WiSe'21/'22, hhu
K. Halupczok

Vorlesung Einführung in die Zahlentheorie

EZ1: Teilbarkeit

Stichworte: Teiler, Vielfache, Gegenteiler, Gaußklammer, Division mit Rest, kleinster nichtnegativer und absolut kleinster Rest, ggT, teilerfremd, Satz von Bézout, agV

1.1. Einleitung:

Der Gegenstand der Zahlentheorie ist die Untersuchung von $\mathbb{N} = \{1, 2, 3, 4, \dots\}$ bzw. von $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, 4, \dots\}$.
Als Methode wird mindestens die halbe Mathematik eingesetzt.
Wir werden in dieser Vorlesung aber nur Methoden der Linearen Algebra-/Analysis-Grundvorlesung einsetzen, um möglichst elementare Mittel einzusetzen und in die Anfangsgründe der Zahlentheorie einzuführen. Neben der Geometrie ist die Zahlentheorie der älteste Teil der Mathematik. Einerseits sind die ganzen Zahlen begrifflich leicht zugänglich, andererseits bestehen viele höchst schwierige, teilweise ungelöste Probleme, weshalb die Zahlentheorie stets zum bevorzugten Arbeitsgebiet der Mathematiker gehörte (Euler, Gauß, Lagrange, ...). Durch die Entwicklung der Computer sind zahlentheoretische Methoden in den letzten Jahrzehnten für Anwendungen (z.B. Kryptographie, Quantencomputer, KI, Data Science ...) sehr wichtig geworden.

Die Umkehrung der Addition, die Subtraktion, ist im Ring $(\mathbb{Z}, +, \cdot)$ uneingeschränkt ausführbar, wohingegen die Division nicht immer möglich ist. Der grundlegende Begriff hierzu ist der der Teilbarkeit.

1.2. **Def.:** (1) Seien $a, b \in \mathbb{Z}$. Die Zahl a teilt b, falls es ein $c \in \mathbb{Z}$ gibt mit $b = a \cdot c$.
(oder: a ist Teiler von b, b wird von a geteilt, b ist Vielfaches von a)

Kurz: $a \mid b \;:\Leftrightarrow\; \exists c : b = ac$
Andernfalls: $a \nmid b$ (a teilt b nicht).
Die Zahl c in der Gleichung $b = ac$ nennen wir Gegenteiler bzw. Coteiler von a.
(2) $a \in \mathbb{Z}$ heißt echter Teiler von $b \in \mathbb{Z}$, falls $a \mid b$ und $|a| < |b|$ gelten.
Dann heißt b echtes Vielfaches von a.

1.3. Bsp.: $1 \mid 5$, $5 \mid 5$, $2 \nmid 5$, $10 \mid 0$, $-2 \mid 6$, $0 \mid 0$, $\forall a \neq 0 : 0 \nmid a$

1.4. Folgerung (triviale Teilbarkeitsregeln): Für alle $a, b, c \in \mathbb{Z}$ gilt:

(1) $a \mid b \Rightarrow \forall z \in \mathbb{Z} : a \mid (bz)$

(2) $a \mid b \wedge b \mid c \Rightarrow a \mid c$

(3) $a \mid b \wedge a \mid c \Rightarrow \forall x, y \in \mathbb{Z} : a \mid (xb + yc)$

(4) $a \mid b \wedge b \mid a \Rightarrow |a| = |b|$

(5) $a \mid b \wedge b \neq 0 \Rightarrow |a| \leq |b|$

(6) $a \mid b \Rightarrow \forall z \in \mathbb{Z} : (za) \mid (zb)$.

Bew.: Von (4): Es gibt ein $c_1 \in \mathbb{Z}$ und ein $c_2 \in \mathbb{Z}$ mit $b = c_1 a$ und $a = c_2 b$.
Also ist $b = c_1 c_2 b$. Im Fall $b = 0$ folgt $a = 0$. Im Fall $b \neq 0$ folgt $c_1 c_2 = 1$,
also $c_1, c_2 \in \{-1, 1\}$. □

1.5. Def. (Gaußklammer): Die Abbildung
$\lfloor \cdot \rfloor : \mathbb{R} \to \mathbb{Z}$, $t \mapsto \lfloor t \rfloor := \max \{a \in \mathbb{Z} : a \leq t\}$ heißt
Gaußklammer bzw. Gaußsche Größte-Ganze-Funktion. (Andere Notation: $[t]$)
Die ganze Zahl $\lfloor t \rfloor$ ist die größte ganze Zahl kleiner oder gleich $t \in \mathbb{R}$.
Kurz: Größtes Ganzes von t oder Gaußklammer von t.

