# Eksplicitno generiranje skoro svih prostih brojeva

*Petar Svirčević*[1]

U ovome radu je definirana funkcija, kao kompozicija idempotentnih funkcija

$$|\,|:\mathbb{R}\to\{0\}\cup\mathbb{R}^+;\quad \lfloor\,\rfloor:\mathbb{R}\to\mathbb{Z};\quad \lceil\,\rceil:\mathbb{R}\to\mathbb{Z};\quad \operatorname{sgn}:\mathbb{R}\to\{-1,0,1\},$$

čija je domena unija disjunktnih klasa iz skupa prirodnih brojeva, a ona generira makar sve proste brojeve, dakle između prostih brojeva će se pojavljivati i brojevi koji nisu prosti. Recimo i to, da je definiran funkcijski faktor koji reducira dobivanje iracionalnih brojeva i broja 0. Nadalje, eliminirane su klase prirodnih brojeva, koje sigurno ne generiraju proste brojeve. Iz svega toga slijedi da se povećava vjerojatnost dobivanja prostih brojeva iz unije preostalih klasa kao domene. Tom funkcijom ćemo sigurno dobiti sve proste brojeve iz kodomene $\mathbb{P}\setminus\{2,3\}$ i neke prirodne brojeve.

Iz definicije prostog broja lako se matodom kontradikcije dokazuje, da ih je beskonačno ali prebrojivo mnogo, dakle njih ima isto kao i prirodnih brojeva, a to znači da im je kardinalni broj $k\mathbb{P}=k\mathbb{N}=\aleph$. No, više od dva milenija matematičari teže da nađu "recept" kako generirati sve proste brojeve po redu, dakle bez drugih prirodnih brojeva. To htijenje, što je prije čovjeku bila filozofska znatiženja, je danas potreba u programerskoj praksi, a ono još nije ostvareno ni do danas. Zapravo, matematičari bi bili zadovoljni, da znaju generirati sve proste brojeve eksplicite po redu, pa da makar između njih "ulijeću" i složeni prirodni brojevi.

Napomenimo i mišljenje velikog švicarskog matematičara L. Eulera vezano uz proste brojeve, koje glasi: *Matematičari su uzalud do danas pokušavali otkriti pravilnost u slijedu prostih brojeva, a mi imamo razloga vjerovati da je to misterija u koju ljudski um nikada neće prodrijeti.* I sam veliki Euler dao je puno radova koji su vezani za proste brojeve. No, misterij vezan za eksplicitno generiranje prostih brojeva ni do danas nije riješen, premda su publicirani nebrojeni radovi vezani za to područje matematike, pa tako ispada da Eulerovo proročanstvo ima smisla, iako je izrečeno prije više od 250 godina.

Najprije ćemo dati pet važnih napomena, koje su vezane za proste brojeve.

**Napomena 1.** Francuski pravnik *Pierre de Fermat* (1601.–1665.) je dobro poznat po svojim radovima i iz matematike, iako po struci nije bio matematičar. On je dao veliki doprinos analitičkoj geometriji i vjerojatnosti, a bio je i jedan od začetnika diferencijalnog računa. Vjerojatno ne postoji matematičar, koji nije čuo za *Veliki Fermatom teorem*, ili *Posljednji Fermatov teorem,* kojega su najveći matematički umovi skoro 350 godina pokušavali riješiti, ali to je ostalo bez uspjeha. Doduše riješeni su neki specijalni slučajevi. Taj teorem je konačno 1995. u potpunosti riješio *J. Wiles*. Dobro je poznato, da taj problem glasi: "$x^n+y^n\neq z^n$; gdje je $n,x,y,z\in\mathbb{N}$ i $n>2$."

Recimo još i to, da je jedan od osnovnih teorema u teoriji brojeva *Mali Fermatov teorem*, koji glasi: "Ako je $p$ prost broj ($p\in\mathbb{P}$) i $a\in\mathbb{N}$, takav da $p\nmid a$, tada je $a^{p-1}\equiv 1\pmod p$".

