MAT-KOL (Banja Luka)
ISSN 0354-6969
Vol. XV (2)(2009), 51-60

MERSENNEOVI I SAVRŠENI BROJEVI

Bernadin Ibrahimpašić[1], Edin Liđan[2]

Sažetak:

U ovom članku pokazaćemo kakav oblik imaju elementi nekih podskupova skupa prirodnih brojeva (Mersenneovi i savršeni brojevi), te uz kratak prikaz istorije otkrića prostih Mersenneovih brojeva objasniti u kakvom su odnosu Mersenneovi i savšeni brojevi.

Ključne riječi i fraze: Mersenneovi brojevi, savšeni brojevi, prosti brojevi.

Abstract

In this paper we describe Mersenne and perfect numbers and give some results on connection between Mersenne primes and perfect numbers.

AMS Mathematics Subject Classification (2000): 11A25, 11A41

Key words and phrases: Mersenne numbers, Perfect numbers, Primes.

1 Uvod

U XVII vijeku brojeve oblika $2^p - 1$, gdje je p prost broj, počinje izučavati francuski redovnik Marin Mersenne (1588. – 1648.). Ti brojevi su po njemu dobili ime Mersenneovi brojevi. Ako je broj $M_p = 2^p - 1$ prost broj, onda se on naziva Mersenneov prost broj. Mersenne je bio matematičar, fizičar, filozof, teoretičar muzike i teolog. Bio je centralna ličnost jedne od najznačajnijih naučnih grupa u Francuskoj na početku XVII vijeka. Uz Mersenneove brojeve vezuju se savršeni brojevi (perfect numbers). To su brojevi koji imaju osobinu da su jednaki zbiru svojih pravih djelitelja. Tako imamo da su pravi djelitelji broja 6 brojevi 1, 2 i 3, a njihov zbir je

$$1 + 2 + 3 = 6,$$

pa je broj 6 savršen broj. Mersenneovi brojevi su se nekad nazivali tajni brojevi, a Pitagorejci su savršenim brojevima pripisivali mistična pa i apsurdna svojstva. Traženje i jednih i drugih matematičarima je zadavalo velike poteškoće.

[1]Pedagoški fakultet Univerziteta u Bihaću, Bosna i Hercegovina, e-mail: bernadin@bih.net.ba
[2]Pedagoški fakultet Univerziteta u Bihaću, Bosna i Hercegovina, e-mail: edin.lidjan@yahoo.com

2 Kratak prikaz istorije otkrića prostih Mersenneovih brojeva

Stari Grci su poznavali 4 prosta Mersenneova broja i to:

$$\begin{aligned} M_2 &= 2^2 - 1 = 3, \\ M_3 &= 2^3 - 1 = 7, \\ M_5 &= 2^5 - 1 = 31, \\ M_7 &= 2^7 - 1 = 127. \end{aligned}$$

U srednjem vijeku otkriven još jedan Mersenneov prost broj

$$M_{13} = 2^{13} - 1 = 8191.$$

Nikad nije prestajalo traganje za prostim Mersenneovim brojevima. Mersenne je tvrdio, bez dokaza, da su $2, 3, 5, 7, 13, 17, 19, 31, 67, 127$ i 257 jedini prosti brojevi, ne veći od 257, za koje je broj $2^p - 1$ prost broj. Ovu tvrdnju je dokazao Euler, ali samo za $M_{31} = 2^{31} - 1 = 2147483647$, dok za ostale to nije mogao zbog nedostatka tehnike u to vrijeme. Mersenneova hipoteza sadrži greške koje su otkrivene mnogo vremena poslije njegove smrti. Godine 1947. je pokazano da su ispuštena 3 broja, M_{61}, M_{89} i M_{107}, a da su M_{67} i M_{257}, složeni brojevi.

Do 1996. godine bila su poznata 34 Mersenneova prosta broja, a 34. prosti Mersenneov broj bio je $M_{1257787}$, s 378632 cifre. Otkrili su ga Slowinski i Gage (3. 9. 1996.).