1.6. Bsp.: $\lfloor a \rfloor = a$ für alle $a \in \mathbb{Z}$, $\lfloor \pi \rfloor = 3$, $\lfloor -\pi \rfloor = -4$.

1.7. Satz (Division mit Rest): (1) $\forall a \in \mathbb{Z}\ \forall n \in \mathbb{N}\ \exists r \in \mathbb{N}_0$ mit $r < n$: $a = \lfloor \frac{a}{n} \rfloor n + r$.
("Division von a durch n", $\lfloor \frac{a}{n} \rfloor$ ist "Quotient" dabei, r heißt "Rest")

(2) In der Darstellung $a = bn + r$ mit $b \in \mathbb{Z}$, $r \in \mathbb{N}_0$ und $r < n$
sind b und r für alle $a \in \mathbb{Z}$ und alle $n \in \mathbb{N}$ eindeutig festgelegt.

Bew.: Nach Def. von $\lfloor \cdot \rfloor$ ist $\lfloor \frac{a}{n} \rfloor \leq \frac{a}{n} < \lfloor \frac{a}{n} \rfloor + 1$, also $0 \leq a - \lfloor \frac{a}{n} \rfloor n < n$.
Dies ist die Ungleichung für r und es folgt Beh. (1).

(2): Seien $a \in \mathbb{Z}$, $n \in \mathbb{N}$. Es ex. $b \in \mathbb{Z}$, $r \in \mathbb{N}_0$ mit $a = bn + r$ und $r < n$.
Seien $b' \in \mathbb{Z}$, $r' \in \mathbb{N}_0$ mit $a = b'n + r'$ und $r' < n$.
Also ist $0 = (b - b')n + (r - r')$ mit $-n < r - r' < n$, so dass $b = b'$, $r = r'$. □

1.8. **Bem.:** Das zu $a \in \mathbb{Z}$, $n \in \mathbb{N}$ eind. bestimmte $r \in \mathbb{N}_0$ in Satz 1.7 heißt der Kleinste nichtnegative Rest von a bei Division durch n.
Es kann r auch durch die Forderung $|r| \leq \frac{n}{2}$ (absolut Kleinster Rest) festgelegt werden; dann ist es nicht immer eindeutig festgelegt.
Bsp.: $30 = 7 \cdot 4 + 2 = 8 \cdot 4 - 2$.

1.9. **Def.** (gemeinsame Teiler):
Für diese Def. seien $a, b \in \mathbb{Z}$, $n \in \mathbb{N} \setminus \{1\}$, und $a_j \in \mathbb{Z}$ für alle $j \in \mathbb{N}$ mit $j \leq n$.
(1) d heißt gemeinsamer Teiler von a und b, falls $d \mid a$ und $d \mid b$.
(2) Ist $a^2 + b^2 \neq 0$, so heißt $ggT(a,b) := \max\{c \in \mathbb{N};\ c \mid a \text{ und } c \mid b\} \in \mathbb{N}$.
größter gemeinsamer Teiler von a und b. Kurz: $(a,b) := ggT(a,b)$.
(3) Ist $a \neq 0$, so sei $ggT(a) := |a|$.
Sind $n \neq 2$ und $\sum_{j=1}^{n-1} a_j^2 \neq 0$, so seien $ggT(a_1, \dots, a_n) := ((a_1, \dots, a_{n-1}), a_n)$
und $ggT(0, \dots, 0, a_n) := |a_n|$, falls $a_n \neq 0$ ist.
Kurz: $(a_1, \dots, a_n) := ggT(a_1, \dots, a_n)$.
Sind $n \neq 2$ und $\sum_{j=1}^{n-1} a_j^2 \neq 0$, so heißt $ggT(a_1, \dots, a_n)$ größter gemeinsamer Teiler von $a_1, \dots, a_n$.
(4) a und b heißen teilerfremd (selten: relativ prim, engl.: relatively prime), wenn $(a,b) = 1$ und $a^2 + b^2 \neq 0$ sind.
$a_1, \dots, a_n$ heißen teilerfremd, wenn $(a_1, \dots, a_n) = 1$ und $\sum_{j=1}^{n} a_j^2 \neq 0$ sind.

