# Savršeni i Mersenneovi brojevi

**Patković, Kristina**

**Master's thesis / Diplomski rad**

**2019**

*Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj:* **Josip Juraj Strossmayer University of Osijek, Department of Mathematics / Sveučilište Josipa Jurja Strossmayera u Osijeku, Odjel za matematiku**

*Permanent link / Trajna poveznica:* https://urn.nsk.hr/urn:nbn:hr:126:517555

Sveučilište J.J. Strossmayera u Osijeku
Odjel za matematiku

**Kristina Patković**

# Savršeni i Mersenneovi brojevi

Diplomski rad

Osijek, 2019.

Sveučilište J.J. Strossmayera u Osijeku
Odjel za matematiku

**Kristina Patković**

# Savršeni i Mersenneovi brojevi

Diplomski rad

Mentor: izv. prof. dr. sc. Ivan Matić

Osijek, 2019.

# Sadržaj

# Uvod

Teorija brojeva jedna je od najstarijih grana matematike. Ona proučava svojstva cijelih brojeva, a posebno svojstva prirodnih brojeva. Otkrivanje zanimljivih i neočekivanih odnosa između različitih vrsta brojeva kao i dokazivanje istinitosti različitih tvrdnji cilj je ove teorije. Friedrich Gauss (Gauss, C. F., 1777.-1855.) je matematiku nazivao kraljicom znanosti, a teoriju brojeva kraljicom matematike. Problemi i tvrdnje u ovoj teoriji se iskazuju na vrlo jednostavan i razumljiv način, iako rješenja problema i dokazi zahtijevaju sofisticiranu matematičku pozadinu.

U sklopu teorije brojeva, svoje mjesto pronašla je i priča o savršenim i Mersenneovim prostim brojevima. Potraga za ovim brojevima zaokuplja pozornost istraživača od samih početaka razvoja matematike kao znanosti. Proučavanje ovih brojeva, kao i njihovog međusobnog odnosa, predstavlja temu ovog rada.

U prvom dijelu ćemo promotriti razvoj znanosti u 16. stoljeću. Znatan utjecaj na taj razvoj imao je redovnik Marin Mersenne koji je organizirao redovita okupljanja matematičara čime je omogućena brža razmjena ideja.

U drugom dijelu ćemo se upoznati s jednim od najstarijih problema u teoriji brojeva, pronalaskom savršenih brojeva. Definirat ćemo savršene brojeve te promotriti dva bitna teorema koji govore o vezi savršenih i prostih brojeva. Također, reći ćemo nešto i o strukturi neparnih savršenih brojeva.

U trećem dijelu ćemo proučiti Mersenneove proste brojeve, broj znamenaka Mersenneovog prostog broja te neke uvjete za testiranje prostosti Mersenneovih brojeva. Na kraju, promotrit ćemo zanimljivu vezu između Mersenneovih brojeva i Pascalovog trokuta.

# 1 Marin Mersenne i znanstvena okupljanja

U 16. stoljeću mali broj ljudi je bio ozbiljno zainteresiran za matematiku ili znanost. Bilo ih je tek nekoliko tisuća, od kojih se većina samo zanimala, ali nisu bili aktivni. Znatan je broj zainteresiranih, koji su se bavili matematikom i znanošću, radio u izolaciji, jer čak i unutar sveučilišnih zajednica njihovi interesi nisu smatrani posebno značajnima. Znanost se još uvijek dovodila u vezu sa magijom te nije bila poštovana kao intelektualna djelatnost. Van knjiga, nije bilo redovitog načina da učeni ljudi održavaju međusobni kontakt, a izdavanje je bilo teško zbog crkvene cenzure i osude. Kako je sve više ljudi ulazilo u znanstvena istraživanja, uvidjelo se da na napredak u znanju utječe domet i brzina komunikacije vezane za otkrića. Neprekidno testiranje ideja održava jačinu znanosti tako što vodi ka odbacivanju opovrgnutih hipoteza. Za razliku od doba renesanse, kada se sva znanstvena rasprava održavala u okviru sveučilišnih krugova, početkom 17. stoljeća pojavljuju se učena društva i akademije neovisna o sveučilištima.

Najranija poznata redovita okupljanja matematičara su ona koja je organizirao redovnik Marin Mersenne (1588.–1648.), matematičar i fizičar. Mersenneov značaj za matematiku je prije svega u njegovoj korespondenciji sa svim važnim matematičarima toga doba, čime je omogućena razmjena ideja u doba u koje još nisu postojali matematički znanstveni časopisi niti brzi načini komunikacije. Kao čovjek koji nije puno pridonio novim saznanjima, Mer-

Slika 1: Marin Mersenne (1588.–1648.)

senne je imao sposobnost razumijevanja i cijenjenja radova drugih. Došavši u Pariz 1619. godine uvidio je da ne postoji nijedna formalna organizacija u kojoj bi se okupljali učeni ljudi. Potrudio se promijeniti situaciju tako što je svoj samostan učinio mjestom okupljanja za one koji su bili voljni raspravljati o svojim rezultatima i čuti slične radove, te tako što je povezivao učenjake iz različitih zemalja. U vrijeme kada još nisu postojala objavljivanja tehničkih otkrića, Mersenne je služio kao osobna i učinkovita "kućna razmjena" znanstvenih informacija. Namjera mu je bila upoznati se sa svima koji su bitni u znanstvenom svijetu kroz razrađenu mrežu dopisivanja preko koje je prenosio vijesti o znanstvenim otkrićima u zamjenu za iste. Poticao je znanstvenu misao kroz brojna pitanja koja je postavljao svakome

tko bi mogao doprinijeti pronalasku odgovora. Prosljeđivao je pitanja i odgovore drugima kako bi izazvao reakcije. Kada je umro, u njegovoj ćeliji su pronađena pisma 78 različitih dopisnika širom Europe, uključujući Fermata iz Francuske, Huygensa iz Holandije, Pella i Hobesa iz Engleske i Galilea i Torricellia iz Italije.

Održavanje konferencija za razmjenu ideja bilo je redovito od 1635. godine sve do Mersenneove smrti 1648. Kao sasvim neformalno okupljanje bez objavljivanja radova, ove konferencije ne mogu se smatrati akademijom. Ipak, njihov značaj je u slavi onih koji su ga sačinjavali: Desargues, Descartes, Pascal - otac i sin i drugi. Kada bi netko htio prezentirati svoje rezultate on bi ih otisnuo na mekim listovima papira i podijelio. Sa samo 14 godina, napredni Blaise Pascal je na jednom od sastanaka prezentirao letak na kojemu je bio teorem o mističnom heksagramu. Ovaj esej je bio najava teze koju je Pascal pripremao. Nikada nije objavljen i sada je izgubljen, iako ga je Leibniz vidio u Parizu 1676. godine i opisao njegov sadržaj.

Mersenne se također smatra i Galileovim predstavnikom u Francuskoj. Kada je čuo da Galileo piše knjigu o kretanju planete, ponudio se da ju objavi. Ipak, Galileo je sam objavio knjigu i kopije su poslane u Francusku. Do Mersennea je ubrzo stigla vijest o suđenju i paljenju knjiga. Ova odluka crkve da osudi Galilea, snažno je utjecala na Mersennea te je 1634. godine objavio verziju Galileovih ranih predavanja o mehanici, a 1639. godine preveo je "Discorsi" na francuski. Nije preveo Galileov "Diagolo" jer je smatrao da je Galileo prekršio obećanje koje je dao papi da neće pisati puno u korist Kopernikove teorije. Ipak, objavio je sažetke nekoliko dijelova. Kako Galileo nije bio shvaćen van svoje zemlje, Mersenne se potrudio popularizirati njegova otkrića. Vrijedi napomenuti da je to napravio jedan vjeran član katoličkog reda na vrhuncu crkvenog neprijateljstva prema znanosti. Kada je Mersenne umro, konferencije su se nastavile održavati na raznim mjestima u Parizu.

# 2 Savršeni brojevi

Mersenneovo ime povezano je sa jednim od najstarijih problema u teoriji brojeva, pronalaskom savršenih brojeva. Rani grčki matematičari su bili zainteresirani za odnose između broja i djelitelja (pozitivni djelitelji manji od samog broja). U doba kada se vjerovalo da brojevi imaju mistična svojstva, smatrano je izvanrednim da je broj 6 suma svojih pravih djelitelja: $6 = 1 + 2 + 3$. Idući broj koji ima ovo svojstvo je broj 28, $28 = 1 + 2 + 4 + 7 + 14$. Pitagorejci, u skladu s njihovom filozofijom pridavanja određenih socijalnih kvaliteta brojevima, nazvali su ove brojeve savršenima. Godine 1888., matematičar James Sylvester je napisao:

> "Grčkim geometrima se mora odati priznanje jer su uspjeli otkriti klasu savršenih brojeva koji su, po svemu sudeći, jedini brojevi koji su savršeni."

**Definicija 2.1.** Pozitivni cijeli broj $n$ je savršen ako je $n$ jednak sumi svih svojih pozitivnih djelitelja, ne uključujući sam $n$.

Ako sa $\sigma(n)$ označimo sumu svih pozitivnih djelitelja broja $n$, onda je suma svih pozitivnih djelitelja broja $n$ manjih od $n$ jednaka $\sigma(n) - n$. Da bi $n$ bio savršen mora vrijediti $\sigma(n) - n = n$ ili $\sigma(n) = 2n$. Na primjer, $\sigma(28) = 1 + 2 + 4 + 7 + 14 + 28 = 2 \cdot 28$.

