1. Die ganzen Zahlen

1.1 Def $b \in \mathbb{Z}$ heißt Teiler von $a \in \mathbb{Z}$, falls $\exists\, c \in \mathbb{Z}$: $bc = a$. Wir schreiben $b \mid a$, b teilt a.

1.2 Satz (Division mit Rest) Seien $a, b \in \mathbb{Z}$, $b \neq 0$, dann $\exists!\, q, r \in \mathbb{Z}$ mit

$a = qb + r$, $0 \leq r < b$.

r nennen wir Rest.

Beweis: OE $b > 0$. Die Menge $\{w \in \mathbb{Z} \mid a < bw\}$ hat ein minimales Element $q+1$. Es gilt $qb \leq a < (q+1)b$ und für $r = a - qb$ gilt

$$0 \leq a - qb < (q+1)b - qb = b.$$

Eindeutigkeit:

Sei $a = q_1 b + r_1 = q_2 b + r_2$

OE $r_2 \geq r_1$. Dann ist

$$0 \leq r_2 - r_1 = a - q_2 b - (a - q_1 b)$$

$$= (q_1 - q_2) b \Rightarrow b \mid r_2 - r_1$$

Aber $0 \leq r_2 - r_1 < b \Rightarrow$

$0 = r_2 - r_1 \Rightarrow r_2 = r_1 \Rightarrow q_2 = q_1$

$\square$

1.3 Def (Kongruenz)

$a \equiv b \mod m$

a ist kongruent zu b modulo m

$:\Leftrightarrow m \mid a - b$

$\Leftrightarrow$ a und b haben bei Division durch m denselben Rest.

1.4 Def Seien $a, b \in \mathbb{Z} \setminus \{0\}$. Wir nennen $d \in \mathbb{N} \setminus \{0\}$ den größten gemeinsamen Teiler von a und b, $ggT(a,b)$, wenn

1) $d | a$, $d | b$
2) $\forall c \in \mathbb{Z}: c | a$ und $c | b \Rightarrow c | d$.

1.5 Bemerkung: Es gibt höchstens einen $ggT(a,b)$: Angenommen, d, d' erfüllen beide 1), 2) aus 1.4. Wende 2) auf d an, so folgt $d | d'$, genauso $d' | d \Rightarrow \exists c: c \cdot d = d'$, $\exists c': c' \cdot d' = d \Rightarrow c \cdot c' \cdot d' = d'$ $\Rightarrow c \cdot c' = 1$. Da $c, c' \in \mathbb{Z} \Rightarrow$ $c, c' \in \{1, -1\}$, da $d, d' > 0 \Rightarrow$ $c = c' = 1 \Rightarrow d = d'$.

Gibt es einen ggT? Ja, Beweis konstruktiv:

1.6 Euklidischer Algorithmus:

Da $ggT(a,b) = ggT(-a,b) = ggT(-a,-b)$ können wir OE (ohne Einschränkung, o.B.d.A ohne Beschränkung der Allgemeinheit) annehmen, daß $0 < b < a$.

1. Schritt: $a_1 := a$, $b_1 := b$

2. Schritt: Berechne eine Division mit Rest $a_1 = q_1 b_1 + r_1$

Wenn $r_1 = 0$ dann ist $ggT(a,b) = b_1$, stop.

Sonst setze $a_2 := b_1$, $b_2 := r_1$ und wiederhole Schritt 2 mit diesen.

Beweis:

Terminierung: Der Algorithmus liefert bei jedem Durchlauf von Schritt 2 eine Zahl r_i mit $0 \leq r_i = b_{i+1} < b_i$. In jedem Schritt wird b echt kleiner, das geht nur endlich oft und endet nach endlich vielen Schritten mit $r_n = 0$.

Korrektheit: Sei N die Anzahl der Durchläufe von Schritt 2.

Induktion nach N.

IA: Falls $N=1$ gilt $a = a_1 = q_1 b_1 + r_1$
mit $r_1 = 0$, also $a = q_1 \cdot b$, also
$b \mid a$. Damit $b \mid a$, $b \mid b$ und $\forall c$
mit $c \mid a$, $c \mid b$ gilt $c \mid b$ $\Rightarrow$
$b = ggT(a,b)$.

IV: Wenn der Algorithmus nach N Schritten endet, liefert er den ggT der Anfangszahlen.

