ACTA MATHEMATICA SPALATENSIA
Series didactica
Vol.3 (2020) 63–76

Raznovrsni prosti brojevi

Zrinka Franušić, Nikola Pavlinić

Sažetak

Prost broj je vrlo jednostavan matematički pojam koji se pojavljuje u različitim oblicima. Prostim brojevima fascinirani su matematičari, ali i amateri, od davnina. Na prvi pogled izgleda kao da su u skupu prirodnih brojeva raspoređeni sasvim nasumično, no pomnijim promatranjem mogu se ustanoviti mnoge zakonitosti (o kojima smo pisali detaljnije u [3]) kao i slutnje čije su potvrde ili opovrgavanja još daleko izvan dosega naših matematičko-logičkih spoznaja. Ono što znamo jest da ne postoji čarobno pravilo ili čudotvorna formula koja *proizvodi* proste brojeve, no ipak proste brojeve *volimo* tražiti u nekim specijalnim oblicima, bilo da se radi o egzaktnoj formuli, svojstvu ili *vanjskom* izgledu koje moraju zadovoljiti. U ovom radu ćemo predstaviti samo neke oblike prostih te ukazati na njihovu *raznovrsnost*. Istraživanje različitosti prostih brojeva ponekad nalikuje dobroj umnoj gimnastici, no s vremenom to prerasta i snažno potiče razvoj teorije brojeva i teorije algoritama te nalazi učinkovitu primjenu u kriptografiji. Ne čudi stoga što su se proučavanjem različitih oblika prostih brojeva bavili, a i danas se time bave, mnogi amateri koji su doprinijeli razvoju znanosti.

Ključni pojmovi: oblici prostih brojeva, testiranje prostosti

1 Faktorijelni i primorijalni prosti brojevi

Prostih brojeva ima beskonačno mnogo. Dokaz te važne tvrdnje bio je poznat već starim Grcima, a nalazimo ga u 9. knjizi Euklidovih *Elemenata* iz 3. st. pr. Kr. Temelji se na ideji da pretpostavka o konačnosti skupa prostih brojeva povlači egzistenciju *novog* prostog broja. Dakle,

ako bi $\{p_1, \ldots, p_k\}$ bio skup svih prostih brojeva, onda broj $p_1 \cdots p_k + 1$ ima prosti djelitelj q koji je očito različit od p_i za sve $i = 1, \ldots, k$. Stoga zaključujemo da je pretpostavka o postojanju konačno mnogo prostih brojeva kriva. Ovu ideju možemo iskoristi upravo u konstrukciji *novih* prostih brojeva. Tako se prost broj oblika $p_n\sharp \pm 1$, gdje je $p_n\sharp = p_1 \cdots p_n$ umnožak prvih n prostih brojeva, zove *primorijalan prost broj*. Prvih nekoliko primorijalnih prostih brojeva su $5, 29, 2309, 30629$ (oblika $p_n\sharp - 1$ za $n = 2, 3, 5, 6$) te $3, 7, 31, 211$ (oblika $p_n\sharp + 1$ za $n = 1, 2, 3, 4$). Najveći do sada poznati primorijalni prost broj je $p_n\sharp - 1$ za $n = 1\,098\,133$ pronađen 2012. godine i ima 476 311 znamenki.

Uz malu modifikaciju, prosti brojevi se traže i u obliku $n! \pm 1$. Njih nazivamo *faktorijelnim prostim brojevima*. Prvih nekoliko faktorijelnih prostih brojeva su $7, 23, 719, 5039$ (oblika $n! - 1$ za $n = 3, 4, 6, 7$) te $2, 3, 7, 39916801$ (oblika $n! + 1$ za $n = 1, 2, 3, 11$). Najveći do sada pronađeni faktorijelni prost broj je iz 2016. godine. Oblika je $n! - 1$ i ima 1 015 843 znamenke.

2 Mersenneovi prosti brojevi

Marin Mersenne (1588. – 1648.) bio je francuski svećenik, teolog, filozof i matematičar. Kao matematičar bavio se različitim granama matematike te se aktivno dopisivao s mnogim istaknutim znanstvenicima toga vremena kao što su René Descartes[1], Étienne Pascal[2] i Pierre de Fermat[3]. Do danas je najviše ostao upamćen po prirodnim brojevima oblika

$$M_n = 2^n - 1, \ n \in \mathbb{N}, \tag{1}$$

koji su, njemu u čast, prozvani *Mersenneovim brojevima*. Prosti brojevi oblika (1) nazivaju se *Mersenneovi prosti brojevi*. Jednostavno je pokazati sljedeću tvrdnju.

