LAG+ Skript

basierend auf den Mitschriften von Maicon Hieronymus in LaTeX gebracht von Sven Bamberger

JOHANNES GUTENBERG UNIVERSITÄT MAINZ

Mainz, 17. Dezember 2012

Dieses Skript wurde erstellt, um sich besser auf die Klausur vorzubereiten und eine ordentliche und für alle Personen lesbare Mitschrift zu haben.

Dieses Dokument garantiert weder Richtigkeit noch Vollständigkeit, da es aus Mitschriften gefertigt wurde und dabei immer Fehler entstehen können. Falls ein Fehler enthalten ist, bitte melden oder selbst korrigieren und neu hochladen.

Hier kleine Notizen zu einzelne Besonderheiten dieses Dokumentes.

1. /* */ alles zwischen diesen Zeichen sind Kommentare und sollen zum tiferen Verständnis oder Besondere Fragestellungen darstellen. Dabei ist zu beachten, das die Notation nciht immer komplett korrekt ist.Es können also kleinere mathematische Fehler auftauchen, welche aber für das Verständnis relevant sind.

Inhaltsverzeichnis

I. Grundlagen

I.1. Abbildungen

I.1.1. Idee:

Es seien A und B Mengen. Unter einer Abbildung f stellen wir uns einen Algorithmus vor, der aus jeder eingabe $a \in A$ ein eindeutig bestimmte Ausgabe $b \in B$ errechnet, b ist nur durch a (und f) festgelegt.

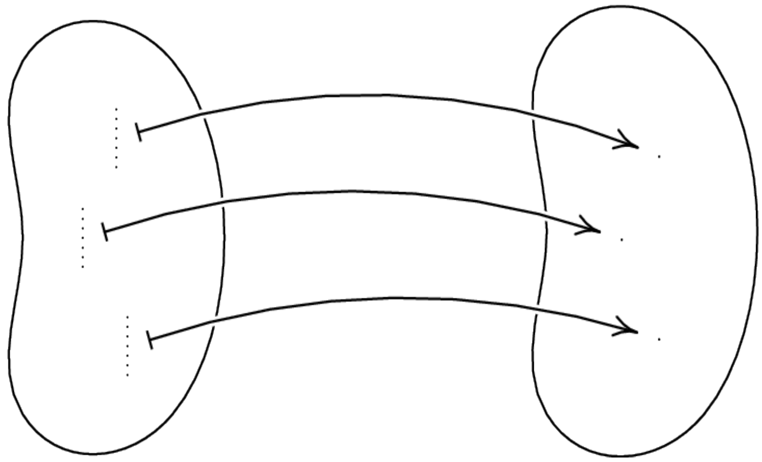

Abbildung I.1.: Eine einfache Abbildung

I.1.2. Definition:

Es seien A und B Mengen. Eine Abbildung f mit $f : A \to B$ sei eine Teilmenge f von $AxB = \{(a,b) | a \in A, b \in B\}$ so, dass gilt:

- zu jedem $a \in A$ existiert ein $b \in B$ mit $(a,b)\ inf$

- sind $(a,b_1),(a,b_2) \in f$, so gilt $b_1 = b_2$

f ist also das, was in der Schule im Fall reller Funktionen als Graph der Funktion bezeichnet wurde. Anstatt $(a,b) \in f$ schreiben wir $b = f(a)$. Die Menge A heißt Definitionsbereich von f, die Menge B heißt Zielbereich von f. Ferner sei Bild $f = \{b \in B | \exists a \in A$ mit $f(a) = b\} = \{f(a) | a \in A\} = f(A))$ (Wertebereich)

I.1.3. Beispiel:

1. Vorzeichenfunktion $sign. \mathbb{Z} \to \{-1, 0, 1\}$ $sign = \{(z,1)|z < 0\} \cup \{(0,0)\} \cup \{(z,1)|z > 0\}$
2. Identität: Für jede Menge A sei $id_A : A \to A$ gegeben durch $id_A(b) = a \ \forall a \in A$

   $f : \mathbb{R} \to \mathbb{R},\ f(a) = a^2 \ \forall a \in \mathbb{R}$

   $g : \mathbb{R} \to \mathbb{R},\ g(a) = 2a \ \forall a \in \mathbb{R}$

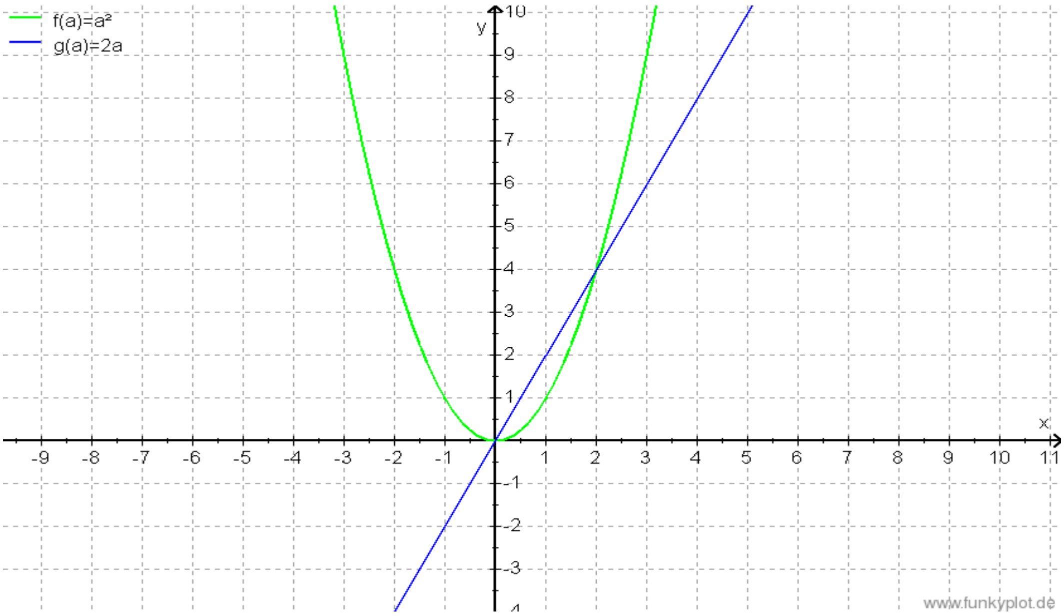

Abbildung I.2.: Ein Beispiel Graph

   Bild $f = \{b \in \mathbb{R} | b \geq 0\} \subsetneq \mathbb{R}$

   Bild $g = \mathbb{R}$

3. $g : \mathbb{Z} \to \mathbb{Z},\ g(a) = \{2a | a \in \mathbb{Z}\} \subsetneq \mathbb{Z}$ (Kurzschreibweise: $(= 2\mathbb{Z})$)

I.1.4. Definition:

Eine Abbildung $f : A \to B$ heiße:

- surjektiv, falls Bild $f = B$ ist d.h., falls $\forall b \in B$ ein $a \in A$ existiert mit $f(a) = b$
- injektiv, falls es zu jedem $b \in B$ höchstens ein $a \in A$ gibt mit $f(a) = b$.

  d.h.

  - aus $f(a_1) = f(a_2)$ folgt $a_1 = a_2$
  - aus $a_1 \neq a_2$ folgt $f(a_1) \neq f(a_2)$

- bijektiv, falls f injektiv und surjektiv ist

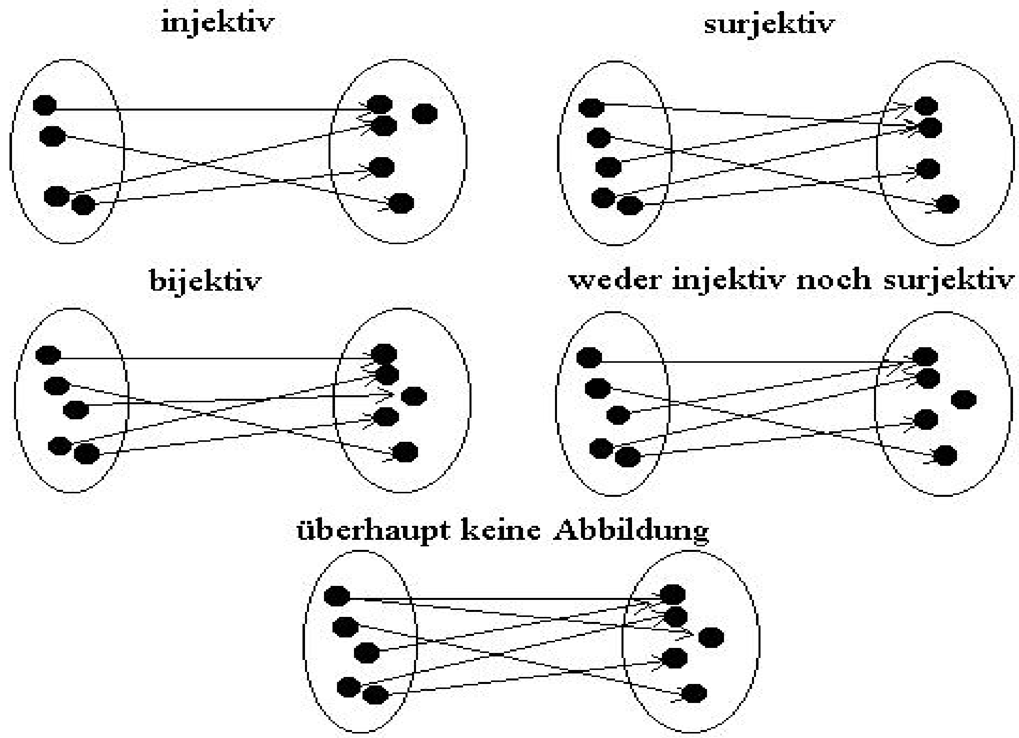

Abbildung I.3.: Mögliche Abbildungen auf einen Blick

I.1.5. Beispiel:

