# Diofantske aproksimacije – od problema kalendara do razbijanja šifara

Andrej Dujella

PMF, Matematički odsjek, Sveučilište u Zagrebu
HAZU, Razred za matematičke, fizičke i kemijske znanosti
e-mail: duje@math.hr
URL: https://web.math.pmf.unizg.hr/~duje/

# Diofant Aleksandrijski

Diofant Aleksandrijski – starogrčki matematičar koji je živio u III. st. prije Krista

Najznačajnije mu je djelo *Aritmetika* koje se sastoji od 13 knjiga algebarskih problema, jednadžbi i sustava jednadžbi, od kojih je sačuvano 6.

Veliki utjecaj na indijsku i arapsku matematiku, a od XVII. stoljeća i na zapadnoeuropsku (Fermat, Euler).

Po njemu je nazvan niz pojmova moderne matematike (diofantske jednadžbe, diofantske aproksimacije, Diofantove četvorke, itd.).

# Diofantske jednadžbe i diofantske aproksimacije

**Pellova jednadžba**: $x^2 - 2y^2 = 1$

$$0 < x - y\sqrt{2} = \frac{1}{x + y\sqrt{2}} < \frac{1}{2y\sqrt{2}} < \frac{1}{2y}$$

$$\left|\sqrt{2} - \frac{x}{y}\right| < \frac{1}{2y^2}$$

beskonačno mnogo rješenja: $(x, y) = (3, 2)$, $(17, 12)$, $(99, 70)$, $(577, 408)$, $(3363, 2378)$, $(19601, 13860)$, $(114243, 80782)$, $(665857, 470832)$, ...

**Thueova jednadžba** (primjer): $x^3 - 2y^3 = 1$

$$\left| \sqrt[3]{2} - \frac{x}{y} \right| < \frac{1}{3y^{\mathbf{3}}}$$

nema rješenja (osim trivijalnog $(x, y) = (1, 0)$)

**Sustav Pellovih jednadžbi**: $x^2 - 2y^2 = 1$, $z^2 - 3y^2 = 1$

$$\left| \sqrt{2} - \frac{x}{y} \right| < \frac{1}{2y^{\mathbf{2}}}, \quad \left| \sqrt{3} - \frac{z}{y} \right| < \frac{1}{2y^{\mathbf{2}}}$$

nema rješenja (osim trivijalnog $(x, y, z) = (1, 0, 1)$)

# Diofantske aproksimacije

Diofantske aproksimacije se bave pitanjem koliko se dobro zadani iracionalni broj može aproksimirati s pomoću racionalnih brojeva. Pitamo se koliko mala može biti udaljenost iracionalnog broja $\alpha$ i racionalnog broja $p/q$, tj. broj $|\alpha - \frac{p}{q}|$. Pritom ćemo tu razliku uspoređivati s $q$, tj. za veće nazivnike očekujemo bolje aproksimacije.

Ako za fiksirani $q$ izaberemo razlomak $p/q$ s nazivnikom $q$ koji je najbliži broju $\alpha$, bit će zadovoljena nejednakost

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q}.$$

Pitanje: Može li se i koliko poboljšati ovaj jednostavni rezultat?

**Dirichletov teorem:** $\alpha$ iracionalan broj, postoji beskonačno mnogo racionalnih brojeva $p/q$ takvih da je

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}.$$

**Simultane aproksimacije:** $\alpha_1, \ldots, \alpha_n$ iracionalni brojevi, postoji beskonačno mnogo $n$-torki racionalnih brojeva $\frac{p_1}{q}, \ldots \frac{p_n}{q}$ takvih da je $\left|\alpha_i - \frac{p_i}{q}\right| < \frac{1}{q^{1+1/n}}$

**Thueov teorem:** $\alpha$ algebarski broj stupnja $d \geq 2$, nejednadžba $\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^m}$ ima samo konačno mnogo rješenja $p/q$ ako je $m > \frac{d}{2} + 1$

# Problem kalendara

Postoje dvije očite prirodne jedinice vremena: dan i (Sunčeva) godina. Kako ih međusobno uskladiti (budući da Sunčeva godina ne sadrži cijeli broj dana)?

$$\begin{aligned} 1 \text{ godina} &= 365 \text{ dana } \ 5 \text{ sati } \ 48 \text{ minuta } \ 46 \text{ sekundi} \\ &= 365.242199 \text{ dana} \end{aligned}$$

Kalendar u kome broj dana u godini ne bi bio prirodan broj bio bi vrlo nepraktičan.

