Eulerova funkcija u teoriji particija

Jurić, Andrea

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Andrea Jurić

EULEROVA FUNKCIJA U TEORIJI PARTICIJA

Diplomski rad

Voditelj rada:
dr. sc. Goran Igaly
izv. prof. dr. sc. Ivica Martinjak

Zagreb, veljača 2024.

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

1. ____________________________, predsjednik
2. ____________________________, član
3. ____________________________, član

Povjerenstvo je rad ocijenilo ocjenom _______________.

Potpisi članova povjerenstva:

1. ____________________________
2. ____________________________
3. ____________________________

Sadržaj

Sadržaj iii

Uvod 1

1 Osnove teorije particija 3
- 1.1 Particija prirodnog broja . . . 3
- 1.2 Youngovi dijagrami . . . 5
- 1.3 Eulerov teorem . . . 7

2 Osnove aritmetičkih funkcija 11
- 2.1 Funkcije najveće i najmanje cijelo . . . 11
- 2.2 Eulerova funkcija . . . 13
- 2.3 Möbiusova funkcija . . . 16
- 2.4 Ramanujanove sume . . . 18

3 Eulerova funkcija u teoriji particija 21
- 3.1 Funkcije izvodnice . . . 21
- 3.2 Merca-Schmidt teoremi . . . 25

Bibliografija 29

Uvod

Eulerova funkcija, koja je dobila naziv po poznatom švicarskom matematičaru Leonhardu Euleru, ima široku primjenu u raznim granama matematike, ponajviše u teoriji brojeva i kriptografiji. Jedan od ciljeva ovog rada je prikazati intrigantne nove teoreme koji Eulerovu funkciju povezuju s drugim područjima diskretne matematike. Točnije, bit će istražena i obrađena poveznica između teorije particija i Eulerove funkcije.

U fokusu prvog poglavlja je teorija particija. Definirat ćemo osnovne pojmove i rezultate iz teorije particija te ćemo ilustrirati njihove primjene raznim primjerima.

U drugom poglavlju, bit će obrađene aritmetičke funkcije. Bit će definiran i obrađen pojam multiplikativnih funkcija uz nekoliko primjera funkcija s tim svojstvom. Poseban naglasak bit će na definiranju Eulerove funkcije i rezulatima vezanim uz nju. Na kraju poglavlja upoznajemo Ramanujanove sume.

Posljednje poglavlje bit će posvećeno Eulerovoj funkciji u teoriji particija gdje će biti navedeni i dokazani zanimljivi rezultati koji povezuju Eulerovu funkciju i particije prirodnih brojeva. Za dokaz tih rezultata će biti potrebne funkcije izvodnice, pa se na početku poglavlja bavimo njima i njihovom primjenom. Konačni cilj ovog rada je proširiti razumijevanje veze između teorije brojeva i teorije particija te pružiti nove uvide u matematičke strukture i njihove primjene.

Poglavlje 1

Osnove teorije particija

Teorija particija je područje matematike koje se bavi enumeracijom načina na koji se ne-negativni broj n može prikazati kao suma pozitivnih cijelih brojeva. Ovo poglavlje služi kao uvod u teoriju particija. Nakon definicije pojma particije prikazujemo najpoznatije identitete za particijsku funkciju. Pritom koristimo bijekcije putem Youngovih dijagrama. Dijeljenjem promatranih objekata u disjunktne podskupove dokazujemo rekurzivnu relaciju za broj particija s fiksnim brojem dijelova.

1.1 Particija prirodnog broja

Svaki prirodni broj možemo zapisati kao sumu prirodnih brojeva. Primjerice, broj 12 možemo zapisati kao $6 + 6$ ili $4 + 3 + 3 + 2$ ili $5 + 1 + 1 + 1 + 1 + 1 + 1 + 1$. Ukupno imamo 77 takvih zapisa. Ovim razmatranjem motivirana je sljedeća definicija.

Definicija 1.1.1. *Particija broja $n \in \mathbb{N}_0$ je monotoni niz prirodnih brojeva $\lambda = (\lambda_1, \dots, \lambda_k)$ pri čemu je $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_k$ te $\lambda_1 + \lambda_2 + \dots + \lambda_k = n$. Pišemo $\lambda \vdash n$. Brojeve λ_i zovemo dijelovima particije, a broj n težina particije.*

Broj dijelova particije označavamo s $l(\lambda)$ i zovemo *duljina particije*. Dijelove particije dogovorno pišemo u padajućem poretku. Uvodimo sljedeće oznake:

- $p(n)$ označava ukupan broj particija broja n, p još zovemo *particijska funkcija*
- $p_k(n)$ označava broj particija od n duljine k
- $p'_k(n)$ označava broj particija od n duljine najviše k

Često je od interesa promatrati particije koje zadovoljavaju neko svojstvo. Općenito to označavamo s $p(n|uvjet)$. Označimo sada skup svih particija od n s $\mathcal{P}_n$,

$$\mathcal{P}_n := \{\lambda : \lambda \vdash n\}.$$

Podskup $\mathcal{O}_n$ skupa $\mathcal{P}_n$ je skup svih particija od n čiji su svi dijelovi neparni. Njih zovemo *neparne particije*. Particije čiji su dijelovi međusobno različiti zovemo *striktnim particijama* i taj skup označavamo s $\mathcal{D}_n$. Dakle,

$$\begin{aligned}\mathcal{O}_n &:= \{\lambda \vdash n : 2 \nmid \lambda_i,\ i = 1, \ldots, l(\lambda)\},\\ \mathcal{D}_n &:= \{\lambda \vdash n : \lambda_i \neq \lambda_j,\ \text{za sve } i \neq j\}.\end{aligned}$$

Vrijedi sljedeće:

$$\begin{aligned}&p(0) = 1,\\ &p_n(n) = 1,\\ &p_{n-1}(n) = 1,\ \text{za } n \geq 1,\\ &p_1(n) = 1,\\ &p_2(n) = \left\lfloor \frac{n}{2} \right\rfloor,\\ &p(n) = p_1(n) + p_2(n) + \ldots + p_n(n).\end{aligned}$$

Primjer 1.1.2. *Postoji 7 particija težine 5, $p(5) = 7$. To su*

$$\begin{aligned}&(5),\\ &(4, 1),\\ &(3, 2),\\ &(3, 1, 1),\\ &(2, 2, 1),\\ &(2, 1, 1, 1),\\ &(1, 1, 1, 1, 1).\end{aligned}$$

Uočimo da među navedenim particijama postoje 3 striktne particije. Također, postoje 3 neparne particije te vrijedi $p_3(5) = 2$.

Poznato je mnogo identiteta za particijsku funkciju, a jedan od najpoznatijih je jednakost striktnih particija i particija s neparnim dijelovima dane težine. O tome govori Eulerov teorem koji prikazujemo u nastavku. Identitete za particijsku funkciju dokazujemo bijektivno. Kako bismo to učinili potrebno je pronaći bijekciju između dva zadana skupa. Primjerice, ako želimo dokazati da je

$$p(n \big| \text{svi dijelovi parni}) = p(n \big| \text{paran broj dijelova}),$$

onda moramo pronaći bijekciju između skupa koji sadrži sve particije broja n čiji su dijelovi parni i skupa koji sadrži sve particije od n koje imaju paran broj dijelova. Ukoliko svaki parni dio particije, koja sadrži sve parne dijelove, podijelimo na dva jednaka dijela dobijemo particiju s parnim brojem dijelova. Obratno, ukoliko dva jednaka dijela spojimo u jedan, dobijemo particiju čiji su svi dijelovi parni. Ovim postupkom dobivamo traženu bijekciju. Pokazat ćemo kako bi ta bijekcija izgledala za broj 6:

$$\begin{aligned} 6 &\to (3,3) \\ (4,2) &\to (2,2,1,1) \\ (2,2,2) &\to (1,1,1,1,1,1). \end{aligned}$$

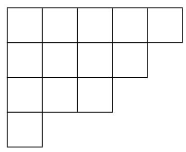
1.2 Youngovi dijagrami

Particije prirodnih brojeva možemo prikazati grafički na dva vrlo slična načina, pomoću Ferrerovog grafa i Youngovog dijagrama. Ferrerov graf prikazujemo pomoću točkica, a Youngov dijagram pomoću kvadratića.

