Fibonaccijeva števila - 2.del

Ana Marija Podboršek, 15. december 2009

1 Verižni ulomki in matrike

Vsako pozitivno število x lahko zapišemo v obliki verižnega ulomka kot

$$a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \cfrac{1}{a_5 + \ddots}}}},$$

kjer je vsak a_i nenegativno število za vsak i. Posamezni del ulomka predstavlja zaporedje števil, ki se približuje številu x. Npr.: a_1, $a_1 + \frac{1}{a_2}$, $a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3}}$, ... Za začetek izberimo nek začetni kos, npr: $\frac{p_3}{q_3} = a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3}}$.
Tak ulomek očitno računamo od spodaj navzgor po korakih.

KORAK1 Izračun spodnjega dela:

$$a_2 + \frac{1}{a_3} = \frac{a_2 a_3 + 1}{a_3}.$$

KORAK2 Vzamemo obratno vrednost koraka 1:

$$\frac{1}{\frac{a_2 a_3 + 1}{a_3}} = \frac{a_3}{a_2 a_3 + 1}.$$

KORAK3 Koraku 2 prištejemo a_1:

$$a_1 + \frac{a_3}{a_2 a_3 + 1} = \frac{a_1 a_2 a_3 + a_1 + a_3}{a_2 a_3 + 1}.$$

Očitno bi po še nekaj korakih prišli do zelo zapletenih izrazov. Na srečo imamo rešitev. Vse skupaj lahko zakodiramo z uporabo matrik. Zakodirati hočemo zaporedje ukazov: Vzemi obratno vrednost in ji dodaj celo število. Kot vidimo v našem primeru, sta to ravno koraka 2 in 3.

Torej, imamo na vsaki stopnji ulomek oblike $\frac{s}{t}$. Vzamemo njegovo obratno vrednost $\frac{t}{s}$ in mu dodamo celo število a_i. Tako dobimo

$$a_i + \frac{t}{s} = \frac{a_i s + t}{s}.$$

Transformacijo števila $\frac{s}{t}$ v število $\frac{a_i s+t}{s}$ lahko gledamo tudi kot transformacijo para (s,t) v par $(a_i s + t, s)$. Transformacijo para (s,t) v par $(a_i s + t, s)$ lahko predstavimo z matriko

$$(\, s, t \,) \begin{pmatrix} a_i & 1 \\ 1 & 0 \end{pmatrix} = (\, a_i s + t, s \,) .$$

Iz tega vidimo, da je primerna matrika za to transformacijo $\begin{pmatrix} a_i & 1 \\ 1 & 0 \end{pmatrix}$. Nadalje lahko zgradimo n-to aproksimacijo $\frac{p_n}{q_n}$ tako, da zmnožimo vse matrike oblike $\begin{pmatrix} a_i & 1 \\ 1 & 0 \end{pmatrix}$, ker je $i = 1, \ldots, n-1$.

Primer. Kako najdemo $\frac{p_3}{q_3}$? Začnemo s številom $a_3 = \frac{a_3}{1}$, ga enačimo s predpisom $(\, a_3, 1 \,)$, pomnožimo z matriko

$$\begin{pmatrix} a_2 & 1 \\ 1 & 0 \end{pmatrix}$$

in nato še z matriko

$$\begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} .$$

Tako dobimo:

$$(\, p_3, q_3 \,) = (\, a_3, 1 \,) \begin{pmatrix} a_2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} .$$

V splošnem dobimo n-to aproksimacijo:

$$(\, p_n, q_n \,) = (\, a_n, 1 \,) \begin{pmatrix} a_{n-1} & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} .$$

Kot vidimo, lahko v tej obliki veliko lažje računamo kot v obliki verižnih ulomkov. Sedaj pa izrazimo še (n-1) aproksimacijo. (n-1) aproksimacija je podana kot:

$$(\, p_{n-1}, q_{n-1} \,) = (\, a_{n-1}, 1 \,) \begin{pmatrix} a_{n-2} & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} .$$

Vidimo, da lahko par $(\, a_{n-1}, 1 \,)$ zapišemo v že znani obliki, in sicer:

$$(\, a_{n-1}, 1 \,) = (\, 1, 0 \,) \begin{pmatrix} a_{n-1} & 1 \\ 1 & 0 \end{pmatrix} .$$

