Sveučilište J.J. Strossmayera u Osijeku
Odjel za matematiku
Diplomski studij matematike

Ana Maslać

Mersenneovi i savršeni brojevi

Diplomski rad

Osijek, 2012.

Sveučilište J.J. Strossmayera u Osijeku
Odjel za matematiku
Diplomski studij matematike

Ana Maslać

Mersenneovi i savršeni brojevi

Diplomski rad

Mentor: doc. dr. sc. Ivan Matić

Osijek, 2012.

Sadržaj

1. Uvod

Teorija brojeva jedna je od najstarijih disciplina koja postoji više od 2000 godina. Prvi teoretičari bili su zainteresirani za proučavanje brojeva s posebnim svojstvima, a neki problemi iz teorije brojeva ostaju neriješeni stotinama godina. Ovaj rad obrađuje neke od neriješenih problema - koji su zaokupljali matematičare od samih početaka - Mersenneove i savršene brojeve. Proučavanjem tih problema došlo se do mnogih otkrića u teoriji brojeva. Cilj rada je dati kratak pregled otkrića na području Mersenneovih i savršenih brojeva.

U prvom dijelu rada definirani su osnovni pojmovi iz teorije brojeva koji su potrebni u glavnom dijelu rada.

U drugom dijelu rada riječ je o Mersenneovim brojevima. Posebno su proučavani Mersenneovi prosti brojevi, uz čije je pronalažanje usko vezano pronalaženje parnih savršenih brojeva. Najbolja dosad znana metoda kojom se određuje je li neki Mersenneov broj prost ili složen, takozvani test prostosti, Lucas-Lehmerov je test, koji se i danas koristi u pronalaženju Mersenneovih prostih brojeva korištenjem računala.

U trećem dijelu rada riječ je o savršenim brojevima. Svi dosad otkriveni savršeni brojevi parni su savršeni brojevi. No neparni savršeni brojevi dugo su proučavani od strane matematičara. Pitanje njihova postojanja najduže je neriješena hipoteza u teoriji brojeva. Postavljeni su mnogi uvjeti koje bi neparni savršeni brojevi trebali zadovoljavati u slučaju postojanja, a uz sve jača računala određene uvjete se konstantno poboljšava.

2. Osnovni pojmovi iz teorije brojeva

Definicija 2.1 *Neka su $a \neq 0$ i b cijeli brojevi. Kažemo da je b djeljiv s a, odnosno da a dijeli b, ako postoji cijeli broj x takav da je $b = ax$. To zapisujemo kao $a \mid b$. Ako b nije djeljiv s a, onda pišemo $a \nmid b$. Ako $a \mid b$, onda još kažemo da je a djelitelj od b, te da je b višekratnik od a.*

Teorem 2.1 (Teorem o dijeljenju s ostatkom) *Za proizvoljan prirodan broj a i cijeli broj b postoje jedinstveni cijeli brojevi q i r takvi da je $b = qa + r$, $0 \leq r < a$.*

Definicija 2.2 *Neka su b i c cijeli brojevi. Cijeli broj a zovemo zajednički djelitelj od b i c ako $a \mid b$ i $a \mid c$. Ako je barem jedan od brojeva b i c različit od nule, onda postoji samo konačno mnogo zajedničkih djelitelja od b i c. Najveći među njima zove se najveći zajednički djelitelj od b i c i označava se s (b, c).*

Uočimo da je $(b, c) \geq 1$.

Teorem 2.2

$$(b, c) = \min(\{bx + cy : x, y \in \mathbb{Z}\} \cap \mathbb{N}).$$

Ako se cijeli broj d može prikazati u obliku $d = bx + cy$, onda je (b, c) djelitelj od d. Posebno, ako je $bx + cy = 1$, onda je $(b, c) = 1$.

Definicija 2.3 *Reći ćemo da su cijeli brojevi a i b relativno prosti ako je $(a, b) = 1$. Za cijele brojeve $a_1, a_2, ..., a_n$ reći ćemo da su relativno prosti ako je $(a_1, a_2, ..., a_n) = 1$, a da su u parovima relativno prosti ako je $(a_i, a_j) = 1$ za sve $1 \leq i, j \leq n$, $i \neq j$.*

Definicija 2.4 *Prirodan broj $p > 1$ zove se prost ako p nema niti jednog djelitelja d takvog da je $1 < d < p$. Ako prirodan broj $a > 1$ nije prost, onda kažemo da je složen.*

Propozicija 2.1 *Ako je p prost broj i $p \mid ab$, onda $p \mid a$ ili $p \mid b$.*

*D*okaz:
Ako $p \nmid a$, onda je $(p, a) = 1$, pa postoje cijeli brojevi x i y takvi da je $ax + py = 1$. Sada je $abx + pby = b$, pa p dijeli b.

□

Teorem 2.3 (Osnovni teorem aritmetike) *Faktorizacija svakog prirodnog broja $n > 1$ na proste faktore jedinstvena je do na poredak prostih faktora.*

Teorem 2.4 (Dirichlet) *Ako su $d \geq 2$ i $a \neq 0$ cijeli brojevi koji su relativno prosti, onda aritmetički niz*

$$a, a+d, a+2d, a+3d, \ldots$$

sadrži beskonačno mnogo prostih brojeva.

Definicija 2.5 *Ako cijeli broj $m \neq 0$ dijeli razliku $a-b$, onda kažemo da je a kongruentan b modulo m i pišemo $a \equiv b \pmod{m}$. U suprotnom, kažemo da a nije kongruentan b modulo m i pišemo $a \not\equiv b \pmod{m}$.*

Definicija 2.6 *Skup $\{x_1, ..., x_m\}$ zove se potpuni sustav ostataka modulo m ako za svaki $y \in \mathbb{Z}$ postoji točno jedan x_j takav da je $y \equiv x_j \pmod{m}$. Drugim riječima, potpuni sustav ostataka dobivamo tako da iz svake klase ekvivalencije modulo m uzmemo po jedan član.*

Teorem 2.5 (Kineski teorem o ostacima) *Neka su $m_1, m_2, \ldots, m_r$ u parovima relativno prosti prirodni brojevi, te neka su $a_1, a_2, \ldots, a_r$ cijeli brojevi. Tada sustav kongruencija*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1}, \\ x &\equiv a_2 \pmod{m_2}, \\ &\vdots \\ x &\equiv a_r \pmod{m_r} \end{aligned}$$

ima rješenja. Ako je x_0 jedno rješenje, onda su sva rješenja sustava dana s

$$x \equiv x_0 \pmod{m_1 m_2 \cdots m_r}.$$

Definicija 2.7 *Reducirani sustav ostataka modulo m skup je cijelih brojeva r_i sa svojstvom da je $(r_i, m) = 1$, $r_i \not\equiv r_j \pmod{m}$ i da za svaki cijeli broj x takav da je $(x, m) = 1$ postoji r_i takav da je $x \equiv r_i \pmod{m}$. Jedan reducirani sustav ostataka modulo m skup je svih brojeva $a \in \{1, 2, ..., m\}$ takvih da je $(a, m) = 1$. Jasno je da svi reducirani sustavi ostataka modulo m imaju isti broj elemenata. Taj broj označavamo s $\varphi(m)$, a funkciju φ zovemo Eulerova funkcija. Drugim riječima, $\varphi(m)$ je broj brojeva u nizu $1, 2, ..., m$ koji su relativno prosti sa m.*

Teorem 2.6 (Eulerov teorem) *Ako je $(a, m) = 1$, onda je $a^{\varphi(m)} \equiv 1 \pmod{m}$.*

Teorem 2.7 (Mali Fermatov teorem) *Neka je p prost broj. Ako $p \nmid a$, onda je $a^{p-1} \equiv 1 \pmod{p}$. Za svaki cijeli broj a vrijedi $a^p \equiv a \pmod{p}$.*

Lema 2.1 *Za svaki prost broj p vrijedi $(x+y)^p \equiv x^p + y^p \pmod{p}$.*

Definicija 2.8 *Funkciju $\vartheta : \mathbb{N} \to \mathbb{C}$ za koju vrijedi*

1. $\vartheta(1) = 1$,

2. $\vartheta(mn) = \vartheta(m)\vartheta(n)$ *za sve* m, n *takve da je* $(m, n) = 1$,

zovemo multiplikativna funkcija.

Definicija 2.9 *Neka su a i n relativno prosti prirodni brojevi. Najmanji prirodni broj d sa svojstvom da je $a^d \equiv 1 \pmod{n}$ zove se red od a modulo n. Još se kaže da a pripada eksponentu d modulo n.*

Propozicija 2.2 *Neka je d red od a modulo n. Tada za prirodan broj k vrijedi $a^k \equiv 1 \pmod{n}$ ako i samo ako $d \mid k$. Posebno $d \mid \varphi(n)$.*

*D*okaz:
Ako $d \mid k$, recimo $k = d \cdot l$, onda je $a^k \equiv (a^d)^l \equiv 1 \pmod{n}$.
Obratno, neka je $a^k \equiv 1 \pmod{n}$. Podijelimo k s d, pa dobivamo $k = q \cdot d + r$, gdje je $0 \leq r < d$. Sada je

$$1 \equiv a^k \equiv a^{qd+r} \equiv (a^d)^q \cdot a^r \equiv a^r \pmod{n},$$

pa zbog minimalnosti od d slijedi da je $r = 0$, tj. $d \mid k$.

□

Definicija 2.10 *Neka je $(a, m) = 1$. Ako kongruencija $x^2 \equiv a \pmod{m}$ ima rješenja, onda kažemo da je a kvadratni ostatak modulo m. U suprotnom kažemo da je a kvadratni neostatak modulo m.*

Definicija 2.11 *Neka je p neparan prost broj. Po definiciji, Legendreov simbol $(\frac{a}{p})$ je jednak 1 ako je a kvadratni ostatak modulo p, -1 ako je a kvadratni neostatak modulo p, te 0 ako $p \mid a$.*

Dakle, broj rješenja kongruencije $x^2 \equiv a \pmod{p}$ jednak je $1 + (\frac{a}{p})$.

Teorem 2.8 (Eulerov kriterij)

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Teorem 2.9 (Gaussova lema) *Neka je p neparan prost broj i $(a, p) = 1$. Promotrimo brojeve $a, 2a, 3a, ..., \frac{p-1}{2} \cdot a$, te njihove najmanje nenegativne ostatke pri dijeljenju s p. Označimo s n broj ostataka koji su veći od $\frac{p}{2}$. Tada je $(\frac{a}{p}) = (-1)^n$.*

Teorem 2.10 (Gaussov kvadratni zakon reciprociteta) *Ako su p i q različiti neparni prosti brojevi, onda vrijedi*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Drugim riječima, ako su p i q oba oblika $4k+3$, onda jedna od kongruencija $x^2 \equiv p \pmod{q}$, $x^2 \equiv q \pmod{p}$ ima rješenja, a druga nema. Ako barem jedan od brojeva p i q ima oblik $4k+1$, onda ili obje ove kongruencije imaju rješenja ili obje nemaju rješenja.

Teorem 2.11 *Ako je p neparan prost broj, onda vrijedi*

$$\left(\frac{2}{p}\right) = \begin{cases} 1\,, & \text{ako je } p \equiv 1 \pmod 8 \text{ ili } p \equiv 7 \pmod 8; \\ -1\,, & \text{ako je } p \equiv 3 \pmod 8 \text{ ili } p \equiv 5 \pmod 8. \end{cases}$$

Teorem 2.12 (Fermat) *Neparan prost broj p možemo zapisati kao $p = x^2+y^2$, $x, y \in \mathbb{Z}$, ako i samo ako je $p \equiv 1 \pmod 4$.*

Definicija 2.12 *Neka je n prirodan broj. S $\tau(n)$ ćemo označavati broj pozitivnih djelitelja broja n, a sa $\sigma(n)$ sumu svih pozitivnih djelitelja broja n.*

Jasno je da vrijedi $\tau(n) = \sum_{d|n} 1$, $\sigma(n) = \sum_{d|n} d$. Stoga su funkcije τ i σ multiplikativne. Budući da je $\tau(p^j) = j+1$, $\sigma(p^j) = 1 + p + p^2 + \cdots + p^j = \frac{p^{j+1}-1}{p-1}$, dobivamo sljedeće formule za τ i σ:

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

Lema 2.2 (Diofantov identitet) *Produkt suma dvaju kvadrata ponovno je suma dvaju kvadrata:*

$$(a_1^2+b_1^2)(a_2^2+b_2^2) = (a_1a_2-b_1b_2)^2 + (a_1b_2+b_1a_2)^2.$$

3. Mersenneovi brojevi

Brojevi oblika

$$M_n = 2^n - 1, (n \geq 1)$$

nazvani su *Mersenneovim brojevima* po francuskom redovniku Marinu Mersseneu (1588.-1648.). Prvih nekoliko Mersenneovih brojeva su $1, 3, 7, 15, 31, 63, 127, 255$, iz čega je vidljivo da su neki Mersenneovi brojevi prosti, a neki složeni. Mersenneovi brojevi koji su prosti zovu se *Mersenneovi prosti brojevi.*

Teorem 3.1 *Ako je $M_n = 2^n - 1$ prost broj, onda je n prost broj.*

Dokaz:
Neka su r i s pozitivni cijeli brojevi. Primijetimo da vrijedi

$$x^{rs} - 1 = (x^s - 1) \cdot (x^{s(r-1)} + x^{s(r-2)} + ... + x^s + 1).$$

Ako je broj n složen, recimo $n = rs$, $r, s > 1$, onda je $2^n - 1$ također složen (jer je djeljiv sa $2^s - 1$).

