O nekim Eulerovim doprinosima u teoriji brojeva

Cafuk, Jelena

Master's thesis / Diplomski rad

2018

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: University of Zagreb, Faculty of Science / Sveučilište u Zagrebu, Prirodoslovno-matematički fakultet

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:217:863766

Rights / Prava: In copyright

Download date / Datum preuzimanja: 2021-05-10

Repository / Repozitorij:

Repository of Faculty of Science - University of Zagreb
Jelena Cafuk

O NEKIM EULEROVIM DOPRINOSIMA U TEORIJI BROJEVA

Diplomski rad

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

Zagreb, rujan, 2018.
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. ______________________
Diplomski rad napravljen je u sklopu aktivnosti Projekta KK.01.1.1.01.0004 - Znanstveni centar izvrsnosti za kvantne i kompleksne sustave te reprezentacije Liejevih algebri.
Sadržaj

Sadržaj iv

Uvod 3

1 Djeljivost 4
  1.1 Osnovni pojmovi 4
  1.2 Fermatovi brojevi 5
  1.3 Savršeni brojevi 6
  1.4 Prijateljski brojevi 9

2 Euler-Fermatov teorem 12
  2.1 Mali Fermatov teorem 12
  2.2 Prvi dokaz MFT-a 13
  2.3 Drugi dokaz MFT-a 16
  2.4 Treći dokaz MFT-a 17
  2.5 Četvrti dokaz MFT-a 20
  2.6 Eulerov teorem 24
  2.7 Svojstva Eulerove funkcije 25

3 Sume kvadrata 27
  3.1 Sume dva kvadrata 27
  3.2 Sume četiri kvadrata 33

4 Kvadratni ostatci 34
  4.1 Legendreov simbol 34
  4.2 Eulerov kriterij 35
  4.3 Svojstva Legendreova simbola 37

5 Veliki Fermatov teorem 38
  5.1 Fermatova slutnja 38
SADRŽAJ

5.2 Eulerov doprinos ................................................................. 39

6 Pellova jednadžba ................................................................. 43
   6.1 Eulerovi primjeri ............................................................ 44
   6.2 Veza s verižnim razlomcima ........................................... 47

Bibliografija ........................................................................ 52


Zbog nestabilne političke situacije u St. Peterburgu, na poziv pruskog kralja Frederika II., 1741. godine Euler se s obitelji preselio u Berlin. Na Berlinskoj je akademiji dobio mjesto voditelja odjela za matematiku. No s godinama su se zaoštrili odnosi između Frederika II. i Eulera. Eulerovo je nezadovoljstvo Berlinskom akademijom sve više raslo te se 1766. godine na poziv ruske carice Katarine Velike s obitelji vratio u St. Peterburg i Rusku akademiju. Godinama se borio s mrenom
Leonhard Euler je bio jedan od najplodnijih i najsvestranijih matematičara svih vremena. Za vrijeme svog života napisao je preko 500 radova, a gotovo 400 ih je objavljeno posthumno. Njegovi su znanstveni doprinosi obogatili svaku matematičku granu tog vremena, a pridonio je razvoju mnogih područja, primjerice balistici, kartografiji, hidrodinamici, hidraulici, teoriji glazbe i mnogim drugim. Smatra ga se osnivačem opće teorije diferencijalnih jednadžbi. 1748. godine izdao je knjigu iz matematičke analize *Introductio in analysin infinitorum* u kojoj definira pojam funkcije te proučava verižne razlomke, eksponencijalnu i logaritamsku funkciju, trigonometrijske funkcije, Eulerove kutove i drugo. Uveo je oznake $f(x)$ za zapis pravila pridruživanja realne funkcije, oznaku imaginarnje jedinice $i$ te slovo $e$ za bazu prirodnog logaritma. Dokazao je da je broj $e$ iracionalan broj. Eksponencijalnu je funkciju razvio u red i povezao ju s trigonometrijskim funkcijama iz čega je proizašla čuvena Eulerova formula:

$$e^{i\varphi} = \cos \varphi + i \sin \varphi, \quad \forall \varphi \in \mathbb{R}.$$  

Postavio je temelje suvremene diferencijalne geometrije i teorije grafova. Naime, Euler je prvi riješio problem Königsbergskih mostova, a u pismu Goldbachu 1750.
godine iskazao je Eulerovu poliedarsku formulu koju je kasnije i detaljnije analizirao. 1765. godine Euler je dokazao da težište trokuta, središte trokuta opisane kružnice i njegov ortocentar leže na jednom pravcu kojeg danas nazivamo Eulerovim pravcem. Dokazao je i da je udaljenost težišta trokuta do ortocentra dvostruko dulja od udaljenosti težišta do središta trokuta opisane kružnice.

Veliki se dio Eulerova opusa odnosi na teoriju brojeva. Neki njegovi doprinosi toj, u to doba ne tako popularnoj grani matematike, predstavljaju temu ovog rada. Zbog lakšeg razumijevanja i kraćeg zapisa u radu uglavnom rabimo suvremenu matematičku terminologiju i simboliku koje nisu postojale u Eulerovo doba.
Poglavlje 1

Djeljivost

1.1 Osnovni pojmovi

U ovom su odjeljku navedene definicije, oznake i važnija svojstva nekih pojmova iz teorije brojeva koja su korisna za razumijevanje sadržaja rada.

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

Za djelitelja $d \in \mathbb{N}$ prirodnog broja $n$ kažemo da je pravi ako je $d \neq n$.

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

Definicija 1.1.3. Neka su $b$ i $c$ cijeli brojevi. Cijeli broj $a$ zovemo zajedničkim djeliteljem brojeva $b$ i $c$ ako $a$ dijeli $b$ i $c$. Najveći među njima zove se najveći zajednički djelitelj i označava se $(b, c)$.

Prema definiciji najvećeg zajedničkog djelitelja brojeva $b$ i $c$ jasno je da je $(b, c)$ prirodan broj.

Definicija 1.1.4. Prirodni brojevi $a$ i $b$ su relativno prosti ako im je najveći zajednički djelitelj 1.

Definicija 1.1.5. Prirodan broj veći od 1 je prost ili prim broj ako nema pravog djelitelja većeg od 1. U suprotnom kažemo da je broj složen. Broj 1 nije niti prost, niti složen.

Uočimo da je broj prost ako i samo ako ima točno dva djelitelja, 1 i sebe samog.
POGLAVLJE 1. DJELJIVOST

Definicija 1.1.6. Ako cijeli broj \( m \neq 0 \) dijeli razliku \( a - b \), onda kažemo da je \( a \) kongruentan \( b \) modulo \( m \) i pišemo \( a \equiv b \pmod{m} \). U protivnom kažemo da je \( a \) nekongruentan \( b \) modulo \( m \) i pišemo \( a \not\equiv b \pmod{m} \).

Oznaku za kongruenciju te teoriju vezanu uz nju uveo je 1801. godine Gauss \(^1\) pa ju Euler nije mogao poznavati ni rabiti. Mi ćemo ipak u mnogim Eulerovim tvrdnjama i dokazima koristiti kongruencije zbog preglednijeg zapisa i boljeg razumijevanja.

Navedimo osnovna svojstva kongruencija.

Propozicija 1.1.7. Neka su \( a, b, c \text{ i } d \) cijeli brojevi i \( m \) prirodan.

1. Ako je \( a \equiv b \pmod{m} \) i \( c \equiv d \pmod{m} \), onda je \( a + c \equiv b + d \pmod{m} \), \( a - c \equiv b - d \pmod{m} \) i \( ac \equiv bd \pmod{m} \).

2. Ako je \( a \equiv b \pmod{m} \) i \( d \mid m \), onda je \( d \mid a \equiv b \pmod{d} \).

3. Ako je \( a \equiv b \pmod{m} \) i \( c \neq 0 \), onda je \( ac \equiv bc \pmod{mc} \).

Propozicija 1.1.8. Neka su \( a, b, c \in \mathbb{Z} \), \( m \in \mathbb{N} \), te \( (c, m) = d \). Tada je \( ac \equiv bc \pmod{m} \) ako i samo ako \( a \equiv b \pmod{\frac{m}{d}} \).

U slučaju \( (a, m) = 1 \) vrijedi da je relacija \( ac \equiv bc \pmod{m} \) ekvivalentna relaciji \( a \equiv b \pmod{m} \).

1.2 Fermatovi brojevi


U Eulerovo su se doba Fermatove pretpostavke uglavnom mogle pronaći u tri izvora: u *Commercium Epistolicum* (1658.) u kojem su objavljena neka Fermatova pisma, u Bachetovom prijevodu Diofantove *Arithmetice* s Fermatovim bilješkama (1670.) te u djelu *Varia Opera* (1679.). Jedna od osoba s kojom se Fermat najviše dopisivao bio je redovnik Marin Mersenne (1588. - 1648.). U jednom je pismu Mersenneu Fermat postavio hipotezu da su svi brojevi oblika \( 2^{2^n} + 1 \), gdje je \( n \) nenegativan

\(^1\) Johann Karl Friedrich Gauss, 1777. - 1855., njemački matematičar i fizičar.
cijeli broj, prosti. Postavljenu je hipotezu Fermat provjerio za \( n = 0, 1, 2, 3, 4 \), ali svoju tvrdnju nije dokazao. Euler je za hipotezu saznao iz pisma kojeg mu je 1. prosinca 1729. uputio Goldbach te ga pritom upitao:

"Je li Vam poznato Fermatovo mišljenje da su brojevi oblika \( 2^{2x-1} + 1 \), kao što su 3, 5, 17, ..., prosti? On to nije dokazao, a koliko znam nije niti itko drugi."

Christian Goldbach (1690. - 1764.) bio je pruski matematičar koji je u jednom pismu Euleru postavio jednu od najpoznatijih hipoteza iz teorije brojeva. Kao i Fermat, više je volio postavljati hipoteze nego ih dokazivati.

**Slutnja 1** (Goldbachova hipoteza). **Svaki je prirodan broj veći od 2 moguće napisati kao zbroj dva prosta broja.**

Euler je prvotno Fermatovu hipotezu smatrao nebitnom. No Goldbach ga je ipak uspio zainteresirati za teoriju brojeva i postavljenu hipotezu te ju je u rujnu 1732. godine Euler opovrgnuo. Naime, za \( n = 5 \) je dobio:

\[
2^{2^5} + 1 = 2^{32} + 1 = 641 \cdot 6700417.
\]

Danas brojeve oblika \( 2^n + 1 \) nazivamo \textit{Fermatovim brojevima}. Fermatove je proste brojeve iskoristio Gauss pri opisivanju kriterija koji govori koje je pravilne \( n \)-terokute moguće konstruirati samo ravnalom i šestarom. Za neparan \( n \), kružnicu je ravnalom i šestarom moguće podijeliti na \( n \) jednaka dijelova samo ako je \( n \) kvadratno slobodan produkt Fermatovih prostih brojeva. Općenito, pravilni \( n \)-terokut se može konstruirati ravnalom i šestarom ako i samo ako je \( n \) potencija broja 2 ili je \( n = 2^r p_1 p_2 \cdots p_k \), gdje je \( r \) nenegativan cijeli broj, a \( p_i \) različiti Fermatovi prosti brojevi.

### 1.3 Savršeni brojevi

Već spomenuti Marin Mersenne bio je svestran matematičar i fizičar koji je oko sebe okupljao velik broj intelektualaca među kojima su bili Pierre de Fermat, Blaise Pascal⁴, René Descartes⁵, John Pell⁴, Girard Desargues⁵ i mnogi drugi. Sa suvremenicima je često komunicirao putem pisama. Katkada im je davao ideje za daljnja istraživanja, a katkada je bio samo posrednik. Omgudio je razmjenu ideja među matematičarima i time neupitno utjecao na mnoge od njih. Mersenne je proučavao alkemiju, astrologiju i fizikalne i matematičke probleme. Međuostalim, bavio se i teorijom brojeva. Pokušavao je pronaći formulu za prose brojeve te je pritom proučavao brojeve oblika \( 2^n - 1 \), gdje je \( n \) prirodan broj.

—

⁴Blaise Pascal, 1623. - 1662., francuski matematičar i fizičar.
⁵René Descartes, 1596. - 1650., francuski matematičar zaslužan za otkriće analitičke geometrije.
⁶John Pell, 1611. - 1685., engleski matematičar.
⁵Girard Desargues, 1591. - 1661., francuski matematičar, inženjer i arhitekt.
POGLAVLJE 1. DJELJIVOST

Definicija 1.3.1. Brojevi oblika $2^n - 1$, $n \in \mathbb{N}$ se nazivaju Mersenneovim brojevima. Mersenneove brojeve koji su prosti nazivamo Mersenneovim prostim brojevima.

Do danas nije poznato postoji li konačno ili beskonačno mnogo Mersenneovih prostih brojeva. Sluti se da ih je beskonačno.

Slutnja 2. Postoji beskonačno mnogo Mersenneovih prostih brojeva.

Najveći do sada poznat Mersenneov prost broj otkriven je početkom 2018. godine, $2^{77,232,917} - 1$, broj s preko 23 milijuna znamenaka. Potraga za sve većim Mersenneovim prostim brojevima traje u sklopu međunarodnog projekta Great Internet Mersenne Prime Search ili kraće GIMPS koji uključuje niz matematičara i programera kao profesionalaca, tako i amatere. S jačanjem računala, pronalaze se sve veći brojevi koji idu u prilog tezi da bi ih moglo biti beskonačno.

Propozicija 1.3.2. Neka je $2^n - 1$ prost broj. Tada je $n$ prost.

Zbog prethodne propozicije je jasno da Mersenneove proste brojeve tražimo među onima oblika $2^p - 1$, za $p$ prost. Obrat prethodne propozicije ne vrijedi, a najmanji prost za kojeg to ne vrijedi je $p = 11$. Zaista, $2^{11} - 1 = 23 \cdot 89$.

Definicija 1.3.3. Za prirodan broj $n$ kažemo da je savršen ako je jednak sumi svih svojih pravih djelitelja.

Definicija 1.3.4. Funkcija $\sigma : \mathbb{N} \to \mathbb{N}$ svakom prirodnom broju pridružuje sumu svih njegovih pozitivnih djelitelja. Dakle, za $n \in \mathbb{N}$ je

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

S obzirom na prethodne dvije definicije vidimo da je prirodan broj $n$ savršen ako i samo ako je $\sigma(n) = 2n$.

Funkcija $\sigma$ zadovoljava vrlo važno svojstvo multiplikativnosti. To znači da vrijede sljedeća dva svojstva:

1. $\sigma(1) = 1$,
2. $\sigma(mn) = \sigma(m)\sigma(n)$ za sve $m, n \in \mathbb{N}$ takve da je $(m, n) = 1$.

