Diskrete Strukturen

Wilfried Buchholz

Skriptum einer 3-std. Vorlesung im Sommersemester 2009

Mathematisches Institut der Universität München

§1 Vollständige Induktion

Wir setzen hier das System $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, 3, \ldots\}$ der *ganzen Zahlen* und das Rechnen mit diesen Zahlen als bekannt voraus. Es sei $\mathbb{N} := \{0, 1, 2, 3, \ldots\}$ die Menge der nicht-negative ganzen Zahlen. Die Elemente dieser Menge heißen *natürliche Zahlen.*

Im folgenden bezeichen wir mit den Buchstaben i, j, k, l, m, n stets natürliche Zahlen.

Das Beweisprinzip der **vollständigen Induktion** lautet:

$\mathcal{A}(n_0)\ \&\ \forall n \geq n_0(\mathcal{A}(n) \Rightarrow \mathcal{A}(n{+}1)) \ \Rightarrow\ \forall n \geq n_0\, \mathcal{A}(n)$,

d.h. um die Aussage $\forall n \geq n_0 \mathcal{A}(n)$ zu beweisen, genügt es, folgendes zu zeigen:

(I) $\mathcal{A}(n_0)$ (*Induktionsanfang*)

(II) $\forall n \geq n_0[\,\mathcal{A}(n) \Rightarrow \mathcal{A}(n{+}1)\,]$ (*Induktionsschritt* oder *Schluß von n auf $n{+}1$*).

Die Annahme $\mathcal{A}(n)$ in (II) nennt man *Induktionsvoraussetzung* oder *Induktionshypothese* (kurz IH).

Beispiele.

(a) Für alle $n \geq 5$ gilt $n^2 < 2^n$.

(b) Sind $a_0 < \ldots < a_n$ natürliche Zahlen, so gilt $n \leq a_n$.

Beweis durch (vollständige) Induktion nach n:

(a) (I) $5^2 = 25 < 32 = 2^5$. (II) $n \geq 5\ \&\ n^2 < 2^n \ \Rightarrow\ (n+1)^2 = n^2 + 2n + 1 < n^2 + n^2 < 2^n + 2^n = 2^{n+1}$.

(b) (I) $0 \leq a_0$.

(II) $a_0 < ... < a_n < a_{n+1} \overset{\text{IH}}{\Rightarrow}\ n \leq a_n < a_{n+1} \ \Rightarrow\ n{+}1 \leq a_{n+1}$.

1.1 Satz (Allgemeine Induktion).

Sei M eine Menge und $\mu : M \to \mathbb{N}$. Dann gilt fuer jede Aussage $\mathcal{A}(x)$:

$\forall x \in M[\forall y \in M(\mu(y) < \mu(x) \Rightarrow \mathcal{A}(y)) \Rightarrow \mathcal{A}(x)] \ \Rightarrow\ \forall x \in M \mathcal{A}(x)$.

Beweis:

Abk.: $\mathcal{A}^*(n) \ :\Leftrightarrow\ \forall y \in M(\mu(y) < n \Rightarrow \mathcal{A}(y))$.

Gelte $\forall x \in M[\forall y \in M(\mu(y) < \mu(x) \Rightarrow \mathcal{A}(y)) \to \mathcal{A}(x)]$. Dann: (1) $\forall x \in M(\mathcal{A}^*(\mu(x)) \Rightarrow \mathcal{A}(x))$.

Wir zeigen nun $\forall n \mathcal{A}^*(n)$ durch Induktion nach n. Mit (1) folgt daraus dann $\forall x \in M \mathcal{A}(x)$.

(I) $\mathcal{A}^*(0)$ gilt trivialerweise.

(II) $\mathcal{A}^*(n) \overset{(1)}{\Rightarrow}\ \mathcal{A}^*(n)\ \&\ \forall x \in M(\mu(x) = n \Rightarrow \mathcal{A}(x)) \ \Rightarrow\ \forall x(\mu(x) < n + 1 \to \mathcal{A}(x))$, i.e. $\mathcal{A}^*(n+1)$.

Korollar ($<_{\mathbb{N}}$-Induktion). $\forall n(\forall k < n \mathcal{A}(k) \Rightarrow \mathcal{A}(n)) \Rightarrow \forall n \mathcal{A}(n)$.

Beispiel.

Die Folge $(a_n)_{n \in \mathbb{N}}$ der Fibonacci-Zahlen wird durch folgende Rekursionsgleichungen definiert:

$a_0 := 0$, $a_1 := 1$, $a_{n+2} := a_n + a_{n+1}$. $(a_2 = 1,\ a_3 = 2,\ a_4 = 3,\ a_5 = 5,\ a_6 = 8, ...)$

Behauptung: $n \geq 2 \Rightarrow a_{n+2} \geq (\frac{3}{2})^n$.

Beweis durch $<_{\mathbb{N}}$-Induktion:

Fall 1: $n < 2$. Trivial. Fall 2: $n = 2$. $a_4 = 3 > \frac{9}{4} = (\frac{3}{2})^2$. Fall 3: $n = 3$. $a_5 = 5 > \frac{27}{8} = (\frac{3}{2})^3$.

Fall 4: $n \geq 4$. $a_{n+2} = a_n + a_{n+1} \overset{\text{IH}}{\geq} (\frac{3}{2})^{n-2} + (\frac{3}{2})^{n-1} = (\frac{3}{2})^{n-2}(1 + \frac{3}{2}) > (\frac{3}{2})^{n-2} \cdot \frac{9}{4} = (\frac{3}{2})^n$.

Definition. $n \in \mathbb{N}$ heißt *Primzahl* $:\Leftrightarrow\ 2 \leq n\ \&\ \neg\exists m,k < n(n = mk)$.

1.2 Satz. Jede natürliche Zahl $n \geq 2$ kann als Produkt von Primzahlen dargestellt werden.

Beweis durch $<_{\mathbb{N}}$-Induktion: Sei $n \geq 2$.

Fall 1: n Primzahl. Dann fertig.

Fall 2: n ist keine Primzahl. Dann existieren $m,k < n$ mit $n = mk$. Wegen $2 \leq n$ gilt $2 \leq m,k$. Nach IH haben wir Darstellungen $m = p_1 \cdots p_r$ und $k = q_1 \cdots q_s$, also $n = mk = p_1 \cdots p_r q_1 \cdots q_s$.

1.3 Satz (Prinzip vom kleinsten Element).

$\emptyset \neq A \subseteq \mathbb{N}\ \Rightarrow\ \exists n \in A \forall k \in A(n \leq k)$.

(Jede nichtleere Menge natürlicher Zahlen besitzt ein Minimum, d.h. kleinstes Element.)

Beweis:

(1) $\forall n[\forall k < n(k \notin A \Rightarrow n \notin A) \Rightarrow \forall n(n \notin A)$ [$<_{\mathbb{N}}$-Induktion]

(2) $\neg\forall n(n \notin A) \Rightarrow \neg\forall n(\forall k < n(k \notin A) \Rightarrow n \notin A)$ [logisch äquivalent zu (1)]

(3) $\exists n(n \in A) \Rightarrow \exists n(\forall k < n(k \notin A)\ \&\ n \in A)$ [logisch äquivalent zu (2)].

1.4 Lemma.

Jede nach unten (oben) beschränkte nichtleere Menge $A \subseteq \mathbb{Z}$ besitzt ein Minimum (Maximum).

Beweis:

1. Sei $a \in A$ und c eine untere Schranke. Dann ist $B := \{n : c + n \in A\} \neq \emptyset$ (denn $a - c \in B$); es existiert also $n_0 := \min(B)$. Dann ist $c + n_0 = \min(A)$. ($x \in A\ \Rightarrow\ x - c \in B\ \Rightarrow\ n_0 \leq x - c\ \Rightarrow\ c + n_0 \leq x$.)

2. A nach oben beschränkt $\Rightarrow\ -A = \{-x : x \in A\}$ nach unten beschränkt ....

1.5 Lemma. Seien $a, b \in \mathbb{Z}$, $1 \leq b$.

(a) Es existiert genau ein $q \in \mathbb{Z}$ mit $bq \leq a < b(q+1)$.

(b) Es existieren eindeutig $q, r \in \mathbb{Z}$ mit $a = bq + r$ und $0 \leq r < b$.

Beweis:

(a) Eindeutigkeit: $bq_i \leq a < b(q_i + 1)$ $(i = 0, 1)\ \Rightarrow\ bq_0 \leq a < b(q_1 + 1)\ \&\ bq_1 \leq a < b(q_0 + 1)\ \Rightarrow$
$\Rightarrow\ q_0 < q_1 + 1\ \&\ q_1 < q_0 + 1\ \Rightarrow\ q_0 = q_1$.

Existenz: Fall 1: $0 \leq a$. Sei $M := \{x \in \mathbb{Z} : xb \leq a\}$. M ist nicht leer (z.B. ist $0 \in M$) und nach oben beschränkt (z.B. durch a). Somit existiert $q := \max(M)$. Es folgt $bq \leq a < b(q+1)$.

Fall 2: $a < 0$. Nach 1. existiert $\tilde{q}$ mit $b\tilde{q} \leq -a < b(\tilde{q}+1)$, also $b \cdot (-\tilde{q} - 1) < a \leq b \cdot (-\tilde{q})$.
Mit $q := \begin{cases} -\tilde{q} & \text{falls } a = b \cdot (-\tilde{q}) \\ -\tilde{q} - 1 & \text{sonst} \end{cases}$ folgt daraus $bq \leq a < b(q+1)$.

(b) Sei q wie in (a) und $r := a - bq$.

b-adische Darstellung natürlicher Zahlen

1.6 Lemma. Sei $b, c_i, c_i' \in \mathbb{N}$ und $2 \leq b$.

(a) $0 \leq c_0, ..., c_n < b\ \Rightarrow\ \sum_{i=0}^{n} c_i b^i < b^{n+1}$.

(b) $0 \leq c_0, c_0', \ldots, c_n, c_n' < b\ \&\ \sum_{i=0}^{n} c_i b^i = \sum_{i=0}^{n} c_i' b^i\ \Rightarrow\ c_i = c_i'$ für $i = 0, ..., n$.

