

IZDAJA DRUŠTVO MATEMATIKOV, FIZIKOV IN ASTRONOMOV SLOVENIJE

ISSN 0473-7466

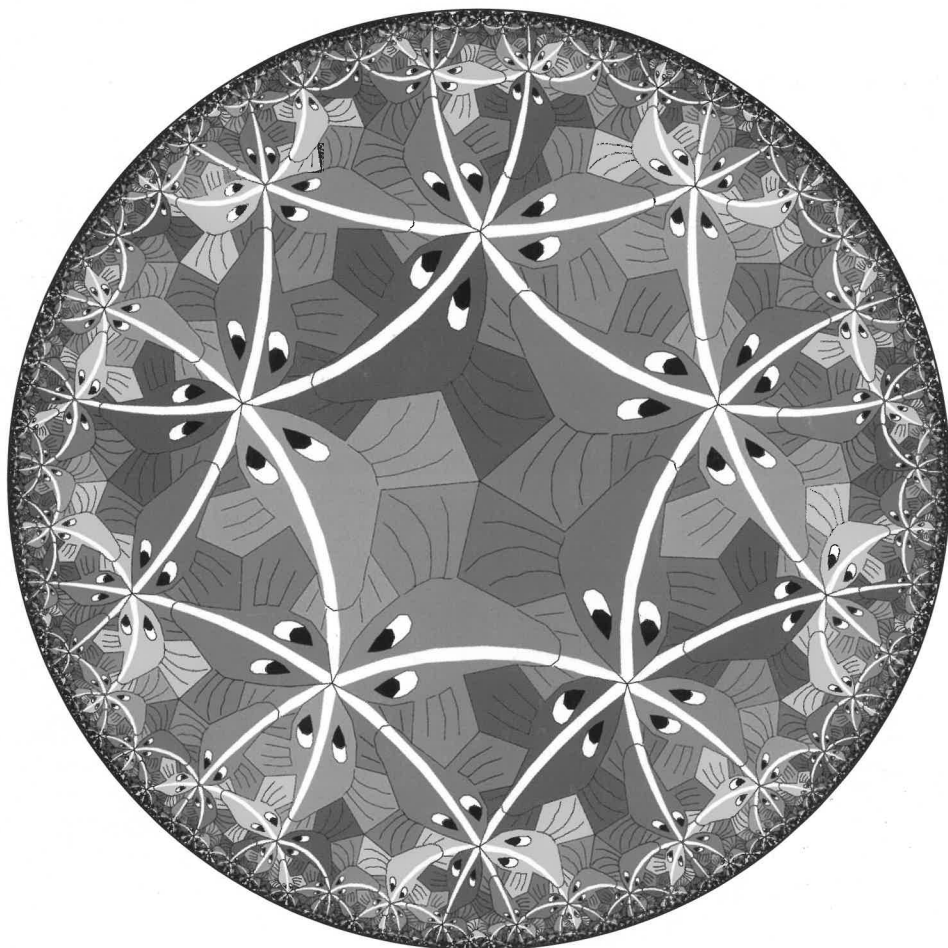
**ODPISANO**

2003

Letnik 50

5

# **OBZORNIK ZA MATEMATIKO IN FIZIKO**



## OBZORNIK ZA MATEMATIKO IN FIZIKO

Glasilo Društva matematikov, fizikov in astronomov Slovenije  
Ljubljana, SEPTEMBER 2003, letnik 50, številka 5, strani 129–160

**Naslov uredništva:** DMFA-založništvo, Jadranska ul. 19, p. p. 2964, 1001 Ljubljana.  
**Spletna stran:** <http://www.fmf.uni-lj.si/~zaloznistvo/omf/> **Telefon:** (01) 4766 553, 4232 460. **Telefaks:** (01) 2517281. **Devizna nakazila:** SKB banka d. d., Ajdovščina 4, Ljubljana. **SWIFT:** SKBASIX. **Transakcijski račun:** 03100-1000018787.

**Uredniški odbor:** Mirko Dobovišek (glavni urednik), Roman Drnovšek (urednik za matematiko in odgovorni urednik), Marko Zgonik (urednik za fiziko), Alenka Klokočovnik (društvene novice), Marjan Jerman (tehnični urednik).

Jezikovno pregledal Janez Juvan, računalniško oblikoval Martin Zemljič. Natisnjeno v Tiskarni KURIR v nakladi 1450 izvodov.

Člani društva prejema Obzornik brezplačno. Celoletna članarina je 4000 SIT, za študente 2000 SIT. Naročnina v knjigarnah in za ustanove je 8000 SIT, za tujino 30 EUR. Posamezna številka za člane je 800 SIT, stare številke 520 SIT.

DMFA je včlanjeno v Evropsko matematično društvo (EMS), v Mednarodno matematično unijo (IMU), v Evropsko fizikalno društvo (EPS) in v Mednarodno združenje za čisto in uporabno fiziko (IUPAP). DMFA ima pogodbo o recipročnosti z Ameriškim matematičnim društvom (AMS).

Revija izhaja praviloma vsak drugi mesec. Sofinancira jo Ministrstvo za šolstvo, znanost in šport.

© 2003 DMFA Slovenije – 1547

Poštšina plačana na pošti 1102 Ljubljana.

---

### NAVODILA SODELAVCEM OBZORNIKA ZA ODDAJO PRISPEVKOV

Obzornik za matematiko in fiziko objavlja znanstvene in strokovne članke iz matematike, fizike in astronomije, včasih tudi kak prevod. Poleg člankov objavlja prikaze novih knjig s teh področij, poročila o dejavnosti Društva matematikov, fizikov in astronomov Slovenije in vesti o drugih pomembnih dogodkih v okviru omenjenih znanstvenih ved. Prispevki naj bodo zanimivi in razumljivi širšemu krogu bralcev, diplomantov iz omenjenih strok.

Članek naj vsebuje naslov, ime avtorja (oz. avtorjev), sedež institucije, kjer avtor(ji) dela(jo), izvleček v slovenskem jeziku, naslov in izvleček v angleškem jeziku, klasifikacijo (MSC oziroma PACS) in citirano literaturo. Slike in tabele, ki naj bodo oštevilčene, morajo imeti dovolj izčrpen opis, da jih lahko večinoma razumemo ločeno od besedila. Avtorji člankov, ki želijo objaviti slike iz drugih virov, si morajo za to sami priskrbeti dovoljenje (copyright). Prispevki morajo biti poslani v dvojniku, natisnjeni enostransko na belem papirju formata A4. Zaželena velikost črk je vsaj 12 pt, razmik med vrsticami pa vsaj 18 pt.

Prispevke pošljite odgovornemu uredniku ali uredniku za matematiko oziroma fiziko na zgoraj napisani naslov uredništva. Vsak članek se praviloma pošlje vsaj enemu anonimnemu recenzentu, ki mora predvsem natančno oceniti, kako je obravnavana tema predstavljena, manj pomembna pa je originalnost (in pri matematičnih člankih splošnost) rezultatov. Če je prispevek sprejet v objavo in če je besedilo napisano z računalnikom, potem urednik prosi avtorja za izvirno datoteko. Le-te naj bodo praviloma napisane v eni od standardnih različic urejevalnikov  $\text{T}_{\text{E}}\text{X}$  oziroma  $\text{L}_{\text{A}}\text{T}_{\text{E}}\text{X}$ , kar bo olajšalo uredniški postopek.

# ODLOČITVENI PROBLEM PRAŠTEVILO

TADEJ NOVAK

Math. Subj. Class. (2000): 11-04, 11A41, 11A51

Odločitveni problem praštevilo je računski problem s področja teorije števil, pri katerem za dano naravno število sprašujemo, ali je praštevilo. Šele leta 2002 so Agrawal, Kayal in Saxena pokazali, da je ta problem deterministično rešljiv v polinomskem času. V članku opišemo njihov algoritem ter dokažemo njegovo pravilnost in polinomsko časovno zahtevnost. Podamo tudi pregled algoritmov, ki se uporabljajo v praksi.

## DECISION PROBLEM PRIMES

Prime is a decision problem from number theory where a given natural number is checked for primality. Only in 2002 Agrawal, Kayal and Saxena proved that this problem is solvable deterministically in polynomial time. We present their algorithm and prove its correctness, as well as polynomial time complexity. We also survey the algorithms which are used in practice.

### 1. Uvod

Kako za dano število ugotoviti, ali je praštevilo (t. i. odločitveni problem praštevilo), je problem, ki zaposluje matematike že od antičnih časov. Karl Friedrich Gauss (1777–1855) je v svoji knjigi *Disquisitiones Arithmeticae* (1801) zapisal tudi: „... *praetereaue scientiae dignitas requirere videtur, ut omnia subsidia ad solutionem problematis tam elegantis ac celebris sedulo excolantur.*”<sup>1</sup> Od leta 1960 dalje zaradi prihoda računalnikov poudarek ni več na iskanju matematične formule, ki bi dajala praštevila, ampak na iskanju učinkovitega algoritma za razpoznavanje praštevil.

Do leta 2002 sta bili za problem praštevilo znani dve vrsti algoritmov polinomske časovne zahtevnosti, to je deterministični, katerih pravilnosti nismo znali dokazati, ter verjetnostni algoritmi. Omenimo najpomembnejše prelomnice pri iskanju čimboljšega algoritma za problem praštevilo. Najstarejši znani algoritem je Eratostenovo rešeto iz leta 240 pr. n. š., toda njegova časovna zahtevnost je  $O(n)$ , torej eksponentna glede na dolžino zapisa obravnavanega števila  $n$ . Večji korak naprej je napravil Fermat v 17. stoletju, ko je dokazal, da za vsako naravno število  $a$  velja  $a^{p-1} \equiv 1 \pmod{p}$  za vsako praštevilo  $p$ , ki ne deli  $a$  (Fermatov mali izrek). Izrek so uporabili pri dokazovanju pravilnosti mnogih algoritmov za problem praštevilo. Leta 1976 je Miller predstavil determinističen algoritem polinomske časovne zahtevnosti, katerega pravilnost pa ni v celoti dokazana, saj temelji na predpostavki, da velja razširjena Riemannova hipoteza<sup>2</sup>. Nato sta Solovay in Strassen leta 1977 predstavila verjetnosten algoritem časovne zahtevnosti  $O(\log^3 n)$ . Rabin je leta 1980 modificiral Millerjev test in sestavil verjetnostni algoritem, katerega pravilnost delovanja je lahko dokazal, saj se mu ni

<sup>1</sup> „... razen tega se zdi, da ugled znanosti zahteva uporabo vseh možnih sredstev za rešitev tako lepega in znamenitega problema.”

<sup>2</sup> <http://www.claymath.org/prizeproblems/riemann.htm>

bilo treba sklicati na Riemannovo hipotezo. Ta algoritem je ſe danes med najuĹinkovitejſimi. NajveĹji preskok na poti do deterministiĹnega algoritma polinomske Ĺasovne zahtevnosti pa so napravili Adleman, Pomerance in Rummely leta 1983 z algoritmom Ĺasovne zahtevnosti  $O(\log n^{O(\log \log \log n)})$ . Goldwasser in Kilian sta leta 1986 sestavila verjetnostni algoritem z uporabo eliptiĹnih krivulj, katerega priĹakovana Ĺasovna zahtevnost je polinomska za skoraj vse moŹne vhodne podatke oz. za vse, Ĺe je izpolnjena doloĹena predpostavka. Leta 2002 pa so Agrawal, Kayal in Saxena sestavili deterministiĹni algoritem (algoritem AKS) Ĺasovne zahtevnosti najveĹ  $O(\log^{12} n)$  – v praksi  $O(\log^6 n)$ . Predstavili so tudi deterministiĹni algoritem Ĺasovne zahtevnosti  $O(\log^3 n)$ , vendar pa jim njegove pravilnosti ſe ni uspelo v celoti dokazati.

O odkritju algoritma AKS so poroĹali mnogi svetovni dnevni Ĺasopisi, tudi slovenski Ĺasnik Delo<sup>3</sup>. O avtorjih algoritma, Bernsteinovi [5] poenostavitvi<sup>4</sup>, dokaza ter izboljſavi ocene Ĺasovne zahtevnosti algoritma na  $O(\log^{7,5} n)$ , ki so jo avtorji dobili od H. Lenstre in so jo Źe objavili na spletu<sup>5</sup>, pa si lahko veĹ preberemo v prispevku revije *Notices of the AMS* [8].

Opise Eratostenovega reſeta, Solovay-Strassenovega testa ter Miller-Rabinovega algoritma najdemo v Stinsonovem uĹbeniku za kriptografijo [19] ali pa pri Bressoudu [9], idejo verjetnostnih algoritmov pa bomo spoznali v razdelku 4.

Oznaka  $P$  predstavlja mnoŹico problemov, za katere obstaja deterministiĹni algoritem  $\mathcal{A}$  polinomske Ĺasovne zahtevnosti glede na dolŹino zapisa vhodnih podatkov. Torej obstaja polinom  $p(x) \in \mathbb{Z}[x]$ , da je  $T_{\mathcal{A}}(x) \leq p(n)$  za vsak vhodni podatek  $x$  dolŹine  $n$ , kjer je  $T_{\mathcal{A}}(x)$  oznaka za ſtevilo korakov algoritma. DeterministiĹne algoritme lahko bolj natanĹno opredelimo kot Turingove stroje, o katerih je za *Obzornik* pisal Źe T. Pisanski [18], Ĺasovno zahtevnost pa kot ſtevilo izpolnjenih ukazov stroja. VeĹ o algoritmih in Ĺasovni zahtevnosti lahko preberemo v uĹbeniku J. Kozaka [15] ali pa v Horowitz in Sahni [13].

Vpeljimo ſe nekaj oznak, ki jih bomo pogosto uporabljali v nadaljevanju. S  $\mathbb{P}$  oznaĹimo mnoŹico praſtevil, s  $P(n)$  najveĹji praſtevilski delitelj ſtevila  $n$ ,  $\text{GF}(p^d)$  pa naj bo konĹni obseg moĹi  $p^d$ . Oznaka  $f(n) = \mathcal{O}(t(n))$  pomeni, da obstajajo polinom  $p(x)$  ter konstanti  $C$  in  $n_0$ , tako da za  $n \geq n_0$  velja  $|f(n)| \leq C t(n) p(\log t(n))$ . Oznako sreĹamo na primer, ko s pomoĹjo rekurzivnega izraĹuna izboljſamo Ĺasovno zahtevnost za en red velikosti, pri Ĺemer pridobimo logaritemski faktor  $\log n$ , ki je asimptotiĹno zanemarljiv v primerjavi z  $n$ . To pa je tudi razlog, zakaj namesto  $\mathcal{O}$  ponavadi piſemo kar  $O$ . Vseskozi bomo z  $\log$  oznaĹevali logaritem z osnovo 2, z  $o_r(n)$  pa red elementa  $n$  v grupi  $\mathbb{Z}_r^*$ , kjer je  $\mathbb{Z}_r$  kolobar ſtevil  $\{0, 1, 2, \dots, r-1\}$ , v katerem

<sup>3</sup> V prilogi Znanost 9. septembra 2002.

<sup>4</sup> Avtor v dokazu obstoja ‚primernega‘  $r$  pri izvajanju algoritma ne potrebuje veĹ sklicevanja na netrivialni lemi 2.2 in 2.3, paĹ pa le uporabo znanega Ĺebiſevega izreka, ki pravi, da je produkt praſtevil  $\leq 2k$  velik vsaj  $2^k$

<sup>5</sup> <http://www.cse.iitk.ac.in/news/primality.v3.pdf>

izvajamo običajni operaciji seštevanja in množenja po modulu  $r$ . Grupa  $\mathbb{Z}_r^*$  pa je grupa vseh obrnljivih elementov iz  $\mathbb{Z}_r$ .

V osrednjem delu članka bomo predstavili deterministični algoritem PrastQ polinomske časovne zahtevnosti, ki reši problem praštevilo. Na kratko rečemo, da je praštevilo v  $P$ . Na koncu bomo opisali še algoritme za reševanje problema praštevilo, ki se uporabljajo v praksi. Predstavljeni bodo tudi nekateri odprti problemi.

