WiSe'21/'22, hhu
K. Halupczok

Vorlesung Einführung in die Zahlentheorie

EZ5: Fibonaccizahlen

Stichworte: Fibonaccizahlen, KBE und Fibonaccizahlen, goldener Schnitt, Binetsche Formel, Formeln mit Fibonaccizahlen, Fibonacci-Primzahlen, Dauer des euklidischen Algorithmus (Satz von Lamé)

5.1. Einleitung: Der einfachste KB ist $[1;1,1,1,\dots]$ führt auf den goldenen Schnitt, seine NBe führen auf die Fibonaccizahlen, die viele interessante Eigenschaften haben. Als Anwendungen zeigen wir den Satz von Lamé über die Dauer/Laufzeit eines KBE bzw. des euklidischen Algorithmus.

5.2. **Def.:** Der unendliche KB $\alpha = [1;1,1,1,\dots]$ führt auf die Rekursionen
$\left.\begin{matrix} c_n = 1\cdot c_{n-1} + c_{n-2} \\ d_n = 1\cdot d_{n-1} + d_{n-2} \end{matrix}\right|$, $n=0,1,2,\dots$ Setze $u_n := d_{n-1} = c_{n-2}$, $n\geq 2$, also $d_n = u_{n+1}$, $c_n = u_{n+2}$ mit der Folge $(u_n)_{n\geq 0}$ der Fibonaccizahlen.
Hier ist u_n die n-te Fibonaccizahl und $u_{n+1} = u_n + u_{n-1}$, $n\geq 1$; $u_0 = 0$, $u_1 = 1$.

u_0	u_1	u_2	u_3	u_4	u_5	u_6	u_7	u_8	u_9	u_{10}	…
0,	1	1	2	3	5	8	13	21	34	55	…

5.3. **Bem.:**
- Mit $u_{n-1} = u_{n+1} - u_n$, $u_{-1} := u_1 - u_0 = 1$ wird u_n rekursiv für $n<0$ def. Haben für $n<0$ dann $u_{-n} = (-1)^{n+1} u_n$.
- Oft wird auch die Bezeichnung F_n anstelle u_n für die n-te Fibonaccizahl benutzt. Wir folgen einer in der Zahlentheorie verbreiteten Notation, u_n zu schreiben. Die Notation F_n ist für die n-te Fermatzahl $F_n = 2^{2^n}+1$ reserviert.

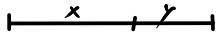
Aus der KB-theorie sind bereits folgende Eigenschaften klar:

5.4. **KBE und Fibonaccizahlen:** (1) Für $n\geq 1$ ist $\frac{u_{n+1}}{u_n} = \frac{c_{n-1}}{d_{n-1}}$, $n\geq 1$, für $\alpha = [1;1,1,\dots]$.

(2) $\begin{pmatrix} u_{n+2} \\ u_{n+1} \end{pmatrix} = \begin{pmatrix} u_{n+1} & u_n \\ u_n & u_{n-1} \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ für alle $n\in\mathbb{Z}$ nach Lemma 4.11.

(3) Für $n\geq 1$ ist $\begin{pmatrix} u_{n+1} & u_n \\ u_n & u_{n-1} \end{pmatrix} = M^n \overset{\text{Lemma 4.12 (2)}}{=} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n$, auch für $n\leq 0$. (!)

(4) Die Folge $\frac{u_{m+1}}{u_m} = \frac{c_{m-1}}{d_{m-1}}$ konvergiert gegen $\alpha = [1; 1, 1, \dots]$.
Kgz. unendlicher KBe i.a. haben wir nicht behandelt. Hier folgt die Kgz. z.B. aus 5.5.(2).
Haben $\alpha = \frac{1}{2} + \frac{1}{2}\sqrt{5}$. Berechnung: $\alpha = 1 + \frac{1}{\alpha} \overset{\alpha > 0}{\Rightarrow} \alpha > 0$, und die Gl. $\alpha = 1 + \frac{1}{\alpha}$ führt auf $\alpha^2 - \alpha - 1 = 0$
"goldener Schnitt" aus der Vor., dass $\frac{u_{m+1}}{u_m}$ Kgt.
$\hookrightarrow \frac{x}{y} \overset{!}{=} \frac{x+y}{x} = 1 + \frac{1}{x/y} \rightsquigarrow \left(\frac{x}{y}\right)^2 - \left(\frac{x}{y}\right) - 1 = 0$