Tako lahko (p_{n-1}, q_{n-1}) zapišemo tudi kot:

$$(\, p_{n-1}, q_{n-1} \,) = (\, 1, 0 \,) \begin{pmatrix} a_{n-1} & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_{n-2} & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} .$$

Od prej že vemo, da lahko n-to aproksimacijo zapišemo kot:

$$(\, p_n, q_n \,) = (\, a_1, 1 \,) \begin{pmatrix} a_{n-1} & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_{n-2} & 1 \\ 1 & 0 \end{pmatrix} \dots \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix}.$$

Tako smo dobili enaka niza matrik pri n-ti in (n-1) aproksimaciji. Iz tega sledi, da lahko oba izraza združimo v eno matrično enačbo. Dobimo:

$$\begin{pmatrix} p_n & q_n \\ p_{n-1} & q_{n-1} \end{pmatrix} = \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_{n-1} & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_{n-2} & 1 \\ 1 & 0 \end{pmatrix} \dots \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix}.$$

Vidimo, da izgleda ta enačba zelo uravnoteženo, saj je v njej število a_n izraženo na enak način kot ostala števila a_i.

Kaj nam to pove o Fibonaccijevih številih? Pri zlatem rezu je verižni ulomek definiran kot $a_i = 1$ za vsak i. Tko lahko zapišemo našo matrično n-to aproksimacijo kot,

$$\begin{pmatrix} p_n & q_n \\ p_{n-1} & q_{n-1} \end{pmatrix} = \underbrace{\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \dots \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}}_{n-krat} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n.$$

Ker so števila p_n in q_n podana kot števila Fibonaccijevega zaporedja, tako dobimo $\begin{pmatrix} u_{n+1} & u_n \\ u_n & u_{n-1} \end{pmatrix}$. Vidimo, da je $p_n = u_{n+1}$ in $q_n = u_n$. Iz tega sledi:

$$\begin{pmatrix} u_{n+1} & u_n \\ u_n & u_{n-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n.$$

To matriko imenujemo Fibonaccijeva matrika.

Vstavimo nekj n-jev v fibonaccijevo matriko.

<u>n=1</u>:

$$\begin{pmatrix} u_2 & u_1 \\ u_1 & u_0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

<u>n=2</u>:

$$\begin{pmatrix} u_3 & u_2 \\ u_2 & u_1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}.$$

<u>n=3</u>:

$$\begin{pmatrix} u_4 & u_3 \\ u_3 & u_2 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^3 = \begin{pmatrix} 3 & 2 \\ 2 & 1 \end{pmatrix}.$$

<u>n=4</u>:

$$\begin{pmatrix} u_5 & u_4 \\ u_4 & u_3 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^4 = \begin{pmatrix} 5 & 3 \\ 3 & 2 \end{pmatrix}.$$

n=5:

$$\begin{pmatrix} u_6 & u_5 \\ u_5 & u_4 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^5 = \begin{pmatrix} 8 & 5 \\ 5 & 3 \end{pmatrix}.$$

Dobimo: $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 3 & 2 \\ 2 & 1 \end{pmatrix}, \begin{pmatrix} 5 & 3 \\ 3 & 2 \end{pmatrix}, \begin{pmatrix} 8 & 5 \\ 5 & 3 \end{pmatrix}$. Fibonaccijevo matriko bi lahko zlahka preverili s Fibonaccijevimi števili brez predhodnega znanja o lastnostih verižnih ulomkov. Od sedaj naprej bomo uporabljali le še Fibonaccijevo matriko, na verižne ulomke bomo pa pozabili.

Trditev 1 *Za n-to aproksimacijo, podano z verižnim ulomkom*

$$\frac{p_n}{q_n} = a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \cfrac{1}{a_5 + \ddots}}}},$$

velja formula $p_n q_{n-1} - p_{n-1} q_n = (-1)^n$.

