Neki doprinosi Leonharda Eulera u matematici

Orsag, Mario

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Mario Orsag

NEKI DOPRINOSI LEONHARDA EULERA U MATEMATICI

Diplomski rad

Voditelj rada:
doc.dr.sc. Igor Ciganović

Zagreb, rujan, 2023.

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 posvećujem svojim roditeljima, sestrama i djevojci Ivani za svu potporu pruženu tokom mog školovanja.
Zahvaljujem nećacima Mateu i Marti na svim osmijesima kojima su mi uljepšali zadnje godine studiranja, dedi Tomašu na svim pruženim trenucima razbibrige "vu Gradecu", baki Ani za svu iskazanu brigu te dedi Ivi za sve poticajne riječi koje me prate kroz život.
Naposlijetku, zahvaljujem mentoru, doc.dr.sc. Igoru Ciganoviću, na ukazanom povjerenju i uloženom trudu prilikom izrade diplomskog rada.

Sadržaj

Uvod

Leonhard Euler, znameniti švicarski matematičar, rođen je 15. travnja 1707. u Baselu. Eulerovo zanimanje za matematiku potaknuo je njegov otac, protestantski svećenik koji je tokom studija slušao predavanja Jacoba Bernoullija. Iako je Leonhard Euler najprije studirao teologiju, uz poticaj Johanna Bernoullija upisuje studij matematike u Baselu.
Studij završava 1726. godine te se iste godine, uz pomoć Danielea Bernoullija, zapošljava na matematičko-fizičkom odjelu akademije znanosti u St. Petersburgu. 1727. objavljuje rad o najboljem rasporedu jarbola na brodu kojim osvaja drugo mjesto u natječaju za *Grand Prix* Pariške akademije znanosti. Kada je Daniel Bernoulli 1733. godine napustio St. Petersburg, Euler je preuzeo upražnjeno mjesto glavnog profesora matematike. Poboljšanjem financijskog stanja, 1734. godine oženio je Katharin Gsell s kojom je imao trinaestero djece, od kojih je samo petero doživjelo odraslu dob. Poznata je Eulerova izjava da je neka od svojih najvećih matematičkih otkrića imao držeći jedno dijete u rukama, dok su se ostala djeca igrala oko njega. 1735. godine počinju Eulerovi zdravstveni problemi. Najprije je jedva preživio napad groznice, a nakon toga mu se počeo pogoršavati vid, da bi do 1740. godine potpuno izgubio vid. Iako lošijeg zdravstvenog stanja, Euler je i dalje ostvarivao iznimne matematičke rezultate pa je tako 1738. i 1740. osvojio *Grand Prix* Pariške akademije znanosti.
Uslijed političkih nemira u St. Petersburgu, pozicija stranaca u Rusiji je postajala sve teža pa Euler 1941. godine napušta Rusiju i, na poziv cara Friedricha velikog, odlazi u Berlin gdje se zapošljava na Berlinskoj akademiji znanosti. U samom početku rada na akademiji Euler je smatrao da je najsretniji čovjek na svijetu što je doprinijelo tome da je tokom svog boravka u Berlinu napisao gotovo 400 članaka koji su se bavili različitim matematičkim temama. Također, u 25 godina svog boravka u Parizu izdao je i nekoliko knjiga koje su se bavile temama matematičke analize, varijacijskog računa, artiljerije, balistike, gradnje brodova, navigacije, proračunavanja orbite planeta itd. Iz tog vremena potječe i popularno znanstveno djelo *Pisma jednoj princezi*.
S vremenom, uslijed carevog miješanja u rad akademije, Euler postaje sve nezadovoljniji radom i životom u Berlinu te se 1766. vraća u St. Petersburg. Ubrzo nakon toga potpuno je oslijepio, a 1771. njegov dom je izgorio u požaru te je prilikom požara uspio spasiti samo sebe i svoja djela. Unatoč sljepoći, uz pomoć dvojice svojih sinova i kolega te zahva-

ljujući svom iznimno dobrom pamćenju, Euler je nastavio svoj znanstveni rad te je u tom razdoblju objavio gotovo polovinu svojih djela. Na sam dan svoje smrti, 18. rujna 1783., podučavao je jednog od svojih unuka matematici, raspravljao o otkriću planeta Urana i bavio se proračunima kretanja dvaju balona. U 17 sati, uslijed krvarenja u mozgu, izjavio je ”Umirem.” te ubrzo nakon toga umro. O njegovoj golemoj ostavštini matematičkih rezultata i otkrića svjedoči činjenica da je nakon njegove smrti akademija znanosti u St. Petersburgu još gotovo pedeset godina objavljivala njegove neobjavljene radove.

Poglavlje 1

Teorija grafova

Kao početak teorije grafova, jedne od najpopularnijih grana moderne matematike, smatra se Eulerovo rješenje poznatog problema šetnje Königsberškim mostovima U ovome poglavlju upoznat ćemo se sa temeljnim pojmovima vezanim uz grafove te prikazati utjecaj Leonharda Eulera teoriju grafova, odnosno objasniti zbog čega ga smatramo utemeljiteljem topologije, poddiscipline teorije grafova. Glavni izvori ovog poglavlja su [7], [8] i [16].

1.1 Osnovni pojmovi

Kako bismo lakše mogli shvatiti doprinose Leonharda Eulera u teoriji grafova, najprije se moramo upoznati sa samim pojmom grafa te njegovim svojstvima.