Očito vrijedi da je prirodan broj $p$ prost ako i samo ako je

$$\sigma(p) = p + 1.$$
POGLAVLJE 1. DJELJIVOST

Nadalje, ako je \( n = p^\alpha \) gdje je \( p \) prost broj i \( \alpha \in \mathbb{N} \), tada je

\[
\sigma(n) = 1 + p + p^2 + \cdots + p^\alpha = \frac{p^{\alpha+1} - 1}{p - 1}.
\]

Koristeći svojstvo multiplikativnosti funkcije lako se može ustanoviti sljedeće:

**Propozicija 1.3.5.** Neka je \( n > 2 \) prirodan broj čiji je kanonski rastav dan s

\[
n = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}.
\]

Tada je

\[
\sigma(n) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \cdots \frac{p_k^{\alpha_k+1} - 1}{p_k - 1}.
\]


**Teorem 1.3.6.** Paran prirodan broj \( n \) je savršen ako i samo ako se može prikazati u obliku

\[
n = 2^{p-1}(2^p - 1),
\]

dje su \( p \) i \( 2^p - 1 \) prosti brojevi.

**Dokaz.** \( \Leftarrow \): Neka su \( p \) i \( 2^p - 1 \) prosti brojevi te neka je \( n = 2^{p-1}(2^p - 1) \). Tada vrijedi:

\[
\sigma(n) = \sigma(2^{p-1})\sigma(2^p - 1) = (1 + 2 + \ldots + 2^{p-1})(1 + 2^p - 1)
\]

\[
= \frac{2^p - 1}{2 - 1}2^p = 2^p(2^p - 1) = 2n.
\]

\( \Rightarrow \): Neka je \( n \) paran savršen broj oblika \( n = 2^k \cdot m \), gdje su \( k, m \in \mathbb{N} \) i \( m \) neparan. Kako su \( 2^k \) i \( m \) očito relativno prosti, vrijedi:

\[
\sigma(n) = \sigma(2^k \cdot m) = \sigma(2^k)\sigma(m) = \left(2^{k+1} - 1\right)\sigma(m).
\]

Nadalje, jer je \( n \) savršen vrijedi

\[
\sigma(n) = 2n = 2^{k+1} \cdot m,
\]

\footnote{Euklid Aleksandrijski, oko 330. - 275., grčki matematičar čije se najpoznatije djelo zove *Elementi*.}
POGLAVLJE 1. DJELJIVOST

pa je
\[ (2^{k+1} - 1) \sigma(m) = 2^{k+1} \cdot m. \] \hspace{1cm} (1.1)

Otuda slijedi da \( 2^{k+1} - 1 \) dijeli \( 2^{k+1} \cdot m \). Kako su \( 2^{k+1} \) i \( 2^{k+1} - 1 \) relativno prosti, dobivamo da \( 2^{k+1} - 1 \) mora dijeliti \( m \). Stoga, \( m \) možemo zapisati kao
\[ m = (2^{k+1} - 1) l, \]
za neki \( l \in \mathbb{N} \). S druge strane, prema (1.1) je
\[ \sigma(m) = 2^{k+1} \cdot \frac{m}{2^{k+1} - 1} = 2^{k+1} \cdot l. \]

Promotrimo sada dva moguća slučaja:

1. Neka je \( l > 1 \). Tada je \( \sigma(m) \geq l + m + 1 \), a to je nemoguće jer je
\[ \sigma(m) = 2^{k+1} \cdot l = 2^{k+1}l - l + l = (2^{k+1} - 1) l + l = m + l < l + m + 1. \]

2. Neka je \( l = 1 \). Tada je \( \sigma(m) = m + 1 \), iz čega slijedi da je \( m \) prost broj. No, ako je \( 2^{k+1} - 1 \) prost broj, onda je \( k + 1 = p \) također prost broj pa je \( n = 2^{p-1}(2^p - 1) \).

Euler je 1772. otkrio i 8. savršeni broj, broj 2305843008139952128. Do danas nije poznato postoji li beskonačno ili konačno mnogo savršenih brojeva jer je to očito u direktnoj vezi sa Slutnjom \[2\] niti mogu li oni biti neparni. Do sada nije pronađen niti jedan neparan savršen broj.

1.4 Prijateljski brojevi

Osim savršenih brojevima, Euler se zanimao i za tzv. prijateljske brojeve. Otkrio je 62 para prijateljskih brojeva.

Definicija 1.4.1. Za dva prirodna broja kažemo da su prijateljski brojevi ako je svaki od ta dva broja jednak zbroju svih pravih djelitelja drugog broja.

Ako su \( m \) i \( n \) prijateljski, onda je \( \sigma(m) - m = n \) i \( \sigma(n) - n = m \). Stoga su \( m \) i \( n \) prijateljski ako i samo ako je
\[ \sigma(m) = \sigma(n) = m + n. \]

Za savršene brojeve možemo reći da su to oni brojevi koji su prijateljski sami sa sobom.
Primjer 1.4.2. Brojevi 220 i 284 su prijateljski.
Pravi djeljitelji broja 220 su 1, 2, 4, 5, 10, 11, 20, 22, 44, 55 i 110 i njihova suma iznosi 284.
Pravi djeljitelji broja 284 su 1, 2, 4, 71 i 142 i njihova suma iznosi 220.


Teorem 1.4.3 (Thabitov teorem o prijateljskim brojevima). Ako su za neki prirodan broj \( n > 1 \) brojevi \( p = 3 \cdot 2^{n-1}, q = 3 \cdot 2^{n-1} - 1 \) i \( r = 9 \cdot 2^{2n-1} - 1 \) prosti, onda su brojevi \( 2^n pq \) i \( 2^n r \) prijateljski.

Do danas su poznata samo 3 takva para brojeva koji se dobiju za \( n = 2, n = 4 \) te \( n = 7 \).

Definicija 1.4.4. Brojevi oblika \( 3 \cdot 2^n - 1 \) zovu se Thabitovi brojevi.

Euler je generalizirao Thabitov teorem o prijateljskim brojevima i time omogućio pronažak još dva para prijateljskih brojeva.

Teorem 1.4.5 (Eulerovo pravilo). Neka su \( m \), \( n \) prirodni brojevi, \( n > m \), takvi da su

\[
p = \left(2^{n-m} + 1\right) \cdot 2^m - 1, \quad q = \left(2^{n-m} + 1\right) \cdot 2^n - 1, \quad r = \left(2^{n-m} + 1\right)^2 \cdot 2^{m+n} - 1
\]

prosti brojevi. Tada su brojevi \( 2^n pq \) i \( 2^n r \) prijateljski.

Dokaz. Djelitelji broja \( 2^n pq \) su oblika \( 2^i, 2^i p, 2^i q, 2^i pq \), gdje je \( i = 0, \ldots, n \) pa je

\[
\sigma(2^n pq) - 2^n pq = \sum_{i=0}^{n} 2^i + \sum_{i=0}^{n} 2^i p + \sum_{i=0}^{n} 2^i q + \sum_{i=0}^{n-1} 2^i pq
\]

\[
= \sum_{i=0}^{n-1} 2^i(1 + p + q + pq) + 2^n + 2^n p + 2^n q
\]

\[
=(2^n - 1)(1 + p + q + pq) + 2^n + 2^n p + 2^n q
\]

\[
=2^{n+1}(1 + p + q) + 2^n pq - 1 - p - q - pq.
\]
POGLAVLJE 1. DJELJIVOST

Kada uvrstimo \( p = (2^{n-m} + 1) \cdot 2^m - 1 \) i \( q = (2^{n-m} + 1) \cdot 2^n - 1 \), dobivamo

\[
\sigma(2^n pq) - 2^n pq = 2^{2n+m} + 2^{4n-m} + 2^{3n+1} - 2^n
= 2^n \left[ (2^{n-m} + 1)^2 \cdot 2^{m+n} - 1 \right]
= 2^n r.
\]

Djelitelji broja \( 2^n r \) su oblika \( 2^i, 2^i r \), gdje je \( i = 0, \ldots, n \) pa je

\[
\sigma(2^n r) - 2^n r = \sum_{i=0}^{n} 2^i + \sum_{i=0}^{n-1} 2^i r = (2^n - 1)(1 + r) + 2^n = 2^n(2 + r) - 1 - r.
\]

Nakon uvrštavanja \( r = (2^{n-m} + 1)^2 \cdot 2^{m+n} - 1 \) i sređivanja izraza dobivamo

\[
\sigma(2^n r) - 2^n r = 2^n \left( 1 + 2^{3n-m} + 2^{2n+1} + 2^{m+n} - 2^{2n-m} - 2^{n+1} - 2^{m} \right)
= 2^n \left[ \left( (2^{n-m} + 1) \cdot 2^m - 1 \right) \left( (2^{n-m} + 1) \cdot 2^n - 1 \right) \right]
= 2^n pq.
\]

Kako je

\[
\sigma(2^n pq) = 2^n pq + 2^n r = \sigma(2^n r),
\]
brojevi \( 2^n pq \) i \( 2^n r \) su prijateljski. \( \square \)

Primijetimo, kada u Teoremu 1.4.5 uvrstimo \( m = n - 1 \) dobivamo Thabitov teorem o prijateljskim brojevima. Nadalje, brojevi iz Primjera 1.4.2 su oblika danog u Teoremu 1.4.5 za \( n = 2 \) i \( m = 1 \) (te \( p = 5, q = 11, r = 71 \)).
Poglavlje 2

Euler-Fermatov teorem

2.1 Mali Fermatov teorem

Jedan od Fermatovih najvažnijih teorema nalazimo u njegovom pismu upućenom Frenicle de Bessyju 18. listopada 1640. Pismo je objavljeno u ranije spomenutom djelu Varia Opera, a teorem je danas poznat pod nazivom Mali Fermatov teorem, u daljnjem kraće MFT. Kasnije će se pokazati da upravo taj teorem omogućava najlakši način faktorizacije Fermatovih brojeva. Moguće je da ga je čak Euler iskoristio za pronalazak faktora 641 Fermatovog broja $2^{31} + 1$.

Originalan Fermatov iskaz, u suvremenoj terminologiji, glasio je:

Fermat je izostavio nužan uvjet da $p$ i $a$ nemaju zajedničkih faktora, odnosno da $p \nmid a$.

Danas pod nazivom Mali Fermatov teorem podrazumijevamo sljedeću tvrdnju.

**Teorem 2.1.1 (MFT).** Ako je $p$ prost broj i $a$ prirodan broj koji nije djeljiv s $p$, onda je $a^{p-1} - 1$ djeljiv s $p$.

Ponekad se iskaz formulira i na sljedeći način:

**Teorem 2.1.2 (MFT).** Ako je $p$ prost broj, onda $p$ dijeli $a^p - a$.

Uočimo da su tvrdnje Teorema 2.1.1 i 2.1.2 ekvivalentne. Zaista, trivijalno iz $p \mid a^{p-1} - 1$ slijedi $p \mid a^p - a$. Obratno, ako $p \mid a^p - a = a(a^{p-1} - 1)$ i $p \nmid a$, tada $p \mid a^{p-1} - 1$.

---

1Bernard Frénicle de Bessy, oko 1604. – 1674., francuski matematičar koji je posebnu pažnju posvetio teoriji brojeva i kombinatorici.
Fermata je za iskaz gornje tvrdnje vjerojatno “inspirirao” binomni identitet. Za cijeli broj $a$ i prost broj $p$ vrijedi:

$$(a + 1)^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k} = a^p + \sum_{1\leq k<p} \binom{p}{k} a^{p-k} + 1.$$  

Činjenica da su binomni koeficijenti $\binom{p}{k}$, $1 \leq k < p$, djeljivi s $p$ nije sama po sebi dovoljna da bi se teorem i dokazao. Nije poznato je li Fermat znao dokazati navedeni teorem. U onom što slijedi navesti ćemo nekoliko varijanti dokaza MFT-a za koje je zaslužan Euler.

**Teorem 2.1.3** (Mali Fermatov teorem u Eulerovoj formulaciji). *Ako je $p$ prost broj, onda svaka potencija s eksponentom $p - 1$ pri dijeljenju s $p$ daje ostatak 0 ili 1.*

### 2.2 Prvi dokaz MFT-a


Neki smatraju da je od upravo ovoga trenutka Euler postao uvjeren kako je teorija brojeva matematička grana vrijedna zanimanja. Ono što je Eulera smetalo proučavajući Fermatova djela bio je njegov nedovoljno znanstveni pristup koji se oslanjao više na intuiticiju, nego na matematički dokaz.

Euler dokazuje MFT koristeći princip matematičke indukcije, što je za ono vrijeme rijetko. Štoviše, ne samo da daje dokaz već detaljno opisuje proces iz kojeg je proizašao sam dokaz. Najprije je krenuo od specijalnog slučaja za $a = 2$. Nazovimo to pomoćnom tvrđnjom.

**Lema 2.2.1.** *Ako je $p$ neparan prost broj, onda je $2^{p-1} - 1$ djeljivo s $p$. *

*Dokaz.* Prema Binomnom poučku vrijedi

$$(1+1)^{p-1} = \sum_{k=0}^{p-1} \binom{p-1}{k} = 1 + \sum_{k=1}^{p-1} \frac{p-1}{1} \cdot \frac{(p-1)(p-2)}{1 \cdot 2} + \cdots + \frac{(p-1)(p-2)}{1 \cdot 2} + \frac{p-1}{1} + 1.$$ 

\[\text{Gottfried Wilhelm Leibniz, 1646.} - 1716., \text{njemački matematičar, jedan od utemeljitelja modernog infinitezimalnog računa.}\]
POGLAVLJE 2. EULER-FERMATOV TEOREM

Broj pribrojnika u gornjem izrazu je jednak \( p \) pa ih ima neparan broj. Oduzmemo li izrazu 1, ostaje nam paran broj pribrojnika pa preostalu sumu, odnosno pribrojnine, možemo grupirati na sljedeći način:

\[
(1 + 1)^{p-1} - 1 = \left( \binom{p-1}{1} + \binom{p-1}{2} \right) + \left( \binom{p-1}{3} + \binom{p-1}{4} \right) + \ldots \\
+ \left( \binom{p-1}{p-2} + \binom{p-1}{p-1} \right).
\]

Sada primijenimo pravilo za binomne koeficijente

\[
\binom{p-1}{k-1} + \binom{p-1}{k} = \binom{p}{k}
\]

i dobivamo

\[
(1 + 1)^{p-1} - 1 = \binom{p}{2} + \binom{p}{3} + \ldots + \binom{p}{p-1}.
\]

Kako je za \( 1 \leq k < p \),

\[
\binom{p}{k} = \frac{p(p-1) \cdots (p-k+1)}{1 \cdot 2 \cdots k},
\]

vidimo da \( p \) dijeli \( \binom{p}{k} \), odnosno dijeli zbroj na desnoj strani jednakosti. Stoga

\[ p \mid 2^{p-1} - 1. \]

No Euler ovaj dokaz nije mogao poopćiti pa je uočio da bi od veće koristi bila malo izmijenjena tvrdnju koju iznosimo kao sljedeću lemu. Ta će lema ujedno činiti bazu matematičke indukcije u dokazu MFT-a.

**Lema 2.2.2.** Ako \( p \) prost broj, onda \( p \) dijeli \( 2^p - 2 \).

**Dokaz.** Neka je \( p \neq 2 \) prost broj, tj. \( p \) je neparan prost. Tada vrijedi:

\[
(1 + 1)^p - 2 = 1 + p + \frac{p(p-1)}{1 \cdot 2} + \frac{p(p-1)(p-3)}{1 \cdot 2 \cdot 3} + \ldots + p + 1 - 2 \\
= p + \frac{p(p-1)}{1 \cdot 2} + \frac{p(p-1)(p-3)}{1 \cdot 2 \cdot 3} + \ldots + p
\]

iz čega je vidljivo da \( p \) dijeli svaki pribrojnik pa dijeli i \( 2^p - 2 \).