Ako bi uzeli da svaka godina ima 365 dana (takav se kalendar koristio u starom Egiptu), tada bi se svake četvrte godine kalendarska godina razlikovala od Sunčeve godine otprilike za 1 dan, pa bi se ubrzo izgubila veza između datuma u godini i godišnjih doba.

Rješenje: neke godine imaju 365 dana (obične godine), a neke 366 dana (prijestupne godine).

Kako to napraviti pa da prosječan broj dana u godini bude što bliže broju 365.242199?

Općenitije, postavlja se pitanje kako dani realni broj što bolje aproksimirati pomoću razlomaka s relativno malim nazivnicima. Odgovor na to pitanje daju nam tzv. **verižni ili neprekidni razlomci**.

# Verižni razlomci

Konačni verižni razlomak je izraz oblika

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{}{\ddots + \cfrac{1}{a_n}}}},$$

gdje je $a_0$ cijeli, a $a_1, a_2, \ldots, a_n$ prirodni brojevi. Ovaj izraz kraće zapisujemo sa $[a_0; a_1, a_2, \ldots, a_n]$. Jasno je da se sređivanjem konačnog verižnog razlomka dobiva običan razlomak, tj. racionalan broj. Obrnuto, svaki racionalan broj $\alpha = \frac{p}{q}$ može se zapisati u gornjem obliku. To se onda zove razvoj broja $\alpha$ u verižni razlomak. Razvoj je jedinstven ako zahtjevamo da je $a_n \neq 1$.

Brojevi $a_i$ zovu se parcijalni kvocijenti od $\alpha$. To su upravo kvocijenti koji se dobiju primjenom **Euklidovog algoritma** na brojeve $p$ i $q$:

$$\begin{aligned} p &= q \cdot a_0 + r_1 \\ q &= r_1 \cdot a_1 + r_2 \\ r_1 &= r_2 \cdot a_2 + r_3 \\ &\vdots \\ r_{n-1} &= r_n \cdot a_n \,. \end{aligned}$$

Racionalan broj $\frac{p_k}{q_k} = [a_0; a_1, \ldots, a_k]$ za $k \leq n$ zovemo $k$-ta konvergenta od $\alpha$.

Svaki iracionalan broj $\alpha$ se može zapisati u obliku beskonačnog verižnog razlomka $\alpha = [a_0; a_1, a_2, \ldots]$. To znači da je

$$\alpha = \lim_{k \to \infty} \frac{p_k}{q_k}.$$

Brojnici i nazivnici konvergenti zadovoljaju rekurzije

$$p_0 = a_0, \quad p_1 = a_0 a_1 + 1, \quad p_k = a_k p_{k-1} + p_{k-2}\,,$$

$$q_0 = 1, \quad q_1 = a_1, \quad q_k = a_k q_{k-1} + q_{k-2}\,.$$

Iz rekurzivne formule je jasno da niz nazivnika $(q_k)_{k\geq 0}$ strogo raste, te također da je $q_k \geq F_k$, gdje je $F_k$ $k$-ti Fibonaccijev broj.

Pomoću ovih formula se indukcijom dokazuje važna formula

$$p_{k-1}q_k - p_k q_{k-1} = (-1)^k$$

koja povezuje susjedne konvergente. Ona povlači da su brojevi $p_k$ i $q_k$ relativno prosti, što znači da su razlomci $\frac{p_k}{q_k}$ potpuno skraćeni. Formula također pokazuje da su parne konvergente manje od neparnih. Štoviše, za iracionalan broj $\alpha$ vrijedi

$$\frac{p_0}{q_0} < \frac{p_2}{q_2} < \frac{p_4}{q_4} < \cdots < \alpha < \cdots < \frac{p_5}{q_5} < \frac{p_3}{q_3} < \frac{p_1}{q_1}.$$