Beweis durch Induktion nach n:
(a) $\sum_{i=0}^{n} c_i b^i = \sum_{i=0}^{n-1} c_i b^i + c_n b^n \overset{\text{IH bzw.}(*)}{<} b^n + c_n b^n = (1+c_n)b^n \leq b^{n+1}$.
$(*)$ Im Fall $n = 0$ ist $\sum_{i=0}^{n-1} c_i b^i = 0 < b^n$.
(b) $\sum_{i=0}^{n} c_i b^i = \sum_{i=0}^{n} c'_i b^i =: a \;\Rightarrow\; a = b(\sum_{i=0}^{n-1} c_{i+1} b^i) + c_0$ & $a = b(\sum_{i=0}^{n-1} c'_{i+1} b^i) + c'_0 \overset{\text{Lemma 1.5b}}{\Rightarrow}$
$c_0 = c'_0$ & $\sum_{i=0}^{n-1} c_{i+1} b^i = \sum_{i=0}^{n-1} c'_{i+1} b^i \overset{\text{IH}}{\Rightarrow} c_0 = c'_0$ & $c_{i+1} = c_{i+1}$ für $i = 0, ..., n-1$.

1.7 Satz. Seien $a, b \in \mathbb{N}$ mit $2 \leq b$ und $0 < a$.
Dann existiert genau eine Tupel $(c_n, ..., c_0)$ natürlicher Zahlen $< b$, so daß $a = \sum_{i=0}^{n} c_i b^i$ und $c_n > 0$.

Man nennt $(c_n, \ldots, c_0)$ die b-adische Darstellung von a. Die b-adische Darstellung von 0 sei ( ).

Beweis:
Existenz: Induktion nach a. Nach Lemma 1.5b existieren c_0, a' mit $a = ba' + c_0$ und $0 \leq c_0 < b$. Wegen $2 \leq b$ ist $0 \leq a' < a$. Ist $a' = 0$, so $c_0 = a > 0$. Andernfalls haben wir nach IH $a' = \sum_{i=0}^{n} c'_i b^i$ mit $0 \leq c'_i < b$ und $c'_n > 0$. Wir setzen $c_{i+1} := c'_i$ und erhalten $a = ba' + c_0 = b(c'_n b^n + \ldots + c'_0 b^0) + c_0 = c_{n+1} b^{n+1} + \ldots + c_1 b^1 + c_0 b^0$.
Eindeutigkeit: Ist $a = \sum_{i=0}^{n} c_i b^i$ mit $0 \leq c_0, ..., c_n < b$ und $0 < c_n$, so gilt $b^n \leq a \overset{\text{L.1.6a}}{<} b^{n+1}$. Damit ist n eindeutig bestimmt. Die Eindeutigkeit von $c_0, ..., c_n$ folgt aus L.1.6b.

Bezeichnung.
$D(b; a)$ bezeichne die b-adische Darstellung von $a \in \mathbb{N}$.
Ferner sei $[\,]_b := 0$ und $[c_n, ..., c_0]_b := \sum_{i=0}^{n} c_i b^i$.

Bemerkung.
Aus dem Beweis von Satz 1.7 erhält man folgende rekursive Beschreibung von $D(b; a)$:

$$D(b;a) = \begin{cases} ( ) & \text{falls } a = 0 \\ D(b;q) * (r) & \text{falls } 0 < a = bq + r \text{ mit } 0 \leq r < b \end{cases}.$$

Umgekehrt gilt: $[c_n, ..., c_0]_b := b \cdot [c_n, ..., c_1]_b + c_0$.

Beispiele.

$[5,4,3,2,1]_7 = 7{\cdot}[5,4,3,2]_7{+}1 = 7(7{\cdot}[5,4,3]_7{+}2){+}1 = 7(7(7{\cdot}[5,4]_7{+}3){+}2){+}1 = 7(7(7(7{\cdot}[5]_7{+}4){+}3){+}2){+}1 =$
$= 7(7(7(7{\cdot}5+4)+3)+2)+1 = 7(7(7{\cdot}39+3)+2)+1 = 7(7{\cdot}276+2)+1 = 7{\cdot}1934+1 = 13539.$

Verschiedene Darstellungen von 893:

Hexadesimal: $893 = 16{\cdot}55 + 13 = 16(16{\cdot}3+7)+13 = 16(16(16{\cdot}0+3)+7)+13 = [3,7,13]_{16}$.

Oktal: $893 = 8{\cdot}111 + 5 = 8(8{\cdot}13+7)+5 = 8(8(8{\cdot}1+5)+7)+5 = 8(8(8(8{\cdot}0+1)+5)+7)+5 = [1,5,7,5]_8$.

Binär: $893 = 2{\cdot}446 + \mathbf{1}$, $446 = 2{\cdot}223 + \mathbf{0}$, $223 = 2{\cdot}111 + \mathbf{1}$, $111 = 2{\cdot}55 + \mathbf{1}$, $55 = 2{\cdot}27 + \mathbf{1}$, $27 = 2{\cdot}13 + \mathbf{1}$, $13 = 2{\cdot}6 + \mathbf{1}$, $6 = 2{\cdot}3 + \mathbf{0}$, $3 = 2{\cdot}1 + \mathbf{1}$, $1 = 2{\cdot}0 + \mathbf{1}$. Also $893 = [1,1,0,1,1,1,1,1,0,1]_2$.

§2 Endliche Mengen; Grundlagen der Kombinatorik

Abkürzungen.

1. Für $n \in \mathbb{N}$ sei $I_n := \{i \in \mathbb{N} : i < n\}$ $(= \{0, ..., n-1\})$

2. $f : X \to Y$ $:\Leftrightarrow$ f ist eine Abbildung (Funktion) von X nach Y.

3. $f : X \leftrightarrow Y$ $:\Leftrightarrow$ f ist eine bijektive Abbildung (Bijektion) von X nach (auf) Y.

4. Y^X := Menge aller Abbildungen von X nach Y.

5. $\mathcal{P}(X)$:= Menge aller Teilmengen von X (*Potenzmenge* von X).

2.1 Lemma. Ist $f : I_m \to I_n$ injektiv, so $m \leq n$.

Korollar. Aus $f : I_m \leftrightarrow I_n$ folgt $m = n$.

Beweis durch Induktion nach n:

1. $n = 0$: Dann auch $m = 0$.

2. $n = n_0 + 1$ und $f(I_m) \subseteq I_{n_0}$: Aus IH folgt $m \leq n_0$.

3. $n = n_0 + 1$ und $f(I_m) \not\subseteq I_{n_0}$: Dann ist $m = m_0 + 1$ und es existiert ein $j \leq m_0$ mit $f(j) = n_0$.

3.1. $j = m_0$: Dann $f|I_{m_0} : I_{m_0} \to I_{n_0}$ injektiv und somit nach IH $m_0 \leq n_0$, also auch $m \leq n$.

3.2. $j < m_0$: Dann $f(m_0) < n_0$. Definition $g : I_{m_0} \to I_{n_0}$, $g(i) := \begin{cases} f(m_0) & \text{falls } i = j \\ f(i) & \text{sonst} \end{cases}$.

Wie man leicht sieht, ist g injektiv und folglich $m_0 \leq n_0$.

Definition.

Eine Menge X heißt *endlich*, wenn es ein $n \in \mathbb{N}$ und eine Bijektion $f : I_n \to X$ gibt. Dieses (nach Lemma 2.1 eindeutig bestimmte) n heißt *Mächtigkeit* oder *Anzahl der Elemente* von X und wird mit $|X|$ bezeichnet.

(Eindeutigkeit $f : X \leftrightarrow I_n$ & $g : X \leftrightarrow I_m$ $\Rightarrow$ $f \circ g^{-1} : I_m \leftrightarrow I_n$ $\Rightarrow$ $m = n$.)

Eine Menge X heißt *unendlich*, wenn sie nicht endlich ist. Für unendliches X sei $|X| := \infty$.

Für $n \in \mathbb{N}$ sei (per Definition) $n < \infty$.

Bemerkung. $\mathbb{N}$ ist unendlich.

Beweis: $f : \mathbb{N} \to I_n$ injektiv $\Rightarrow$ $f|I_{n+1} \to I_n$ injektiv $\overset{\text{L.2.1}}{\Rightarrow}$ $n+1 \leq n$. Widerspruch.

Bemerkung. $|\emptyset| = 0$, $|\{a\}| = 1$.

2.2 Lemma. X, Y endlich und $X \cap Y = \emptyset$ $\Rightarrow$ $|X \cup Y| = |X| + |Y|$.

Beweis :

Sei $f : X \leftrightarrow I_m$ und $g : Y \leftrightarrow I_n$. Definition: $h : X \cup Y \to I_{m+n}$, $h(z) := \begin{cases} f(z) & \text{falls } z \in X \\ m + g(z) & \text{falls } z \in Y \end{cases}$.

h ist offenbar bijektiv, also $|X \cup Y| = m + n = |X| + |Y|$.

2.3 Lemma. $Y \subseteq I_n$ $\Rightarrow$ $|Y| \leq n$.

Beweis durch Induktion nach n:

Für $n = 0$ ist die Behauptung trivial, denn $I_0 = \emptyset$. Sei jetzt $n = n_0 + 1$.

Fall 1: $Y \subseteq I_{n_0}$: Beh. folgt aus IH.

Fall 2: $Y = Y_0 \cup \{n_0\}$ mit $Y_0 \subseteq I_{n_0}$: $|Y_0| \overset{\text{IH}}{\leq} n_0$ & $|\{n_0\}| = 1$ $\Rightarrow$ $|Y| \overset{\text{L.2.2}}{=} |Y_0| + |\{n_0\}| \leq n_0 + 1 = n$.

2.4 Lemma.

(a) $f : X \to Y$ bijektiv $\Rightarrow\ |X| = |Y|$.

(b) $f : X \to Y$ injektiv $\Rightarrow\ |X| \leq |Y|$.

(c) $f : X \to Y\ \ \Rightarrow\ |f(X)| \leq |X|$.

(d) X endlich & $X \subsetneqq Y\ \Rightarrow\ |X| < |Y|$.

Beweis :

(a) klar.

(b) Sei $g : Y \leftrightarrow I_n$ und $Z := g(f(X))$. Dann $g \circ f : X \leftrightarrow Z \subseteq I_n$ und folglich $|X| \overset{\text{(a)}}{=} |Z| \overset{\text{L.2.3}}{\leq} n = |Y|$.

(c) Ohne Beschränkung der Allgemeinheit können wir $X = I_n$, also $f : I_n \to Y$, annehmen. Offenbar ist dann $g : f(I_n) \to I_n$, $g(x) := \min\{i < n : f(i) = x\}$ injektiv. Nach (b) gilt deshalb $|f(I_n)| \leq |I_n|$.

(d) Sei $y_0 \in Y \setminus X$. Dann $|X| < |X| + 1 = |X \cup \{y_0\}| \overset{\text{(b)}}{\leq} |Y|$.

2.5 Lemma. Ist X endlich und $f : X \to Y$, so gilt:

(a) f injektiv $\Leftrightarrow\ |f(X)| = |X|$.

(b) $|X| = |Y|\ \Rightarrow\ (\,f$ injektiv $\Leftrightarrow\ f$ surjektiv$\,)$.