□

Nadalje, pretpostavimo da je $n > 1$. Budući da $x - 1$ dijeli $x^n - 1$, da bi potonji bio prost, prethodni mora biti jednak 1. Iz toga slijedi Korolar 3.1.

Korolar 3.1 *Neka su a i n cijeli brojevi veći od 1. Ako je $a^n - 1$ prost, onda je $a = 2$ i n je prost.*

Bitno je napomenuti da obrat Teorema 3.1 ne vrijedi. Odnosno, činjenica da je n prost broj ne povlači da je $M_n = 2^n - 1$ prost broj. Na primjer, Mersenneov broj $M_{11} = 2^{11} - 1 = 2047 = 23 \cdot 89$ nije prost iako broj 11 jest prost. Budući da ne postoji očito pravilo po kojem se određuje jesu li određeni Mersenneovi brojevi prosti, upravo to čini pronalaženje Mersenneovih prostih brojeva zanimljivim, a istovremeno i vrlo teškim.

3.1. Mersenneovi prosti brojevi

U uvodu svoje knjige *Cogitata physico mathematica* 1644. godine, Mersenne je iznio netočnu, ali provokativnu tvrdnju o Mersenneovim prostim brojevima. Ustvrdio je da je M_p prost broj za $p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$, odnosno složen broj za sve ostale proste brojeve $p < 257$. Mersseneova tvrdnja pobudila je veliko zanimanje zato što su brojevi toliko veliki da nekoliko stotina godina nitko nije mogao potvrditi ni opovrgnuti njegovu tvrdnju. Tadašnjim matematičarima bilo je jasno da Mersenne nije mogao provjeriti tvrdnju za sve navedene brojeve, ali isto tako nisu mogli ni oni.

Leonhard Euler pokazao je 1772. godine da je M_{31} prost tako što je provjerio sve proste brojeve do 46339 kao moguće djelitelje, ali tu metodu nije mogao upotrijebiti na brojevima M_{67}, M_{127} i M_{257}. Na sličan način je Pietro Cataldi 1588. godine pokazao da su M_{17} i M_{19} prosti brojevi.

Godine 1876. Édouard Lucas uspio je dokazati da je M_{127} zaista prost broj. Osim toga, Lucas je radio na testu kojim bi dokazao da je Mersenneov broj M_{67} složen, ali nije uspio naći njegove faktore.

U listopadu 1903. godine, američki matematičar Frederick Nelson Cole izlagao je pred Američkim matematičkim društvom na temu faktorizacije velikih brojeva. Izišao je pred ploču i ništa ne rekavši izračunao $2^{67} - 1$, a zatim na čistoj strani ploče pomnožio $193\,707\,721 \cdot 761\,838\,257\,287$. Rezultati ta dva računa, a za što je nagrađen velikim pljeskom, bili su jednaki. Trebalo mu je 20 godina nedjeljnih popodneva da bi pronašao faktore Mersenneovog broja M_{67}.

Ivan Mikheevich Pervushin pokazao je 1883. godine da je M_{61} prost broj. R. E. Powers pokazao je 1911. godine da je M_{89} prost broj, te 1914. godine da je M_{107} prost broj. Konačno, Lehmer je 1927. godine pokazao da je M_{257} složen broj.

Do 1947. godine testirani su svi brojevi oblika $2^n - 1$ za $n \leq 257$. Sada je poznato da je Mersenne napravio pet pogrešaka: neispravno je zaključio da su M_{67} i M_{257} prosti, a M_{61}, M_{89} i M_{107} je isključio sa svoje liste prostih brojeva.

Postoje različite metode kojima se određuje jesu li neki Mersseneovi brojevi prosti ili složeni. Jedan takav test slijedi.

Teorem 3.2 *Ako su p i $q = 2p + 1$ prosti brojevi, onda $q \mid M_p$ ili $q \mid M_p + 2$.*

Dokaz:
Prema Malom Fermatovom teoremu znamo da vrijedi

$$2^{q-1} - 1 \equiv 0 \pmod{q}$$

i da nakon faktorizacije lijeve strane vrijedi

$$(2^{(q-1)/2} - 1)(2^{(q-1)/2} + 1) = (2^p - 1)(2^p + 1) \equiv 0 \pmod{q},$$

a to je isto što i

$$M_p(M_p + 2) \equiv 0 \pmod{q}.$$

Tvrdnja teorema sada slijedi iz Propozicije 2.1. Dakle, ne može vrijediti i $q \mid M_p$ i $q \mid M_p + 2$, jer bi vrijedilo $q \mid 2$, što je kontradikcija.

□

Primjer 3.1 *Ilustracija Teorema 3.2.*
Ako je $p = 23$, onda je $q = 2p + 1 = 47$ također prost broj, pa to promatramo kao slučaj M_{23}. Provjeravamo vrijedi li $47 \mid M_{23}$, tj. je li $2^{23} \equiv 1 \pmod{47}$. Sada je

$$2^{23} = 2^3(2^5)^4 \equiv 2^3(-15)^4 \pmod{47}.$$

Ali

$$(-15)^4 = (225)^2 \equiv (-10)^2 \equiv 6 \pmod{47}.$$

Kada napišemo ove dvije kongruencije skupa, vidimo da je

$$2^{23} \equiv 2^3 \cdot 6 \equiv 48 \equiv 1 \pmod{47}$$

pa je prema tome M_{23} složen broj.

Potrebno je istaknuti da se Teoremom 3.2 ne može testirati je li na primjer broj M_{29} prost ili složen. U ovom slučaju $59 \nmid M_{29}$, ali $59 \mid M_{29} + 2$.

U sljedećem teoremu prikazano je pod kojim uvjetima vrijedi $q \mid M_p$, odnosno $q \mid M_p + 2$.

Teorem 3.3 *Ako je $q = 2n + 1$ prost broj, onda vrijedi*

1. *$q \mid M_n$, kada je $q \equiv 1 \pmod{8}$ ili $q \equiv 7 \pmod{8}$;*
2. *$q \mid M_n + 2$, kada je $q \equiv 3 \pmod{8}$ ili $q \equiv 5 \pmod{8}$.*

Dokaz:
Tvrdnja da $q \mid M_n$ ekvivalentna je tvrdnji da je

$$2^{(q-1)/2} = 2^n \equiv 1 \pmod{q}.$$

U terminima Legendreovog simbola, potonji uvjet postaje $(\frac{2}{q}) = 1$. Ali prema Teoremu 2.11, $(\frac{2}{q}) = 1$ kada je $q \equiv 1 \pmod{8}$ ili $q \equiv 7 \pmod{8}$.

Druga se tvrdnja može pokazati na sličan način.

□

Slijedi direktna posljedica Teorema 3.3.

Korolar 3.2 *Ako su p i $q = 2p+1$ neparni prosti brojevi, gdje je $p \equiv 3 \pmod 4$, onda $q \mid M_p$.*

Dokaz:
Neparan prost broj p je oblika $4k+1$ ili oblika $4k+3$. Ako je $p = 4k+3$, onda je $q = 8k+7$ i po Teoremu 3.3 slijedi da $q \mid M_p$. Ako je $p = 4k+1$, onda je $q = 8k+3$, pa slijedi da $q \nmid M_p$.

□

Neki prosti brojevi $p \equiv 3 \pmod 4$ za koje je $q = 2p+1$ također prost su na primjer $11, 23, 83, 131, 179, 181, 239, 251$. U svim slučajevima, M_p je složen broj.

Primjer 3.2 *Ilustracija Korolara 3.2.*
Pokažimo da Mersenneov broj $M_{251} = 2^{251} - 1$ nije prost.
Brojevi $p = 251$ i $q = 2p+1 = 2 \cdot 251 + 1 = 503$ su prosti i $251 \equiv 3 \pmod 4$, pa iz Korolara 3.2 slijedi da $503 \mid M_{251}$, što znači da M_{251} nije prost.

U sljedeća dva teorema bavimo se određivanjem djelitelja od M_p.

Teorem 3.4 *Ako je p neparan prost broj, onda je svaki djelitelj od M_p oblika $2kp+1$.*

Dokaz:
Neka je q bilo koji prost djelitelj od M_p, takav da je $2^p \equiv 1 \pmod q$. Ako je k red od 2 modulo q (tj. ako je k najmanji prirodni broj sa svojstvom $2^k \equiv 1 \pmod q$), onda prema Propoziciji 2.2 slijedi da $k \mid p$. Ne može biti slučaj da je $k = 1$, jer bi to povlačilo da $q \mid 1$, što je nemoguće. Prema tome, budući da $k \mid p$ i $k > 1$, te da je p prost broj, mora biti $k = p$.
Sukladno Malom Fermatovom teoremu, imamo $2^{q-1} \equiv 1 \pmod q$ i, zahvaljujući Propoziciji 2.2, imamo $k \mid q-1$. Znajući da je $k = p$, vrijedi $p \mid q-1$. Sada stavimo $q-1 = pt$, pa je $q = pt+1$. Uočimo da u slučaju da je t neparan prost broj, q bi bio paran što je kontradikcija. Stoga, za proizvoljni k mora vrijediti $q = 2kp+1$.

□

Teorem 3.5 *Ako je p neparan prost broj, onda je svaki prost djelitelj q od M_p oblika $q \equiv \pm 1 \pmod 8$.*

Dokaz:
Pretpostavimo da je $q = 2n+1$ prost djelitelj od M_p. Ako je $a = 2^{(p+1)/2}$, onda

$$a^2 - 2 = 2^{p+1} - 2 = 2M_p \equiv 0 \pmod q.$$

Potenciranjem obje strane kongruencije $a^2 \equiv 2 \pmod{q}$ na n-tu potenciju, dobijemo

$$a^{q-1} = a^{2n} \equiv 2^n \pmod{q}.$$

Budući da je q neparan cijeli broj, vrijedi $(a, q) = 1$, pa je $a^{q-1} \equiv 1 \pmod{q}$. Spajanjem zadnjih dviju kongruencija dobijemo $2^n \equiv 1 \pmod{q}$, odnosno da $q \mid M_n$. Sada iz Teorema 3.3 možemo zaključiti da je $q \equiv \pm 1 \pmod{8}$.

□

Primjer 3.3 *Ilustracija prethodnih teorema.*
Pogledajmo M_{17}. Cijeli brojevi oblika $34k + 1$ koji su manji od $362 < \sqrt{M_{17}}$ su:

$$35, 69, 103, 137, 171, 205, 239, 273, 307, 341.$$

Budući da najmanji (netrivijalni) djelitelj od M_{17} mora biti prost broj, trebamo među prethodnih deset brojeva razmotriti samo proste brojeve; redom $103, 137, 239, 307$. Budući da 307 nije kongruentno $\pm 1 \pmod{8}$, možemo 307 isključiti s liste. Sada je ili M_{17} prost broj ili ga jedan od preostala tri broja dijeli. Računanjem se lako provjeri da M_{17} nije djeljiv ni s jednim od brojeva $103, 137, 239$. Stoga zaključujemo da je M_{17} prost broj.

Primjer 3.4 *Prikaz Eulerova dokaza prostosti broja M_{31}.*
Bilo koji q koji dijeli M_{31} je oblika $q \equiv 1 \pmod{62}$. Budući da prosti brojevi koji dijele izraze oblika $x^2 - 2y^2$ moraju zadovoljavati $q \equiv \pm 1 \pmod{8}$, Euler je znao da ako $q \mid M_{31}$, onda je $q \equiv 1, 63 \pmod{248}$, s obzirom da $q \mid ((2^{16})^2 - 2)$. Budući da je $\lfloor \sqrt{M_{31}} \rfloor = 46340$, Euler je trebao provjeriti je li M_{31} djeljiv s prostim brojevima oblika $q = 248k + 1$ ili $q = 248k + 63$, gdje je $q \leq 46340$. S obzirom da nije pronašao takve proste brojeve, zaključio je da je Mersenneov broj M_{31} prost.

3.2. Lucas-Lehmerov test

Jedan od najutjecajnijih matematičara 19. stoljeća u ovom području bio je François Édouard Anatole Lucas (1842.-1891.). Lucas je proučavao Fibonaccijeve brojeve i do 1877. godine je faktorizirao prvih 60. Proučavajući djeljivost Fibonaccijevih brojeva došao je do dokaza da je M_{127} prost. Najvećim poznatim prostim brojem M_{127} ostao je više od 70 godina. Veći prost broj otkrili su 1951. godine Miller i Wheeler.

Teorem 3.6 *Pretpostavimo da je sa F_k označen k-ti Fibonaccijev broj i da je $n \in \mathbb{N}$. Ako je $n \equiv \pm 3 \pmod{10}$ i $n \mid F_{n+1}$ ali $n \nmid F_m$ za sve djelitelje m od n gdje $1 \leq m \leq n$, onda je n prost broj. Također, ako je $n \equiv \pm 1 \pmod{10}$ i $n \mid F_{n-1}$ ali $n \nmid F_m$ za sve djelitelje m od n gdje $1 \leq m \leq n - 2$, onda je n prost broj.*

Bazirano na ovom rezultatu, Lucas je trebao dokazati samo da $M_{127} \mid F_{2^{127}}$ ali da $M_{127} \nmid F_{2^n}$ za sve prirodne brojeve $n < 127$. Uspio je to 1876. godine koristeći metode koje su dovele do testa prostosti.

Derrick Henry Lehmer (1905.-1991.) proširio je 1930. godine Lucasove ideje, te je stvorena najbolja dosad znana metoda kojom se određuje je li neki Mersenneov broj prost ili složen (test prostosti). Lucas-Lehmerov test koristi se u pronalaženju Mersenneovih prostih brojeva korištenjem računala od 1952. godine pa do danas.