$a_1, \dots, a_n$ heißen paarweise teilerfremd, wenn $\#\{j \in \mathbb{N};\ j \leq n \text{ und } a_j = 0\} \leq 1$ und $(a_j, a_k) = 1$ für alle $j, k \in \mathbb{N}$ mit $j < k \leq n$ gilt.

1.10. **Bem.:** Aus der paarweisen Teilerfremdheit folgt die Teilerfremdheit.
Die Umkehrung muss nicht gelten.

1.11. **Bsp.:** $(-2,6) = 2$, $(3,7) = 1$, $(2,6,7) = 1$, $(2,6) = 2$, $(2,7) = 1$, $(6,7) = 1$
2, 6, 7 sind teilerfremd, aber nicht paarweise teilerfremd.

1.12. Bem.: Um praktische Rechenregeln für die Teilbarkeit formulieren zu können, wird bereits der folgende Satz (mit etwas Tiefgang) benutzt. Wir zeigen ihn erst später in EZ3.

1.13. Satz (Bézout, Darstellung des ggT als $\mathbb{Z}$-Linearkombination):
Seien $n \in \mathbb{N}$ und $a_1, \dots, a_n \in \mathbb{Z}$ mit $\sum_{j=1}^{n} a_j^2 \neq 0$.
Dann ist $(a_1, \dots, a_n) = \min\{d \in \mathbb{N};\ \exists z_1, \dots, z_n \in \mathbb{Z} : d = z_1 a_1 + \dots + z_n a_n\}$.
Die Koeffizienten $z_1, \dots, z_n$ in einer solchen Darstellung des ggT von $a_1, \dots, a_n$ heißen Bézout-Koeffizienten.

1.14. Folgerung: Seien $a, b \in \mathbb{Z}$ mit $a^2 + b^2 \neq 0$, seien $a_1, \dots, a_n \in \mathbb{Z}$ mit $\sum_{j=1}^{n} a_j^2 \neq 0$ und sei $d \in \mathbb{N}$ und $\sigma : \{1, \dots, n\} \to \{1, \dots, n\}$ bijektiv (d.h. σ ist eine Permutation von $\{1, \dots, n\}$).
Dann gilt:
(1) $d = (a,b) \Leftrightarrow d \mid a \wedge d \mid b \wedge \forall c \in \mathbb{N} : (c \mid a \wedge c \mid b \Rightarrow c \mid d)$,
(2) $(ca, cb) = |c|(a,b)$ für alle $c \in \mathbb{Z} \setminus \{0\}$,
(3) $(a_1, \dots, a_n) = (a_{\sigma(1)}, \dots, a_{\sigma(n)})$.

Bew.: (1)„⇒": Es gelte $d = (a,b)$, so dass $d \mid a$ und $d \mid b$ folgt. Nach Satz 1.13 (Bézout) gibt es $z_1, z_2 \in \mathbb{Z}$ mit $d = z_1 a + z_2 b$.
Für alle $c \in \mathbb{Z}$ mit $c \mid a$ und $c \mid b$ gibt es $d_1, d_2 \in \mathbb{Z}$ mit $a = d_1 c$ und $b = d_2 c$.
Daraus folgt $d = z_1 a + z_2 b = z_1 d_1 c + z_2 d_2 c = (z_1 d_1 + z_2 d_2) c$.
Also ist c auch ein Teiler von d für alle $c \in \mathbb{Z}$ mit $c \mid a$ und $c \mid b$.
(1)„⇐": Es gelte $d \mid a$, $d \mid b$ und $c \mid d$ für alle $c \in \mathbb{Z}$ mit $c \mid a$ und $c \mid b$.
Sei $c' := \max\{c \in \mathbb{N};\ c \mid a \text{ und } c \mid b\}$. Dann ist $c' = (a,b)$ nach Def. 1.9(2).
Nach Vor. ist $c' \mid d$. Wegen $d \mid a$, $d \mid b$ und $d \in \mathbb{N}$ ist aber $d \leq c'$ nach Def. von c'.
Damit folgt $d = c' = (a,b)$.
(2): Sei $c \in \mathbb{Z} \setminus \{0\}$ und $d = (a,b)$. Zu zeigen ist also $|c| d = (ac, bc)$.
Bézout! → Nach Satz 1.13 (Bézout) gibt es $z_1, z_2 \in \mathbb{Z}$ mit $d = z_1 a + z_2 b$, $d \mid a$ und $d \mid b$.
Nach Folgerung 1.4(6) ist $|c| d$ ein Teiler von $a|c|$ und von $b|c|$.
Dann teilt $|c| d$ aber auch ac und bc.
Sei $e \in \mathbb{Z}$ mit $e \mid (ac)$ und $e \mid (bc)$. Dann teilt e auch $|c| d$
$= |c| \cdot (z_1 a + z_2 b) = z_1 a |c| + z_2 b |c| = \operatorname{sign}(c)\, z_1 ac + \operatorname{sign}(c)\, z_2 bc$. Nach (1) ist $|c| d = (a,b)$.
(3): $(a_1, \dots, a_n) = (a_{\sigma(1)}, \dots, a_{\sigma(n)})$ ist klar nach Satz 1.13 (Bézout). □

