W.Se'21/'22, hhu
K. Halupczok

Vorlesung Einführung in die Zahlentheorie

EZ3: Euklidischer Algorithmus

Stichworte: Bézout-Identität, Euklidischer Algorithmus, explizite ggT-Berechnung und Berechnung der Bézout-Koeffizienten, lineare diophantische Gleichung, endlicher Kettenbruch

---

3.1. Einleitung:
Das Lemma von Bézout spielt bereits für den Hauptsatz der Arithmetik eine wesentliche Rolle (das Euklid-Lemma kommt ohne ihm nicht aus). Dafür nicht bereits die reine Existenzaussage der Bézout-Koeffizienten. Wir werden in diesem Kapitel aber darüberhinaus untersuchen, wie diese explizit berechnet werden können. Dies führt auf den euklidischen Algorithmus und eine Verallgemeinerung davon, und hängt eng mit der Theorie endlicher Kettenbrüche zusammen, vgl. EZ4.

3.2. Lemma von Bézout / Bézout-Identität: Seien $a,b \in \mathbb{Z}$ mit $a^2+b^2 \neq 0$.
$\mathbb{Z}a+\mathbb{Z}b = \mathbb{Z}(a,b)$
Dann gibt es $x,y \in \mathbb{Z}$ mit $(a,b) = xa+yb$. [Und es ist $\min\{xa+yb;\ x,y\in\mathbb{Z}\} \cap \mathbb{N} = (a,b)$.]

Bew.: 1. Sei $\mathcal{D}(a,b) := \{xa+yb;\ x,y\in\mathbb{Z}\}$, diese Menge enthält natürliche Zahlen.
[Denn falls $a>0$, ist $1\cdot a + 0\cdot b > 0$, für $a<0$ ist $(-1)\cdot a + 0\cdot b > 0$, ebenso für $b\neq 0$ argumentiert, wenn $a=0$ sein sollte.] Daher existiert darin eine kleinste natürliche Zahl, etwa
$g := \min\{n\in\mathcal{D}(a,b);\ n\geq 1\}$ mit $g = x_0 a + y_0 b$ für $x_0, y_0 \in \mathbb{Z}$.
2. Dann ist $g \mid a$. [Denn Div. mit Rest 1.7.(1) zeigt $a = qg + r$ mit $0 \leq r < g$, für den Rest r gilt aber $r = 1\cdot a + (-q)\cdot g = 1\cdot a + (-q)(x_0 a + y_0 b)$
$= (1-qx_0)a + (-qy_0)b \in \mathcal{D}(a,b)$, die minimale Wahl von g erzwingt dann $r=0$.]
3. Analog ist $g \mid b$.
4. Es folgt $g \leq (a,b)$, da (a,b) der größte gemeinsame Teiler von a und b ist
5. Mit $(a,b)\cdot a_0 = a$ und $(a,b)\cdot b_0 = b$ folgt $g = x_0 a + y_0 b = (x_0 a_0 + y_0 b_0)\cdot (a,b)$, also auch $(a,b) \mid g$, bzw. $(a,b) \leq g$. Mit 4. folgt $(a,b) = g = \min\{n\in\mathcal{D}(a,b);\ n\geq 1\}$.

□

3.3. Bem.: Der Beweis benutzt nur die Division mit Rest und die Definitionen von "Teiler" und "ggT". Keine Folgerungen des Lemmas / Satz 1.13, wie etwa 1.14(1), sind hier verwendet worden.

3.4. Bem.: Die Version in Satz 1.13. lässt sich nun mit einer Induktion aus 3.2 herleiten.
Dazu nochmals die Version des Satzes 1.13 im Wortlaut:

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 $(a_1, \dots, a_n) = \min\{d \in \mathbb{N};\ \exists z_1, \dots, z_n \in \mathbb{Z} : d = z_1 a_1 + \dots + z_n a_n\}$.

3.5. Bew.:

Induktion nach n: Für $n=1$ ist die Beh. $(a_1) = |a_1| = \min \mathbb{N} \cap \mathbb{Z} a_1$ klar,
für $n=2$ ist die Beh. genau die Aussage von Lemma 3.2.
Sei die Beh. wahr für ein $n \in \mathbb{N}$ mit $n \geq 2$. Seien $a_1, \dots, a_{n+1} \in \mathbb{Z}$ mit $\sum_{j=1}^{n+1} a_j^2 \neq 0$.

