Savršeni brojevi

Atlija, Josipa

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Josipa Atlija

SAVRŠENI BROJEVI

Diplomski rad

Voditelj rada:
doc. dr. sc. Marija Galić

Zagreb, rujan 2024.

Ovaj diplomski rad obranjen je dana _____ pred ispitnim povjerenstvom u sastavu:

1. _____, predsjednik
2. _____, član
3. _____, član

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Rad posvećujem svima mojima.
Posebna zahvala mentorici doc.dr.sc. Mariji Galić.

Sadržaj

Uvod

"Bilo bi teško pronaći skup cijelih brojeva s fascinantnijom povijesti i elegantnijim svojstvima okružen većim dubinama misterije – i više beskorisnima — od savršenih brojeva."
– Martin Gardner[1]

Savršeni brojevi intrigiraju brojne matematičare još od jonskog razdoblja. Prisjetimo se, savršeni broj je svaki prirodan broj koji je jednak sumi svojih pravih djelitelja. No, unatoč njihovoj sofisticiranoj definiciji i naizgled jednostavnim svojstvima, brojna su pitanja vezana uz savršene brojeve na koja još uvijek nemamo odgovore. Još oko 300.-te godine prije Krista, Euklid je pokazao da ako je $2^p - 1$ prost broj, da je tada $2^{p-1}(2^p - 1)$ savršen. Oko dvije tisuće godine kasnije, Euler je dokazao da su svi savršeni parni brojevi nužno ovoga oblika. Unatoč Eulerovoj karakterizaciji parnih savršenih brojeva, i dalje ne znamo koliko ih ima, kao niti postoje li uopće neparni savršeni brojevi.

Ovim diplomskim radom skrećemo pozornost na sve ono što o savršenim brojevima znamo te na sve ono što bismo još htjeli saznati. Rad je organiziran na sljedeći način. U prvom poglavlju dajemo pregled osnovnih definicija i teorema iz teorije brojeva koji će biti potrebni za razumijevanje rada.

Drugo poglavlje posvećeno je Mersenneovim brojevima s posebnim naglaskom na Mersenneove proste brojeve, čiji je pronalazak usko vezan uz pronalazak parnih savršenih brojeva. Nadalje, opisat ćemo i Lucas – Lehmerov test provjere prostosti Mersenneovih brojeva. Upravo se taj test koristi i u suvremenim matematičkim istraživanjima kao što je *Great Internet Mersenne Prime Search (GIMPS)*, pomoću kojega je 2018. godine otkriven i posljednji nama znan Mersenneov prost broj (ujedno i najveći nama znan prost broj) $2^{82589933} - 1$ koji u bazi 10 ima 24862048 znamenki.

U trećem poglavlju definiramo savršene brojeve. S obzirom da su svi dosad otkriveni savršeni brojevi parni, navodimo njihove oblike te poznate karakteristike. Definirat ćemo višestruko savršene brojeve i pokazati metodu za pronalazak istih. Također, diskutiramo postojanje neparnih savršenih brojeva, uvjete koje oni moraju zadovoljavati i pronađenu donju granicu veličine takvih brojeva ukoliko postoje.

[1] američki matematičar i pisac, 1914.–2010.

Poglavlje 1

Kratki uvod u teoriju brojeva

1.1 Pregled osnovnih pojmova

Ovo poglavlje služi za ponavljanje definicija, tvrdnji, teorema i propozicija koji su potrebni za razumijevanje daljnjeg teksta.

Jedan od najvažnijih pojmova teorije brojeva je i djeljivost, koju definiramo na sljedeći način.

Definicija 1.1.1. *Neka su $a \neq 0$ i b cijeli brojevi. Kažemo da je b **djeljiv** s a (ili da a **dijeli** b) ako postoji cijeli broj x takav da vrijedi $b = ax$. Tada je a **djelitelj** od b, a b je **višekratnik** od a i pišemo $a \mid b$. Ako b nije djeljiv s a, onda pišemo $b \nmid a$.*

U sljedećem teoremu navodimo neka od svojstava djeljivosti.

Teorem 1.1.2. *Za cijele brojeve a, b, c vrijedi:*

1. *Ako $a \mid b$ i $b \neq 0$, tada $|a| \leq |b|$.*
2. *Ako $a \mid b$ i $a \mid c$, tada $a \mid (bx + cy)$ za proizvoljne cijele brojeve x i y.*

Dokaz. 1. Neka $a \mid b$, tada postoji cijeli broj c takav da je $b = ac$. Također, iz $b \neq 0$ slijedi $c \neq 0$. Sada,

$$|b| = |ac| = |a||c|.$$

Iz $c > 0$ slijedi $|c| \geq 1$, pa

$$|b| = |ac| \geq |a|.$$

2. Iz $a \mid b$ i $a \mid c$ slijedi $b = ar$ i $c = as$ za neke cijele brojeve r i s. Tada za bilo koje x i y vrijedi

$$bx + cy = arx + asy = a(rx + sy).$$

Suma $rx + sy$ je cijeli broj, pa vrijedi $a \mid (bx + cy)$. □

Teorem 1.1.3. *Neka je p prost i $p \mid ab$, tada $p \mid a$ ili $p \mid b$.*

Dokaz. Za $p \mid a$ tvrdnja je dokazana. Pretpostavimo suprotno, $p \nmid a$. Pozitivni djelitelji od p su samo 1 i p. Dakle, $M(p,a) = 1$ (općenito, $M(p,a) = p$ ili $M(p,a) = 1$). Dakle, koristeći Euklidovu lemu mora vrijediti $p \mid b$. □

Pri dijeljenju dvaju brojeva iz skupa cijelih brojeva kvocijent neće nužno biti iz tog skupa, odnosno cijeli broj. Tu činjenicu precizno iskazujemo i dokazujemo u sljedećem teoremu.

Teorem 1.1.4 (Teorem o dijeljenju s ostatkom)**.** *Za proizvoljan prirodan broj a i cijeli broj b postoje jedinstveni cijeli brojevi q i r takvi da je $b = qa + r,\ 0 \leq r < a$.*

Dokaz. Neka je $S = \{b - am :\ m \in \mathbb{Z}\}$. Neka postoji najmanji nenegativan element $r \in S$. Uvjet $0 \leq r < a$ osigurava postojanje cijelog broja q takvog da je $b - qa = r$, to jest $b = qa + r$.

Pretpostavimo da postoji još jedan par cijelih brojeva $r',\ q'$ koji zadovoljava iste uvjete. Pokažimo da vrijedi $r' = r$. Bez smanjenja općenitosti neka je $r < r'$. Onda $0 < r' - r < a$ i $r' - r = a(q - q') \geq a$. Dakle, $r' = r$ i $q' = q$. Ovime smo pokazali jedinstvenost q i r. □

Definicija 1.1.5. ***Zajednički djelitelj*** *dvaju cijelih brojeva a i b je cijeli broj c takav da $c \mid a$ i $c \mid b$. Uz uvjet da je barem jedan od brojeva a i b različit od nule postoji konačno mnogo njihovih djelitelja.* ***Najveći zajednički djelitelj****, u oznaci $M(a,b)$, je najveći među njima koji dijeli oba broja.*

Navedimo sada Euklidov algoritam i Euklidovu lemu te njihove dokaze.

Teorem 1.1.6 (Euklidov algoritam)**.** *Neka su a i $b > 0$ cijeli brojevi. Pretpostavimo da je uzastopnom primjenom Teorema 1.1.4 dobiven niz jednakosti*

$$a = bq_1 + r_1,\ 0 < r_1 < b,$$

$$b = r_1q_2 + r_2,\ 0 < r_2 < r_1,$$

$$r_1 = r_2q_3 + r_3,\ 0 < r_3 < r_2,$$

$$\dots$$

$$r_{j-2} = r_{j-1}q_j + r_j,\ 0 < r_j < r_{j-1},$$

$$r_{j-1} = r_jq_{j+1}.$$

Tada je $M(a,b) = r_j$, gdje je r_j posljednji ostatak različit od nule. Vrijednosti od x_0 i y_0 u izrazu $M(a,b) = ax_0 + by_0$ mogu se dobiti izražavanjem svakog ostatka r_i, $i = 1, 2, \dots, j$, kao linearne kombinacije od a i b.

Dokaz. Koristeći svojstvo $M(a,b) = M(a,b+ax)$, $M(a,b)$ možemo raspisati kao

$$\begin{aligned} M(a,b) &= M(a-bq_1,b) = M(r_1,b) = M(r_1,b-r_1q_2) \\ &= M(r_1,r_2) = M(r_1-r_2q_3,r_2) = M(r_3,r_2). \end{aligned}$$

Nastavljajući ovaj proces, dobivamo

$$M(q,b) = (r_{j-1},r_j) = M(r_j,0) = r_j. \tag{1.1}$$

Matematičkom indukcijom pokazat ćemo da je svaki r_i linearna kombinacija od a i b. Baza matematičke indukcije je osigurana za r_1 i r_2. Kako je r_i linearna kombinacija od r_{i-1} i r_{i-2}, po pretpostavci (1.1) dobivamo da je i linearna kombinacija od a i b. □

Primjenu Euklidovog algoritma prikažimo na kratkom primjeru.

Primjer 1.1.7. *Primjenom Euklidovog algoritma odredimo najveći zajednički djelitelj brojeva* 928 *i* 512*, te ga prikažimo kao linearnu kombinaciju tih brojeva. Prvo pronađimo najveći zajednički djelitelj zadanih brojeva:*

$$\begin{aligned} 928 &= 512\cdot 1 + 416 \\ 512 &= 416\cdot 1 + 96 \\ 416 &= 96\cdot 4 + 32 \\ 96 &= 32\cdot 3. \end{aligned}$$

Stoga vrijedi $M(928,512) = 32$*. Sada ćemo* 18 *prikazati kao linearnu kombinaciju brojeva* 928 *i* 512*.*

$$\begin{aligned} 32 &= 416 - 96\cdot 4 \\ &= 416 - (512 - 416\cdot 1)\cdot 4 \\ &= 5\cdot 416 - 4\cdot 512 \\ &= 5\cdot(928 - 512\cdot 1) - 4\cdot 512 \\ &= 5\cdot 928 - 9\cdot 512. \end{aligned}$$

Rješenja jednadžbe

$$ax + by = M(a,b)$$

možemo izračunati i na drugačiji način. Neka je

$$r_{-1} = a, r_0 = b;\ r_i = r_{i-2} - q_i r_{i-1};$$

$$x_{-1} = 1, x_0 = 0 \; x_i = x_{i-2} - q_i x_{i-1};$$
$$y_{-1} = 0, y_0 = 1; \; y_i = y_{i-2} - q_i y_{i-1}.$$

Tada vrijedi

$$ax_i + cy_i = r_i, \text{ za } i = -1, 0, 1, \ldots, j+1.$$

Ova formula vrijedi za $i = -1$ i $i = 0$, pa stoga indukcijom slijedi da vrijedi i trivijalno. Posebno, vrijedi

$$ax_j + by_j = M(a, b).$$

Primjer 1.1.8. *Odredimo najveći zajednički djelitelj brojeva* 319 *i* 187 *te izračunajmo rješenja jednadžbe* $319x + 187y = M(319, 187)$.