Definicija 1.1.1. *Graf G je uređena trojka* (V, E, φ)*,* $G=(V, E, \varphi)$ *gdje je V neprazan skup čije elemente nazivamo* ***vrhovima****, E je skup disjunktan s V čije elemente nazivamo* ***bridovima*** *i* φ *preslikavanje koje svakom bridu pridružuje neuređeni par (ne nužno različitih) vrhova. Preslikavanje* $\varphi : E \to \{\{u, v\} : u, v \in V\}$ *nazivamo* ***incidencijska funkcija*** *grafa G.*

Definicija 1.1.2. *Kada imamo preslikavanje* $\varphi(e)=\{u, v\}$*, tada vrhove u i v nazivamo* ***krajevi*** *brida e te kažemo da su ti bridovi međusobno* ***susjedni****. Također, kažemo da su vrhovi u i v spojeni bridom e, odnosno vrhovi u i v su* ***incidentni*** *s bridom e i obrnuto. Dva brida su susjedna ako su incidentni istom vrhu.*

Definicija 1.1.3. *Brid e kojemu su krajevi isti vrh naziva se* ***petlja****. Ako brid e nije petlja, tada je on* ***pravi brid*** *ili* ***karika****.*

Definicija 1.1.4. *Dva ili više različitih bridova međusobno su* ***paralelni*** *ako imaju iste krajeve. Skup međusobno paralelnih bridova nazivamo* ***višestruki brid****.*

Definicija 1.1.5. *Graf bez petlji i višestrukih bridova naziva se* ***jednostavan graf****. Ako graf nema bridova te ima samo jedan vrh, tada kažemo da je graf* ***trivijalan****.*

Za graf $G=(V, E, \varphi)$ kažemo da je **konačan** ako su skupovi V i E konačni. Ako barem jedan od tih skupova nije konačan, tada graf G nazivamo **beskonačnim**.
Broj vrhova grafa nazivamo **red** i označavamo $|V_G|$ ili $v(G)$. Broj bridova grafa nazivamo **veličina** grafa G i označavamo $|E_G|$ ili $e(G)$.

Definicija 1.1.6. ***Potpun graf****, u oznaci K_n, je jednostavan graf kojemu je svaki par vrhova spojen bridom.*

Ako je graf G potpun i ima n vrhova, tada vrijedi $|E_G|=\binom{n}{2}$.

Definicija 1.1.7. ***Stupanj (valencija) vrha*** *v, u oznaci $deg(v)$, u grafu G definiramo kao broj bridova grafa G koji su incidentni s v pri čemu se za svaku petlju broje dvije incidencije.*

Najmanju vrijednost među stupnjevima grafa označavamo s $\delta(G)$ i nazivamo **minimalni stupanj grafa**, a najveću među tim vrijednostima označavamo s $\triangle(G)$ i nazivamo **maksimalni stupanj grafa**.

Definicija 1.1.8. *Ako za vrh v u grafu G vrijedi $deg(v)= 0$ tada vrh v nazivamo* ***izolirani vrh****.*

Definicija 1.1.9. *Ako za vrh v u grafu G vrijedi $deg(v)= 1$, kažemo da je vrh v* ***krajnji vrh*** *ili* ***list*** *grafa G. Krajnjem vrhu incidentan je* ***krajnji brid****.*

Definicija 1.1.10. *Za graf G kažemo da je* ***regularan*** *ako su mu svi vrhovi istog stupnja, odnosno da je r-****regularan*** *ako za sve v iz V_G vrijedi $deg(v) = r$. Broj r nazivamo* ***stupanj regularnosti*** *grafa G.*

Ako iz jednog vrha grafa, preko niza bridova, možemo doći do drugoga vrha smatramo da su ta dva vrha povezana. Analogno, graf smatramo povezanim ako se iz svakog njegovog vrha možemo ”prošetati” do bilo kojeg drugog njegovog vrha. Na tragu ovakvih opisa definiramo pojmove šetnje, staze, puta, ciklusa pomoću kojih analiziramo svojstva grafova.

Definicija 1.1.11. *Konačan niz vrhova v_i i bridova e_i oblika $v_0, e_1, v_1, \ldots, e_l, v_l$ pri čemu su krajevi brida e_i vrhovi v_{i-1} i v_i nazivamo* ***šetnja*** *W u grafu G.Vrh v_0 nazivamo* ***početni vrh*** *ili* ***početak****, dok vrh v_l nazivamo* ***završni vrh*** *ili* ***završetak****. Ostale vrhove koji pripadaju šetnji nazivamo* ***unutarnji*** *vrhovi. Za šetnju W s početkom u vrhu v_0 i završetkom u vrhu v_l kažemo da je to (v_0, v_l)-* ***šetnja****. Broj bridova l naziva se* ***duljina šetnje****. Kažemo da je šetnja* ***zatvorena*** *ako vrijedi $v_0 = v_l$, inače je šetnja* ***otvorena****.*

Definicija 1.1.12. *Šetnju čiji su svi bridovi međusobno različiti nazivamo* ***staza****. Stazu koja ima međusobno različite vrhove nazivamo* ***put****.*

Definicija 1.1.13. *Šetnja (staza, put) koja se sastoji od samo jednog vrha i nema bridova se zove* ***trivijalna šetnja (staza, put)****.*

Definicija 1.1.14. *Zatvorenu stazu koja sadrži barem jedan brid i ima međusobno različite unutarnje vrhove nazivamo* ***ciklus****.*

Definicija 1.1.15. *Neka su zadana dva grafa, G i H. Ako vrijedi $V_H \subseteq V_G$, $E_H \subseteq E_G$ i svaki brid grafa H ima iste krajeve u H kao što ih ima u G, onda kažemo da je H* ***podgraf*** *grafa G i pišemo $H \subseteq G$. Dodatno, kažemo da je graf G* ***nadgraf*** *grafa H.*

