O nekim otvorenim problemima iz teorije brojeva

Kuzek, Anđela

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Anđela Kuzek

O NEKIM OTVORENIM PROBLEMIMA IZ TEORIJE BROJEVA

Diplomski rad

Voditelj rada:
izv. prof. dr. sc. Zrinka Franušić

Zagreb, 2017.

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. _____

Sadržaj

Uvod

Teorija brojeva je grana matematike koja se bavi proučavanjem svojstava skupa prirodnih, cijelih i racionalnih brojeva i sadrži mnoštvo matematičkih problema koje je vrlo jednostavno formulirati i razumijeti, ali vrlo teško dokazati. Mnoge velike matematičke ideje i slutnje izazvale su zanimanje kroz povijest, a neke od njih muče matematičare već stotinama godinu i još uvijek nisu dokazane. Brojne novčane nagrade su raspisane kako bi potaknule znanstvenike da pokušaju pronaći odgovore i dokazati te naizgled jednostavne tvrdnje. Zbog svoje jednostavnosti, privlače i amatere te su pravi izazov za matematičare koji su pokušavajući ih dokazati došli do brojnih drugih rezultata i dokaza. Iako mnoge nedokazane tvrdnje imaju uvjerljive razloge koji navode na njihovu točnost, stogi matematički dokaz još uvijek ne postoji. Stoga se možemo pitati, jesu li te tvrdnje točne i postoje li uopće odgovori na njih.

U ovom radu biti će navedeni neki od najpoznatijih otvorenih problema u teoriji brojeva, povijesne zanimljivosti te važniji teoremi i rezultati potrebni za razumijevanje tih problema. Prvo poglavlje sadrži najpoznatije otvorene problema vezane uz savršene brojeve. Savršeni brojevi su prirodni brojevi koji su jednaki zbroju svih svojih pozitivnih djelitelja različitih od njih samih. Poznati su matematičarima još od Euklidovog doba (oko 330.-275.pr.Kr.). Neka od otvorenih pitanja su postoji li beskonačno mnogo savršenih brojeva te postoji li neparan savršen broj. Drugo poglavlje sadrži najpoznatije otvorene probleme vezane uz proste brojeve koji su osnovni pojam u teoriji brojeva. To su prirodni brojevi veći od broja 1 koji nemaju drugih djelitelja osim broja 1 i samih sebe. Tu su nam posebno zanimljivi Fermatovi i Mersenneovi brojevi te parovi blizanaca i slavna Goldbachova slutnja.

Francuski pravnik i matematičar Pierre de Fermat (1601.-1665.) proučavao je brojeve oblika

$$F_n = 2^{2^n} + 1,$$

za cijele brojeve n koji se, njemu u čast, nazivaju *Fermatovi brojevi*. Uvrštavajući $n = 0, 1, 2, 3, 4$ dobio je proste brojeve

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65\,537$$

te je postavio hipotezu da su svi brojevi oblika F_n prosti. Međutim, Leonhard Euler (1707. - 1783.) je pokazao da F_5 nije prost broj i tako opovrgnuo Fermatovu hipotezu. Stoga je još uvijek otvoreno pitanje postoji li samo pet prostih Fermatovih brojeva, odnosno jesu li svi Fermatovi brojevi F_n za $n > 4$ složeni. Isto tako i Fermatovi složeni brojevi su zainteresirali matematičare koji su uspjeli faktorizirati samo prvih dvanaest Fermatovih brojeva te je faktorizacija preostalih Fermatovih složenih brojeva još jedno otvoreno pitanje.

Francuski matematičar Marin Mersenne (1588.-1648.) bavio se prostim i složenim brojevima te je promatrao brojeve oblika

$$M_n = 2^n - 1,$$

za prirodan broj n koji se, njemu u čast, nazivaju *Mersenneovi brojevi*. Mersenneovi brojevi koji su prosti nazivaju se *Mersenneovi prosti brojevi* te još uvijek nije poznato postoji li beskonačno mnogo Mersenneovih prostih brojeva niti postoji li beskonačno mnogo Mersenneovih složenih brojeva. Isto tako, nije poznato postoji li beskonačno mnogo *parova blizanaca*, odnosno prostih brojeva oblika p i $p + 2$. Neki od parova blizanaca su

$$(3, 5), \quad (5, 7), \quad (11, 13), \quad (17, 19), \quad (29, 31)$$

te postoji mnogo rezultata koji idu u prilog hipotezi o beskonačnom broju parova blizanaca, međutim strogog matematičkog dokaza još uvijek nema.

Svakako jedan od najpoznatijih i najstarijih otvorenih problema, uz problem o parovima blizanaca je Goldbachova slutnja, koja je privukla pažnju mnogih te se pojavila u televizijskim emisijama, filmomovima pa i knjigama. Njemački matematičar Christian Goldbach (1690.-1764.) je 1742. godine izrazio slutnju da se svaki paran broj veći od broja 2 može zapisati kao zbroj dva prosta broja. Iako tvrdnja zvuči jako jednostavno i vjerojatno, od davne 1742. godine pa do danas, niti jedan matematičar nije ju uspio dokazati.

Iako se čini da ne postoje odgovori ni dokazi za stotinama godina nedokazane tvrdnje, primjer koji daje nadu je dokaz takozvanog Velikog Fermatovog teorema. Naime, on je više od 350 godina bio otvoreni problem, te ga je nakon mnogih pokušaja, 1995. godine priveo kraju matematičar Andrew Wiles.

Poglavlje 1

Djeljivost

1.1 Najveći zajednički djelitelj. Euklidov algoritam

Definicija 1.1.1. *Neka su a i b cijeli brojevi i $a \neq 0$. Kažemo da a **dijeli** b ako postoji cijeli broj x takav da je $b = ax$. Pišemo $a \mid b$. Još kažemo da je a **djelitelj** broja b, odnosno da je b **višekratnik** od a. Ako a **ne dijeli** b, onda pišemo $a \nmid b$.*

Na primjer, $8 \mid 1024$ i $3 \nmid 121$.

Teorem 1.1.2 (Teorem o dijeljenju s ostatkom)**.** *Za proizvoljan prirodan broj a i cijeli broj b postoje jedinstveni cijeli brojevi q i r takvi da je $b = qa + r$, gdje je $0 \leq r < a$.*

Dokaz. Promotrimo skup $\{b - am : m \in \mathbb{Z}\}$. S r označimo najmanji nenegativni član tog skupa. Tada je po definiciji $0 \leq r < a$ i postoji $q \in \mathbb{Z}$ takav da je $b - qa = r$, odnosno $b = qa + r$. Time smo pokazali da brojevi r i q postoje. Preostaje pokazati da su q i r jedinstveni. Pretpostavimo da postoji još jedan par q_1 i r_1 koji zadovoljava isto. Ako su q i r jedinstveni, mora vrijediti $r = r_1$ i $q = q_1$. Pretpostavimo da je npr. $r < r_1$. Tada je $0 \leq r_1 - r < a$, dok s druge strane vrijedi $b = qa + r$ i $b = q_1a + r_1$ i oduzimanjem dobivamo $r_1 - r = a(q - q_1) \geq a$. Prema tome je $r = r_1$ pa je stoga i $q = q_1$.

□

Definicija 1.1.3. *Neka su a i b cijeli brojevi koji nisu oba jednaka 0. Najveći cijeli broj koji dijeli oba broja a i b zove se **najveći zajednički djelitelj brojeva** i označava s $g = (a, b)$. Posebno, ako je najveći zajednički djelitelj brojeva a i b jednak 1, odnosno $(a, b) = 1$, tada kažemo da su brojevi a i b **relativno prosti**.*

Na primjer, $(4, 14) = 2$, $(n - 1, n) = 1$ za svaki $n \in \mathbb{Z}$. Uočimo da iz same definicije slijedi da je najveći zajednički djelitelj brojeva uvijek prirodan broj. Nadalje, Definicija 1.1.3 može se poopćiti za konačno mogo cijelih brojeva koji nisu svi jednaki nuli, odnosno

na najveći zajednički djelitelj brojeva $a_1, \ldots, a_k$ kojeg označavamo s $(a_1, \ldots, a_k)$.

Uzastopnom primjenom Teorema o dijeljenju s ostatkom 1.1.2 dobit ćemo poznati *Euklidov algoritam* - efikasan algoritam za određivanje najvećeg zajedničkog djelitelja dvaju brojeva. Prvi poznati sačuvani zapis Euklidovog algoritma nalazi se u njegovom djelu *Elementi* i predstavlja jedan od najstarijih algoritama koji je još i danas u uporabi. Za a i b cijele brojeve i $a \neq 0$, algoritam glasi:

$$\begin{aligned} b &= q_0 a + a_1,\ 0 < a_1 < a, \\ a &= q_1 a_1 + a_2,\ 0 < a_2 < a_1, \\ a_1 &= q_2 a_2 + a_3,\ 0 < a_3 < a_2, \\ &\vdots \\ a_{n-2} &= q_{n-1} a_{n-1} + a_n,\ 0 < a_n < a_{n-1}, \\ a_{n-1} &= q_n a_n. \end{aligned} \tag{1.1}$$

Uočimo da algoritam 'staje' kad neki od ostataka a_i bude jednak nuli.

Teorem 1.1.4. *Neka su a i b cijeli brojevi, $a \neq 0$, te $a_1, \ldots, a_n$ niz prirodnih brojeva dobiven Euklidovim algoritmom (1.1). Tada je*

$$(a, b) = a_n.$$

Dokaz. Prepostavimo da je $(a, b) = g$. Treba pokazati da je $g = a_n$. Budući da $g \mid a$ i $g \mid b$, iz prve jednakosti u (1.1) slijedi da $g \mid a_1$. Indukcijom dalje lako možemo ustanoviti da

$$g \mid a_n. \tag{1.2}$$

S druge strane, iz posljednje jednakosti u (1.1) slijedi da $a_n \mid a_{n-1}$, iz pretposljednje da $a_n \mid a_{n-2}$, te tako redom zaključujemo da $a_n \mid a$ i $a_n \mid b$. Stoga je a_n jedan zajednički djelitelj brojeva a i b pa

$$a_n \mid g \tag{1.3}$$

jer je g najveći zajednički djelitelj. Sada iz (1.2) i (1.3) te zbog činjenice da su a_n i g prirodni brojevi slijedi da je $g = a_n$. □

Teorem 1.1.5. *Neka su a i b cijeli brojevi i $g = (a, b)$. Tada postoje cijeli brojevi m i n takvi da je g linearna kombinacija brojeva a i b, to jest*

$$g = ma + nb.$$

Dokaz. Iz pretposljednje jednakosti u (1.1) slijedi da je g_n cjelobrojna linearna kombinacija brojeva a_{n-1} i a_{n-2}. Iz jednakosti prije te zaključili bi da je a_{n-1} cjelobrojna linearna kombinacija brojeva a_{n-2} i a_{n-1}, pa je to i a_n. Induktivno, zaključujemo da je a_n cjelobrojna linearna kombinacija brojeva a i b. □

Primjer 1.1.6. *Odredimo* $g = (891, 319)$ *i prikažimo ga kao cjelobrojnu linearnu kombinaciju brojeva* 891 *i* 319*.*

$$\begin{aligned} 891 &= 2 \cdot 319 + 253 \\ 319 &= 1 \cdot 253 + 66 \\ 253 &= 3 \cdot 66 + 55 \\ 66 &= 1 \cdot 55 + 11 \\ 55 &= 5 \cdot 11. \end{aligned}$$

Dakle, $g = 11$ *te*

$$\begin{aligned} 11 &= 66 - 1 \cdot 55 \\ &= 4 \cdot 66 - 253 \\ &= 4 \cdot 319 - 5 \cdot 253 \\ &= 14 \cdot 319 - 5 \cdot 891. \end{aligned}$$

Korolar 1.1.7. *Ako je* $(a, c) = (b, c) = 1$*, onda je* $(ab, c) = 1$*.*

Dokaz. Imamo

$$m_1 a + n_1 c = 1 \quad \text{i} \quad m_2 b + n_2 c = 1,$$

i množenjem dobivamo

$$Mab + Nc = 1,$$

gdje je $M = m_1 m_2$ i $N = m_1 n_2 a + m_2 n_1 b + n_1 n_2 c$. Dakle, $(ab, c) = 1$. □

Propozicija 1.1.8. *Ako su a,b i c cijeli brojevi takvi da je* $c \mid ab$ *i* $(c, a) = 1$*, onda* $c \mid b$*.*

Dokaz. Prema Teoremu1.3.3 slijedi

$$mc + na = 1.$$

Stoga, množenjem imamo

$$mcb + nab = b.$$

Budući da vrijedi $c \mid ab$, odnosno $ab = cd$, za neki cijeli broj d, slijedi

$$mcb + ncd = b,$$

te dobivamo

$$c(mb + nd) = b,$$

odnosno $c \mid b$. □

1.2 Kanonski prikaz prirodnog broja

Definicija 1.2.1. *Prirodan broj $p > 1$ zove se **prost** ako p nema niti jednog djelitelja d takvog da je $1 < d < p$. Ako prirodan broj veći od 1 nije prost, onda kažemo da je **složen**.*

Dakle, jedini pozitivni djelitelji prostog broja p su brojevi 1 i p. Broj 1 nije niti prost niti složen.