Nalaženje što većeg prostog broja je veliki izazov za mnoge matematičare. Danas se to uglavnom svodi na traženje što većeg Mersenneovog prostog broja.

George Woltman je 1996. godine osnovao međunarodno udruženje **GIMPS** (the **G**reat **I**nternet **M**ersenne **P**rime **S**earch) koje ima više od 100000 članova koji tragaju za što većim Mersenneovim prostim brojem. Pri tome koriste internet i zajednički centralni računar za testiranje i provjeru. Od osnivanja ovog udruženja do danas otkriveno je 13 Mersenneovih brojeva. Svih 13 otkriveno je u okviru GIMPS projekta.

Prvi prost broj otkriven u okviru GIMPS projekta je 35. po redu otkriveni Mersenneov broj. To je $M_{1398269}$, s 420921 cifrom, a otkrili su ga Armengaud i Woltman (13. 11. 1996.).

Evo i prikaza ostalih 12 prostih Mersenneovih brojeva otkrivenih pomoću GIMPS projekta:

M_p	Broj cifara	Pronalazač	Datum otkrića
36. $M_{2976221}$	895932	*Gordon Spence*	24.08.1997.
37. $M_{3021377}$	909526	*Roland Clarkson*	27.01.1998.
38. $M_{6972593}$	2098960	*Nayan Hajratwala*	01.06.1999.
39. $M_{13466917}$	4053946	*Michael Cameron*	14.11.2001.
40. $M_{20996011}$	6320430	*Michael Shaffer*	17.11.2003.
41. $M_{24036583}$	7235733	*Josh Findley*	15.05.2004.
42. $M_{25964951}$	7816230	*Martin Nowak*	18.02.2005.
43. $M_{30402457}$	9152052	*C. Cooper i S. Boone*	15.12.2005.
44. $M_{32582657}$	9808358	*C. Cooper i S. Boone*	04.09.2006.
45. $M_{43112609}$	12978189	*Edson Smith*	23.08.2008.
46. $M_{37156667}$	11185272	*Hans – Michael Elvenich*	06.09.2008.
47. $M_{42643801}$	12837064	*Odd Magnar Strindmo*	12.04.2009.

Danas najveći poznati Mersenneov prost broj je upravo 45., odnosno $M_{43112609}$. To je ujedno danas i najveći poznati prost broj.

3 Mersenneovi i savršeni brojevi

Pojam savršenog broja pojavio se još u Starih Grka kao razbibriga koja se zvala numerologija.

Definicija 3.1 *Prirodan broj n je* savršen broj *ako je jednak zbiru svojih pravih djelitelja.*

Definicija 3.2 *Za prirodan broj n definišemo aritmetičku funkciju*

$$\sigma(n) = \sum_{d|n} d$$

kao zbir svih pozitivnih djelitelja *od n.*

Očigledno je da je Definicija 3.1 ekvivalentna činjenici da je prirodan broj n savršen ako je

$$n = \sigma(n) - n,$$

tj. ako je

$$\sigma(n) = 2n.$$

Iskažimo sada jedan teorem koji govori o osobinama funkcije $\sigma(n)$, no prije toga definišimo multiplikativnu funkciju.

Definicija 3.3 *Za funkciju $f\colon \mathbb{N} \to \mathbb{N}$ kažemo da je* multiplikativna *ako za sve relativno proste prirodne brojeve m i n vrijedi*

$$f(mn) = f(m) \cdot f(n).$$

Teorem 3.1 *Neka su m i n relativno prosti prirodni brojevi.*

(i) Funkcija $\sigma(n)$ je multiplikativna.

