Povezanost prostih brojeva s Fermatovim, Mersenneovim i Fibonaccijevim brojevima

Crnić, Sara

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Sara Crnić

POVEZANOST PROSTIH BROJEVA S FERMATOVIM, MERSENNOVIM I FIBONACCIJEVIM BROJEVIMA

Diplomski rad

Voditelj rada:
prof. dr. sc. Boris Širola

Zagreb, veljača 2016.

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

Glavni cilj ovog diplomskog rada je istražiti nekoliko specijalnih nizova cijelih brojeva; Fermatovih, Mersennovih i Fibonaccijevih brojeva, odnosno njihovu povezanost sa skupom prostih brojeva. Počinjemo s prvim poglavljem u kojem ćemo uvesti oznaku $\mathcal{P}$ za skup svih prostih prirodnih brojeva, koja će imati nepromijenjeno značenje u čitavom radu. Također navodimo *Euklidovu lemu*, poznatu kao karakterizacija prostih brojeva, koja se po prvi put pojavila kao Propozicija 30 u Knjizi VII *Euklidovih Elemenata*. Nadalje, bez dokaza, uvodimo i fundamentalan rezultat teorije brojeva, poznat kao *Osnovni teorem aritmetike*, te Eulerovu funkciju, koju L. Euler uveo 1763. godine. U drugom poglavlju, uz neke elementarne i analitičke dokaze beskonačnosti skupa $\mathcal{P}$, navodimo i dva stožerna teorema. Prvi je tzv. *Dirichletov teorem*, za čiji su dokaz potrebni neki preliminarni rezultati o tzv. karakterima abelovih grupa, te neki pojmovi i rezultati iz kompleksne analize, a drugi je rezultat *Teorem o prostim brojevima*, za koji dajemo tablicu relevantnih numeričkih podataka za funkcije promatrane u teoremu. Nadalje, dokazujemo jedan od najvažnijih rezultata drugog poglavlja; tojest, dokaz teorema divergencije reda $\sum_{p\in\mathcal{P}} \frac{1}{p}$. Njega je prvi dokazao Euler 1737. godine, uz napomenu kako je to još jedan dokaz beskonačnosti skupa $\mathcal{P}$. Mi ćemo dati dva dokaza, od kojih je prvi direktan, dok drugi uvodi u igru Riemannovu zeta funkciju. Naposlijetku, konačno dolazimo do glavnog dijela ovog rada, a to je zadnje poglavlje u kojem najprije promatramo vezu skupa prostih i Fermatovih brojeva, te dajemo još jedan dokaz beskonačnosti skupa prostih brojeva u $\mathbb{N}$. Nadalje, promatramo niz Mersennovih brojeva, koje je uveo francuski klerikalac i matematičar M. Mersenne, te ih koristimo u svrhu još jednog dokaza beskonačnosti skupa $\mathcal{P}$. Uz karakterizaciju savršenih parnih brojeva, u terminima Mersennovih brojeva, bez dokaza, spomenut ćemo Lukas-Lehmerov test, koji je vrlo koristan u testiranju za nalaženje velikih Mersennovih brojeva. Na kraju rada govorit ćemo o nizu Fibonaccijevih brojeva, koji je 1202. godine u svojoj knjizi *Liber Abaci*, definirao talijanski matematičar Leonardo Pisano. Uvest ćemo i vrlo bitan rezultat poznat kao *Binetova formula*, koji će biti bitan u nastavku rada kako bi pokazali vezu Fibonaccijevih i prostih brojeva, te naposlijetku za još jedan dokaz beskonačnosti skupa prostih brojeva.

Poglavlje 1

Neki osnovni pomoćni rezultati

U ovom uvodnom poglavlju podsjetit ćemo se na neke standardne pojmove i rezultate elementarne teorije brojeva. Više detalja, i posebno dokaze nekih tvrdnji koje ovdje navodimo, može se npr. naći u [5, Chapter 2], [4] i [2, Chapter 1,2].

1.1 Djeljivost cijelih brojeva

Predmet proučavanja ovog diplomskog rada je skup cijelih brojeva $\mathbb{Z}$, ili bolje rečeno, njegovi prosti elementi.

Definicija 1.1.1. *Prirodan broj $p > 1$ je **prost broj**, ili* prim broj*, ukoliko su 1 i p jedini njegovi pozitivni djelitelji.*

Označimo

$$\mathcal{P} = \text{skup svih prostih prirodnih brojeva.}$$

Napomena 1.1.2. *Gornja će oznaka $\mathcal{P}$ imati nepromijenjeno značenje u čitavom ovom radu.*

Pojam djeljivosti u $\mathbb{Z}$ dobro je poznat. Činjenicu da $0 \neq a \in \mathbb{Z}$ dijeli neki $b \in \mathbb{Z}$ označavamo standardno s $a|b$. Prisjetimo se sada na ovaj važan i dobro poznat rezultat.

Teorem 1.1.3. ***(o dijeljenju s ostatkom u $\mathbb{Z}$)***
Neka su $a \in \mathbb{Z}$ i $b \in \mathbb{N}$ proizvoljni brojevi. Tada postoje, i jedinstveni su, $q, r \in \mathbb{Z}$ takvi da je

$$a = bq + r \qquad i \qquad 0 \leqslant r < b.$$

Dalje, podsjetimo se na pojam najvećeg zajedničkog djelitelja.

Definicija 1.1.4. *Za brojeve $0 \neq a, b \in \mathbb{Z}$, prirodan broj d je* ***najveći zajednički djelitelj*** *(NZD) od a i b ako vrijedi:*

(1) $d|a$ i $d|b$;

(2) ako je d' bilo koji zajednički djelitelj od a i b, onda $d'|d$.

U tom slučaju pišemo

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

Posebno, kažemo da su brojevi a i b ***relativno prosti*** *ako je NZD $(a, b) = 1$.*

Teorem 1.1.5. *Za proizvoljne cijele brojeve $0 \neq a, b \in \mathbb{Z}$ postoji, i jedinstven je, njihov NZD $d = (a, b)$. Nadalje, u tom slučaju postoje cijeli brojevi x, y takvi da je*

$$ax + by = d.$$

Korisno je spomenuti i sljedeću jednostavnu lemu.

Lema 1.1.6. *Za bilo koje cijele brojeve $a, b \neq 0$ i x, takve da je $b + ax \neq 0$, imamo*

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

Sljedeći rezultat daje nam tehniku računanja NZD $d = (a, b)$, za zadane a i b. Pored toga, dobivamo i efektivan način nalaženja cijelih brojeva x i y takvih da je $ax + by = d$.

Teorem 1.1.7. ***(Euklidov algoritam)***
Neka su $a \in \mathbb{Z}$ i $b \in \mathbb{N}$ proizvoljni. Pretpostavimo da je uzastopnom primjenom teorema o dijeljenju s ostatkom dobiven niz jednakosti:

$$\begin{aligned}
a &= bq_1 + r_1, & 0 < r_1 < b,\\
b &= r_1q_2 + r_2, & 0 < r_2 < r_1,\\
r_1 &= r_2q_3 + r_3, & 0 < r_3 < r_2,\\
&\dots\\
r_{j-2} &= r_{j-1}q_j + r_j, & 0 < r_j < r_{j-1},\\
r_{j-1} &= r_jq_{j+1}.
\end{aligned}$$

Tada je $(a, b) = d$ jednak r_j, posljednjem ostatku različitom od nule. Vrijednosti x i y u jednakosti $d = ax+by$ mogu se dobiti induktivno, uzastopnim prikazivanjem svakog ostatka r_i kao linearne kombinacije a i b.

Dokaz. Za početak, prisjetimo se jednakosti, iz prethodne leme; da je $(n, m) = (n, m + nx)$ za $0 \neq n, m \in \mathbb{Z}$ i $x \in \mathbb{Z}$. Tada primjenom na cijele brojeve a i b vrijedi

$$(a, b) = (a - bq_1, b) = (r_1, b) = (r_1, b - r_1q_2) = (r_1, r_2) = (r_1 - r_2q_3, r_2) = (r_3, r_2).$$

Nastavljajući ovaj proces, dobivamo: $(a, b) = (r_j, r_{j-1}) = r_j$.

Indukcijom ćemo dokazati da je svaki r_i linearna kombinacija od a i b. To je točno za r_1 i r_2, pa pretpostavimo da vrijedi za r_{i-1} i r_{i-2}. Budući da je r_i linearna kombinacija od r_{i-1} i r_{i-2}, po pretpostavci indukcije dobivamo da je i linearna kombinacija od a i b. □

Radi daljnje potrebe, navedimo i sljedeći rezultat; koji između ostalog karakterizira proste brojeve.

Lema 1.1.8. ***(Euklidova lema)***
Pretpostavimo da $a|bc$ i da je NZD $(a, b) = 1$. Tada $a|c$. Posebno, da je p prost broj i $p|ab$, onda $p|a$ ili $p|b$.

Dokaz. Pretpostavimo da je NZD $(a, b) = 1$. Tada iz Teorema 1.1.5 vrijedi da se 1 može prikazati kao linearna kombinacija a i b, tojest

$$ax + by = 1.$$

Množenjem s brojem c dobivamo

$$acx + bcy = c.$$

Sada imamo da $a|a$ i $a|bc$, pa a dijeli i linearnu kombinaciju $acx + bcy$, odnosno $a|c$.

Za drugi dio tvrdnje teorema, pretpostavimo da $p|ab$. Ako p ne dijeli a, tada su a i p relativno prosti, tojest $(a, p) = 1$. Iz prethodno dokazanog, slijedi da $p|b$. □

Sada navedimo, bez dokaza, i ovaj fundamentalan rezultat teorije brojeva.

Teorem 1.1.9. ***(Osnovni teorem aritmetike)***
Za svaki $0 \neq n \in \mathbb{Z}$ postoje prosti brojevi $p_1, \ldots, p_k \in \mathbb{N}$ takvi da je

$$n = \pm p_1 p_2 \cdots p_k.$$

Gornja je faktorizacija jedinstvena do na poredak faktora.

Kao posljedicu gornjeg teorema imamo da se svaki $0 \neq n \in \mathbb{Z}$ može na jedinstven način, do na poredak faktora, zapisati u obliku

$$n = \pm p_1^{a_1} \cdots p_k^{a_k}, \qquad \text{gdje su } p_1 < p_2 < \cdots < p_k;$$

ovdje su $a_i \in \mathbb{N}$. Taj se rastav naziva **standardna dekompozicija** na proste faktore.

Napomena 1.1.10. *Naglasimo kako se svi gore navedeni pojmovi i rezultati mogu generalizirati. Tako npr. za bilo koja dva ne-nul elementa u nekoj domeni glavnih ideala A postoji NZD ta dva elementa. Isto tako, u takvom je prstenu A dobro definiran pojam prostog elementa. I pokazuje se da je takav A i tzv. prsten jedinstvene faktorizacije. To znači da vrijedi analogon gore navedenog osnovnog teorema aritmetike, koji je sada specijalan slučaj $A = \mathbb{Z}$. O svemu navedenom više detalja može se naći u [7].*

1.2 Aritmetičke funkcije

Sada ćemo navesti još jedan pojam, koji ima veliku ulogu u teoriji brojeva, te nam je bitan za daljnje potrebe.

Definicija 1.2.1. *Funkcija $f : \mathbb{N} \to \mathbb{C}$ zove se **aritmetička funkcija**; odnosno, to je funkcija čija je domena skup prirodnih brojeva, a njezina kodomena je skup kompleksnih brojeva.*

Neke od važnijih aritmetičkih funkcija u teoriji brojeva su:

$$\begin{aligned}\tau(n) &= \text{broj pozitivnih djelitelja od } n;\\ \sigma(n) &= \text{zbroj pozitivnih djelitelja od } n;\\ \sigma_k(n) &= \text{zbroj } k\text{-tih potencija pozitivnih djelitelja od } n.\end{aligned}$$

Isto se može napisati i ovako:

$$\tau(n) = \sum_{d|n} 1, \qquad \sigma(n) = \sum_{d|n} d, \qquad \sigma_k(n) = \sum_{d|n} d^k.$$

Za početak, definirat ćemo važno svojstvo koje zadovoljavaju neke aritmetičke funkcije.

Definicija 1.2.2. *Aritmetička funkcija f je **multiplikativna**, ako vrijedi*

$$f(mn) = f(m)f(n)$$

za bilo koje $m, n \in \mathbb{N}$, takve da je $(m, n) = 1$.

Sljedeći teorem direktno će nam dati multiplikativnost gore definiranih aritmetičkih funkcija $\tau(n)$, $\sigma(n)$ i $\sigma_k(n)$.

Teorem 1.2.3. *Pretpostavimo da je $f(n)$ multiplikativna aritmetička funkcija i da vrijedi*

$$F(n) = \sum_{d|n} f(d).$$

Tada je $F(n)$ također multiplikativna.