Za \( p = 2 \) tvrdnja očito vrijedi.
Kao što smo već uočili u prethodnom odjeljkueme, Leme 2.2.1 i 2.2.2 su ekvivalentne. Euler je potom uočio da iz činjenice da \( p \) dijeli \( 2^{p-1} - 1 \) slijedi da \( p \) dijeli \( 2^{p-1} - 1, 4^{p-1} - 1, 8^{p-1} - 1 \), odnosno vrijedi:

**Korolar 2.2.3.** Neka je \( p \neq 2 \) prost broj, onda \( p \) dijeli brojeve oblika
\[
2^{k(p-1)} - 1, \ k \in \mathbb{N}.
\]

Čini se da je u ovom trenutku Euler razmišlao o sljedećoj strategiji u dokazu: ako tvrdnju pokaže za sve proste brojeve \( a \), onda ju je zbog prethodnog korolara pokazao i za sve potencije \( a^n \), ali i za sve umnoške prostih brojeva. Zaista, ako \( p \mid a^{p-1} - 1 \) i \( p \mid b^{p-1} - 1 \), onda \( p \mid (a^{p-1} - 1)(b^{p-1} - 1) \). Kako je \( (a^{p-1} - 1)(b^{p-1} - 1) = (ab)^{p-1} - 1 - (a^{p-1} - 1) - (b^{p-1} - 1) \), slijedi da \( p \mid (ab)^{p-1} - 1 \).

Zato se kao sljedeći korak nametnuo dokaz za sljedeći prost broj \( a = 3 \).

**Lema 2.2.4.** Ako je \( p \) prost broj, onda \( p \) dijeli \( 3^p - 3 \).

**Dokaz.** Vrijedi:
\[
3^p = (1 + 2)^p = \sum_{k=0}^{p} \binom{p}{k} 2^k = 1 + p \cdot 2 + \frac{p(p-1)}{2} \cdot 4 + \cdots + 2^p.
\]
Svaki pribrojnik, osim prvog i zadnjeg, djeljiv je \( p \), pa je \( 3^p - 3 = 3^p - 3 \). prema Lemi 2.2.2 imamo da \( p \) dijeli \( 2^p - 2 \). Slijedi da
\[
p \mid 3^p - 3.
\]

Sada bi se tvrdnja MFT-a mogla pokazati za sljedeći prost broj \( 5 = 4 + 1 \) gdje bi kako pretpostavku indukcije koristili Korolar 2.2.3. No može i jednostavnije. Pretpostavka da tvrdnja MFT-a vrijedi za prirodan broj \( a \) povlači da vrijedi i za \( a + 1 \). To je upravo korak indukcije opisan u sljedećoj lemi.

**Lema 2.2.5.** Neka je \( p \) prost broj i \( a > 1 \) prirodan broj takav da \( p \) dijeli \( a^p - a \). Tada \( p \) dijeli \( (a + 1)^p - (a + 1) \).

**Dokaz.** Vrijedi:
\[
(a + 1)^p - (a + 1) = \sum_{k=0}^{p} \binom{p}{k} a^{p-k} - (a + 1) = a^p + \sum_{k=1}^{p-1} \binom{p}{k} a^{p-k} + 1 - a - 1 = (a^p - a) + \sum_{k=1}^{p-1} \binom{p}{k} a^{p-k}.
\]
POGLAVLJE 2. EULER-FERMATOV TEOREM

Prema pretpostavci leme $p \mid a^p - a$. Nadalje, $p \mid \left(\frac{a}{p}\right)$ za sve $1 \leq k < p$, pa $p$ dijeli desnu strane gornje jednakosti i stoga $p \mid (a + 1)^p - (a + 1)$.

MFL slijedi prema principu matematičke indukcije. Lema 2.2.2 predstavlja bazu, a Lema 2.2.5 korak indukcije.

2.3 Drugi dokaz MFT-a


\begin{figure}[h]
\centering
\includegraphics[width=0.7\textwidth]{goldbach_euler_letter.png}
\caption{Goldbachovo pismo Euleru, 1742. godina}
\end{figure}

**Lema 2.3.1.** Neka su $a, b$ cijeli brojevi i $p$ prost. Tada $p$ dijeli $(a + b)^p - a^p - b^p$.

**Dokaz.** Očito iz

$$(a + b)^p - a^p - b^p = \sum_{k=1}^{p-1} \binom{p}{k} a^{p-k} b^k.$$

Sada baza indukcije predstavlja specijalan slučaj prethodne leme za $a = b = 1$, a u koraku indukcije lema se primijeni na $a$ i $b = 1$. 

}\end{document}
2.4 Treći dokaz MFT-a


**Teorem 2.4.1.** Ako prost broj \( p \) ne dijeli \( a \), onda ne dijeli niti jednu potenciju od \( a \).

Euler se u dokazu prethodnog teorema poziva na Euklidovu tvrdnju iz *Elemenata* koja kaže da ako \( p \) ne dijeli ni \( a \) ni \( b \), onda ne dijeli ni njihov umnožak \( ab \).

Budući da je ostataka pri dijeljenju konačno mnogo, jasno je da vrijedi sljedeća tvrdnja.

**Propozicija 2.4.2.** Beskonačni niz brojeva \( 1, a, a^2, a^3, \ldots \) sadrži neke članove koji daju isti ostatak pri dijeljenju s prostim brojem \( p \).

**Teorem 2.4.3.** Neka je \( p \) prost broj i \( a > 1 \). Ako \( p \) ne dijeli \( a \), onda postoji beskonačno mnogo članova geometrijskog niza \( 1, a, a^2, a^3, \ldots \) koji daju ostatak 1 pri dijeljenju s \( p \).

Štoviše, eksponenti članova niza koji daju ostatak 1 pri dijeljenju s \( p \) tvore aritmetički niz.

**Dokaz.** Prema Korolaru [2.4.2] postoje bar dva člana tog niza koji pri dijeljenju s \( p \) daju isti ostatak. Neka su to \( a^m \) i \( a^n \), \( m, n \in \mathbb{N}, m > n \). Dakle, pisano suvremenim oznakama

\[
a^m \equiv a^n \pmod{p}.
\]

Stoga,

\[
p \mid a^m - a^n = a^n(a^{m-n} - 1).
\]

Prema Teoremu [2.4.1] \( p \nmid a^n \) što povlači da

\[
p \mid a^{m-n} - 1.
\]

Označimo li sa \( \lambda = m - n \), svaki član niza

\[
1, a^{\lambda}, a^{2\lambda}, a^{3\lambda}, \ldots
\]
POGLAVLJE 2. EULER-FERMATOV TEOREM

18

pri dijeljenju s \( p \) daje ostatak 1. Dakle, postoji beskonačno mnogo potencija od \( a \) koje daju ostatak 1 pri dijeljenju s \( p \).

Neka je \( \lambda_0 \in \mathbb{N} \) najmanji prirodan broj za kojeg je

\[ a^{\lambda_0} \equiv 1 \pmod{p}. \]

Tada su svi članovi geometrijskog niza \( 1, a, a^2, a^3, \ldots \) koji pri dijeljenju s \( p \) daju ostatak 1 dani s:

\[ 1, a^{\lambda_0}, a^{2\lambda_0}, a^{3\lambda_0}, \ldots \]

Očito eksponenti čine aritmetički niz, no ostaje nam još za pokazati da ne postoji potencija \( a^m \equiv 1 \pmod{p} \) takva da \( m \neq k\lambda_0, k \in \mathbb{N}_0 \). Zaista, tada je \( m = k\lambda_0 + r \) za neki \( k \in \mathbb{N}_0 \) i \( 0 < r < \lambda_0 \) prema Teoremu o dijeljenju s ostatkom. Očito je

\[ a^m = a^{k\lambda_0} \cdot a^r \equiv 1 \pmod{p} \]

pa slijedi da je \( a^r \equiv 1 \pmod{p} \) što je u kontradikciji s pretpostavkom minimalnosti od \( \lambda_0 \).

Sada Euler uočava sljedeće, ako je \( \lambda_0 \in \mathbb{N} \) najmanji takav za koji vrijedi \( a^{\lambda_0} \equiv 1 \pmod{p} \), onda nikoje dvije potencije iz skupa

\[ S = \{a^0 = 1, a^1, a^2, \ldots, a^{\lambda_0-1}\} \]

ne daju isti ostatak pri dijeljenju s \( p \), tj. nisu međusobno kongruentne modulo \( p \). Ako bi postojale takve dvije npr. \( a^\mu \equiv a^\nu \pmod{p} \) za \( 1 \leq \nu < \mu < \lambda_0 \) tada je \( a^{\mu-\nu} \equiv 1 \pmod{p} \) i \( 1 < \mu - \nu < \lambda_0 \) što je kontradikciji s minimalnošću. Dakle, za zaključiti je da je broj elemenata skupa \( S \) najviše \( p - 1 \) jer pri dijeljenju s \( p \) moraju dati različite ostatke 1, 2, \ldots, \( p - 1 \), odnosno

\[ |S| \leq p - 1. \]

S druge strane je \( |S| = \lambda_0 \) pa je

\[ \lambda_0 \leq p - 1. \]

Euler dalje pretpostavlja da je \( \lambda_0 < p - 1 \). Tada postoji ostatak \( k_1 \in \{2, \ldots, p - 1\} \) takav da niti jedan element iz skupa \( S \) ne daje ostatak \( k_1 \) pri dijeljenju s \( p \), odnosno \( a^i \not\equiv k_1 \pmod{p} \), za \( i = 0, 1, \ldots, \lambda_0 - 1 \). Promotrimo skup

\[ S_1 = \{a^0k_1 = k_1, a^1k_1, a^2k_1, \ldots, a^{\lambda_0-1}k_1\}. \]

Niti jedan od elemenata iz \( S_1 \) nije kongruentan modulo \( p \) s niti jednim elementom iz \( S \). Ako bi bilo

\[ a^j k_1 \equiv a^i \pmod{p}, \]

\[ a^i k_1 \equiv a^j \pmod{p}. \]

\[ a^i k_1 \equiv a^j \pmod{p}. \]
onda bi, uz npr. pretpostavku $j \geq i$, slijelilo da je
$$a^j(a^{j-i}k_1 - 1) \equiv 0 \pmod{p}.$$ Otuda je
$$a^{j-i}k_1 \equiv 1 \pmod{p},$$ odnosno
$$k_1 \equiv a^\lambda_0 - (j-i) \pmod{p},$$ što je u kontradikciji s izborom elementa $k_1$. Slično se pokaže ako pretpostavimo da $j < i$.

Nadalje, lako se pokaže da su elementi iz $S_1$ međusobno nekongruentni modulo $p$. Stoga iz sljedeće tri činjenice:
1. $|S| = \lambda_0$, $|S_1| = \lambda_0$,
2. $S \cap S_1 = \emptyset$,
3. svi elementi iz $S \cup S_1$ su međusobno nekongruentni modulo $p$,
slijedi da je $|S \cup S_1| = 2\lambda_0$ pa je
$$2\lambda_0 = p - 1 \text{ ili } 2\lambda_0 < p - 1.$$ Ako je $2\lambda_0 < p - 1$, onda postoji ostatak $k_2 \in \{2, \ldots, p - 1\}$, $k_2 \neq k_1$ takav da niti jedan element iz skupa $S \cup S_1$ ne daje ostatak $k_2$ pri dijeljenju s $p$, te definiramo skup
$$S_2 = \{a^0k_2 = k_2, a^1k_2, a^2k_2, \ldots, a^{\lambda_0 - 1}k_2\}.$$ Analognim zaključivanjem dobili bismo da je
$$3\lambda_0 = p - 1 \text{ ili } 3\lambda_0 < p - 1.$$ Ako $3\lambda_0 < p - 1$, onda ponavljamo postupak. Postupak mora stati u konačno mnogo koraka. Time je dokazan sljedeći teorem.

Teorem 2.4.4. Ako je $\lambda_0 \in \mathbb{N}$ najmanji prirodan broj za kojeg potencija $a^{\lambda_0}$ daje 1 pri dijeljenju s $p$, tada postoji $n \in \mathbb{N}$ takav da je
$$n\lambda_0 = p - 1.$$ Drugim riječima, ako je $\lambda_0 \in \mathbb{N}$ najmanji takav za koji vrijedi $a^{\lambda_0} \equiv 1 \pmod{p}$, onda je $\lambda_0$ djelitelj od $p - 1$. Posljedica ovog teorema je upravo MFT.

Danas je uobičajeno broj $\lambda_0$ zvati red elementa $a$ modulo $p$. Precizno ga definiramo na sljedeći način, a pojam se može poopći za prirodan broj $n$ takav da su $a$ i $m$ relativno prosti.
POGLAVLJE 2. EULER-FERMATOV TEOREM

Definicija 2.4.5. Neka je $a$ cijeli broj i $n$ prirodan broj takav da $(a, n) = 1$. Najmanji prirodan broj $\lambda_0$ za koji vrijedi

$$a^{\lambda_0} \equiv 1 \pmod{n}$$

zove se red broja $a$ modulo $n$.

2.5 Četvrti dokaz MFT-a

8. lipnja 1758. Euler predstavlja svoj rad *Theoremeta arithmetic nova methodo demonstrata* (Teoremi dokazani novom aritmetičkom metodom) koji ne samo da uključuje još jedan dokaz MFT-a, već i njegovu generalizaciju nazvanu Euler-Fermatov teorem, a danas poznatiju pod nazivom Eulerov teorem. Pritom uvodi vrlo korisnu aritmetičku funkciju koja, ponovo njemu u čast, nosi naziv Eulerova funkcija ili Eulerova $\varphi$-funkcija. Ukratko ćemo opisati sadržaj ovog Eulerovog članka.

U prethodnoj verziji dokaza MFT-a Euler je promatrao geometrijski niz, dok ovaj dokaz započinje promatranjem aritmetičkog niza $a, a+d, a+2d, \ldots$.

**Teorem 2.5.1.** Ako su $n$ i razlika $d$ relativno prosti, tada svaki nenegativan broj manji od $n$ predstavlja ostatak pri dijeljenju s $n$ nekog od prvih $n$ članova aritmetičkog niza: $a, a+d, a+2d, \ldots, a+(n-1)d$.

Drugim riječima, Teorem 2.5.1 kaže da skup $\{a, a+d, \ldots, a+(n-1)d\}$ predstavlja jedan potpuni sustav ostataka modulo $n$. Prisjetimo se:

Definicija 2.5.2. Neka je $n$ prirodan broj. Skup cijelih brojeva $\{x_1, x_2, \ldots, x_n\}$ sa svojstvom da za svaki cijeli broj $y$ postoji točno jedan $j \in \{1, 2, \ldots, n\}$ takav da je

$$y \equiv x_j \pmod{n}$$

zove se potpuni sustav ostataka modulo $n$.

