Mathe 1

Mitschrift

Fabian Damken

4. November 2016

Inhaltsverzeichnis

1 Grundbegriffe

1.1 Aussagen

Beispiele:

- A_1: 3 ist eine gerade Zahl.
- A_2: Jede natürliche Zahl ist gerade.
- A_3: 3 ist prim.

1.1.1 Aussageformen

Aussagen mit Variablen.
Beispiele:

- E_1: $x + 10 = 5$
- E_2: $x^2 >= 0$
- E_3: n ist gerade.
- E_4: $x^2 + y^2 = 1$

1.1.2 Quantoren

- $\forall x \in M : E(x)$ - Für alle x in M gilt $E(x)$ wobei E eine Aussageform darstellt.
- $\exists x \in M : E(x)$ - Es existiert mindestens ein x in M für das gilt $E(x)$ wobei E eine Aussageform darstellt.

Beispiele:

- $\forall x \in \mathbb{R} : x^2 >= 0$ - (w)
- $\forall n \in \mathbb{N} : E_3(n)$ - (f)
- $\exists n \in \mathbb{N} : E_3(n)$ - (w)

1.1.3 Aussagenlogische Verknüpfungen

- $A \wedge B$ - Konjunktion (und)
- $A \vee B$ - Disjunktion (oder)
- $A \implies B$ - Implikation (aus A folgt B)
- $\neg A$ - Negation (nicht)
- $A \iff B$ - Äquivalenz (Gleichheit)

A	B	$\neg A$	$\neg B$	$A \wedge B$	$A \vee B$	$A \implies B$ $((\neg A) \vee B)$	$A \iff B$
w	w	f	f	w	w	w	w
w	f	f	w	f	w	f	f
f	w	w	f	f	w	w	f
f	f	w	w	f	f	w	f

Äquivalenz $A \iff B \equiv (A \implies B) \wedge (B \implies A)$

Kontraposition $A \implies B \iff (\neg B \implies \neg A)$

1.1.3.1 de Morgan'schen Regeln

- $\neg(A \vee B) \iff \neg A \wedge \neg B$
- $\neg(A \wedge B) \iff \neg A \vee \neg B$

1.1.3.2 Distributivgesetz

- $(A \vee B) \wedge C \iff (A \wedge C) \vee (B \wedge C)$
- $(A \wedge B) \vee C \iff (A \vee C) \wedge (B \vee C)$

1.2 Mengen

Beispiele:

- $\mathbb{N} = \{0; 1; ...; n; ...\}$
- $\mathbb{N}* = \{1; 2; ...; n; ...\} = \{n \in \mathbb{N} : n \neq 0\}$
- $\{x \in M : E(x)\}$ wobei E eine Aussagenform darstellt.
- $\{n \in \mathbb{N} : prim(x) \wedge n <= 6\} = \{2; 3; 5\}$

1.2.1 Formalia

- $A \subseteq B \equiv \forall x \in A : x \in B$
- $A = B \equiv (A \subseteq B) \wedge (B \subseteq A) \equiv \forall x \in M : (x \in A \implies x \in B) \wedge (x \in B \implies x \in A)$
- $\emptyset \equiv \{x \in A : x \neq x\}$ $(x \neq x \equiv \neg x = x)$