Dokaz: Verižni ulomek $\frac{p_n}{q_n}$ lahko zapišemo v obliki matrike, in sicer:

$$\begin{pmatrix} p_n & q_n \\ p_{n-1} & q_{n-1} \end{pmatrix} = \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_{n-1} & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_{n-2} & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix}.$$

Izraz $p_n q_{n-1} - p_{n-1} q_n$ predstavlja ravno determinanto zgornjga izraza.

$$det \begin{pmatrix} p_n & q_n \\ p_{n-1} & q_{n-1} \end{pmatrix} = p_n q_{n-1} - p_{n-1} q_n$$

Vemo, da za determinante v splošnem velja: $det(AB) = det(A)det(B)$.
Poglejmo si determinanto za i-to matriko:

$$det \begin{pmatrix} a_i & 1 \\ 1 & 0 \end{pmatrix} = a_i * o - 1 = -1$$

Vidimo, da ima vsaka matrika take oblike determinanto enako -1. Zgornji izraz je na desni strani sestavljen iz samih matrik take oblike. Teh matrik je n, in zato iz tega sledi $\underbrace{(-1)(-1)\ldots(-1) = (1)^n}_{n}$.
Iz tega vidimo $p_n q_{n-1} - p_{n-1} q_n = (-1)^n$.
S tem je trditev dokazana.

2 Preskakovanje Fibonaccijevih števil

Označimo matriko $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ s Q:

$$Q = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

Q je Fibonaccijeva matrika. Opazimo, da lahko matriko Q^{2n} zapišemo kot $Q^{2n} = Q^n * Q^n$. V našem primeru dobimo:

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

Iz tega izraza vidimo, da za vsak n velja:
1. $u_{2n+1} = u_n^2 + u_{n+1}^2$ in
2. $u_{2n} = u_n(u_{n+1} + u_{n-1})$.
Za Fibonaccijeva števila vemo, da velja $u_{n+1} = u_n + u_{n-1}$. Iz te enčbe izrazimo $u_{n-1} = u_{n+1} - u_n$. Tako iz točke 2. sledi:

$$u_{2n} = u_n(u_{n+1} + u_{n+1} - u_n) = u_n(2u_{n+1} - u_n).$$

Primer. Pogledami pri $n = 5$. Vemo, da je $u_5 = 5$ in $u_6 = 8$. Iz točke 1. in 2. dobimo:
$u_{2*5+1} = u_{11} = u_5^2 + u_6^2 = 5^2 + 8^2 = 89$ in
$u_{2*5} = u_{10} = u_5(2u_6 - u_5) = 5(2 * 8 - 5) = 55$.

Naša naloga je ohraniti dober numerični približek za zlati rez ϕ. Vemo, da je dobra aproksimacija za ϕ podana z razmerjem $\frac{u_{n+1}}{u_n}$, pri čemer sta u_{n+1} in u_n Fibonaccijevi števili. Iz enačb 1. in 2. vidimo, da lahko števili u_{2n+1} in u_{2n} neposredno izračunamo iz u_{n+1} in u_n brez predhodnega računanja vmesnih Fibonaccijevih števil. Na primer, števili u_{21} in u_{20} lahko izračunamo iz u_{11} in u_{10}. Na ta način lahko pospešimo izračun za dobro aproksimacijo ϕ. To pomeni, da z manj računanja pridemo do boljšega približka ϕ. Naprimer, poznamo u_2 in u_3. Iz u_2 in u_3 lahko izračunamo u_4 in u_5. Nadalje lahko izračunamo u_8 in u_9, sledi izračun u_{16} in u_{17}, in tako naprej. To je dober način za računanje približka ϕ, saj nas zanima razmerje in ne vmesna števila. Večji je n, boljši približek dobimo.

Zanima nas razmerje $\frac{u_{n+1}}{u_n}$, saj je $\phi = \frac{u_{n+1}}{u_n}$. Iz tega sledi naravno vprašanje. Ali lahko razmerje $\frac{u_{2n+1}}{u_{2n}}$ izrazimo z razmerjem $\frac{u_{n+1}}{u_n}$? Seveda je odgovor da. Dobimo:

$$\frac{u_{2n+1}}{u_{2n}} = \frac{u_n^2 + u_{n+1}^2}{u_n(2u_{n+1} - u_n)} = \frac{1 + (\frac{u_{n+1}}{u_n})^2}{2\frac{u_{n+1}}{u_n} - 1}.$$

Označimo $\frac{u_{n+1}}{u_n}$ z r. Tako dobimo:

$$\frac{u_{2n+1}}{u_2 n} = \frac{1+r^2}{2r-1}.$$

Ker nam ni potrebno računati še vseh vmesnih števil med n in $2n$, nam to izjemno pospeši računanje za približek zlatega reza. Oglejmo si, kako naša formula deluje za nekaj n-jev.