Teorem 1.2.2. *Svaki prirodan broj $n > 1$ može se prikazati kao produkt prostih brojeva s jednim ili više faktora.*

Dokaz. Teorem ćemo dokazati matematičkom indukcijom. Broj 2 je prost. Pretpostavimo da je $n > 2$ te da tvrdnja vrijedi za sve prirodne brojeve m takve da je $2 \leq m < n$. Želimo dokazati da se i n može prikazati kao produkt prostih faktora. Ako je n prost, nemamo što dokazivati. Neka je n složen broj, onda vrijedi $n = n_1 n_2$, gdje je $1 < n_1 < n$ i $1 < n_2 < n$. Po pretpostavci indukcije, n_1 i n_2 su produkti prostih brojeva pa stoga tvrdnja vrijedi i za broj n. □

Štoviše, dokazat ćemo da je takav rastav jedinstven do na poredak prostih faktora. Za to nam je potrebna sljedeća tehnička lema.

Lema 1.2.3. *Ako prost broj p dijeli produkt n cijelih brojeva, tada mora dijeliti barem jedan od tih brojeva.*

Dokaz. Dokaz provodimo indukcijom po n. Baza za $n = 2$, slijedi iz Propozicije 1.1.8. Zaista, ako $p \mid a_1 a_2$, onda $p \mid a_1$ ili $(p, a_1) = 1$ pa $p \mid a_2$. Prepostavimo da tvrdnja korolara vrijedi za $n - 1 \geq 2$ i pokažimo da vrijedi za n. Dakle, neka

$$p \mid (a_1 a_2 \cdots a_{n-1}) a_n.$$

Ako $p \mid a_1 a_2 \cdots a_{n-1}$, onda prema pretpostavci indukcije $p \mid a_i$ za neki $i \in \{1, 2, \ldots, n-1\}$. Ako $p \nmid a_1 a_2 \cdots a_{n-1}$, odnosno $(p, a_1 a_2 \cdots a_{n-1}) = 1$ jer je p prost, onda prema Propoziciji 1.1.8 slijedi da $p \mod a_n$. □

Teorem 1.2.4 (Osnovni teorem aritmetike)**.** *Svaki cijeli broj $N > 1$ ima jedinstvenu faktorizaciju na proste faktore do na poredak prostih faktora.*

Dokaz. Pretpostavimo da N ima dvije različite faktorizacije na proste faktore. Dijeleći s prostim brojevima koji su zajednički objema reprezentacijama, dobivamo jednakost oblika

$$p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m,$$

gdje su p_i, q_j prosti brojevi takvi da je $p_i \neq q_j$ za sve i, j. Međutim, to je nemoguće jer iz $p_1 \mid q_1 q_2 \cdots q_m$, po Lemi 1.2.3 slijedi da p_1 dijeli barem jedan od q_j. No, to znači da je $p_1 = q_j$, što je kontradikcija. □

Iz teorema 1.2.2 i 1.2.4 slijedi da svaki prirodan broj n možemo prikazati u obliku

$$n = p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m},$$

gdje su $p_1, p_2, \ldots, p_m$ različiti prosti brojevi, a $a_1, a_2, \ldots, a_m$ prirodni brojevi. Ovakav prikaz broja n naziva se *kanonski rastav* broja n na proste faktore. Prikaz je jedinstven uz pretpostavku da je $p_1 < p_2 < \cdots < p_m$.

Korolar 1.2.5. *Jedini pozitivni djelitelji broja*

$$N = p_1^{a_1} \cdots p_n^{a_n} \tag{1.4}$$

su brojevi oblika

$$p_1^{c_1} p_2^{c_2} \cdots p_n^{c_n} \tag{1.5}$$

gdje je

$$0 \leq c_i \leq a_i,\ i = 1, \ldots, n.$$

Dokaz. Ako je $d = p_1^{c_1} p_2^{c_2} \cdots p_n^{c_n}$, gdje je $0 \leq c_i \leq a_i$. Tada za $b_i = a_i - c_i \geq 0$ i $m = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$ vrijedi $N = d \cdot m$ pa $d \mid N$.

S druge strane, pretpostavimo da $d \mid N$. Tada ako potencija prostog broja dijeli d onda dijeli i N, pa je d oblika (1.5). □

1.3 Savršeni brojevi

Mnogi teoremi iz teorije brojeva bave se problemima koje su otkrili stari Grci. Jedan od njih je i problem savršenih brojeva. U ovom poglavlju navest ćemo neke koncepte, teoreme i još uvijek otvorena pitanja vezana uz savršene brojeve.

Nije poznato kada su otkriveni savršeni brojevi niti tko ih je otkrio, ali najraniji matematički zapis o savršenim brojevima pojavio se u Euklidovom djelu *Elementi* koje je napisano oko 300. g. pr. Kr. Grčki matematičar Euklid je definirao savršen broj kao broj koji je jednak zbroju svih svojih pozitivnih djelitelja različitih od njega samog.

Primjer savršenog broja, a ujedno i najmanji savršen broj je broj 6. Pozitivni djelitelji broja 6 različiti od njega samog su 1, 2 i 3 i vrijedi $1 + 2 + 3 = 6$. Stari Grci poznavali su prva četiri savršena broja:

$$\begin{aligned} P_1 &= 6, \\ P_2 &= 28, \\ P_3 &= 496, \\ P_4 &= 8\,128. \end{aligned}$$

U srednjem vijeku smatrano je da P_n, n-ti savršen broj, ima točno n znamenki te da savršeni brojevi naizmjeničko završavaju sa znamenkama 6 i 8. Obje tvrdnje pokazale su se krivima. Štoviše, ne postoji savršen broj sa 5 znamenki, a peti savršen broj je

$$P_5 = 33\,550\,336.$$

Budući da završava znamenkom 6, sljedeći savršen broj trebao bi završavati znamenkom 8, što također nije točno jer je

$$P_6 = 8\,589\,869\,056.$$

Još nije poznato koliko ima savršenih brojeva, odnosno ima li ih konačano ili beskonačno.

Otvoren problem 1. *Koliko ima savršenih brojeva?*

Pretpostavlja se da postoji beskonačno mnogo savršenih brojeva jer se iz godine u godinu pronalazi sve veći savršen broj. No, zanimljivo je da su do sada otkriveni isključivo parni savršeni brojevi. Nije poznato postoji li neparan savršen broj.

Otvoren problem 2. *Postoji li neparan savršen broj?*

Do danas su, pomoću naprednih računalnih programa, ispitani brojevi do 10^{1500}, ali nije pronađen niti jedan neparan savršen broj. Pretpostavlja se da takvih brojeva niti nema.

U sljedećoj tablici vidimo prikaz prva četiri savršena broja u binarnom zapisu.

	Decimalni zapis	Binarni zapis
P_1	6	110
P_2	28	11100
P_3	496	111110000
P_4	8 128	1111111000000

Vidimo da za sva ova četiri broja vrijedi da se njihov binarni zapis sastoji od niza od n uzastopnih jedinica i $n-1$ uzastopne nule. Dakle,

$$(\underbrace{11\cdots1}_{n}\underbrace{00\cdots0}_{n-1})_2 = 1\cdot 2^{n-1} + 1\cdot 2^n + \cdots + 1\cdot 2^{2n-2} = 2^{n-1}(1+2+\cdots+2^{n-1}) = 2^{n-1}(2^n-1).$$

Stoga se naša prva četiri savršena broja faktoriziraju na sljedeći način:

$$\begin{aligned} P_1 &= 2^1(2^2-1) = 2\cdot 3, \\ P_2 &= 2^2(2^3-1) = 4\cdot 7, \\ P_3 &= 2^4(2^5-1) = 16\cdot 31, \\ P_4 &= 2^6(2^7-1) = 64\cdot 127. \end{aligned}$$

Za ove brojeve još vrijedi i da je neparni faktor $2^n - 1$ prost broj, odnosno broj koji nema djelitelja većeg od 1 i manjeg od samog sebe. Tu je spoznaju imao još i Euklid pa se u IX. knjizi *Elemenata* može naći sljedeća tvrdnja.

Propozicija 1.3.1. *Ako je $2^n - 1$ prost broj, onda je broj oblika $2^{n-1}(2^n - 1)$ savršen.*

Za dokaz ćemo koristi sljedeću pomoćnu tvrdnju.

Lema 1.3.2 (Cataldi-Fermat)**.** *Ako je $2^n - 1$ prost broj, onda je n prost broj.*

Dokaz. Znamo da je

$$a^n - 1 = (a - 1)(a^{n-1} + a^{n-2} + \cdots + a + 1) \tag{1.6}$$

Ako n nije prost broj, onda ga možemo zapisati u obliku $n = rs$, gdje je $r > 1$ i $s > 1$. Pa slijedi

$$2^n - 1 = 2^{rs} - 1 = (2^r)^s - 1.$$

Uvrštavanjem u (1.6) slijedi

$$(2^r)^s - 1 = (2^r - 1)(2^{r(s-1)} + 2^{r(s-2)} + \cdots + 2^r + 1).$$

Slijedi da je $2^n - 1$ djeljiv sa $2^r - 1$ koji je veći od 1 jer je $r > 1$, što je u kontradikciji s pretpostavkom da je $2^n - 1$ prost broj. □

Obrat prethodne tvrdnja općenito ne vrijedi. Na primjer, za prost broj $n = 11$ slijedi da je $2^{11} - 1 = 2047 = 23 \cdot 89$ složen broj.

Dokaz Propozicije1.3.1. Zbog Leme 2.2 naš broj je oblika $2^{p-1}(2^p - 1)$ za neki prost broj p takav da je i $2^p - 1$ prost broj. Svi njegovi djelitelji su

$$1, 2, 2^2, \ldots, 2^{p-1}$$

i

$$2^p - 1, 2(2^p - 1), 2^2(2^p - 1), \ldots, 2^{p-2}(2^p - 1).$$

Zbrajanjem svih djelitelja manjih od $2^{p-1}(2^p - 1)$ dobivamo

$$\underbrace{\sum_{i=1}^{p-1} 2^i}_{=2^p-1} + (2^p - 1) \underbrace{\sum_{i=1}^{p-2} 2^i}_{=2^{p-1}-1} = (2^p - 1)(1 + 2^{p-1} - 1) = 2^{p-1}(2^p - 1).$$

□

No, vrijedi i obrat Propozicije 1.3.1 kojeg je oko 2 000 godina nakon Euklida iskazao i dokazao švicarski matematičar Leonhard Euler (1707.-1783.).

Teorem 1.3.3. *Paran broj je savršen ako i samo ako je oblika* $2^{n-1}(2^n-1)$ *pri čemu je* 2^n-1 *prost broj.*

Dokaz. Dovoljnost slijedi iz Propozicije 1.3.1.

Neka je N paran savršen broj. Zapišimo ga u obliku

$$N = 2^{n-1}F,$$

gdje je F neparan broj. Neka je S suma svih pozitivinih djelitelja broja F. Pozitivni djelitelji broja N uključuju sve neparne djelitelje broja F te sve parne djelitelje oblika $2^j f$, gdje je $j \in \{1, \ldots, n-1\}$ i $f \mid F$. Budući da je N savršen, slijedi

$$N = 2^{n-1}F = (1 + 2 + \cdots + 2^{n-1})S - N$$

ili

$$2N = 2^nF = (2^n - 1)S.$$

Prema tome,

$$S = \frac{2N}{2^n-1} = \frac{2^nF}{2^n-1} = \frac{2^nF - F + F}{2^n-1} = F + \frac{F}{2^n-1}.$$

Kako su S i F cijeli brojevi i broj $\dfrac{F}{2^n-1}$ mora biti cijeli broj. Stoga je $F = k(2^n-1)$ za neki prirodan broj k. No, ako je $k > 1$ onda je i k djelitelj od F pa je $S = F + k > F + 1 + k$, što nije moguće. Stoga je nužno

$$F = 2^n - 1.$$

Uz to zaključujemo i da je F nužno prost jer je zbroj njegovih djelitelja jednak $F + 1$. □

Teorem 1.3.4. *Svaki paran savršen broj završava znamenkom 6 ili 8.*

Dokaz. Neka je N paran savršen broj. Tada prema Teoremu 1.3.3 postoji p prost takav da je $2^p - 1$ prost i N oblika

$$N = 2^{p-1}(2^p - 1). \tag{1.7}$$

Svaki prost broj veći od 2 je oblika $4m + 1$ ili $4m + 3$, u suprotnom bi bio djeljiv brojem 2. Uvrštavanjem $p = 4m + 1$ u (1.7) slijedi

$$N = 2^{4m+1-1}(2^{4m+1} - 1) = 2^{4m}(2^{4m+1} - 1) = 16^m(16^m \cdot 2 - 1),$$

gdje je $m \geq 1$. Očito je da broj oblika 16^m uvijek završava znamenkom 6, dok broj oblika $2 \cdot 16^m$ uvijek završava znamenkom 2 pa broj oblika $2 \cdot 16^m - 1$ uvijek završava znamenkom 1. Iz čega slijedi da paran savršen broj N završava znamenkom 6.

Analognim postupkom za $p = 4m + 3$ slijedi

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

Broj oblika $4 \cdot 16^m$ uvijek završava znamenkom 4, dok broj oblika $16^m \cdot 8$ uvijek završava znamenkom 8, pa broj oblika $16^m \cdot 8 - 1$ uvijek završava znamenkom 7. Iz čega slijedi da paran savršen broj N završava znamenkom 8.

Konačno za $p = 2$ imamo $N = P_1 = 6$, pa smo pokazali tvrdnju. □

Poglavlje 2

Prosti brojevi

2.1 O oblicima prostih brojeva

U prvom poglavlju ukazali smo na važnost prostih brojeva - oni su poput atoma od kojih je građena molekula. Konkretno, vidjeli smo da svaki prirodan broj veći od 1 ima jedinstvenu faktorizaciju na proste faktore do na poredak prostih faktora (Osnovni teorem aritmetike 1.2.4). Nadalje, važna je činjenica koja je još bila poznata starim Grcima da prostih brojeva ima beskočno mnogo. To je Euklid znao dokazati oko 300. g. pr. Kr. te se dokaz može naći u njegovom djelu *Elementi* i koristi se još i danas.