1.15. **Bem.:** 1.14 (1) kann auch so ausgedrückt werden:
Für $a \in \mathbb{Z}$ sei $T(a) := \{c \in \mathbb{Z};\ c \mid a\}$ die Menge der Teiler von a.
Haben $T(0) = \mathbb{Z}$, $\#T(a) < \infty$ für alle $a \in \mathbb{Z} \setminus \{0\}$.
Es gilt für alle $a, b \in \mathbb{Z}$ mit $a^2 + b^2 \neq 0$: $T(a) \cap T(b) = T((a,b))$.
1.14(3) bedeutet, dass es zur Berechnung eines größten gemeinsamen Teilers von beliebig (endlich) vielen Zahlen nicht auf ihre Reihenfolge ankommt.

1.16. **Lemma (Gauß-Lemma):** Seien $a, b, c \in \mathbb{Z}$. Dann:
(1) Aus $(a,c) = (b,c) = 1$ folgt $(ab, c) = 1$, sofern $a^2 + c^2 + 0 \neq b^2 + c^2$ ist.
(2) Aus $c \mid ab$ und $(c,a) = 1$ folgt $c \mid b$.
(Bezout!) $(c \neq 0) \to$ 1.14(2) $= 1$
Bew.: (2): Haben $c \mid cb$. Gilt $c \mid ab$ und $(c,a) = 1$, folgt $c \mid (cb, ab) = |b| \cdot (c,a) = |b|$, also $c \mid b$.
(1): Sei $(a,c) = (b,c) = 1$, $d := (ab, c)$. Mit 1.14.(1) folgt $d \mid (ab, ac)$ wegen $d \mid ab$, $d \mid c$, $d \mid ac$.
Mit 1.14(2) folgt $(ab, ac) = |a| \cdot (b,c) = |a|$, und somit ist $d \mid a$.
Mit $d \mid c$ und 1.14.(1) folgt $d \mid (a,c)$. Wegen $(a,c) = 1$ bleibt nur $d = 1$. □

1.17. **Def. (Kleinstes gemeinsames Vielfaches):** Sind $n \in \mathbb{N}$, $a_1, \dots, a_n \in \mathbb{Z} \setminus \{0\}$, so heißt $kgV(a_1, \dots, a_n) := \min\{m \in \mathbb{N};\ \forall j \in \{1, \dots, n\} : a_j \mid m\}$
Kleinstes gemeinsames Vielfaches von $a_1, \dots, a_n$.
Kurz: $[a_1, \dots, a_n] := kgV(a_1, \dots, a_n)$.

1.18. **Hinweis:** Wird die Gauß-Klammer mit $[\,]$ geschrieben, darf diese nicht mit dem kgV im Fall $n = 1$ verwechselt werden. Für alle $a_1 \in \mathbb{N}$ ist $kgV(-a_1) = a_1$, aber $[-a_1] = -a_1$.

1.19. **Satz (über das kgV):** Seien $n \in \mathbb{N}$, $a_1, \dots, a_n \in \mathbb{Z} \setminus \{0\}$, $b \in \mathbb{Z}$. Dann:
(1) b ist gemeinsames Vielfaches von $a_1, \dots, a_n$ (d.h. $a_1 \mid b$, $a_2 \mid b$, …, $a_n \mid b$) genau dann, wenn b Vielfaches von $[a_1, \dots, a_n]$ ist.
(2) Es ist $[a_1, a_2] \cdot (a_1, a_2) = |a_1 a_2|$, falls $n = 2$ ist.

1.20. **Bem.:** Folgerung 1.4.(a) und Satz 1.19 entsprechen einander:
a) $\{d \in \mathbb{Z};\ d \mid a_1 \wedge \dots \wedge d \mid a_n\} = \{d \in \mathbb{Z};\ d \mid (a_1, \dots, a_n)\}$,
b) $\{v \in \mathbb{Z};\ a_1 \mid v \wedge \dots \wedge a_n \mid v\} = \{v \in \mathbb{Z};\ [a_1, \dots, a_n] \mid v\}$.