Dokaz. Pretpostavimo da je $n = n_1 n_2$, tako da $(n_1, n_2) = 1$. Tada, ako $d|n$, te su n_1 i n_2 relativno prosti, vrijedi da je d oblika $d = d_1 d_2$ i $d_1|n_1$, $d_2|n_2$, te $(d_1, d_2) = 1$. Obratno, ako je $d = d_1 d_2$ takav da $d_1|n_1$, $d_2|n_2$, tada $d|n$. Ovime smo uspostavili korespondenciju između pozitivnih djelitelja d broja n i parova djelitelja d_1, d_2 brojeva n_1, n_2. Vrijedi sljedeće

$$F(n) = \sum_{d|n} f(d) = \sum_{d_1|n_1} \sum_{d_2|n_2} f(d_1 d_2).$$

Nadalje, pretpostavili smo da je funkcija f multiplikativna, pa je stoga $f(d_1 d_2) = f(d_1) f(d_2)$. Konačno slijedi tvrdnja teorema:

$$F(n) = \sum_{d_1|n_1} f(d_1) \sum_{d_2|n_2} f(d_2) = F(n_1) F(n_2).$$

□

Za ilustraciju, u sljedećem teoremu dajemo primjenu prethodnog rezultata na standardnu dekompoziciju na proste faktore; i to za funkcije $\tau(n)$ i $\sigma(n)$.

Teorem 1.2.4. *Pretpostavimo da je $n = p_1^{a_1} \cdots p_k^{a_k}$. Tada vrijedi*

$$\tau(n) = (a_1 + 1) \cdots (a_k + 1),$$
$$\sigma(n) = \left(\frac{p_1^{a_1+1} - 1}{p_1 - 1}\right)\left(\frac{p_2^{a_2+1} - 1}{p_2 - 1}\right) \cdots \left(\frac{p_k^{a_k+1} - 1}{p_k - 1}\right).$$

Dokaz. Pretpostavimo da je $n = p^a$, te promotrimo sumu

$$\sum_{d|n} 1.$$

Djelitelji broja p^a su $1, p, p^2, \ldots, p^a$, pa stoga imamo

$$\tau(n) = \tau(p^a) = \sum_{i=0}^{a} 1 = a + 1.$$

Sada kada znamo da je τ multiplikativna funkcija, gornje nam dokazuje prvi dio teorema.

Slično, za drugi dio teorema, ponovno uzmimo da je $n = p^a$, te promotrimo

$$\sum_{d|n} d.$$

Ponovo, djelitelji broja p^a su $1, p, p^2, \ldots, p^a$, pa stoga dobivamo

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

Time smo dokazali i drugi dio teorema. □

Ovaj odjeljak završavamo osnovnim razmatranjima o tzv. *Eulerovoj φ-funkciji*. Za početak sjetimo se da u proizvoljnom komutativnom prstenu A, skup svih invertibilnih elemenata $A^\times = U(A)$ ima strukturu (multiplikativne) grupe. Posebno, za kvocijentni prsten $A = \mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ lako se pokaže, uz korištenje Teorema 1.1.5, da vrijedi sljedeća tvrdnja.

Lema 1.2.5. *Za broj $a \in \mathbb{Z}$ vrijedi da je element $a + n\mathbb{Z} \in \mathbb{Z}_n^\times$, tj. invertibilan, ako i samo ako je NZD $(a, n) = 1$.*

Sada smo spremni uvesti spomenutu funkciju.

Definicija 1.2.6. *Za svaki prirodan broj n definiramo*

$$\varphi(n) = \text{card}\{a \in \{1, \ldots, n\} \mid \textit{NZD}\ (a, n) = 1\};$$

tojest,

$$\varphi(n) = \text{card}(\mathbb{Z}_n^\times),$$

*broj invertibilnih elemenata u prstenu $\mathbb{Z}_n$. Funkcija $\varphi : \mathbb{N} \to \mathbb{N}$ zove se **Eulerova φ–funkcija**.*

Kako bismo pokazali da je φ multiplikativna funkcija, treba nam još jedan pojam.

Definicija 1.2.7. *Za prirodan broj m, **reduciran sustav ostataka** modulo m je skup cijelih brojeva $r_1, \ldots, r_k$ takvih da je svaki r_i relativno prost s m, te vrijedi $r_i \not\equiv r_j \pmod m$ za $i \neq j$, i za svaki cijeli broj x takav da je $(x, m) = 1$ postoji neki i da vrijedi $x \equiv r_i \pmod m$.*

Naprimjer, za $m = 12$ je $\{1, 5, 7, 11\}$ jedan reduciran sustav ostataka modulo 12; i jasno, onda je $\varphi(12) = 4$. Sljedeća je lema prvi korak prema dobivanju formule za efektivno računanje $\varphi(m)$, za $m \in \mathbb{N}$.

Lema 1.2.8. *Ako je $p \in \mathbb{N}$ prost broj i $m \in \mathbb{N}$ proizvoljan, tada je*

$$\varphi(p^m) = p^m - p^{m-1} = p^m(1 - 1/p).$$

Dokaz. Jasno; ako je $1 \leq a < p$, onda je NZD $(a, p) = 1$. Slijedi da broj $1 \leq x \leq p^m$ nije relativno prost s p samo u slučaju ako je x višekratnik od p; tojest, ako je $x = kp$ za $k = 1, 2, \ldots p^{m-1}$. To znači da onih brojeva $1 \leq x \leq p^m$ koji su relativno prosti s p ima točno $p^m - p^{m-1}$; tojest, $\varphi(p^m) = p^m - p^{m-1}$. □

Sada dajemo najavljeni dokaz multiplikativnosti Eulerove funkcije.

Teorem 1.2.9. *Eulerova funkcija φ je multiplikativna.*

Dokaz. Neka su m i n relativno prosti prirodni brojevi, te neka su $R = \{r_1, r_2, \ldots, r_{\varphi(m)}\}$ i $S = \{s_1, s_2, \ldots, s_{\varphi(n)}\}$ reducirani sustavi ostataka modulo m i n, redom. Pokazat ćemo da je skup

$$T = \{nr + ms \mid r \in R \text{ i } s \in S\}$$

također reducirani skup ostataka modulo mn. Kako skup T očito ima $\varphi(m)\varphi(n)$ elemenata, slijedit će da je $\varphi(mn) = \varphi(m)\varphi(n)$; ili drugim riječima, dobit ćemo željenu multiplikativnost funkcije φ.

Prvo ćemo pokazati da za svaki $k \in T$ vrijedi $(k, mn) = 1$. U tu svrhu, pretpostavimo da za neki $k = nr + ms \in T$ postoji neki prost broj p takav da $p|(k, mn)$. Tada posebno $p|mn$, i onda, jer su m i n relativno prosti, slijedi da $p|m$ ili $p|n$. Neka naprimjer $p|m$. Tada bismo iz činjenice $p|nr + ms$ imali da $p|nr$, odnosno $p|r$; posljednje jer $p \nmid n$. No to bi značilo da $p|(r, m) = 1$, što je nemoguće. Slično bismo dobili i da smo pretpostavili da $p|n$. Dakle, tako smo pokazali da su svi elementi iz skupa T relativno su prosti s mn.

Nadalje, pokazat ćemo da svaka dva broja iz skupa T međusobno nisu kongruentna. Da bismo to vidjeli, pretpostavimo suprotno, tojest da za neke $r, r' \in R$ i $s, s' \in S$ vrijedi

$$nr + ms \equiv nr' + ms' \pmod{mn}.$$

Tada bi bilo $n(r - r') + m(s - s') = k(mn)$, za neki $k \in \mathbb{Z}$. Odavde bi slijedilo da $m|n(r - r')$, odnosno zbog $(m, n) = 1$ imali bismo da $m|(r - r')$. Drugim riječima, bilo bi $r \equiv r' \pmod{m}$. No kako su $r, r' \in R$ mora vrijediti $r = r'$, što nije. Sasvim aanalogno bismo dobili i da je $s = s'$.

Još nam preostaje pokazati da je svaki cijeli broj relativno prost s mn kongruentan modulo mn nekom elementu iz skupa T. Za to, neka je $k \in \mathbb{Z}$ i $(k, mn) = 1$. Kako su m i n relativno prosti, k možemo napisati kao $k = nr' + ms'$, za neke $r', s' \in \mathbb{Z}$. Nadalje, pretpostavimo sada da postoji prost broj p takav da $p|m$ i $p|r'$. Tada bi p bio zajednički djelitelj od mn i od k, što je kontradikcija s prepostavkom da su mn i k relativno prosti. To nam pokazuje da vrijedi $(r', m) = 1$ i r' je kongruentan modulo m nekom od elemenata iz skupa R. Analognim razmatranjem dobivamo da je s' kongruentan modulo n nekom od elemenata iz skupa S. To znači da sada r' i s' možemo napisati ovako: $r' = r + am$ i $s' = s + bn$, za neke a i b. Slijedi kongruencija

$$k = nr' + ms' = n(r + am) + m(s + bn) = nr + ms + mn(a + b) \equiv nr + ms \pmod{mn}.$$

Tako je teorem u potpunosti dokazan. □

Kao posljedicu gornjeg teorema i prijašnje leme, dobivamo i najavljenu formulu.

Teorem 1.2.10. *Ako je dan prirodan broj $n = p_1^{a_1} \cdots p_k^{a_k}$, tada je*

$$\varphi(n) = n \prod_{i=1}^{k} (1 - 1/p_i).$$

Dokaz. Iz prethodnog Teorema 1.2.9 slijedi

$$\begin{aligned}\varphi(n) &= \varphi(p_1^{a_1}) \cdot \varphi(p_2^{a_2}) \cdots \varphi(p_k^{a_k}) \\ &= (p_1^{a_1} - p_1^{a_1-1})(p_2^{a_2} - p_2^{a_2-1}) \cdots (p_k^{a_k} - p_k^{a_k-1}) \\ &= p_1^{a_1}(1 - 1/p_1) \cdots p_k^{a_k}(1 - 1/p_k) = p_1^{a_1} \cdots p_k^{a_k} \cdot (1 - 1/p_1) \cdots (1 - 1/p_k) \\ &= n \prod_{i=1}^{k} (1 - 1/p_i).\end{aligned}$$

□

Poglavlje 2

Skup prostih brojeva $\mathcal{P}$

Problem distribucije prostih brojeva, u skupu prirodnih brojeva $\mathbb{N}$, izuzetno je zanimljiv, ali u isto vrijeme i nevjerojatno težak. Početak bavljenja tim problemom nalazi se u antičkoj Grčkoj, kada su dobivena dva osnovna rezultata. Prvi je da je skup prostih brojeva $\mathcal{P} \subseteq \mathbb{N}$ beskonačan, a drugi je *Osnovni teorem aritmetike*. Nakon toga, nekih dvije tisuće godina nije bilo značajnijih pozitivnih pomaka u razumijevanju spomenutog problema. No u drugoj polovici 18. stoljeća započela su neka istraživanja koja se mogu smatrati početcima moderne teorije brojeva, posebno tzv. analitičke teorije brojeva. Tu svakako treba spomenuti ime L. Eulera, kao jednog od pionira na tom polju. Ta su istraživanja doživjela puni procvat u 19. stoljeću, kada su dobivena i dva stožerna teorema. Prvi je tzv. Dirichletov teorem o prostim brojevima u aritmetičkim nizovima, koji je motiviran nekim prije dobivenim Eulerovim rezultatima. Navedimo ovdje taj teorem, tek uz napomenu kako za njegov dokaz trebaju neki preliminarni rezultati o tzv. karakterima abelovih grupa, kao i neki pojmovi i rezultati iz kompleksne analize, posebno o tzv. Dirichletovim redovima.

Teorem (**Dirichletov teorem**) *Neka su $d, a \in \mathbb{N}$ relativno prosti. Tada postoji beskonačno mnogo prostih brojeva oblika*

$$a + dn, \qquad n \in \mathbb{N}.$$

Štoviše, red $\sum \frac{1}{p}$, recipročnih vrijednosti prostih brojeva iz navedenog aritmetičkog niza, divergira; tojest,

$$\sum_{p \equiv a \pmod{d}} \frac{1}{p} = \infty.$$

Drugi je rezultat tzv. *Teorem o prostim brojevima*, o kojem će biti više riječi u odjeljku (2.2). Naglasimo kako je dokaz tog teorema podosta zahtjevan, i koristi neke od glavnih rezultata iz kompleksne analize, posebno o tzv. beskonačnim produktima brojeva i funkcija. Malo više detalja o svemu ovdje rečenom može se naći npr. u [6].

2.1 Neki elementarni dokazi beskonačnosti skupa $\mathcal{P}$

Svrha ovog potpoglavlja je pokazati koliko je širok spektar dokaza tvrdnje da je skup prostih brojeva $\mathcal{P}$ beskonačan. Svaki od njih dati će nam jasniju sliku o prirodi skupa $\mathcal{P}$, ali i samog prstena cijelih brojeva $\mathbb{Z}$. Počinjemo s osnovnim teoremom o beskonačnosti skupa prostih brojeva, za koji ćemo pokazati nekoliko varijacija dokaza.