1.2.2 de'Morganschen Regeln

- $(A \cup B)^{\mathsf{c}} = A^{\mathsf{c}} \cap B^{\mathsf{c}}$

1.2.3 Kardinalität

Seien A und B endliche Mengen.
Anzahl der Elemente (Kardinalität): $|A|$

- $|A \cup B| = |A| + |B| - |A \cap B|$
- $|A \times B| = |A| \cdot |B|$

$|A \cup B| = |A| + |B|$ wenn $A \cap B = \emptyset$

1.2.4 Operationen

$M, N \in G$

- $M \cap N \equiv \{x \in M : x \in N\} \equiv \{x \in G : x \in M \wedge x \in N\}$
- $M \cup N \equiv \{x \in G : x \in M \vee x \in N\}$
- $M \setminus N \equiv \{x \in M : x \notin N\} \equiv \{x \in M : \neg x \in N\}$
- $M^{\mathsf{c}} \equiv \{x \in G : x \notin M\} \equiv \{x \in G : \neg x \in M\}$
- $M \times N \equiv \{(x, y) : x \in M, y \in N\}$ - Kartesisches Produkt
- $A_1 \times ... \times A_n \equiv \{(x_1, ..., x_n) : x_y \in A_1, ..., x_n \in A_n\}$
- $P(M) = \{x : x \in M\}$
  - $\emptyset \subseteq P(\emptyset) \subseteq P(P(\emptyset)) \subseteq ...$
  - $V_w \subseteq P^n(\emptyset)$ $(n \in \mathbb{N})$
  - $P(V_w) = V_(w + 1)$

1.2.5 Obere/Untere Schranken

- **Obere Schranken:** $OS(Y) = \{x \in X : \forall y \in Y : x \geq y\}$
- **Untere Schranken:** $US(Y) = \{x \in X : \forall y \in Y : x \leq y\}$
- **Supremum:** Das kleinste Element von $OS(Y) \iff sup(Y)$.
- **Infimum:** Das größte Element von $US(X) \iff inf(Y)$.

1.2.5.1 Beispiel

$\mathbb{Q}^+ = \{x \in \mathbb{Q} : 0 < x\}$

- **Supremum:** Nicht vorhanden.
- **Infimum:** $US(\mathbb{Q}^+) = \{x \in \mathbb{Q} : x \leq 0\} \implies inf(\mathbb{Q}^+) = 0$

1.2.6 Relationen

$R \subseteq A_1 \times ... \times A_n$

1.2.6.1 Relationen von identischen Mengen

$A^n = A \times ... \times A$ (n mal)
Für $n = 2$ kann die Infixnotation verwendet werden, das heißt $xRy \iff (x, y) \in R$.

1.2.6.2 Definition von kleiner-gleich

$\leq = \{(n, m)\mathbb{N}^2 : n \leq m\}$

1.2.6.3 Eigenschaften

- **Reflexivität** $\forall x \in M : xRx$
- **Symmetrie** $xRy \implies yRx$
- **Transivität** $xRy \wedge yRz \implies xRz$
- **Antisymmetrie** $xRy \wedge yRx \implies x = y$
- R ist eine Äquivalenzrelation $\iff$ R reflexiv, transitiv und symmetrisch
- R ist eine partitielle Ordnung $\iff$ R reflexiv, transitiv, antisymmetrisch
- R ist total $\iff \forall xy \in M : xRy \vee yRx$

1.2.7 Ordnungsrelationen

1.2.7.1 Ordnungstypen

p.O. $:=$ partielle Ordnung

- **Totale Ordnung:** Jedes Element ist mit jedem anderen vergleichbar.
- **Partielle Ordnung:** Nicht jedes Element ist nicht mit jedem anderen vergleichbar.

1.2.7.2 Ordnungsäquivalenz

(x, R) p.O. $y \subseteq x \implies (y, R \cap (y \times x))$ p.O.

- $x \geq y \iff y \leq x$
- $x > y \iff x \geq y \wedge x \neq y \iff x \geq y \wedge \neg(x = y)$
- $x < y \iff y > x$

1.2.7.3 Extreme

$(x, \leq)$ p.O. $y \subseteq x$

- $g \in X$ größtes Element von $X \iff \forall x \in X : x \leq g$
- $k \in X$ kleinstes Element von $X \iff \forall x \in X : x \geq k$

Satz: Die größten Elemente sind immer eindeutig.
Beweis:
Seien g und g' die größten Elemente.

$$\implies g \leq g' \wedge g' \leq g \implies g = g$$

q.e.d.