1. Fall: $a_1 = \dots = a_n = 0$. Dann muss $a_{n+1} \neq 0$ sein, und haben $(0, \dots, 0, a_{n+1}) = |a_{n+1}| = \min \mathbb{N} \cap \mathbb{Z} a_{n+1}$.

2. Fall: $\sum_{j=1}^{n} a_j^2 \neq 0$, und die Induktionsvor. kann auf $a_1, \dots, a_n$ angewendet werden.
Nach dieser ist $d_n := (a_1, \dots, a_n) = \tilde{x}_1 a_1 + \dots + \tilde{x}_n a_n$ für $\tilde{x}_1, \dots, \tilde{x}_n \in \mathbb{Z}$.
Dann ist $(a_1, \dots, a_n, a_{n+1}) \overset{1.9.(3)}{=} ((a_1, \dots, a_n), a_{n+1}) = (d_n, a_{n+1}) = x d_n + \tilde{x}_{n+1} a_{n+1}$ $\overset{3.2}{=}$ für $\tilde{x}_{n+1}, x \in \mathbb{Z}$.
Weiter ist $(a_1, \dots, a_n, a_{n+1}) = x(\tilde{x}_1 a_1 + \dots + \tilde{x}_n a_n) + \tilde{x}_{n+1} a_{n+1} \in \mathbb{N}$.

- Ist nun k das Minimum $k := \min \mathbb{N} \cap \{x_1 a_1 + \dots + x_{n+1} a_{n+1};\ x_1, \dots, x_{n+1} \in \mathbb{Z}\}$,
so folgt $0 < k \leq (a_1, \dots, a_{n+1}) =: d_{n+1}$.
- Da umgekehrt $d_{n+1} | a_1, \dots, d_{n+1} | a_{n+1}$ gilt,
etwa $a_1 = \hat{a}_1 d_{n+1}, \dots, a_{n+1} = \hat{a}_{n+1} d_{n+1}$, folgt $k = (x_1 \hat{a}_1 + \dots + x_{n+1} \hat{a}_{n+1}) \cdot d_{n+1}$ für $x_1, \dots, x_{n+1} \in \mathbb{Z}$, also
$d_{n+1} | k$ bzw. $d_{n+1} \leq k$.
- Daher kann nur $d_{n+1} = k$ sein. □

3.6. Bem.: Der Beweis ist ein reiner Existenzbeweis, es gibt keinerlei Aufschluss, wie die Bézout-Koeffizienten explizit berechnet werden können.
Deswegen benötigen wir einen schärferen Beweis, der uns sogar eine Konstruktionsvorschrift liefern kann. Dies gelingt mit dem euklidischen Algorithmus, dem ersten nicht auf der Hand liegenden algorithmischen Verfahren der Mathematik.

3.7. **Satz (Euklidischer Algorithmus):** Seien $a, b \in \mathbb{Z} \setminus \{0\}$, führen sukzessive, d.h. fortlaufend, eine Division mit Rest durch: Setze $r_{-1} := b$, $r_0 := a$.

"b durch a"

Ist $r_i \neq 0$, so sei r_{i+1} (der) bei der Division von r_{i-1} (geteilt) durch r_i auftretende Rest, d.h. $\boxed{r_{i-1} = q_i r_i + r_{i+1}}$ mit $0 \leq r_{i+1} < r_i$.
(und q_i der Quotient)

für $i = 0, 1, 2, 3, \ldots$

Ist dann n der größte Index mit $r_n \neq 0$, so ist $r_n = (a, b)$, d.h. der letzte Rest $\neq 0$ ist größter gemeinsamer Teiler von a und b.

Bew.: • OE sei $b \geq a$. Laut Satz 1.7.(1) (Div. mit Rest) haben wir dann

$$b \geq a > r_1 > r_2 > \ldots \geq 0.$$

Der Algorithmus bricht jedenfalls ab.

$r_n \mid r_{n-1}, r_{n-2}, \ldots, a, b$

• Sei nun r_n der letzte nichtverschwindende Rest bei dieser Kette von Divisionen. Dann haben wir

$$\begin{aligned} b &= q_0 \cdot a + r_1 && \leftarrow \text{bzw. } r_{-1} = q_0 r_0 + r_1 \\ a &= q_1 r_1 + r_2 && \leftarrow \text{bzw. } r_0 = q_1 r_1 + r_2 \\ r_1 &= q_2 r_2 + r_3 && \\ &\vdots && \\ r_{n-2} &= q_{n-1} r_{n-1} + r_n && \leftarrow \text{Letzter Rest} \neq 0, \\ r_{n-1} &= q_n r_n && \leftarrow \text{geht restlos auf, d.h. } r_{n+1} = 0. \end{aligned}$$

Damit ist $r_n \mid r_{n-1}$, denn mit $s_{n-1} := q_n$ gilt $r_{n-1} = s_{n-1} r_n$.