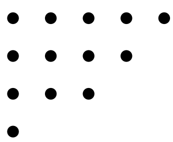
Definicija 1.2.1. *Neka je* $\lambda = (\lambda_1, \ldots, \lambda_k)$ *particija broja n. Youngov dijagram je skup parova* $(i, j) \in \mathbb{Z} \times \mathbb{Z}$*, takvih da* $1 \leq i \leq k, 1 \leq j \leq \lambda_i$.

Youngov dijagram prikazujemo u ravnini $\mathbb{R}^2$ tako da točke i rastu u smjeru ordinate s orijentacijom prema ishodištu, a točke j rastu u smjeru apscise s orijentacijom od ishodišta.

Primjer 1.2.2. *Na slici 1.1, vidimo grafički prikaz particije* $\lambda = (5, 4, 3, 1)$ *pomoću Youngovog dijagrama. Prikaz pomoću Ferrerovog grafa vidimo na slici 1.2.*



Slika 1.1: Youngov dijagram particije λ.



Slika 1.2: Ferrerov graf particije λ.

Postoje brojne transformacije Youngovih dijagrama. Ukoliko je neka takva transformacija invertibilna, onda se radi o bijekciji i možemo ju iskoristiti kako bismo dokazali neki identitet particije. Sada ćemo navesti nekoliko transformacija.

Najjednostavniji primjer transformacije je uklanjanje prvog retka (stupca) Youngovog dijagrama. Kada uklonimo prvi redak (stupac) duljine k, ostaje nam opet Youngov dijagram. Sada su duljine preostalih redaka (stupaca) manje ili jednake k što možemo promotriti na slikama 1.3a i 1.3b.

(a) Youngov dijagram particije λ (b) Youngov dijagram nakon transformacije

Slika 1.3: Transformacija Youngovog dijagrama uklanjanjem prvog retka.

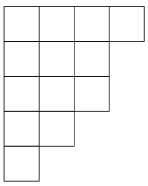
Obratno, ukoliko dodamo redak (stupac) duljine k na vrh Youngovog dijagrama, opet dobivamo Youngov dijagram. Iz ovoga slijedi bijekcija za dokazivanje identiteta

$$p(n \big| \text{ najveći dio particije je } r) = p(n - r \big| \text{ svi dijelovi} \leq r).$$

Konjugirani Youngov dijagram dobivamo zamjenom redaka i stupaca, odnosno transponiramo ga. Na taj način dobijemo *konjugiranu particiju* koju označavamo s λ'. Ova transformacija daje particiju čiji je najveći dio jednak broju dijelova početne particije što nam daje bijekciju za dokaz identiteta

$$p(n \big| \text{ m dijelova }) = p(n \big| \text{ najveći dio m}).$$

Primjer 1.2.3. *U primjeru 1.2.2, vidjeli smo Youngov dijagram za particiju* $\lambda = (5, 4, 3, 1)$. *Slika 1.4 prikazuje konjugirani dijagram te particije.*



Slika 1.4: Konjugirani Youngov dijagram particije λ.

Ako je particija jednaka svojoj konjugiranoj particiji, onda kažemo da je ta particija *samo-konjugirana*.

Primjer 1.2.4. *Slike 1.5a i 1.5b prikazuju particije brojeva 6 i 8 koje su samo-konjugirane.*

(a) $\lambda = (3, 2, 1)$ (b) $\mu = (4, 2, 1, 1)$

Slika 1.5: Samo-konjugirane particije $\lambda \vdash 6$ i $\mu \vdash 8$.

Postoji transformacija Youngovog dijagrama kojom iz samo-konjugirane particije dobijemo neparnu particiju u različite dijelove. Transformacija se vrši tako da od prvog retka i stupca dijagrama početne particije λ napravimo jedan redak nove particije μ. Zatim, od drugog stupca i retka particije λ napravimo drugi redak particije μ i tako dalje. Primjer ove transformacije vidimo na slikama 1.6a i 1.6b.

(a) $\lambda = (4, 3, 2, 1)$ (b) $\mu = (7, 3)$

Slika 1.6: Transformacija Youngovog dijagrama spajanjem retka i stupca.

Dakle, uvijek spajamo redak i stupac iste duljine. Taj redak i stupac dijele jednu zajedničku točku, odnosno ćeliju, pa će duljina novog retka biti jednaka dvostrukoj duljini starog retka umanjenoj za jedan, to jest duljina će biti neparna. Dobiveni dijelovi su različiti. Obratno, ako krenemo od particije koja se sastoji od različitih neparnih dijelova, te dijelove možemo presavinuti oko središnje ćelije pod pravim kutem. Dobivene "kuke" stanu jedna u drugu formirajući Youngov dijagram samo-konjugirane particije. Dobivamo bijekciju koja dokazuje sljedeći identitet:

$$p(n \,|\, \text{samo-konjugirana}\,) = p(n \,|\, \text{različiti neparni dijelovi}\,).$$

1.3 Eulerov teorem

Teorem 1.3.1. *(Euler) Za svaki prirodni broj n, broj neparnih particija $\lambda \vdash n$ jednak je broju striktnih particija $\mu \vdash n$, odnosno*

$$|\mathcal{O}_n| = |\mathcal{D}_n|.$$

Dokaz. Konstruiramo bijekciju koja skup particija broja n s neparnim dijelovima preslikava u skup particija u različite dijelove. Ukoliko neka particija broja n sadrži dva jednaka dijela, morat ćemo izvršiti neku operaciju nad tim dijelovima. Najprirodnije je spajanje ta dva dijela u jedan. Ovaj proces možemo ponavljati sve dok svi dijelovi unutar particije nisu različiti. Budući da se ovom operacijom broj particija smanjuje, u nekom trenu ćemo sigurno doći do različitih dijelova, u krajnjem slučaju može nam ostati particija koja se sastoji od samo jednog dijela. Primjerice,

$$\begin{aligned}(2,2,3,1,1,1,1) &\to ((2+2),3,(1+1),(1+1))\\ &\to (4,3,2,2)\\ &\to (4,3,(2+2))\\ &\to (4,3,4)\\ &\to (8,3).\end{aligned}$$

Obratno, želimo iz različitih dijelova dobiti particije s neparnim dijelovima. Inverz spajanja dva ista dijela bi bio razdvajanje parnog dijela na dvije jednake polovice. Ponavljanjem ove operacije ćemo sigurno doći do particije u neparne dijelove. Primjerice,

$$\begin{aligned}(6,3,4) &\to (6,3,(2+2))\\ &\to (6,3,2,2)\\ &\to ((3+3),3,(1+1),(1+1))\\ &\to (3,3,3,1,1,1,1).\end{aligned}$$

Redoslijed vršenja navedenih operacija nad dijelovima nije bitan. Gore opisani postupak je bijekcija koja dokazuje traženi identitet. $\square$

Primjer 1.3.2. *Pokažimo kako izgleda bijekcija iz dokaza teorema 1.3.1 za* $n = 6$.

$$\begin{aligned}(5,1) &\to (5,1)\\ (3,3) &\to (6)\\ (3,1,1,1) &\to (3,2,1)\\ (1,1,1,1,1,1) &\to (4,2)\end{aligned}$$

Propozicija 1.3.3. *Vrijedi sljedeće:*

a) Broj particija od n u najviše k dijelova, odnosno $p'_k(n)$, *jednak je broju particija od n u dijelove od kojih je svaki* $\leq k$.

b) $p_k(n) = p_{k-1}(n-1) + p_k(n-k)$ *(rekurzija za brojeve* $p_k(n)$*)*

c) $p(n) = p_n(2n)$.

Dokaz. a) Konstruirat ćemo bijekciju između pripadnih skupova particija. Ako je $\lambda = (\lambda_1, \lambda_2 \ldots)$ neka particija od n, onda je $\lambda' = (\lambda'_1, \lambda'_2 \ldots)$ njegova konjugirana particija. Očito je $\lambda'_i = \#\{j \big| \lambda_j \geq i\}$. Dakle, preslikavanje koje λ preslikava u λ' je bijekcija. Pogledajmo sliku 1.7.