1.2.8 Große Vereinigung/Schittmenge / Leere Menge

1.2.8.1 Allgemein

Allgemein gilt für Teilmengen von Potenzmengen $Y \subseteq P(M)$:

- $sup(Y) = \bigcup Y = \bigcup\limits_{A \in Y} A$
- $inf(Y) = \bigcap Y = \bigcap\limits_{A \in Y} A$

1.2.8.2 Sonderfall

Für die leere Teilmenge der Potenzmenge $Y = \emptyset$, $Y \subseteq P(M)$ gilt:

- $OS(\emptyset) = US(\emptyset) = P(M)$
- $sup(Y) = \bigcup \emptyset = \emptyset$
- $inf(Y) = \bigcap \emptyset = M$

1.2.9 Äquivalenzrelation

Seien $a, b, c, k, l, n \in \mathbb{Z}$.

Satz: $a \sim_n b$ genau dann wenn $\exists k \in \mathbb{Z} : a - b = k \cdot n$
Beweis:
Symmetrie:

$$a - b = k \cdot n \implies b - a = (-k) \cdot n$$

Transitivität:

$$a - b = k \cdot n$$

$$b - c = l \cdot n \implies a - c = (a - b) + (b - c) = k \cdot n + l \cdot n = (k + l) \cdot n$$

q.e.d.

1.2.10 Äquivalenzklassen

Es gilt (X, R), $a \in X$.

- $a \in X$
- $\tilde{a} := \{x \in X : a \sim x\}$
- $\tilde{a} \neq \emptyset$
- $\bigcup \tilde{a} = X$
- $\tilde{a} \neq \tilde{b} \implies \tilde{a} \cap \tilde{b} = \emptyset$

Satz: $\tilde{a} \neq \tilde{b} \implies \tilde{a} \cap \tilde{b} = \emptyset \equiv \tilde{a} \cap \tilde{b} \neq \emptyset \implies \tilde{a} = \tilde{b}$
Beweis:
Sei $c \in \tilde{a} \cap \tilde{b}$, das heißt cRa und cRb, also $a \sim b$ und somit $\tilde{a} = \tilde{b}$ und somit $\tilde{a} \neq \tilde{b} \implies \tilde{a} \cap \tilde{b} = \emptyset$.

q.e.d.

1.2.11 Partitionen

$P \subseteq P(X)$ ist genau dann eine Partition, wenn:

- $\bigcup P = X$
- $\forall A \in P : A \neq \emptyset$
- $\forall S_1 S_2 \in P : S_1 \neq S_2 \implies S_1 \cap S_2 = \emptyset$

Äquivalenz:

- $x \sim_p y \iff \exists S \in P : x \in A \land y \in A$
- $X_{/P} = P$
- $x \sim_{X_{/\sim}} y \iff x \sim y$
- $\frac{a}{b} \sim \frac{c}{d} \iff a \cdot b \sim c \cdot d$

1.3 Abbildungen/Funktionen

$f : A \to B$ gdw. $f \subseteq A \times B$, so dass

- $xfy \land xfy' \implies y = y'$
- $\forall x \in A : \exists y \in B : xfy$

$f = graph(f) = \{(x, f(x)) : x \in A\}$

$C \subseteq A \ : f(C) = f[C] = \{f(x) : x \in C\}$ (Bild von C unter f).

$D \subseteq B \ : f^{-1}(D) = f^{-1}[D] = \{x \in A : f(x) \in D\}$

1.3.1 Umkehrfunktion (inverse Funktion)

Vorraussetzung zur Bildung einer inversen Funktion: Die Funktion muss bijektiv sein.

Sei $f : A \to B$ bijektiv.
Somit gilt für die Umkehrfunktion $f^{-1} = \{(f(x), x) : x \in A\} : B \to A$
Beziehungsweise $R \in A \times B$, $R^{-1} = \{(y, x) \in B \times A : xRy\}$

1.3.2 Identitätsfunktion

Sei M eine Menge.
Für die Identitätsfunktion gilt: $id_M : M \to M : x \mapsto x$

1.3.3 Notation

Im allgemeinen gilt $f : A \to B : x \mapsto f(x)$. Wobei A den Definitionsbereich und B den Wertebereich darstellt.