Teorem 2.1.1 (Euklid)**.** *Skup svih prostih brojeva je beskonačan.*

Dokaz. Pretpostavimo suprotno, tj. da je skup svih prostih brojeva konačan. Neka su $p_1, p_2, \ldots, p_n$ svi prosti brojevi. Tada broj

$$N = 1 + p_1 p_2 \cdots p_n.$$

nije djeljiv niti s jednim od brojeva $p_1, p_2, \ldots, p_n$. Prema Teoremu 1.2.2 postoji prost broj q takav da $q \mid N$ i $q \neq p_i$, $i = 1, \ldots, n$. Kontradikcija! □

Svi prosti brojevi veći od 2 su neparni pa s obzirom na to daju pri dijeljenju s 4 ostatke 1 i 3. Prirodno se pitati ima li prostih brojeva p oblika $p = 4k + 1$, odnosno $p = 4k + 3$ beskonačno mnogo. U slučaju oblika $p = 4k + 3$, to možemo jednostavno utvrditi koristeći Euklidov dokaz Teorema 2.1.1.

Propozicija 2.1.2. *Prostih brojeva oblika* $4k + 3$ *ima beskonačno mnogo.*

Dokaz. Pretpostavimo suprotno, tj. da je skup svih prostih brojeva oblika $4k + 3$ konačan. Neka su $p_1, p_2, \ldots, p_n$ svi prosti brojevi oblika $4k + 3$. Promotrimo broj

$$N = p_1 p_2 \cdots p_n - 1.$$

Očito vrijedi $N \equiv -1 \equiv 3 \pmod 4$ i ako prost broj q dijeli N, onda je $q \neq p_i$, $i = 1, \ldots, n$. Ako bi svi njegovi prosti faktori bili oblika $4k + 1$, onda bi bilo

$$N = q_1 q_2 \cdots q_k \equiv 1 \cdot 1 \cdots 1 = 1 \pmod 4,$$

što očito nije. Prema tome, N ima barem jedan prosti faktor q oblika $4k + 3$ koji nije među prostim brojevima $p_1, p_2, \ldots, p_n$ pa smo dobili kontradikciju. □

No, pokazati da prostih brojeva p oblika $p = 4k+1$ ima beskonačno mnogo nije sasvim jednostavno. Za to nam je potreban Wilsonov teorem, odnosno njegova posljedica.

Teorem 2.1.3 (Wilson)**.** *Ako je p prost broj, onda je $(p-1)! \equiv -1 \pmod p$.*

Lema 2.1.4. *Neka je p prost broj. Tada kongruencija $x^2 \equiv -1 \pmod p$ ima rješenja ako i samo ako je $p = 2$ ili $p \equiv 1 \pmod 4$.*

Prethodna lema dobiva se direktnom primjenom Wilsonovog teorema 2.1.3 i Malog Fermatovog teorema 2.2.1 (kojeg ćemo iskazati i dokazati u sljedećem odjeljku).

Propozicija 2.1.5. *Prostih brojeva oblika $4k + 1$ ima beskonačno mnogo.*

Dokaz. Neka su $p_1, p_2, \ldots, p_n$ svi prosti brojevi oblika $4k + 1$. Promotrimo broj

$$N = (2p_1 p_2 \cdots p_n)^2 + 1.$$

Neka je q neki prosti faktor od N. Tada kongruencija $x^2 \equiv -1 \pmod q$ ima rješenje $x = 2p_1 p_2 \cdots p_n$, pa p mora biti oblika $4k + 1$. Kako je $q \neq p_i$, $i = 1, 2, \ldots, n$, dobivamo kontradikciju. □

Općenito može se pokazati da postoji beskonačno mnogo prostih brojeva oblika $ak + b$, za prirodne brojeve a i b koji su relativno prosti. Ta je činjenica poznata kao Diricletov teorem i obično se iskazuje na sljedeći način:

Teorem 2.1.6 (Diriclet)**.** *Neka su $a, d \in \mathbb{N}$ i $(a, d) = 1$. Postoji beskonačno mnogo prostih brojeva u aritmetičkom nizu $a, a + d, a + 2d, a + 3d, \ldots$.*

Propozicije 2.1.2 i 2.1.5 su zapravo posljedice Diricletovog teorema.

U slučaju da prost broj p želimo prikazati nekom kvadratnom formom, makar i sasvim konkretnom kao n^2+1, stvari postaju jako komplicirane i dobivamo niz nedokazanih slutnji.

Otvoren problem 3. *Postoji beskonačno mnogo brojeva n takvih da je $n^2 - 2$ prost broj čije su sve znamenke prosti brojevi.*

Primjeri prostih brojeva oblika $n^2 - 2$ čije su sve znamenke prosti brojevi su $2, 7, 23$, $223, 727$ a dobiveni su za $n = 2, 3, 5, 15, 27$. To otvoreno pitanje je očito povezano sa sljedećim.

Otvoren problem 4. *Postoji beskonačno mnogo prostih brojeva oblika* $n^2 - 2$.

Iako je poznato više od 15 000 takvih prostih brojeva nije poznato ima li beskonačno mnogo. Neki od primjera mogu se dobiti za $n = 2, 3, 5, 7, 9, \ldots, 179\,965, \ldots$, ali dokaz se i dalje čeka.

Otvoren problem 5. *Postoji beskonačno mnogo prostih brojeva oblika* $n^2 + 1$.

Brojevi tog oblika su prosti za $n = 1, 2, 4, 6, 10, 14, 16, 20, 24, 26, 36...$, ali još uvijek nije poznato ima li ih beskonačno mnogo.

Postavljene su i hipoteze o broju prostih brojeva oblika $n^2 + a$ koji su manji od nekog zadanog broja. Uvodimo oznaku $P_a(N)$ za broj prostih brojeva oblika $n^2 + a$ za $1 \leq n \leq N$.

Otvoren problem 6. *Neka je* $P_{-2}(N)$ *broj prostih brojeva oblika* $n^2 - 2$ *za* $1 \leq n \leq N$. *Tada je*

$$P_{-2}(N) \sim 0.9259272 \int_2^N \frac{dn}{\log n}.$$

Otvoren problem 7. *Neka je* $P_1(N)$ *broj prostih brojeva oblika* $n^2 + 1$ *za* $1 \leq n \leq N$. *Tada je*

$$P_1(N) \sim 0.6864067 \int_2^N \frac{dn}{\log n}.$$

Ako su prethodne hipoteze točne tada su češći prosti brojevi oblika $n^2 - 2$ nego prostih brojeva oblika $n^2 + 1$.

2.2 Fermatovi brojevi

Francuski pravnik i matematičar Piere de Fermat (1601.-1665.) poznat je po značajnim doprinosima u mnogim područjima matematike npr. u području infinitezimalnog računa, analitičke geometrije, vjerojatnosti te teorije brojeva. Istaknut ćemo dvije važne tvrdnje koje su poznate pod nazivom Veliki Fermatov teorem i Mali Fermatov teorem.

Teorem 2.2.1 (Mali Fermatov teorem)**.** *Neka je* p *prost broj i* $a \in \mathbb{N}$ *tako da vrijedi* $p \nmid a$. *Tada vrijedi*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Dokaz. Pretpostavimo da u nizu od $p-1$ pozitivnih višekratnika broja a:

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

postoje višekratnici ra i sa koji pri dijeljenju s p daju isti ostatak, tj. $ra = sa \pmod{p}$. Kako su p i a relativno prosti slijedi $r \equiv s \pmod{p}$, što nije moguće jer su r i s brojevi iz reduciranog sustava ostataka modulo p (tj. međusobno su nekongruentni modulo p) i međusobno različiti. Dakle,

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

Kako je $((p-1)!, p) = 1$, nakon dijeljenja prethodne kongruencije s $(p-1)!$ dobivamo

$$a^{p-1} \equiv 1 \pmod{p}.$$

□

Teorem 2.2.2 (Veliki Fermatov teorem)**.** *Ne postoje pozitivni cijeli brojevi a, b i c takvi da je*

$$a^n + b^n = c^n,$$

gdje je n prirodan broj veći od 2.

Za prethodni teorem, poznat još i pod nazivom Posljednji Fermatov teorem, sigurno nećemo dati dokaz. Naime, on je dugo vremena bio otvoreni problem u teoriji brojeva te je napokon dokazan nakon više od 350 godina. Fermat ga je zapisao na marginama knjige uz napomenu da ima sjajan dokaz te tvrdnje, ali da je margina za njega preuska. Iako je tvrdnja bila iznimno lako shvatljiva, zanimljivo je da je bila gotovo nedokaziva. Euler je uspio pokazati da tvrdnja vrijedi za $n = 3$ i $n = 4$, no preostalo je još uvijek beskonačno mnogo vrijednosti broja n za koje Euler nije znao odgovor, kao ni ostali matematičari kroz dugi niz godina. Kroz povijest, matematičari su uspjeli dokazati tvrdnju za $n = 3, 4, 5, 6, 7$. Nakon mnogih pokušaja priča se konačno završila 1995. godine, kada je matematičar Andrew Wiles, nakon mnogo godina rada i na više od 100 stranica, napokon prikazao cijeli dokaz tvrdnje.

Fermat je, međuostalog, proučavao brojeve oblika

$$F_n = 2^{2^n} + 1$$

za cijele pozitivne brojeve $n \geq 0$ koji se njemu u čast zovu *Fermatovi brojevi*. Postavio je i hipotezu da su svi brojevi oblika F_n prosti. Do svoje slutnje je došao provjerivši brojeve oblika F_n za $n = 0, 1, 2, 3, 4$. Konkretno, dobio je sljedeće proste brojeve:

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65\,537.$$

No, 1732. godine Euler je pokazao da Fermatova hipoteza nije točna i da je

$$F_5 = 2^{32} + 1 = 4\,294\,967\,297$$

djeljiv s 641, dakle nije prost broj. Zanimljivo je da je do danas poznato samo pet Fermatovih prostih brojeva, odnosno točno onih pet koje je otkrio sam Fermat. Stoga se možemo pitati postoji li beskonačno ili konačno mnogo Fermatovih prostih brojeva. Zapravo, samo na temelju saznanja da je pet Fermatovih prostih bojeva i da se za njih 292 zna da su složeni (prema aktulnim podatcima na internetskoj stranici *Proth Search Page* u ožujku 2017.) moguća su tri ishoda:

- prostih Fermatovih brojeva ima beskonačno mnogo, a složenih Fermatovih brojeva konačno mnogo;
- složenih Fermatovih brojeva ima beskonačno mnogo, a prostih Fermatovih brojeva konačno mnogo;
- i prostih i složenih Fermatovih brojeva ima beskonačno mnogo.

Ipak mnoga istraživanja idu u prilog sljedećoj hipotezi:

Otvoren problem 8. *Postoji li samo pet Fermatovih prostih brojeva? Odnosno, jesu li svi Fermatovi brojevi F_n za $n > 4$ složeni?*

U prilog pozitivnog odgovora na prethodno pitanje, tj. u prilog tvrdnji da postoji samo konačno mnogo Fermatovih prostih brojeva ide i sljedeće heurističko promišljanje. Budući da je broj prostih brojeva koji su manji ili jednaki broju n približno jednak $\frac{n}{\ln n}$, vjerojatnost da je proizvoljno odabrani broj n prost broj je $\frac{1}{\log n}$. Stoga je za broj $2^{2^n} + 1$ vjerojatnost je manja ili jednaka od $\frac{1}{\ln(2^{2^n} + 1)}$. Stoga je očekivani broj Fermatovih prostih brojeva manji ili jednak od

$$\sum_{n=0}^{\infty} \frac{1}{\ln(2^{2^n} + 1)} = \frac{1}{\ln 2} \sum_{n=0}^{\infty} \frac{1}{\log_2(2^{2^n} + 1)} < \frac{1}{\ln 2} \sum_{n=0}^{\infty} \frac{1}{\log_2 2^n} = \frac{2}{\ln 2},$$

što je konačan broj (< 7). No, prethodnu argumentaciju nipošto ne smijemo smatrati rigoroznim matematičkim dokazom. Za početak ovaj "dokaz" podrazumijeva da se prosti Fermatovi brojevi pojavljuju nasumično, što se ne može sa sigurnošću tvrditi. Moramo napomenuti da se koristeći uvjetnom vjerojatnošću (u kojoj pretpostavljamo da su prosti faktori Fermatovog broja kongruentni 1 modulo $2^n + 1$, gdje je n Fermatov broj) može dobiti da očekivani broj prostih Fermatovih brojeva teži u beskonačno.

Općenito možemo reći da se o Fermatovim brojevim još uvijek vrlo malo zna. Iako su nam na prvi pogled zanimljivi Fermatovi prosti brojevi, složeni Fermatovi brojevi otvaraju drugo pitanje. Naime, ako je Fermatov broj složen, zanima nas njegova faktorizacija ili barem kako izgledaju njegovi djelitelji. Budući da Fermatovi brojevi rastu jako brzo, faktoriziranje ili utvrđivanje je li Fermatov broj prost, nije nimalo lako i predstavlja veliki izazov čak i za današnja superračunala. Potpuna faktorizacija Fermatovih brojeva bila je izazov za matematičare još od Eulerovog doba. Samo prvih dvanaest Fermatovih brojeva (od F_0 do F_{11}) su potpuno faktorizirani. Nažalost, ne postoji jedinstvena metoda za faktorizaciju Fermatovih brojeva, odnosno metoda za faktorizaciju broja F_n možda nije najprikladnija za faktorizaciju broja F_{n+1}. Za utvrđivanje je li Fermatov broj prost koriste se neki od sljedećih *testova prostosti*.