(a) $\lambda = (6, 4, 4, 1)$ (b) $\lambda' = (4, 3, 3, 3, 1)$

Slika 1.7: Bijekcija između λ i λ'.

b) Ako particija broja n u k dijelova sadrži jedinicu, onda ostatak $n - 1$ možemo particionirati na $p_{k-1}(n-1)$ načina. Ako particija broja n u k dijelova nema jedinicu, onda svakom dijelu oduzmimo jedinicu i imamo $p_k(n-k)$ particija ostatka $n-k$ u k dijelova. Ovo je bijekcija.

c) Ova tvrdnja slijedi iz b). Vrijedi

$$\begin{aligned} p_n(2n) &= p_{n-1}(2n-1) + p_n(n) \\ &= p_{n-2}(2n-2) + p_{n-1}(n) + p_n(n) \\ &= \ldots = p_1(n) + p_2(n) + \ldots + p_n(n) \\ &= p(n). \end{aligned}$$

□

Primjer 1.3.4. *Opet promatramo particije broja 5. Ukupan broj jedinica u svim particijama je jednak 12. Prebrojimo sada koliko ima različitih brojeva unutar svake particije. Primjerice, unutar particije* $(2, 3)$ *imamo dva različita broja, unutar particije* $(1, 1, 3)$ *isto imamo dva različita broja i tako dalje. Sumiranjem broja različitih brojeva po svim particijama dolazimo do* $(1, 2, 2, 2, 2, 2, 1) = 12$.

Prethodni primjer je generaliziran Stanleyevim teoremom.

Teorem 1.3.5. *(Stanley) Broj jedinica koje se pojavljuju u particijama broja n ekvivalentan je broju dijelova koji se pojavljuju barem jednom u danoj particiji broja n, sumirano po svim particijama broja n.*

Ovaj teorem služi kao uvod u zadnje poglavlje gdje ćemo vidjeti još jedan rezultat vezan za Eulerovu funkciju i broj jedinica unutar particije.

Poglavlje 2

Osnove aritmetičkih funkcija

U ovom poglavlju prikazujemo aritmetičke funkcije. To su funkcije čija domena je skup prirodnih brojeva $\mathbb{N}$, a kodomena podskup skupa kompleksnih brojeva $\mathbb{C}$. Na početku će biti obrađene funkcije najveće i najmanje cijelo, a dalje će od interesa biti multiplikativne aritmetičke funkcije, od kojih je najpoznatija Eulerova funkcija. Na kraju dajemo kratki osvrt na Ramanujanove sume.

2.1 Funkcije najveće i najmanje cijelo

Definicija 2.1.1. *Neka je $x \in \mathbb{R}$ proizvoljan. Funkcija najmanje cijelo ili strop od x, u oznaci $\lceil x \rceil$, je najmanji cijeli broj veći ili jednak x. Funkcija najveće cijelo ili pod od x, u oznaci $\lfloor x \rfloor$ je najveći cijeli broj manji ili jednak x. Razliku brojeva x i $\lfloor x \rfloor$ zovemo frakcijski dio broja x i označavamo s $\{x\} = x - \lfloor x \rfloor$.*

Primjerice, za broj π vrijedi $\lfloor \pi \rfloor = 3$, $\lfloor -\pi \rfloor = -4$, $\lceil \pi \rceil = 4$ i $\lceil -\pi \rceil = -3$. Iz prethodnog možemo primijetiti neka svojstva ovih funkcija. Vrijednosti poda i stropa su jednake samo u cjelobrojnim točkama,

$$\lfloor x \rfloor = x \iff x \text{ cijeli broj} \iff \lceil x \rceil = x,$$

inače se razlikuju za točno 1. Također, vrijedi

$$\lfloor -x \rfloor = -\lceil x \rceil \,, \lceil -x \rceil = -\lfloor x \rfloor.$$

Uočimo da je $x - 1 < \lfloor x \rfloor$ i $x + 1 > \lceil x \rceil$. Kombiniranjem ovih nejednakosti dobivamo

$$x - 1 < \lfloor x \rfloor \leq x \leq \lceil x \rceil < x + 1.$$

Primijetimo da za cijeli broj n vrijede i sljedeća svojstva:

$$\begin{aligned}
\lfloor x \rfloor = n &\iff n \leq x < n+1, \\
\lfloor x \rfloor = n &\iff x-1 < n \leq x, \\
\lceil x \rceil = n &\iff n-1 < x \leq n, \\
\lceil x \rceil = n &\iff x \leq n < x+1.
\end{aligned}$$

Korisno je primijetiti da vrijedi i jednakost $\lfloor x+n \rfloor = \lfloor x \rfloor + n$, dok jednakost $\lfloor nx \rfloor = n\lfloor x \rfloor$ ne mora uvijek vrijediti. Primjerice, za $x = 1/5$ i $n = 5$ ne vrijedi. Nekada možemo izbjeći korištenje poda i stropa radi jednostavnosti. Na primjer, ako je x realan broj i n cijeli broj, onda vrijede sljedeće ekvivalencije:

$$\begin{aligned}
x < n &\iff \lfloor x \rfloor < n, \\
n < x &\iff n < \lceil x \rceil,
\end{aligned}$$

Pokažimo da prva ekvivalencija doista vrijedi, dokaz druge ekvivalencije je analogan. Ako je $x < n$, onda sigurno vrijedi $\lfloor x \rfloor < n$ jer je $\lfloor x \rfloor \leq x$. Obratno, neka je $\lfloor x \rfloor < n$. Vrijedi $x < \lfloor x \rfloor + 1$ te $\lfloor x \rfloor + 1 \leq n$, dakle $x < n$.

Prosti brojevi

Kažemo da je pozitivni cijeli broj $p > 1$ *prost* ako je djeljiv samo s 1 i sa samim sobom, inače kažemo da je *složen*. Broj 1 nije ni prost ni složen broj. Bez eksplicitnog navođenja, s p obično označavamo prosti broj. Svaki pozitivni cijeli broj može, na jedinstven način, biti zapisan kao umnožak prostih faktora $n = p_1 \cdot \ldots \cdot p_k$ odnosno $\prod_p p^{n_p}$ gdje je $n_p \geq 0$. Kažemo da su brojevi $m, n \in \mathbb{N}$ *relativno prosti*, u oznaci $m \perp n$, ako im je najveći zajednički djelitelj jednak 1, to jest ako je $nzd(m, n) = 1$. Vrijedi sljedeća ekvivalencija:

$$k \perp m \text{ i } k \perp n \iff k \perp mn. \tag{2.1}$$

U sljedećoj propoziciji dokazujemo jedan rezultat koji povezuje proste brojeve i funkciju pod.

Propozicija 2.1.2. *Potencija s kojom prosti broj p ulazi u rastav broja $n!$ na proste faktore je jednaka*

$$\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \ldots$$

Dokaz. Primijetimo da je u $n! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n$ svaki p-ti faktor djeljiv s p. Dakle, postoji $\lfloor \frac{n}{p} \rfloor$ faktora koji su djeljivi s p. Svaki doprinosi s eksponentom koji iznosi barem 1. Zatim djelitelji broja p^2 doprinose s još 1 u potenciji pa to trebamo pribrojiti i tako dalje. Neka je l najveći prirodni broj za koji vrijedi da p^l dijeli $n!$. Tada vrijedi sljedeće:

$$l = \sum_{m=1}^{n} \sum_{\substack{j=1, \\ p^j | m}}^{\infty} 1 = \sum_{j=1}^{\infty} \sum_{\substack{m=1, \\ p^j | m}}^{n} 1 = \sum_{j=1}^{\infty} \left\lfloor \frac{n}{p^j} \right\rfloor.$$

Uočimo da je prethodna suma konačna jer će za dovoljno velik j vrijediti $p^j > n$ pa za svaki takav j vrijedi $\lfloor \frac{n}{p^j} \rfloor = 0$.