Beispiele:

- $f : x \to x^2$
- $add : \mathbb{R} \times \mathbb{R} : (x, y) \mapsto x + y$
- $id_A : A \to A : x \mapsto x$
- Sei A eine Menge und $\sim$ eine Äquivalenzrelation auf dieser. $\mu : A \to A_{/\sim} : x \mapsto \tilde{x}$
- $f : \mathbb{R} \to \mathbb{R} : x \mapsto x^2$
- $f : \mathbb{R} \to [0, \infty) : x \mapsto x^2$
- $f : [0, \infty) \to [0, \infty) : x \mapsto x^2$ (bijektiv) $f^{-1} : [0, \infty) \to [0, \infty) : y \mapsto \sqrt{y}$
- $f : [1, \infty) \to (0, 1] : x \mapsto \frac{1}{x}$ (bijektiv) $f^{-1} : (0, 1] \to [1, \infty) : x \mapsto \frac{1}{x}$

1.3.4 Eigenschaften

- f ist injektiv, wenn $\forall x, x' \in A : f(x) = f(x') \implies x = x'$.
- f ist surjektiv, wenn $\forall y \in B : \exists x \in A : f(x) = y$.
- f ist bijektiv, wenn $\forall y \in B : \exists^1 x \in A : f(x) = y$.

Für jede Funktion $f : A \to B$ existiert eine Funktion $f^\# : A \to f[A] : x \mapsto f(x)$.

1.3.5 Funktionskomposition

Sei $f : A \to B$ und $g : B \to C$

Durch die Verkettung entsteht eine neue Funktion: $g \circ f : A \to C : x \mapsto g(f(x))$

Außerdem gilt:

- $f^{-1} \circ f = id_A$
- $f \circ f^{-1} = id_B$

1.4 Beweisprinzipien

1.4.1 Direkter Beweis

Bei einem dirkten Beweis wird die Prämisse direkt bewiesen.

1.4.1.1 Beispiel

Satz: Sind $n, m \in \mathbb{N}$ gerade, dann ist $n + m$ gerade.
Beweis:
Es gilt $n = 2 \cdot k$ und $m = 2 \cdot l$, wobei $k, l \in \mathbb{N}$. Das heißt, dass

$$n + m = 2 \cdot k + 2 \cdot l = 2 \cdot (k + l)$$

gerade ist.

q.e.d.

1.4.2 Beweis durch Kontraposition

Anstelle von $A \implies B$ wird $\neg B \implies \neg A$ bewiesen.

1.4.2.1 Beispiel

Satz: Gilt für $n \in \mathbb{N}$, dass n^2 gerade ist, ist n gerade.
Beweis:
Der Beweis wird über n ungerade $\implies n^2$ ungerade geführt.
Es gilt für $k \in \mathbb{N}$, dass $n = 2 \cdot k + 1$. Somit gilt dass

$$n^2 = (2 \cdot k + 1)^2 = 4 \cdot k^2 + 4 \cdot k + 1 = 2 \cdot (2 \cdot k^2 + 2 \cdot k) + 1$$

ungerade ist.
Daraus folgt dass n ungerade $\iff n^2$ ungerade und n gerade $\iff n^2$ gerade.

q.e.d.

1.4.3 Indirekter Beweis

Anstelle von $A \implies B$ wird $\neg(A \wedge \neg B)$ bewiesen. Alternativ kann $\neg(\neg A)$ anstelle von A bewiesen werden ($\neg A \implies \bot$).

1.4.3.1 Beispiel

Satz: $\sqrt{2}$ is irrational.
Beweis:
Ist $\sqrt{2}$ rational, muss

$$\sqrt{2} = \frac{n}{m}$$

($n, m \in \mathbb{N}$) gelten wobei n und m teilerfremd sind. Somit gilt

$$2 = \frac{n^2}{m^2}$$

also

$$n^2 = 2 \cdot m^2$$

. Somit gilt n^2 gerade $\implies$ n gerade. Daraus folgt dass

$$(2 \cdot k)^2 = n^2 = 2 \cdot m^2$$

. Somit gilt n^2 gerade $\implies$ n gerade.
$\lightning$ n und m sollten teilerfremd sein. Somit ist $\sqrt{2} \neq \frac{n}{m}$.

q.e.d.