Kažemo da je razlomak $\frac{p}{q}$ dobra aproksimacija realnog broja $\alpha$ ako je greška aproksimacije $|\alpha - \frac{p}{q}|$ najmanja među svim razlomcima s nazivnikom $\leq q$, tj.

$$\left|\alpha - \frac{p}{q}\right| = \min\left\{\left|\alpha - \frac{x}{y}\right| \,:\, x \in \mathbb{Z},\ y \in \mathbb{N},\ y \leq q\right\}.$$

Može se pokazati da su uz ovakvu definiciju konvergente $\frac{p_k}{q_k}$ dobre aproksimacije. Primijetimo međutim da ne vrijedi obrat. Naime, ako je $\frac{p}{q}$ dobra aproksimacija, onda je $\frac{p}{q}$ jednak ili nekoj konvergenti od $\alpha$ ili nekoj tzv. sekundarnoj konvergenti od $\alpha$, gdje je sekundarna konvergenta izraz oblika

$$\frac{p_{k,l}}{q_{k,l}} = \frac{p_{k+1} \cdot l + p_k}{q_{k+1} \cdot l + q_k} \quad \text{za } l = 1, 2, \ldots, a_{k+2} - 1.$$

Kod prethodne definicije dobre aproksimacije zahtjeva se da je apsolutna greška minimalna. Možda je prirodnije zahjevati da je relativna greška minimalna, tj. tražiti veću točnost od razlomaka s većim nazivnikom. Tako se može reći da je $\frac{p}{q}$ dobra aproksimacija realnog broja $\alpha$ ako je izraz $|q\alpha - p|$ minimalan, tj. ako je

$$|q\alpha - p| = \min\{|y\alpha - x| \,:\, x \in \mathbb{Z},\ y \in \mathbb{N},\ y \leq q\}.$$

Može se pokazati su u ovom slučaju dobre aproksimacije upravo konvergente od $\alpha$. Štoviše, vrijedi da je

$$|q_k\alpha - p_k| \leq |q\alpha - p|$$

za sve $q \leq q_{k+1}$.

Konvergente verižnih razlomaka kao konkretne realizacije aproksimacija iz Dirichletovog teorema:

$$\left|\alpha - \frac{p_k}{q_k}\right| < \frac{1}{q_k^2}.$$

"Obrat": Ako je $\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q^2}$, onda je $\frac{p}{q} = \frac{p_k}{q_k}$ za neki $k$.

Poopćenje: Ako je $\left|\alpha - \frac{p}{q}\right| < \frac{c}{q^2}$ za $c > 0$, onda je

$$\frac{p}{q} = \frac{rp_{k+1} \pm sp_k}{rq_{k+1} \pm sq_k},$$

za neki $k$, te $r$ i $s$ takve da je $rs < 2c$.

Preciznija ocjena greške aproksimacije:

$$\frac{1}{(a_{k+1}+2)q_k^2} < \left|\alpha - \frac{p_k}{q_k}\right| < \frac{1}{a_{k+1}q_k^2}.$$

# Problem kalendara (nastavak)

Navedena svojstva verižnih razlomaka sugeriraju nam da bi upravo njih trebalo koristiti u rješenju problema kalendara. Trajanje jedne Sunčeve godine je eksperimentalna veličina. Stoga nema smisla razmatrati je li taj broj racionalan ili iracionalan. Mi ćemo taj broj zamijeniti s njegovom približnom vrijednošću

$$\alpha = 365 + \frac{5\text{ h }\ 48\text{ m }\ 46\text{ s}}{1\text{ dan}} = 365 + \frac{20926\text{ s}}{86400\text{ s}} = 365\frac{10463}{43200}.$$

Broj $\alpha$ je racionalan pa je njegov razvoj u verižni razlomak konačan.