Propozicija 1. *Ako je Mersenneov broj M_n prost, onda je n prost broj.*

Dokaz. Pretpostavimo da je n složen broj, odnosno $n = mk$, za neke $m, k \in \mathbb{N}$, $m, k > 1$. Tada je

$$M_n = (2^m)^k - 1 = (2^m - 1)\left((2^m)^{k-1} + (2^m)^{k-2} + \cdots + 2^m + 1\right),$$

odnosno M_n je složen broj. □

Obrat prethodne tvrdnje ne vrijedi. Naime, $2^{11} - 1 = 2047 = 23 \cdot 89$, a to je ujedno i najmanji složen Mersenneov broj s prostim eksponentom.

[1] francuski matematičar, fizičar i filozof, 1596. – 1650.
[2] francuski matematičar i poreznik, 1588. – 1651.
[3] francuski matematičar i pravnik, 1601. – 1665.

U svojoj knjizi *Cogitata Physico-Mathematica* iz 1644. godine Mersenne je naveo da su brojevi oblika (1) prosti za $n = 2,\ 3,\ 5,\ 7,\ 13,\ 17,\ 19,\ 31,\ 67,\ 127,\ 257$ te da su to svi prosti za $n \leq 257$. No, brojevi M_{67} i M_{257} su složeni i teško je da to možemo uzeti za pogrešku matematičaru 17. stoljeća budući se radi o brojevima s 21, odnosno 78 znamenki. Uz broj M_{67} veže se zanimljiva priča. Na znanstvenom skupu Američkog matematičkog društa (AMS) 1903. godine, F. N. Cole[4] je održao priopćenje pod naslovom *On The Factorization of Large Numbers* (O faktorizaciji velikih brojeva). Njegovo se predavanje sastojalo samo od toga da je s jedne strane ploče izračunao potenciju 2^{67} te oduzeo broj 1, a s druge pomnožio brojeve 93 707 721 i 761 838 257 287 te na iznenađenje mnogih dobio isti broj. Nakon *predavanja bez riječi*, uslijedio je gromoglasan pljesak te pitanje koliko mu je trebalo da nađe te faktore. Cole je odgovorio—*Three years of Sundays* (Tri godine nedjelja). Njemu u čast AMS je ustanovio nagradu koja se naziva *Cole Prize*.

Sredinom 20. stoljeća Mersenneova lista prostih brojeva oblika (1) čiji je eksponent manji ili jednak 257, bez dva navedena izuzetka, nadopunjena je s još tri prosta broja, M_{61}, M_{89} i M_{107}.

Danas su Mersenneovi prosti brojevi vrlo aktualni jer su najveći pronađeni prosti brojevi upravo oblika (1). Prema broju znamenki veliki prosti brojevi se svrstavaju u tri skupine: titanski (s barem 10^3 znamenki), gigantski (s barem 10^5 znamenki) i megaprosti (s barem milijun znamenki). Najveći do sada poznati megaprost broj, s više od 24 milijuna znamenki, upravo je Mersenneov: $2^{82\,589\,933} - 1$. Pronađen je nedavno, u prosincu 2018. Do sada je poznato točno 51 Mersenneovih prostih brojeva a više o tome može se saznati na stranicama projekta GIMPS (Great Internet Mersenne Prime Search).

Razlozi što se ogromni prosti, odnosno megaprosti, traže u obliku (1) su u tome što niz Mersenneovih brojeva izuzetno brzo raste, što se može nešto reći o djeliteljima Mersenneovih brojeva, te što postoje učinkoviti algoritmi upravo za tu vrstu brojeva.

Propozicija 2. *Ako je q prosti djelitelj Mersenneovog broja M_p, gdje je p prost, onda je $q = 2kp + 1$, za neki cijeli broj k.*

Za dokaz prethodne tvrdnje trebaju nam neki važni i dobro poznati rezultati teorije brojeva.

Teorem 3 (Mali Fermatov teorem)**.** *Ako su $a, p \in \mathbb{N}$, p prost broj i p ne dijeli a, tada je $a^{p-1} \equiv 1 \pmod{p}$.*

Definicija 4. *Neka su a i n relativno prosti prirodni brojevi. Najmanji*

[4] američki matematičar, 1861. – 1926.

prirodan broj d sa svojstvom da je $a^d \equiv 1 \pmod{n}$ zove se red *od a modulo n.*

Propozicija 5. *Neka je d red od a modulo n. Tada za prirodni broj k vrijedi $a^m \equiv 1 \pmod{n}$ ako i samo ako d dijeli m.*

Dokaz Propozicije 2. Kako je q prost, i očito neparan, prema Teoremu 3 slijedi da q dijeli broj $2^{q-1}-1$. Prema pretpostavci propozicije q dijeli i broj $M_p = 2^p - 1$. Nadalje, jer je p prost broj slijedi da je p najmanji prirodan broj za kojeg je $2^p \equiv 1 \pmod{q}$, odnosno p je *red* broja 2 modulo q. Stoga prema Propoziciji 5 slijedi da p dijeli $q-1$, odnosno $2p$ dijeli $q-1$ budući da je $q-1$ paran broj a p neparan. Dakle, postoji $k \in \mathbb{N}$ za koji je $q = 2kp + 1$. □

Za ispitivanje prostosti Mersenneovih bojeva može se koristiti tzv. *Lucas–Lehmer test prostosti*, kraće zvan LLT. Izvorno ga je osmislio Édouard Lucas[5] u drugoj polovici 19. stoljeća a usavršio Derrick Henry Lehmer[6] u 30-tim godinama 20. stoljeća. Algoritam se temelji na sljedećem teoremu.