1.4.4 Beweis durch vollständige Induktion

Es wird beweisen, dass für eine *Induktionshypothese* (*IH*) $A(n)$ gilt

$$(A(0) \land (\forall n \in \mathbb{N} : A(n) \implies A(n+1))) \implies \forall n \in \mathbb{N} : A(n)$$

Der Beweis von $A(0)$ wird *Induktionsanfang* (*IA*) genannt.
Der Beweis von $A(n) \implies A(n+1)$ wird *Induktionsschritt* (*IS*) genannt.
Es gilt:

$$A(0) \implies A(1) \implies A(2) \implies \cdots \implies A(n)$$

1.4.4.1 Beispiel 1

Satz: $\forall n \in \mathbb{N} : \sum_{k=1}^{n} k = \frac{n \cdot (n+1)}{2}$
Beweis:
Induktionsanfang:

$$A(0) = \sum_{k=1}^{0} k = \frac{0 \cdot (0+1)}{2} = 0$$

Induktionsschritt:

$$\begin{aligned} A(n+1) = \sum_{k=1}^{n+1} = (\sum_{k=1}^{n}) + (n+1) \quad &= \frac{n \cdot (n+1)}{2} + (n+1) \\ &= \frac{n + (n+1)}{2} + \frac{2 \cdot (n+1)}{2} \\ &= \frac{n \cdot (n+1) + 2 \cdot (n+1)}{2} \\ &= \frac{n^2 + 3 \cdot n + 2}{2} \\ &= \frac{(n+1) \cdot (n+2)}{2} \end{aligned}$$

q.e.d.

1.4.4.2 Beispiel 2

Satz: Für endliche Mengen M gilt $|P(M)| = 2^{|P(M)|}$, also $\forall n \in \mathbb{N} : \forall M; |M| = n \implies |P(M)| = 2^n$.
Beweis:
Induktionsanfang:

$$|M| = 0 \implies |P(M)| = 2^0 = 1$$

Induktionsschritt: Sei M eine Menge mit $|M| = n + 1$ wobei $n \in \mathbb{N}$. Zu zeigen: $|P(M)| = 2^{n+1} = 2 \cdot 2^n$.
Sei $a \in M$.

- $S_0 = \{A \in P(M) : a \in A\} \implies |S_0| = n$
- $S_1 = \{A \in P(M) : a \notin A\} \implies |S_1| = n$

$$S_0 \approx P(M \setminus \{a\}) \approx S_1$$

$$|P(M)| = |S_0| + |S_1| = 2 \cdot |P(M \setminus \{a\})| = 2 \cdot 2^n = 2^{n+1}$$

q.e.d.

2 Algebraische Strukturen

Strukturen, in denen man „wie üblich“ rechnen kann.

2.1 Rechnen in $\mathbb{Z}$ - Primzahlen, Teiler

Seien $a, b \in \mathbb{Z}$.

- $b \mid a \equiv \exists c \in \mathbb{Z} : b \cdot c = a \equiv b$ teilt a.
- $p \in \mathbb{N}$ ist prim $\iff (p > 1) \wedge (\forall n \in \mathbb{N} : n \mid p \implies (n = 1 \vee n = p))$
- $ggt(a, b) = max\{n \in \mathbb{N} : n \mid a \wedge n \mid b\}$

Satz: Sei $a, b \in \mathbb{Z}*$, dann gibt es eindeutige $q \in \mathbb{Z}$ und $r \in \{0, 1, \ldots, b-1\}$, so dass $a = q \cdot b + r$, $q = \lfloor \frac{a}{b} \rfloor$ und $r = a \ \mathbf{mod}\ b$

Beweis:

Sei $q = max\{s \in \mathbb{Z} : s \cdot b \leq a\}$ und $r = a - q \cdot b$.

