Aljaž Bertoncelj

Lucasova števila, matrike in problem deljivosti

Seminarska naloga pri predmetu Seminar I, 10. 5. 2011

Fakulteta za matematiko in fiziko, Univerza v Ljubljani

Uvod

Fibonaccijeva števila, ki so starejši bratje Lucasovim, zagotovo sestavljajo najslavnejše zaporedje števil sploh. Skorajda vsak laik je že slišal zanje in v navezi s še popularnejšim zlatim rezom se z njimi srečujejo strokovnjaki na vseh področjih znanosti, umetnosti in celo zabavne industrije.

V pričujočem članku bomo navidez naključno krmarili med različnimi matematičnimi teorijami, dokler ne bomo naposled prišli do glavnega izreka, čigar dokaz je zares matematično lep.

1 Na splošno o Fibonaccijevih in Lucasovih številih

1.1 Fibonaccijeva števila

Fibonaccijevo število f_n je definiramo z rekurzivno formulo $f_n = f_{n-1} + f_{n-2}$, pri čemer velja $f_1 = f_2 = 1$. Običajno v skladu z rekurzivno zvezo na začetek dodamo še ničto Fibonaccijevo število $f_0 = 0$, če želimo, pa lahko zaporedje nadaljujemo tudi v smeri negativnih indeksov in sicer po preprosti aritmetični manipulaciji osnovne rekurzije: $f_{n-2} = f_n - f_{n-1}$.

Rekurzija je relativno počasna metoda računanja novih členov danega zaporedja, zato je precej priročnejša naslednja eksplicitna formula, ki jo poznamo pod (morda ne najbolj upravičenim) imenom *Binetova formula*:

$$f_n = \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right].$$

Pot do nje je z upoštevanjem standardnega postopka zamenjave člena f_n z nastavkom λ^n preprosta in ker smo natanko to formulo vsi izpeljali že vsaj enkrat (in sicer pri Analizi I), bom dokaz izpustil. Zelo pomembni sta konstanti, ki se pojavljata v njej, zato ju bomo posebej poimenovali: $\phi := \frac{1+\sqrt{5}}{2}$ in $\psi := \frac{1-\sqrt{5}}{2}$. Konstanta ϕ je eno najslavnejših iracionalnih števil, ki mu najpogosteje pravimo kar *zlati rez*.

Zapišimo zdaj prejšnjo Binetovo formulo v novi, ličnejši obliki in dodajmo še par identitet, ki nam bodo prišle prav kasneje:

$$f_n = \frac{\phi^n - \psi^n}{\phi - \psi}, \qquad \phi + \psi = 1, \qquad \phi - \psi = \sqrt{5}, \qquad \phi\psi = -1.$$

1.2 Lucasova števila

Obstaja več definicij *Lucasovih števil* L_n, najpogostejša pa je sledeča: $L_n = f_{n-1} + f_{n+1}$ (f_{n-1} in f_{n+1} sta seveda Fibonaccijevi števili ustreznih indeksov). Hitro vidimo, da velja $L_n = f_{n-1} + f_{n+1} = f_{n-2} + f_{n-3} + f_{n-1} + f_n = (f_{n-2} + f_n) + (f_{n-3} + f_{n-1}) = L_{n-1} + L_{n-2}$ in zato lahko Lucasova števila definiramo z isto rekurzivno zvezo kot Fibonaccijeva, le da imamo drugačne začetne pogoje. Zapišimo prvih nekaj členov obeh zaporedij:

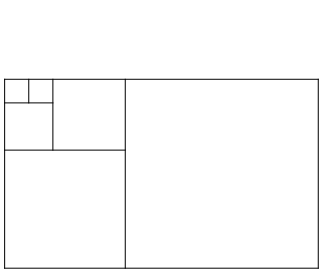
n	0	1	2	3	4	5	6	7	8	9	10
f_n	0	1	1	2	3	5	8	13	21	34	55
L_n	2	1	3	4	7	11	18	29	47	76	123