Uočimo da podgraf nekog grafa možemo dobiti **uklanjanjem bridova** i/ili vrhova tog istog grafa te restringiranjem funkcije incidencije.
Neka je e brid grafa, tada $G - e$ označava graf dobiven uklanjanjem brida e iz grafa G te restringiranjem funkcije incidencije. Ukoliko je F neprazan skup bridova od G, tada $G - F$ označava graf dobiven uklanjanjem svih bridova skupa F iz grafa G. Graf iz kojeg se uklanjanjem odgovarajućeg skupa bridova dobije graf G označavamo s $G + e$ ili $G + F$.
Analogno, neka je v brid grafa, tada $G - v$ označava graf dobiven uklanjanjem vrha v i incidentnih bridova iz grafa G te restringiranjem funkcije incidencije. Ukoliko je S neprazan pravi podskup skupa vrhova V_G, tada $G - S$ označava graf dobiven uklanjanjem svih vrhova skupa S iz grafa G.
Ukoliko iz grafa uklonimo petlje i svaki njegov višestruki brid, tada dobivamo jednostavan graf te takav graf nazivamo **pripadajući jednostavni graf** tog grafa.

Definicija 1.1.16. *Ako su svaka dva vrha grafa G povezana putem, kažemo da je graf G povezan. U suprotnom kažemo da je graf G nepovezan. Povezani podgraf koji nije sadržan ni u jednom većem povezanom podgrafu nazivamo* ***komponenta povezanosti*** *te broj komponenti grafa G označavamo s $c(G)$.*

Definicija 1.1.17. *Povezani graf bez ciklusa nazivamo* ***stablo****.*

Teorem 1.1.18. *Stablo s n vrhova ima točno $n - 1$ bridova.*

Dokaz. Tvrdnja se dokazuje pomoću matematičke indukcije, a dokaz tvrdnje se nalazi u [7]. □

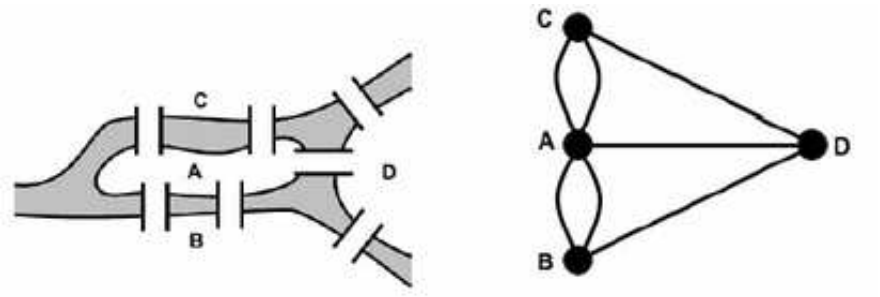
Definicija 1.1.19. *Neka su zadani vrh v i brid e grafa G. Ako vrijedi $c(G - v) > c(G)$, tada vrh v nazivamo* ***rezni vrh****. Ako vrijedi $c(G - e) > c(G)$ tada brid e nazivamo* ***rezni brid*** *ili* ***most*** *grafa G.*

Teorem 1.1.20. *Neka je G jednostavni povezani graf minimalnog stupnja $\delta(G)$, onda G sadrži put P duljine $d(P) \geq \delta(G)$. Ako dodatno vrijedi $\delta(G) \geq 2$, tada graf G sadrži ciklus duljine $d(C) \geq \delta(G) + 1$.*

Dokaz. Pretpostavimo da je put $Q = v_1, v_2, \ldots, v_t$ put maksimalne duljine grafa G. Ako je vrh v susjedan vrhu v_1, onda $v \in \{v_2, \ldots, v_t\}$. U suprotnom bi put $v, v_1, v_2, \ldots, v_t$ bio dulji od Q, što je u kontradikciji s maksimalnosti puta Q. Dakle, put Q sadrži svih $deg(v_1)$ vrhova susjednih vrhu v_1. Put Q sadrži barem $\deg(v_1) + 1 \geq \delta(G) + 1$ vrhova, odnosno ima duljinu $d(Q) \geq \delta(G)$. Neka je $\delta(G) \geq 2$, tada je maksimalan put duljine barem 2. Neka uz to vrijedi $v_1, v_2, \ldots, v_t, t \geq 3$. Zbog $\delta(G) \geq 2$ postoji $v_i, i \in \{3, \ldots, t\}$ incidentan s v_1 i $v_i \neq 2$. Tada je $v_1, v_2, \ldots, v_i, v_1$ traženi ciklus. □

1.2 Eulerovi grafovi

Jedan od najpoznatijih problema vezan uz Eulerove grafove je problem Königsberških mostova. 1736. godine, Euler je u svom radu *Solutio problematis ad geometriam situs pertinentis* uz odgovarajuće objašnjenje dao negativan odgovor na pitanje "Mogu li građani Königsberga obići grad tako da se svaki od njegovih sedam mostova prijeđe točno jednom i na kraju se vratiti na početnu poziciju?". Na slici 1.1 lijevo nalazi se prikaz Königsberških mostova.



Slika 1.1: Prikaz Königsberških mostova (preuzeto iz [8])

Euler je uočio da, ako povezanost grada mostovima prikažemo shematskim prikazom gdje vrhovi predstavljaju pojedina područja grada, odnosno obale, a bridovi predstavljaju mostove, se promatrani problem svodi na traženje zatvorene staze koja prolazi svakim bridom točno jedanput. Na slici 1.1 desno nalazi se shematski prikaz Königsberških mostova.