Vemo: $r = \frac{u_{n+1}}{u_n}$, $\frac{u_{2n-1}}{u_{2n}} = \frac{1+r^2}{2r-1}$ in $\phi = 1,618033988749894848\ldots$.

Prvi korak: $n = 1$
$u_1 = 1$ in $u_2 = 1 \Rightarrow r = \frac{1}{1} = 1$
$\frac{u_{2n+1}}{u_{2n}} = \frac{u_2}{u_3} = \frac{1+1^2}{2*1-1} = \frac{2}{1} = 2$

Drugi korak: $n = 2$
Iz prvega koraka vidimo, da je $u_3 = 2$ in $u_2 = 1$.
$u_2 = 1$ in $u_3 = 2 \Rightarrow r = \frac{2}{1} = 2$
$\frac{u_{2n+1}}{u_{2n}} = \frac{u_5}{u_4} = \frac{1+2^2}{2*2-1} = \frac{5}{3} = 1,66\ldots$

Tretji korak: $n = 4$
Iz drugega koraka vidimo, da je $u_4 = 3$ in $u_5 = 5$.
$u_4 = 3$ in $u_5 = 5 \Rightarrow r = \frac{5}{3}$
$\frac{u_{2n+1}}{u_{2n}} = \frac{u_9}{u_8} = \frac{1+(\frac{5}{3})^2}{2*\frac{5}{3}-1} = \frac{34}{21} = 1,619\ldots$

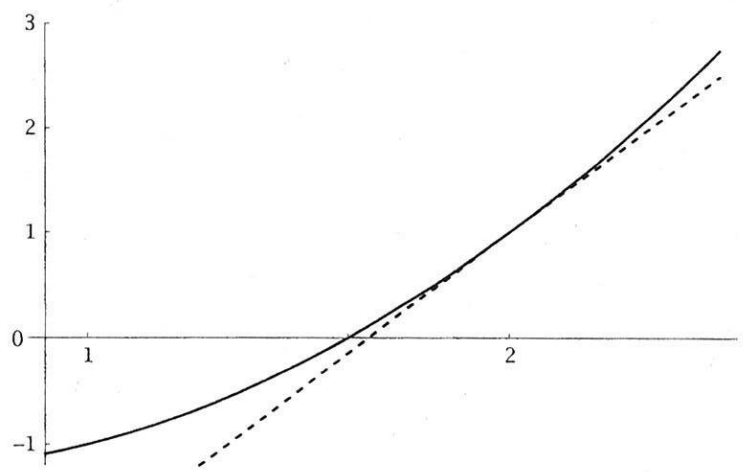
Četrti korak: $n = 8$
Iz tretjega koraka vidimo, da je $u_8 = 21$ in $u_9 = 34$.
$u_8 = 21$ in $u_9 = 34 \Rightarrow r = \frac{34}{21}$
$\frac{u_{2n+1}}{u_{2n}} = \frac{u_{17}}{u_{16}} = \frac{1+(\frac{34}{21})^2}{2*\frac{34}{21}-1} = \frac{1597}{987} = 1,618034\ldots$

Peti korak: $n = 16$
Iz četrtega koraka vidimo, da je $u_{16} = 987$ in $u_{17} = 1597$.
$u_{16} = 987$ in $u_{17} = 1597 \Rightarrow r = \frac{1597}{987}$
$\frac{u_{2n+1}}{u_{2n}} = \frac{u_{33}}{u_{32}} = \frac{1+(\frac{1597}{987})^2}{2*\frac{1597}{987}-1} = 1,618033988749\ldots$

Po petih korakih dobimo približek za ϕ na 12 mest natančno. Kot vidimo, je transformacija $r \mapsto \frac{1+r^2}{2r-1}$ veliko preprostejša za računanje kot pa vsa Fibonaccijeva števila in posledično tudi Fibonaccijeva matrika. Še vedno pa ostaja vprašanje, zakaj ta metoda deluje. Kako je možno, da se $\frac{1+r^2}{2r-1}$ tako hitro približuje številu ϕ.