Teorem 3.7 (Lucas-Lehmerov test prostosti za Mersenneove brojeve) *Neka je p neparan prost broj. Mersenneov broj M_p prost je ako i samo ako je*

$$S_{p-2} \equiv 0 \pmod{M_p},$$

gdje je $S_0 = 4$ i $S_n = S_{n-1}^2 - 2$.

Dokaz:

Definicija 3.1 *Uređen par $(G, \cdot)$, gdje je G skup i $\cdot : G \times G \to G$ funkcija koja svakom uređenom paru $(x, y) \in G \times G$ pridružuje element $x \cdot y \in G$, zovemo grupom ako vrijede sljedeća tri svojstva:*

1. *Asocijativnost: $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ za sve $x, y, z \in G$,*
2. *Postojanje neutralnog elementa: $(\exists e \in G)(\forall x \in G)\ x \cdot e = e \cdot x = x$,*
3. *Svi imaju inverz: $(\forall x \in G)(\exists y \in G)\ x \cdot y = y \cdot x = e$.*

Ako uz navedena tri svojstva još vrijedi i $x \cdot y = y \cdot x$ za sve $x, y \in G$, onda kažemo da je grupa G komutativna ili Abelova.

Propozicija 3.1 *Neka je $m \in \mathbb{N}$. Tada vrijedi:*

1. *Skup $\mathbb{Z}_m$ s obzirom na zbrajanje modulo m Abelova je grupa.*
2. *Množenje modulo m na skupu $\mathbb{Z}_m$ asocijativno je, komutativno i posjeduje neutralni element $[1] \in \mathbb{Z}_m$.*
3. *Skup $\mathbb{Z}_m^*$ Abelova je grupa s obzirom na množenje modulo m ako i samo ako je m prost.*
4. *Množenje modulo m distributivno je s obzirom na zbrajanje modulo m, tj.*

$$[a]([b] + [c]) = [a][b] + [a][c],\ ([a], [b], [c] \in \mathbb{Z}_m).$$

Propozicija 3.2 *Neka je G grupa i $a \in G$.*

1. *Ako postoji $k \in \mathbb{N}$ t.d. $a^k = e$, onda je a konačnog reda. Štoviše, ako je $d \in \mathbb{N}$ najmanji broj sa svojstvom $a^d = e$, onda su $e, a, \ldots, a^{d-1}$ međusobno različiti i vrijedi $\langle a \rangle = \{e, a, \ldots, a^{d-1}\}$. Posebno, $|a| = d$.*

2. *Neka je a konačnog reda $|a| = d \in \mathbb{N}$ i $m \in \mathbb{Z}$. Tada je $a^m = e$ ako i samo ako d dijeli m.*

3. *Neka je a konačnog reda $|a| = d \in \mathbb{N}$ i p prost broj t.d. $d \mid p^k$ i $d \nmid p^{k-1}$. Tada je $d = p^k$.*

($\Leftarrow$) Neka je $S_{p-2} \equiv 0 \pmod{M_p}$. Tvrdimo da je tada M_p prost. Pretpostavimo da je M_p složen i neka je $q > 2$ prost faktor od M_p za koji vrijedi $q^2 \leq M_p$.

Neka je $\omega = 2 + \sqrt{3}$, $\bar{\omega} = 2 - \sqrt{3}$. Matematičkom indukcijom lako se dokazuje da vrijedi

$$S_n = \omega^{2^n} + \bar{\omega}^{2^n}.$$

Iz $S_{p-2} \equiv 0 \pmod{M_p}$ slijedi da postoji cijeli broj k takav da je $\omega^{2^{p-2}} + \bar{\omega}^{2^{p-2}} = kM_p$. Množenjem obje strane jednakosti s $\omega^{2^{p-2}}$ dobivamo

$$(\omega^{2^{p-2}})^2 = kM_p\omega^{2^{p-2}} - (\omega\bar{\omega})^{2^{p-2}},$$

pa je

$$\omega^{2^{p-1}} = kM_p\omega^{2^{p-2}} - 1. \tag{1}$$

Neka je $G \subseteq \mathbb{Z}_q(\sqrt{3})$ skup svih invertibilnih elemenata skupa

$$\mathbb{Z}_q(\sqrt{3}) = \{a + b\sqrt{3} | a, b \in \mathbb{Z}_q\} \subseteq \mathbb{R}.$$

Lako se provjeri da je G grupa, a zbog $|\mathbb{Z}_q(\sqrt{3})| = q^2$ i $0 \notin G$ vrijedi $|G| \leq q^2 - 1$.

Nadalje, iz $M_p \equiv 0 \pmod{q}$ i $\omega \in \mathbb{Z}_q(\sqrt{3})$ slijedi $kM_p\omega^{2^{p-2}} = 0$, što zajedno s (1) daje $\omega^{2^{p-1}} = -1$. Kvadriranjem obje strane jednakosti dobivamo

$$\omega^{2^p} = 1,$$

što pokazuje da je ω invertibilan u $\mathbb{Z}_q(\sqrt{3})$ s inverzom $\omega^{2^{p-1}}$. Iz toga slijedi da red elementa $\omega \in G$ dijeli 2^p. Štoviše, red mora biti jednak 2^p budući da je $\omega^{2^{p-1}} \neq 1$, pa red ne dijeli 2^{p-1}. Sada slijedi

$$2^p \leq q^2 - 1 < q^2 \leq M_p = 2^p - 1,$$

što je kontradikcija. Prema tome, Mersenneov broj M_p jest prost.

($\Rightarrow$) Pretpostavimo da je Mersenneov broj M_p prost. Treba pokazati da je tada $S_{p-2} \equiv 0 \pmod{M_p}$. Kako je $M_p, 3 \equiv 3 \pmod 4$ i $M_p \equiv 1 \pmod 3$, iz Gaussovog kvadratnog zakona reciprociteta slijedi da je 3 kvadratni neostatak modulo M_p, pa iz Eulerovog kriterija dobivamo

$$3^{\frac{M_p-1}{2}} \equiv -1 \pmod{M_p},$$

što zajedno s Lemom 2.1 daje

$$(1+\sqrt{3})^{M_p} \equiv 1 + (\sqrt{3})^{M_p} \equiv 1 + (\sqrt{3})3^{\frac{M_p-1}{2}} \equiv 1 - \sqrt{3} \pmod{M_p}.$$

Množenjem obje strane s $1+\sqrt{3}$ dobivamo

$$(1+\sqrt{3})^{M_p+1} \equiv -2 \pmod{M_p}.$$

Uočimo da je $(1+\sqrt{3})^2 = 2\omega$. Stoga vrijedi

$$(2\omega)^{\frac{M_p+1}{2}} \equiv -2 \pmod{M_p}.$$

Lijevu stranu jednakosti možemo zapisati u obliku

$$(2\omega)^{\frac{M_p+1}{2}} = 2^{\frac{M_p+1}{2}}\omega^{\frac{M_p+1}{2}} = 2 \cdot 2^{\frac{M_p-1}{2}}\omega^{\frac{M_p+1}{2}}.$$

Nadalje, 2 je kvadratni ostatak modulo M_p, budući da je $2^p \equiv 1 \pmod{M_p}$, iz čega slijedi $(2^{\frac{p+1}{2}})^2 \equiv 2 \pmod{M_p}$, pa iz Eulerovog kriterija dobivamo

$$2^{\frac{M_p-1}{2}} \equiv 1 \pmod{M_p}.$$

Sada imamo da je $2\omega^{\frac{M_p+1}{2}} \equiv -2 \pmod{M_p}$, to jest

$$\omega^{\frac{M_p+1}{2}} \equiv -1 \pmod{M_p}.$$

To možemo zapisati u obliku

$$\omega^{2^{p-1}} \equiv \omega^{2^{p-2}}\omega^{2^{p-2}} \equiv -1 \pmod{M_p},$$

a množenjem obje strane s $\bar{\omega}^{2^{p-2}}$ dobivamo

$$\omega^{2^{p-2}} + \bar{\omega}^{2^{p-2}} \equiv 0 \pmod{M_p},$$

što zajedno s $S_n = \omega^{2^n} + \bar{\omega}^{2^n}$ daje $S_{p-2} \equiv 0 \pmod{M_p}$, čime je dokaz završen.

□

Alternativno, možemo početi sa $S_0 = 10$; ili, ako je $p \equiv 3 \pmod 4$, također možemo koristiti $S_0 = 3$.

Lucas je znao samo da test ispituje dovoljne uvjete za prostost, i to samo za određene ograničene tipove vrijednosti od p. U 1930., Lehmer je dokazao da je uvjet nužan i da test vrijedi za bilo koji neparan prost broj p.

Primjer 3.5 *Ilustracija Lucas-Lehmerovog testa.*
Provjerimo je li $M_7 = 2^7 - 1 = 127$ *prost. Da bi Mersenneov broj* M_7 *bio prost, po Lucas-Lehmerovom testu mora vrijediti* $S_5 \equiv 0 \pmod{M_7}$.

$$\begin{aligned}
S_0 &= 4, \\
S_1 &= 4^2 - 2 = 14 \equiv 14 \pmod{127}, \\
S_2 &= 14^2 - 2 = 194 \equiv 67 \pmod{127}, \\
S_3 &= 67^2 - 2 = 4487 \equiv 42 \pmod{127}, \\
S_4 &= 42^2 - 2 = 1762 \equiv 111 \pmod{127}, \\
S_5 &= 111^2 - 2 = 12319 \equiv 0 \pmod{127}.
\end{aligned}$$

Vidimo da zaista vrijedi $S_5 \equiv 0 \pmod{M_7}$*, što znači da je Mersenneov broj* M_7 *prost.*

Primjer 3.6 *Sada provjerimo je li Mersenneov broj* $M_{11} = 2^{11} - 1 = 2047$ *prost broj. Da bi* M_{11} *bio prost, po Lucas-Lehmerovom testu mora vrijediti* $S_9 \equiv 0 \pmod{M_{11}}$.

$$\begin{aligned}
S_0 &= 4, \\
S_1 &= 4^2 - 2 = 14 \equiv 14 \pmod{2047}, \\
S_2 &= 14^2 - 2 = 194 \equiv 194 \pmod{2047}, \\
S_3 &= 194^2 - 2 = 37634 \equiv 788 \pmod{2047}, \\
S_4 &= 788^2 - 2 = 620942 \equiv 701 \pmod{2047}, \\
S_5 &= 701^2 - 2 = 491399 \equiv 119 \pmod{2047}, \\
S_6 &= 119^2 - 2 = 14159 \equiv 1877 \pmod{2047}, \\
S_7 &= 1877^2 - 2 = 3523127 \equiv 240 \pmod{2047}, \\
S_8 &= 240^2 - 2 = 57598 \equiv 282 \pmod{2047}, \\
S_9 &= 282^2 - 2 = 79522 \equiv 1736 \pmod{2047}.
\end{aligned}$$

Vidimo da je $S_9 \equiv 1736 \pmod{M_{11}}$*, pa prema tome Mersenneov broj* M_{11} *nije prost. Ovim testom ne dobiju se faktori nekog složenog broja, nego Lucas-Lehmerov ostatak, koji za* M_{11} *iznosi* 1736.

3.3. Pronalaženje Mersenneovih prostih brojeva korištenjem računala

Prvu primjenu elektroničkog računala na testiranje prostosti Mersenneovih brojeva napravio je 1951. godine A. M. Turing na Sveučilištu Manchester. No nisu nađeni novi prosti brojevi.

Program za testiranje Mersenneovih brojeva na **SWAC**-u (the National Bureau of Standards' Western Automatic Computer, na Institutu za Numeričku Analizu u Los Angelesu) predstavljen je 1952. godine. Načinio ga je Raphael Mitchel Robinson koristeći Lucasov test uz pomoć D.H. Lehmer i E. Lehmer. Program je prvi put isproban 30. siječnja kada su pronađena dva nova prosta broja (M_{521} i M_{607}); još tri prosta broja (M_{1279}, M_{2203}, M_{2281}) pronađena su 25. lipnja, 7. listopada i 9. listopada. Vrijeme trajanja testiranja je bilo minutu za prvi i sat vremena za preostala četiri nova prosta broja. Svaka minuta rada računala ekvivalentna je radu od više od godinu dana osobe koristeći stolni kalkulator.

Švedski matematičar Hans Ivar Riesel otkrio je 1957. godine osamnaesti poznati Mersenneov prost broj M_{3217} koristeći računalo **BESK** (Binary Electronic Sequence Calculator). To je bio najveći poznati Mersenneov prost broj od 1957. do 1961. godine, kada je Alexander Hurwitz otkrio sljedeća dva Mersenneova prosta broja, M_{4253} i M_{4423}, koristeći računalo **IBM 7090**.

Sljedeća tri Mersenneova prosta broja, M_{9689}, M_{9941} i M_{11213}, otkrio je 1963. godine Donald Bruce Gillies koristeći računalo **ILLIAC II** na Sveučilištu Illinois. Vrijeme računanja bilo je sat i 23 minute za prvi, sat i 30 minuta za drugi, te 2 sata i 15 minuta za treći Mersenneov prost broj.

Sljedeći Mersenneov prost broj, M_{19937}, otkrio je 1971. godine Bryant Tuckerman koristeći **IBM 360/91** računalo. Vrijeme računanja bilo je oko 35 minuta. Za usporedbu brzine više računala, vrijeme testiranja Mersenneovog broja M_{8191} na računalu Illiac I bilo je 100 sati, na računalu IBM 7090 bilo je nešto više od 5 sati, na računalu Illiac II 49 minuta, a na računalu IBM 360/91 oko 3 minute.