"Die Gesamtlänge durch die Länge des größeren Abschnitts ergibt die Länge des größeren Abschnitts durch die des kleineren Abschnitts." ~ Ästhetik

(5) Für $\beta = \frac{1}{2} - \frac{1}{2}\sqrt{5}$ ist $\alpha + \beta = 1$ und $\alpha\beta = -1$, d.h. $\beta = -\frac{1}{\alpha}$, so dass $|\beta| < 1$ ist.
(β heißt die Konjugierte von $\alpha = \frac{1}{2} + \frac{1}{2}\sqrt{5}$)
Mit $\alpha^2 = \alpha + 1$, $\beta^2 = \beta + 1$ ist $\alpha^{m+2} = \alpha^{m+1} + \alpha^m$, $\beta^{m+2} = \beta^{m+1} + \beta^m$,
also $\begin{pmatrix} \alpha^{m+2} & \alpha^{m+1} \\ \beta^{m+2} & \beta^{m+1} \end{pmatrix} = \begin{pmatrix} \alpha^{m+1} & \alpha^m \\ \beta^{m+1} & \beta^m \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \dots = \underbrace{\text{induktiv}}\ \begin{pmatrix} \alpha & 1 \\ \beta & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^{m+1} \overset{(3)}{=} \begin{pmatrix} \alpha & 1 \\ \beta & 1 \end{pmatrix} \begin{pmatrix} u_{m+2} & u_{m+1} \\ u_{m+1} & u_m \end{pmatrix}$.
Es folgt:
$\begin{pmatrix} u_{m+2} & u_{m+1} \\ u_{m+1} & u_m \end{pmatrix} = \begin{pmatrix} \alpha & 1 \\ \beta & 1 \end{pmatrix}^{-1} \cdot \begin{pmatrix} \alpha^{m+2} & \alpha^{m+1} \\ \beta^{m+2} & \beta^{m+1} \end{pmatrix} = \frac{1}{\alpha - \beta} \begin{pmatrix} 1 & -1 \\ -\beta & \alpha \end{pmatrix} \cdot \begin{pmatrix} \alpha^{m+2} & \alpha^{m+1} \\ \beta^{m+2} & \beta^{m+1} \end{pmatrix} = \frac{1}{\alpha - \beta} \begin{pmatrix} \alpha^{m+2} - \beta^{m+2} & * \\ * & * \end{pmatrix}$,
also ist $u_{m+2} = \frac{\alpha^{m+2} - \beta^{m+2}}{\alpha - \beta}$.

Mit $\alpha - \beta = \sqrt{5}$ erhalten wir die
Binetsche Formel $\quad u_m = \frac{\alpha^m - \beta^m}{\sqrt{5}} = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^m - \left(\frac{1-\sqrt{5}}{2}\right)^m\right)$, $m \geq 0$, sogar für alle $m \in \mathbb{Z}$.
explizite Berechnungsformel der Fibonaccizahlen

5.5. (1) Bem.: u_m ist die zu $\frac{\alpha^m}{\sqrt{5}}$ nächstgelegene ganze Zahl, $m \geq 0$.
Bew.: $\left|\underbrace{\frac{\alpha^m - \beta^m}{\sqrt{5}}}_{= u_m} - \frac{\alpha^m}{\sqrt{5}}\right| = \frac{|\beta|^m}{\sqrt{5}} \leq \frac{1}{\sqrt{5}} < \frac{1}{2}$. □ Bsp.: $\frac{\alpha^{12}}{\sqrt{5}} \overset{\text{TR}}{\approx} 144.00138\dots \rightsquigarrow u_{12} = 144$

(2) $\frac{u_{m+1}}{u_m} \overset{(1)}{=} \frac{\alpha^{m+1}/\sqrt{5} + \varepsilon}{\alpha^m/\sqrt{5} + \varepsilon'} = \frac{\alpha + \frac{\sqrt{5}\varepsilon}{\alpha^m}}{1 + \frac{\sqrt{5}\varepsilon'}{\alpha^m}} \to \alpha$, da $|\varepsilon| < \frac{1}{2}, |\varepsilon'| < \frac{1}{2}$, $\alpha > 1$.