IS: Wir zeigen: auch wenn er nach $N+1$ Schritten stoppt, liefert er den ggT der Anfangszahlen.
Sei (a_1, b_1) ein Zahlenpaar, für das er nach $N+1$ Schritten stoppt.
Dann stoppt er für (a_2, b_2) bereits nach N Schritten, nach IV gilt also
$b_{N+1} = ggT(a_2, b_2) =: d$.
Das erste Durchlaufen liefert
$a_1 = q_1 b_1 + b_2$ und $a_2 = b_1$.
Da $d \mid a_2$, $d \mid b_2 \Rightarrow d \mid b_1$ und
$d \mid q_1 b_1 + b_2$, also $d \mid a_1$.
Sei $c \in \mathbb{Z}$ mit $c \mid a_1$, $c \mid b_1$
$\Rightarrow c \mid a_2$ und $c \mid a_1 - q_1 b_1$
$\Rightarrow c \mid a_2$ und $c \mid b_2 \Rightarrow c \mid d$ $\square$

Bsp $a = 104$, $b = 47$

i	(a_i, b_i)	$a_i - q_i b_i = b_{i+1}$
1	$(104, 47)$	$104 - 2 \cdot 47 = 10$
2	$(47, 10)$	$47 - 4 \cdot 10 = 7$
3	$(10, 7)$	$10 - 1 \cdot 7 = 3$
4	$(7, 3)$	$7 - 2 \cdot 3 = 1$
5	$(3, 1)$	$3 - 3 \cdot 1 = 0$

$\Rightarrow \operatorname{ggT}(104, 47) = 1.$

Rückwärtseinsetzen liefert noch mehr:

$$1 = 7 - 2 \cdot 3 = 7 - 2 \cdot (10 - 1 \cdot 7) =$$
$$3 \cdot 7 - 2 \cdot 10 = 3 \cdot (47 - 4 \cdot 10) - 2 \cdot 10 =$$
$$3 \cdot 47 - 14 \cdot 10 = 3 \cdot 47 - 14 \cdot (104 - 2 \cdot 47)$$
$$= (-14) \cdot 104 + 31 \cdot 47.$$

1.7 Satz Seien $a, b \in \mathbb{Z} \setminus \{0\}$, $d \in \mathbb{N}$

$d = \operatorname{ggT}(a, b) \Leftrightarrow$

1) $\exists\, r, s \in \mathbb{Z}$ mit $d = ra + sb$
2) Jede ganze Zahl der Form $ra + sb$ ist durch d teilbar.

"Bézout-Gleichung"

Beweis:

„$\Rightarrow$" 1) euklidischer Algorithmus mit Rückwärtseinsetzen

2) klar

„$\Leftarrow$" Sei $d' = ra + sb$ eine Zahl, die 1) + 2) erfüllt, sei $d = ggT(a,b)$.
Wegen „$\Rightarrow$" $\exists\ r', s' \in \mathbb{Z}$ mit $d = r'a + s'b$ und d erfüllt 2).
Da $d' = ra + sb$ folgt mit 2) für d: $d \mid d'$. Weil $d = r'a + s'b$ und d' n.V. 2) erfüllt, folgt $d' \mid d$.
Damit gilt $d = d'$. $\square$

1.8 Satz (Chinesischer Restsatz)

Seien $n_1, \dots, n_r \in \mathbb{N}_{>0}$ paarweise teilerfremd (i.e. $ggT(n_i, n_j) = 1$ $\forall\ i \neq j$), $a_1, \dots, a_r \in \mathbb{Z}$, dann ist das Kongruenzgleichungssystem

$$\begin{aligned} X &\equiv a_1 \mod n_1 \\ &\ \vdots \\ X &\equiv a_r \mod n_r \end{aligned}$$

lösbar. Die Lösung ist eindeutig mod $n := n_1 \cdot \ldots \cdot n_r$.

<u>Beweis</u>: Setze $\hat{n}_i = \frac{n}{n_i}$ und schreibe mit dem euklidischen Algorithmus und Rückwärtseinsetzen
$1 = ggT(n_i, \hat{n}_i) = x_i n_i + y_i \hat{n}_i$.