Definicija 1.2.1. ***Eulerova staza*** *je staza u grafu koja sadrži svaki brid grafa. Zatvorenu Eulerovu stazu nazivamo* ***Eulerovom turom****. Graf G je* ***Eulerov*** *ili* ***euleorovski*** *ako je*

graf povezan te sadrži Eulerovu turu. Kažemo da je povezani graf ***skoro Eulerov*** *ako nije Eulerov, ali sadrži Eulerovu stazu.*

Baveći se problemom Königsberških mostova, Euler nije samo dokazao da je navedena šetnje nemoguća, već je dao postupak za sve takve zadatke koji ćemo iskazati kroz slijedeće teoreme i korolare.

Teorem 1.2.2. *Povezani graf je Eulerov ako i samo ako je svaki njegov vrh parnog stupnja.*

Da bismo dokazali navedeni teorem potrebna nam je lema koja povezuje stupanj grafa i postojanje ciklusa.

Lema 1.2.3. *Ako je svaki vrh grafa stupnja većeg ili jednakog 2, tada graf sadrži ciklus.*

Dokaz. Ukoliko graf sadrži petlje ili višestruke bridove, tada oni određuju ciklus pa tvrdnja u tom slučaju vrijedi.
Ako je G jednostavni graf s minimalnim stupnjem vrhova $\delta(G) \geq 2$, tada prema Teoremu 1.1.20 graf G sadrži ciklus. □

Dokažimo sada Teorem 1.2.2

Dokaz. $\Rightarrow$: Pretpostavimo da je graf G Eulerov, tada graf sadrži Eulerovu turu Q. Svaki puta kada Eulerova tura uđe u vrh v, ona mora i izaći iz njega pa Eulerova tura definira bijekciju između bridova koji ulaze u v, a nisu petlje, te bridova koji izlaze iz v, a također nisu petlje. Budući da Q, sadrži sve bridove grafa, slijedi da je stupanj svakog vrha višekratnik broja 2, odnosno paran broj.
$\Leftarrow$: Pretpostavimo da povezani graf G ima sve vrhove parnog stupnja. Dokaz ćemo provoditi koristeći se indukcijom po broju m bridova grafa. Pretpostavimo da je $m = 0$ ili $m = 1$. Tada graf G ima jedan vrh koji je izoliran ili je u njemu petlja pa tvrdnja očigledno vrijedi. Neka je $m \geq 2$. Koristeći pretpostavku da je graf G povezan te su mu svi vrhovi parnog stupnja, slijedi da je stupanj svakog vrha najmanje 2. Prema Lemi 1.2.3 slijedi da graf G sadrži ciklus. Označimo taj ciklus s C. Ukoliko ciklus C sadrži svaki brid grafa G tada smo dokazali tvrdnju. Ukoliko C ne sadrži svaki brid grafa G, uklanjanjem svih bridova koji pripadaju ciklusu C dobivamo novi graf H koji ne mora biti povezan. Uočimo da graf H ima manje bridova nego graf G, no i dalje su svi vrhovi grafa H parnog stupnja. Koristeći indukcijsku pretpostavku, svaka komponentnta povezanosti grafa H ima Eulerovu turu. Eulerovu turu u grafu G dobijemo slijedeći vrhove ciklusa C krenuvši od proizvoljno izabranog vrha. Svaka komponenta grafa H ima zajednički vrh s C. Kada, ciklusom C, dođemo do komponente grafa H koja nije izolirani vrh, prođemo Eulerovom turom te komponente povezanosti te istim postupkom nastavljamo dalje po ciklusu. Na kraju ćemo doći u vrh ciklusa C iz kojeg smo krenuli, a prijeđeni vrhovi i bridovi činit će Eulerovu turu grafa G. □

Koristeći razmišljanje kao u dokazu prethodnog teorema, možemo okarakterizirati Eulerov graf pomoću ciklusa.

Definicija 1.2.4. *Ako su skupovi bridova dva ciklusa grafa G disjunktni, tada kažemo da su ciklusi* ***bridno disjunktni****. Ukoliko postoji skup međusobno bridno disjunktnih ciklusa takvih da oni sadrže sve bridove grafa G onda kažemo da graf G možemo rastaviti na bridno disjunktne cikluse, odnosno graf G ima ciklički rastav.*

Korolar 1.2.5. *Ako je graf G povezan, sljedeće tvrdnje su ekvivalentne:*

(1) *G je Eulerov graf.*

(2) *Svaki vrh grafa G je parnog stupnja.*

(3) *Graf G možemo rastaviti na bridno disjunktne cikluse.*

Dokaz. Ekvivalentnost tvrdnji (1) i (2) proizlazi iz Teorema 1.2.2
Dokažimo sada da su tvrdnje (2) i (3) ekvivalentne. Koristeći se analognim postupkom, kao kod dokazivanja drugog smjera Teorema 1.2.2, uočavamo da povezani graf kojem su svi vrhovi parnog stupnja ima ciklički rastav. Ukoliko graf možemo rastaviti na bridno disjunktne cikluse, tada je stupanj svakog njegovog vrha jednak dvostrukom broju ciklusa kojima taj vrh pripada, pa slijedi da su svi vrhovi parnog stupnja. Time smo dokazali da su tvrdnje (2) i (3) ekvivalentne.
Iz dokazanih ekvivalencija proizlazi ekvivalentnost tvrdnji (1), (2) i (3). □

Dokažimo još nekoliko činjenica o skoro Eulerovim grafovima.