## 2. praštevilo je v $P$

Trditev iz naslova razdelka bomo dokazali v treh podrazdelkih. V 2.1 bomo predstavili deterministični algoritem za problem praštevilo, povzet po Agrawal in drugi [1], v 2.2 bomo dokazali, da je ta algoritem polinomske časovne zahtevnosti, v 2.3 pa še pravilnost njegovega delovanja.

### 2.1. Ključna ideja in algoritem

Poglejmo si karakterizacijo praštevil, ki je ključnega pomena pri konstrukciji algoritma.

**Trditev 2.1.** *Naj bosta  $a$  in  $n$  tuji si naravni števili. Potem je  $n$  praštevilo natanko tedaj, ko je*

$$(x - a)^n \equiv (x^n - a) \pmod{n} \quad (1)$$

(relacija v kolobarju polinomov  $\mathbb{Z}_n[x]$ .)

*Dokaz.* Definirajmo  $w(x) = (x - a)^n - (x^n - a)$ , kar je z upoštevanjem binomske formule enako  $w(x) = \sum_{0 < i < n} (-1)^{n-i} \binom{n}{i} a^{n-i} x^i + (-1)^n a^n + a$ . Trditev dokažemo v vsako smer posebej.

( $\Rightarrow$ ) Naj bo  $n \in \mathbb{P}$ . Potem je  $\binom{n}{i} \equiv 0 \pmod{n}$  za vsak  $i$ ,  $0 < i < n$ . Če upoštevamo še Fermatov izrek, dobimo  $w(x) \equiv 0 \pmod{n}$  za vsak  $n \in \mathbb{P}$ .

( $\Leftarrow$ ) Naj bo  $n$  sedaj sestavljeno število. Potem obstaja  $q \in \mathbb{P}$ ,  $1 < q < n$ , in obstaja  $k \in \mathbb{N}$ , tako da  $q^k | n$  in  $q^{k+1} \nmid n$ . Ker je  $\binom{n}{q} = \frac{n(n-1) \cdots (n-q+1)}{q(q-1) \cdots 1}$ , velja  $q^{k-1} | \binom{n}{q}$  ter  $q^k \nmid \binom{n}{q}$  in zato  $n$  ne deli  $\binom{n}{q}$ . Ker je  $n$  tuj  $a$ , je  $D(n, a^{n-q}) = 1$  in zato koeficient  $(-1)^{n-q} \binom{n}{q} a^{n-q}$  v polinomu  $w(x)$  pred  $x^q$  ni deljiv z  $n$ . ■

Če preverimo kongruenco ((1)) za neki  $a < n$ , pri katerem je  $D(a, n) = 1$ , npr.  $a = 1$ , potem se lahko na podlagi trditve 2.1 odločimo, ali je  $n$  praštevilo. Za izračun  $(x - a)^n$  uporabimo algoritem 'kvadriraj in množi', vendar pa je časovna zahtevnost takega izračuna eksponentna glede na dolžino zapisa števila  $n$ , saj je kvadriranje polinoma  $(x - a)^{\lfloor n/2 \rfloor}$ , ki je stopnje  $\lfloor n/2 \rfloor$ , časovne zahtevnosti vsaj  $O(n)$ . Algoritem izboljšamo tako, da izberemo „primeren“  $r \in \mathbb{N}$  in za  $a = 1$  do  $2\sqrt{r} \log n$  preverjamo

$$(x - a)^n \equiv (x^n - a) \pmod{x^r - 1, n}. \quad (2)$$

To so kongruence v faktorskem kolobarju  $\mathbb{Z}[x]/(n, x^r - 1)$ , to je faktorskem kolobarju kolobarja  $\mathbb{Z}[x]$  po idealu  $(n, x^r - 1)$ . Če je  $n$  praštevilo, je kongruenca ((2)) posledica trditve 2.1. Težava pa je v tem, da kongruenca ((2)) lahko velja tudi pri nekaterih sestavljenih številih.

Dejali bomo, da je eksponent  $r$  „primeren“, če je (i)  $r \in \mathbb{P}$ , (ii)  $r = O(\log^6 n)$  in (iii)  $r - 1$  vsebuje praštevilski delitelj  $q$  velikosti vsaj  $r^{\frac{1}{2} + \delta}$ ,  $\delta > 0$ , ter z lastnostjo  $q | o_r(n)$ . Tako dobljeni algoritem za testiranje praštevilskosti bomo poimenovali PrastQ<sup>6</sup>. Predstavljen je v okvirju na sliki 1. Pokazali bomo, da je  $n$  praštevilo, če pri takem  $r$  velja kongruenca ((2)) za vsak  $a$ ,  $1 \leq a \leq 2\sqrt{n} \log n$ . V algoritmu pogoj za velikost  $q$  preverimo s  $q \geq 4\sqrt{r} \log n$ , iz  $n^{\frac{r-1}{q}} \not\equiv 1 \pmod{r}$  pa sledi  $q \mid o_r(n)$ , saj je  $n^{r-1} \equiv 1 \pmod{r}$ .

**Algoritem:** PrastQ

**Podatek:** celo število  $n > 1$

**Rezultat:** SESTAVLJENO / PRAŠTEVILO

1. če je  $n$  oblike  $a^b$ ,  $b > 1$  vrni SESTAVLJENO;
2.  $r = 2$ ;
3. dokler je  $r < n$  {
4. če  $D(n, r) \neq 1$  vrni SESTAVLJENO;
5. če je  $r$  praštevilo
6. naj bo  $q$  največji praštevilski delitelj števila  $r - 1$ ;
7. če  $q \geq 4\sqrt{r} \log n$  in  $n^{\frac{r-1}{q}} \not\equiv 1 \pmod{r}$
8. zapusti zanko; (\* dokler je \*)
9.  $r \leftarrow r + 1$ ;
10. }
11. za  $a = 1$  do  $2\sqrt{r} \log n$
12. če  $(x - a)^n \not\equiv (x^n - a) \pmod{x^r - 1, n}$  vrni SESTAVLJENO;
13. vrni PRAŠTEVILO;

Slika 1. Algoritem za testiranje praštevilskosti

## 2.2. Časovna zahtevnost

Program PrastQ si lahko ogledamo tudi na internetu<sup>7</sup>. Napisan je v Mathematici in uporablja funkcije AnabQ, MaksPrast, PoliPotencMod in KongruencaQ.

<sup>6</sup> Nepisano pravilo pri programiranju v programskem paketu Mathematica je, da imenom funkcij, ki vračajo vrednosti True/False (pravilno/nepravilno), dodamo črko Q (question – angl. vprašanje)

<sup>7</sup> <http://www.fmf.uni-lj.si/~novakta/research/PrastQ.htm>

AnabQ[n] preveri, ali je število  $n$  oblike  $a^b$ . Naj bo  $m \in \mathbb{R}$  tak, da je  $n = m^m$ , torej je  $m = O(\log n)$ . Algoritem preizkusi vse celoštevilске  $a \in [2, m]$  in preveri, ali je  $b = \log_a n \in \mathbb{Z}$ , nato pa še vse celoštevilске  $b \in [2, m]$  in preveri, ali  $a = \sqrt[b]{n} \in \mathbb{Z}$ . Skupaj je to  $2m$  korakov in časovna zahtevnost algoritma je  $O(\log^3 n)$  bitnih operacij.

MaksPrast[n] s preizkusom deliteljev števila  $n$ , ki ne presegajo  $\sqrt{n}$ , poišče največji praštevski delitelj števila  $n$  in je časovne zahtevnosti  $O(\sqrt{n})$ .

PoliPotencMod[u,r,v,n] izračuna  $u(x)^r \pmod{v(x), n}$  s pomočjo algoritma „kvadriraj in množi“ (glej Stinson [19, str. 127]), kjer na vsakem koraku rezultat tudi reduciramo po modulu  $x^r - 1$  in po modulu  $n$ . To storimo tudi na začetku izvajanja. Potrebni so torej  $O(\log r)$  korakov. Če uporabimo Fourierovo transformacijo za množenje polinomov (glej Bini in Pan [7, str. 8–13]) in še hitro metodo za deljenje polinomov (glej Bini in Pan [7, str. 18–23]), je časovna zahtevnost algoritma  $O((\log n)(\deg u + \log r \deg v))$ .

KongruencaQ[a,n,r] nam s pomočjo PoliPotencMod preveri, ali je  $(x-a)^n \equiv (x^n - a) \pmod{x^r - 1, n}$ . S tem porabi  $O(r \log^2 n)$  bitnih operacij.

Za algoritem PrastQ[n] bomo s trditvijo 2.4 pokazali, da najde primeren  $r$  v največ  $O(\log^6 n)$  korakih (algoritem se lahko ustavi, še preden najde primeren  $r$ ). Časovna zahtevnost enega koraka v zanki „dokler je  $r < n$ “ je  $O(\log^3 n)$ , v zanki „za  $a = 1$  do  $2\sqrt{r} \log n$ “ pa  $O(\log^8 n)$ . Skupaj algoritem PrastQ[n] porabi največ  $O(\log^{12} n)$  bitnih operacij, kar pomeni, da je praštevilo v  $P$ .

**Lema 2.2.** (Fouvry [10], Baker in Harman [4]) *Obstajata konstanti  $c > 0$  in  $n_0$ , tako da za vsak  $n \geq n_0$  velja*

$$|\{p|p \text{ je praštevilo, } p \leq n \text{ in } P(p-1) > n^{2/3}\}| \geq c \frac{n}{\log n}.$$

**Lema 2.3** (Apostol [2]). *Naj bo  $\pi(n)$  število praštevil  $\leq n$ . Potem za vsak  $n \geq 1$  velja*

$$\frac{n}{6 \log n} \leq \pi(n) \leq \frac{8n}{\log n}.$$

**Trditev 2.4.** *Obstajajo konstante  $c_1, c_2$  in  $n_1$ , pri katerih za vsak  $n \geq n_1$  obstaja praštevilo  $r$  na intervalu  $[c_1 \log^6 n, c_2 \log^6 n]$ , za katero velja, da ima  $r-1$  praštevski delitelj  $q$ , ki zadošča pogoju  $q \geq 4\sqrt{r} \log n$  in  $n^{\frac{r-1}{q}} \not\equiv 1 \pmod{r}$ .*

*Dokaz.* Vzemimo konstanti  $c$  in  $n_0$  iz leme 2.2. Definirajmo  $c_1$  in  $c_2$  tako, da velja (i)  $c_2 > c_1 > 0$ , (ii)  $\frac{c c_2}{7} - \frac{8 c_1}{6} > 0$  ter (iii)  $c_1^4 > 4^6 c_2^3$ . Bralec si lahko nariše ustrezne pare  $(c_1, c_2)$  kot neprazno območje v  $\mathbb{R}^2$ . Praštevila  $p$ , za katera velja  $P(p-1) > p^{2/3}$ , poimenujmo „posebna praštevila“.

S pomočjo leme 2.2 in leme 2.3 ocenimo, koliko je posebnih praštevil na intervalu  $[c_1 \log^6 n, c_2 \log^6 n]$ , kjer je  $n \geq n_0$  in  $\log n \geq c_2$ :

$$\begin{aligned} & |\{p \in \mathbb{P} \mid p \in [c_1 \log^6 n, c_2 \log^6 n], P(p-1) > p^{2/3}\}| \geq \\ & \geq |\{p \in \mathbb{P} \mid p \leq c_2 \log^6 n, P(p-1) > p^{2/3}\}| - \\ & \quad - |\{p \in \mathbb{P} \mid p < c_1 \log^6 n\}| \geq \\ & \geq c \frac{c_2 \log^6 n}{\log(c_2 \log^6 n)} - \frac{8(c_1 \log^6 n)}{\log(c_1 \log^6 n)} \\ & \geq \frac{\log^6 n}{\log \log n} \left( \frac{c c_2}{7} - \frac{8 c_1}{6} \right) \\ & = c_3 \frac{\log^6 n}{\log \log n}, \end{aligned}$$

kjer smo definirali  $c_3 = \frac{c c_2}{7} - \frac{8 c_1}{6}$ . Po predpostavki je  $c_3 > 0$ .

Naj bo  $x = c_2 \log^6 n$  in

$$N = (n-1)(n^2-1)(n^3-1) \cdots (n^{\lfloor x^{1/3} \rfloor} - 1).$$

Pokažimo, da obstaja posebno praštevilo na intervalu  $[c_1 \log^6 n, c_2 \log^6 n]$ , ki ne deli  $N$ . Najprej ocenimo število praštevilskih deliteljev števila  $N$ :

$$\begin{aligned} & |\{p \in \mathbb{P} \mid p \text{ deli } N\}| \leq \\ & \leq \log N = \log(n-1) + \log(n^2-1) + \cdots + \log(n^{x^{1/3}}-1) \leq \\ & \leq \log(n) + 2 \log n + \cdots + x^{1/3} \log n = \frac{x^{1/3}(x^{1/3}+1)}{2} \log n. \end{aligned}$$

Za dovolj velik  $n$  je  $x > 1$ , tedaj pa je vrednost zgornjega izraza manjša od  $x^{2/3} \log n$  oziroma  $c_2^{2/3} \log^5 n$ , kar je za dovolj velik  $n$  manj kot  $c_3 \frac{\log^6 n}{\log \log n}$ .

Torej obstaja posebno praštevilo na intervalu  $[c_1 \log^6 n, c_2 \log^6 n]$ , ki ne deli  $N$ . Izberimo enega in ga označimo z  $r$ . Pokažimo, da  $r$  ustreza pogojem iz trditve. Ocenimo velikost  $q = P(r-1)$ :

$$q \geq r^{2/3} \geq c_1^{2/3} \log^4 n = \frac{c_1^{2/3}}{c_2^{1/2}} (c_2 \log^6 n)^{1/2} \log n \geq 4\sqrt{r} \log n.$$

Če hočemo pokazati  $n^{\frac{r-1}{q}} \not\equiv 1 \pmod{r}$ , je dovolj, da pokažemo  $\frac{r-1}{q} < o_r(n)$ . Ker  $r$  ne deli  $N$ , potem  $r$  ne deli  $(n^i - 1)$  za noben  $i$ ,  $1 \leq i \leq \lfloor x^{1/3} \rfloor$ , kar pomeni, da  $n^i \not\equiv 1 \pmod{r}$  za noben  $i$ ,  $1 \leq i \leq \lfloor x^{1/3} \rfloor$ , torej je  $o_r(n) > x^{1/3}$ .

Ker je  $\frac{r-1}{q} \leq \frac{r}{r^{2/3}} = r^{1/3} \leq (c_2 \log^6 n)^{1/3} = x^{1/3} < o_r(n)$ , sledi  $n^{\frac{r-1}{q}} \not\equiv 1 \pmod{r}$ . ■

## 2.3. Dokaz pravilnosti algoritma

Če je  $n$  praštevilo, se algoritem ne more ustaviti v vrsticah 1, 4 ali 12, torej nam vrne odgovor praštevilo. Za dokaz pravilnosti v drugo smer pa bomo potrebovali nekaj splošnih dejstev iz algebre – o grupah in končnih obsegih. Nato bomo v lemi 2.7 definirali grupo  $G$  in ocenili njeno velikost. Definirali bomo tudi množico  $I_{g(x)}$  in v lemah 2.8 in 2.9 pokazali njene lastnosti, nato pa bomo v trditvi 2.10 s protislovjem pokazali, da ko je  $n$  sestavljeno število, algoritem vrne odgovor sestavljeno.

**Lema 2.5.** *Naj bosta  $p$  in  $r$  praštevili in  $p \neq r$ . Potem velja:*

1. *Multiplikativna grupa obsega  $F = \text{GF}(p^d)$ ,  $d > 0$ , označena z  $F^*$ , je ciklična.*
2. *Če je  $f(x)$  polinom s celoštevilskimi koeficienti, velja*

$$f(x)^p \equiv f(x^p) \pmod{p}.$$

3. *Če je  $h(x)$  katerikoli faktor polinoma  $x^r - 1$  in  $m \equiv m_r \pmod{r}$ , potem velja*

$$x^m \equiv x^{m_r} \pmod{h(x)}.$$

4. *Polinom  $\frac{x^r-1}{x-1}$  se nad  $\mathbb{Z}_p$  faktorizira v nerazcepne polinome stopnje  $o_r(p)$ .*

*Dokaz.* (1) Poglavje o končnih obsegih v kateremkoli učbeniku algebre, npr. Vidav [20].