Teorem 2.1.1. *Skup prostih brojeva je beskonačan.*

Dokazivanje ovog teorema najprije počinjemo sa standardnim Euklidovim dokazom.

Dokaz. Prepostavimo da postoji konačno mnogo prostih brojeva $p_1, p_2, \ldots, p_n$. Svaki od navedenih brojeva je pozitivan, pa možemo definirati $N \in \mathbb{Z}_+$ kao

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

Iz prethodno definiranog očito je da broj N ima dekompoziciju na proste faktore, pa postoji prost broj p takav da $p|N$, tojest

$$p|p_1 p_2 \cdots p_n + 1$$

Pretpostavili smo da je skup prostih brojeva konačan, pa vrijedi da je $p = p_i$, za neki $i = 1, 2, \ldots, n$. No, tada $p|p_1 p_2 \cdots p_n$, a kako za svaka dva susjedna prosta broja vrijedi da su međusobno relativno prosti, slijedi da p ne može dijeliti $p_1 p_2 \cdots p_n + 1$. Došli smo do kontradikcije, pa slijedi da je skup $\mathcal{P}$ beskonačan. □

Posebno u ovom odjeljku dajemo tri nova dokaza koja su varijacije na Euklidov dokaz, dat uz Teorem 2.1.1. Primijetimo kako niti jedan od tih dokaza ne koristi analizu.

Prvi dokaz koji navodimo koristi sumu $\sum_{p\in\mathcal{P}} \frac{1}{p}$, uz početnu pretpostavku da je skup $\mathcal{P}$ konačan; što će nam, jasno, dati željenu kontradikciju.

Dokaz. Pretpostavimo da je $\mathcal{P}$= $\{p_1, \ldots, p_n\}$ skup svih prostih brojeva, te neka je $N = p_1 p_2 \cdots p_n$. Definirajmo

$$a = \sum_{i=1}^{n} \frac{1}{p_i}; \qquad \text{tada je } \; aN = \sum_{i=1}^{n} \frac{N}{p_i}.$$

Iz definicije vidimo da je aN cijeli broj, pa postoji neki prost broj $p_j \in \mathcal{P}$ koji je njegov djelitelj. S druge strane, očito $p_j|\frac{N}{p_i}$ za svaki $i \neq j$. I onda slijedi da taj p_j mora dijeliti i broj $\frac{N}{p_j} = aN - \sum_{i\neq j} \frac{N}{p_i}$. Došli smo do kontradikcije; pa slijedi da je skup $\mathcal{P}$ beskonačan. □

Sljedeći je dokaz preko Eulerove funkcije φ. Podsjetimo se da za $k \in \mathbb{N}$, definiramo

$$\varphi(k) := \text{card}\{x \in \mathbb{N} \mid x < k \ \ \& \ \ (x,k) = 1\}.$$

Nadalje, ta je funkcija multiplikativna; tojest, vrijedi $\varphi(ab) = \varphi(a)\varphi(b)$ za bilo koje relativno proste brojeve $a, b \in \mathbb{N}$.

Dokaz. Ponovo pretpostavimo da je $\mathcal{P} = \{p_1, \ldots, p_n\}$ skup svih prostih brojeva, te da je $N = p_1 p_2 \cdots p_n$. Za $p_1 = 2$ imamo $\varphi(p_1) = 1$, i očito je $\varphi(p_i) = p_i - 1$ za svaki $i \geqslant 2$.

Ako je sada $1 < n < N$, tada postoji neki prost broj $p_j \in \mathcal{P}$ takav da $p_j | n$. To onda znači da je taj p_j djelitelj i od n i od N, za svaki n, što posebno znači da je NZD $(n, N) \neq 1$. Slijedi, po definiciji funkcije φ, da je $\varphi(N) = 1$. S druge pak strane, zbog multiplikativnosti imamo da je

$$\varphi(N) = \varphi(p_1 \cdots p_n) = \varphi(p_1) \cdots \varphi(p_n) = (p_1 - 1) \cdots (p_n - 1) > 1;$$

što je i opet kontradikcija. □

Posljednji dokaz koji dajemo je preko polinoma s cjelobrojnim koeficijentima. Standardno, ovdje s $\mathbb{Z}[x]$ označavamo prsten polinoma s koeficijentima iz $\mathbb{Z}$.

Lema 2.1.2. *Za svaki nekonstantan polinom $f(x) \in \mathbb{Z}[x]$, skup svih prostih brojeva koji su djelitelji cijelih brojeva u skupu $\{f(k) \mid k \in \mathbb{N}_0\}$ je beskonačan. Posebno, onda slijedi da je i $\mathcal{P}$ beskonačan skup.*

Dokaz. Neka je dan polinom

$$f(x) = a_r x^r + a_{r+1} x^{r+1} + \cdots + a_m x^m, \qquad a_i \in \mathbb{Z};$$

ovdje je $m \geqslant 1$ i $a_m \neq 0$, te $0 \leqslant r \leqslant m$ takav da je $a_r \neq 0$. Označimo $S_f = \{f(k) \mid k \in \mathbb{N}_0\}$, i onda s U_f skup svih prostih brojeva p za koje postoji neki $f(k) \in S_f$ takav da $p \mid f(k)$. Pretpostavimo sada da je skup U_f konačan; tojest, da je $U_f = \{p_1, \ldots, p_n\}$. Kao i u prethodna dva dokaza, stavimo $N = p_1 \cdots p_n$. Najprije pogledajmo slučaj kada je $r < m$, i onda definirajmo polinom

$$g(x) = a_r + a_{r+1} x + \ldots + a_m x^{m-r}.$$

Kako je $x^r \cdot g(x) = f(x)$, i onda $k^r \cdot g(k) = f(k)$ za svaki $k \in \mathbb{N}_0$, očito za pripadne skupove U_f i U_g imamo inkluziju $U_g \subseteq U_f$. Znači, ako pokažemo da je U_g beskonačan skup, imat ćemo da je i U_f također beskonačan. Drugim riječima, za ovaj slučaj koji promatramo mi zapravo bez smanjenja općenitosti možemo pretpostaviti da je u danom polinomu $f(x)$ slobodan član $a_0 \neq 0$. Sada, uz tu pretpostavku, izaberimo $t \in \mathbb{N}$ takav da p_i^t ne dijeli $a_0 = f(0)$ za svaki $i = 1, \ldots, n$. Naime, kako su svi prosti djelitelji od $f(0)$ u skupu U_f,

imamo da se taj $f(0) = a_0$ može napisati u obliku $a_0 = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$, za neki $\alpha_i \in \mathbb{N}_0$. I onda je dovoljno uzeti t takav da je $t > \alpha_i$, za svaki i. No onda naravno imamo da $a_0 \mid N^t$; tojest, $N^t = a_0 b$ za neki $b \in \mathbb{Z}$. Promatrajmo sada za $k \geqslant 1$ brojeve

$$f(kN^{2t}) = a_0 + \sum_{j=1}^{m} a_j k^j (N^t)^{2j} = a_0 + \sum_{j=1}^{m} a_j k^j (a_0 b)^{2j} = a_0 \Big(\sum_{j=1}^{m} a_j k^j b^{2j} a_0^{2j-1} + 1 \Big).$$

Neka je sada k dovoljno velik tako da za cijeli broj

$$M = M_k := \sum_{j=1}^{m} a_j k^j b^{2j} a_0^{2j-1} + 1$$

imamo $\mid M \mid > 1$; što očito možemo. Konačno, uzmimo bilo koji prost broj p koji je djelitelj od M. Ekvivalentno, taj p ne dijeli $a_0 b$, jer bismo u suprotnom imali i da taj p dijeli razliku

$$M - \sum_{j=1}^{m} a_j k^j b (a_0 b)^{2j-1} = 1,$$

što je nemoguće. Znači, p ne dijeli $a_0 b = N^t = p_1^t \cdots p_n^t$; što konačno daje da $p \notin U_f$, a to je kontradikcija. Drugi je slučaj $r = m$; tojest, $f(x) = a_m x^m$. Sada izaberimo $t \in \mathbb{N}$ tako da p_i^t ne dijeli $f(1) = a_m$ za svaki i. Isto kao u prvom slučaju imamo $N^t = a_0 b$, za neki b. Sada gledamo

$$f(N^{2t} + 1) = a_m (N^{2t} + 1)^m.$$

Jasno je da $N^{2t} + 1 > 1$, te da svaki prost djelitelj p od $N^{2t} + 1$ nije u skupu U_f; što je kontradikcija. Time je lema dokazana. □

2.2 Analitički dokaz beskonačnosti skupa $\mathcal{P}$

Još uvijek ne postoji egzaktna formula uz pomoć koje bi bilo moguće odrediti n-ti prosti broj, što predstavlja jedan od najvećih otvorenih matematičkih problema. Podjednako težak problem je i određivanje načina i gustoće raspodjele prostih brojeva u skupu $\mathbb{N}$. Postavlja se iduće pitanje: "Koliki je udio prostih brojeva na nekom proizvoljno odabranom intervalu?"

Označimo s $\pi(x)$ broj prostih brojeva p takvih da je $p \leq x$, za $x \in [2, \infty)$; tojest,

$$\pi(x) = \text{card}\{p \in \mathcal{P} \mid p \leq x\}.$$

Tako dobivamo funkciju

$$\pi : [2, \infty) \to \mathbb{N}.$$

Jedan od prvih velikih problema matematike 19. stoljeća bio je razumijeti ponašanje te funkcije, odnosno dobiti informaciju o njenom asimptotskom ponašanju. Kao kruna tih nastojanja dobiven je sljedeći netrivijalan rezultat koji se standardno zove *Teorem o prostim brojevima*.

Teorem 2.2.1. *Za funkciju π vrijedi*

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\ln x} = 1.$$

Ili drugačije rečeno, za dovoljno velike vrijednosti x, imamo asimptotsko ponašanje funkcije π dano kao

$$\pi(x) \sim \frac{x}{\ln x}.$$

Kako bismo ilustrirali gornji teorem, dajemo sljedeću tablicu, koja daje relevantne numeričke podatke za funkcije promatrane u teoremu:

n	$\pi(n)$	$\frac{n}{\ln(n)}$	$\frac{\pi(n)}{\frac{n}{\ln(n)}}$
10	4	4.34294	0.921
100	25	21.7147	1.151
1000	168	144.765	1.160
10000	1229	1085.74	1.131
100000	9592	8685.89	1.104
1000000	78498	72382.4	1.084
10000000	664579	620421.0	1.071
100000000	5761455	5428681.02	1.061
1000000000	50847534	48254942.4	1.053
10000000000	455052511	434294481.9	1.047

Kako smo već spomenuli, sam dokaz Teorema o prostim brojevima je dosta kompliciran, i mi ga ovdje nismo u stanju dokazati; ali pokazat ćemo neke vezane zanimljive rezultate o ponašanju funkcije π. No za informaciju tek kažimo kako su prvi detaljan dokaz, nakon stoljeća napora raznih matematičara, koncem 19. stoljeća dali J. Hadamard i C. J. de la Valée Poussin. Pritom se ključnom pokazala uloga B. Riemanna, koji je 1959. u svom jedinom radu iz teorije brojeva, pod naslovom *Uber die Anzahl der Primzahlen unter einer gegebenen Grösse*, skicirao program i ideje dokaza. (Taj se rad pokazao od fundamentalne važnosti za cijelu matematiku, do današnjih dana.) Konačno, svakako treba reći i to da su prvu slutnju o tvrdnji teorema, neovisno jedan o drugome, dali C. F. Gauss i A. M. Legendre na prijelazu iz 18. u 19. stoljeće. Njihova je slutnja bila utemeljena heuristikom.

Naime, oni su promatrali vrijednosti $\pi(n)$, za velike n-ove; onako kako je to prikazano u gornjoj tablici. No, nisu imali ideje kako bi se to i precizno dokazalo.

Naš glavni cilj u ovom odjeljku je dokazati sljedeći teorem, koji je sam za sebe vrlo zanimljiv. Njega je prvi dokazao Euler 1737. godine, uz napomenu kako je to još jedan dokaz beskonačnosti skupa $\mathcal{P}$. Mi ćemo dati dva dokaza, od kojih je prvi direktan, dok drugi uvodi u igru Riemannovu zeta funkciju.

Teorem 2.2.2. *Red $\sum_{p\in\mathcal{P}} \frac{1}{p}$ divergira.*

Prvi dokaz ovog teorema dajemo onako kako je to napravljeno u članku [3]; zapravo mi slijedimo [2, Theorem 1.13]. Najprije jedna lema.

Lema 2.2.3. *Neka je realan broj $\Omega \geqslant 1$ proizvoljan. Tada red*

$$\sum_{n=1}^{\infty} \frac{1}{1+n\Omega}$$

divergira.