(ii) Ako je $n = p$ prost broj, tada je

$$\sigma(p) = p + 1.$$

U opštem slučaju, za stepen od p vrijedi

$$\sigma(p^\alpha) = \frac{p^{\alpha+1} - 1}{p - 1}.$$

(iii) Ako je $n = p_1^{\alpha_i} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ rastav broja n na proste faktore, onda je

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

Dokaz:

(i) Neka je $\gcd(m, n) = 1$. Tada je

$$\sigma(mn) = \sum_{d|mn} d = \sum_{d_1|m} \sum_{d_2|n} d_1 d_2 = \sum_{d_1|m} d_1 \sum_{d_2|n} d_2 = \sigma(m) \cdot \sigma(n)\,.$$

(ii) U dijelu (iii) dokazujemo mnogo opštiji slučaj.

(iii) Zbir pozitivnih djelitelja broja

$$n = p_1^{\alpha_i} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

može biti prikazan kao proizvod

$$\left(1 + p_1 + p_1^2 + \cdots + p_1^{\alpha_1}\right) \cdots \left(1 + p_k + p_k^2 + \cdots + p_k^{\alpha_k}\right).$$

Kako je

$$1 + x + x^2 + \cdots x^n = \frac{x^{n+1} - 1}{x - 1},$$

to je

$$\begin{aligned} \sigma(n) &= \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \cdots \frac{p_k^{\alpha_k+1} - 1}{p_k - 1} \\ &= \prod_{i=1}^{k} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}. \end{aligned}$$

□

Pojam savršenog broja definisao je Euklid u 22. (posljednjoj) definiciji VII knjige Euklidovih Elemenata, a u 36. (posljednjoj) propoziciji IX knjige dao metodu kako se može odrediti savršen broj.

Neka je dat geometrijski red

$$1 + 2 + 4 + 8 + 16 + 32 + \cdots ,$$

i odredimo niz njegovih parcijalnih suma. Među članovima toga niza 1, 3, 7, 15, 31, 63, 127, ... uočimo one članove koji su prosti brojevi, pa ih pomnožimo sa njihovim posljednjim sabirkom.

Na primjer, prva parcijalna suma

$$S_1 = 1 + 2 = 3$$

je prost broj. Pomnožimo li ga brojem 2, što je posljednji sabirak u toj sumi, dobijemo $3 \cdot 2 = 6$. Ovo je najmanji (prvi) savršeni broj $(1 + 2 + 3 = 6)$. Druga parcijalna suma

$$S_2 = (1 + 2) + 4 = 7$$

je također prost broj. Ako ga pomnožimo brojem 4 dobijemo $7 \cdot 4 = 28$, što je drugi savršeni broj $(1 + 2 + 4 + 7 + 14 = 28)$. Treća parcijalna suma

$$S_3 = (1 + 2 + 4) + 8 = 15$$

nije prost broj, pa broj $15 \cdot 8 = 120$ nije savršen broj, itd... Sljedeći savršeni broj je 496. Njegovi pravi djelitelji su $1, 2, 4, 8, 16, 31, 62, 124$ i 248 i očito je

$$496 = 1 + 2 + 4 + 8 + 16 + 31 + 62 + 124 + 248.$$

Uočimo da se navedeni brojevi mogu napisati u obliku

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

Napomenimo da nije poznato da li postoje neparni savršeni brojevi. Ovo je jedan od najstarijih neriješenih problema u matematici. Turcaninov [1] je 1908. godine pokazao da ako postoji, da bi morao imati najmanje 5 različitih prostih faktora i da bi morao biti veći od $2 \cdot 10^6$. U novije vrijeme, uz pomoć savremenih računara, je pokazano da bi takav broj, kada bi postojao, morao biti veći od 10^{100}.

Pokažimo da vrijedi sljedeći teorem koji daje potreban i dovoljan uslov da paran prirodan broj bude savršen. Prije nego iskažemo taj teorem, navedimo tvrdnje koje će nam trebati u njegovom dokazu.

