Vorlesung Zahlentheorie I (Algebraische ZT)

WiSe '22/'23, Uni
K. Halupczok

Z21: Konvergenz unendlicher Kettenbrüche

Stichworte: Kgz.satz über unendl. KBe, Abstand von α zu den NBen, natürlicher kB, α rational $\Leftrightarrow$ KBE endlich, Eindeutigkeit der KBE, normierter KB, Mediante, Zwischenbruch, schneller Algorithmus zur Berechnung von Bézout-Elementen / modularer Inverser

---

21.1. Einleitung: Wir zeigen den Konvergenzsatz über unendliche (natürliche) KBe. Genau die rationalen Zahlen haben eine endliche KBE. Die KBE ist genau für normierte KBe eindeutig: Unendliche KBe sind per Def. normiert, und endliche heißen normiert, wenn ihr Letzter Eintrag >1 ist. Unter den vielen Anwendungen der KBe ist die algorithmisch schnelle Berechnung von Bézout-Elementen und modularer Inverser.

21.2. **Satz (Konvergenz unendlicher Kettenbrüche):**
Geg. sei ein unendlicher KB $\alpha = [q_0; q_1, q_2, \dots]$. Dann gelten:
(i) α konvergent $\Rightarrow$ jeder Rest $S_n = [q_n; q_{n+1}, \dots]$ konvergiert
(ii) ein S_n konvergent $\Rightarrow$ α konvergent
(iii) Ist α konvergent, so hat man für die Werte von α bzw. S_n:

$$(*) \quad \alpha = \frac{c_{n-1} S_n + c_{n-2}}{d_{n-1} S_n + d_{n-2}}, \quad n = 1, 2, \dots \quad (\text{Nenner} > 0),$$

d.h. $[q_0; q_1, \dots] = [q_0; q_1, \dots, q_{n-1}, S_n]$.
(iv) Ist α konvergent, so gilt $\frac{c_{2n}}{d_{2n}} < \alpha < \frac{c_{2n+1}}{d_{2n+1}}$ für alle $n, n \geq 0$.

Bew.:
Haben $\frac{c_{n+k}}{d_{n+k}} = [q_0; q_1, \dots, q_{n+k}] \overset{\text{Lemma 20.20(i)}}{=} \frac{c_{n-1}\frac{c'_k}{d'_k} + c_{n-2}}{d_{n-1}\frac{c'_k}{d'_k} + d_{n-2}}$, wo $[q_n; q_{n+1}, \dots, q_{n+k}] = \frac{c'_k}{d'_k}$ der k-te NB von S_n ist.

- Sei S_n konvergent, d.h. $\frac{c'_k}{d'_k} \to S_n$ für $k \to \infty$.
  Dann folgt: $\frac{c_{n+k}}{d_{n+k}} \longrightarrow \frac{c_{n-1} S_n + c_{n-2}}{d_{n-1} S_n + d_{n-2}}$ für $k \to \infty$, also ist α kgt. mit dem Wert $(*)$.

Der Nenner ist >0, da $S_n > 0$ (denn nach Lemma 20.19(i) ist $0 < \frac{q_n}{1} = \frac{c'_0}{d'_0} < S_n$).

• Sei α Konvergent. Löse auf: $\frac{c_n'}{d_n'} = -\frac{d_{n-2}\frac{c_{n+n}}{d_{n+n}} - c_{n-2}}{d_{n-1}\frac{c_{n+n}}{d_{n+n}} - c_{n-1}}$,
ausgenommen der Fall Nenner $=0$, was nach Lemma 20.19 unmöglich. Zähler und Nenner gehen für $n\to\infty$ gegen $d_{n-2}\alpha - c_{n-2}$ bzw. $d_{n-1}\alpha - c_{n-1}$.
Der Nenner $d_{n-1}\alpha - c_{n-1} = 0$ ist wiederum unmöglich wegen Lemma 20.19.
Also ist $\frac{c_n'}{d_n'}$ konvergent, d.h. S_n' ist konvergentes KB.