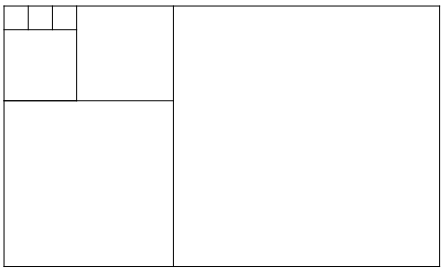
Hiter račun nam potrdi, da velja zveza $f_n = \frac{L_{n-1}+L_{n+1}}{5}$, za konec tega uvodnega poglavja pa navedimo še pet kapljic iz pravega morja zanimivih lastnosti obeh zaporedij:

$$f_n | f_{kn}, \qquad f_{2n} = L_n f_n, \qquad D(f_m, f_n) = f_{D(m,n)},$$

$$\sum_{k=1}^{n} f_k^2 = f_n f_{n+1}, \qquad \sum_{k=1}^{n} L_k^2 = L_n L_{n+1} - 2.$$

Prvo lastnost bomo dokazali kasneje, ko bomo vpeljali zelo uporabne *Fibonaccijeve matrike*, pri zadnjih dveh vsotah pa si navkljub samoponujajoči se indukciji oglejmo precej zanimivejši geometrijski pristop. Na obeh spodnjih slikah je zgornji levi kvadratek enotski, vsoti pa naj bralec iz ustreznih slik razbere sam.





2 Aproksimacija ϕ in Fibonaccijevi hiperboli

2.1 Rekurzija približkov

Definirajmo $r_n := \frac{f_{n+1}}{f_n}$. Ko zapišemo prvih nekaj členov zaporedja r_n, se za limito že ponuja število ϕ. Preverimo to dejstvo s pomočjo Binetove formule:

$$\lim_{n\to\infty} \frac{f_{n+1}}{f_n} = \frac{\frac{1}{\sqrt{5}} \lim_{n\to\infty} \left(\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n+1} \right)}{\frac{1}{\sqrt{5}} \lim_{n\to\infty} \left(\left(\frac{1+\sqrt{5}}{2}\right)^{n} - \left(\frac{1-\sqrt{5}}{2}\right)^{n} \right)} = \frac{\left(\frac{1+\sqrt{5}}{2}\right)^{n+1}}{\left(\frac{1+\sqrt{5}}{2}\right)^{n}} = \frac{1+\sqrt{5}}{2}.$$

Členi zaporedja r_n so torej vedno boljši približki zlatega reza. Zdaj, ko limito že poznamo, jo lahko poiščemo tudi v sami rekurzivni zvezi in sicer na naslednji način. Enačbo $f_n = f_{n-1} + f_{n-2}$ na obeh straneh delimo z f_{n-1} in dobimo $\frac{f_n}{f_{n-1}} = 1 + \frac{f_{n-2}}{f_{n-1}}$, kar je enako $r_{n-1} = 1 + \frac{1}{r_{n-2}}$. Če oba indeksa povečamo za 1, dobimo $r_n = 1 + \frac{1}{r_{n-1}}$ in po predpostavki, da limita r obstaja, velja $r = 1 + \frac{1}{r}$ oziroma $r^2 - r - 1 = 0$. Rešitvi te enačbe sta natanko števili ϕ in ψ, ker pa je $\psi < 0$ in je očitno, da mora biti r nenegativen, ostane edini kandidat za limito število ϕ.

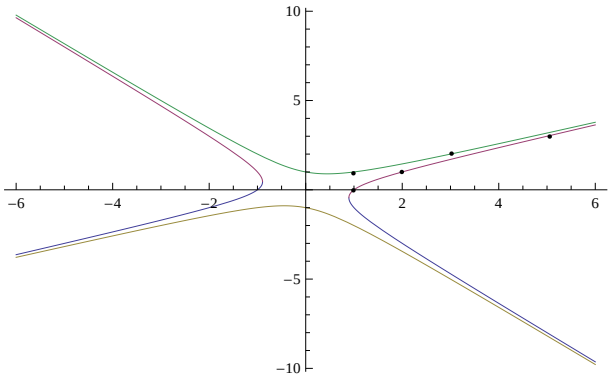
2.2 Fibonaccijevi hiperboli

Začnimo podrazdelek z dokazom naslednje trditve.

