Formelsammlung - Grundlagen der Mathematik - Stand: 02.02.2014 - Christian Löhle

Logik

		Negation	Konjunktion	Disjunktion	Exklusives Oder	Implikation	Äquivalenz
		Nicht A	A und B	A oder B	Entweder A oder B	wenn A dann B	A genau dann wenn B
A	B	$\neg A$	$A \wedge B$	$A \vee B$	$A \oplus B$	$A \Rightarrow B$	$A \Leftrightarrow B$
0	0	1	0	0	0	1	1
0	1	1	0	1	1	1	0
1	0	0	0	1	1	0	0
1	1	0	1	1	0	1	1

Eine Formel F heißt:

- **erfüllbar**, wenn F bei mindestens einer Variabelbelegung 1 ist.
- **unerfüllbar**, wenn F bei jeder Variabelbelegung 0 ist.
- **Tautologie($\top$)/gültig**, wenn F bei jeder Variabelbelegung 1 ist.

Rechengesetze:

Kommutativgesetze:

$x \wedge y = y \wedge x$

$x \vee y = y \vee y$

Assoziativgesetze:

$x \wedge (y \wedge z) = (x \wedge y) \wedge z$

$(x \vee y) \vee z = x \vee (y \vee z)$

Distributivgesetze:

$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$

$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$

Absorptionsgesetze:

$x \wedge (x \vee y) = x$

$x \vee (x \wedge y) = x$

De Morgansche Gesetze:

$\neg(x \wedge y) = \neg x \vee \neg y$

Sonstiges:

$x \oplus 0 = x$

$x \oplus 1 = \neg x$

$x \oplus y = (x \vee y) \wedge \neg(x \wedge y) = (x \wedge \neg y) \vee (\neg x \wedge y)$

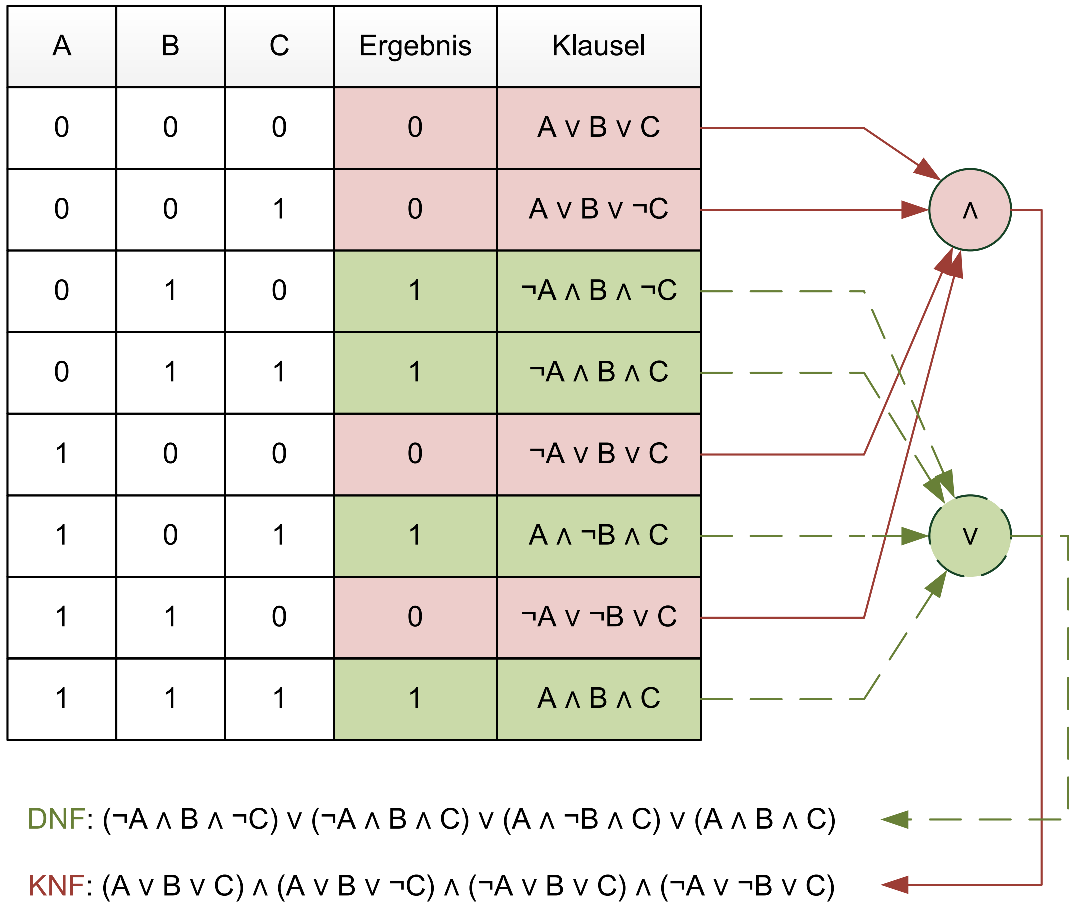
$x \Rightarrow y = \neg x \vee y$

Normalformen:

Disjunktive Normalform(DNF) besteht aus einer Disjunktion($\vee$) von Konjunktionstermen($\wedge$). Nehme die Variabelbelegung(z.B. $A \wedge \neg B \wedge \neg C$) wo F=1 ist und verknüpfe sie mit $\vee$.

Konjunktive Normalform(KNF) besteht aus einer Konjunktion($\wedge$) von Disjunktionstermen($\vee$). Nehme die Variabelbelegung(z.B. $A \wedge \neg B \wedge \neg C$) wo F=0 ist, **negiere** sie($\neg A \wedge B \wedge C$) und verknüpfe sie mit $\vee$.

Normalformen sind möglich, da $\wedge$, $\neg$ und $\vee$, $\neg$ eine vollständige Basis für die Aussagenlogik bilden. Um zu zeigen, dass andere Operatoren ebenfalls eine vollständige Basis bilden, muss man $\wedge$, $\neg$ oder $\vee$, $\neg$ als Formel bilden.



A	B	C	Ergebnis	Klausel
0	0	0	0	A ∨ B ∨ C
0	0	1	0	A ∨ B ∨ ¬C
0	1	0	1	¬A ∧ B ∧ ¬C
0	1	1	1	¬A ∧ B ∧ C
1	0	0	0	¬A ∨ B ∨ C
1	0	1	1	A ∧ ¬B ∧ C
1	1	0	0	¬A ∨ ¬B ∨ C
1	1	1	1	A ∧ B ∧ C

Mengen
[n] := {1, 2, 3, ..., n}
A = {1, 3, 7, 21} ⇒ |A| = 4
Die **Potenzmenge** $\mathcal{P}(A)$ ist eine neue Menge, die aus allen Teilmengen von A besteht.
$\mathcal{P}(\emptyset) = \{\emptyset\}$
$\mathcal{P}(\{a\}) = \big\{\emptyset, \{a\}\big\}$
$\mathcal{P}(\{a,b\}) = \big\{\emptyset, \{a\}, \{b\}, \{a,b\}\big\}$
$\mathcal{P}(\{a,b,c\}) = \big\{\emptyset, \{a\}, \{b\}, \{c\}, \{a,b\}, \{a,c\}, \{b,c\}, \{a,b,c\}\big\}$
$\mathcal{P}(\mathcal{P}(\emptyset)) = \big\{\emptyset, \{\emptyset\}\big\}$
$|\mathcal{P}(A)| = 2^{|A|}$

Operationen auf Mengen:

- Schnitt: $A \cap B := \{x \mid (x \in A) \wedge (x \in B)\}$
- Vereinigung: $A \cup B := \{x \mid (x \in A) \vee (x \in B)\}$
- Differenz: $A \setminus B := \{x \mid (x \in A) \wedge (x \notin B)\} = A \cap \neg B$
- Symmetrische Differenz: $A \triangle B := (A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$

Rechengesetze:

- Reflexivität: $A \subseteq A$
- Antisymmetrie: $AusA \subseteq BundB \subseteq AfolgtA = B$
- Transitivität: Aus $A \subseteq B$ und $B \subseteq C$ folgt $A \subseteq C$
  Die Mengen-Operationen Schnitt ∩ und Vereinigung ∪ sind kommutativ, assoziativ und zueinander distributiv:
- Assoziativgesetz: $(A \cup B) \cup C = A \cup (B \cup C)$ und $(A \cap B) \cap C = A \cap (B \cap C)$