Najpoznatiji potpuni sustav ostataka modulo $n$ sastoji se od najmanjih nenegativnih brojeva $\{0, 1, \ldots, n-1\}$. Općenito, svaki $n$-član skup cijelih brojeva čiji su elementi međusobno nekongruentni modulo $n$ čini potpuni sustav ostataka modulo $n$. Tu jednostavnu činjenicu koristimo u dokazu Teorema 2.5.1.

**Dokaz Teorema 2.5.1.** Neka je dan aritmetički niz $a, a+d, a+2d, \ldots$ i prirodan broj $n$ koji je relativno prost s razlikom $d$. Promotrimo prvih $n$ članova tog niza:

$$a, a+d, a+2d, \ldots, a+(n-1)d.$$
Pretpostavimo da je
\[ a + x_i d \equiv a + x_j d \pmod{n}, \]
za \( x_i, x_j \in \{0, 1, \ldots, n - 1\} \), \( i \neq j \). Tada je i
\[ x_i d \equiv x_j d \pmod{n}. \]
Kako je \( (n, d) = 1 \), prema Propoziciji 1.1.8 slijedi da je
\[ x_i \equiv x_j \pmod{n}, \]
pa smo dobili kontradikciju. Dakle, \( n \)-član skup \( \{a, a + d, a + 2d, \ldots, a + (n - 1)d\} \)
sastoji se od elemenata koji su međusobno nekongruentni modulo \( n \), odnosno čini potpuni sustav ostataka modulo \( n \).

**Teorem 2.5.3.** Neka su \( d \) i \( n > 0 \) relativno prosti cijeli brojevi. Ako član \( a + \nu d \) aritmetičkog niza daje ostatak \( 0 < r < n \) pri dijeljenju s \( n \), te su \( r \) i \( n \) relativno prosti, tada su i brojevi \( a + \nu d \) i \( n \) relativno prosti. Nadalje, ako \( r \) i \( n \) nisu relativno prosti, tada ni \( a + \nu d \) i \( n \) nisu relativno prosti.

**Dokaz.** Prema Teoremu o dijeljenju s ostatkom postoje jedinstveni cijeli brojevi \( q \) i \( 0 \leq r < n \) takvi da je
\[ a + \nu d = nq + r. \tag{2.1} \]
Prema pretpostavci teorema je \( r > 0 \).

Pretpostavimo da \( r \) i \( n \) nisu relativno prosti te označimo sa \( z > 1 \) njihov najveći zajednički djelitelj, \( (r, n) = z \). Tada je \( r = r_1 z \), \( n = n_1 z \) i \( (r_1, n_1) = 1 \), te
\[ a + \nu d = z(n_1 q + r_1). \]
Kako \( z \) dijeli desnu stranu, mora dijeliti i lijevu, odnosno \( a + \nu d \) pa je \( z > 1 \) ujedno i zajednički djelitelj od \( n \) i \( a + \nu d \).

Neka su \( r \) i \( n \) relativno prosti. Pretpostavimo da je \( (n, a + \nu d) = z > 1 \), odnosno vrijedi \( n = n_1 z \), \( a + \nu d = xz \). Tada iz (2.1) dobivamo
\[ axz = n_1 z + r, \]
što znači da \( z \) dijeli \( r \). No kako \( z \) dijeli i \( n \), slijedi da \( r \) i \( n \) nisu relativno prosti. Kontradikcija! Dakle, \( z = 1 \), odnosno \( (a + \nu d, n) = 1 \).

Kao posljedicu prethodnog teorema imamo činjenicu da je broj članova niza \( a \), \( a + d \), ..., \( a + (n - 1)d \) koji su relativno prosti s \( n \) jednak broju nenegativnih brojeva manjih od \( n \) koji su relativno prosti s \( n \). Euler je uočio važnost tog broja koji danas zovemo vrijednošću Eulerove funkcije u \( n \).
Definicija 2.5.4. Neka je n prirodan broj. Broj prirodnih brojeva u nizu 1, 2, \ldots, n koji su relativno prosti s n se označava s \( \varphi(n) \). Ovime je definirana funkcija \( \varphi : \mathbb{N} \to \mathbb{N} \) koja se naziva Eulerova funkcija.

Primjer 2.5.5. \( \varphi(6) = 2 \), jer su u nizu 1, 2, 3, 4, 5, 6 jedino 1 i 5 relativno prosti sa 6. \( \varphi(7) = 6 \), jer su u nizu 1, 2, 3, 4, 5, 6, 7 svi osim 7 relativno prosti sa 7. Općenito, lako zaključujemo da je \( \varphi(p) = p - 1 \).

Prisjetimo se sljedeće definicije.

Definicija 2.5.6. Reducirani sustav ostataka modulo n je skup cijelih brojeva \( \{r_1, r_2, \ldots, r_k\} \) sa svojstvom da je \( (r_i, n) = 1 \), \( r_i \not\equiv r_j \pmod{n} \) za \( i \neq j \), te da za svaki cijeli broj x takav da je \( (x, n) = 1 \) postoji \( i \in \{1, 2, \ldots, k\} \) takav da je \( x \equiv r_i \pmod{n} \).

Kako je jedan reducirani sustav ostataka modulo n skup svih brojeva \( a \in \{1, 2, \ldots, n\} \) za koje je \( (a, n) = 1 \), to je broj elemenata u reduciranom sustavu ostataka jedanak upravo \( \varphi(n) \).

U sljedećem teoremu Euler zapravo naslućuje strukturu grupe. Pojam grupe razvijen je u drugoj polovici 19. stoljeća (Cauchy4, Galois4). Napomenimo i da operacija množenja koja se spominje u sljedećem teoremu predstavlja zapravo množenje modulo n.

Teorem 2.5.7. Neka su a i n relativno prosti. Skup ostataka dobivenih dijeljenjem s n geometrijskog niza brojeva 1, a, a^2, a^3, \ldots zatvoren je s obzirom na operaciju množenja.

Dokaz. Neka je \( \lambda_0 \) red broja a modulo n. Označimo s \( r_0, r_1, \ldots, r_{\lambda_0-1} \in \{0, 1, \ldots, n-1\} \) ostatke pri dijeljenju s n brojeva 1, a, a^2, \ldots, a^{\lambda_0-1}, tj.

\[ r_j \equiv a^j \pmod{n} \]

za \( j = 0, 1, \ldots, \lambda_0 - 1 \). Uočimo da je \( r_i > 0 \) za sve \( i \) jer su \( a^i \) i n relativno prosti. Nadalje, vrijedi da je

\[ r_i \not\equiv r_j \pmod{n}, \ i \neq j. \]

Zaista, ako \( r_i \equiv r_j \pmod{n} \) i \( i > j \), onda je

\[ a^{i-j} \equiv 1 \pmod{n}, \]

\(^{3}\text{Augustin Louis Cauchy, 1789. - 1857.}, \text{ francuski matematičar.}\)

\(^{4}\text{Évariste Galois, 1811. - 1832.}, \text{ francuski matematičar.}\)
što je nemoguće jer je $0 < i - j < \lambda_0$ a $\lambda_0$ je red elementa $a$.

Sada uočimo da za svaku potenciju $a^k$, $k \geq 0$ postoji $j \in \{0, 1, \ldots, \lambda_0 - 1\}$ takav da je

$$a^k \equiv r_j \pmod{n}.$$ 

Uistinu, prema Teoremu o dijeljenju s ostatkom postoje jedinstveni $q \in \mathbb{Z}$ i $0 \leq j < \lambda_0$ za koje je $k = \lambda_0 q + j$ pa je

$$a^k = a^{\lambda_0 q + j} = (a^{\lambda_0})^q a^j \equiv a^j \equiv r_j \pmod{n}.$$ 

Dakle, skup ostataka dobiven dijeljenjem s $n$ geometrijskog niza $(a_k)$ je

$$\{r_0, r_1, \ldots, r_{\lambda_0 - 1}\}.$$ 

Preostaje još provjeriti da je zatvoren na množenje. Neka su $i, j \in \{0, 1, \ldots, \lambda_0 - 1\}$. Tada je

$$r_i r_j \equiv a^i a^j = a^{i+j} \equiv a^k = r_k \pmod{n},$$ 

dgje je $i + j = \lambda_0 q + k$, $0 \leq k < \lambda_0$.

Danas bismo lako mogli ustanoviti da skup ostataka koji smo definirali u prethodnom dokazu, $\{r_0, r_1, \ldots, r_{\lambda_0 - 1}\}$ čini multiplikativnu grupu. Zatvorenost smo upravo pokazali, komutativnost i asocijativnost su očite pa nam prestaje pokazati postojanje inverza. Uočimo, za $i > 0$ vrijedi

$$r_i r_{\lambda_0 - i} \equiv a^{\lambda_0} \equiv 1 \pmod{n}.$$ 

Stoga je inverz od $r_i$, $i > 0$, jednak $r_{\lambda_0 - i}$, a $r_0 = 1$ je sam sebi inverz.

**Primjer 2.5.8.** Neka je $a = 2$, $m = 15$. Određimo grupu ostataka modulo $n$ geometrijskog niza $(a_k)$. Prvo ustanovimo da je red broja 2 modulo 15 jednak 4, $2^4 = 16 \equiv 1 \pmod{15}$, $\lambda_0 = 4$. Stoga je $\{r_0, r_1, r_2, r_3\} = \{1, 2, 4, 8\}$.

**Primjer 2.5.9.** Neka je $a = 3$, $m = 10$. Red broja 3 modulo 10 jednak je 4, $3^4 = 81 \equiv 1 \pmod{10}$, $\lambda_0 = 4$. Stoga je $\{r_0, r_1, r_2, r_3\} = \{1, 3, 9, 7\}$. U ovom slučaju se naša grupa poklopila s reduciranim sustavom ostataka modulo 10.

U predhodna dva primjera opisali smo slučajeve koji mogu nastupiti pri određivanju grupe ostataka modulo $n$ geometrijskog niza $(a_k)$. U Primjeru 2.5.8 smo dobili grupu $\{1, 2, 4, 8\}$ čiji je red, odnosno broj elemenata jednak 4, dok se reducirani sustav ostataka modulo 15, $\{1, 2, 4, 7, 8, 11, 13, 14\}$ sastoji od 8 elemenata i 4 | 8. U Primjeru 2.5.9 broj elemenata grupe je upravo jednak broju elemenata u reduciranom
sustavu ostataka. Ovo što smo opazili zapravo je činjenica da red elementa modulo \( n \) dijeli vrijednost Eulerove funkcije u \( n, \varphi(n) \). Euler to iskazuje sljedećim teoremom. Uočimo da u specijalnom slučaju, za \( n = p \) prost broj, ovo svojstvo predstavlja tvrdnju Teorema 2.4.4.

**Teorem 2.5.10.** Neka su \( a \) i \( n \) relativno prosti. Broj različitih ostataka pri dijeljenju s \( n \) niza potencija \( 1, a, a^2, a^3, \ldots \) dijeli broj brojeva brojeva manjih od \( n \) i relativno prostih s \( n \).

Euler je prethodni teorem dokazao slično kao Teorem 2.4.4. I ovdje bi tvrdnju mogli formulirati koristeći algebarske strukture i pozivajući se na Lagrangeov teorem da red podgrupe dijeli red grupe, no Euler to u svoje vrijeme nije mogao formulirati na taj način. Ako pažljivije pogledamo dokaz, možemo uočiti da je Euler zapravo koristio ideju "razbijanja" grupe na klase. Kao posljedicu je dobio jedan od najvažnijih rezultata teorije brojeva.

**Teorem 2.5.11** (Izvorna formulacija Euler-Fermatova teorema). Neka su \( a \) i \( n \) relativno prosti. Ako je \( \nu \) jednak broju brojeva manjih od \( n \) koji su relativno prosti s \( n \) ili djelitelju tog broja, onda \( a^\nu \) pri dijeljenju s \( n \) daje ostatak 1.

Iz toga slijedi da ako je \( n \) prost broj, vrijedi \( \varphi(n) = n - 1 \), čime je dokazan Mali Fermatov teorem.

### 2.6 Eulerov teorem

Danas Euler-Fermatov teorem češće nazivamo samo Eulerovim teoremom te ga iskazuju u sljedećem obliku.

**Teorem 2.6.1** (Eulerov teorem). Neka je \( a \) cijeli broj te \( n \) prirodan broj. Ako su brojevi \( a \) i \( n \) relativno prosti, onda je \( a^{\varphi(n)} \equiv 1 \pmod{n} \).

Navest ćemo kraći i jednostavniji dokaz prethodne tvrdnje. Za to nam je potrebna sljedeća jednostavna lema.

**Lema 2.6.2.** Neka je \( \{r_1, r_2, \ldots, r_{\varphi(n)}\} \) reducirani sustav ostataka modulo \( n \) te neka je \( (a, n) = 1 \). Tada je \( i \{ar_1, ar_2, \ldots, ar_{\varphi(n)}\} \) reducirani sustav ostataka modulo \( n \).

---

Dokaz Teorema 2.6.1. Neka je \( \{ r_1, r_2, \ldots, r_{\phi(n)} \} \) reducirani sustav ostataka modulo \( n \). Tada je prema Lemi 2.6.2 i \( \{ ar_1, ar_2, \ldots, ar_{\phi(n)} \} \) reducirani sustav ostataka modulo \( n \). Dakle, vrijedi
\[
\phi(n) \prod_{j=1}^{\phi(n)} ar_j \equiv \phi(n) \prod_{i=1}^{\phi(n)} r_i \pmod{n},
\]
odnosno
\[
a^{\phi(n)} \prod_{j=1}^{\phi(n)} r_j \equiv \prod_{i=1}^{\phi(n)} r_i \pmod{n}.
\]
Kako su \( r_i \) i \( n \) relativno prosti za svaki \( i \), prema Propoziciji 1.1.8 slijedi da je \( a^{\phi(n)} \equiv 1 \pmod{n} \).

2.7 Svojstva Eulerove funkcije

Iz same definicije Eulerove funkcije je očito \( \phi(p) = p - 1 \) za prost broj \( p \). Jednostavno možemo odrediti vrijednost Eulerove funkcije za potenciju prostog broja:

Propozicija 2.7.1. Neka je \( p \) prost broj i \( k \in \mathbb{N} \). Tada je \( \phi(p^k) = p^k - p^{k-1} \).

Dokaz. Neka je dan prost broj \( p \) i \( k \in \mathbb{N} \). Jedini brojevi u nizu 1, 2, 3, \ldots, \( p^k \) koji nisu relativno prosti s \( p \) su brojevi \( p, 2p, 3p, \ldots, p^{k-1} \cdot p \). Njih ima \( p^{k-1} \). Kako je ukupan broj brojeva u nizu 1, 2, 3, \ldots, \( p^k \) jednak \( p^k \) slijedi da je \( \phi(p^k) = p^k - p^{k-1} \).

Eulerova funkcija \( \varphi \) također (kako i funkcija \( \sigma \)) zadovoljava svojstvo multiplikativnosti. Odnosno, \( \varphi(mn) = \varphi(m) \varphi(n) \), za \( (m, n) = 1 \). Ako iskoristimo to svojstvo i Propoziciju 2.7.1 dobit ćemo eksplicitnu formulu za računanje vrijednosti Eulerove funkcije za svaki prirodan broj \( n \). Jedino što možda može biti problem jest činjenica da se formula bazira na kanonskom rastavu broja \( n \) na proste faktore.