5.6. Allgemeinere Rekursionsformel: Für $m, k \in \mathbb{Z}$ ist $u_{m+k} = u_{m+1} u_k + u_m u_{k-1}$.
Bew.: Haben $\begin{pmatrix} u_{m+1} \\ u_m \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^{m-1} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ aus 5.4 (2) und (3), also
$\begin{pmatrix} u_{m+k+1} \\ u_{m+k} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^{m+k-1} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^k \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^{m-1} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$
$= \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^k \begin{pmatrix} u_{m+1} \\ u_m \end{pmatrix} = \begin{pmatrix} u_{m+1} u_k \\ u_k u_{k-1} \end{pmatrix} \begin{pmatrix} u_{m+1} \\ u_m \end{pmatrix}$. □

5.7. **Formeln mit Fibonaccizahlen:**

(1) $\frac{u_{n+2}}{u_{n+1}}$ ist der n-te NB von $\alpha = [1; 1, 1, 1, \dots]$, $n \geq -2$.

(2) $\frac{u_{n+2}}{u_{n+1}} \to \alpha = \frac{1}{2} + \frac{1}{2}\sqrt{5}$

(3) $u_n = \frac{\alpha^n - \beta^n}{\sqrt{5}}$ mit $\beta = \frac{1}{2} - \frac{1}{2}\sqrt{5}$, $n \in \mathbb{Z}$

(4) $u_{m+n} = u_m u_{n+1} + u_{m-1} u_n$ für $m, n \in \mathbb{Z}$, vgl. 5.6.

(4') $n = m-1$: $u_{2m-1} = u_m^2 + u_{m-1}^2$, z.B. $u_{19} = u_{10}^2 + u_9^2 = 55^2 + 34^2 = 4181$.

(5) $u_{n+1} u_{n-1} - u_n^2 = (-1)^n$ } det von $\begin{pmatrix} u_{n+1} & u_n \\ u_n & u_{n-1} \end{pmatrix} = M_n = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n$.

(5') $u_n^2 = u_{n-1} u_{n+1} + (-1)^{n+1}$ }

$\vdots$

5.8. **Bem.:** Für $a, b \in \mathbb{Z}$ gilt $(u_a, u_b) = u_{(a,b)}$, insb. $a \mid b \Rightarrow u_a \mid u_b$.

Bew.: (1) $u_m \mid u_{km}$ für alle $m, k \in \mathbb{Z}$.

O.E. seien $m, k \in \mathbb{N}$ [$u_{-n} = (-1)^{n+1} u_n$], Ind. nach k: $k = 1$: V, $k \to k+1$:

$u_{(k+1)m} = u_{km+m} \overset{5.6}{=} u_{km} u_{m+1} + u_{km-1} u_m$ teilbar durch u_m.

(2) Sei $d = (a, b)$. Haben $u_d \mid u_a$, $u_d \mid u_b$, also $u_d \mid (u_a, u_b)$.

Sei $d = xa + yb$ mit $x, y \in \mathbb{Z}$. Es folgt $u_d = u_{xa+yb} \overset{5.6}{=} u_{xa} u_{yb+1} + u_{xa-1} u_{yb}$.

Sei nun c gemeinsamer Teiler von u_a, u_b. Es folgt: $c \mid u_a, c \mid u_b \Rightarrow c \mid u_d$ mit (1). □

5.9. **Bem.:** u_n Primzahl $\overset{5.8}{\Rightarrow}$ n Primzahl, außer $n = 4$: $u_4 = 3$.

(Nicht umgekehrt: $u_{19} = 4181 = 37 \cdot 113$)

Ungelöste Probleme: Ex. unendl. viele Fibonacci-Pzen?

Ist u_p unendl. oft nicht prim?

5.10. **Bem:** Unter den vielen Anwendungen der Fibonaccizahlen ist vor allem folgende für uns interessant: Man kann mit ihnen zeigen, dass der euklidische Algorithmus, d.i. die KBE eines Bruches $\frac{b}{a}$, schnell ist.

5.11. **Lemma:** Bed. Bruch $\frac{b}{a}$ mit $b > a$, $a, b \in \mathbb{N}$. Sei $a < u_{m+1}$.
Der eukl. Algo., auf b, a angewandt, braucht dann $< m$ Schritte.

Bew.: z.z.: ist $[q_0; q_1, \dots, q_m]$ die KBE von $\frac{b}{a}$, so gilt $n+1 \le m-1$.