□

Primjer 2.1.3. *Odredimo eksponent s kojim prosti broj 7 ulazi u rastav broja 29!. Ovo možemo vrlo lako izračunati koristeći prethodni teorem. Ukupni broj pojavljivanja broja 7 je*

$$\left\lfloor \frac{29}{7} \right\rfloor + \left\lfloor \frac{29}{7^2} \right\rfloor = 5 + 0 = 5.$$

2.2 Eulerova funkcija

Definicija 2.2.1. *Preslikavanje $\phi : \mathbb{N} \to \mathbb{N}$ koje svakom prirodnom broju n pridružuje broj brojeva manjih od n koji su relativno prosti s n, nazivamo Eulerovom funkcijom.*

Drugim riječima $\phi(n)$ je broj brojeva u nizu $1, \ldots, n$ koji su relativno prosti s n. Primjerice $\phi(10) = 4$ jer su brojevi 1, 3, 7, 9 relativno prosti s 10. Vrijedi primijetiti i da je $\phi(1) = 1$, $\phi(p) = p - 1$ te $\phi(m) < m - 1$ ukoliko je m složen broj. Lako možemo odrediti $\phi(m)$ ako je m potencija prostog broja, $m = p^k$. U tom slučaju broj m dijele $p, 2p, \ldots, p^{k-1}p$. Dakle, tih brojeva je p^{k-1} pa vrijedi

$$\phi(p^k) = p^k - p^{k-1} = p^k(1 - \frac{1}{p}). \tag{2.2}$$

Uočimo da uvrštavanjem $k = 1$ u formulu (2.2) upravo dobijemo jednakost $\phi(p) = p-1$ koju smo na početku naveli.

Definicija 2.2.2. *Za funkciju $f : \mathbb{N} \to \mathbb{C}$ kažemo da je multiplikativna ako vrijedi sljedeće:*

1. $f(1) = 1$,
2. $f(mn) = f(m)f(n)$, *gdje su m i n relativno prosti brojevi.*

Lema 2.2.3. *Eulerova funkcija je multiplikativna.*

Dokaz. Dokaz se može pronaći u [8]. □

Koristeći multiplikativnost Eulerove funkcije možemo doći do općenite formule za računanje vrijednosti te funkcije.

Teorem 2.2.4. *Za svaki prirodni broj $n > 1$ vrijedi*

$$\phi(n) = n \prod_{p|n} (1 - \frac{1}{p}).$$

Dokaz. Neka su $p_1, \dots, p_k$ različiti prosti faktori broja n, odnosno $n = p_1^{r_1} \dots p_k^{r_k}$. Koristeći multiplikativnost Eulerove funkcije imamo

$$\phi(n) = \phi(p_1^{r_1} \dots p_k^{r_k}) = \phi(p_1^{r_1}) \dots \phi(p_k^{r_k}).$$

Nadalje, koristeći formulu $\phi(p^k) = p^k - p^{k-1} = p^k(1 - \frac{1}{p})$ računamo:

$$\begin{aligned}
\phi(n) &= p_1^{r_1}(1 - \frac{1}{p_1}) \cdot \ldots \cdot p_k^{r_k}(1 - \frac{1}{p_k}) \\
&= \prod_{i=1}^{k} p^{r_i}(1 - \frac{1}{p_i}) \\
&= n \prod_{i=1}^{k} (1 - \frac{1}{p_i}) \\
&= n \prod_{p|n} (1 - \frac{1}{p})
\end{aligned}$$

□

U teoriji brojeva vrlo često sumiramo po djeliteljima danog broja. Korisno je primijetiti sljedeće:

$$\sum_{d|n} d = \sum_{d|n} \frac{n}{d}, \ n > 0. \tag{2.3}$$

Neka je $n = 12$, vidimo da je $1 + 2 + 3 + 4 + 6 + 12 = \frac{12}{1} + \frac{12}{2} + \frac{12}{3} + \frac{12}{4} + \frac{12}{6} + \frac{12}{12}$. U dokazima ćemo koristiti i jednakost

$$\sum_{m|n} \sum_{k|m} a_{k,m} = \sum_{k|n} \sum_{l|\frac{n}{k}} a_{k,kl}. \tag{2.4}$$

Ako je f funkcija takva da je suma po djeliteljima $g(n) = \sum_{d|n} f(d)$ multiplikativna, onda je i sama funkcija f multiplikativna. Ovu činjenicu dokazujemo indukcijom po n. Za $n = 1$ vrijedi $f(1) = g(1) = 1$. Neka je sada $n > 1$. Pretpostavimo da vrijedi $f(m_1 m_2) = f(m_1) f(m_2)$ za sve m_1 i m_2 takve da $m_1 m_2 < n$ i $m_1 \perp m_2$. Ako je $n = m_1 m_2$ i $m_1 \perp m_2$, imamo

$$g(m_1 m_2) = \sum_{d|m_1 m_2} f(d) = \sum_{d_1|m_1} \sum_{d_2|m_2} f(d_1 d_2)$$

te vrijedi $d_1 \perp d_2$ jer su svi djelitelji od m_1 relativno prosti sa svim djeliteljima od m_2. Po pretpostavci indukcije znamo da vrijedi $f(d_1 d_2) = f(d_1)f(d_2)$ za $d_1 < m_1$ i $d_2 < m_2$. Stoga, imamo

$$\left(\sum_{d_1|m_1} f(d_1) \sum_{d_2|m_2} f(d_2)\right) - f(m_1)f(m_2) + f(m_1m_2) = g(m_1)g(m_2) - f(m_1)f(m_2) + f(m_1m_2)$$

Vrijedi $g(m_1m_2) = g(m_1)g(m_2)$ pa zaključujemo da je $f(m_1m_2) = f(m_1)f(m_2)$ čime smo dokazali tvrdnju. Vrijedi i obrat. Neka je $f(n)$ multiplikativna, tada je suma po svim djeliteljima, $\sum_{d|n} f(d)$ također multiplikativna.

Promotrimo sljedeći niz

$$\frac{1}{12}, \frac{2}{12}, \frac{3}{12}, \frac{4}{12}, \frac{5}{12}, \frac{6}{12}, \frac{7}{12}, \frac{8}{12}, \frac{9}{12}, \frac{10}{12}, \frac{11}{12}, \frac{12}{12}.$$

Nakon skraćivanja dobijemo

$$\frac{1}{12}, \frac{1}{6}, \frac{1}{4}, \frac{1}{3}, \frac{5}{12}, \frac{1}{2}, \frac{7}{12}, \frac{2}{3}, \frac{3}{4}, \frac{5}{6}, \frac{11}{12}, \frac{1}{1}.$$

Grupirajmo sada članove niza po nazivnicima. Dobijemo

$$\frac{1}{1}; \frac{1}{2}; \frac{1}{3}, \frac{2}{3}; \frac{1}{4}, \frac{3}{4}; \frac{1}{6}, \frac{5}{6}; \frac{1}{12}, \frac{5}{12}, \frac{7}{12}, \frac{11}{12}.$$

Zapažamo da su svi djelitelji broja 12 sadržani u nazivnicima članova niza. Ako promotrimo, primjerice, grupu gdje je nazivnik broj 6, onda možemo uočiti da se u brojniku nalaze samo brojevi koji su relativno prosti sa 6, dakle 1 i 5. Možemo zaključiti da se svaki djelitelj d (odnosno razlomak s nazivnikom d) pojavljuje upravo $\phi(d)$ puta. Vrijedi

$$\phi(1) + \phi(2) + \phi(3) + \phi(4) + \phi(6) + \phi(12) = 12 \tag{2.5}$$

Iduća propozicija pokazuje da jednakost (2.5) možemo zapisati i općenito.

Propozicija 2.2.5. *Za Eulerovu funkciju vrijedi*

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

Dokaz. Neka je $n = p_1^{r_1} \cdot \ldots \cdot p_k^{r_k}$. Iz multiplikativnosti Eulerove funkcije slijedi

$$\sum_{d|n} \phi(d) = \prod_{i=1}^{k} (1 + \phi(p_i) + \phi(p_i^2) + \ldots + \phi(p_i^{r_i}))$$

Ako pomnožimo faktore na desnoj strani jednakosti, dobivamo sumu čiji su sumandi oblika

$$\phi(p_1^{q_1}) \cdot \ldots \cdot \phi(p_k^{q_k}) = \phi(p_1^{q_1} \cdot \ldots \cdot p_k^{q_k}), \text{ gdje je } 0 \leq q_i \leq r_i, i = 1, \ldots, k$$

Sada imamo

$$\begin{aligned}\sum_{d|n} \phi(d) &= \prod_{i=1}^{k} (1 + (p_i - 1) + (p_i^2 - p_i) + \ldots + (p_i^{r_i} - p_i^{r_i - 1})) \\ &= \prod_{i=1}^{k} p_i^{r_i} = n.\end{aligned}$$

□

2.3 Möbiusova funkcija

Izraz $[n = m]$ poprima vrijednost 1 ako je $n = m$, inače poprima vrijednost 0. Sada možemo dati definiciju Möbiusove funkcije.