Bew. (von 1.19): (2): Sei $n=2$, und $m \in \mathbb{N}$ ein Vielfaches von a_1 und a_2.
Dann gibt es ein $b \in \mathbb{Z}$ mit $m = a_1 b$ und m ist zugleich Vielfaches von a_2.
Damit folgt $k := \frac{m}{a_2} = \frac{a_1 b}{a_2} \in \mathbb{Z}$.
Seien $d := (a_1, a_2)$, $c_1 := \frac{a_1}{d}$ und $c_2 := \frac{a_2}{d}$. Nach 1.14 (2) ist $(c_1, c_2) = 1$.
Dies ergibt $k = \frac{a_1 b}{a_2} = \frac{c_1 b}{c_2}$, also $c_2 \mid c_1 b$.
Wegen $(c_2, c_1) = 1$ und Lemma 1.16 (2) (Gauß) folgt $c_2 \mid b$,
und es gibt ein $c \in \mathbb{Z}$ mit $b = c_2 c$.
Es folgt $m = a_1 b = a_1 c_2 c = \frac{a_1 a_2}{d} \cdot c$.
Also wird jedes gemeinsame Vielfache von a_1 und a_2 von $\frac{a_1 a_2}{(a_1, a_2)}$ geteilt.
Das kleinstmögliche gemeinsame Vielfache von a_1 und a_2 ist damit $\frac{|a_1 a_2|}{(a_1, a_2)}$.
Es folgt Beh. (2).

(1): Die letzten Überlegungen beinhalten Aussage (1) für $n=2$. Für $n=1$ ist sie trivial.
Die Erweiterung auf $n>2$ erfolgt induktiv. Man erhält wie beim ggT die Rekursion

$$[a_1, \dots, a_n] = [[a_1, \dots, a_{n-1}], a_n].$$

□

1.21. Bem.: Satz 1.20 (2) gilt i.a. nicht für $n \geq 3$. Richtig ist dagegen:
$a_1, \dots, a_n$ sind genau dann paarweise teilerfremd, wenn $[a_1, \dots, a_n] = |a_1 \cdots a_n|$.

Bew.: „$\Rightarrow$": Per Induktion: Der Induktionsanfang ist mit $n=2$ die Aussage von 1.20 (2).
Mit der Induktionsvoraussetzung und Satz 1.20 (2) folgt für $n \geq 2$:

$$[a_1, \dots, a_{n+1}] = [[a_1, \dots, a_n], a_{n+1}] = [|a_1 \cdots a_n|, a_{n+1}]$$
$$= \underbrace{\frac{1}{(|a_1 \cdots a_n|, a_{n+1})}}_{=1} \cdot |a_1 \cdots a_n \cdot a_{n+1}| = |a_1 \cdot \dots \cdot a_{n+1}|.$$

„$\Leftarrow$": Per Induktion: Der Induktionsanfang ist mit $n=2$ die Aussage von 1.20 (2).
Mit der Voraussetzung und Satz 1.20 (2) folgt für $n \geq 2$:

$$|a_1 \cdots a_{n+1}| = [a_1, \dots, a_{n+1}] = [[a_1, \dots, a_n], a_{n+1}] = \frac{|[a_1, \dots, a_n]| \cdot |a_{n+1}|}{([a_1, \dots, a_n], a_{n+1})}.$$

Das heißt $([a_1, \dots, a_n], a_{n+1}) \cdot |a_1 \cdots a_n| = [a_1, \dots, a_n]$.
Also ist $|a_1 \cdots a_n|$ Teiler von $[a_1, \dots, a_n]$. Da $|a_1 \cdots a_n|$ Vielfaches aller $a_1, \dots, a_n$ ist,
ist $|a_1 \cdots a_n| \geq [a_1, \dots, a_n]$. Es bleibt nur $|a_1 \cdots a_n| = [a_1, \dots, a_n]$. Damit folgt $([a_1, \dots, a_n], a_{n+1}) = 1$.
Das heißt insbesondere $(a_j, a_{n+1}) = 1$ für alle $j \in \{1, \dots, n\}$. Nach Induktionsvoraussetzung folgt aus
$|a_1 \cdots a_n| = [a_1, \dots, a_n]$ außerdem $(a_j, a_k) = 1$ für alle $j, k \in \{1, \dots, n\}$ mit $j \neq k$.

□