Pronađimo najprije najveći zajednički djelitelj primjenom Euklidovog algoritma.

$$\begin{aligned} 319 &= 187 \cdot 1 + 132 \\ 187 &= 132 \cdot 1 + 55 \\ 132 &= 55 \cdot 2 + 22 \\ 55 &= 22 \cdot 2 + 11 \\ 22 &= 11 \cdot 2. \end{aligned}$$

Sada izračunajmo rješenja jednadžbe $319x + 187y = 11$. *Radi preglednosti formirat ćemo tablicu.*

i	q_i	x_i	y_i
-1		1	0
0		0	1
1	1	1	-1
2	1	-1	2
3	2	3	-5
4	2	-7	12

Tablica 1.1: Računanje najvećeg zajedničkog djelitelja

Dakle, rješenja su $x = -7$, $y = 12$, *odnosno,*

$$11 = 319 \cdot (-7) + 187 \cdot 12.$$

Najveći zajednički djelitelj cijelih brojeva a i b možemo zapisati i kao njihovu linearnu kombinaciju o čemu nam govori sljedeći teorem.

Teorem 1.1.9. *Neka su a i b cijeli brojevi takvi da barem jedan nije jednak nuli. Tada postoje cijeli brojevi x i y takvi da*

$$M(a,b) = ax + by.$$

Dokaz. Neka je S skup svih pozitivnih linearnih kombinacija a i b:

$$S = \{au + bv \mid au + bv > 0; u, v \text{ cijeli brojevi}\}.$$

Vidimo da je S neprazan skup. Na primjer, za $a \neq 0$ vrijedi $|a| = au + b \cdot 0 \in S$, gdje je $u = 1$ ili $u = -1$. Dakle, S mora sadržavati neki najmanji element d (prema Aksiomu potpunosti). Iz definicije skupa S sada slijedi postojanje cijelih brojeva x i y takvih da je $d = ax + by$.

Tvrdimo da je $d = M(a,b)$. Koristeći Euklidov algoritam, znamo da postoje cijeli brojevi q i r takvi da je $a = qd + r$, gdje je $0 \leq r \leq d$. Tada r možemo zapisati kao

$$\begin{aligned} r = a - qd &= a - q(ax + by) \\ &= a(1 - qx) + b(-qy). \end{aligned}$$

Ako je r pozitivan, tada je $r \in S$, što je kontradikcija (d je najmanji element iz S). Dakle, $r = 0$ i $a = qd$, odnosno $d \mid a$. Slično dokazujemo da $d \mid b$ iz čega slijedi da je d zajednički djelitelj od a i b.

Neka je c proizvoljan pozitivan zajednički djelitelj od a i b. Koristeći Teorem 1.1.2, tada $c \mid (ax + by)$, odnosno $c \mid d$. Sada

$$c = |c| \leq |d| = d,$$

pa je d veći od svakog zajedničkog djelitelja brojeva a i b. Zaključujemo da je d najveći zajednički djelitelj od a i b. □

Lema 1.1.10 (Euklidova lema)**.** *Neka $a \mid bc$ i $M(a,b) = 1$, tada $a \mid c$.*

Dokaz. Koristeći Teorem 1.1.9 zapišimo 1 u obliku $1 = ax + by$, gdje su x i y cijeli brojevi. Množenjem tog izraza s c dobivamo

$$c = c \cdot 1 = (ax + by)c = acx + bcy.$$

Kako $a \mid ac$ i $a \mid bc$, slijedi $a \mid (acx + bcy)$ što je ekvivalentno s $a \mid c$. □

Svaki prirodan broj možemo na jedinstven način prikazati kao produkt prostih brojeva. O tome nam govori sljedeći vrlo bitan teorem.

Teorem 1.1.11 (Osnovni teorem aritmetike)**.** *Faktorizacija svakog prirodnog broja $n > 1$ na proste faktore je jedinstvena do na poredak prostih faktora.*

Dokaz. Pretpostavimo suprotno, neka n ima dvije različite faktorizacije. Dijeleći s prostim brojevima koji se pojavljuju u obje reprezentacije dobivamo jednakost oblika

$$p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s,$$

gdje su p_i, q_j, ne nužno različiti, prosti brojevi takvi da se niti jedan prost broj s lijeve strane ne pojavljuje na desnoj strani, to jest da vrijedi $p_i \neq q_j$, za svaki i i j. No, to je nemoguće. Ako je p prost broj i $p \mid ab$, onda $p \mid a$ ili $p \mid b$ (po Teoremu 1.1.3). Generaliziramo li tu tvrdnju, ako $p \mid a_1 a_2 \cdots a_n$, onda p dijeli barem jedan faktor a_i, $i = 1, 2, \ldots, n$. Dakle, iz $p_1 \mid q_1 q_2 \cdots q_s$ slijedi da p_1 dijeli barem jedan od $q_1, q_2, \ldots, q_s$. To bi značilo da je $p_1 = q_j$ što je kontradikcija. □

Definicija 1.1.12. ***Zbroj djelitelja*** *prirodnog broja n definiramo kao funkciju*

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

gdje je d pozitivan djelitelj broja n uključujući 1 *i n.*

Primjer 1.1.13. *Izračunajmo zbroj djelitelja brojeva $n = 6, 7, 28$.*

$$\begin{aligned} \sigma(6) &= 1 + 2 + 3 + 6 = 12, \\ \sigma(7) &= 1 + 7 = 8, \\ \sigma(28) &= 1 + 2 + 4 + 7 + 14 + 28 = 46. \end{aligned}$$

Multiplikativnost artimetičke funkcije f različite od nul funkcije za relativno proste argumente m i n je svojstvo $f(mn) = f(m)f(n)$.

Teorem 1.1.14. *Neka je $M(m, n) = 1$, tada vrijedi $\sigma(mn) = \sigma(m)\sigma(n)$.*

Dokaz. Prikažemo li m i n kao produkte njihovih djelitelja, gdje su djelitelji prosti brojevi, tada je djelitelj od mn moguće na jedinstveni način prikazati kao produkt djelitelja od m i od n. Slijedi da se svaki član sume $\sigma(mn)$ pojavljuje točno jednom u sumi $\sigma(m)\sigma(n)$. Svaki takav produkt je djelitelj od mn pa sume moraju biti jednake. □

Sada ćemo definirati pojam kongruentnosti koji će biti od iznimne važnosti u ostatku rada.

Definicija 1.1.15. *Ako cijeli broj $m \neq 0$ dijeli razliku $a - b$, onda kažemo da je a **kongruentan** b **modulo** m i pišemo $a \equiv b \bmod m$. U protivnom, kažemo da a nije kongruentan b modulo m i pišemo $a \not\equiv b \bmod m$.*

Moduli mogu biti i pozitivni i negativni, no konvencionalno je za module koristiti pozitivne brojeve.

Navedimo u obliku teorema nekoliko svojstava kongruencije.

Teorem 1.1.16. *Neka su a, b, c i d cijeli brojevi.*

1. *Ako je $a \equiv b \bmod m$ i $c \equiv d \bmod m$, onda je*

$$\begin{aligned} a + c &\equiv b + d \bmod m, \\ a - c &\equiv b - d \bmod m, \\ ac &\equiv bd \bmod m. \end{aligned}$$

2. *Ako je $a \equiv b \bmod m$ i $d \mid m$, onda je $a \equiv b \bmod d$.*

3. *Ako je $a \equiv b \bmod m$, onda je $ac \equiv bc \bmod mc$ za svaki $c \neq 0$.*

Dokaz. 1. Neka je $a - b = mk$ i $c - d = ml$.
Tada je

$$(a + c) - (b + d) = m(k + l)$$

i

$$(a - c) - (b - d) = m(k - l),$$

pa je $a + c \equiv b + d \bmod m$ i $a - c \equiv b - d \bmod m$. Zbog

$$ac - bd = a(c - d) + d(a - b) = m(al + dk)$$

slijedi da je $ac \equiv bd \bmod m$.

2. Neka je $m = de$. Tada iz $a - b = mk$ slijedi $a - b = d \cdot (ck)$, pa je $a \equiv b \bmod d$.

3. Iz $a - b = mk$ slijedi $ac - bc = (mc) \cdot k$, pa je $ac \equiv bc \bmod mc$. □

Ostatak pri dijeljenju a^p s p, gdje je p prost broj, jednak je ostatku pri dijeljenju a s p. O tome nam govori sljedeći teorem.

Teorem 1.1.17 (Mali Fermatov teorem)**.** *Neka je p prost broj. Pretpostavimo da $p \nmid a$. Tada vrijedi $a^{p-1} \equiv 1 \bmod p$.*

Dokaz. Promotrimo prvih $p-1$ pozitivnih višekratnika od a:

$$a, 2a, 3a, \ldots, (p-1)a.$$

Niti jedan od tih brojeva nije kongruentan modulo p s ostalima, niti je kongruentan s 0 modulo p. Kada bi vrijedilo

$$ra \equiv sa \bmod p, \quad 1 \leq r < s \leq p-1,$$

slijedilo bi $r \equiv s \bmod p$, što nije moguće. Dakle, navedeni cijeli brojevi moraju biti kongruentni modulo p s $1, 2, 3, \ldots, p-1$ nekim redom. Produkt tih kongruencija

$$a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \bmod p$$

povlači

$$a^{p-1}(p-1)! \equiv (p-1)! \bmod p.$$

Jer je $p \nmid (p-1)!$ prethodna kongruencija je ekvivalentna $a^{p-1} \equiv \bmod p$. □

Teorem 1.1.18. *Vrijedi sljedeće:*

$$ax \equiv ay \bmod m \text{ ako i samo ako } x \equiv y \bmod \frac{m}{M(a,m)},$$

gdje je $M(a,m)$ najveći zajednički djelitelj brojeva a i m.