(2) Naj bo  $f(x) = a_0 + a_1x + \dots + a_dx^d$ . Koeficient pred  $x^i$  v  $f(x)^p$  je enak

$$\sum_{\substack{i_0+i_1+\dots+i_d=p \\ i_1+2i_2+\dots+di_d=i}} \frac{p!}{i_0!i_1!\dots i_d!} a_0^{i_0} a_1^{i_1} \dots a_d^{i_d}.$$

Ta koeficient je deljiv s  $p$  natanko tedaj, ko so vsi  $i_k < p$  v vsoti. Upoštevamo še Fermatov izrek in dobimo  $f(x)^p \equiv \sum_{k=0}^d a_k x^{kp} \pmod{p}$ . Dokaz je končan, saj je tudi  $f(x^p) = \sum_{k=0}^d a_k x^{kp}$ .

(3) Naj bo  $m = kr + m_r$ . Če kongruenco  $x^r \equiv 1 \pmod{x^r - 1}$  na obeh straneh potenciramo s  $k$  in nato še obe strani pomnožimo z  $x^{m_r}$ , dobimo  $x^m \equiv x^{m_r} \pmod{x^r - 1}$ . Ker  $h(x)$  deli  $x^r - 1$ , je  $x^m \equiv x^{m_r} \pmod{h(x)}$ .

(4) Naj bodo  $d = o_r(p)$ ,  $Q(x) = \frac{x^r-1}{x-1}$ ,  $h(x)$  neki nerazcepen faktor polinoma  $Q(x)$  in  $k = \deg h(x)$ . Pokažimo, da je  $k \leq d$  in še  $d \leq k$ , torej da velja  $k = d$ . Naj bo  $F = \text{GF}(p^k)$  definiran s polinomom  $h(x)$  in naj bo  $g(x)$  generator  $F^*$ . Po 2. točki leme je

$$g(x)^p \equiv g(x^p) \pmod{p},$$

oziroma če to točko uporabimo  $d$ -krat, dobimo

$$g(x)^{p^d} \equiv g(x^{p^d}) \pmod{p}.$$

Ker je  $p^d \equiv 1 \pmod{r}$ , je po 3. točki leme

$$g(x^{p^d}) \equiv g(x) \pmod{h(x)}.$$

Predzadnja kongruenca velja tudi po modulu  $h(x)$ , saj če sta dva elementa enaka v kolobarju  $\mathbb{Z}_p[x]$ , potem predstavljata isti element v faktorskem kolobarju  $\mathbb{Z}_p[x]/h(x)$ , ki pa je izomorfen  $\mathbb{Z}[x]/(h(x), p)$ . Podobno velja za zadnjo kongruenco in zato je

$$g(x)^{p^d} \equiv g(x) \pmod{h(x), p}.$$

Torej  $h(x)$  deli  $g(x)(g(x)^{p^d-1} - 1)$  v obsegu  $F$ . Ker je  $h(x)$  nerazcepen v  $F$ , deli vsaj enega od faktorjev. Če bi  $h(x)$  delil  $g(x)$ , bi bil  $g(x)$  ničelni element v  $F$ , torej je

$$g(x)^{p^d-1} \equiv 1 \pmod{h(x)}.$$

To pomeni, da red polinoma  $g(x)$  ne presega  $p^d - 1$ . Ker je  $g(x)$  generator grupe  $F^*$ , je njegov red enak moči te grupe,  $\text{red}(g(x)) = p^k - 1$ . Od tod sledi, da je  $p^k - 1 \leq p^d - 1$  in zato tudi  $k \leq d$ . Pokažimo še, da velja  $d \leq k$ . Ker  $h(x)$  deli  $x^r - 1$  v  $\mathbb{Z}_p[x]$ , je

$$x^r \equiv 1 \pmod{h(x), p}.$$

To pomeni, da  $\text{red}(x)$  deli  $r$ , in ker je  $r \in \mathbb{P}$  in ker  $x$  ni enica v  $F$ , je  $\text{red}(x) = r$ . Ker  $\text{red}$  vedno deli moč grupe, velja  $r | p^k - 1$ , torej  $p^k \equiv 1 \pmod{r}$ . Ker je  $d = o_r(p)$ , sledi  $d \leq k$ . ■

Naj bo  $n$  sedaj sestavljeno število in predpostavimo, da se algoritem ne ustavi v vrsticah 1 ali 4. Naj bo  $r$  praštevilo, pri katerem se ustavi zanka dokler je, in  $q = P(r - 1)$ .

**Lema 2.6.** *Obstaja prafaktor  $p$  števila  $n$ , tako da  $q$  deli  $o_r(p)$ .*

*Dokaz.* Naj bo  $n = \prod_{i=1}^s p_i^{k_i}$ . Potem  $o_r(n)$  deli  $v(o_r(p_1), \dots, o_r(p_s))$ , kjer je  $v$  oznaka za najmanjši skupni večkratnik (če bi bil  $n = \prod_{i=1}^s p_i$ , potem bi bil  $o_r(n) = v(o_r(p_1), \dots, o_r(p_s))$ ). Ker  $q$  deli  $o_r(n)$  (eden od pogojev za primernost  $r$ ),  $q$  deli tudi  $v(o_r(p_1), \dots, o_r(p_s))$ , in ker je  $q$  praštevilo, obstaja  $i$ , tako da  $q | o_r(p_i)$ . ■

Naj bo  $p$  praštevilo iz zadnje leme ter  $h(x)$  nerazcepen faktor polinoma  $x^r - 1$  stopnje  $d = o_r(p)$ , glej lemo 2.5.4. Ker iz  $(x - a)^n \equiv (x^n - a) \pmod{x^r - 1, n}$  sledi

$$(x - a)^n \equiv (x^n - a) \pmod{h(x), p},$$

lahko na kongruence iz algoritma gledamo kot na kongruence v obsegu  $F = \mathbb{Z}_p[x]/h(x)$ .

**Lema 2.7.** *Naj bo  $l = 2\sqrt{r} \log n$ . V obsegu  $F = \mathbb{Z}_p[x]/h(x)$  je multiplikativna podgrupa*

$$G = \left\{ \prod_{1 \leq a \leq l} (x - a)^{\alpha_a} \mid \alpha_a \geq 0 \right\}$$

*ciklična in moči  $> \left(\frac{d}{l}\right)^l \geq n^{2\sqrt{r}}$ .*

*Dokaz.* Ker je  $F^*$  ciklična, je tudi  $G \leq F^*$  ciklična. Ocenimo še velikost grupe  $G$  s pomočjo množice

$$S = \left\{ \prod_{1 \leq a \leq l} (x - a)^{\alpha_a} \mid \alpha_a \geq 0, \sum_{1 \leq a \leq l} \alpha_a \leq d - 1 \right\}.$$

Ker se algoritem ne ustavi v vrsticah 1 ali 4, nam najde  $r$ , za katerega velja  $r > q \geq 4\sqrt{r} \log n > l$  in  $D(n, b) = 1$  za vsak  $b \leq r$ . Če bi bila katera  $a_1, a_2 \in \mathbb{N}$ ,  $1 \leq a_1 < a_2 \leq l$ , kongruentna po modulu  $p$ , potem bi  $p$  delil  $a_2 - a_1$ , kar pa je v protislovju z  $D(n, a_2 - a_1) = 1$ , saj je  $0 < a_2 - a_1 < a_2 \leq l < r$ .

Ker so vsi polinomi v  $S$  stopnje  $\leq d - 1 < \deg h(x)$  in ker so vsi  $a$ -ji različni po modulu  $p$ , nam elementi v  $S$  predstavljajo paroma različne elemente iz  $F$ . Vsak polinom v  $S$  je produkt  $d - 1$  faktorjev, pri čemer imamo na izbiro  $l + 1$  možnih faktorjev, to so  $1, x - 1, \dots, x - l$ . Iz formule za kombinacije s ponavljanjem dobimo

$$\begin{aligned} |G| &\geq |S| = \binom{(d-1) + (l+1) - 1}{d-1} = \binom{d+l-1}{l} = \\ &= \frac{(d+l-1)(d+l-2) \cdots d}{l!} > \frac{d^l}{l!} = \left(\frac{d}{l}\right)^l. \end{aligned}$$

Ker  $q$  deli  $o_r(p)$ , je  $d = o_r(p) \geq q \geq 4\sqrt{r} \log n = 2l$  in zato

$$|G| > \left(\frac{2l}{l}\right)^l = 2^l = 2^{2\sqrt{r} \log n} = n^{2\sqrt{r}}. \quad \blacksquare$$

Naj bo  $g(x)$  generator grupe  $G$ . Označimo z  $o_g$  red elementa  $g(x)$  v  $\mathbb{Z}_p[x]/h(x)$ . Enak je moči grupe  $G$  in zato velik vsaj  $n^{2\sqrt{r}}$ . Definirajmo

$$I_{g(x)} = \{m \in \mathbb{N} \mid g(x)^m \equiv g(x^m) \pmod{x^r - 1, p}\}$$

in pokažimo nekaj njenih osnovnih lastnosti.

**Lema 2.8.** *Množica  $I_{g(x)}$  je zaprta za množenje.*

*Dokaz.* Naj bosta  $m_1, m_2 \in I_{g(x)}$ . To pomeni, da je

$$g(x)^{m_1} \equiv g(x^{m_1}) \pmod{x^r - 1, p} \quad \text{in} \quad (3)$$

$$g(x)^{m_2} \equiv g(x^{m_2}) \pmod{x^r - 1, p}. \quad (4)$$

Če v kongruenci ((4)) pišemo  $x^{m_1}$  namesto  $x$  in upoštevamo, da  $x^r - 1$  deli  $x^{m_1 r} - 1$ , dobimo  $g(x^{m_1})^{m_2} \equiv g(x^{m_1 m_2}) \pmod{x^r - 1, p}$ , kar nam da skupaj s kongruenco ((3))

$$g(x)^{m_1 m_2} \equiv g(x^{m_1 m_2}) \pmod{x^r - 1, p},$$

to pa pomeni, da  $m_1 m_2 \in I_{g(x)}$ . ■

**Lema 2.9.** *Če sta  $m_1, m_2 \in I_{g(x)}$ , potem iz  $m_1 \equiv m_2 \pmod{r}$  sledi  $m_1 \equiv m_2 \pmod{o_g}$ .*

*Dokaz.* Ker je  $m_2 \in I_{g(x)}$ , je  $g(x)^{m_2} \equiv g(x^{m_2}) \pmod{h(x), p}$ , saj  $h(x)$  deli  $x^r - 1$ . Ker je  $m_1 \equiv m_2 \pmod{r}$ , je  $m_2 = m_1 + kr$  in po lemi 2.5.3 je  $x^{m_2} \equiv x^{m_1} \pmod{h(x)}$ , torej velja tudi  $x^{m_2} \equiv x^{m_1} \pmod{h(x), p}$ . Dobimo  $g(x)^{m_1} g(x)^{kr} \equiv g(x^{m_1}) \pmod{h(x), p}$  in ker  $m_1 \in I_{g(x)}$ , dobimo, da  $h(x)$  deli  $g(x)^{m_1} (g(x)^{kr} - 1)$  v  $\mathbb{Z}_p[x]$ . Ker je  $h(x)$  nerazcepen nad  $\mathbb{Z}_p$ , velja, da  $h(x)$  deli  $g(x)$  ali  $h(x)$  deli  $g(x)^{kr} - 1$ . Če bi bil  $g(x)$  deljiv s  $h(x)$ , bi bil ničelni element v  $F$ . Torej je  $g(x)^{kr} \equiv 1 \pmod{h(x), p}$ , kar pomeni, da red polinoma  $g(x)$ , to je  $o_g$ , deli  $kr$  in s tem  $m_2 - m_1$ . ■

**Trditev 2.10.** *Če je  $n$  sestavljeno število, algoritem vrne odgovor sestavljeno.*

*Dokaz.* Recimo, da je  $n$  sestavljeno število in da algoritem vrne odgovor praštevilo. Pokažimo najprej, da je  $\{1, p, n\} \subset I_{g(x)}$ . Po definiciji  $I_{g(x)}$  je očitno, da  $1 \in I_{g(x)}$ , iz druge točke leme 2.5 pa sledi  $p \in I_{g(x)}$ . Če upoštevamo, da je  $g(x) \in G$ , torej da je oblike

$$g(x) = \prod_{1 \leq a \leq l} (x - a)^{\gamma_a},$$

in še, da so pravilne vse kongruence v zanki za, saj algoritem vrne odgovor praštevilo, dobimo

$$g(x)^n \equiv g(x^n) \pmod{x^r - 1, p}.$$

Sedaj definirajmo

$$E = \{n^i p^j \mid 0 \leq (i, j) \leq \lfloor \sqrt{r} \rfloor\}.$$

Ker je  $\{1, p, n\} \subset I_{g(x)}$  in ker je  $I_{g(x)}$  zaprta za množenje, je  $E \subset I_{g(x)}$ . Ker je  $|E| = (1 + \sqrt{r})^2 > r$ , obstajata po Dirichletovem principu  $n^{i_1} p^{j_1}$  in  $n^{i_2} p^{j_2}$  iz  $E$ ,  $(i_1, j_1) \neq (i_2, j_2)$  taka, da velja  $n^{i_1} p^{j_1} \equiv n^{i_2} p^{j_2} \pmod{r}$ . Po lemi 2.9 je  $n^{i_1} p^{j_1} \equiv n^{i_2} p^{j_2} \pmod{o_g}$ . Ker je  $o_g > n^{2\sqrt{r}}$  in ker sta  $n^{i_1} p^{j_1}, n^{i_2} p^{j_2} \leq n^{2\sqrt{r}}$ , je  $n^{i_1} p^{j_1} = n^{i_2} p^{j_2}$ . Torej je  $n^{i_1 - i_2} = p^{j_2 - j_1}$  in algoritem bi se moral ustaviti v vrstici 1. To pa je v protislovju s predpostavko, da algoritem vrne odgovor praštevilo. ■

### 3. Pospesitve in odprti problemi

Predstavili bomo dve hipotezi s področja, ki obravnava praštevila. Če velja hipoteza 3.11, potem je časovna zahtevnost algoritma PrastQ največ  $\mathcal{O}(\log^6 n)$ , s pomočjo hipoteze 3.13 pa dobimo determinističen algoritem časovne zahtevnosti  $\mathcal{O}(\log^3 n)$ .

Če sta  $r$  in  $\frac{r-1}{2}$  praštevili, imenujemo  $\frac{r-1}{2}$  praštevilo *Sophie Germain* in  $r$  *sopraštevilo Sophie Germain*.

**Hipoteza 3.11** (Hardy in Littlewood [12] preverjena za  $r \leq 10^{10}$ ). Število *sopraštev* *Sophie Germain*, manjših od  $n$ , je asimptotično enako  $D \frac{n}{\log^2 n}$ , kjer je  $D \in \mathbb{R}$ .

Konstanti  $D$  pravimo *konstanta praštevilskih dvojčkov*. Če hipoteza velja, potem nam naslednja lema zagotavlja, da je časovna zahtevnost algoritma PrastQ največ  $\mathcal{O}(\log^6 n)$ .

**Lema 3.12.** Če velja hipoteza 3.11, potem obstajajo take pozitivne konstante  $n_0$  in  $c_1$  in  $c_2$ , da obstaja primeren'  $r$  na intervalu  $[c_1 \log^2 n, c_2 \log^2 n]$  za vsak  $n \geq n_0$ .