Dokaz. Funkcija $f : [1, +\infty) \to \mathbb{R}$, $f(x) = \frac{1}{1+\Omega x}$, očito je strogo padajuća. Onda, za bilo koji prirodan broj $N > 1$, očito imamo

$$I_N := \int_1^N f(x)dx < \sum_{n=1}^{N} \frac{1}{1+n\Omega}.$$

Ali,

$$I_N = \int_1^N \frac{dx}{1+\Omega x} = \frac{1}{\Omega} \ln(1+\Omega x)\Big|_1^N = \frac{1}{\Omega} \ln \frac{1+\Omega N}{1+\Omega}.$$

Još primijetimo da je npr. $\frac{1+\Omega N}{1+\Omega} > \frac{N}{2}$, i zato je

$$I_N > \frac{1}{\Omega} \ln \frac{N}{2}.$$

Budući da je $\lim_{N\to\infty} \ln \frac{N}{2} = +\infty$, zaključujemo da je i $\lim_{N\to\infty} I_N = +\infty$. I tako slijedi lema. □

Za daljnje potrebe numerirajmo proste brojeve $p \in \mathcal{P}$ po veličini; tojest, $p_1 = 2, p_2 = 3, p_3 = 5, \ldots$ Znači,

$$\mathcal{P} = \{p_1, p_2, p_3, \ldots\}.$$

Sada dajemo najavljeni dokaz Teorema 2.2.2.

Dokaz. Pretpostavimo suprotno, da dani red konvergira. Onda posebno postoji $m \in \mathbb{N}$ takav da

$$\sum_{k=m+1}^{\infty} \frac{1}{p_k} < \frac{1}{2}.$$

Označimo $\Omega = p_1 \cdots p_m$, i onda gledajmo brojeve $1 + n\Omega$, za $n \in \mathbb{N}$. Jasno, niti jedan od tih brojeva nije djeljiv s niti jednim prostim brojem iz skupa $\{p_1, \ldots, p_m\}$. To znači da su svi prosti djelitelji brojeva $1 + n\Omega$ u skupu $\{p_{m+1}, p_{m+2}, \ldots\}$. No to onda znači da za svaki $N \geqslant 1$ vrijedi nejednakost

$$\sum_{n=1}^{N} \frac{1}{1 + n\Omega} \leqslant \sum_{t=1}^{\infty} \Big(\sum_{k=m+1}^{\infty} \frac{1}{p_k} \Big)^t. \tag{2.1}$$

Naime, pretpostavimo da je, za neki, n,

$$1 + n\Omega = p_{m+1}^{\alpha_{m+1}} \cdot p_{m+2}^{\alpha_{m+2}} \cdots;$$

jasno, to je konačan produkt. Zapravo, ovako za svaki $n \in \mathbb{N}$ dobivamo niz brojeva $(\alpha_{m+1}, \alpha_{m+2}, \ldots)$, gdje su $\alpha_j \in \mathbb{N}_0$, i od nekog mjesta nadalje su svi α_i - ovi jednaki 0. Ekvivalentno, funkcija koja prirodni broj n preslikava u odgovarajući niz $(\alpha_{m+1}, \alpha_{m+2}, \ldots)$ je injekcija. Sada, recimo da za konkretan n imamo

$$1 + n\Omega = p_{m+1}^{\alpha_{m+1}} \cdot p_{m+2}^{\alpha_{m+2}} \cdots p_{m+l}^{\alpha_{m+l}},$$

za neki $l \in \mathbb{N}_0$. Stavimo

$$t = \alpha_{m+1} + \cdots + \alpha_{m+l}.$$

Onda očito suma

$$\Big(\sum_{k=m+1}^{\infty} \frac{1}{p_k} \Big)^t = \Big(\frac{1}{p_{m+1}} + \frac{1}{p_{m+2}} + \cdots \Big)^t$$

sadrži sumand

$$\Big(\frac{1}{p_{m+1}} \Big)^{\alpha_{m+1}} \cdot \Big(\frac{1}{p_{m+2}} \Big)^{\alpha_{m+2}} \cdots \Big(\frac{1}{p_{m+l}} \Big)^{\alpha_{m+l}} = \frac{1}{1 + n\Omega};$$

što pokazuje da (2.1) doista vrijedi. I sada primijetimo da je desna strana u (2.1) manja ili jednaka od sume geometrijskog reda

$$\sum_{t=1}^{\infty} \Big(\frac{1}{2} \Big)^t = 1.$$

Za posljedicu imamo da je $\sum_{n=1}^{N} \frac{1}{1+n\Omega} \leqslant 1$, za svaki $n \in \mathbb{N}$; i onda da je i

$$\sum_{n=1}^{\infty} \frac{1}{1 + n\Omega} = \lim_{N \to \infty} \sum_{n=1}^{N} \frac{1}{1 + n\Omega} \leqslant 1.$$

No to je u kontradikciji s Lemom 2.2.3. Zaključujemo da promatrani red divergira. □

Sada ćemo dati drugi dokaz Teorema 2.2.2, koji uvodi Riemannovu zeta funkciju i tzv. Eulerove produkte; pojmove od centralne važnosti u analitičkoj teoriji brojeva.

Definicija 2.2.4. *Za realnu varijablu $s > 1$ definiramo Riemannovu zeta funkciju redom*

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

Zapravo Riemannova zeta funkcija je realna funkcija

$$\zeta : (1, +\infty) \to \mathbb{R}.$$

Naglasimo kako je zapravo od velike važnosti promatrati zeta funkciju kao kompleksnu funkciju kompleksne varijable $s \in \mathbb{C} \setminus \{1\}$; to nama ovdje neće trebati.

Nadalje, sjetimo se da harmonijski red $\sum_{n=1}^{\infty} \frac{1}{n}$ divergira; vidi Lemu 2.2.3. To ima za posljedicu da uzimanjem jednostranog limesa u $s = 1$, zdesna, imamo

$$\lim_{s \to 1^+} \zeta(s) = \infty. \tag{2.2}$$

Isto tako, primjenom osnovnog teorema aritmetike odmah slijedi da je

$$\zeta(s) = \prod_{p \in \mathcal{P}} \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots\right).$$

Međutim, teorem o geometrijskom redu nam daje

$$1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots = \frac{1}{1 - p^{-s}}.$$

Kao posljedicu gore navedenoga, dobivamo sljedeći korolar.

Korolar 2.2.5. *Riemannova zeta funkcija može se napisati kao (beskonačan) produkt*

$$\zeta(s) = \prod_{p \in \mathcal{P}} \left(\frac{1}{1 - p^{-s}}\right);$$

to je tzv. prikaz zeta funkcije kao ***Eulerovog produkta****.*

Primijetimo i ovo; što smo već više puta dokazivali. Kad bi skup $\mathcal{P}$ bio konačan, onda bi za svaki $s \in [1, +\infty)$ i broj $\zeta(s)$ bio konačan; kao produkt od konačno faktora $\frac{1}{1-p^{-s}}$. No, to je u kontradikciji s (2.2), kada uzmemo da $s \to 1^+$. Zaključak je i ovdje da je $\mathcal{P}$ beskonačan skup.

Sada smo spremni za najavljeni drugi dokaz Teorema 2.2.2

Dokaz. Znajući da je Taylorov razvoj

$$\ln\left(\frac{1}{1-x}\right) = \sum_{n=1}^{\infty} \frac{x^n}{n},$$

te da po teoremu o geometrijskom redu imamo

$$\sum_{n=1}^{\infty} x^n = \frac{x}{1-x},$$

za $0 < x < 1$, slijedi

$$\ln\left(\frac{1}{1-x}\right) = \sum_{n=1}^{\infty} \frac{x^n}{n} < \sum_{n=1}^{\infty} x^n = \frac{x}{1-x}.$$

Odavde, koristeći činjenicu da je $\frac{x}{1-x} < 2x$ za $0 < x < \frac{1}{2}$, dobivamo nejednakost

$$\ln\left(\frac{1}{1-x}\right) < 2x, \qquad \text{za } 0 < x < \frac{1}{2}.$$

Sada, logaritmirajući Eulerov produkt, dobivamo

$$\ln(\zeta(s)) = \sum_{p\in\mathcal{P}} \ln\left(\frac{1}{1-p^{-s}}\right) < 2\sum_{p\in\mathcal{P}} p^{-s}.$$

Konačno, kad bi red $\sum_{p\in\mathcal{P}} \frac{1}{p}$ konvergirao, onda bismo imali i da red $\sum_{p\in\mathcal{P}} p^{-s}$ konvergira, za svaki $s > 1$; ovdje koristimo da je $p^{-s} < \frac{1}{p}$, i onda usporedni kriterij konvergencije za redove. Kao posljedicu bismo imali da je limes

$$\lim_{s\to 1^+} \ln(\zeta(s)) \quad \text{konačan.}$$

No, to je ponovno u kontradikciji s (2.2). □

Primijetimo da prethodni rezultat upućuje na činjenicu da je gustoća niza prostih brojeva prilično velika. Usporedno s gustoćom niza kvadrata $\{1, 4, 9, 16, \ldots\}$, gustoća skupa prostih brojeva je veća. Podsjetimo se da $\sum_{n=1}^{\infty} \frac{1}{n^2}$ konvergira, dok smo mi dokazali da $\sum_p \frac{1}{p}$ divergira.

Kao posljednji rezultat u ovom odjeljku, odredit ćemo donju među za $\pi(x)$; tojest za broj prostih brojeva koji su manji ili jednaki x. Nakon toga, slijedi još jedan dokaz o beskonačnosti skupa prostih brojeva.

Teorem 2.2.6. *Za svaki prirodni broj $x \geqslant 2$ imamo*

$$\pi(x) > \ln\ln x.$$

Dokaz. Neka je $p_1, \ldots, p_k, \ldots$ rastući niz prostih brojeva. Iz [5, Lemma 3.1.2.1] vrijedi da je $p_n < 2^{2^{n-1}}$ za svaki $n > 1$. Tada, za dani x, odaberimo k takav da vrijedi

$$2^{2^{k-1}} \leqslant x < 2^{2^k}.$$

Kako je $p_k < 2^{2^{k-1}}$, te je funkcija π rastuća, imamo

$$k \leqslant \pi(2^{2^{k-1}}) \leqslant \pi(x).$$

Iz $x < 2^{2^k} < e^{e^k}$ slijedi

$$\ln \ln x < k \leqslant \pi(x).$$

□

Koristeći osnovni teorem aritmetike, možemo dobiti i jos jednu formu donje međe za $\pi(x)$, koja je slična onoj u prethodnom teoremu.

Teorem 2.2.7. *Za svaki prirodni broj $x \geqslant 21$,vrijedi*

$$\pi(x) > \frac{\ln x}{2 \ln \ln x}.$$

Dokaz. Neka je x fiksan, te neka su p_i, za $i = 1, 2, \ldots, \pi(x)$, svi prosti brojevi manji ili jednaki x. Tada iz osnovnog teorema aritmetike slijedi da je broj cjelobrojnih rješenja nejednakosti

$$\prod_{p_i} p_i^{e_i} \leqslant x$$

za $e_i \geqslant 0$, upravo jednak x. S druge strane, broj rješenja je umnožak broja odabira za svaki e_i. Kako za $p_i^{e_i} \leqslant x$; tojest, $e_i \leqslant \frac{\ln x}{\ln p_i}$ imamo

$$e_i \leqslant 1 + \frac{\ln x}{\ln p_i} \leqslant 1 + \frac{\ln x}{\ln 2} = \frac{\ln 2 + \ln x}{\ln 2} < \ln 2 + \ln x < (\ln x)^2$$

za $x > 20$, slijedi

$$x \leqslant \prod_{p_i} \left(1 + \frac{\ln x}{\ln p_i}\right) < \left((\ln x)^2\right)^{\pi(x)},$$

što nas vodi do konačnog rezultata, odnosno $\pi(x) > \frac{\ln x}{2 \ln \ln x}$. □

Korolar 2.2.8. *$\pi(x) \to \infty$ kada $x \to \infty$. Posebno, skup prostih brojeva je beskonačan.*

Dokaz. Iz Teorema 2.2.6 za $x \geq 2$ vrijedi nejednakost $\pi(x) > \ln \ln x$. Tada za $x \to \infty$ vrijedi nejednakost $\pi(x) \to \infty$. □

Poglavlje 3

Fermatovi i Mersennovi brojevi

3.1 Fermatovi brojevi

U sljedećim odjeljcima istražit ćemo vezu skupa prostih brojeva $\mathcal{P}$ sa nekoliko specijalnih nizova cijelih brojeva. Prvi takav niz koji ćemo promatrati je skup Fermatovih brojeva.

