§1 Teiler, Primzahlen und Hauptsatz der Arithmetik

1. Erinnerung: Wir betrachten die Menge der natürlichen Zahlen $\mathbb{N} = \{0, 1, 2, \dots\}$ sowie der ganzen Zahlen $\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$ mit den üblichen arithmetischen Operationen "$+$", "$\cdot$" und der Anordnung "$\leq$".
Weiter benutzen wir den Absolutbetrag $|z| = \max\{\pm z\}$.

In $\mathbb{N}$ ist die Subtraktion nur eingeschränkt möglich ($2-3$ hat keine Lösung in $\mathbb{N}$), in $\mathbb{Z}$ ist die Division nur eingeschränkt möglich ($2x = 3$ hat keine Lösung in $\mathbb{Z}$).
Es gelten aber in $\mathbb{N}$ und in $\mathbb{Z}$ die

Kürzungsregeln:

$$a + x = a + y \Rightarrow x = y$$

$$a \neq 0,\ ax = ay \Rightarrow x = y$$

2. Induktion und Wohlordnung

Ein wichtiges Beweishilfsmittel ist das Induktionsprinzip.

<u>1. Induktionsprinzip</u> Ist $S \subseteq \mathbb{N}$ mit

(i) $0 \in S$

(ii) $s \in S \Rightarrow s+1 \in S$

so folgt $S = \mathbb{N}$ ("alle natürlichen Zahlen erreicht man, wenn man bei Null anfängt zu zählen")

Das 1. Induktionsprinzip folgt aus der Konstruktion von $\mathbb{N}$ in der Mengenlehre. Aus ihm folgen weitere nützliche Prinzipien.

<u>Wohlordnungsprinzip für $\mathbb{N}$</u> Ist $S \subseteq \mathbb{N}$ mit $S \neq \emptyset$, so hat S ein eindeutiges kleinstes Element, $t_0 = \min S$

<u>Beweis</u> $\boxed{IP1 \Rightarrow WP}$ Sei $\emptyset \neq S \subseteq \mathbb{N}$. Setze $T = \{ t \in \mathbb{N} \mid$ für alle $s \in S$ gilt $t \leq s \}$

Es folgt $0 \in T$. Für $s \in S$ gilt $s+1 \notin T$ (weil $s+1 \not\leq s$), also $T \neq \mathbb{N}$. Nach IP1 gibt es also $t_0 \in T$ mit $t_0 + 1 \notin T$.

<u>Beh:</u> $t_0 \in S$. Denn sonst wäre $t_0 < s$ für alle $s \in S$, also $t_0 + 1 \leq s$ für alle $s \in S$, damit $t_0 + 1 \in T$ ↯

Also $t_0 \in S$. Wenn $t' \in S$ ein weiteres kleinstes Element in S wäre, hätten wir $t_0 \leq t' \leq t_0$, damit $t' = t_0$. □

<u>2. Induktionsprinzip</u> Ist $S \subseteq \mathbb{N}$ mit

(i) $0 \in S$

(ii) für alle $t < s$ gilt $t \in S \Rightarrow s \in S$

so folgt $S = \mathbb{N}$.

<u>Beweis</u> [WP $\Rightarrow$ IP2] Angenommen $S \subsetneq \mathbb{N}$ erfüllt (i) und (ii). Setze $R = \underbrace{\mathbb{N} - S}_{\neq \emptyset}$ und $r = \min R$.

Wegen $0 \in S$ ist $r > 0$. Für alle $t \in \mathbb{N}$ mit $t < r$ gilt nun $t \in S \Rightarrow r \in S$ ↯ □

<u>Vorsicht.</u> 1. und 2. Induktionsprinzip und Wohlordnungsprinzip gilt für Teilmengen von $\mathbb{N}$, <u>nicht</u> unbedingt für Teilmengen von $\mathbb{Z}$. Zum Beispiel hat $\mathbb{Z}$ <u>kein</u> kleinstes Element. Es gilt aber folgendes nützliches Ergebnis.

3. <u>Lemma</u> Sei $S \subseteq \mathbb{Z}$, $\emptyset \neq S$. Wenn S eine obere (bzw untere) Schranke hat, so hat S ein größtes Element $\max S$ (bzw ein kleinstes Element $\min S$).

__Bew:__ Sei $k \in \mathbb{Z}$ obere Schranke für S (d.h. für alle $s \in S$ gilt $s \le k$).
Betrachte $R = \{ k - s \mid s \in S \} \subseteq \mathbb{N}$, setze $r = \min R$. Dann ist $k - r$ das (eindeutige) größte Element in S (nachrechnen!)
Ist $l \in \mathbb{Z}$ untere Schranke für S, so betrachte $R = \{ l + s \mid s \in S \} \subseteq \mathbb{N}$, $r = \min R$
$\leadsto$ $r - l$ ist (eindeutiges) kleinstes Element in S (auch nachrechnen) $\square$

Jetzt betrachten wir Teilbarkeit.