*Dokaz.* Zaradi preprostejšega izračuna v dokazu vzemimo  $c_1 = 100$  in  $c_2 = 101$ , čeprav bi bila ustrezna že  $c_1 \approx c_2 \approx 64$ . Definirajmo množico  $T = [c_1 \log^2 n, c_2 \log^2 n] \cap \mathbb{P}_{\text{co-Sop-Ger}}$ , kjer je  $\mathbb{P}_{\text{co-Sop-Ger}}$  množica *sopraštev* *Sophie Germain*, in s pomočjo hipoteze 3.11 asimptotično ocenimo njeno moč:

$$|T| \approx \frac{D(c_2 \log^2 n)}{(\log(c_2 \log^2 n))^2} - \frac{D(c_1 \log^2 n)}{(\log(c_1 \log^2 n))^2} \approx \frac{D(c_2 - c_1) \log^2 n}{4(\log \log n)^2}.$$

Pokažimo, da za praštevila  $r \in T$  velja  $P(r-1) \geq 4\sqrt{r} \log n$ :

$$\begin{aligned} P(r-1) &= \frac{r-1}{2} \geq \frac{c_1 \log^2 n - 1}{2} \geq \frac{c_1 - 1}{2} (\log n)(\log n) \geq \\ &\geq \frac{c_1 - 1}{2} \sqrt{\frac{r}{c_2}} \log n \geq \frac{c_1 - 1}{2\sqrt{c_2}} \sqrt{r} \log n \geq 4\sqrt{r} \log n. \end{aligned}$$

Na intervalu  $[c_1 \log^2 n, c_2 \log^2 n]$  je asimptotično  $O\left(\frac{\log^2 n}{(\log \log n)^2}\right)$  spraševal Sophie Germain. Neprimerna so tista, pri katerih je  $n^{\frac{r-1}{r}} \equiv 1 \pmod{r}$ , torej  $n^2 \equiv 1 \pmod{r}$ , kar pomeni  $n^2 - 1 = kr$ . Neprimernih je torej največ  $\log(n^2 - 1) \approx 2 \log n$ , saj ima  $n^2 - 1$  največ  $\log(n^2 - 1)$  prašteviskih deliteljev (možnosti za  $r$ ). Seveda pa je  $O(\log n)$  asimptotično manj kot  $O\left(\frac{\log^2 n}{(\log \log n)^2}\right)$ , torej za dovolj velik  $n$  obstaja „primeren“  $r \in T$ . ■

Sedaj bomo predstavili še hitrejši algoritem, katerega pravilnost še ni dokazana. Da smo za PrastQ dobili grupo  $G$  moči vsaj  $n^{2\sqrt{r}}$ , smo morali vzeti  $l = 2\sqrt{r} \log n$ . Konstanto  $l$  lahko ustrezno zmanjšamo in še vedno dobimo grupo zahtevane moči.

**Hipoteza 3.13** (Bhattacharjee in Pandey [6]<sup>8</sup>, preverjena v Kayal in Saxena [14]<sup>9</sup> za  $r \leq 100$  in  $n \leq 10^{10}$ ). Če  $r$  ne deli  $n$  in če velja

$$(x - 1)^n \equiv (x^n - 1) \pmod{x^r - 1, n},$$

potem je  $n$  praštevilo ali pa  $n^2 \equiv 1 \pmod{r}$ .

Če hipoteza 3.13 drži, lahko sestavimo hiter algoritem za testiranje prašteviskosti, glej okvir na sliki 2. Poiščemo  $r$ , ki ne deli niti  $n$  niti  $n^2 - 1$ . Po lemi 3.14 obstaja na intervalu  $[2, 6 \ln n]$ . Nato za ta  $r$  preverimo kongruenco iz hipoteze 3.13 in časovna zahtevnost algoritma je tako omejena z  $O(\log^3 n)$ .

**Lema 3.14.** Na intervalu  $[2, 6 \ln n]$  obstaja  $r$ , ki ne deli niti  $n$  niti  $n^2 - 1$ .

*Dokaz.* Po učbeniku za analitično teorijo števil (Apostol [2]) povzamemo  $\prod_{\substack{p \in \mathbb{P} \\ p \leq x}} p \geq e^{\frac{x}{2}}$  za vsak  $x \geq 5$ . Če bi vsa praštevila  $p \leq 6 \ln n$  delila  $n^2 - 1$  ali  $n$ , torej njun produkt  $n^3 - n$ , potem bi bil  $\prod_{\substack{p \in \mathbb{P} \\ p \leq 6 \ln n}} p \leq n^3 - n$ .

Iz gornje ocene pa vemo, da je  $\prod_{\substack{p \in \mathbb{P} \\ p \leq 6 \ln n}} p \geq e^{\frac{6 \ln n}{2}} = n^3$ . ■

#### 4. Iskanje praštevil v praksi

V praksi mnogokrat potrebujemo naključno izbrano veliko praštevilo. Pri implementaciji kriptosistema RSA, glej Stinson [19, str. 124], potrebujemo za 1024-bitni modul naključno izbrano 512-bitno praštevilo. Dobimo ga tako, da izberemo naključno 512-bitno liho število in preverimo, ali je praštevilo. Glede na lemo 2.3 najdemo praštevilo v  $O(\log(n))$  korakih. Če

<sup>8</sup> <http://www.cse.iitk.ac.in/research/btp2001/primality.htm>

<sup>9</sup> <http://www.cse.iitk.ac.in/research/btp2002/primality.htm>

**Algoritem :** PrastHipoQ

**Podatek:** celo število  $n > 1$

**Rezultat:** SESTAVLJENO / PRAŠTEVÍLO

1.  $r = 2$ ;
2. **dokler je**  $r < n$  {
3.   **če**  $n \equiv 0 \pmod{r}$  **vrni** SESTAVLJENO;
4.   **če**  $n^2 \not\equiv 1 \pmod{r}$  **zapusti zanko**; (\* dokler je \*)
5.    $r \leftarrow r + 1$ ;
6. }
7.   **če**  $(x - 1)^n \equiv (x^n - 1) \pmod{x^r - 1, n}$
8.   **vrni** PRAŠTEVÍLO;
9.   **sicer**
10.   **vrni** SESTAVLJENO;

**Slika 2.** Algoritem za testiranje praštevílskosti, pravílnost temelji na hipotezi 3.13

bi v tem programu uporabljali algoritem PrastQ, bi ob predpostavki, da velja hipoteza 3.11, porabil največ  $512^6$  bitnih operacij (od vseh korakov pri iskanju praštevíla je najdaljši tisti, ko najdemo praštevílo). Ker je  $512^6 = 1.8 \cdot 10^{16}$ , bi računalnik z  $1 \text{ GHz} = 10^9 \text{ Hz}$  procesorjem za iskanje enega 512-bitnega praštevíla potreboval približno  $10^7$  sekund, oziroma 4 mesece, kar pa je nesprejemljivo.

Zato se v praksi za problem praštevílo še vedno uporabljajo verjetnostni algoritmi, ki za svoje delo potrebujejo funkcijo za generiranje naključnih števíl. Posebna zvrst teh algoritmov so algoritmi tipa Monte-Carlo, pri katerih je posebnost to, da vrnejo enega od dveh odgovorov, npr. TRUE ali FALSE, in eden od odgovorov je vedno pravílen, drugi pa je lahko tudi napačen. O verjetnostnih algoritmih je za *Obzornik* pisal že J. Žerovnik [21].

Najbolj znana za testiranje praštevílskosti sta Solovay-Strassenov test ter Miller-Rabinov test, glej Stinson [19, str. 129–138]. Čeprav je Miller-Rabinov test hitrejši, si bomo raje ogledali Solovay-Strassenovega, glej okvir na sliki 3, saj je na videz bolj preprost in bomo z njim lažje prikazali, kako delujejo algoritmi tipa Monte-Carlo.

Za nenegativno celo število  $a$  in liho naravno število  $n = p_1^{e_1} \cdots p_k^{e_k}$  je Jacobijev simbol  $\left(\frac{a}{n}\right)$  definiran kot

$$\left(\frac{a}{n}\right) = \prod_{i=1}^k \left(\frac{a}{p_i}\right)^{e_i},$$

in je posplošitev definícije Legendrovega simbola

$$\left(\frac{a}{p}\right) = \begin{cases} 0; & a \equiv 0 \pmod{p} \\ 1; & \exists b \in \mathbb{Z}_p : b^2 \equiv a \pmod{p}, \\ -1; & \text{sicer} \end{cases}$$

**Algoritem:** PrastVerjTestQ

**Podatek:** celo število  $n > 1$

**Rezultat:** SESTAVLJENO / PRAŠTEVILO

1. naključno izberi celo število  $a$ ,  $1 \leq a \leq n - 1$ ;
2. če  $\left(\frac{a}{n}\right) \equiv a^{(n-1)/2} \pmod{n}$
3. vrni PRAŠTEVILO;
4. sicer
5. vrni SESTAVLJENO;

**Slika 3.** Solovay-Strassenov verjetnostni test za testiranje praštevilskosti

kjer je spodnji argument liho praštevilo, zgornji pa nenegativno celo število. Postopka za izračun vrednosti Jacobijevega simbola ne bomo opisali, saj presega okvir članka. Časovna zahtevnost testa je  $O(\log^2 n)$ , pri njegovem delovanju pa je pomembno naslednje: če vrne odgovor sestavljeno, potem je  $n$  res sestavljeno število, če pa vrne odgovor praštevilo, ta odgovor ni nujno pravilen. Verjetnost napake je v našem primeru manjša od  $1/2$ :

$$P(\text{algoritem vrne odgovor praštevilo} \mid n \text{ ni praštevilo}) < 1/2.$$

Če test ponovimo  $m$ -krat, potem z nekaj truda (glej Stinson [19, str. 135]) za velike  $n$  izpeljemo

$$P(n \text{ ni praštevilo} \mid \text{algoritem } m\text{-krat vrne odgovor praštevilo}) \leq \frac{\ln n - 2}{\ln n - 2 + 2^{m+1}}$$

in ne  $1 - (1/2)^m$ , kakor bi intuitivno pričakovali. Če test ponovimo  $\log n$ -krat in vedno dobimo odgovor praštevilo, je torej verjetnost, da  $n$  ni praštevilo, velikostnega reda  $\frac{\ln n}{2n}$ , kar je dovolj zanesljivo za uporabo v praksi. Časovna zahtevnost Solovay-Strassenovega algoritma za preverjanje, ali je  $n$  praštevilo, je torej  $O(\log^3 n)$ . Prav tolikšna je tudi za Miller-Rabinov algoritem. Podobno kot prej lahko dobimo, da na 1 GHz računalniku stestiramo 512-bitno praštevilo v približno 0,13 sekunde.

V programskem paketu Mathematica 4 sta za testiranje praštevilskosti vgrajeni funkciji PrimeQ in ProvablePrimeQ, pri slednji je treba poprej naložiti paket NumberTheoryPrimeQ'.

Za testiranje praštevilskosti funkcija PrimeQ najprej preveri, ali ima število  $n$  kak majhen praštevilski delitelj, nato uporabi Miller-Rabinov test (kreпки psevdopraštevilski test) pri bazi 2 in bazi 3, na koncu pa še Lucasov test<sup>10</sup>.

Funkcija ProvablePrimeQ uporablja verjetnostni algoritem, ki vedno vrne pravilen rezultat. Pričakovana vrednost za časovno zahtevnost algoritma

<sup>10</sup> <http://mathpages.com/home/kmath473.htm>

je polinomska za skoraj vsa naravna števila oz. za vsa pod neko hipotezo. Algoritem uporablja eliptične krivulje in sta ga prva predstavila Goldwasser in Kilian [11], Atkin pa je z uporabo idej teorije kompleksnega množenja (del teorije števil, ki združuje kompleksno analizo, Galoisovo teorijo in modularne forme) pokazal, kako bi se ga dalo uporabiti v praksi, glej [3]. To je leta 1989 storil Morain [16] in to je tudi prvi algoritem, ki je certificiral več kot 1000-mestna praštevila (**praštevila tipa Titanik**) brez upoštevanja njihovih posebnih lastnosti (pri faktorizaciji števila oblike  $2^{2^k} \pm 1$  upoštevamo to lepo obliko, glej Stinson [19, str. 156]). Za certificiranje praštevil  $10^{100} + 267$  potrebuje Mathematica na 300 MHz računalniku 35 sekund.

Čeprav je problem certificiranja praštevil že globoko raziskan, bomo še vedno čakali na elegantnejši algoritem. Mogoče še dolgo časa, saj so za varnost kriptosistema RSA pomembnejši rezultati in algoritmi za problem faktorizacije, ki je še vedno odprt.

## LITERATURA

- [1] M. Agrawal, N. Kayal, N. Saxena, *PRIMES is in P*, Preprint, <http://www.cse.iitk.ac.in/primalty.pdf>, 6. avg. 2002.
- [2] T. M. Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag, 1996.
- [3] A. O. L. Atkin, F. Morain, *Elliptic curves and primality proving*, Mathematics of Computation, **61** (1993), 29–68.
- [4] R. C. Baker, G. Harman, *The Brun-Titchmarsh Theorem on Average*, Proceedings of a conference in Honor of Heini Halberstam, Volume 1, 1996, 39–103.
- [5] D. Bernstein, *Proving primality after Agrawal-Kayal-Saxena*, version of January 25, 2003, <http://cr.yp.to/papers.html#aks>.
- [6] R. Bhattacharjee, P. Pandey, *Primality testing. Technical report*, IIT Kanpur, 2001.
- [7] D. Bini, V. Pan, *Polynomial and Matrix Computation: Fundamental Algorithms, Volume 1*, Birkhäuser, Boston-Basel-Berlin, 1994.
- [8] F. Bornemann, *PRIMES Is in P: A breakthrough for "Everyman"*, Notices of the American Mathematical Society, **50** (maj 2003), 545–552.
- [9] D. Bressoud, *Factorization and Primality Testing*, Springer-Verlag, 1989.
- [10] E. Fouvry, *Théorème de Brun-Titchmarsh: application au théorème de Fermat*, Invent. Math., **79** (1985), 383–407.
- [11] S. Goldwasser, J. Kilian, *Almost all primes can be quickly certified*, Proceedings of 18th STOC, 1986, 316–329.
- [12] G. H. Hardy, J. E. Littlewood, *Some problems of 'Partitio Numerorum' III: On the expression of a number as a sum of primes*, Acta Mathematica, **44** (1922), 1–70.
- [13] E. Horowitz, S. Sahni, *Fundamentals of Computer Algorithms*, Computer Science Press, Rockville, 1978.
- [14] N. Kayal, N. Saxena, *Towards a deterministic polynomial-time test. Technical report*, IIT Kanpur, 2002.
- [15] J. Kozak, *Podatkovne strukture in algoritmi*, DMFA Slovenije, Ljubljana, 1986.
- [16] F. Morain, *Implementation of the Atkin-Goldwasser-Kilian Primality Testing Algorithm*, INRIA Research Report, #911, Oktober 1988.
- [17] R. Petek, *RSA kriptosistem, diplomsko delo*, Ljubljana, 2000.
- [18] T. Pisanski, *Izračunljivost in rešljivost*, Obzornik za mat. in fiz., **25** (1978), 41–54.
- [19] D. R. Stinson, *Cryptography: Theory and Practice*, CRC Press, 1995.
- [20] I. Vidav, *Algebra, 2. natis*, DMFA SRS, IMFM in FNT, Ljubljana, 1980.
- [21] J. Žerovnik, *Verjetnostni algoritmi*, Obzornik za mat. in fiz., **39** (1992), 129–139.

# RAVNINSKE MREŽE IN VERIŽNI ULOMKI PRISPEVEK K RAZUMEVANJU FILOTAKSE, 3. DEL

MILAN HLADNIK

Math. Subj. Class. (2000): 52 C 05; 11 A 55

V sestavku predstavimo uporabo verižnih ulomkov pri linearno transformirani ravninski celoštevilski mreži, reducirani v eni dimenziji po modulu 1, tj. naviti na valj z obsegom 1. Taka cilindrična mreža točk ima pomen v rastlinski filotaksi, se pravi, pri razporeditvi listov vzdolž stebela in tudi pri spiralnih vzorcih cvetov ali semen.