Teorem 2.2.3 (Lucasov test)**.** *Neka je N prirodan broj. Ako postoji prirodan broj a, $1 < a < N$ takav da je*

$$a^{n-1} \equiv 1 \pmod{N}$$

i

$$a^{\frac{N-1}{p}} \not\equiv 1$$

za sve proste brojeve $p \mid N-1$, onda je N prost broj. Ako takav a ne postoji onda je $N = 1$ ili je složen.

Teorem 2.2.4 (Pepinov test)**.** *Za $n \geq 2$, Fermatov broj F_n je prost ako i samo ako je*

$$3^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}.$$

Međutim, pomoću testova prostosti ne možemo odrediti niti jedan netrivijalni faktor danog broja. Najefikasniji poznati algoritam za faktorizaciju je, kao i za utvrđivanje prostosti nekog broja, metoda faktorizacije pomoću *eliptičke krivulje*. Nešto je ipak poznato o djeliteljima Fermatovih brojeva.

Teorem 2.2.5 (Euler)**.** *Ako je p prost broj takav da $p \mid F_n$, onda je p oblika*

$$p = k2^{n+1} + 1,$$

gdje je k pozitivan cijeli broj.

Za dokaz prethodnog teorema potrebne su nam sljedeća definicija i propozicija.

Definicija 2.2.6. *Neka su a i n relativno prosti brojevi. Najmanji prirodan 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.*

Uz pojam reda nekog broja usko je vezana važna funkcija u teoriji brojeva, tzv. *Eulerova funkcija*.

Definicija 2.2.7. *Za prirodan broj n s $\varphi(n)$ označavamo broj brojeva u nizu $1, 2 \ldots, n$ koji su relativno prosti s n. Tako definirana funkcija $\varphi : \mathbb{N} \to \mathbb{N}$ naziva se* ***Eulerova funkcija****.*

Pokazuje se da je Eulerova funkcija *multiplikativna*, tj. $\varphi(mn) = \varphi(m)\varphi(n)$ za sve $m, n \in \mathbb{N}$ takve da je $(m, n) = 1$. Nadalje, vrijedi sljedeće važno svojstvo.

Teorem 2.2.8 (Euler)**.** *Neka je $a \in \mathbb{Z}$ i $n \in \mathbb{N}$. Ako je $(a, n) = 1$, onda je*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Prethodni teorem predstavlja poopćenje Malog Fermatovog teorema 2.2.1.

Propozicija 2.2.9. *Neka je d red od a modulo n. Tada za prirodni broj k vrijedi $a^k \equiv 1 \pmod{n}$ ako i samo ako $d \mid k$. Posebno, $d \mid \varphi(n)$.*

Dokaz. 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 sa d, pa dobivamo $k = q \cdot d + r$, gdje je $0 \leq r < d$. Imamo

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

pa zbog minimalnosti od d slijedi da je $r = 0$, odnosno da $d \mid k$. Zadnja tvrdnja slijedi direktno iz Eulerovog teorema 2.2.8. □

Dokaz Teorema 2.2.5. Neka je p prosti djelitelj Fermatovog broja, pa vrijedi $2^{2^n} + 1 \equiv 0 \pmod{p}$. Iz toga slijedi $2^{2^n} \equiv -1 \pmod{p}$ i $2^{2^{n+1}} \equiv 1 \pmod{p}$, pa slijedi da 2 pripada eksponentu 2^{n+1} modulo p. Budući da je broj brojeva koji su relativno prosti s p jednak $p - 1$, slijedi da $2^{n+1} \mid p - 1$. Odnosno, postoji $k \in \mathbb{N}$ takav da je $p = k \cdot 2^{n+1} + 1$.

□

Francuski matematičar E. A. Lucas pokazao je da je broj k u Teoremu 2.2.5 uvijek paran broj, odnosno vrijedi:

Teorem 2.2.10 (Lucas)**.** *Ako je $n > 1$ i prost broj p dijeli F_n, onda je p oblika*

$$p = k2^{n+2} + 1,$$

gdje je k paran prirodan broj.

Do sada je poznato šest prostih faktora za Fermatov broj F_{12}, četiri prosta faktora za Fermatov broj F_{13}, tri prosta faktora za Fermatove brojeve F_{15}, F_{19}, F_{25}, F_{52} i F_{287}, dva prosta faktora za Fermatove brojeve F_{16}, F_{17}, F_{18}, F_{27}, F_{30}, F_{36}, F_{38}, F_{39}, F_{42}, F_{77}, F_{147}, F_{150}, F_{284}, F_{416} i F_{417}, samo jedan prosti faktor za Fermatove brojeve F_{14}, F_{21}, F_{22}, F_{23}, F_{26}, F_{28}, F_{29}, F_{31}, F_{32}, F_{37}, F_{43} i 250 vrijednosti od n za $43 < m \leq 3\ 329\ 780$. Fermatovi brojevi koji su složeni, a kojima nisu poznati prosti faktori su brojevi F_{20} i F_{24}. Najveći poznati složeni Fermatov broj je $F_{3\,329\,780}$. S obzirom na to možemo postaviti i sljedeća pitanja:

Otvoren problem 9. *Koji su preostali prosti faktori poznatih složenih Fermatovih brojeva (F_{12}, F_{13}, F_{14}, F_{15},...)?*

Otvoren problem 10. *Određivanje barem jednog prostog faktora Fermatovih brojeva F_{20} i F_{24}?*

Nema poznatih Fermatovih brojeva koji su djeljivi s kvadratom nekog prostog broja. Smatra se da takvi Fermatovi brojevi niti ne postoje. Međutim, ta tvrdnja još nije dokazana.

Otvoren problem 11. *Postoji li Fermatov broj koji je djeljiv s kvadratom prostog broja?*

Njemački matematičar C. F. Gauss našao je zanimljivu vezu između euklidske konstrukcije pravilnih n - terokuta i Fermatovih prostih brojeva. Pokazao je da se pravilni n - terokut može konstruirati ako je broj stranica $n = 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, ...$ Odnosno, dokazao je da postoji euklidska konstrukcija pravilnog n - terokuta ako i samo ako je

$$n = 2^i p_{n_1} p_{n_2} ... p_{n_j}, \tag{2.1}$$

za $n \geq 3, i \geq 0, j \geq 0$ gdje su p_{n_1}, p_{n_2}, ..., p_{n_j} različiti Fermatovi prosti brojevi. Specijalno, svi 2^n-poligoni, za $n \geq 2$ mogu konstruirati. Nadalje, budući da je poznato da je 5 Fermatih prostih brojeva, iz (2.1) slijedi da se može konstruirati 31 n-terokut kojem je broj stranica neparan, tj. $n = 2k + 1$. To su poligoni sa sljedećim brojem stranica: 3, 5, 15, 17, 51, 85, 255, 257, 771, 1285, 3855, 4369, 13107, 21845, 65535, 65537, 196611, 327685, 983055, 1114129, 3342387, 5570645, 16711935, 16843009, 50529027, 84215045, 252645135, 286331153, 858993459, 1431655765. Kako je nepoznat broj Fermatih prostih brojeva, prirodno se nameće i sljedeće otvoreno pitanje.

Otvoren problem 12. *Je li broj pravilnih poligona s neparnim brojem stranica za koje postoji euklidska konstrukcija konačan?*

2.3 Mersenneovi brojevi

Francuski svećenik, teolog, matematičar i teoretičar glazbe, Marin Mersenne (1588.-1648.) u matematici je posebno značajan zbog dopisivanja s mnogim matematičarima svog doba, čime je omogućena razmjena ideja u doba u kojem nisu postojali brzi načini komunikacije. U matematici se bavio prostim i složenim brojevima te mu je cilj bio otkriti opću formulu za proste brojeve. Promatrao je brojeve oblika

$$M_n = 2^n - 1,$$

gdje je n prirodan broj. Ti se brojevi, njemu u čast, nazivaju *Mersenneovi brojevi*. Prvih nekoliko Mersenneovih brojeva su:

$$M_1 = 1, \quad M_2 = 3, \quad M_3 = 7, \quad M_4 = 15, \quad M_5 = 31, \ldots$$

Za sve složene brojeve n i pripadni Mersenneov broj je složen broj. U Lemi 2.2 smo pokazali da ako je Mersenneov broj $M_n = 2^n - 1$ prost broj, onda je n prost. Obrat te tvrdnje ne vrijedi što znači da za proste brojeve n pripadni Mersenneov broj može, ali i ne mora biti prost broj. Na primjer,

$$M_3 = 2^3 - 1 = 7,$$

je prost, dok je

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

složen. Mersenneovi brojevi koji su prosti nazivaju se *Mersenneovi prosti brojevi*.

Mersenne je smatrao da su za $n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$ pripadni brojevi M_n prosti, a svi ostali, za prirodne brojeve n manje od 257, složeni. Ta tvrdnja je poznata pod nazivom *Originalna* ili *Stara Mersenneova hipoteza*. Kasnije su provjere pokazale kako je Mersenne pogriješio. Brojevi M_{67} i M_{257} nisu prosti, a prosti brojevi koji nedostaju su M_{61}, M_{89} i M_{107}.

Mersennovi prosti brojevi su veoma rijetki. Do danas je nađeno samo 49 Mersenneovih prostih brojeva, a najveći među njima je $M_{74\,207\,281}$ koji ima 22 338 618 znamenki i ujedno je najveći dosad poznati prosti broj. Pretpostavlja se da Mersenneovih prostih brojeva ima beskonačno mnogo.

Otvoren problem 13. *Postoji li beskonačno mnogo Mersenneovih prostih brojeva?*

Kako se Mersenneova hipoteza pokazala netočnom, matematičari Lenstra, Pomerance i Wagstaff postavili su hipotezu da postoji beskonačno mnogo Mersenneovih prostih brojeva. U prilog toj hipotezi ide sljedeće razmatranje. Vjerojatnost da je Mersenneov broj prost je

$$\frac{1}{\ln(2^p - 1)} \approx \frac{1}{p \ln 2}.$$

Stoga je očekivani broj Mersenneovih prostih brojeva približno jednak

$$\frac{1}{\ln 2} \sum_{p-\text{prost}} \frac{1}{p}$$

Budući da je red $\sum_{p-\text{prost}} \frac{1}{p}$ divergentan, ovaj račun sugerira da je broj Mersenneovih prostih brojeva beskonačan, no to nikako nije strogi matematički dokaz.

Preciznije Lenstra, Pomerance i Wagstaffova 1983. godine postavljaju slutnju o približnom broju Mersenneovih prostih brojeva manjih ili jednakih od neke zadane vrijednosti.

Otvoren problem 14. *Broj Mersenneovih prostih brojeva manjih ili jednakih od x je asimptotski jednak*

$$\frac{e^{\gamma} \cdot \ln \ln x}{\ln 2},$$

gdje je γ Euler - Mascheronijeva konstanta.

Konstanta γ koja se u nekoj literaturi naziva samo Eulerova konstanta ili samo Mascheronijeva konstanta definira se kao limes niza

$$\lim_{n\to\infty}(1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots + \frac{1}{n} - \ln n).$$

Njena približna vrijednost je $\gamma \approx 0.5772156649$. Zanimljivo je da i uz nju vežemo niz otvorenih pitanja. Na primjer, još uvijek nije poznato je li γ racionalan ili iracionalan broj premda je matematičarima poznato preko milijun znamenaka u njenom decimalnom zapisu.

Napomenimo još da kažemo da su funkcije f i g *asimptotski* jednake, i pišemo $f \sim g$, ako je

$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1.$$

Lenstra - Pomerance - Wagstaffova hipoteza 14 može se formulirati na sljedeći način:

Otvoren problem 15. *Broj Mersenneovih prostih brojeva M_p takvih da je p manji ili jednak od y je asimptotski jednak*

$$\frac{e^{\gamma} \cdot \ln y}{\ln 2}.$$

Ako bi prethodna slutnja bila točna onda bi Mersenneovih prostih brojeva M_p sa zadanim brojem znamenaka prostog broja p trebalo biti približno

$$\frac{e^\gamma \cdot \ln 10}{\ln 2} \approx 5.92.$$

Zaista, broj Mersenneovih prostih brojeva M_p takvih da p ima n znamenaka je

$$\frac{e^\gamma \cdot \ln 10^n}{\ln 2} - \frac{e^\gamma \cdot \ln 10^{n-1}}{\ln 2} = n\frac{e^\gamma \cdot \ln 10}{\ln 2} - (n-1)\frac{e^\gamma \cdot \ln 10}{\ln 2} = \frac{e^\gamma \cdot \ln 10}{\ln 2}.$$

S druge strane, nije poznato postoji li konačno ili beskonačno mnogo Mersenneovih složenih brojeva za n prost broj.

Otvoren problem 16. *Postoji li beskonačno mnogo složenih Mersenneovih brojeva M_p za prost broj p?*

Već smo spomenuli da je najveći do sada pronađen prost broj zapravo Mersennov prost broj. Možemo se zapitati zašto ne bismo tražili proste brojeve oblika $a^n - 1$ za neki $a \neq 2$. Razlog tomu je sljedeća tvrdnja.