Lema 3.1 *Neka je k prirodan broj. Tada su brojevi 2^{k-1} i $2^k - 1$ relativno prosti.*

Dokaz: Jedini pozitivni djelitelji broja 2^{k-1} su stepeni broja 2, tj. brojevi $1, 2, 2^2, 2^3, \ldots, 2^{k-1}$, pa ukoliko brojevi 2^{k-1} i $2^k - 1$ ne bi bili relativno prosti, tada bi broj $2^k - 1$ morao biti djeljiv s nekim od navedenih stepena broja 2, osim brojem 1, što je nemoguće jer je broj $2^k - 1$ neparan. □

Teorem 3.2 *Ako je p prirodan broj i $2^p - 1$ prost broj, onda je i p prost broj.*

Dokaz: Dokažimo ekvivalentnu tvrdnju, tj. da je $2^p - 1$ složen broj ako je p složen broj. Neka je $p = rs$, $r > 1$, $s > 1$. Tada je

$$2^p - 1 = 2^{rs} - 1 = (2^r)^s - 1 = (2^r - 1)((2^r)^{s-1} + (2^r)^{s-2} + \cdots + 1),$$

pa je broj $2^p - 1$ je složen. □

Sada možemo iskazati i dokazati spomenuti teorem.

Teorem 3.3 (Euclid–Eulerov teorem) *Paran broj n je savršen ako i samo ako je $n = 2^{p-1}(2^p - 1)$, gdje je $M_p = 2^p - 1$ Mersenneov prost broj.*

Dokaz: Neka je $n = 2^{p-1}(2^p - 1)$. Kako su, prema Lemi 3.1, 2^{p-1} i $2^p - 1$ relativno prosti brojevi, to zbog multiplikativnosti funkcije σ imamo da je

$$\begin{aligned}
\sigma(n) &= \sigma(2^{p-1}) \cdot \sigma(2^p - 1) \\
&= (1 + 2 + \cdots + 2^{p-1}) \cdot (1 + 2^p - 1) \\
&= \frac{2^p - 1}{2 - 1} \cdot 2^p = (2^p - 1) \cdot 2^p \\
&= 2 \cdot 2^{p-1} \cdot (2^p - 1) \\
&= 2n,
\end{aligned}$$

pa je n savršen.

Obratno, pretpostavimo da je n savršen, tj. da je $\sigma(n) = 2n$, te da je n paran oblika $n = 2^k \cdot m >$, gdje su k i m prirodni brojevi i gdje je m neparan. Sada zbog relativne prostosti brojeva 2^k i m, te multiplikativnosti funkcije σ, imamo da je

$$\sigma(n) = \sigma(2^k) \cdot \sigma(m) = (2^{k+1} - 1) \cdot \sigma(m). \tag{1}$$

Kako je n savršen, to je

$$\sigma(n) = 2n = 2 \cdot 2^k \cdot m = 2^{k+1} \cdot m. \tag{2}$$

Sada iz (1) i (2) slijedi da je

$$(2^{k+1} - 1) \cdot \sigma(m) = 2^{k+1} \cdot m,$$

pa je

$$\sigma(m) = 2^{k+1} \cdot l \tag{3}$$

i

$$m = (2^{k+1} - 1) \cdot l, \tag{4}$$

za neki neparan broj l.

Pretpostavimo li da je $l > 1$, to iz (4) slijedi da m ima bar 3 djelitelja i to $1, m$ i l, pa je sigurno

$$\sigma(m) \geq 1 + m + l.$$

Međutim, sada je

$$\sigma(m) \geq 1 + m + l = 1 + (2^{k+1} - 1) \cdot l + l = 1 + 2^{k+1} \cdot l > 2^{k+1} \cdot l = \sigma(m),$$

što je kontradikcija. Stoga je $l = 1$, pa iz (3) i (4) slijedi da je

$$\sigma(m) = m + 1,$$

što povlači da je m prost broj. Kako je $m = 2^{k+1} - 1$ prost broj, to prema Teoremu 3.2 slijedi da je $k + 1 = p$ također prost broj, pa je

$$\begin{aligned} n &= 2^k \cdot m \\ &= 2^{p-1} \cdot (2^{k+1} - 1) \\ &= 2^{p-1} \cdot (2^p - 1). \end{aligned}$$

□

Kako je danas poznato 47 Mersenneovih prostih brojeva, to na osnovu Teorema 3.3 zaključujemo da je danas poznato 47 savršenih brojeva od kojih je najveći $2^{43112608} \cdot (2^{43112609} - 1)$.