Sei $\mathbb{R}_{\geq 0} = \{a \in \mathbb{R} | a \geq 0\}$

1. $f : \mathbb{R} \to \mathbb{R}$, $f(a) = a^2$ nicht surjektiv, nicht injektiv $(-1 \notin \text{Bild } f)$ $((-1)^2 = 1^2)$
2. $f : \mathbb{R} \to \mathbb{R}_{\geq 0}$, $f(a) = a^2$ surjektiv, nicht injektiv
3. $f : \mathbb{R}_{\geq 0} \to \mathbb{R}$, $f(a) = a^2$ nicht surjektiv, injektiv
4. $f : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$, $f(a) = a^2$ bijektiv

I.1.6. Definition

Komposition von Abbildungen

Es seien $f : A \to B$ und $g : B \to C$ Abbildungen. Wir definieren $g \circ f : A \to C$ vermöge $(g \circ f)(a) = g(f(a))$ $\forall a \in A$

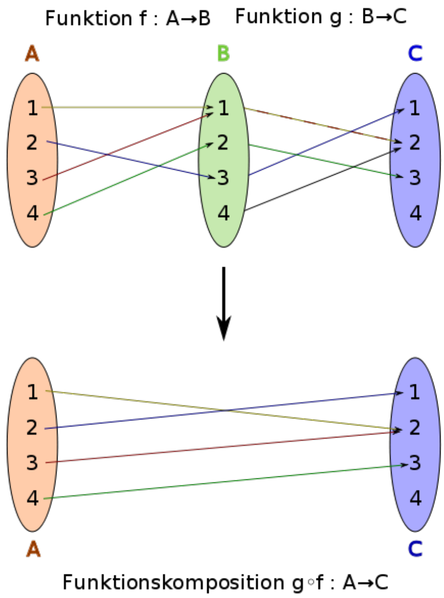

Abbildung I.4.: Eine mögliche Komposition

I.1.7. Beispiel

$f, g : \mathbb{R} \to \mathbb{R},\ f(x) = x^2,\ g(x) = 2x\ \forall x \in \mathbb{R}$

Dann:

$$(g \circ f)(x) = g(f(x)) = g(x^2) = 2x^2$$
$$(f \circ g)(x) = f(g(x)) = f(2x) = (2x)^2 = 4x^2$$

Es kommt auf die Reihenfolge von f und g an!

I.1.8. Satz

Seien $f : A \to B$ und $g : B \to A$ Abbildungen mit $g \circ f = id_A$ Dann ist f injektiv und g surjektiv.

Beweis:

f injektiv: Seien $a_1, a_2 \in A$ mit $f(a_1) = f(a_2)$ z.z. $a_1 = a_2$

Dazu: $a_1 = id_A(a_1) = (g \circ f)(a_1) = g(f(1_1)) = g(f(a_2)) = (g \circ f)(a_2) = id_A(a_2) = a_2$

g surjektiv: Sei $a \in A$ (=Zielbereich von g)

z.z. Es gibt ein $b \in B$ (=Definitionsbereich von g) mit $g(f(a)) = (g \circ f)(a) = id_A(a) = a$
wähle daher $b = f(a)$

/* $f : A \to B \qquad f \circ id_A : A \to B \qquad f \circ id_A = f$ */

I.1.9. Definition:

In der Situation I.1.8 nennen wir g eine linksinverse von f und f eine rechtsinverse von g.

I.1.10. Definition:

Ist $f : A \to B$ bijektiv, so sei die zu f inverse Abbildung $f^{-1} : B \to A$ gegeben durch $f^{-1} = \{(b,a) \in B\text{x}A | a, b \in f\}$

Warnung: Das klappt nur bei bijektiven Abbildungen f, da f_{-1} beidseitig invers zu f ist.

Hinweis: f^{-1} inverse der Abbildung $\quad f1^{-}$ volles Urbild jedoch ist dies nicht zwangsläufig bijektiv

I.1.11. Definition:

Sei $f : A \to B$ und $Y \leq B$. Dann nennen wir $j(Y) = \{a \in A | f(a) \in Y\}$ das volle Urbild zu Y unter f.

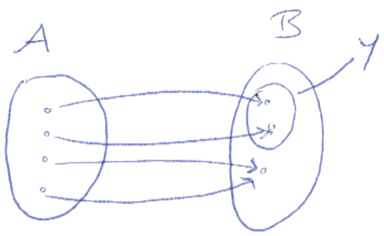

Abbildung I.5.: Eine Abbildung auf Untermengen

I.1.12. Beispiel:

In 1.5(1) war $f : \mathbb{R} \to \mathbb{R}$, $f(a) = a^2$. $f(\{0,1,4\}) = \{-2,-1,0,1,2\}$

Beispiel: $g : \mathbb{Z} \to \mathbb{Z}$, $g(a) = a^2$
$f^{-}(\{0,1,2,3,4\}) = \{-2,-1,0,1,2\}$

I.2. Äquivalenzrelationen

I.2.1. Bemerkung:

Es sei $f : A \to B$ eine Abbildung. Für jedes feste $b \in B$ nennen wir $f^{-}(b) = \{a \in A | f(a) = b\}$ die Faster von b unter f. Offenbar sind je zwei Fasern disjunkt: $b_1 \neq b_2 \Longrightarrow f^{-}(b_1) \cap j(b_2) = \varnothing$ ferner ist $A = \bigcup_{b \in B} j(b)$. Wir sprechen von einer disjunkten Zerlegung bzw. Partition von A. /* Faser $\widehat{=}$ volles Urbild; disjunkt $=$ Schnitt ist leer. */

I.2.2. Beispiel:

A = Menge aller Autos.
F = Menge aller Farbcodes von Autos.
$f : A \to F$ ordnet jedem Auto seinen Farbcode zu. Damit werde die Autos andhand ihrer Farbe (Faser von blaue (blaue Autos)) in unterschiedliche Schubladen gepackt, die Faser von f. Die Fasern sind disjunkt, da jedes Auto einen bestimmten Farbcode hat. Jedes Auto hat einen Farbcode, liegt also in einer Faser.
Vermöge f können zwei Autos gleicher Farbe als „gleichwertig“ angesehen werden.

I.2.3. Definition:

Eine Äquivalenzrelation auf einer Menge A sei eine Teilmenge von $!_R$ von AxA mit folgenden Eigenschaften:

R ist refelxiv: für jedes $a \in A$ ist $(a, a) \in$ R

R ist symmetrisch: ist $(a_1, a_2) \in$ R, so auch $(a_2, a_1) \in$ R

R ist transitiv: sind $(a_1, a_2), (a_2, a_3) \in$ R, so auch $(a_1, a_3) \in$ R

Anstatt $(a, b) \in$ R schreiben wir $a \sim_R b$ und sagen „a äquivalent b“.

I.2.4. Beispiel:

a) zu Beispiel 2.2 ist $\mathbb{R} = \{(a, b) \in A\text{x}A | f(a) = f(b)\}$ eine Äquivalenzrelation auf der Menge A aller Autos.

b) Auf jede Menge ist die Gleichheit „=“ von Elmenten eine Äquivalenzrelation.

c) Kongruenz von Dreiecken in der Zeichenebene R^2 ist eine Äquivalenzrelation auf der Menge dieser Dreiecke.

Erinnerung

Äquivalenzrelation $\sim$ auf M

- reflexiv $\forall a \in M a \sim a$

- symmetrisch wenn $a \sim b$, dann $b \sim a$

- transitiv wenn $a \sim b \wedge b \sim c$, dann $a \sim c$

I.2.5. Definition:

Es sei $\sim$ eine Äquivalenzrelation auf M. Für jede
$a \in M$ sei $\{b \in M | a \sim b\} = [a] =_{wegenSymmetrie} \{b \in M | b \sim a\}$ die sogenannte Äquivalenzklasse zu a.
Jedes $b \in [a]$ heiße ein Vertreter von $[a]$.