Stoljećima, filozofi su više bili okupirani etičkim i religioznim značenjima savršenih brojeva, nego njihovim matematičkim svojstvima. U "De Civitate Dei" sveti Augustin objašnjava da, iako je Bog mogao stvoriti svijet odjednom, odabrao je da to učini za 6 dana, jer je savršenstvo rada simbolizirano savršenim brojem 6. Rani komentatori Starog zavjeta smatrali su da je savršenstvo svemira reperezentirano brojem 28, brojem dana za koje mjesec obiđe Zemlju. U sličnom stilu, Alcuin od Yorka, savjetnik Karla Velikog, smatra da ljudska vrsta potiče od 8 duša sa Noine arke, te da je ovo drugo stvaranje manje savršeno od prvoga pa 8 nije savršen broj.

Stari Grci su znali samo 4 savršena broja. Nicomachus iz Gerase, koji je sumirao postojeće znanje o teoriji brojeva, u svojoj "Introductio Arithmetica" navodi: $P_1 = 6$, $P_2 = 28$, $P_3 = 496$ i $P_4 = 8128$. Tvrdio je da su savršeni brojevi poredani u prikladnom redu, jedan među jedinicama, drugi među deseticama, treći među stoticama, a četvrti među tisućicama. Kasnije su neki autori pretpostavljali sljedeće:

1. $n$-ti savršeni broj $P_n$ sadrži točno $n$ znamenaka.
2. Parni savršeni brojevi završavaju znamenkom 6 ili 8, naizmjenično.

Pokazano je da su obje pretpostavke bile pogrešne. Idući savršen broj, otkriven u anonimnim bilješkama iz 15. stoljeća, jest $P_5 = 33550336$. Iako je njegova posljednja znamenka 6, sljedeći savršen broj $P_6 = 8589869056$, također završava sa 6, a ne sa 8 kako je pretpostavljeno. Može se pokazati da parni savršeni brojevi zaista završavaju znamenkama 6 ili 8, ali ne naizmjenično. Veličina broja $P_6$ trebala bi uvjeriti čitatelja u rijetkost savršenih brojeva.

Određivanje općeg oblika svih savršenih brojeva datira od antičkog doba. Djelomično je to uspio Euklid kada je u Propoziciji 36, 9. knjige Elemenata, dokazao da ako je suma: $1 + 2 + 2^2 + 2^3 + \cdots + 2^{k-1} = p$ prost broj, onda je $2^{k-1}p$ savršen broj (nužno je i paran broj).

**Primjer 2.1.** $1+2+4=7$, suma je prost broj, dakle $4 \cdot 7 = 28$ je savršen broj.

Primijetimo da su svi prethodno navedeni savršeni brojevi oblika $2^{p-1}(2^p-1)$, pri čemu su $p$ i $2^p-1$ prosti brojevi. Trebalo bi nas impresionirati što je Euklid dokazao da je svaki takav broj savršen, što sljedeći teorem i potvrđuje.

**Teorem 2.1** (Euklid)**.** Ako je $2^n-1$ prost broj ($n>1$), onda je $N=2^{n-1}(2^n-1)$ savršen broj.

*Dokaz.* Kako je $2^n-1$ prost broj, $\sigma(2^n-1) = 1+(2^n-1) = 2^n$. Nadalje, kako je $\sigma$ multiplikativna funkcija

$$\begin{aligned} \sigma(N) &= \sigma(2^{n-1})\sigma(2^n-1) = (2^n-1)(2^n) \\ &= 2 \cdot 2^{n-1}(2^n-1) = 2N. \end{aligned}$$

Dakle, $N$ je savršen broj. □

Kako bismo demonstrirali ovaj teorem, potrebno je znati sve djelitelje cijelog broja $2^{k-1}(2^k-1)$. Promotrimo problem pronalaska djelitelja proizvoljnog cijelog broja.

**Lema 2.1.** Ako je $N = p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$ rastav cijelog broja $N$ na proste faktore, pri čemu je $N>1$, onda su pozitivni djelitelji broja $N$ svi cijeli brojevi $d$ oblika $d = p_1^{a_1}p_2^{a_2}\cdots p_r^{a_r}$, gdje je $0 \le a_i \le k_i$, $i = 1, 2, ..., r$.

Na primjer, za $N=180$ vrijedi $N = 2^2 \cdot 3^2 \cdot 5$. Lema 2.1 nam govori da su pozitivni djelitelji broja 180 cijeli brojevi oblika $2^{a_1} \cdot 3^{a_2} \cdot 5^{a_3}$, gdje je $a_1 = 0, 1, 2$; $a_2 = 0, 1, 2$; $a_3 = 0, 1$. Ovo su ti brojevi:

$$\begin{array}{cccccc} 1\cdot1\cdot1 & 1\cdot1\cdot5 & 1\cdot3\cdot1 & 1\cdot3\cdot5 & 1\cdot3^2\cdot1 & 1\cdot3^2\cdot5 \\ 2\cdot1\cdot1 & 2\cdot1\cdot5 & 2\cdot3\cdot1 & 2\cdot3\cdot5 & 2\cdot3^2\cdot1 & 2\cdot3^2\cdot5 \\ 2^2\cdot1\cdot1 & 2^2\cdot1\cdot5 & 2^2\cdot3\cdot1 & 2^2\cdot3\cdot5 & 2^2\cdot3^2\cdot1 & 2^2\cdot3^2\cdot5, \end{array}$$

ili poredani: 1, 2, 3, 4, 5, 6, 9, 10, 12, 15, 18, 20, 30, 36, 45, 60, 90, 180. Lema 2.1 omogućuje nam da demonstriramo Euklidov teorem. Govori da, ukoliko je $2^{k-1}$ prost broj, onda je svaki od $1, 2, 2^2, 2^{k-1}, 2^k-1, 2(2^k-1), 2^2(2^k-1), \ldots, 2^{k-1}(2^k-1)$ djelitelj broja $N = 2^{k-1}(2^k-1)$, a ovo isključuje mogućnost drugih djelitelja. Pogledajmo sljedeće dvije sume:

$$s_1 = 1+2+2^2+\cdots+2^{k-1}$$

i

$$\begin{aligned} s_2 &= (2^k-1)+2(2^k-1)+2^2(2^k-1)+\cdots+2^{k-1}(2^k-1) \\ &= (1+2+2^2+\cdots+2^{k-1})(2^k-1) \\ &= s_1(2^k-1). \end{aligned}$$

Ukoliko ih zbrojimo, rezultat je sljedeći:

$$\sigma(N) = s_1 + s_1(2^k-1) = 2^k s_1.$$

S druge strane, formula za sumu geometrijskog niza daje $s_1 = 2^k - 1$ pa je naša ukupna formula $\sigma(N) = 2^k(2^k - 1) = 2 \cdot 2^{k-1}(2^k - 1) = 2N$ čija je posljedica da je $N$ savršen broj.

U 18. stoljeću, veliki švicarski matematičar Leonard Euler pokazao je da svi parni savršeni brojevi moraju imati oblik iz Euklidovog teorema. Odnosno, parni broj $N$ je savršen ako i samo ako je oblika $N = 2^{k-1}(2^k - 1)$, gdje je $2^k - 1$ prost broj. Dakle, Eulerov i Euklidov teorem karakteriziraju parne savršene brojeve.

**Teorem 2.2** (Euler)**.** Ako je $N = 2^{n-1}(2^n - 1)$ paran savršen broj, onda je $2^n - 1$ prost broj.

*Dokaz.* Neka je $N$ oblika $2^e s$, gdje je $s$ neparan broj i $e \geq 1$. Kako je $N$ savršen,

$$\sigma(N) = 2N = 2^{e+1}s.$$

Očito, $(2^e, s) = 1$ pa vrijedi

$$\begin{aligned} \sigma(N) &= \sigma(2^e s) = \sigma(2^e)\sigma(s) \\ &= (2^{e+1} - 1)\sigma(s). \end{aligned}$$

Dakle,

$$2^{e+1}s = (2^{e+1} - 1)\sigma(s). \tag{1}$$

Kako je $(2^{e+1}, 2^{e+1} - 1) = 1$, slijedi $2^{e+1} | \sigma(s)$ pa $\sigma(s) = 2^{e+1}t$ za neki prirodan broj $t$. Zamijenimo li $\sigma(s)$ u formuli (1), dobivamo

$$\begin{aligned} 2^{e+1}s &= (2^{e+1} - 1)2^{e+1}t \\ s &= (2^{e+1} - 1)t. \end{aligned} \tag{2}$$

Ovo povlači da $t|s$ i $t < s$. Kako $t = s$ povlači $e = 0$, dolazimo do kontradikcije.

Sada ćemo pokazati $t = 1$. Jednadžbu (2) možemo napisati u obliku

$$\begin{aligned} s + t &= 2^{e+1}t \\ s + t &= \sigma(s). \end{aligned} \tag{3}$$

Ovo pokazuje kako je $t$ suma pravih djelitelja od $s$, ali prema (2) $t$ je i sam pravi djelitelj od $s$. Dakle, kako bi vrijedilo (3), $t$ mora biti jednak 1.

Dakle, $s + t = \sigma(s)$ pa $s$ ima točno dva pozitivna djelitelja, 1 i $s$. Slijedi, $s = 2^{e+1} - 1$ mora biti prost broj.

Dakle, $N = 2^e(2^{e+1} - 1)$ pri čemu je $2^{e+1} - 1$ prost broj. □

Iako ovaj teorem pruža izvrsnu formulu za konstruiranje parnih savršenih brojeva, ne zna se postoji li beskonačno mnogo parnih savršenih brojeva. Odgovor bježi mnogim teoretičarima brojeva širom svijeta unatoč njihovim upornim istraživanjima.

Euklidov teorem vodi ka novom pitanju: Za koje vrijednosti $k$ je cijeli broj $2^k - 1$ prost broj? Prvi korak do rješenja se može odmah napraviti: ako je $2^k - 1$ prost broj, onda i sam eksponent $k$ mora biti prost broj.