Primjenom Euklidovog algoritma na brojeve 43200 i 10463 dobivamo:

$$\begin{aligned} 43200 &= 10463 \cdot 4 + 1348 \\ 10463 &= 1348 \cdot 7 + 1027 \\ 1348 &= 1027 \cdot 1 + 321 \\ 1027 &= 321 \cdot 3 + 64 \\ 321 &= 64 \cdot 5 + 1 \\ 64 &= 1 \cdot 64\,. \end{aligned}$$

Stoga je $\alpha = [365;\, 4,\, 7,\, 1,\, 3,\, 5,\, 64]$. Konvergente razlike $\alpha - 365$ su redom

$$\frac{1}{4},\ \frac{7}{29},\ \frac{8}{33},\ \frac{31}{128},\ \frac{163}{673},\ \frac{10463}{43200}.$$

Svaka od ovih konvergenti daje jedno rješenje problema kalendara. Tako je kod prve konvergente prosječno trajanje godine $365\frac{1}{4}$ dana. To točno znači da je svaka četvrta godina prijestupna. Općenito, nazivnik konvergente nam daje duljinu ciklusa, a brojnik nam daje broj prijestupnih godina u svakom ciklusu. Vidljivo je da peta i šesta konvergenta daju vrlo nepraktična rješenja. Stoga razmotrimo pobliže kalendare koje nam daju prve četiri konvergente.

| broj prijestupnih godina u ciklusu | duljina ciklusa | prosječno trajanje godine | greška |
|---|---|---|---|
| 1 | 4 | 365 d 6 h 00 m 00 s | −11 m 14 s |
| 7 | 29 | 365 d 5 h 47 m 35 s | +1 m 11 s |
| 8 | 33 | 365 d 5 h 49 m 05 s | −19 s |
| 31 | 128 | 365 d 5 h 48 m 45 s | +1 s |

Prva konvergenta nam daje upravo julijanski kalendar koji je po zamisli egipatskog astronoma Sosigena uveo rimski car Julije Cezar 45. godine prije Krista. Druga mogućnost nije dobra jer je jednako kompliciranа kao treća, a puno je netočnija. Ovu treću mogućnost (8 prijestupnih godina u ciklusu od 33 godine) predložio je perzijski znanstvenik Omar Khayyan u 11. stoljeću.

Četvrta mogućnost je vrlo precizna. Greška od jedne sekunde je praktički zanemariva. Ovaj kalendar bi zahtjevao samo jednu modifikaciju u julijanskom kalendaru. Naime, da se svaka 128. godina proglasi običnom, a ne prijestupnom. Zaista, julijanski kalendar u svakom ciklusu od 128 godina sadrži 32 prijestupne godine.

Ovaj kalendar je predložio ruski astronom Medler 1864. godine i s čisto matematičkog stajališta ovo se može smatrati najboljim rješenjem problema kalendara. Možda je jedini njegov nedostatak taj da broj 128 nije dovoljno "okrugli".

Stoga je i danas opće prihvaćen gregorijanski kalendar u kojem se u svakom ciklusu od 400 godina nalazi 97 prijestupnih. Preciznije, u gregorijanskom kalendaru prijestupna je svaka četvrta godina s tim da ako je godina djeljiva sa 100, a nije djeljiva sa 400 (takvih ima 3 u svakom ciklusu od 400 godina), onda se takva godina smatra običnom, a ne prijestupnom. Prosječno trajanje godine u ovom kalendaru je 365 d 5 h 49 m 12 s, pa greška iznosi $-26$ s.

Gregorijanski kalendar je 1582. godine uveo papa Grgur XIII. Osnovna značajka ovog kalendara je jednostavnost provjere je li dana godina prijestupna ili ne. Naime, kriteriji djeljivosti sa 4, sa 100 i sa 400 su vrlo jednostavni. Pritom, preciznost aproksimacije kod ovog kalendara nije idealna, ali je puno bolja nego kod julijanskog kalendara.

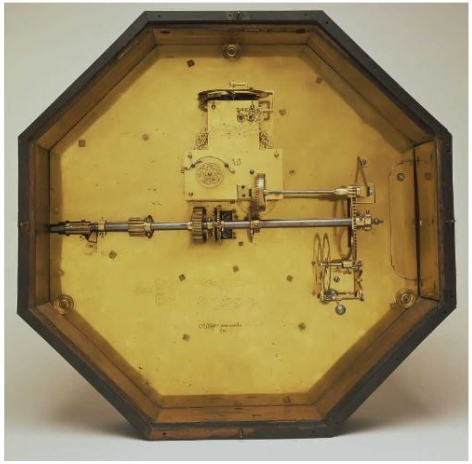
Ovdje treba još reći i to da u 16. stoljeću za trajanje jedne Sunčeve godine nije bila poznata tako precizna vrijednost kao danas. Naime, tada se smatralo da jedna Sunčeva godina ima 365 dana 5 sati 49 minuta 16 sekundi, pa je uz tu pretpostavku greška kod gregorijanskog kalendara iznosila samo $+4$ sekunde.