Beachte: Reflexivität $\Rightarrow a$ Vertreter von $[a]$ (wegen Symmetrie).

I.2.6. Hauptsatz:

Es sei M eine feste Menge. Dann gilt:

- Die Äquivalenzrelationen auf M entsprechen genau den Partitionen von M.

Genauer:

(a) Ist $M = \dot{\bigcup\limits_{i \in I}} M_i$ ($\dot{\bigcup}$ = disjunkte Vereinigung) eine Partition von M, so ist eine Äquivalenzrelation $\sim$ auf M gegeben durch: $a \sim b \Leftrightarrow$ es gibt ein $i \in I$ mit $a, b \in M_i$ Die Äquivalenzklassen zu $\sim$ sind genau die Mengen $M_i (i \in I)$

(b) Ist $\sim$ eine Äquivalenzrelation auf M, so bilden die 'quivalenzklassen zu $\sim$ eine Partition von M.

(c) Die durch (a) und (b) gegebenen Abbildungen sind bijektiv und gegenseitig invers.

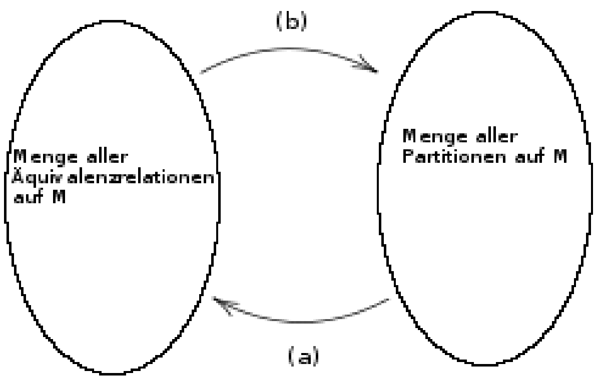

Abbildung I.6.: Eine bijektive und inverse Abbildung

Beweis:

(a)

reflexiv: Sei $a \in M$. Dann existiert ein $i \in I$ mit $a \in M_i \Rightarrow a \sim a$.

symmetrisch: Seien $a, b \in M$ mit $a \sim b \Rightarrow \exists i \in I : a, b \in M_i \Rightarrow b \sim a$.

transitiv: Seien $a, b, c \in M$ mit $a \sim b$ und $b \sim c \Rightarrow$ es gibt $i \in I$ mit $a, b \in M_i$ und es gibt $j \in J$ mit $b, c \in M_j$ Da $b \in M_i \wedge M_j$ und die Partition $M = \dot{\bigcup\limits_{i \in I}} M_i$ disjunkt ist, ist $i = j \Rightarrow a, c \in M_i = M_j$ und somit $a \sim c$. Nach Definition von $\sim$ ist $[a] = M_i$ für das einzige $i \in I$ mit $a \in M_i$

(b) Jeder $a \in M$ liegt in einer Äquivalenzklasse, z.B. in $[a]$. Also genügt es z.z.: Verschiedene Äquivalenzklassen zu $\sim$ sind sogar disjunkt. Seien dazu $a, b \in M$ mit $[a] \cap [b] \neq \emptyset$ zeige $[a] = [b]$.
Wähle $c \in [a] \cap [b]$. Dann: $a \sim c$ und $c \sim b$ transitiv $\Rightarrow a \sim b \Rightarrow a \in [b]$ und $b \in [a]$.
Ist nun $x \in [a]$, so $x \sim a$ und $a \sim b$, somit $x \sim b$ und $x \in [b]$.
Fazit: $[a] \subseteq [b]$ Analog: $[b] \subseteq [a]$

(c) Die Abbildungen sind offentsichtlich zueinander invers, daher bijektiv.

I.2.7. Bemerkung:

Gemäß 2.1 liefern die nicht leeren Fasern einer Abbildung $f : A \to B$ eine Partition von A, also eine Äquivalenzrelation auf A.
Umgekehrt kann zu jeder Partition $A = \dot{\bigcup\limits_{i \in I}} A_i$ von A eine Abbildung $g : A \to I$ definiert werden via $g(a) = i$ falls $a \in A_i$
Dann $A_i = g(i)$ und die Partition der A_i ist die Faser-Partition von g.

II. Elementare Zahlentheorie

II.1. Teilbarkeit

II.1.1. Definition:

Seien $a, b \in \mathbb{Z}$. Gibt es ein $s \in \mathbb{Z}$ mit $a = b \cdot s$, so sagen wir „b teilt a“, schreiben $b|a$ und nennen b einen Teiler von a.

II.1.2. Bemerkung:

- aus $a|b$ und $a|c$ folgt stets $a|(b \pm c)$
  $(b = a \cdot x)$ und $c = a \cdot y \Rightarrow b \pm c = a(x \pm y))$

- aus $a|b$ und $c|d$ folgt stets $ac|bd$
  $(b = ax)$ und $d = c \cdot y \Rightarrow bd = (ac)(xy)$

II.1.3. Satz:

Sei $n \in \mathbb{N}_{\setminus\{0\}}$ fest. eine Äquivalenzrelation $\equiv_n$ auf $\mathbb{Z}$ ist gegeben durch: $a \equiv_n b \Leftrightarrow n|(b-a)$ (sogenannte Kongruenz modulo n)

II.1.4. Beweis:

- **reflexiv:** Sei $a \in \mathbb{Z}$. Da $0 = n \cdot 0$, ist $n \setminus 0 = (a - b)$
  $\Rightarrow a \equiv_n a$

- **symmetrisch:** Seien $a, b \in \mathbb{Z}$ mit $a \equiv_n b \Rightarrow n|(b - a)$
  $\Rightarrow n|(a - b) \Rightarrow bn \equiv_n a$

- **transitiv:** Seien $a, b \in \mathbb{Z}$ mit $a \equiv_n b$ und $b \equiv_n c$
  $\Rightarrow n|(b - a)$ und $n|(c - b)$
  $\Rightarrow^{1.2} n|(c - b) + (b - a) = c - a$
  $\Rightarrow a \equiv_n c$

II.1.5. Satz:

Die Äquivalenzklasse zu $\equiv_n$ sind genau: $[0], [1], [2], \dots, [n-1]$ Insbesondere gilt die sogenannte Division mit Rest in $\mathbb{Z}$: zu gegebenen $a \in \mathbb{Z}, 0 < n \in \mathbb{N}$ existieren $q, r \in \mathbb{Z}$ mit $a = qn + r$ und $r \in \{0, \dots, n-1\}$ und q und r sind eindeutig bestimmt.

Beweis: Sei K eine Äquivalenzklasse zu $\equiv_n$. Wähle $r \in \mathbb{N}$ minimal bzgl. $r \in K$.

Beachte: K enthält eine natürliche Zahl. Ist $a \in K$ negativ, so addiere ein Vielfaches $q \cdot n$ von n sodass $a + qn > 0$. Dann ist $n | qn = (a + qn) - a$, also $a + qn \in K$.
Dann ist $r \in \{0, \dots, n-q\}$, dann wäre $r \geq n$, so $n | n = r - (r - n)$ also $r - n \in K$ natürliche Zahl $< r$. $\lightning$
Somit ist K eine der Äquivalenzklassen $[0], [1], \dots, [n-1]$
Sei nun $0 \leq r < s \leq n-1$

Annahme: $[r] = [s] \Rightarrow r \equiv_n s, n | s - r \quad \lightning$ zu $0 < s - r < n$

Fazit: $[r] \neq [s]$
Damit $\mathbb{Z} = [0] \mathbin{\dot\cup} [1] \mathbin{\dot\cup} \dots \mathbin{\dot\cup} [n-1]$
Ist $a \in \mathbb{Z}$, so $a \in [r]$ für ein $r \in \{0, \dots, n-1\} \Rightarrow n | a - r$
also: $a - r = qn$ für ein $q \in \mathbb{Z}, a = qn + r$

Eindeutigkeit von q und r:
Sei $q_1 n + r_1 = a = q_2 n + r_2$ mit $r_1, r_2 \in \{0, \dots, n-1\}$
Dann: $(q_1 - q_2) n = r_2 - r_1$, $n | r_2 - r_1$, $r_1 \equiv_n r_2 \Rightarrow r$.
Somit $(q_1 - a_2) \cdot n = 0 \Rightarrow^{n \neq 0} q_1 - a_2 = 0$, $q_1 = q_2$ □

II.1.6. Definition:

Eine natürliche Zahl $p \geq 2$ heißt Primzahl, wenn 1 und p die einzigigen natürlichen Zahlen sind, die p teilen.