Pretpostavimo suprotno, neka je $k$ složen broj, na primjer $k = rs$, gdje je $1 < r \leq s < k$. Koristeći formulu $x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \cdots + x^2 + x + 1)$ mogli bismo napisati:

$$\begin{aligned} 2^k - 1 &= 2^{rs} - 1 = (2^r)^s - 1 \\ &= (2^r - 1)(2^{r(s-1)} + 2^{r(s-2)} + \cdots + 2^r + 1). \end{aligned}$$

Kako je svaki faktor s desne strane veći od 1, ovo narušava "prostost" broja $2^k - 1$. Zbog toga $k$ mora biti prost broj.

Za proste brojeve $p$ =2, 3, 5 i 7, vrijednosti 3, 7, 31, 127 od $2^p - 1$ su prosti brojevi pa prema Euklidovoj formuli:

$$\begin{aligned} 2(2^2 - 1) &= 2 \cdot 3 = 6, \\ 2^2(2^3 - 1) &= 4 \cdot 7 = 28, \\ 2^4(2^5 - 1) &= 16 \cdot 31 = 496, \\ 2^6(2^7 - 1) &= 64 \cdot 127 = 8128 \end{aligned}$$

su svi savršeni brojevi.

Mnogi su rani autori vjerovali da je $2^p - 1$ prost broj za svaki izbor prostog broja $p$. 1536. godine Hudalrichus Regius, u svom djelu *"Utriusque Arithmetices"* predočio je točnu faktorizaciju $2^{11} - 1 = 2047 = 23 \cdot 89$. Ako ovo djeluje kao mali uspjeh, treba shvatiti da su ove računice, najvjerojatnije, izvedene sa rimskim brojevima uz pomoć abakusa (tek je krajem 16. stoljeća arapski sustav brojeva u potpunosti potisnuo rimski). Regius je pokazao da je $p = 13$ sljedeća vrijednost broja $p$ za koju je izraz $2^p - 1$ prost broj. Iz ovoga, došlo se do petog savršenog broja $P_5 = 2^{12}(2^{13} - 1)$ =33 550 336.

Godine 1603., Pietro Cataldi objavio je tablicu faktora svih brojeva do 800, sa odvojenom listom prostih brojeva do 750. Putem marljive procedure, dijeljenjem sa svim prostim brojevima, ne prelazeći njihove kvadratne korjene, Cataldi je ustanovio da su $2^{17} - 1$ i $2^{19} - 1$ prosti brojevi, što znači

$$\begin{aligned} P_6 &= 2^{16}(2^{17} - 1) = 8\ 589\ 869\ 056, \\ P_7 &= 2^{18}(2^{19} - 1) = 137\ 438\ 691\ 328. \end{aligned}$$

Dakle, otkriveni su 6. i 7. savršeni brojevi. Također se tvrdilo da je $2^n - 1$ prost broj za vrijednosti $n = 2, 3, 5, 7, 13, 17, 19, 23, 29, 31$ i 37. Ipak, 1640. godine Fermat je opovrgnuo ovu tvrdnju pronašavši faktore za $2^{23} - 1$ i $2^{37} - 1$, dok je Euler 1738. dokazao da je $2^{29} - 1$ složen broj.

Sada ćemo proučiti problem kojega je 1990. predložio Peter L. Montgomery sa Sveučilišta Kalifornije u Los Angelesu i John L. Selfridge sa Sveučilišta Sjevernog Illinoisa u DeKalbu. Problem eksplicitno identificira specijalnu klasu savršenih parnih brojeva. Prije rješavanja problema, pogledajmo sljedeća dva rezultata koja će nam biti potrebna pri rješavanju.

**Lema 2.2.** Ako je $n$ neparan broj oblika $6k - 1$, onda on nije savršen broj.

*Dokaz.* Pretpostavimo da je $n$ prirodan broj oblika $6k-1$. Tada je $n \equiv -1 \pmod 3$. Kako su svi potpuni kvadrati kongruentni 1 modulo 3, $n$ nije potpuni kvadrat. Također, za svaki dijelitelj $d$ od $n$, $n = d \cdot \frac{n}{d} \equiv -1 \pmod 3$ implicira $d \equiv -1 \pmod 3$ i $\frac{n}{d} \equiv 1 \pmod 3$, ili $d \equiv 1 \pmod 3$ i $\frac{n}{d} \equiv -1 \pmod 3$. U svakom slučaju, $d + \frac{n}{d} \equiv 0 \pmod 3$ i

$$\sigma(n) = \sum_{d|n, d<\sqrt{n}} d + \frac{n}{d} \equiv 0 \pmod 3.$$

Kako za $2n$ vrijedi $2n = 2(6k-1) \equiv 1 \pmod 3$, zaključujemo da $n = 6k-1$ ne može biti savršen broj. □

Sada možemo iskorisiti Lemu 2.2 kako bismo dokazali Touchardov teorem.

**Teorem 2.3** (Touchard)**.** Svaki neparan savršen broj mora biti oblika $12m+1$ ili $36m+9$.

*Dokaz.* Neka je $n$ neparan savršen broj. Iz Leme 2.2 slijedi da niti jedan broj oblika $6k-1$ ne može biti savršen pa $n$ mora biti oblika $6k+1$ ili $6k+3$. Dakle, ili je $n \equiv 1 \pmod 6$ i $n \equiv 1 \pmod 4$, ili $n \equiv 3 \pmod 6$ i $n \equiv 1 \pmod 4$. Rješavanjem ova dva sustava zaključujemo da $n$ mora biti oblika $12m+1$ ili $12m+9$. Konačno, primijetimo da ako je $n = 12m+9$ i $3 \nmid m$, $\sigma(n) = \sigma(3(4m+3)) = \sigma(3)\sigma(4m+3) = 4\sigma(4m+3)$. U ovome slučaju, $\sigma(n) \equiv 0 \pmod 4$, dok je $2n = 2(12m+9) \equiv 2 \pmod 4$ i $n$ nije savršen. Zaključujemo da $3|m$ i $n$ je oblika $36m+9$. □

Promotrimo sada rješenje Montgomeryjevog problema koje je dugačko i potrebno ga je pratiti pažljivo.

**Primjer 2.2.** Pronađi sve savršene brojeve oblika $n^n + 1$.

*Rješenje.* Neka je $N = n^n + 1$.

***1. slučaj:*** Neka je $n$ neparan broj. Kako je $N$ paran savršen broj, on mora biti oblika $N = 2^{m-1}(2^m - 1)$ pri čemu je $2^m - 1$ prost broj.

Očito, $N$ možemo faktorizirati kao $N = n^n + 1 = (n+1)r$, gdje je

$$r = n^{n-1} - n^{n-2} + \cdots - n + 1.$$

Tvrdimo $(n+1, r) = 1$. Kako bismo ovo pokazali, primijetimo da, kako je $n$ neparan broj, $r$ je naparan i $n+1$ je paran. Neka je $n+1 = 2^s t$, pri čemu je $t$ neparan cijeli broj $\geq 1$. Tada je $N = 2^s tr$, pri čemu su i $t$ i $r$ neparni brojevi. Kako je $N$ paran savršen broj, ovo je moguće jedino ako je $t = 1$. Dakle, $n+1 = 2^s$ pa je $(n+1, r) = 1$. (Primijetimo da ako je $r = 1$ vrijedi $N = n^n + 1 = n + 1$ pa je $n = 1$. Tada je $N = 2$ što nije savršen broj.)

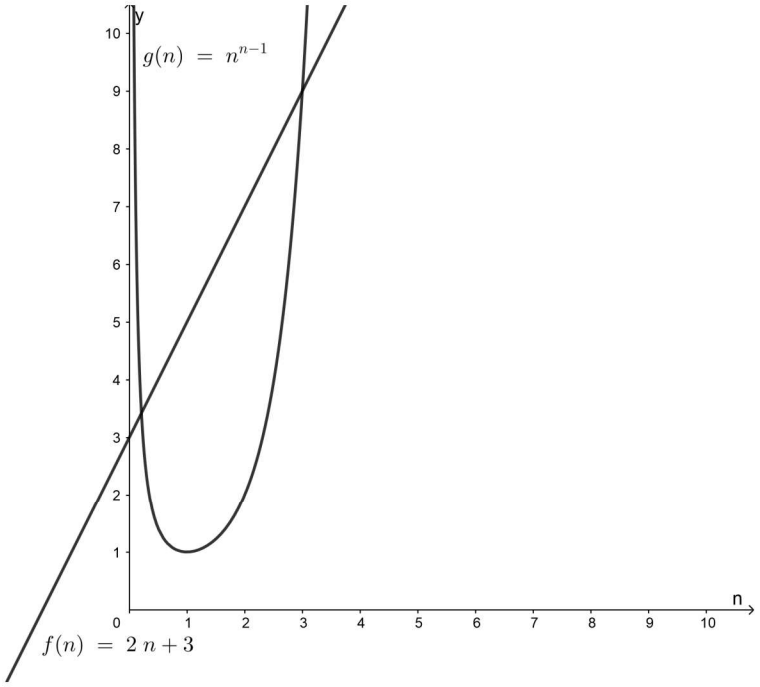
Kako je $N = 2^{m-1}(2^m - 1) = (n+1)r = 2^s r$, gdje je $2^m - 1$ prost broj i $r$ neparan, $2^s = 2^{m-1} = n+1$ i $r = 2^m - 1 = 2 \cdot 2^{m-1} - 1 = 2(n+1) - 1 = 2n+1$. Dakle,

$$N = n^n + 1 = (n+1)(2n+1) = 2n^2 + 3n + 1.$$

Ovo povlači:

$$\begin{aligned} n^n &= 2n^2 + 3n \\ n^{n-1} &= 2n + 3. \end{aligned}$$

Kako je $n$ cijeli broj, ova jednadžba ima jedinstveno rješenje $n = 3$ (Slika 2). Tada je $N = 3^3 + 1 = 28$. Dakle, 28 je jedini paran savršen broj željenog oblika.