Definicija 2.3.1. *Möbiusovu funkciju definiramo implicitno na sljedeći način*

$$\sum_{d|n} \mu(d) = [n = 1], \ n \geq 1. \tag{2.6}$$

Primijetimo da je navedena relacija rekurzija s početnom vrijednosti $\mu(1) = 1$. Izračunajmo vrijednosti Möbiusove funkcije za brojeve $n = 1, \ldots 12$.

n	1	2	3	4	5	6	7	8	9	10	11	12
$\mu(n)$	1	−1	−1	0	−1	1	−1	0	0	1	−1	0

Jedan vrlo važan rezultat koji su zapazili matematičari Dedekind i Liouville dan je sljedećim teoremom.

Teorem 2.3.2. *(Möbiusov princip inverzije) Neka je $f : \mathbb{N} \to \mathbb{C}$ proizvoljna funkcija i neka je $F(n) = \sum_{d|n} f(d), n \in \mathbb{N}$. Tada vrijedi*

$$f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right).$$

Obratno, ako je $f(n) = \sum_{d|n} \mu(d) F(\frac{n}{d}), n \in \mathbb{N}$, onda je $F(n) = \sum_{d|n} f(d)$.

Dokaz. Neka je $F(n) = \sum_{d|n} f(d)$. Koristeći 2.3 i 2.4 računamo

$$\begin{aligned}\sum_{d|n} \mu(d)F\left(\frac{n}{d}\right) &= \sum_{d|n} \mu\left(\frac{n}{d}\right)F(d) \\ &= \sum_{d|n} \mu\left(\frac{n}{d}\right)\sum_{k|d} f(k) \\ &= \sum_{k|n}\sum_{d|\frac{n}{k}} \mu(d)f(k) \\ &= \sum_{k|n}\left[\frac{m}{k} = 1\right]f(k) = f(n).\end{aligned}$$

Dokažimo i obrat. Neka je $f(n) = \sum_{d|n} \mu(d)F(\frac{n}{d})$. Vrijedi

$$\sum_{d|n} f(d) = \sum_{d|n}\sum_{k|d} \mu\left(\frac{d}{k}\right)F(k) = \sum_{k|n}\sum_{d|\frac{n}{k}} \mu(d)F(k) = \sum_{k|m} F(k)\left[\frac{n}{k} = 1\right] = F(n)$$

čime je tvrdnja dokazana. □

Primjenom Möbiusovog principa inverzije na relaciju $\sum_{d|n} \phi(d) = n$ dobijemo sljedeću jednakost

$$\phi(n) = n\sum_{d|n}\frac{\mu(d)}{d}.$$

Primjerice,

$$\phi(12) = 12 \cdot \mu(1) + 6 \cdot \mu(2) + 4 \cdot \mu(3) + 2 \cdot \mu(6) + 1 \cdot \mu(12) = 12 - 6 - 4 + 0 + 2 + 0 = 4.$$

Potpuni kvadrat je prirodan broj koji je kvadrat nekog drugog prirodnog broja. Za broj $n \in \mathbb{N}$ kažemo da je *kvadratno slobodan* ako je 1 najveći potpuni kvadrat koji ga dijeli. Primjerice, 25 je potpuni kvadrat jer je $25 = 5^2$ dok je broj 6 kvadratno slobodan broj.

Želimo riješiti rekurziju iz definicije Mobusove funkcije. Funkcija $g(m) = [m = 1]$ je očito multiplikativna jer je uvijek 0 osim za $m = 1$. Iz toga slijedi da je i μ multiplikativna. Dovoljno je odrediti što je $\mu(p^k)$. Djelitelji od p^k su $1, p, \ldots, p^k$ pa vrijedi $\mu(1) + \mu(p) + \mu(p^2) + \ldots + \mu(p^k) = 0$, po definiciji 2.6. Slijedi, $\mu(p) = -1$ te $\mu(p^k) = 0$ za svaki $k > 1$, čime smo dokazali sljedeću propoziciju.

Propozicija 2.3.3. *Za $n > 1$ vrijedi*

$$\mu(n) = \prod_{p|n} \mu(p^{n_p}) = \begin{cases} 0, & \text{ako } n \text{ nije kvadratno slobodan} \\ (-1)^r, & \text{ako je } n = p_1p_2p_3\ldots p_r, \text{ gdje su } p_i \text{ različiti prosti brojevi.}\end{cases}$$

Definicija 2.3.4. *Neka je $n \in \mathbb{N}$. Broj pozitivnih djelitelja broja n označavamo s $\tau(n)$. Sumu svih pozitivnih djelitelja broja n označavamo s $\sigma(n)$.*

Prethodne funkcije možemo zapisati na sljedeći način:

$$\tau(n) = \sum_{d|n} 1,$$

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

Funkcija $f(d) = 1$ je konstanta pa je τ očito multiplikativna. Funkcija σ je također multiplikativna jer je $f(d) = d$ multiplikativna. Iz definicija funkcija σ i ϕ primjećujemo da vrijedi $\sigma(n) \geq n$ i $\phi(n) \leq n$ za svaki $n \in \mathbb{N}$. Sljedeća propozicija nam daje donju ogradu za ϕ i gornju za σ.

Propozicija 2.3.5. *Za sve $n \in \mathbb{N}$, $n > 1$ vrijedi $\sigma(n) < n(1 + \ln n)$. Također, za sve $n \in \mathbb{N}$, $n > 1$ vrijedi $\phi(n) > \frac{1}{4}\frac{n}{\ln n}$.*

Dokaz. Dokazujemo samo drugu tvrdnju, dokaz prve tvrdnje se može pronaći u [4]. Funkcija $f(n) = \frac{\sigma(n)\phi(n)}{n}$ je multiplikativna kao produkt multiplikatvnih funkcija. Iz izraza

$$f(p^j) = \frac{(p^{j+1}-1)p^{j-1}(p-1)}{(p-1)p^{2j}} = 1 - \frac{1}{p^{j+1}} \geq 1 - \frac{1}{p^2}$$

slijedi

$$f(n) \geq \prod_{p|n}(1 - \frac{1}{p^2}) \geq \prod_{m=2}^{\infty}(1 - \frac{1}{m^2}) = \frac{1\cdot 3}{2\cdot 2}\cdot\frac{2\cdot 4}{3\cdot 3}\cdot\frac{3\cdot 5}{4\cdot 4}\cdot\ldots = \frac{1}{2}$$

Očito vrijedi $\sigma(n)\phi(n) \geq \frac{1}{2}n^2$. Iz prve tvrdnje propozicije slijedi da je $\sigma(n) < 2n\ln n$, za sve $n \geq 3$. Iz toga slijedi druga tražena nejednakost. Da nejednakost vrijedi i za $n = 2$ možemo dokazati direktnim uvrštavanjem. □

2.4 Ramanujanove sume

Ramanujanove sume imaju široku primjenu u raznim granama matematike i fizike. Ime su dobile po indijskom matematičaru Srinivasi Ramanujanu koji ih je otkrio.

Definicija 2.4.1. *Za cijele brojeve $n \geq 1$ i $k \geq 0$ definiramo sumu*

$$c_n(k) = \sum_{r\perp n; r\leq n} e^{2ikr\pi/n}$$

koju zovemo Ramanujanova suma.