## PLANNAR LATTICES AND CONTINUED FRACTIONS A CONTRIBUTION TO UNDERSTANDING PHYLLOTAXIS, PART 3

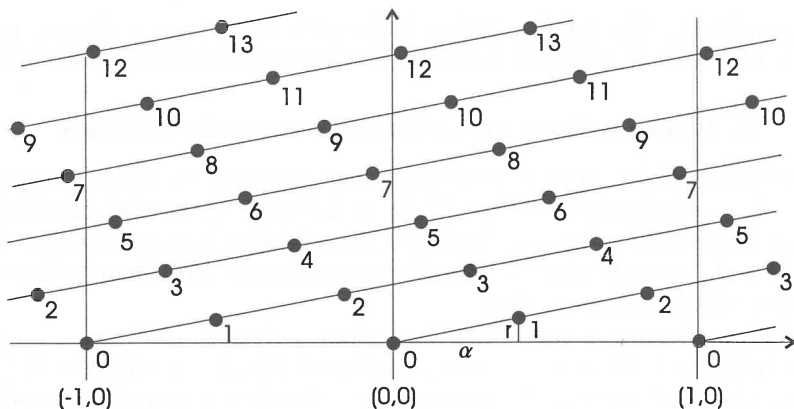
In the article we present an application of continued fractions to a linearly transformed integer-valued planar lattice reduced in one dimension modulo 1, i.e. wrapped on a cylinder with perimeter 1. Such a cylindrical lattice plays a role in plantal phyllotaxis, i.e. in the distribution of leaves along the stem and also in spiral patterns of blossoms and seeds.

V članku [5] smo z uporabo teorije verižnih ulomkov opisali strukturo poljubne iracionalne delitve krožnice in do neke mere razložili prednost zlate delitve (tj. delitve v razmerju zlatega reza) pred drugimi iracionalnimi delitvami. Tu si bomo kot dopolnilo k [5] ogledali, kako se taka struktura kaže pri mrežah točk na valju. S pomočjo [1] in [2] bomo odkrili lep geometrijski opis količin, ki smo jih v [5] izrazili z vmesnimi konvergenti (in njihovimi imenovalci) iz razvoja iracionalnega števila v enostavni verižni ulomek. Z ustrezno transformacijo lahko potem pojasnimo tudi nastanek mreže točk na drugih geometrijskih ploskvah in v posebnem primeru nastanek spiralne simetrije v ravninski mreži z danim središčem. Oboje lahko uporabimo v botaniki pri razlagi rastlinske filotakse (glej [4]).

### 1. Mreža točk na valju

Denimo, da imamo v koordinatni ravnini  $(xy)$  snop poševnih vzporednih premic, ki sekajo abscisno os v celoštevilskih točkah. Na teh premicah imejmo mrežo ekvidistančnih točk, ki se na vsaki premici začenja v presečišču z abscisno osjo. Razdalja do naslednje točke na isti premici je enaka za vse premice, in sicer naj bo njena projekcija na os  $x$  enaka  $\alpha$ , na os  $y$  pa  $r$  (glej sliko 1).

Koordinatno ravnino s snopom vzporednih premic in mrežo točk na teh premicah navijmo na pokončni valj, ki ima obseg osnovne krožnice enak 1, tako da se osnovni pas  $0 \leq x < 1$  bijektivno preslika na plašč valja. Pri tem se poševne premice navijejo v eno samo vijačnico, točke mreže pa se natanko pokrijejo. Število  $\alpha$  postane t. i. *divergenčni kot*, tj. kot zasuka od ene do naslednje točke, število  $r$  pa meri *rast* sistema. Skupaj z  $\alpha$  določa *naklon* vijačnice, ki je enak  $r/\alpha$ .



Slika 1

Točke na vijačnici označimo po vrsti kar z naravnimi števili; posledično na isti način, tj. reducirano v smeri  $x$  po modulu 1, označimo tudi mrežne točke v ravnini. Če predpostavimo, da je  $\alpha$  iracionalno število, leži na vsaki tvorilki valja (tj. na vsaki navpični premici v ravnini) kvečjemu ena od mrežnih točk.

Vpeljimo analitične koordinate. Položaj mrežne točke v ravnini je določen z dvema podatkom: na kateri premici leži in katera po vrsti je. Premico naj določa celoštevilska koordinata  $p$ , točke na posamezni premici pa naj šteje celoštevilska koordinata  $q \geq 0$  (zanimajo nas samo točke na zgornji polravnini oziroma na zgornjem delu valja). Kartezični koordinati mrežne točke lahko torej izrazimo s  $p$  in  $q$  na naslednji način:

$$x = \alpha q - p, \quad y = rq. \quad (1)$$

Pri  $p = 0$  dobimo točke na premici skozi koordinatno izhodišče z naklonom  $r/\alpha$ , torej na premici  $y = rx/\alpha$ . Točka  $q = 0$  se nahaja v koordinatnem izhodišču, naslednja točka  $q = 1$  na tej premici ima kartezični koordinati  $x_1 = \alpha$ ,  $y_1 = r$ , naslednja točka  $q = 2$  ima koordinati  $x_2 = 2\alpha$ ,  $y_2 = 2r$ , itd. Prva vzporedna premica nad premico skozi izhodišče je premica  $p = 1$  z enačbo  $y = r(x+1)/\alpha$ , naslednja premica  $p = 2$  ima enačbo  $y = r(x+2)/\alpha$  itd. Točke na abscisni osi  $y = 0$  dobimo le v primeru  $q = 0$ , in sicer  $x = -p$ ,  $p \in \mathbb{Z}$ . Edina točka na ordinatni osi  $x = 0$  je izhodišče, ki ga dobimo pri  $q = 0$  in  $p = 0$  (za  $q \neq 0$  enakost  $\alpha q = p$  ni možna, ker je  $\alpha$  iracionalno število).

Mrežne točke na osnovnem polpasu  $0 \leq x < 1$ ,  $y \geq 0$ , imajo kartezične koordinate  $x = \{\alpha q\}$ ,  $y = rq$ , kjer je  $\{\alpha q\} = \alpha q - [\alpha q]$  in  $[\alpha q]$  celi del števila  $\alpha q$ . Če označimo  $p = [\alpha q]$ , vidimo, da leži točka z oznako  $q$  v osnovnem polpasu na  $p$ -ti premici. In obratno, če  $q$ -ta točka na  $p$ -ti premici leži v osnovnem pasu, mora nujno veljati  $p = [\alpha q]$ , njeni koordinati pa sta dani z (1).

**Opomba 1.** Če mrežne točke, ki ležijo v osnovnem polpasu, projiciramo na abscisno os, dobimo ravno delilne točke odseka  $[0, 1]$  iz članka [5].

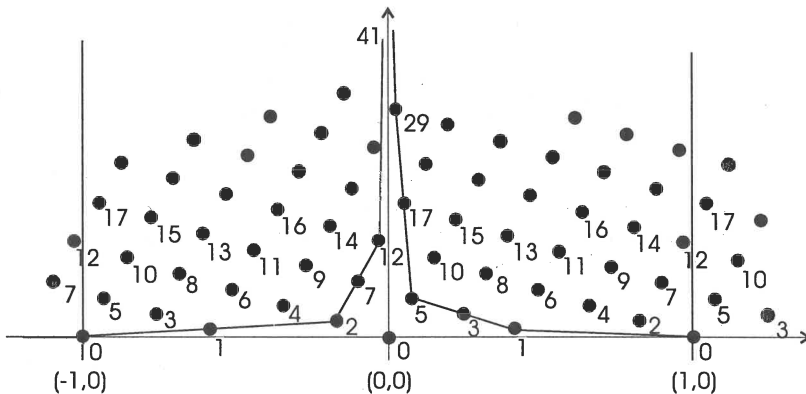
## 2. Geometrijska interpretacija verižnih ulomkov

Mrežnim točkam, ki so znotraj osnovnega polpasu, tj. točkam  $(\{\alpha q\}, r_q)$ ,  $q = 1, 2, 3, \dots$ , dodajmo še točko  $(1, 0)$  in dobljeni neskončni množici točk poiščimo konveksno ovojnico. Njen rob je sestavljen iz navpičnega poltraka  $x = 1, y \geq 0$ , in neskončnega konveksnega poligona (lomljene premice), ki od spodaj oklepa dano množico.

Podobno storimo z mrežnimi točkami v polpasu  $-1 \leq x < 0, y \geq 0$  (zdaj je točka  $(-1, 0)$  zraven!), torej s točkami  $(\{\alpha q\} - 1, r_q)$ ,  $q = 0, 1, 2, \dots$ . Rob konveksne ovojnice za to množico je sestavljen iz navpičnega poltraka  $x = -1, y \geq 0$ , in neskončnega konveksnega poligona, ki od spodaj oklepa dano množico.

Lahko si pomagamo z naslednjo predstavo obeh neskončnih poligonov: Mrežne točke v ravnini si predstavljajmo kot neskončno veliko drevesnico ali sadovnjak (točke pomenijo posamezna drevesa). Denimo, da za drevo v točki  $(1, 0)$  privežemo neskončno dolgo vrv in jo napnemo iz smeri osi  $x$  okrog dreves, ki so znotraj polpasu  $0 \leq x < 1, y > 0$ . Nekatera drevesa vrvi spremenijo smer (voglne točke konveksnega poligona), drugih se vrv le dotakne (notranje točke stranic poligona). Isto storimo z drevesom v točki  $(-1, 0)$ . Vzdolž ordinatne osi  $x = 0$  se vrvi asimptotično približujeta druga drugi.

Na sliki 2 je narisani primer, ko je  $\alpha = \sqrt{2}$ . Točke 1, 5, 29 so npr. oglišča desnega poligona, točki 2, 12 levega, medtem ko sta npr. 3 in 17 notranji točki na stranicah desnega, 1, 7 in 41 pa notranje točke na stranicah levega poligona.



Slika 2

Prepričajmo se, da ustrezajo oglišča poligona konvergentom v razvoju števila  $\alpha$  v verižni ulomek, notranje točke stranic pa vmesnim konvergentom

(glej npr. dodatek v [5] ali [3], [7]). Natančneje, pokažimo, da velja naslednja trditev:

**Trditev 1.** *Za točko z oznako  $q$ , ki leži na premici  $p$  in je oglišče poligona, je  $p/q$  konvergent za  $\alpha$ . Oglišča levega poligona pripadajo lihim konvergentom, oglišča desnega poligona pa sodim konvergentom. Za točko z oznako  $q$ , ki leži na premici  $p$  in je notranja točka stranice poligona, pa je  $p/q$  vmesni konvergent in leži med dvema zaporednima lihima ali zaporednima sodima konvergentoma, odvisno od tega, ali je točka  $q$  na levem ali na desnem poligonu.*

*Dokaz.* Potujmo vzdolž enega od obeh poligonov v smeri naraščajočega števila  $q$  in sproti opazujemo oddaljenosti točk z oznako  $q$  od ordinatne osi  $x = 0$ . Zaradi konveksnosti obeh poligonov se te oddaljenosti z rastočim  $q$  manjšajo. Za točko  $q$ , ki leži na premici  $p$ , je oddaljenost od ordinatne osi enaka  $|\{\alpha q\} - 1| = p - \alpha q$ , če leži na levem poligonu, in  $\{\alpha q\} = \alpha q - p$ , če leži na desnem poligonu. Ta razdalja je hkrati dolžina prvega ali zadnjega odseka pri delitvi enotskega intervala  $[0, 1)$  z abscisami mrežnih točk. V [5] smo videli, da se daljši odsek deli prej kot krajši. Če obstaja na drugem poligonu točka  $q' < q$ , katere oddaljenost do ordinatne osi je manjša od oddaljenosti točke  $q$ , potem  $q$  še ne more biti oglišče poligona. Če je točka  $q$  oglišče enega od poligonov, mora potemtaka za vsako drugo točko  $b < q$  in za vsako naravno število  $a$  veljati  $|\alpha q - p| < |\alpha b - a|$ . Rečemo, da je ulomek  $p/q$  najboljši približek 2. vrste za število  $\alpha$ . Iz teorije verižnih ulomkov pa je znano (glej npr. [7] ali dodatek v [5]), da so pri iracionalnem številu  $\alpha$  najboljši približki druge vrste prav konvergenti v razvoju števila  $\alpha$  v verižni ulomek. Torej ustrezajo oglišča poligonov natanko konvergentom, lihim na levem polpasu in sodim na desnem polpasu.

Vsaka notranja točka ene od poligonskih stranic je očitno konveksna kombinacija sosednjih oglišč istega poligona. Še več, na isti stranici so notranje točke enakomerno (ekvidistančno) razporejene med krajiščema. Potem to velja tako za oznake točk kot premic,  $q$  in  $p$ . V istem razmerju pa so porazdeljeni tako števcji kot imenovalci vmesnih konvergentov  $p_{k,i}/q_{k,i}$ ,  $i = 1, 2, \dots, a_k$ . Velja namreč  $p_{k,i} = ip_{k-1} + p_{k-2}$  in  $q_{k,i} = iq_{k-1} + q_{k-2}$ ; potem pa je ob upoštevanju rekurzivnih formul  $p_k = a_k p_{k-1} + p_{k-2}$  in  $q_k = a_k q_{k-1} + q_{k-2}$  res

$$p_{k,i} = i(p_k - p_{k-2})/a_k + p_{k-2} = \frac{i}{a_k} p_k + (1 - \frac{i}{a_k}) p_{k-2};$$

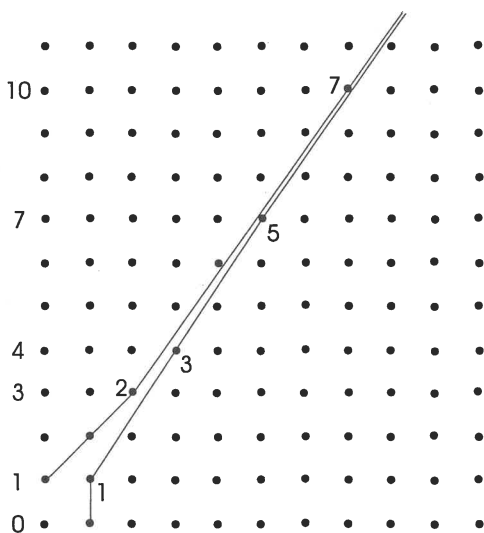
$$q_{k,i} = i(q_k - q_{k-2})/a_k + q_{k-2} = \frac{i}{a_k} q_k + (1 - \frac{i}{a_k}) q_{k-2}.$$

Torej je npr. točka  $(\alpha q_{k,i} - p_{k,i}, r q_{k,i})$  res konveksna kombinacija točk  $(\alpha q_k - p_k, r q_k)$  in  $(\alpha q_{k-2} - p_{k-2}, r q_{k-2})$ , se pravi, da leži na daljici med ogliščema, ki pripadata konvergentoma  $p_k/q_k$  in  $p_{k-2}/q_{k-2}$ . Spoznali smo torej, da ustrezajo notranje točke stranic obeh poligonov natanko vmesnim konvergentom.

Poleg tega velja za vsak  $k$  in za vsak  $i = 1, 2, \dots, a_k - 1$  tudi  $|\alpha q_{k,i} - p_{k,i}| > |\alpha q_{k-1} - p_{k-1}|$ , medtem ko je seveda  $|\alpha q_{k,a_k} - p_{k,a_k}| = |\alpha q_k - p_k| < |\alpha q_{k-1} - p_{k-1}|$ . O tem se lahko prepričamo z neposrednim računom z uporabo definicije vmesnih konvergentov, saj je  $(\alpha q_{k,i} - p_{k,i}) - (p_{k-1} - \alpha q_{k-1}) = (i+1)(\alpha q_{k-1} - p_{k-1}) + (\alpha q_{k-2} - p_{k-2}) = \alpha q_{k,i+1} - p_{k,i+1}$  oziroma  $|\alpha q_{k,i} - p_{k,i}| - |\alpha q_{k-1} - p_{k-1}| = |\alpha q_{k,i+1} - p_{k,i+1}|$  za  $i < a_k$ .