Eindeutigkeit: Sei $a = q' \cdot b + r'$ und $r' \in \{0, 1, \ldots, b-1\}$, so folgt $(q - q') \cdot b = r' - r$ und $|r - r'| < b$.

$$\implies q - q' = 0 \implies q = q'$$
$$\implies r' - r = 0 \implies r = r'$$

q.e.d.

2.1.1 Modulare Arithmetik (Rechnen mit Restklassen)

Sei $n \in \mathbb{N}*$ und $a, b \in \mathbb{Z}$, dann gilt für $k \in \mathbb{N}$:

- $(a + b) \ \mathbf{mod}\ n = ((a \ \mathbf{mod}\ n) + (b \ \mathbf{mod}\ n)) \ \mathbf{mod}\ n$
- $(a \cdot b) \ \mathbf{mod}\ n = ((a \ \mathbf{mod}\ n) \cdot (b \ \mathbf{mod}\ n)) \ \mathbf{mod}\ n$
- $a^k \ \mathbf{mod}\ n = (a \ \mathbf{mod}\ n)^k \ \mathbf{mod}\ n$

Satz: $(a+b) \textbf{ mod } n = ((a \textbf{ mod } n) + (b \textbf{ mod } n)) \textbf{ mod } n$
Beweis:
Sei $q_1 = \lfloor \frac{a}{n} \rfloor$, $r_1 = a \textbf{ mod } n$ und $q_2 = \lfloor \frac{b}{n} \rfloor$, $r_2 = b \textbf{ mod } n$, dann gilt:

$$\begin{aligned} a+b &= (q_1 n + r_1) + (q_2 n + r_2) \\ &= n(q_1 + q_2) + r_1 + r_2 \\ &\implies (a+b) \sim_n (r_1 + r_2) \end{aligned}$$

q.e.d.

Satz: $(a \cdot b) \textbf{ mod } n = ((a \textbf{ mod } n) \cdot (b \textbf{ mod } n)) \textbf{ mod } n$
Beweis:
Sei $q_1 = \lfloor \frac{a}{n} \rfloor$, $r_1 = a \textbf{ mod } n$ und $q_2 = \lfloor \frac{b}{n} \rfloor$, $r_2 = b \textbf{ mod } n$, dann gilt:

$$\begin{aligned} a \cdot b &= (q_1 \cdot n + r_1)(q_2 \cdot n + r_2) \\ &= q_1 \cdot q_2 \cdot n^2 + q_1 \cdot n \cdot r_2 + q_2 \cdot n \cdot r_1 + r_1 \cdot r_2 \\ &= n \cdot (q_1 \cdot q_2 \cdot n + q_1 \cdot r_2 + q_2 \cdot r_1) + r_1 \cdot r_2 \\ &\implies (a \cdot b) \sim_n (r_1 \cdot r_2) \end{aligned}$$

q.e.d.

Satz: $a^k \textbf{ mod } n = (a \textbf{ mod } n)^k \textbf{ mod } n$
Beweis:
Induktionsanfang: $k = 0$, $n > 1$

$$a^0 \textbf{ mod } n = 1 = (a \textbf{ mod } n)^0 \textbf{ mod } n = 1$$

Induktionsschritt:

$$\begin{aligned} a^{k+1} \textbf{ mod } n &= ((a^k \textbf{ mod } n) \cdot (a \textbf{ mod } n)) \textbf{ mod } n \\ &= (((a \textbf{ mod } n)^k \textbf{ mod } n) \cdot ((a \textbf{ mod } n) \textbf{ mod } n)) \textbf{ mod } n \\ &= ((a \textbf{ mod } n)^k \cdot (a \textbf{ mod } n)) \textbf{ mod } n \\ &= (a \textbf{ mod } n)^{k+1} \textbf{ mod } n \end{aligned}$$

q.e.d.