• Dies zeigt (i)–(iii), und (iv) klar nach Lemma 20.19. □

21.3. **Lemma:** Der Wert α eines konvergenten unendlichen KBes genügt der Ungleichung
$$\left|\alpha - \frac{c_n}{d_n}\right| < \frac{1}{d_n d_{n+1}} \quad \text{für jedes } n \geq 0.$$
Bew.: Nach Lemma 20.18 (iv) ist $\left|\frac{c_n}{d_n} - \frac{c_{n+1}}{d_{n+1}}\right| = \left|\frac{(-1)^{n+1}}{d_{n+1}d_n}\right| = \frac{1}{d_n d_{n+1}}$.
Nach Satz 21.2 (iv) liegt α echt zwischen je zwei aufeinanderfolgenden NBen.
Falls n gerade: $\frac{c_n}{d_n}$ — α — $\frac{c_{n+1}}{d_{n+1}}$, falls n ungerade: $\frac{c_{n+1}}{d_{n+1}}$ — α — $\frac{c_n}{d_n}$ → Es folgt die Beh. □

21.4. **Bem.:** Die Ungl. in Lemma 21.3 ist interessant, falls $c_n, d_n \in \mathbb{Z}$, zur Approximation der reellen Zahl α durch rationale Zahlen.

21.5 **Def.:** Ein KB $[q_0; q_1, \ldots]$, endlich oder unendlich, heißt **natürliches/regulärer KB**, wenn $q_n \in \mathbb{Z}$ für alle $n \geq 0$ und $q_n > 0$ für $n \geq 1$, also $q_1, q_2, \ldots \in \mathbb{N}$ und $q_0 \in \mathbb{Z}$.

21.6. **Bem.:** Behandeln ab jetzt nur noch natürliche KBe, nennen diese schlechthin KBe.
Nach Lemma 20.14 ist dann $c_n, d_n \in \mathbb{Z}$ für alle $n \geq -2$, und $d_n \in \mathbb{N}$ für $n \geq 0$.
Weiter ist $d_n \overset{\geq}{=} q_n d_{n-1} + d_{n-2} \geq d_{n-1} + 1 > d_{n-1}$ für $n \geq 2$, und $d_n \geq n$ für $n \geq 1$.
($d_0 = 1, d_1 = 1$ möglich)
Induktiv: $d_n > 2^{(n-1)/2}$ für $n \geq 2$.

21.7. **Lemma:** Jeder unendliche (nat.) KB ist konvergent.

Bew.: Haben $[q_0; q_1, \dots, q_m] = \frac{c_m}{d_m}$, z.z.: $\left(\frac{c_m}{d_m}\right)_m$ konvergiert.

Es ist: $\left(\frac{c_{2m+1}}{d_{2m+1}}\right)_m$ mon. fallend, $\left(\frac{c_{2m}}{d_{2m}}\right)_m$ mon. wachsend, $\frac{c_{2m}}{d_{2m}} < \frac{c_{2m+1}}{d_{2m+1}}$ nach Lemma 20.19.

Weiter: $\frac{c_{2m+1}}{d_{2m+1}} - \frac{c_{2m}}{d_{2m}} = \frac{1}{d_{2m} d_{2m+1}} \leq \frac{1}{2m \cdot (2m+1)} \xrightarrow{m\to\infty} 0$.

($= \frac{1}{d_{2m} d_{2m+1}}$ aus Lemma 20.18; $\leq \frac{1}{2m(2m+1)}$ Bem. 21.6)

Haben also eine klassische IUschachtelung.