- Kommutativgesetz: $A \cup B = B \cup A$ und $A \cap B = B \cap A$
- Distributivgesetz: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ und $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
- De Morgansche Gesetze: $\neg (A \cup B) = \neg A \cap \neg B$ und $\neg (A \cap B) = \neg A \cup \neg B$
- Absorptionsgesetz: $A \cup (A \cap B) = A$ und $A \cap (A \cup B) = A$
  Differenzmenge:
- Assoziativgesetze: $(A \setminus B) \setminus C = A \setminus (B \cup C)$ und $A \setminus (B \setminus C) = (A \setminus B) \cup (A \cap C)$
- Distributivgesetze: $(A \cap B) \setminus C = (A \setminus C) \cap (B \setminus C)$ und $(A \cup B) \setminus C = (A \setminus C) \cup (B \setminus C)$ und $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$ und $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$
  Sonstiges:
- $A \triangle B = \neg A \triangle \neg B$
- $A \setminus B = \neg B \setminus \neg A$

Kartesisches Produkt:
$A \times B := \{(a, b) \mid a \in A, b \in B\}$
$A^2 = A \times A = \{(a, a') \mid a, a' \in A\}$
Sei $A = \{a, b, c\} und B = \{x, y\}$ dann gilt:
$A \times B = \{(a, x), (a, y), (b, x), (b, y), (c, x), (c, y)\}$
$B \times A = \{(x, a), (x, b), (x, c), (y, a), (y, b), (y, c)\}$
$A \times A = \{(a, a), (a, b), (a, c), (b, a), (b, b), (b, c), (c, a), (c, b), (c, c)\}$
Ausserdem: $|A_1 \times A_2 \times A_3 \times ... \times A_n| = |A_1| * |A_2| * |A_3| * ... * |A_n|$ wenn A_1 bis A_n endlich sind.

Summen
Sei $m > n$ dann gilt: $\sum_{k=m}^{n} a_k = 0$

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

Konstantes Glied(wie bei Gauss): $\sum_{k=m}^{n} x = (n - m + 1)x$

$\sum_{k=m}^{n} c \cdot a_k = c \cdot \sum_{k=m}^{n} a_k$

Geometrische Reihe: $s_n = a_0 \sum_{k=0}^{n} q^k = a_0 \frac{1-q^{n+1}}{1-q}$

Aufteilung: $\sum_{k=m}^{n} a(k) = \sum_{k=m}^{l} a(k) + \sum_{k=l+1}^{n} a(k)$

Vollständige Induktion
Die Gaußsche Summenformel lautet: Für alle natürliche Zahlen n ≥ 1 gilt

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

Der Induktionsanfang ergibt sich unmittelbar:

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

Der Induktionsschritt wird über folgende Gleichungskette gewonnen, bei der die Induktionsvoraussetzung mit der zweiten Umformung verwendet wird:

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

Relationen

Eine Relation ist eine Teilmenge des Kreuzprodukt zweier Mengen: $R \subseteq A \times B$

Sei Relation R $\subseteq [4]^2$ und R $= \{(1,2),(2,1),(2,3),(3,4)(4,3)\}$, dann ist die Adjazenzmatrix R $= \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$

Verkettung: $S \circ R := RS := \{(a,d) \in A \times D \mid \exists\, b \in B \cap C \colon (a,b) \in R \wedge (b,d) \in S\}$
Umkehrrelation: $R^{-1} = \{(b,a) \in B \times A \mid (a,b) \in R\}$ Man erhält die Umkehrrelation an einem Graphen indem man die Pfeilspitzen umdreht. An der Adjazenzmatrix muss man alle 1en an der Hauptdiagonalen spiegeln.

Eigenschaften von Relationen:
Reflexivität(R): $\forall a \in A \colon (a,a) \in R$ Jedes Element steht zu sich selbst in Relation. Die Hauptdiagonale ist 1.
Symmetrie(S): $\forall a,b \in A \colon (a,b) \in R \Rightarrow\ (b,a) \in R$ Pfeilspitzen sind immer auf beiden Seiten, können dann auch weggelassen werden(ungerichtet Graph). Die Adjazenzmatrix ist symmetrisch zur Hauptdiagonalen
Transitivität(T): $\forall a,b,c \in A \colon (a,b) \in R\ \wedge\ (b,c) \in R \Rightarrow (a,c) \in R$ Wenn es einen Weg über mehrere Relationen von einem Knoten zum Anderen gibt, müssen diese auch direkt in Relation stehen.
Asymmetrie: $\forall a,b \in A \colon (a,b) \in R \Rightarrow (b,a) \notin R$ Pfeilspitze immer nur auf maximal einer Seite. Keine Reflexivität.
Antisymmetrie(AS): $\forall a,b \in A \colon (a,b) \in R\ \wedge\ (b,a) \in R \Rightarrow\ a = b$ Gleich wie Asymmetrie, aber Reflexivität ist erlaubt.
Totalität(TO): $\forall a,b \in A \colon (a,b) \in R\ \vee\ (b,a) \in R$ Zwischen zwei beliebigen Knoten gibt es immer eine Relation in mindestens eine Richtung.
R heißt **Äquivalenzrelation** wenn (R), (S) und (T) gelten.
R heißt **Halbordnung** wenn (R), (AS) und (T) gelten.
R heißt **(Totale) Ordnung** wenn sie eine Halbordnung ist und (TO) erfüllt.
Die **Äquivalenzklasse** eines Objektes a ist die Klasse der Objekte, die äquivalent zu a sind. Sei R $\subseteq A^2$.
$[a]_R = \{x \in A \mid (x,a) \in R\} \subseteq M$
Der **Quotient** von R bezüglich R ist die Menge A/R $= \{[a[_R \mid a \subseteq A\}$ (Die Anzahl Äquivalenzklassen)
Ein Graph beschreibt nur dann eine Halbordnung, wenn er azyklisch ist(da Symmetrie $\implies$ azyklisch)