Dokaz. Ako je $ax \equiv ay \bmod m$, onda postoji cijeli broj z takav da je $ay - ax = mz$.
Sada vrijedi:

$$\frac{a}{M(a,m)}(y-x) = \frac{m}{M(a,m)}z,$$

to jest

$$\frac{m}{M(a,m)} \text{ dijeli } \frac{a}{M(a,m)}(y-x).$$

Brojevi $\frac{a}{M(a,m)}$ i $\frac{m}{M(a,m)}$ su relativno prosti, pa možemo zaključiti da $\frac{m}{M(a,m)}$ dijeli $y-x$, odnosno da vrijedi

$$x \equiv y \bmod \left(\frac{m}{(a,m)}\right).$$

Obratno, ako je $x \equiv y \bmod (\frac{m}{M(a,m)})$, onda po Teoremu 1.1.16.3 dobivamo

$$ax \equiv ay \bmod (\frac{am}{M(a,m)}).$$

$M(a,b)$ dijeli a, pa po Teoremu 1.1.16.2 dobivamo $ax \equiv ay \bmod m$. □

Definicija 1.1.19. ***Potpunim sustavom ostataka modulo*** *m zovemo skup $\{x_1, \ldots, x_m\}$ ako za svaki $y \in \mathbb{Z}$ postoji jedinstveni x_j takav da je $y \equiv x_j \bmod m$.*

Postoji ih beskonačno mnogo, a jedan od njih je takozvani sustav najmanjih nenegativnih ostataka $\{0, 1, \ldots, m-1\}$.

Teorem 1.1.20. *Ako je $\{x_1, \ldots, x_n\}$ potpuni sustav ostataka modulo m i a i m su relativno prosti, onda je i $\{ax_1, \ldots, ax_m\}$ potpuni sustav ostataka modulo m.*

Dokaz. Dovoljno je dokazati da je $ax_i \not\equiv ax_j \bmod m$ za $i \neq j$. Pretpostavimo da vrijedi $ax_i \equiv ax_j \bmod m$. Iz Teorema 1.1.18 slijedi da je $x_i \equiv x_j \bmod m$, odnosno $i = j$. □

Eulerova funkcija $\varphi(n)$ je broj prirodnih brojeva manjih ili jednakih n koji su s n relativno prosti.

Uvedimo sada definicije reda od a modulo m i primitivnog korijena.

Definicija 1.1.21. ***Red od*** *a* ***modulo*** *m je najmanji prirodni broj d za koji vrijedi $a^d \equiv 1 \bmod n$ uz uvjet da su a i n relativno prosti prirodni brojevi.*

Definicija 1.1.22. *Ako je red od a modulo n jednak $\varphi(n)$, tada je a* ***primitivni korijen modulo*** *n.*

U ovome trenu navedimo teorem koji ćemo koristiti pri dokazivanju Eulerovog kriterija navedenog nešto kasnije.

Teorem 1.1.23 (Wilsonov teorem)**.** *Ako je p prost broj, onda je $(p-1)! \equiv -1 \bmod p$.*

Dokaz. Za $p = 2$ i $p = 3$ kongruencija je zadovoljena. Stoga smijemo pretpostaviti da je $p \geq 5$. Grupirajmo članove skupa $2, 3, \ldots p-2$ u parove (i, j) sa svojstvom $i \cdot j \equiv 1 \bmod p$. Vidimo da je $i \neq j$ jer bi inače broj $(i-1)(i+1)$ bio djeljiv s p, a to je nemoguće zbog $0 \leq i - 1 \leq i \leq p$. Tako dobivamo $\frac{p-3}{2}$ parova i ako pomnožimo odgovarajućih $\frac{p-3}{2}$ parova i ako pomnožimo odgovarajućih $\frac{p-3}{2}$ kongruencija, dobit ćemo

$$2 \cdot 3 \cdots (p-2) \equiv 1 \bmod p,$$

pa je

$$(p-1)! \equiv 1 \cdot 1 \cdot 1 \cdot (p-1) \equiv -1 \bmod p.$$

Vrijedi i obrat Wilsonovog teorema. Zaista, neka vrijedi

$$(p-1)! \equiv -1 \bmod p$$

i pretpostavimo da p nije prost. Tada p ima djelitelj d takav da vrijedi $1 \leq d \leq p$ i d dijeli $(p-1)!$. No, tada d mora dijeliti i -1, što je kontradikcija. □

Za kraj ovog uvodnog poglavlja definirat ćemo što su to kvadratni ostatci te iskazati Eulerov kriterij.

Definicija 1.1.24. *Neka je p prost broj i $M(a, p) = 1$. Ako za $x^2 \equiv a \bmod p$ postoji rješenje, tada je a **kvadratni ostatak pri dijeljenju s** p. Inače je a kvadratni neostatak pri dijeljenju s p.*

Definicija 1.1.25. *Neka je p neparan prost broj. **Legendreov**[1] **simbol** je notacija $\frac{a}{p}$ koju definiramo na sljedeći način:*

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{ako je } a \text{ kvadratni ostatak modulo } p, \\ -1, & \text{ako je } a \text{ kvadratni neostatak modulo } p, \\ 0, & \text{ako } p \mid a. \end{cases}$$

Sljedeći teoremi, od kojih jedan koristi red od a modulo m, a drugi Legendreov simbol, koristit će nam u dokazu teorema vezanih uz Mersenneove brojeve.

Teorem 1.1.26. *Neka je d red od a modulo n. Tada za prirodan broj k vrijedi $a^k \equiv 1 \bmod n$ ako i samo ako $d \mid k$. Posebno, $d \mid \varphi(n)$.*

Dokaz. Ako $d \mid k$, postoji l takav da vrijedi $k = dl$. Tada je $a^k \equiv (a^d)^l \equiv 1 \bmod n$.
S druge strane, neka je $a^k \equiv 1 \bmod n$. Podijelimo li k s d, dobivamo $k = qd + r$, gdje je $0 \leq r < d$. Sada

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

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

Teorem 1.1.27. *Neka je p neparan prost broj. Tada vrijedi:*

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

Dokaz ovog teorema može se pronaći u knjizi [3].
Napokon, iskažimo i dokažimo Eulerov kriterij.

Teorem 1.1.28 (Eulerov kriterij)**.**

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

[1] Adrien-Marie Legendre, francuski matematičar i astronom, 1752.–1833.

Dokaz. Ako je $\left(\frac{a}{p}\right) = 0$, onda $p \mid a$, pa je tvrdnja zadovoljena.

Ako je $\left(\frac{a}{p}\right) = 1$, onda postoji cijeli broj x_0 takav da je $x_0^2 \equiv a \bmod p$. Sada iz Teorema 1.1.17 slijedi $a^{\frac{p-1}{2}} \equiv x_0^{p-1} \equiv 1 \equiv \left(\frac{a}{p}\right)$. Neka je $\left(\frac{a}{p}\right) = -1$. Za svaki $i = 1, \ldots, p-1$ odaberimo $j = 1, \ldots, p-1$ tako da vrijedi $i \cdot j \equiv a \bmod p$. Uočimo da je $i \neq j$, budući da kongruencija $x^2 \equiv a \bmod p$ nema rješenja. Dakle, skup $\{1, \ldots, p-1\}$ se raspada na $\frac{p-1}{2}$ parova (i, j) za koje vrijedi $i \cdot j \equiv a \bmod p$. Množenjem ovih $\frac{p-1}{2}$ kongruencija, to koristeći Teorem 1.1.23 dobivamo

$$a^{\frac{p-1}{2}} \equiv (p-1)! \equiv -1 \bmod p.$$

□

Poglavlje 2

Mersenneovi brojevi

2.1 Mersenneovi brojevi

Mersenneovi brojevi su brojevi oblika

$$M_p = 2^p - 1,$$

pri čemu je p prost broj. Naziv su dobili po francuskom svećeniku Marinu Mersenneu[1] koji je veliki dio života bio okružen vrhunskim matematičarima. Nekad se u literaturi Mersenneovim brojevima zovu i brojevi oblika $M_n = 2^n - 1,\ n \geq 1$, gdje je n prirodan broj (koji ne mora biti prost).

Od posebnog su interesa *Mersenneovi prosti brojevi*, odnosno Mersenneovi brojevi koji su ujedno i prosti. Sredinom 17. stoljeća, Mersenne je iznio (netočnu) tvrdnju da je M_p prost broj ukoliko je $p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$, a da je složen za sve ostale proste brojeve $p < 257$i. U to vrijeme, ta tvrdnja je pobudila veliko zanimanje jer se radilo o velikim brojevima i nitko je nije mogao provjeriti pa tako niti Mersenne.

Da je M_{31} prost, dokazao je Euler direktnom provjerom svih prostih brojeva do 46339 kao potencijalnih djelitelja, no to tehniku nije uspio primijeniti na M_{67}, M_{127}, M_{257}. Nije poznato zašto je Mersenne u svoj popis uključio M_{67}, a isključio brojeve poput M_{61}, M_{89} i M_{107}. Édouard Lucas[2] je 1876. godine pokazao da je M_{127} prost broj.

Lucas je osmislio test kojime je pokazao da M_{67} zapravo nije prost. Iako nije pronašao faktore koji čine M_{67} njegov test prostosti bio je pouzdan. Test je poboljšao Derrick H. Lehmer[3] te danas nosi ime po obojici.

[1] francuski matematičar, fizičar, filozof i glazbeni teotičar, 1588.–1648.

[2] francuski matematičar, 1842.–1891.

[3] američki matematičar, 1905.–1991.