Trditev. *Naj bo f_n n-to Fibonaccijevo število. Potem za poljuben n velja:* $f_{n+1}f_{n-1} - f_n^2 = (-1)^n$.

Dokaz. Trditev lahko brez problemov dokažemo s klasično indukcijo, a obstaja bolj prefinjen način. Definirajmo zaporedje $a_n = f_{n+1}f_{n-1} - f_n^2$. Očitno je $a_1 = -1$. Če dokažemo, da sta si vsaka dva zaporedna člena a_{n-1} in a_n nasprotno enaka, torej da je njuna vsota enaka 0, je trditev dokazana. In res: $a_n + a_{n-1} = f_{n+1}f_{n-1} - f_n^2 + f_n f_{n-2} - f_{n-1}^2 = f_{n-1}(f_{n+1} - f_{n-1}) - f_n(f_n - f_{n-2}) = f_{n-1}f_n - f_n f_{n-1} = 0$. ■

Zgornja trditev nas bo pripeljala do para krivulj, ki jima pravimo *Fibonaccijevi hiperboli* in imata cel kup zanimivih lastnosti. Naj bosta p in q po vrsti števec in imenovalec racionalnega približka r_n, torej $p := f_{n+1}$ in $q := f_n$. Sledi, da je $f_{n-1} = f_{n+1} - f_n = p - q$. Zapišimo zdaj zgornjo trditev s substitucijama p in q: $p(p-q) - q^2 = (-1)^n$ oziroma $p^2 - pq - q^2 = (-1)^n$. Dobimo dve t.i. Fibonaccijevi hiperboli s formulama $p^2 - pq - q^2 = \pm 1$. Njuna grafa izgledata takole:



Naj bodo *Fibonaccijeve točke* tiste točke ravnine, ki imajo vsako izmed koordinat enako nekemu (ne nujno istemu) Fibonaccijevemu številu. Na grafu je označenih 5 takih točk: $(1,0)$, $(1,1)$, $(2,1)$, $(3,2)$, $(5,3)$. Vse seveda ležijo v prvem kvadrantu na obeh hiperbolah in če jih drugače predznačimo, dobimo še 15 točk v preostalih treh kvadrantih. Ker vemo, da vrednosti r_n oziroma $\frac{p}{q}$ limitirajo proti ϕ, hitro vidimo, da sta smerna koeficienta obeh skupnih asimptot hiperbol zaporedoma enaka $\frac{1}{\phi}$ in $\frac{1}{\psi}$. Naslednjo trditev bomo dokazali na dva načina, pri čemer bomo pri drugi poti uporabili *Pickov izrek*, ki ga brez dokaza podajamo še pred trditvijo.

Pickov izrek. *Naj bo P preprost večkotnik (brez lukenj in samopresečišč) na celoštevilski kvadratni mreži, ki vsebuje r robnih in i notranjih točk. Potem je njegova ploščina enaka* $S = \frac{r}{2} + i - 1$.

Trditev. *Fibonaccijeve točke so edine celoštevilske točke na obeh Fibonaccijevih hiperbolah.*

Dokaz. Celoštevilske točke so seveda tiste točke, ki imajo celoštevilski koordinati. Naj bo $T(t_1, t_2)$ poljubna taka točka iz prvega kvadranta, ki leži na eni izmed hiperbol. Če jo preslikamo s preslikavo $F : (a, b) \mapsto (b, a-b)$, spet dobimo celoštevilsko točko na hiperbolah: $b^2 - b(a-b) - (a-b)^2 = \ldots = -(a^2 - ab - b^2)$. Razvidno je, da F točko zaporedoma pomika v levo, a pri tem obe koordinati ohranja pozitivni, vse dokler je naposled ne preslika v točko $(1, 1)$, ki edina ne leži *pod* simetralo lihih kvadrantov. Ko se to zgodi, lahko točko $(1, 1)$ začnemo slikati z inverzno preslikavo $F^{-1} : (a, b) \mapsto (a + b, a)$, dokler spet ne dosežemo originalnega T. Kot ste najbrž že opazili, pa preslikava F^{-1} v resnici vsaki Fibonaccijevi točki priredi njeno „naslednico“ in ker je točka $(1, 1)$ Fibonaccijeva, je tudi točka $T(t_1, t_2)$ Fibonaccijeva. Trditev podobno dokažemo za točke iz preostalih treh kvadrantov. ■