Daher ex. (genau) ein $\beta \in \mathbb{R}$ mit $\beta \in \left]\frac{c_{2m}}{d_{2m}}, \frac{c_{2m+1}}{d_{2m+1}}\right[$ für alle m und $\lim_{m\to\infty} \frac{c_{2m}}{d_{2m}} = \beta = \lim_{m\to\infty} \frac{c_{2m+1}}{d_{2m+1}}$. Es folgt $\beta = \lim_{m\to\infty} \frac{c_m}{d_m}$. □

21.8. **Lemma:** Die NBe eines (nat.) KBs lassen sich nicht kürzen, d.h. $(c_k, d_k) = 1$ für $k \geq -2$.

Bew.: $d_k c_{k-1} - c_k d_{k-1} = (-1)^k$ für $k \geq -1$ nach Lemma 20.18(iii), also $(c_{k-1}, d_{k-1}) = 1$. □

21.9. **Lemma:** Jede rationale Zahl ist durch einen endlichen KB darstellbar.

Bew.:
- $\alpha = \frac{b}{a}$, $a > 0$, $a, b \in \mathbb{Z}$ ~ eukl. Algo. mit "Quotienten" $q_0, q_1, \dots, q_m$ und Resten $r_1, \dots, r_m$.
- Im Fall $\alpha \in \mathbb{Z}$ ist $\alpha = [q_0]$, $q_0 = \alpha$. Für $\alpha \notin \mathbb{Z}$ ist $\alpha = [q_0; q_1, \dots, q_m]$ mit $m \geq 1$, $q_1, \dots, q_m \in \mathbb{N}$, $q_m = \frac{r_{m-1}}{r_m} \geq 2$. □

21.10. **Def.:** Sei $\alpha \in \mathbb{R}$. Erhalten wie oben in 21.2 (ev. endliche) Folgen:

$q_0, q_1, \dots, q_{m-1}, \dots$ ($q_0 \in \mathbb{Z}$, $q_1, \dots, q_{m-1} \in \mathbb{N}$) bzw. $s_1, s_2, \dots, s_m, \dots$, die $s_k > 1$

($q_0 = \lfloor \alpha \rfloor$, $\alpha = \lfloor \alpha \rfloor + \frac{1}{s_1}$ falls $\alpha \notin \mathbb{Z}$).

Es ist (+) $s_k = q_k + \frac{1}{s_{k+1}}$ falls $s_k \notin \mathbb{Z}$, $0 \leq k \leq m-1$,

$\alpha = [q_0; q_1, \dots, q_{m-1}, s_m]$.

Wir erhalten so einen endlichen bzw. unendl. (nat.) KB

$[q_0; q_1, \dots, q_m]$ bzw. $[q_0; q_1, q_2, \dots]$, die KBE von α.

($s_m'' \lceil$)

Es folgt aus (+):
- $\alpha \in \mathbb{Q} \Rightarrow s_k \in \mathbb{Q}$,
- $\alpha \notin \mathbb{Q} \Rightarrow s_k \notin \mathbb{Q}$: die KBE von α bricht nicht ab.

Bsp: $\sqrt{2} = [1; 2, 2, \dots]$, denn $\sqrt{2} = \overset{q_0}{1} + \frac{1}{s_1}$ mit $s_1 > 1$ ~ $s_1 = \frac{1}{\sqrt{2}-1} = \frac{\sqrt{2}+1}{2-1} = \sqrt{2}+1$,

dabei $\lfloor s_1 \rfloor = \lfloor \sqrt{2}+1 \rfloor = 2 = q_1$, und $s_1 = 2 + \frac{1}{s_2}$ mit $\frac{1}{s_2} = s_1 - 2 = \sqrt{2} - 1 = \frac{1}{s_1} \Rightarrow s_1 = s_2 = s_3 = \dots$,

also $2 = q_1 = q_2 = \dots$

21.11. **Lemma:** Jede irrationale Zahl α ist auf genau eine Art als (nat.) KB darstellbar (welcher notwendig unendlich ist).