Teorem 2.1.1 (Lucas–Lehmerov test)**.** *Neka je p prost broj. Induktivno definiramo niz relacijama*

$$s_0 = 4,$$
$$s_{i+1} = s_i^2 - 2,$$

pri čemu je $i = 0, 1, 2, 3, \ldots$. Tada je broj M_p prost ako i samo ako je

$$s_{p-2} \equiv 0 \bmod M_p.$$

Primjer 2.1.2. *Koristeći Lucas–Lehmerov test provjerimo je li M_7 prost broj. Najprije definirajmo niz s indeksom zadnjeg člana $i - 2 = 7 - 2 = 5$:*

$$s_0 = 4,$$
$$s_1 = 4^2 - 2 = 14,$$
$$s_2 = 14^2 - 2 = 194,$$
$$s_3 = 194^2 - 2 = 37634,$$
$$s_4 = 37634^2 - 2 = 1416317954,$$
$$s_5 = 1416317954^2 - 2 = 2005956546822746114.$$

Sada, za $p = 7$ i $M_7 = 2^7 - 1 = 127$ treba vrijediti

$$s_5 \equiv 0 \bmod M_7.$$

Direktnim dijeljenjem vidi se da je 127 *djelitelj od s_5 te je prema Teoremu 2.1.1 M_7 Mersenneov prosti broj.*

Faktori za M_{67} pronađeni su od strane matematičara Franka Nelsona Colea[4]. Teatralno ih je bez riječi predstavio tako što je na matematičkom skupu s jedne strane izračunao $2^{67} - 1$ te s druge strane pomnožio 193707721 i 761838257287. Iako zvuči jednostavno, priznao je da je na tome radio svake nedjelje dvadeset godina što nam ukazuje na to koliko je zaista značajan Lucas–Lehmerov test pri istraživanju ovih brojeva.

Sam Lehmer je otkrio da je M_{257} s "originalne" Mersenneove liste složen broj uloživši 700 sati u račun kako bi pokazao da $S_{256} \not\equiv 0 \bmod M_{257}$. Njegovo otkriće potvrđeno je 20 godina kasnije od strane *National Bureau of Standards Western Automatic Computer* kada je računalo za 68 sekundi pronašlo najmanji faktor broja M_{257}, broj 535006138814359.

Postoji još načina za ispitati je li Mersenneov broj prost ili složen. Za razumijevanje idućeg testa kojeg ćemo navesti prvo je potrebno poznavanje sljedećih teorema čije ćemo rezultate prikazati na primjerima.

[4]američki matematičar, 1861. – 1926.

Teorem 2.1.3. *Neka su p i $q = 2p + 1$ prosti brojevi. Tada vrijedi $q \mid M_p$ ili $q \mid M_p + 2$, ali ne oboje.*

Dokaz. Koristeći Mali Fermatov teorem znamo da vrijedi

$$2^{q-1} - 1 \equiv 0 \bmod q,$$

dok faktorizacijom lijeve strane dobivamo

$$(2^{\frac{q-1}{2}} - 1)(2^{\frac{q-1}{2}} + 1) = (2^p - 1)(2^p + 1) \equiv 0 \bmod q.$$

Ekvivalentan je zapis

$$M_p(M_p + 2) \equiv 0 \bmod q.$$

Tvrdnja sada slijedi direktno iz Teorema 1.1.3. Naime, kada bi u isto vrijeme vrijedilo da $q \mid M_p$ i $q \mid M_p + 2$ moralo bi vrijediti da $q \mid 2$, što je nemoguće. □

Primijenimo prethodni teorem na sljedećem primjeru.

Primjer 2.1.4. *Koristeći tvrdnju Teorema 2.1.3 dokažimo da za proste brojeve $p = 5$ i $q = 2p + 1 = 11$ vrijedi da $11 \mid M_5$ ili $11 \mid M_5 + 2$. Drugim riječima, trebamo provjeriti vrijedi li $2^5 \equiv 1 \bmod 11$ ili $2^5 + 2 \equiv 1 \bmod 11$. Računamo:*

$$2^5 = 32 \equiv 10 \bmod 11,$$
$$2^5 + 2 = 34 \equiv 1 \bmod 11.$$

Dakle, $11 \mid M_5 + 2$.

Prirodno je pitati se postoji li način da unaprijed znamo hoće li vrijediti $q \mid M_p$ ili $q \mid M_p + 2$. Odgovor nam daje idući teorem.

Teorem 2.1.5. *Neka je $q = 2n + 1$ prost, tada:*

1. *$q \mid M_n$, ako $q \equiv 1 \bmod 8$ ili $q \equiv 7 \bmod 8$,*
2. *$q \mid M_n + 2$, ako $q \equiv 3 \bmod 8$ ili $q \equiv 5 \bmod 8$.*

Dokaz. Tvrdnja $q \mid M_n$ ekvivalentna je s

$$2^{\frac{q-1}{2}} = 2^n \equiv 1 \bmod q.$$

Promatramo li Legendreov simbol, uvjet je ekvivalentan tome da $\left(\frac{2}{q}\right) = 1$. Ali, primjenom Teorema 1.1.27 znamo da $\left(\frac{2}{q}\right) = 1$ vrijedi kada je $q \equiv 1 \bmod 8$ ili $q \equiv 7 \bmod 8$.

Dokaz druge tvrdnje provodi se na sličan način. □

Navedimo sada neposrednu posljedicu prethodnog teorema.

Korolar 2.1.6. *Neka su p i $q = 2p + 1$ neparni prosti brojevi za koje vrijedi $p \equiv 3 \bmod 4$. Tada vrijedi $q \mid M_p$.*

Dokaz. Neparni prosti broj p je oblika $4k + 1$ ili $4k + 3$, gdje je $k \in \mathbb{Z}$. Ako je $p = 4k + 3$, tada je $q = 8k + 7$ i po Teoremu 2.1.5 vrijedi $q \mid M_p$. Ako je $p = 4k + 1$, tada je $q = 8k + 3$ te $q \nmid M_p$. □

Precizniju karakterizaciju djelitelja od M_p opisuju sljedeća dva teorema.

Teorem 2.1.7. *Neka je p neparan prost broj. Tada je svaki prost djelitelj od M_p oblika $2kp + 1$.*

Dokaz. Neka je q djelitelj od M_p takav da vrijedi $2^p \equiv 1 \bmod q$. Ako je k najmanji pozitivan cijeli broj takav da vrijedi $2^k \equiv 1 \bmod q$, tada po Teoremu 1.1.26 slijedi da $k \mid q - 1$. Znajući da je $k = p$, slijedi $p \mid q-1$. Da bismo osigurali istinitost tvrdnje, neka je $q-1 = pt$, tada $q = pt + 1$. Dokaz je dovršen ako je t neparan cijeli broj. To bi značilo da je q paran što upućuje na kontradikciju. Dakle, mora vrijediti $q = 2kp + 1$ za neki k što nam daje traženi oblik od q. □

Teorem 2.1.8. *Neka je p neparan prost broj. Tada je prost djelitelj q od M_p oblika $q \equiv \pm 1 \bmod 8$.*

Dokaz. Pretpostavimo da je q prost djelitelj od M_p takav da vrijedi $2^p \equiv 1 \bmod q$. Iz Teorema 2.1.7 slijedi da je q oblika $q = 2kp + 1$ za neki cijeli broj k. Nadalje, koristeći Teorem 1.1.28, vrijedi $\left(\frac{2}{q}\right) \equiv 2^{(q-1)/2} \equiv 1 \bmod q$, odnosno $\left(\frac{2}{q}\right) = 1$. Naposlijetku, koristeći Teorem 1.1.27 pokaže se da vrijedi $q \equiv \pm 1 \bmod 8$. □

Prikažimo sada primjenu prethodna dva teorema na konkretnom primjeru.

Primjer 2.1.9. *Pokažimo da je M_{17} neparan prost broj. Prosti brojevi oblika $34k + 1$ koji su manji od $362 < \sqrt{M_{17}}$ su redom:*

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

Budući da je najmanji netrivijalni djelitelj od M_{17} prost, u obzir uzimamo samo proste brojeve od prethodno navedenih, to jest

$$103, 137, 239, 307.$$

Lako je uvjeriti se da vrijedi $308 \not\equiv 0 \bmod 8$, odnosno $307 \not\equiv 1 \bmod 8$. Ostala tri broja isključimo direktnim dijeljenjem pa M_{17} mora biti prost.

Pri istraživanju Mersenneovih brojeva primijetilo se da u slučaju prva četiri Mersenneova prosta broja postoji specifična dosljednost. Naime, ukoliko se u zapisu $2^n - 1$ umjesto n uvrsti $3, 7, 31$ ili 127, dobiveni broj također će biti Mersennov prost broj. Ta tvrdnja značila bi da postoji beskonačno Mersenneovih prostih brojeva jer svaki pronađeni M_n automatski generira još jedan oblika M_{M_n}. Nažalost, koristeći super-računalo, pokazano je da je $M_{M_{13}} = 2^{M_{13}} - 1 = 2^{8191} - 1$ složen broj, odnosno da tvrdnja općenito ne vrijedi.

Poglavlje 3

Savršeni brojevi

Fascinacija savršenim brojevima te njihovo proučavanje seže čak do jonskog razdoblja. Teorijom brojeva u tom razdoblju bavili su se Pitagorejci. Uvedene su razne klasifikacije brojeva koje su se razmatrale – od onih najjednostavnijih, s obzirom na parnost brojeva, preko složenosti, to jest razlikovanja prostih i složenih do savršenih brojeva. Savršeni broj je onaj prirodan broj kojemu je zbroj pravih djelitelja jednak upravo njemu samomu. Tada se znalo za svega četiri savršena broja: 6, 28, 496 i 8128.

U ranijem razdoblju, veći značaj se pridodavao tumačenju savršenih brojeva s religijskog aspekta u odnosu na njihov matematički značaj i proučavanje njihovih svojstava. Primjer tome su brojevi 6 i 28 koji su dobili svoj religijski opis. Tako je broju 6 pridodan aspekt stvaralaštva. Pri tome se naravno misli na stvaranje Zemlje na što se osvrnuo sveti Augustin tvrdivši da ju je Bog, budući da je svemoguć, mogao stvoriti u jednome danu, no ipak je to učinio u šest. Time ju je obilježio savršenstvom. S druge strane, znalo se da mjesecu treba 28 dana za obilazak Zemlje te je stoga i on dobio religijski značaj savršenosti.

3.1 Svojstva savršenih brojeva i otkrića vezana uz savršene brojeve

Ovo poglavlje započinjemo definicijom savršenih brojeva.