[1] Autor je professor u mirovini na Tehničkoj školi u Zagrebu; e-pošta: petar.svircevic@zg.t-com.hr

**Napomena 2.** Svakako, da je i sam Fermat pokušao dati algoritam barem za neku klasu prostih brojeva, pa je tako heuristički tvrdio, da su brojevi oblika

$$F_n = 2^{2^n} + 1, \quad \text{za} \quad n \in \mathbb{N}_0 = \{0, 1, 2, 3, \ldots\} \tag{1}$$

prosti. Stvarno i dobivamo proste brojeve: $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65\,537$. No, Fermatovu hipotezu već je za $n = 5$ negirao *L. Euler*, jer je 1732. godine dobio rastav $F_5 = 2^{2^5}+1 = 2^{32}+1 = 4\,294\,967\,297 = 641{\cdot}6\,700\,417$, a to je zadivljujuće, jer u to vrijeme nisu postojala računalska pomagala velikih mogućnosti. Recimo i to, da se brojevi (1) zovu *Fermatovi brojevi*. Zanimljivo je npr., da je broj $F_{1945}$ složen i da ima oko $10^{585}$ znamenaka. Koliko je to velik broj vidi se po tome, ako se usporedi s brojem $10^{73}$, koji predstavlja broj svih atoma u *svemiru*, a ta hipoteza slijedi iz opće teorije relativnosti.

**Napomena 3.** Važno je reći, da je *K. F. Gauss* (1777.–1855.) dokazao, kako su samo *pravilni ravninski poligoni* s vrhovima u točkama $A_1A_2\ldots A_k$, gdje je $k = F_n = 2^{2^n} + 1$ $(n \in \mathbb{N})$ prost broj, konstruktibilni s ravnalom i šestarom, dakle moguće ih je konstruirati u smislu konstruktivne geometrije, a to znači da se mogu konstruirati pravilni poligoni; $A_1A_2A_3, A_1A_2\ldots A_{17}$, $A_1A_2\ldots A_{257}$, $A_1A_2\ldots A_{66\,537}, \ldots$; jer su 3, 17, 257, 66573,... prosti brojevi; ali se ne mogu navedenim instrumentima konstruirati pravilni poligoni: $A_1A_2\ldots A_7$, $A_1A_2\ldots A_{11}$, $A_1A_2\ldots A_{13}, \ldots$

**Napomena 4.** Budući da znamo konstruirati polovinu kuta, slijedi da možemo konstruirati i pravilne poligone $A_1A_2\ldots A_l$ u smislu konstruktivne geometrije, ako je $l = k2^m$ za $k = F_n$ i $m = 1, 2, 3, \ldots$.

Dodajmo i to, da je Gauss u devetnaestoj godini dokazao, da je pravilni sedamnaesterokut $A_1A_2\ldots A_{17}$ moguće konstruirati, jer je pokazao da je

$$\cos\frac{2\pi}{17} = \frac{1}{16}\left(\sqrt{17} - 1 + \sqrt{34 - 2\sqrt{17}} + 2\sqrt{17 + 3\sqrt{17} - \sqrt{170 + 38\sqrt{17}}}\right). \tag{2}$$

Naime, iz (2) vidimo da je $\cos 2\pi/17$ izražen u kvadratnim radikalima, pa onda slijedi, da se i pravilni sedamnaesterokut može konstruirati. Tim svojim uspjehom je bio toliko oduševljen, da mu je po njegovoj želji na nadgrobnoj ploči ugraviran pravilni sedamnaesterokut.