4. __Def__ Sei $a, b \in \mathbb{Z}$. Wenn es ein $m \in \mathbb{Z}$ gibt, mit $am = b$, so heißt a __Teiler__ von b und man schreibt $a \mid b$ (lies: "a teilt b").
Wenn es kein $m \in \mathbb{Z}$ gibt mit $am = b$ schreibe $a \nmid b$.

__Rechenregeln für Teiler__

(i) $1 \mid a$, $a \mid a$, $a \mid 0$ gilt für alle $a \in \mathbb{Z}$

(ii) $a \mid b$ und $b \mid c$ $\Rightarrow$ $a \mid c$

(iii) $a \mid b$ und $b \mid a$ $\Rightarrow$ $a = \pm b$

(iv) $a \mid b$ und $a \mid c$ $\Rightarrow$ $a \mid b \pm c$

(v) $a \neq 0$ und $ab \mid ac$ $\Rightarrow$ $b \mid c$

Beweis (i) klar
(ii) klar } nach Definition

(iii) $am = b$, $bn = a \Rightarrow amn = a \Rightarrow$

$a = 0$ oder $mn = 1 \Rightarrow a = 0$ oder $\begin{matrix} m = \pm 1 \\ n = \pm 1 \end{matrix}$

$\Rightarrow a = \pm b$

(iv) klar

(v) $abm = ac$ a kürzen ($a \neq 0$!) $\square$

5. Satz (Teilen mit Rest)

Sei $a, b \in \mathbb{Z}$ mit $b \neq 0$. Dann gibt es eindeutig bestimmte Zahl $r, s \in \mathbb{Z}$ mit

$$a = b \cdot s + r \quad \text{und} \quad 0 \leq r < |b|$$

Beweis Eindeutigkeit Angenommen,

$$a = b \cdot s + r = b \cdot s' + r' \qquad 0 \leq r, r' < |b|$$

OE $r' \geq r$ Umstellen liefert $b(s - s') = r' - r$

und $0 \leq r' - r < |b|$ sowie $b \mid r' - r$, also

$0 \leq b \cdot m = r' - r < |b| \Rightarrow m = 0 \Rightarrow r = r'$

Existenz Sei $S = \{ k \in \mathbb{Z} \mid k \cdot |b| \leq a \}$

Es gilt $-|a| \in S$, also $S \neq \emptyset$. Weiter ist $|a|$ eine obere Schranke für S. Also existiert $s = \max S$ nach Lemma §1.3.

Es folgt $s \cdot |b| \le a \Rightarrow s \cdot |b| + r = a$ für ein $r \in \mathbb{N}$ und $(s+1)|b| > a = s \cdot |b| + r \Rightarrow |b| > r$

Für $b \geq 0$ erhalten wir $a = b \cdot s + r$. Für $b < 0$ erhalten wir $a = (-s) \cdot b + r$ $\square$

6. <u>Satz</u> Sei $H \subseteq \mathbb{Z}$ eine Teilmenge mit

(i) $H \neq \emptyset$
(ii) $a, b \in H \Rightarrow a - b \in H$.

Dann gibt es ein eindeutiges $d \in \mathbb{N}$ mit

$$H = d\mathbb{Z} = \{ dz \mid z \in \mathbb{Z} \}$$

<u>Beweis</u> Für $a, b \in H$ folgt $a - a = 0 \in H$, $0 - b = -b \in H$, also auch $a + b \in H$.

Falls $H = \{0\}$ fertig mit $d = 0$ (eindeutig)

Sonst sei $S = \{ h \in H \mid h > 0 \} \subseteq \mathbb{N} \Rightarrow S \neq \emptyset$ (denn: es gibt $h \neq 0$ in H, also $h \in \mathbb{N}$ oder $-h \in \mathbb{N}$)

Sei $d = \min S \Rightarrow d > 0$. Für $h \in H$ beliebig liefert Teilen mit Rest

$$h = s \cdot d + r \qquad 0 \le r < d$$

$s \cdot d \in H \Rightarrow r \in H \Rightarrow r = 0$ also $h = s \cdot d$.

Dann $d = \min \{ h \in H \mid h > 0 \}$ eindeutig. $\square$

<u>Korollar</u> Sei $a_1, \dots, a_n \in \mathbb{Z}$, $n \geq 1$.

Sei $H = \{ z_1 a_1 + \dots + z_n a_n \mid z_1, \dots, z_n \in \mathbb{Z} \}$

die Menge der <u>ganzzahligen Linearkombinationen</u> der a_j.