To preverimo z Newton-Raphsonovo metodo, ali po nekaterih virih samo Newronovo metodo. Ta metoda je dobra za aproksimacijo rešitev enačb oblike $x^2 - x - 1 = 0$.
Iščemo $x = \phi$. To je vrednost kjer krivulja $y = x^2 - x - 1$ seka abcisno os (tj. $y = 0$). Recimo, da je $\phi = 2$ (to pomeni, da krivulja seka abcisno os v točki 2).

$$x = 2 \Rightarrow y = 1$$



Točka $(2, 1)$ leži na premici. Nato narišemo tangento na krivuljo v točki $(2, 1)$ in pogledamo točke, ki so blizu $x = 2$. Iz slike vidimo, da sta krivulja in tangenta na to krivuljo v točki $(2, 1)$ na abcisni osi zelo skupaj. S tem, da vemo, kje krivulja seka abcisno os, lahko ocenimo presečišče krivulje z abcisno osjo. Kot vidimo, sta si ti točki zelo blizu. Z računanjem dobimo enačbo tangente.

$$x^2 - x - 1 = y$$

Z odvodom dobimo smerni koeficient tangente k: $y' = 2x - 1$, pri $x = 2$ je $y' = 3$. Iz tega sledi, da je smerni koeficient tangente enak 3.

$$k = 3$$

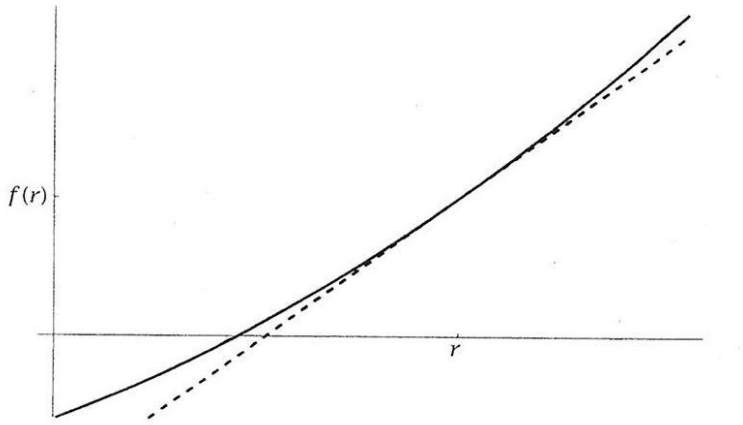
Iz $k = 3$ in dane točke skozi katero gre tangenta, dobimo enačbo tangente:

$$y = 3x - 5.$$

Zanima nas, kje tangenta seka abcisno os. Gledamo vrednost pri $y = 0$ in dobimo $\phi \approx \frac{5}{3}$.
Izkaže se, da je naša transformacija $r \mapsto \frac{1+r^2}{2r-1}$ prikrita Newtoova metoda. Z naslednjo trditvijo bomo dokazalu to metodo.

Trditev 2 *Želimo aproksimirati rešitev enačbe $f(x) = 0$, pri čemer že poznamo aproksimacijo r. Newtonova tangentna metoda da novo aproksimacijo $r - \frac{f(r)}{f'(r)}$.*

Dokaz: Želimo pokazati, da Newtonova metoda vedno da novo aproksimacijo $r - \frac{f(r)}{f'(r)}$. Najprej poiščemo enačbo tangente na krivuljo $y = f(x)$ v točki $(r, f(r))$.



Smerni koeficient tangente je $f'(r)$. Iz tega dobimo enačbo tangente, in sicer $y = f'(r)x + f(r) - f'(r)r$. Iščemo vrednost, kjer tangenta seka abcisno os (tj. $y = 0$). In dobimo $x = r - \frac{f(r)}{f'(r)}$. Tako dobimo aproksimacijo za Newtonovo metodo. S tem je trditev dokazana.