Definicija 3.1.1. ***Fermatovi brojevi*** *definirani su nizom (F_n) pozitivnih cijelih brojeva na sljedeći način:*

$$F_n = 2^{2^n} + 1, \qquad n = 1, 2, 3, \ldots$$

Posebno, ukoliko je F_m prost broj, naziva se ***Fermatov prost broj****.*

Fermatova slutnja bila je da su svi brojevi u ovom nizu prosti. Zapravo, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ i $F_4 = 65537$ su prosti brojevi, ali F_5 je složen, tojest

$$F_5 = 641 \cdot 6700417.$$

Još je uvijek otvoreno pitanje postoji li beskonačno mnogo Fermatovih prostih brojeva. Slutnja je da ih ima konačno mnogo. No ukoliko je broj oblika $2^n + 1$ prost za neki cijeli broj n, tada on mora biti Fermatov prost broj. Zapravo, imamo ovaj malo jači rezultat.

Teorem 3.1.2. *Ako je $a \geqslant 2$ i $a^n + 1$ prost, tada je a paran broj i $n = 2^m$ za neki nenegativan cijeli broj m. Posebno, ukoliko je $p = 2^k + 1$ prost broj, tada je $k = 2^n$ za neki n, a taj p je Fermatov prost broj.*

Dokaz. Ukoliko je a neparan broj, tada je $a^n + 1$ paran, dakle nije prost broj. Pretpostavimo sada da je a paran broj, te da je n oblika $n = kl$ pri čemu je k neparan i $k \geq 3$. Tada vrijedi

$$a^{kl} + 1 = (a^l + 1)(a^{(k-1)l} - a^{(k-2)l} + \cdots + 1).$$

Budući je drugi faktor u desnoj strani gornje jednakosti očito prirodan broj veći od 1, imamo da je $a^n + 1 = a^{kl} + 1$ složen broj; što je kontradikcija s pretpostavkom teorema. Zaključak je da ukoliko $a^n + 1$ je prost, onda nužno n nema neparnih djelitelja; tojest, n mora biti neka potencija broja 2.
Jasno, druga tvrdnja teorema je specijalan slučaj kada stavimo $a = 2$. □

Koristeći Fermatove brojeve dat ćemo još jedan dokaz beskonačnosti skupa prostih brojeva u $\mathbb{N}$. Za to nam je potrebna sljedeća lema.

Lema 3.1.3. *Neka je (F_n) niz Fermatovih brojeva. Ako je $m \neq n$, onda su F_n i F_m relativno prosti, tojest $(F_n, F_m) = 1$.*

Dokaz. Prvo primijetimo da za bilo koji $x \in \mathbb{R}$ i paran $k \in \mathbb{N}$ vrijedi jednakost

$$x^k - 1 = (x + 1)(x^{k-1} - x^{k-2} + \cdots - 1);$$

to se odmah vidi množenjem faktora na desnoj strani i sređivanjem dobivenog izraza.
Pretpostavimo sada da je npr. $n > m$, te da za neki $1 \neq d \in \mathbb{N}$ imamo da $d|F_n$ i $d|F_m$. Tada vrijedi

$$\frac{F_n - 2}{F_m} = \frac{2^{2^n} - 1}{2^{2^m} + 1} = (2^{2^m})^{2^{n-m}-1} - (2^{2^m})^{2^{n-m}-2} + \cdots - 1;$$

to dobijemo tako da u gornjoj jednakosti stavimo $x = 2^{2m}$ i $k = 2^{n-m}$. Slijedi da $F_m|F_n - 2$, a onda iz činjenice da $d|F_m$ imamo i da $d|F_n - 2$. Kako $d|F_n$, tada mora vrijediti i da $d|2$; tj. $d = 2$. No Fermatovi brojevi su neparni pa je to nemoguće. Time je lema dokazana. □

Napomena 3.1.4. *Neka je $a \in \mathbb{N}$, i onda definirajmo niz brojeva $A_n = a^{2^n} + 1$. Tada analogno kao u prethodnoj lemi, vidimo da vrijedi:*

1. *Ako je $n > m$, tada $a^{2^m} + 1|a^{2^n} - 1$; tj. $A_m|A_n - 2$*
2. *Imamo $(A_n, A_m) = 1$ ukoliko je a paran i $n \neq m$, odnosno $(A_n, A_m) = 2$ ukoliko je a neparan i $n \neq m$.*

Slijedi najavljeni novi dokaz Teorema 2.1.1.

Dokaz. Kako su elementi beskonačnog niza (F_n) u parovima relativno prosti, a svaki F_n mora imati barem jednog prostog djelitelja, odmah slijedi da skup $\mathcal{P}$ mora biti beskonačan.
□

3.2 Mersennovi brojevi

Sada ćemo promatrati niz tzv. Mersennovih brojeva.

Definicija 3.2.1. ***Mersennovi brojevi*** *su niz* (M_n) *pozitivnih cijelih brojeva definirani na sljedeći način:*

$$M_n = 2^n - 1, \qquad n = 1, 2, 3, \ldots$$

Posebno, ukoliko je M_n *prost broj, naziva se* ***Mersennov prost broj****.*

Mersennove brojeve uveo je francuski klerikalac i matematičar M. Mersenne, koji je pokazao da ako je M_n prost broj, tada i n mora biti prost. Također, on je tvrdio da je M_n prost broj za $n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$ i složen za sve ostale. Danas je poznato da M_{67} i M_{257} nisu prosti brojevi, dok M_{61} i M_{89} jesu. Nadalje, M_p je prost broj za nekoliko velikih eksponenata p, te potraga za sve većim i većim prostim brojevima općenito uključuje Mersennove brojeve. Kao i kod Fermatovih brojeva, još uvijek stoji otvoreno pitanje o beskonačnosti skupa Mersennovih brojeva. Međutim, slutnja je da Mersennovih brojeva ima beskonačno mnogo. Do danas su poznata 44 Mersennova broja, od kojih je najveći $M_{32582657}$. Više detalja može se naći na web-stranici [1].

Teorem 3.2.2. *Pretpostavimo da su* a *i* n *pozitivni cijeli brojevi. Ukoliko je* $a^n - 1$ *prost broj, tada je* $a = 2$ *i* n *je prost broj. Posebno, ako je Mersennov broj* M_n *Mersennov prost broj, tada je* n *prost.*

Dokaz. Pretpostavimo da je $a \geqslant 3$. Iz jednakosti

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

slijedi da $a - 1 | a^n - 1$. Pa ukoliko je $a^n - 1$ prost broj, tada je $a = 2$. Nadalje, dokazujemo drugi dio tvrdnje teorema. Kada bi bilo $n = kl$, tako da $2 \leqslant k, l < n$, tada bismo imali

$$2^k - 1 | 2^n - 1.$$

Dakle, ukoliko je $2^n - 1$ prost broj, onda i n mora biti prost. □

U skladu s temom ovog poglavlja, Mersennove brojeve koristit ćemo u još jednom dokazu beskonačnosti skupa prostih brojeva $\mathcal{P}$.

Lema 3.2.3. *Za bilo koji par Mersennovih brojeva* M_n, M_m *vrijedi*

$$(M_m, M_n) = (2^m - 1, 2^n - 1) = 2^{(m,n)} - 1.$$

Dokaz. Trivijalno za $m = n$ ili $m = 1$ ili $n = 1$. Pretpostavimo onda da je $n > m > 1$. Iz Teorema 1.1.7 primijenjenog na m, n imamo

$$\begin{aligned} n &= mq_0 + r_1, \\ m &= r_1q_1 + r_2, \\ &\cdots \\ r_{s-2} &= r_{s-1}q_{s-1} + r_s, \\ r_{s-1} &= r_sq_s, \end{aligned}$$

za neke $q_i, r_j \in \mathbb{N}$. Dakle, imamo

$$r_s = (m, n),$$

najveća zajednička mjera brojeva m i n. Odavde slijede jednakosti

$$\begin{aligned} 2^n - 1 &= 2^{mq_0+r_1} - 1 = 2^{r_1}(2^{q_0m} - 1) + (2^{r_1} - 1), \\ 2^m - 1 &= 2^{r_1q_1+r_2} - 1 = 2^{r_2}(2^{q_1r_1} - 1) + (2^{r_2} - 1), \\ &\cdots \\ 2^{r_{s-2}} - 1 &= 2^{r_{s-1}q_{s-1}+r_s} - 1 = 2^{r_s}(2^{q_{s-1}r_{s-1}} - 1) + (2^{r_s} - 1), \\ 2^{r_{s-1}} - 1 &= 2^{r_sq_s} - 1 = (2^{r_s} - 1)(2^{r_s(q_s-1)} + \cdots + 1). \end{aligned} \tag{3.1}$$

Također vrijedi sljedeće:

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

Iz posljednje jednakosti i zadnja dva retka u (3.1) odmah slijedi

$$2^{r_s} - 1 | 2^{r_{s-1}} - 1 \qquad \text{i} \qquad 2^{r_s} - 1 | 2^{r_{s-2}} - 1.$$

Korak po korak, postupajući analogno, dobivamo da

$$2^{r_s} - 1 | 2^{r_i} - 1, \qquad \text{za } i = s - 1, s - 2, \ldots, 1.$$

I na kraju konačno

$$2^{r_s} - 1 | 2^m - 1 \qquad \text{i} \qquad 2^{r_s} - 1 | 2^n - 1.$$

Pretpostavimo sada da je najveća zajednička mjera $d = (M_n, M_m) = (2^n - 1, 2^m - 1)$. Iz gore pokazanog, po definiciji najveće zajedničke mjere slijedi da $2^{r_s} - 1 | d$. S druge strane, ako u nizu jednakosti (3.1) idemo odozgo prema dolje, analogno rezoniranje kao prije dat će nam da

$$d | (2^{r_i} - 1), \qquad \text{za } i = 1, 2, \ldots, s.$$

Znači, posebno $d | 2^{r_s} - 1$; i onda iz toga i gore dobivenog $2^{r_s} - 1 | d$ slijedi da je

$$d = 2^{r_s} - 1 = 2^{(m,n)} - 1.$$

Time je lema dokazana. □

Sada smo u mogućnosti dati, još jedan, najavljeni novi dokaz Teorema 2.1.1.

Dokaz. Pretpostavimo da je $\mathcal{P} = \{p_1, p_2, \ldots, p_n\}$, konačan skup prostih brojeva takvih da je $2 = p_1 < p_2 < \ldots < p_n$. Tada slijedi

$$(2^{p_i} - 1, 2^{p_j} - 1) = 2^{(p_i, p_j)} - 1 = 1, \qquad \text{za} \quad i \neq j.$$

Za $i = 1, 2, \ldots, n$ svaki član $2^{p_i} - 1$ je neparan broj, te ne postoji neparni prosti broj koji je zajednički djelitelj dvaju članova. Kako skup $\mathcal{P}$ sadrži samo $n-1$ neparnih prostih brojeva, zaključujemo da mora postojati prost broj koji ne pripada tom skupu. □

Mersennovi brojevi usko su vezani uz takozvane savršene brojeve. Prije same definicije podsjetimo se da za $n \in \mathbb{N}$ sa $\sigma(n)$ označavamo zbroj svih pozitivnih djelitelja $d \in \mathbb{N}$ od n, tojest

$$\sigma(n) = \sum_{d|n, d \geqslant 1} d.$$

Definicija 3.2.4. *Broj $n \in \mathbb{N}$ je **savršen broj** ukoliko je jednak zbroju svojih pravih djelitelja, tojest*

$$\sum_{d|n, d \geqslant 1, d \neq n} d = \sigma(n) - n.$$

Primijetimo očitu ekvivalenciju:

$$n \text{ je savršen broj} \iff \sigma(n) = 2n.$$

Kao prve primjere savršenih brojeva imamo 6 i 28, jer je

$$6 = 1 + 2 + 3 \quad \text{i} \quad 28 = 1 + 2 + 4 + 7 + 14.$$

Euklid je dao prvi značajan rezultat o problemu koji su postavili Pitagorejci:

Pronaći sve savršene brojeve.

Naime, on je pronašao sve savršene parne brojeve; iako je puni dokaz te činjenice dao tek Euler nekih dvije tisuće godina kasnije.

Teorem 3.2.5. *Neka je (M_n) niz Mersennovih brojeva. Tada imamo sljedeće:*

(i) (Euklid) Ako je $M_p = 2^p - 1$ Mersennov prost broj, tada je

$$n = 2^{p-1}(2^p - 1)$$

savršen broj.

(ii) (Euler) Ako je $n \geqslant 2$ paran savršen broj, tada je $n = 2^{p-1}(2^p - 1)$ i $M_p = 2^p - 1$ je Mersennov prost broj.

Dokaz. (*i*) Pretpostavimo da je $q = 2^p - 1$ prost broj i stavimo $n = 2^{p-1}(2^p - 1)$. Tada je

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

Dakle, $\sigma(n) = 2n$, pa zaključujemo da je n savršen broj.