Definicija 3.1.1 (Savršeni brojevi)**.** *Za prirodan broj n kažemo da je* ***savršen*** *ako je* $\sigma(n) = 2n$*, to jest ako je n jednak sumi svojih pravih djelitelja.*

Kroz godine, matematičari su postavljali razne hipoteze vezane uz savršene brojeve od kojih su neke pokazane istinitima, a neke ne. Hipoteze vezane uz svojstva savršenih brojeva bit će navedene u ovome dijelu rada, a također i obrazložena njihova (ne)istinitost.

Promatrajući prva četiri savršena broja Nicomachus u svome djelu *Uvod u aritmetiku* ukazuje na njihov raspored među deseticama, stoticama i tisućicama. Naime, u prvih 10 brojeva nalazi se samo jedan savršeni broj, također u brojevima od 10 do 100 nalazi se samo jedan savršeni broj, a isto se ponavlja i gledajući brojeve od 100 do 1000 te brojeve od 1000 do 10 000. Ta opservacija dovela je do zaključka da se n-ti savršeni broj (ako ih poredamo od najmanjega prema najvećemu) sastoji od n znamenki. No, ta tvrdnja je pokazana neistinitom kada je pronađen idući, peti, savršeni broj 33550336, koji se sastoji od osam znamenki.

Nadalje, jedinice brojeva 6, 28, 496 i 8128 su naizmjence brojevi 6 i 8, što je potaknulo zaključak da svi parni savršeni brojevi naizmjence završavaju znamenkom 6 i 8 (ponovno gledajući od najmanjega). Ovaj put trebao se pronaći još jedan savršeni broj 8589869056 kako bi se pokazalo da tvrdnja ne vrijedi.

Iako nije istina da su zadnje znamenke savršenih brojeva naizmjence 6 i 8, s pravom se možemo pitati jesu li uvijek samo 6 ili 8? Za parne savršene brojeve, jesu. Kako bismo dokazali tu tvrdnju, prvo moramo uvesti opći oblik savršenih brojeva. Način provjere, odnosno pronalaska savršenih brojeva predstavio je Euklid u svojoj knjizi *Elementi* kada je dokazao da ako je suma brojeva $1 + 2 + 2^2 + 2^3 + \ldots + 2^{k-1}$ jednaka p, gdje je p prost broj i k prirodan broj veći od 2, tada je $2^{k-1}p$ savršeni broj. Jedan od primjera je

$$1 + 2 + 2^2 + 2^3 + 2^{(5-1)} = 31, \text{ gdje je } k = 5, p = 31$$

te je stoga

$$2^{k-1} \cdot 31 = 2^4 \cdot 31 = 16 \cdot 31 = 496,$$

odnosno 496 je savršeni broj i to upravo treći gledajući od najmanjega. Kako je broj p prikazan kao suma geometrijskog niza gdje je početni član jednak 1 te kvocijent jednak 2, primjećujemo da vrijedi i tvrdnja sljedećeg oblika:

$$2^{k-1}(2^k - 1) \text{ je savršeni broj ako je } 2^k - 1 \text{ prost broj, gdje je } k > 1.$$

Teorem 3.1.2 (Euklid)**.** *Neka je* $2^n - 1$ *prost, gdje je* $n > 1$*. Tada je* $N = 2^{n-1}(2^n - 1)$ *savršen.*

Dokaz. Jedini prosti faktori od N su $2^n - 1$ i 2. Kako se $2^n - 1$ pojavljuje s potencijom 1 vrijedi $\sigma(2^n - 1) = (1 + (2^n - 1)) = 2^n$. Slijedi

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

Dakle, N je savršeni broj. □

Za brojeve N iz prethodnog teorema kažemo da su Euklidovog oblika.

Sljedeći teorem, kojeg je dokazao Euler, govori nam kako svaki paran savršen broj mora biti upravo Euklidovog oblika.

Teorem 3.1.3. *Neka je N paran savršen broj. Tada N možemo napisati u obliku $N = 2^{n-1}(2^n - 1)$, gdje je $2^n - 1$ prost broj.*

Navest ćemo nekoliko dokaza ovog teorema.

Prvi dokaz. Neka je $N = 2^{n-1}m$ paran savršeni broj, gdje je m neparan. Kako 2 ne dijeli m, znači da su m i 2^{n-1} relativno prosti te da vrijedi

$$\sigma(N) = \sigma(2^{n-1}m) = \sigma(2^{n-1})\sigma(m) = \left(\frac{2^n - 1}{2 - 1}\right)\sigma(m) = (2^n - 1)\sigma(m). \tag{3.1}$$

Broj N je savršen pa vrijedi $\sigma(N) = 2N = 2(2^{n-1}m) = 2^n m$ te uz jednadžbu (3.1) imamo $2^n m = (2^n - 1)\sigma(m)$.

Neka je sada $s = \sigma(m)$. Tada je $m = (2^n - 1)\left(\frac{s}{2^n}\right)$ jer 2^n ne dijeli $2^n - 1$, onda mora dijeliti s (jer je m cijeli broj). Vrijedi $m = (2^n - 1)q$ za neki $q = \frac{s}{2^n}$.

Ako je $q = 1$, imamo broj Euklidovog oblika, takav da $m = 2^n - 1$ i $s = \sigma(m) = 2^n = (2^n - 1) + 1 = m + 1$. Kako je $\sigma(m)$ zbroj svih pravih djelitelja od m, onda $m = 2^n - 1$ mora biti prost broj i $N = 2^{n-1}m = 2^{n-1}(2^n - 1)$.

Ako je $q > 1$, u prave djelitelje spadaju i $1, q, 2^n - 1$ i m. Tada

$$s = \sigma(m) \geq 1 + q + (2^n - 1) + (2^n - 1)q = ((2^n - 1) + 1)(q + 1) = 2^n(q + 1).$$

To povlači

$$\frac{m}{s} \leq \frac{(2^n - 1)q}{2^n(q + 1)} = \left(\frac{2^n - 1}{2^n}\right)\left(\frac{q}{q + 1}\right) < \frac{2^n - 1}{2^n},$$

što je kontradikcija s $\sigma(N) = 2^n m = (2^n - 1)s$, odnosno, $\frac{m}{s} = \frac{2^n - 1}{2^n}$. □

Drugi dokaz. Iz $2^n m = (2^n - 1)\sigma(m)$ slijedi

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

Budući da su $\sigma(m)$ i m cijeli brojevi, i $d = \frac{m}{2^n - 1}$ mora biti cijeli broj. Dakle, mora vrijediti

$$(2^n - 1) \mid m, \text{ odnosno } d \mid m.$$

Suma $\sigma(m) = m + \frac{m}{2^n - 1} = m + d$ je onda suma svih pravih djelitelja od m samo ako je $d = 1$. Kada bi imali d različit od 1, vrijedilo bi $\sigma(m) = m + d + 1$, što je kontradikcija.

Dakle, $m = 2^n - 1$, i preciznije, m nema drugih djelitelja osim 1 i sebe samoga, pa $2^n - 1$ mora biti prost. □

Treći dokaz. Kako je $2^n m = (2^n - 1)\sigma(m)$, svaki prosti djelitelj od $2^n - 1$ mora također biti i djelitelj od m jer su neparni pa ne dijele 2^n.

Pretpostavimo sada da p^α dijeli $2^n - 1$, gdje je p prost. Kada a dijeli b, vrijedi $\frac{\sigma(a)}{a} \leq \frac{\sigma(b)}{b}$ (jednakost vrijedi za $a = b$). Dakle,

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

To jest,

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

Stoga drugi sumand na desnoj strani mora biti jednak nuli, odnosno $p = 2^n - 1, \alpha = 1$ i $m = p$, odnosno N je Euklidovog oblika. □

Četvrti dokaz. Ponovno počnimo s $2^n m = (2^n - 1)\sigma(m)$, gdje $2^n - 1 \mid m$. Tada

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

Sada

$$\frac{2^n}{2^n - 1} = \frac{\sigma(m)}{m} > \frac{\sigma(2^n - 1)}{2^n - 1} \geq \frac{1 + (2^n - 1)}{2^n - 1} = \frac{2^n}{2^n - 1}.$$

Kako bi vrijedila jednakost, mora biti $2^n - 1 = m$ i $\sigma(m) = 1 + (2^n - 1) = 1 + m$ ili je $m = 2^n - 1$ prost. □

Pronalazak parnih savršenih brojeva ovim teoremom pojednostavljen je na pronalazak prostih brojeva oblika $2^k - 1$, odnosno Mersenneovih prostih brojeva. Ako je $2^k - 1$ prost broj, može se dokazati da je i k prost broj.

Generalizacija te tvrdnje slijedi u sljedećoj lemi:

Lema 3.1.4. *Ako je $a^k - 1$ prost broj i $a > 0,\ k \geq 2$, tada je $a = 2$ i k je prost broj.*

Dokaz. Lako se pokaže da

$$a^k - 1 = (a-1)(a^{k-1} + a^{k-2} + \ldots + a + 1), \tag{3.2}$$

odnosno,

$$a^{k-1} + a^{k-2} + \ldots + a + 1 \geq a + 1 > 1.$$

Po pretpostavci leme je $a^k - 1$ prost pa prvi faktor u jednadžbi (3.2) mora biti 1, to jest $a - 1 = 1$, iz čega slijedi da je $a = 2$.

Kada bi k bio složen, mogli bismo ga zapisati kao $k = rs$, gdje je $1 < r$ i $1 < s$. Tada bi vrijedilo da je

$$a^k - 1 = (a^r)^s - 1 = (a^r - 1)(a^{r(s-1)} + a^{r(s-2)} + \ldots + a^r + 1)$$

i da je svaki faktor s desne strane veći od 1. Slijedi da je $a^k - 1$ složen, što je kontradikcija s pretpostavkom leme. Dakle, k mora biti prost. □

Za prva četiri prosta broja obrat leme vrijedi, odnosno za $p = 2, 3, 5, 7$ vrijednosti izraza $2^p - 1$ jesu prosti brojevi te vrijednosti izraza $2^{p-1}(2^p - 1)$ savršeni brojevi. No, općenito obrat ne vrijedi. Prvi je to dokazao Hudalricus Regius[1] kontraprimjerom za

$$2^{11} - 1 = 2047 = 23 \cdot 89.$$

Idući po redu prosti broj $p = 13$ ponovo izrazu $2^p - 1$ pridružuje vrijednost koja je prosti broj te je vrijednost izraza $2^{12}(2^{13} - 1)$ peti po redu savršen broj. Postavlja se pitanje koliko zapravo savršenih brojeva postoji, ima li ih beskonačno te jesu li svi oni parni. Dokažimo prvo već spomenutu tvrdnju koristeći prethodno dokazanu lemu da je onima koji jesu parni zadnja znamenka upravo 6 ili 8.