Eine Relation heißt **Funktion**, wenn sie eindeutig ist, sprich von jedem Knoten genau ein Pfeil weggeht. Eine Funktion f ordnet jedem Element x einer Definitionsmenge D genau ein Element y einer Zielmenge Z zu. $f \colon D \to Z,\ x \mapsto y$.
Eine Funktion ist **injektiv**, wenn jedes Element der Zielmenge höchstens ein Urbild hat. D. h. aus $f(x_1) = y = f(x_2)$ folgt $x_1 = x_2$.
Sie ist **surjektiv**, wenn jedes Element der Zielmenge mindestens ein Urbild hat. D. h. zu beliebigem y gibt es ein x, so dass f(x)=y.
Gelten diese beiden Eigenschaften für f, nennt man f **bijektiv**. wenn eine Funktion bijektiv ist ihre Umkehrfunktion(f^{-1}) auch eine (bijektive) Funktion.
Eine bijektive Funktion $f\colon$ [n]$\to$[n] heißt **Permutation**. Die Adjazentmatrix einer Permutation hat in jeder Spalte und Zeile genau eine 1. $\quad \varphi^0 = \ id \quad\quad \varphi^2 = \varphi \circ \varphi$
Bsp: S_6

k	1	2	3	4	5	6
$\varphi(k)$	4	6	5	2	3	1
φ^2	2	1	3	6	5	4
φ^0	1	2	3	4	5	6

Die Ordnung von φ ist dann wie oft sich φ mit sich selbst verknüpfen lässt bis wieder id herauskommt und eins dazu addiert(wegen φ^0). Die Ordnung von dem Beispiel wäre 5 da $\varphi^4 = \varphi^0$.
Die Vorgehensweise um die nächstgrößten Permutation zu bestimmen ist:

1. Bestimme längstes abfallend-sortiertes Endstück.

2. Erhöhe vorgehende Zahl kleinstmöglich mit einer der Ziffer rechts davon.

3. Sortiere Endstück aufsteigend.

Graphentheorie

Ein ungerichteter Graph G=(V,E) heißt **Baum**, falls G azyklisch und zusammenhängend ist.
Ein ungerichteter Graph G=(V,E) heißt **Wald**, falls G azyklisch ist. Die Anzahl der benachbarten Knoten eines Knoten v nennt man **grad(v)**. Ist grad(v) = 1 heißt der Knoten **Blatt**.
Man nennt einen Graph **planar**, wenn man ihn ohne Überschneidungen zeichnen kann. Der **Satz von Kuratowski** besagt, dass K5 und K3,3 die einzig nichtplanaren Graphen sind, ein nichtplanarer Graph muss also einer der beiden Graphen als Minor enthalten.