Landon Curt Noll i Laura Nickel, kao studenti, otkrili su sljedeći Mersenneov prost broj, M_{21701}, 1978. godine koristeći računalo **CDC Cyber 174**, a 1979. godine Noll je otkrio još jedan Mersenneov prost broj, M_{23209}. Za prvi broj trebalo je oko 7 minuta, a za drugi oko 8 minuta.

Sljedeći Mersenneov prost broj, M_{44497}, otkrili su David Slowinski i Harry L. Nelson 1979. godine koristeći **Cray 1** računalo, a 1982. godine koristeći isto računalo Slowinski je otkrio Mersenneov prost broj M_{86243}.

Walter N. Colquitt i Luther Welsh, Jr. otkrili su 1988. godine Mersenneov prost broj M_{110503} koristeći **NEC SX-2** računalo. Vrijeme računanja bilo je približno 11 minuta.

Koristeći računalo **Cray X-MP**, Slowinski je 1983. godine otkrio trideseti Mersenneov prost broj M_{132049}, te sljedeći Mersenneov prost broj, M_{216091}, 1985. godine. Slowinski i Paul Gage otkrili su 1992. godine koristeći računalo **Cray 2** prost broj M_{756839}, 1994. godine koristeći računalo **Cray C90** otkrili su prost broj M_{859433}, te 1996. godine prost broj $M_{1257787}$ koristeći računalo **Cray T94**.

Lucas-Lehmerov test za ispitivanje prostosti broja M_p, gdje je p jako velik, zahtijeva mnogo računanja, pa time i vrlo jaka računala. Programi Crandalla i Woltmana služe za određivanje velikih prostih brojeva. Ogromni Mersenneovi prosti brojevi otkriveni su uz pomoć **GIMPS**-a (Great Internet Mersenne Prime Search), kojeg je organizirao Woltman. George Woltman i Joel Armengaud otkrili su 1996. godine 35. Mersenneov prost broj $M_{1398269}$, zatim 1997. godine Gordon Spence i Woltman prost broj $M_{2976221}$, 1998. godine Roland Clarkson, Woltman i Scott Kurowski pronalaze prost broj $M_{3021377}$, 1999. godine Nayan Hajratwala, Woltman i Kurowski pronalaze prost broj $M_{6972593}$. Michael Cameron otkrio je 2001. godine prost broj $M_{13466917}$, a 2003. godine Michael Shafer prost broj $M_{20996011}$. Josh Findley 2004. godine otkrio je prost broj $M_{24036583}$, 2005. godine Martin Nowak, Woltman i Kurowski pronalaze prost broj $M_{25964951}$, te iste godine Curtis Cooper, Steven Boone, Woltman i Kurowski pronalaze prost broj $M_{30402457}$. Ista je četvorka 2006. godine otkrila prost broj $M_{32582657}$. Hans-Michael Elvenich, Woltman i Kurowski 2008. otkrili su prost broj $M_{37156667}$, a iste godine Edson Smith, Woltman i Kurowski pronalaze prost broj $M_{43112609}$, što je trenutno najveći poznati Mersenneov prost broj. Odd M. Strindmo, Woltman i Kurowski 2009. godine otkrili su prost broj $M_{42643801}$, što je zadnji otkriveni Mersenneov prost broj.

U *Tablici 3.1* slijedi prikaz svih poznatih prostih brojeva p za koje je M_p Mersenneov prost broj.

#	p	$M_p = 2^p - 1$	Broj znamenki broja M_p	Godina	Pronalazač
1.	2	3	1	-	-
2.	3	7	1	-	-
3.	5	31	2	-	-
4.	7	127	3	-	-
5.	13	8 191	4	1456.	Nepoznat
6.	17	131 071	6	1588.	Cataldi
7.	19	524 287	6	1588.	Cataldi
8.	31	2 147 483 647	10	1772.	Euler
9.	61	2305843009213693951	19	1883.	Pervushin
10.	89	618970019...449562111	27	1911.	Powers
11.	107	162259276...010288127	33	1914.	Powers
12.	127	170141183...884105727	39	1876.	Lucas
13.	521	686479766...115057151	157	1952.	Robinson

#	p	$M_p = 2^p - 1$	Br. znamenki	Godina	Pronalazač
14.	607	531137992...031728127	183	1952.	Robinson
15.	1 279	104079321...168729087	386	1952.	Robinson
16.	2 203	147597991...697771007	664	1952.	Robinson
17.	2 281	446087557...132836351	687	1952.	Robinson
18.	3 217	259117086...909315071	969	1957.	Riesel
19.	4 253	190797007...350484991	1 281	1961.	Hurwitz
20.	4 423	285542542...608580607	1 332	1961.	Hurwitz
21.	9 689	478220278...225754111	2 917	1963.	Gillies
22.	9 941	346088282...789463551	2 993	1963.	Gillies
23.	11 213	281411201...696392191	3 376	1963.	Gillies
24.	19 937	431542479...968041471	6 002	1971.	Tuckerman
25.	21 701	448679166...511882751	6 533	1978.	Noll & Nickel
26.	23 209	402874115...779264511	6 987	1979.	Noll
27.	44 497	854509824...011228671	13 395	1979.	Nelson & Slowinski
28.	86 243	536927995...433438207	25 962	1982.	Slowinski
29.	110 503	521928313...465515007	33 265	1988.	Colquitt & Welsh
30.	132 049	512740276...730061311	39 751	1983.	Slowinski
31.	216 091	746093103...815528447	65 050	1985.	Slowinski
32.	756 839	174135906...544677887	227 832	1992.	Slowinski & Gage
33.	859 433	129498125...500142591	258 716	1994.	Slowinski & Gage
34.	1 257 787	412245773...089366527	378 632	1996.	Slowinski & Gage
35.	1 398 269	814717564...451315711	420 921	1996.	Armengaud
36.	2 976 221	623340076...729201151	895 932	1997.	Spence
37.	3 021 377	127411683...024694271	909 526	1998.	Clarkson
38.	6 972 593	437075744...924193791	2 098 960	1999.	Hajratwala
39.	13 466 917	924947738...256259071	4 053 946	2001.	Cameron
40.	20 996 011	125976895...855682047	6 320 430	2003.	Shafer
41.	24 036 583	299410429...733969407	7 235 733	2004.	Findley
42.*	25 964 951	122164630...577077247	7 816 230	2005.	Nowak
43.*	30 402 457	315416475...652943871	9 152 052	2005.	Cooper & Boone
44.*	32 582 657	124575026...053967871	9 808 358	2006.	Cooper & Boone
45.*	37 156 667	202254406...308220927	11 185 272	2008.	Elvenich
46.*	42 643 801	169873516...562314751	12 837 064	2009.	Strindmo
47.*	43 112 609	316470269...697152511	12 978 189	2008.	Smith

Tablica 3.1. Prikaz svih poznatih prostih brojeva p za koje je M_p Mersenneov prost broj.

** Nije poznato postoje li neotkriveni Mersenneovi prosti brojevi između 41. i 47. Mersenneovog prostog broja jer još uvijek nisu testirani svi manji eksponenti. Prosti brojevi nisu uvijek otkrivani rastućim redoslijedom. Npr., 29. Mersenneov prost broj otkriven je poslije 30. i 31. Slično je trenutni najveći Mersenneov prost broj otkriven prije 45. i 46. iz gornje tablice.*

Kako bismo si vizualizirali veličinu najvećeg poznatog Mersenneovog prostog broja $M_{43\,112\,609}$, bilo bi potrebno 3 461 stranica sa 75 znamenki u redu i 50 redova po stranici da se prikaže dotični broj.

Najveći Mersenneov prost broj $(2^{43\,112\,609} - 1)$ ujedno je i najveći poznati prost broj.

3.4. Problemi vezani uz Mersenneove brojeve

Postoji mnogo neriješenih problema vezanih uz Mersenneove brojeve:

1. Postoji li beskonačno mnogo Mersenneovih prostih brojeva?

   Po hipotezi (Lenstra, Pomerance & Wagstaff, 1983.) postoji beskonačno mnogo Mersenneovih prostih brojeva.

   (a) Broj Mersenneovih prostih brojeva manjih od x je približno $\dfrac{e^\gamma}{\log 2} \log\log x$, gdje je γ Euler-Mascheronijeva konstanta jednaka

   $$\gamma = \lim_{x\to\infty} \left(\sum_{k=1}^{n} \frac{1}{k} - \ln(n) \right) \approx 0.577216.$$

   (b) Očekivani broj Mersenneovih prostih brojeva $2^p - 1$ s p između x i $2x$ približno je e^γ.

   (c) Vjerojatnost da je $2^p - 1$ prost broj približno je

   $$\frac{e^\gamma \log ap}{p \log 2}$$

   gdje je $a = 2$ ako je $p \equiv 3 \pmod 4$, $a = 6$ ako je $p \equiv 1 \pmod 4$.

2. Postoji li beskonačno mnogo složenih Mersenneovih brojeva?

   Iako još nije dokazano da postoji beskonačno mnogo složenih Mersenneovih brojeva, lako je dokazati da drugi nizovi, slični nizu Mersenneovih brojeva, sadrže beskonačno mnogo složenih brojeva. Sljedeći problem postavio je Powell 1982. godine, a rješenje je dao Israel 1983. godine.

   Teorem 3.8 *Ako su m, n cijeli brojevi takvi da je $m > 1$, $mn > 2$ (ovo isključuje $m = 2$, $n = 1$), onda postoji beskonačno mnogo složenih brojeva oblika $m^p - n$, gdje je p prost broj.*

Dokaz:
Neka je q prost broj koji dijeli $mn-1$, te $q \nmid m$. Ako je p prost broj takav da $p \equiv q-2 \pmod{q-1}$, onda $m(m^p - n) \equiv m(m^{q-2} - n) \equiv 1 - mn \equiv 0 \pmod{q}$, stoga q dijeli $m^p - n$. Po Dirichletovom teoremu, postoji beskonačno mnogo prostih brojeva p takvih da $p \equiv q-2 \pmod{q-1}$, stoga postoji beskonačno mnogo složenih brojeva $m^p - n$, gdje je p prost broj.

□

3. Mogu li Mersenneovi brojevi M_p, gdje je p prost broj, imati djelitelje koji su kvadrati nekog broja? Tj. je li svaki Mersenneov broj kvadratno slobodan?

Rotkiewicz je pokazao 1965. godine da ako je q prost i ako q^2 dijeli neki Mersenneov broj, onda je $2^{q-1} \equiv 1 \pmod{q^2}$.

Teorem 3.9 *Neka su p i q prosti brojevi. Ako q^2 dijeli M_p, onda $2^{(q-1)/2} \equiv 1 \pmod{q^2}$, pa specijalno, q je Wieferichov prost broj.*

Definicija 3.2 *Prost broj q je Wieferichov prost broj ako q^2 dijeli $2^{q-1} - 1$.*

Dokaz:
Uočimo da p i q moraju biti neparni. U Teoremu 3.4 je pokazano da ako q dijeli M_p, onda je $q = 2kp + 1$ za neki cijeli broj k. Stoga

$$2^p = 2^{(q-1)/2k} \equiv 1 \pmod{q^2}.$$

Potenciranjem na k-tu potenciju dobije se prvi rezultat teorema. Podsjetimo se da su Wieferichovi prosti brojevi oni prosti brojevi q za koje je $2^{q-1} \equiv 1 \pmod{q^2}$, pa je sada potenciranjem na $2k$-tu potenciju dokaz završen.

□

Jedini Wieferichovi prosti brojevi manji od $4\,000\,000\,000\,000$ su 1093 i 3511. Prvi ne zadovoljava tvrdnju teorema, a drugi nikad ne dijeli M_p (gdje je p prost broj). Prema tome je M_p kvadratno slobodan za sve proste brojeve manje od $4 \cdot 10^{12}$.

4. Ako je M_p Mersenneov prost broj, je li M_{M_p} također Mersenneov prost broj?

Proučavanjem Mersenneovih brojeva ustanovljeno je da kada se u formulu $2^p - 1$ umjesto p uvrsti neki od prva četiri Mersenneova prosta broja (tj. M_2, M_3, M_5, M_7), kao rezultat se dobije veći Mersenneov prost broj (redom M_3, M_7, M_{31}, M_{127}).

Matematičari su se nadali da će ovaj način dati beskonačan skup Mersenneovih prostih brojeva; odnosno, pretpostavka je bila da ako je broj M_p prost, onda je M_{M_p} također prost broj. No 1953. godine uz pomoć kompjutera je Wheeler pokazao da se uvrštavanjem u navedenu formulu sljedećeg Mersenneovog prostog broja

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

dobije složen broj.

Takvi Mersenneovi prosti brojevi, oblika $M_{M_p} = 2^{2^p-1} - 1$, gdje je p prost broj, zovu se dvostruki Mersenneovi prosti brojevi. Vjerojatno ne postoje drugi dvostruki Mersenneovi prosti brojevi osim M_{M_2}, M_{M_3}, M_{M_5} i M_{M_7}. Pronađeni su faktori za $p = 13, 17, 19, 31$ što znači da odgovarajući dvostruki Mersenneovi brojevi nisu prosti. Najmanji kandidat za sljedećeg dvostrukog Mersenneovog prostog broja je $M_{M_{61}} = 2^{2305843009213693951} - 1$, što je prevelik broj za provjeriti dosad poznatim testovima.

