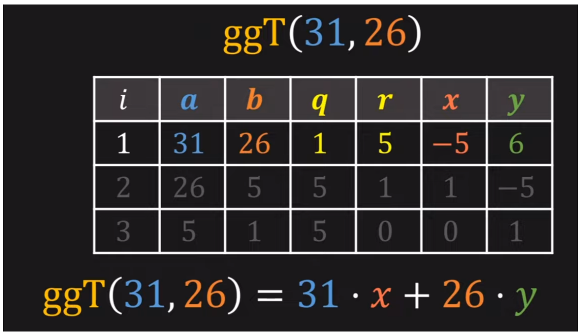




ggT(31, 26)

i	a	b	q	r	
1	31	26	1	5	
2	26	5	5	1 =	ggT(31, 26)
3	5	1	5	0	

erweiterter Euklidischer Algorithmus zur Bestimmung von ggT(a, b)



ggT(31, 26)

i	a	b	q	r	x	y
1	31	26	1	5	−5	6
2	26	5	5	1	1	−5
3	5	1	5	0	0	1

$\mathrm{ggT}(31, 26) = 31 \cdot x + 26 \cdot y$

1. $x_3 = 0;$ $\quad y_3 = 1$
2. $x_2 = y_3 = 1$ $\quad y_2 = x_3 - q_2 \cdot y_3 = 0 - (5 \cdot 1) = -5$
3. $x_1 = y_2 = -5$ $\quad y_1 = x_2 - q_1 \cdot y_2 = 1 - (1 \cdot -5) = 4$

Wenn in der obersten zeile angekommen = fertig.

$31 \cdot x + 26 \cdot y = 31 \cdot -5 + 26 \cdot 6$

Multiplikative Inverse

Wenn $ggt(x, n) = 1 \rightarrow$ multiplakatives inverses

$ggt(x, 12) = 1$

x = 1 → ja

x = 2 → nein (weil 2 ist ggt)

x = 3 → nein (weil 3 ist ggt)

x = 4 → nein

Beispiel:

Welche Elemente von $\mathbb{Z}/12$ besitzen multiplikative Inverse?

$\mathbb{Z}/12 = \{1, 2, 3, 4.., 11\}$

$Lösung: \; \{1, 5, 7, 11\}$

x = 5 → ja

...

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 $a \equiv b \ (mod\ m)$. Die Zahl m heisst Modul. → 17 ≡ 22 (mod 5)

Zwei Zahlen sind also genau dann kongruent modulo m, wenn sie sich um ein Vielfaches von m unterscheiden.

Chinesischer Restatz

TR: Q....r

$$x \equiv_7 3$$
$$x \equiv_5 2$$
$$x \equiv_9 6$$

$$a_1 = 3, a_2 = 2, a_3 = 6$$

$$m_1 = 7, m_2 = 5, m_3 = 9$$

$$M = m_1 \cdot m_2 \cdot m_3 = 7 * 5 * 9 = 315$$

$$x = a_1 \cdot m_2 \cdot m_3 \cdot x_1 + a_2 \cdot m_1 \cdot m_3 \cdot x_2 + a_3 \cdot m_1 \cdot m_2 \cdot x_3$$

$$x = 3 * 5 * 9 * 5 + 2 * 7 * 9 * 2 + 6 * 7 * 5 * (-1)$$

$$x = 675 + 252 - 210 = 717$$

$$x\ mod\ M = 717\ mod\ 315 = 87$$

$$Lösung : [87]_{315}$$

$$x = 87 + z * 315, z \in \mathbb{Z}$$

$$x_1 \cdot m_2 \cdot m_3 \equiv 1\ mod\ 7$$

$$m_2 \cdot m_3\ mod\ 7 :$$

$$5 \cdot 9\ mod\ 7 = 45\ mod\ 7 = 3$$

$$x_1 \cdot 3 \equiv 1\ mod\ 7 \Rightarrow \underline{x_1 = 5}$$

$$x_2 \cdot m_1 \cdot m_3 \equiv 1\ mod\ 5$$

$$63\ mod\ 5 = 3$$

$$x_2 \cdot 3 \equiv 1\ mod\ 5 \Rightarrow \underline{x_2 = 2}$$

$$x_3 \cdot m_1 \cdot m_2 \equiv 1\ mod\ 9$$

$$35\ mod\ 9 = 8$$

$$x_3 \cdot 8 \equiv 1\ mod\ 9 \Rightarrow \underline{x_3 = -1}$$