Beweis :

(a) "$\Rightarrow$": f injektiv $\Rightarrow\ f : X \to f(X)$ bijektiv $\overset{\text{L.2.4a}}{\Rightarrow}\ |f(X)| = |X|$.

"$\Leftarrow$": Sei f nicht injektiv. Dann gibt es $x_0, x_1 \in X$ mit $f(x_0) = f(x_1)$ und $x_0 \neq x_1$. Sei $X_0 := X \setminus \{x_0\}$. Dann $|X| = |X_0| + 1$ und $f(X_0) = f(X)$, also $|f(X)| = |f(X_0)| \overset{\text{2.4c}}{\leq} |X_0| < |X|$.

(b) f injektiv $\overset{\text{(a)}}{\Leftrightarrow}\ |f(X)| = |X|\ \overset{|X|=|Y|}{\Leftrightarrow}\ |f(X)| = |Y|\ \ \overset{(*)}{\Longleftrightarrow} f(X) = Y$. $(*)$ $f(X) \subseteq Y$ und L.2.4c,d.

2.6 Lemma. Für endliche Mengen X, Y gilt:

(a) $|X \times Y| = |X| \cdot |Y|$.

(b) $|Y^X| = |Y|^{|X|}$.

(c) $|\mathcal{P}(X)| = 2^{|X|}$.

Beweis :

(a) Induktion nach $|X|$: 1. $X = \emptyset$: $|X \times Y| = |\emptyset| = 0 = |X| \cdot |Y|$.

2. $X = X_0 \dot\cup \{a\}$: Dann $X \times Y = (X_0 \times Y) \dot\cup (\{a\} \times Y)$ und folglich

$|X \times Y| = |X_0 \times Y| + |\{a\} \times Y| = |X_0| \cdot |Y| + |Y| = (|X_0|+1) \cdot |Y| = |X| \cdot |Y|$.

(b) Induktion nach $|X|$:

1. $X = \emptyset$: $|Y^X| = 1 = |Y|^0$.

2. $X = X_0 \dot\cup \{a\}$: Die Abbildung $Y^{X_0} \times Y \to Y^X$, $(f, y) \mapsto f \cup \{(a, y)\}$ ist bijektiv und folglich

$|Y^X| = |Y^{X_0} \times Y| \overset{\text{(a)}}{=} |Y^{X_0}| \cdot |Y| \overset{\text{IH}}{=} |Y|^{|X_0|} \cdot |Y| = |Y|^{|X|}$.

(c) Für $M \subseteq X$ sei $\chi_M : X \to \{0,1\}$, $\chi_M(x) := \begin{cases} 1 & \text{falls } x \in X \\ 0 & \text{sonst} \end{cases}$.

Dann ist die Abbildung $\mathcal{P}(X) \to \{0,1\}^X$, $M \mapsto \chi_M$ bijektiv und folglich gilt $|\mathcal{P}(X)| = |\{0,1\}^X| \overset{\text{(b)}}{=} 2^{|X|}$

Bemerkung. In Verallgemeinerung von 2.2 und 2.6a gilt:

(a) Ist X die disjunkte Vereinigung der Mengen $X_1, ..., X_n$, so ist $|X| = |X_1| + \ldots + |X_n|$.

(b) $|X_1 \times \ldots \times X_n| = |X_1| \cdot \ldots \cdot |X_n|$.

Definitionen.

$0! := 1$, $(n+1)! := n! \cdot (n+1)$; $\quad \binom{n}{k} = \frac{n!}{k!(n-k)!}$, falls $k \leq n$; für $k > n$ sei $\binom{n}{k} = 0$.

$\mathcal{P}_k(X) := \{Y \in \mathcal{P}(X) : |Y| = k\}$. *Bemerkung.* $\binom{n}{k} = \binom{n}{n-k}$ für $k \leq n$.

2.7 Lemma.

(a) $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$, falls $0 < k, n$.

(b) $|\mathcal{P}_k(X)| = \binom{n}{k}$, falls $n = |X|$.

(c) $\sum_{k=0}^{n} \binom{n}{k} = 2^n$.

Beweis :

(a) 1. $k = n$: $\binom{n}{n} = 1 = \binom{n-1}{n-1} + \binom{n-1}{n}$.

2. $k > n$: $\binom{n}{k} = 0 = \binom{n-1}{k-1} + \binom{n-1}{k}$.

3. $0 < k < n$: $\frac{(n-1)!}{(k-1)!(n-1-(k-1))!} + \frac{(n-1)!}{k!(n-1-k)!} = \frac{(n-1)!\,k + (n-1)!(n-k)}{k!(n-k)!} = \frac{n!}{k!(n-k)!}$.

(b) Induktion nach n:

1. $n = 0$ oder $k = 0$: klar.

2. $0 < n, k$: Dann $X = X_0 \cup \{a\}$ mit $|X_0| = n - 1$.

Ferner $\mathcal{P}_k(X) = \mathcal{P}_k(X_0) \,\dot\cup\, M$ mit $M := \{Y \cup \{a\} : Y \in \mathcal{P}_{k-1}(X_0)\}$.

Somit $|\mathcal{P}_k(X)| = |\mathcal{P}_k(X_0)| + |M| = |\mathcal{P}_k(X_0)| + |\mathcal{P}_{k-1}(X_0)| \overset{\text{IH}}{=} \binom{n-1}{k} + \binom{n-1}{k-1} \overset{\text{(a)}}{=} \binom{n}{k}$.

(c) Sei $X = \{1, ..., n\}$. Offenbar ist $\mathcal{P}(X)$ die disjunkte Vereinigung der Mengen $\mathcal{P}_k(X)$ $(k = 0, ..., n)$.

Daraus folgt $\sum_{k=0}^{n} |\mathcal{P}_k(X)| = |\mathcal{P}(X)|$ und weiter (mit (b) und 2.6c) die Behauptung.

2.8 Lemma (Binomischer Satz). $\quad (x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$, für alle $x, y \in \mathbb{R}$ und $n \in \mathbb{N}$.

Beweis durch Induktion nach n:

I. $n = 0$: $(x+y)^0 = 1 = \binom{0}{0} x^0 y^0 = \sum_{i=0}^{0} \binom{0}{k} x^{0-k} y^k$.

II. $(x+y)^{n+1} = (x+y) \cdot (x+y)^n \overset{\text{IH}}{=} (x+y) \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k = \sum_{k=0}^{n} \binom{n}{k} x^{n+1-k} y^k + \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^{k+1} =$

$\sum_{k=0}^{n} \binom{n}{k} x^{n+1-k} y^k + \sum_{k=1}^{n+1} \binom{n}{k-1} x^{n+1-k} y^k = x^{n+1} + \sum_{k=1}^{n} \left[\binom{n}{k} + \binom{n}{k-1}\right] x^{n+1-k} y^k + y^{n+1} =$

$x^{n+1} + \sum_{k=1}^{n} \binom{n+1}{k} x^{n+1-k} y^k + y^{n+1} = \sum_{k=0}^{n+1} \binom{n+1}{k} x^{n+1-k} y^k$.

Abkürzungen.

$\mathrm{Bij}(X, Y)$ (bzw. $\mathrm{Inj}(X, Y)$ bzw. $\mathrm{Surj}(X, Y)$) bezeichne die Menge aller bijektiven (bzw. injektiven bzw. surjektiven) Abbildungen von X nach Y. $\mathcal{S}(X) := \mathrm{Bij}(X, X)$ nennt man die *symmetrische Gruppe* der Menge X. Schließlich sei $\mathcal{S}_n := \mathcal{S}(\{1, ..., n\})$. Die Elemente von $\mathcal{S}_n$ nennt man *Permutationen* der Zahlen $1, ..., n$.

2.9 Lemma.

(a) $|X| = |Y| = n \;\Rightarrow\; |\mathrm{Bij}(X, Y)| = n!$.

(b) $m = |X| \leq |Y| = n \;\Rightarrow\; |\mathrm{Inj}(X, Y)| = \frac{n!}{(n-m)!} = n \cdot (n-1) \cdot (n-2) \cdots (n-m+1)$.

Beweis :

(a) Induktion nach n: 1. $n = 0$: $|\mathrm{Bij}(X, Y)| = 1 = 0!$. 2. $n > 0$: Sei $a \in X$ und

$\mathcal{F}_y := \{f \in \mathrm{Bij}(X, Y) : f(a) = y\}$. Offenbar ist $\mathrm{Bij}(X, Y)$ die disjunkte Vereiningung aller $\mathcal{F}_y$ $(y \in Y)$. Ferner gilt $|\mathcal{F}_y| = |\mathrm{Bij}(X \setminus \{a\}, Y \setminus \{y\})| \overset{\mathrm{IH}}{=} (n-1)!$. Folglich $|\mathrm{Bij}(X, Y)| = \sum_{y \in Y} |\mathcal{F}_y| = (n-1)! \cdot n = n!$.

(b) Offenbar ist $\mathrm{Inj}(X, Y)$ die disjunkte Vereinigung aller Mengen $\mathrm{Bij}(X, Z)$ $(Z \in \mathcal{P}_m(Y))$, und folglich $|\mathrm{Inj}(X, Y)| = \sum_{Z \in \mathcal{P}_m(Y)} |\mathrm{Bij}(X, Z)| \overset{\text{(a)+L.2.7b}}{=} \binom{n}{m} \cdot m! = \frac{n!}{(n-m)!}$.

Beispiel.

Auf einer Party, auf der mindestens 23 Personen sind, ist die Chance, dass davon zwei Personen am gleichen Tag Geburtstag haben, größer als die, daß es keine Geburtstagspaare gibt.

Sei $X := \{1, ..., m\}$, $Y := \{1, ..., n\}$. $(m = 23,\ n = 365)$

$\frac{|Y^X \setminus \mathrm{Inj}(X, Y)|}{|Y^X|} = \frac{|Y^X| - |\mathrm{Inj}(X, Y)|}{|Y^X|} = 1 - \frac{n \cdot (n-1) \cdots (n-m+1)}{n^m}$. $\quad 1 - \frac{365 \cdot 364 \cdots 343}{365^{23}} = 0.5073$

Beispiel.

Wieviele "Möglichkeiten" gibt es, aus einer Menge von n Kugeln m Kugeln (genauer, m mal eine Kugel) zu ziehen, wobei folgende vier Versionen unterschieden werden?