5. Sljedeći problem je neriješen, a postavio ga je Catalan 1876. godine.

   Promotrimo niz brojeva:

$$\begin{aligned} C_1 &= 2^2 - 1 = 3 = M_2, \\ C_2 &= 2^{C_1} - 1 = 7 = M_3, \\ C_3 &= 2^{C_2} - 1 = 127 = M_7, \\ C_4 &= 2^{C_3} - 1 = 2^{127} - 1 = M_{127}, \\ &\dots \\ C_{p+1} &= 2^{C_p} - 1 \\ &\dots \end{aligned}$$

   Jesu li svi C_p prosti brojevi? Postoji li beskonačno mnogo takvih prostih brojeva? Trenutno je nemoguće testirati C_5, broj koji ima više od 10^{37} znamenki.

6. Hipoteza (Bateman, Selfridge & Wagstaff, 1989.). Neka je p neparan prirodan broj (ne nužno prost). Ako su od sljedećih uvjeta zadovoljena dva, tada je i treći:

   (a) p je jednak $2^k \pm 1$ ili je jednak $4^k \pm 3$ (za neki $k \geq 1$).

   (b) M_p je prost broj.

   (c) $(2^p + 1)/3$ je prost broj (Wagstaffov prost broj).

Jedini poznati prosti brojevi koji zadovoljavaju sva tri uvjeta su

$$p = 3, 5, 7, 13, 17, 19, 31, 61, 127.$$

Hipoteza je provjerena za sve proste brojeve $p < 100\,000$ i za sve poznate Mersenneove proste brojeve, pa je vjerojatno da su ovo jedini prosti brojevi za koje vrijede gornja tri uvjeta.

4. Savršeni brojevi

Još jedan niz brojeva koji je imao veliki utjecaj na razvoj testova prostosti niz je savršenih brojeva.

Pitagorijanci su smatrali značajnim što je broj 6 jednak sumi svojih pravih djelitelja (svojih pozitivnih djelitelja, ne uključujući samog sebe):

$$6 = 1 + 2 + 3.$$

Sljedeći broj s ovom značajkom jest 28:

$$28 = 1 + 2 + 4 + 7 + 14.$$

U skladu s njihovom filozofijom pridavanja mističnih osobina brojevima, Pitagorijanci su brojeve tog oblika nazvali *savršenima*.

Definicija 4.1 *Pozitivan cijeli broj N savršen je broj ako je jednak sumi svojih pravih djelitelja.*

Ako sa $\sigma(N) = \sum_{d|N} d$ označimo sumu svih pozitivnih djelitelja od N (uključujući i N), N je savršen ako vrijedi $\sigma(N) = 2N$. Na primjer,

$$\sigma(6) = 1 + 2 + 3 + 6 = 2 \cdot 6.$$

$$\sigma(28) = 1 + 2 + 4 + 7 + 14 + 28 = 2 \cdot 28.$$

Prema tome, 6 i 28 su savršeni brojevi.

Mnogo su se stoljeća filozofi bavili više mističnim ili religijskim značajem savršenih brojeva nego njihovim matematičkim svojstvima. Tako je Sveti Augustin objasnio da je Bog mogao stvoriti svijet odjednom, ali je izabrao to učiniti u šest dana jer je savršenstvo stvaranja svijeta simbolizirano savršenim brojem 6. Rani komentatori Starog zavjeta objašnjavali su da je savršenstvo svemira reprezentirano brojem 28, brojem dana koji je potreban da Mjesec obiđe Zemlju.

4.1. Parni savršeni brojevi

Problem određivanja općenitog oblika savršenih brojeva datira gotovo od matematičkih početaka. Djelomično je to riješio Euklid u Knjizi IX svojih *Elemenata* (oko 300. godine

prije Krista). Primijetio je da su prva četiri savršena broja specifičnog oblika:

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

Primijetimo da nedostaju brojevi

$$90 = 2^3(1+2+2^2+2^3) = 8 \cdot 15$$

i

$$2016 = 2^5(1+2+2^2+\cdots+2^5) = 32 \cdot 63.$$

Euklid je istaknuo da je to zato što su $15 = 3 \cdot 5$ i $63 = 3^2 \cdot 7$ složeni brojevi, dok su brojevi $3, 7, 31, 127$ svi redom prosti.

Teorem 4.1 (Euklid) *Ako je broj $2^n - 1$ prost, onda je broj $N = 2^{n-1}(2^n - 1)$ savršen.*

Dokaz:
Očito je da su $2^n - 1$ i 2 jedini prosti faktori od N. Budući da se broj $2^n - 1$ pojavljuje kao zaseban prost broj, imamo jednostavno da je

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

Stoga je

$$\sigma(N) = \sigma(2^{n-1})\sigma(2^n - 1) = \Big(\frac{2^n - 1}{2 - 1}\Big)2^n = 2^n(2^n - 1) = 2N.$$

Prema tome, broj N je savršen.

□

Starim Grcima bila su poznata samo četiri savršena broja. Nicomachus je u svojoj knjizi *Introductio Arithmeticae* (oko 100. godine poslije Krista) kao savršene brojeve naveo

$$P_1 = 6,\ P_2 = 28,\ P_3 = 496,\ P_4 = 8128,$$

te je zaključio da postoji jedan jednoznamenkast, jedan dvoznamenkast, jedan troznamenkast i jedan četveroznamenkast savršen broj. Na osnovu toga nastala je sljedeća hipoteza.

1. n-ti savršen broj P_n sadrži točno n znamenki;
2. parni savršeni brojevi završavaju naizmjence na 6 i 8.

Obje pretpostavke su pogrešne. Ne postoji savršen broj s pet znamenki. Sljedeći savršen broj je $P_5 = 33\,550\,336$. Iako posljednja znamenka od P_5 jest 6, sljedeći savršen broj $P_6 = 8\,589\,869\,056$ završava također znamenkom 6, a ne znamenkom 8 kao što je pretpostavljeno. No kasnije će biti pokazano da parni savršeni brojevi ipak završavaju na 6 ili 8, ali ne nužno naizmjence.

Da su Nicomachusove pretpostavke pogrešne, pokazao je Cataldi kada je dokazao da su peti, šesti i sedmi savršeni brojevi sljedeći:

$$\begin{aligned} 33\,550\,336 &= 2^{12}(2^{13}-1), \\ 8\,589\,869\,056 &= 2^{16}(2^{17}-1), \\ 137\,438\,691\,328 &= 2^{18}(2^{19}-1). \end{aligned}$$

Cataldi nije bio prvi koji je otkrio ove savršene brojeve, ali njegovi su dokazi prvi poznati dokazi tih činjenica. Prije njega otkrio ih je arapski matematičar Ismail ibn Fallus (1194.-1239.) koji je slijedio Nicomachusov rad, te dao deset savršenih brojeva, ali su se tri pokazala netočnima. Zatim je oko 1460. godine Johann Müller Regiomontanus ponovno otkrio peti i šesti savršeni broj. Hudalrichus Regius otkrio je 1536. godine prvi prost broj n takav da $2^{n-1}(2^n-1)$ nije savršen broj, kada je u svojoj knjizi *Utriusque Arithmetices* pokazao da je $2^{11}-1 = 2047 = 23 \cdot 89$. Također je ponovno otkrio peti savršeni broj. J. Scheybl otkrio je 1555. godine ponovno šesti savršeni broj ali je to ostalo neprimijećeno do 1977. godine.

Izuzetan doprinos dao je 1640. godine Fermat, čijim je radom na savršenim brojevima nastao Mali Fermatov teorem, uz pomoć kojeg je onda pokazao da su $2^{23}-1$ i $2^{37}-1$ složeni brojevi. Time je pokazao da je Cataldi pogrešno pretpostavio da je $N = 2^{n-1}(2^n-1)$ savršen broj za $n = 23$ i $n = 37$. Mersenne je bio vrlo zainteresiran za Fermatove rezultate o savršenim brojevima, te je uskoro iznio i svoju tvrdnju, te su tako brojevi oblika $2^n - 1$ dobili ime po njemu.

Oko 2000 godina poslije Euklida, Euler je dokazao da su svi parni savršeni brojevi oblika danog u Teoremu 4.1.

Teorem 4.2 (Euler) *Ako je N paran savršen broj, onda je N oblika $N = 2^{n-1}(2^n-1)$, gdje je $2^n - 1$ prost broj.*

Dokaz:
Neka je $N = 2^{n-1}m$ savršen broj, gdje je m neparan. Budući da 2 ne dijeli m, 2^{n-1} i m su relativno prosti, tj. $(2^{n-1}, m) = 1$, iz čega slijedi da je

$$\sigma(N) = \sigma(2^{n-1}m) = \sigma(2^{n-1})\sigma(m) = \Big(\frac{2^n-1}{2-1}\Big)\sigma(m) = (2^n-1)\sigma(m).$$

Budući da je N savršen, imamo

$$\sigma(N) = 2N = 2(2^{n-1}m) = 2^n m.$$

Te dvije relacije zajedno daju

$$2^n m = (2^n - 1)\sigma(m).$$

Budući da je $2^n - 1$ neparan, $(2^n - 1)$ dijeli m, pa možemo pisati $m = (2^n - 1)k$. Sada je

$$(2^n - 1)\sigma(m) = 2^n(2^n - 1)k,$$

što implicira

$$\sigma(m) = 2^n k = (2^n - 1)k + k = m + k.$$

Ali k dijeli m, pa $\sigma(m) = m + k$ znači da m ima samo dva pozitivna djelitelja, k i m, što nadalje implicira da je $k = 1$. Prema tome, $\sigma(m) = m + 1$ i m je prost broj. Budući da $(2^n - 1)$ dijeli m, $2^n - 1 = m$. Stoga je $N = 2^{n-1}(2^n - 1)$, gdje je $2^n - 1$ prost broj.

□

Sada je vidljivo da je pronalaženje parnih savršenih brojeva usko vezano uz pronalaženje prostih brojeva oblika $2^n - 1$, odnosno Mersenneovih prostih brojeva.

Euler je znao za prvih sedam savršenih brojeva, $2^{n-1}(2^n - 1)$ za $n = 2, 3, 5, 7, 13, 17, 19$, a kako je 1772. godine pokazao da je Mersenneov broj M_{31} prost, otkriven je osmi savršeni broj:

$$2\,305\,843\,008\,139\,952\,128 = 2^{30}(2^{31} - 1).$$

Peter Barlow 1811. godine u svojoj knjizi *Elementary Investigation of the Theory of Numbers* pogrešno je ustvrdio da je $2^{30}(2^{31} - 1)$ najveći savršeni broj što će ikad biti otkriven.

Budući da je dosad poznato 47 Mersenneovih prostih brojeva, poznat je jednak broj parnih savršenih brojeva. U *Tablici 4.1* slijedi prikaz svih poznatih prostih brojeva n za koje je $N = 2^{n-1}(2^n - 1)$ paran savršen broj.

#	n	$N = 2^{n-1}(2^n - 1)$	Broj znamenki broja N
1.	2	6	1
2.	3	28	2
3.	5	496	3
4.	7	8 128	4
5.	13	33 550 336	8
6.	17	8 589 869 056	10

#	n	$N = 2^{n-1}(2^n - 1)$	Broj znamenki broja N
7.	19	137 438 691 328	12
8.	31	2305843008139952128	19
9.	61	265845599...953842176	37
10.	89	191561942...548169216	54
11.	107	131640364...783728128	65
12.	127	144740111...199152128	77
13.	521	235627234...555646976	314
14.	607	141053783...537328128	366
15.	1 279	541625262...984291328	770
16.	2 203	108925835...453782528	1 327
17.	2 281	994970543...139915776	1 373
18.	3 217	335708321...628525056	1 937
19.	4 253	182017490...133377536	2 561
20.	4 423	407672717...912534528	2 663
21.	9 689	114347317...429577216	5 834
22.	9 941	598885496...073496576	5 985
23.	11 213	395961321...691086336	6 751
24.	19 937	931144559...271942656	12 003
25.	21 701	100656497...141605376	13 066
26.	23 209	811537765...941666816	13 973
27.	44 497	365093519...031827456	26 790
28.	86 243	144145836...360406528	51 924
29.	110 503	136204582...603862528	66 530
30.	132 049	131451295...774550016	79 502
31.	216 091	278327459...840880128	130 100
32.	756 839	151616570...565731328	455 663
33.	859 433	838488226...416167936	517 430
34.	1 257 787	849732889...118704128	757 263
35.	1 398 269	331882354...723375616	841 842
36.	2 976 221	194276425...174462976	1 791 864
37.	3 021 377	811686848...022457856	1 819 050
38.	6 972 593	955176030...123572736	4 197 919
39.	13 466 917	427764159...863021056	8 107 892
40.	20 996 011	793508909...206896128	12 640 858
41.	24 036 583	448233026...572950528	14 471 465
42.	25 964 951	746209841...791088128	15 632 458
43.	30 402 457	497437765...164704256	18 304 103
44.	32 582 657	775946855...577120256	19 616 714
45.	37 156 667	204534225...074480128	22 370 543
46.	42 643 801	144285057...377253376	25 674 127
47.	43 112 609	500767156...145378816	25 956 377

Tablica 4.1. Prikaz svih poznatih prostih brojeva n za koje je $N = 2^{n-1}(2^n - 1)$ paran savršen broj.

4.1.1. Svojstva parnih savršenih brojeva

U sljedećim propozicijama prikazana su neka svojstva parnih savršenih brojeva.