Slika 2: Grafovi funkcija $f(n) = 2n + 3$ i $g(n) = n^{n-1}$

***2. slučaj:*** Neka je $n$ paran broj, $n = 2k$. Tada je $N$ neparan broj, $n^n$ je kvadrat i $n^n \equiv -1 \pmod{N}$. Tvrdimo $3 \nmid N$. Pretpostavimo $3|N$. Tada je $n^n \equiv -1 \pmod{3}$. Tada,

$$\begin{aligned} (2k)^{2k} &\equiv -1 \pmod{3} \\ 4^k \cdot k^{2k} &\equiv 2 \pmod{3} \\ 1 \cdot k^{2k} &\equiv 2 \pmod{3} \\ k^{2k} &\equiv 2 \pmod{3}. \end{aligned}$$

Očito, $k \not\equiv 0$ ili 1 modulo 3. Ako $k \equiv 2 \pmod{3}$, tada $k^{2k} \equiv 2 \pmod{3}$ povlači

$$\begin{aligned} 2^{2k} &\equiv 2 \pmod{3} \\ 4^k &\equiv 2 \pmod{3} \\ 1 &\equiv 2 \pmod{3} \end{aligned}$$

što je kontradikcija. Dakle, $k$ ne može biti kongruentno 0, 1 ili 2, što je nemoguće. Dakle, $3 \nmid N$.

Prema Touchardovom teoremu, $N = 12m+1$ ili $N = 36m+9$ za neki cijeli broj $m$. Ako

je $N = 36m + 9$ tada $3|N$ što je kontradikcija. Dakle, $N = 12m + 1$ što povlači $n^n = 12m$. Kako $3|12m$ i $3|n^n$ slijedi $3|n$. Dakle, $2|n$ i $3|n$ pa vrijedi $6|n$.

Neka je sada $N = a^6 + 1$ gdje je $a = n^{\frac{n}{6}} > 1$. Tada $N$ možemo rastaviti na faktore kao:

$$N = (a^2 + 1)(a^4 - a^2 + 1). \tag{4}$$

Sada ćemo pokazati da su ti faktori od $N$ relativno prosti. Neka je sada $p$ zajednički prost faktor od $a^2 + 1$ i $a^4 - a^2 + 1$. Kako je

$$\begin{aligned} a^4 - a^2 + 1 &= (a^4 + 2a^2 + 1) - 3a^2 \\ &= (a^2 + 1)^2 - 3a^2 \\ &= (a^2 + 1)^2 - 3(a^2 + 1) + 3, \end{aligned}$$

$p|3$. Dakle, $p = 3$. Ovo povlači $2|N$ što je kontradikcija. Slijedi da su faktori $a^2 + 1$ i $a^4 - a^2 + 1$ relativno prosti. Također, kako je $N$ neparan, oba faktora su također neparna.

Kako je $N$ savršen i $\sigma$ je multiplikativna iz (4) slijedi

$$\sigma(n) = \sigma(a^2 + 1) \cdot \sigma(a^4 - a^2 + 1).$$

Dakle,

$$2N = \sigma(a^2 + 1) \cdot \sigma(a^4 - a^2 + 1).$$

Kako je $N$ neparan broj, jedan od faktora s desne strane mora biti neparan. Ali, ako su $m$ i $\sigma(m)$ oba neparni tada je $m$ potpuni kvadrat. Kada bi $m$ i $\sigma(m)$ bili neparni, a $m$ ne bi bio potpuni kvadrat, tada bismo djelitelje od $m$ mogli složiti u parove $d$,$m/d$. Elementi svakog od tih parova su neparni brojevi pa je njihova suma paran broj iz čega slijedi da je $\sigma(m)$ paran broj što je kontradikcija. Ovo implicira da je ili $a^2 + 1$, ili $a^4 - a^2 + 1$ potpuni kvadrat. Ali, $a^2 < a^2 + 1 < (a + 1)^2$ i $(a^2 - 1)^2 < a^4 - a^2 + 1 < (a^2)^2$ pa nijedan ne mogu biti potpuni kvadrat, što je kontradikcija.

Slijedi, ne postoji neparan savršen broj oblika $n^n + 1$. Dakle, 28 je jedini savršen broj željenog oblika. □

## 2.1 Neparni savršeni brojevi?

Još nije pronađen neparan savršen broj, ali nije ni dokazano da ne postoji. Iako se ne zna postoje li, prikupljeno je dosta zanimljivih rezultata koji se odnose na strukturu neparnih savršenih brojeva. Trenutno znamo da neparni savršeni broj ne može imati manje od 8 različitih prostih faktora i da ne može biti manji od $100^{300}$. Iako nas ovo navodi na zaključak da ne postoje neparni savršeni brojevi, samo dokaz o njihovom nepostojanju možemo smatrati konačnim. Pored toga što su ustanovljeni neki uvjeti koje neparan savršen broj mora zadovoljiti, još nitko nije pronašao takav broj, unatoč velikim potragama pomoću modernih superračunala.

Godine 1953., J. Touchard iz Francuske ustanovio je da $N$ mora biti oblika $12k + 1$ ili $36k + 9$ (Teorem 2.3). Pedeset godina kasnije W. Chau iz tvrtke Soft Techies iz New

Jersey-a pokazao je da, ako je $N$ oblika $36k+9$, onda mora biti i oblika $108k+9$, $108k+35$ ili $324k+81$, mora imati barem 8 različitih prostih faktora, a ako $N$ ima točno 8 različitih faktora, onda najmanji faktor mora biti oblika $p^{4a+1}n^2$, gdje je $p$ prost broj oblika $4m+1$, $a \geq 0$, $p \nmid n$.

Godine 1991., R. P. Brent, G. L. Coher i H. J. J. te Riele pokazali su da neparan savršen broj mora biti veći od $100^{300}$, a 1998. G. L. Coher sa Tehnološkog sveučilišta u Sidney-u i P. Hagis Jr. sa sveučilišta Temple dokazali su da najveći prosti faktor neparnog savršenog broja prelazi vrijednost $10^6$. Tri godine ranije D. E. Iannucci je pokazao da drugi prosti faktor prelazi vrijednost $10^4$, a da je treći prosti faktor veći od 100.

2000. godine, Paul A. Weiner sa sveučilišta St. Mary iz Minesote, ustanovio je da, ako je $3\sigma(n) = 5n$, za neki cijeli broj $n$, onda je $5n$ neparan savršen broj.

Ipak, postoji snažno uvjerenje u matematičkoj zajednici da ne postoji neparan savršen broj.

Prema Eulerovom teoremu, potraga za savršenim brojevima svodi se na pronalazak prostih brojeva oblika $2^m - 1$ pa je takve brojeve potrebno pažljivije proučiti. U idućem poglavlju ćemo analizirati ove brojeve.

# 3 Mersenneovi prosti brojevi

Postalo je tradicionalno nazivati brojeve koji su oblika $M_n = 2^n - 1$, $n \geq 1$, Mersenneovim brojevima, u čast netočne, ali intrigirajuće pretpostavke koju je Mersenne izrekao u vezi njihove prostosti. Oni Mersenneovi brojevi koji su prosti se zovu Mersenneovi prosti brojevi.

Kao što smo vidjeli, određivanje Mersenneovih prostih brojeva, te potraga za novim savršenim brojevima se može suziti do slučaja u kojem je sam eksponent $n$ prost broj. Kada bismo znali da postoji beskonačno mnogo prostih $p$ za koje je $M_p$ prost broj, onda bismo znali i da postoji beskonačno mnogo (parnih) savršenih brojeva. Nažalost, ovo je još jedan od poznatih neriješenih problema.

U uvodu svoje *"Cogitata Physico-Mathematica"* 1644. godine, Mersenne je tvrdio da je $M_p$ prost za vrijednosti $p$ =2, 3, 5, 7, 13, 17, 19, 31, 67, 127 i 257, a složen za sve druge proste brojeve $p \leq 257$. Drugim matematičarima je bilo jasno da Mersenne nije mogao testirati prostost svih brojeva koje je najavio, ali nisu mogli ni oni. Je li Mersenneu bio dostupan još neki, ostalima nepoznat, teorem ili se oslanjao samo na svoje pogađanje, ostaje nepoznato. Priznao je: *"Da bi se utvrdilo je li broj s* 15 *ili* 20 *znamenaka prost, svo vrijeme ovog svijeta ne bi bilo dovoljno"*. Broj $M_{127}$ ima 39 znamenaka, a broj $M_{257}$ 78 znamenaka.

Skoro 150 godina, Cataldijev $M_{19}$ bio je najveći Mersenneov prost broj. Onda je Euler (1732. godine) dokazao da je $M_{31}$ prost broj, istražujući sve proste brojeve do 46339 kao moguće dijelitelje. Brojevi $M_{67}$, $M_{127}$ i $M_{257}$ ostali su van dometa njegovih mogućnosti. $M_{31}$ je bio najveći poznati prost broj idućih 100 godina i pridonio je pronalasku 9. savršenog broja:

$$P_9 = 2^{30}(2^{31} - 1) = 2305843008139952128.$$

Euler, jedan od najvećih matematičara svih vremena, nije bio imun na pogrešne pretpostavke o savršenim brojevima. Pisao je:

> *"Riskiram pretpostaviti da, osim zabilježenih slučajeva [Euler je ranije spomenuo* 11, 23, 29, 37, 43, 73, 83*], svi prosti brojevi manji od* 50, *i zapravo manji od* 100, *čine* $2^{n-1}(2^n - 1)$ *savršenim brojem. Vrijednosti broja n:* 1, 2, 3, 5, 7, 13, 17, 19, 31, 41, 47 *daju savršene brojeve."*

Euler je 1753. godine utvrdio osobnu grešku za $n = 41$ i $n = 47$.