Dann gibt es ein eindeutiges $d \in \mathbb{N}$ mit

$$H = d\mathbb{Z}.$$

<u>Beweis</u> H erfüllt die Voraussetzung aus Satz §1.6 $\square$

Wir definieren in der Situation

$$d = \mathrm{ggT}(a_1, \dots, a_n) \qquad \underline{\text{größter gemeinsamer}} \; \underline{\text{Teiler}}$$

Der Name ggT ist berechtigt:

7. <u>Lemma</u> Sei $a_1, \dots, a_n \in \mathbb{Z}$, $n \geq 1$ und sei $d = \mathrm{ggT}(a_1, \dots, a_n)$. Dann gilt:

(i) $d \mid a_i$ für alle $i = 1, \dots, n$

(ii) Ist $b \in \mathbb{Z}$ und gilt $b \mid a_i$ für alle $i = 1, \dots, n$, so folgt $b \mid d$

[Sei $H = \{ z_1 a_1 + \dots + z_n a_n \mid z_1, \dots, z_n \in \mathbb{Z} \}$]

<u>Beweis</u> (i) $a_i = 1 \cdot a_i \in H = d\mathbb{Z} \Rightarrow a_i = m \cdot d$ für ein $m \in \mathbb{Z}$, d.h. $d \mid a_i$

(ii) $b \mid a_i$ für alle $i = 1, \dots, n \Rightarrow b \mid h$ für alle $h \in H \Rightarrow b \mid d \in H$ $\square$

8. Def Die Zahlen $a_1, \dots, a_n \in \mathbb{Z}$ heißen **teilerfremd** oder **coprim**, wenn gilt

$$ggT(a_1, \dots, a_n) = 1$$

Satz Sei $a_1, \dots, a_n \in \mathbb{Z}$. Dann sind äquivalent:

(i) $ggT(a_1, \dots, a_n) = 1$

(ii) es gibt $z_1, \dots, z_n \in \mathbb{Z}$ mit $a_1 z_1 + \dots + a_n z_n = 1$

Beweis (i) $\Rightarrow$ (ii) nach Definition §1.6.

(ii) $\Rightarrow$ (i) $a_1 z_1 + \dots + a_n z_n = 1 \in d\mathbb{Z} \Rightarrow d\mathbb{Z} = 1\mathbb{Z} \Rightarrow$

$\Rightarrow \quad d = ggT(a_1, \dots, a_n) = 1$ $\square$

Korollar Sind $a, b, c \in \mathbb{Z}$ mit $ggT(a,b) = 1 = ggT(a,c)$, so gilt $ggT(a, bc) = 1$.

Beweis Wähle $x, y, u, v \in \mathbb{Z}$ mit $1 = ax + by = au + cv$

$$\Rightarrow 1 = (ax+by)(au+cv)$$
$$= a(uxa + cvx + byu) + bc(vy) \quad \square$$

Korollar Sind $a_1, \dots, a_n; b \in \mathbb{Z}$ und gilt $ggT(a_i, b) = 1$ für $i = 1, \dots, n$, so gilt auch $ggT(a_1 \cdot a_2 \cdot a_3 \cdots a_n, b) = 1$

Beweis mit Induktion nach n. $n = 1$ klar.

$\boxed{n \to n+1}$ $\quad ggT(a_1 \cdots a_n, b) = 1 = ggT(a_{n+1}, b)$

$\overset{\text{Kor}}{\Rightarrow} ggT(a_1 \cdots a_n a_{n+1}, b) = 1$ $\square$

9. Def Eine natürliche Zahl $p \geq 2$ heißt **Primzahl**, falls 1 und p die einzigen positiven Teiler von p sind, d.h. wenn gilt

$$d \mid p \Rightarrow d = \pm 1 \text{ oder } d = \pm p.$$

Setze $\mathbb{P} = \{ p \in \mathbb{N} \mid p \text{ Primzahl} \}$

$\mathbb{P} = \{ 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, \ldots \}$

Lemma Sei $n \in \mathbb{N}$ mit $n \geq 2$ und sei

$$p(n) = \min \underbrace{\{ k \in \mathbb{N} \mid k \geq 2 \text{ und } k \mid n \}}_{\text{enthält } n}$$

Dann ist $p(n)$ Primzahl.

Bew: Sei d ein positiver Teiler von $p(n)$. Es folgt $1 \leq d \leq p(n)$ und $d \mid n \Rightarrow d = 1$ oder $d = p(n)$ $\square$

10. Theorem (Euklid) Es gibt unendlich viele Primzahlen.

Bew: Angenommen, $\mathbb{P} = \{ p_1 < p_2 < \ldots < p_m \}$ wäre endlich. Setze $n = (p_1 \cdot p_2 \cdot p_3 \cdots p_m) + 1 \geq 2$.