Kombinatorik

	Ohne Zurücklegen	Mit Zurücklegen
Ohne Reihenfolge	$\binom{n}{k} = \binom{n}{n-k}$	$\binom{n+k-1}{k}$
Mit Reihenfolge	$n^{\underline{k}} = \frac{n!}{(n-k)!}$	n^k

Rechenregeln:

- wenn $k > n$ dann gilt $\binom{n}{k} = 0$
- $\binom{n}{0} = \binom{n}{n} = 1$
- $\binom{n}{1} = \binom{n}{n-1} = n$
- $\binom{n}{2} = \frac{n(n-1)}{2}$
- $k \cdot \binom{n}{k} = n \cdot \binom{n-1}{k-1}$
- $\binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1}$

Binomialtheorem:
$(x+y)^3 = x^3 + 3x^2y + 3xy^2 + y^3$,
$(x+y)^4 = x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4$

- $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$
- $(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k$
- $(x+y+z)^n = \sum_{k=0}^{n} \sum_{l=0}^{n-k} \binom{n}{k,l} x^k y^l z^{n-k-l}$ wobei $\binom{n}{k,l} = \frac{n!}{k!l!(n-k-l)!}$

Kürzeste Gitterwege
Es gibt w(s,t) = $\binom{a+b}{a} = \binom{a+b}{b}$ kürzeste Wege von s nach t in einem a×b-Gitter.
Ist der Punkt c gesperrt dann gibt es $w(s,t) - \binom{a+c}{a} * \binom{b+c}{c}$ Wege.
Wenn Punkt c und d gegeben sind und mindestens einer der beiden besucht werden muss gilt: $w(a,c) * w(c,b) + w(a,d) * w(d,b) - w(a,c) * w(c,d) * w(d,b)$.
Umformuliert: $\binom{a+c}{a} * \binom{b+c}{c} - \binom{a+d}{a} * \binom{b+d}{b} - \binom{a+c}{a} * \binom{c+d}{c} * \binom{b+d}{b}$

Zahlentheorie

Für m,n $\in \mathbb{Z}$ und $m > 0$, ist m **Teiler von** n, falls $\exists t \in \mathbb{Z}\ n = t * m$. Kurz: $m \backslash n$.
Die Menge aller Teiler ist $T_n = \{\ m \mid m \backslash n\ \}$. $T_{m,n} = T_m \cap T_n$.
Der **größte gemeinsame Teiler** von n und m ist: max $T_{m,n}$. Das **kleinste gemeinsame Vielfache** ist: min $\{\ k \mid m \backslash k \ \wedge\ n \backslash k\ \}$.

Es gilt $kgV(m,n) * ggT(m,n) = mn$ oder $kgV(m,n) = mn/ggT(m,n)$.
Lemmas: 1) $\forall a, b \in \mathbb{Z}\ \ T_{m,n} \subseteq T_{am+bn}$ 2) $\forall a \in \mathbb{Z}\ \ T_{m,n} = T_{m,n-am}$ 3) $T_{m,n} = T_{ggT(m,n)}$
Der **euklidische Algorithmus** $euklid(m,n)$ bestimmt den ggT:(für $m < n$)
$if\ m = 0\ return\ n$
$else\ euklid(n\ mod\ m, m)$
Der ggT lässt sich als Linearkombination von m und n darstellen, berechnet wird diese mithilfe des **erweiterten euklidischen Algorithmus**:

n	m	q	r	x	y
84	60	1	24	-2	$1-(-2)*1=3$
60	24	2	12	1	$0-1*2=-2$
24	12	2	0	0	1

Hierbei muss auch wieder $m \leq n$ gelten. Allgemein betrachtet(Zeile 0 ist die unterste):
$q_i = \lfloor \frac{n_i}{m_i} \rfloor \qquad r_i = n_i\ mod\ m_i$
$x_0 = 0\ y_0 = x_1 = 1 \qquad x_i = y_{i-1} \qquad y_i = x_{-1} - q_i * y_{-1}$
Als Probe: $n_i * x_i + m_i * y_I = ggT(m,n)$ gilt in jeder Zeile.