Tek je 1947., nakon silnog posla uslijed nepouzdanih kalkulatora, završeno ispitivanje prostosti, odnosno složenosti Mersenneovih $M_p$ za zadnjih 55 prostih brojeva, $p \leq 257$. Danas znamo da je Mersenne napravio 5 grešaka, iako je nevjerojatno da je trebalo 300 godina da se greške isprave. Prva je greška pronađena kada su Pervusin (1883. godine) i Seelhof (1886. godine) neovisno dokazali da je $M_{61}$ prost broj. Kada je Cole (1903. godine) otkrio faktore broja $M_{67}$, Mersenneovi branitelji su tvrdili da je 67 greška u tiskanju (da je trebalo pisati 61).

Prvobitna je pretpostavka bila da, ako je $m$ prost broj, onda je i $2^m - 1$ prost broj. Kao što smo vidjeli, 1536. godine Hudalrichus Regius je otkrio da to nije točno ($2^{11} - 1 =$

$2047 = 23 \cdot 89$).

Godine 1876., Lucas je dokazao da je je $M_{67}$ složen, iako nije prikazao faktore. To je uradio američki matematičar Frank Nelson Cole, 1903. godine:

$$2^{67} - 1 = 193707721 \cdot 761838257287.$$

Priča se da je Cole proveo svoja nedjeljna popodneva, u periodu od 20 godina, u pronalaženju ovih faktora.

1883. godine I. M. Pervusin je pokazao da je $M_{61} = 2^{61} - 1$ prost broj, što je Mersenne propustio. R. E. Powers je 1911. i 1914. godine otkrio da su $2^{89} - 1$ i $2^{107} - 1$ prosti brojevi. 1922. godine M. Kraitchik je dokazao da je $M_{257} = 2^{257} - 1$ složen broj. Ironično, 1936. New York Herald Tribune je pogrešno objavio da je Samuel Krieger iz Chicaga pokazao da je $2^{257} - 1$ prost. Pokazano je, 1931. i 1947., koristeći ručni kalkulator, a zatim i potvrđeno 1952. godine, pomoću računala, da je $2^{257} - 1$ ipak složen.

Mersenneovi prosti brojevi se proređuju kako raste vrijednost $p$. Godine 1963., Donald B. Grillies sa sveučilišta Illinois zaključio je da postoje dva prosta $p$ u intervalu $[n,\ 2n]$. Zanimljivo, njegov zaključak je u suglasnosti sa opaženom frekvencijom prostih $p$. Slaže se i s Eberhartovim zaključkom da za $i$-ti Mersenneov prost broj $M_p$, $p \approx 1.5^i$. Na primjer, $i = 23$, $p \sim 1.5^{23} \sim 11223$, što nije daleko od stvarne vrijednosti $p = 11213$.

Moderna su računala postala moćno sredstvo u pronalaženju velikih Mersenneovih prostih brojeva. Idućih 5 velikih $M_p$ gdje je $p = 521, 607, 1279, 2203$ i 2281 otkriveni su 1952. godine.

Do 1994. godine otkrivena su 33 Mersenneova prosta broja. Mersenneov prost broj koji je 33. po redu otkrio je David Slowinski iz Harwell Laboratory u Engleskoj 1993. godine. Superračunalu Cray C90 je trebalo $7.2h$ da otkrije njegovu prostost. Njegov decimalni zapis ima 258 716 znamenaka. Iduća dva također je otkrio Slowinski.

Najveći prosti broj do 1999., $M_{6972593}$, otkrili su N. Hajrawala, G. Woltman i S. Kurowski, a ima 2 098 960 znamenaka. Dakle, u 1999. najveći savršeni broj je $2^{6972592}(2^{6972593} - 1)$ koji ima 4 197 919 znamenaka.

$M_{25964951}$ otkrio je Martin Nowak 2005. godine, očni kirurg iz Njemačke. Sastoji se od 7 816 230 znamenaka. Računanje na njegovom računalu od 1GHz, Pentium 4, trajalo je 50 dana.

Danas je najpoznatiji Mersenneov prost broj $2^{30402457}$ koji ma 9 152 052 znamenaka. Otkrili su ga 2005. godine C. Cooper i S. R. Boone sa centralnog sveučilišta države Missouri.

Godine 1989., P. T. Bateman i J. L. Selfridge sa sveučilišta sjevernog Illinoisa i S. S. Wagstaff Jr. sa sveučilišta Purdue, iznijeli su zanimljivu pretpostavku o Mersenneovim prostim brojevima:
Ako su sljedeće dvije tvrdnje o neparnim prostim brojevima $p$ točne, onda je točna i treća:

- $p = 2^k \pm 1$ ili $p = 4^k \pm 3$
- $M_p$ je prost
- $(2^p + 1)/3$ je prost.

Na primjer, $p = 7$, $7 = 2^3 - 1$ i $(2^7 + 1)/3 = 43$ je prost. Kao što znamo, $M_7$ je prost. Pretpostavka je točna za $p = 7$. Zapravo, dokazano je da je točno za sve $p < 100000$.

## 3.1 Broj znamenaka broja $M_p$

Lako se može predodrediti broj znamenaka Mersenneovog broja $M_p$. Najprije, podsjetimo se da je svaki neparni prost $p$ oblika $4k + 1$ ili $4k + 3$. Ako je $p = 4k + 1$, onda $2^p = 2^{4k+1} = (2^4)^k \cdot 2 \equiv 6^k \cdot 2 \equiv 6 \cdot 2 \equiv 2 \pmod{10}$. Isto tako, ako je $p = 4k+3$, onda vrijedi $2^p \equiv 8 \pmod{10}$. Dakle, $2^p = M_p + 1$ završava s 2 ili 8. Posljedično, $M_p$ završava s 1 ili 7 te ima isti broj znamenaka kao $2^p$.

Pri izračunavanju broja znamenaka u $2^p$, primijetimo da je $\log 2^p = p \cdot \log 2$. Dakle, broj znamenaka u $2^p$ jednak je:

$$\lceil p \cdot \log 2 \rceil.$$

**Primjer 3.1.** $M_{25964951}$ sadrži $\lceil M_{25964951} \log 2 \rceil = \lceil 0.301029995664 \cdot 25964951 \rceil = 7816290$ znamenaka, kao što je i očekivano.

Zanimljivo, najveći složeni Mersenneov broj je $M_p$ sa $p = 39051 \cdot 2^{6001} - 1$ kojeg je otkrio W. Keller 1987.godine.

Tablica 1 sadrži 44 poznata $M_p$, broj znamenaka svakog, broj znamenaka odgovarajućeg savršenog broja $2^{p-1}M_p$, godinu otkrića $M_p$ te ime pronalazača.

## 3.2 Mersenneov broj - prost ili složen?

Postoji više uvjeta za testiranje prostosti Mersenneovih brojeva. Sljedeći teorem govori o mogućem prostom faktoru Mersenneovog broja $M_p$.

**Teorem 3.1** (Euler)**.** Neka je $p = 4k+3$ prost broj, gdje je $k > 1$. Tada je $2p+1$ prost broj ako i samo ako je $2^p \equiv 1 \pmod{2p + 1}$. □

Iz teorema slijedi da ako su $p = 4k + 3$ i $2p + 1$ prosti brojevi, gdje je $k > 1$, onda $2p + 1 | M_p$ i $M_p$ je složen broj.

Sljedeći primjer prikazuje zanimljivu primjenu ovog teorema. Predložio ga je kao problem 1988. godine David Grannis iz Vancouvera, British Columbia.

**Primjer 3.2.** Pronađi faktor Mersenneovog broja $M_{1000151}$.

*Rješenje:* $p = 1000151 = 4 \cdot 257037 + 3$, kao i $2p + 1 = 2000303$ su prosti brojevi. Dakle, prema Teoremu 3.1, $2000303 | M_{1000151}$.

Neka je $n$ prirodan broj. Broj prirodnih brojeva u nizu $1, 2, \ldots n$ koji su relativno prosti s $n$ označava se s $\varphi(n)$. Ovim je definirana funkcija $\varphi : \mathbb{N} \to \mathbb{N}$ koja se naziva Eulerova funkcija.

**Teorem 3.2** (Euler)**.** Neka je $a$ cijeli broj i $n$ prirodan broj. Ako su brojevi $a$ i $n$ relativno prosti, tada je $a^{\varphi(n)} \equiv 1 \pmod{n}$. □