Teorem 6 (LLT)**.** *Neka je p neparan prost broj i (s_n) niz rekurzivno zadan sa $s_n = s_{n-1}^2 - 2$, za $n \geq 1$ pri čemu je $s_0 = 4$. Tada je M_p prost broj ako i samo ako vrijedi $s_{p-2} \equiv 0 \pmod{M_p}$.*

Složenost prethodnog algoritma, ukoliko se koristi standardni algoritam za množenje, je $O(p^3)$. Samo za usporedbu, spomenimo da bi složenost klasičnog algoritma dijeljenjem bila $O(2^{p/2})$.

Primjer 1. Provedimo LLT test prostosti na broj $M_7 = 2^7 - 1 = 127$. Prema Teoremu 6 M_7 je prost ako i samo ako je $s_5 \equiv 0 \pmod{M_7}$. Računamo vrijednosti niza (s_n) modulo M_7:

$$\begin{aligned}
s_0 &= 4,\\
s_1 &= 4^2 - 2 = 14,\\
s_2 &= 14^2 - 2 = 194 \equiv 67 \pmod{127},\\
s_3 &\equiv 67^2 - 2 = 4487 \equiv 42 \pmod{127},\\
s_4 &\equiv 42^2 - 2 = 1762 \equiv 111 \pmod{127},\\
s_5 &\equiv 111^2 - 2 = 12319 \equiv 0 \pmod{127}.
\end{aligned}$$

Stoga nam LLT test daje da je $M_7 = 127$ prost broj.

Uz Mersenneove proste brojeve vežu se još mnoge slutnje. Navodimo neke od njih.

[5]francuski matematičar, 1842. – 1891.
[6]američki matematičar, 1905. – 1991.

Slutnja 1. *Postoji beskonačno mnogo Mersenneovih prostih brojeva.*

O prethodnoj slutnji Richard K. Guy[7] kaže: *Njihov je broj nedvojbeno beskonačan, ali nam je dokaz beznadno izvan dosega.*

Slutnja 2 (Wagstaff[8])**.** *Neka je $M(x)$ broj prostih $p \leq x$ za koje je M_p prost. Tada je*

$$M(x) \approx \frac{e^{\gamma}}{\ln 2} \ln \ln x,$$

odnosno

$$M(x) \approx 2.5695 \ln \ln x,$$

pri čemu je γ Euler - Mascheronijeva konstanta.

Slutnja 3 (Bateman[9], Selfridge[10], Wagstaff)**.** *Neka je p neparan prost broj. Tada je ekvivalentno:*

1. *M_p je prost.*
2. *Sljedeće dvije tvrdnje su obje istinite ili obje lažne:*
   (a) *$\frac{1}{3}(2^p + 1)$ je prost.*
   (b) *p je oblika $2^k \pm 1$ ili $4^k \pm 3$.*

Slutnja 4. *Svaki element niza Mersenneovih brojeva*

$$2^2 - 1 = 3,\ 2^3 - 1 = 7,\ 2^7 - 1 = 127,\ 2^{127} - 1 = \underbrace{170 \ldots 727}_{39\ znamenki},\ \ldots$$

je prost.

Sljedeći član niza danog u Slutnji 4 ima više od 10^{38} znamenki pa još uvijek nije moguće ispitati njegovu prostost.

3 Fermatovi prosti brojevi

Pierre de Fermat jedan je od najznamenitijih francuskih matematičara iz prve polovice 17. stoljeća. Iako se matematikom bavio kao amater, jer je po zanimanju bio pravnik, uvelike je pridonio razvoju teorije brojeva te ga se s razlogom smatra *ocem* moderne teorije brojeva. Radove nije objavljivao, već su oni postali poznati preko njegove korespondencije s drugim matematičarima te kroz njegove zabilješke na marginama Bachetovog[11] prijevoda Diofantove Aritmetike.

[7] britanski matematičar, 1916.
[8] Samuel S. Wagstaff Jr., američki matematičar, 1945.
[9] Paul T. Bateman američki matematičar, 1919. – 2012.
[10] John L. Selfridge, američki matematičar, 1927. – 2010.
[11] Claude Gaspard Bachet de Méziriac, francuski matematičar, lingvist i pjesnik, 1581. – 1638.

