DISKRETE MATHEMATIK

Kapitel 4: Elementare Zahlentheorie

MAT.106UB Vorlesung im WS 2018/19

Günter LETTL

Institut für Mathematik und wissenschaftliches Rechnen
an der Karl-Franzens-Universität Graz

4.1 Teilbarkeit

[I-L] 4.1, [L-P-V] 6.1, [S-S] 5.3.30-5.3.60

Definition (1)

a) (Teilbarkeitsrelation auf $\mathbb{Z}$) [vgl. Übung Bsp. 9]
Für $a, b \in \mathbb{Z}$ gilt *„a teilt b"* (in Zeichen: $a \mid b$) genau dann, wenn es ein $a' \in \mathbb{Z}$ mit $a \cdot a' = b$ gibt.

Gilt $a \mid b$, so sagt man auch: b *ist* durch a *teilbar*, a ist ein *Teiler* von b bzw. b ist ein *Vielfaches* von a,
und – falls $a \neq 0$ – nennt $a' = \frac{b}{a}$ den *Komplementärteiler zu a* (bezüglich b).

Gilt $a \mid b$ nicht, so schreibt man: $a \nmid b$.

Definition (1) (Fortsetzung)

b) (Assoziiertheitsrelation auf $\mathbb{Z}$)
Ganze Zahlen $a, b \in \mathbb{Z}$ heißen *zueinander assoziiert* (in Zeichen: $a \sim b$) genau dann, wenn $a \mid b$ und $b \mid a$ gilt.

c) Für $a \in \mathbb{Z}$ definieren wir:

$T(a) = \{t \in \mathbb{N} \mid \; t \mid a\}$ die *Menge aller positiven Teiler von a*,

$V(a) = \{v \in \mathbb{N} \mid \; a \mid v\}$ die *Menge aller positiven Vielfachen von a*

und die *Teileranzahlfunktion* τ

$$\begin{aligned} \tau : \mathbb{N} &\to \mathbb{N} \\ n &\mapsto \tau(n) := \# T(n) \end{aligned}$$

Lemma (1) (Eigenschaften der Teilerrelation)

Für beliebige $a, b, c \in \mathbb{Z}$ *gilt:*

a) $1 \mid a, \quad a \mid a, \quad a \mid 0 \quad \textit{und} \quad \big(0 \mid a \;\Leftrightarrow\; a = 0\big).$

Also: $T(0) = \mathbb{N}, \quad 1 \in T(a).$

b) $\big(a \mid b \;\wedge\; b \mid c\big) \;\Rightarrow\; a \mid c.$

c) $a \mid b \;\Leftrightarrow\; |a| \;\big|\; |b| \;\Leftrightarrow\; \pm a \mid \pm b$

$\big(a \mid b \;\wedge\; b \neq 0\big) \;\Rightarrow\; |a| \leq |b|.$

Also: für $a \neq 0$ *ist* $\{1, |a|\} \subset T(a) \subset \{1, 2, \ldots, |a|\},$

$\tau(1) = 1,$ *und für* $|a| \geq 2$ *gilt:* $2 \leq \tau(a) \leq |a|.$

d) $a \sim b \;\Leftrightarrow\; |a| = |b| \;\Leftrightarrow\; b = \pm a$

e) $\big(a \mid b \;\wedge\; a \mid c\big) \;\Rightarrow\; a \mid (b \pm c)$

$a \mid b \;\Rightarrow\; \big(a \mid bc \;\wedge\; ac \mid bc\big).$

Definition (2)

Es seien $a, b \in \mathbb{Z}$.

a) Eine Zahl $d \in \mathbb{Z}$ heißt ein *größter gemeinsamer Teiler von a und b*, wenn gilt:

(GGT1) $d \mid a$ und $d \mid b$

(GGT2) $\forall t \in \mathbb{Z}$ mit $t \mid a$ und $t \mid b$ gilt: $t \mid d$.

b) Ist $(a, b) \neq (0, 0)$, so heißt

$$\mathrm{ggT}(a, b) := \max\Big(T(a) \cap T(b)\Big) \in \mathbb{N}$$

der *größte gemeinsame Teiler von a und b*.

Satz (1)

Es seien $a, b \in \mathbb{Z}$. Dann gilt:

a) $a \mid b \;\Leftrightarrow\; T(a) \subset T(b)$.

b) $\forall k \in \mathbb{Z}: \;\; T(a) \cap T(b) = T(a) \cap T(b + ka)$.