Lema 1.2.6. *(Lema o rukovanju) U svakom grafu je zbroj stupnjeva svih vrhova paran broj. Ako je m broj bridova grafa, onda je:*

$$\sum_{v \in V} deg(v) = 2m$$

Dokaz. Prebrojimo na dva načina incidencije u grafu (par vrh i brid koji su incidentni) računajući dvostruko incidencije petlji. Kada brojimo po vrhovima, ukupan broj incidencija jednak je zbroju stupnjeva svih vrhova. Brojimo li po bridovima, svaki brid ima dvije incidencije pa ih je ukupan broj $2m$. Izjednačavanjem dobivenih vrijednosti, dokazali smo tvrdnju. □

Korolar 1.2.7. *Povezani graf G ima Eulerovu stazu ako i samo ako ima najviše dva vrha neparnog stupnja.*

Dokaz. $\Rightarrow$ Pretpostavimo da graf G ima Eulerovu stazu. Budući da je Eulerova staza staza koja svakim bridom grafa G prolazi točno jedanput, slijedi da svaki vrh tog grafa koji nije početak ni kraj te staze ima paran broj incidentnih bridova.
$\Leftarrow$ Pretpostavimo da povezani graf G ima najviše dva vrha neparnog stupnja. Tada slijedi da graf G ima 0, 1 ili 2 vrha neparnog stupnja. Ako ima 0 takvih vrhova, slijedi da su svi vrhovi parnog stupnja, odnosno prema Korolaru 1.2.7. slijedi da je graf G Eulerov pa sadrži zatvorenu Eulerovu stazu. Iz Leme o rukovanju, znamo da je zbroj stupnjeva svih vrhova grafa paran broj, pa graf ne može imati samo jedan vrh neparnog stupnja. Pretpostavimo sada da graf G ima točno dva vrha neparnog stupnja te nazovimo te vrhove u i v. Ako grafu G dodamo novi brid $e = uv$ tada novodobiveni graf $G + e$ ima sve vrhove parnog stupnja pa prema Teoremu 1.2.2 je taj graf Eulerov, odnosno sadrži Eulerovu turu T. Tada slijedi da je $T - e$ Eulerova staza grafa G. □

Iz prethodno dokazanog korolara, možemo iznijeti zaključak kada će graf G biti skoro Eulerov.

Korolar 1.2.8. *Povezani graf G je skoro Eulerov ako i samo ako ima točno dva vrha neparnog stupnja.*

Vodeći se prethodno iznesenim i dokazanim teoremima i korolarima, Eulerov postupak za rješavanje problema Königsberških mostova i sličnih tipova zadataka možemo sažeti:

(1) Ako graf sadrži više od dva vrha neparnog stupnja, tada nema Eulerovu stazu.

(2) Ako graf sadrži točno dva vrha neparnog stupnja, tada ima Eulerovu stazu, ali nema Eulerovu turu.

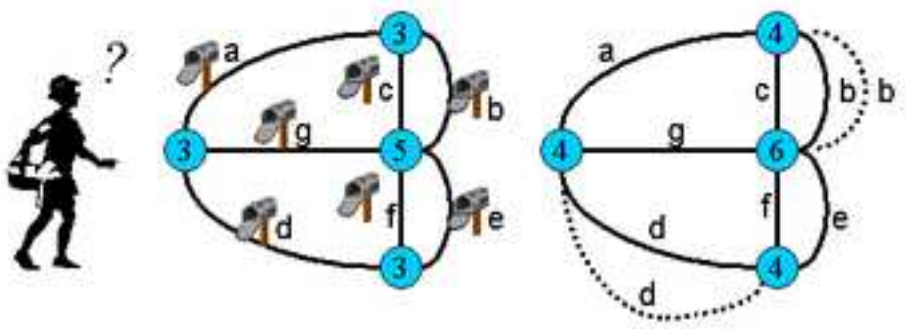
(3) Ako su svi vrhovi grafa parnog stupnja, tada ima Eulerovu turu.

1.3 Problem kineskog poštara

Jedna od najpoznatijih primjena Eulerovih grafova vezana je uz **problem kineskog poštara**. Problem je, sredinom 20. stoljeća, iznio kineski matematičar M. Guan proučavajući pitanje pitanje optimizacije puta pri dostavi poštanskih pošiljki te on glasi:
Poštar kreće iz poštanskog ureda, dijeli poštu i vraća se u ured. Cilj je svakom ulicom proći barem jedanput i pritom prijeći najkraći mogući put.

Definicija 1.3.1. *Uređeni par (G, ω), gdje je G graf, a ω funkcija koja svakom bridu e grafa G pridružuje nenegativan broj $\omega(e)$, $\omega(e) : E_G \to \mathbb{R}^+$ naziva se **težinski graf**. Vrijednost $\omega(e)$ naziva se **težina brida** e. Težina podgrafa težinskog grafa ukupna je težina njegovih bridova.*

U smislu teorije grafova, tražimo zatvorenu šetnju, **poštarovu turu**, koja uključuje svaki brid grafa barem jednom. **Optimalna poštarova tura** jest poštarova tura kojoj je ukupna težina uključenih bridova minimalna. Težinski grafovi svoju primjenu nalaze u kombinatornoj optimizaciji, kada bridu trebamo pridružiti neku brojčanu vrijednost koja može označavati udaljenost, kapacitet, visinu troška itd.



Slika 1.2: Problem kineskog poštara (preuzeto iz [8])