Sedaj vemo, da nam Newtonova metoda poda aproksimacijo $r - \frac{f(r)}{f'(r)}$. To uporabimo pri enačbi $x^2 - x - 1 = 0$, iz česar dobimo Fibonaccijevo transformacijo:

$$f(x) = x^2 - x - 1 \Rightarrow f'(x) = 2x - 1.$$

$$r - \frac{f(r)}{f'(r)} = r - \frac{r^2 - r - 1}{2r - 1} = \frac{2r^2 - r - r^2 + r + 1}{2r - 1} = \frac{r^2 + 1}{2r - 1}.$$

Tako smo dobili novo aproksimacijo $r - \frac{f(r)}{f'(r)}$. Opazimo, da ima Newtonova metoda pomembno vlogo pri računanju približkov za presečišča krivulj z abcisno osjo. Uporabljamo jo predvsem takrat, kadar verižni ulomki ne obstajajo ali pa so preveč zahtevni za zapis.

3 Lucasova števila s praštevilskimi indeksi

Naj bo p praštevilo in L_p Lucasovo število s praštevilskim indeksom. Lastnost, da za vsako praštevilo p velja, da je število $L_p - 1$ deljivo s p, je prvi opazil nek študent na londonski univerzi. Zanimalo ga je, če to drži za vsako praštevilo, zato je naslovil vprašanje na tamkajšnje matematike, in tako je nastal nov problem. V tem razdelku bomo dokazali to lastnost.

Najprej poglejmo za prvih nekaj p-jev.
$\underline{p = 2}$: $L_2 - 1 = 3 - 1 = 2 \qquad (= 2 * 1)$.
$\underline{p = 3}$: $L_3 - 1 = 4 - 1 = 3 \qquad (= 3 * 1)$.
$\underline{n = 5}$: $L_5 - 1 = 11 - 1 = 10 \qquad (= 5 * 2)$.
$\underline{n = 7}$: $L_7 - 1 = 29 - 1 = 28 \qquad (= 7 * 4)$.
$\underline{n = 11}$: $L_{11} - 1 = 199 - 1 = 198 \qquad (= 11 * 18)$.

Vidimo, da ta lastnost drži za prvih nekaj p-jev. Vendar nas zanima, ali ta lastnost drži za poljubno praštevilo p. Avtor na ta problem ni gledal kot na Lucasova števila, ampak je opazil povezavo z malim Fermatovim izrekom.

Izrek 3 (Mali Fermatov izrek) *Naj bo p praštevilo. Za vsako celo število a velja $a^p \equiv a \pmod{p}$. To pomeni, da kadar vzamemo celo število a in ga pomnožimo s samim seboj p-krat in odštejemo a, dobimo število deljivo s p.*

Splošna formula za Lucasova števila je $L_n = \phi^n + \psi^n$, pri čemer je $\phi = \frac{1+\sqrt{5}}{2}$ in $\psi = \frac{1-\sqrt{5}}{2}$. Poskusimo dokazati, da je $\phi^p + \psi^p - 1$ deljivo s p, pri čemer je p praštevilo. Opazimo, da je $\phi + \psi = 1$. Iz tega sledi:

$$\phi^p + \psi^p - 1 = \phi^p + \psi^p - \phi - \psi = (\phi^p - \phi) + (\psi^p - \psi).$$

Ta izraz je sestavljen iz $\phi^p - \phi$ in $\psi^p - \psi$, pri čemer oba dela spominjata na izraz v malem Fermatovem izreku. Vendar pridemo do problema, saj ϕ in ψ nista celi števili in zato ne sledi, da sta izraza $\phi^p - \phi$ in $\psi^p - \psi$ deljiva s p, saj tudi ta izraza nista celi števili. Videli bomo, da vseeno obstaja povezava mad malim Fermatovim izrekom in našim problemom.

Čeprav $\phi^p - \phi$ in $\psi^p - \psi$ nista celi števili, pa skupaj tvorita celo število ki se obnaša kot $n^p - n$, ki jo po malem Fermatovem izreku deljiv s p. S tem je naš problem rešen.