Propozicija 4.1 *Ako je broj N paran savršen broj, onda je broj N trokutast.*

Dokaz:
Kažemo da je T trokutast broj ako vrijedi

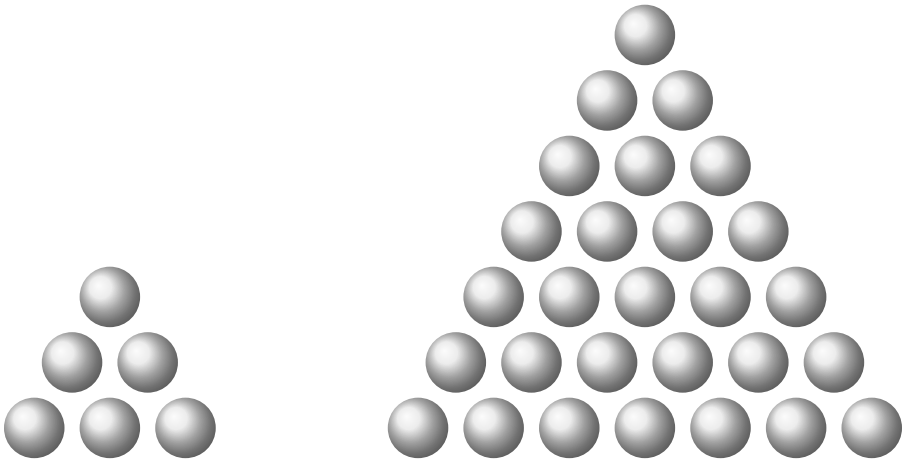
$$T = \sum_{i=1}^{k} i = 1 + 2 + \cdots + k = \frac{1}{2}k(k+1)$$

za neki k. Znamo da su parni savršeni brojevi oblika

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

Neka je $2^n = k + 1$. Sada su parni savršeni brojevi oblika $N = \frac{1}{2}(k+1)k$. Prema tome, parni savršeni brojevi su trokutasti brojevi.

□



Slika 4.1. Prikaz trokutastih parnih savršenih brojeva $N = 6$ i $N = 28$.

Propozicija 4.2 *Ako je $N = 2^{n-1}(2^n - 1)$ paran savršen broj, $N \neq 6$, onda je*

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

Dokaz:
Koristimo formulu

$$\sum_{i=1}^{n} i^3 = \frac{n^2(n+1)^2}{4},$$

koju se lako može dokazati matematičkom indukcijom. Neka je $m = 2^{(n-1)/2}$. Onda imamo

$$\begin{aligned} 1^3 + 3^3 + \cdots + (2m-1)^3 &= \left(1^3 + 2^3 + \cdots + (2m)^3\right) - \left(2^3 + 4^3 + \cdots + (2m)^3\right) \\ &= \frac{(2m)^2(2m+1)^2}{4} - 2^3\frac{m^2(m+1)^2}{4} \\ &= m^2(2m+1)^2 - 2m^2(m+1)^2 \\ &= m^2(4m^2 + 4m + 1 - 2m^2 - 4m - 2) = m^2(2m^2 - 1). \end{aligned}$$

Sada zamijenimo m i dobijemo

$$1^3 + 3^3 + \cdots + (2^{(n-1)/2} - 1)^3 = 2^{n-1}(2^n - 1),$$

čime je dokaz završen. Prema tome, svaki paran savršen broj $N = 2^{n-1}(2^n - 1)$, osim 6, jednak je sumi kubova prvih $2^{(n-1)/2}$ neparnih prirodnih brojeva.

□

Primjer 4.1 *Ilustracija Propozicije 4.2.*

$$\begin{aligned} 28 &= 1^3 + 3^3, \\ 496 &= 1^3 + 3^3 + 5^3 + 7^3, \\ 8128 &= 1^3 + 3^3 + 5^3 + 7^3 + 9^3 + 11^3 + 13^3 + 15^3. \end{aligned}$$

Propozicija 4.3 *Ako je savršen broj $N = 2^{n-1}(2^n - 1)$ zapisan u bazi 2, onda ima $2n-1$ znamenki, od čega su prvih n jedinice, a posljednjih $n-1$ nule.*

Dokaz:

Definicija 4.2 *Zapis broja $B \in \mathbb{N}$ u bazi $b = 2$ je oblika $B = b_k \cdot 2^k + \cdots + b_1 \cdot 2 + b_o$, $b_k > 0$, $b_i \in \{0, 1\}$, gdje su b_i binarne znamenke. Skraćeni zapis je $B = (b_k \cdots b_0)_2$.*

Dokaz izravno slijedi iz definicije binarnog zapisa brojeva i činjenice da je

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

□

Primjer 4.2 *Ilustracija Propozicije 4.3.*

$$\begin{aligned} 6 &= 110_2, \\ 28 &= 11100_2, \\ 496 &= 111110000_2, \\ 8128 &= 1111111000000_2. \end{aligned}$$

Propozicija 4.4 *Svaki paran savršen broj završava na* 6 *ili* 8*; to jest,* $N \equiv 6 \pmod{10}$ *ili* $N \equiv 8 \pmod{10}$.

Dokaz:
Svaki prost broj $n > 2$ je oblika $4m + 1$ ili $4m + 3$. U prvom slučaju,

$$\begin{aligned} N &= 2^{n-1}(2^n - 1) = 2^{4m}(2^{4m+1} - 1) = 2^{8m+1} - 2^{4m} = 2 \cdot 16^{2m} - 16^m \\ &\equiv 2 \cdot 6 - 6 \equiv 6 \pmod{10}, \end{aligned}$$

budući da se induktivno lako može vidjeti da vrijedi $16^t \equiv 6 \pmod{10}$ za svaki pozitivni cijeli broj t.
Slično, u drugom slučaju,

$$\begin{aligned} N &= 2^{n-1}(2^n - 1) = 2^{4m+2}(2^{4m+3} - 1) = 2^{8m+5} - 2^{4m+2} = 2 \cdot 16^{2m+1} - 4 \cdot 16^m \\ &\equiv 2 \cdot 6 - 4 \cdot 6 \equiv -12 \equiv 8 \pmod{10}. \end{aligned}$$

Konačno, ako je $n = 2$, onda je $N = 6$, i time su pokrivene sve mogućnosti. Prema tome, svaki paran savršen broj ima posljednju znamenku jednaku 6 ili 8.

□

Sljedeća propozicija daje još precizniji rezultat.

Propozicija 4.5 *Svaki paran savršen broj završava na* 6 *ili* 28.

Dokaz:
U prethodnoj propoziciji pokazano je da je $N \equiv 6 \pmod{10}$ za prost broj n oblika $4m+1$. Sada trebamo pokazati da ako je n oblika $4m + 3$, onda vrijedi $N \equiv 28 \pmod{100}$. Primijetimo da je

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

Nadalje, za $n > 2$ očito 4 dijeli 2^{n-1}, pa je broj koji se sastoji od posljednje dvije znamenke broja 2^{n-1} djeljiv sa 4. Situacija je sljedeća: posljednja znamenka broja 2^{n-1} je 4, dok 4 dijeli posljednje dvije znamenke. Stoga imamo sljedeće mogućnosti:

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

Iz toga slijedi da je

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

te dobivamo da je

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

Da bi dokaz bio završen, treba pokazati da su svi dobiveni brojevi kongruentni 28 modulo 100. Za $4 \cdot 7 = 28$ je to očigledno. Zatim imamo

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

Preostala tri slučaja mogu se provjeriti na sličan način.

□

Promotrimo li *Tablicu 4.1*, uočit ćemo da svi parni savršeni brojevi zaista završavaju na 6 ili 28.

Propozicija 4.6 *Iterativna suma znamenki parnog savršenog broja ($N > 6$) jednaka je* 1.

Dokaz:
Neka je $N = \overline{d_k \dots d_1 d_0}$, gdje su d_i, $i = 0, 1, ..., k$, decimalne znamenke i $d_k \neq 0$. Tada vrijedi

$$N = \sum_{i=0}^{k} d_i \cdot 10^i \equiv \sum_{i=0}^{k} d_i \cdot 1^i = \sum_{i=0}^{k} d_i \pmod{9}.$$

Prema tome, N je kongruentan sumi svojih znamenki modulo 9, odnosno kongruentan je iterativnoj sumi svojih znamenki modulo 9. Svaki paran savršen broj je oblika $N = 2^{n-1}(2^n - 1)$, gdje su n i $2^n - 1$ prosti brojevi. Za prva dva savršena broja $N = 6, 28$ je n redom jednak 2 i 3. Za parne savršene brojeve $N > 28$ je $n > 3$ iz čega slijedi da je n neparan i oblika $6k + 1$ ili $6k + 5$. Ako je $n = 6k + 1$, tada vrijedi

$$N = 2^{6k}(2^{6k+1} - 1) = 64^k(2 \cdot 64^k - 1) \equiv 1^k(2 \cdot 1^k - 1) = 1 \pmod{9}.$$

Slično, ako je $n = 6k + 5$, vrijedi

$$N = 2^{6k+4}(2^{6k+5} - 1) \equiv 16 \cdot 64^k(32 \cdot 64^k - 1) \equiv -2 \cdot 1^k(-4 \cdot 1^k - 1) \equiv 1 \pmod{9}.$$

Budući da je 28 također kongruentan $1 \pmod{9}$, slijedi da je iterativna suma znamenki svih parnih savršenih brojeva $N > 6$ jednaka 1.

□

Primjer 4.3 *Ilustracija Propozicije 4.6.*

$$\begin{aligned} 28 &= 2+8=10; 1+0=1; \\ 496 &= 4+9+6=19; 1+9=10:1+0=1; \\ 8128 &= 8+1+2+8=19; 1+9=10; 1+0=1. \end{aligned}$$

Propozicija 4.7 *Suma recipročnih vrijednosti svih pozitivnih djelitelja nekog savršenog broja jednaka je* 2.

Dokaz:
Neka je N savršen broj. Uočimo da ako $d \mid N$, onda je $kd = N$ za neki k, pa je $k = (N/d) \mid N$. Vrijedi i obrnuto iz čega slijedi da $d \mid N$ ako i samo ako $(N/d) \mid N$. Sada je

$$\sum_{d|N} \frac{1}{d} = \frac{\sum_{d|N}(N/d)}{N} = \frac{\sum_{d|N} d}{N} = \frac{\sigma(N)}{N} = \frac{2N}{N} = 2,$$

čime je dokaz završen.

□

Primjer 4.4 *Ilustracija Propozicije 4.7.*

$$\begin{aligned} \frac{1}{6}+\frac{1}{3}+\frac{1}{2}+\frac{1}{1} &= 2, \\ \frac{1}{28}+\frac{1}{14}+\frac{1}{7}+\frac{1}{2}+\frac{1}{1} &= 2, \\ \frac{1}{496}+\frac{1}{248}+\frac{1}{124}+\frac{1}{62}+\frac{1}{31}+\frac{1}{16}+\frac{1}{8}+\frac{1}{4}+\frac{1}{2}+\frac{1}{1} &= 2. \end{aligned}$$

Jedno od neriješenih pitanja vezanih uz parne savršene brojeve jest postoji li beskonačno mnogo parnih savršenih brojeva, što se nadovezuje na pitanje postoji li beskonačno mnogo Mersenneovih prostih brojeva o čemu je pisano u Poglavlju 3.4. Ako postoji beskonačno mnogo Mersenneovih prostih brojeva, onda postoji i beskonačno mnogo parnih savršenih brojeva.

4.2. Neparni savršeni brojevi

Drugi neriješeni problem vezan uz savršene brojeve jest postoje li neparni savršeni brojevi. Iako su postavljeni mnogi uvjeti koje bi neparan savršen broj N trebao zadovoljavati, još uvijek nije pronađen niti jedan takav broj. No s druge strane, nije niti dokazano da neparni savršeni brojevi ne postoje. Prvi uvjet dao je Euler, koji je pokazao da je svaki neparan savršen broj N oblika

$$N = p^k q_1^{2a_1} q_2^{2a_2} \cdots q_r^{2a_r},$$

gdje su $p, q_1, q_2, \ldots, q_r$ različiti neparni prosti brojevi i $p \equiv k \equiv 1 \pmod 4$.

Teorem 4.3 (Euler) *Neka je N neparan savršen broj. Tada je faktorizacija od N oblika $N = p^{4e+1} q_1^{2a_1} \cdots q_r^{2a_r}$, gdje je $p \equiv 1 \pmod 4$.*

Dokaz:
Neka je $N = l_1^{e_1} l_2^{e_2} \cdots l_s^{e_s}$ za neke proste brojeve $l_1, l_2, \ldots, l_s$. Budući da je N neparan, svi l_i su neparni. Konačno, $\sigma(N) = 2N$. Budući da je

$$\sigma(N) = \sigma(l_1^{e_1} l_2^{e_2} \cdots l_s^{e_s}) = \sigma(l_1^{e_1}) \sigma(l_2^{e_2}) \cdots \sigma(l_s^{e_s}),$$

promatramo $\sigma(l^e) = 1 + l + l^2 + \cdots + l^e$, sumu $e+1$ neparnih brojeva, koja je neparna samo ako je e paran. Kako je

$$\sigma(l_1^{e_1} l_2^{e_2} \cdots l_s^{e_s}) = \sigma(l_1^{e_1}) \sigma(l_2^{e_2}) \cdots \sigma(l_s^{e_s}) = 2 l_1^{e_1} l_2^{e_2} \cdots l_s^{e_s},$$

imamo samo jedan faktor jednak 2. Stoga su parni svi e_i osim jednog, recimo e_1. Prema tome, $N = l_1^{e_1} q_1^{2a_1} \cdots q_r{}^{2a_r}$.