1. Ziehen ohne Zurücklegen, Reihenfolge nicht relevant:
   Ziehung $\widehat{=}$ m-elementige Teilmenge von $\{1, ..., n\}$. Zahl der möglichen Ziehungen: $\binom{n}{m}$.
3. Ziehen ohne Zurücklegen, Reihenfolge relevant:
   Ziehung $\widehat{=}$ Injektion von $\{1, ..., m\}$ nach $\{1, ..., n\}$. Zahl der möglichen Ziehungen: $\frac{n!}{(n-m)!}$.
3. Ziehen mit Zurücklegen, Reihenfolge relevant:
   Ziehung $\widehat{=}$ m-tupel aus $\{1, ..., n\}$ (d.h. Element von $\{1, ..., n\}^m$). Zahl der möglichen Ziehungen: n^m.
4. Ziehen mit Zurücklegen, Reihenfolge nicht relevant:
   Eine Ziehung ist ein m-Tupel von Elementen aus $\{1, ..., n\}$, wobei es nicht auf die Reihenfolge ankommt.
   Die möglichen Ziehungen *entsprechen* deshalb den Elementen von
   $Z_{m,n} := \{(k_1, ..., k_m) : 1 \le k_1 \le \ldots \le k_m \le n\}$.

   Bestimmung von $|Z_{m,n}|$

   Definition: $\Phi : Z_{m,n} \to \mathcal{P}_m(\{2, \ldots, n+m\})$, $\Phi(k_1, \ldots, k_m) = \{k_i + i : i = 1, ..., m\}$.

   Φ ist bijektiv, folglich $|Z_{m,n}| = |\mathcal{P}_m(\{2, \ldots, n+m\})| = \binom{n+m-1}{m}$.

   Beweis von "Φ surjektiv": Sei $X \in \mathcal{P}_m(\{2, \ldots, n+m\})$.
   Dann existiert $k'_1 < \ldots < k'_m$ mit $X = \{k'_1, ..., k'_m\}$.
   Sei $k_i := k'_i - i$. Dann $1 \le k_1 \le \ldots \le k_m \le n$ und $\Phi(k_1, ..., k_m) = X$.

   Beweis von "Φ injektiv": Seien $(k_1, ..., k_m) \neq (l_1, ..., l_m)$ Elemente von $Z_{m,n}$.
   Dann existiert ein $j \in \{1, ..., m\}$ mit $k_j \neq l_j$ und $k_i = l_i$ für $1 \le i < j$. O.E.d.A. $k_j < l_j$.
   Es folgt $k_j + j \in \Phi(k_1, ..., k_m) \setminus \Phi(l_1, ..., l_m)$ und somit $\Phi(k_1, ..., k_m) \neq \Phi(l_1, ..., l_m)$.

§3 Teilbarkeit in $\mathbb{Z}$

Vereinbarung.

Die Buchstaben $a, b, c, d, q, p, x, y, z$ bezeichnen im folgenden stets ganze Zahlen (d.h. Elemente von $\mathbb{Z}$).

$|x|$ bezeichnet den *Absolutbetrag* von x. $\quad \mathbb{N}_1 := \{n \in \mathbb{N} : 1 \leq n\}$.

Definition. $b|a \ :\Leftrightarrow \ \exists x \in \mathbb{Z}(xb = a)$ (b teilt a, b ist Teiler von a)

Folgerungen.

(a) $c|b \ \& \ b|a \ \Rightarrow \ c|a$

(b) $c|a \ \& \ c|b \ \Rightarrow \ c|xa + yb$

(c) $c \neq 0 \ \Rightarrow \ (b|a \ \Leftrightarrow \ bc|ac)$

(d) $b|a \ \Leftrightarrow \ -b|a \ \Leftrightarrow \ b|-a$

(e) $a|0$ und $1|a$

(f) $(0|a \Leftrightarrow a = 0)$ und $(a|1 \Leftrightarrow a \in \{-1, 1\})$

(g) $b|a \ \& \ 1 \leq a \ \Rightarrow \ b \leq a$

(h) $b|a \ \ \& \ \ a \neq 0 \ \Rightarrow \ 1 \leq |b| \leq |a|$

(i) $b|a \ \& \ a|b \ \Rightarrow \ |a| = |b|$

(j) $\forall k \geq 1(k|a \Leftrightarrow k|b) \ \Rightarrow \ |a| = |b|$

Definition

Eine Teilmenge $\mathfrak{a}$ von $\mathbb{Z}$ heißt *Ideal* in $\mathbb{Z}$, wenn gilt:

(i) $\quad 0 \in \mathfrak{a}$

(ii) $\quad a, b \in \mathfrak{a} \Rightarrow a + b \in \mathfrak{a}$

(iii) $\quad x \in \mathbb{Z} \ \& \ a \in \mathfrak{a} \Rightarrow xa \in \mathfrak{a}$

z.B. sind $\{0\}$ und $\mathbb{Z}$ Ideale, ebenso $\mathbb{Z}a := \{xa : x \in \mathbb{Z}\}$ (für $a \in \mathbb{Z}$),

allgemeiner $\mathbb{Z}a_1 + \cdots + \mathbb{Z}a_n := \{\sum_{i=1}^{n} x_i a_i : x_1, ..., x_n \in \mathbb{Z}\}$ (für $a_1, ..., a_n \in \mathbb{Z}$).

Bemerkung. $\quad b|a \ \Leftrightarrow \ a \in \mathbb{Z}b \ \Leftrightarrow \ \mathbb{Z}a \subseteq \mathbb{Z}b.$

3.1 Satz ($\mathbb{Z}$ ist Hauptidealring).

Zu jedem Ideal $\mathfrak{a}$ von $\mathbb{Z}$ gibt es genau ein $a \in \mathbb{N}$ mit $\mathfrak{a} = \mathbb{Z}a$.

Beweis:

Für $\mathfrak{a} = \{0\}$ ist die Behauptung trivial ($a = 0$). Sei jetzt $\mathfrak{a} \neq \{0\}$.

Existenz: Die Menge $\mathbb{N}_1 \cap \mathfrak{a}$ ist nicht leer [$0 \neq b \in \mathfrak{a} \Rightarrow -b \in \mathfrak{a}$], hat also ein kleinstes Element a.

$\mathbb{Z}a \subseteq \mathfrak{a}$: trivial. $\quad \mathfrak{a} \subseteq \mathbb{Z}a$: $y \in \mathfrak{a} \ \& \ y = qa + r$ mit $0 \leq r < a \ \Rightarrow \ r \in \mathfrak{a} \ \Rightarrow \ r = 0 \ \Rightarrow \ y \in \mathbb{Z}a$.

Eindeutigkeit: Ist auch $\mathfrak{a} = \mathbb{Z}a'$ mit $a' \in \mathbb{N}_0$, so folgt $a|a' \ \& \ a'|a$, also $a = a'$.

Definition (größter gemeinsamer Teiler). Für $a_1, ..., a_n \in \mathbb{Z}$ $(n \geq 1)$ sei

$T(a_1, ..., a_n) := \{b \in \mathbb{Z} : b|a_1 \ \& \ ... \ \& \ b|a_n\}$

$$\mathsf{ggT}(a_1, ..., a_n) := \begin{cases} \max T(a_1, ..., a_n) & \text{falls } \exists i(a_i \neq 0) \\ 0 & \text{sonst} \end{cases}$$

Bemerkung. $T(a_1, ..., a_n) = T(b_1, ..., b_m) \ \Rightarrow \ \mathsf{ggT}(a_1, ..., a_n) = \mathsf{ggT}(b_1, ..., b_m)$.

3.2 Lemma.

(a) $a_1, ..., a_n \in \mathbb{Z}a \;\Leftrightarrow\; a \in T(a_1, ..., a_n)$.

(b) $a \in \mathbb{Z}a_1 + ... + \mathbb{Z}a_n \;\Rightarrow\; T(a_1, ..., a_n) \subseteq T(a)$.

(c) $a \in T(a_1, ..., a_n) \;\Rightarrow\; T(a) \subseteq T(a_1, ..., a_n)$.

(d) $\mathbb{Z}a = \mathbb{Z}a_1 + \ldots + \mathbb{Z}a_n \;\Rightarrow\; T(a_1, ..., a_n) = T(a)$.

Beweis :

(a) klar

(b) $a = x_1a_1 + ... + x_na_n$ & $b|a_1$ & ... & $b|a_n \;\Rightarrow\; b|a$.

(c) $a|a_i$ & $b|a \;\Rightarrow\; b|a_i$.

(d) $\mathbb{Z}a = \mathbb{Z}a_1 + \ldots + \mathbb{Z}a_n \;\Rightarrow\; a_1, ..., a_n \in \mathbb{Z}a$ & $a \in \mathbb{Z}a_1 + ... + \mathbb{Z}a_n \overset{(a),(b)}{\Rightarrow}$
$\Rightarrow\; a \in T(a_1, ..., a_n)$ & $T(a_1, ..., a_n) \subseteq T(a) \overset{(c)}{\Rightarrow} T(a_1, ..., a_n) = T(a)$.

3.3 Lemma. (Darstellung von ggT).

Für $a_1, ..., a_n \in \mathbb{Z}$ und $d \in \mathbb{N}$ sind äquivalent:

(i) $d = \mathsf{ggT}(a_1, ..., a_n)$

(ii) $d \in T(a_1, ..., a_n)$ & $d \in \mathbb{Z}a_1 + ... + \mathbb{Z}a_n$

(iii) $\mathbb{Z}d = \mathbb{Z}a_1 + \ldots + \mathbb{Z}a_n$

(iv) $T(d) = T(a_1, ..., a_n)$

Beweis:

Nach Satz 3.1 gibt es ein $a \in \mathbb{N}$ mit $\mathbb{Z}a_1 + \cdots + \mathbb{Z}a_n = \mathbb{Z}a$. Für dieses gilt: $(*)$ $a = \mathsf{ggT}(a_1, ..., a_n)$.

Beweis von $(*)$: Im Fall $a = 0$ ist die Beh. klar. Sei jetzt $a > 0$. Dann: $a_1, ..., a_n \in \mathbb{Z}a \;\Rightarrow\; a \in T(a_1, ..., a_n)$;
$a \in \mathbb{Z}a_1 + ... + \mathbb{Z}a_n \overset{\text{L.3.2b}}{\Rightarrow} \forall b \in T(a_1, ..., a_n)(\, b|a\,) \;\Rightarrow\; \forall b \in T(a_1, ..., a_n)(b \leq a)$.

Das Lemma ergibt sich nun wie folgt:
(i) $\overset{(*)}{\Rightarrow} d \in T(a_1, ..., a_n)$ & $d = a \;\Rightarrow$ (ii) $\overset{\text{L.3.2a}}{\Rightarrow}\; a_1, ..., a_n \in \mathbb{Z}d$ & $d \in \mathbb{Z}a_1 + ... + \mathbb{Z}a_n \;\Rightarrow$ (iii) $\overset{\text{L.3.2d}}{\Rightarrow}$ (iv) $\Rightarrow$ (i).