**Zgled.** Na sliki 2 so npr. točke 1, 2, 5, 12, 29 imenovalci (izmenično) lihih in sodih konvergentov, točke 3, 7, 17, 41 pa imenovalci (lihih in sodih) vmesnih konvergentov. Res je zaporedje vmesnih konvergentov za število  $\alpha = \sqrt{2}$  enako  $1/1, 2/1, 3/2, 4/3, 7/5, 10/7, 17/12$  itd., pri čemer je vsak drugi člen pravi konvergent:  $1/1, 3/2, 7/5, 17/12$  itd. To sledi iz dejstva, da je razvoj števila  $\sqrt{2}$  v enostavni verižni ulomek enak  $[1; 2, 2, \dots]$ . Poleg tega vidimo, da so npr. točke 1, 2 in 7 na levem poligonu bolj oddaljene od ordinatne osi kot oglišče 5 na desnem poligonu, točka 12 pa že leži bližje ordinatni osi.

Še lepše kot v ravnini  $(xy)$  vidimo sode (spodnje) in lihe (zgornje) vmesne konvergente v transformirani ravnini  $(qp)$ . Namesto poševne mreže točk  $(x, y)$ , kjer bi bilo treba ustrezen  $q$  in  $p$  še določiti, imamo zdaj kar kvadratno mrežo celoštevilskih točk  $(q, p)$ . To je t. i. *Kleinova geometrizacija* verižnega ulomka za  $\alpha$  (na sliki 3 je prikazana Kleinova geometrizacija verižnega ulomka za  $\sqrt{2}$ ).



Slika 3

Premica  $x = 0$  s slike 2 se je transformirala v premico  $p = \alpha q$ , ki na sliki 3 sicer ni prikazana, narisana pa sta oba transformirana poligona, ki se tej premici asimptotično približujeta od spodaj in od zgoraj. Sodi

konvergenti so zdaj predstavljeni z oglišči spodnjega poligona, lihi pa z oglišči zgornjega poligona. Če je  $(q, p)$  tako oglišče, je  $p/q$  (sodi ali lihi) konvergent za  $\alpha$ . Vmesne točke predstavljajo vmesne konvergente. Na sliki 3 določa npr. oglišče  $(2, 3)$  lihi konvergent  $3/2 = [1; 2]$ , oglišče  $(3, 4)$  pa sodi vmesni konvergent  $4/3 = [1; 2, 1]$ .

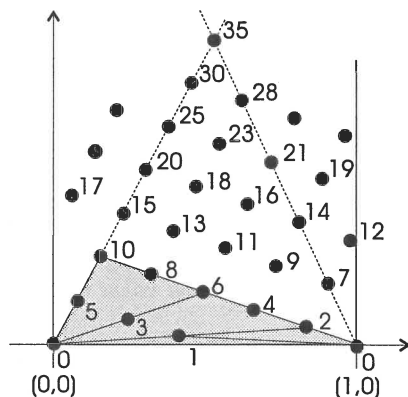
### 3. Vidnost parastihij

V zvezi z razporeditvijo mrežnih točk na valju (ali v ravnini) obravnavajmo še en problem: *Katere vijačnice na valju vidimo oziroma katere smeri v ravnini so najbolj opazne?*

To so gotovo smeri, v katerih je gostota točk največja (točke so najbližje skupaj). Izhajajmo npr. iz točke 0 (tj. izhodišča  $(0, 0)$  na sliki 4). Desno od 0 poiščimo najbližjo točko (naj ima npr. oznako  $n$ ) in enako storimo tudi levo (točka z oznako  $m$ ), vendar to točko premaknimo za enoto v desno, tako da vse opazujemo v osnovnem polpasu  $0 \leq x < 1, y \geq 0$ . Točka  $m$  je torej v tem polpasu najbližja mrežna točka k točki  $(1, 0)$ . Potegnimo poltraka iz točke  $(0, 0)$  skozi  $n$  in iz točke  $(1, 0)$  skozi  $m$ . Sekata se v točki  $mn$ . V primeru  $\alpha = \sqrt{2}$  sta taki točki  $n = 5$  in  $m = 2$ , poltraka se sekata v točki  $mn = 10$  (slika 4). Smeri teh dveh poltrakov sta optično odlikovani, imenujemo ju *osnovni parastihiji*, par  $(m, n)$  pa *osnovni parastihijski par*, ki določa število vidnih parastihij oziroma, kot rečemo, filotakso tipa  $(m, n)$ . V osnovnem pasu izhaja iz odseka  $[0, 1)$  natanko  $m$  vzporednih poltrakov z enako gostoto mrežnih točk v levo in natanko  $n$  vzporednih poltrakov v desno (glej sliko 4). Po definiciji vidnosti morajo biti presečišča vsakega od njih z vsakim iz druge skupine vzporednih poltrakov zasedena z mrežnimi točkami. Včasih govorimo tudi o *osnovnem parastihiskem trikotniku*, določenem s točkami  $(0, 0)$ ,  $(1, 0)$  in točko z oznako  $mn$  (na sliki 4 je trikotnik zatemnjen).

To je glavna vidna značilnost filotakse. V oči pa nam padejo morda še druge smeri, določene bodisi z restrikcijami ali ekstenzijami osnovnega parastihijskega para. Pod restrikcijo para  $(m, n)$ , kjer je npr.  $m < n$  kot v zgornjem primeru, razumemo par  $(m, n - m)$ . Ekstenzije pa so lahko leve  $(m + n, n)$  ali desne  $(m, m + n)$ . V primeru filotakse  $(2, 5)$  na sliki 4 imamo npr. vidne še restrikcije  $(2, 3)$ ,  $(2, 1)$  in  $(1, 1)$  ter levi ekstenziji  $(7, 5)$  in  $(12, 5)$ . Za tema levima ekstenzijama bi prišli dve desni ekstenziji  $(12, 17)$  in  $(12, 29)$  itd., vedno v skladu s pravilom  $a_i$  levih in nato  $a_{i+1}$  desnih ekstenzij, kjer so  $a_i$  elementi verižnega ulomka (glej [1]). To je spet ena od uporab verižnih ulomkov pri razporeditvi mrežnih točk oziroma pri vidnih efektih filotakse.

**Opomba 2.** Ko ugotavljamo vidnost parastihij, je pomembno, kolikšna je razdalja točke  $q$  do izhodišča  $(0, 0)$ ? Kartezična koordinata točke  $q$  je  $(\{\alpha q\}, r q)$  na desnem in  $(\{\alpha q\} - 1, r q)$  na levem polpasu (primerjaj sliko 2). Torej je razdalja do izhodišča  $d_q = \sqrt{\{\alpha q\}^2 + r^2 q^2}$  na desnem oziroma  $d_q = \sqrt{(\{\alpha q\} - 1)^2 + r^2 q^2}$  na levem pasu. Naj bo  $q$  izhodišču najbližje oglišče enega od obeh poligonov. Če  $r$  zmanjšujemo, pridejo bližje izhodišču



Slika 4

druga, kasnejša oglišča obeh polygonov. Tako vidimo, da razpored vidnih parastihij, tj. tip filotakse  $(m, n)$ , ni odvisen samo od divergenčnega kota  $\alpha$ , ampak tudi od rasti sistema, ki jo določa  $r$ . S spreminjanjem parametra  $r$  se spreminja tudi tip filotakse. Na sliki 2 je npr. oglišče 5 na desnem polygonu najbližje izhodišču, na levem je to točka 2, in imamo, kot smo ugotovili prej, filotakso tipa  $(2, 5)$ . Če bi  $r$  primerno povečali, bi bila izhodišču najbližja točka 2 na levem polygonu, za njo pa točka 1 na desnem polygonu. Dobili bi filotakso tipa  $(2, 1)$ . Ko pa bi  $r$  zmanjšali, bi izhodišču najbližja točka prej ali slej postalo npr. oglišče 12 na levem polygonu in tip filotakse bi se spremenil v  $(12, 5)$  (primerjaj zgornjo razlago o ekstenzijah).

V naravi je hitrost rasti odvisna od mnogih dejavnikov. V obdobju hitre rasti (večjega  $r$ ) je tip filotakse nizek, v kriznem času (pri majhnem  $r$ ) pa opazimo filotakso višjega reda. Nemalokrat pri isti rastlini (npr. v glavi sončnice) opazimo spremembo števila vidnih parastihij, kar je gotovo posledica spremenjenih razmer, ki vplivajo na hitrost rasti.

#### 4. Mreža točk na geometrijskih objektih

Verižne ulomke oziroma (vmesne) konvergente iracionalnega števila  $\alpha$  smo na naraven način povezali z ravninsko mrežo točk, ki smo jo brez težav prenesli na valj. Pogosto pa je zanimiva tudi drugačna geometrija. Radi bi npr. imeli podoben sistem mrežnih točk na valju, polkrogli, polstožcu ali celo v krogu. To lahko dosežemo z ustrezno transformacijo ravnine  $(xy)$ .

Vsa telesa (in tudi ravninski krog) naj imajo obseg osnovne krožnice enak 1 (tj. polmer enak  $1/(2\pi)$ ).

Rekli smo že, da lahko osnovni ravninski polpas preprosto zvijemo v neskončni valj s polmerom  $1/(2\pi)$ . Položaj točke na takem valju lahko elegantno podamo s kompleksno koordinato v polarni obliki  $w = \frac{1}{2\pi} e^{i\phi}$  in z nenegativno realno koordinato  $z$ . Iz realne ravnine  $(xy)$  potem preidemo

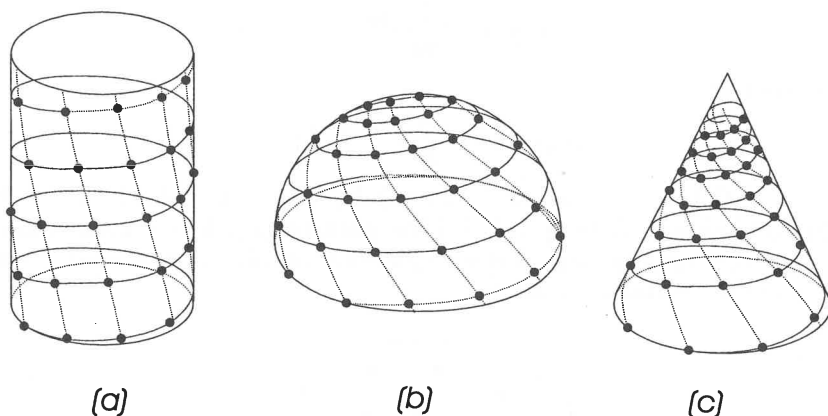
na plašč valja s transformacijo

$$(x, y) \mapsto \left( \frac{1}{2\pi} e^{2\pi i x}, y \right).$$

Ker celo število  $p$  ne prispeva ničesar k vrednosti funkcije  $e^{2\pi i(\alpha q - p)}$ , je za  $q$ -to mrežno točko na premici  $p$  polarni kot enak  $\phi = 2\pi(\alpha q - p) = 2\pi\{\alpha q\}$  in višina  $z = rq$ . Položaj  $q$ -te mrežne točke na valju lahko potemtakem zapišemo s parom

$$(w_q, z_q) = \left( \frac{1}{2\pi} e^{2\pi i \alpha q}, rq \right).$$

Vsaka taka točka leži na ustrezni vijačnici, ki se ovija okrog valja (slika 5a).



Slika 5

Podobno lahko mrežo točk v ravnini  $(xy)$  upodobimo na zgornji hemisferi krogle s polmerom  $1/2\pi$  npr. z uporabo transformacije

$$(x, y) \mapsto \left( \frac{1}{2\pi} (e^{2\pi i x - y}, \sqrt{1 - e^{-2y}}) \right).$$

Pri tem se točka  $q$  s kartezičnimi koordinatami  $(\alpha q - p, rq)$  preslika v točko

$$(w_q, z_q) = \left( \frac{1}{2\pi} (e^{2\pi i \alpha q - rq}, \sqrt{1 - e^{-2rq}}) \right).$$

Zaporedje točk  $(w_q, z_q)$  se navije na sfero okrog severnega pola (slika 5b).

Za stožec s polmerom osnovne ploskve  $1/2\pi$  in višino  $h$  uporabimo npr. transformacijo

$$(x, y) \mapsto \left( \frac{1}{2\pi} e^{2\pi i x - y/(h+1)}, h(1 - e^{-y/(h+1)}) \right).$$

Za  $q = 0, 1, 2, \dots$  dobimo zdaj zaporedje točk

$$(w_q, z_q) = \left( \frac{1}{2\pi} e^{2\pi i \alpha q - r q / (h+1)}, h(1 - e^{-r q / (h+1)}) \right),$$

vzdolž stožčaste vijajnice, ki se navija proti vrhu stožca (slika 5c).

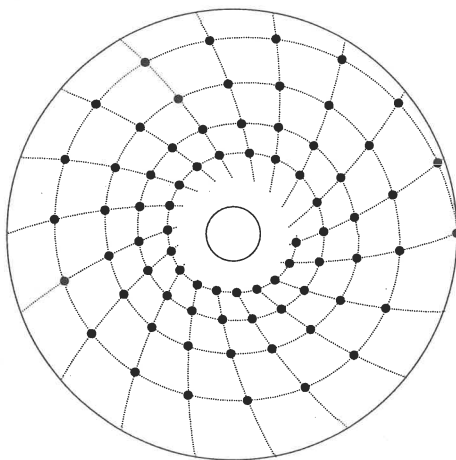
Stožec z zelo veliko višino  $h$  je skoraj enak neskončnemu valju. Hitro se lahko prepričamo, da v limiti  $h \rightarrow \infty$  res dobimo iz stožca valj. Mreža točk na valju je limitna lega mreže točk na stožcu. Po drugi strani se stožec splošči v svojo osnovno ploskev, ko njegova višina  $h$  konvergira proti 0. Torej je tudi mreža točk na krogu v ravnini ( $w$ ) limitna lega mreže točk na stožcu. Pri  $h = 0$  res dobimo transformacijo ravnine ( $xy$ ) v krog. Podana je s predpisom

$$(x, y) \mapsto \left( \frac{1}{2\pi} e^{2\pi i x - y}, 0 \right).$$

Zaporedje točk

$$(w_q, z_q) = \left( \frac{1}{2\pi} e^{2\pi i \alpha q - r q}, 0 \right),$$

kjer je  $q = 0, 1, 2, \dots$ , leži na (rodovni) logaritemski spirali. Pri velikem številu točk vidimo tiste spirale (vidne parastihije), ki so transformiranke vidnih smeri iz ravnine ( $xy$ ), kot smo jih obravnavali v 3. razdelku. Rezultat je t. i. *spiralna filotaksa* (slika 6).



Slika 6

**Opomba 3.** Prenesimo mrežo točk na katerem koli od obravnavanih objektov (valju, krogli, stožcu ali krogu) na osnovno krožnico z obsegom 1, tako da povsod v zgornjih formulah izberemo  $r = 0$ , tj. odpravimo rast sistema in obdržimo le divergenčni kot  $\alpha$ . (Isto dosežemo s pravokotno projekcijo mrežnih točk v osnovnem pasu ravnine ( $xy$ ) na osnovnico tega

pasu, glej opombo 1.) Tako dobimo iracionalno delitev te krožnice (glej [5]). V [5] smo skušali utemeljiti prednosti zlate delitve krožnice pred poljubno iracionalno delitvijo. Vse to se seveda odraža tako na ravninski mreži kot na transformiranih mrežah točk. Tiste, ki ustrezajo zlati delitvi in so zato povezane s Fibonaccijevimi števili, so lepše. S takimi mrežami točk lahko potem opišemo marsikatero dogajanje v rastlinski morfogenezi. Odprto pa še vedno ostane glavno vprašanje, zakaj v rastlinskem svetu tako pogosto, menda v več kot 90% primerov (glej npr. [6]), nastopi ravno Fibonaccijeva filotaksa.