Bew.: 1.) Sei $\alpha \in \mathbb{R}$, $\alpha \notin \mathbb{Q}$. Betr. den zugeordneten unendl. KB $[q_0; q_1, q_2, \dots]$. Dieser ist nach Lemma 21.7 konvergent. Sei β sein Wert (d.h. = Grenzwert der endlichen Abschnitte). Beh.: $\beta = \alpha$. Denn: Seien $\frac{c_n}{d_n}$ die NBe, z.z.: $\frac{c_n}{d_n} \to \alpha$ für $n \to \infty$.
Mit den wie oben def. $q_0, q_1, \dots, q_{m-1}, s_m$ gilt $\alpha = [q_0; q_1, \dots, q_{m-1}, s_m]$, $m \geq 1$.
Dann: n-ter NB von $[q_0; q_1, \dots, q_{m-1}, s_m]$ ist α,
$(n-1)$-ter NB von $[q_0; q_1, \dots, q_{m-1}, s_m]$ ist $\frac{c_{n-1}}{d_{n-1}}$. (vgl. Def. 20.12)
Für die Differenz zweier aufeinanderfolgender NBe gilt aber nach Lemma 20.18 $\left|\alpha - \frac{c_{n-1}}{d_{n-1}}\right| = \frac{1}{d_{n-1} d_n'}$, wo d_n' der Nenner des letzten NBs von $\alpha = [q_0; q_1, \dots, q_{m-1}, s_m]$ ist, also ist $d_n' = d_{n-1} s_m + d_{n-2}$ nach Lemma 20.14.
Wegen $s_m > 0$ geht $\left|\alpha - \frac{c_{n-1}}{d_{n-1}}\right|$ gegen 0 für $n \to \infty$.
2.) Eindeutigkeit: Gelte $\alpha = [q_0; q_1, \dots] = [q_0'; q_1', \dots]$. Dann ist $\alpha = q_0 + \frac{1}{s_1} = q_0' + \frac{1}{s_1'}$, $s_1 > 1$, $s_1' > 1$. Dann: $q_0 = \lfloor \alpha \rfloor = q_0' \Rightarrow s_1 = s_1' \Rightarrow q_1 = q_1'$, usw. □

21.12. **Bem.:** Ist $\alpha \in \mathbb{Q}$, so hat α die Darstellung $\alpha = [q_0; q_1, \dots, q_m]$ als endl. KB, oder, falls $m \geq 1$, mit einem $q_m \geq 2$ endet.
1. Bew.: Für $\alpha \in \mathbb{Z}$ ist $\alpha = [q_0] = q_0$ ✓, für $\alpha \notin \mathbb{Z}$ liefert der endl. Algo. die KB darstellung mit $m \geq 1$ und $q_m \geq 2$.
2. Bew.: Sei $\alpha = [q_0; q_1, \dots, q_m]$, $m \geq 1$, $q_m = 1$. Für $m = 1$ ist $\alpha = q_0 + \frac{1}{q_1} = q_0 + 1 \in \mathbb{Z}$, also $\alpha = [q_0 + 1]$. ✓
Für $m \geq 2$ ist $s_{m-1} = q_{m-1} + \frac{1}{q_m} = q_{m-1} + 1 \in \mathbb{Z}_{\geq 2}$, also $\alpha = [q_0; q_1, \dots, q_{m-2}, s_{m-1}] = [q_0; q_1, \dots, q_{m-2}, q_{m-2} + 1]$. ✓

21.13. **Def.:** Ein (nat.) KB, der nicht mit 1 endet, falls er nicht von der Form $[q_0]$ ist, heißt ein normierter KB. Unendliche KBe sind normiert.