Poznato je da je i sam Fermat proučavao Mersenneove brojeve (1). Malom modifikacijom, zamjenom *minusa* u *plus*, Fermat se zainteresirao za brojeve oblika $2^n + 1$.

Propozicija 7. *Ako je $2^k + 1$ neparan prost broj, tada je k potencija broja 2.*

Dokaz. Pretpostavimo da k nije potencija broja 2, odnosno pretpostavimo da k ima neparnog prostog djelitelja. Dakle, $k = mp$ za neki neparan prost broj p i prirodan broj m. No, tada $2^m + 1$ dijeli $2^{mp} + 1$.

Pokazali smo da ako k nije potencija broja 2, onda je $2^k + 1$ složen. Obrat po kontrapoziciji glasi, ako je $2^k + 1$ prost, onda je $k = 2^n$ za neki nenegativan cijeli broj n, što je trebalo pokazati. □

Broj oblika

$$f_n = 2^{2^n} + 1, \ n \in \mathbb{N}_0 \tag{2}$$

zove se *Fermatov broj*, odnosno *Fermatov prost broj* ako je (2) prost. Fermat je znao da su prvih 5 brojeva ovog oblika prosti:

$$f_0 = 3, \ f_1 = 5, \ f_2 = 17, \ f_3 = 257, \ f_4 = 65537,$$

te na temelju toga iznio slavnu slutnju da su svi brojevi oblika (2) prosti. No, 1732. godine Euler[12] je pokazao da 641 dijeli broj $f_5 = 4\,294\,967\,297$ i štoviše ustanovio kako izgledaju djelitelji Fermatovih složenih brojeva.

Teorem 8 (Euler)**.** *Neka je p prost djelitelj od f_n. Tada je $p = k2^{n+1}+1$, za neki $k \in \mathbb{N}$.*

Dokaz. Budući da p dijeli $2^{2^n} + 1$, slijedi da p dijeli i

$$2^{2^{n+1}} - 1 = (2^{2^n} + 1)(2^{2^n} - 1),$$

odnosno $2^{2^{n+1}} \equiv 1 \pmod{p}$. Stoga prema Propoziciji 5, slijedi da red d broja 2 modulo q dijeli 2^{n+1}, tj. $d = 2^m$, $m \leq n+1$. Ako pretpostavimo da je $m < n + 1$, tada i za višekratnik 2^n od d vrijedi $2^{2^n} \equiv 1 \pmod{p}$. Stoga p dijeli dva uzastopna neparna broja $2^{2^n} - 1$ i $2^{2^n} + 1$ što je nemoguće pa je i naša pretpostavka da je $m < n + 1$ pogrešna. Dakle, red broja 2 modulo p je $d = 2^{n+1}$.

Kako je prema Malom Fermatovom teoremu, $2^{p-1} \equiv 1 \pmod{p}$, slijedi da 2^{n+1} dijeli $p - 1$, odnosno $p = k2^{n+1} + 1$, $k \in \mathbb{N}$. □

Do danas je ustanovljeno da su Fermatovi brojevi f_n za $5 \leq n \leq 32$ složeni, za f_{33} nije ustanovljeno je li prost ili složen, a za 266 vrijednosti broja n za koji je $33 < n \leq 3329780$ poznato je da je f_n složen. S obzirom na ove empirijske podatke uz Fermatove brojeve se vežu slutnje:

[12] Leonhard Euler, švicarski matematičar, fizičar i astronom, 1707. – 1783.

Slutnja 5. *Skup Fermatovih prostih brojeva je konačan.*

Slutnja 6. *Skup Fermatovih složenih brojeva je beskonačan.*

Najjednostavniji test prostosti koji se primjenjuje na Fermatove brojeve je *Pépinov*[13] *test.*

Teorem 9 (Pépinov test)**.** *Neka je $n > 1$. Fermatov broj f_n je prost broj ako i samo ako f_n dijeli broj $3^{\frac{1}{2}(f_n-1)} + 1$.*

Primjer 2. Pépinov test provodi se uzastopnim modularnim kvadriranjem. Konkretno, broj $a = 3^{\frac{1}{2}(f_n-1)} \bmod f_n$ računamo pomoću sljedećeg algoritma:

$$\texttt{za}\ \ i = 1\ \ \texttt{do}\ \ 2^n - 1\ \ \texttt{računaj}\ \ a := a^2 \bmod f_n.$$

Za $n = 4$, dobivamo $a = 65536$, odnosno $a + 1 \equiv 0 \pmod{f_4}$, a za $n = 5$ je $a = 10324303$ i $a + 1 \not\equiv 0 \pmod{f_4}$. Pépinov test nam sada potvrđuje poznatu činjenicu da je f_4 prost, a f_5 složen.

Za ispitivanje prostosti mogućih djelitelja Fermatovih brojeva, odnosno brojeva oblika $k \cdot 2^m + 1$, može poslužiti sljedeći test.