3.4 Lemma. Aus $a = qb + c$ folgt $T(a, b) = T(b, c)$ und weiter $\mathsf{ggT}(a, b) = \mathsf{ggT}(b, c)$.

Beweis: $d \in T(b, c)$ & $a = qb + c \Rightarrow d|a$. $d \in T(a, b)$ & $c = a - qb \;\Rightarrow\; d|c$.

Euklidischer Algorithmus zur Bestimmung des ggT

Seien $r_0, r_1 \in \mathbb{N} \setminus \{0\}$ gegeben.

(i) Man berechnet $k, q_0, ..., q_{k-1}, r_2, ..., r_{k+1} \in \mathbb{N}$, so daß
$r_1 > r_2 > \ldots > r_{k+1} = 0$ und $(*_n)$ $r_n = q_n \cdot r_{n+1} + r_{n+2}$ für $n = 0, \ldots, k-1$.

(ii) Dann ist $\mathsf{ggT}(r_0, r_1) = r_k$, und durch Elimination von $r_2, ..., r_{k-1}$ aus den Gleichungen $(*_0), \ldots, (*_{k-2})$ erhält man eine Linearkombination $r_k = x \cdot r_0 + y \cdot r_1$.

Beweis:

1. Aus $(*_0), \ldots, (*_{k-1})$ folgt mit 3.4: $\mathsf{ggT}(r_0, r_1) = \mathsf{ggT}(r_1, r_2) = \ldots = \mathsf{ggT}(r_{k-1}, r_k) = \mathsf{ggT}(r_k, 0) = r_k$.

2. Durch Induktion nach $k-n$ zeigt man $\exists x,y(r_k = xr_n + yr_{n+1})$:

2.1. Aus $(*_{k-2})$ folgt $r_k = r_{k-2} - q_{k-2}r_{k-1}$.

2.2. $r_k = x{\cdot}r_{n+1} + y{\cdot}r_{n+2} \overset{(*)_n}{\Rightarrow} r_k = x{\cdot}r_{n+1} + y{\cdot}(r_n - q_n r_{n+1}) = y{\cdot}r_n + (x - yq_n){\cdot}r_{n+1}$.

Beispiel: $r_0 = 111$, $r_1 = 39$.

$$\begin{array}{rrl} & r_n = q_n{\cdot}r_{n+1} & + r_{n+2} \\ r_0 = 111 = & 2 \cdot 39 & + 33 \\ r_1 = & 39 = 1 \cdot 33 & + 6 \\ r_2 = & 33 = 5 \cdot 6 & + 3 \\ r_3 = & 6 = 2 \cdot 3 & + 0 \\ & r_4 & r_5 \end{array}$$

$\mathsf{ggT}(111,39) = 3 =$

$1 \cdot \mathbf{33} + (-5) \cdot \mathbf{6} = 1 \cdot 33 + (-5)(39 - 1{\cdot}33) =$

$(-5) \cdot \mathbf{39} + 6 \cdot \mathbf{33} = (-5) \cdot 39 + 6(111 - 2{\cdot}39) =$

$6 \cdot \mathbf{111} + (-17) \cdot \mathbf{39}$

Bemerkung. $\mathsf{ggT}(a_1,...,a_n) = \mathsf{ggT}(\mathsf{ggT}(a_1,...,a_{n-1}),a_n)$ $(n \geq 2)$.

Beweis:

Sei $d := \mathsf{ggT}(a_1,...,a_{n-1})$. Dann $T(a_1,...,a_n) = T(a_1,...,a_{n-1}) \cap T(a_n) \overset{\text{L.3.3}}{=} T(d) \cap T(a_n) = T(d,a_n)$.

Bemerkung. Aus Lemma 3.3 folgt: $\mathsf{ggT}(a_1,...,a_n) = 1 \Leftrightarrow 1 \in \mathbb{Z}a_1 + ... + \mathbb{Z}a_n$.

Definition

$a_1,...,a_n$ heißen *teilerfremd (relativ prim)*, wenn $\mathsf{ggT}(a_1,...,a_n) = 1$.

$a_1,...,a_n$ heißen *paarweise teilerfremd*, wenn $\mathsf{ggT}(a_i,a_j) = 1$ für alle $i,j \in \{1,...,n\}$ mit $i \neq j$.

3.5 Lemma.

(a) $a|bc \;\&\; \mathsf{ggT}(a,b) = 1 \implies a|c$

(b) $\mathsf{ggT}(a_1,b) = \ldots = \mathsf{ggT}(a_n,b) = 1 \implies \mathsf{ggT}(a_1 \cdot ... \cdot a_n, b) = 1$.

(c) $a_1,...,a_n$ paarweise teilerfremd und $a_i|b$ für $i = 1,...,n \implies a_1 \cdot \ldots \cdot a_n|b$.

Beweis :

(a) $a|bc \;\&\; xa + yb = 1 \;\Rightarrow\; a|bc \;\&\; xac + ybc = c \;\Rightarrow\; a|c$.

(b) Induktion nach n: 1. $n = 1$: trivial.

2. Schritt: $\forall i \in \{1,...,n{+}1\}(\mathsf{ggT}(a_i,b) = 1) \;\Rightarrow\; \forall i \in \{1,...,n\}(\mathsf{ggT}(a_i,b) = 1) \;\&\; \mathsf{ggT}(a_{n+1},b) = 1 \overset{\text{IH}}{\Rightarrow}$

$\Rightarrow \mathsf{ggT}(a_1 \cdot \ldots \cdot a_n, b) = 1 \;\&\; \mathsf{ggT}(a_{n+1},b) = 1 \overset{(*)}{\Rightarrow} \mathsf{ggT}(a_1 \cdot \ldots \cdot a_{n+1}, b) = 1$.

$(*)$ $\mathsf{ggT}(a,b) = 1 \;\&\; \mathsf{ggT}(c,b) = 1 \;\Rightarrow\; \mathsf{ggT}(ac,b) = 1$.

Beweis: $xa + yb = 1 \;\&\; x'c + y'b = 1 \;\Rightarrow\; 1 = (xa + yb)(x'c + y'b) = xx' \cdot ac + (xay' + yx'c + yby') \cdot b$.

(c) Induktion nach n: 1. $n = 1$: trivial.

2. Schritt: Vorauss. $\overset{\text{IH \& (b)}}{\Rightarrow}$ $a_1 \cdot \ldots \cdot a_n|b \;\&\; a_{n+1}|b \;\&\; \mathsf{ggT}(a_1 \cdot \ldots \cdot a_n, a_{n+1}) = 1 \overset{(*)}{\Rightarrow} a_1 \cdot \ldots \cdot a_{n+1}|b$.

$(*)$ $a|b \;\&\; c|b \;\&\; \mathsf{ggT}(a,c) = 1 \;\Rightarrow\; ac|b$.

Beweis: $xa = b \;\&\; yc = b \;\&\; x'a + y'c = 1 \Rightarrow b = x'ab + y'cb = x'ayc + y'cxa = (x'y + y'x)ac$.

Definition

$\mathbb{P} := \{n \in \mathbb{N} : 2 \leq n \;\&\; \neg\exists m,k < n(n = mk)\}$ (Menge aller *Primzahlen*)

3.6 Lemma.

Für alle $a_0, ..., a_k \in \mathbb{Z}$ und $p \in \mathbb{P}$ gilt:

(a) $a \in \mathbb{N}\ \&\ a|p \implies a = 1$ oder $a = p$.

(b) $p|a_0 \cdot \ldots \cdot a_k \implies \exists i \leq k(p|a_i)$.

Beweis :

(a) Sei $a \in \mathbb{N}$ mit $a|p$. Dann $1 \leq a \leq p$ und es existiert $k \in \mathbb{N}$ mit $ka = p$. Wäre $1 < a < p$, so auch $k < p$ und p wäre keine Primzahl.

(b) Annahme: $p \nmid a_i$ für $i = 0, ..., k$. Nach (a) gilt dann $\mathsf{ggT}(a_i, p) = 1$ für $i = 0, ..., k$. Mit Lemma 3.5b folgt daraus $\mathsf{ggT}(a_0 \cdots a_k, p) = 1$, d.h. $p \nmid a_1 \cdots a_k$

Definition. Für $p \in \mathbb{P}$ und $a \in \mathbb{Z} \setminus \{0\}$ sei $v_p(a) := \max\{m \in \mathbb{N} : p^m | a\}$.

3.7 Lemma.

Ist $a = p_0^{n_0} \cdot \ldots \cdot p_k^{n_k}$ mit paarw. verschiedenen Primzahlen $p_0, ..., p_k$ und $n_0, ..., n_k \in \mathbb{N}$, so gilt für alle $p \in \mathbb{P}$:

$v_p(a) = \begin{cases} 0 & \text{falls } p \notin \{p_0, ..., p_k\} \\ n_i & \text{falls } p = p_i \in \{p_0, ..., p_k\} \end{cases}$.

Beweis :

(1) $p|a \Leftrightarrow \exists i \leq k(p = p_i\ \&\ n_i > 0)$

Beweis von "⇒": $p|a \overset{3.6b}{\Rightarrow} \exists i \leq k(\, p|p_i^{n_i}\,)$. $p|p_i^{n_i} \Rightarrow p \leq p_i^{n_i} \Rightarrow 0 < n_i$. $p|p_i^{n_i}\ \&\ n_i > 0 \overset{3.6b}{\Rightarrow} p|p_i \overset{3.6a}{\Rightarrow} p = p_i$.

(2) $i \in \{0, ..., k\} \Rightarrow v_{p_i}(a) = n_i$.

Beweis: o.E. $i = 0$. $p_0^{n_0}|a$: klar. $p_0^{n_0+1} \nmid a$: Annahme: $a = p_0^{n_0+1} \cdot c$. Dann $p_0^{n_0} \cdot p_1^{n_1} \cdots p_k^{n_k} = p_0^{n_0+1} \cdot c$ und somit $p_1^{n_1} \cdots p_k^{n_k} = p_0 \cdot c$. Mit (1) folgt $p_0 \in \{p_1, ..., p_k\}$. Widerspruch.

(3) $p \notin \{p_0, ..., p_k\} \overset{(1)}{\Rightarrow} p \nmid a \Rightarrow v_p(a) = 0$.

3.8 Lemma. Für alle $a, b \in \mathbb{N} \setminus \{0\}$ gilt:

(a) $a = b \iff \forall p \in \mathbb{P}(\, v_p(a) = v_p(b)\,)$.

(b) $\forall p \in \mathbb{P}(\, v_p(a \cdot b) = v_p(a) + v_p(b)\,)$.

(c) $a|b \iff \forall p \in \mathbb{P}(\, v_p(a) \leq v_p(b)\,)$.