Dann ist $y_i \hat{n}_i \equiv 0 \mod n_j \ \forall j \neq i$

$y_i \hat{n}_i \equiv 1 \mod n_i$

Setze $x = \sum_{i=1}^{r} a_i y_i \hat{n}_i$, dann gilt

$x \equiv a_i \mod n_i \quad \forall i.$

Zahlen der Form $x + kn$ mit $k \in \mathbb{Z}$ lösen das Kongruenzgleichungssystem ebenso.
Sind x, x' Lösungen, dann gilt

$n_i \mid (x-x') \ \forall i \Rightarrow$

$n \mid (x-x') \Rightarrow$ die Lösung

ist eindeutig mod n. $\square$

<u>Bsp</u> Löse
$$x \equiv 1 \mod 5$$
$$x \equiv 3 \mod 6$$
$$x \equiv -2 \mod 7$$

$n = 5 \cdot 6 \cdot 7 = 210$

$\hat{n}_1 = 6 \cdot 7 = 42$

$\hat{n}_2 = 5 \cdot 7 = 35$

$\hat{n}_3 = 5 \cdot 6 = 30$

ggT$(5,42)$: $42 = 8 \cdot 5 + 2$

$5 = 2 \cdot 2 + 1$

$\Rightarrow 1 = 5 - 2 \cdot 2 = 5 - 2 \cdot (42 - 8 \cdot 5)$

$= (-2) \cdot 42 + 17 \cdot 5$

ggT$(6,35)$: $35 = 5 \cdot 6 + 5$

$6 = 1 \cdot 5 + 1$

$\Rightarrow 1 = 6 - 5 = 6 - (35 - 5 \cdot 6)$

$= (-1) \cdot 35 + 6 \cdot 6$

ggT(7, 30): $30 = 4 \cdot 7 + 2$
$7 = 3 \cdot 2 + 1$

$$\Rightarrow 1 = 7 - 3 \cdot 2 = 7 - 3 \cdot (30 - 4 \cdot 7)$$
$$= (-3) \cdot 30 + 13 \cdot 7$$

Setze

$$x = 1 \cdot (-2) \cdot 42 + 3 \cdot (-1) \cdot 35 + (-2) \cdot (-3) \cdot 30$$
$$= -9$$

$-9 \equiv 1 \mod 5$, $-9 \equiv 3 \mod 6$, $-9 \equiv -2 \mod 7$

Die kleinste positive Lösung ist

$-9 + 210 = 201$.

$201 \equiv 1 \mod 5$,
$201 \equiv 3 \mod 6$, denn $198 = 33 \cdot 6$
$201 \equiv -2 \mod 7$, denn $203 = 29 \cdot 7$.

Den chinesischen Restsatz werden wir noch verallgemeinern.

<u>1.9 Def</u> Seien $a, b \in \mathbb{Z}$.

$m \in \mathbb{Z}$ heißt <u>kleinstes gemeinsames Vielfaches</u> von a, b, $m = \text{kgV}(a, b)$, wenn

1) $a \mid m$, $b \mid m$

2) Für $m' \in \mathbb{Z}$ mit $a \mid m'$, $b \mid m'$ gilt $m \mid m'$.

Das kgV ist bis auf Vorzeichen eindeutig (Übung).

1.10 Def $p \in \mathbb{N}$ heißt Primzahl, falls $p > 1$ und p besitzt keine weiteren positiven Teiler außer 1 und p.

Anders gesagt: falls $p = ab$ mit $a, b \in \mathbb{N}_{>0}$, so folgt $a = 1$ oder $b = 1$.

1.11 Def $a \in \mathbb{Z}$ heißt zerlegbar / reduzibel, wenn $\exists\ b \neq \pm 1$, $c \neq \pm 1$, $b, c \in \mathbb{Z}$ mit $a = bc$.

Eine von ± 1 verschiedene Zahl, die nicht zerlegbar ist, heißt Primzahl.

1.12 Satz Seien $a, b, c, d, e \in \mathbb{Z}$.

1) Sei $ggT(c,d) = 1$ und $c \mid de$

$\Rightarrow c \mid e$.

2) $p \neq 0, 1, -1$ ist Primzahl $\Leftrightarrow$

$\forall a, b \in \mathbb{Z}$: $p \mid ab$ gilt

$p \mid a$ oder $p \mid b$.

Beweis:

1) $\exists r, s$: $1 = rc + sd \Rightarrow$

$e = erc + esd$. Da $c \mid de$

$\Rightarrow c \mid esd$, da auch

$c \mid erc$ folgt $c \mid e$.