# Huygensov planetarij

Christiaan Huygens, nizozemski matematičar, fizičar i astronom: 1680. dizajnirao planetarij pomoću verižnih razlomaka.

Planetarij je opisivao relativno kretanje tada poznatih šest planeta (Merkur, Venera, Zemlja, Mars, Jupiter, Saturn) oko Sunca. Realiziran je pomoću zupčanika u kojima je omjer između broja zubaca vodoravne osovine i pripadnog koncentričnog prstena približno jednak omjeru između orbitalnog perioda Zemlje i odgovarajućeg planeta.

| planet | Merkur | Venera | Zemlja | Mars | Jupiter | Saturn |
|---|---|---|---|---|---|---|
| omjer | $\frac{25335}{105190}$ | $\frac{64725}{105190}$ | 1 | $\frac{197836}{105190}$ | $\frac{1247057}{105190}$ | $\frac{3095277}{105190}$ |
| konver. | $\frac{p_5}{q_5} = \frac{33}{137}$ | $\frac{p_5}{q_5} = \frac{8}{13}$ | | $\frac{p_5}{q_5} = \frac{79}{42}$ | $\frac{p_3}{q_3} = \frac{83}{7}$ | $\frac{p_1}{q_1} = \frac{59}{2}$ |
| zupci | 33 : 137 | 32 : 52 | 60 : 60 | 158 : 84 | 166 : 14 | 118 : 4 |



# Glazbena ljestvica

Pokušajmo odrediti (u nekom smislu) idealni broj tonova u glazbenoj ljestvici. Ako želimo uskladiti oktave (tonove kod kojih jedan ima $2$ puta veću frekvenciju od drugog) i kvinte (tonove kod kojih jedan ima $3/2$ puta veću frekvenciju od drugog), dolazimo do pitanja može li $2^n$ biti približno jednako $\left(\frac{3}{2}\right)^m$ za neke prirodne brojeve $m$ i $n$.

Jasno je da ovi brojevi ne mogu biti doslovno jednaki jer je u jednakosti $2^{m+n} = 3^m$ broj na lijevoj strani paran, a onaj na desnoj strani neparan. Stoga želimo što bolje aproksimirati iracionalni broj $\log_2 3$ racionalnim brojem $\frac{m+n}{m}$.

Jedno zadovoljavajuće rješenje je $m = 12$, $n = 7$, dakle, 12 polutonova u oktavi sa 7. polutonom kao kvintom.

$$\log_2 3 = [1; 1, 1, 2, 2, 3, 1, 5, 2, 23, 2, 2, 1, 1, 55, 1, 4, 3, \ldots]$$

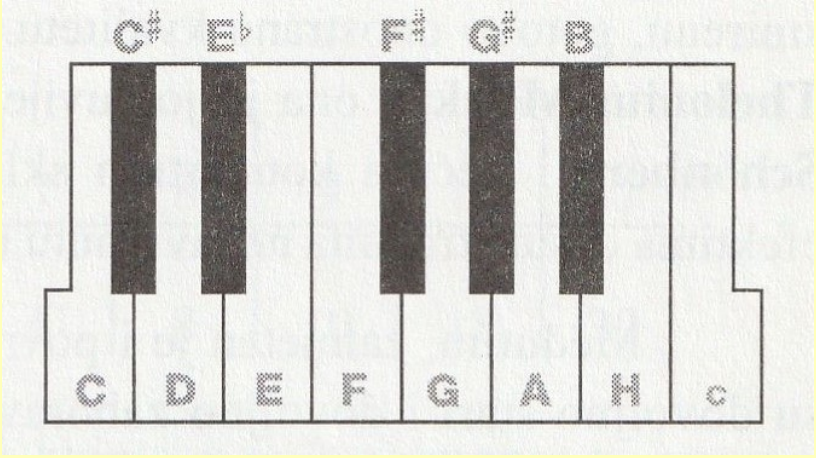
konvergente: $1,\ 2,\ \frac{3}{2},\ \frac{8}{5},\ \frac{19}{12},\ \frac{65}{41},\ \frac{84}{53},\ \frac{485}{306},\ \ldots$