Es sei nun zusätzlich $(a, b) \neq (0, 0)$ und $d = ggT(a, b)$ (vgl. Definition 2.b)). Dann gilt:

c) $T(d) = T(a) \cap T(b)$, *und es existieren $x, y \in \mathbb{Z}$ mit*

$$d = ax + by \;.$$

d) *d ist ein größter gemeinsamer Teiler von a und b (nach Definition 2.a)).*

Korollar (1)

Für $a, b, k \in \mathbb{Z}$ mit $(a, b) \neq (0, 0)$ gilt:

$$ggT(a, b) = ggT(a, b + ka) \;.$$

Satz (1)

Es seien $a, b \in \mathbb{Z}$. *Dann gilt:*

a) $a \mid b \;\Leftrightarrow\; T(a) \subset T(b)$.

b) $\forall k \in \mathbb{Z}: \;\; T(a) \cap T(b) = T(a) \cap T(b + ka)$.

Es sei nun zusätzlich $(a, b) \neq (0, 0)$ *und* $d = ggT(a, b)$ *(vgl. Definition 2.b)). Dann gilt:*

c) $T(d) = T(a) \cap T(b)$, *und es existieren* $x, y \in \mathbb{Z}$ *mit*

$$d = ax + by \; .$$

d) *d ist ein größter gemeinsamer Teiler von a und b (nach Definition 2.a)).*

Korollar (1)

Für $a, b, k \in \mathbb{Z}$ *mit* $(a, b) \neq (0, 0)$ *gilt:*

$$ggT(a, b) = ggT(a, b + ka) \; .$$

4.2 Primzahlen

[I-L] 4.3, [L-P-V] 6.2-6.4, [S-S] 2.1, 5.3.45-5.3.51, [St] 3.1

Definition (3)

a) Zahlen $a, b \in \mathbb{Z}$ heißen *zueinander relativ prim* (oder *teilerfremd*), wenn $\mathrm{ggT}(a, b) = 1$ ist.

b) Eine Zahl $q \in \mathbb{Z}$ heißt ein *Primelement* (von $\mathbb{Z}$), wenn $|q| \geq 2$ und für alle $a, b \in \mathbb{Z}$ gilt:

$$q \mid ab \;\Rightarrow\; (q \mid a \;\vee\; q \mid b)\;.$$

c) Eine Zahl $p \in \mathbb{N}$ heißt eine *Primzahl*, wenn $\tau(p) = 2$ gilt
$(\iff ((p \geq 2) \wedge (T(p) = \{1, p\})))$.

Die Menge aller Primzahlen wird mit $\mathbb{P} = \{2, 3, 5, 7, 11, 13, \dots\}$ bezeichnet.

d) Eine Zahl $a \in \mathbb{Z} \setminus \{0\}$ heißt *zusammengesetzte Zahl*, wenn $\tau(|a|) \geq 3$ gilt ($\iff$ es gibt ein $t \in \mathbb{N}$ mit $1 < t < |a|$ und $t \mid n$).

Satz (2)

a) *Ist* $a \in \mathbb{Z}$ *mit* $|a| \geq 2$, *so ist*

$$p := \min(T(a) \setminus \{1\})$$

eine Primzahl mit $p \mid a$.

b) *Jede Primzahl* $p \in \mathbb{P}$ *ist ein Primelement von* $\mathbb{Z}$.

c) (Hauptsatz der elementaren Zahlentheorie)
Für jedes $0 \neq a \in \mathbb{Z}$ *existieren eindeutig bestimmte* $r \in \mathbb{N}_0$ *und Primzahlen* $p_1, p_2, \ldots, p_r \in \mathbb{P}$ *mit*

$$a = sgn(a) \cdot \prod_{i=1}^{r} p_i \quad \text{und} \quad p_1 \leq p_2 \leq \cdots \leq p_r \ .$$

d) *Jedes Primelement* $q \in \mathbb{Z}$ *ist von der Form* $q = \pm p$ *mit* $p \in \mathbb{P}$.

Varianten zu Satz 2.c):

Für jedes $0 \neq a \in \mathbb{Z}$ existieren eindeutig bestimmte

A) $k \in \mathbb{N}_0$, $p_1 < p_2 < \cdots < p_k \in \mathbb{P}$ und $e_1, \ldots, e_k \in \mathbb{N}$, sodass

$$a = \operatorname{sgn}(a) \cdot \prod_{i=1}^{k} p_i^{e_i} .$$

B) $e_1 \in \{0, 1\}$ und für alle $p \in \mathbb{P}$ $e_p \in \mathbb{N}_0$, wobei $e_p \neq 0$ nur für endlich viele $p \in \mathbb{P}$ gilt, sodass

$$a = (-1)^{e_1} \cdot \prod_{p \in \mathbb{P}} p^{e_p} .$$

Satz (3) (Satz von Euklid)

$$\#\mathbb{P} = \infty \ .$$

Definition (4)

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

$$\mathrm{kgV}(a, b) := \min\Big(V(a) \cap V(b)\Big) \in \mathbb{N}$$

das *kleinste gemeinsame Vielfache von a und b*.