**Napomena 5.** Nadalje, može se dokazati, da se svaki prosti broj veći od 3 može prikazati u jednom od oblika

$$p = 6k \pm 1; \quad k \in \mathbb{N}. \tag{3}$$

Naime, iz (3) dobivamo proste brojeve; $5 = 6\cdot 1 - 1$, $7 = 6\cdot 1 + 1$, $11 = 6\cdot 2 - 1$, $13 = 6\cdot 2 + 1$, $23 = 6\cdot 4 - 1$, ali npr. $25 = 6\cdot 4 + 1$ je složen. Već na osnovu ovoga zaključujemo, da obrat od (3) ne vrijedi, dakle prema tome pomoću te relacije ne možemo generirati proste brojeve bez provjere njihove složenosti, pa to za praksu nije pogodno. Dokažimo, da svaki prosti broj veći od 3 ima oblik $6n - 1$ ili $6n + 1$, gdje je $n \in \mathbb{N}$. Jasno je, da svaki prirodni broj veći od 5 u dijeljenju sa 6 daje točno jedan ostatak koji je iz skupa $\{0, 1, 2, 3, 4, 5\}$, a to znači da su brojevi iz skupa $\{6k, 6k+2, 6k+3, 6k+4\}$ složeni, odakle zaključujemo, da su prosti brojevi oblika $6k + 1$ ili $6k + 5$. Recimo još, da je $6k + 5 = 6(k + 1) - 1 = 6n - 1$, pa smo time dobili oba tražena oblika. Svakako, da među tim brojevima ima složenih, kako ćemo sada pokazati. Možemo definirati i ove

dvije funkcije

$$f_i : \mathbb{N} \to \mathbb{P}_i \cup \mathbb{N}_i, \quad \text{za } i \in \{1,2\}; \quad \text{gdje je } f_i(n) = 6n + (-1)^i. \tag{3.1}$$

Iz (3.1) slijedi da je $f_1(n) = 6n - 1$, pa dobivamo

$$\mathbb{P}_1 \cup \mathbb{N}_1 = \{5, 11, 17, 23, 29, \underline{35}, 41, 47, 53, 59, \underline{65}, 71, \underline{77}, 83, 89, \ldots\}, \tag{3.2}$$

a za $f_2(n) = 6n + 1$ slijedi

$$\mathbb{P}_2 \cup \mathbb{N}_2 = \{7, 13, 19, \underline{25}, 31, 37, 43, \underline{49}, \underline{55}, 61, 67, 73, 79, \underline{85}, \underline{91}, \ldots\}, \tag{3.3}$$

pa je jasno da je $\mathbb{N}_1 \cap \mathbb{N}_2 = \emptyset$. Na osnovi (3), (3.2) i (3.3) zaključujemo,

$$\mathbb{P}_1 = \{5, 11, 17, 23, 29, 41, 47, 53, 59, 71, 83, 89, \ldots\}, \tag{3.4}$$

$$\mathbb{P}_2 = \{7, 13, 19, 31, 37, 43, 61, 67, 73, 79, \ldots\}, \tag{3.5}$$

dakle smo dobili dvije klase disjunktnih prostih brojeva, a to znači da je skup svih prostih brojeva dan s relacijom

$$\mathbb{P} = \mathbb{P}_1 \cup \mathbb{P}_2 \cup \{2, 3\}. \tag{3.6}$$

Na osnovi dobivenih rezultata zaključujemo, da smo pomoću (3.1) testiranjem 30 vrijednosti, po 15 vrijednosti za svaku funkciju, od toga dobili ukupno 22 prosta broja. Svakako, da pomoću navedenih funkcija nismo mogli dobiti proste brojeve 2 i 3, a to je naglašeno i u (3.6).

Unatoč iznesenom mišljenju, da ne postoji način za eksplicitno nalaženje svih prostih brojeva po redu, ali mi ćemo ipak sada definirati jednu funkciju, koja će generirati makar sve proste brojeve osim 2 i 3, a to znači da će između prostih brojeva "ulijetati" i složeni brojevi. Ideja vodilja za definiranje navedene funkcije je kongruencija

$$p^2 - 1 \equiv 0 \pmod{24}; \quad \text{za } p \in \mathbb{P} \setminus \{2,3\} = \{5, 7, 11, 13, \ldots\}, \tag{4}$$