(*ii*) Pretpostavimo da je n savršen broj. Neka je $n = 2^t u$, gdje je u neparan broj. Budući da je najveća zajednička mjera $(2^t, u) = 1$, a σ je multiplikativna aritmetička funkcija, imamo

$$\sigma(n) = \sigma(2^t u) = \sigma(2^t)\sigma(u) = (1 + 2 + \cdots + 2^t)\sigma(u) = (2^{t+1} - 1)\sigma(u).$$

Kako je n savršen broj vrijedi $\sigma(n) = 2n$, tojest $\sigma(n) = 2(2^t u) = 2^{t+1}u$. I onda slijedi

$$2^{t+1}u = (2^{t+1} - 1)\sigma(u). \tag{3.2}$$

Iz gornje jednakosti posebno imamo da $2^{t+1}u|(2^{t+1} - 1)\sigma(u)$, i onda Euklidova lema daje $2^{t+1}|\sigma(u)$; tojest,

$$\sigma(u) = 2^{t+1}a, \tag{3.3}$$

za neki $a \in \mathbb{N}$. Kako posljedicu (3.2) i (3.3), imamo

$$u = (2^{t+1} - 1)a.$$

Broj u ima dva različita djelitelja, a i $(2^{t+1} - 1)a > a$. Njihov zbroj iznosi $2^{t+1}a = \sigma(u)$. To je moguće jedino u slučaju ako $u = (2^{t+1} - 1)a$ nema drugih djelitelja, odnosno jedino ako je $a = 1$ i $u = 2^{t+1} - 1$. Iz Teorema3.2.2 slijedi da je $p = t + 1$ prost broj, te je $2^p - 1$ Mersennov prost broj i n ima traženi oblik $n = 2^t u = 2^{p-1}(2^p - 1)$. □

Prethodni teorem nam u potpunosti daje karakterizaciju savršenih parnih brojeva, u terminima Mersennovih brojeva, no još je otvoreno pitanje postoji li savršen neparan broj.

Na kraju ovog odjeljka spomenimo, bez dokaza, rezultat koji se zove Lukas - Lehmerov test, a koji je vrlo koristan u testiranju za nalaženje velikih Mersennovih prostih brojeva, a dokaz se može pronaći u knjizi [5].

Teorem 3.2.6. *Neka je p neparan prost broj, te induktivno definirajmo niz (S_n)*

$$S_1 = 4 \quad i \quad S_n = S_{n-1}^2 - 2.$$

Tada je Mersennov broj $M_p = 2^p - 1$ Mersennov prost broj ako i samo ako M_p dijeli S_{p-1}.

3.3 Fibonaccijevi brojevi i Zlatni rez

U ovom odjeljku govorit ćemo o nizu cijelih brojeva zvanim Fibonaccijevi brojevi. Ovaj niz brojeva ima mnogo zanimljivih svojstava, a neke od njih istražit ćemo u ovom odjeljku. Tek kažimo da je zanimanje za ovaj niz brojeva, od strane amatera kao i strane matematičara, gotovo mističan. (Npr. časopis *The Fibonacci Quarterly* objavljuje isključivo rezultate vezane uz Fibonaccijeve brojeve.) Dodatno, ovaj odjeljak usko je vezan uz broj zvan **zlatni rez**, koji ima veliko značenje i primjenu u geometriji.

Definicija 3.3.1. ***Fibonaccijevi brojevi*** *su niz* (f_n) *definiran rekurzivno sa* $f_1 = 1$, $f_2 = 1$, *te*

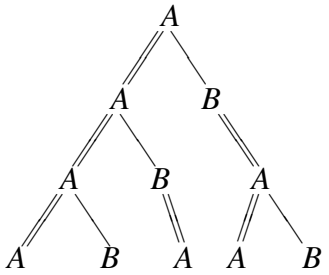
$$f_n = f_{n-1} + f_{n-2}.$$

U skladu s definicijom, prvih nekoliko članova niza je

$$1, 1, 2, 3, 5, 8, 13, 21, \ldots$$

Ovaj niz definirao je talijanski matematičar Leonardo Pisano, također poznat i kao Leonardo od Pise, u svojoj knjizi *Liber Abaci*, objavljenoj 1202. godine. U iznošenju svog problema, postavio je sljedeće pitanje:

Koliko će parova zečeva biti proizvedeno u godini dana, počevši od jednog para, ako svaki mjesec svaki par proizvede novi par, koji postaje produktivan od sljedećeg mjeseca nadalje.



Slovo A označava produktivan par zečeva, a slovo B neproduktivan par, tojest, par koji će postati produktivan za mjesec dana. Isto tako, jednostrukom crtom prikazano je nastajanje jednog novog para B, iz produktivnog para A. S dvije crte označeno je "prenašanje" para zečeva u sljedeći mjesec. Preciznije, kada iz para A imamo dvostruku crtu u par A, to označava da je produktivan par iz jednog mjeseca produktivan i u sljedećem mjesecu. A ako iz para B izlazi dvostuka crta u par A, to znači da je u jednom mjesecu novo izlegnuti par zečeva u idućem mjesecu postao produktivan par zečeva. Prebrojavanjem dobivamo sljedeću tablicu, tojest prvih nekoliko njezinih redaka:

Broj A-ova	Broj B-ova	Ukupno
1	0	1
1	1	2
2	1	3
3	2	5

Vidimo da dobivamo upravo rekurzivnu formulu za Fibonaccijeve brojeve. Alternativni način definiranja Fibonaccijevih brojeva dan je u sljedećem teoremu.

Teorem 3.3.2. *Neka je $P_1 = 1$ i za $n \geqslant 2$ neka je P_n broj $0-1$ nizova duljine $n-2$ bez ponavljanja jedinica. Tada je $P_n = f_n$ za svaki n.*

Dokaz. Za P_2 postoji samo jedan niz (0), pa je $P_2 = f_2 = 1$. Za $n > 2$ neka je q_n broj 0-1 nizova duljine $n-2$ bez ponavljanja jedinica, te sa završetkom 0. Neka je h_n broj 0-1 nizova duljine $n-2$ bez ponavljanja jedinica, te sa završetkom 1. Za svaki takav niz duljine $n-2$ koji završava sa 0, postoje 2 nova niza duljina $n-1$, dok za one koji završavaju sa 1 postoji samo jedan novi niz. Dakle,

$$q_n = q_{n-1} + h_{n-1} \quad \text{i} \quad h_n = q_{n-1},$$

i onda

$$P_n = q_n + h_n.$$

Isto tako primijetimo da za $n > 2$ imamo:

$$P_{n-1} = q_{n-1} + h_{n-1} = q_n.$$

I onda slijedi da je:

$$P_n = q_n + h_n = P_{n-1} + h_n = P_{n-1} + q_{n-1} = P_{n-1} + P_{n-2}.$$

Znači, niz (P_n) zadovoljava istu rekurzivnu formulu kao i (f_n); tojest, $P_n = f_n$ za svaki $n \in \mathbb{N}$. □

Sljedeći teorem pokazat će nam usku povezanost između Fibonaccijevih brojeva i broja

$$\alpha = \frac{1+\sqrt{5}}{2}.$$

Broj α koji se prirodno pojavljuje u mnogim geometrijskim primjenama je takozvani **zlatni rez**.

Teorem 3.3.3. ***(Binetova formula)*** *Neka je (f_n) Fibonaccijev niz, α zlatni rez i broj $\beta = -\alpha^{-1} = \frac{1-\sqrt{5}}{2}$. Tada je za $n \geqslant 1$,*

$$f_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}.$$

Dokaz. Brojevi α i β očito su nultočke polinoma

$$x^2 - x - 1 = 0.$$

Slijede jednakosti,

$$\alpha^{n+2} = \alpha^{n+1} + \alpha^n \quad \text{i} \quad \beta^{n+2} = \beta^{n+1} + \beta^n \quad za \quad n \geqslant 1.$$

Nadalje, $\alpha - \beta = \sqrt{5}$, pa imamo

$$f_1 = \frac{\alpha - \beta}{\alpha - \beta} = 1 \quad \text{i} \quad f_2 = \frac{\alpha^2 - \beta^2}{\alpha - \beta} = \alpha + \beta = 1,$$

te onda

$$f_{n+2} = \frac{\alpha^{n+2} - \beta^{n+2}}{\alpha - \beta} = \frac{\alpha^{n+1} + \alpha^n - (\beta^{n+1} + \beta^n)}{\alpha - \beta} = \frac{\alpha^{n+1} - \beta^{n+1}}{\alpha - \beta} + \frac{\alpha^n - \beta^n}{\alpha - \beta} = f_{n+1} + f_n,$$

za $n \geqslant 3$. □

Korolar 3.3.4. *Ako su f_n i α kao u prethodnom teoremu, tada vrijedi*

$$\lim_{n\to\infty} \frac{f_{n+1}}{f_n} = \alpha = 1 + \frac{1}{1 + \frac{1}{1+\cdots}}$$

Dokaz. Iz Binetove formule slijedi,

$$\frac{f_{n+1}}{f_n} = \frac{\alpha^{n+1} - \beta^{n+1}}{\alpha^n - \beta^n} = \frac{1 - (\frac{\beta}{\alpha})^{n+1}}{\alpha^{-1}(1 - (\frac{\beta}{\alpha})^n)}.$$

Kako je $\left|\frac{\beta}{\alpha}\right| = \left|\frac{1-\sqrt{5}}{1+\sqrt{5}}\right| < 1$, slijedi da izraz $\frac{f_{n+1}}{f_n}$ teži ka α kada $n \to \infty$. Dalje primijetimo kako vrijedi

$$\frac{f_{n+1}}{f_n} = \frac{f_n + f_{n-1}}{f_n} = 1 + \frac{f_{n-1}}{f_n} = 1 + \frac{1}{\frac{f_n}{f_{n-1}}} = 1 + \frac{1}{\frac{f_{n-1}+f_{n-2}}{f_{n-1}}} = 1 + \frac{1}{1 + \frac{f_{n-2}}{f_{n-1}}}.$$

Tako je posebno naprimjer

$$\frac{f_3}{f_2} = 1 + \frac{1}{\frac{f_2}{f_1}} = 1 + \frac{1}{1} \quad \text{i} \quad \frac{f_4}{f_3} = 1 + \frac{1}{\frac{f_3}{f_2}} = 1 + \frac{1}{1 + \frac{1}{1}}.$$

Indukcijom odmah slijedi da je $\lim_{n\to\infty} \frac{f_{n+1}}{f_n}$ jednak navedenom verižnom razlomku. □

Sada ćemo navesti niz svojstava Fibonaccijevih brojeva. Pored toga što ćemo pokazati bogatu teoriju tih brojeva, oni će nas dovesti do dva dodatna dokaza beskonačnosti skupa prostih brojeva $\mathcal{P}$. Napomenimo kako do kraja ovog odjeljka koristimo ove oznake: (f_n) za Fibonaccijeve brojeve i α za zlatni rez.

Lema 3.3.5. $f_1 + f_2 + \cdots + f_n = f_{n+2} - 1, n \geqslant 1.$

Dokaz. Tvrdnja očito vrijedi za $n = 1$ i $n = 2$. Nadalje, za $n \geqslant 3$ imamo

$$f_1 + f_2 + \cdots + f_{n-1} + f_n = f_{n+1} - 1 + f_n = f_{n+2} - 1.$$

□

Sljedeće dvije leme dokazat ćemo indukcijom, koristeći definicijsku jednakost $f_{n+1} = f_n + f_{n-1}$.

Lema 3.3.6. $f_n f_{n+1} = f_1^2 + f_2^2 + \cdots + f_n^2,$ *za* $n \geqslant 1.$

Dokaz. Jednakost je očito zadovoljena za $n = 1$ i $n = 2$. Pretpostavimo sada da tvrdnja vrijedi za $n - 1$, gdje je $n \geqslant 3$. Onda imamo

$$f_n f_{n+1} = f_n(f_n + f_{n-1}) = f_n^2 + f_n f_{n-1} = f_n^2 + (f_1^2 + f_2^2 + \cdots + f_{n-1}^2) = f_1^2 + f_2^2 + \cdots + f_n^2.$$

□

Lema 3.3.7. $f_{n+m} = f_{n-1} f_m + f_n f_{m+1},$ *za* $m, n \geqslant 1.$

Dokaz. Za proizvoljni m i $n = 1$, jednakost postaje

$$f_{1+m} = f_0 f_m + f_1 f_{m+1};$$

što vrijedi ukoliko stavimo $f_0 = 0$. Nadalje, jednakost očito vrijedi i za $n = 2$. Pretpostavimo sada da tvrdnja leme vrijedi za $n \geqslant 2$. Onda imamo

$$\begin{aligned} f_{n+m+1} &= f_{n+m} + f_{n-1+m} \\ &= f_{n-1} f_m + f_n f_{m+1} + f_{n-2} f_m + f_{n-1} f_{m+1} \\ &= (f_{n-1} + f_{n-2}) f_m + (f_n + f_{n-1}) f_{m+1} \\ &= f_n f_m + f_{n+1} f_{m+1}. \end{aligned}$$

Tako je lema dokazana. □

Lema 3.3.8. *(a) Ako su r,s, pozitivni cijeli brojevi takvi da r dijeli s tada vrijedi da f_r dijeli f_s. Obratno, ako je $m \geqslant 2$ i $f_n | f_m$ tada $n|m$.*

(b) $(f_n, f_m) = f_{(n,m)}$. *Tojest, najveći zajednički djelitelj (NZD) od* f_n *i* f_m *je* (n, m) *– ti član Fibonaccijevog niza. Posebno,* f_n *i* f_m *su relativno prosti ako je n relativno prost s m.*

Dokaz. Pokažimo najprije prvu tvrdnju dijela (a) leme. Znamo da vrijedi $\alpha\beta = -1$ i $\alpha + \beta = 1$. Pretpostavimo da $r|s$, tojest da je $s = r \cdot t$ za neki $t \in \mathbb{N}$. Tada imamo

$$\begin{aligned} f_s = f_{rt} &= \frac{\alpha^{rt} - \beta^{rt}}{\alpha - \beta} = \frac{\alpha^r - \beta^r}{\alpha - \beta}(\alpha^{(t-1)r} + \alpha^{(t-2)r}\beta^r + \cdots + \alpha^r\beta^{(t-2)r} + \beta^{(t-1)r}) \\ &= f_r(\alpha^{(t-1)r} + \alpha^{(t-2)r}\beta^r + \cdots + \alpha^r\beta^{(t-2)r} + \beta^{(t-1)r}). \end{aligned}$$

Dakle, ako $r|s$, tada vrijedi da $f_r|f_s$.