Es folgt $p_j \nmid n$ für $j = 1, \ldots, m$ (sonst $p_j \mid 1$ ↯).

Also gilt $p(n) \neq p_1, \ldots, p_m$. Aber $p(n) \in \mathbb{P}$ ↯

$\square$

11. <u>Theorem</u> (Hauptsatz der Arithmetik) Sei $n \in \mathbb{N}$ mit $n \geq 2$. Dann existieren eindeutig bestimmte Primzahlen $p_1 \leq p_2 \leq p_3 \leq \dots \leq p_m$ mit

$$n = p_1 \cdot p_2 \cdot p_3 \cdots p_m$$

Man nennt die p_i die <u>Primfaktoren</u> von n.

<u>Beweis</u> <u>Existenz</u> einer Primfaktorzerlegung mit 2. Induktionsprinzip. Für $n = 0, 1$ wird nichts behauptet $\to$ ok. Sei nun $n \geq 2$, und für alle $m < n$ existiere eine Primfaktorzerlegung. Betrachte

$$p(n) \in \mathbb{P} \leadsto n = \underbrace{p(n)}_{\geq 2} \cdot s \quad \text{mit } s < n$$

$\Rightarrow$ $s = 1$ ($\to$ fertig)

<u>oder</u> $s = p_1 \cdots p_k \quad p_i \in \mathbb{P}$

Damit $n = p(n) \cdot p_1 \cdot \ldots \cdot p_k$, sortiere jetzt die Primfaktoren der Größe nach.

<u>Eindeutigkeit</u> der Primfaktoren.

Schreibe $n = p_1 \cdots p_k \quad p_i \in \mathbb{P}$

Sei $q \in \mathbb{P}$ beliebige Primzahl, sei l die Anzahl der i mit $p_i = q$ (also $l = 0$ falls alle $p_i \neq q$)

Es folgt $n = q^l \cdot s$ und s ist Produkt von Primzahlen p_j mit $p_j \neq q$, also insbesondere mit $ggT(q, p_j) = 1$. Nach § 1.8 gilt dann $ggT(q, s) = 1$, insbesondere $q \nmid s$. Es folgt $q^{l+1} \nmid n$ (wegen Kürzungsregel, $n = q^{l+1} \cdot t = q^l \cdot s \Rightarrow q \cdot t = s$!). Wir haben gezeigt:

$$l = \max\{k \in \mathbb{N} \mid q^k \mid n\}$$

Diese Zahlen hängen nicht von der gewählten Primfaktorzerlegung ab. Wenn wir also definieren

$$\nu_q(n) = \max\{k \in \mathbb{N} \mid q^k \mid n\}$$

so folgt $\{p_1, \dots, p_k\} = \{q \in \mathbb{P} \mid \nu_q(n) \neq 0\}$ und jedes p_i kommt genau mit der Vielfachheit $\nu_q(n)$ in der Primfaktorzerlegung vor. $\square$

Def Für $n \in \mathbb{Z}$ und $q \in \mathbb{P}$ definieren wir die <u>q-adische Bewertung</u> von n durch

$$\nu_q(n) = \begin{cases} \infty & \text{falls } n = 0 \\ \max\{k \in \mathbb{N} \mid q^k \mid n\} & \text{falls } n \neq 0 \end{cases}$$

Damit erhalten wir folgende Umformulierung des Hauptsatzes:

<u>Fundamentalsatz der Arithmetik, 2. Version</u>

Sei $n \in \mathbb{Z}$ mit $n \neq 0$. Sei $\varepsilon(n) = \begin{cases} 1 & \text{wenn } n > 0 \\ -1 & \text{wenn } n < 0 \end{cases}$

Es gilt

$$n = \varepsilon(n) \cdot \prod_{q \in \mathbb{P}} q^{v_q(n)}$$

Das ist ein unendliches Produkt, in dem aber fast alle Faktoren 1 sind. Also steht rechts ein Produkt aus <u>endlich</u> vielen Primzahlpotenzen.

12. <u>Korollar</u> Sei $a, b \in \mathbb{Z}$. Dann sind äquivalent:
(i) $a \mid b$ (ii) Für alle $q \in \mathbb{P}$ gilt $v_q(a) \leq v_q(b)$.

<u>Beweis</u> (i) $\Rightarrow$ (ii) klar nach Definition der v_q, denn $q^k \mid a$ und $a \mid b \Rightarrow q^k \mid b$.
(ii) $\Rightarrow$ (i) ist richtig, falls $b = 0$. Wenn aber $b \neq 0$, so folgt die Behauptung aus der 2. Version des Hauptsatzes □

13. <u>Lemma</u> Sei $a, b \in \mathbb{Z}$ und $p \in \mathbb{P}$. Wenn gilt $p \mid ab$, so folgt $p \mid a$ oder $p \mid b$.