Teorem 2.3.1. *Ako su a i n prirodni brojevi takvi da je $a^n - 1$ prost broj, onda je $a = 2$ ili $p = 1$.*

Dokaz. Imamo $a \equiv 1 \pmod{a-1}$. Tada je $a^p \equiv 1 \pmod{a-1}$, odnosno $a^p - 1 \equiv 0 \pmod{a-1}$. Stoga vrijedi $a - 1 \mid a^p - 1$. Kako je $a^p - 1$ prost broj, mora vrijediti da je $a - 1 = \pm 1$ ili $a - 1 = a^p - 1$. Iz prve jednakosti slijedi da je $a = 2$ ili $a = 0$. Budući da je a prirodan broj, slijedi da je $a = 2$. Iz druge jednakosti slijedi $a = a^p$, pa imamo sljedeće mogućnosti $a = 0$ ili $a = 1$ ili $p = 1$. Znamo da $a \neq 0$, a za $a = 1$ imamo $1^p - 1 = 0$ što nije prost broj. Dakle, $a = 2$ ili $p = 1$. □

Ispitivanje je li neki Mersenneov broj M_p prost može se svesti na ispitivanje mogućih djelitelja broja M_p. Vrijedi tvrdnja.

Teorem 2.3.2. *Neka je p prost broj. Ako je q prosti djelitelj Mersenneovog broja M_p, onda je*

$$q = 2kp + 1,$$

za neki cijeli broj k.

Dokaz. Jasno je da je q neparan i prema Malom Fermatovom teoremu 2.2.1 slijedi

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

Nadalje, prema pretpostavci $q|2^p - 1$ pa je

$$2^p \equiv 1 \pmod{q}.$$

Prema Propoziciji 2.2.9 red broja 2 modulo q mora dijeliti i $q-1$ i p. Kako je p prost slijedi da je red upravo jednak p i $p|q-1$, to jest $q \equiv 1 \pmod{p}$. Kako je q neparan broj, slijedi $q \equiv 1 \pmod{2p}$. □

Da bismo dokazali neke od sljedećih tvrdnji trebat će nam pojam *kvadratnog ostatka modulo p*, gdje je p prost broj te pojam *Legendreovog simbola*.

Definicija 2.3.3. *Neka je a cijeli broj te n prirodan, te* $(a, n) = 1$. *Ako kongruencija*

$$x^2 \equiv a \pmod{n}$$

ima rješenja, onda kažemo da je a ***kvadratni ostatak modulo*** *n. U protivnom je a* ***kvadratni neostatak modulo*** *n.*

Definicija 2.3.4. *Neka je p neparan prost broj.* ***Legendreov simbol*** *definira se kao*

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

U sljedećih nekoliko teorema navodimo neka od najvažnjih svojstava Legendreovog simbola.

Teorem 2.3.5 (Eulerov kriterij)**.** *Neka je a cijeli broj i p neparan prost broj. Vrijedi:*

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

Teorem 2.3.6. *Neka su a, b cijeli brojevi i p neparan prost broj. Vrijedi:*

1) ako $a \equiv b \pmod{p}$, *onda* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$;

2) ako $(a, p) = 1$, *onda* $\left(\frac{a^2}{p}\right) = 1$;

3) $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$;

4) $\left(\frac{1}{p}\right) = 1, \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Teorem 2.3.7 (Gaussov kvadratni zakon reciprociteta)**.** *Neka su p, q neparni prosti brojevi i $p \neq q$. Tada je*

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

Teorem 2.3.8. *Neka je p neparan prost broj. Ako je q prosti djelitelj Mersenneovog broja M_p, onda je*

$$q = 8k \pm 1$$

za neki cijeli broj k.

Dokaz. Kako je q prosti djelitelj Mersenneovog broja $2^p - 1$ slijedi da je $2^p \equiv 1 \pmod{q}$. Po Teoremu 2.3.2 znamo da je djelitelj Mersenneovog broja M_p oblika $q = 2kp + 1$, odnosno $q - 1 = 2kp$ za neki cijeli broj k. Iz toga slijedi

$$2^{\frac{q-1}{2}} \equiv 2^{pk} \equiv 1 \pmod{q},$$

pa je 2 kvadratni ostatak modulo q i slijedi da je $q \equiv \pm 1 \pmod{8}$. □

Provjera je li neki Mersenneov broj prost nije jednostavna. Broj 2^n vrlo brzo raste te je neophodno u provjerama koristiti računalo. Iz tog razloga su neki stariji rezultati uistinu impresivni. Francuski matematičar E. A. Lucas dokazao je 1876. godine da je broj

$$M_{127} = 170141183460469231731687303715884105727$$

prost broj. U traganje za prostim Mersenneovim brojevima uputili su se mnogi mnogi matematičari pa i studenti. Tako su, primjerice L. Nickel i C. Noll, dvoje osamnaestogodišnjih studenata Kalifornijskog sveučilišta u Haywardu, otkrili uz pomoć računala, da je $2^{21\,701} - 1$ prost broj. Broj se sastoji od čak 6 533 znamenke. Devetnaestogodišnji Amerikanac R. Clarkson je 1998. godine na svom kućnom računalu otkrio Mersenneov prost broj $M_{3\,021\,377}$. Broj se sastoji od 909 536 znamenki te se dojam o veličini tog broja može steći ako se kaže da bi za njegov zapis bila potrebna knjiga od oko 500 stranica. Zanimljivo je da se na internet stranici *The Electronic Frontier Foundation*, u okviru projekta *Great Internet Mersenne Prime Search*, nudi nagrada od 100 000 USD onome tko prvi otkrije prost broj s barem 10 000 000 znamenki.

Za utvrđivanje prostosti Mersenneovih brojeva može se korisiti tzv. *Lucas-Lehmerov test*. Test je ustanovio E. A. Lucas 1856. godine, a naknadno, oko 1930. godine, ga je poboljšao D. H. Lehmer. Test omogućuje testiranje prostosti velikih Mersenneovih brojeva na računalima mnogo brže od "običnih" brojeva iste veličine. Iz tog razloga je upravo najveći poznati prost broj Mersenneov broj.

Teorem 2.3.9 (Lucas-Lehmerov test)**.** *Neka je p neparan prost broj i (S_k) rekuzivni niz zadan s*

$$S_0 = 4,\ S_k = S_{k-1}^2 - 2,\ k \geq 2.$$

Tada je M_p prost broj ako i samo ako vrijedi

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

Dokaz. Neka je $\omega = 2 + \sqrt{3}$ i $\overline{\omega} = 2 - \sqrt{3}$. Principom matematičke indukcije pokazujemo da je da je $S_n = \omega^{2^n} + \overline{\omega}^{2^n}$ za svaki $n \in \mathbb{N}_0$. Baza indukcije vrijedi jer je

$$S_0 = \omega^{2^0} + \overline{\omega}^{2^0} = (2 + \sqrt{3} + (2 - \sqrt{3})) = 4.$$

Neka je $n \in \mathbb{N}$. Pretpostavimo da tvrdnja vrijedi za $n - 1$. Sada je

$$S_n = S_{n-1}^2 - 2 = (\omega^{2^{n-1}} + \overline{\omega}^{2^{n-1}})^2 - 2 = \omega^{2^n} + \overline{\omega}^{2^n} + 2(\omega\overline{\omega})^{2^{n-1}} - 2 = \omega^{2^n} + \overline{\omega}^{2^n},$$

pri čemu smo koristili da je $\omega\overline{\omega} = (2 + \sqrt{3})(2 - \sqrt{3}) = 1$.

Sada pretpostavimo da vrijedi $S_{p-2} \equiv 0 \pmod{M_p}$. Pokazat ćemo da je M_p prost broj. Dakle, prema pretpostavci je

$$\omega^{2^{p-2}} + \overline{\omega}^{2^{p-2}} = kM_p,$$

za neki cijeli broj k, odnosno

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

Množenjem prethodne jednakosti s $\omega^{2^{p-2}}$ dobivamo

$$\left(\omega^{2^{p-2}}\right)^2 = kM_p\omega^{2^{p-2}} - (\overline{\omega}\omega)^{2^{p-2}}.$$

Stoga je

$$\omega^{2^{p-1}} = kM_p\omega^{2^{p-2}} - 1. \tag{2.2}$$

Pretpostavimo suprotno, da je M_p složen broj i neka je q najmanji prosti faktor od M_p. Mersenneovi brojevi su neparni, pa je $q > 2$. Definiramo skup

$$X = \{a + b\sqrt{3} \,:\, a, b \in \mathbb{Z}_q\}, \tag{2.3}$$

gdje je $\mathbb{Z}_q$ (konačno) polje ostataka modulo q. Množenje u X definirano je na sljedeći način:

$$(a + \sqrt{3}b)(c + \sqrt{3}d) = (ac + 3bd \mod q) + (ad + bc \mod q)\ \sqrt{3}.$$

Ovako definirano množenje na X je zatvoreno, komutativno i asocijativno te je $1 \in X$ očito jedinica u X (odnosno neutralni element). Stoga X uz množenje tvori komutativan monoid.

Broj elemenata ovog monoida, tj. kardinalni broj označit ćemo s $|X|$. Uočimo da X nije grupa jer 0 nema multiplikativni inverz. Stoga za grupu inverbilnih elemenata X^* sigurno vrijedi:

$$|X^*| < |X|,$$

odnosno

$$|X^*| \leq |X| - 1 = q^2 - 1.$$

Kako je $M_p \equiv 0 \pmod{q}$ i $\omega \in X$, slijedi da je

$$kM_p\omega^{2^{p-2}} = 0$$

u monoidu X. Iz relacije (2.2) imamo da je

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

također u skupu X i kvadriranjem obje strane jednakosti dobivamo

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

Stoga je ω element skupa X^*, odnosno invertibilan je, a njegov je inverz $\omega^{2^{p-1}}$. Štoviše, red od ω je 2^p jer $\omega^{2^{p-1}} \neq 1$ i vrijedi

$$2^p \leq |X^*| \leq q^2 - 1 < q^2,$$

ali q je najmanji prosti faktor složenog broja M_p, pa je

$$q^2 \leq M_p = 2^p - 1.$$

To daje kontradikciju $2^p < 2^p - 1$. Dakle, M_p je prost broj.

U drugom smjeru, cilj je pokazati da pretpostavka da je broja M_p prost povlači da vrijedi $S_{p-2} \equiv 0 \pmod{M_p}$. Najprije ustanovimo da je

$$2^p - 1 \equiv 7 \pmod{12},$$

za neparan broj $p > 1$. Zaista, kako je

$$2^p - 1 \equiv -1 \equiv 3 \pmod{4}$$

te

$$2^p - 1 \equiv (-1)^p - 1 = -2 \equiv 1 \pmod{3},$$

prema Kineskom teoremu o ostatcima slijedi da je $M_p = 2^p - 1 \equiv -1 \equiv 7 \pmod{12}$. Nadalje zbog svojstava Legendreovog simbola slijedi

$$\left(\frac{3}{M_p}\right) = -\left(\frac{M_p}{3}\right) = -\left(\frac{1}{3}\right) = -1,$$

što znači da je 3 kvadratni neostatak modulo M_p. Po Eulerovom kriteriju to je ekvivalentno sljedećem

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

Sada ćemo ustanoviti da je 2 kvadratni ostatak modulo M_p. Jer $2^p \equiv 1 \pmod{M_p}$ slijedi

$$2 \equiv 2^{p+1} = \left(2^{\frac{p+1}{2}}\right)^2 \pmod{M_p},$$

što znači da kvadratna kongruencija $x^2 \equiv 2 \pmod{M_p}$ ima rješenja, odnosno da je 2 kvadratni ostatak modulo M_p. Iz Eulerovog kriterija sada slijedi

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

Kombinirajući obje relacije koje smo dobili Eulerovim kriterijem imamo

$$24^{\frac{M_p-1}{2}} \equiv \left(2^{\frac{M_p-1}{2}}\right)^3 \left(3^{\frac{M_p-1}{2}}\right) \equiv (1)^3(-1) \equiv -1 \pmod{M_p}.$$

Neka je $\sigma = 2\sqrt{3}$ i X kao u (2.3) za $q = M_p$. Uz zbrajanje i množenje modulo M_p skup X ima algebarsku strukturu prstena. U X vrijedi:

$$\begin{aligned}(6+\sigma)^{M_p} &= 6^{M_p} + (2^{M_p})(\sqrt{3}^{M_p}) = 6 + 2\left(3^{\frac{M_p-1}{2}}\right)\sqrt{3} \\ &= 6 + 2(-1)\sqrt{3} = 6 - \sigma,\end{aligned}$$

gdje je u prvoj jednakosti primijenjen Binomni teorem $(x+y)^{M_p} \equiv x^{M_p} + y^{M_p} \pmod{M_p}$, a u drugoj jednakosti je primijenjen Mali Fermatov teorem $a^{M_p} \equiv a \pmod{M_p}$, za neki cijeli broj a. Vrijednost od σ je odabrana tako da je

$$\omega = \frac{(6+\sigma)^2}{24}.$$

Prethodnu jednakost upotrijebit ćemo za izračun $\omega^{\frac{M_p+1}{2}}$ u prstenu X:

$$\omega^{\frac{M_p+1}{2}} = \frac{(6+\sigma)^{M_p+1}}{24^{\frac{M_p+1}{2}}} = \frac{(6+\sigma)(6+\sigma)^{M_p}}{24 \cdot 24^{\frac{M_p-1}{2}}} = \frac{(6+\sigma)(6-\sigma)}{-24} = -1.$$

Množenjem obje strane jednakosti sa $\overline{\omega}^{\frac{M_p+1}{4}}$ dobivamo

$$\omega^{\frac{M_p+1}{2}}\overline{\omega}^{\frac{M_p+1}{4}} = -\overline{\omega}^{\frac{M_p+1}{4}},$$

odnosno

$$\omega^{\frac{M_p+1}{4}}\underbrace{\omega^{\frac{M_p+1}{4}}\overline{\omega}^{\frac{M_p+1}{4}}}_{=1} = -\overline{\omega}^{\frac{M_p+1}{4}},$$

jer je $\omega\overline{\omega} = 1$. Nadalje,

$$\omega^{\frac{M_p+1}{4}} + \overline{\omega}^{\frac{M_p+1}{4}} = 0,$$

odnosno

$$\omega^{2^{p-2}} + \overline{\omega}^{2^{p-2}} = 0$$

daje $S_{p-2} = 0$ u X, tj. $S_{p-2} \equiv 0 \pmod{M_p}$ što je i trebalo pokazati. □