Neka je
\[
n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},
\]
gdje su \( p_1 < p_2 < \ldots < p_k \) prosti i \( \alpha_1, \ldots, \alpha_k \in \mathbb{N} \). Tada je
\[
\varphi(n) = \varphi \left( \prod_{i=1}^{k} p_i^{\alpha_i} \right) = \prod_{i=1}^{k} \varphi(p_i^{\alpha_i}),
\]
zbog multiplikativnosti i
\[
\varphi(n) = \prod_{i=1}^{k} \left( p_i^{\alpha_i} - p_i^{\alpha_i-1} \right) = \prod_{i=1}^{k} p_i^{\alpha_i} \left( 1 - \frac{1}{p_i} \right),
\]
zbog Propozicije 2.7.1. Formulu često zapisujemo u sljedećem obliku

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right),$$

(2.2)

a koristan je i oblik

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

(2.3)

**Primjer 2.7.2.** Neka je \(n = 12\). Prosti djelitelji broja 12 su 2 i 3 pa je

$$\varphi(12) = 12 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) = 4.$$

S druge strane, jedini brojevi u nizu 1, 2, ..., 12 koji su relativno prosti s 12 su brojevi 1, 5, 7 i 11.

Koristeći multiplikativnost funkcije \(\varphi\) i formulu (2.3) mogu se pokazati sljedeća svojstva.

**Propozicija 2.7.3.** Neka su \(m\) i \(n\) prirodni brojevi. Vrijedi:

1. Ako je \(n \geq 3\), onda je \(\varphi(n)\) je paran broj.
2. Ako \(n\) dijeli \(m\), onda \(\varphi(n)\) dijeli \(\varphi(m)\).
3. Ako je \(n\) paran broj, onda \(\varphi(2n) = 2\varphi(n)\), a ako je neparan, onda \(\varphi(2n) = \varphi(n)\).
4. \(\varphi(n^m) = n^{m-1}\varphi(n)\).
5. \(\varphi([m,n])\varphi((m,n)) = \varphi(m)\varphi(n)\), gdje je \([m,n]\) najmanji zajednički višekratnik brojeva \(m\) i \(n\), a \((m,n)\) njihov najveći zajednički djelitelj.
6. \(\varphi(mn) = \varphi(m)\varphi(n) \cdot \frac{(m,n)}{\varphi((m,n))}\).

Danas je poznato da za neparan broj \(n\) vrijedi \(\varphi(n) = \varphi(2n)\) te da ako \(n\) nije djeljiv ni s 2 ni 3, onda je \(\varphi(3n) = \varphi(4n) = \varphi(6n)\). Pretpostavlja se, ali nije dokazano da vrijedi i sljedeće.

**Slutnja 3.** Za svaki broj \(n\) postoji broj \(n'\) takav da vrijedi \(\varphi(n) = \varphi(n')\).
Poglavlje 3

Sume kvadrata

3.1 Sume dva kvadrata

**Teorem 3.1.1** (Teorem o dva kvadrata). *Svaki prosti broj p oblika 4k + 1 se može na jedinstveni način prikazati kao zbroj kvadrata dvaju cijelih brojeva.*

U nastavku rada kraće ćemo govoriti samo o sumi, odnosno zbroju dva kvadrata.

Teorem o dva kvadrata se ponekad naziva i *Fermatov teorem o dva kvadrata* ili *Fermatov božićni teorem* jer je svoju tvrđnju elaborirao u pismu Marinu Mersenneu koje je datirano 25. prosinca 1640. Neki ovaj teorem nazivaju i *Girardovim teoremom* prema Albertu Girardu koji se 15 godina prije Fermata bavio prirodnim brojevima koji se mogu reprezentirati kao zbroj dva kvadrata.

Fermat je teorem dokazao djelomično, a prvi koji ga je u potpunosti dokazao bio je Euler 1747. U dokazu je koristio metodu neprekidnog silaska. Jedan dio dokaza objavljen je u članku pod naslovom teorema kojeg je objavio u radu *De numeris, qui sunt aggregata duorum quadratorum* (O brojevima koji su zbroj dva kvadrata) 1758. godine, a drugi *Demonstratio theorematis Fermatiani omnem numerum primum formae 4n+1 esse summam duorum quadratorum* (Dokaz Fermatova teorema da se svaki broj oblika 4n + 1 može prikazati kao suma dva kvadrata) 1760. godine.

U nastavku slijedi Eulerov dokaz, ali uz današnju notaciju (npr. kongruencije). U njemu se koristi tzv. *Diofantov identitet* koji kaže da je umnožak brojeva koji su prikazivi kao zbroj dva kvadrata i sam zbroj dva kvadrata, odnosno

\[(a^2 + b^2) (c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2. \tag{3.1}\]

1Albert Girard, 1595. - 1632., flamanski matematičar.
Dokaz se sastoji od nekoliko koraka koje Euler naziva propozicijama.

**Propozicija 3.1.2.** Količnik broja koji se može prikazati kao suma dva kvadrata i prostog broja koji se može prikazati kao suma dva kvadrata je isto suma dva kvadrata.

**Dokaz.** Neka su $a, b, p, q \in \mathbb{Z}$. Pretpostavimo da prost broj $p^2 + q^2$ dijeli broj $a^2 + b^2$. Tada $p^2 + q^2$ dijeli i

$$p^2(a^2 + b^2) - a^2(p^2 + q^2) = (pb - aq)(pb + aq).$$

Budući je $p^2 + q^2$ prost, vrijedi da $(p^2 + q^2)| (pb - aq)$ ili $(p^2 + q^2)| (pb + aq)$. Ako $(p^2 + q^2)| (pb - aq)$ onda prema (3.1) imamo

$$(a^2 + b^2)(p^2 + q^2) = (ap + bq)^2 + (aq - bp)^2,$$

pa slijedi da $(p^2 + q^2)| (pb + aq)$. Sada tvrdnju dobivamo iz

$$\frac{a^2 + b^2}{p^2 + q^2} = \frac{(a^2 + b^2)(p^2 + q^2)}{(p^2 + q^2)^2} = \left(\frac{ap + bq}{p^2 + q^2}\right)^2 + \left(\frac{aq - bp}{p^2 + q^2}\right)^2 \in \mathbb{N}.$$

**Propozicija 3.1.3.** Količnik broja koji se može prikazati kao suma dva kvadrata i prostog broja koji se ne može prikazati kao suma dva kvadrata ima prostog djelitelja koji nije suma dva kvadrata.

**Dokaz.** Pretpostavimo da je

$$\frac{a^2 + b^2}{c} = p_1p_2\cdots p_n,$$

gdje $c$ nije suma dva kvadrata, a $p_1, \ldots, p_n$ su prosti i, suprotno tvrdnji, prikazivi kao zbroj dva kvadrata. Dijeljenjem $a^2 + b^2$ s $p_1$ dobivamo količnik $cp_2\cdots p_n$ koji prema Propoziciji 3.1.2 je suma dva kvadrata. Uzastopnim dijeljenjem s $p_2, \ldots, p_n$ i primjenom Propozicije 3.1.2 doći ćemo do zaključka da je $c$ suma dva kvadrata što je u suprotnosti s pretpostavkom propozicije. Stoga postoji $p_i, 1 \leq i \leq n$, koji se ne može prikazati kao suma dva kvadrata.

**Propozicija 3.1.4.** Neka su $a$ i $b$ relativno prosti cijeli brojevi. Tada je svaki (prosti) djelitelj od $a^2 + b^2$ moguće zapisati kao sumu dva kvadrata.
**POGLAVLJE 3. SUME KVADRATA**

**Dokaz.** Neka je $p$ prost djelitelj od $a^2 + b^2$. Nadalje, neka su $c, d \in \mathbb{Z}$ takvi da je $|c|, |d| < \frac{p}{2}$ i

$$a \equiv c \pmod{p}, \ b \equiv d \pmod{p}.$$ 

Tada je i $c^2 + d^2 \equiv 0 \pmod{p}$, odnosno $p | c^2 + d^2$ i

$$c^2 + d^2 < 2 \left( \frac{p}{2} \right)^2 = \frac{p^2}{2} = \frac{p}{2} \cdot p.$$ 

Stoga postoji $1 \leq k \leq \frac{p}{2}$ takav da je

$$c^2 + d^2 = kp. \quad (3.2)$$

Nadalje, možemo bez smanjenja općenitosti pretpostaviti da su $c$ i $d$ relativno prosti. Ako ne bi bili, umjesto njih uzeli bi $c' = \frac{c}{(c,d)}$, $d' = \frac{d}{(c,d)}$, $k' = \frac{k}{(c,d)^2}$, pri čemu je $(c, d)$ najveći zajednički djelitelj od $c$ i $d$.

Ako je $k = 1$, onda je dokaz naše tvrdnje gotov jer smo prostog djelitelja prikazali kako sumu kvadrata. Ako $k > 1$, tada je moguće primijeniti *metod neprekidnog silaska* koja vodi do kontradikcije.

Pretpostavimo da je $k > 1$. Neka su $u, v \in \mathbb{Z}$ takvi da je $|u|, |v| \leq \frac{k}{2}$ i za koje vrijedi

$$u \equiv c \pmod{k}, \ v \equiv d \pmod{k}. \quad (3.3)$$

Tada je

$$u^2 + v^2 \equiv c^2 + d^2 \equiv 0 \pmod{k},$$

iz čega slijedi da je

$$u^2 + v^2 = kr, \quad (3.4)$$

za neki prirodan broj $r$. Uočimo da $r$ ne može biti $0$. U tom slučaju bi bilo $u = v = 0$, odnosno $k > 1$ bi dijelio $c, d$ što nije moguće jer su relativno prosti. Za broj $r$ dobivamo sljedeću gornju ogradu

$$r = \frac{1}{k} \left( u^2 + v^2 \right) \leq \frac{1}{k} \left( \frac{k^2}{4} + \frac{k^2}{4} \right) \leq \frac{k}{2} \leq \frac{p}{2}. $$


$$k^2 pr = \left( c^2 + d^2 \right) \left( u^2 + v^2 \right) = (cu + dv)^2 + (cv - du)^2. \quad (3.5)$$

Primjetimo, $cu + dv$ i $cv - du$ su višekratnici broja $k$,

$$cu + dv \equiv c^2 + d^2 \equiv 0 \pmod{k},$$
POGLAVLJE 3. SUME KVADRATA

\[ cv - du \equiv cy - dx \equiv 0 \pmod{k}. \]

Stoga jednakost (3.5) možemo podijeliti s \( k^2 \) čime dobivamo

\[ rp = c_1^2 + d_1^2, \]

gdje su \( c_1 = \frac{cu + dv}{k} \) i \( d_1 = \frac{cv - du}{k} \) cijeli brojevi. Nadalje, bez smanjenja općenitosti \((c_1, d_1) = 1\). Time smo pokazali da postoji prirodan broj \( r \) koji je

\[ p = x^2 + y^2. \]

Propozicija 3.1.5. Svaki prost broj oblika \( 4n + 1 \) jednak je sumi dva kvadrata.

Dokaz. Budući je \( 4n + 1 = p \) prost, MFT 2.1.1 povlači da je

\[ 1, 2^{4n}, 3^{4n}, \ldots, (4n)^{4n} \equiv 1 \pmod{p}. \]

Otuda je razlika svaka dva susjedna člana djeljiva s \( 4n + 1 \), odnosno

\[ 2^{4n} - 1, 3^{4n} - 2^{4n}, \ldots, (4n)^{4n} - (4n - 1)^{4n} \equiv 0 \pmod{p}. \]

Svaku od gornjih razlika faktoriziramo kao razliku kvadrata:

\[ x^{4n} - y^{4n} = (x^{2n} + y^{2n})(x^{2n} - y^{2n}). \]

Ako postoji \( 1 \leq a \leq 4n - 1 \) takav da \( p \) dijeli \((a + 1)^{2n} + a^{2n}\), onda prema Propoziciji 3.1.4 slijedi da je i sam \( p \) jednak sumi kvadrata. Zato pretpostavimo da \( p \) dijeli sve razlike

\[ 2^{2n} - 1, 3^{2n} - 2^{2n}, \ldots, (4n)^{2n} - (4n - 1)^{2n}. \]

No i \( 4n - 2 \) dijeli uzastopne razlike prethodnog niza,

\[ 3^{2n} - 2 \cdot 2^{2n} + 1, \ldots, (4n)^{2n} - 2 \cdot (4n - 1)^{2n} + (4n - 2)^{2n}. \]

Nastavljajući tako dalje, nakon \( 2n \) koraka, prema Lemi 3.1.6 ćemo dobiti (za \( f(x) = x^{2n} \)) broj \( (2n)! \) koji mora biti djeljiv s \( p \), što nije moguće. Stoga \( p \) dijeli barem jedan faktor oblika \((a + 1)^{2n} + a^{2n}\). \( \square \)
U dokazu prethodne tvrdnje koristila se tzv. diferencija polinoma. Za funkciju \( f : \mathbb{R} \rightarrow \mathbb{R} \) definiramo diferenciju 1. reda kao
\[
D_1(x) = f(x + 1) - f(x),
\]
zatim diferenciju 2. reda
\[
D_2(x) = D_1(x + 1) - D_1(x).
\]
Općenito, diferencija \( k \)-tog reda je
\[
D_k(x) = D_{k-1}(x + 1) - D_{k-1}(x),
\]
za \( k \in \mathbb{N} \), pri čemu je \( D_0(x) = f(x) \).

Lema 3.1.6. Ako je \( f \) polinom stupnja \( k \), tada je \( k \)-ta diferencija konstantna funkcija.

Konkretno,
\[
D_k(x) = a_k \cdot k!,
\]
gdje je \( a_k \) vodeći koeficijent polinoma \( f \).

Dokaz. Neka je
\[
f(x) = a_k x^k + a_{k-1} x^{k-1} + \cdots + a_1 x + a_0,
\]
gdje je \( a_k \neq 0 \). Tada je
\[
D_1(x) = f(x + 1) - f(x) = \sum_{i=1}^{k} a_i \left( (x + 1)^i - x^i \right),
\]
a prema Binomnom teoremu
\[
(x + 1)^i - x^i = \binom{i}{1} x^{i-1} + \binom{i}{2} x^{i-2} + \cdots + \binom{i}{i-1} x^1 + \binom{i}{0} x^0.
\]
Stoga je \( D_1 \) polinom stupnja \( k - 1 \):
\[
D_1(x) = a_k \binom{k}{1} x^{k-1} + \left( a_k \binom{k}{2} + a_{k-1} \binom{k-1}{1} \right) x^{k-2} + \cdots + (a_k + a_{k-1} + \cdots + a_1) x^0.
\]
Analognim zaključivanjem, polinom \( D_2 \) je stupnja \( k - 2 \) i koeficijent uz vodeću potenciju je
\[
a_k \binom{k}{1} \binom{k-1}{1} \binom{1}{1}.
\]
Konačno, možemo zaključiti da je \( D_k \) je stupnja 0, odnosno konstantan polinom i
\[
D_k(x) = a_k \binom{k}{1} \binom{k-1}{1} \cdots \binom{2}{1} \binom{1}{1} = a_k \cdot k!.
\]
Propozicija 3.1.7. Prikaz prostog broja $4n+1$ kao sume kvadrata dva prirodna broja je jedinstven, do na poredak pribrojnika.