Ideja dokaza 2. Predstavljajmo si, da na grafu obeh hiperbol v trikotnike povežemo trojice Fibonaccijevih točk $\{(f_{3k+1}, f_{3k}), (f_{3k+2}, f_{3k+1}), (f_{3k+3}, f_{3k+2})\}$ za $k \in \mathbb{N}_0$. Prvi tak trikotnik bo na primer imel za oglišča točke $(1, 0)$, $(1, 1)$ in $(2, 1)$. Ker so koordinate točk med seboj povezane po že znanih zvezah, lahko z nekaj truda izračunamo, da je ploščina vsakega takega trikotnika natančno $\frac{1}{2}$. Ko ta rezultat vstavimo v Pickov izrek, dobimo $i = S - \frac{r}{2} + 1 = \frac{1}{2} - \frac{3}{2} + 1 = 0$. Če narišemo prvih nekaj trikotnikov, vidimo, da obe hiperboli vsaj v prvem kvadrantu desno od abscise $x = 1$ v celoti ležita znotraj unije naših trikotnikov in jih dejansko sekata le v njihovih oglišči. To pomeni, da bi vsaka druga (Nefibonaccijeva) celoštevilska točka ležala v notranjosti natanko enega izmed trikotnikov, ker pa teh notranjih točk ni ($i = 0$), je trditev dokazana. ■

Pomudimo se še za trenutek pri naših hiperbolah in delimo enakost $p^2 - pq - q^2 = (-1)^n$ s q^2. Dobimo $\frac{p^2}{q^2} - \frac{p}{q} - 1 = \frac{(-1)^n}{q^2}$, kar pa lahko zapišemo tudi kot $r^2 - r - 1 = \frac{(-1)^n}{q^2}$. Ta enačba nam da nekako intuitivno vedeti, da imamo glede na dan imenovalec q najboljši možen približek števila ϕ, torej ničle leve strani enačbe. O približkih bomo še veliko razpravljali v prihodnjih razdelkih.

3 Verižni ulomki in Fibonaccijeve matrike

3.1 Verižni ulomki

Naslednje veliko področje matematike, ki ga bomo le za hip obiskali na našem potovanju, so *verižni ulomki*. Vsako pozitivno število a se da zapisati v obliki (ne nujno končnega) verižnega ulomka, tako da so vsi a_i nenegativna cela števila:

$$a = a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots + \frac{1}{a_n}}}}.$$

Tak verižni ulomek lahko zapišemo tudi v obliki $[a_1, a_2, \ldots, a_n]$, števila a_i pa izračunamo s pomočjo Evklidovega algoritma. Za zgled določimo verižni ulomek števila $\frac{23}{18}$.

$$\begin{aligned} 23 &= \underline{1}\cdot 18 + 5 \\ 18 &= \underline{3}\cdot 5 + 3 \\ 5 &= \underline{1}\cdot 3 + 2 \\ 3 &= \underline{1}\cdot 2 + 1 \\ 2 &= \underline{2}\cdot 1 \end{aligned} \qquad \frac{23}{18} = 1 + \frac{1}{3 + \frac{1}{1 + \frac{1}{1 + \frac{1}{2}}}}$$

Izkaže se tudi, da je verižni ulomek, za katerega je $a_n \neq 0$, končen natanko tedaj, ko predstavlja racionalno število in njegov zapis je enoličen. Iracionalnemu številu ϕ torej pritiče neskončen ulomek, njegove koeficiente a_i pa bomo prepoznali s pomočjo rekurzivne zveze približkov r_n. Spomnimo se, da velja $r_n = 1 + \frac{1}{r_{n-1}}$. Če razpišemo prvih nekaj r_n, ugotovimo, da gre za končne približke neskončnega verižnega ulomka števila ϕ, torej je $r_n = [a_1, a_2, \ldots, a_n]_\phi$ in odtod sledi, da so vsi a_i enaki 1. To pomeni, da je zlati rez najtežje aproksimirati z verižnim ulomkom in je zato na nek način „najbolj iracionalno“ realno število.