21.14. **Bem.:** Sind $[q_0; q_1, \dots, q_m]$ und $[q_0'; q_1', \dots, q_m']$ mit $n \geq m$ beide normiert vom selben Wert α, so folgt $m = n$ und $q_i' = q_i$ für alle i.
Bew.: Sei $n > 0$. Dann ist $\alpha = q_0 + \frac{1}{s_n}$ und $s_n > 1$ wegen Normiertheit. Also ist $\alpha \notin \mathbb{Z}$. Daher ist auch $m > 0$. Dann ist $q_0 + \frac{1}{s_n} = q_0' + \frac{1}{s_n'}$ mit $s_n' > 1$. Es folgt $q_0 = \lfloor \alpha \rfloor = q_0'$, also $s_n = s_n'$. Dann Induktion. Im Fall $n = 0$ ist $m = 0$ und Beh. klar. □

21.15. **Zusammenfassung im Satz:** (i) Ordnet man jeder reellen Zahl ihre KBE zu, erhält man eine Bijektion zwischen $\mathbb{R}$ und der Menge der normierten KBe,

$$\mathbb{R} \ni \alpha \longleftrightarrow [q_0; q_1, \ldots].$$

Die Umkehrabb. ordnet jedem normierten Kettenbruch dessen Wert zu: $\alpha = [q_0; q_1, \ldots]$.

(ii) α rational $\Leftrightarrow$ KBE von α ist endlich

(iii) Für die NBe $\frac{c_k}{d_k}$ des zu α gehörenden KBs gilt für $k \geq 0$: [falls d_{k+1} vorhanden]

$$\frac{1}{d_k(d_k+d_{k+1})} < \left|\alpha - \frac{c_k}{d_k}\right| \leq \frac{1}{d_k d_{k+1}} \quad (\Leftrightarrow) \quad \frac{1}{d_k+d_{k+1}} < |d_k\alpha - c_k| \leq \frac{1}{d_{k+1}}.$$

Zusatz: Anstelle $\leq$ gilt $<$ bis auf den Fall $\alpha = [q_0; q_1, \ldots, q_m]$ und $k = m-1$.

Bew.: 1.) Haben (i) und (ii) schon gezeigt (vgl. Lemma 21.11).

- Die Ungl. $\leq$ und der Zusatz ist klar für $\alpha \notin \mathbb{Q}$, vgl. Lemma 21.3.
- Sei $\alpha \in \mathbb{Q}$ und $\alpha = [q_0; q_1, \ldots, q_m]$ mit $q_m > 1$, $m \geq 1$. Für $k \leq m-1$ gilt
$$\left|\frac{c_{k+1}}{d_{k+1}} - \frac{c_k}{d_k}\right| = \frac{1}{d_k d_{k+1}} \text{ nach Lemma 20.18.}$$
- Sei $k < m-1$, also $k, k+1 \leq m-1$. Für $l \leq m-1$ gilt: NBe: geradem Index l $<\alpha<$ NBe: ungerad. Index l. Die Zahl α liegt also echt zwischen $\frac{c_{k+1}}{d_{k+1}}$ und $\frac{c_k}{d_k}$, also gilt "$<$" anstelle "$\leq$".
- Für $k = m-1$ ist $\left|\alpha - \frac{c_k}{d_k}\right| = \left|\frac{c_m}{d_m} - \frac{c_{m-1}}{d_{m-1}}\right| = \frac{1}{d_{m-1}d_m} = \frac{1}{d_m d_{m+1}}$.

2.) Noch z.z.: die untere Abschätzung "$<$" in (iii). Für k gerade ist $\frac{c_k}{d_k} < \alpha \leq \frac{c_{k+1}}{d_{k+1}}$.

[Falls k ungerade gilt $\frac{c_{k+1}}{d_{k+1}} \leq \alpha < \frac{c_k}{d_k}$, das Folgende gilt analog.]

Es folgt $\frac{c_k}{d_k} < \frac{c_k+c_{k+1}}{d_k+d_{k+1}} < \frac{c_{k+1}}{d_{k+1}}$ [Denn $\frac{c}{d} < \frac{c+c'}{d+d'} < \frac{c'}{d'}$ für alle $c, c', d, d' \in \mathbb{R}$, $d, d' > 0$, $\frac{c}{d} < \frac{c'}{d'}$.]

Es genügt nun, Lemma 21.16 zu zeigen.