Kongruenzen
$a \equiv b\ (mod\ m) \iff m \backslash (a-b)$
Seien $a \equiv b\ (mod\ m)$ und $c \equiv d\ (mod\ m)$ Dann gilt:
1) $a + c \equiv b + d\ (mod\ m)$ 2) $a - c \equiv b - d\ (mod\ m)$ 3) $ac \equiv bd\ (mod\ m)$
Ist $a \equiv b\ (mod\ m)$, dann ist $a^n \equiv b^n\ (mod\ m)$
Die Division gilt nur wenn der Quotient teilerfremd zu m ist: Sei $d \perp m$ und $ad \equiv bd\ (mod\ m)$, dann gilt $a \equiv b\ (mod\ m)$.
ist $a \perp m$, dann hat die Kongruenz $ax \equiv b\ (mod\ m)$ die in $\mathbb{Z}_m$ eindeutige Lösung $x = a^{-1}b\ mod\ m$. Man erhält a^{-1} indem man den erweiterten euklidischen Algorithmus auf a und m anwendet.
Die Anzahl der teilerfremdem Zahlen m in $\mathbb{Z}_m$ wird als **eulersche φ-Funktion** bezeichnet: $\varphi(m) = |\mathbb{Z}_m^*|$
Es gilt: $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$
Für Primzahlen: $\varphi(p) = p - 1$
Für Primzahlpotenzen: $\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1) = p^k \left(1 - \frac{1}{p}\right)$
z.B. $\varphi(16) = \varphi(2^4) = 2^4 - 2^3 = 2^3 \cdot (2-1) = 2^4 \cdot \left(1 - \frac{1}{2}\right) = 8$
Allgemein: $\varphi(n) = \prod_{p|n} p^{k_p - 1}(p-1) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$
z.B. $\varphi(84) = \varphi(2^2 * 3 * 7) = 84 * (1 - \frac{1}{2}) * (1 - \frac{1}{3}) * (1 - \frac{1}{7}) = 24$
Exponentation: $a^{\varphi(m)} \equiv 1\ (mod\ m)$
z.B. $5^{99} (mod\ 84) \quad \varphi(84) = 24 \longrightarrow 5^{24} * 5^{24} * 5^{24} * 5^3 = 1 * 1 * 1 * 125 \equiv 41\ (mod\ 84)$

Lineare Kongruenzen(Chinesischer Restsatz)
Ist ein Gleichungssystem der folgenden Art gegeben:
$x \equiv a_1\ mod\ m_1$
$x \equiv a_2\ mod\ m_2$
Dann bestimmt man x_1 und x_2 mithilfe des erweiterten euklidischen Algorithmus jeweils über m_1 und m_2:
$m_2 * x_1 \equiv 1\ mod\ m_1$
$m_1 * x_2 \equiv 1\ mod\ m_2$
Dann gilt: $x = a_1 * m_2 * x_1 + a_2 * m_1 * x_2$.

Algebraische Strukturen
$(G, \circ)$ heißt **Gruppe** falls folgende Eigenschaften gelten:
(AG) Assoziativgesetz: $\forall a, b, c, \in G \qquad a \circ (b \circ c) = (a \circ b) \circ c$
(N) Neutrales Element: $\exists e \in G\ \forall a \in G \qquad a \circ e = a$
(I) Inverses Element: $\forall a \in G\ \exists b \in G \qquad a \circ b = e$
Die Verknüpfung muss außerdem abgeschlossen über G sein. Falls auch auch das Kommutativgesetz(KG) $a \circ b = b \circ a$ gilt, heißt die Gruppe kommutativ(oder abelsch).

Ist $U \subseteq G$ und $(U, \circ)$ ebenfalls eine Gruppe, heißt sie **Untergruppe**. {e} und G sind **triviale Untergruppen**.
Sei $(G, \circ)$ endliche Gruppe und $a \in G$. Dann ist $< a >= \{a^0, a^1, a^2, ...\}$ die von a **erzeugte Untergruppe**. a heißt **Generator** oder **erzeugendes Element** von G.
$|U|$ heißt **Ordnung** von $< a >$ und teilt immer $|G|$.
$(R, +, \cdot)$ heißt **Ring** falls:
1) $(R, +)$ ist kommutative Gruppe. 2) (AG) $\forall a, b, c, \in G \quad a \cdot (b \cdot c) = (a \cdot b) \cdot c$
3)(DG) $\forall a, b, c, \in G \quad a \cdot (b + c) = a \cdot b + a \cdot c$
R ist kommutativer Ring falls $\forall a, b \in R \quad a \cdot b = b \cdot a$
R ist Ring mit **Eins(-Element)** falls $\exists 1 \in R \quad a \cdot 1 = a$

RSA

Wähle zwei ungleiche Primzahlen p und q.
$N = p * q$
$\varphi(N) = (p - 1) * (q - 1)$
Wähle eine zu $\varphi(N)$ teilerfremde Zahl e, für die gilt $1 < e < \varphi(N)$.
Berechne den Entschlässelungsexponenten d als Multiplikatives Inverses(erweiterter euklidischer Algorithmus) von e bezüglich des Moduls $\varphi(N)$. Es soll also die folgende Kongruenz gelten:

$$e * d \equiv 1 \bmod \varphi(N)$$

Verschlüsseln: $c \equiv m^e \bmod N$
Entschlüsseln: $m \equiv c^d \bmod N$