<u>Beweis</u> (<u>ohne</u> Hauptsatz!) Angenommen, $p \nmid a$ und $p \nmid b$. Dann ist $ggT(p, a) = 1 = ggT(p, b)$, weil $p \in \mathbb{P}$. Also $ggT(p, ab) = 1$ nach §1.8, damit $p \nmid ab$ □

Wir machen als Anwendung einen kleinen Exkurs über vollkommene Zahlen. Eine Zahl $n \in \mathbb{N}$ heißt vollkommen, falls n die Summe aller echt positiven Teiler von n ist. In der Antike interessierte man sich aus Gründen der Mystik für solche Zahlen.

Bsp $6 = 1+2+3$ vollkommen

$8 \neq 1+2+4$ nicht vollkommen.

14. Def Für $n \in \mathbb{N}$, $n \geq 1$ sei

$$\sigma(n) = \sum_{\substack{k \geq 0 \\ k \mid n}} k$$

die Summe aller positiven Teiler von n. Also: n vollkommen $\iff \sigma(n) = 2n$

Weiter sei

$$\tau(n) = \sum_{\substack{k \geq 0 \\ k \mid n}} 1$$

die Anzahl aller positiven Teiler von n. Also $n \in \mathbb{P} \iff \tau(n) = 2$

Bsp

n	$\tau(n)$	$\sigma(n)$	
1	1	1	
2	2	3	
3	2	4	
4	3	7	
5	2	6	
6	4	12	← vollkommen

Lemma Es gilt $\tau(n) = \prod_{q \in \mathbb{P}} (1 + \nu_q(n))$

Beweis Folgt direkt aus §1.12

Folgerung Wenn $ggT(a,b) = 1$ für $a, b \in \mathbb{N}$, $a, b \geq 1$, so gilt $\tau(ab) = \tau(a) \cdot \tau(b)$.

Lemma Es gilt
$$\sigma(n) = \prod_{q \in \mathbb{P}} \sigma(q^{\nu_q(n)})$$
$$= \prod_{q \in \mathbb{P}} \frac{q^{1+\nu_q(n)} - 1}{q - 1}$$

Beweis Mit §1.12 folgt

$$\sigma(n) = \sum_{0 \leq l_q \leq \nu_q(n)} \prod_{q \in \mathbb{P}} q^{l_q} = \prod_{q \in \mathbb{P}} \sum_{l_q = 0}^{\nu_q(n)} q^{l_q}$$

rechte Seite ausmultiplizieren

$$= \prod_{q \in \mathbb{P}} \sigma(q^{\nu_q(n)})$$

$$= \prod_{q \in \mathbb{P}} \frac{q^{\nu_q(n)+1} - 1}{q - 1}$$

geometrische Summe

∎

Folgerung Wenn $ggT(a,b) = 1$ und $a, b \geq 1$, so gilt $\sigma(ab) = \sigma(a) \cdot \sigma(b)$.

15 **Theorem** (Euklid / Euler) Sei $n \geq 2$ gerade.

Dann sind äquivalent:

(i) n ist vollkommen

(ii) $n = 2^{k-1}(2^k - 1)$ für ein $k \geq 2$ und $2^k - 1 \in \mathbb{P}$. #

Beweis (ii) $\Rightarrow$ (i) (Euklid) Angenommen,

$$n = 2^{k-1} \cdot \underbrace{(2^k - 1)}_{= q} \quad \text{mit } k \geq 2 \Rightarrow q \geq 3.$$

Also
$$\sigma(n) = \sigma(2^{k-1}) \cdot \sigma(q) = \frac{2^k - 1}{2 - 1} \cdot (1 + q) = (2^k - 1) \cdot 2^k = 2 \cdot n$$

(i) $\Rightarrow$ (ii) (Euler) Schreibe $n = 2^{k-1} \cdot m$ mit m ungerade $\Rightarrow k \geq 2$, da n gerade ist.

Also
$$\sigma(n) = 2 \cdot n = \underbrace{\frac{2^k - 1}{2 - 1}}_{\text{ungerade}} \cdot \sigma(m) = 2^k \cdot m$$

↑ n vollkommen

Es folgt $2^k \mid \sigma(m)$, d.h. $\sigma(m) = 2^k \cdot l$ für ein $l \in \mathbb{N}$. Insgesamt

$$2n = \cancel{2^k} \cdot m = (2^k - 1) \cdot \cancel{2^k} \cdot l \qquad \text{(kürzen)}$$
$$m = (2^k - 1)\, l$$

Beh $l = 1$.