Problem možemo prikazati pomoću grafa. Svaki brid lijevog grafa na slici 1.2 predstavlja ulicu kojom poštar mora proći, dok nam vrhovi grafa predstavljaju mjesto gdje poštar može promijeniti smjer. Uočimo da lijevi graf na slici 1.2 nije Eulerov (nisu mu svi vrhovi parnog stupnja) pa ne možemo izbjeći višestruki prolazak nekim ulicama. Ponovni prolazak istom ulicom prikazujemo dodavajući bridove. Dodavanjem bridova postižemo da svaki vrh novog grafa bude parnog stupnja. Koristeći Teorem 1.2.2 možemo zaključiti da je desni graf na slici 1.2 Eulerov pa možemo pronaći Eulerovu turu, odnosno zatvorenu stazu takvu da svakim bridom danog grafa prođemo točno jednom. U ovom slučaju tražena poštarova tura je *a b c b e f g d d*.
Dakle, možemo zaključiti da ako je graf Eulerov tada je svaka Eulerova tura optimalna poštarova tura, jer kod Eulerovog grafa postoji zatvorena šetnja koja uključuje sve bridove grafa točno jedanput. Ako graf nije Eulerov, tada dodajemo paralelne bridove čime graf svodimo na Eulerov. Zadatak je pronaći optimalni skup bridova težinskog grafa čije umnožavanje daje Eulerov graf minimalne težine. Ukoliko je graf G Eulerov graf, tada problem kineskog poštara možemo riješiti pomoći Fleuryevog algoritma koji konstruira zatvorenu Eulerovu stazu tako da počne u nekom proizvoljnom vrhu i u svakom koraku odabire rezni brid neprijeđenog podgrafa samo ako nema druge alternative.
Protekom vremena, otkrivene su razne varijacije problema kineskog poštara te razvijeni algoritmi za rješavanje tih vrsta problema.

1.4 Eulerova formula

Euler je uspio povezati broj vrhova, bridova i strana ravninskog grafa pomoću formule koju danas poznajemo pod nazivmo *Eulerova formula*. Euler je tu formulu prvi puta spomenuo 1752. godine u svom pismu Goldbachu, a formula se odnosila na konveksne poliedre.
Kako bismo mogli opisati Eulerovu formulu, najprije moramo smjestiti grafove u ravninu.

Definicija 1.4.1. ***Crtež grafa*** $G = (V, E, \varphi)$ *u ravnini preslikavanje je* ϱ *definirano na skupu* $V \cup E$ *tako da vrijedi:*

1. *Vrhovima grafa pridružuju se međusobno različite točke ravnine.*
2. *Svakom bridu e pridruži se jednostavna krivulja* $\varrho(e)$ *u ravnini kojoj su krajevi elementi skupa* $\varphi(e)$ *te* $\varrho(e)$ *ne sadrži sliku ni jednog drugog vrha iz V.*

Presijecanje *bridova grafa zajednička je unutarnja točka krivulja* $\varrho(e_1)$ *i* $\varrho(e_2)$, $e_1, e_2 \in E$, *tj. točka iz* $\varrho(e_1) \cap \varrho(e_2)$ *koja nije slika nekog vrha grafa G.*

Definicija 1.4.2. *Crtež grafa u ravnini koji nema presijecanja bridova naziva se* ***smještenje grafa u ravninu*** *ili* ***ravninsko smještenje grafa***. ***Planarni graf*** *ili* ***graf smjestiv u ravninu*** *je graf koji ima ravninsko smještenje, odnosno koji se može nacrtati u ravnini bez presijecanja bridova. U protivnom kažemo da je graf* ***neplanaran***.

Definicija 1.4.3. *Ravninsko smještenje* $\varrho(G)$ *grafa G nazivamo* ***ravninski graf***, ***ravninski prikaz*** *ili* ***ravninski crtež planarnog grafa*** *G.*

Bilo koji ravninski graf dijeli skup točaka ravnine koje ne pripadaju bridovima toga grafa na disjunktne otvorene povezane podskupove odnosno **područja** u ravnini. Svako područje određeno je skupom bridova grafa koji čine njegov rub. Točno je jedno od tih područja neomeđeno.

Definicija 1.4.4. *Područja ravnine određena ravninskim smještenjem grafa nazivamo* ***stranama*** *tog grafa. Neomeđena strana grafa je* ***vanjska***, *a ostale su* ***unutarnje***. *Kažemo da je strana* ***incidentna*** *nekom vrhu, odnosno bridu ako oni pripadaju njezinom rubu. Dvije strane su* ***susjedne*** *ako su incidentne istom bridu. Strana incidentna reznom bridu je* ***sebi susjedna***.

Teorem 1.4.5. *Neka je G smještenje u ravnini povezanog planarnog grafa, a* $e(G)$, $v(G)$ *i* $f(G)$ *označavaju redom broj bridova, broj vrhova i broj strana grafa G. Tada vrijedi Eulerova formula.*

$$v(G) - e(G) + f(G) = 2.$$

Dokaz. Dokaz ćemo provesti indukcijom po $e(G)$.
Neka je $e(G) = 0$. Budući da je graf G povezan, tada slijedi da je $v(G) = 1$ i $f(G) = 1$ pa tvrdnja očito vrijedi.
Pretpostavimo sada da vrijedi $e(G) \geq 1$ i da tvrdnja vrijedi za sve grafove s manje od $e(G)$ bridova. Ako je G stablo, prema Teoremu 1.1.18 slijedi $e(G) = v(G) - 1$ i $f(G) = 1$ pa vrijedi $v(G) - e(G) + f(G) = v(G) - v(G) + 1 + 1 = 2$.
Pretpostavimo da G nije stablo te uzmimo da je e brid u nekom od ciklusa grafa. Tada je $G - e$ povezani planarni graf s $v(G)$ vrhova, $e(G) - 1$ bridova i $f(G) - 1$ strana. Po indukcijskoj pretpostavci $v(G) - e(G) + 1 + f(G) - 1 = 2$ što daje $v(G) - e(G) + f(G) = 2$. □