Kompleksni broj w je *primitivni n-ti korijen jedinice* ako vrijedi: $w^n = 1$ i $w^k \neq 1$ za bilo koji $k \leq n$. Drugim riječima, Ramanujanova suma je suma k-tih potencija primitivnih n-tih korijena jedinice. Primijetimo da su primitivni n-ti korijeni jedinice brojevi $e^{2ik\pi/n}$ za sve one $r \leq n$ takve da je $r \perp n$. Prikladno je uvesti sljedeću oznaku:

$$\triangle_n = \{e^{2ikr\pi/n} : r \perp n, 1 \leq r \leq n\}.$$

Uočimo da je skup svi $n-$tih korijena jedinice $\{e^{2ikr\pi/n} : 0 \leq k < n\}$ jednak uniji disjunktnih skupova $\triangle_d$, gdje d ide po djeliteljima broja n, jer je n-ti korijen iz jedinice primitivan d-ti korijen iz jedinice za jedinstveni djelitelj d broja n. Uvodimo i karakterističnu funkciju $\delta_{k|n}$ koja poprima vrijednost 1 ako $k|n$, inače 0.
Sada možemo navesti svojstva Ramanujanovih suma:

1. $c_n(k) = c_n(-k) = c_n(n-k)$
2. $c_n(0) = \phi(n)$ i $c_n(1) = \mu(n)$
3. $c_n(ks) = c_n(k)$ ako je $s \perp n$. Posebno, $c_n(s) = \mu(n)$ ako je $s \perp n$
4. $c_n(k) = c_n(k')$ ako je $nzd(k,n) = nzd(k',n)$, posebno $c_n(k) \equiv c_n(k') \mod n$ ako je $k \equiv k' \mod n$
5. $\sum_{k=0}^{n-1} c_n(k) = 0$
6. $\sum_{d|n} c_d(k) = \delta_{n|k} n$ i $c_n(k) = \sum_{d|n} d\mu(\frac{n}{d})\delta_{d|k} = \sum_{d|} d\mu(\frac{n}{d})$. Posebno, za potencije prostih brojeva p^k imamo
$$c_{p^r}(k) = \begin{cases} p^r - p^{r-1}, & \text{ako } p^r|k \\ -p^{r-1}, & \text{ako } p^{r-1}|k \\ 0, & \text{inače} \end{cases}$$
7. $c_{mn}(k) = c_m(k)c_n(k)$ ako je $m \perp n$
8. $\sum_{k=1}^{n} c_m(k)c_n(k) = \delta_{mn} n\phi(n)$

Korisno je primijetiti da nam svojstvo 6 upravo kaže da su vrijednosti Ramanujanove sume cijeli brojevi. Svojstva 1 i prvi dijelovi svojstava 2 i 3 slijede iz definicije. Dokažimo sada svojstvo 5. Imamo

$$\sum_{k=0}^{n-1} c_n(k) = \sum_{k=0}^{n-1} \sum_{\zeta \in \triangle_n} \zeta^k = \sum_{\zeta \in \triangle_n} \sum_{k=0}^{n-1} \zeta^k = 0,$$

gdje zadnja jednakost vrijedi zbog

$$\sum_{k=0}^{n-1} \zeta^k = \frac{1-\zeta^n}{1-\zeta} = 0.$$

za svaki $\zeta \in \triangle_n$. Ovo nam je kratki uvod u funkcije izvodnice. Dokažimo i tvrdnju 6. Primijetimo da druga tvrdnja slijedi iz prve po Möbiusovom principu inverzije. Zato sada dokazujemo prvu tvrdnju. Vrijedi

$$\sum_{d|n} c_d(k) = \sum_{d|n} \sum_{\zeta \in \triangle_d} \zeta^k = \sum_{m=0}^{n-1} e^{2imk\pi/n}$$

jer je disjunktna unija $\triangle_d$, gdje d ide po djeliteljima od n, skup svih n-tih korijena jedinice. Ako gornju sumu pomnožimo s $e^{2ik\pi/n}$ dobijemo istu sumu, što znači da je jednaka 0, osim ako $n|k$. Kada $k|n$ suma je jednaka n. Iz ove dvije tvrdnje slijede ostala svojstva koja nećemo dokazivati. Više o Ramanujanovim sumama se pronaći u [9].

Na kraju navodimo jedno osnovno brojevno svojstvo za particijsku funkciju koje je također otkrio Ramanujan. Promotrimo vrijednosti te funkcije za nekoliko brojeva

n	$p(n)$	n	$p(n)$	n	$p(n)$
0	1	5	7	10	42
1	1	6	11	11	56
2	2	7	15	12	77
3	3	8	22	13	101
4	5	9	30	14	135

Znamo da za računanje broja $p(n)$ ne postoji neka zatvorena formula, međutim, možemo uočiti da je svaka peta vrijednost $p(n)$ djeljiva s 5. Upravo to je uočio i dokazao Ramanujan. Dakle, za sve $n \in \mathbb{N}_0$ vrijedi

$$p(5n+4) \equiv 0 \pmod 5.$$

Također, otkrio je i da vrijede sljedeće kongruencije:

$$\begin{aligned} p(7n+5) &\equiv 0 \pmod 7 \\ p(11n+6) &\equiv 0 \pmod{11}. \end{aligned} \tag{2.7}$$

Više o ovoj temi može se pronaći u [1].

Poglavlje 3

Eulerova funkcija u teoriji particija

Nakon upoznavanja osnova teorije particija i aritmetičkih funkcija, slijede dva nova rezultata koja povezuju artimetičke funkcije, točnije Eulerovu funkciju, i broj particija. Za dokaz tih rezultata bit će nam potreban novi alat, funkcije izvodnice, stoga početak poglavlja posvećujemo funkcijama izvodnicama i njihovoj primjeni.

3.1 Funkcije izvodnice

Funkcije izvodnice se vrlo često koriste u kombinatorici za rješavanje brojnih problema, a od posebne važnosti bit će nam za ovo poglavlje.

Definicija 3.1.1. *Neka je $a_0, \ldots, a_n, \ldots$ niz realnih (ili kompleksnih) brojeva. Pripadna obična funkcija izvodnica $F(x)$ je formalni red potencija*

$$F(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n + \ldots = \sum_{n=0}^{\infty} a_n x^n.$$

Koristit ćemo oznaku $\langle x^n \rangle F(x) = a_n$ koja označava da je koeficijent od $F(x)$ uz x^n jednak a_n.

U definiciji govorimo o formalnom redu potencija jer nas ne zanima koju vrijednost poprima varijabla x. Korisno je znati da je funkcija izvodnica za niz $(a_n)_{n \geq 0}$ gdje je $a_n = 1$ jednaka

$$1 + x + x^2 + \ldots + x^n + \ldots = \frac{1}{1-x}. \tag{3.1}$$

Slijedi jedan jednostavan primjer kako bismo stekli intiuiciju o tome što su funkcije izvodnice i čemu služe.

Primjer 3.1.2. *Pretpostavimo da imamo 24 bombona koja želimo podijeliti na četvero ljudi tako da svaki čovjek dobije barem 3 bombona, ali ne više od 8. Dakle, jedan čovjek može dobiti između 3 i 8 bombona, što možemo prikazati izrazom*

$$x^3 + x^4 + x^5 + x^6 + x^7 + x^8.$$

Budući da imamo četiri čovjeka, funkcija izvodnica će biti definirana s

$$F(x) = (x^3 + x^4 + x^5 + x^6 + x^7 + x^8)^4.$$

Zanima nas na koliko načina možemo rasporediti 24 bombona , a ta vrijednost je upravo $\langle x^{24} \rangle$*. Uz korištenje formule za konačne redove*

$$\sum_{j=0}^{n} x^j = \frac{1 - x^{n+1}}{1 - x},$$

imamo

$$\begin{aligned}
F(x) &= (x^3 + x^4 + x^5 + x^6 + x^7 + x^8) \cdot \ldots \cdot (x^3 + x^4 + x^5 + x^6 + x^7 + x^8) \\
&= (x^3 \cdot (1 + x + x^2 + x^3 + x^4 + x^5))^4 \\
&= x^{12}(1 + x + x^2 + x^3 + x^4 + x^5)^4 \\
&= x^{12}\left(\frac{1 - x^6}{1 - x}\right)^4 \\
&= x^{12}(1 - x^6)^4(1 - x)^{-4}.
\end{aligned}$$

Prisjetimo se kratko binomnog poučka,

$$(a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k.$$

Upotrebom binomnog poučka i formule

$$\binom{-N}{n}(-1)^n = \binom{N + n - 1}{n}$$

slijedi

$$\begin{aligned}
\langle x^{24} \rangle F(x) &= \langle x^{12} \rangle (1 - x^6)^4 (1 - x)^{-4} \\
&= \langle x^{12} \rangle \left(1 - \binom{4}{1}x^6 + \binom{4}{2}x^{12} - \ldots\right)\left(\binom{-4}{0} + \binom{-4}{1}(-x) + \binom{-4}{2}(-x)^2 + \ldots\right) \\
&= \binom{-4}{12}(-1)^{12} - \binom{4}{1}\binom{-4}{6}(-1)^6 + \binom{4}{2}\binom{-4}{0} \\
&= \binom{15}{3} - 4\binom{9}{3} + \binom{4}{2} \\
&= 125.
\end{aligned}$$

Promotrimo sada funkcije izvodnice u kontekstu particija brojeva. U tu svrhu pronađimo sve striktne particije čiji su dijelovi iz skupa $\{1, 2, 3\}$. To su

$$(1), (2), (3), (2, 1), (3, 1), (3, 2), (3, 2, 1).$$

Slijedi,

$$(1 + x)(1 + x^2)(1 + x^3) = 1 + x + x^2 + x^{1+2} + x^3 + x^{1+3} + x^{2+3} + x^{1+2+3}.$$

Uočimo da eksponenti dobivenog polinoma daju sve striktne particije čiji su dijelovi iz prethodno navedenog skupa. Postoje dvije particije broja 3 i po jedna particija za brojeve 1, 2, 4, 5, 6. Ovaj rezultat je formaliziran idućim teoremom.