Sonst $\sigma(m) \geq \underbrace{1 + l + (2^k - 1)\cdot l}_{\text{alles Teiler}} > 2^k \cdot l = \sigma(m)$ ↯

Also $m = 2^k - 1 = \sigma(m) - 1 \Rightarrow m \in \mathbb{P}$ □

16. Bemerkungen

(1) Es ist unbekannt, ob es ungerade vollkommene Zahlen gibt (wenn ja, so sind sie größer als 10^{1500})

(2) Primzahlen der Form $q = 2^l - 1$ heißen Mersenne'sche Primzahlen. Nicht alle Zahlen dieser Form sind Primzahlen, zum Beispiel gilt

$$2^6 - 1 = 63 = 3^2 \cdot 7$$

Im Moment sind 49 Mersenne'sche Primzahlen bekannt. Es ist ein offenes Problem, ob es unendlich viele Mersenne'sche Primzahlen gibt.

Bem Wenn $2^l - 1 \in \mathbb{P}$ gilt, dann folgt auch $l \in \mathbb{P}$. Denn wenn $l = u \cdot v$ mit $u, v \in \mathbb{N}$, $u, v > 1$, so gilt

$$2^{uv} - 1 = (2^u)^v - 1 = \underbrace{(2^u - 1)}_{\geq 2} \cdot \underbrace{\sum_{j=0}^{v-1} (2^u)^j}_{\geq 2}$$

(geometrische Summe)

Achtung: $11 \in \mathbb{P}$, aber $2^{11} - 1 = 2048 - 1 = 23 \cdot 89$ ist keine Primzahl.

Damit ist der Exkurs zu vollkommenen Zahlen beendet.

Wir bleiben aber in der Antike.

17. Lemma Sei $a, b, m \in \mathbb{Z}$. Dann gilt

$$ggT(a,b) = ggT(a, b+ma)$$

Beweis

$$\{u_1 a + v_2 b \mid u_1, v \in \mathbb{Z}\} = \{ua + v(b+ma) \mid u, v \in \mathbb{Z}\} \quad \square$$

Euklids Algorithmus

Euklid "Wenn b aber a nicht misst (= teilt) und man nimmt von a, b abwechselnd immer das Kleinere vom Größeren weg, dann muss schließlich eine Zahl übrig bleiben, die die voran gegangenen misst."

Wir schreiben das als Pseudocode auf und passen den Algorithmus so an, dass $a, b \in \mathbb{Z}$ erlaubt sind.

Pseudocode:

```
ggT(a,b) {
    if a<0        a ← -a          ggT(a,b) = ggT(-a,b)
    if b<0        b ← -b          ggT(a,b) = ggT(a,-b)
ab jetzt a,b≥0 —
    if a=0        return b        ggT(0,b) = b
    if b=0        return a        ggT(a,0) = a
ab jetzt a,b>0 —
    while a≠b {
        if a>b    a ← a-b    ggT(a,b)=ggT(a-b,b)
        if b>a    b ← b-a    ggT(a,b)=ggT(a,b-a)
    }
ab jetzt a=b —
    return a
}
```

In der while-Schleife ist $|a-b|$ streng monoton fallend, also nach endlich vielen Durchläufen $a=b>0$. Dann gilt $ggT(a,b) = a = b$.

Beachte: Als arithmetische Operation wird nur Subtraktion verwendet.

18. Der euklidische Algorithmus wird oft etwas anders aufgeschrieben:

Gegeben sind ganze Zahlen r_0, r_1 mit $r_1 \neq 0$.

Gesucht ist der ggT von r_0 und r_1. Wir teilen immer wieder mit Rest, vgl. § 1.5.

$$r_0 = s_0 \cdot r_1 + r_2 \qquad 0 \le r_2 < |r_1| \qquad \mathrm{ggT}(r_0, r_1)$$

$$\downarrow r_2 \neq 0 \qquad\qquad \| \ \S 1.17 \text{ Lemma}$$

$$r_1 = s_1 \cdot r_2 + r_3 \qquad 0 \le r_2 < |r_2| < |r_1| \qquad \mathrm{ggT}(r_1, r_2)$$

(Rest wird immer kleiner)

$$\downarrow r_3 \neq 0 \qquad\qquad \|$$

$$\vdots \qquad\qquad \vdots$$

$$r_k = s_k \cdot r_{k+1} + r_{k+2} \qquad \mathrm{ggT}(r_k, r_{k+1})$$

$$\downarrow r_{k+2} \neq 0 \qquad\qquad \|$$

$$r_{k+1} = s_{k+1} \cdot r_{k+2} \qquad \mathrm{ggT}(r_{k+1}, r_{k+2}) = r_{k+2}$$

<u>fertig</u>

Rückwärts einsetzen liefert für $d = \mathrm{ggT}(r_0, r_1)$, dass

$$r_k - s_k \cdot r_{k+1} = r_{k+2} = d$$

$$r_{k-1} - s_{k-1} \cdot r_k = r_{k+1}$$

$$\vdots$$

$$r_0 - s_0 \cdot r_1 = r_2.$$

und erhält $d = a r_0 + b r_1$ <u>konstruktiv</u>.