Lucasova števila smo definirali kot vsoto dveh Fibonccijevih števil:

$$L_n = u_{n-1} + u_{n+1}.$$

Ta izraz lahko zapišemo tudi v obliki Fibonaccijeve matrike kot:

$$Q^n = \begin{pmatrix} u_{n+1} & u_n \\ u_n & u_{n-1} \end{pmatrix}.$$

Lucasovo število je enako vsoti diagonalnih elementov v matriki.

Pri vsaki kvadratni matriki A rečemo vsoti diagonalnih elementov sled in označimo z $sl(A)$.
Primer.

$$sl\begin{pmatrix} 3 & 4 & 4 \\ 1 & 2 & 1 \\ 5 & 7 & 6 \end{pmatrix} = 3 + 2 + 6 = 11.$$

Iz tega vidimo, da lahko zapišemo n-ti člen Lucasovega zaporedja kot $L_n = sl(Q^n)$. Zanima nas število $L_p - 1$. Število 1 lahko zapišemo kot $sl(Q)$. Potrebno je dokazati, da za vsako praštevilo p sledi, da je izraz $sl(Q^p) - sl(Q)$ deljiv s p. Za sled velja $sl(Q^p) - sl(Q) = sl(Q^p - Q)$, zato želimo pokazati, da p deli $sl(Q^p - Q)$. Ta izraz je zelo podoben izrazu v malem Fermatovem izreku. V izreku nastopa $n^p - n$, kjer je n celo število, v našem problemu pa nastopa $sl(Q^p - Q)$, kjer je Q matrika s celimi števili.
Zato sklepamo, če je M katerakoli matrika s celimi števili, je $sl(M^p - M) = sl(M^p) - sl(M)$ deljiva s p.

Poglejmo si primere za nekaj p-jev in 2×2 matriko.
$\underline{p = 2}$: $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

$$M^p = M^2 = \begin{pmatrix} a^2 + bc & ab + bd \\ ac + cd & bc + d^2 \end{pmatrix}$$

$$sl(M^2) = a^2 + bc + bc + d^2 = a^2 + 2bc + d^2$$

$$sl(M) = a + d$$

Ali je $sl(M^2) - sl(M) = a^2 + 2bc + d^2 - a - d$ deljiva z 2? Da. Izraz $2bc$ je deljiv z 2, saj je večkratnik števila 2. Po malem Frematovem izreku sledi, da sta izraza $a^2 - a$ in $d^2 - d$ deljiva z 2.

$\underline{p = 3}$: $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

$$sl(M) = a + d$$

$$sl(M^3) = a^3 + d^3 + 3abc + 3bcd$$

$$sl(M^3) - sl(M) = a^3 + d^3 + 3abc + 3bcd - a - d$$

Ali je $sl(M^3) - sl(M) = a^3 + d^3 + 3abc + 3bcd - a - d$ deljiva s 3? Da. Izraza $3abc$ in $3bcd$ sta deljiva s 3, saj sta večkratnika števila 3. Izraza $a^3 - a$ in $d^3 - d$ sta deljiva s 3 po malem Fermatovem izreku.

V vsakem primeru iz $sl(M^p - M)$ dobimo izraz, ki je deljiv s p in števila oblike $a^p - a$ ter $d^p - d$, za katera pa velja da so deljiva s p po malem Fermatovem izerku. Z večanjem števila p dobimo zelo zapletene izraze, zato dokaza za sploše p ni preprosto dobiti.

Trditev 4 *Naj bosta A in B poljubni $m \times m$ matriki s celoštevilskimi koeficienti in naj bo p praštevilo. Tedaj p deli $sl((A + B)^p - A^p - B^p)$.*

Dokaz: Sledi kasneje.

Zgornja trditev pomaga rešiti trenutni problem. Kot v poglavju 3 lahko tudi tukaj nemudoma preidemo na poljubne tri matrike s celoštevilskimi koeficienti. Kar pomeni, da p deli $sl((A + B + C)^p - A^p - B^p - C^p)$.
V našem primeru vzamemo $Q = A + B + C$, kjer so matrike A, B, C enake:

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \qquad B = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \qquad C = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

Za vsak p velja, da je $A^p = A$ in da sta B^p in C^p ničelni matriki. Iz tega sledi, da je za vsak p, $sl(a^p + B^p + C^p) = 1$. Iz tega sledi, da p deli $sl(Q^p) - 1$.