Teorem 3.1.5. *Parni savršeni broj n za posljednju znamenku ima broj* 6 *ili* 8. *Ekvivalentno, vrijedi $n \equiv 6 \bmod 10$ ili $n \equiv 8 \bmod 10$.*

Dokaz. Zapišimo n kao $n = 2^{k-1}(2^k - 1)$, gdje je $2^k - 1$ prost. Koristeći Lemu 3.1.4, broj k također mora biti prost. Ako je $k = 2$, tada je $n = 6$ te tvrdnja vrijedi. Za $k > 2$ razlikujemo dva slučaja.

Ako je k oblika $4m + 1$, tada

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

Matematičkom indukcijom pokaže se da vrijedi $16^t \equiv 6 \bmod 10$ za svaki pozitivan cijeli broj t. Koristeći tu tvrdnju, imamo

$$n \equiv 2 \cdot 6 - 6 \equiv 6 \bmod 10.$$

Ako je k oblika $k = 4m + 3$, tada

$$n = 2^{4m+2}(2^{4m+3} - 1) = 2^{8m+5} - 2^{4m+2} = 2 \cdot 16^{2m+1} - 4 \cdot 16^m.$$

Koristeći da je $16^t \equiv 6 \bmod 10$ vidimo da je

$$n \equiv 2 \cdot 6 - 4 \cdot 6 \equiv -12 \equiv 8 \bmod 10.$$

Dakle, svaki paran savršeni broj završava znamenkom 6 ili 8. □

[1] danski matematičar, 16. stoljeće

Vrijedi i stroža tvrdnja prethodnog teorema, svaki paran savršeni broj završava znamenkom 6 ili znamenkama 28. Ovu tvrdnju nećemo formalno dokazivati, ali objasnit ćemo ideju dokaza. Naime, ako je k oblika $4m + 3$, tada je $n \equiv 28 \bmod 100$. Počnimo s faktorom 2^{k-1} raspisa savršenog broja $n = 2^{k-1}(2^k - 1)$.

$$2^{k-1} = 2^{4m+2} = 16^m \cdot 4 \equiv 6 \cdot 4 \equiv 4 \bmod 100.$$

Sada za $k > 2$, $4 \mid 2^{k-1}$ pa je broj koji čini posljednje dvije znamenke broja 2^{k-1} djeljiv s 4. Mogućnosti su 4, 24, 44, 64, 84. No, to znači da je $2^k - 1 = 2 \cdot 2^{k-1} - 1 \equiv 7, 47, 87, 27, 67 \bmod 100$, odnosno $n = 2^{k-1}(2^k - 1) \equiv 4 \cdot 7, 24 \cdot 47, 44 \cdot 87, 64 \cdot 27, 84 \cdot 67 \bmod 100$. Lako se provjeri da je ostatak pri dijeljenju sa 100 za ove produkte upravo 28.

3.2 Višestruko savršeni brojevi

Osim savršenih brojeva, postoje i višestruko savršeni brojevi. Njih definiramo na sljedeći način.

Definicija 3.2.1. *Neka je suma djelitelja broja n, uključujući n i* 1*, jednaka višekratniku broja n. Tada je n* ***višestruko savršen broj****. Za sumu mn, m je višestrukost od n. Višestruko savršeni broj višestrukosti m pišemo kao* P_m*.*

S obzirom na definiciju možemo zaključiti da je obični savršeni broj ujedno i višestruko savršeni broj višestrukosti $m = 2$, to jest P_2.

Primjer 3.2.2. *Pokažimo po definiciji da je prvi otkriveni broj* $P_3 = 120$ *višestruko savršen. Djelitelji broja* 120 *su redom:* $1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 24, 30, 40, 60, 120$*. Njihova suma iznosi* $360 = 3 \cdot 120$*. Dakle, suma djelitelja broja* 120 *je njegov višekratnik, odnosno* $n = 120, m = 3$*.*

Mersenne je postavio problem pronalaska brojeva P_4, P_5 i $P_3 \neq 120$. Također tu je i problem pronalaska univerzalnog pravila koje će pomoći pri određivanju što više višestruko savršenih brojeva.

Pierre de Fermat[2] pronašao je $P_3 = 672 = 2^5 \cdot 3 \cdot 7$ čija je suma djelitelja jednaka $2016 = 3 \cdot 672$. Također je osmislio i metodu za pronalazak preostalih višestruko savršenih brojeva višestrukosti 3. Najprije odaberemo proizvoljan n. Nadalje računamo $p = \frac{2^{n+3}-1}{2^n+1}$. Ako je p prost broj, tada je $3 \cdot 2^{n+2} \cdot p$ višestruko savršen broj P_3.

Primjer 3.2.3. *Koristeći prethodnu metodu pokažimo da je* 120 P_3*. Neka je* $n = 1$*. Tada je*

$$p = \frac{2^{n+3} - 1}{2^n + 1} = \frac{2^4 - 1}{2^1 + 1} = \frac{15}{3} = 5.$$

[2]francuski matematičar, 1607. — 1665.

Vidimo da je p prost broj što znači da je uvjet zadovoljen. Sada je P_3

$$3 \cdot 2^{n+2} \cdot p = 3 \cdot 2^3 \cdot 5 = 3 \cdot 8 \cdot 5 = 120.$$

Jednaka metoda vrijedi i za pronazalak drugog i trećeg P_3 broja,

$$P_3^2 = 3 \cdot 7 \cdot 32 = 672$$

i

$$P_3^3 = 2^9 \cdot 3 \cdot 11 \cdot 31 = 523776.$$

No, Descartes[3] je bio kritičan prema toj metodi. Tvrdio je da je Fermat prilagodio metodu brojevima 120 i 672 nakon što ih je već pronašao. Također je pronašao i četvrti P_3 te nekoliko P_4 brojeva i jedan P_5 broj.

$$\begin{aligned}
P_3^{(4)} &= 1476304896 = 2^{13} \cdot 3 \cdot 11 \cdot 43 \cdot 127,\\
P_4^{(1)} &= 30240 = 2^5 \cdot 3^3 \cdot 5 \cdot 7,\\
P_4^{(2)} &= 32760 = 2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13,\\
P_4^{(3)} &= 23569920 = 2^9 \cdot 3^3 \cdot 5 \cdot 11 \cdot 31,\\
P_4^{(4)} &= 142990848 = 2^9 \cdot 3^2 \cdot 7 \cdot 11 \cdot 13 \cdot 31,\\
P_4^{(5)} &= 66433720320 = 2^{13} \cdot 3^3 \cdot 5 \cdot 11 \cdot 43 \cdot 127,\\
P_4^{(6)} &= 403031236608 = 2^{13} \cdot 3^2 \cdot 7 \cdot 11 \cdot 13 \cdot 43 \cdot 127,\\
P_5^{(1)} &= 14182439040 = 2^7 \cdot 3^4 \cdot 5 \cdot 7 \cdot 11^2 \cdot 17 \cdot 19.
\end{aligned}$$

Metodu koju je koristio, Descartes nije oblikovao u formulu, no analizu je opisao pomoću nekoliko pravila:

1. Ako je n broj P_3 koji nije djeljiv s 3, onda je $3n$ broj P_4.
2. Ako je P_3 djeljiv s 3, ali nije djeljiv ni s 5 ni s 9, onda vrijedi da je $45 \cdot P_3$ broj P_4.
3. Ako je P_3 djeljiv s 3, ali nije djeljiv sa $7, 9$ ni s 13, onda vrijedi da je $3 \cdot 7 \cdot 13 \cdot P_3$ broj P_4.
4. Ako je n djeljiv s 2^9, ali nije djeljiv ni s jednim od brojeva $2^{10}, 31, 43, 127$, onda su $31 \cdot n$ i $16 \cdot 43 \cdot 127 \cdot n$ proporcionalne sumi njihovih djelitalja (ne uključujući njih same).
5. Ako n nije djeljiv s 3 i ako je $3n$ broj P_{4k}, onda je n broj P_{3k}.

[3] René Descartes, francuski filozof, znanstvenik i matematičar, 1596. – 1650.

Primjenom drugog pravila na brojeve $P_3^{(2)}, P_3^{(3)}, P_3^{(4)}$, Descartes je pronašao brojeve $P_4^{(1)}, P_4^{(3)}, P_4^{(5)}$, a primjenom trećeg pravila na brojeve $P_3^{(1)}, P_3^{(3)}, P_3^{(4)}$, brojeve $P_4^{(2)}, P_4^{(4)}, P_4^{(6)}$. Vjerovao je da se može postaviti beskonačno mnogo ovakvih pravila te pomoću njih pronaći beskonačno mnogo brojeva P_m.

Robert Daniel Carmichael[4] pokazao je da:

1. ne postoje neparni brojevi P_m sa samo tri različita prosta broja u svojoj faktorizaciji,
2. su $2^3 \cdot 3 \cdot 5$ i $2^5 \cdot 3 \cdot 7$ jedini brojevi P_m sa samo tri različita prosta broja u svojoj faktorizaciji,
3. su $P_3^{(3)} = 523776 = 2^9 \cdot 3 \cdot 11 \cdot 31$ i Descarteov $P_4^{(1)}$ jedini brojevi P_m s četiri različita prosta broja u svojoj faktorizaciji,
4. su Descarteovi $P_3^{(4)}, P_4^{(2)}, P_4^{(3)}$ i Mersenneov $P_4^{(8)} = 45532800 = 2^7 \cdot 3^3 \cdot 5^2 \cdot 17 \cdot 31$ parni višestruko savršeni brojevi s pet različitih prostih faktora u svojoj faktorizaciji.

3.3 Neparni savršeni brojevi

Do sada smo spominjali savršene brojeve u kontekstu parnih savršenih brojeva, no postoje li i oni koji su neparni? Upravo to je jedno od velikih pitanja teorije brojeva. Iako do sada nije otkriven niti jedan neparan savršeni broj, postoje svojstva koja ga karakteriziraju. Prvi od uvjeta koji mora zadovoljiti, a koji je postavio Euler, dajemo idućom tvrdnjom.