## LITERATURA

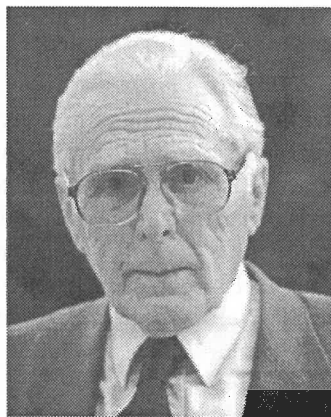
- [1] I. Adler, *The role of continued fractions in phyllotaxis*, J. Algebra **205** (1998), 227–243.
- [2] H. S. M. Coxeter, *The role of intermediate convergents in Tait's explanation for phyllotaxis*, J. Algebra **20** (1972), 167–175.
- [3] J. Grasselli, *Diofantovski približki*, Knjižnica Sigma 51, DMFAS, Ljubljana 1992.
- [4] M. Hladnik, *Dinamični model spiralne filotakse. Prispevek k razumevanju filotakse, 1. del*, Obzornik mat. fiz. **50** (2003), 33–41.
- [5] M. Hladnik, *Zlata delitev krožnice. Prispevek k razumevanju filotakse, 2. del*, Obzornik za mat. in fiz. **50** (2003), 97–109.
- [6] R. V. Jean, *Phyllotaxis, A Systemic Study in Plant Morphogenesis*, Cambridge University Press 1994.
- [7] A. Ya. Khinchin, *Continued fractions*, Dover Publ. 1992.

## VESTI

### Profesorju Niku Prijatelju v slovo

Govor prof. Jožeta Vrabca na pogrebu na Žalah 21. julija 2003

Niko Prijatelj se je rodil leta 1922 v Ljubljani. Po maturi leta 1940 se je vpisal na Filozofsko fakulteto v Ljubljani in na njej študiral matematiko s fiziko in filozofijo. Med vojno je bil nekaj časa v koncentracijskem taborišču v Gonarsu. Po vrnitvi je študij nadaljeval in diplomiral leta 1946. Že leto pred diplomo je začel učiti na III. ženski gimnaziji v Ljubljani. Kasneje je poučeval še na nekaterih drugih srednjih šolah v Ljubljani, v Postojni in eno leto v Sarajevu. Za univerzitetno kariero po vojni ni bilo prave možnosti. Šele na koncu petdesetih let je bilo matematiki dodeljenih nekaj novih asistent-skih mest in na eno od njih je bil leta 1957 sprejet profesor Prijatelj. S tem je dobil priložnost, da se znova poglobi v študij matematike. Leta 1960 je bil imenovan za predavatelja matematike. Kot štipendist francoske vlade je bil v študijskem letu 1959/60 na 8-mesečnem izpopolnjevanju na inštitutu H. Poincaré v Parizu. Ko se je vrnil, je leta



1961 na Univerzi v Ljubljani promoviral za doktorja matematičnih znanosti. Istega leta je bil imenovan za docenta, nato leta 1970 za izrednega profesorja in leta 1977 za rednega profesorja.

Še kot srednješolski profesor je sodeloval z univerzo, in sicer je v letih 1954–57 kot honorarni predavatelj na Višji pedagoški šoli poučeval predmet Metodika pouka matematike in v letih 1955–61 na Naravoslovni fakulteti predmet Elementarna matematika z metodiko. Po izvolitvi za visokošolskega učitelja je predaval najprej predmeta Matematika 1 in 2 za študente kemije, kasneje pa vrsto predmetov za študente matematike: Analizo 1 in 2, Teorijo množic, Osnove topologije in Osnove matematike. Za študente fizike je nekaj let predaval predmeta Analiza 1 in 2, na podiplomskem študiju iz matematičnega izobraževanja pa predmet Izbrana poglavja iz osnov matematike.

Prof. Prijatelj je bil eden najboljših predavateljev na matematičnem oddelku. Njegova predavanja so bila vedno zelo dobro pripravljena, na primernem nivoju zahtevnosti, matematično izjemno precizna in metodično izpiljena. Toda vsi ti izrazi povedo premalo. Prof. Prijatelj je bil zaljubljen v matematiko in znal je to svojo zaljubljenost, to ljubezen prelit v svoja predavanja. Zato so bila ta ne samo odlična, ampak tudi virtuoзна in navdušujoča. Njegovo vzgojno delo pa ni bilo omejeno na redna predavanja na univerzi. Bil je pogost in zelo zaželen predavatelj na seminarjih za izpopolnjevanje znanja srednješolskih učiteljev matematike, pa tudi pri posebnih predavanjih za srednješolce. Tudi pri teh predavanjih je razlival med poslušalce svojo navdušenje za matematiko, a jim tudi vzbujal ljubezen do pedagoškega poklica, ki je, žal, danes tako malo cenjen.

Raziskovalno in publicistično delo je prof. Prijatelj posvetil matematični analizi, algebri in osnovam matematike. Medtem ko njegovi izvirni znanstveni članki sodijo v prvi dve od teh treh področij, se je neizbrisno zapisal v slovensko matematično zgodovino predvsem s svojim delom na tretjem področju. Bil je začetnik in utemeljitelj študija matematične logike in širših osnov matematike v našem prostoru. Na prvem mestu je treba omeniti njegovo knjižico *Uvod v matematično logiko*, ki je izšla že davnega leta 1960, in njeno 20 let mlajšo nadgradnjo *Osnove matematične logike* v treh delih. Po teh knjigah smo se spoznali s tedaj za nas povsem novim področjem skoraj vsi slovenski matematiki, a posebno prva si je našla še mnogo širši krog bralcev. Podobno nalogo je opravila njegova trilogija *Matematične strukture* 1, 2, 3. O odmevnosti teh knjig priča to, da je doslej izšlo že nekaj ponovnih izdaj, od katerih so bile nekatere predelane in dopolnjene. Za ožji krog uporabnikov je napisal univerzitetna učbenika *Uvod v matematično analizo* 1 in 2, ki po globini in širini marsikje presegata učni program.

Prof. Prijatelj spada v generacijo slovenskih matematikov, ki je ustvarjala in razširjala osnove visokošolske matematike pri nas in omogočila

njen razcvet. K temu je ogromno prispeval s svojim organizacijskim in vodstvenim delom. Tri leta je bil direktor Inštituta za matematiko, fiziko in mehaniko in dve leti predstojnik njegovega oddelka za matematiko. V tem času si je pridobil velike zasluge za gradnjo nove stavbe na Jadranski cesti, kjer imata še vedno svoje prostore ta inštitut in Fakulteta za matematiko in fiziko. Dvakrat po dve leti je bil predstojnik našega oddelka (za matematiko in fiziko oziroma za matematiko in mehaniko) na Fakulteti za naravoslovje in tehnologijo. Dve leti je bil predsednik Društva matematikov, fizikov in astronomov Slovenije, nekaj let predsednik njegove komisije za tisk in 10 let član uredniškega odbora revije *Obzornik za matematiko in fiziko*. Mnogo let je zastopal našo stroko v raznih organih Raziskovalne skupnosti Slovenije, slovensko matematiko v jugoslovanskih strokovnih združenjih in jugoslovansko v balkanskih in evropskih. Za svoj mnogostranski prispevek k razvoju slovenske matematike je bil leta 1974 odlikovan z redom dela z zlatim vencem in s plaketo Zveze društev matematikov, fizikov in astronomov Jugoslavije.

Spoštovani prof. Prijatelj, dragi Niko! Naj tem, bolj suhoparnim podatkom dodam še nekaj besed. Želja po znanju in iskanje resnice sta Te oblikovala v razumnika, v osebnost, ki daleč presega okvir ene stroke. Kot prepričan demokrat si se kljub tveganju postavil v prve vrste tistih, ki so raztrgali spono preživelega sistema in vzpostavili samostojno Slovenijo. Tvoji ljubezni do knjige se moramo zahvaliti ne le za besedila, s katerimi si oral ledino slovenske matematične besede, ampak tudi za sooblikovanje naše knjižnice. S svojim osebnim zgledom si nam pričeval, da je življenje človeka v skladu z njegovim notranjim moralnim zakonom ne le najvišja vrednotna zanj, temveč močno pozitivno vpliva tudi na vso njegovo okolico. Občudovali smo Tvojo držo, s katero si prenašal neusmiljene udarce usode, ki so Ti najprej vzeli drago ženo, nedavno pa še hčer in našo kolegico Andrejo, čeprav si se do zadnjega boril za njeno življenje.

Tvoj duh ni klonil, le telo se je utrudilo. Odpočij si, dragi Niko! Naj ti bo zemljica lahka! Vsem Tvojim pa izrekam iskreno sožalje v imenu slovenskih matematikov in v svojem osebnem imenu.

Govor so napisali:

*Edvard Kramar, Tomaž Pisanski in Jože Vrabec*

## APRIL 2003 – MESEC MATEMATIČNEGA OZAVEŠČANJA

Od leta 1999 naprej je v Združenih državah Amerike april razglašen za *mesec matematičnega ozaveščanja* (Mathematics Awareness Month). Že pred tem so od leta 1986 dalje pripravljali tedne matematičnega ozaveščanja. Vsako leto je bila izbrana nova tema; v osemnajstih letih delovanja je odbor *Joint Policy Board for Mathematics*, ki ga sestavljajo Mathematical

Association of America (MAA), American Mathematical Society (AMS) in Society for Industrial and Applied Mathematics (SIAM), izbral tako različne naslove, kot so npr. *Sto let ameriške matematike*, *Matematika in internet*, *Matematika in genom*.

Letošnja tema je bila *Matematika in umetnost*. Ameriški kolidži, univerze, študentske skupine in drugi so organizirali delavnice, tekmovanja, razstave, predavanja in simpozije, na katerih so se osredotočili na globoke in zanimive povezave med matematiko in umetnostjo, ki niso omejene zgolj na dela nizozemskega slikarja M. C. Escherja, na katerega sicer najprej pomislimo. Eno od del tega umetnika, ki je imel težave celo s srednješolsko matematiko, je bilo objavljeno na naslovnici letošnje tretje številke *Obzornika*.

Bralcu svetujemo, da za podrobnejše informacije o aktivnostih obišče spletno stran <http://mathforum.org/mam/03> (če 03 nadomestimo z drugo letnico, lahko vidimo tudi arhive aktivnosti od leta 1991 naprej). V nadaljevanju pa povzemimo nekaj misli iz eseja ameriške matematičarke Doris Schattschneider, ki je pred kratkim gostovala na našem matematičnem kolokviju.

Ravnilo in šestilo, preprosti matematični orodji, so že pred tisočletji uporabljali pri gradnji palač, svetišč in utrdb. V renesansi so uspešno rabili principe projekтивne geometrije in linearne perspektive za prepričljive predstavitve trirazsežnih podob na dvorazsežnih podlagah. Dandanes je najpomembnejše matematično orodje računalnik, v katerem sofisticirani matematični programi ustvarjajo in transformirajo podobe, kar arhitektu, slikarju, grafičnemu oblikovalcu ali komu drugemu pomaga pri delu.

Avtorica najde številne glagole, ki jih lahko vrinemo med samostalnika „matematika” in „umetnost”. Matematika tako umetnost *generira*; tlakovanja in fraktali so morda najbolj naraven primer prelepih struktur, ki jih ustvari preprost algoritem. Take avtomatizirano narejene podobe morda še ne moremo šteti za čisto „pravo” umetnost, a matematika lahko umetnost tudi *navdihuje*; preprosto tlakovanje, ki ga lahko ustvari vsakdo s primernim računalniškim orodjem, bo človek z ustvarjalno žilico znal uporabiti kot podlago za ustvarjanje umetniških del. Po drugi strani matematika umetnost tudi *omejuje*. Naj se slikar še tako trudi, ne bo mogel zaobiti matematičnih izrekov, na primer Eulerjeve formule ali izreka o vsoti notranjih kotov večkotnika. Seveda je omejevanje lahko tudi prostovoljno, kot na primer upoštevanje razmerij v arhitekturi, slikarstvu, kiparstvu.

Na naslovnici tokratnega *Obzornika* je prikazana zanimiva fraktalna struktura sferičnih trikotnikov in petkotnikov, napolnjenih z motivom rib, delo Douglasa Dunhama, ki so ga uporabili kot emblema za letošnji mesec matematičnega ozaveščanja.

Matjaž Konvalinka

# KAKO SEM PISAL UČBENIK ZA FIZIKO

JANEZ STRNAD

PACS 01.40.Gm

Težave pri pisanju srednješolskega učbenika fizike so zbudile razmišljanje o učnem načrtu za fiziko. Na eni strani so fiziko prestavili v prvi letnik in zmanjšali njen obseg in na drugi v učnem načrtu za matematiko nekatere dele prestavili v višje letnike. Zapis si prizadeva izzvati v strokovnih krogih razpravo o vprašanju, ki utegne prizadeti prihodnji položaj fizike v naši šoli in zunaj nje.

## HOW I WROTE A PHYSICS TEXTBOOK

Difficulties encountered writing a high school physics text gave rise to reflections on the physics curriculum. On the one hand physics was shifted to the first class and its content reduced and on the other in the mathematics curriculum some parts were transferred to higher classes. The intent of the article is to engage professional circles in a discussion on questions that may influence the future situation of physics in our school and outside of it.

Ne spodobi se, da pisec piše o svoji knjigi, še posebej o srednješolskem učbeniku. Toda ob škripanju z zobmi med pisanjem *Male fizike* sem si obljudil, da bom prekršil zapoved. Zdaj bom obljudbo izpolnil.

Pisanje učbenika je nevhvaležno delo, ki zahteva veliko časa. Na splošno ni dobro, če se ga pisec loti prezgodaj, preden si lahko pridobi izkušnje, a tudi odlašati ne sme predolgo, ker bi ga lahko izkušnje pripeljale do tega, da bi načrt opustil. Da pisanje učbenikov vzame veliko časa raziskovanju, sta ugotovila L. D. Landau in R. P. Feynman, ki svojih učbenikov nista napisala sama. Vseeno se je veliko fizikov lotilo pisanja učbenikov.

Pisanje srednješolskega učbenika je še posebej nevhvaležno, ker so učbeniki te vrste vsi podobni in ker se je treba omejiti zgolj na osnove. Sprva na tak učbenik nisem niti pomislil. Dolgo sem predaval fiziko študentom fizike v prvih dveh letih in zanje postopno napisal učbenik v štirih delih. Mislil sem, da je predavatelj na „matični fakulteti“ to dolžan storiti. Za pisanje srednješolskih besedil sem se dal nagovoriti pozneje, češ da bi to „koristilo fiziki“. Tako sem napisal tretji del učbenika za fiziko za prvi letnik srednjih šol v okviru Skupne vzgojno izobrazbene osnove (SVIO) in ustrezno *Fiziko za družboslovno usmeritev*. Potem dolgo časa nisem prebolel tega, da so ta učbenika opustili.

Odtlej sem odklanjal vabila, naj sodelujem pri pisanju srednješolskega učbenika. Nato me je srednješolski učitelj fizike prepričal, da je potreben nov učbenik, češ da obstoječi niso pripravljeni za uporabo v razredu. Z njim in njegovim kolegom smo začeli pisati učbenik, a je načrt zgodaj padel v vodo. Po tem sem sklepal, da je dovolj srednješolskih učbenikov za fiziko na našem majhnem tržišču, ki je medtem postalo prosto. Čez nekaj časa pa me je urednik začel prepričevati, naj bi se vendarle lotil pisanja učbenika, ki ga namerava izdati njegova založba. Precej časa sem ponavljal, da je načrt za založbo tvegan, češ da je tovrstnih učbenikov najbrž dovolj, a nazadnje

sem popustil. Morda je k temu prispevalo spoznanje, da so se možnosti za objavljane v domačih revijah zmanjšale. Odlašal sem s pisanjem in upal, da bo založba načrt opustila. Nazadnje sem uvidel, da misli resno. Dopovedal sem si, da pisec ni dolžan presojudati, ali je novi učbenik potreben ali ne. O tem mora presoditi založba, pisec lahko samo sprejme ponudbo ali jo odkloni. Lotil sem se dela in rokopis prvega dela oddal sredi leta 2002 in rokopis drugega dela dobro leto pozneje.