Poglavlje 2

Teorija brojeva

Teorija brojeva je grana matematike koja se bavi svojstvima cijelih brojeva. Njeni začeci sežu još u doba pitagorejaca. Uz Grke, teorijom brojeva bavili su se i arapski matematičari. Kroz europski srednji vijek jedine značajnije rezultate vezane uz teoriju brojeva objavili su Fibonacci i Stiefel. Za obnovu interesa za teorijom brojeva u 17. stoljeću posebno je zaslužan Pierre de Fermat. Fermatov doprinos teoriji brojeve se očituje o čitavom nizu tvrdnji, od kojih je mnoge dao bez dokaza. Točnost tvrdnji dokazivana je još desecima godina nakon Fermatove smrti, a u tome je veliku ulogu imao Leonhard Euler.
Smatra se da je Eulerov interes za tom granom matematike potaknuo Christian Goldbach, kojeg je Euler upoznao prilikom svog dolaska u Rusiju 1727. godine. Goldbach je koristeći se raznim izvorima pokušao naći odgovore na neka otvorena pitanja pa je tako 1729. godine u svom pismu Euleru postavio pitanje: "*Je li Vam poznato Fermatovo mišljenje da su brojevi oblika* $2^{2^p}+1$ *prosti? On to nije dokazao, a koliko znam nije niti itko drugi.*". Euler je uočio da vrijedi $2^{2^5}+1 = 6\,700\,417 \cdot 641$, odnosno dokazao je da Fermatova tvrdnja ne vrijedi. Danas brojeve oblika $F_n = 2^{2^n}+1$ nazivamo **Fermatovim brojevima**. Daljnjim proučavanjem Fermatovog rada, Eulerov interes za teorijom brojeva sve je više rastao.

2.1 Eulerova funkcija

U ovome poglavlju baviti ćemo se jednom od najvažnijih funkcija u teoriji brojeva, Eulerovom funkcijom. Euler je spomenutu funkciju opisao kao "*funkciju koja broji broj prirodnih brojeva, koji su manji od nekog prirodnog broja n, takvih da ti prirodni brojevi nemaju zajedničkih djelitelja s brojem n*" te ju je označavao oznakom π. Danas za Eulerovu funkciju koristimo oznaku φ koju je uveo Carl Friedrich Gauss 1801. godine.
Prema samom Eulerovom opisu funkcije, istu možemo definirati kao funkciju $\varphi : \mathbb{N} \to \mathbb{N}$, $\varphi(n) = \text{card}(U_n)$ gdje je U_n skup prirodnih brojeva, manjih ili jednakih n, relativno prostih s n, odnosno $U_n = \{k \in \mathbb{N} : 1 \leq k \leq n \ \wedge \ (n,k) = 1\}$. Primijetimo, da se ova funkcija raz-

likuje od Eulerove definicije funkcije u tome što u ovom slučaju vrijedi $\varphi(1) = 1$, dok po samoj Eulerovoj definiciji vrijedi $\varphi(1)=0$.
Kako bismo preciznije definirali Eulerovu funkciju, moramo se prvo upoznati sa pojmom reduciranog sustava ostataka.

Lema 2.1.1. *Neka su a i b cijeli brojevi različiti od nule. Tada postoje cijeli brojevi x i y takvi da je* $\text{nzd}(a, b) = ax + by$.

Dokaz. Tvrdnja se dokazuje pomoću Euklidovog algoritma, a dokaz se nalazi u [5]. □

Lema 2.1.2. *Neka su a, b, c, d cijeli brojevi. Ako je $a \equiv b \pmod{m}$ i $c \equiv d \pmod{m}$, onda je $a + c \equiv b + d \pmod{m}$ i $ac \equiv bd \pmod{m}$.*

Dokaz. Neka je $a-b = mk$ i $c-d = ml$. Tada je $(a+c)-(b+d) = m(k+l)$ pa je $a+c \equiv b+d \pmod{m}$.
Zbog $ac - bd = a(c - d) + d(a - b) = m(al + dk)$ slijedi da je $ac \equiv bd \pmod{m}$. □

Korolar 2.1.3. *Ako su m, n relativno prosti brojevi, tada vrijedi $n \equiv 1 \pmod{m}$.*

Definicija 2.1.4. ***Reducirani sustav ostataka modulo m*** *je skup cijelih brojeva r_i sa svojstvom da je* $\text{nzd}(r_i, m) = 1, r_i \not\equiv r_j \pmod{m}$ *za $i \neq j$ te da za svaki cijeli broj x takav da je* $\text{nzd}(x, m) = 1$ *postoji r_i takav da je $x \equiv r_i \pmod{m}$*

Iz same definicije jasno slijedi da svi reducirani sustavi ostataka modulo m imaju isti broj elemenata.

Teorem 2.1.5. *Ako je $\{r_1, r_2, \ldots, r_{\varphi(m)}\}$ reducirani sustav ostataka modulo m te ako je* $\text{nzd}(a, m) = 1$, *tada je $\{ar_1, ar_2, \ldots, ar_{\varphi(m)}\}$ također reducirani sustav ostataka modulo m.*

Dokaz. Zbog $\text{nzd}(a, m) = 1$ slijedi $ar_i \equiv 1r_i \equiv r_i \pmod{m}$. Neka je p prost broj te neka $p \mid m$ i $p \mid ar_i$. Tada $p \mid a$ ili $p \mid r_i$ što je u kontradikciji s time da je $\{r_1, r_2, \ldots, r_{\varphi(m)}\}$ reducirani sustav ostataka modulo m i da je $\text{nzd}(a, m) = 1$. □

Definicija 2.1.6. *Funkciju $\varphi : \mathbb{N} \to \mathbb{N}$ definiranu s $\varphi(n) = \text{card}\,\{k \in \mathbb{N} : 1 \leq k \leq n \wedge (n, k) = 1\}$ nazivamo* ***Eulerovom funkcijom***.

Svojstva Eulerove funkcije

Definicija 2.1.7. *Funkciju $f : \mathbb{N} \to \mathbb{C}$ za koju vrijedi*

(1) $f(1) = 1$,

(2) $f(mn) = f(m)f(n)$ *za sve m, n takve da je* $\text{nzd}(m, n) = 1$,

nazivamo multiplikativna funkcija.