Teorem 3.3.1 (Eulerov teorem)**.** *Neka je n neparan savršen broj, tada vrijedi*

$$n = p_1^{k_1} p_2^{2j_2} \cdots p_r^{2j_r},$$

gdje su $p_1, p_2, \ldots, p_r$ različiti neparni prosti brojevi i vrijedi $p_1 \equiv k_1 \equiv 1 \bmod 4$.

Dokaz. Neka je $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ jednoznačna faktorizacija broja n. Budući da je n savršen, $2n$ možemo zapisati kao

$$2n = \sigma(n) = \sigma(p_1^{k_1})\sigma(p_2^{k_2}) \cdots \sigma(p_r^{k_r}).$$

Kako je n neparan cijeli broj, vrijedi ili $n \equiv 1 \bmod 4$ ili $n \equiv 3 \bmod 4$, a u oba slučaja vrijedi $2n \equiv 2 \bmod 4$. Slijedi da je $\sigma(n) = 2n$ djeljiv s 2, ali ne i s 4. Dakle, mora vrijediti da je jedan od $\sigma(p_i^{k_i})$, na primjer $\sigma(p_q^{k_1})$ paran cijeli broj (koji nije djeljiv s 4), dok su svi ostali neparni cijeli brojevi. Za dani p_i promatramo dva moguća slučaja: $p_i \equiv 1 \bmod 4$ i $p_i \equiv 3 \bmod 4$.

[4] američki matematičar, 1879.– 1967.

Ako je $p_i \equiv 3 \bmod 4 \equiv -1 \bmod 4$, vrijedi

$$\begin{aligned}\sigma(p_i^{k_i}) &= 1 + p_i + p_i^2 + \cdots + p_i^{k_i} \\ &\equiv 1 + (-1) + (-1)^2 + \cdots + (-1)^{k_i} \bmod 4 \\ &\equiv \begin{cases} 0 \bmod 4, & k_i \text{ neparan} \\ 1 \bmod 4, & k_i \text{ paran} \end{cases}.\end{aligned}$$

Jer je $\sigma(p_1^{k_1}) \equiv 2 \bmod 4$ slijedi $p_1 \not\equiv 3 \bmod 4$, odnosno $p_1 \equiv 1 \bmod 4$. Nadalje iz $\sigma(p_i^{k_i}) \equiv 0 \bmod 4$, slijedi da 4 dijeli $\sigma(p_i^{k_i})$ što nije moguće. Dakle, ako vrijedi $p_i \equiv 3 \bmod 4$, gdje $i = 2, \ldots, r$, tada je k_i paran cijeli broj.

Ako je $p_i \equiv 1 \bmod 4$, što je istina na primjer za $i = 1$, tada

$$\begin{aligned}\sigma(p_i^{k_i}) &= 1 + p_i + p_i^2 + \cdots + p_i^{k_i} \\ &\equiv 1 + 1 + 1^2 + \cdots + 1^{k_i} \bmod 4 \\ &\equiv k_i + 1 \bmod 1.\end{aligned}$$

Budući da je $\sigma(p_1^{k_1}) \equiv 2 \bmod 4$ mora biti $k_1 \equiv 1 \bmod 4$. Za ostale vrijednosti i, znamo da vrijedi $\sigma(p_i^{k_i}) \equiv 1 \bmod 4$ ili $\sigma(p_i^{k_i}) \equiv 3 \bmod 4$ iz čega slijedi $k_i \equiv 0 \bmod 4$ ili $k_i \equiv 2 \bmod 4$, a za oba slučaja vrijedi da je k_i paran cijeli broj.

Dakle, bez obzira je li $p_i \equiv 1 \bmod 4$ ili $p_i \equiv 3 \bmod 4$, k_i je uvijek paran za $i \neq 1$. □

Drugim riječima, Eulerov nam teorem govori kako svaki neparan savršeni broj možemo prikazati kao produkt

$$n = p_1^{k_1} p_2^{2j_2} \cdots p_r^{2j_r} = p_1^{k_1}(p_2^{j_2} \cdots p_r^{j_r})^2 = p_1^{k_1} m^2,$$

iz čega slijedi sljedeći korolar.

Korolar 3.3.2. *Ako je n neparan savršeni broj, onda je oblika*

$$n = p^k m^2,$$

gdje je p prost broj, $p \nmid m$ *i* $p \equiv k \equiv q \bmod 4$. *Posebno,* $n \equiv 1 \bmod 4$.

Dokaz. Jedini netrivijalni dio ovog korolara je posljednja tvrdnja $n \equiv 1 \bmod 4$ te ćemo nju i dokazati.

Kako je $p \equiv 1 \bmod 4$, slijedi $p^k \equiv 1 \bmod 4$. Primijetimo da m mora biti neparan, stoga vrijedi $m \equiv 1 \bmod 4$ ili $m \equiv 3 \bmod 4$. Kvadriranjem $m^2 \equiv 1 \bmod 4$ slijedi

$$n = p^k m^2 \equiv 1 \cdot 1 \equiv 1 \bmod 4.$$

□

Nekolicina matematičara koja je proučavala ovaj teorem navela je dodatna svojstva koje se trebaju ispuniti kako bi teorem vrijedio. Godine 1937. njemački matematičar Rudolf Steuerwald je pokazao da ne smiju svi $j_2, \ldots, j_r$ biti jednaki 1. Odnosno, ako vrijedi da je $n = p_1^{k_1} p_2^2 \cdots p_r^2$ neparan broj uz uvjet $p \equiv k_1 \equiv 1 \bmod 4$ tada n nije savršen broj. Zatim je 1941. drugi njemački matematičar Hans–Joachim Kanold ustanovio da ne smiju svi $j_2, \ldots, j_r$ biti jednaki 2, niti smije jedan od njih biti jednak 2 i ostali jednaki 1. Naposljetku, američki matematičari Peter Hagis Jr. i Wayne L. McDaniel su 1972. otkrili da također svi $j_2, \ldots, j_r$ ne smiju biti jednaki 3.

Iduće svojstvo koje se definiralo je veličina neparnog savršenog broja, odnosno njegova donja granica. Nju je odredio Turcaninov te opisao na sljedeći način: ako je n neparan savršeni broj, onda ima barem četiri različita prosta faktora te je veći od $2 \cdot 10^6$. Upotreba računala i suvremene matematike precizirala su taj zahtjev te povećala donju granicu na $n > 10^{1500}$. Također je pokazano da n mora biti djeljiv s najmanje 101 ne nužno različitih prostih djelitelja te da je najveći od njih veći od 10^{62}.

Prije no što opišemo dokaz da ne postoji neparan savršeni broj manji od 10^{1500}, opišimo algoritam za dokazivanje da ne postoji neparan savršeni broj manji od dane granice 10^K, gdje je $K = 160$.

Teorem 3.3.3. *Ne postoji neparan savršen broj manji od* 10^{160}.

Dokaz je gotovo u cijelosti računalno generiran, a koristi se metoda eliptične zakrivljenosti. Pod pretpostavkom da postoji neparan savršeni broj n, koristeći Teorem 3.3.1 uz uvjet $a_i \equiv 0 \bmod 2$ za $i = 1, \ldots, t$, znamo da je n oblika $n = \prod_{i=0}^{t} p_i^{a_i}$, gdje su $p_0, \ldots, p_t$ različiti prosti brojevi i $p_o \equiv a_0 \equiv 1 \bmod 4$. Nadalje ćemo koristiti taj zapis te elemente produkta $p_i^{a_i}$ zvati komponentama od n.

Kako je σ (podsjetimo se, funkcija zbroja djelitelja) multiplikativna funkcija i vrijedi $\sigma(n) = 2n$, slijedi da su skupovi $\{q : q \text{ prost}, q > 2,\ q \mid \sigma(p_i^{a_i}) \text{ za } i = 0, 1, \ldots, t\}$ i $\{p_0, \ldots, p_t\}$ jednaki. Pretpostavimo li da postoji komponenta p^a od n možemo generirati ostale proste faktore od n, odnosno neparne proste faktore od $\sigma(p^a)$. Nazovemo li neki od tih faktora q, za njega pretpostavimo da postoji eksponent b te onda za q na isti način možemo generirati još prostih faktora od n. Taj postupak nazivamo grananje i on se nastavlja sve dok se ne naiđe na kontradikciju ili na neparni savršeni broj. Rezultirajuće kontradikcije pronalaska navedenih faktora i njihovih eksponenata sačinjavaju dokaz vrlo bitnog teorema. Prvo navedimo još neka svojstva koja će nam biti korisna za razumijevanje istog.

Za neki prost broj p vrijedi $\sigma(p^a) \mid \sigma(p^b)$ ako $a + 1 \mid b + 1$. Uz pretpostavku da a postoji, zahtijevamo da je $a + 1$ prost broj. Preciznije, možemo pretpostaviti da vrijedi $a_0 = 1$. Mogući prosti djelitelji od $\sigma(p^a)$ (gdje su p i $a + 1$ prosti brojevi i vrijedi $a > 1$) su $a + 1$ ako i samo ako vrijedi $p \equiv 1 \bmod a + 1$ i $q \equiv 1 \bmod a + 1$.

Teorem 3.3.4. *Pretpostavimo da je n neparan savršeni broj manji od* 10^{160}. *Neka postoji komponenta* p^a *od n, gdje je a paran broj. Tada možemo pretpostaviti da je* $p^a < 10^{80}$ *jer bi u protivnome vrijedilo* $n \geq p^a\sigma(p^a) > p^{2a} > 10^{160}$.