Teorem 10 (Prothov[14] teorem)**.** *Neka je $N = k \cdot 2^n + 1$ i $2^n > k$, te neka je $a \in \mathbb{Z}$ takav da $N \mid (a^{(N-1)/2} + 1)$. Tada je N prost broj.*

Uočimo da Teorem 10 za $N = f_n$ i $a = 3$ upravo daje Pépinov test. François Proth bio je francuski seljak iz okolice Verduna te samouki matematičar. Proth je još jedan izvrstan primjer kako doprinos u matematici, odnosno specijalno teoriji brojeva, može dati amater. Njemu u čast su brojevi oblika $k \cdot 2^m + 1$ za $m \in \mathbb{N}$ i $k < 2^m$ nazvani *Prothovi brojevi*, a ako prođu test Teorema 10 onda su to *Prothovi prosti brojevi.* Na stranici `http://www.prothsearch.com/` može se naći popis svih prostih oblika $k2^n \pm 1$ te provjeriti status faktorizacije poopćenih Fermatovih brojeva, $a^{2^n} + b^{2^n}$.

Zanimljivo je da svaki do sada ispitan složen Fermatov broj ima međusobno različite proste faktore. Zato se pretpostavlja da vrijedi sljedeće:

Slutnja 7. *Fermatovi složeni brojevi su kvadratno slobodni.*

[13] Jean François Théophile Pépin, francuski matematičar, 1826. – 1904.
[14] François Proth, 1852. – 1879.

4 Fibonaccijevi prosti brojevi

Leonardo Pisano[15] znan još i kao Leonardo Bonacci ili Leonardo iz Pise, najpoznatiji je pod nadimkom *Fibonacci* koji predstavlja skraćenicu od *filius Bonacci* (Bonaccijev sin), a kojeg mu je u 19. stoljeću nadjenuo talijanski povjesničar G. Libri. Fibonacci je 1202. godine u svojoj knjizi *Liber Abaci* predstavio Hindu-arapski brojevni sustav koji se nakon toga brzo proširio zapadnom Europom. Također je napravio listu prostih brojeva iz intervala $[10, 100]$ te primijetio da je za testiranje prostosti broja n dovoljno provjeriti ima li n prostih djelitelja manjih od $\sqrt{n}$. No, ipak prva asocijacija na Fibonaccija je sljedeći niz prirodnih brojeva:

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

Do tog niza Fibonacci je došao proučavajući problem razmnožavanja zečeva u idealnim uvjetima:

U ograđen prostor stavljen je jedan par zečeva, zečica i zec. Koliko će parova zečeva biti u tom prostoru nakon godine dana, ako znamo da svaki mjesec jedan par zečeva okoti još jedan par koji postaje aktivan tek nakon dva mjeseca?

Rješenje problema je niz (3) koji zadovoljava sljedeću rekurzivnu relaciju:

$$F_n = F_{n-1} + F_{n-2},\ n \geq 3$$

pri čemu je $F_1 = F_2 = 1$ a nazivamo ga *Fibonaccijevim nizom.* F_n je n-ti *Fibonaccijev broj.* Možemo, bez pretjerivanja, reći da je ovo najpoznatiji niz brojeva koji se aktivno proučava sve do danas o čemu svjedoči i znanstveni časopis *Fibonacci Quarterly.* Osim u različitim područjima matematike, Fibonaccijevi brojevi mogu se naći u prirodi, glazbi, odnosno umjetnosti općenito, arhitekturi itd. gdje opisuju različite pravilnosti.

Fibonaccijevi brojevi zadovoljavaju vrlo mnogo identiteta. Posebno se korisnom pokazala sljedeća matrična jednakost

$$\begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^n = Q^n. \tag{4}$$

Računanjem determinante u (4) slijedi poznati *Cassinijev identitet*

$$F_{n+1}^2 = F_n F_{n+2} + (-1)^n$$

iz kojeg možemo *pročitati* da su svaka dva uzastopna Fibonacijeva broja relativno prosta. No, nas ponovo zanimaju *prosti* Fibonaccijevi brojevi. U tu svrhu od koristi nam je sljedeći teorem.

[15] talijanski matematičar, 1175. – 1250.

Teorem 11. *F_n dijeli F_{mn}, za sve $m, n \in \mathbb{N}$.*

Dokaz. Iz (4) slijedi

$$Q^n \bmod F_n = \begin{bmatrix} F_{n-1} & 0 \\ 0 & F_{n-1} \end{bmatrix} = \operatorname{diag}(F_{n-1}, F_{n-1}).$$