4 Neke osobine savršenih brojeva

Savršeni brojevi posjeduju neka interesantna svojstva. Mi ćemo ovdje navesti dva takva svojstva. Jedno od svojstava je da svaki paran savršen broj završava cifrom 6 ili 8. Pogledajmo slikovit dokaz ove tvrdnje. Kako prema Teoremu 3.3 znamo da je $n = 2^{p-1}(2^p - 1)$, pogledajmo tabelarno zadnju cifru njegovih faktora i njega samog.

$2^{p-1} \bmod 10$	$2^p \bmod 10$	$(2^p - 1) \bmod 10$	$\big(n = 2^{p-1}(2^p - 1)\big) \bmod 10$
2	4	3	6
4	8	7	8
6	2	1	6
8	6	5	0

Tabela nam sugeriše da je tvrdnja istinita osim u slučaju kada je zadnja cifra od 2^{p-1} jednaka 8. Međutim, tada imamo da je zadnja cifra od n jednaka 0, što znači da je broj n višekratnik broja 10. Kako $2^p - 1$ mora biti višekratnik broja 5 i mora biti prost, dobijamo da je $2^p - 1 = 5$. Iz toga slijedi da je $2^p = 6$, što je nemoguće. Tako zaključujemo da paran savršen broj mora završavati cifrom 6 ili 8.

Mi ćemo iskazati i dokazati nešto opštiju tvrdnju. Pogledajmo prije toga jednu tvrdnju koja će nam biti potrebna.

Lema 4.1 *Za svaki prirodan broj $n \in \mathbb{N}$ je*

$$16^n \equiv 6 \pmod{10}.$$

Dokaz: Tvrdnju ćemo dokazati indukcijom. Očito je tvrdnja istinita za $n = 1$, pa pretpostavimo da je istinita i za neki prirodan broj k. Pokažimo da je tada istinita i za broj $k + 1$.

$$\begin{aligned} 16^{k+1} = 16 \cdot 16^k &\equiv 16 \cdot 6 \pmod{10} \\ &\equiv 6 \cdot 6 \pmod{10} \\ &\equiv 36 \pmod{10} \\ &\equiv 6 \pmod{10} \end{aligned}$$

□

Sada možemo iskazati i dokazati sljedeći teorem.

Teorem 4.1 *Svaki paran savršen broj n završava cifrom 6 ili ciframa 28.*

Dokaz: Očito je da trebamo dokazati da je

$$n \equiv 6 \pmod{10} \qquad \text{ili} \qquad n \equiv 28 \pmod{100}.$$

Kao što znamo, n je oblika $n = 2^{p-1}(2^p - 1)$ i p je prost. U slučaju da je $p = 2$, imamo da je $n = 6$, pa je tvrdnja istinita. Zato pretpostavimo da je $p > 2$. Tada, zbog svoje prostosti, p može biti oblika $p = 4m + 1$ ili $p = 4m + 3$, za prirodan broj m.

Neka je $p = 4m + 1$. Tada je

$$n = 2^{4m}(2^{4m+1} - 1) = 2^{8m+1} - 2^{4m} = 2 \cdot 16^{2m} - 16^m.$$

Prema Lemi 4.1 je $16^k \equiv 6 \pmod{10}$, za svaki prirodan broj k, pa je

$$n \equiv 2 \cdot 6 - 6 \equiv 6 \pmod{10}.$$

Neka je sada $p = 4m + 3$. Tada je

$$2^{p-1} = 2^{4m+2} = 4 \cdot 16^m \equiv 4 \cdot 6 \equiv 4 \pmod{10}.$$

Štaviše, za $p > 2$, imamo da 4 dijeli 2^{p-1}, pa je dvocifreni završetak broja 2^{p-1} djeljiv s 4 i završava cifrom 4. To znači imamo sljedeće mogućnosti:

$$2^{p-1} = 4, 24, 44, 64, 84 \pmod{100}.$$

Iz ovoga slijedi da je

$$2^p - 1 = 2 \cdot 2^{p-1} - 1 \equiv 7, 47, 87, 27, 67 \pmod{100},$$

pa dobijamo

$$n = 2^{p-1}(2^p - 1) \equiv 4 \cdot 7, 24 \cdot 47, 44 \cdot 87, 64 \cdot 27, 84 \cdot 67 \pmod{100}.$$