[Daraus folgt $\left|\alpha - \frac{c_k}{d_k}\right| > \left|\frac{c_k+c_{k+1}}{d_k+d_{k+1}} - \frac{c_k}{d_k}\right| = \left|\frac{c_k d_k + c_{k+1}d_k - c_k d_k - c_k d_{k+1}}{d_k(d_k+d_{k+1})}\right| \overset{\text{Lemma 20.18}}{=} \frac{1}{d_k(d_k+d_{k+1})}$ ✓] □

21.16. **Lemma:** Es gilt $\frac{c_k+c_{k+1}}{d_k+d_{k+1}} < \alpha \leq \frac{c_{k+1}}{d_{k+1}}$ für k gerade.

Benötigen dafür die folgende Definition.

21.17. **Def.:** Seien $\frac{c}{d}$, $\frac{c'}{d'}$ Brüche mit $\frac{c}{d} < \frac{c'}{d'}$ und $d, d' > 0$.

Der Bruch $\frac{c+c'}{d+d'}$ heißt **Mediante / Medianwert** von $\frac{c}{d}$, $\frac{c'}{d'}$.

Die Brüche $\frac{c_k + q c_{k+1}}{d_k + q d_{k+1}}$, $q = 1, \ldots, q_{k+2}$, heißen **Zwischenbrüche** der NBe $\frac{c_k}{d_k}$, $\frac{c_{k+1}}{d_{k+1}}$.

[q_{k+2}-ter Zwischenbruch ist $\frac{c_{k+2}}{d_{k+2}}$]

Bem.: die Mediante ist sozusagen die "falsche Summe" zweier Brüche $\frac{c}{d}, \frac{c'}{d'}$ und liegt zwischen ihnen, denn $\frac{c}{d} < \frac{c+c'}{d+d'} \Leftrightarrow cd+cd' < cd+c'd \Leftrightarrow \frac{c}{d} < \frac{c'}{d'}$, und $\frac{c+c'}{d+d'} < \frac{c'}{d'}$ analog.

Bew. von Lemma 21.16:

Für $q>0$ ist der Zwischenbruch von $\frac{c_n}{d_n}, \frac{c_{n+1}}{d_{n+1}}$ eine Mediante von $\frac{c_n}{d_n}, \frac{q c_{n+1}}{q d_{n+1}} = \frac{c_{n+1}}{d_{n+1}}$.

Damit folgt $\frac{c_n}{d_n} < \frac{c_n + c_{n+1}}{d_n + d_{n+1}} \leq \frac{c_n + q_{n+2} c_{n+1}}{d_n + q_{n+2} d_{n+1}} \leq \alpha \leq \frac{c_{n+1}}{d_{n+1}}$.

$\frac{c_{n+2}}{d_{n+2}} =$ — für $q_{n+2} > 1$ Mediante von und $\frac{(q_{n+2}-1)c_{n+1}}{(q_{n+2}-1)d_{n+1}} =$

Dies zeigt die Beh., müssen aber noch ausschließen, dass $\frac{c_n + c_{n+1}}{d_n + d_{n+1}} = \frac{c_{n+2}}{d_{n+2}} = \alpha$, $q_{n+2} = 1$.

Wäre dies so, wäre $\alpha \in \mathbb{Q}$, $\alpha = [a_0; q_1, \dots, q_{n+2}]$ mit $q_{n+2} = 1$, was nicht möglich ist, da nur normierte KBe zugelassen sind. □

21.18 **Bem.:** Aus (iii) in Satz 21.15 folgt $\left|\alpha - \frac{c_{n+1}}{d_{n+1}}\right| < \left|\alpha - \frac{c_n}{d_n}\right|$.