Nadalje očito vrijedi da $2 \mid \sigma(l_1^{e_1})$, ali $4 \nmid \sigma(l_1^{e_1})$. Budući da je l_1 neparan, e_1 je neparan. Sada vidimo da vrijedi ili $l_1 \equiv 1 \pmod 4$ ili $l_1 \equiv -1 \pmod 4$. Ali ako je $l_1 \equiv -1 \pmod 4$, onda vrijedi

$$\begin{aligned} \sigma(l_1^{e_1}) &= 1 + l_1 + l_1^2 + l_1^3 \cdots + l_1^{e_1 - 1} + l_1^{e_1} \\ &\equiv 1 + (-1) + 1 + (-1) + \cdots + 1 + (-1) \equiv 0 \pmod 4, \end{aligned}$$

što je očito kontradikcija budući da $4 \nmid \sigma(l_1^{e_1})$. Prema tome, $l_1 \equiv 1 \pmod 4$. Sada vrijedi

$$\begin{aligned} \sigma(l_1^{e_1}) &= 1 + l_1 + l_1^2 + l_1^3 \cdots + l_1^{e_1 - 1} + l_1^{e_1} \\ &\equiv 1 + 1 + 1 + 1 + \cdots + 1 + 1 \equiv e_1 + 1 \pmod 4. \end{aligned}$$

Budući da je e_1 neparan, vrijedi ili $e_1 + 1 \equiv 0 \pmod 4$ ili $e_1 + 1 \equiv 2 \pmod 4$. Ako je $e_1 + 1 \equiv 0 \pmod 4$, onda $4 \mid \sigma(l_1^{e_1})$ što je kontradikcija. Prema tome, $e_1 + 1 \equiv 2 \pmod 4$ onda i samo onda ako je $e_1 + 1 = 4e + 2$, to jest, $e_1 = 4e + 1$. Sada slijedi da je

$$N = p^{4e+1} q_1^{2a_1} \cdots q_r^{2a_r}, \text{ za } p \equiv 1 \pmod 4,$$

čime je dokaz završen.

□

Svaki neparan savršen broj N može se zapisati u obliku

$$N = p^k q_1^{2a_1} \cdots q_r^{2a_r} = p^k (q_1^{a_1} \cdots q_r^{a_r})^2 = p^k m^2.$$

Korolar 4.1 *Ako je N neparan savršen broj, onda je N oblika $N = p^k m^2$, gdje je p prost broj, $p \nmid m$, te $p \equiv k \equiv 1 \pmod 4$. Posebno, $N \equiv 1 \pmod 4$.*

Dokaz:
Jedino posljednja tvrdnja nije očigledna. Budući da je $p \equiv 1 \pmod 4$, imamo $p^k \equiv 1 \pmod 4$. Primijetimo da m mora biti neparan. Stoga je $m \equiv 1 \pmod 4$ ili $m \equiv 3 \pmod 4$. Nakon kvadriranja vrijedi $m^2 \equiv 1 \pmod 4$. Sada slijedi

$$N = p^k m^2 \equiv 1 \cdot 1 \equiv 1 \pmod 4.$$

□

Teorem 4.4 *Svaki neparan savršen broj N suma je dva kvadrata.*

Dokaz:
Neka je $N = p^k m^2$ neparan savršen broj. Budući da je $p \equiv 1 \pmod 4$, po Teoremu 2.12 možemo p zapisati kao sumu dva kvadrata, pa prema Lemi 2.2 i p^k možemo zapisati kao sumu dva kvadrata. Dakle, $p^k = r^2 + s^2$ za neke pozitivne cijele brojeve r i s. Množenjem obje strane s m^2 dobivamo

$$N = p^k m^2 = m^2(r^2 + s^2) = (mr)^2 + (ms)^2.$$

Prema tome, svaki neparan savršen broj je suma dva kvadrata.

□

Rudolf Steuerwald pokazao je 1937. godine da ako je $N = p^k q_1^{2a_1} q_2^{2a_2} \cdots q_r^{2a_r}$ neparan savršen broj, gdje su $p, q_1, q_2, \ldots, q_r$ različiti neparni prosti brojevi i $p \equiv k \equiv 1 \pmod 4$, onda ne mogu svi a_i biti jednaki 1; to jest, ako je $N = p^k q_1^2 q_2^2 \cdots q_r^2$ neparan broj s $p \equiv k \equiv 1 \pmod 4$, onda N nije savršen. Zatim je 1941. godine Hans-Joachim Kanold pokazao da niti mogu svi a_i biti jednaki 2, niti može jedan a_i biti jednak 2 dok su svi ostali jednaki 1. Peter Hagis, Jr. i Wayne L. McDaniel dokazali su 1972. godine da ne mogu svi a_i biti jednaki 3. Douglas E. Iannucci i Ronald M. Sorli dokazali su 2003. godine da ako vrijedi $a_i \equiv 1 \pmod 3$ i $a_i \equiv 2 \pmod 5$ za sve i, onda $3 \nmid N$.

Broj prostih faktora neparnog savršenog broja N

Za neparan savršen broj

$$N = p^k \prod_{i=1}^{r} q_i^{2a_i},$$

gdje su $p, q_1, q_2, \ldots, q_r$ različiti neparni prosti brojevi i $p \equiv k \equiv 1 \pmod 4$, broj prostih faktora je definiran s

$$\Omega(N) := k + 2\sum_{i=1}^{r} a_i.$$

Broj različitih prostih faktora neparnog savršenog broja N je definiran s

$$\omega(N) := 1 + r.$$

Graeme L. Cohen dokazao je 1982. godine da neparan savršen broj N ima najmanje 23 prosta faktora, to jest $\Omega(N) \geq 23$. M. Sayers dokazao je 1986. godine da neparan savršen broj N ima najmanje 29 prostih faktora. Iannucci i Sorli dokazali su 2003. godine da neparan savršen broj N ima najmanje 37 prostih faktora. Kevin G. Hare dokazao je 2004. godine da neparan savršen broj N ima najmanje 47 prostih faktora, a 2005. godine došao je do rezultata da ih mora biti najmanje 75.

Hare je objasnio da je 75 kao granicu izabrao jer je "estetski lijep" broj, te iako je isto mogao dokazati i za 77, a moguće i za 79, za time nije bilo potrebe jer se se ne bi saznalo ništa značajno, a 75 kao granica je dovoljno da bi se pokazalo poboljšanje u odnosu na prethodnu metodu kojom se pronašla granica od najmanje 47 prostih faktora. Sljedeći cilj je 101, što je sadašnjim metodama i računalima izvan dosega. Za usporedbu, za dokaz rezultata za 75 trebalo je 25 dana, a za dokaz rezultata za 101 trebalo bi 11 godina (vidjeti [10]).

Broj različitih prostih faktora neparnog savršenog broja N

Benjamin Peirce dokazao je 1832. godine da neparan savršen broj N ima najmanje 4 različita prosta faktora, to jest $\omega(N) \geq 4$. Do istog je rezultata samostalno došao James Joseph Sylvester 1888. godine, a iste je godine dokazao i da je $\omega(N) \geq 5$. Zatim je I. S. Gradstein 1925. godine dokazao da je $\omega(N) \geq 6$. U 70-im godinama prošlog stoljeća Neville Robbins i Carl Pomerance neovisno su dokazali da je $\omega(N) \geq 7$. Joseph E. Z. Chein dokazao je 1979. godine da je $\omega(N) \geq 8$, a isto je neovisno učinio Hagis 1980. godine. Nadalje, Hagis i Masao Kishore 1983. godine neovisno su dokazali da ako $3 \nmid N$, onda je $\omega(N) \geq 11$. Konačno, Pace P. Nielsen dokazao je 2006. godine da je $\omega(N) \geq 9$, a ako $3 \nmid N$, onda je $\omega(N) \geq 12$. Karl K. Norton dokazao je 1960. godine da ako $3 \nmid N$ i $5 \nmid N$, onda je $\omega(N) \geq 15$, a Charles Greathouse 2005. godine dokazao je da ako $3 \nmid N$ i $5 \nmid N$, onda je $\omega(N) \geq 17$. Catalan je 1888. godine dokazao da ako $3 \nmid N$, $5 \nmid N$ i $7 \nmid N$, onda je $\omega(N) \geq 26$, Norton je 1960. godine dokazao da ako $3 \nmid N$, $5 \nmid N$ i $7 \nmid N$, onda je $\omega(N) \geq 27$, a Greathouse je 2005. godine dokazao da ako $3 \nmid N$, $5 \nmid N$ i $7 \nmid N$, onda je $\omega(N) \geq 29$. John Voight dokazao je 2003. godine da ako je $\omega(N) = 8$, onda $5 \mid N$.

Donja granica veličine neparnog savršenog broja N

Turcaninov je 1908. godine pokazao da je donja granica neparnog savršenog broja N jednaka $2 \cdot 10^6$, to jest da je neparan savršen broj N veći od $2 \cdot 10^6$. Kanold je 1957. godine pokazao da je neparan savršen broj N veći od 10^{20}. Zatim je B. Tuckerman 1973. godine pokazao da je neparan savršen broj N veći od 10^{36}, a iste je godine Hagis pokazao da je N veći od 10^{50}. Richard P. Brent i Graeme L. Cohen pokazali su 1989. godine da je neparan savršen broj N veći od 10^{160}, a 1991. godine je Brent pokazao da je N veći od 10^{300}. Uskoro bi se moglo doći do rezultata da je neparan savršen broj N veći od 10^{500}.

Gornja granica veličine neparnog savršenog broja N

Leonard E. Dickson pokazao je 1913. godine da postoji samo konačno mnogo neparnih savršenih brojeva N s k različitih prostih faktora. Pomerance je 1977. godine dao gornju ogradu na veličinu neparnog savršenog broja N s k različitih prostih faktora, to jest da je $N < (4k)^{(4k)^{2^{k^2}}}$. Zatim je David R. Heath-Brown 1994. godine pokazao da za neparan savršen broj N vrijedi $N < 4^{4^k}$. Sljedeće je Roger J. Cook 1999. godine pokazao da za neparan savršen broj N vrijedi $N < D^{4^k}$, gdje je $D = (195)^{1/7} \approx 2.124$. Konačno, 2003. godine Nielsen pokazuje da za neparan savršen broj N vrijedi $N < 2^{4^k}$.

Veliki faktori neparnog savršenog broja N

Hagis i Cohen pokazali su 1998. godine da je svaki neparan savršen broj N djeljiv s prostim brojem većim od 10^6, to jest da je najveći prost faktor nekog neparnog savršenog broja $p_k > 10^6$. Osim toga, Hagis je pokazao da je drugi najveći prost faktor nekog neparnog savršenog broja $p_{k-1} > 10^3$. Iannucci je 1999. godine pokazao da je drugi najveći prost faktor nekog neparnog savršenog broja $p_{k-1} > 10^4$, a 2000. godine je pokazao da je treći najveći prost faktor nekog neparnog savršenog broja $p_{k-2} > 10^2$. Zatim je Paul M. Jenkins 2003. godine pokazao da je najveći prost faktor nekog neparnog savršenog broja $p_k > 10^7$. Takeshi Goto i Yasuo Ohno pokazali su 2006. godine da je najveći prost faktor nekog neparnog savršenog broja $p_k > 10^8$.

Maleni faktori neparnog savršenog broja N

Otto Grün dokazao je 1952. godine da za neparan savršen broj N oblika $N = \prod_{i=1}^{k} p_i^{a_i}$, gdje prosti brojevi p_i zadovoljavaju $p_1 < p_2 < \cdots < p_k$, najmanji prost faktor zadovoljava $p_1 < \frac{2}{3}k+2$. Kishore je 1981. godine pokazao da za $i = 2, \ldots, 6$ vrijedi $p_i < 2^{2^{i-1}}(k-i+1)$.

Cohen i Sorli neznatno su 2003. godine unaprijedili Kishoreov rezultat pokazavši da za $i = 2, \ldots, 6$ vrijedi $p_i < (2^{2^{i-1}} - 1)(k - i + 1)$.

Veliki djelitelji neparnog savršenog broja N

Za neparan savršen broj $N = \prod_{i=1}^{k} p_i^{a_i}$, svaki $p_i^{a_i}$ je djelitelj od N. Joseph B. Muskat dokazao je 1965. godine da svaki neparan savršen broj N ima djelitelj $p_k^{a_k} > 10^{12}$. Tuckerman je 1973. godine dokazao da je $p_k^{a_k} > 10^{18}$ za specijalan slučaj kada 3 ili 5 dijeli N. Cohen je 1987. dokazao da svaki neparan savršen broj N ima djelitelj $p_k^{a_k} > 10^{20}$.

Svaki neparan savršen broj N **je oblika** $12m + 1$ **ili** $36m + 9$**.**

Ovaj rezultat pokazao je Jacques Touchard 1953. godine.

Lema 4.1 *Ako je* $N \equiv 5 \pmod 6$*, onda* N *nije savršen.*

Dokaz:
Pretpostavimo da je $N \equiv 5 \pmod 6$. Onda je N oblika $6k + 5 = 3(2k + 1) + 2$, pa je $N \equiv 2 \pmod 3$. Budući da su svi kvadrati kongruentni 1 modulo 3, N nije kvadrat. Nadalje, uočimo da za svaki djelitelj d od N, iz $N = d \cdot (\frac{N}{d}) \equiv 2 \equiv -1 \pmod 3$ slijedi da vrijedi ili $d \equiv -1 \pmod 3$ 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 vrijedi

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

Prema tome, $\sigma(N) \equiv 0 \pmod 3$ dok je $2N \equiv 4 \equiv 1 \pmod 3$. To nam pokazuje da broj $N = 6k + 5$ ne može biti savršen.