Beispiel $ggT(343, 280) = d$

$$343 = 1 \cdot 280 + 63$$

$$280 = 4 \cdot 63 + 28$$

$$63 = 2 \cdot 28 + 7$$

$$28 = 4 \cdot \underline{\underline{7}} + 0$$

$\Rightarrow ggT(343, 280) = 7$

Jetzt rückwärts einsetzen

$$7 = 63 - 2 \cdot 28$$

$$28 = 280 - 4 \cdot 63$$

$$63 = 343 - 1 \cdot 280$$

also $7 = 63 - 2 \cdot (280 - 4 \cdot 63)$

$$= (343 - 1 \cdot 280) - 2(280 - 4(343 - 1 \cdot 280))$$

$$= 9 \cdot 343 + (-11) \cdot 280 \qquad (✓) \qquad \#$$

Als eine Anwendung betrachten wir <u>lineare Diophantische Gleichungen</u> (Diophantos von Alexandria, griech. Mathematiker)

19. **Def** Sei $a_1, \dots, a_n \in \mathbb{Z}$, für $n \geq 1$, sei $c \in \mathbb{Z}$. Eine Gleichung der Form

$$a_1 z_1 + a_2 z_2 + \dots + a_n z_n = c$$

wird lineare Diophantische Gleichung genannt.

Gesucht ist die Lösungsmenge $L = \{ z_1, \dots, z_n \in \mathbb{Z} \mid a_1 z_1 + \dots + a_n z_n = c \}$

Satz Die lineare Diophantische Gleichung

$$a_1 z_1 + \dots + a_n z_n = c$$

hat genau dann Lösungen $(z_1, \dots, z_n) \in \mathbb{Z}^n$, wenn gilt

$$\operatorname{ggT}(a_1, \dots, a_n) \mid c.$$

Beweis Sei $H = \{ a_1 z_1 + \dots + a_n z_n \mid z_1, \dots, z_n \in \mathbb{Z} \}$ die Menge der ganzzahligen Linearkombination von $a_1, \dots, a_n$. Nach § 1.6 gilt $H = d \cdot \mathbb{Z}$ mit $d = \operatorname{ggT}(a_1, \dots, a_n)$. Folglich gilt $c \in H$ genau dann, wenn $d \mid c$. $\square$

Wie berechnet man aber alle Lösungen?

Für $n = 1$ ist das einfach:

$$L = \{ z \mid az = c \} = \begin{cases} \emptyset & \text{falls } a \nmid c \\ \{b\} & \text{falls } c = a \cdot b \end{cases}$$

20. Wir betrachten jetzt den Fall $n=2$ systematisch, d.h. wir suchen ganzzahlige Lösungen der Gleichung

$$ax+by=c \qquad \text{für} \qquad a,b,c\in\mathbb{Z} \text{ vorgegeben.}$$

__Lemma__ Sind $a,b,d\in\mathbb{Z}$ mit $ggT(a,d)=1$ und gilt $d\mid ab$, so folgt $d\mid b$.

__Beweis__ Schreibe $1=ax+dy$ mit $x,y\in\mathbb{Z}$, es folgt

$b=1\cdot b=abx+bdy$ $\square$

__Lemma__ Sind $a,b,m\in\mathbb{Z}$ mit $ggT(a,b)=1$ und gilt $a\mid m$ und $b\mid m$, so folgt $ab\mid m$.

__Beweis__ Schreibe $m=b\cdot s \xrightarrow{\text{voriges Lemma}} a\mid s \leadsto s=r\cdot a$

$\leadsto \quad m=ab\cdot r$ $\square$

__Satz__ Ist $a,b\in\mathbb{Z}$ mit $ggT(a,b)=1$, so ist die Lösungsmenge L aller ganzzahligen Lösungen der Gleichung $ax+by=0$ die Menge

$$L=\{(-t\cdot b,\ t\cdot a)\mid t\in\mathbb{Z}\}$$

__Beweis__ Es gilt $a(-t\cdot b)+b(t\cdot a)=0$ $(\checkmark)$

Sei umgekehrt $(x,y)\in\mathbb{Z}^2$ eine Lösung, also $ax+by=0$. Es folgt $a\mid ax=-by \leadsto a\mid y$ (voriges Lemma) $y=a\cdot t$. Genauso: $b\mid x$, $x=b\cdot s \Rightarrow a\cdot(b\cdot s)+b(a\cdot t)=ab(s+t)=0$

Wenn $ab\neq 0$, dann also $s=-t \leadsto$ fertig.