2.1.2 Größter gemeinsamter Teiler

Definition: $ggt(a,b) := max\{n \in \mathbb{N} : n|a \land n|b\}$
Ferner gilt $ggt \equiv ggT$.

Lemma: $a, b \in \mathbb{N}$, $a \geq b$ gilt $ggt(a,b) = ggt(b, a \textbf{ mod } b)$
Beweis:
Sei $r = a \textbf{ mod } b$

$$(n|a) \wedge (n|b) \iff (n|b) \wedge (n|r)$$

$\Longrightarrow$ **:** Sei $a = k \cdot n$ und $q = l \cdot n$, so gilt:
$r = a - q \cdot b = k \cdot n - q \cdot l \cdot n = n \cdot (k - q \cdot l) \implies n|r$

$\Longleftarrow$ **:** Sei $b = k \cdot n$ und $r = l \cdot n$, so gilt:
$a = q \cdot b + r = q \cdot k \cdot n + l \cdot n = n \cdot (q \cdot k + l) \implies n|a$

q.e.d.

2.1.2.1 Euklidischer Algorithmus

Der euklidische Algorithmus ist ein Algorithmus zur berechnung des größten gemeinsamen Teilers ($ggt(a,b)$) zweier Zahlen.

Für alle $a, b \in \mathbb{N}$, $a \geq b$ gilt:

```
function ggt(a, b)
    if b = 0 then
        return a
    else
        return ggt(b, a mod b)
    end if
end function
```

2.1.2.2 Erweiterter euklidischer Algorithmus

Der erweiterte euklidische Algorithmus dient zur von k und l in $\exists k, l \in \mathbb{Z} : ggt(a,b) = k \cdot a + l \cdot b$.

$eggt : \mathbb{N} \times \mathbb{N} \to \mathbb{N} \times \mathbb{Z} \times \mathbb{Z}$

```
function eggt(a, b)
    if b = 0 then
        return (a, 1, 0)
    else
        (d, x, y) ← eggt(b, a mod b)
        return (d, y, x − floor(a/b) ∗ y)
    end if
end function
```

Satz: $\exists k, l \in \mathbb{Z} : ggt(a,b) = k \cdot a + l \cdot b$
Beweis:
TODO: Understand this proof!
Seien $a, b, x, y \in \mathbb{Z}$ und $d \in \mathbb{N}$, so gilt

$$a \geq b \wedge (d, x, y) = eggt(a,b) \implies d = ggt(a,b) = x \cdot a + y \cdot b$$

$eggt(a,0) = (a,1,0) \implies a = ggt(a,0) \wedge a = 1 \cdot a + 0 \cdot b$
$d = ggt(b, a \textbf{ mod } b) = x \cdot b + y \cdot (a \textbf{ mod } b) = ggt(a,b)$

$$\begin{aligned}
ggt(a,b) \qquad &= y \cdot a + (x - \lfloor \frac{a}{b} \rfloor) \cdot b \\
&= c \cdot b + y \cdot a - y \cdot (\lfloor \frac{a}{b} \rfloor \cdot b) \\
&= x \cdot b + y \cdot (a - \lfloor \frac{a}{b} \rfloor \cdot b) \\
&= x \cdot b + y \cdot (a \textbf{ mod } b) \\
&= ggt(b, a \textbf{ mod } b) \\
&= ggt(a,b)
\end{aligned}$$

q.e.d.

Korollar: $ggt(a,b) = 1 \implies \exists x, y \in \mathbb{Z} : 1 = y \cdot a \wedge y \cdot b$

Satz: Wenn $ggt(a,n) = 1$, dann $(n|a \cdot b \implies n|b)$ für $a, b, n \in \mathbb{N}*$
Beweis:
Seien $x, y \in \mathbb{Z}$.
$1 = ggt(a,n) = x \cdot a + y \cdot n \iff b = x \cdot a \cdot b + y \cdot n \cdot b$
$\implies n|b$

q.e.d.