□

Na sličan način možemo pokazati Eulerov rezultat da je neparan savršen broj kongruentan 1 modulo 4. Pretpostavimo naprotiv da je $N \equiv 3 \pmod 4$. Onda, opet, N nije kvadrat i vrijedi

$$\sigma(N) = \sum_{d|N, d<\sqrt{N}} \left(d + \frac{N}{d} \right) \equiv 0 \pmod 4.$$

Prema tome, $\sigma(N) \equiv 0 \pmod 4$, dok $2N \equiv 6 \equiv 2 \pmod 4$.

Korolar 4.2 *Ako broj M zadovoljava kongruenciju $M \equiv 2 \pmod 3$, onda M nije savršen.*

Dokaz:
Uočimo da je u Lemi 4.1 riješen slučaj kada je M neparan. Sada želimo pokazati da tvrdnja vrijedi kada je M paran. Dakle, pretpostavimo da je broj $M \equiv 2 \pmod 3$ paran. Želimo pokazati da M ne može biti savršen. Sada pretpostavimo da je M paran savršen broj. Onda je po Euklid-Eulerovom teoremu $M = 2^{p-1}(2^p - 1)$ za neki prost broj p. Ako je $p = 2$, onda je $M = 6$ što je djeljivo sa 3. Pretpostavimo $p \geq 3$. Tada je p neparan prost broj. Prema tome,

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

Dakle, $2^p - 1 \equiv 1 \pmod 3$. Također vrijedi $2^{p-1} \equiv (-1)^{p-1} \equiv 1 \pmod 3$ budući da smo pretpostavili da je p neparan prost broj. Stoga, ako je M paran savršen broj, vrijedi ili $M \equiv 0 \pmod 3$ (što je slučaj samo kada je $p = 2$ i $M = 6$) ili $M \equiv 1 \pmod 3$ (kada je p prost broj ≥ 3). Prema tome, ako je broj $M \equiv 2 \pmod 3$ paran, ne može biti savršen. Prema Lemi 4.1 ovo vrijedi i kada je M neparan. Stoga slijedi da ako broj M zadovoljava $M \equiv 2 \pmod 3$, onda M nije savršen.

□

Teorem 4.5 (Touchard) *Svaki neparan savršen broj N je oblika $12m + 1$ ili $36m + 9$.*

Dokaz:
Neka je N neparan savršen broj, te primijenimo Lemu 4.1. Nijedan broj oblika $6k + 5$ ne može biti savršen, pa je N oblika $6k + 1$ ili $6k + 3$. Ali iz Eulerovog rezultata znamo da je N oblika $4j + 1$. Stoga vrijedi ili $N = 6k + 1$ i $N = 4j + 1$ ili $6k + 1$ i $N = 4j + 1$.

U prvom slučaju, $N = 6k + 1$ i $N = 4j + 1$. To znači da je

$$N - 1 = 6k = 4j = 12m$$

(po Kineskom teoremu o ostacima) gdje je $k = 2m$ i $j = 3m$, iz čega slijedi da je $N = 12m + 1$.

U drugom slučaju, $6k + 3$ i $N = 4j + 1$. To znači da je

$$N + 3 = 6k + 6 = 4j + 4 = 6(k + 1) = 4(j + 1) = 12p$$

(po Kineskom teoremu o ostacima) gdje je $k + 1 = 2p$ i $j + 1 = 3p$, iz čega slijedi da je $N = 12p - 3$. Stavimo li $p = m_0 + 1$, dobijemo $N = 12m_0 + 9$.

Konačno, uočimo da u drugom slučaju, ako je $N = 12m_0 + 9$ i $3 \nmid m_0$, onda vrijedi

$$\sigma(N) = \sigma(3(4m_0 + 3)) = \sigma(3)\sigma(4m_0 + 3) = 4\sigma(4m_0 + 3).$$

Sada imamo $\sigma(N) \equiv 0 \pmod 4$, dok vrijedi

$$2N = 2(12m_0 + 9) = 24m_0 + 18 = 4(6m_0 + 4) + 2 \equiv 2 \pmod 4.$$

Prema tome, N ne može biti savršen ako $3 \nmid m_0$ u drugom slučaju, pa zaključujemo da $3 \mid m_0$ u ovom slučaju, te stavimo li $m_0 = 3m$, dobijemo $N = 12m_0 + 9 = 12(3m) + 9 = 36m + 9$.

□

Tim Roberts poboljšao je prethodni rezultat 2008. godine.

Teorem 4.6 (Roberts) *Ako je N neparan savršen broj, tada vrijedi jedna od sljedećih kongruencija:*

- $N \equiv 1 \pmod{12}$.
- $N \equiv 117 \pmod{468}$.
- $N \equiv 81 \pmod{324}$.

Dokaz:
Neka je N neparan savršen broj. Uočimo da ako $3 \mid N$, onda $3^k \mid N$, gdje je k paran (Euler). Ako je $k = 0$, onda po Teoremu 4.5 vrijedi $N \equiv 1 \pmod{12}$. Također, ako je N neparan savršen broj i 3^k je faktor od N, tada je N također djeljiv sa $\sigma(3^k) = 1 + 3 + 3^2 + \cdots + 3^k$.

Ako je $k = 2$, onda opet po Teoremu 4.5 vrijedi $N \equiv 9 \pmod{36}$. Nadalje, budući da je N neparan savršen broj, znamo da $\sigma(3^2) = 1 + 3 + 3^2 = 13$ dijeli N. Prema tome, $N \equiv 0 \pmod{13}$. Sada iz Kineskog teorema o ostacima možemo zaključiti da je $N \equiv 117 \pmod{468}$.

Ako je $k > 2$, onda je N djeljiv sa $3^4 = 81$. Prema tome, opet po Teoremu 4.5, N mora zadovoljavati i $N \equiv 9 \pmod{36}$ i $N \equiv 0 \pmod{81}$. Iz Kineskog teorema o ostacima možemo zaključiti da je $N \equiv 81 \pmod{324}$. Prema tome, ako je N neparan savršen broj, vrijedi $N \equiv 1 \pmod{12}$, $N \equiv 117 \pmod{468}$ ili $N \equiv 81 \pmod{324}$.

□

Teorem 4.7 *Neparan savršen broj nije djeljiv sa* 105.

Lema 4.2 *Ako je N savršen broj s faktorizacijom oblika $N = \prod_{i=1}^{\omega(N)} p_i^{\alpha_i}$, tada vrijedi*

$$2 \geq \prod_{i=1}^{\omega(N)} \left(1 + \frac{1}{p_i} + \cdots + \frac{1}{p_i^{\beta_i}}\right),$$

gdje je $0 \leq \beta_i \leq \alpha_i \ \forall i$.

Dokaz teorema:
Pretpostavimo da je N djeljiv sa $105 = 3 \cdot 5 \cdot 7$. Faktorizacija od N je oblika

$$N = 3^{a_1} \cdot 5^{a_2} \cdot 7^{a_3} \cdot p_4^{a_4} \cdots p_k^{a_k},$$

gdje su $a_1, a_2, a_3 \geq 1$. Nadalje, $\sigma(N)$ je suma svih pozitivnih djelitelja od N, pa prema Lemi 4.2 imamo

$$\begin{aligned} \sigma(N) &= N\left(1 + \frac{1}{3} + \cdots + \frac{1}{3^{a_1}}\right)\left(1 + \frac{1}{5} + \cdots + \frac{1}{5^{a_2}}\right)\left(1 + \frac{1}{7} + \cdots + \frac{1}{7^{a_3}}\right) \cdot \\ &\quad \left(1 + \frac{1}{p_4} + \cdots + \frac{1}{p_4^{a_4}}\right) \cdots \left(1 + \frac{1}{p_k} + \cdots + \frac{1}{p_k^{a_k}}\right). \end{aligned}$$

Budući da je N neparan savršen broj, znamo da je $\sigma(N) = 2N$ i da $\sigma(N)$ nije djeljiv sa 4. Budući da su svi prosti faktori od N neparni, a_1 i a_3 su jednaki najmanje 2, inače bi vrijedilo $\left(1 + \frac{1}{3} + \cdots + \frac{1}{3^{a_1}}\right) = \frac{4}{3}$ i $\left(1 + \frac{1}{7} + \cdots + \frac{1}{7^{a_3}}\right) = \frac{8}{7}$, te bi $\sigma(N)$ bio djeljiv sa 4. Konačno,

$$2 = \frac{\sigma(N)}{N} \geq \left(1 + \frac{1}{3} + \frac{1}{3^2}\right)\left(1 + \frac{1}{5}\right)\left(1 + \frac{1}{7} + \frac{1}{7^2}\right) = \frac{13}{9} \cdot \frac{6}{5} \cdot \frac{57}{49} = \frac{4446}{2205} = 2.016326531 > 2,$$

što je kontradikcija. Dakle, neparan savršen broj N ne može biti djeljiv sa 105.

□

Literatura

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

[2] G. L. Cohen, *On the Largest Component of an Odd Perfect Number*, J. Austral. Math. Soc., 42 (1987), 280-286.

[3] G. L. Cohen, R. M. Sorli, *On the Number of Distinct Prime Factors of an Odd Perfect Number*, Journal of Discrete Algorithms, 1 (2003), 21-35.

[4] W. N. Colquitt, L. Welsh, Jr., *A New Mersenne Prime*, Math. Comp., 56 (1991), 867-870.

[5] J. H. Conway, R. K. Guy, *The Book of Numbers*, Copernicus, New York, 1996.

[6] R. Crandall, C. Pomerance, *Prime Numbers - A Computational Perspective*, Springer, New York, 2005.

[7] J. A. B. Dris, *Solving the Odd Perfect Number Problem: Some Old and New Approaches*, De La Salle University - Manila, 2008.

[8] A. Dujella, *Uvod u teoriju brojeva* (skripta), PMF Zagreb.

[9] D. B. Gillies, *Three New Mersenne Primes and a Statistical Theory*, Math. Comp., 18 (1964), 93-95.

[10] K. G. Hare, *New Techniques for Bounds on the Total Number of Prime Factors of an Odd Perfect Number*, Mathematics of Computation, 74 (2005), 1003-1008.

[11] I. Matić, *Uvod u teoriju brojeva* (skripta), Odjel za matematiku, Osijek.

[12] R. A. Mollin, *A Brief History of Factoring and Primality Testing B. C. (Before Computers)*, Mathematics Magazine, 75 (2002), 18-29.

[13] C. Noll, L. Nickel, *The 25th and 26th Mersenne Primes*, Math. Comp., 35 (1980), 1387-1390.

[14] P. P. Nielsen, *Odd Perfect Numbers Have at least Nine Distinct Prime Factors*, Math. Comp., 76 (2007), 2109-2126.

[15] P. Ribenboim, *The Little Book of Bigger Primes*, Springer, New York, 2004.

[16] R. M. Robinson, *Mersenne and Fermat Numbers*, Proc. Amer. Math. Soc., 5 (1954), 842-846.

[17] B. Tuckerman, *The 24th Mersenne Prime*, Proc. Nat. Acad. Sci. U. S. A., 68 (1971), 2319-2320.

[18] J. Voight, *On the Nonexistence of Odd Perfect Numbers*, MASS selecta, Amer. Math. Soc., (2003), 293-300.

[19] J. Voight, *Perfect Numbers: An Elementary Introduction*, University of California, Berkeley, 1998.

[20] http://primes.utm.edu/notes/proofs/

[21] http://primes.utm.edu/mersenne/

[22] http://en.wikipedia.org/wiki/Mersenne_prime

[23] http://en.wikipedia.org/wiki/Lucas-Lehmer_primality_test

[24] http://www.mersennewiki.org/index.php/Lucas-Lehmer_Test

[25] http://www-history.mcs.st-and.ac.uk/HistTopics/Perfect_numbers.html

[26] http://en.wikipedia.org/wiki/Perfect_number

Sažetak. U ovom radu proučavamo Mersenneove i savršene brojeve. Mersenneov broj je 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 Lucas-Lehmerov je test. Lucas-Lehmerov test koristi se na jakim računalima za pronalaženje velikih Mersenneovih prostih brojeva. Zaključno s 2011. godinom otkriveno je samo 47 Mersenneovih prostih brojeva.

Kažemo da je prirodan broj N savršen ako je $\sigma(N) = 2N$, gdje je $\sigma(N)$ suma pozitivnih djelitelja od 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. Većina uvjeta poboljšana je tijekom posljednjih 50 godina.

Ključne riječi: Teorija brojeva, prosti brojevi, Mersenneovi brojevi, Mersenneovi prosti brojevi, testovi prostosti, Lucas-Lehmerov test, savršeni brojevi, parni savršeni brojevi, neparni savršeni brojevi

Summary. In this paper we study Mersenne numbers and perfect numbers. 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. Modern computers with an implementation of the Lucas-Lehmer test have become a powerful tool for finding large Mersenne primes. As of the year 2011 only 47 Mersenne primes were known.

We say $N \in \mathbb{N}$ 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. Most conditions have been improved over the last 50 years.

Key words: Number theory, prime numbers, Mersenne numbers, Mersenne primes, primality tests, Lucas-Lehmer test, perfect numbers, even perfect numbers, odd perfect numbers

Životopis

Rođena sam 11. svibnja 1987. godine u Osijeku. Osnovnu školu završavam 2001. godine u Belišću, a iste godine upisujem Opću gimnaziju u Valpovu. Gimnaziju završavam 2005. godine, te upisujem Preddiplomski sveučilišni studij matematike na Odjelu za matematiku u Osijeku. Nakon završenog preddiplomskog studija, 2008. godine na Odjelu za matematiku upisujem Sveučilišni diplomski studij matematike, smjer Financijska i poslovna matematika.