Otuda je

$$Q^{mn} \bmod F_n = \operatorname{diag}(F_{n-1}^m, F_{n-1}^m)$$

pa je $F_{mn} \bmod F_n = 0$ što je i trebalo pokazati. □

Korolar 12. *Ako je $n > 4$ i F_n prost broj, onda je n prost.*

Obrat prethodnog korolara ne vrijedi, odnosno iz činjenice da je p prost broj ne mora nužno slijediti da je F_p prost. Najmanji prost broj p za koji je F_p složen je $p = 19$, $F_{19} = 4181 = 37 \cdot 113$. Zbog svega navedenog proste brojeve u Fibonacccijevom nizu tražimo u podnizu $(F_p)_{p\,\text{prost}}$ s jedinim izuzetkom $F_4 = 3$ (jer je $F_2 = 1$). Zasad je poznato da su Fibonaccijevi brojevi F_n su prosti za točno sljedeće vrijednosti $n =$ 3, 4, 5, 7, 11, 13, 17, 23, 29, 43, 47, 83, 131, 137, 359, 431, 433, 449, 509, 569, 571, 2971, 4723, 5387, 9311, 9677, 14431, 25561, 30757, 35999 i 81839. Kao i za mnoge druge oblike prostih brojeva i ovdje se sluti da ih je beskonačno mnogo.

Slutnja 8. *Postoji beskonačno mnogo Fibonaccijevih prostih brojeva.*

5 Sophie Germain prosti brojevi

Sophie Germain[16] je bila jedna od prvih matematičarki u povijesti. Samostalno se educiravši podigla je svoju matematičku pismenost na razinu s koje je mogla surađivati s najuglednijim matematičarima tog vremena, Lagrangeom[17] i Gaussom[18] i to sa svega osamnaest godina. Prva pisma je bila prisiljena pisati pod pseudonimom muškarca te su se oba matematičara iznenadili kada su shvatili da je riječ o ženi. Lagrange je neke njezine rezultate zapisao u knjizi *Théorie des nombres* (Teorija brojeva). Također je dobila nagradu *Academie des Sciences*. Sophie Germain je hrabro zakoračila u svijet znanosti i uvelike pridonijela razbijanju tradicionalne predrasude da je matematika rezervirana isključivo za muškarce te je pokazala svijetu da i žene mogu pridonijeti znanosti, što je za to vrijeme bio veliki iskorak. Počasni doktorat primila je posthumno za što se osobno zauzeo sam Gauss.

[16] francuska matematičarka, 1776. – 1831.
[17] Joseph-Louis Lagrange, talijanski matematičar i astronom, 1736. – 1813.
[18] Carl Friedrich Gauss, njemački matematičar, 1777. – 1855.

Sophie Germain pokazivala je izniman interes za teoriju brojeva. Godine 1832. dokazala je specijalan slučaj *Velikog Fermatovog teorema* koji kaže da jednadžba $x^n + y^n = z^n$ za prirodan broj $n > 2$ nema rješenja u skupu prirodnih brojeva. Štoviše, njezin rad na Velikom Fermatovom teoremu rezultirao je tim da se njegov dokaz treba dijeliti na dva slučaja: prvi u kojem su x, y, z i p relativno prosti te drugi u kojem p dijeli barem jedan od x, y i z.

Teorem 13 (Germain)**.** *Neka je p prost broj takav da je $2p+1$ također prost. Tada ne postoje $x, y, z \in \mathbb{N}$ takvi da p ne dijeli ni jedan od njih i da je $x^p + y^p = z^p$.*

Prost broj p sa svojstvom iz Teorema 13, odnosno takav da je i $2p+1$ prost, naziva se *Sophie Germain prost broj*. Prvih dvadeset Sophie Germain prostih brojeva je

$$2, 3, 5, 11, 23, 29, 41, 53, 83, 89, 113, 131, 173, 179, 191, 233, 239, 251, 281, 293.$$

Najveći poznati Sophie Germain prost broj ima 388 342 znamenke, a otkriven je 2016. godine. Sluti se da ih je beskonačno mnogo.

Slutnja 9. *Postoji beskonačno mnogo Sophie Germain prostih brojeva.*

Sophie Germain prosti brojevi se primjenjuju u kriptografiji javnog ključa. Na primjer, kod RSA kriptosustava sigurnost se zasniva na činjenici da je teško faktorizirati veliki složen broj. Konkretno, u slučaju ovog kriptosustava *veliki* složeni broj je oblika $n = pq$ gdje su p i q *veliki* prosti brojevi pri čemu atribut *veliki* označava brojeve s više stotina znamenki. Međutim, veličina ovih brojeva nije sama po sebi dovoljna za sigurnost ovog kriptosustava jer postoje algoritmi za faktorizaciju koji relativno lako određuju proste faktore ukoliko su oni specijalnog oblika. Jedan od njih je *Pollardov ρ-algoritam* koji lako pronalazi traženu faktorizaciju, ako je barem jedan od brojeva $p-1$ i $q-1$ jednak umnošku malih prostih brojeva. Takav je, na primjer, $p = 109$ jer je $108 = 2^2 \cdot 3^3$. Prosti brojevi p oblika $2s+1$, gdje je s prost broj, otporni su, odnosno *sigurni* na ovaj algoritam. Stoga se prost broj oblika $p = 2s+1$ takav da je s prost zove *siguran prost broj*. Očito je $p = 2s+1$ siguran ako i samo ako je s Sophie Germain prost broj.