| Poredak | $p$ | Broj znamenaka u $M_p$ | Broj znamenaka u $2^{p-1}M_p$ | Godina | Pronalazač(i) |
|---|---|---|---|---|---|
| 1 | 2 | 1 | 1 | nepoznata | Pitagorejci |
| 2 | 3 | 1 | 2 | nepoznata | Pitagorejci |
| 3 | 5 | 2 | 3 | nepoznata | Pitagorejci |
| 4 | 7 | 3 | 4 | nepoznata | Pitagorejci |
| 5 | 13 | 4 | 8 | 15. st. | H. Regius |
| 6 | 17 | 6 | 10 | 1588. | P. A. Cataldi |
| 7 | 19 | 6 | 12 | 1588. | P. A. Cataldi |
| 8 | 31 | 10 | 19 | 1772. | L. Euler |
| 9 | 61 | 19 | 37 | 1883. | I. M. Pervushin |
| 10 | 89 | 27 | 54 | 1911. | R. E. Powers |
| 11 | 107 | 33 | 65 | 1914. | R. E. Powers, E. Fauquembergue |
| 12 | 127 | 39 | 77 | 1876. | E. Lucas |
| 13 | 521 | 157 | 314 | 1952. | D. H. Lehmer |
| 14 | 607 | 183 | 366 | 1952. | D. H. Lehmer |
| 15 | 1279 | 386 | 770 | 1952. | D. H. Lehmer |
| 16 | 2203 | 664 | 1327 | 1952. | D. H. Lehmer |
| 17 | 2281 | 687 | 1373 | 1952. | D. H. Lehmer |
| 18 | 3217 | 969 | 1937 | 1957. | H. Riesel |
| 19 | 4253 | 1281 | 2561 | 1961. | A. Hurwitz |
| 20 | 4423 | 1332 | 2663 | 1961. | A. Hurwitz |
| 21 | 9689 | 2917 | 5834 | 1963. | D. B. Gillies |
| 22 | 9941 | 2993 | 5985 | 1963. | D. B. Gillies |
| 23 | 11 213 | 3376 | 6751 | 1963. | D. B. Gillies |
| 24 | 19 937 | 6002 | 12 003 | 1971. | B. Tuckerman |
| 25 | 21 701 | 6533 | 13 066 | 1978. | L. Nickel, C. Noll |
| 26 | 23 209 | 6987 | 13 973 | 1979. | C. Noll |
| 27 | 44 497 | 13 395 | 26 790 | 1979. | D. Slowinski, H. Nelson |
| 28 | 86 243 | 25 962 | 51 924 | 1983. | D. Slowinski |
| 29 | 110 503 | 33 265 | 66 530 | 1988. | W. N. Colquitt, L. Welch Jr. |
| 30 | 132 049 | 39 751 | 79 502 | 1983. | D. Slowinski |
| 31 | 216 091 | 65 050 | 130 100 | 1985. | D. Slowinski |
| 32 | 756 839 | 227 832 | 455 663 | 1992. | D. Slowinski, P. Gage |
| 33 | 859 433 | 258 716 | 517 430 | 1993. | D. Slowinski, P. Gage |
| 34 | 1 257 787 | 378 632 | 757 263 | 1996. | D. Slowinski, P. Gage |
| 35 | 1 398 269 | 420 921 | 841 842 | 1996. | J. Armengaud, G. Woltman |
| 36 | 2 976 221 | 895 932 | 1 791 864 | 1997. | G. Spence, G. Woltman |
| 37 | 3 021 377 | 900 526 | 1 819 050 | 1998. | R. Clarkson i sur. |
| 38 | 6 972 593 | 2 098 960 | 4 197 919 | 1999. | N. Hajrawala i sur. |
| 39 | 13 466 917 | 4 053 946 | 8 107 892 | 2001. | M. Cameron |
| 40 | 20 996 011 | 6 320 430 | 12 640 858 | 2003. | M. Shafer |
| 41 | 24 036 583 | 7 235 733 | 14 471 465 | 2004. | J. Findley |
| 42 | 25 964 951 | 7 816 230 | 15 632 458 | 2005. | M. Novak |
| 43 | 30 402 457 | 9 152 052 | 18 304 103 | 2005. | C. Cooper, S. R. Boone |
| 44 | 32 582 657 | 9 808 358 | 19 616 715 | 2006. | C. Cooper, S. R. Boone |

Tablica 1: 44 poznata Mersenneova prosta broja

Prije nego što predstavimo test prostosti za Mersenneove proste brojeve, pripremit ćemo put s Lemom 3.1, ali najprije, promotrimo primjer. Neka su $a$ i $n$ relativno prosti prirodni brojevi. Tada prema Teoremu 3.2, $a^{\varphi(n)} \equiv 1 \pmod{n}$. Međutim, često mogu postojati eksponenti $k$ manji od $\varphi(n)$ takvi da $a^k \equiv 1 \pmod{n}$, kao što pokazuje sljedeći primjer.

**Primjer 3.3.** Neka je $n = 12$. Tada je $\varphi(n) = \varphi(12) = 4$. Najmanji ostatci $a$ modulo 12 koji su relativno prosti s 12 su 1, 5, 7, i 11. Prema Eulerovom teoremu, $a^{\varphi(n)} = a^4 \equiv 1 \pmod{12}$. Ali, $1^2 \equiv 1 \pmod{12}$, $5^2 \equiv 1 \pmod{12}$, $7^2 \equiv 1 \pmod{12}$ i $11^2 \equiv 1 \pmod{12}$. Dakle, $k = 2$ jest najmanji pozitivan eksponent takav da je $a^k \equiv 1 \pmod{12}$. (Primijetimo da $k|\varphi(n)$).

Općenitije, imamo sljedeći rezultat.

**Lema 3.1.** Neka su $a$, $m$ i $n$ pozitivni cijeli brojevi za koje vrijedi $(a, n) = 1$ i $k$ je najmanji pozitivan cijeli broj takav da je $a^k \equiv 1 \pmod{n}$. Tada je $a^m \equiv 1 \pmod{n}$ ako i samo ako $k$ dijeli $m$.

*Dokaz.* Pretpostavimo $a^k \equiv 1 \pmod{n}$. Prema Euklidovom algoritmu, $m = kq + r$ za neke cijele brojeve $q$ i $r$, gde je $0 \leq r < k$. Tada vrijedi

$$a^m = a^{kq+r} = (a^k)^q \cdot a^r.$$

Kako je $a^k \equiv 1 \pmod{n}$ i $a^m \equiv 1 \pmod{n}$ slijedi

$$\begin{aligned} 1 &\equiv 1^q \cdot a^r \pmod{n} \\ 1 &\equiv a^r \pmod{n}, \end{aligned}$$

tj.

$$a^r \equiv 1 \pmod{n}, \text{ gdje je } 0 \leq r < k.$$

Kada bi vrijedilo $r > 0$ to bi bilo u kontradikciji s pretpostavkom da je $k$ najmanji. Slijedi $r = 0$ i $m = kq$. Prema tome, $k|m$.

Obrnuto, neka $k|m$, tj. $m = kq$ za neki cijeli broj $q$. Tada vrijedi

$$\begin{aligned} a^m = a^{kq} &= (a^k)^q \\ &\equiv 1^q \equiv 1 \pmod{n} \end{aligned}$$

iz čega zaključujemo $a^m \equiv 1 \pmod{n}$ ako i samo ako $k|m$. □

Ova lema za neposrednu posljedicu ima sljedeći korolar.

**Korolar 3.1.** Neka su $a$ i $n$ relativno prosti pozitivni cijeli brojevi i neka je $k$ najmanji pozitivan cijeli broj takav da $a^k \equiv 1 \pmod{n}$. Tada $k$ dijeli $\varphi(n)$. □

Sada možemo iskazati test prostosti Mersenneovih brojeva.

**Teorem 3.3** (Fermat, 1640.)**.** Ako je $p$ neparan prost broj, svaki prost faktor od $M_p$ je oblika $2kp + 1$, gdje je $k$ pozitivan cijeli broj.

*Dokaz.* Neka je $q$ prost faktor od $M_p$. Očito je $q$ neparan. Tada $q|M_p$ pa vrijedi $2^p \equiv 1 \pmod{q}$. Neka je $k$ najmanji cijeli broj takav da vrijedi $2^k \equiv 1 \pmod{q}$. Tada, prema Lemi 3.1, $k|p$. Ali, $k \neq 1$ jer kada bi vrijedilo $k = 1$, bilo bi $2^1 \equiv 1 \pmod{q}$ što znači $q = 1$, a to je u kontradikciji s pretpostavkom. Dakle, $k = p$ što znači $p$ je najmanji pozitivan cijeli broj takav da vrijedi $2^p \equiv 1 \pmod{q}$.

Prema malom Fermatovom teoremu, $2^{q-1} \equiv 1 \pmod{q}$ pa prema Lemi 8.2 $p|q - 1$. Neka je $q - 1 = pm$ za neki pozitivan cijeli broj $m$. Kako je $q - 1$ paran, a $p$ neparan broj, $m$ također mora biti paran broj, na primjer $m = 2k$ za neki pozitivan cijeli broj $k$. Tada je $q - 1 = 2pk$ tj. $q = 2pk + 1$.

Dakle, ako je $p$ neparan broj, svaki prost faktor od $M_p$ je oblika $2kp + 1$. □

Promotrimo sada primjer koji će nam biti koristan.

**Primjer 3.4.** Dokažite da svaki složen broj $n$ ima prosti faktor $p \leq \sqrt{n}$.

*Rješenje.* Neka je $p$ najmanji djelitelj od $n$ koji je veći od 1. Tada je $p$ očito prost i postoji $m \in \mathbb{N}$ takav da je $n = p \cdot m$. Budući da je $m \geq p$, dobivamo da je $p \leq \sqrt{n}$. □

Sljedeća dva primjera ilustriraju Fermatov test.

**Primjer 3.5.** Pokažite da je $M_{11}$ složen broj.

*Rješenje.* $M_{11} = 2^{11} - 1 = 2047$. Prema Teoremu 3.3, svaki prost faktor od $M_{11}$ je oblika $22k+1$. Ako je $M_{11}$ složen broj, onda prema Primjeru 3.4 mora imati prost faktor $\leq \lfloor\sqrt{M_{11}}\rfloor$, tj. $\leq 45$. Postoji točno jedan prost broj oblika $22k + 1$ i $\leq 45$. To je broj 23. Kako $23|M_{11}$, $M_{11}$ je složen broj. □

**Primjer 3.6.** Provjeri je li $M_{19}$ prost broj.

*Rješenje.* $M_{19} = 2^{19} - 1 = 524287$. Ako je $M_{19}$ složen broj, prema Primjeru 3.4 mora imati prost faktor $\leq \lfloor\sqrt{M_{19}}\rfloor$, tj. $\leq 724$. Prema Teoremu 3.3, svaki prost faktor od $M_{19}$ je oblika $38k + 1$ i $\leq 725$. Takvi prosti brojevi su 191, 229, 419, 457, 571 i 647. Nijedan od njih ne dijeli $M_{19}$ pa zaključujemo da je $M_{19}$ prost broj. □

## 3.3 Lucas - Lehmer test

U ovome poglavlju ćemo promotriti učinkovit test prostosti za Mersenneove proste brojeve, kojeg je razvio Lucas 1877. godine, a doradio 1930. američki matematičar Derrick H. Lehmer. Lucas je uporabio svoju verziju kako bi utvrdio prostost broja $M_{127}$, najvećeg Mersenneovog broja koji je bio provjeren bez pomoći stroja za računanje.