Bew.:
- Ist $\frac{c_{n+1}}{d_{n+1}}$ der letzte NB, d.h. $\alpha = \frac{c_{n+1}}{d_{n+1}}$, gilt dies (l.S. = 0, r.S. > 0 nach 21.15(iii)).
- Andernfalls gilt $\left|\alpha - \frac{c_{n+1}}{d_{n+1}}\right| \leq \left|\frac{c_{n+2}}{d_{n+2}} - \frac{c_{n+1}}{d_{n+1}}\right| = \frac{1}{d_{n+1} d_{n+2}}$,

und wegen 21.15(iii) dann

$$\left|\alpha - \frac{c_n}{d_n}\right| > \frac{1}{d_n(d_{n+1}+d_n)} \geq \frac{1}{d_n(q_{n+2}d_{n+1}+d_n)} = \frac{1}{d_n d_{n+2}} \geq \frac{1}{d_{n+1} d_{n+2}}.$$

Es folgt die Beh. □

Wir erinnern an eine wichtige Anwendung der (endlichen) KBE aus Einf ZT:

21.19 **Altes Bsp.:** $b = 133$, $a = 84$, Bestimmung der q_i:

$133 : 84 = 1$ q_0

$\frac{84}{84 : 49} = 1$ q_1

$\frac{49}{49 : 35} = 1$ q_2

$\frac{35}{35 : 14} = 2$ q_3

$\frac{28}{14 : 7} = 2$ (Rest 0) q_4

Tabelle:

k		0	1	2	3	4
q_k		1	1	1	2	2
c	0 1	1	2	3	(8)	19
d	1 0	1	1	2	(5)	12
$\frac{c}{d}$		$\frac{1}{1}$	$\frac{2}{1}$	$\frac{3}{2}$	$\frac{8}{5}$	$\frac{19}{12}$

Zelle = vorletzte Zelle + letzter Zelle mal q_k-Wert darüber

= Rekursionen

$\rightsquigarrow n = 4$, $r_4 = 7$ Haben $8 \cdot 84 - 5 \cdot 133 = (-1)^4 \cdot 7 = 7$

können die Bézout-Elemente von a, b direkt ablesen! Auch VZ klar: s. 21.20.

21.20. **Algorithmus zur Berechnung der Bézout-Elemente:**
Führe den enkl. Algo. und obiges Schema durch. In Spalte $n-1$ stehen c_{n-1}, d_{n-1}, für die $c_{n-1}a - d_{n-1}b = (-1)^n r_n$ gilt, d.h. bis auf das VZ sind dies die Bézout-El.

Korrektheit:
Betr. $\frac{b}{a}$ mit $a>0$. Haben $\frac{b}{a} = \frac{r_n b'}{r_n a'}$ mit $\frac{b'=c_n}{a'=d_n}$ und dem letzten Rest $r_n \neq 0$.
Nach Lemma 20.18 gilt
$d_n c_{n-1} - c_n d_{n-1} = (-1)^n$, wegen $b'=c_n$, $a'=d_n$ also
$c_{n-1}a' - d_{n-1}b' = (-1)^n$, nach Multiplikation mit r_n folgt die Beh. □

21.21. **Algorithmus zur Berechnung modularer Inverser:**
Geg. sei der Rest x mod m, $x, m \in \mathbb{Z}$, $m>1$, $(x,m)=1$. Das modulare Inverse $\bar{x}$ mod m, d.h. $\bar{x} \in \mathbb{Z}$ so, dass $x\bar{x} \equiv 1 \ (m)$, berechnet sich als $\bar{x} \equiv (-1)^n c_{n-1} \ (m)$.
Korrektheit: Aus $c_{n-1}x - d_{n-1}m = (-1)^n$ folgt $(-1)^n c_{n-1}x - (-1)^n d_{n-1}m = 1$, also $(-1)^n c_{n-1}x \equiv 1 \ (m)$, so dass $\bar{x} \equiv (-1)^n c_{n-1}$ folgt. □

21.22. **Bem.:** Die Algorithmen in 21.20, 21.21 laufen im Prinzip so schnell wie der euklidische Algo. (Satz von Lamé, vgl. EinfZT 5.13).