Kako bi se izbjeglo ponavljanje istih faktorizacija, potencijalni prosti faktori od n pripadaju skupu $S = \{127, 19, 7, 11, 31, 13, 3, 5\}$ te se eliminiraju točno tim redom kojim su zapisani. Ako niti jedan od elemenata skupa S nije prosti faktor broja n, tada n mora sadržati barem 101 različit prost faktor. Kada bi ih bilo manje, vrijedilo bi

$$\frac{\sigma(n)}{n} = \prod_{i=0}^{t} \frac{p_i - p_i^{-a_i}}{p_i - 1} < \prod_{i=0}^{t} \frac{p_i}{p_i - 1} \leq \frac{17}{16} \cdot \frac{23}{22} \cdot \frac{29}{28} \prod_{P} \frac{p}{p-1} < 2,$$

gdje je $P = \{p : p \text{ prost}, 37 \leq p \leq 599,\ p \neq 127\}$. To je kontradikcija jer se na desnoj strani nejednadžbe nalazi ukupno 100 prostih faktora. Dakle, imamo

$$n \geq \left(17 \cdot 23 \cdot 29 \cdot \prod_{P} p\right)^2 \cdot 601 > 10^{473},$$

što znači da ćemo eliminacijom osam navedenih elemenata skupa S dokazati Teorem 3.3.4. Jednom kada se jedan od elemenata skupa S eliminira, njegovo kasnije pojavljivanje u lancu faktora završava taj lanac. Pojedinačni lanci faktora nastavljaju se, koristeći najveći pronađeni faktor iz zadnje faktorizacije sve dok ili jedan od faktora nije veći od 10^{80} ili dok produkt svih elemenata lanca (uključujući njihove potencije prilagođene Eulerovom teoremu (Teorem 3.3.1) nije veći od 10^{160}.

Inzistira se i na tome da je potencija najvećeg generiranog prostog broja kongruentnog s q mod 4 upravo 1 ukoliko ne postoji niti jedan drugi element lanca koji je prva komponenta u Eulerovom zapisu. Iznimka bi postojala ukoliko bi najveći element bio generiran više nego jednom, što nikada nije.

Ukoliko lanci nisu završeni pojavljivanjem već eliminiranog elementa skupa S, to se događa tako što ne zadovoljavaju "S-test". Odnosno, ako nekoliko generiranih "malih" prostih faktora (prilagođenih Eulerovom obliku) daju produkt m takav da $S = \frac{\sigma(m)}{m} > 2$, onda djelitelj l od n mora zadovoljavati $\frac{\sigma(l)}{l} \leq 2$.

Mnogi složeni brojevi ili potencijalni prosti brojevi ne zahtijevaju posebnu provjeru. Tim brojevima provjeravaju se zajednički faktori s ostalim brojevima unutar lanca te su potom dodani u produkt s tim brojevima uz potenciju 1. Testiranje Euklidovim algoritmom generalno je puno brže od faktorizacije tih brojeva.

Sada opišimo kako se dokazuje tvrdnja za $K = 1500$, odnosno sljedeći teorem.

Teorem 3.3.5. *Ne postoji neparan savršeni broj manji od* 10^{1500}.

Opis dokaza ovog teorema oslanja se na metodu predstavljenu u prethodnome. Za početak, na isti način definiramo skup faktora S, no ovaj put s više elemenata:

$$S = \{127, 19, 7, 11, 331, 31, 97, 61, 13, 398581, 1093, 3, 5, 307, 17\}.$$

Ponovno se prvo počinje grananjem lanaca. Koriste se dvije moguće kontradikcije:

1. $\frac{\sigma(p^a)}{p^a}$ je strogo veći od 2 za trenutnu komponentu p^a.

2. Trenutna komponenta p^a je veća od 10^{1500}.

Kod grananja prostog broja p uzima se u obzir potencija od p u n. Lanac se završava kada je potencija od p takva da $p^a > 10^{1500}$. Poseban uvjet je (osim u kasnije navedenim iznimkama) da se u obzir uzimaju samo oni a za koje je $a+1$ prost. Taj uvjet važan je zbog skraćivanja posla provjere kontradikcija, uzima se p^a kao reprezentacija za sve $p^{(a+1)t-1}$ jer se za njih pojavljuju jednake kontradikcije.

U situcijama kada ne postoje kontradikcije, niti mogućnost za grananje prostih faktora koristi se sljedeća metoda za koju je potrebno poznavanje gornje granice $\frac{\sigma(p^a)}{p^a}$ trenutne komponente te da je ona strogo manja od 2. Očita gornja granica je $\sigma(p^\infty)_{-1} = \frac{p}{p-1}$. No, ona ne osigurava da je $\frac{\sigma(p^a)}{p^a} < 2$. Kako bi se to omogućilo radi se ili egzaktno grananje komponenti $p^1, 3^2, 3^4$ i 7^2) ili standardno grananje (sve ostalo) što donosi nove dodatne kontradikcije.

U slučaju egzaktnog grananja moramo dodati standardno grananje na $3^8, 3^{14}, 3^{24}$ i 7^8 kako bismo pokrili sve moguće eksponente za 3 i 7. Spomenimo i da se za p^1 uvijek koristi egzaktno grananje.

Naposljetku prokomentirajmo σ ne faktoriziranih složenih faktora. Provjeravamo da složeni broj s nema faktora manjih od α (koristimo $\alpha = 10^8$ tako da s ima najviše $\lfloor \frac{\ln s}{\ln \alpha} \rfloor$ različitih prostih faktora od kojih je svaki veći od α. Tada je $\sigma(s)$ najviše $\frac{\alpha}{\alpha-1}^{\lfloor \frac{\ln s}{\ln \alpha} \rfloor}$. Metoda je ispravna ako je $a < 2$.

Komentirajmo posebno slučaj kada n nema komponenti u S, tada je $n > 10^{1500}$. Argumentacija je unaprijeđena verzija prethodne.

Za preostala dva uvjeta, iako ponovno postoje posebni slučajevi kod kojih su nužne drugačije metode i pristupi) navest ćemo samo tražene kontradikcije koje ih dokazuju.

Teorem 3.3.6. *Ukupan broj prostih faktora neparnog savršenog broja je barem* 101.

U dokazu se koriste sljedeće kontradikcije:

1. $\frac{\sigma(p^a)}{p^a}$ je strogo veći od 2 za trenutnu komponentu p^a.

2. Trenutna komponenta p^a ima barem 101 prost faktor.

Teorem 3.3.7. *Najveća komponenta neparnog savršenog broja je veća od* 10^{62}.

U dokazu se koriste sljedeće kontradikcije:

1. $\frac{\sigma(p^a)}{p^a}$ je strogo veći od 2 za trenutnu komponentu p^a.
2. Trenutna komponenta p^a ima komponentu veću od 10^{62}.

Bibliografija

[1] R. P. Brent, G. L. Cohen, *A New Lower Bound for Odd Perfect Numbers*, Mathematics of Computation, Volume 53, Number 187, 1989., PAGES 431-437, https://www.ams.org/journals/mcom/1989-53-187/S0025-5718-1989-0968150-2/S0025-5718-1989-0968150-2.pdf, (pristupljeno 16. srpanj 2024.).

[2] F. M. Brückler, *Povijest matematike*, skripta s predavanja, PMF – Matematički odsjek, 2022., https://www.pmf.unizg.hr/_download/repository/skripta2024.pdf, (pristupljeno 16. svibanj 2024.).

[3] D. M. Burton, *Elementary Number Theory*, seventh edition, University of New Hampshire, 2011.

[4] L. E. Dickson, *History of the Theory of Numbers, Volume 1, Divisibility and Primality*, Dover Publications, Inc. Mineola, Neq York

[5] A. Dujella, *Uvod u teoriju brojeva (skripta)*, skripta s predavanja, PMF –Matematički odjel, Sveučiliste u Zagrebu, https://web.math.pmf.unizg.hr/~duje/utb/utblink.pdf, (pristupljeno 16. svibanj 2024.).

[6] M. Moguš, *Testovi prostosti*, završni rad, Osijek 2022., https://repozitorij.mathos.hr/islandora/object/mathos%3A649/datastream/PDF/view, (pristupljeno 16. srpanj 2024.).

[7] P. Ochem, M. Rao, *Odd perfect numbers are greater than* $10^{1}500$, Mathematics of Computation, Volume 00, Number 0, Pages 000–000 S 0025-5718(XX)0000-0, https://www.lirmm.fr/~ochem/opn/opn.pdf, (pristupljeno 16. srpanj 2024.).

[8] J. Voight, *Perfect Numbers: An Elementary Introduction*, Department of Mathematics, University of California, Berkeley, https://magma.maths.usyd.edu.au/~voight/notes/perfelem.pdf, (pristupljeno 09. rujan 2024.).

Sažetak

Savršeni brojevi interesantan su dio teorije brojeva. Matematičari ih godinama istražuju, no još uvijek nije poznata njihova primjena. Usko vezani uz savršene brojeve su i Mersenneovi brojevi. Jedan od načina pronalaska savršenih brojeva je pronalazak nešto jednostavnijih Mersenneovih prostih brojeva.

U ovom diplomskom radu navedeni su matematički temelji potrebni za razumijevanje istoga. Nakon toga slijede definicija i svojstva Mersenneovih brojeva te se spominje i opisuje Lucas–Lehmerov test provjere prostosti. Naposljetku se govori o savršenim brojecima, njihovim svojstvima, višestruko savršenim brojevima te uvjetima koje bi neparni savršeni brojevi trebali zadovoljavati ukoliko postoje.

Summary

Perfect numbers are an interesting part of number theory. Mathematicians have been researching them for years, but their application is still unknown. Closely related to perfect numbers are Mersenne numbers. One way to find perfect numbers is to find the simpler Mersenne primes.

This thesis presents the mathematical foundations necessary for understanding perfect numbers. This is followed by the definition and properties of Mersenne numbers, and the Lucas–Lehmer test for primality is mentioned and described. At the end, perfect numbers and their properties are discussed as well as multiply perfect numbers and conditions that odd perfect numbers should meet if they exist.

Životopis

Rođena sam 19. ožujka 1998. godine u Zagrebu u Republici Hrvatskoj. Osnovnu školu Luka u Sesvetama završila sam 2012. godine te tada upisala Srednju školu Jelkovec, smjer tehničar za računalstvo. Na Prirodoslovno - matematičkom fakultetu Sveučilišta u Zagrebu 2022. godine stječem akademski naziv sveučilišnog prvostupnika edukacije matematike. Iste godine upisala sam Diplomski sveučilišni studij Matematika; smjer nastavnički.

Tijekom studija sudjelujem u projektu Financijska pismenost u suvremenom matematičkom obrazovanju pod vodstvom profesora Željke Milin Šipuš te Matije Bašića te radim u Photomathu (veljača 2021. – lipanj 2024.)