Ovaj test, koji se koristi od 1930. godine za dokazivanje prostosti Mersenneovih brojeva, temelji se na redoslijedu brojeva 4, 14, 194, 37 634, 1 416 317 954, ...

Definiran je rekurzivno:

$$\begin{aligned} s_1 &= 4 \\ s_k &= s_{k-1}^2 - 2,\ k \geq 2. \end{aligned}$$

Prema testu, $M_p$ je prost ako i samo ako $s_{p-1} \equiv 0 \pmod{M_p}$, gdje je $p$ neparan prost broj. Lehmer je uz pomoć ovog testa dokazao prostost brojeva $M_{521}$, $M_{607}$, $M_{1279}$, $M_{2203}$ i $M_{2281}$ koristeći računalo SWAC (*Standards Western Automatic Computer*). Također je, koristeći SWAC, potvrdio da je broj $M_{257}$ složen. Računalu je trebalo samo 48 sekundi. Bio je to zadatak za koji je 20 godina ranije trebalo 700 sati rada.

Test je formalno predstavljen u sljedećem teoremu.

**Teorem 3.4** (Lucas-Lehmer Test)**.** Neka je $p \geq 3$. Mersenneov broj $M_p$ je prost ako i samo ako $S_{p-1} \equiv 0 \pmod{M_p}$, gdje je $S_k$ najmanji ostatak modulo $M_p$ definiran rekurzivno s

$$\begin{aligned} S_1 &= 4 \\ S_k &= S_{k-1}^2 - 2 \pmod{M_p},\ k \geq 2. \end{aligned}$$

Sljedeća dva primjera ilustriraju ovaj test.

**Primjer 3.7.** Koristeći Lucas-Lehmer test, pokažite da je $M_{13}$ prost broj.

*Dokaz.* $p = 13$ i $M_{13} = 2^{13} - 1 = 8191$. Ispišimo $S_2$ do $S_{13}$ modulo $M_{13}$:

$$\begin{aligned} S_2 &\equiv 4^2 - 2 \equiv 14 \pmod{M_{13}} \\ S_3 &\equiv 14^2 - 2 \equiv 194 \pmod{M_{13}} \\ S_4 &\equiv 194^2 - 2 \equiv 4870 \pmod{M_{13}} \\ S_5 &\equiv 4870^2 - 2 \equiv 3953 \pmod{M_{13}} \\ S_6 &\equiv 3953^2 - 2 \equiv -2221 \pmod{M_{13}} \\ S_7 &\equiv 2221^2 - 2 \equiv 1857 \pmod{M_{13}} \\ S_8 &\equiv 1857^2 - 2 \equiv 36 \pmod{M_{13}} \\ S_9 &\equiv 36^2 - 2 \equiv 1294 \pmod{M_{13}} \\ S_{10} &\equiv 1294^2 - 2 \equiv 3470 \pmod{M_{13}} \\ S_{11} &\equiv 3470^2 - 2 \equiv 128 \pmod{M_{13}} \\ S_{12} &\equiv 128^2 - 2 \equiv 0 \pmod{M_{13}}. \end{aligned}$$

Kako je $S_{12} \equiv 0 \pmod{M_{13}}$, $M_{13}$ je prost broj. □

**Primjer 3.8.** Koristeći Lucas-Lehmer test, pokažite da $M_{11}$ nije prost broj.

*Dokaz.* Kao i u prošlom primjeru, računamo $S_2$ do $S_{10}$ modulo $M_{11}$.

$$\begin{aligned}
S_2 &\equiv 14 \pmod{M_{11}} \\
S_3 &\equiv 194 \pmod{M_{11}} \\
S_4 &\equiv 788 \pmod{M_{11}} \\
S_5 &\equiv 701 \pmod{M_{11}} \\
S_6 &\equiv 119 \pmod{M_{11}} \\
S_7 &\equiv -170 \pmod{M_{11}} \\
S_8 &\equiv 240 \pmod{M_{11}} \\
S_9 &\equiv 282 \pmod{M_{11}} \\
S_{10} &\equiv 1736 \pmod{M_{11}}.
\end{aligned}$$

Kako $S_{10} \not\equiv 0 \pmod{M_{11}}$, $M_{11}$ nije prost broj. □

Do danas, najveći poznati prost broj koji nije Mersenneov prost broj jest:

$$27653 \cdot 2^{9167433} + 1,$$

kojeg je 2005. godine otkrio Samuel Yates, a sadrži 2 759 677 znamenaka.

Sljedeći problem predložio je Jeffrey Shallit sa Dartmouth Collegea, New Hampshire 1989. godine.

**Primjer 3.9.** Dokaži da je $\sigma(n)$ potencija broja 2 ako i samo ako je $n$ produkt različitih Mersenneovih prostih brojeva.

*Rješenje.* Neka je $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ rastav na proste faktore broja $n$. Tada vrijedi:

$$\sigma(n) = \prod_{i=1}^{k} \frac{p_i^{e_i+1} - 1}{p_i - 1}.$$

Pretpostavimo da je to potencija broja 2. Neka je $p^e$ proizvoljna prosta potencija u rastavu na proste faktore od $n$. Tada

$$\sigma(p^e) = \tfrac{p^{e+1}-1}{p-1} = p^e + \cdots + p + 1$$

mora biti potencija broja 2 pa $p$ i $e$ moraju biti neparni brojevi.

Neka je $e = 2s + 1$. Tada je

$$\begin{aligned}
\sigma(p^e) &= p^{2s+1} + \cdots + p + 1 \\
&= (p+1)(p^{2s} + p^{2s-2} + \cdots + p^2 + 1). \qquad (5)
\end{aligned}$$

Kako $(p+1) | \sigma(p^e)$ i $\sigma(p^e)$ je potencija broja 2, $p+1$ mora biti potencija broja 2 iz čega slijedi da je $p$ Mersenneov prost broj.

Preostaje pokazati $e = 1$ tj. $s = 0$. Pretpostavimo da je $s > 0$. Prema (5), kako je

$p^{2s} + p^{2s-2} + \cdots + p^2 + 1$ potencija broja 2 i $p$ je neparan broj, $s$ mora biti neparan broj. Uzmimo $s = 2t + 1$. Tada

$$\begin{aligned} p^{2s} + p^{2s-2} + \cdots + p^2 + 1 &= p^{4t+2} + p^{4t} + \cdots + p^2 + 1 \\ &= (p^2 + 1)(p^{4t} + p^{4t-4} + \cdots + p^4 + 1) \end{aligned}$$

jest potencija broja 2, pa $p^2 + 1$ mora biti potencija broja 2. Dakle, $4|(p^2 + 1)$ tj. $p^2 \equiv -1 \pmod 4$ što je kontradikcija. Dakle, $s = 0$ i $e = 1$. Posljedica ovoga jest da je $n$ produkt različitih Mersenneovih prostih brojeva.

Obratno, neka je $n = \prod_i p_i$ produkt Mersenneovih prostih brojeva $p_i = 2^{m_i} - 1$. Tada je

$$\sigma(n) = \prod_i \sigma(p_i) = \prod_i p_i + 1 = \prod_i 2^{m_i} = 2^{\sum_i m_i}$$

potencija broja 2. □

## 3.4 Pascalov trokut i Mersenneovi brojevi

Temeljno svojstvo Pascalovog trokuta je da svaki njegov redak čine brojevi koji predstavljaju koeficijente u razvoju odgovarajuće potencije binoma po binomnom poučku. Na primjer,

$$(a + b)^4 = 1 \cdot a^4 + 4 \cdot a^3 b + 6 \cdot a^2 b^2 + 4 \cdot ab^3 + 1 \cdot b^4.$$

Koeficijenti 1, 4, 6, 4, 1 odgovaraju 4. retku Pascalovog trokuta.

$$\begin{array}{ccccccccccc} & & & & & 1 & & & & & \\ & & & & 1 & & 1 & & & & \\ & & & 1 & & 2 & & 1 & & & \\ & & 1 & & 3 & & 3 & & 1 & & \\ & 1 & & 4 & & 6 & & 4 & & 1 & \\ 1 & & 5 & & 10 & & 10 & & 5 & & 1 \\ & 1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1 \\ 1 & & 7 & & 21 & & 35 & & 35 & & 21 & & 7 & & 1 \end{array}$$

Slika 3: Pascalov trokut

**Definicija 3.1.** Binomni koeficijent je izraz oblika

$$\binom{n}{k} = \begin{cases} \frac{n(n-1)\cdots(n-k+1)}{k!}, & k, n \in \mathbb{N}_0, \quad k \leq n \\ 0 & , \textit{inače.} \end{cases}$$

Binomni koeficijenti $\binom{n}{k}$ za $n \in \mathbb{N}_0$, $k = 0, 1, \ldots, n$ elementi su Pascalovog trokuta.

Postoji zanimljiva veza između Mersenneovih brojeva i Pascalovog trokuta. Sljedeći teorem pokazuje da svaki broj u retku $n$, gdje je $n$ Mersenneov broj, jest neparan. Dokaz je pružio Rade M. Dačić iz Beograda.

**Teorem 3.5.** Prirodan broj $n$ je Mersenneov broj ako i samo ako je svaki binomni koeficijent $\binom{n}{r}$ neparan, pri čemu je $0 \leq r < n$.