Wenn $a=0$, dann $b=\pm 1$, $L=\{(t,0)\mid t\in\mathbb{Z}\}(\checkmark)$

genauso, wenn $b=0$ $\square$

Satz Sei $a,b,c \in \mathbb{Z}$ mit $(a,b) \neq (0,0)$.
Die lineare Diophantische Gleichung
$$ax + by = c$$
hat genau dann ganzzahlige Lösungen, wenn gilt $\operatorname{ggT}(a,b) \mid c$. Wenn $(x_0, y_0) \in \mathbb{Z}^2$ eine Lösung ist, so ist jede weitere Lösung (x,y) von der Form
$$(x,y) = (x_0 - t \cdot b', \; y_0 + t \cdot a')$$
mit $t \in \mathbb{Z}$, wobei $b = d \cdot b'$, $a = d \cdot a'$, $d = \operatorname{ggT}(a,b)$.

Beweis Die erste Behauptung ist ein Spezialfall von Satz §1.9. Es geht nur noch um die Struktur der Lösungsmenge. Sei also $d = \operatorname{ggT}(a,b)$ und $b = d \cdot b'$, $a = d \cdot a'$. Sei $(x_0, y_0) \in \mathbb{Z}^2$ eine Lösung, sei $x, y \in \mathbb{Z}$ beliebig. Es gilt nun:

$d \neq 0$ weil $(a,b) \neq (0,0)$

$$\begin{aligned}
ax + by = c &\iff a(x - x_0) + b(y - y_0) = 0 \\
&\iff d \cdot a'(x - x_0) + d \cdot b'(y - y_0) = 0 \\
&\overset{(*)}{\iff} a'(x - x_0) + b' \cdot (y - y_0) = 0 \\
&\overset{(**)}{\iff} x - x_0 = t \cdot b' \text{ und } y_0 - y = t \cdot a' \\
&\quad \text{für ein } t \in \mathbb{Z}
\end{aligned}$$

$(*)$: $d \neq 0$ kürzen

$(**)$: $\operatorname{ggT}(a', b') = 1$ $\left[\begin{array}{l} \text{denn: } au + bv = d \\ \Rightarrow a'du + b'dv = d \\ \Rightarrow a'u + b'v = 1, \text{ §1.8} \end{array}\right]$

wende jetzt vorigen Satz an. $\square$

Beachte Wir können eine Lösung x_0, y_0 explizit finden wie folgt. Sei $d = ggT(a,b)$. Mit dem euklidischen Algorithmus aus § 1.18 finden wir $u, v \in \mathbb{Z}$ mit $au + bv = d$. Schreibe $c = d \cdot d'$

$\Rightarrow$ $a(ud') + b(vd') = c$, also ist $(x_0, y_0) = (ud', vd')$ eine Lösung. Der Satz liefert dann den Rest der Lösungsmenge L.

21 Zum Abschluss betrachten wir noch den Fall $n \geq 0$. Nach Satz § 1.19 wissen wir: die lineare Diophantische Gleichung

$$a_1 z_1 + a_2 z_2 + \dots + a_n z_n = c$$

ist genau dann lösbar, wenn gilt $ggT(a_1, \dots, a_n) \mid c$. Es geht also nur noch um ein Lösungsverfahren. Dafür gehen wir rekursiv vor: für $n = 1, 2$ haben wir Lösungsverfahren. Wir können also annehmen, dass wir für $n-1$ Variablen ein Lösungsverfahren haben, und dass $a_1, \dots, a_n \neq 0$ gilt.

Sei

Lemma Sei $a_1, \dots, a_n \in \mathbb{Z}$, sei $b = \mathrm{ggT}(a_{n-1}, a_n)$.

Dann ist $(z_1, \dots, z_n) \in \mathbb{Z}^n$ genau dann eine Lösung der Gleichung

(1) $a_1 z_1 + \dots + a_n z_n = c$

wenn es $y \in \mathbb{Z}$ gibt, so dass gilt

(2a) $a_1 z_1 + \dots + a_{n-2} z_{n-2} + b \cdot y = c$

(2b) $a_{n-1} z_{n-1} + a_n \cdot z_n = b \cdot y$

Beweis: Klar: wenn wir (2a) und (2b) lösen, erhalten wir eine Lösung von (1).
Ist umgekehrt $(z_1, \dots, z_n)$ eine Lösung von (1), so gibt es $y \in \mathbb{Z}$ mit $a_{n-1} \cdot z_{n-1} + a_n z_n = b \cdot y$, weil $b = \mathrm{ggT}(a_{n-1}, a_n)$, vgl. § 1.6.

$\square$

#