gdje je $\mathbb{P}$ skup svih prostih brojeva. Da bi dokazali (4) moramo uvažiti tvrdnju, da je produkt od tri uzastopna prirodna broja dijeljiv s $3! = 1 \cdot 2 \cdot 3 = 6$. Naime, iz rastava $p^2 - 1 = (p-1)(p+1)$ slijedi kongruencija $p^2 - 1 = (p-1)(p+1) \equiv 0 \pmod 4$ jer su faktori $p-1$ i $p-1$ parni. Nadalje $(p-1)p(p+1) \equiv 0 \pmod{3!}$, budući je $p$ prost, slijedi da je (4) točna kongruencija. Ako izvršimo u (4) neke specijalizacije, imamo npr.: $5^2 - 1 = 24 \equiv 0 \pmod{24}$, $7^2 - 1 = 48 \equiv 0 \pmod{24}$, $11^2 - 1 = 120 \equiv 0 \pmod{24}$, $13^2 - 1 = 168 \equiv 0 \pmod{24}, \ldots$; ali je npr. $6^2 - 1 = 35 \equiv 0 \pmod{24}$, $8^2 - 1 = 63 \equiv 0 \pmod{24}, \ldots$

Iz (4) slijedi, da postoji funkcija

$$f_3 : \mathbb{N} \to (\mathbb{P} \setminus \{2,3\}) \cup Y, \tag{5}$$

$$f_3(x) = \sqrt{24x + 1}; \tag{6}$$

koja generira makar sve proste brojeve osim 2 i 3; jer je npr.

$\boxed{f_3(1) = 5}$, $\boxed{f_3(2) = 7}$, $f_3(3) = \sqrt{73}$, $f_3(4) = \sqrt{97}$, $\boxed{f_3(5) = 11}$,

$f_3(6) = \sqrt{145}$, $\boxed{f_3(7) = 13}$, $f_3(8) = \sqrt{193}$, $f_3(9) = \sqrt{217}$, $f_3(10) = \sqrt{241}$,

$f_3(11) = \sqrt{265}$, $\boxed{f_3(12) = 17}$, $f_3(13) = \sqrt{313}$, $f_3(14) = \sqrt{337}$, $\boxed{f_3(15) = 19}$,

$f_3(16) = \sqrt{385}$, $f_3(17) = \sqrt{409}$, $f_3(18) = \sqrt{433}$, $f_3(19) = \sqrt{457}$, $f_3(20) = \sqrt{481}$,

$f_3(21) = \sqrt{505}$, $\boxed{f_3(22) = 23}$, $f_3(23) = \sqrt{553}$, $f_3(24) = \sqrt{577}$, $f_3(25) = \sqrt{601}$,

$f_3(26) = 25 = 5 \cdot 5$ (broj nije prost), $f_3(27) = \sqrt{649}$, $f_3(28) = \sqrt{673}$,

$f_3(29) = \sqrt{697}$, $f_3(30) = \sqrt{721}$, $f_3(31) = \sqrt{745}$, $f_3(32) = \sqrt{769}$,

$$f_3(33)=\sqrt{793},\quad f_3(34)=\sqrt{817},\quad \boxed{f_3(35)=29},\ldots$$

Nakon ovoga testiranja funkcije (5) za $x\in\{1,2,\ldots,35\}$ dobili smo, kako smo i očekivali, proste brojeve iz skupa $\{5,7,11,13,17,19,23,29,\ldots\}$ i složeni broj 25, dok su svi ostali brojevi iracionalni, koji su nam suvišni i pokazat ćemo način kako ih eliminirati iz kodomene.

Dakle zbog preglednosti generiranja prostih brojeva potrebno je eliminirati iracionalne vrijednosti brojeva, a to ćemo najlakše postići da koristimo idenpotentne funkcije: $\lfloor\ \rfloor$ (*Floor Brackets* (*Half Brackets*)), $\lceil\ \rceil$ (*Ceilling Brackets* (*Quine Corners*)) i $|\ |$ (*Vertical Bars*).