Also: $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, \dots$

Satz:

a) Jede natürliche Zahl $n \geq 2$ ist ein Produkt von Primzahlen.

b) Euklid: Es gibt unendlich viele Primzahlen

Beweis:

a) Wähle einen kleinsten Teiler > 1 von n. Dieser muß Primzhal sein, also $n = p \cdot b$ mit $b < n$. Zerlege nun b weiter.

b) Annahme $p_1, \dots, p_s$ sind die einzigen Primzahlen.

Bild: $m = p_1, \dots, p_s + 1$. Nach (a) muss einer der p_i Teiler von m sein.

Dann: $p_i | m$ und $p_i | p_1 - p_s \Rightarrow^{1.2} p_i | m - p_1 - p_2 = 1$ ↯

II.1.7. Fundamentalsatz der Zahlentheorie

$0 \neq z \in \mathbb{Z}$ Dann hat z eine eindeutige Darstellung der Form $z = \varepsilon \cdot p_1 \cdot p_2 \cdot \dots \cdot p_s$ mit $\varepsilon \in \{\pm 1\}, p_1 \leq p_2 \leq \dots \leq p_s$ Primzahlen.

Beweis: o.E. $z \geq 0$ Induktion nach z. $z = 1$ Wähle $s = 0$

$Z \geq z$ Sei $z = p_1, \dots, p_z = q_1, \dots, q_t$ für gewisse Primzahlen p_i, q_j mit $p_1 \leq \dots \leq p_s, q_1 \leq \dots \leq q_t$.

z.z.: $s = t$ und $p_i = a_i$ für $1 \leq i \leq s$.
$s \geq$ und $t \geq 1$
o.E. $p_1 \leq q_1$

Annahme: $p_1 \lneqq q_1 \leq q_2 \leq \dots \leq q_t$
Division mit Rest durch p_1 $\quad q_j = a_j p_1 + rj$ mit $0 \leq rj < p_1$ Da p_j Primzahl $\Rightarrow rj > 0 fr 1 \leq j \leq t$.

Betrachte: $m = r_1, r_2 \dots r_t < p_1^t < q_1 \cdot q_2 \dots q_t = z$

Induktion $\Rightarrow m$ hat eindeutige Zerlegung im Produkt vin Primzahlen Insbesondere $p_1 \nmid m$ (da $p_1 \nmid rj \quad \forall j$)
Nun: $m = (q_1 - a_1 p_1)(q_2 - a_2 p_1) \dots (q_t - a_t p_1) = q_1 \cdot q_2 \dots q_t + p_1(\dots) \Rightarrow^{p_4|2} p_1 | m$ ↯

Fazit: $p_1 = q_q$ und $p_2 \dots p_s = q_2 \dots q_t$
Induktion liefer $p_j = q_j$ für $z \leq j \leq t = s$

II.1.8. Definition:

Für $a, b \in \mathbb{Z} \setminus \{0\}$ sei

- $ggT(a,b) = max\{d \in \mathbb{Z} \mid d|a \wedge d|b\}$
- kleinster gemeinsamer Vielfaches $kgV(a,b) = min\{c \in \mathbb{N} \mid a|c \wedge b|c\}$

II.1.9. Bemerkung:

Ist $a = \pm p_1^{\alpha_1} \dots p_s^{\alpha_s}$ und $b = \pm p_1^{\beta_1} \dots p_s^{\beta_s}$ mit Primzahlen $p_1 < p_2 < \dots p_s$ und gewissen $\alpha_i \geq 0, \ \beta_i \geq 0$, so gilt $ggT(a,b) = p_1^{\gamma_1} \dots p_s^{\gamma_s}$ wo $\gamma = min\{\alpha_i \beta_i\}$
$kgV(a,b) = p_1^{\delta_1} \dots p_s^{\delta_s}$ wo $\delta_i = max\{\alpha_i, \beta_i\}$
Insbesondere: $\gamma_i + \delta_i = \alpha_i + \beta_i$ und daher $|a \cdot b| = ggT(a,b) \cdot kgV(a,b)$

II.1.10. Euklidischer Algorithmus

Zur Bestimmung von $ggT(a,b)$
Seien $a, b \in \mathbb{Z} \setminus \{0\}$

1. Setze $a_0 = |a|$, $a_1 = |b|$, o.E. $q_1 < q_0$
2. Wiederhole Division mit Rest:
   $q_{i-1} = q_i \cdot a_i + a_{i+1}$ wo $0 \leq a_{i+1} < a_i$
3. Ergibt sich erstmalig $a_{m+1} = 0$, so ist $a_m = ggT(a,b)$
   Beispiel:

   $a = 90, b = 84$

   $90 = a = 1 \cdot 84 + 6$

   $84 = 14 \cdot 6 + 0$

   $\Rightarrow 6 = ggT(90, 84)$

II.1.11.

/* Fehlerhafte Nummerierung an der Tafel, oder in der Mitschrift. */

II.1.12. Satz

Der Euklidischer Alogorithmus terminiert und liefert den ggT

Beweis: Er terminiert, da $a_0 > a_1 > a_2 > \ldots > a_m > a_{m+1} \geq 0$ in $\mathbb{N}$

Zwischenschritte: - Ist $a = q \cdot b + r$, so $ggT(a,b) = ggT(b,r)$

- Ist $d|a$ und $d|b$, so $d|a - q \cdot b = r \Rightarrow d|b$ und $d|r$
- Ist $d|b$ und $d|r$, so $d|q \cdot b + r = a \Rightarrow d|a$ und $d|b$

Daher ergibt sich in 1.10
$ggT(a,b) = ggT(a_0, q_1) = ggT(a_1, q_2) = ggT(a_2, q_3) = ggT(a_{m-1}, q_m) \equiv a_m$
/* $0 = a_{am+1}$, d.h. $a_{m-1} = q_m \cdot a_{m+0}$ = dem oben genannten $\equiv$ */

II.1.13. Bemerkung:

Der Euklidische Algorithmus ist schnell.

II.1.14. Erweiterter Euklidischer Algorithmus

Mit der Notation aus 1.10 berechnen wir zustäzlich für $0 \leq j \leq m$ ganze Zahlen v_i, v_j wie folgt:

- in Schritt $1 u_0 = 1, v_0 = 0, u_1 = 0, v_1 = 1$

- in jedem Durchlauf der Schleife 2:
  $u_{i+1} = v_{i-1} - q_i \cdot u_i$
  $v_{i+1} = v_{i-1} - q_i \cdot v_i$

Dann gilt $\forall i$: $a_i = u_i \cdot a_0 + v_i \cdot a_i$
Insbesondere ist am Ende $a_m = u_m \cdot a_0 + v_m \cdot a_1 = ggT(a_0, q_1)$

Beweis: mit Induktion nach i:

$\underline{i=0}$ $a_0 = 1 \cdot a_0 + 0 \cdot a_1$ ✓

$\underline{i=1}$ $a_1 = 0 \cdot a_1 0 + 1 \cdot a_1$ ✓

$\underline{1 \leq i \to i+1}$ $a_{i-1} = a_{i-1} - q_i \cdot a_i =^{Ind} (u_{i-1} \cdot a_0 + v_{i-1} \cdot a_1) - q_i(u_i \cdot a_0 + v_i \cdot a_1)$

$$= a_0 \underbrace{(u_{i-1} - q_i \cdot u_i)}_{= u_i} + a_1 \underbrace{(v_{i-1} - q_i \cdot v_i)}_{= v_{i+1}} \qquad \square$$

II.1.15. Folgerung:

Zu beliebigen $a, b \in \mathbb{Z} \setminus \{0\}$ existieren $\underbrace{u, v \in \mathbb{Z}}_{\text{sogenannte Bezout-Koeffizienten}}$ mit $ggT(a,b) = u \cdot a + v \cdot b$
.

II.1.16. Beispiel:

$a_0 = 245,\ a_1 = 112$

a_i	q_i	u_i	v_i
245		1	0
112	2	0	1
21	5	1	−2
7	3	−5	11
0			

$7 = ggT(a_0, a_1) = (-5) \cdot 245 + 11 \cdot 112$

II.2. Modulo Rechnen

II.2.1. Motivation

Für ein festes $0 < n \in \mathbb{N}$ betrachten wir die Äquivalenzklassen zwischen Äquivalenzrelation $\equiv_n$. Es sei $\mathbb{Z}/n\mathbb{Z} = \{[0],[1],\dots,[n-1]\}$. Wir wollen eine Addition und Multiplikation auf $\mathbb{Z}/n\mathbb{Z}$ einführen, so wie wir das von der Uhr (für $n = 12$) gewöhnt sind.
$[a] + [b] = [a+b]$ und $[a]\cdot[b] = [a\cdot b] \forall\ a,b \in \mathbb{Z}$
Frage: Ist das möglich oder ergeben sich Widersprüche?