Dokaz. Pretpostavimo da postoje prirodni brojevi $x, y, X, Y$, za koje vrijedi

$$p = x^2 + y^2, \quad p = X^2 + Y^2.$$  \hspace{1cm} (3.6)

Nakon množenja jednakosti u (3.6) i primjene identiteta (3.1) dobivamo

$$p^2 = (x^2 + y^2) (X^2 + Y^2) = (xX + yY)^2 + (xY - yX)^2.$$  \hspace{1cm} (3.7)

Uočimo da je $xX + yY \equiv xY - yX \equiv 0 \pmod{p}$. Zaista, iz (3.6) slijedi $x \equiv -y \pmod{p}$, $X \equiv -Y \pmod{p}$ pa je $x^2X^2 \equiv y^2Y^2 \pmod{p}$. Stoga,

$$xX + yY \equiv 0 \pmod{p} \text{ ili } xX - yY \equiv 0 \pmod{p}.$$  

Vrijede implikacije:

$$xX + yY \equiv 0 \pmod{p} \implies xX \equiv -yY \pmod{p} \implies -xY \equiv -yX \pmod{p} \implies xY \equiv yX \pmod{p}.$$  

Ako bi vrijedilo $xX - yY \equiv 0 \pmod{p}$, onda bi dobili $xY + yX \equiv 0 \pmod{p}$ pa bi u (3.7) zamijenili $y$ s $-y$.

Dakle, $xX + yY$ i $xY - yX$ su višekratnici broja $p$. Sada izraz (3.7) možemo podijeliti s $p^2$ čime dobivamo

$$1 = A^2 + B^2,$$  

za $A, B \in \mathbb{Z}$. Jedina moguća rješenja prethodne jednadžbe do na poredak pribrojnika su $A = \pm 1$, $B = 0$ što znači da je i u jednadžbi (3.7) jedan od pribrojnika morao biti 0. Kako su $x$ i $y$ te $X$ i $Y$ relativno prosti, iz $xX + yY = 0$ slijedi da je

$$(x, y) = (Y, -X) \text{ ili } (x, y) = (-Y, X).$$

Ako bi vrijedilo $xY - yX = 0$, slijedilo bi

$$(x, y) = (X, Y) \text{ ili } (x, y) = (-X, -Y).$$

Dakle, jedina mogućnost je $(x, y) = (X, Y)$. \hfill \square
3.2 Sume četiri kvadrata

U Fermatovom pismu Carcaviju nalazimo i Teorem o četiri kvadrata. Rene Descartes jednom je prilikom izrekao: "Neupitno je da je ovaj teorem jedan od najljepših teorema teorije brojeva, ali ja nemam njegov dokaz. Po mojoj procjeni, bilo bi toliko teško dokazati ga da dokaz nisam ni tražio."

Da je dokaz uistinu bilo teško pronaći potvrđuje i činjenica da je Euler preko 40 godina pokušavao dokazati navedeni teorem, ali u tome nije uspio. Dokaz teorema dao je Lagrange krajem 18. stoljeća pa se danas taj teorem naziva i Lagrangeovim teoremom o četiri kvadrata.

Teorem 3.2.1 (Teorem o četiri kvadrata). Svaki se prirodan broj može zapisati kao suma kvadrata četiri cijela broja.

Lagrange je u dokazu iskoristio Eulerov teorem o sumi četiri kvadrata kojeg je potonji izrekao u pismu upućenom Goldbachu 1748. godine.

Teorem 3.2.2 (Eulerov teorem o četiri kvadrata). Umnožak dva broja, od kojih je svaki suma četiri kvadrata, je i sam suma četiri kvadrata.

Zapisano simbolima, teorem kaže sljedeće:

\[(a_1^2 + a_2^2 + a_3^2 + a_4^2) \cdot (b_1^2 + b_2^2 + b_3^2 + b_4^2) = (a_1b_1 - a_2b_2 - a_3b_3 - a_4b_4)^2 + (a_1b_2 + a_2b_1 + a_3b_4 - a_4b_3)^2 + (a_1b_3 - a_2b_4 + a_3b_1 + a_4b_2)^2 + (a_1b_4 + a_2b_3 - a_3b_2 + a_4b_1)^2.\]

Primjer 3.2.3. Broj 30 možemo izraziti kao \(1^2 + 2^2 + 3^2 + 4^2\), a broj 10 kao \(1^2 + 1^2 + 2^2 + 2^2\). Primjenom Eulerova teorema o četiri kvadrata slijedi da i umnožak 30 \(\cdot\) 10 možemo izraziti pomoću sume četiri kvadrata. Zaista, vrijedi

\[30 \cdot 10 = (-15)^2 + 1^2 + (-5)^2 + 7^2.\]

---

2Pierre de Carcavi, oko 1600. - 1684., francuski matematičar.
Poglavlje 4

Kvadratni ostatci

4.1 Legendreov simbol

Definicija 4.1.1. Neka su $a$ i $m$ relativno prosti prirodni brojevi. Ako kongruencija

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

ima rješenja, onda kažemo da je $a$ kvadratni ostatak modulo $m$. U suprotnom kažemo da je $a$ kvadratni neostatak modulo $m$.

Teorem 4.1.2. Neka je $p$ neparan prost broj. Reducirani sustav ostataka modulo $p$ se sastoji od $\frac{p-1}{2}$ kvadratnih ostataka i $\frac{p-1}{2}$ kvadratnih neostataka.

Dokaz. Neka je $p$ neparan prost broj. Skup

$$S = \left\{ \frac{-p-1}{2}, \ldots, -2, -1, 0, 1, 2, \ldots, \frac{p-1}{2} \right\}$$

čini potpuni sustav ostataka modulo $p$. Svaki kvadratni ostatak modulo $p$ mora biti kongruentan nekom od brojeva

$$\left( \pm 1 \right)^2, \left( \pm 2 \right)^2, \ldots, \left( \pm \frac{p-1}{2} \right)^2.$$

Njih ima ukupno $\frac{p-1}{2}$. Pretpostavimo sada da je

$$k^2 \equiv l^2 \pmod{p},$$

pri čemu je $1 \leq k < l \leq \frac{p-1}{2}$. Tada je $(l+k)(l-k) \equiv 0 \pmod{p}$ iz čega slijedi da je $l+k \equiv 0 \pmod{p}$ ili $l-k \equiv 0 \pmod{p}$. No kako su $k, l \in R$ to je nemoguće, odnosno vrijedi

$$k^2 \neq l^2 \pmod{p},$$
POGLAVLJE 4. KVADRATNI OSTATCI

za $1 \leq k < l \leq \frac{p-1}{2}$.

**Primjer 4.1.3.** Odredit ćemo sve kvadratne ostatke, odnosno neostatke modulo $p = 11$. Na temelju dokaza prethodnog teorema slijedi da su kvadratni ostatci modulo 11 jednaki

$$1, 4, 9, 16 \equiv 5 \pmod{11}, 25 \equiv 3 \pmod{11}.$$

Stoga su neostatci jednaki $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\} \setminus \{1, 3, 4, 5, 9\} = \{2, 6, 7, 8, 10\}$.

**Definicija 4.1.4.** Neka je $p$ neparan prost broj i $a$ prirodan broj. Legendreov simbol, u oznaci $\left(\frac{a}{p}\right)$, je jednak 1 ako je $a$ kvadratni ostatak modulo $p$, $-1$ ako je $a$ kvadratni neostatak modulo $p$, a jednak 0 ako $p$ dijeli $a$.

### 4.2 Eulerov kriterij

Odrediti vrijednost Legendreova simbola nije posebno teško ako je prost $p$ dovoljno mali broj (npr. kao u Primjeru 4.1.3), no za veće $p$ to predstavlja problem. Euler je koristeći MFT, našao "formulu" za određivanje Legendreova simbola.

**Teorem 4.2.1** (Eulerov kriterij). Ako je $p$ neparan prost broj, onda je

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

**Dokaz.** Neka je $p$ neparan prost broj. Treba ustanoviti da je

$$a^{\frac{p-1}{2}} \equiv 0, 1, -1 \pmod{p}$$

za

$$\left(\frac{a}{p}\right) = 0, 1, -1,$$

respektivno. Stoga razlikujemo tri slučaja.

1. Ako je $\left(\frac{a}{p}\right) = 0$, onda $p \mid a$, odnosno $a \equiv 0 \pmod{p}$ pa analogna relacija vrijedi i za svaku potenciju od $a$.

2. Pretpostavimo da je $a$ kvadratni ostatak modulo $p$, odnosno da je $\left(\frac{a}{p}\right) = 1$. Tada postoji cijeli broj $x_1$ takav da je

$$x_1^2 \equiv a \pmod{p}.$$
Kako su $a$ i $p$ relativno prosti, slijedi da su i $x_1$ i $p$ relativno prosti. Iz MFT primijenjenog na brojeve $x_1$ i $p$ slijedi
\[ x_1^{p-1} \equiv 1 \pmod{p}. \]
Kako je $x_1^{p-1} \equiv a^{\frac{p-1}{2}} \pmod{p}$ dobivamo
\[ a^{\frac{p-1}{2}} \equiv 1 \pmod{p}. \]

3. Pretpostavimo da je $a$ kvadratni neostatak modulo $p$, odnosno da je $\left( \frac{a}{p} \right) = -1$.
Ustanovimo da za svaki $i \in \{1, 2, \ldots, p-1\}$ postoji jedinstven $j \in \{1, 2, \ldots, p-1\}$, $i \neq j$ takav da je
\[ i \cdot j \equiv a \pmod{p}. \]  
\[(4.1)\]

Razlog tome jest što linearna kongruencija $i \cdot x \equiv a \pmod{p}$ ima jedinstveno rješenje u skupu $\{1, 2, \ldots, p-1\}$ jer su brojevi $i$ i $p$ relativno prosti. Nadalje, $j \neq i$ jer je $a$ kvadratni neostatak modulo $p$. Stoga skup $\{1, 2, \ldots, p-1\}$ možemo rasporediti u $\frac{p-1}{2}$ parova $(i, j)$ za koje vrijedi (4.1), odnosno
\[ 1 \cdot 2 \cdots (p-1) \equiv a^{\frac{p-1}{2}} \pmod{p}. \]
S druge strane koristeći Wilsonov teorem koji kaže da je
\[ 1 \cdot 2 \cdots (p-1) \equiv -1 \pmod{p}, \]

slijedi
\[ a^{\frac{p-1}{2}} \equiv -1 \pmod{p}. \]

U dokazu prethodne tvrdnje korišten je Wilsonov teorem kojeg je iskazao John Wilson 1770. godine (iako je navodno ipak poznat Leibnizu, a još prije i arapskim matematičarima u 11. stoljeću). Dokazao ga je 1773. godine Lagrange. U dokazu se koristi ideja slična onoj u slučaju 3. prethodnog dokaza.

**Teorem 4.2.2** (Wilsonov teorem). Ako je $p$ prost broj, onda je $(p-1)! + 1$ višekratnik od $p$.

Vrijedi i obrat Teorema 4.2.2. Ako je $(p-1)! \equiv -1 \pmod{p}$, onda je $p$ prost.\[ ^1\text{John Wilson, 1741. - 1793., engleski matematičar.} \]
POGLAVLJE 4. KVADRATNI OSTATCI

4.3 Svojstva Legendreova simbola

U ovom odjeljku navodimo neka svojstva Legendreova simbola koja direktno slijede iz Eulerova kriterija.

Teorem 4.3.1. Za svaka dva cijela broja $a$ i $b$ te neparan prost broj $p$ vrijedi:

1. Ako je $a \equiv b \pmod{p}$, onda je $\left( \frac{a}{p} \right) = \left( \frac{b}{p} \right)$.

2. $\left( \frac{a}{p} \right) \left( \frac{b}{p} \right) = \left( \frac{ab}{p} \right)$.

3. Ako je $(a, p) = 1$, onda je $\left( \frac{a^2}{p} \right) = 1$.

**Dokaz.** Neka su dati cijeli brojevi $a$ i $b$ te neparan prost broj $p$.

1. Koristeći Eulerov kriterij i pretpostavku $a \equiv b \pmod{p}$, imamo $\left( \frac{a}{p} \right) \equiv a^{p-1} \equiv b^{p-1} \equiv \left( \frac{b}{p} \right) \pmod{p}$.

2. Primjenom Eulerova kriterija dobivamo $\left( \frac{a}{p} \right) \left( \frac{b}{p} \right) \equiv a^{p-1} b^{p-1} \equiv (ab)^{p-1} \equiv \left( \frac{ab}{p} \right) \pmod{p}$.

Kako je Legendreov simbol jednak $-1$, $0$ ili $1$ slijedi $\left( \frac{a}{p} \right) \left( \frac{b}{p} \right) = \left( \frac{ab}{p} \right)$.

3. Pretpostavimo da je $(a, p) = 1$. Kako kongruencija $x^2 \equiv a^2 \pmod{p}$ ima rješenje $x = a$, to je $a^2$ kvadratni ostatak modulo $p$.

Teorem 4.3.2. Za neparan prost broj $p$ vrijedi:

1. $\left( \frac{1}{p} \right) = 1$,

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

**Dokaz.** Neka je $p$ neparan prost broj.

Dokaz od (1) slijedi direktno iz tvrdnje (3) prethodnog teorema.

Tvrdnju (2) dobivamo uvrštavanjem $a = -1$ u Eulerov kriterij.
Poglavlje 5

Veliki Fermatov teorem

5.1 Fermatova slutnja

Kao što smo već ranije spomenuli Fermat je svoje spoznaje ponekad zapisivao na margine knjiga. Tako je u svom primjerku Bachetovog prijevoda Diofantove Arithmetice zapisao sljedeće:

"Nije moguće kub rastaviti na dva kuba ili bikvadrat na dva bikvadrata niti općenitije neku potenciju veću od druge na dvije potencije s istim eksponentom. Za to imam stvarno čudesan dokaz, no rub je ovdje preuzak da ga zapišem."

Danas taj teorem znamo pod nazivom Veliki Fermatov teorem, u nastavku kraće VFT i pamtimo ga u sljedećem obliku.

Teorem 5.1.1 (VFT). Ne postoje pozitivni cijeli brojevi \(x, y, z\) takvi da vrijedi

\[
x^n + y^n = z^n,
\]

gdje je \(n \in \mathbb{N}, n > 2\).

Jasno je da za \(n = 1\) jednadžba ima beskonačno mnogo rješenja. Za \(n = 2\) također postoji beskonačno mnogo rješenja, a neka su od njih bila poznata još Babiloncima oko 1800 godina prije Krista. Danas uređenu trojku \((x, y, z)\) prirodnih brojeva za koju vrijedi \(x^2 + y^2 = z^2\) nazivamo Pitagorinom trojkom.

Fermat je i prije iskazao samog VFT, u pismu iz 1658. godine, izrekao dva specijalna slučaja tog teorema.

Slutnja 4. Ne postoje pravokutan trokut čije su duljine stranica prirodni brojevi čija je površina kvadrat prirodnog broja.