Da bi dokazali obratno, moramo prvo dokazati tvrdnju (b) leme. (Primijetimo kako će nam za to trebati gore pokazan prvi dio tvrdnje (a)). Za to pretpostavimo da je $m > n$. Tada prema Euklidovom algoritmu slijedi $r_t = (m, n)$, gdje je

$$\begin{aligned} m &= nq_0 + r_1 \quad \text{i} \quad 0 < r_1 < n, \\ n &= r_1q_1 + r_2 \quad \text{i} \quad 0 < r_2 < r_1, \\ &\cdots \\ r_{t-2} &= r_{t-1}q_{t-1} + r_t \quad \text{i} \quad 0 < r_t < r_{t-1}, \\ r_{t-1} &= r_tq_t. \end{aligned} \tag{3.4}$$

U sljedećem koraku uvesti ćemo supstituciju $w = nq_0$, te dokazujemo da vrijedi sljedeće:

$$(f_{w-1}f_{r_1}, f_n) = (f_{r_1}, f_n).$$

Označimo sa $d = (f_{r_1}, f_n)$, tada d dijeli f_{r_1} i f_n, nadalje $d|f_{w-1}f_{r_1}$, $d|f_n$, pa slijedi da $d|(f_{w-1}f_{r_1}, f_n)$.

Obratno, neka je $D = (f_{w-1}f_{r_1}, f_n)$, dakle $D|f_n$ i $D|f_{w-1}$, pa iz dijela (a) imamo da D dijeli i f_{nq_0}. Nadalje, za svaki $k \in \mathbb{N}$ je NZD $(f_k, f_{k+1}) = 1$, pa D ne može dijeliti f_{nq_0-1}, odnosno f_{w-1}, stoga slijedi da $D|f_{r_1}$. Time smo dokazali gornju tvrdnju.

Sada, primjenom jednakosti(3.4) na odgovarajuće Fibonaccijeve brojeve, možemo tvrditi sljedeće

$$\begin{aligned} (f_m, f_n) = (f_{nq_0+r_1}, f_n) &= (f_{nq_0-1}f_{r_1} + f_{nq_0}f_{r_1+1}, f_n) \\ &= (f_{nq_0-1}f_{r_1}, f_n) = (f_{r_1}, f_n). \end{aligned}$$

U drugoj jednakosti koristili smo Lemu 3.3.7, te s obzirom da prvi dio dokaza dijela (a) znamo da vrijedi $f_n|f_{nq_0}$, slijedi tvrdnja. Kako vrijedi da $f_{r_t}|f_{r_{t-1}}$, analogno imamo

$$(f_1, f_n) = (f_1, f_2) = \cdots = (f_{r_t}, f_{r_{t-1}}) = f_{r_t}.$$

Time smo dokazali tvrdnju pod (b).

Sada imamo sve potrebno kako bismo dokazali drugi dio dokaza dijela (a). U tu svrhu pretpostavimo da je $m \geqslant 2$ i da $f_n | f_m$. Tada korištenjem tvrdnje (b), imamo da je

$$f_n = (f_m, f_n) = f_{(m,n)}.$$

Odavde slijedi da $n|m$, budući da je $m \geqslant 2$ i imamo $f_r < f_s$ ukoliko je $2 \leqslant r < s$. □

Lema 3.3.9. *(a)* $f_{2k} = f_k(f_{k+1} + f_{k-1}) = f_{k+1}^2 - f_{k-1}^2$.

(b) $f_{2k} = \sum_{i=0}^{k} \binom{k}{i} f_i$, *gdje je* $\binom{k}{i}$ *binomni koeficijent.*

(c) $f_{n+1} = \sum_{i=0}^{\lceil \frac{n}{2} \rceil} \binom{n-i}{i}$, *gdje je* $\lceil x \rceil$ *funkcija najveće cijelo.*

Dokaz. U dokazima ćemo primjenjivati Binetovu formulu. Prisjetimo se isto tako da je $\alpha\beta = -1$ i $\alpha + \beta = 1$.
(a) Imamo sljedeći niz jednakosti

$$\begin{aligned} f_{2k} &= \frac{\alpha^{2k} - \beta^{2k}}{\alpha - \beta} = \frac{(\alpha^k - \beta^k)(\alpha^k + \beta^k)}{\alpha - \beta} = f_k(\alpha^k + \beta^k) \\ &= f_k\Big(\frac{(\alpha^k + \beta^k)(\alpha - \beta)}{\alpha - \beta}\Big) = f_k\Big(\frac{\alpha^{k+1} - \alpha^k\beta + \beta^k\alpha - \beta^{k+1}}{\alpha - \beta}\Big) \\ &= f_k\Big(\frac{\alpha^{k+1} - \beta^{k+1}}{\alpha - \beta} + \frac{\alpha\beta(\beta^{k-1} - \alpha^{k-1})}{\alpha - \beta}\Big) \\ &= f_k(f_{k+1} + f_{k-1}) = (f_{k+1} - f_{k-1})(f_{k+1} + f_{k-1}) \\ &= f_{k+1}^2 - f_{k-1}^2. \end{aligned}$$

(b) Imamo sljedeći niz jednakosti

$$\begin{aligned} \sum_{i=0}^{k} \binom{k}{i} f_i &= \frac{1}{\alpha - \beta}\Big(\sum_{i=0}^{k} \binom{k}{i}(\alpha^i - \beta^i)\Big) = \frac{1}{\alpha - \beta}\Big(\sum_{i=0}^{k} \binom{k}{i}\alpha^i - \sum_{i=0}^{k} \binom{k}{i}\beta^i\Big) \\ &= \frac{1}{\alpha - \beta}[(1 + \alpha)^k - (1 + \beta)^k] = \frac{1}{\alpha - \beta}(\alpha^{2k} - \beta^{2k}) \\ &= f_{2k}. \end{aligned}$$

(c) Tvrdnja očito vrijedi za $0 \leqslant n \leqslant 2$. Pretpostavimo da je $n \geqslant 2$ i nastavljamo sa indukcijom. Tada vrijedi

$$f_{n+1} = f_n + f_{n-1} = \sum_{i=0}^{\lceil \frac{n-1}{2} \rceil} \binom{n-1-i}{i} + \sum_{i=0}^{\lceil \frac{n-2}{2} \rceil} \binom{n-2-i}{i}. \tag{3.5}$$

U prvom slučaju uzet ćemo da je $n = 2m$, gdje je $m \geqslant 1$. Tada je

$$\left\lceil \frac{n-1}{2} \right\rceil = m - 1 = \left\lceil \frac{n-2}{2} \right\rceil,$$

i koristeći (3.5) imamo jednakosti,

$$\begin{aligned}
f_{n+1} &= \sum_{i=0}^{m-1} \binom{2m-1-i}{i} + \sum_{i=0}^{m-1} \binom{2m-1-(i+1)}{(i+1)-1} = \sum_{i=0}^{m-1} \binom{2m-1-i}{i} + \sum_{i=1}^{m} \binom{2m-1-i}{i-1} \\
&= \binom{2m-1}{0} + \sum_{i=1}^{m-1} \binom{2m-1-i}{i} + \binom{2m-1-m}{m-1} + \sum_{i=1}^{m-1} \binom{2m-1-i}{i-1} \\
&= \binom{2m-1}{0} + \binom{m-1}{m-1} + \sum_{i=1}^{m-1} \left[\binom{2m-1-i}{i} + \binom{2m-1-i}{i-1} \right] \\
&= \binom{2m-0}{0} + \binom{2m-m}{m} + \sum_{i=1}^{m-1} \binom{2m-i}{i} = \sum_{i=0}^{m} \binom{2m-i}{i} \\
&= \sum_{i=0}^{\lceil \frac{n}{2} \rceil} \binom{n-i}{i}.
\end{aligned}$$

Ovime smo dokazali slučaj u kojem je n paran broj.
U drugom slučaju uzet ćemo da je n neparan broj, odnosno $n = 2m + 1$ i $m \geqslant 1$. Tada je

$$\left\lceil \frac{n-1}{2} \right\rceil = m, \qquad \left\lceil \frac{n-2}{2} \right\rceil = m - 1, \qquad \left\lceil \frac{n}{2} \right\rceil = m.$$

Onda ponovno s obzirom na (3.5) imamo

$$\begin{aligned}
f_{n+1} &= \sum_{i=0}^{m} \binom{2m-i}{i} + \sum_{i=0}^{m-1} \binom{2m-(i+1)}{(i+1)-1} = \sum_{i=0}^{m} \binom{2m-i}{i} + \sum_{i=1}^{m} \binom{2m-i}{i-1} \\
&= \binom{2m}{0} + \sum_{i=1}^{m} \binom{2m-i}{i} + \sum_{i=1}^{m} \binom{2m-i}{i-1} \\
&= \binom{2m}{0} + \sum_{i=1}^{m} \binom{2m-i+1}{i} \\
&= \sum_{i=0}^{\lceil \frac{n-1}{2} \rceil} \binom{n-i}{i}.
\end{aligned}$$

□

Teoremom i korolarom u nastavku, pokazat ćemo vezu između Fibonaccijevih i prostih brojeva, a to će nas naposlijetku odvesti do još jednog dokaza o beskonačnosti skupa prostih brojeva.

Teorem 3.3.10. *Neka je p prost broj. Tada vrijede sljedeće tvrdnje*

(i) $p|f_p$ *ako je* $p = 5$*, te* $p|f_{p-1}$ *ili* $p|f_{p+1}$ *ako je* $p \neq 5$*.*

(ii) $p|f_{p+1}$ *ako je* $p = 2$*.*

(iii) $p|f_{p-1}$ *ako je p kongruentan* ± 1 *modulo 10.*

(iv) $p|f_{p+1}$ *ako je p kongruentan* ± 3 *modulo 10.*

Dokaz. Ako je $p = 2$, tada je $f_3 = 2$ i vrijedi $p|f_{p+1}$. Ako je $p = 3$, tada je $f_4 = 3$ i vrijedi $p|f_{p+1}$. Ako je $p = 5$, tada je $f_5 = 5$ i vrijedi $p|f_p$. Neka je $p \geqslant 7$. Koristeći Binetovu formulu slijedi,

$$f_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n\right] - \frac{1}{\sqrt{5}}\left[\left(\frac{1-\sqrt{5}}{2}\right)^n\right], \quad n \geqslant 1,$$

a po binomnoj formuli imamo,

$$(1 \pm \sqrt{5})^n = 1 \pm \binom{n}{1}\sqrt{5} + \binom{n}{2}5 \pm \binom{n}{3}(\sqrt{5})^3 + \cdots + (\pm 1)^n(\sqrt{5})^n.$$

Pretpostavimo da je n neparan broj. Tada slijedi

$$\begin{aligned} 2^n f_n &= \frac{1}{\sqrt{5}}\left[\binom{n}{1}2\sqrt{5} + \binom{n}{3}2(\sqrt{5})^3 + \cdots + \binom{n}{n}2(\sqrt{5})^n\right] \\ &= \binom{n}{1}2 + \binom{n}{3}2(\sqrt{5})^2 + \cdots + \binom{n}{n}2(\sqrt{5})^{n-1} \end{aligned}$$

Neka je $n = p$ prost broj. Kako je $\binom{p}{i} \equiv 0$ mod(p), za $1 \leqslant i < p$, slijedi

$$2^p f_p - \binom{p}{p}2(\sqrt{5})^{p-1} \equiv \binom{p}{1}2 + \binom{p}{3}2(\sqrt{5})^2 + \ldots + \binom{p}{p-2}2(\sqrt{5})^{p-3} \equiv 0 \pmod{p}.$$

po Malom Fermatovom teoremu vrijedi $2^p \equiv 2 \pmod{p}$, pa mora vrijediti

$$f_p \equiv 5^{\frac{p-1}{2}} \pmod{p},$$

i onda ponovno koristeći Mali Fermatov teorem imamo

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

Nadalje,

$$\begin{aligned} f_p^2 - f_{p-1}f_{p+1} &= \left(\frac{\alpha^p - \beta^p}{\alpha - \beta}\right)^2 - \left[\left(\frac{\alpha^{p-1} - \beta^{p-1}}{\alpha - \beta}\right)\left(\frac{\alpha^{p+1} - \beta^{p+1}}{\alpha - \beta}\right)\right] \\ &= \frac{\alpha^{2p} + \beta^{2p} - 2(-1)^p}{(\alpha - \beta)^2} - \left(\frac{\alpha^{2p} + \beta^{2p} - (-1)^{p-1}(\alpha^2 + \beta^2)}{(\alpha - \beta)^2}\right) \\ &= \frac{5(-1)^{p-1}}{(\sqrt{5})^2} = (-1)^{p-1} = 1. \end{aligned}$$

Slijedi

$$0 \equiv f_p^2 - 1 \equiv f_{p-1}f_{p+1} \pmod{p}.$$

I onda imamo da $p|f_{p-1}$ ili $p|f_{p+1}$.