(d) $\forall p \in \mathbb{P}(\, v_p(\mathsf{ggT}(a, b)) = \min\{v_p(a), v_p(b)\}\,)$.

Beweis :

Nach Satz 1.2 gibt es paarweise verschiedene Primzahlen $p_0, ..., p_k$, sowie $n_0, ..., n_k, m_0, ..., m_k \in \mathbb{N}$ mit $a = p_0^{n_0} \cdots p_k^{n_k}$ und $b = p_0^{m_0} \cdots p_k^{m_k}$. Nach 3.7 gilt dann $v_{p_i}(a) = n_i$ und $v_{p_i}(b) = m_i$ für $i = 1, ..., k$, sowie $v_p(a) = 0 = v_p(b)$ für $p \notin \{p_0, ..., p_k\}$.

(a) $\forall p \in \mathbb{P}(v_p(a) = v_p(b)) \Rightarrow n_i = v_{p_i}(a) = v_{p_i}(b) = m_i$ für $i = 1, ..., k \Rightarrow a = b$.

(b) $a \cdot b = p_0^{n_0+m_0} \cdots p_k^{n_k+m_k}$ und somit (nach 3.7) $v_{p_i}(a \cdot b) = n_i + m_i = v_{p_i}(a) + v_{p_i}(b)$ für $i = 1, ..., k$, sowie $v_p(a \cdot b) = 0 = v_p(a) + v_p(b)$ für $p \notin \{p_0, ..., p_k\}$.

(c) "⇒": $xa = b \overset{(b)}{\Rightarrow} v_p(a) \leq v_p(x) + v_p(a) = v_p(b)$.

"⇐" : Nach Voraussetzung gilt $n_i \leq m_i$ für $i = 0, ..., k$. Deshalb $c := p_0^{m_0-n_0} \cdot \ldots \cdot p_k^{m_k-n_k} \in \mathbb{N}$.

Es folgt $a \cdot c = p_0^{m_0} \cdot \ldots \cdot p_k^{m_k} = b$.

(d) Sei $c := p_0^{\min(n_0,m_0)} \cdot \ldots \cdot p_k^{\min(n_k,m_k)}$. Dann $v_p(c) = \min\{v_p(a), v_p(b)\}$ $(*)$
Es folgt: $d|a \;\&\; d|b \overset{(c)}{\Leftrightarrow} \forall p \in \mathbb{P}(v_p(d) \le v_p(a)) \;\&\; \forall p \in \mathbb{P}(v_p(d) \le v_p(b)) \Leftrightarrow$
$\Leftrightarrow \forall p \in \mathbb{P}(v_p(d) \le \min\{v_p(a), v_p(b)\}) \overset{(c)+(*)}{\Leftrightarrow} d|c$. Also $T(a,b) = T(c)$ und deshalb $c = \mathsf{ggT}(a,b)$.

Beispiel: $n = 360 = 2^3 \cdot 3^2 \cdot 5$, $m = 756 = 2^2 \cdot 3^3 \cdot 7 \Rightarrow \mathsf{ggT}(n,m) = 2^2 \cdot 3^2 = 36$.

3.9 Satz (Primzahlsatz von Euklid). Es gibt unendlich viele Primzahlen.

Beweis:

Für jedes $n \ge 2$ gibt es eine Primzahl p mit $n < p \le n!+1$, denn sind $p_0 < \ldots < p_k$ alle Primzahlen $\le n$ und ist p ein Primteiler von $p_0 \cdots p_k+1$, folgt $p \notin \{p_0, ..., p_k\}$, also $p > n$, und natürlich ist $p \le p_0 \cdots p_k+1 \le n!+1$.

Zusatz: Es gibt beliebig große Lücken in der Primzahlfolge, denn für jedes $n \ge 2$ kommt unter den Zahlen $n!+2$, $n!+3, \ldots, n!+n$ keine Primzahl vor [$n!+i$ hat den echten Teiler i].

§4 Restklassen

Definitionen.

Sind x_1, x_2 irgendwelche Objekte, so bezeichnet (x_1, x_2) das *(geordnete) Paar* mit *erster Komponente* x_1 und *zweiter Komponente* x_2. Für Paare $(x_1, x_2), (y_1, y_2)$ gilt: $(x_1, x_2) = (y_1, y_2) \Leftrightarrow x_1 = y_1 \;\&\; x_2 = y_2$.

Für Mengen X_1, X_2 bezeichnet $X_1 \times X_2$ die Menge aller geordneten Paare (x_1, x_2) mit $x_1 \in X_1$ und $x_2 \in X_2$, d.h.: $X_1 \times X_2 := \{(x_1, x_2) : x_1 \in X_1 \;\&\; x_2 \in X_2\}$ *(kartesisches Produkt).*

Eine *binäre* (oder *2-stellige*) *Relation* ist eine Menge von geordneten Paaren. Ist $R \subseteq M \times M$, so nennt man R eine binäre Relation auf M.

Schreibweise; Ist R eine binäre Relation, so schreibt man oft 'Rxy' (oder auch 'xRy') statt '$(x, y) \in R$'

Eine binäre Relation R auf der Menge M heißt

- *reflexiv*, wenn $\forall x \in M(xRx)$;
- *antireflexiv*, wenn $\forall x(\neg\, xRx)$;
- *symmetrisch*, wenn $\forall x, y(xRy \Rightarrow yRx)$;
- *transitiv*, wenn $\forall x, y, z(xRy \;\&\; yRz \Rightarrow xRz)$.

Eine Relation $R \subseteq X \times X$ heißt *Äquivalenzrelation auf* M, wenn sie reflexiv, symmetrisch und transitiv ist.

Ist R eine Äquivalenzrelation auf M, so sei

$[x]_R := \{y \in M : xRy\}$ $(\textit{Äquivalenzklasse von } x \in M)$,

$M/R := \{[x]_R : x \in M\}$.

4.1 Lemma.

Ist R eine Äquivalenzrelation auf der Menge M, so gilt:

(a) $x \in [x]_R$ $(\forall x \in M)$,

(b) $xRx' \Leftrightarrow [x]_R = [x']_R \Leftrightarrow [x]_R \cap [x']_R \neq \emptyset$ $(\forall x, x' \in M)$,

(c) $M = \bigcup_{x \in M} [x]_R$.

Beweis:

(a) $x \in M \Rightarrow xRx \Rightarrow x \in [x]$.

(b) $xRx' \;\&\; y \in [x'] \Rightarrow xRx' \;\&\; x'Ry \Rightarrow xRy \Rightarrow y \in [x]$.

$xRx' \;\&\; y \in [x] \Rightarrow x'Rx \;\&\; xRy \Rightarrow x'Ry \Rightarrow y \in [x']$.

$[x] = [x'] \Rightarrow x \in [x] = [x] \cap [x']$.

$y \in [x] \cap [x'] \Rightarrow xRy \;\&\; x'Ry \Rightarrow xRy \;\&\; yRx' \Rightarrow xRx'$.

(c) folgt aus (a).

Vereinbarung. Im folgenden sei stets $m \geq 1$ und $p \in \mathbb{P}$.

Definitionen.

$a \equiv_m b \;:\Leftrightarrow\; a \equiv b \,\mathtt{mod}\, m \;:\Leftrightarrow\; m|a-b$ *(a und b sind kongruent modulo m)*

$\mathbf{r}_m(a) :=$ Rest von a bei Division durch m, [andere (übliche) Notation: $a \,\mathtt{mod}\, m$]

d.h. $\mathbf{r}_m(a) \in \{0, \ldots, m-1\}$ und $\exists q \in \mathbb{Z}(a = mq + \mathbf{r}_m(a))$.

$[a]_m := \{y \in \mathbb{Z} : a \equiv_m y\}$ *(Restklasse von a modulo m)*

$a + \mathbb{Z}m := \{a + x : x \in \mathbb{Z}m\}$.

4.2 Lemma.

(a) $\mathbf{r}_m(a) = \mathbf{r}_m(b) \;\Leftrightarrow\; a \equiv_m b$.

(b) $\equiv_m$ ist eine Äquivalenzrelation auf $\mathbb{Z}$.

(c) $a + \mathbb{Z}m = [a]_m$.

(d) $a + \mathbb{Z}m = b + \mathbb{Z}m \;\Leftrightarrow\; a \equiv_m b$.

Beweis:

(a) Sei $r := \mathbf{r}_m(a)$ und $r' := \mathbf{r}_m(b)$. Dann $a = mq + r$ und $b = mq' + r'$ mit $r, r' \in \{0, ..., m-1\}$.

"$\Rightarrow$": $r = r' \;\Rightarrow\; a - b = (mq + r) - (mq' + r) = m(q - q')$.

"$\Leftarrow$": $a \equiv_m b \Rightarrow m|a - b \Rightarrow m|m(q-q') + r - r' \Rightarrow m|r-r' \Rightarrow r-r' = 0$, denn $|r-r'| < m$.

(b) folgt aus (a).

(c) $y \in a + \mathbb{Z}m \Leftrightarrow \exists x \in \mathbb{Z}m(y = a + x) \Leftrightarrow \exists q(y = a + qm) \Leftrightarrow m|y - a \Leftrightarrow a \equiv_m y \Leftrightarrow y \in [a]_m$.

(d) folgt aus (b), (c) und 4.1b.

4.3 Lemma. (Regeln für das Rechnen modulo m)

(a) $a_i \equiv_m b_i$ für $i = 1, ..., n \implies \sum_{i=1}^n a_i \equiv_m \sum_{i=1}^n b_i$ und $\prod_{i=1}^n a_i \equiv_m \prod_{i=1}^n b_i$

(b) $a \equiv_m b \implies a^n \equiv_m b^n$.

(c) $m_1, ..., m_k$ paarweise teilerfremd und $a \equiv b \,\mathtt{mod}\, m_j$ für $j = 1, ..., k \implies a \equiv b \,\mathtt{mod}\, m_1 \cdots m_k$.

(d) $ac \equiv_m bc \;\&\; \mathtt{ggT}(m, c) = 1 \implies a \equiv_m b$.

Beweis :

(a) Es reicht, den Fall $l = 2$ zu betrachten: $m|b_i - a_i \;(i = 1, 2) \;\Rightarrow\; m|(b_1 - a_1) + (b_2 - a_2)$ &

$m|(b_1 - a_1)b_2 + a_1(b_2 - a_2) \;\Rightarrow\; m|(b_1 + b_2) - (a_1 + a_2)$ & $m|b_1 b_2 - a_1 a_2$.

(b) folgt aus (a).

(c) $m_j|b-a \,(\forall j) \overset{3.5c}{\Rightarrow} m_1 \cdot \ldots \cdot m_k|b-a$.