Mimogrede naj omenim zanimivi ugotovitvi, ki zadevata tehnični del posla. Prva se dotika računalniškega stavljaja besedila. Dandanes pišemo in urejamo besedilo z računalnikom in poleg izpisa oddamo tudi disketo. Na Fakulteti za matematiko in fiziko nas veliko dela z urejevalnikom  $\text{T}_{\text{E}}\text{X}$ . Toda med pripravo na tiskanje opravljeno delo razvrednotijo in besedilo na novo obdelajo, tako da se v njem pojavijo nove napake. Napake so trdovratna zadeva in se jih je mogoče znebiti postopno z večkratnim branjem. Možnost, da se pojavijo v besedilu in na slikah napake, ki jih prej ni bilo, na pisca ne deluje spodbudno. Marsikdo bo svetoval, naj se pisec z založbo vnaprej dogovori o vseh podrobnostih. V resnici pa pisec nima nobene izbire. Najprej ima pred očmi predvsem strokovna vprašanja, potem pa ima kljub nenavadnim potezam založbe malo upanja, da bi dosegel svoje. Od sporov ga odvrača še spoznanje, da naj bi založba navsezadnje želela enako kot on, da učbenik izide in rabi svojemu namenu.

Druga ugotovitev zadeva večbarvni tisk. Zaradi pocenitve tiska so učbeniki postali večbarvni. Ugotovitev ne leti na lepe barvne fotografije, ki naj pritegnejo pozornost dijakov, čeprav so s snovjo učbenika le rahlo povezane in jih z znanjem iz učbenika navadno ni mogoče razumeti. Risbe so v učbeniku pomembnejše, ker pojasnjujejo besedilo. Dijaki v zvezek navadno rišejo enobarvno, tudi učitelj pri risanju po tabli navadno ne uporablja barv, lahko pa barvne risbe projicira z grafoskopom. Tako je treba posebej razmisliti, kako izkoristiti „nove prostostne stopnje“, barve. Medtem ko so na nekaterih risbah barve koristne, lahko na drugih motijo. V nekaterih univerzitetnih učbenikih so barve poskusili uporabiti na nov način. Serway [1] je priredil določenim fizikalnim količinam določene barve, a kaj, ko je moral v „pedagoškem seznamu barv“ sprejeti tri različne dogovore za tri poglavja. Drugi učbeniki utegnejo uporabiti drugačne dogovore. Keller, Gettys in Skove [2] so uporabili barve tudi v „barvnem stroboskopu“, pri katerem različnim časom ustrezajo različne barve. Te načine bo treba še oceniti in razmisliti o uporabi barv.

Bralke in bralce Obzornika utegnejo bolj zanimati splošne ugotovitve, do katerih sem se dokopal. Kaže, da nisem popolnoma opustil upanja, da je mogoče razmere izboljšati. Založba se navadno ne vmešava v vsebino učbenika neposredno, pričakuje le, da se vsebina sklada z veljavnim učnim načrtom. V okviru tega ima pisec nekaj svobode. O njej priča to, da se učbenika dveh piscev za isti učni načrt med seboj vendarle nekoliko razlikujeta. Včasih se je – pri nas in drugod – primerilo, da je pisec učbenika imel možnost vplivati na učni načrt ali je celo sodeloval pri sestavljanju načrta. Zdaj ni tako. Vsekakor po mojem mnenju še ni bilo tako neugodnega

učnega načrta za fiziko v gimnazijah kot zdaj. Morda se tega poleg učiteljev še posebej zave pisec učbenika. Toda učitelji molčijo.

Delno je za slabost krivo zmanjšanje obsega ur za fiziko, čeprav se je fizika medtem še bolj razvila in razvejila in je zrasel njen pomen. Pogubne posledice je pokazal tudi premik: nekdanj se je v gimnaziji fizika začela v današnjem drugem letniku, medtem ko so zdaj premaknili njen začetek v prvi letnik. Vrh tega so uvedli maturo in fizika ni obvezen predmet na njej. Matura je postala taka, da odvrta pozornost od predmetov, ki na njej niso obvezni. Te težave so povzročili tisti, ki odločajo in med katerimi so najbrž tudi fiziki in matematiki.

Toda to je le del težav. Drugi del izvira iz matematike. Matematiki so v današnjem duhu „olajšali“ svoj predmet, morda tudi zato, da bi ostal obvezen na maturi. V učnem načrtu so dele snovi predstavili v višje letnike, na primer vektorje, kotne funkcije in infinitezimalni račun, nekaj snovi pa so tudi spustili. Tako učitelju fizike manjkajo pomembna matematična orodja. Brez njih je v kratkem času, ki je na voljo, zelo težavno dati dijakom uravnovešen in na njihovi stopnji zaključen vtis o fiziki. Ni mogoče trditi, da je to vrnitev k Aristotelu, a ne manjka dosti, da se znajdemo v Newtonovem času. Kotne funkcije, logaritem in infinitezimalni račun so tedaj že poznali, vektorji segajo v 19. stoletje. Pri fiziki pa naj bi obravnavali tudi odkritja iz 20. stoletja!

Med učitelji fizike so nasploh pogledi na vlogo matematike v poučevanju fizike različni. Nekateri menijo, da uporaba matematike fiziko in njeno poučevanje oteži, drugi so prepričani o nasprotnem [3]. Vendar lahko matematika olajša poučevanje fizike samo, če uporabimo pri fiziki le matematične pojme in zakone, ki so jih že obdelali pri matematiki. Zato je razumljiva težnja učiteljev fizike, da si sami pripravijo nekatere od matematičnih pojmov pri fiziki. K temu prispeva tudi težnja, da bi še naprej učili tako, kot so bili to vajeni delati dotlej. O hitrosti in sili je težko razpravljati brez vektorjev. Ali naj torej učitelj fizike in pisec učbenika fizike uvedeta vektorje? Številni učitelji fizike jih uporabljajo v prvem letniku, čeprav jih pri matematiki vpeljejo šele v drugem. Če jih učitelj ne uporabi, je vezan na gibanje telesa po premici in na delovanje telesa na telo na premici. Podobno vprašanje se pojavi pri kotnih funkcijah. Če učitelj ne uvede teh funkcij, je vezan na Pitagorov izrek ali pa se mora omejiti na polovice enakostraničnih trikotnikov in enakokrake pravokotne trikotnike. Pozneje pridejo na vrsto še eksponentna funkcija in naravni logaritem ter nazadnje še odvajanje in integriranje. To postavi pred pisca dodatno vprašanje. Ali naj napiše učbenik, ki ga učitelji in dijaki uporabljajo pri vsakdanjem delu? Ali naj raje napiše učbenik za tiste dijake, ki se bodo odločili za maturo iz fizike in ki že poznajo odvode in integrale. Ali bosta potrebni obe vrsti učbenikov? Preden sem se lotil pisanja, se teh težav nisem v celoti zavedal; fizika brez osnovnih matematičnih orodij je dokaj neogljenjena.

Ali naj potemtakem učitelj fizike žrtvuje del skromno odmerjenega časa, namenjenega fiziki, in pisec učbenika fizike del skopo odmerjenega prostora za razlago matematičnih pojmov in zakonov, ko je matematiki odmerjeno

veliko več časa in prostora? Ali s tem bogati ne postaja še bogatejši in revni še revnejši? Ali se učitelji matematike ne bodo pritožili, če bodo učitelji fizike prevzeli del njihovih nalog? Vrh tega utegnejo matematični pojmi, ki jih na hitro in za silo vpeljejo pri fiziki, pozneje dijakom povzročati težave.

Ali se zaradi vsega tega ni zmanjšala raven, do katere dijaki spoznajo fiziko? Sodeč po nekdanji *Fiziki za družboslovje* je odgovor pritrdilen. Današnji gimnazijci se morajo zadovoljiti z enako ravniyo kot nekdanji „usmerjeni“ dijaki, ki jih je zanimalo družboslovje ali so se v tej smeri namenili nadaljevati študij, čeprav je res, da „usmerjeni“ dijaki niso spoznali vseh delov fizike.

Podrobnejši pregled sedanjega učnega načrta za fiziko razkrije, da so njegovi sestavljanci mislili predvsem na to, kaj bi bilo mogoče spustiti, ne pa na to, kako bi bilo mogoče s tistim, kar so obdržali, dati z razpoložljivim matematičnim orodjem notranje usklajeno sliko fizike brez velikih vrzeli.

Kaže, da si zdaj posamezniki in skupine prizadevajo, da bi čim bolj olajšali srednjo šolo. Čeprav je večina tovrstnih teženj najbrž dobronamerna, utegnejo imeti nepričakovane in neželene dolgoročne učinke. Med drugim pri dijakih zbujaajo vtis, da je do znanja mogoče priti brez truda. To utegne zmanjšati njihovo pripravljenost, da bi v učenje vložili svoje delo.

Predvsem si je težko predstavljati, da bi na delo v šoli ugodno vplivali predlogi tistih, ki tega dela ne poznajo v podrobnosti. Predlogi – konkretni in premišljeni – ne bi smeli obiti učiteljev, ki to delo najbolje poznajo. Nadaljnje nepremišljeno razvrednotenje gimnazije v smeri, ki smo jo nakazali pri fiziki, utegne slovenske dijake postaviti v neenakopraven položaj.

## LITERATURA

- [1] R. A. Serway, *Physics for Scientists & Engineers*, Saunders, Philadelphia 1996.
- [2] F. J. Keller, W. E. Gettys, M. J. Skove, *Physics. Classical and Modern*, McGraw-Hill, New York 1993.
- [3] J. Strnad, *Poučevanje fizike in matematika*, Obzornik mat. fiz. **46** (1999) 83.

## NOVE KNJIGE

**Vesna Omladič, Matematika in odločanje, Knjižnica Sigma, DMFA – založništvo, Ljubljana 2002, 184 strani.**

Zbirka Sigma je bogatejša za knjižico z zgornjim naslovom. Delo pomeni pomemben prispevek k slovenski matematični literaturi, ne samo kot prvi učbenik za novo področje teorije odločanja, ampak tudi, ker širi matematično kulturo na družboslovna področja. Avtorica priporoča to delo kot del literature za predmet Operacijske raziskave, ki ga predava na Fakulteti za družbene vede v Ljubljani.

Knjižica obsega poleg kazala, predgovora, literature in stvarnega kazala 7 poglavij na 179 straneh. Tekst ilustrirajo številni primeri in 5 slik. Seznam literature obsega 11 tekstov, od tega 6 domačih. Stvarno kazalo, ki je zelo pregledno in popolno, obsega kar 5 strani.

Odlika knjižice je v tem, da je lahko razumljiva širšemu krogu bralcev, torej tistim, ki nimajo večje matematične izobrazbe. Za večino teksta zadostuje predznanje v obsegu gimnazijske matematike. Ker se s problemom odločanja srečujemo skoraj vsak dan, bi bilo koristno za vsakogar, da se seznani z nekaterimi ugotovitvami teorije odločanja in njenimi metodami.

Opišimo na kratko vsebino knjižice. V uvodnem poglavju Problemi odločanja nas avtorica najprej seznani z osnovnim pojmom matematičnega modela in matematičnega načina premišljevanja. Nato opiše normativno in opisno teorijo odločanja. Drugo poglavje Vrednostne funkcije je posvečeno preferenčnim relacijam, ordinalnim vrednostnim funkcijam in merjenju razlik. Tretje poglavje Odločanje v popolni negotovosti vpelje koristen pojem tabele odločanja in se posveti različnim kriterijem odločanja in njihovim lastnostim. V četrtem poglavju Teorija uporabnosti se avtorica ukvarja s problemi odločanja v pogojih tveganja. Vpelje pojem preference na loterijah in opiše, kako si lahko pomagamo s teorijo uporabnosti. Razloži tudi, kako na odločanje vpliva različen odnos do tveganja. Peto poglavje Odločanje po več kriterijih je že nekoliko bolj zahtevno in opisuje, kako naj se odločamo, če zasledujemo več ciljev. Problem je nekoliko enostavnejši, če je vrednostna funkcija linearna. Šesto poglavje Skupinsko odločanje in družbena izbira je še posebej zanimivo, saj se dotika zelo pogostih življenjskih situacij, npr. podelitev priznanj ali raznih volitev. V zadnjem poglavju Teorija iger je na kratko opisano to zelo pomembno matematično področje, ki je povezano s teorijo odločanja, ko si interesi odločevalcev nasprotujejo. Obravnavane so t. i. strateške in antagonistične igre ter igre s pogajanji.

*Zvonimir Bohte*

## VESTI

### Novi člani društva v letu 2002

Lani se je v Društvo matematikov, fizikov in astronomov Slovenije včlanilo 37 novih članov:

|                             |                       |                       |
|-----------------------------|-----------------------|-----------------------|
| 2061. Antolin Tibaut Helena | 2062. Bajc Borut      | 2063. Božič Mateja    |
| 2064. Breznik Kristijan     | 2065. Breznik Maja    | 2066. Budin Mateja    |
| 2067. Čufar Zdravko         | 2068. Dokler Joahim   | 2069. Harej Suzana    |
| 2070. Hribernik Francka     | 2071. Hromc Felicita  | 2072. Ivanuša Blaž    |
| 2073. Kauran Zora           | 2074. Konečnik Lidija | 2075. Kovač Barbara   |
| 2076. Kromek Mihail         | 2077. Kuzman Boštjan  | 2078. Likar Mateja    |
| 2079. Marušič Dragan        | 2080. Marušič Nadja   | 2081. Mlakar Matej    |
| 2082. Pavlič Polonca        | 2083. Pem Danica      | 2084. Petrica Polonca |
| 2085. Pivk Tatjana          | 2086. Poličar Jana    | 2087. Rojht Mihela    |
| 2088. Šalamon Tanja         | 2089. Šamu Simona     | 2090. Šilak Marta     |
| 2091. Šmid Andreja          | 2092. Špilak Goran    | 2093. Špolad Marko    |
| 2094. Štandeker Lidija      | 2095. Vidmar Tim      | 2096. Zupan Dejan     |
| 2097. Žigert Petra          |                       |                       |

*Vladimir Bensa*

\* Novi člani za leto 2001 so bili objavljeni v Obzorniku za matematiko in fiziko 49 (2002), XI.

**OBZORNIK ZA MATEMATIKO**  
**LJUBLJANA, SEPTEMBER**  
 Letnik 50, številka 5

ISSN 0473-7466, UDK 51 + 5

R 177/03



100001170,5

COBISS

VSEBINA

ODPISANO

**Članki**

**Strani**

|                                                                                                          |         |
|----------------------------------------------------------------------------------------------------------|---------|
| Odločitveni problem Praštevilo, Tadej Novak . . . . .                                                    | 129–143 |
| Ravninske mreže in verižni ulomki. Prispevek k razumevanju filotakse, 3.<br>del, Milan Hladnik . . . . . | 144–153 |
| Kako sem pisal učbenik za fiziko, Janez Strnad . . . . .                                                 | 157–160 |

**Nove knjige**

|                                                   |         |
|---------------------------------------------------|---------|
| Matematika in odločanje, Zvonimir Bohte . . . . . | 160–III |
|---------------------------------------------------|---------|

**Vesti**

|                                                                                              |         |
|----------------------------------------------------------------------------------------------|---------|
| Profesorju Niku Prijatelju v slovo, Edvard Kramar, Tomaž Pisanski in Jože<br>Vrabc . . . . . | 153–155 |
| April 2003 – mesec matematičnega ozaveščanja, Matjaž Konvalinka . . . .                      | 155–156 |
| Novi člani društva v letu 2002, Vladimir Bensa . . . . .                                     | III     |

**CONTENTS**

**Articles**

**Pages**

|                                                                                                                             |         |
|-----------------------------------------------------------------------------------------------------------------------------|---------|
| Decision problem Primes, Tadej Novak . . . . .                                                                              | 129–143 |
| Plannar Lattices And Continued Fractions. A contribution to understand-<br>ing phyllotaxis, part 3, Milan Hladnik . . . . . | 144–153 |
| How I wrote a physics textbook, Janez Strnad . . . . .                                                                      | 157–160 |

|                            |         |
|----------------------------|---------|
| <b>New books</b> . . . . . | 160–III |
|----------------------------|---------|

|                       |         |
|-----------------------|---------|
| <b>News</b> . . . . . | 153–III |
|-----------------------|---------|

Na naslovnici, ki jo je izdelal Douglas Dunham, je emblem letošnjega Meseca matematičnega ozaveščanja (glej prispevek na strani 155).