3.2 Vpeljava matrik

Oglejmo si poljubno zaporedje verižnih ulomkov oziroma približkov $t_n = [a_1, a_2, \ldots, a_n]$, ki konvergirajo k limiti t. Posamezen člen $t_i = \frac{p_i}{q_i}$ izračunamo tako, da začnemo s številom a_i, vzamemo njegovo obratno vrednost in ji prištejemo a_{i-1}. Nato spet vzamemo obratno vrednost danega racionalnega števila ter ji prištejemo a_{i-2}. Postopek ponavljamo, dokler v zadnjem koraku ne prištejemo še a_1. To „preslikavo“ smo tako slikovito opisali z namenom, da bi v njej prepoznali matriko A_j, ki na vsakem koraku preslika urejen par števca p in imenovalca q na naslednji način:

$$(p, q) \begin{pmatrix} a_j & 1 \\ 1 & 0 \end{pmatrix} = (a_j p + q, p).$$

Vrednost verižnega ulomka t_n torej dobimo tako, da par $(a_n, 1)$ preslikamo s kompozitumom zgornjih preslikav oziroma produktom matrik A_i, ko i teče od $n-1$ do 1:

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

Iščoč lepšo obliko zgornje enačbe, zapišimo še prvi faktor desnega dela v podobni matrični obliki. Da velja $(a_{n-1}, 1) = (1, 0) \begin{pmatrix} a_{n-1} & 1 \\ 1 & 0 \end{pmatrix}$, se bralec z lahkoto prepriča sam. Odtod sledi:

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

Ker imamo opravka z matrikami, lahko izraza, ki predstavljata (p_n, q_n) in (p_{n-1}, q_{n-1}), preprosto zložimo drugega na drugega:

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

Spomnimo se spet, da v primeru kvocientov r_n, ki konvergirajo k ϕ, velja $p_n = f_{n+1}$, $p_{n-1} = q_n = f_n$ in $q_{n-1} = f_{n-1}$, vsi a_i pa so enaki 1. Imamo torej izraz:

$$\begin{pmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n.$$

3.3 Fibonaccijeve matrike

Matrikam, ki so potence matrike $Q = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$, pravimo *Fibonaccijeve matrike*, zdaj pa se z dokazoma naslednjih dveh trditev prepričajmo o koristnosti njihove vpeljave.

Trditev. *Naj bo $\frac{p_n}{q_n}$ vrednost verižnega ulomka $[a_1, \ldots, a_n]$, pri čemer je: $\lim_{n\to\infty} [a_1, \ldots, a_n] = a$. Potem velja: $p_n q_{n-1} - q_n p_{n-1} = (-1)^n$ za vsak n.*

Dokaz. Naj bo n poljubno naravno število. Oglejmo si enakost, ki smo jo izpeljali v prejšnjem razdelku:

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

Če izračunamo *determinante* obeh strani, dobimo na levi $\begin{vmatrix} p_n & q_n \\ p_{n-1} & q_{n-1} \end{vmatrix} = p_n q_{n-1} - q_n p_{n-1}$, na desni pa upoštevajoč, da je determinanta produkta matrik enaka produktu determinant matrik, dobimo $(-1)^n$, saj je $\begin{vmatrix} a_i & 1 \\ 1 & 0 \end{vmatrix} = -1$ za vsak i. ■

Trditev. *Naj bo f_n n-to Fibonaccijevo število. Za vsak $n \in \mathbb{N}$ velja $f_n | f_{kn}$.*