6 Wilsonovi prosti brojevi

John Wilson[19] je u teoriji brojeva zapamćen po teoremu koji karakterizira proste brojeve iako je taj teorem bio poznat arapskom matematičaru

[19] engleski matematičar, 1741. – 1793.

Alhazenu[20] sedam stoljeća prije te Leibnizu[21] stoljeće prije. Prvi ga je dokazao Lagrange.

Teorem 14 (Wilsonov teorem)**.** *Broj p je prost ako i samo ako p dijeli $(p-1)!+1$.*

Dokaz. Tvrdnja očito vrijedi za $p \in \{2,3\}$. Zato pretpostavimo da je $p \geq 5$ i p prost broj. Uočimo da za svaki $a \in \{2,3,\ldots,p-2\}$ postoji jedinstven $b \in \{2,3,\ldots,p-2\}$ takav da je $b \neq a$ i $ab \equiv 1 \pmod{p}$. Zaista, linearna kongruencija $ax \equiv 1 \pmod{p}$ ima jedinstveno rješenje modulo p jer je $\gcd(a,p)=1$. Nadalje, $x=a$ ako i samo je $a \in \{1,p-1\}$. Stoga, skup $\{2,3,\ldots,p-2\}$ možemo grupirati u parove elemenata čiji je umnožak kongruentan 1 modulo p i zaključiti da je

$$2 \cdot 3 \cdots (p-2) \equiv 1 \pmod{p}.$$

Otuda je $(p-1)! \equiv -1 \pmod{p}$.

S druge strane, ako pretpostavimo da je p složen broj, tada su svi pravi djelitelji od p iz skupa $\{2,3,\ldots,p-1\}$ pa ne može vrijediti da je $(p-1)! \equiv -1 \pmod{p}$. □

Wilsonov teorem karakterizira proste brojeve, no u praksi je neučinkovit. Najveći prost broj čija je prostost pokazana pomoću Wilsonovog teorema je 1 099 511 628 401 (prema [9]).

Wilsonov teorem poslužio je i kao inspiracija za proste brojeve p koji zadovoljavaju uvjet

$$(p-1)! \equiv -1 \pmod{p^2}.$$

Oni se nazivaju *Wilsonovi prosti brojevi.* Jedini poznati Wilsonovi prosti brojevi su 5, 13, 563 te su ujedno i jedini u intervalu $\langle 1, 5 \cdot 10^8 \rangle$. Našao ih je Karl Goldberg 1953. godine koristeći rana elektronička računala. Usprkos činjenici da su poznata samo tri Wilsonova prosta broja, postavljene su sljedeće slutnje:

Slutnja 10. *Postoji beskonačno mnogo Wilsonovih prostih brojeva.*

Slutnja 11. *Vjerojatnost da je prost broj p Wilsonov jednak je $\frac{1}{p}$.*

Očekuje se da bi četvrti Wilsonov prost broj trebao biti reda veličine $5 \cdot 10^{23}$, a za to ipak još treba pričekati neko vrijeme.

[20] Hasan Ibn al-Haytham, arapski matematičar, astronom i filozof, 965. – 1040.
[21] Gottfried Wilhelm Leibniz, njemački matematičar i filozof, 1646.– 1716.

7 *Igranje* sa znamenkama

7.1 Palindromski prosti brojevi

Palindrom (od grčkog *palíndromos*) ili *obrtaljka* je naziv za dio teksta koji čitan od početka prema kraju ili obrnuto glasi jednako. Nas zanimaju numerički palindromi, odnosno brojevi koji pročitani s desna na lijevo i s lijeva na desno predstavljaju isti broj. Palindromski prosti broj je broj koji je palindrom i prost. Svi jednoznamenkasti prosti su, naravno, palindromski prosti brojevi. Jedini dvoznamenkasti palindromski prost broj je 11. To je ujedno i jedini palindromski prost broj s parnim brojem znamenki. Zaista, za palindrom $m = \overline{x_0x_1\cdots x_nx_n\cdots x_1x_0}$, pri čemu su $x_0, \ldots, x_n$ znamenke broja m i $n \geq 1$, vrijedi da je

$$m = x_0\underbrace{(10^{2n+1}+1)}_{11|} + x_1\underbrace{(10^{2n}+10)}_{11|} + \cdots + x_n\underbrace{(10^{n+1}+10^n)}_{11|}.$$

Stoga zaključujemo da je svaki palindrom s parnim brojem znamenki većim od 3 djeljiv s 11.

Postoji petnaest troznamenkastih prostih brojeva koji su palindromi. To su 101, 131, 151, 181, 191, 313, 353, 373, 383, 727, 757, 787, 797, 919 i 929.