Weiter: $r_n \mid r_{n-2}$, denn $r_{n-2} = q_{n-1} r_{n-1} + r_n = \underbrace{(q_{n-1} s_{n-1} + 1)}_{=: s_{n-2}} r_n$,

weiter $r_n \mid r_{n-3}, \ldots$ Die Fortsetzung/Iteration dieses Schlusses zeigt dann $r_n \mid r_0$ und $r_n \mid r_{-1}$, d.h. r_n ist gemeinsamer Teiler von a und b.

$d \mid a \wedge d \mid b$ $\Rightarrow d \mid r_1, r_2, \ldots, r_n$

• Ist nun d (irgend) ein gemeinsamer Teiler von a und b, so ex. ganze Zahlen s_1, s_2 mit $b = s_1 d$, $a = s_2 d$. Dann ist $r_1 = r_{-1} - q_0 r_0 = s_1 d - s_2 d q_0$, also $r_1 = (s_1 - s_2 q_0) \cdot d$, d.h. $d \mid r_1$.

Wenden wir dies auf r_0, r_1 an, folgt wie eben $d \mid r_2$, dann $d \mid r_3$ usw.

Durch Fortsetzung/Iteration dieses Schlusses folgt: $d \mid r_n$.

$\Rightarrow r_n = (a, b)$

• Also gilt: 1.) $r_n \mid a$, $r_n \mid b$, 2.) $d \mid a \wedge d \mid b \Rightarrow d \mid r_n$.

Nach Folgerung 1.14 (1) „$\Leftarrow$", die ohne Bézout auskommt (!), folgt $r_n = (r_{-1}, r_0) = (a, b)$. $\square$

3.8 Bem.: Der euklidische Algorithmus kann - anstelle dem kleinsten nicht negativen Rest - auch mit dem absolut kleinsten Rest bei den Divisionen benutzt werden, bzw. diese können sogar gemischt werden. Der Vorteil ist, dass die Rechnungen meist kürzer/schneller sind.

Bsp.:

$b \quad a$
$r_{-1} = q_0 r_0 + r_1$,
$r_0 = q_1 r_1 + r_2$
$r_1 = q_2 r_2 + r_3$
$\vdots$
letzter Rest $\neq 0$ sei $r_m \rightsquigarrow r_m = (a,b)$

$b \quad a$
$12378 = 4 \cdot 3054 + 162 \rightarrow r_1 < r_0$
$3054 = 18 \cdot 162 + 138 \rightarrow r_2 < r_1$
$162 = 1 \cdot 138 + 24$
$138 = 5 \cdot 24 + 18$
$24 = 1 \cdot 18 + \underline{6} \rightsquigarrow r_5 < r_4 \rightsquigarrow r_5 = 6 = ggT(12378, 3054)$.
$18 = 3 \cdot 6$
$r_6 = 0$

Kürzer:
$12378 = 4 \cdot 3054 + 162 \rightarrow |r_1| < |r_0|/2$
$3054 = 19 \cdot 162 - 24 \rightsquigarrow |r_2| < |r_1|/2$
$162 = 7 \cdot 24 - \underline{6} \rightarrow |r_3| < |r_2|/2$, $|r_3| = 6 = ggT(12378, 3054)$.
$24 = 4 \cdot 6$
$r_4 = 0$

3.9. Konstruktion von Bézout-Koeffizienten in Lemma 3.2 (Bézout-Identität):
Seien $a, b \in \mathbb{Z}$ mit $a^2 + b^2 \neq 0$. Geben ein Verfahren zur Konstruktion von $x, y \in \mathbb{Z}$ mit $(a,b) = xa + yb$ an durch Verwendung von Satz 3.7 (euklidischer Algorithmus):

Sei $d := r_n$ der letzte im euklidischen Algorithmus 3.7 Rest $\neq 0$, also $d = (a,b)$, und wir haben eine Darstellung $d = r_n = r_{n-2} - q_{n-1} r_{n-1}$ das ist eine "Linear-"Kombination von r_{n-2} und r_{n-1}.