4 Problem sledi

Potrebno je dokazati še trditev 4, ki pove, da za poljubni 2×2 matriki s celoštevilskimi koeficienti velja, da praštevilo p deli $sl((A+B)^p - A^p - B^p)$.

Primer. $p = 3$

$$(A+B)^2 - A^2 - B^2 = A^2 + AB + BA + B^2 - A^2 - B^2 = AB + BA$$

$$A = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \qquad B = \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix}$$

$$A*B = \begin{pmatrix} a_1b_1 + a_2b_3 & a_1b_2 + a_2b_4 \\ a_3b_1 + a_4b_3 & a_3b_2 + a_4b_4 \end{pmatrix} \qquad B*A = \begin{pmatrix} a_1b_1 + a_3b_2 & a_2b_1 + a_4b_2 \\ a_1b_3 + a_3b_4 & a_2b_3 + a_3b_4 \end{pmatrix}$$

V splošnem imamo $A * B \neq B * A$. Vendar velja: $sl(AB) = sl(BA)$!

V primeru treh matrik A, B, C gledamo kot na $sl(A(BC)) = sl((BC)A)$. Sled se ne spremeni če damo matriko A iz začetka na konec, kar velja tudi v splošnem, in sicer,

$$sl(AM_1 \dots M_k) = sl(M_1 \dots M_k A).$$

Takoj opazimo, da ciklično množenje matrik ne spremeni vrednosti sledi. Tej lastnosti pravimo ciklanje sledi.

Primer. $p = 3$

$$(A+B)^3 - A^3 - B^3 = (AAB + ABA + BAA) + (ABB + BAB + BBA)$$

Radi bi dokazali, da imajo posamezni produkti med seboj enako sled in hrati tudi, da je seštevek sledi posameznih produktov v istem oklepaju deljiv s 3. Opazimo, da se v obeh oklepajih ena matrika cikla. Iz tega sledi, da imajo vsi ti produkti enako sled.

Za poljubno praštevilo p bo izraz $(A+B)^p - A^p - B^p$ vseboval vse možne zmnožke matrik A in B dolžine p, razen zmnožkov oblike $AA \dots A$ in $BB \dots B$, saj se izničita.

Če hočemo, da je sled deljiva s p, moramo te nize pogrupirati v enake ciklične tipe in dokazati, da je število nizov v vsakem tipu deljiv s p.

Primer. $p = 5$

$AAAAB$	$AAABB$	$AABAB$	$AABBB$	$ABABB$	$ABBBB$
$AAABA$	$AABBA$	$ABABA$	$ABBBA$	$BABBA$	$BBBBA$
$AABAA$	$ABBAA$	$BABAA$	$BBBAA$	$ABBAB$	$BBBAB$
$ABAAA$	$BBAAA$	$ABAAB$	$BBAAB$	$BBABA$	$BBABB$
$BAABA$	$BAAAB$	$BAABA$	$BAABB$	$BABAB$	$BABBB$

V vsakem bloku je vsak produkt dobljen s prvim v bloku s ciklično permutacijo. Vsi nizi v istem bloku imajo enako sled in vidimo, da jih je v vsakem bloku 5. Iz tega sledi, da je seštevek sledi deljiv s 5.

Iz zgornjega primera vidimo, da lahko za vsako praštevilo p zgrupiramo produkte v bloke z istim cikličnim tipom. V vsakem bloku pričakujemo p zmnožkov matrik, saj moramo niz dolžine p obrniti p-krat, da pridemo na prvotno mesto. To velja, saj je p praštevilo, kar nam tudi pove spodnja trditev. Če p ne bi bilo praštevilo, ta princip ne bi deloval.

Trditev 5 *Naj bo p praštevilo in naj bo vsaj en element v nizu različen od ostalih. Niz dolžine p dobi pri ciklanju prvotno obliko po p korakih.*

Dokaz: Dokaz smo naredili pri diskretni matematiki.

Literatura

[1] Keith Ball: *Strange Curves, Counting Rabbits and Other Mathematical Explortions*, Princteon University Press, 2003.

[2] $http://sl.wikipedia.org/wiki/Fermatovmaliizrek$