Teorem 3.1.3. *Funkcija izvodnica P za particije s međusobno različitim dijelovima je dana s*

$$P(x) = \prod_{i=1}^{\infty}(1 + x^i) = \sum_{n=0}^{\infty} p^d(n)x^n.$$

Dokaz. Neka je $S = \{1, 2, \ldots, m\}$. Sve particije s različitim dijelovima, pri čemu su dijelovi iz S su

$$(1), \ldots, (m), (1, 2), (1, 3), \ldots, (m - 1, m), (1, 2, 3), \ldots, (m - 2, m - 1, m), \ldots, (1, 2, \ldots, m)$$

. Te particije možemo prikazati na sljedeći način

$$(1 + x)(1 + x^2) \ldots (1 + x^m) = 1 + x^1 + x^2 + \ldots + x^m + x^{1+2} + \ldots + x^{1+2+\ldots+m}.$$

Time smo dokazali

$$\prod_{i=1}^{m}(1 + x^i) = \sum_{n>0} p'^d(n)x^n$$

gdje je $p'^d(n)$ broj particija od n s različitim dijelovima pri čemu su ti dijelovi iz skupa S. Ukoliko je $S = \mathbb{N}_0$, na desnoj strani dobivamo sve moguće particije od n s međusobno različitim dijelovima. □

I dalje promatramo skup $\{1, 2, 3\}$ i particije čiji su dijelovi iz tog skupa. Ukoliko se dijelovi particije smiju pojaviti više puta, recimo najviše d, vrijedi

$$(1 + x + \ldots + x^d)(1 + x^2 + \ldots + x^{2d})(1 + x^3 + \ldots + x^{3d}),$$

što nas dovodi do sljedećeg teorema.

Propozicija 3.1.4. *Funkcija izvodnica za niz brojeva* $p(0), p(1), \ldots, p(n), \ldots$ *je produkt*

$$P(x) = \prod_{k=0}^{\infty} \frac{1}{1-x^k}.$$

Broj $p(n)$ *je koeficijent uz* x^n *u produktu od konačno mnogo faktora:*

$$p(n) = \langle x^n \rangle \prod_{k=1}^{m} \frac{1}{1-x^k},\ m \geq n.$$

Dokaz. Vrijedi

$$\frac{1}{1-x^k} = 1 + x^k + x^{2k} + x^{3k} + \ldots.$$

Stoga je koeficijent uz x^n u umnošku

$$(1 + x + x^2 + x^3 \ldots)(1 + x^2 + x^4 + \ldots)(1 + x^3 + x^6 + \ldots)(1 + x^4 + x^8 + \ldots)\cdots$$

jednak broju načina na koji se x^n može prikazati kao $x^{k_1}x^{2k_2}\ldots x^{nk_n} = x^{k_1+2k_2+\ldots+nk_n}$, što je upravo broj particija $p(n)$. □

Primjer 3.1.5. *Želimo prikazati sve particije koje se sastoje od jednog parnog dijela i jednog neparnog dijela, s time da je svaki dio manji od 8. Pomoću funkcija izvodnica to možemo napisati na sljedeći način:*

$$\begin{aligned}(x^2 + x^4 + x^6)(x^1 + x^3 + x^5 + x^7) &= x^{2+1} + x^{2+3} + x^{2+5} + x^{2+7} + x^{4+1} + x^{4+3} + x^{4+5} + x^{4+7}\\ &\quad + x^{6+1} + x^{6+3} + x^{6+5} + x^{6+7}\\ &= x^3 + x^5 + x^7 + x^9 + x^5 + x^7 + x^9 + x^{11} + x^7 + x^9 + x^{11} + x^{13}\\ &= x^3 + 2x^5 + 3x^7 + 3x^9 + 2x^{11} + x^{13}.\end{aligned}$$

Primjerice, promotrimo koeficijent uz x^7 *to jest* $\langle x^7 \rangle$. *Koeficijent* $\langle x^7 \rangle = 3$ *nam govori da postoje tri particije od* 7 *u kojoj je jedan broj paran, a drugi neparan. To su upravo particije* $(1, 6)$, $(2, 5)$ *i* $(3, 4)$.

Propozicija 3.1.6. *Vrijedi*

$$\prod_{i=1}^{\infty}(1 + zx^i) = \sum_{n\geq 0}\sum_{m\geq 0} p_m(n) z^m x^n.$$

Prethodna propozicija je izravna posljedica teorema 3.1.3 te ju stoga nećemo dokazivati.

Eulerov teorem

Prisjetimo se Eulerovog teorema iz prvog poglavlja. On nam kaže da je broj particija od n u neparne dijelove jednak broju striktnih particija. U prvom poglavlju smo ovaj teorem dokazali bijektivno, a sada ćemo pokazati kako se može dokazati pomoću funkcija izvodnica.
Neka je $p'(n)$ broj particija od n u različite sumande i P' pripadna funkcija izvodnica. Neka je $p(n)$ broj particija u neparne sumande i P pripadna funkcija izvodnica. Trebamo pokazati da su te dvije funkcije izvodnice jednake. Ako su one jednake, onda su jednaki i koeficijenti uz x^n to jest $p(n) = p'(n)$. Prvo računamo $p'(n)$. Svaki prirodni broj k se ili ne pojavljuje kao sumand ili se pojavi točno jednom, što možemo zapisati kao $1 + x$. Odmah zapažamo

$$P'(x) = (1 + x)(1 + x^2)(1 + x^3)\ldots = \prod_{k=1}^{\infty}(1 + x^k).$$

Funkcija izvodnica za $p(n)$ je

$$\begin{aligned}P(x) &= (1 + x + x^2 + x^3 + \ldots)(1 + x^3 + x^6 + \ldots)(1 + x^5 + x^{10} + \ldots)\ldots\\ &= \frac{1}{1-x}\cdot\frac{1}{1-x^3}\cdot\frac{1}{1-x^5}\cdot\ldots.\end{aligned}$$

Proširivanjem i skraćivanjem razlomaka u $P'(x)$ dobijemo

$$\begin{aligned}P'(x) &= \frac{1-x^2}{1-x}\cdot\frac{1-x^4}{1-x^2}\cdot\frac{1-x^6}{1-x^3}\ldots\\ &= \frac{1}{1-x}\cdot\frac{1}{1-x^3}\cdot\frac{1}{1-x^5}\ldots\\ &= P(x).\end{aligned}$$

3.2 Merca-Schmidt teoremi

Jedan od rezultata koji govori o particijama prirodnog broja koje sadrže jedinice dan je Stanleyevim teoremom 1.3.5 u prvom poglavlju. Matematičari Mircea Merca i Maxie D. Schmidt dokazali su dva nova teorema o broju jedinica sadržanih u particijama. Prije samih teorema uvodimo novu oznaku koja će nam biti potrebna. Sa $S^{(r)}_{n,k}$ označavamo broj k-ova u particiji broja n gdje je najmanji dio barem r.

Teorem 3.2.1. *Neka je λ particija težine n. Tada je broj jedinica u particiji broja n jednak*

$$\sum_{k=2}^{n+1}\phi(k)S^{(2)}_{n+1,k}.$$

Prije dokaza, ilustrirajmo ovaj teorem kratkim primjerom.