Preostaje nam pokazati tvrdnje (*iii*) i (*iv*), što je malo zahtjevnije. U tu svrhu sjetimo se kako je definiran Legendreov simbol; za više detalja o svemu što slijedi vidjeti npr. [4, Poglavlje 3]. Za neparan prost broj p i $a \in \mathbb{N}$ je Legendreov simbol $\left(\frac{a}{p}\right) = 1$ ako kongruencija $x^2 \equiv a \pmod{p}$ ima rješenje, odnosno $\left(\frac{a}{p}\right) = -1$ ako ta kongruencija nema rješenja. Neka je sada

$$p \equiv \pm 1 \pmod{10}.$$

Onda je $\left(\frac{p}{5}\right) = 1$, jer $x^2 \equiv p \pmod 5$ ima rješenja. Naime, ukoliko je $p \equiv 1 \pmod{10}$ stavimo npr. $x = 1$, a ukoliko je $p \equiv -1 \pmod{10}$ stavimo npr. $x = 2$. Sada se sjetimo da za neparne i međusobno različite proste brojeve p i q vrijedi Gaussov kvadratni zakon reciprociteta:

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

To posebno daje

$$\left(\frac{5}{p}\right)\left(\frac{p}{5}\right) = (-1)^{\frac{5-1}{2}\frac{p-1}{2}} = 1,$$

i onda $\left(\frac{5}{p}\right) = 1$. Dalje, po tzv. Eulerovom kriteriju imamo

$$\left(\frac{5}{p}\right) \equiv 5^{\frac{p-1}{2}} \pmod{p},$$

i zato

$$5^{\frac{p-1}{2}} - 1 \equiv 0 \pmod{p}. \tag{3.6}$$

Sada, analogno kao prije, za n paran imamo

$$2^{n-1}f_n = \binom{n}{1} + \binom{n}{3}5 + \cdots + \binom{n}{n-1}5^{\frac{n-2}{2}}.$$

Dalje, neka je sada p prost broj i $n = p - 1$; tu trenutno ne pretpostavljamo da je $p \equiv \pm 1 \pmod{10}$. Onda imamo

$$1 + \binom{p-1}{1} = \binom{p-1}{0} + \binom{p-1}{1} = \binom{p}{1} \equiv 0 \pmod{p} \quad \Longrightarrow \quad \binom{p-1}{1} \equiv -1 \pmod{p}.$$

Zatim,

$$\binom{p-1}{1} + \binom{p-1}{2} = \binom{p}{2} \equiv 0 \pmod{p} \quad \Longrightarrow \quad \binom{p-1}{2} \equiv -\binom{p-1}{1} \equiv 1 \pmod{p}.$$

Induktivnim argumentom vidimo da je posebno

$$\binom{p-1}{1} \equiv \binom{p-1}{3} \equiv \cdots \equiv \binom{p-1}{p-2} \equiv -1 \pmod{p},$$

i zato imamo

$$\begin{aligned} 2^{p-2}f_{p-1} &\equiv -(1 + 5 + 5^2 + \cdots + 5^{\frac{p-3}{2}}) \equiv -\frac{(5^{\frac{p-3}{2}+1} - 1)}{5 - 1} \\ &\equiv -\frac{(5^{\frac{p-1}{2}+1} - 1)}{4} \pmod{p}. \end{aligned} \tag{3.7}$$

Sada; iz (3.6) i (3.7) slijedi

$$2^{p-2}f_{p-1} \equiv 0 \pmod{p};$$

tojest, $p|f_{p-1}$, kako smo i tvrdili. Slično se vidi i tvrdnja (*iv*). □

Korolar 3.3.11. *Neka je p prost broj veći od 7. Tada je svaki prosti djelitelj od f_p veći od p.*

Dokaz. Neka je q prosti djelitelj od f_p i $p \geqslant 7$ prost broj. Pretpostavimo da je $q \leqslant p$. Ako je $q = p$, tada iz Teorema 3.3.10(*i*) vrijedi $q = p = 5$; pa možemo pretpostaviti da je $q < p$. Tada, koristeći Lemu 3.3.8(*b*) imamo

$$\begin{aligned} (f_p, f_q) &= f_{(p,q)} = f_1 = 1, \\ (f_p, f_{q-1}) &= f_{(p,q-1)} = f_1 = 1, \\ (f_p, f_{q+1}) &= f_{(p,q+1)} = f_1 = 1. \end{aligned}$$

Sada, ponovno po Teoremu 3.3.10(*i*) imamo da ili $q|f_q$ ili $q|f_{q-1}$ ili $q|f_{q+1}$. Ali ako $q|f_q$, onda to zajedno s činjenicom $q|f_p$ daje da $q|(f_p, f_q)$; tojest, $q|1$, što je kontradikcija. Analogno se vidi i za ostala dva slučaja. Zaključujemo da $q > p$. □

Koristeći Fibonaccijeve brojeve, sada možemo dati još dva dokaza Teorema 2.1.1 o beskonačnosti skupa prostih brojeva.

Dokaz. Pretpostavimo da je $\mathcal{P} = \{p_1, \ldots, p_n\}$, konačan skup različitih prostih brojeva, takvih da je $p_1 < p_2 < \ldots < p_n$, te da je $p_n \geqslant 7$. Neka je p prost djelitelj od f_{p_n}. Tada iz Korolara 3.3.11 slijedi da je svaki prosti djelitelj od f_{p_n} veći od p_n, odnosno $p > p_n$. Tako dobivamo da $p \notin \mathcal{P}$, što pokazuje da skup $\mathcal{P}$ nije konačan. □

Dokaz. Pretpostavimo da je $\mathcal{P} = \{p_1, \ldots, p_n\}$ skup svih prostih brojeva, te neka je $p_1 = 2$. Za njih imamo da je $f_{p_i} > 1$ za $i = 2, \ldots, n$. Tada najviše jedan f_{p_i} za $i = 2, \ldots, n$ ima dva prosta djelitelja. U suprotnom, kako je $(f_{p_i}, f_{p_j}) = f_{(p_i, p_j)}$, za $i \neq j$, već bi imali $n+1$ prostih djelitelja. Došli smo do kontradikcije, jer naprimjer

$$f_{19} = 37 \cdot 113 \qquad \text{i} \qquad f_{53} = 557 \cdot 2417.$$

□

U nastavku navesti ćemo nekoliko primjera generaliziranih ideja vezanih uz Fibonaccijeve brojeve.

1. Neka je K proizvoljno polje, te neka su $x, y \in K$. Tada definirajmo sljedeće

   $$T_0(x, y) = 0, \quad T_1(x, y) = 1$$

   te nadalje

   $$T_n(x, y) = xT_{n-1}(x, y) - yT_{n-2}(x, y).$$

   Ovaj niz u polju K zadovoljava puno zajedničkih svojstava s Fibonaccijevim brojevima. Ukoliko je A 2 x 2 invertibilna matrica nad poljem K takva da vrijedi $tr(A) = x$ i $det(A) = y$, tada vrijedi

   $$A^n = T_n(x, y)A + yT_{n-1}(x, y)I,$$

   gdje je I matrica identiteta. Posebno,

   $$T_n(x, y)^2 - T_{n+1}(x, y)T_{n-1}(x, y) = y^{n-1}, \quad n \geqslant 1.$$

   Ukoliko je $x = 1$ i $y = -1$, tada je $T_n(x, y) = f_n$ za $n \geqslant 0$.

2. Sljedeći primjer pokazuje vezu između Čebiševljevih polinoma, koji igraju veliku ulogu u aproksimaciji funkcija, i Fibonaccijevih brojeva. Ako je $y = 1$ i $n \geqslant 1$, tada

   $$T_n(x, 1) = S_n(x),$$

gdje je $S_n(x)$ n - ti Čebiševljev polinom druge vrste. Nadalje imamo

$$S_{nm} = S_n(x)S_{m+1}(x) - S_m(x)S_{n-1}(x)$$

i

$$S_{nm} = S_m(S_{n+1}(x) - S_{n-1}(x)) \cdot S_n(x)$$

za sve prirodne brojeve n, m. U točki x, ovi Čebiševljevi polinomi zadovoljavaju sljedeće

$$S_{(n,m)}(x) = (S_n(x), S_m(x)).$$

3. Za pozitivne realne vrijednosti, Čebiševljevi polinomi imaju jednostavnu formu. Ako je $K = \mathbb{R}$, $x \geqslant 0$ i neka je $x = cos(\theta) < 2$. Vrijedi sljedeće

$$S_n(x) = \frac{\sin(n\theta)}{\sin(\theta)}.$$

Ako je $x = \cosh(\theta) > 2$, tada imamo

$$S_n(x) = \frac{2\sinh(n\theta)}{\sinh(\theta)},$$

te za $x = 2$ vrijedi

$$S_n(x) = n.$$

Bibliografija

[1] http://www.mersenne.org/.

[2] Tom M. Apostol, *Introduction to Analytic Number Theory*, Springer - Verlag New York, 1976.

[3] Clarkson i A. James, *On the series of prime reciprocals*, Proc. Amer. Math. Soc., 17 : 541 : MR 32 **5573** (1966).

[4] A. Dujella, *Uvod u teoriju brojeva*, https://web.math.pmf.unizg.hr/~duje/utb/utblink.pdf.

[5] B. Fine i G. Rosenberg, *Number theory: An Introduction via the Distribution of Primes*, Birkhäuser, 2007.

[6] B. Širola, *Distribucija prim brojeva i Riemannova Zeta - funkcija*, Prvi dio, Hrvatski matematički elektronički časopis math.e. **13** (2008).

[7] ———, *Algebarske strukture*, https://web.math.pmf.unizg.hr/nastava/alg/predavanja/ASpred.pdf.

Sažetak

U ovom radu govorimo o skupu cijelih brojeva, točnije rečeno o njegovim prostim elementima. Polazeći od definicije i elementarnih pojmova teorije brojeva, pokazujemo neke od osnovnih rezultata, te karakterizacija tog skupa. Nadalje, navodimo razne varijacije dokaza beskonačnosti skupa prostih brojeva, gdje pritom koristimo neke od zanimljivih analitičkih pristupa. Na kraju proučavamo vezu skupa prostih brojeva s nizom Fermatovih, Mersennovih i Fibonaccijevih brojeva, te pomoću tih nizova i njihovih svojstava, ponovno pokazujemo tvrdnju da je skup prostih brojeva beskonačan.

Summary

In this diploma thesis we consider the set of integers, or better said its prime elements. Starting from definitions and basic concepts of number theory, we are showing some of the main results, and characterizations of this set. Furthermore, we consider variations of proof refered to infinity of the set of prime numbers, where while we are using some of interesting analytical approaches. Finally, we are exploring the relation of the set of prime numbers with a sequences of Fermat, Mersenne and Fibonacci numbers, and using these sequences and their properties, again showing the claim that the set of prime numbers is infinite.

Životopis

Moje ime je Sara Crnić. Rođena sam u Sisku 13.11.1990. Osnovnu školu Zvonka Cara, te nakon toga, opću gimnaziju u Srednjoj školi dr. Antuna Barca, završila sam u Crikvenici. Nakon završetka srednje škole, 2009. godine, upisala sam Prirodoslovno matematički fakultet (PMF) u Zagrebu, smjer Matematika. Titulu sveučilišne prvostupnice (baccalaureus) matematike stekla sam 2013. godine, te iste godine upisala diplomski studij Financijska i poslovna matematika na istom fakultetu.