Primjer 2.3.10. *Potvrdimo pomoću Lucas - Lehmerovog testa da je Mersenneov broj* $M_{13} = 8\ 191$ *prost broj. Znamo da je* $S_0 = 4$ *i da je* $p = 13$. *Želimo pokazati da je*

$$S_{11} \equiv 0 \pmod{M_{13}}.$$

Odredimo S_{11}*:*

$$\begin{aligned}
S_1 &= S_0^2 - 2 = 4^2 - 2 = 14 \equiv 14 \pmod{8\ 191},\\
S_2 &= S_1^2 - 2 = 14^2 - 2 = 194 \equiv 194 \pmod{8\ 191},\\
S_3 &= S_2^2 - 2 = 194^2 - 2 = 37\ 634 \equiv 4\ 870 \pmod{8\ 191}\\
S_4 &= S_3^2 - 2 = 4\ 870^2 - 2 = 23\ 716\ 898 \equiv 3\ 953 \pmod{8\ 191}\\
&\vdots\\
S_k &\equiv 5\ 970, 1\ 857, 36, 1\ 294, 3\ 470, 128, 0 \pmod{8\ 191},\ k = 5, 6, ..., 11.
\end{aligned}$$

Vidimo da vrijedi

$$S_{11} \equiv 0 \pmod{8\ 191},$$

pa je $M_{13} = 8\ 191$ *prost broj.*

Pomoću Lucas-Lehmerovog testa ne možemo odrediti niti jedan netrivijalni faktor Mersenneovog broja. Čak i kad znamo oblike prostih djelitelja broja M_p (Teoremi 2.3.2 i 2.3.8) nije lako odrediti faktorizaciju. Prvih nekoliko faktoriziranih složenih Mersenneovih brojeva dano je u sljedećoj tablici.

Mersenneov broj	Faktorizacija
M_4	$3 \cdot 5$
M_6	$3 \cdot 3 \cdot 7$
M_8	$3 \cdot 5 \cdot 17$
M_9	$7 \cdot 73$
M_{10}	$3 \cdot 11 \cdot 31$

Najmanji složen Mersenneov broj koji do sada nije faktoriziran je $M_{1\,277}$, a najveći kojem je poznata faktorizacija (na "vjerojatno" proste brojeve) $M_{5\,240\,707}$ (što rezultat iz travnja 2016. godine).

U do sada poznatim faktorizacijama složenih Mersennovih brojeva nije se dogodio slučaj da je i kvadrat prostog djelitelja također djelitelj. Kao i za Fermatove brojeve, pretpostavlja se da Mersenneovi brojevi nisu djeljivi s kvadratom prostog broja.

Otvoren problem 17. *Postoji li Mersenneov broj koji je djeljiv s kvadratom prostog broja?*

Zadržimo se još malo na djeliteljima brojeva M_p. U Teoremu 2.3.2 smo pokazali da su prosti djelitelji broja M_p oblika $q = 2kp + 1$, za neki cijeli broj k. Prirodno je prvo proučiti slučaj $k = 1$. Dakle, pitamo se za koje p broj $2p + 1$ dijeli broj M_p, uz pretpostavku da je $2p + 1$ prost. Napomenimo da se prost broj $2p + 1$, za p prost, zove *Sophiein prosti broj* nazvan po francuskoj matematičarki Marie-Sophie Germain (1776.-1831.) koja ga je koristila u traženju dokaza za Veliki Fermatov teorem 2.2.2, a danas nalazi primjenu u kriptografiji javnog ključa. U prilog tomu da je naše zanimanje opravdano ide činjenica da npr. $23 = 2 \cdot 11 + 1$ dijeli M_{11}, te $47 = 2 \cdot 23 + 1$ dijeli M_{23}. No, ima i protuprimjera, $59 = 2 \cdot 29 + 1$ ne dijeli broj M_{29}.

Teorem 2.3.11. *Neka je p prost broj oblika $p = 4m + 3$, za $m \in \mathbb{N}$. Ako je $q = 2p + 1$ također prost broj, tada $q \mid M_p$*

Dokaz. Neka je $q = 2p + 1$ prost broj. Po Malom Fermatovom teoremu 2.2.1 vrijedi

$$2^{2p} \equiv 1 \pmod{q},$$

pa je

$$2^p \equiv 1 \pmod{q} \quad \text{ili} \quad 2^p \equiv -1 \pmod{q}.$$

Pretpostavimo da je druga tvrdnja istinita, tada je

$$2^{p+1} = \left(2^{\frac{1}{2}(p+1)}\right)^2 \equiv -2 \pmod{q},$$

pa slijedi da je -2 kvadratni ostatak modulo q. Nadalje, kako je $p \equiv 3 \pmod 4$, slijedi da je $q \equiv 7 \pmod 8$ pa je 2 kvadratni ostatak modulo q. Također, budući da je $q \equiv 3 \pmod 4$, -1 je kvadratni neostatak modulo q. Stoga je $-2 = (-1) \cdot 2$ - produkt kvadratnog neostatka i kvadratnog ostatka pa je stoga neostatak, što je kontradikcija. Dakle, prva kongruencija mora biti istinita. □

Prema prethodnoj tvrdnji je jasno da ako bismo znali pokazati da postoji beskonačno mnogo Sophieinih prostih broja za $p \equiv 3 \pmod 4$, onda bi znali i odgovor na pitanje 13.

Otvoren problem 18. *Postoji li beskonačno mnogo prostih brojeva oblika $p = 4m + 3$ takvih da je $2p + 1$ prost broj?*

Lako se vidi da su Mersenneovi brojevi povezani i s parnim savršenim brojevima. Znamo da je paran broj savršen ako i samo je oblika $2^{n-1}(2^n - 1)$, gdje je $2^n - 1$ prost (Teorem 1.3.3). Može se reći da ima onoliko parnih savršenih brojeva koliko ima Mersenneovih prostih brojeva. Ako je hipoteza da Mersenneovih prostih brojeva ima beskonačno mnogo točna, onda i parnih savršenih brojeva ima beskonačno mnogo. Iz Teorema 2.3.11 direktno slijedi.

Korolar 2.3.12. *Neka je p prost broj oblika $p = 4m + 3$, za $m \in \mathbb{N}$. Ako je $q = 2p + 1$ također prost broj, tada $2^{p-1}M_p$ nije savršen broj.*

Matematičari Bateman, Selfridge i Wagstaff postavili su sljedeću hipotezu, koja je još poznata kao *Nova Mersenneova hipoteza*.

Otvoren problem 19. *Neka je p neparan prirodan broj. Ako vrijede dvije od navedenih tvrdnji, onda vrijedi i treća:*

1. *$p = 2^k \pm 1$ ili $p = 4^k \pm 3$ za neki prirodan broj k,*
2. *$2^p - 1$ je prost broj (- Mersenneov prost broj),*
3. *$\dfrac{2^p + 1}{3}$ je prost broj (- Wagstaffov prost broj).*

Ako je p neparan složen broj, onda su brojevi oblika $2^p - 1$ i $\dfrac{2^p + 1}{3}$ oba složeni brojevi. Poznati brojevi koji zadovoljavaju sva tri uvjeta hipoteze su $p = 3, 5, 7, 13, 17, 19, 31, 61$, 127. Postavljena je i hipoteza da niti jedan broj p veći od 127 ne zadovoljava sva tri uvjeta. Neki od prostih brojeva koji zadovoljavaju barem jedan od uvjeta su $p = 2$, 3, 5, 7, 11, 13, 19, 23, 31, 43, 61, 67, 79, 89, 101, 107, 127, 167, 191, 199, 257, 313,... Možemo uočiti da se dva prosta broja $p = 67 = 4^3 + 3$ i $p = 257 = 4^4 + 1$, za koja je Mersenne mislio da su M_{67} i M_{257} prosti brojevi i bio u krivu, oba nalaze u hipotezi i zadovoljavaju samo prvi uvjet. Stoga se možemo zapitati je li Mersenne možda mislio da je broj oblika $2^p - 1$ prost ako i samo ako je $p = 2^k \pm 1$ ili $p = 4^k \pm 3$, za neki prirodan broj k.

Nova Mersenneova hipoteza može se smatrati pokušajem spašavanja stoljetne Mersenneove pretpostavke, koja se pokazala netočnom. Međutim, prema Robertu D. Silvermanu, John Selfridge složio se da je Nova Mersenneova hipoteza očito istinita, budući da je odabrana tako da odgovara poznatim podatcima i protuprimjeri izvan tih slučajeva su malo

vjerojatni. Renaud Lifchitz je pokazao da je Nova Mersenneova hipoteza točna za sve brojeve manje ili jednake 20 996 010 sustavnim testiranjem svih neparnih prostih brojeva za koje je već poznato da zadovoljavaju bar jedan od uvjeta.

Brojevi oblika

$$M_{M_n} = 2^{2^n-1} - 1,$$

gdje je M_n Mersenneov broj zovu se *dvostruki Mersenneovi brojevi*. Prvih nekoliko dvostrukih Mersenneovih brojeva je

$$M_{M_1} = 1,\ M_{M_2} = 7,\ M_{M_3} = 127,\ M_{M_4} = 32\,767 \quad M_{M_5} = 2\,147\,483\,647.$$

Ispitivati prostost dvostrukog Mersenneovog broja M_{M_n} smisleno je samo ako je M_n Mersenneov prost broj. Za prva četiri Mersenneova prosta broja M_2, M_3, M_5, M_7 vrijedi da su i pripadni dvostruki Mersenneovi brojevi prosti. I to su jedini poznati prosti dvostruki Mersenneovi brojevi.

Otvoren problem 20. *Postoje li samo četiri dvostuka Mersenneova prosta broja?*

Za samo četiri složena dvostuka Mersenneova broja poznata je potpuna faktorizacija. To su brojevi $M_{M_{13}}$, $M_{M_{17}}$, $M_{M_{19}}$, $M_{M_{31}}$. Sljedeći kandidat za prostog dvostukog Mersenneovog broja mogao bi biti $M_{M_{61}}$. To je 694127911065419642-znamenkasti broj! Koliko je poznato on nema prostog djelitelja manjeg od $4 \cdot 10^{33}$.

Otvoren problem 21. *Je li dvostuki Mersenneovi broj $M_{M_{61}}$ prost ili složen?*

2.4 Parovi blizanaca

Par blizanaca je par prostih brojeva oblika p i $p + 2$. Ime im je dao njemački matematičar P. Stackel na kraju 19.stoljeća. Obično se prvih par prostih brojeva $(2, 3)$ ne smatra parom blizanaca jer je broj 2 jedini paran prost broj i brojevi se razlikuju za 1. Prvih par primjera parova blizanaca su:

$$(3, 5), \quad (5, 7), \quad (11, 13), \quad (17, 19), \quad (29, 31), \quad (41, 43).$$

Jedan od prvih rezultata istraživanja parova blizanaca je da je svaki par, osim para $(3, 5)$, oblika

$$(6n - 1, 6n + 1),$$

za neki prirodan broj n, što povlači da je zbroj blizanaca p i $p + 2$ za $p > 3$ djeljiv s 12. Poznate su još neke činjenice o parovima blizanaca. Na primjer, broj 5 je jedini broj koji se nalazi u dva para blizanaca.

Iako je poznato preko sto tisuća parova blizanaca, još nije poznato je li taj broj konačan ili beskonačan. Pitanje postoji li beskonačno mnogo parova blizanaca je jedno od najpoznatijih otvorenih pitanja u teoriji brojeva. Parovi blizanaca postaju sve rjeđi kada se ispituju sve veći i veći brojevi te se smatra da i razmak između parova blizanaca postaje sve veći. Trenutno najveći poznati par blizanaca je $2\,996\,863\,034\,895 \cdot 2^{1\,290\,000} \pm 1$ koji je otkriven 2016. godine i ima 388 342 znamenke.

Otvoren problem 22. *Postoji li beskonačno mnogo cijelih brojeva p takvih da su brojevi p i $p + 2$ prosti?*

Postoji mnogo rezultata koji bi išli u prilog hipotezi o beskonačnom broju parova blizanaca. Američki matematičar R. F. Arenstorf objavio je 2004. godine navodni dokaz hipoteze o parovima blizanaca. Na žalost, u dokazu je pronađena ozbiljna pogreška, stoga je odbijen te je pitanje i dalje ostalo otvoreno.

Francuski matematičar A. de Polignac je 1849. godine postavio općenitiju hipotezu da za svaki prirodni broj k postoji beskonačno mnogo prostih brojeva p tako da je i $p + 2k$ također prost. Za $k = 1$ radi se o hipotezi za parove blizanaca. Hipoteza do sad nije niti dokazana niti opovrgnuta niti za jednu vrijednost prirodnog broja k.