II.2.2. Satz

Die in 2.1 definierte Addition $+\ \mathbb{Z}/n\mathbb{Z}$ x $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$
und Multiplikation $\cdot\ \mathbb{Z}/n\mathbb{Z}$ x $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ sind <u>wohldefiniert</u> (widerspruchsfrei definiert), da das Ergebnis $[a]+[b]$ bzw. $[a]\cdot[b]$ nur von den Äquivalenzklassen $[a]$ und $[b]$ abhängt sind nicht von a und b selbst.

Beweis: Seien $[a_1] = [a_2], [b_1] = [b_2]$. Dann: $n|a_2 - a_1 \wedge n|b_0 - b_1$

$$\Rightarrow n|a_2 - a_1 + b_2 - b_1 = (a_2+b_2) - (a_1+b_1)$$

$$\Rightarrow \underbrace{[a_2]+[b_2]}_{[a_2]+[b_2]} = \underbrace{[a_1+b_1]}_{[a_1]+[b_2]}$$

.

Ebenso: $n|a_2(b_2 - b_2) + b_1(a_2 - a_1) = a_2b_2 - a_1b_1$

$$\Rightarrow \underbrace{[a_2b_2]}_{[a_2][b_2]} = \underbrace{[a_1b_1]}_{[a_1][b_1]}$$

.

II.2.3. Beispiel:

In $\mathbb{Z}/12\mathbb{Z}$ gilt: $[11]^2 = [11^2] = [121] = [1]$
geschickter: $[11]^2 = [-1]^2 = [(-1)^2] = [1]$

Beachte: $[3]\cdot[4] = [3\cdot 4] = [12] = [0]$ wobei $[3]$ und $[4]$ alleine gesehen jeweils $\neq 0$

Wenn klar ist, dass wir $\mathbb{Z}/n\mathbb{Z}$ rechnen für ein konstantes n, so lassen wir die Klammern i.d.R. weg.

WDH:

$\mathbb{Z}/n\mathbb{Z} = \{[0],[1],\dots,[n-1]\}$ $\quad a \equiv_n \Leftrightarrow n|b-a$ für $a,b \in \mathbb{Z}$
$[a]+[b] = [a+b]$
$[a]\cdot[b] = [a\cdot b]$

II.2.4. Bemerkung:

Da + und $\cdot$ in $\mathbb{Z}/n\mathbb{Z}$ auf die entsprechenden Rechenoperationen in $\mathbb{Z}$ zurückgeführt werden, erbt $\mathbb{Z}/n\mathbb{Z}$ die aus $\mathbb{Z}$ bekannten Rechengesetze.
Beachte jedoch: Es kann elemente $x \neq u \neq y$ in $\mathbb{Z}/n\mathbb{Z}$ geben mit $x \cdot y = 0$. (etwa $[2] \cdot [3] = [0]$ in $\mathbb{Z}/6\mathbb{Z}$)
Solche x, y heißen Nullteiler.

II.2.5. Definition:

Wir nennen $x \in \mathbb{Z}/n\mathbb{Z}$ invertierbar, falls es in $y \in \mathbb{Z}/n\mathbb{Z}$ gibt mit $x \cdot y = 1$. Mit $(\mathbb{Z}/n\mathbb{Z})^x$ bezeichnen die Menge aller invertierbaren Elemente in $\mathbb{Z}/n\mathbb{Z}$.

II.2.6. Satz:

$n \geq 1$ ist fest. Für $a \in \mathbb{Z}$ sind äquivalent:

1. $[a]$ ist invertierbar in $\mathbb{Z}/n\mathbb{Z}$

2. $ggT(a, n) = 1$

   Beweis:

$$
\begin{aligned}
(1) \Rightarrow (2)\text{: } & \text{Sei } [a] \cdot [b] = [1], \qquad n | ab - 1, n \cdot v = ab - 1 \text{ für ein } v \in \mathbb{Z} \\
. \quad & \Rightarrow 1 = ab - nv \\
. \quad & \text{Ist } q \text{ ein Teiler von } a \text{ und } n \text{, so auch von 1.} \\
. \quad & \Rightarrow q = \pm 1, ggT(a, n) = 1
\end{aligned}
$$

$$
\begin{aligned}
(1) \Rightarrow (2)\text{: } & \text{Sei } 1 = ggT(a, n) = a \cdot u + n \cdot v \text{ für gewisse } u, v \in \mathbb{Z} \\
. \quad & \Rightarrow n | nv = 1 - au \Rightarrow [1] = [a] \cdot [a] \qquad \square
\end{aligned}
$$

II.2.7. Folgerung:

$(\mathbb{Z}/n\mathbb{Z})^x = \{[a] | 0 < a < n \text{ und } ggT(a, n) = 1\}$. Ist $n = p$ eine Primzahl, so ist jedes Element $\neq 0$ in $\mathbb{Z}/p\mathbb{Z}$ invertierbar.

Beachte:

Für $n = a \cdot b$ mit $0 < a \leq b < n$ wird dies falsch.

$[a] \cdot [b] = [n] = [0]$

Wäre nun $[c] \cdot [a] = [1]$, so $[c] \cdot [a] \cdot [b] = [1] \cdot [b] = [b]$ wobei $[c] \cdot [0] = [0]$

II.2.8. Definition:

$\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^x|$ = Anzahl der $a \in \{1, \ldots, n-1\}$ mit $ggT(a,n) = 1$.
Das definiert die eulersche φ - Funktion $\varphi : \mathbb{N} \setminus \{0\} \to \mathbb{N}$

II.2.9. Satz: (Euler)

$n \geq 1$ **fest** . für jedes $x \in (\mathbb{Z}/n\mathbb{Z})^x$ gilt $x^{\varphi(n)} = 1$

Mit anderen Worten: Für jedes zu n teilerfremde $a \in \mathbb{Z}$ gilt $a^{\varphi(n)} \equiv_n 1$.

Insbesondere: Ist $n = p$ Primzahl, so $x^p = x \quad \forall x \in \mathbb{Z}/n\mathbb{Z}$. (da $\varphi(p) = p - 1$)

Beweis:

Sei $(\mathbb{Z}/n\mathbb{Z})^x = \{x_1, x_2, \ldots, x_{\varphi(n)}\}$
Für festes $z \in (\mathbb{Z}/n\mathbb{Z})^x$ definieren wir $\alpha_z : (\mathbb{Z}/n\mathbb{Z})^x \to (\mathbb{Z}/n\mathbb{Z})^x$ durch $\alpha_z(x) = x \cdot z$ $\forall x \in (\mathbb{Z}/n\mathbb{Z})^x$
(da: $x \cdot z \cdot z^{-1} \cdot x^{-1} = x \cdot 1 \cdot x^{-1} = 1 \Rightarrow xz \in (\mathbb{Z}/n\mathbb{Z})^x$) Da z invertierbar ist $z \cdot y = 1y \cdot z$ für ein $y \in (\mathbb{Z}/n\mathbb{Z})^x$ somit $\alpha_z \cdot \alpha_y = id = \alpha_y \cdot \alpha_z \Rightarrow \alpha_z$ bijekktiv.
$\Rightarrow \alpha_z$ vertauscht die Elmente $x_1, x_2, \ldots, x_{\varphi(n)}$

Somit: $\underbrace{\prod_{i=1}^{\varphi(n)} x_i}_{=:\, d} = \prod_{i=1}^{\varphi(n)} \alpha_2(x_i) = \prod_{i=1}^{\varphi(n)} (x_i \cdot z) = \underbrace{(\prod_{i=1}^{\varphi(n)} x_i)}_{=\, d} \cdot z^{\varphi(n)}$
.

Multiplikation mit d^{-1} liefert $1 = z^{\varphi(n)}$ □

II.3. Kryptographie

II.3.1. Ziel:

Anna und Bruno wollen vertrauliche Nachrichten austauschen. Jedoch ist der Übertragungsweg unsicher. Sie wissen, dass der böse Lasko lauschen wird. Gibt es eine sichere Verschlüsselungsmethode?

II.3.2. Problem:

Alle klassischen Verfahren (z.B. Caesar-Verschlüsselung) arbeiten mit einem geheimen Schlüsselwort, welches von Anna und Bruno zuvor vereinbart werden muss. Insbesondere bei häufigem Wechsel des Schlüsselworts ist das schwierig, da persönliche Treffen in aller Regel zu aufwendig sind.