(d) $m|(a-b)c \;\&\; \mathtt{ggT}(m, c) = 1 \overset{3.5a}{\Rightarrow} m|a - b$.

Folgerung. Ist $n = \sum_{i=0}^{k} a_i 10^i$ mit $0 \le a_i < 10$ für alle i, so gilt:
$n \equiv a_0 + a_1 + \cdots + a_k \bmod 3$, $n \equiv a_0 + a_1 + \cdots + a_k \bmod 9$, $n \equiv a_0 - a_1 + a_2 \mp \cdots \bmod 11$.
d.h. n ist genau dann durch 3 (bzw. 9) teilbar, wenn die Summe der Ziffern durch 3 (bzw. 9) teilbar ist; n ist genau dann durch 11 teilbar, wenn die alternierende Summe der Ziffern durch 11 teilbar ist.

Beweis: Für alle $i \in \mathbb{N}$ ist $10^i \equiv 1 \bmod 3$, $10^i \equiv 1 \bmod 9$ und $10^i \equiv (-1)^i \bmod 11$.

Beispiel: Rest von 2^{16} bei Division durch 11: $2^4 = 16 \equiv_{11} 5 \Rightarrow 2^{16} \equiv (2^4)^4 \equiv 5^4 \equiv 25^2 \equiv 3^2 \equiv 9 \bmod 11$.

Definition. $\mathbb{Z}/\mathbb{Z}m := \{[a]_m : a \in \mathbb{Z}\}$ *(Menge aller Restklassen modulo m)*

4.4 Lemma.

(a) $\mathbb{Z}/\mathbb{Z}m = \{[0]_m, [1]_m, \ldots, [m-1]_m\}$ und $|\mathbb{Z}/\mathbb{Z}m| = m$.

(b) $\mathbb{Z}$ ist disjunkte Vereinigung von $[0]_m, \ldots, [m-1]_m$.

Beweis:

(a) Für alle $a \in \mathbb{Z}$ gilt $\mathbf{r}_m(a) \in \{0, \ldots, m-1\}$ und $m | a - \mathbf{r}_m(a)$, also $[a]_m = [\mathbf{r}_m(a)]_m$.

Außerdem $[i]_m \neq [j]_m$ für alle $i, j \in \{0, ..., m-1\}$ mit $i \neq j$.

(b) folgt aus 4.2d und 4.1c.

Definition $\varphi(m) := \big|\{a \in \{0, \ldots, m-1\} : \mathsf{ggT}(a, m) = 1\}\big|$ *(Euler-Funktion* oder *Eulersche φ-Funktion)*

4.5 Lemma. Für $p \in \mathbb{P}$ und $n \ge 1$ gilt $\varphi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1)$.

Beweis: Für alle $a \in \{0, \ldots, p^n - 1\}$ gilt:

$\mathsf{ggT}(a, p^n) \neq 1 \Leftrightarrow \exists b > 1 (b|a \,\&\, b|p^n) \overset{(*)}{\Leftrightarrow} p|a \Leftrightarrow \exists k (k \cdot p = a < p^n) \Leftrightarrow \exists k < p^n (k \cdot p = a)$.

Also $\big|\{a \in \{0, ..., p^n-1\} : \mathsf{ggT}(a, p^n) \neq 1\}\big| = \big|\{p \cdot k : k = 0, ..., p^{n-1}-1\}\big| = p^{n-1}$.

$(*)$ $1 < b \,\&\, b|p^n \Rightarrow p|b$. [Bew.: $1 < b \,\&\, b|p^n \Rightarrow (\exists q \in \mathbb{P})\, q|b \,\&\, b|p^n \Rightarrow q|p^n \Rightarrow q = p \Rightarrow p|b$]

4.6 Lemma.

(a) $\mathsf{ggT}(a, m) = 1 \iff \exists a' (aa' \equiv_m 1)$. (b) $a \equiv_m b \implies \mathsf{ggT}(a, m) = \mathsf{ggT}(b, m)$.

Beweis:

(a) $\mathsf{ggT}(a, m) = 1 \Leftrightarrow \exists a', q (aa' + qm = 1) \Leftrightarrow \exists a' (m | aa' - 1) \Leftrightarrow \exists a' (aa' \equiv_m 1)$.

(b) $m|a - b \Rightarrow \forall x (x|a \,\&\, x|m \Leftrightarrow x|b \,\&\, x|m) \Rightarrow \mathsf{ggT}(a, m) = \mathsf{ggT}(b, m)$.

Definition.

Die Restklassen $[x]_m$ mit $\mathsf{ggT}(x, m) = 1$ heißen *prime Restklassen modulo m*. (Def. sinnvoll wegen L.4.6b)
$(\mathbb{Z}/\mathbb{Z}m)^* := \{[x]_m : [x]_m$ ist prime Restklasse modulo $m\}$ heißt die *prime Restklassengruppe modulo m*.

Bemerkung. $\varphi(m) = \big|(\mathbb{Z}/\mathbb{Z}m)^*\big|$.

Definition.

$B \subseteq \mathbb{Z}$ heißt *primes Restsystem modulo m*, wenn B aus jeder primen Restklasse modulo m genau ein Element enthält, d.h. wenn B durch $b \mapsto [b]_m$ bijektiv auf $(\mathbb{Z}/\mathbb{Z}m)^*$ abgebildet wird, d.h. wenn $B = \{b_1, ..., b_{\varphi(m)}\}$ mit $\forall i (\, \mathsf{ggT}(b_i, m) = 1\,)$ und $\forall i, j (b_i \equiv_m b_j \Rightarrow i = j)$.

Beispiel. $\varphi(12) = 4$. $\{1, 5, 7, 11\}$ und $\{-5, -1, 13, 17\}$ sind prime Restsysteme modulo 12.

4.7 Lemma.

Ist $\{b_1, ..., b_{\varphi(m)}\}$ ein primes Restsystem modulo m und gilt $\mathtt{ggT}(a, m) = 1$,
so ist auch $\{ab_1, ..., ab_{\varphi(m)}\}$ ein primes Restsystem modulo m.

Beweis:

$\mathtt{ggT}(b_i, m) = 1$ & $\mathtt{ggT}(a, m) = 1 \overset{3.5b}{\Rightarrow} \mathtt{ggT}(ab_i, m) = 1$.

$ab_i \equiv_m ab_j$ & $\mathtt{ggT}(a, m) = 1 \overset{4.3d}{\Rightarrow} b_i \equiv_m b_j \Rightarrow i = j$.

4.8 Satz.

(a) (Euler) $\mathtt{ggT}(a, m) = 1 \implies a^{\varphi(m)} \equiv 1 \bmod m$

(b) (Fermat) $a^p \equiv a \bmod p$, insbesondere $a^{p-1} \equiv 1 \bmod p$ falls $p \not| a$

Beweis:

(a) Sei $\{b_1, ..., b_{\varphi(m)}\}$ primes Restsystem. Dann ist auch $\{ab_1, ..., ab_{\varphi(m)}\}$ primes Restsystem, also existiert eine Permutation π mit $ab_{\pi(i)} \equiv_m b_i$. Es folgt $a^{\varphi(m)} b_1 \cdots b_{\varphi(m)} = ab_{\pi(1)} \cdots ab_{\pi(\varphi(m))} \overset{4.3a}{\equiv_m} b_1 \cdots b_{\varphi(m)}$.
Aus $a^{\varphi(m)} b_1 \cdots b_{\varphi(m)} \equiv_m b_1 \cdots b_{\varphi(m)}$ und $\mathtt{ggT}(b_i, m) = 1$ für $i = 1, ..., \varphi(m)$ folgt (mit 4.3d) $a^{\varphi(m)} \equiv_m 1$.

(b) $p \not| a \Rightarrow \mathtt{ggT}(a, p) = 1 \overset{4.5 \text{ und (a)}}{\Rightarrow} a^{p-1} = a^{\varphi(p)} \equiv_p 1 \Rightarrow a^p \equiv_p a$. $p|a \Rightarrow p|a^p - a$.

4.9 Lemma.

Sei $\mathbb{Z}_m = \{0, \ldots, m-1\}$ mit $m = p \cdot q$, wobei p, q zwei verschiedene Primzahlen.
Wie unten gezeigt wird, ist dann $\varphi(m) = (p-1)\cdot(q-1)$.
Für $s \in \mathbb{N}$ sei $V_s : \mathbb{Z}_m \to \mathbb{Z}_m$, $V_s(n) := \mathbf{r}_m(n^s)$. Dann gilt für alle $s, t, n \in \mathbb{N}$ mit $st \equiv 1 \bmod \varphi(m)$:
(a) $(n^s)^t \equiv_m n$.
(b) $V_t(V_s(n)) = n$, falls $n \in \mathbb{Z}_m$.

Beweis:

(a) Da p und q verschiedene Primzahlen sind, genügt es (nach 4.3c), die Kongruenzen $(n^s)^t \equiv_p n$ und $(n^s)^t \equiv_q n$ zu beweisen. Aus Symmetriegründen können wir uns auf den Beweis für p beschränken. Im Fall $p|n$ ist die Behauptung offenbar richtig, denn wegen $st \equiv 1 \bmod \varphi(m)$ ist $st \geq 1$ und somit p auch Teiler von $(n^s)^t$. Sei also p kein Teiler von n. Nach 4.8b gilt dann $n^{p-1} \equiv 1 \bmod p$ $(*)$. Wegen $st \equiv 1 \bmod \varphi(m)$ existiert ein $x \in \mathbb{N}$ mit $st = 1 + x\cdot\varphi(m)$. Es folgt $(n^s)^t = n^{st} = n^{1+x(p-1)(q-1)} = n \cdot (n^{p-1})^{x(q-1)} \overset{(*)}{\equiv_p} n$.

(b) Sei $a := V_s(n)$. Dann $V_t(V_s(n)) = V_t(a) \overset{\text{Def}}{\equiv_m} a^t \equiv_m (n^s)^t \overset{\text{(a)}}{\equiv_m} n$, also $V_t(V_s(n)) = n$.

Anwendung: RSA-Verfahren. Eine Faktorisierung zufällig gewählter großer Zahlen läßt sich auch mit leistungsfähigen Großrechnern nicht in vernünftiger Zeit durchführen. Auf dieser praktischen Unmöglichkeit der Faktorisierung beruht eine gängige Verschlüsselungstechnik, nämlich das nach seinen Erfindern Ronald Rivest, Adi Shamir und Leonard Adleman benannte RSA-Verfahren. Dessen Grundidee besteht darin, daß die Verschlüsselung mit Hilfe eines sogenannten *öffentlichen Schlüssels* einfach durchzuführen ist, jedoch das Entschlüsseln nur bei Verwendung eines geheimen *privaten* Schlüssels in vernünftiger Zeit möglich ist.