Satz (3) (Satz von Euklid)

$$\#\mathbb{P} = \infty\ .$$

Definition (4)

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

$$\mathrm{kgV}(a, b) := \min\Big(V(a) \cap V(b)\Big) \in \mathbb{N}$$

das *kleinste gemeinsame Vielfache von a und b*.

Satz (4)

Sind $a, b \in \mathbb{Z} \setminus \{0\}$ *mit* $a = sgn(a) \cdot \prod_{p \in \mathbb{P}} p^{e_p}$, $b = sgn(b) \cdot \prod_{p \in \mathbb{P}} p^{f_p}$ *(so wie in Variante B) zu Satz 2.c)), so gilt:*

a) $a \mid b \iff$ *für alle* $p \in \mathbb{P}$ *gilt:* $e_p \leq f_p$.

b) $T(a) = \left\{ \prod_{p \in \mathbb{P}} p^{h_p} \mid 0 \leq h_p \leq e_p \right\}$, $\tau(|a|) = \prod_{p \in \mathbb{P}} (e_p + 1)$ *und*

$V(a) = \left\{ \prod_{p \in \mathbb{P}} p^{k_p} \,\middle|\, k_p \in \mathbb{N}, e_p \leq k_p \text{ und } k_p = 0 \text{ für fast alle } p \in \mathbb{P} \right\}$.

c) $ggT(a, b) = \prod_{p \in \mathbb{P}} p^{\min\{e_p, f_p\}}$, $kgV(a, b) = \prod_{p \in \mathbb{P}} p^{\max\{e_p, f_p\}}$ *und*

$$ggT(a, b) \cdot kgV(a, b) = |ab| \; .$$

4.3 Der Euklid'sche Algorithmus

[I-L] 4.2, [L-P-V] 6.6, [St] 3.2.2

Satz (5) (Division mit Rest)

Es seien $a, b \in \mathbb{Z}$ und $b \neq 0$.
Dann existieren eindeutig bestimmte $q, r \in \mathbb{Z}$ mit $0 \leq r < |b|$, sodass gilt:

$$a = bq + r \ .$$

Beispiel zu Satz 6: $\mathrm{ggT}(94729, 93439) = ?$

$94729 = 1 \cdot 93439 + 1290$ $(= \text{Rest } r_1)$
$93439 = 72 \cdot 1290 + 559$ $(= \text{Rest } r_2)$
$1290 = 2 \cdot 559 + 172$ $(= \text{Rest } r_3)$
$559 = 3 \cdot 172 + 43$ $(= \text{Rest } r_4)$
$172 = 4 \cdot 43 + 0$ $(= \text{Rest } r_5)$

$\mathrm{ggT}(94729, 93439) = \mathrm{ggT}(93439, 1290) = \mathrm{ggT}(1290, 559) =$
$= \mathrm{ggT}(559, 172) = \mathrm{ggT}(172, 43) = \mathrm{ggT}(43, 0) = 43.$

Satz (6) (Erweiterter Euklid'scher Algorithmus)

Es seien $a, b \in \mathbb{N}$.
Für $i \geq -1$ *und* $j \geq 0$ *werden* $q_j, r_i, x_i, y_i \in \mathbb{N}_0$ *rekursiv definiert durch:*

•) $\quad r_{-1} = a, \; r_0 = b, \; x_{-1} = 1, \; y_{-1} = 0, \; x_0 = 0, \; y_0 = 1$

•) *für* $i \geq 0$*: falls* r_i *(und* $r_{i-1}, x_i, x_{i-1}, y_i, y_{i-1}$*) bereits definiert sind und* $r_i > 0$*:*

$$\begin{aligned} r_{i-1} &= q_i r_i + r_{i+1} \quad \textit{Division von } r_{i-1} \textit{ durch } r_i \textit{ mit Rest} \\ x_{i+1} &= x_{i-1} - q_i x_i \\ y_{i+1} &= y_{i-1} - q_i y_i \end{aligned}$$

Dann existiert ein $n \in \mathbb{N}_0$ *mit* $r_n > 0$ *und* $r_{n+1} = 0$*, und es gilt:*

$$r_n = ggT(a, b) = a x_n + b y_n \; .$$

4.4 Kongruenzen und Restklassen

[A] 12.1, [I-L] 4.4, [L-P-V] 6.7, [St] 3.2.1

Definition (5)

Es sei $m \in \mathbb{Z}$.
Ganze Zahlen $a, b \in \mathbb{Z}$ heißen *zueinander kongruent modulo* (m) (Schreibweise: $a \equiv b \mod (m)$) genau dann, wenn folgende (zueinander äquivalente) Bedingungen erfüllt sind:

(K1) $m \mid (b - a)$

(K2) $\exists\, k \in \mathbb{Z}\colon\, b = a + km$

(K3) Falls $m \neq 0$: sind $q, q' \in \mathbb{Z}$ und $r, r' \in \{0, 1, 2, \ldots, m-1\}$ mit $a = mq + r,\ b = mq' + r'$, so gilt $r = r'$
(d.h.: a und b haben bei Division durch m denselben Rest.)

m heißt der *Modul* der Kongruenz $a \equiv b \mod (m)$.