II.3.3. Erinnerung:

Sei $0 < a \in \mathbb{R}$ fest. Die Logarithmusfunktion $\log_a :]0, \infty[\to \mathbb{R}$ zu Basis a. ist die Inverse der Abbildung $a^{\breve{}} : \mathbb{R} \to]0, \infty[$ speziell $a = e$ $\;x \to a^x$ für alle $x \in \mathbb{R}$ liefert $a^{\breve{}} = exp(^{\breve{}})$
$a^x = y \leftrightarrow x = \log_a y$

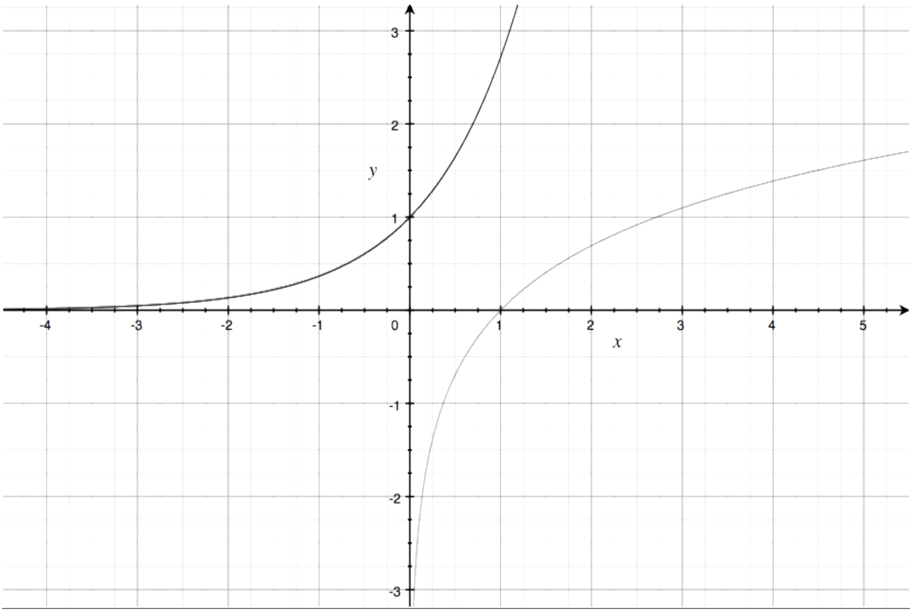

Abbildung II.1.: Es wurden $y_1 = e^x$ und $y_2 = \ln x$

II.3.4. Definition:

Es seien $2 \le n \in \mathbb{N}$ und $0 < a < n$ fest gewählt. Gilt $a^k \equiv_n b$, so nennen wir k einen diskreten Logarithmus von b zur Basis a modulo n.

II.3.5. Beispiel:

$n = 13 \quad a = 7$

b	1	2	3	4	5	6	7	8	9	10	11	12
$\log_a b \bmod n$	12	11	8	10	3	7	1	9	4	2	5	6

II.3.6. Idee:

- Die Abbildung $k \to a^k \bmod n$ ist relativ rasch zu berechnen (vgl. 3.7).

- Die Umkehrfunktion, des diskreten Logarithmus erlaubt mit heutigen Methoden keine systematische rasche Berechnung.

Wir nennen daher $k \to a^k \bmod n$ eine Einwegsfunktion.

II.3.7. Rasche Berechnung von a^k mod n

Sei $k = \varepsilon_0 \cdot 2^0 + \varepsilon_1 \cdot 2^1 + \ldots + \varepsilon_s \cdot 2^s$ mit $\varepsilon_i \in \{0,1\} = \sum_{j=0}^{s} \varepsilon_j 2^j$ die eindeutige Binärdarstellung von k.
Dann gilt:

$$a^k = a^{\sum_{j=0}^{s} \varepsilon_j 2^j} = \prod_{j=0}^{s} a^{\varepsilon_j s^j} = \prod_{j=0}^{s} (a^{2^j})^{\varepsilon_j} = \prod_{\varepsilon_j = 1}^{s} a^{2^j}$$

Wir berechnendaher die a^{2^j} mod n durch sukzessives Quadrieren und sofortiges Reduzieren modulo n.

Beispiel:
Berechne 3^{48} mod 23: Dazu: $48 = 32 + 16 = 2^5 + 2^4 = (110000)_2$

j	0	1	2	3	4	5
3^{2^j} mod_{23}	3	9	$81 \equiv 12$	$144 \equiv 6$	$36 \equiv 13$	$169 \equiv 9$

Fazit:
Anstelle von 48 Multiplikationen genügen 6 Multiplikationen.
Schlüsseltauschalgorithmus (Diffie-Hellmann)

- Anna & Bruno vereinbaren öffentlich eine Primzahl p und eine Basis $a \in \{2, \ldots, p-2\}$

- Anna & Bruno wählen jeder für sich eine persönliche Geheimzahl k_A bzw. k_B.

- Beide berechnen insgeheim $a^{k_A} \bmod p = b_A$ bzw. $a^{k_B} \bmod p = b_B$

- Anna sendet b_A an Bruno, Bruno sendet b_B an Anna (öffentlich)

- Nun können beide für sich den Rest $a^{k_A k_B} \bmod p$ berechnen.

Da
$a^{k_A k_B} = (a^{k_B})^{k_B} \equiv_p b_A^{k_B} \leftarrow$ Bruno!
$(a^{k_B})^{k_A} \equiv_p b_B^{k_A} \leftarrow$ Anna!
Damit haben beide die Geheimzahl $a^{k_A k_B}$ mod$p$ vereinbart

- Carlo kennt das ganze System, er kennt a, p, b_A, b_B und kann trotzdem nicht $a^{k_A k_B}$ mod$p$ berechnen.

II.3.8. Definition:

Es sei T eine Menge an Teilnehmern in einem Netzwerk.
Ein System öffentlicher Schlüssel sei eine Familie $\{f_t, g_t | t \in T\}$ von Abbildungen derart, dass gilt:

- f_t ist eine öffentlich bekannte Einwegsfunktion

- g_t ist eine nur dem Teilnehmer t bekannte Inverse zu f_t

II.3.9. Definition:

T = Menge der Teilnehmer $\{f_t, g_t | t \in T\}$ wo f_t Einwegsfunktion mit Inverser g_t
System öffentlicher Schlüssel

II.3.10. Vorteile:

- Gibt es ein solches System, in dem jeder Teilnehmer seinen Schlüssel f_t, g_t selbst bestimmen kann, so entfällt der Schlüsseltausch.

- Neue Teilnehmer können jederzeit hinzustoßen.

- Spontane Kommunikation wird möglich

- n Teilnehmer benötigen lediglich $2 \cdot n$Schlüssel. (anstelle $\frac{n(n-1)}{2}$ Schlüssel für Paare von Teilnehmern

II.3.11. RSA-Verfahren

1. Schlüsselerzeugung

   - Teilnemer t wählt zwei froße PRimzahlen $p_t \neq q_t$ und bildet $n_t = p_t \cdot q_t$. Dann berechnet t die Eulersche φ - Funktion $\varphi(n_t)$
     Dies ist ganz einfach:
     Die einzigen Teiler $d \in \{1, \dots, n_{t-1}\}$ mit $ggT(d, n) \neq 1$ von n_t zwischen 1 und $n_t - 1$ sind von der Form $p_t \cdot a$ (a geeignet ($1 \leq a \leq q_t - 1$)) oder $q_t \cdot b$ (b geeignet ($1 \leq b \leq p_t - 1$))
     $\Rightarrow$ Es gibt genau $(q_t - 1) + (p_t - 1)$ solche d.
     $\Rightarrow \varphi(n_t) = |\{c | 0 < c < n_t,\ ggT(c_t, n_t) = 1\}| = (n_t - 1) - (q_t - 1) - (p_t - 1) = (p_t - 1)(q_t - 1)$

   - Nun wählt t eine Zahl $k_t \in \{2, \dots, \varphi(n_t) - 1\}$ teilerfram zu $\varphi(n_t)$ (z.B. eine Primzahl $> \varphi(n_t)$ reduziert modulo$\varphi(n_t)$)

   - Mit dem erwarteten Euklid- Algorithmus bestimmt t Zahlen l_t und v_t so dass $1 = k_t \cdot l_t + \varphi(n_t) \cdot v_t$

   - t vernichtet vorraussichtlich $p_t, q_t, \varphi(n_t), v_t$

- als öffentlichen Schlüssel gibt t das Paar (k_t, n_t) heraus i als Geheimschlüssel verbleibt l_t bei t.

2. Die Sicherheit des Verfahrens beruht darauf, dass es für große p_t, q_t keinen raschen, systematischen Weg gibt, um aus n_t heraus p_t, q_t oder $\varphi(n_t)$ zu bestimmen.