Primjer 3.2.2. *Broj jedinica u particijama broja 5 je jednak 12. Particije broja 6 koje ne sadrže jedinicu su*

$$(6),\ (4,2),\ (3,3),\ (2,2,2).$$

Uočimo da vrijedi

$$\phi(2)\cdot 4+\phi(3)\cdot 2+\phi(4)\cdot 1+\phi(6)\cdot 1 = 4+4+2+2 = 12.$$

Iz ovoga možemo vidjeti da broj particija broja n koje sadrže jedinice možemo dobiti iz skupa particija broja $n-1$ na način da svakoj particiji dodamo jedinicu. Ovo je primjer bijekcije između dva skupa particija. Dakle, teorem povezuje skup particija broja n koje sadrže jedinicu i skup particija broja n koje ne sadrže jedinicu u particiji

$$\sum_{1+t_1+2t_2+\ldots+nt_n=n} t_1 = \sum_{2t_2+\ldots+nt_n=n} \phi(2)t_2+\ldots+\phi(n)t_n.$$

Slijedi dokaz teorema 3.2.1

Dokaz. Teorem ćemo dokazati koristeći funkcije izvodnice.
Uvodimo oznaku koju ćemo koristiti u dokazu:

$$(a;q)_\infty = \prod_{k=0}^{\infty}(1-aq^k).$$

Za sve $k \geq r$, funkcija izvodnica za particije glasi

$$\sum_{n=k}^{\infty} S_{n,k}^{(r)} q^n = (q^k+q^{2k}+\ldots)\cdot\frac{(1-q)(1-q^2)\ldots(1-q^{r-1})}{(q;q)_\infty} = \frac{q^k}{1-q^k}\cdot\frac{1}{(q^r;q)_\infty}.$$

Zbog toga što $(a;q)_\infty$ divergira kada je $a \neq 0$ i $|q| \leq 1$, kada god se $(a;q)_\infty$ pojavi u formuli pretpostavljamo da je $|q| < 1$. Slijedi

$$\frac{1-q}{(q;q)_\infty}\sum_{k=1}^{\infty}\frac{\phi(k)q^k}{1-q^k} = \frac{q}{(q;q)_\infty} + \sum_{n=2}^{\infty}\sum_{k=2}^{\infty}\phi(k)S_{n,k}^{(2)}q^n.$$

Iz

$$\sum_{k=1}^{\infty}\frac{\phi(k)q^k}{1-q^k} = \frac{q}{(1-q)^2},$$

imamo

$$\frac{1-q}{(q;q)_\infty}\sum_{k=1}^{\infty}\frac{\phi(k)q^k}{1-q^k} = \frac{q}{(q;q)_\infty} + \frac{q}{1-q}\cdot\frac{q}{(q;q)_\infty} = \frac{q}{(q;q)_\infty} + \sum_{n=1}^{\infty} S_{n,1}^{(1)} q^{n+1}.$$

Sada slijedi

$$S^{(1)}_{n,1} = \sum_{k=2}^{n+1} \phi(k) S^{(2)}_{n+1,k}$$

čime je tvrdnja teorema dokazana.
Osim pomoću funkcija izvodnica, teorem možemo dokazati i kombinatorno. Dokaz se može pronaći u [6]. □

Sada slijedi još jedan teorem koji povezuje Eulerovu funkciju i particije prirodnog broja n. Za potrebe ovog teorema uvodimo sljedeće: za $n > 2, P_\phi(n) = \frac{\phi(n)}{2}$ označava broj particija broja n u dva relativno prosta dijela.

Teorem 3.2.3. *Za $n \geq 0$ vrijedi*

$$p(n) = \sum_{k=3}^{n+3} P_\phi(k) S^{(3)}_{n+3,k}.$$

Dokaz. Pomoću funkcije izvodnice za $S^{(3)}_{n,k}$ imamo

$$\frac{(1-q)(1-q^2)}{(q;q)_\infty} \sum_{k=1}^{\infty} \frac{\phi(k) q^k}{1-q^k} = \frac{q+q^2-2q^3}{(q;q)_\infty} + \sum_{k=3}^{\infty} \sum_{n=3}^{\infty} \phi(k) S^{(3)}_{n,k} q^n$$

i

$$\frac{(1-q)(1-q^2)}{(q;q)_\infty} \sum_{k=1}^{\infty} \frac{\phi(k) q^k}{1-q^k} = \frac{q+q^2}{(q;q)_\infty}$$

Možemo zaključiti

$$\sum_{n=3}^{\infty} (\sum_{k=3}^{n} \phi(k) S^{(3)}_{n,k}) q^n = \frac{2q^3}{(q;q)_\infty} = \sum_{n=3}^{\infty} 2p(n-3) q^n.$$

Time smo izveli funkciju izvodnicu za $p(n)$,

$$\sum_{n=0}^{\infty} p(n) q^n = \frac{1}{(q;q)_\infty}.$$

□

Bibliografija

[1] K. Andrews, G.and Eriksson, *Integer partitions*, Cambridge University Press, 2004.

[2] A. Baker, *A concise introduction to the theory of numbers*, Cambridge University Press, 1985.

[3] ______, *A comprehensive course in number theory*, Cambridge University Press, 2012.

[4] A. Dujella, *Number theory*, Školska Knjiga, 2021.

[5] Patashnik O. Graham R., Knuth D., *Concrete Mathematics*, Addison-Wesley publishing company, 1990.

[6] Merca M. i Schmidt D. Maxie, *A Partition Identity Related to Stanley's Theorem*, American Mathematical Monthly **125** (2018), br. 10, 929–933.

[7] I. Martinjak, *Eulerov pentagonalni teorem*, Matematičko fzički list **261** (2015), br. 2, 243–249.

[8] ______, *O Eulerovom teoremu o particijama*, Osječki matematički list **16** (2016), br. 1, 1–14.

[9] B. Sury, *Ramanujan's awesome sums*, Mathematics Newsletter **24** (2013), br. 2, 31–36.

[10] D. Veljan, *Kombinatorna i diskretna matematika*, Algoritam, 2001.

Sažetak

U ovom diplomskom radu prikazujemo primjenu Eulerove funkcije u teoriji particija. Definiramo pojam particije prirodnog broja i obrađujemo osnove teorije particija. Particije prirodnog broja reprezentiramo Youngovim dijagramima i pomoću tog grafičkog prikaza dokazujemo osnovne identitete za particijsku funkciju. Dokazujemo Eulerov teorem, po kojem je broj striktnih particija jednak broju particija s neparnim dijelovima, za danu težinu.

Prikazujemo najpoznatije aritmetičke funkcije, kao što su pod, strop, Eulerova i Möbiusova funkcija. Dajemo kratki osvrt na Ramanujanove sume, koje se pojavljuju u više područja matematike i imaju istaknuta brojevna svojstva.

Suvremeni matematičari Mircea Merca i Maxie D. Schmidt otkrili su intrigantnu prisutnost aritmetičkih funkcija u teoriji particija. Prikazujemo njihova dva teorema iz 2017. godine. U svrhu dokazivanja ovih rezultata uvodimo funkcije izvodnice. Također, dokazujemo Eulerov teorem pomoću funkcija izvodnica.

Summary

In this Master thesis, we present the application of the Euler function in the theory of partitions. We define the concept of partition of a natural number and discuss the basics of partition theory. We represent partitions of natural numbers using Young diagrams and use this graphical representation to prove basic identities for the partition function. We prove Euler's theorem, according to which the number of strict partitions is equal to the number of partitions with odd parts, for a given weight.

We present the most famous arithmetic functions, such as floor, ceiling, Euler's, and Möbius function. We give a brief overview of Ramanujan's sums, which appear in various areas of mathematics and have prominent numerical properties.

Contemporary mathematicians Mircea Merca and Maxie D. Schmidt discovered the intriguing presence of arithmetic functions in partition theory. We present their two theorems from 2017. In order to prove these results, we introduce generating functions. Additionally, we prove Euler's theorem using generating functions.

Životopis

Rođena sam 20.03.1998. u Remscheidu, Savezna Republika Njemačka. Osnovnu i srednju školu pohađala sam u Zagrebu. Nakon srednjoškolskog obrazovanja, 2016. upisujem preddiplomski studij Matematike na Prirodoslovno-matematičkom fakultetu u Zagrebu gdje 2021. upisujem i diplomski studij Računarstva i matematike.