Dokaz. Razpišimo enakost $Q^{n+m-1} = Q^m Q^{n-1}$:

$$\begin{pmatrix} f_{n+m} & f_{n+m-1} \\ f_{n+m-1} & f_{n+m-2} \end{pmatrix} = \begin{pmatrix} f_{m+1} & f_m \\ f_m & f_{m-1} \end{pmatrix} \begin{pmatrix} f_n & f_{n-1} \\ f_{n-1} & f_{n-2} \end{pmatrix} =$$

$$== \begin{pmatrix} f_{m+1}f_n + f_m f_{n-1} & f_{m+1}f_{n-1} + f_m f_{n-2} \\ f_m f_n + f_{m-1} f_{n-1} & f_m f_{n-1} + f_{m-1} f_{n-2} \end{pmatrix}.$$

Odtod sledi identiteta $f_{n+m} = f_n f_{m+1} + f_{n-1} f_m$. Očitno velja, da f_n deli f_{kn} za poljuben n, če je $k = 1$, zato lahko trditev induktivno dokažemo tako, da v pravkar pridobljeno identiteto vstavimo $m = kn$.
Dobimo $f_{n+kn} = f_{(k+1)n} = f_n f_{kn+1} + f_{n-1} f_{kn}$ in takoj vidimo, da sta oba sumanda na desni deljiva s f_n. ■

Posledica. *Obstajajo poljubno dolgi nizi zaporednih Fibonaccijevih števil, med katerimi ni nobeno praštevilo.*

Dokaz. Za poljuben n vzemimo zaporedje $f_{(n+2)!+3}, f_{(n+2)!+4}, \ldots, f_{(n+2)!+(n+2)}$. Indeks prvega Fibonaccijevega števila v zaporedju je očitno deljiv s 3, indeks drugega s 4 ... Po prejšnji trditvi sledi, da je prvo število v zaporedju deljivo z f_3, drugo z f_4 itd. ■

Opomba. Navkljub zgornji posledici do danes še nikomur ni uspelo dokazati, da obstaja neskončno Fibonaccijevih praštevil.

4 Približki in Newtonova metoda

4.1 Hitrejše aproksimiranje zlatega reza

Na popolnoma enak način kot pri dokazu druge trditve prejšnjega podrazdelka lahko bralec sam iz enakosti $Q^{2n} = Q^n Q^n$ izpelje naslednji identiteti:

$$f_{2n+1} = f_n^2 + f_{n+1}^2, \qquad f_{2n} = f_n(2f_{n+1} - f_n).$$

Če torej poznamo približek $r_n = \frac{f_{n+1}}{f_n}$ lahko takoj neposredno izračunamo približek $r_{2n} = \frac{f_{2n+1}}{f_{2n}}$. Na tak način hitro pridemo do zelo natančnih aproksimacij, a lahko računanje še pospešimo, če zapišemo kar iskani kvocient:

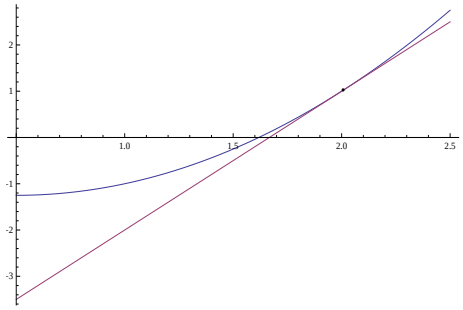
$$r_{2n} = \frac{f_{2n+1}}{f_{2n}} = \frac{f_n^2 + f_{n+1}^2}{f_n(2f_{n+1} - f_n)} : f_n^2 = \frac{1 + \frac{f_{n+1}^2}{f_n^2}}{2\frac{f_{n+1}}{f_n} - 1} = \frac{1 + r_n^2}{2r_n - 1}.$$

Pričnimo s približkom $r_1 = 1$. Po komaj šestih korakih dobimo zaporedoma približke r_2, r_4, r_8, r_{16}, r_{32} in r_{64}, med katerimi je zadnji že na 26 decimalnih mest natančen!

Enačba, ki smo jo izpeljali s pomočjo Fibonaccijevih matrik se torej izkaže za precej koristno, kako bi do nje lahko prišli še drugače, pa si bomo ogledali v naslednjem podrazdelku.