3. Kryptographie mittels RSA
Anna will Bruno eine nachricht senden. Der Klartext sei eine große ganze Zahl. $x \in \{2, \ldots, n_B - 2\}$ (alle ASCII-Zeichen einer Nachricht können in einer einzigen großen Zahl zusammengefasst werden.
   - Anna verschatt sicht den öffentlichen Schlüssel (k_b, n_b) von Bruno
   - Bruno berechnet $z \equiv y^{l_B} \bmod n_B$
   - Nach Satz von Euler (2.9) gilt:
     $z \equiv y^{l_B} \equiv x^{k_B l_B + v_t \varphi(n_B)} \equiv x^1 \equiv \bmod n_B$
   - Es ist extrem unwahrscheinlich dass $ggT(x, n_B) \neq 1$ ist, da Anna sonst eine Zerlegung von n_B gefunden hätte.
   - Carlo ist machtlos, da er aus y, k_B, n_B nicht auf x kommen kann, obwohl er das Verfahren genau versteht.

II.3.12. elektronische Unterschrift

Bruno will Anna einen unterschriebenen = authentifizierten Geheimauftrag x senden. Er sendet $y \equiv x^{k_A} \bmod n_A$ und zugleich $z \equiv y^{l_B} \bmod n_B$
Jeder kann verifizieren, dass die verschlüsselte Nachricht von Bruno stammt, indem er y mti $z^{k_B} \bmod n_B$ vergleicht. Denn nur Bruno war in der Lage, z aus y heraus zu berechnen.

II.4. Primzahlen:

II.4.1. Motivation:

Wie wir gesehen haben, spielt die Bestimmung großer Primzahlen eine wichtige Rolle.

II.4.2.

(a) die Verteilung der PRimzahlen in $\mathbb{N}$ ist sehr unregelmäßig. Zu jeder Zahl $s \geq 2$ gibt es s aufeinanderfolgende Zahlen, die nicht prim sind.

Beweis: Wähle $t = s + 1$ und betrachte $t! + 2, t! + 3, \ldots, t! + t$ Offenbar ist $k | t! + k$ für $z \leq k \leq t$

(b) Die Verteilung der Rpimzahlen in $\mathbb{N}$ ist sehr regelmäßig: Bezeichne mit $\pi(x)$ die Anzahl der Primzahlen $\leq x$. Dann nähert sich $\pi(x)$ für wachsende x immer nahe der

Funktion $x \to \frac{x}{\ln(x)}$ an.

Genauer: $\lim\limits_{x\to\infty} \frac{x}{\ln(x)} = 1$ (ohne Beweis)

II.4.3. Bemerkung:

Wie viele Primzahlen gibt es zwischen 10^{199} und 10^{200} ?
Wie in 4.2 (b): Ungefähr

$$\frac{1}{\ln 10}\left(\frac{10^{200}}{200} - \frac{10^{199}}{199}\right) \approx \frac{1}{2,3} \cdot 10^{199}\left(\frac{1790}{4 \cdot 10^4}\right)$$

Die Anzahl der Atome auf der Erde $\approx 10^{51}$
Wir können es gar nicht schaffen, diese Primzahlen alle auszurechnen.

II.4.4. Satz (Fermat-Test)

Genau dann ist $n \geq 2$ eine Primzahl, wenn gilt

$$a^{n-1} \equiv_n 1 \qquad \forall a \leq \sqrt{n}$$

Beweis: „$\Rightarrow$“ Satz von Euler
(n Primzahl $\Rightarrow \varphi(n) = n-1$)
„$\Leftarrow$“
Sei n keine Primzahl, etwa $n = a \cdot b$ mit $2 \leq a \leq \sqrt{n}$
Dann $a \nmid a^{n-1} \Rightarrow n \nmid a^{n-1} - 1$, d.h. $a^{n-1} \not\equiv_n 1$

II.4.5. Problem:

Für ein einzelnes a ist die Gleichung $a^{n-1} \equiv_n 1$ schnell geprüft:
Es dauert jedoch viel zu lang, das für alle $a \leq \sqrt{n}$ zu tun.

II.4.6. Probalistischer Fermat-Test (Ausweg)

Sei $n \geq 3$ ungerade. Ist n eine Primzahl?

- Wähle $a \in \{2, \dots, n-2\}$ zufällig
- Bestimme $d = ggT(a, n)$. Ist $d > 1$, so STOP $\rightsquigarrow$ Ausgabe keine Primzahl
- Andernfalls berechne $a^{n-1} \bmod n$
  - Ist $a^{n-1} \not\equiv_n 1$, so STOP $\rightsquigarrow$ Ausgabe: Keine Primzahl
  - Ist $a^{n-1} \equiv_n 1$, so gehe zurück auf LOS.

Idee:

Entweder stellt sich nach kurzer Zeit heraus, dass n keine Primzahl, oder n ist mit hoher Wahrscheinlichkeit eine Primzahl

II.4.7. Beispiel:

Ist $341 = 11 \cdot 31$ eine Primzahl?

1. Runde $a = 2$ $\quad ggT(2, 341) = 1$ $\quad$ zeige $2^{340} \equiv_{341} 1$

   Nun: $1023 = 11 \cdot 93 \Rightarrow 11 | 2^{10} - 1 | 2^{340} - 1$

   Ferne: $31 | 2^5 - 1 | 2^{340} - 1$

   $\Rightarrow 341 = 11 \cdot 31 | 2^{340} - 1$ mit $ggT(11, 31) = 11$

   $\rightsquigarrow$ 1. Runde liefert keine Information.

2. Runde $a = 3$ $\quad ggT(341, 3) = 1$ $\quad$ Berechne 3^{340} mod341

   $340 = 2^2 \cdot 85 = 2^2(64 + 16 + 4 + 1) = 2^8 + 2^6 + 2^4 + 2^2$

2^k	2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8
3^{2^k} mod341	9	81	$6561 \equiv 82$	$6724 \equiv -96$	$9216 \equiv 9$	81	82	-98

$$\Rightarrow 3^{340} \equiv_{341} (-96)^2 \cdot 81^2 \equiv_{341} 9 \cdot 82 = 738 \not\equiv_{341} 1$$

Fazit: $a = 3$ zeigt uns, dass 341 keine Primzahl ist. Wir nennen $a = 3$ einen Zeugen für 341. $a = 2$ war kein Zeuge.

Beachte: Der Test liefert keine Zerlegung von $n = 341$.

II.4.8. Bemerkung

Es gibt Nicht-Primzahlen, für die kein Zeuge existiert. Die kleinste solche ist $561 = 3 \cdot 11 \cdot 17$

n Primzahl $\Leftrightarrow a^{n-1} \equiv_n 1 \quad \forall 2 \leq a \leq n - z$

II.4.9. Miller-Rabin-Test

Sei $n \geq 3$ ungerade. Dann ist $n-1 = 2^v \cdot m$ für ein $v \geq 1$ und m ungerade. Es folgt: $a^{n-1} - 1 = (a^{2^{v-1} \cdot m})^2 - 1^2 = (a^{2^{v-1} \cdot m} + 1) \cdot (a^{2^{v-1} \cdot m} - 1) = usw. = (a^{2^{v-1} \cdot m} + 1) \cdot (a^{2^{v-2} \cdot m}) \cdot (a^m + 1)(a^m - 1)$
Ist n Primzahl, so muss n eine der Klammern rechts teilen. Wir nennen daher n eine starke Pseudoprimzahl zur Basis a, wenn n eine der Klammern teilt.

Klar: n starke Pseudoprimzahl zu jeder Basis $a \in \{2, \ldots, n - z\} \Leftrightarrow n$ Primzahl

Beim probabilistischen Miller-Rabin-Test wird in gleicher Weise beim probabilistischen Fermat-Test für diverse Basen geprüft, ob n starke Pseudoprimzahl zur Basis a ist.

II.4.10. Beispiel:

$$n = 561,\ a = 2,\ ggT(a.n) = 1$$
$$2^{560} - 1 = (2^{280}+1)(2^{240}+1)(2^{70}+1)(2^{35}+1)(2^{35}-1)$$
Teste, ob 561 eine der Klammern teilt.
$$35 = 32 + 2 + 1 = 2^5 + 2^1 + 2^0$$

k	0	1	2	3	4	5
2^{2^k} mod561	2	4	16	256	$65536 \equiv -101$	$10201 \equiv 103$

$$\Rightarrow 2^{35} \equiv 103 \cdot 4 \cdot 2 \equiv 8824 \equiv 263 \neq \pm 1 \text{ mod} 561$$
$$2^{70} \equiv 263^2 = 69169 \equiv 166 \not\equiv \pm 1 \text{ mod} 561$$
$$2^{140} \equiv 27556 \equiv 67 \not\equiv \pm 1 \text{ mod} 561$$
$$2^{280} \equiv 67^2 \equiv 4489 \equiv 1 \not\equiv -1 \text{ mod} 561$$

$\Rightarrow$ 561 <u>keine</u> Primzahl

II.4.11. Satz:

Ist $n > 9$ ungerade und keine Primzahl, ist die Anzahl der Basen $a \in \{2, \ldots, n-z\}$ bzgl. derer n eine starke Pseudoprimzahl ist, $\leq \frac{\varphi(n)}{4} < \frac{n}{4}$ (ohne Beweis)
Somit sind min. $\frac{3}{4}$ aller Basen Zeugen für n, und die Wahrscheinlichkeit, dass bei zufällig gewählten a das n starke Pseudoprimzahl ist, ist $< \frac{1}{4}$.
Indem wir 20 Runden durschlaufen, können wir die Wahrscheinlichkeit, dass n immer noch als mögliche Primzahl gehandelt wird, auf $< \frac{1}{4^{20}} \approx \frac{1}{10^{13}}$ senken.
Wir können diese Wahrscheinlichkeit unter jede Grenze senken, also z.B. unter die Wahrscheinlichkeit, dass bei der Rechnung ein zufälliger Computerfehler eintritt.