\(^1\)Claude Gaspard Bachet de Mézières, 1587. - 1638., francuski matematičar i pisac.
Slutnja 5. Ne postoji kub cijelog broja koji je jednak zbroju kubova dva racionalna broja.

Moguće je da je Fermat znao dokazati VFT za slučaj $n = 3$ i $n = 4$. Za posljednji je pronađena njegova skica dokaza u kojoj koristi metodu neprekidnog silaska. Iako je neposredno nakon iskaza teorema Fermat napisao da ga zna u cijelosti dokazati, danas je upućeno mišljenje da dokaz zapravo nije znao. U prilog tome ide i činjenica da su ga mnogi veliki matematičari pokušali dokazati no većinom su uspjevali dokazati samo neke specijalne slučajeve. U novije vrijeme su na dokazu radila trojica matematičara: Gerhard Frey\textsuperscript{2}, Richard Taylor\textsuperscript{3} i Andrew Wiles\textsuperscript{4}. Posljednji je korak napravio Wiles 1995. godine nakon gotovo 360 godina.

5.2 Eulerov doprinos


Teorem 5.2.1. Jednadžba $x^4 - y^4 = z^2$ nema cjelobrojnih rješenja uz uvjet $xyz \neq 0$.

Geometrijski prethodnu tvrdnju možemo interpretirati da ne postoji Pitagorin trokut, odnosno pravokutan trokut čije su stranice cjelobrojne, u kome su hipotenuza i jedna kateta kvadrati prirodnih brojeva. On ima dvije važne posljedice. Jedna je dokaz Slutnje 5.2 koja je zapravo njen korolar.

Korolar 5.2.2. Jednadžba $x^4 + y^4 = z^4$ nema cjelobrojnih rješenja uz uvjet $xyz \neq 0$.

Dokaz. Pretpostavimo suprotno, tj. neka je $(a, b, c) \in \mathbb{Z}^3$, $abc \neq 0$, rješenje jednadžbe $x^4 + y^4 = z^4$. Tada je

$$c^4 - a^4 = (b^2)^2,$$

odnosno $(c, a, b^2)$ je rješenje jednadžbe $x^4 - y^4 = z^2$ koje zadovoljava uvjet $xyz \neq 0$ što nije moguće prema Teoremu 5.2.1. \hfill \Box

\textsuperscript{2}Gerhard Frey, rođen 1944., njemački matematičar.
\textsuperscript{3}Richard Lawrence Taylor, rođen 1962., američki matematičar.
\textsuperscript{4}Sir Andrew John Wiles, rođen 1953., britanski matematičar.
Nepotpun dokaz VFT za slučaj \( n = 3 \) Euler je dao 1753., ali je postao poznat tek nakon objavljivanja djela *Elements of algebra* 1770. godine. Dokaz je proveo *metodom neprekidnog silaska*, a u nastavku donosimo skicu dokaza.

**Dokaz.** Pretpostavimo da je \((a, b, c) \in \mathbb{Z}^3\) rješenje jednadžbe

\[
x^3 + y^3 + z^3 = 0, \tag{5.1}
\]

pri čemu su cijeli brojevi \(a, b, c \neq 0\) u parovima relativno prosti te ne svi pozitivni. Naime, kada bi dva navedena broja sadržavala zajednički faktor, tada bi ga sadržavao i treći broj pa bismo jednadžbu mogli podijeliti tim faktorom. Točno jedan od ta tri broja mora biti paran pa bez smanjenja općenitosti možemo pretpostaviti da je to \(c\). Kako su \(a\) i \(b\) neparni brojevi, oni nužno moraju biti različiti. U protivnom bi vrijedio

\[
2a^3 = -c^3,
\]

iz čega slijedi da je \(a\) paran što je u proturječju s pretpostavkom da je samo \(c\) paran. Zbroj i razlika dva neparna broja je paran broj pa vrijedi

\[
a + b = 2u, \quad a - b = 2v,
\]

iz čega slijedi

\[
a = u + v, \quad b = u - v. \tag{5.2}
\]

Uvrstimo li (5.2) u početnu jednadžbu (5.1) dobivamo

\[
-c^3 = (u + v)^3 + (u - v)^3 = 2u \left( u^2 + 3v^2 \right). \tag{5.3}
\]

Zbog različite parnosti cijelih brojeva \(u \neq 0\) i \(v \neq 0\), broj \(u^2 + 3v^2\) je uvijek neparan. Primjetimo, \(u\) i \(v\) su različite parnosti i relativno prosti. Kada bi imali zajednički faktor veći od 1, on bi djelio i \(a\) i \(b\) što je u suprotnosti s pretpostavkom \((a, b) = 1\). Također možemo pretpostaviti da su \(u\) i \(v\) oba pozitivna, inače zamjenimo \(a\) i \(b\). Prema ranijoj pretpostavci \(c\) je paran iz čega slijedi da je \(u\) paran, a \(v\) neparan. Kako je \((u, v) = 1\) zaključujemo da je najveći zajednički djelitelj brojeva \(2u\) i \(u^2 + 3v^2\) ili 1 ili 3.

1. **slučaj.** Neka je \((2u, u^2 + 3v^2) = 1\). Tada \(3 \nmid u\) i vrijedi

\[
2u = r^3, \tag{5.4}
\]

\[
u^2 + 3v^2 = s^3. \tag{5.5}
\]
Euler je sada uočio sljedeći identitet,
\[
(e^2 + 3f^2)^3 = (e^2 + 3f^2) \left( (e^2 - 3f^2)^2 + 3(2ef)^2 \right),
\]
\[
= \left(e(e^2 - 3f^2) + 3f(2ef)\right)^2 + 3 \left(e(2ef) + f(e^2 - 3f^2)\right)^2
\]
\[
= (e^3 - 9ef^2)^2 + 3(3e^2f - 3f^3)^2.
\]
Dakle, ako
\[
u = e^3 - 9ef^2, \quad v = 3e^2f - 3f^3,
\]
onda
\[
u^2 + 3v^2 = (e^2 + 3f^2)^3.
\]
Ono što je Euleru trebalo u nastavku dokaza jest da je jedini način da broj oblika
\[
u^2 + 3v^2
\]
bude kub, jest da \( u \) i \( v \) budu oblika (5.6). Konkretno, formulirao je u dvije tehničke leme.

**Lema 5.2.3.** Ako je \( s \) neparan broj za koji vrijedi \( s^3 = u^2 + 3v^2 \), tada postoje relativno prosti cijeli brojevi \( e \) i \( f \) takvi da je \( s = e^2 + 3f^2 \).

**Lema 5.2.4.** Ako je broj \( u^2 + 3v^2 \) kub pri čemu su \( u \) i \( v \) relativno prosti brojevi različite parnosti, onda postoje relativno prosti brojevi \( e \) i \( f \) različite parnosti takvi da je \( u = e (e^2 - 9f^2), v = 3f (e^2 - f^2) \).

Euler je dokaz prethodne leme bazirao se na netočnoj tvrdnji. Ispravak njegove greške možemo pronaći u odsječku 2.5 iz [7].

Pretpostavimo da je \( e \) paran, što znači da je \( f \) neparan. Iz (5.4) je
\[
r^3 = 2u = 2e(e - 3f)(e + 3f).
\]
Kako su faktori \( 2e, e - 3f, e + 3f \) u parovima relativno prosti, svaki od njih mora biti kub cijelog broja, odnosno
\[
-2e = a_1^3, \\
e - 3f = b_1^3, \\
e + 3f = c_1^3.
\]
Time smo dobili "manje" rješenje \((a_1, b_1, c_1)\) jednadžbe \( x^3 + y^3 + z^3 = 0 \). Zaista, \(|c_1| \leq 2u \leq a + b < |c|\). Stoga primjenom metode silaska zaključujemo da ne postoji netrivijalno rješenje.
2. slučaj. Neka je \((2u, u^2 + 3v^2) = 3\). Tada 3 \(\mid u\) i 3 \(\nmid v\) pa možemo pisati \(u = 3w\). Tada je

\[-z^3 = 2u \left(u^2 + 3v^2\right) = 2 \cdot 3^2 w \left(3w^2 + v^2\right)\]

iz čega se lako vidi \((2 \cdot 3^2 w, 3w^2 + v^2) = 1\) što znači da su oba broja kubovi nekih cijelih brojeva, odnosno vrijedi

\[18w = r^3,\]
\[3w^2 + v^2 = s^3.\]

Sada je nastavak dokaza analogan postupku u 1. slučaju. \square
Poglavlje 6

Pellova jednadžba

_Diofantska jednadžba_ je polinomijalna jednadžba sa cijelobrojnim koeficijentima koja se rješava u prstenu cijelih brojeva. Specijalna diofantska jednadžba oblika

\[ x^2 - dy^2 = 1, \tag{6.1} \]

gdje je \( d \) prirodan broj koji nije potpuni kvadrat, zove se _Pellova jednadžba_. Pellova jednadžba uvijek ima trivijalno rješenje \((1, 0)\), a ostala rješenja traže se u skupu prirodnih brojeva. Najmanje među njima zove se _fundamentalno rješenje_.

Modifikacija jednadžbe \( (6.1) \) oblika

\[ x^2 - dy^2 = N, \tag{6.2} \]

za \( N \in \mathbb{N} \), zove se _pellovska jednadžba_.


---

1Brahmagupta, 598. - oko 670., indijski matematičar.
2Bhaskara II, 1114.- 1185., indijski matematičar.

Iako jednadžba novi Pellovo ime, najčešće izvori kažu da ona s njim nema mnogo veze. Naime, Euler ju je u jednom članku, misleći da je engleski matematičar John Pell pridonio metodi rješavanja jednadžbe, zabunom pripisao njemu. No jednadžba se javila u knjizi Teutsche Algebra švicarskog matematičara Johanna Rhana (17. st.) koji ju je pisao u suradnji s Pellom. Neki kažu da je knjigu zapravo u cijelosti napisao sam Pell pa Eulerova greška možda i nije bila slučajna.

6.1 Eulerovi primjeri

Iako su neke činjenice o Pellovoj jednadžbi i verižnim razlomcima bile poznate puno prije Eulerova vremena, on je prvi koji je području dao začajniji doprinos. Prvo Eulerovo korištenje Pellove jednadžbe nalazimo u De solutione problematum diophanteorum per numeros integros (O rješenju Diofantovog problema) iz 1732. godine. Euler je pokazao na koji način možemo konstruirati rješenja diofantske jednadžbe \( y^2 = ax^2 + bx + c \) ukoliko nam je poznato jedno njezino rješenje, te rješenje Pellove jednadžbe.

Euler započinje promatranjući jednadžbu \( x^2 = ay^2 + b \), te ustanovljuje da ako je \((f, g)\) jedno njezino rješenje, onda i

\[
(x, y) = \left( \frac{f(p^2 + aq^2) - 2agpq}{p^2 - aq^2}, \frac{2fpq - (p^2 + aq^2)g}{p^2 - aq^2} \right)
\]  (6.3)

 zadovoljava tu jednadžbu, pri čemu su \(p, q \in \mathbb{Z}\). Zaista,

\[
\left( \frac{f(p^2 + aq^2) - 2agpq}{p^2 - aq^2} \right)^2 - a \left( \frac{2fpq - (p^2 + aq^2)g}{p^2 - aq^2} \right)^2 = \left( \frac{f^2 - ag^2}{(p^2 - aq^2)^2} \right)^2 = b.
\]

Jasno, ukoliko je \((p, q)\) rješenje Pellove jednadžbe, \(p^2 - aq^2 = 1\), onda smo sigurni da je rješenje u (6.3) cijelobrojno.

Ako rješenje u (6.3) zapišemo kao

\[
(x, y) = (mf - nag, nf - mg),
\]

gdje su

\[
m = \frac{p^2 + aq^2}{p^2 - aq^2}, \quad n = \frac{2pq}{p^2 - aq^2}.
\]
za koje je

\[ m^2 - an^2 = 1, \]

odnosno \((m, n)\) je rješenje Pellove jednadžbe. Stoga, za određivanje rješenja pellovske jednadžbe \(x^2 - ay^2 = b\), treba riješiti i Pellovu \(x^2 - ay^2 = 1\), a na gore opisani način, iz jednog rješenja \((f, g)\) moći ćemo generirati njih beskonačno mnogo.

Sada ćemo prikazati nekoliko originalnih Eulerovih primjera rješavanja Pellove jednadžbe. I sam Euler je svoje primjere prokomentirao sljedećim riječima: “Ovu metodu nije moguće provesti općenito, za svaki \(a\); primjenjiva je samo samo u posebnim slučajevima.” Ono što je Euler s ovime mislio jest da za proizvoljan \(a\) ne može predvidjeti konkretni broj koraka, ali da će nakon neodređenog (konačnog) broja ponavljanja metoda rezultirati određivanjem rješenja.

**Primjer 6.1.1.** Zadana je jednadžba

\[ x^2 - 5y^2 = 1. \]

Pretpostavimo da je \((m, n)\) njeno rješenje. Tada

\[ \sqrt{5n^2 + 1} > 2n. \]

Stoga postoji \(p \in \mathbb{N}\) za koji je

\[ \sqrt{5m^2 + 1} = 2n + p. \]

odnosno

\[ 5n^2 + 1 = 4n^2 + 4np + p^2. \]

Stoga je \(n^2 - 4np - p^2 + 1 = 0\) i rješavanjem te kvadratne jednadžbe po \(n\) dobivamo

\[ n = 2p + \sqrt{5p^2 - 1}. \]

Iz

\[ \sqrt{5p^2 - 1} > 2p \]

slijedi da postoji \(q \in \mathbb{N}\) za koji je

\[ \sqrt{5p^2 - 1} = 2p + q. \]

Kvadriranjem predhodne jednadžbe dobivamo

\[ 5p^2 - 1 = 4p^2 + 4pq + q^2. \]
Ponovo rješavanjem kvadratne jednadžbe po \( p \) slijedi
\[
p = 2q + \sqrt{5q^2 + 1}.
\]
Budući da će se sada ponoviti situacija kao u (6.4), kao i svaki sljedeći korak, za Eulera je to znak da je \( q = 0 \). Otuda je \( p = 1, n = 4 \) i \( m = 9 \). Zaista, \( 9^2 - 5 \cdot 4^2 = 1 \).