Sei $m = p \cdot q$, wobei $p \neq q$ zwei (sehr große) Primzahlen. Man wählt ein $s < \varphi(m)$ mit $\mathtt{ggT}(\varphi(m), s) = 1$. Das Paar (m, s) nennt man den *öffentlichen Schlüssel*. Aus s und $\varphi(m)$ kann man mit Hilfe des Euklidischen Algorithmus eine Zahl t mit $st \equiv 1 \bmod \varphi(m)$ berechnen (*privater Schlüssel*). Die Verschlüsselung einer Nachricht $n \in \mathbb{Z}_m$ erfolgt durch Anwendung der Funktion V_s. Die verschlüsselte Nachricht $V_s(n)$ kann dann mit Hilfe des privaten Schlüssels t, d.h. der Funktion V_t, wieder entschlüsselt werden (L.4.9).

Beispiel. $p := 53$, $q := 61$, $m = 3233$, $\varphi(m) = 3120$. Wir wählen $s := 1013$ mit $\mathtt{ggT}(\varphi(m), s) = 1$ (s ist sogar eine Primzahl). Mit Hilfe des Euklid. Algorithmus erhalten wir $-25\varphi(m)+77s = 1$. Folglich können wir $t = 77$ als privaten Schlüssel nehmen. Die Nachricht $n = 10$ wird mittels $s = 1013$ zu $n' := \mathbf{r}_m(10^{1013}) = 2189$ verschlüsselt. Aus der verschlüsselten Nachricht n' erhält man mittels $t = 77$ wieder $n = \mathbf{r}_m(2189^{77}) = 10$.

4.10 Lemma.

Sei $m = m_1 \cdot \ldots \cdot m_k$ mit paarweise teilerfremden $m_1, ..., m_k$ ($k \geq 1$), und sei $q_i := \frac{m}{m_i} = \prod_{j \neq i} m_j$ ($i = 1, ..., k$). Dann gilt:

(a) Es gibt $y_1, ..., y_k$, so daß $q_i y_i \equiv 1 \bmod m_i$ für $i = 1, ..., k$.

(b) Ist $q_i y_i \equiv 1 \bmod m_i$ für $i = 1, ..., k$, so gilt für alle $a, b_1, ..., b_k \in \mathbb{Z}$:

$$a \equiv \sum_{i=1}^{k} b_i(q_i y_i) \bmod m \iff a \equiv b_i \bmod m_i \text{ für } i = 1, ..., k.$$

Beweis:

(a) $\mathtt{ggT}(m_i, m_j) = 1$ für $j \neq i \overset{3.5b}{\Rightarrow} \mathtt{ggT}(m_i, q_i) = 1 \overset{4.6a}{\Rightarrow} \exists y_i(q_i y_i \equiv 1 \bmod m_i)$.

(b) Sei $a_0 := \sum_{i=1}^{k} b_i(q_i y_i)$. Wegen $q_i y_i \equiv 1 \bmod m_i$ und $q_j \equiv 0 \bmod m_i$ für $j \neq i$ gilt dann $a_0 \equiv \sum_{j=1}^{k} b_j q_j y_j \equiv b_i q_i y_i \equiv b_i \bmod m_i$, und es folgt: $a \equiv a_0 \bmod m \overset{L.4.3c}{\Leftrightarrow} \forall i(a \equiv a_0 \bmod m_i) \Leftrightarrow \forall i(a \equiv b_i \bmod m_i)$.

Bemerkung.

Mit Hilfe von Lemma 4.10 kann man sogenannte *simultane Kongruenzen*

$$x \equiv b_i \bmod m_i \ (i = 1, ..., k,\ m_1, ..., m_k \text{ paarweise teilerfremd})$$

lösen. Seien z.B. $m_1 = 3$, $m_2 = 7$, $m_3 = 11$. Dann ist $m = m_1 m_2 m_3 = 231$ und $q_1 = m_2 m_3 = 77$, $q_2 = m_1 m_3 = 33$, $q_3 = m_1 m_2 = 21$. Wir bestimmen y_i, so daß $1 \equiv q_i y_i \bmod m_i$:
$y_1 := 2$ [denn $1 \equiv 77 \cdot 2 \bmod 3$], $y_2 := 3$ [denn $1 \equiv 33 \cdot 3 \bmod 7$], $y_3 := -1$ [denn $1 \equiv 21 \cdot (-1) \bmod 11$].

Daraus ergibt sich $q_1 y_1 = 154$, $q_2 y_2 = 99$, $q_3 y_3 = -21$.

Eine Lösung etwa der simultanen Kongruenzen $x \equiv 1 \bmod 3$, $x \equiv 2 \bmod 7$, $x \equiv 6 \bmod 11$ erhält man nach Lemma 4.10 durch $\sum_{i=1}^{3} b_i q_i y_i = 1 \cdot 154 + 2 \cdot 99 + 6 \cdot (-21) = 154 + 198 - 126 = 154 + 72 = 226$.

Beispiel (Berechnung von $97^{23} \bmod 1001$)

$1001 = 7 \cdot 11 \cdot 13$,

$97^{23} \equiv (-1)^{23} \equiv -1 \equiv 6 \bmod 7$,

$97^{23} \equiv (-2)^{23} \equiv -2^{20} \cdot 2^3 \equiv -8 \equiv 3 \bmod 11$ [denn $2^{10} \equiv 1 \bmod 11$ (L.4.8b)]

$97^{23} \equiv 6^{23} \equiv 11 \bmod 13$ [denn $6^{12} \equiv 1 \bmod 13$ (L.4.8b) und $6^{11} \equiv 11 \bmod 13$]

Außerdem gilt: $11 \cdot 13 = 143$, $143 \cdot 5 \equiv 1 \bmod 7$, $7 \cdot 13 = 91$, $91 \cdot 4 \equiv 1 \bmod 11$, $7 \cdot 11 = 77$, $77 \cdot 12 \equiv 1 \bmod 13$.

Mit Lemma 4.10b folgt daraus $97^{23} \equiv 6 \cdot 143 \cdot 5 + 3 \cdot 91 \cdot 4 + 11 \cdot 77 \cdot 12 = 15546 \equiv 531 \bmod 1001$.

4.11 Satz.

Ist $m = m_1 \cdot \ldots \cdot m_k$ mit paarweise teilerfremden $m_1, ..., m_k$, so wird durch $\psi([x]_m) := ([x]_{m_1}, \ldots, [x]_{m_k})$ eine bijektive Abbildung $\psi : \mathbb{Z}/\mathbb{Z}m \to \mathbb{Z}/\mathbb{Z}m_1 \times \ldots \times \mathbb{Z}/\mathbb{Z}m_k$ definiert.

Ferner gilt: $\psi((\mathbb{Z}/\mathbb{Z}m)^*) = (\mathbb{Z}/\mathbb{Z}m_1)^* \times \ldots \times (\mathbb{Z}/\mathbb{Z}m_k)^*$.

Beweis:

Der erste Teil der Behauptung folgt schon aus Lemma 4.10. Wir beweisen das hier aber nochmal direkt.

1. ψ wohldefiniert: $[x]_m = [x']_m \Rightarrow x \equiv_m x' \overset{m_i|m}{\Rightarrow} x \equiv_{m_i} x' \,(\forall i) \Rightarrow ([x]_{m_1}, ..., [x]_{m_k}) = ([x']_{m_1}, ..., [x']_{m_k})$.
2. ψ injektiv: $([x]_{m_1}, ..., [x]_{m_k}) = ([x']_{m_1}, ..., [x']_{m_k}) \Rightarrow x \equiv_{m_i} x' \,(\forall i) \overset{3.5c}{\Rightarrow} x \equiv_m x' \Rightarrow [x]_m = [x']_m$.
3. $|\mathbb{Z}/\mathbb{Z}m| = m = |\mathbb{Z}/\mathbb{Z}m_1| \cdot \ldots \cdot |\mathbb{Z}/\mathbb{Z}m_k| = |\mathbb{Z}/\mathbb{Z}m_1 \times \ldots \times \mathbb{Z}/\mathbb{Z}m_k|$ & ψ injektiv $\overset{\text{L.2,5b}}{\Rightarrow}$ ψ surjektiv.
4. $\psi((\mathbb{Z}/\mathbb{Z}m)^*) = (\mathbb{Z}/\mathbb{Z}m_1)^* \times \ldots \times (\mathbb{Z}/\mathbb{Z}m_k)^*$ gilt wegen:
$[x]_m \in (\mathbb{Z}/\mathbb{Z}m)^* \iff \mathsf{ggT}(x, m) = 1 \overset{3.5b}{\iff} \mathsf{ggT}(x, m_i) = 1 \,(\forall i) \iff [x]_{m_i} \in (\mathbb{Z}/\mathbb{Z}m_i)^* \,(\forall i)$.

Korollar 1 (Die Euler-Funktion ist multiplikativ).
$\varphi(m_1 \cdot \ldots \cdot m_k) = \varphi(m_1) \cdot \ldots \cdot \varphi(m_k)$, falls $m_1, \ldots, m_k$ paarweise teilerfremd.

Beweis:
$\varphi(m) = |(\mathbb{Z}/\mathbb{Z}m)^*| \overset{4.11}{=} |(\mathbb{Z}/\mathbb{Z}m_1)^*| \cdot \ldots \cdot |(\mathbb{Z}/\mathbb{Z}m_k)^*| = \varphi(m_1) \cdot \ldots \cdot \varphi(m_k)$.

Korollar 2 (Chinesischer Restsatz).
Ist $m = m_1 \cdot \ldots \cdot m_k$ mit paarweise teilerfremden $m_1, ..., m_k$, so gilt für alle $b_1, ..., b_k \in \mathbb{Z}$:

Das System von Kongruenzen $x \equiv b_i \bmod m_i \;\; (i = 1, ..., k)$ besitzt eine modulo m eindeutig bestimmte Lösung a. Mit anderen Worten, es gibt genau eine Restklasse $[a]_m$, so daß $a \equiv b_i \bmod m_i$ für $i = 1, ..., k$.

Beweis:
Seien $b_1, ..., b_k \in \mathbb{Z}$ und sei ψ wie 4.11. Dann $([b_1]_{m_1}, \ldots, [b_k]_{m_k}) \in \mathbb{Z}/\mathbb{Z}m_1 \times \ldots \times \mathbb{Z}/\mathbb{Z}m_k$; nach 4.11 existiert also genau ein $[a]_m \in \mathbb{Z}/\mathbb{Z}m$ mit $\psi([a]_m) = ([b_1]_{m_1}, \ldots, [b_k]_{m_k})$, d.h. mit $[a]_{m_i} = [b_i]_{m_i}$ für $i = 1, ..., k$.