Budući da je $\left\lceil\sqrt{24x+1}\right\rceil-\left\lfloor\sqrt{24x+1}\right\rfloor=1$, ako $\sqrt{24x+1}\notin\mathbb{N}$, dobivamo $\frac{1}{2}\left(1+(-1)^{\left\lceil\sqrt{24x+1}\right\rceil-\left\lfloor\sqrt{24x+1}\right\rfloor}\right)=0$. Nadalje, ako je $\sqrt{24x+1}\in\mathbb{N}$, tada je $\frac{1}{2}\left(1+(-1)^{\left\lceil\sqrt{24x+1}\ \right\rceil-\left\lfloor\sqrt{24x+1}\right\rfloor}\right)=1$. Na osnovi ovih rezultata definiramo funkciju

$$\kappa:\mathbb{N}\to\{0,1\},\tag{7}$$

gdje je

$$\kappa(x)=\frac{1}{2}\left(1+(-1)^{\left\lceil\sqrt{24x+1}\ \right\rceil-\left\lfloor\sqrt{24x+1}\right\rfloor}\right),\tag{8}$$

koju ćemo zvati *funkcijski koeficijent*, koji će eliminirati iracionalne brojeve iz kodomene. Dakle, ako uvažimo (8), tada definiramo funkciju

$$g:A\to(\mathbb{P}\setminus\{2,3\})\cup B\cup\{0\};\quad A,B\subset\mathbb{N},\tag{9}$$

gdje je

$$g(x)=\frac{1}{2}\left(1+(-1)^{\left\lceil\sqrt{24x+1}\right\rceil-\left\lfloor\sqrt{24x+1}\right\rfloor}\right)\sqrt{24x+1},\tag{10}$$

koja će generirati makar sve proste brojeve veće od 3, ali zato ona ne generira iracionalne brojeve. Kada kažemo da generira makar sve proste brojeve veće od 3, to znači da dobivamo i neke složene brojeve. Tako npr. ovaj oblik generira složeni broj 25, jer za $x=26$ dobivamo da je

$$g(26)=\frac{1}{2}\left(1+(-1)^{\left\lceil\sqrt{24\cdot26+1}\right\rceil-\left\lfloor\sqrt{24\cdot26+1}\right\rfloor}\right)\sqrt{24\cdot26+1}=\ldots=25.$$

Ako promotrimo sada slijedeće implikacije:

$$24\,(10n+0)+1=240n+1\implies\text{znamenka jedinica je }1,\tag{a}$$
$$24\,(10n+1)+1=240n+25\implies\text{znamenka jedinica je }5,\tag{b}$$
$$24\,(10n+2)+1=240n+49\implies\text{znamenka jedinica je }9,\tag{c}$$
$$24\,(10n+3)+1=240n+73\implies\text{znamenka jedinica je }\boxed{3},\tag{d}$$
$$24\,(10n+4)+1=240n+97\implies\text{znamenka jedinica je }\boxed{7},\tag{e}$$
$$24\,(10n+5)+1=240n+121\implies\text{znamenka jedinica je }1,\tag{f}$$
$$24\,(10n+6)+1=240n+145\implies\text{znamenka jedinica je }5,\tag{g}$$
$$24\,(10n+7)+1=240n+169\implies\text{znamenka jedinica je }9,\tag{h}$$
$$24\,(10n+8)+1=240n+193\implies\text{znamenka jedinica je }\boxed{3},\tag{i}$$
$$24\,(10n+9)+1=240n+217\implies\text{znamenka jedinica je }\boxed{7},\tag{j}$$

i ako definirajmo disjunktne klase prirodnih brojeva iz skupa $\mathbb{N}$, koje neka su

$$a\mathbb{N}+b=\{a1+b,a2+b,a3+b,\ldots\},\quad\text{gdje je }\ \mathbb{N}=\{1,2,3,\ldots\}$$

i uvažimo da je $\mathbb{N}_0 \equiv \{0\} \cup \mathbb{N}$, tada dobivamo uniju restringiranih klasa pirodnih brojeva, koja će predstavljati domenu funkcije (7). Dakle

$$A \equiv (10\mathbb{N}_0+0) \cup (10\mathbb{N}_0+1) \cup (10\mathbb{N}_0+2) \cup (10\mathbb{N}_0+5) \cup (10\mathbb{N}_0+6) \cup (10\mathbb{N}_0+7). \quad (11)$$