4.2 Newtonova metoda

Na spodnji sliki je graf funkcije $f(x) = x^2 - x - 1$. Recimo, da želimo poiskati njene ničle in se nam zdi, da se ena giba nekje v okolici $x_1 = 2$. Po *Newtonovi metodi* boljšo aproksimacijo dobimo tako, da izračunamo, kje absciso seka tangenta na funkcijo f v točki $f(2)$. Elementaren račun nam pove, da ima presečišče kooordinato $x_2 = \frac{5}{3}$. Na enak način (tokrat s tangento skozi $f(\frac{5}{3})$) izračunamo nov približek $x_3 = \frac{34}{21}$. Oba približka se nam zdita nekam sumljivo znana in res, velja $x_2 = r_4$, $x_3 = r_8$.



Izpeljimo zdaj v slošnem aproksimiranje rešitev enačbe $f(x) = 0$, če je dan prvi približek r. Izhajamo iz dobro znane enačbe $y - y_0 = k(x - x_0)$ in ko upoštevamo, da je smerni koeficient tangente na f enak odvodu funkcije f,

dobimo $f(r) - 0 = f'(r)(r - x)$. Odtod izračunamo nov približek $x = r - \frac{f(r)}{f'(r)}$. Ko vstavimo našo prvotno funkcijo $f(x) = x^2 - x - 1$, dobimo znan izraz:

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

5 Glavni izrek

Prišli smo do zadnjega razdelka in čaka nas le še dokaz naslednjega presenetljivega izreka. Dokaz bo kot večina tega članka bolj razpravljalne narave, zato bo zavoljo večje ilustrativnosti vseboval tudi nekatere stranpoti, ki bi se jim formalni dokaz vsekakor izognil.

Izrek. *Naj bo p praštevilo in L_p p-to Lucasovo število. Potem p deli $L_p - 1$.*

Dokaz.

- Zapišimo $L_p - 1$ v nekoliko drugačni obliki: $L_p - 1 = \phi^p + \psi^p - 1 = \phi^p + \psi^p - (\phi + \psi) = (\phi^p - \phi) + (\psi^p - \psi)$. Tak zapis bi nas moral spomniti na *Fermatov mali izrek*, ki pravi, da $p|m^p - m$ za vsak cel m. Problem je seveda v tem, da ϕ in ψ še zdaleč nista celi števili, a se izkaže, da p kljub temu deli njuno vsoto. To se da neposredno dokazati s sredstvi *algebraične teorije števil*, mi pa bomo ubrali drugo pot.

- Spomnimo se matrike $Q = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ in potenc $Q^n = \begin{pmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{pmatrix}$. Opazimo, da je *sled* prve enaka 1, sled Q^n pa $f_{n+1} + f_{n-1}$. Dokazujemo torej, da $p|tr(Q^p) - tr(Q)$. Pa premislimo, ali to velja za poljubno 2×2 matriko M nad $\mathbb{Z}$. Poskusimo s $p = 2$ in pri tem upoštevajmo aditivnost sledi.

  $$tr(\begin{pmatrix} a & b \\ c & d \end{pmatrix}^2 - \begin{pmatrix} a & b \\ c & d \end{pmatrix}) = a^2 + bc + bc + d^2 - a - d = 2bc + (a^2 - a) + (d^2 - d).$$

  Prvi člen vsote je očitno deljiv z 2, druga dva pa 2 delita po Fermatovem izreku. Torej naša predpostavka velja za najmanjše praštevilo, bralec pa se lahko na isti način sam prepriča, da zanesljivo drži tudi za $p = 3$.

- Na vajah iz *algebre II* smo se prepričali, da $p|(a + b)^p - a^p - b^p$, pri čemer sta a in b poljubni celi števili, sicer pa za dokaz tega ne potrebujemo drugega kot *binomski izrek* in nekaj srednješolske kombinatorike, zato ga prepuščam bralcu. Za nas je pomembnejše vprašanje, ali velja tudi $p|tr((A + B)^p - A^p - B^p)$, kjer sta A in B poljubni kvadratni matriki. Poglejmo si spet primer, ko je $p = 2$.