Anstelle r_{n-1} setzen wir darin jetzt $r_{n-1} = r_{n-3} - q_{n-2} r_{n-2}$ ein und können so r_{n-1} eliminieren. Dann erhalten wir

$$d = r_n = r_{n-2} - q_{n-1} \cdot (r_{n-3} - q_{n-2} r_{n-2})$$
$$= (-q_{n-1}) \cdot r_{n-3} + (1 + q_{n-1} q_{n-2}) \cdot r_{n-2},$$

also eine "Linear-"Kombination von r_{n-3} und r_{n-2}.

Dies wird wieder fortgesetzt/iteriert, bis nur noch eine "Linear-"Kombination von $r_0 = a$ und $r_1 = b$ auftritt, in der man x und y ablesen kann (die nicht eindeutig bestimmt sind! Zur Lösungsmenge vgl. 3.13.)

Man kann x, y durch sukzessives Durchgehen "von unten nach oben" in einem Eukl.-Algo-Rechenschema explizit berechnen.

3.10. **Bsp.:** Die Gln. in 3.8, in umgekehrter Reihenfolge:

$$24 = 18\cdot 1 + \textcircled{6}$$
$$138 = 24\cdot 5 + 18$$
$$162 = 138\cdot 1 + 24$$
$$3054 = 162\cdot 18 + 138$$
$$12378 = 3054\cdot 4 + 162$$

Reste einsetzen

Schreiben der ⑥ als Linearkombination:

$$\textcircled{6} = 24 - 18$$
$$= 24 - (138 - 5\cdot 24) = 6\cdot 24 - 138$$
$$= 6\cdot(162 - 1\cdot 138) - 138 = 6\cdot 162 - 7\cdot 138$$
$$= 6\cdot 162 - 7\cdot(3054 - 18\cdot 162) = 132\cdot 162 - 7\cdot 3054$$
$$= 132\cdot(12378 - 4\cdot 3054) - 7\cdot 3054$$
$$= \underbrace{132}_{y}\cdot\underbrace{12378}_{b} + \underbrace{(-535)}_{x}\cdot\underbrace{3054}_{a}.$$

3.11. **Bem.:**
- Der rechentechnische Vorteil des Verfahrens ist es, dass die Zahlen a, b und andere niemals gemäß ihrer PFZ faktorisiert werden müssen.
- Außerdem ist es sehr schnell, vgl. EZ5, und leicht zu implementieren.
- Rechnungen von Hand sind damit eher fehleranfällig. In EZ4 lernen wir eine Verallgemeinerung kennen, die die Bestimmung von Bézout-Koeffizienten erleichtert.

Neben der Berechnung von ggT's und Bézout-Koeffizienten kann der euklidische Algorithmus zur Lösung linearer diophantischer Gleichungen angewendet werden.

3.12. **Def.:** Eine Gleichung der Form $ax+by=c$ mit $a,b,c\in\mathbb{Z}$ mit $a\neq 0\neq b$ heißt Lineare diophantische Gleichung. Gesucht sind alle Lösungspaare $(x,y)\in\mathbb{Z}^2$.

3.13. **Satz:** Seien $a,b,c\in\mathbb{Z}$ mit $(a,b)=1$. (1) Es gibt dann ganze Zahlen $x_0,y_0\in\mathbb{Z}$ mit $ax_0+by_0=c$. (2) Sei $L=\{(x,y)\in\mathbb{Z}^2;\ ax+by=c\}$.
Dann gilt $L=\{(x_0-tb,\ y_0+ta);\ t\in\mathbb{Z}\}$.

Bew.: ⑪ Blatt 3

3.14. **Kor.:** (1) Die lineare diophantische Gleichung $ax+by=c$ hat genau dann (mind.) eine Lösung, wenn $(a,b)\mid c$. (2) Ist $x_0,y_0\in\mathbb{Z}$ ein spezielles Lösungspaar, dann haben alle anderen Lösungspaare die Form $x=x_0-\frac{b}{(a,b)}t$, $y=y_0+\frac{a}{(a,b)}t$ für $t\in\mathbb{Z}$.

Bew.: (1): Ex. eine Lösung x,y, gilt $(a,b)\mid ax+by=c$. Ist umgekehrt $(a,b)\mid c$, so ist die Glg. äquivalent zu $\underbrace{\frac{a}{(a,b)}}_{=:a'}x+\underbrace{\frac{b}{(a,b)}}_{=:b'}\cdot y=\underbrace{\frac{c}{(a,b)}}_{=:c'}$, die wegen $(a',b')=1$ Lösungen besitzt laut Satz 3.13.