Norveški matematičar Viggo Brun promatrao je sumu recipročnih vrijednosti parova blizanaca:

$$\sum_{p,p+2-\text{prosti}} \left(\frac{1}{p} + \frac{1}{p+2}\right).$$

Ako bi taj red divergirao, onda bi moralo postojati beskonačno mnogo parova blizanaca. Međutim, 1919. godine Brun je dokazao da taj red konvergentan. Suma tog reda označava se s

$$B_2 = \left(\frac{1}{3} + \frac{1}{5}\right) + \left(\frac{1}{5} + \frac{1}{7}\right) + \left(\frac{1}{11} + \frac{1}{13}\right) + \cdots$$

i naziva *Brunova konstanta*. Vrijednost te konstante trebala bi biti iracionalan broj ukoliko parova blizanaca ima beskonačno. Empirijski se pokazalo, zbrajanjem do brojeva reda veličine 10^{16} da je $B_2 \approx 1.902160583104$. No, uz pretpostavku da je Riemannova hipoteza (vidi 31) točna može se pokazati da je $B_2 < 2.1754$. S poboljšanjem računala, Brunova konstanta postala je sve preciznija. Budući da ta suma konvergira, nije moguće zaključiti da postoji beskonačno mnogo parova blizanaca. Brun je također dokazao da za svaki pozitivan cijeli broj n postoji n uzastopnih prostih brojeva tako da niti jedan od njih nije par blizanaca.

Generalizirana i jača hipoteza od hipoteze o parovima blizanaca je *Hardy-Littlewood hipoteza*.

Otvoren problem 23 (Hardy-Littlewood hipoteza)**.** *Neka je $\pi_2(n)$ broj parova blizanaca p i $p+2$. Tada vrijedi*

$$\pi_2(n) \sim 2\Pi_2 \int_2^n \frac{dt}{(\ln t)^2},$$

gdje je $\Pi_2 = \prod_{p=3}^{\infty} \left(1 - \frac{1}{(p-1)^2}\right) \approx 0.66016181584686.$

Ukoliko se hipoteza pokaže točnom, vrijedila bi tvrdnja da postoji beskonačno mnogo parova blizanaca. Viggo Brun je također dokazao da za broj parova blizanaca koji su manji od nekog n vrijedi

$$\pi_2(n) < \frac{cn}{(\ln n)^2},$$

za neku pozitivnu konstantu c.

Možemo se i poslužiti *Teoremom o prostim brojevima* koji govori o distribuciji prostih brojeva, odnosno tvrdi je broj prostih brojeva manjih od n približno jednak $\frac{n}{\log n}$, što znači da je vjerojatnost da je proizvoljno odabrani broj koji nije veći od n prost približno jednaka $\frac{1}{\log n}$. Stoga zaključujemo vjerojatnost da su p i $p+2$ koji nisu koji nije veći od n jednaka $\frac{1}{(\log n)^2}$.

Kineski matematičar Y. Zhang 2013. godine objavio je dokaz da za neki N koji je manji od $7 \cdot 10^7$ postoji beskonačno mnogo parova prostih brojeva koji se razlikuju za N. Zhangov rad je iste te godine prihvatio i objavio matematički časopis *Annals of Mathematics*. Neki su matematičari već najavili da je moguće bitno smanjenje gornje granice za N na 246.

Matematičar P. Clement je 1949. godine dokazao da je par $(n, n+2)$ par blizanaca ako i samo ako vrijedi

$$4((n-1)! + 1) \equiv -n \pmod{n(n+2)}.$$

Zanimljivo je uočiti da je polovina zbroja parova blizanaca 5 i 7 savršen broj. Možemo se pitati postoji li još koji par blizanaca sa tim svojstvom.

Budući da su mnogi matematičari istraživali svojstva i oblike prostih brojeva, nakon parova blizanaca, istraživali su i trojke prostih brojeva. Ako je p neparan prost broj, onda postoji samo jedna uzastopna trojka neparnih prostih brojeva $(p, p+2, p+4)$, a to je trojka $(3, 5, 7)$.

Teorem 2.4.1. *Neka je n prirodan broj takav da je $n > 3$. Tada brojevi $n, n+2, n+4$ ne mogu svi biti prosti. Odnosno, jedina trojka prostih uzastopnih neparnih brojeva je* $(3, 5, 7)$.

Dokaz. Neka je $n \in \mathbb{N}$. Za $n \leq 3$ imamo sljedeće slučajeve:

- $(1, 3, 5)$,
- $(2, 4, 6)$,
- $(3, 5, 7)$.

Očito se samo posljednja trojka sastoji od prostih brojeva.

Pretpostavimo da je $n > 3$. Ako je n paran broj, onda se trojka $(n, n+2, n+4)$ sastoji od uzastopnih parnih brojeva pa nije prosta trojka. Stoga pretpostavimo da je n neparan cijeli broj takav da je $n > 3$. S obzirom da n može biti oblika $n = 3k$, $n = 3k + 1$, $n = 3k + 2$, za neki $k \in \mathbb{N}$, slijedi da ako

- $n = 3k$, onda $(n, n + 2, n + 4)$ sadrži složen broj n,
- $n = 3k + 1$, onda $(n, n + 2, n + 4)$ sadrži složen broj $n + 2 = 3k + 3 = 3(k + 1)$,
- $n = 3k + 2$, onda $(n, n + 2, n + 4)$ sadrži složen broj $n + 4 = 3k + 6 = 3(k + 2)$.

Dakle, ne postoji takav $n > 3$ da bi brojevi $n, n + 2, n + 4$ svi bili prosti brojevi. □

Zbog prethodne tvrdnje smisleno je promatrati trojke oblika:

$$(p, p + 2, p + 6), \ (p, p + 4, p + 6),$$

gdje je $p > 2$, p i $p + 6$ prosti brojevi i jedan od brojeva $p + 2$ i $p + 4$ je prost broj. To jest, niz od četiri uzastopna neparna broja $p, p+2, p+4, p+6$ čini *trojku prostih brojeva* ako su prvi i posljednji prosti brojevi i jedan od dva preostala broja "u sredini" je prost. Primjer trojke prostih brojeva je:

$$(5, 7, 11) \quad \text{i} \quad (7, 11, 13).$$

Nije poznato postoji li beskonačno mnogo brojeva koji čine trojku prostih brojeva.

Najmanja *četvorka prostih brojeva* je oblika $(p, p+2, p+6, p+8)$, gdje su p, $p+2$, $p+6$ i $p + 8$ neparni prosti brojevi i to je četvorka $(5, 7, 11, 13)$. Isto tako, nije poznato postoji li beskonačno mnogo brojeva koji čine četvorku prostih brojeva, ali je poznato da postoji samo jedna *osmorka prostih brojeva*, a to je $(11, 13, 17, 19, 23, 29, 31, 37)$. Ta osmorka je jedini primjer osmorke prostih brojeva koja počinje sa neparnim prostim brojem p i završava s neparnim prostim brojem $p + 26$.

Otvoren problem 24. *Postoji li beskonačno mnogo brojeva koji čine trojku ili četvorku prostih brojeva?*

2.5 O udaljenostima između prostih brojeva

U prethodnom odjeljku 2.4 govorili smo o parovima blizanaca, odnosno o uzastopnim prostim brojevima čija je udaljenost, to jest razlika minimalna - jednaka 2. Razliku dva susjedna prosta broja p_{n+1} i p_n označit ćemo s

$$g_n = p_{n+1} - p_n$$

i zvati n-ta *udaljenost* ili n-ti *razmak*. Iznijeli smo hipotezu da postoji beskonačno mnogo n takvih da je $g_n = 2$ (vidjeti 22), no lako se može pokazati da za svaki prirodan broj n postoji n uzastopnih složenih brojeva.

Propozicija 2.5.1. *Za svaki prirodan broj n postoji n uzastopnih složenih brojeva.*

Dokaz. Promotrimo niz brojeva

$$(n+1)! + 2, (n+1)! + 3, \ldots, (n+1)! + n, (n+1)! + n + 1.$$

Svaki od brojeva iz danog niza je složen jer $j \mid (n+1)! + j$ za svaki $j = 2, 3, \ldots, n+1$. □

Budući da postoji "lanac" složenih brojeva proizvoljne duljine, imamo sljedeću posljedicu.

Korolar 2.5.2. *Za svaki prirodan broj n postoje uzastopni prosti brojevi p_k i p_{k+1} takvi da je $g_k > n$.*

S druge strane, vezano uz razmake između prostih brojeva francuski matematičar A. M. Legendre (1752. - 1833.) postavio je sljedeću hipotezu.

Otvoren problem 25 (Legendreova hipoteza)**.** *Postoji prost broj između n^2 i $(n+1)^2$ za svaki prirodan broj n.*

Ako bi se pokazala točnost Legendreova hipoteze, tada bi znali da je razmak izmedju prostog broja p i njegovog prostog sljedbenika reda veličine $\sqrt{p}$. Preciznije, postoji pozitivan realan broj M takav da je

$$g_n < M\sqrt{p_n},$$

za sve n veće od nekog n_0, što se može zapisati kao $g_n = O(\sqrt{p_n})$. Jaču hipotezu postavio je 1986. godine rumunjski matematičar Dorin Andrica.

Otvoren problem 26 (Andricova hipoteza)**.** *Za svaki prirodan broj n vrijedi da je*

$$\sqrt{p_{n+1}} - \sqrt{p_n} < 1.$$

U terminima razmaka između susjednih prostih brojeva, Andricova hipoteza se može zapisati kao

$$g_n < 2\sqrt{p_n} + 1.$$

za svaki $n \in \mathbb{N}$. Andricova slutnja je empirijski potvrđena za sve $n \leq 1.3 \cdot 10^{16}$.

U prethodnom smo govorili o broju prostih brojeva između kvadrata uzastopnih prirodnih brojeva. Možemo se pitati i što je s prostim brojevima između kvadrata uzastopnih prostih brojeva. U vezi toga postavljena je sljedeća slutnja.

Otvoren problem 27 (Brocardova hipoteza)**.** *Postoje bar četiri prosta broja između p_n^2 i p_{n+1}^2, za $n > 1$, gdje je p_n n-ti prosti broj.*

Za prvih nekoliko prostih brojeva lako možemo vidjeti da slutnja vrijedi:

n	p_n	p_n^2	Prosti brojevi	Broj prostih brojeva
1	2	4	5, 7	2
2	3	9	11, 13, 17, 19, 23	5
3	5	25	29, 31, 37, 41, 43, 47	6
4	7	49	53, 59, 61, 67, 71, ...	15
5	11	121	127, 131, 137, 139, 149, ...	9

Ova hipoteza je provjerena za brojeve $n \leq 10^{10}$. Jača pretpostavka od ove je da postoje bar četiri prosta broja između n^2 i $(n+2)^2$ za $n \geq 1$. Ova pretpostavka je provjerena za brojeve do $2 \cdot 10^9$.

Sljedeća hipoteza o distribuciji prostih brojeva nazvana je po danskom matematičaru Ludvigu Oppermannu koji ju je objavio 1882. godine. Povezana je, ali ipak jača od Legendreove, Andricove i Brocardove hipoteze.

Otvoren problem 28 (Oppermanova hipoteza)**.** *Za svaki cijeli broj $n > 1$ postoji bar jedan prost broj između $n(n-1)$ i n^2 i bar jedan prost broj između n^2 i $n(n+1)$.*

Čak i za male vrijednosti broja n broj prostih brojeva u danom rasponu je mnogo veći od 1 što daje razlog da vjerujemo da je hipoteza točna. Međutim, Oppermanova hipoteza još uvijek nije dokazana.

2.6 Goldbachova slutnja

Uz hipotezu o parovima blizanaca, Goldbachova hipoteza jedna je od najstarijih i najpoznatijih u teoriji brojeva. Goldbachova hipoteza privukla je pažnju mnogih, pojavila se u televizijskim emisijama, filmovima, pa čak i romanima kao što je "Stric Petros i Goldbachova slutnja" A. Doxiadisa. U pismu Euleru 1742. godine, njemački matematičar C.

Goldbach (1690. – 1764.), izrazio je slutnju da je svaki paran cijeli broj zbroj dvaju brojeva koji su ili prosti brojevi ili jednaki 1. Ponešto općenitija formulacija je da se svaki paran cijeli broj veći od 4 može zapisati kao zbroj dvaju neparnih prostih brojeva. Tvrdnju možemo lako provjeriti za prvih nekoliko parnih cijelih brojeva:

$$\begin{aligned} 2 &= 1+1 \\ 4 &= 2+2 = 1+3 \\ 6 &= 3+3 = 1+5 \\ 8 &= 3+5 = 1+7 \\ 10 &= 3+7 = 5+5 \\ 12 &= 7+5 \\ &\vdots \end{aligned}$$

Iako se čini da Euler nikada nije pokušao dokazati Goldbachovu slutnju, godinu dana kasnije poslao je pismo Goldbachu i zapisao slutnju na sljedeći način: svaki paran cijeli broj veći ili jednak od 6 oblika $4n + 2$ je zbroj dvaju brojeva koji su ili prosti ili oblika $4n + 1$ ili 1. U to doba, Goldbach je broj 1 smatrao prostim brojem.

Otvoren problem 29. *[Jaka Goldbachova slutnja] Svaki paran broj veći od 2 može se zapisati kao zbroj dva prosta broja.*

Jaka Goldbachova slutnja se još naziva i Binarna Goldbachova slutnja. *Goldbachov broj* je pozitivni cijeli broj koji se može zapisati kao zbroj dva neparna prosta broja. Broj 4 je jedini paran broj veći od 2 koji se može zapisati jedino kao zbroj dva parna prosta broja. Stoga je druga formulacija Jake Goldbachove slutnje ta da su svi parni brojevi veći od 4 Goldbachovi brojevi. Zapis parnog broja kao zbroj dva prosta broja naziva se *Goldbachova particija* tog broja. Preciznije, Goldbachova particija broja n je uređeni par prostih brojeva (p, q) takav da je $p + q = n$. Sijedi nekoliko primjera Goldbachove particije:

$$\begin{aligned} 6 &= 3+3 \\ 8 &= 3+5 \\ 10 &= 3+7 = 5+5 \\ 12 &= 7+5 \\ &\vdots \\ 100 &= 3+97 = 11+89 = 17+83 = 29+71 = 41+59 = 47+53 \\ &\vdots \end{aligned}$$

Uz pomoć računala slutnja se pokazala točnom za sve parne brojeve manje od $4 \cdot 10^{18}$. S rastom broja n, raste i broj različitih particija. Na primjer, postoji 219 400 takvih prikaza

za paran broj 100 000 000. To ide u prilog Goldbachovoj slutnji, međutim to je daleko od matematičkog dokaza i svi pokušaji dokaza su bili potpuno neuspješni. Jedan od najpoznatijih matematičara prošlog stoljeća, G. H. Hardy, koji se posebno istaknuo u teoriji brojeva, u svom obraćanju Matematičkom društvu Kopenhagena 1921. godine, izjavio je da je Goldbachova slutnja vjerojatno jednako teška kao bilo koji neriješeni problem u matematici.