- Ausführung des eukl. Algo.: $\rightsquigarrow r_0 := a$

$$b = q_0 a + r_1, \quad a = q_1 r_1 + r_2, \quad r_1 = q_2 r_2 + r_3,$$
$$r_2 = q_3 r_3 + r_4, \dots \quad r_{m-2} = q_{m-1} r_{m-1} + r_m, \quad r_{m-1} = q_m r_m.$$

- **Beh.:** $u_{k+2} \le r_{m-k}$ für alle $0 \le k \le m$. [D.h. alle Reste sind mind. so groß wie die entspr. Fibonaccizahl]

Bew. mit vollst. Ind., Ind.anf.:
$k=0$: $r_m \ge u_2 = 1$ ✓, $k=1$: $r_{m-1} = q_m r_m \ge u_3 = 2$ ✓, weil $q_m \ge 2$.
Ind.schritt ($1 \le k \le m-1$):
$k-1, k \rightsquigarrow k+1$: $r_{m-k-1} = q_{m-k} r_{m-k} + r_{m-(k-1)} \overset{IV}{\ge} q_{m-k} u_{k+2} + u_{k+1} \ge u_{(k+1)+2}$.

- Mit der Beh. folgt (mit $k=m$): $u_{m+2} \le r_0 = a \overset{\text{Vor.}}{<} u_{m+1}$,
also $u_{m+2} < u_{m+1} \Rightarrow n+1 < m$, d.h. $n+1 \le m-1$. ($a = q_1 r_1 + r_2 \ge u_{m+1} + u_m$) □

5.12. **Bsp.** für Paar b, a, bei dem man $m-1$ Schritte braucht: $b = u_{m+1}$, $a = u_m$ ($= r_0$).
Dann sind alle $q_i = 1$ für $0 \le i \le m-3$, und $r_{m-k} = u_k$ für $k = 1, \dots, m$.
(Algo. fertig bei $u_3 = 2 = u_{m-3}$, $q_{m-2} = 2 \rightsquigarrow r_{m-1} = 1$ ist letzter Rest $\neq 0$)
("Fibonacci braucht am längsten...")

5.13. **Kor. (Satz von Lamé):**
Für $N :=$ Schrittzahl im Eukl. Algo. gilt: $N \le \frac{\log a}{\log \alpha} + 1$, $\alpha := \frac{1}{2} + \frac{1}{2}\sqrt{5}$.

Bem.: Der Eukl. Algo. ist also
"polynomiell schnell" in der Inputgröße "Stellenzahl" $\rightsquigarrow$ wie Konstante mal (Stellenzahl)^1
$\mathcal{O}(\log a)$ also sogar linear in der Stellenzahl (:= # Stellen), Basis egal!
Hierbei sind die "Kosten" für die Multiplikation großer Zahlen nicht mit berücksichtigt. Man kann diese mit einer FFT (= fast fourier transformation), wie sie etwa im Schönhage-Strassen-Algo. vorkommt, kleinhalten. $\rightsquigarrow$ Informatik

5.14. **Bew.:** Die Folge $(u_m)_{m\geq 2}$ ist streng mon. steigend, daher ex. $m \geq 2$ mit $u_m \leq a < u_{m+1}$. Wegen Lemma 5.11 haben wir dann $N = n+1 \leq m-1$.

Noch z.z.: $m \leq \frac{\log a}{\log \alpha} + 2 \Leftrightarrow \log \alpha^m \leq \log a + 2\log \alpha = \log(a \cdot \alpha^2) \Leftrightarrow \alpha^{m-2} \leq a$.

Bew.: Aus $u_m \leq a$ folgt $a \geq u_m = \frac{1}{\sqrt{5}}(\alpha^m - \beta^m)$, und dies ist $\geq \alpha^{m-2}$: Es gilt: $\alpha^m - \beta^m \overset{!}{\geq} \sqrt{5} \cdot \alpha^{m-2}$

$\Leftrightarrow (\alpha^2 - \sqrt{5})\alpha^{m-2} \overset{!}{\geq} \beta^m = \left(-\frac{1}{\alpha}\right)^m$, dies folgt aus (falls $2 \mid m$, und $2 \nmid m$):

$(\alpha^2 - \sqrt{5}) \cdot \alpha^{m-2} \geq \alpha^{-m} \Leftrightarrow \alpha^{2m} \geq \frac{\alpha^2}{\alpha^2 - \sqrt{5}}$ (Nenner > 0)

$\Leftarrow m \geq \frac{\log \alpha^2 - \log(\alpha^2 - \sqrt{5})}{2\log \alpha} = 1 - \frac{\log \beta^2}{2\log \alpha} \overset{\beta = -\frac{1}{\alpha}}{=} 1 - \frac{\log(1/\alpha)}{\log \alpha} = 2$.

da $\frac{\alpha^2 - \beta^2}{\sqrt{5}} = u_2 = 1$
$\rightsquigarrow \alpha^2 - \sqrt{5} = \beta^2$

□