(2): Klar für die Glg. $a'x+b'y=c'$ nach 3.13, somit auch für $ax+by=c$. □

3.15. **Bem.:** In jedem dieser Fälle genügt es, irgendein Lösungspaar zu finden. Dies kann durch die explizite Berechnung von Bézout-Koeffizienten geschehen. Dadurch kann die gesamte Lösungsmenge wie in 3.13 und 3.14 aufgestellt werden. Falls außerdem Lösungspaare in bestimmten Intervallen oder in $\mathbb{N}^2$ etc. gesucht sind, können diese dann innerhalb der Lösungsmenge ermittelt werden.

Um die Konstruktion von Bézout-Koeffizienten wie in EZ4 zu motivieren, betrachten wir die Rechnung mit dem euklidischen Algorithmus von einem anderen Standpunkt.

3.16. Bsp.: Betrachte $a=84$, $b=133$.

$b=$ $133 = 1\cdot 84 + 49$

$a=$ $84 = 1\cdot 49 + 35$

$r_1=$ $49 = 1\cdot 35 + 14$

$r_2=$ $35 = 2\cdot 14 + 7$

$r_3=$ $14 = 2\cdot 7$ Somit $n=4$, $r_4=7$ und $(133,84)=7$.

Dann: $7 = 1\cdot 35 - 2\cdot 14 = 1\cdot 35 - 2\cdot(1\cdot 49 - 1\cdot 35) = 3\cdot 35 - 2\cdot 49$

$= 3\cdot(84 - 1\cdot 49) - 2\cdot 49 = 3\cdot 84 - 5\cdot 49 = 3\cdot 84 - 5\cdot(133 - 1\cdot 84)$

$= 8\cdot 84 - 5\cdot 133$, also $7 = x\cdot 84 + y\cdot 133$ für $x=8$, $y=-5$.

Wir schreiben den euklidischen Algorithmus jetzt wie folgt auf: ($a\neq 0$, $b\in\mathbb{Z}$ bel. $\rightsquigarrow q_0\in\mathbb{Z}$)

$\frac{b}{a} = q_0 + \frac{r_1}{a}$, $q_0 = \lfloor \frac{b}{a} \rfloor$, $0 < \frac{r_1}{a} < 1$, so dass $\frac{a}{r_1} > 1$ (falls $r_1 \neq 0$)

$\frac{a}{r_1} = q_1 + \frac{r_2}{r_1}$, $q_1 = \lfloor \frac{a}{r_1} \rfloor$,

$\frac{r_1}{r_2} = q_2 + \frac{r_3}{r_2}$, $q_2 = \lfloor \frac{r_1}{r_2} \rfloor$,

$\vdots$

$\frac{r_{n-2}}{r_{n-1}} = q_{n-1} + \frac{r_n}{r_{n-1}}$

$\frac{r_{n-1}}{r_n} = q_n$

Beachte: $q_1, q_2, \dots, q_n \in \mathbb{N}$ und $q_n \geq 2$ im Falle $n \geq 1$.

Zusammengefasst: $\frac{b}{a} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{\ddots + \cfrac{1}{q_{n-1} + \frac{1}{q_n}}}}}}$

"Kettenbruch(entwicklung)" von $\frac{b}{a}$

Im Bsp.: $\frac{133}{84} = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2 + \frac{1}{2}}}}$ mit $q_0=1, q_1=1, q_2=1, q_3=2, q_4=2$

Näherungsbrüche: $1 = \frac{1}{1}$, $1 + \frac{1}{1} = \frac{2}{1}$, $1 + \frac{1}{1+1} = \frac{3}{2}$, $1 + \frac{1}{1 + \frac{1}{1+\frac{1}{2}}} = \frac{8}{5}$, $1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{2+\frac{1}{2}}}} = \frac{19}{12} = \frac{133}{84}$,

also $\frac{1}{1}, \frac{2}{1}, \frac{3}{2}, \frac{8}{5}, \frac{19}{12} = \frac{133}{84}$ $\rightarrow 1, 2, 1.5, 1.6, 1.58\overline{3}$

3.17. Fazit:

Der euklidische Algorithmus ist genau die (endliche) Kettenbruchentwicklung des rationalen Falls $\frac{b}{a}$.