2) „$\Leftarrow$" Sei $p = ab \Rightarrow p \mid ab$

$\Rightarrow$ OE $p \mid a$, also $a = rp$ für

ein $r \in \mathbb{Z} \Rightarrow p = brp \Rightarrow$

$br = 1$. Da $b, r \in \mathbb{Z}$ folgt

$b = r = 1$ oder $b = r = -1$

$\Rightarrow p$ ist nicht zerlegbar $\Rightarrow$

p ist Primzahl.

„$\Rightarrow$" Sei p Primzahl und $p \mid ab$.

Angenommen $p \nmid a$. Da p Primzahl ist, hat es nur die Teiler $\pm 1, \pm p$

$\Rightarrow \operatorname{ggT}(p, a) = 1 \overset{1)}{\Rightarrow} p \mid b$. $\square$

<u>1.13 Satz</u> (Eindeutige Primfaktorzerlegung)

Jedes $0 \neq n \in \mathbb{Z}$ läßt sich in eindeutiger Weise als $n = u p_1 \cdots p_k$ schreiben, wobei $u = \pm 1$ das Vorzeichen ist und $1 < p_1 \leq \cdots \leq p_k$ Primzahlen.

<u>Beweis</u>: Falls $n < 0$ setze $u = -1$, sonst $u = 1$. Betrachte $n > 0$.

Existenz: Per Induktion nach n.

$n = 2$ ist Primzahl. Ist $n > 2$ Primzahl, so ist die gewünschte Darstellung $k = 1$, $p_1 = n$.

Ist $n > 2$ keine Primzahl, dann ist $n = ab$ mit $a, b > 1$.

Da $a, b < n$ gibt es die

gesuchte Darstellung für a, b nach Induktionsvoraussetzung. Nach Umsortieren gibt es damit auch die gesuchte Darstellung für n.

Eindeutigkeit: Induktion über k.

Sei $k=1$, $n=p_1$ Primzahl.

Falls $p_1 = p_1' \cdots p_l'$ so folgt $l=1$ und $p_1 = p_1'$ nach Def von Primzahl.

Sei $k>1$, $n = p_1 \cdots p_k = p_1' \cdots p_l'$

$\Rightarrow p_k \mid p_1' \cdots p_l' \overset{1.12\,2)}{\Longrightarrow} \exists i:$

$p_k \mid p_i'$. Da beide prim sind, folgt $p_k = p_i' \Rightarrow p_1 \cdots p_{k-1} =$

$$p_1' \cdots p_{i-1}' p_{i+1}' \cdots p_l'$$

Da nach Induktionsvoraussetzung für Produkt von $k-1$ Primzahlen die Eindeutigkeit gegeben ist, folgt, daß diese Faktoren gleich sind.

Damit sind auch die Faktoren von $p_1 \cdots p_{k-1} p_k = p_1' \cdots p_i' \cdots p_l'$ gleich. $\square$

1.14 Satz (Euklid)

Es gibt unendlich viele Primzahlen.

Beweis: Angenommen, es gäbe endlich viele Primzahlen, $p_1, \dots, p_n > 0$.

Setze $N = \prod_{i=1}^{n} p_i + 1$.

Wegen des Satzes 1.13 über die Primfaktorzerlegung $\exists$ Primzahl p, die N teilt $\Rightarrow \exists\, i = 1, \dots, n$:

$p = p_i \Rightarrow p_i \mid N - \prod_{j=1}^{n} p_j = 1$

$\Rightarrow p_i \mid 1$ ↯. $\square$

Notation: Für $x \in \mathbb{R}$ setze

$\lfloor x \rfloor := \max\{n \in \mathbb{Z} \mid n \leq x\}$

$\lceil x \rceil := \min\{n \in \mathbb{Z} \mid n \geq x\}$

die untere/obere Gaußklammer.

Bemerkung:

Sei $n \in \mathbb{N}$, $n > 1$, n keine Primzahl.
Ein Primteiler p von n erfüllt
$p \leq \lfloor \sqrt{n} \rfloor$.

Daraus ergibt sich ein Primzahltest:
$n > 1$ ist Primzahl $\iff$ n ist durch keine Primzahl $p \leq \lfloor \sqrt{n} \rfloor$ teilbar.

Sieb des Eratosthenes:
Um alle positiven Primzahlen $\leq N$ zu bestimmen, streiche aus der Liste aller ganzen Zahlen $2, \dots, N$ alle Vielfachen von 2 außer 2, alle Vielfachen von 3 außer 3, ...

Nach $\lceil \sqrt{N} \rceil$ kann man aufhören.
Es bleiben nur Primzahlen stehen.