Sada nam preostaje za pokazati da su svi dobijeni brojevi kongruentni s 28 modulo 100. Za prvi broj $4 \cdot 7$ je tvrdnja trivijalno ispunjena. Zato pogledajmo drugi slučaj. Imamo

$$\begin{aligned} 24 \cdot 47 &\equiv 12 \cdot 94 \pmod{100} \\ &\equiv 6 \cdot 188 \pmod{100} \\ &\equiv 6 \cdot 88 \pmod{100} \\ &\equiv 3 \cdot 176 \pmod{100} \\ &\equiv 3 \cdot 76 \pmod{100} \\ &\equiv 228 \pmod{100} \\ &\equiv 28 \pmod{100}. \end{aligned}$$

Ostala 3 slučaja se dokazuju analogno. □

Drugo svojstvo koje posjeduju savršeni brojevi govori o tome da ukoliko bilo kojem parnom savršenom broju, osim broja 6, saberemo cifre i tako dobijenom broju ponovo saberemo cifre, te taj postupak nastavimo dalje, dobijamo kao krajnji rezultat broj 1. Preciznije rečeno, vrijedi sljedeći teorem.

Teorem 4.2 *Svaki paran savršen broj, osim broja 6, pri dijeljenju s 9 daje ostatak 1, tj. ako je $n > 6$ paran savršen broj, tada je*

$$n \equiv 1 \pmod{9}.$$

Dokaz: Kako imamo da je $2^1 \equiv 2 \pmod 9$, $2^2 \equiv 4 \pmod 9$, $2^3 \equiv 8 \pmod 9$, $2^4 \equiv 7 \pmod 9$, $2^5 \equiv 5 \pmod 9$ i $2^6 \equiv 1 \pmod 9$, to prema Teoremu 3.3 slijedi da je dovoljno posmatrati samo brojeve oblika $n = 2^{r-1}(2^r - 1)$, gdje je $r = 6k + 1, 6k + 3, 6k + 5$, za $k \in \mathbb{N} \cup \{0\}$.

Kako vrijede sljedeće kongruencije $2^{6k}\left(2^{6k+1} - 1\right) \equiv 2^0(2^1 - 1) \pmod 9$, $2^{6k+2}\left(2^{6k+3} - 1\right) \equiv 2^2(2^3 - 1) \pmod 9$ i $2^{6k+4}\left(2^{6k+5} - 1\right) \equiv 2^4(2^5 - 1) \pmod 9$, to trebamo samo dokazati da su brojevi oblika

$$2^0(2^1 - 1) = 1,\ 2^2(2^3 - 1) = 28,\ 2^4(2^5 - 1) = 496$$

kongruentni s 1 modulo 9, što je očigledno ispunjeno. □

Literatura

[1] Burton, D.M.,*Elementary Number Theory*. First Edition. Allyn and Bacon Inc, London 1980.

[2] Clark, W.E., *Elementary Number Theory*. Departments of Mathematics, University of South Florida, 2002.

[3] Karahmet, H., *O nekim podskupovima skupa prirodnih brojev*a. Naša škola, 36 (2006), 131-141.

[4] `http://www.mersenne.org/status.htm`

[5] Pavković, B., Dakić, B., Mladinić, P., *Elementarna teorija brojeva*. Element, Zagreb 1994.

[6] Stanić, M., Ikodinović, N., *Teorija brojeva, zbirka zadataka*. Zavod za udžbenike i nastavna sredstva, Beograd 2004.

[7] Yan, S.Y., *Number Theory for Computing*. Springer-Verlag, Berlin 2002.