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

  Upoštevali smo, da velja $tr(AB) = tr(BA)$. Če si pobliže ogledamo to lastnost sledi, opazimo, da imajo enako sled pravzaprav vsi produkti danih matrik, ki so ciklični premiki drug drugega, npr. $A_1 A_2 \dots A_n$ in $A_k A_{k+1} \dots A_n A_1 \dots A_{k-1}$. Lastnost ima prikladno ime: *cikličnost sledi*.

Poskusimo še s $p = 3$:

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

$= tr(AAB+ABA+BAA)+tr(ABB+BAB+BBA) = 3tr(AAB)+3tr(ABB).$

Preštejmo, koliko produktov matrik nam da izraz $(A+B)^p - A^p - B^p$. Na vsakem izmed p mest imamo na izbiro dve matriki, torej je vseh natanko $2^p - 2$, ker se produkta $A \dots A$ in $B \dots B$ odštejeta. Ne vemo pa, ali so si med seboj različni. V primeru da so si, imamo torej vse možne p-mestne besede (razen dveh) iz črk A in B, zato jih lahko razbijemo na disjunktno unijo ekvivalenčnih razredov glede na prej omenjeno relacijo cikličnosti, ki je očitno ekvivalenčna. Ker je vsaka beseda ekvivalentna še $(p-1)$-tim cikličnim premikom, ima vsak razred moč p in velja $p|tr(A+B)^p - A^p - B^p$.

- Dokažimo, da za poljuben $p \in \mathbb{P}$ velja zgornja predpostavka. Če bi bil p sestavljen (npr. 4), bi namreč našli enake cikle (npr. $ABAB$, ki se ne spremeni po cikličnem premiku za 2), ti pa zmanjšajo moč ekvivalenčnih razredov. Za $p = 4$ bi bil recimo eden izmed ekvivalenčnih razredov le moči 2 in sicer $\{ABAB, BABA\}$. Kaj takega se pri praštevilski dolžini p produkta ne more zgoditi, ker mora dolžina vsakega premika, ki bi besedo preslikal samo vase, deliti p. To pa pomeni, da se poljubna beseda v začetno lego vrne šele po natanko p premikih, ko preteče ves svoj ekvivalenčni razred.

- Zdaj, ko vemo, da $p|tr((A+B)^p - A^p - B^p)$, je preskok na $p|tr((A+B+C)^p - A^p - B^p - C^p)$ poslednja vaja iz aritmetike, ki jo nalagam bralcu, saj moramo le še ustrezno definirati matrike A, B in C.

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

  Takoj vidimo, da velja $A^p = A$, $B^p = 0$ in $C^p = 0$. Sledi

  $$tr((A+B+C)^p - A^p - B^p - C^p) = tr(\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^p - \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}) = L_p - 1,$$

  torej $p|L_p - 1$.

■

Zaključek

Še enkrat smo se lahko prepričali, da se že pri reševanju najelementarnejših problemov preplatajo mnoge veje matematike in da vedno obstaja več poti do končne rešitve, med katerimi so najnenavadnejše običajno tudi najhitrejše.

Z nekoliko drugačne perspektive smo spoznali unikatnost konstante ϕ ter začutili neizmernost presenetljivih lastnosti, ki jih premoreta obe zaporedji. Naj omenim, da poleg Fibonaccijevih obstajajo tudi Lucasove matrike, ki jih definiramo na popolnoma enak način in niso nič manj uporabne pri dokazovanju opazk, med katerimi imajo nekatere že 700-letno zgodovino.

Literatura

[1] K.Ball: *Strange Curves, Counting Rabbits and other Mathematical Explorations*, Princeton University Press, Princeton and Oxford, 2003.

[2] Ross Honsberger: *Mathematical Gems III*, The Mathematical Asociation of America, 1985.

[3] Nikolai N. Vorobev: *Fibonacci Numbers*, New Classic Library, 1983.

[4] Stephen A. Parry: *Unique Properties of the Fibonacci and Lucas Sequences*, prosto dostopno s spleta.

[5] David Gajser: *Verižni ulomki*, prosto dostopno s spleta, 2009.

[6] Alenka Trpin: *Pickov izrek*, prosto dostopno s spleta, 2009.