III. Algebraische Strukturen

III.1. Gruppen

III.1.1. Definition:

Eine Gruppe G sei eine Menge mit einer Verknüpfung $* \; G \times G \to G$ derart, dass gilt:

(1) Assoziativität: $(a * b) * c = a * (b * c)$

(2) Neutrales Element: $\exists e \in G | a * e = a = e * a \;\; \forall a \in G$
(e ist eindeutig: „$e_1 = e_1 * e_2 = e_2$“)

(3) Inverse: Zu jedem $a \in G$ exsitiert ein $b \in G$ mit $a * b = e = b * a$
(das b wird als a^{-1} bezeichnet, da es eindeutig von a abhängt:
„$b_1 = b_1 * e = b_1(*a * b_2) = (b_1 * a) * b_2 = e * b_2 = b_2$“)

Beachte: (1) und (2) sind Eigenschaften für einen Monoid

G heiße zusätzlich kommutativ, falls gilt: $a * b = b * a \;\; \forall a, b \in G$

III.1.2. Beispiel:

(a) $\mathbb{N}$ mit $+$ ist Monoid, aber keine Gruppe
$\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ bzgl. $+$ sind Gruppen.
$\mathbb{Z}/n\mathbb{Z}$ bzgl. $+$ ist eine Gruppe (vererbt von $\mathbb{Z}$)
$\mathbb{Z} \setminus \{0\}$ bzgl. $\cdot$ ist Monoid
$(\mathbb{Z}/n\mathbb{Z}) \setminus \{0\}$ bzgl. $\cdot$ ist Gruppe $\Leftrightarrow$ n ist eine Primzahl
Diese Regeln sind Kommutativ

(b) Sei Ω eine Menge. Dann ist Abb $(\Omega, \Omega) = \{f | f : \Omega \to \Omega\}$ bzgl. Komposition von Abbildungen immer im Monoid. Die Mege $\mathrm{Sym}(\Omega) = \{f \in \text{Abb.}\ (\Omega, \Omega) | f \text{ bijektiv}\}$ ist eine Gruppe bzgl. Komposition. „symmetiche Gruppe“ Sym (Ω) ist nicht kommutativ, sofern $|\Omega| \geq 3$

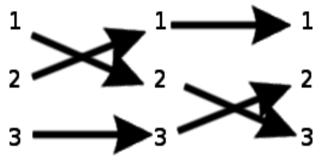

Abbildung III.1.: Fadendiagramm mit der Funktion 1 auf 3

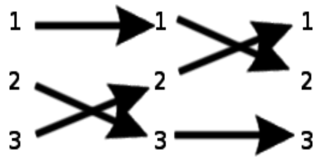

Abbildung III.2.: Fadendiagramm mit der Funktion 1 auf 2

In folgenden lassen wir $*$ weg.

III.1.3. Lemma:

Sei G eine Gruppe und $a, b, c \in G$:

(a) $(ab)^{-1} = b^{-1}a^{-1}$ und $(a^{-1})^{-1} = a$, $e^{-1} = e$

(b) Setzt man $a^0 = e$, $a^n = a(a^{n-1})$ und $a^{-n} = (a^{-1})^n \quad \forall n \geq 1$ so gelten die üblichen Potenzgesetze.

Kurzregeln:

- aus $ab = ac$ folgt stets $b = c$ (Multiplikation mit a^{-1} von links)

- aus $ab = cb$ folgt stets $a = c$ (Multiplikation mit b^{-1} von rechts)

III.1.4. Definition:

Eine Untergruppe U der Gruppe G sei eine Teilmenge von G, die bzgl. der Verknüpfung (Multiplikation) in U selbst eine Gruppe bildet. d.h. es musst gelten:

- $e \in U$

- U ist gegen Multiplikation abgeschlossen und gegen Inversion. (Dies ist gewähtleistet, falls für alle $a, b \in U$ gilt $ab^{-1} \in U$

Schreibe: $U \leq G$

III.1.5. Beispiel:

(a) $\mathbb{Z} \leq \mathbb{Q}$ bzgl. $+$

(b) $\{a^2 | a \in (\mathbb{Z}/n\mathbb{Z})^x\} \leq (\mathbb{Z}/n\mathbb{Z})^x$ (bzgl. $\cdot$) da $1^2 = 1$, $a^2b^2 = aabb$, $abab = (ab)^2$, $(a^2)^{-1} = (a^{-1})^2$

III.1.6. Satz von Lagrange

Sei G endliche Gruppe und $U \leq G$. Dann $|U| \mid |G|$.

Beweis:

Die Rechtsmultiplikation mit festen $g \in G$ ist eine bijektive Abbildung $G \to G$ /* $x \to x \cdot g$ (die Inverse ist Rechtsmultiplikativ mit g^{-1})

Daher gilt $|U| = |U \cdot g|$, $U \cdot g = \{u \cdot g | u \in U\}$ für jedes (feste) $g \in G$

$\mathbb{Z} = \dot{\bigcup}_{k=0}^{n-1} (k + n\ \mathbb{Z})$

$G = \bigcup_{g \in G} U \cdot g$, da $g = e \cdot g \in U \cdot g$

Zeige: Die Ug (g geeignet) bilden eine Partition von G. (dann:
$|G| = |\bigcup_{g \text{ geeignet}} Ug| = \sum_{g \text{ geeignet}} |Ug| = \sum_{g \text{ geeignet}} |U| = m \cdot |U|$ wo m = Anzahl der Ug (g geeignet))

Dazu sei $x \in Ug_1 \cap Ug_2$ Zeige: $Ug_1 = Ug_2$
Dann $u_1 g_1 \cdot x = u_2 g_2$ mit $u_1, u_2 \in U$ geeignet

$$\Rightarrow U \cdot u_1 g_1 = U \cdot u_2 g_2$$

$$\Leftrightarrow Ug_1 = Ug_2$$

III.1.7. Folgerung:

In jeder endlichen Gruppe G gilt: $g^{|G|} = e$ $\forall g \in G$ (vgl. Satz von Euler (II.2.6), wo $(\mathbb{Z}/n\mathbb{Z})^x = \varphi(n)$ war)

Beweis:

Betrachte $U = \{g^z | z \in \mathbb{Z}\} \leq G$ für festes g aus G.
Zeige: $g^{|U|} = e$ (dann $g^{|G|} = (g^{|U|})^m = e$ für $|G| = |U| \cdot m$ gemäß 1.6)
Kopiere hierzu den Beweis des Satzes von Euler und verwende, dass U kommutativ ist.

III.1.8. Definition:

Ein Gruppenhomomorphismus $\varphi : G \to H$ (wobei G, H Gruppen sind) Sei eine Abbildung mit $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b) \ \forall a, b \in G$

III.1.9. In der Notation von 1.8 gilt

(a) $\varphi(e) = e \to$ von h und $\varphi(g^{-1}) = (\varphi(g))^{-1} \ \forall g \in G$

(b) Bild $q \leq H$

Beweis:

(a): $e \cdot \varphi(e) = \varphi(e) = {}'\varphi(e \cdot e) = \varphi(e) \cdot \varphi(e) \overset{\text{kürzen}}{\Rightarrow} e = \varphi(e)$
$e = \varphi(e) = \varphi(g \cdot g^{-1}) = \varphi(g) \cdot \varphi(g^{-1})$
ebenso $= \varphi(g^{-1})\varphi(g)$
$\Rightarrow \varphi(g^{-1}) = (\varphi(g))^{-1}$

(b): $e = \varphi(e) \in$ Bild φ und $\varphi(a) \cdot \varphi(b)^{-1} = \varphi(a) \cdot \varphi(b^{-1}) = {}'\varphi(ab^{-1}) \in$ Bild φ

Abbildungsverzeichnis