$$(m, n) = (1, 0), (1, 1), (2, 1), (5, 3), (12, 7),$$
$$(41, 24), (53, 31), (306, 179), \ldots$$

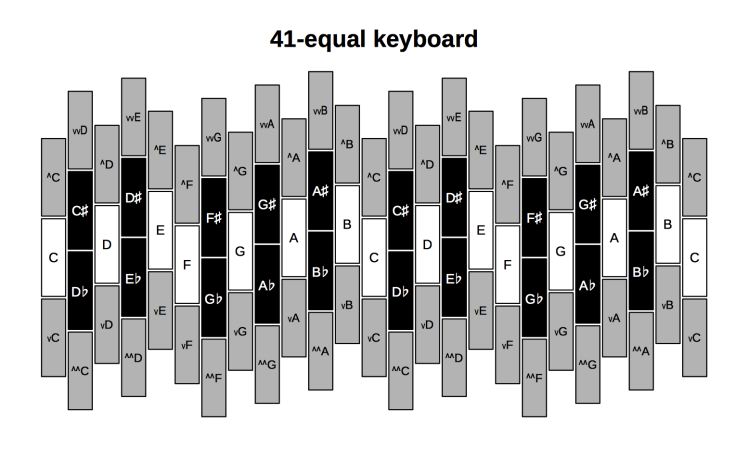
$$E^{\flat} \leftarrow B \leftarrow F \leftarrow C \rightarrow G \rightarrow D \rightarrow A \rightarrow E \rightarrow H \rightarrow F^{\sharp} \rightarrow C^{\sharp} \rightarrow G^{\sharp}$$

| $E^{\flat}$ | B | F | C | G | D | A | E | H | $F^{\sharp}$ | $C^{\sharp}$ | $G^{\sharp}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $2^2\left(\frac{2}{3}\right)^3$ | $2^2\left(\frac{2}{3}\right)^4$ | $2\left(\frac{2}{3}\right)$ | 1 | $\frac{3}{2}$ | $\left(\frac{1}{2}\right)\left(\frac{3}{2}\right)^2$ | $\left(\frac{1}{2}\right)\left(\frac{3}{2}\right)^3$ | $\left(\frac{1}{2}\right)^2\left(\frac{3}{2}\right)^4$ | $\left(\frac{1}{2}\right)^2\left(\frac{3}{2}\right)^5$ | $\left(\frac{1}{2}\right)^3\left(\frac{3}{2}\right)^6$ | $\left(\frac{1}{2}\right)^4\left(\frac{3}{2}\right)^7$ | $\left(\frac{1}{2}\right)^4\left(\frac{3}{2}\right)^8$ |

| C | $C^{\sharp}$ | D | $E^{\flat}$ | E | F | $F^{\sharp}$ | G | $G^{\sharp}$ | A | B | H | c |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1.068 | 1.125 | 1.185 | 1.266 | 1.333 | 1.424 | 1.5 | 1.602 | 1.688 | 1.778 | 1.898 | 2 |



Sljedeća konvergenta $\frac{65}{41}$ znači da bi oktavu trebalo podijeliti na 41 "mikrotonova", s time da bi kvinta bila 24. mikroton. Broj od 41 tonova u oktavi je prevelik za praktičnu izvedbu glazbe (osim možda elektronske).