*Dokaz.* Neka je $n = 2^s - 1$, gdje je $s \geq 0$. Tada

$$\begin{aligned}\binom{n}{r} &= \binom{2^s - 1}{r} \\ &= \frac{2^s - 1}{1} \cdot \frac{2^s - 2}{2} \cdots \frac{2^s - r}{r}. \end{aligned} \tag{6}$$

Neka je $1 \leq i \leq r$ i $i = 2^a b$, pri čemu $0 \leq a \leq s$ i $b$ je neparan broj. Tada

$$\frac{2^s - i}{i} = \frac{2^s - 2^a b}{2^a b} = \frac{2^{s-a} - b}{b}$$

što je kvocijent neparnih cijelih brojeva. Dakle, svaki faktor u (6) jest količnik neparnih cijelih brojeva. Slijedi da je onda i produkt neparan cijeli broj. Dakle, svaki unos $\binom{n}{r}$ u retku $n$ je neparan.

Obrnuto, pretpostavimo da je svaki binomni koeficijent $\binom{n}{r}$ u retku $n$ neparan. Neka je $n$ neparan, ali ne i Mersenneov broj. Tada je $2^{m-1} < n < 2^m$ za neki prirodan broj $m$. Slijedi $n = 2^{m-1} + 2k + 1$, pri čemu $0 \leq k \leq 2^{m-2} - 1$. Neka je $r = 2k + 2$. Tada

$$\begin{aligned}\binom{n}{r} &= \binom{n}{r-1} \cdot \frac{n - r + 1}{r} \\ &= s \cdot \frac{2^{m-1}}{2k+2} \\ &= s \cdot \frac{2^{m-2}}{k+1}\end{aligned}$$

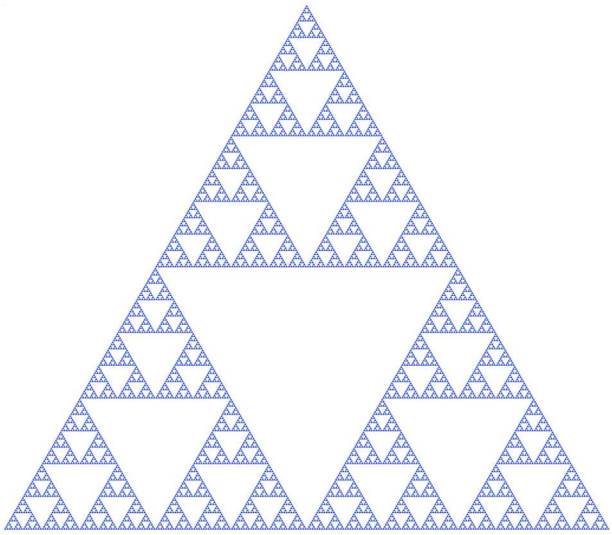
gdje je $s$ cijeli broj. Ako je $k + 1 < 2^{m-2}$, $\binom{n}{r}$ je paran broj. Ako je $k + 1 = 2^{m-2}$, tada je $\binom{n}{r} = 0$ i dalje paran cijeli broj. Oba slučaja su u kontradikciji s pretpostavkom pa $n$ mora biti Mersenneov broj. □

### 3.4.1 Pascalov trokut i parni savršeni brojevi

Pretpostavimo da smo zamijenili svaki parni broj u Pascalovom trokutu s bijelom točkom (0), a svaki neparan broj s plavom točkom (1). Slika 4 pokazuje rezultat, prelijepi binarni obrazac, Pascalov binarni trokut.

Prema Teoremu 3.5, ako je $n$ Mersenneov prost broj, onda redak $n$ sadrži samo plave točke. Postoje 4 takva retka $n$, gdje $1 \leq n \leq 100$. To su retci 1, 3, 7 i 31.

Osim estetske ljepote, binarni trokut sadrži još neke zanimljivosti. Da bi se to vidjelo, trebaju se uzeti u obzir centralno postavljeni trokuti $\bigtriangledown_n$ okrenuti ka dolje, koji imaju baze



Slika 4: Pascalov binarni trokut

u redu $2^n$, gdje je $n \geq 1$. Budući da baza $\bigtriangledown_n$ sadrži $2^n - 1$ nula, broj nula unutar $\bigtriangledown_n$ jednak je

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

što je savršen broj ako je $2^n - 1$ Mersenneov prost broj.

Na primjer, baza $\bigtriangledown_4$ leži u retku 34 i sadrži $2^5 - 1 = 31$ nulu. Broj nula unutar $\bigtriangledown_4$ jednak je:

$$31 + 30 + \cdots + 2 + 1 = \tfrac{31 \cdot 32}{2} = 496,$$

što je treći savršeni broj.

Općenito, svaki broj $N = 2^{n-1} \cdot (2^n - 1)$ reprezentiran je s $\bigtriangledown_n$. Posljedično, svaki parni savršeni broj $N = 2^{p-1} \cdot (2^p - 1)$ je reprezentiran s $\bigtriangledown_p$, gdje je $2^p - 1$ prost broj. Drugim riječima, parni savršeni brojevi reprezentirani su geometrijskim podnizom niza $\{\bigtriangledown_n\}$ , kao što je to uočio Alan L. Brown iz South Orange, New Jersey, 1956. godine.

# Zaključak

Proučavanje savršenih brojeva i potraga za istima predstavlja izazov matematičarima već tisućama godina. Od starih Grka pa sve do današnjih dana, ovi brojevi su okupirali pozornost i maštu mnogih. Kolika je njihova jedinstvenost, ali i složenost, možda najbolje govori podatak da ih je većina pronađena u posljednjih nekoliko desetljeća i to uz pomoć računalne tehnologije. U njihovom otkrivanju najveću ulogu imaju Mersenneovi prosti brojevi. Zajedno, savršeni i Mersenneovi prosti brojevi, zauzimaju posebno mjesto u širokom rasponu tema kojima se bavi teorija brojeva.

Cilj je ovog rada predočiti i opisati ove brojeve, ukazati na njihove međusobne odnose te tako dati doprinos njihovom boljem razumijevanju i potaknuti nove potrage. Na osnovu dostupne literature opisana je priroda savršenih i Mersenneovih prostih brojeva. Prikazan je povijesni razvoj potrage za ovim brojevima te su istaknuta imena pronalazača koji su dali doprinos ovoj potrazi. Putem teorema i dokaza predstavljena je veza između ovih brojeva te prikazana uloga Mersenneovih prostih brojeva u pronalasku savršenih brojeva.

Možemo zaključiti da savršeni i Mersenneovi prosti brojevi, zbog njihovih jedinstvenih svojstava i odnosa, predstavljaju izuzetno zanimljiv problem koji ne prestaje zaokupljati pozornost onih koji ih proučavaju. Unatoč tome što je iznimno teško pronaći ove brojeve, upravo ova jedinstvenost koja ih krasi, daje poticaj za neprestanom potragom. Zbog toga, možemo pretpostaviti kako će potraga za ovim brojevima i u budućnosti biti u središtu pozornosti, ne samo brojnih matematičara, već i drugih znanstvenika i pronalazača.

# Literatura


[1] F. M. Brückler, *Povijest matematike II*, Odjel za matematiku, Osijek, 2010.

[2] D. M. Burton, *The History of Mathematics: An introduction*, McGrow-Hill, New York, 2005.

[3] L. N. Childs, *A Concrete Introduction to Higher Algebra*, Springer, New York, 2009.

[4] J. A. Holdener, *A theorem of Touchard on the form of odd perfect numbers*, The American Mathematical Monthly, 109(2002), 661-663.

[5] V. Ibro, E. Ljajko, *Prosti, savršeni i prijateljski brojevi*, Zbornik radova Učiteljskog fakulteta, 12(2018), 29-39.

[6] V. J. Katz, *A History of Mathematics. An introduction*, Pearson, Boston, 2009.

[7] T. Koshy, *Elementary number theory with applications*, Elsevier Inc., London, 2007.

[8] I. Matić, *Uvod u teoriju brojeva*, Odjel za matematiku, Osijek, 2014.

**Sažetak.** U ovom radu proučavamo Mersenneove i savršene brojeve. Kažemo da je prirodan broj $N$ savršen ako je $\sigma(N) = 2N$, gdje je $\sigma(N)$ suma pravih djelitelja broja $N$. Poznato je da je broj oblika $2^{p-1}(2^p - 1)$, gdje je $2^p - 1$ prost, paran savršen broj. Svi dosad poznati savršeni brojevi su parni. Nije poznato postoje li ili ne neparni savršeni brojevi, ali pronađeni su mnogi uvjeti koje bi trebali zadovoljavati u slučaju postojanja. Mersenneov broj jest broj oblika $M_n = 2^n - 1$, a Mersenneov prost broj je Mersenneov broj koji je prost. Postoje različite metode kojima se testira prostost Mersenneovih brojeva. Vrlo učinkovit test prostosti jest Lucas-Lehmerov test.

**Ključne riječi:** prost broj, savršen broj, Mersenneov broj, Mersenneov prost broj, Lucas-Lehmer test.

**Summary.** In this paper we study Mersenne numbers and perfect numbers. We say that natural number $N$ is perfect if $\sigma(N) = 2N$, where $\sigma(N)$ denotes the sum of the positive divisors of $N$. It is well known that a number is even and perfect if and only if it has the form $2^{p-1}(2^p - 1)$ where $2^p - 1$ is prime. All presently known perfect numbers are even. It is unknown whether or not odd perfect numbers exist, although many conditions necessary for their existance have been found. A number of the form $M_n = 2^n - 1$ is called Mersenne number, and Mersenne number which is prime is called Mersenne prime. There are various methods for testing the primality of Mersenne numbers. Lucas-Lehmer test is an extremely efficient primality test for Mersenne primes.

**Key words:** prime number, perfect number, Mersenne number, Mersenne prime, Lucas-Lehmer test.

# Životopis

Rođena sam 29. siječnja 1992. godine u Vukovaru. U Osnovnoj školi Bobota započela sam svoje obrazovanje. Nakon završetka osnovne škole upisala sam jezičnu gimnaziju u Gimnaziji Vukovar. Po završetku srednjoškolskog obrazovanja, 2010. godine, upisujem Sveučilišni nastavnički studij matematike i informatike na Odjelu za matematiku u Osijeku.