**Primjer 6.1.2.** Zadana je jednadžba
\[
x^2 - 7y^2 = 1.
\]
Pretpostavimo da je \((m, n)\) njeno rješenje. Tada je
\[
\sqrt{7n^2 + 1} > 2n
\]
pa postoji \( p \in \mathbb{N} \) takav da je \( \sqrt{7n^2 + 1} = 2n + p \). Kvadriranjem dobivamo jednadžbu
\[
3n^2 - 4np - p^2 + 1 = 0
\]
pa je njeno pozitivno rješenje dano s
\[
n = \frac{2p + \sqrt{7p^2 - 3}}{3}.
\]
Uočimo li da je
\[
n > \frac{4}{3}p > p,
\]
slijedi
\[
\sqrt{7p^2 - 3} = p + 3q.
\]
Nakon kvadriranja te jednadžbe dobivamo
\[
7p^2 - 3 = p^2 + 6pq + 9q^2,
\]
iz čega rješavanjem jednadžbe po \( p \) slijedi
\[
p = \frac{q + \sqrt{7q^2 + 2}}{2}.
\]
Za razliku od prošlog primjera, ovdje se postupak nastavlja. Iz
\[
p > \frac{3}{2}q > q,
\]
slijedi da postoji \( r \in \mathbb{N} \) za koji je
\[
\sqrt{7q^2 + 2} = q + 2r.
\]
Kvadriranjem i rješavanjem jednadžbe dobivamo

\[ q = \frac{r + \sqrt{7r^2 - 3}}{3}. \]

Kako je \( q > r \), postoji prirodan broj \( s \) takav da je \( q = r + s \), pa je

\[ 2r + 3s = \sqrt{7r^2 - 3}. \]

Kvadriranjem dobivamo

\[ -3r^2 + 12rs + 9s^2 + 3 = 0, \]

pa iz rješavanja po \( r \) slijedi

\[ r = 2s + \sqrt{7s^2 + 1}. \]

Uočimo da će se sada ponoviti situacija kao u (6.5), pa postavljamo \( s = 0 \). Sada vrijedi \( s = 0 \Rightarrow r = 1 \Rightarrow q = 1 \Rightarrow p = 2 \Rightarrow n = 3 \Rightarrow m = 8 \).

Zaista, \( 8^2 - 7 \cdot 3^2 = 1 \), pa je uređeni par \((8, 3)\) rješenje početne jednadžbe.

**6.2 Veza s verižnim razlomcima**

Već smo spomenuli da je Euler pokazao kako se uz pomoć jednog rješenja Pellove jednadžbe mogu konstruirati ostala rješenja, a uočio je i da \( \sqrt{d} \) dobro aproksimira rješenja Pellove jednadžbe \( x^2 - dy^2 = 1 \).

U radu *De usu novi algorithmi in problemate Pelliano solvendo* (O korištenju novog algoritma za rješavanje Pellova problema) prezentiranom 1759. godine (a objavljenom nešto kasnije 1767.) Euler daje algoritam za rješavanje Pellove jednadžbe te pri tome koristi verižne razlomke.

**Definicija 6.2.1.** Neka je \( \alpha \in \mathbb{R} \), te neka je

\[ a_0 = [\alpha]. \]
Ako je $a_0 \neq \alpha$, onda postoji $\alpha_1$ takav da je
\[
\alpha = a_0 + \frac{1}{\alpha_1}.
\]
Kako je $\alpha_1 > 1$, to je $a_1 = \lfloor \alpha \rfloor$ prirodan broj. Ako je $a_1 \neq \alpha_1$, onda postoji $\alpha_2$ takav da je
\[
\alpha = a_0 + \frac{1}{a_1 + \frac{1}{\alpha_2}}.
\]
Za $k > 1$ postupak nastavljamo do dok je $a_k = \lfloor \alpha_k \rfloor \neq \alpha_k$.
Ako je $\alpha_n = a_n$, onda je
\[
\alpha = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\ddots + a_n}}}
\]
razvoj broja $\alpha$ u jednostavni konačni verižni razlomak i pišemo $\alpha = [a_0, a_1, \ldots, a_n]$.

Broj $a_i$ nazivamo $i$-tim parcijalnim kvocijentom od $\alpha$. Razlomak $\frac{p_i}{q_i} = [a_0, a_1, a_2, \ldots, a_i]$ zovemo $i$-ta konvergenta od $\alpha$, a $\alpha_i = [a_i, a_{i+1}, \ldots, a_n]$ je $i$-ti potpuni kvocijent od $\alpha$.

Ako je $\alpha$ iracionalan broj, postupak razvoja u verižni razlomak može se provoditi beskonačno. Tada uvodimo oznaku $\lim_{n \to \infty} [a_0, a_1, \ldots, a_n] = [a_0, a_1, a_2, \ldots]$. Ako je $\alpha = [a_0, a_1, a_2, \ldots]$ onda ovaj izraz zovemo razvoj od $\alpha$ u beskonačni jednostavni verižni razlomak. Razlomak $\frac{p_i}{q_i} = [a_0, a_1, a_2, \ldots, a_i]$ zovemo $i$-ta konvergenta od $\alpha$, a $\alpha_i = [a_i, a_{i+1}, \ldots, a_n]$ je $i$-ti parcijalni kvocijent od $\alpha$, a $\alpha_i = [a_i, a_{i+1}, \ldots]$ je $i$-ti potpuni kvocijent od $\alpha$.

Algoritam za određivanje rješenja Pellove jednadžbe 6.1 sastoji se od sljedećih koraka:
1. Postavimo $z_0 = \sqrt{d}$ i $a_0 = \lfloor d \rfloor$.
2. Za svaki $n$ definiramo $z_n = (z_{n-1} - a_{n-1})^{-1}$ i $a_n = \lfloor z_n \rfloor$.
3. U nekom će se trenutku vrijednosti $z_n$ i $a_n$ početi ponavljati, pretpostavimo da se to dogodilo u koraku $i + 1$.
4. Uređeni par $(p_{i-1}, q_{i-1})$ je rješenje Pellove jednadžbe, gdje je $\frac{p_i}{q_i}$ konvergenta od $\sqrt{d}$.
**POGLAVLJE 6. PELLOVA JEDNADŽBA**

**Primjer 6.2.2.** Neka je dana jednadžba $x^2 - 7y^2 = 1$ kao u Primjeru 6.1.2.

Slijedeći korake:

\[
\begin{align*}
  n &= 0, \quad z_0 = \sqrt{7}, \quad a_0 = 2 \\
  n &= 1, \quad z_1 = \left(\sqrt{7} - 2\right)^{-1} = \frac{2 + \sqrt{7}}{3}, \quad a_1 = 1, \\
  n &= 2, \quad z_2 = \left(\frac{2 + \sqrt{7}}{3} - 1\right)^{-1} = \frac{1 + \sqrt{7}}{2}, \quad a_2 = 1, \\
  n &= 3, \quad z_3 = \left(\frac{1 + \sqrt{7}}{2} - 1\right)^{-1} = \frac{1 + \sqrt{7}}{3}, \quad a_3 = 1, \\
  n &= 4, \quad z_4 = \left(\frac{1 + \sqrt{7}}{3} - 1\right)^{-1} = 2 + \sqrt{7}, \quad a_4 = 4, \\
  n &= 5, \quad z_5 = \left(2 + \sqrt{7} - 4\right)^{-1} = \frac{2 + \sqrt{7}}{3}, \quad a_5 = 1.
\end{align*}
\]

Uočimo da su 1. i 5. korak isti pa će koraci 1-4 ponavljati u nedogled. Rješenje Pellove jednadžbe $(p_3, q_3)$ gdje je

\[
\frac{p_3}{q_3} = 2 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1}}} = \frac{8}{3},
\]

iz čega slijedi $8^2 - 7 \cdot 3^2 = 1$.

Primjenom navedenog algoritma dobiju se najmanja rješenja Pellove jednadžbe, a sva ostala mogu se dobiti na način opisan u sljedećem teoremu.

**Teorem 6.2.3.** Ako je $(x_1, y_1)$ najmanje netrivijalno rješenje u prirodnim brojevima jednadžbe $x^2 - dy^2 = 1$, onda su sva rješenja ove jednadžbe dana s $(x_n, y_n)$, za $n \in \mathbb{N}$, gdje su $x_n$ i $y_n$ prirodni brojevi definirani s

\[
x_n + y_n \sqrt{d} = \left(x_1 + y_1 \sqrt{d}\right)^n.
\]

Euler je uočio, ali ne i dokazao, još nekoliko veza između Pellove jednadžbe i verižnih razlomaka. Veze su izražene sljedećim teoremima.

**Teorem 6.2.4.** Ako prirodan broj $d$ nije potpuni kvadrat, onda razvoj u jednostavni verižni razlomak od $\sqrt{d}$ ima oblik

\[
\sqrt{d} = [a_0, a_1, a_2, \ldots, a_2, a_1, 2a_0],
\]

gdje crta iznad kvocijenata označava ponavljanje tog dijela verižnog razlomka u nedogled.

**Teorem 6.2.5.** Neka je i duljina najmanjeg perioda u razvoju od $\sqrt{d}$. Ako je i paran, onda je $x = p_{i-1}$, $y = q_{i-1}$. Ako je i ne paran, onda je $x = p_{2i-1}$, $y = q_{2i-1}$.
POGLAVLJE 6. PELLOVA JEDNADŽBA

Euler je dao i tablicu razvoja u jednostavni verižni razlomak korijena brojeva od 2 do 120 koji nisu potpuni kvadrati, a pripisujemo mu i sljedeći teorem.

**Teorem 6.2.6.** Ako je \( \alpha \) periodski verižni razlomak, onda je \( \alpha \) kvadratna iracionalnost.

Prisjetimo se, za iracionalan broj \( \alpha \) kažemo da je kvadratna iracionalnost ako je \( \alpha \) korijen kvadratne jednadžbe s racionalnim koeficijentima.

**Dokaz.** Neka je \( \alpha = \left[ b_0, b_1, \ldots, b_{k-1}, a_1, a_2, \ldots, a_{m-1} \right] \) periodski verižni razlomak. Označimo s \( \beta = \left[ a_1, a_2, \ldots, a_{m-1} \right] \) čisto periodski dio od \( \alpha \). Tada iz

\[
\beta = \left[ a_1, a_2, \ldots, a_{m-1}, \beta \right]
\]

slijedi da postoje cijeli brojevi \( p_{m-1}, p_{m-2}, q_{m-1} \) i \( q_{m-2} \) takvi da je

\[
\beta = \frac{p_{m-1} \beta + p_{m-2}}{q_{m-1} \beta + q_{m-2}}.
\]

Time smo dobili kvadratnu jednadžbu s cjelobrojnim koeficijentima za \( \beta \). Kako je \( \beta \) iracionalan broj koji je korijen kvadratne jednadžbe s racionalnim koeficijentima, zaključujemo da je \( \beta \) kvadratna iracionalnost. Sada \( \alpha \) možemo zapisati kao

\[
\alpha = \frac{p \beta + P}{q \beta + Q},
\]

gdje su \( p, P, q, Q \) cijeli brojevi te \( \frac{p}{q}, \frac{P}{Q} \) zadnje dvije konvergente od \( \left[ b_0, b_1, \ldots, b_{k-1} \right] \).

Kako je \( \beta = \frac{a + \sqrt{b}}{c} \), pri čemu je \( c \neq 0 \), a \( b > 0 \) broj koji nije potpuni kvadrat, slijedi da i \( \alpha \) ima isti oblik, dakle, \( \alpha \) je iracionalan broj.

Vrijedi i obrat navedenog teorema, a dokazao ga je Lagrange.

**Primjer 6.2.7.** Neka je dan periodski verižni razlomak \( \alpha = \left[ 3, \frac{1}{\sqrt{6}} \right] \). Tada je

\[
\beta = \left[ \frac{1}{\sqrt{6}} \right] = 1 + \frac{1}{6 + \frac{1}{\sqrt{6}}},
\]

iz čega slijedi da je \( \beta \) rješenje kvadratne jednadžbe \( 6 \beta^2 - \beta - 1 = 0 \). Kako je \( \beta > 0 \) slijedi da je \( \beta = \frac{3 + \sqrt{15}}{6} \). Sada je

\[
\alpha = 3 + \frac{1}{\beta} = 3 + \frac{1}{\frac{3 + \sqrt{15}}{6}} = \sqrt{15},
\]
$a \sqrt{15}$ jest kvadratna iracionalnost.

Na kraju ćemo napomenuti da je Euler razvijao analitičku teoriju verižnih razlomaka. 1748. godine uočio je sljedeću vezu između konačnog zbroja i verižnog razlomka:

\[
a_0 + a_0a_1 + a_0a_1a_2 + \cdots + a_0a_1a_2 \cdots a_n = \frac{a_0}{1 - \frac{a_1}{1 + a_1 - \frac{a_2}{1 + a_2 - \frac{a_3}{\ddots}}}}.
\]

Prethodna relacija se može proširiti na sumu reda, odnosno beskonačni verižni razlomak što postaje vrlo koristan alat matematičke analize. Specijalno, zahvaljujući tome, Euler je broj $e$ prikazao u obliku beskonačnog verižnog razlomka:

\[
e = 2 + \frac{1}{1 + \frac{1}{2 + \frac{2}{3 + \frac{3}{4 + \ddots}}}}.
\]

odnosno

\[
e = [2, 1, 2, 1, 4, 1, 1, 6, 1, 1, 8, \ldots].
\]
Bibliografija


POGLAVLJE 6. PELLOVA JEDNADŽBA

[13] C. E. Sandifer, *How Euler Did It*, dostupno na https://books.google.hr/books?id=sohHs7Ex0sYC&pg=PA66&lpg=PA66&dq=euler+pell+equation&source=bl&ots=1iQ0Wn9Wkg&sig=r7Y1oOSLPt8RPp6DluUT_VM FY3k&hl=en&sa=X&ved=2ahUKEwiuh931x_7cAhUpp4skHb7RAKBQ6AEwB3oECAIQAQ#v=onepage&q=euler%20pell%20equation&f=false (kolovoz 2018.).


[23] *Euler’s four-square identity*, dostupno na https://en.wikipedia.org/wiki/Euler%27s_four-square_identity (kolovoz 2018.).


POGLEVLJE 6. PELLOVA JEDNADŽBA


[31] *Leonhard Euler by Handmann*, dostupno na https://upload.wikimedia.org/wikipedia/commons/0/03/Leonhard_Euler_by_Handmann.png (rujan 2018.).


[38] *Proof of Fermat’s Last Theorem for specific exponents*, dostupno na https://en.wikipedia.org/wiki/Proof_of_Fermat%27s_Last_Theorem_for_specific_exponents#Proof_for_Case_A_2 (kolovoz 2018.).

Leonhard Euler (1707.-1783.) najproduktivniji je matematičar svih vremena. Dao je ogroman doprinos svakom matematičkom području svog vremena, ali i mnogim drugim znanostima kao što su geografija, fizika, teorija glazbe, ... Postavio je temelje nekim matematičkim granama, a smatra se da je posebnu "virtuoznost" pokazao baveći se teorijom brojeva. U radu ćemo opisati samo neke njegove doprinose elementarnoj teoriji brojeva, primjerice dokaz Malog Fermatovog teorema, Velikog Fermatovog teorema za \( n = 3 \) i Teorema o dva kvadrata te mnoge zaključke vezane uz djeljivost prirodnih brojeva, Legendreov simbol i Pellovu jednadžbu.
Summary

Leonhard Euler (1707. - 1783.) is the most productive mathematician of all time. He made enormous contributions to every mathematical branch of his time as well as to many other fields of science such as geography, physics, music theory, . . . He laid the foundations for some mathematical branches, however, number theory is considered the branch where his “virtuosity” was most evident. This paper describes just some of his contributions to elementary number theory, such as the proof of Fermat’s little theorem, Fermat’s last theorem for $n = 3$ and his Theorem on the sum of two squares as well as many conclusions related to the divisibility of natural numbers, the Legendre symbol and Pell’s equation.
Životopis