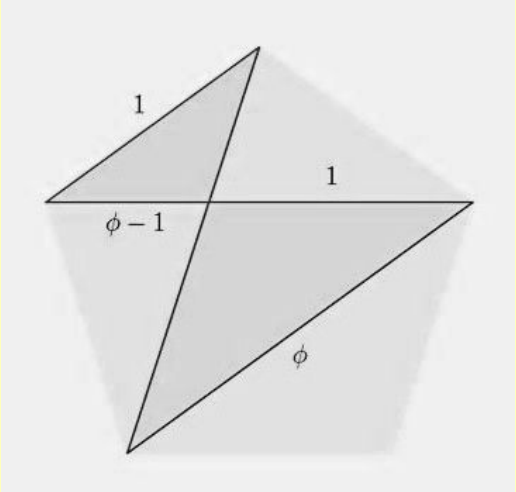

Više o ovoj temi i drugim vezama matematike i glazbe može se naći u knjigama:

Z. Šikić: Matematika i muzika, HMD, 1999.

Z. Šikić, Z. Šćekić: Matematika i muzika, Profil, 2013.

# Zlatni rez i Fibonaccijevi brojevi

Omjer duljine dijagonale i duljine stranice pravilnog peterokuta jednak je zlatnom rezu $\phi$.




$$\phi : 1 = 1 : (\phi - 1), \quad \phi = \frac{1}{\phi - 1}$$

$$\phi^2 - \phi - 1 = 0, \quad \phi = \frac{1 + \sqrt{5}}{2}$$

$$\phi = [1; 1, 1, 1, \ldots] = [\bar{1}]$$

$$p_0 = 1,\ p_1 = 2,\ p_k = p_{k-1} + p_{k-2}$$

$$q_0 = 1,\ q_1 = 1,\ q_k = q_{k-1} + q_{k-2}$$

"pomaknuti" **Fibonaccijevi brojevi**

$(F_0 = 0,\ F_1 = 1,\ F_k = F_{k-1} + F_{k-2})$

$p_k = F_{k+2},\quad q_k = F_{k+1}$

$$1,\ 2,\ \frac{3}{2},\ \frac{5}{3},\ \frac{8}{5},\ \frac{13}{8},\ \frac{21}{13},\ \frac{34}{21},\ \frac{55}{34},\ \frac{89}{55},\ \frac{144}{89},\ \ldots$$

$$\phi \approx 1.618034,\quad \frac{89}{55} \approx 1.618182,\quad \frac{144}{89} \approx 1.617978$$

Općenito, kvadratne iracionalnosti (iracionalni brojevi koji su rješenja kvadratne jednadžbe s racionalnim koeficijentima) imaju periodičan razvoj u verižni razlomak.

Primjeri:

$$\sqrt{2} = [1; 2, 2, 2, \ldots] = [1; \bar{2}]$$

$$\sqrt{3} = [1; 1, 2, 1, 2, \ldots] = [1; \overline{1, 2}]$$

$$\sqrt{43} = [6; \overline{1, 1, 3, 1, 5, 1, 3, 1, 1, 12}]$$

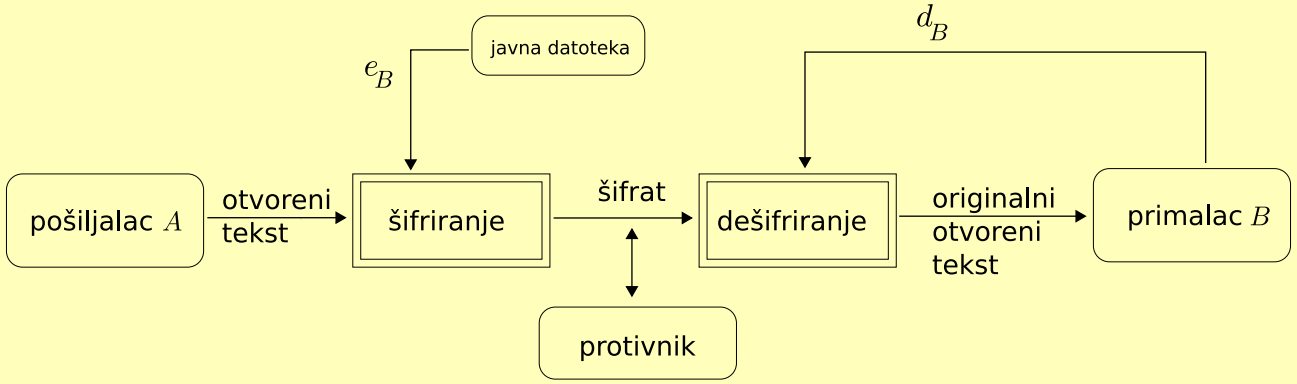
$$\frac{9 + \sqrt{7}}{6} = [1; 1, 15, \overline{1, 14}]$$

# Kriptosustavi s javnim ključem

Sigurnost klasičnih šifara (od Cezarove, Vigenerèove, Playfairove pa do Enigme i drugih naprava za šifranje) leži u tajnosti ključa.