„Zueinander kongruent sein modulo (m)" definiert eine Äquivalenzrelation auf $\mathbb{Z}$ (vgl. Satz 7.a) unten).

Definition (5) (Fortsetzung)

Für $a \in \mathbb{Z}$ heißt

$$\overline{a} = \{b \in \mathbb{Z} \mid a \equiv b \mod (m)\} = \{a + km \mid k \in \mathbb{Z}\} = a + m\mathbb{Z}$$

die *Restklasse von a modulo* (m).

Jedes Element $c \in \overline{a}$ heißt ein *Repräsentant* der Restklasse $\overline{a} = \overline{c}$.

$\mathbb{Z}/(m) = \{\overline{a} \mid a \in \mathbb{Z}\}$ heißt der *Restklassenring modulo* (m).

Bemerkung:
Für $m \neq 0$ hat der Restklassenring $\mathbb{Z}/(m)$ genau m Elemente:

$$\mathbb{Z}/(m) = \{\overline{r} = r + m\mathbb{Z} \mid 0 \leq r < m\} = \{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{(m-1)}\} .$$

Satz (7)

Es sei $m \in \mathbb{Z}$.

a) *„Zueinander kongruent sein modulo (m)" ist eine Äquivalenzrelation auf $\mathbb{Z}$.*

b) *Sind $a, b, a', b' \in \mathbb{Z}$ mit $a \equiv a' \mod (m)$ und $b \equiv b' \mod (m)$, so gilt:*

(i) $a \pm b \equiv a' \pm b' \mod (m)$ *und* $ab \equiv a'b' \mod (m)$.

(ii) $\forall\, k \in \mathbb{N}: \quad a^k \equiv (a')^k \mod (m)$.

(iii) *Ist $(a, m) \neq (0, 0)$, so gilt* $ggT(a, m) = ggT(a', m)$.

Satz (8)

Es seien $m \in \mathbb{N}$ *und* $a, c \in \mathbb{Z}$.
Dann sind folgende Aussagen äquivalent:

a) *Die Kongruenz* $aX \equiv c \mod (m)$ *ist lösbar, d.h.* $\exists x \in \mathbb{Z}$ *mit* $ax \equiv c \mod (m)$.

b) *Die (lineare) Diophantische Gleichung* $aX + mY = c$ *ist lösbar, d.h.* $\exists (x, y) \in \mathbb{Z}^2$ *mit* $ax + my = c$.

c) $ggT(a, m) \mid c$.

Korollar (2)

Es seien $m \in \mathbb{N}$ und $a \in \mathbb{Z}$. Dann gilt:

a) $\exists\, a' \in \mathbb{Z}$ *mit* $a \cdot a' \equiv 1 \mod (m) \iff ggT(a, m) = 1$
($\iff$ *die Restklasse* $\overline{a}$ *besitzt in* $\mathbb{Z}/(m)$ *ein Inverses bezüglich* $\odot$*:*
$\overline{a} \odot \overline{a'} = \overline{1}$*).*

b) $\exists\, a_0 \in \mathbb{Z}$ *mit* $a_0 \not\equiv 0 \mod (m)$ *und* $a \cdot a_0 \equiv 0 \mod (m) \iff$
$ggT(a, m) > 1$
($\iff \exists\, \overline{a_0} \in \mathbb{Z}/(m)$ *mit* $\overline{a_0} \neq \overline{0}$ *und* $\overline{a} \odot \overline{a_0} = \overline{0}$*; d.h.* $\overline{a}$ *ist ein* *„Nullteiler" in* $\mathbb{Z}/(m)$ *).*

Beispiel 1: Bestimme alle $n \in \mathbb{Z}$, für welche $4n^2 + 3$ durch 7 teilbar ist!
Beispiel 2: Bestimme die Einer- (und die Zehner-)-Ziffer der größten derzeit bekannten (Mersenne-)Primzahl

$$q = 2^{82\,589\,933} - 1 \quad \text{(entdeckt am 7. 12. 2018)} \,.$$