Goldbach je smatrao da se svaki cijeli broj koji se može zapisati kao zbroj dvaju prostih brojeva može zapisati i kao zbroj tri prosta broja, što lako možemo provjeriti za prvih par brojeva:

$$\begin{aligned} 7 &= 3+2+2 \\ 11 &= 3+3+5 \\ 13 &= 3+5+5 \\ 17 &= 5+5+7 \\ &\vdots \end{aligned}$$

Otvoren problem 30. *[Slaba Goldbachova slutnja] Svaki neparan broj veći od* 7 *može se zapisati kao zbroj tri neparna prosta broja.*

Prethodna se hipoteza naziva *slabom* jer ako bi slutnja 29 bila pokazana onda bi ovo bio njen korolar. Zaista, ako je svaki neparan broj veći 4 zbroj dva neparna prosta, onda pribrajanjem broja 3 dobivamo upravo tvrdnju 30.

Prvi pravi napredak u pokušaju dokazivanja Goldbachove slutnje u gotovo 200 godina napravili su matematičari Hardy i Littlewood 1922. godine. Uz pretpostavku da vrijedi *generalizirana Riemannova hipoteza*, pokazali su da se svaki dovoljno velik neparan broj može zapisati kao zbroj tri neparna prosta broja.

Ruski matematičar I. Vinogradov je 1937. godine je otklonio ovisnost o generaliziranoj Riemannovoj hipotezi dajući tako bezuvjetni dokaz za tu tvrdnju. To jest, on je utvrdio da se svi neparni cijeli brojevi, veći od nekog n_0, mogu zapisati kao zbroj tri neparna prosta broja, odnosno $n = p_1 + p_2 + p_3$, gdje je n neparan i dovoljno velik. Međutim Vinogradov nije mogao dobiti efektivnu veličinu broja n_0. No, njegov student K. Borozdkin (1956.) pokazao je da je $n_0 < 3^{3^{15}}$. Liu Ming-Chit i Wang Tian-Ze su 2002. godine smanjili gornju ogradu broja n_0 na približno 10^{1346}. Očito je eksponent i dalje prevelik kako bi se uspjele izvršiti provjere na računalima koje su u slučaju Goldbachove hipoteze uspjele stići do broja 10^{18}.

Vinogradov je pokazao da ako je $A(x)$ broj cijelih parnih brojeva $n < x$ koji nisu zbroj od dva prosta broja, onda je

$$\lim_{x\to\infty} \frac{A(x)}{x} = 0.$$

To nam omogućuje da kažemo da gotovo svi parni cijeli brojevi zadovoljavaju slutnju.

Neka je $R(n)$ broj prikaza parnog cijelog broja n kao zbroja dvaju prostih brojeva. Tada vrijedi

$$R(n) \sim 2\Pi_2 \prod_{p>2, p|n} \left(\frac{p-1}{p-2}\right) \int_2^n \frac{dx}{(\ln x)^2} \sim 2\Pi_2 \prod_{p>2, p|n} \left(\frac{p-1}{p-2}\right) \frac{n}{(\ln n)^2},$$

gdje je $\Pi_2 = \prod_{p=3}^{\infty} \left(1 - \frac{1}{(p-1)^2}\right) \approx 0.66016181584686.$

Iako je počelo od jednostavnog problema zapisa parnog broja kao zbroja dvaju prostih brojeva, mnogi matematičari su pokušavajući dokazati Goldbachovu slutnju, dokazali neke druge tvrdnje. Dokazano je da se svaki parni cijeli broj može zapisati kao zbroj od najviše šest prostih brojeva. Kineski matematičar C. Jingrun je 1966. godine dokazao da se svaki dovoljno velik cijeli broj može zapisati kao zbroj prostog broja i broja koji nema više od dva prosta faktora.

Ovaj rad završit ćemo s nekoliko riječi o velikoj *Riemannovoj hipotezi* koju smo doveli u vezu s više navedenih otvorenih problema. Radi se o jednoj od najpoznatijih i najtežih hipoteza koju je prije oko 150 godina postavio njemački matematičar G. F. B. Riemann (1826.-1866.) a govori o nultočkama tzv. *Riemann- zeta funkcije* koja se definira kao

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

za sve $s \in \mathbb{C}$ takve da je $\mathrm{Re}(s) > 1$. Još je Riemann pokazao da se ova funkcija po neprekidnosti može proširiti za sve $s \in \mathbb{C}$, osim u točki $s = 1$ gdje ima pol (tj. u tom slučaju je vrijednost funkcije očito suma harmonijskog reda koji je divergentan).

Otvoren problem 31 (Riemannova hipoteza)**.** *Sve netrivijalne nultočke Riemannove zeta funkcije $\zeta(s)$ leže na pravcu* $\mathrm{Re}(s) = \frac{1}{2}$.

Mnogi rezultati navode na njenu točnost te iako je samo hipoteza, primjenjiva je u mnogim područjima matematike i fizike. Posebno zanimljiva i na prvi pogled nevjerojatna je povezanost s teorijom brojeva i distribucijom prostih brojeva. Njezinu težinu i važnost najbolje dočaravaju riječi velikog njemačkog matematičara Davida Hilberta (1862. - 1943.): *Ako bih se probudio nakon tisuću godina, moje prvo pitanje bilo bi: Je li dokazana Riemannova hipoteza?*

Bibliografija

[1] A. Berke, *An Introduction to The Twin Prime Conjecture*: https://ocw.mit.edu/courses/mathematics/18-104-seminar-in-analysis-applications-to-number-theory-fall-2006/projects/berke.pdf, (svibanj, 2017.)

[2] B. Mazur, W. Stein, *Prime Numbers and the Riemann Hypothesis*, Cambridge University Press, New York, 2016.

[3] C. K. Caldwell, *An Amazing Prime Heuristic*: http://www.utm.edu/staff/caldwell/preprints/Heuristics.pdf, (lipanj, 2017.)

[4] C. K. Caldwell, The Prime Pages, *Heuristisc: deriving the Wagstaff Mersenne Conjecture*: https://primes.utm.edu/mersenne/heuristic.html, (lipanj, 2017.)

[5] C. Pomerance, *Primality Testing: Variations on a Theme of Lucas*:https://math.dartmouth.edu/~m75s14/lucasprime3.pdf, (svibanj, 2017.)

[6] D. Shanks, *Solved and Unsolved Problems in Number Theory*, Chelsea Publishing Co., New York, 1978.

[7] E. W. Weisstein, *Double Mersenne Number*: http://mathworld.wolfram.com/DoubleMersenneNumber.html, (svibanj, 2017.)

[8] R. K. Guy, *Unsolved Problems in Number Theory (Third Edition)*, Springer, 2004.

[9] Department of Mathematics University of Zagreb, A. Dujella, *Uvod u teoriju brojeva*: https://web.math.pmf.unizg.hr/~duje/utb/utblink.pdf, (travanj 2017.)

[10] *Some History about Twin Prime Conjecture*:https://arxiv.org/pdf/1205.0774.pdf, (lipanj, 2017.)

[11] University of Washington, C. Tsang, *Fermat Numbers*: http://wstein.org/edu/2010/414/projects/tsang.pdf, (svibanj, 2017.)

[12] Wikipedia The Free Encyclopedia, *Andrica's conjecture*: https://en.wikipedia.org/wiki/Andrica%27s_conjecture, (lipanj, 2017.)

[13] Wikipedia The Free Encyclopedia, *Brocard's conjecture conjecture*: https://en.wikipedia.org/wiki/Brocard%27s_conjecture, (lipanj, 2017.)

[14] Wikipedia The Free Encyclopedia, *Factors of Mersenne Numbers*: https://proofwiki.org/wiki/Factors_of_Mersenne_Numbers, (svibanj, 2017.)

[15] Wikipedia The Free Encyclopedia, *Fermat number*: https://en.wikipedia.org/wiki/Fermat_number, (svibanj, 2017.)

[16] Wikipedia The Free Encyclopedia, *Goldbach's conjecture*: https://en.wikipedia.org/wiki/Goldbach%27s_conjecture, (lipanj, 2017.)

[17] Wikipedia The Free Encyclopedia, *Legendre's conjecture*: https://en.wikipedia.org/wiki/Legendre%27s_conjecture, (lipanj, 2017.)

[18] Wikipedia The Free Encyclopedia, *Lucas-Lehmer primality test*: https://en.wikipedia.org/wiki/Lucas%E2%80%93Lehmer_primality_test, (svibanj, 2017.)

[19] Wikipedia The Free Encyclopedia, *Mersenne Conjectures*:// https://en.wikipedia.org/wiki/Mersenne_conjectures#Lenstra.E2.80.93Pomerance.E2.80.93Wagstaff_conjecture, (svibanj, 2017.)

[20] Wikipedia The Free Encyclopedia, *Mersenne prime*: https://en.wikipedia.org/wiki/Mersenne_prime, (svibanj, 2017.)

[21] Wikipedia The Free Encyclopedia, *Oppermann's conjecture conjecture*: https://en.wikipedia.org/wiki/Oppermann%27s_conjecture, (lipanj, 2017.)

[22] Wikipedia The Free Encyclopedia, *Twin prime*: https://en.wikipedia.org/wiki/Twin_prime, (lipanj, 2017.)

Sažetak

Teorija brojeva kompleksna je grana matematike koja krije mnogo neistraženih i nedokazanih slutnji na koje matematičari pokušavaju pronaći odgovore i dokaze već stotinama godina. U ovom radu navedene su samo neke, od velikog broja nedokazanih tvrdnji, vezane uz savršene i proste brojeve. Iako su jednostavne i lako razumljive, pa stoga zanimljive matematičarima i amaterima, jako su teško dokazive. Neki od najpoznatijih otvorenih problema u ovom radu vezani su uz beskonačnost savršenih, prostih i složenih Fermatovih, prostih i složenih Mersenneovih brojeva i parova blizanaca čiji su oblici, svojstva i najpoznatiji teoremi navedeni. Pomoću modernih računala otkriveni su vrlo veliki brojevi takvih oblika, međutim strogog matematičkog dokaza da ih postoji beskonačno mnogo još uvijek nema. Najpoznatiji i najstariji otvoreni problem je svakako slavna Goldbachova slutnja: "Svaki paran broj veći od broja 2 može se zapisati kao zbroj dva prosta broja", koja je od davne 1742. godine pravi izazov za matematičare.

Postoje mnogi rezultati koji upućuju na točnost poznatih otvorenih problema te su mnogi matematičari, pokušavajući dokazati te tvrdnje, došli do drugih važnih rezultata i dokaza, koristeći rezultate iz teorije brojeva, ali i drugih područja matematike. Budući da nisu dokazani već stotinama godina, u ovom radu nećemo dobiti odgovore na poznata pitanja, ali ćemo dati neke povijesne zanimljivosti, pokazati neke pokušaje u dokazivanju te iskazati poznate teoreme i rezultate vezane uz otvorena pitanja.

Summary

Number theory is a complex branch of mathematics that conceals many unexplored and unproven conjectures to which mathematicians are trying to find answers and proofs for hundreds of years. In this thesis, we give some of many unproven claims related to perfect and prime numbers. Although they are simple and easy to understand, and therefore interesting to mathematicians and amateurs, they are very difficult to prove. Some of the most famous open questions in this thesis are related to the infinity of perfect numbers, prime and complex Fermat numbers, prime and complex Mersenne numbers and twin primes whose forms, properties and most famous theorems are mentioned. With modern computers, very large numbers of those forms have been discovered, but the strict mathematical proof that there are infinitely many numbers of this form is still missing. The most famous and oldest conjecture is definitely the famous Goldbach‘s conjecture: ”Any even integer greater than 2 can be expressed as the sum of two primes”, which has been a real challenge for mathematicians since 1742.

There are many results that point to the exactness of known open questions and many mathematicians, trying to prove these claims, came to other important results and proves, using the results of number theory but also other branches of mathematics. Since they have not been proved for hundreds of years, in this thesis we are not going to answer the famous questions, but we will give some interesting historical facts, show some attempts of proving them and state famous theorems and results given out of the open questions.

Životopis

Zovem se Anđela Kuzek. Rođena sam 9. listopada 1991. godine u Kotor Varošu, BiH. Odrasla sam i živim s roditeljima u Dugom Selu, gdje sam 1998. godine započela školovanje u Osnovnoj školi Josipa Zorića. Od 2006. godine pohađala sam srednju školu Dugo Selo, smjer opća gimnazija te svaki razred završila s odličnim uspjehom. Kao maturantica, položila sam državnu maturu, te sam 2010. godine upisala Prirodoslovno-matematički fakultet u Zagrebu, matematički odsjek na kojem sam 2015. godine završila preddiplomski studij Matematika; smjer nastavnički. Na istom fakultetu nastavila sam obrazovanje i upisala diplomski sveučilišni studij Matematika; nastavnički smjer.