Problem: Kako sigurno razmijeniti ključ?

Ideja: javni ključ $e_K$ za šifriranje, tajni (osobni) ključ $d_K$ za dešifriranje. Ovdje $e_K$ mora biti tzv. jednosmjerna funkcija, tj. nju se računa lako, a njezin inverz teško.



**RSA kriptosustav** (Rivest, Shamir, Adleman (1977)):

- izaberemo tajno dva velika prosta broja $p$ i $q$,
- izračunamo $n = p \cdot q$ i $\varphi(n) = (p-1)(q-1) = n+1-p-q$ (Eulerova funkcija),
- izaberemo $e$ tako da je $e < \varphi(n)$ i $\text{nzd}(e, \varphi(n)) = 1$,
- izračunamo tajno $d$ takav da je $d \cdot e \equiv 1 \pmod{\varphi(n)}$ (linearna diofantska jednadžba $d \cdot e - t \cdot \varphi(n) = 1$, rješava se proširenim Euklidovim algoritmom).

$(n, e)$ – javni ključ

$(p, q, d)$ – tajni (osobni) ključ

šifriranje: $e_K(x) = x^e \bmod n$

dešifriranje: $d_K(y) = y^d \bmod n$

Provjera:
$d_K(e_K(x)) \equiv d_K(x^d) \equiv x^{de} \equiv x^{t\varphi(n)+1} \equiv (x^{\varphi(n)})^t \cdot x \equiv x \bmod n$ (Eulerov teorem)

- sigurnost leži u teškoći faktorizacije velikih brojeva: onaj tko zna ili može otkriti faktore $p$ i $q$ javno poznatog broja $n$, taj može izračunati $\varphi(n) = (p-1)(q-1)$, te saznati tajni eksponent $d$ rješavajući linearnu diofantsku jednažbu $d \cdot e - t \cdot \varphi(n) = 1$.

## Wienerov napad - bez poznavanja faktorizacije od $n$, uz pretpostavku da je tajni eksponent $d$ relativno mali

Iz jednakosti $d \cdot e - t \cdot \varphi(n) = 1$, vidimo da je $t/d$ jako dobra aproksimacija broja $e/\varphi(n)$. Broj

$$\varphi(n) = (p-1)(q-1) = n - p - q + 1$$

nije poznat napadaču, jer ne zna $p$ i $q$. No, $\varphi(n) \approx n$ može poslužiti kao zadovoljavajuća aproksimacija. Tako dobivamo da je broj $t/d$, koji sadrži tajni podatak $d$, dobra aproksimacija broja $e/n$ koji je u potpunosti javan.

Ako $d$ nije velik ($d < \frac{1}{3}\sqrt[4]{n}$), onda vrijedi

$$\left|\frac{e}{n} - \frac{t}{d}\right| < \frac{1}{2d^2},$$

pa $t/d$ mora biti neka konvergenta verižnog razlomka od $e/n$. Napad se može proširiti i na nešto veće vrijednosti od $d$:

- $d < 2^{30} n^{0.25}$ – korištenjem karakterizacije aproksimacija kod kojih je greška manja od $\frac{c}{d^2}$ umjesto $\frac{1}{2d^2}$;
- $d < n^{0.292}$ – korištenjem **LLL-algoritma** (Lenstra-Lenstra-Lovász), koji se može shvatiti kao višedimenzionalna verzija verižnih razlomaka.

Diofantske aproksimacije se koriste u napadima i na druge kriptosustave s javnim ključem: LUC (poopćeni Fibonaccijevi brojevi), KMOV (eliptičke krivulje), Merkle-Hellman (problem ruksaka).

Hvala Vam na pozornosti!