Najveći poznati palindromski prost broj je otkrio Harvey Dubner 2004. i on je $10^{120016} + 1723271 \cdot 10^{60005} + 1$, broj s više od 120 tisuća znamenki.

7.2 Pandigitalni prosti brojevi

Pandigitalni broj je cijeli broj koji u svom dekadskom zapisu sadrži svaku od znamenki $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$ barem jednom. Naziv *pandigitalni* sastavljen je od riječi *pan* grčkog podrijetla koja se koristi kao prefiks u složenicama sa značenjem: sve, sav, sva, te od engleske riječi *digit* – znamenka. Stoga pandigitalan broj možemo nazvati i *sveznamenkastim* brojem. Najmanji pandigitalni broj je 1023456789 i očito je složen jer je zbroj njegovih znamenki jednak 45. Jasno je da isto vrijedi i za sve druge pandigitalne brojeve koji su dobiveni permutacijom znamenki. Zanimaju li nas takvi prosti brojevi moramo dodati još barem jednu znamenku. Prvih nekoliko pandigitalnih prostih brojeva su 10123457689, 10123465789, 10123465897, 10123485679, ... Najmanji pandigitalni prost broj koji je ujedno i palindrom je 1023456987896543201.

7.3 Repunit prosti brojevi

Repunit je broj čije su sve znamenke 1, na primjer 11, 111, itd. Složenica repunit je nastala od engleskih riječi *repeated* i *unit*. Oznaka za repunit

je R_n pri čemu je n broj znamenki. Prostost broja R_n ovisit će o faktorizaciji broja $10^n - 1$ jer je $R_n = \dfrac{10^n - 1}{9}$. Repunit broj R_n može biti prost broj samo ako je n prost broj pri čemu obrat, naravno, ne vrijedi. Poznato ih je vrlo malo, samo njih 5, za $n \in \{2, 19, 23, 317, 1031\}$, no ipak se pretpostavlja da bi ih moglo biti beskonačno mnogo.

Slutnja 12. *Postoji beskonačno mnogo repunit prostih brojeva.*

Postoji još nekoliko kandidata za repunit proste brojeve i oni su R_{49081}, R_{86453}, R_{270343} i R_{270343}. Za njih je poznato da su *vjerojatno prosti* što znači da kandidati za proste brojeve zadovoljavaju određene probabilističke testove prostosti. Konkretno, ovi brojevi zadovoljavaju testove koji se zasnivaju na Malom Fermatovom teoremu.

7.4 Cirkularni prosti brojevi

Prosti broj je *cirkularan* ili *kružeći* ako nakon svake cikličke permutacije njegovih znamenki dobivamo opet prost broj. Na primjer, 1193 je cirkularan prost broj jer su i njegove cikličke permutacije, 1193, 1931, 9311, 3119, prosti brojevi. Jasno je da cirkularni prosti ne mogu sadržavati niti jednu parnu znamenku te znamenku 5 i stoga ih možemo konstruirati jedino od znamenki $1, 3, 7, 9$. Nadalje, očito je da je svaki repunit prost broj ujedno i cirkularan prost. Svi cirkularni prosti manji od 10^{23} su: 2, 3, 5, 7, R_2, 13, 17, 37, 79, 113, 197, 199, 337, 1193, 3779, 11939, 19937, 193939, 199933, R_{19}, R_{23}, R_{317}, R_{1031} R_{49081}, R_{86453}, R_{109297} i R_{270343}.

Literatura

[1] B. Bakula, Z. Franušić, *Matrice s Fibonaccijevim brojevima*, math.e **26** (2014).

[2] A. Dujella, *Teorija brojeva*, Školska knjiga, Zagreb, 2019.

[3] Z. Franušić, N. Pavlinić, *O distribuciji prostih brojeva*, Acta Math. Spalatensia Ser. Didactica **1** (2018), 41–50.

[4] David Wells, *Prime Numbers*, John Wiley & Sons, Inc., 2005.

[5] Great Internet Mersenne Prime Search, `https://www.mersenne.org/`

[6] *Hrvatska enciklopedija*, `http://www.enciklopedija.hr/`

[7] *List of prime numbers*, https://en.wikipedia.org/wiki/List_of_prime_numbers

[8] *Marie-Sophie Germain*, http://www-groups.dcs.st-and.ac.uk/history/Biographies/Germain.html

[9] *The Prime Pages: Prime Number Research, Records and Results*, https://primes.utm.edu/

Zrinka Franušić
PMF-MO Sveučilišta u Zagrebu
E-mail adresa: fran@math.hr

Nikola Pavlinić
student prediplomskog studija Matematika na PMF-MO Sveučilišta u Zagrebu
E-mail adresa: genericroc@gmail.com

Zaprimljen: 6. ožujka 2019.
Prihvaćen: 12. travnja 2019.