Jasno je, kako smo došli do (11), jer kvadrati prirodnih brojeva imaju znamenku jedinica iz skupa $\{0,1,4,5,6,9\}$, a u našem slučaju te su znamenke iz skupa $\{1,4,5,6,9\}$, jer oblik $24n+1$ za $n \in \mathbb{N}$ ne može generirati 0. Na osnovi iznesene konstatacije slijedi, da se elementi domene nalaze u uniji klasa prirodnih brojeva oblika kako je navedeno u (11).

**Napomena 6.** Napravimo neke provjere:

$$g(1) = 5, \quad g(2) = 7,$$

$$g(3) = \frac{1}{2}\left(1 + (-1)^{\lceil\sqrt{73}\rceil - \lfloor\sqrt{73}\rfloor}\right)\sqrt{73} = \frac{1}{2}(1 + (-1)^{9-8})\sqrt{73} = 0,$$

a to smo i očekivali budući $x = 3$ nije ni iz jedne klase dane domene, jer je to nužan uvjet da vrijednost funkcije bude 0. Dalje dobivamo: $g(5) = 11$, $g(7) = 13$, $g(12) = 17$, $g(15) = 19$, $g(22) = 23$, $g(26) = 25$, $g(35) = 29, \ldots, g(875\,162) = 4583, \ldots$, $g(1\,493\,507) = 5987, \ldots$ Napomenimo, da su brojevi 4583, 5987 prosti. Prema tome vidimo da funkcija (10) generira proste brojeve veće od 3, zatim 0 i neke složene brojeve. *Pomoću te funkcije možemo jednostavno i brzo generirati proizvoljno velike brojeve, koji su vjerojatno prosti.*

**Napomena 7.** Iz ovih razmatranja slijedi da (10) eksplicite generira makar sve proste brojeve osim prostih brojeva 2 i 3, pa prema tome naslov nije u potpunosti istinit. Da bi uključili i ove brojeve i opravdali naslov, definiramo ovu funkciju

$$F : \mathbb{N} \to \mathbb{P} \cup B \cup \{0\}; \quad B \subset \mathbb{N}, \quad (11)$$

$$F(x) = (x+1)[1 - \operatorname{sgn}(x^2 - 3x + 2)] + \frac{1}{2}\operatorname{sgn}(x^2 - 3x + 2)\left(1 + (-1)^{\lceil\sqrt{24x-47}\rceil - \lfloor\sqrt{24x-47}\rfloor}\right)\sqrt{24x-47}. \quad (12)$$

jer je $x^2 - 3x + 2 = (x-1)(x-2)$, a to znači da je

$$\sqrt{24(x-2)+1} = \sqrt{24x-47}.$$

Dakle (12) generira baš sve proste brojeve, 0 i neke složene, ali se ne pojavljuju iracionalni brojevi.

Provjerimo (12): $F(1) = 2$, $F(2) = 3$, $F(3) = 5$, $F(4) = 7, \ldots$; tada bi imali barem sve proste brojeve, a pojavljivali bi se i neki prirodni brojevi, jer su iracionalni brojevi u potpunosti eliminirani već samom definicijom funkcije.

## Literatura


[1] Andrej Duella, *Teorija brojeva*, Školska knjiga, Zagreb 2019.

[2] I. Matić, *Uvod u teoriju brojeva*, Skripta, Odjel za matematiku, Sveučilište J. J. Strossmayera u Osijeku, Osijek, 2011.

[3] Boris Pavković, Darko Veljan, *Elementarna matematika I*, Tehnička knjiga, Zagreb, 1992.

[4] https://bs.wikipedia.org/wiki/Spisak_1000_prostih_brojeva

[5] http://modular.math.washington.edu/edu/2010/414/projects/tsang.pdf

[6] http://hr.wikipedia.org/wiki/Pierre_de_Fermat

[7] http://en.wikipedia.org/wiki/Carl_Friedrich_Gauss