Teorem 2.1.8. *Eulerova funkcija φ je multiplikativna.*

Dokaz. Iz same Definicije 2.1.6 slijedi da vrijedi $\varphi(1) = 1$.
Prikažimo sada brojeve $1, 2, \ldots, mn$ pomoću tablice s n redaka i m stupaca.

$$\begin{array}{ccccc} 1 & 2 & 3 & \cdots & m \\ m+1 & m+2 & m+3 & \cdots & 2m \\ 2m+1 & 2m+2 & 2m+3 & \cdots & 3m \\ \vdots & \vdots & \vdots & & \vdots \\ (n-1)m+1 & (n-1)m+2 & (n-1)m+3 & \cdots & nm \end{array}$$

U nizu brojeva $1, 2, \ldots, mn$, po definiciji Eulerove funkcije, postoji $\varphi(mn)$ brojeva koji su relativno prosti s brojem mn. Uočimo da su svi brojevi u pojedinom stupcu kongruentni s modulo m pa svih m stupaca odgovaraju m klasa ekvivalencije modulo m. Slijedi da su svi brojevi u istom stupcu ili relativno prosti s m ili nijedan nije relativno prost s m. Možemo zaključiti da se točno $\varphi(m)$ stupaca sastoji od brojeva koji su relativno prosti s m, dok ostali stupci se sastoje od brojeva koji nisu relativno prosti s m.
Promotrimo sada jedan od tih $\varphi(m)$ stupaca te ga označimo s k. Skup svih elemenata koje sadrži taj stupac označimo s $S_k = \{k, m+k, 2m+k, \ldots, (n-1)m+k\}$. Sada želimo dokazati da su svi elementi skupa S_k međusobno nekongruentni modulo n. Ako bi postojali $i, j \in \{0, 1, \ldots, n-1\}$ takvi da vrijedi

$$im + k \equiv jm + k \pmod{n}$$

tada oduzimanjem broja k i činjenice da su m i n relativno prosti slijedi da je $i \equiv j \pmod{n}$ pa slijedi da je $i = j$.
Kako S_k ima n međusobno nekongruentnih elemenata modulo n zaključujemo da u S_k imamo predstavnike svih mogućih klasa modulo n, odnosno S_k je potpun sustav ostataka modulo n. Označimo s R_k skup koji sadrži sve elemente skupa S_k koji su relativno prosti s n. Tada je R_k reducirani sustav ostataka modulo n i ima $\varphi(n)$ elemenata.
Sada možemo zaključiti da svaki od $\varphi(m)$ stupaca sadrži $\varphi(n)$ brojeva koji su relativno prosti s m i n. Slijedi da su ti brojevi relativno prosti s mn pa vrijedi $\varphi(mn) = \varphi(m)\varphi(n)$. □

Propozicija 2.1.9. *Neka je p prost broj i $\alpha \in \mathbb{N}$, tada vrijedi:*

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

Dokaz. Jedini brojevi koji nisu relativno prosti s p^α su višekratnici broja p, a to su $1 \cdot p, 2 \cdot p, 3 \cdot p, \ldots, p^{\alpha-1} \cdot p = p^\alpha$, dakle ima ih $p^{\alpha-1}$. Slijedi:

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

□

Koristeći Osnovni teorem aritmetike, znamo da se svaki prirodan n broj veći od 1 može zapisati kao umnožak prostih faktora, odnosno vrijedi $n = {p_1}^{\alpha_1} {p_2}^{\alpha_2} \cdots {p_k}^{\alpha_k}$ gdje su $\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{N}$, a $p_1, p_2, \ldots, p_k$ prosti brojevi primjenom Teorema 2.1.8 i Propozicije 2.1.9 slijedi:

$$\varphi(n) = \prod_{i=1}^{k} {p_i}^{\alpha-1}(p_i - 1) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right) \tag{2.1}$$

Propozicija 2.1.10. *Neka je n prirodan broj, ako $d \mid n$, onda $\varphi(d) \mid \varphi(n)$.*

Dokaz. Neka je $n = {p_1}^{\alpha_1} {p_2}^{\alpha_2} \cdots {p_k}^{\alpha_k}$, tada zbog $d \mid n$ vrijedi $d = {p_1}^{\beta_1} {p_2}^{\beta_2} \cdots {p_k}^{\beta_k}$ gdje je $0 \leq \beta_i \leq \alpha_i, i = 1, \ldots, k$. Slijedi:

$$\frac{\varphi(n)}{\varphi(d)} = {p_1}^{\alpha_1-\beta_1} {p_2}^{\alpha_2-\beta_2} \cdots {p_k}^{\alpha_k-\beta_k} = \prod_{i=1}^{k} p_i^{\alpha_i-\beta_i}.$$

Zbog $0 \leq \beta_i \leq \alpha_i$ slijedi $\alpha_i - \beta_i \geq 0$ pa je broj s desne strane dobivene jednakosti prirodan. Time je tvrdnja dokazana. □

Teorem 2.1.11. *Za svaki prirodan broj n vrijedi:*

$$\sum_{d \mid n} \varphi(d) = n$$

gdje suma prolazi skupom svih pozitivnih djelitelja od n.

Dokaz. Neka je $n = {p_1}^{\alpha_1} {p_2}^{\alpha_2} \cdots {p_k}^{\alpha_k}$ gdje su $\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{N}$, a $p_1, p_2, \ldots, p_k$ prosti brojevi. Uočimo da svaki djelitelj d broja n možemo prikazati kao $d = {p_1}^{\beta_1} \cdot {p_2}^{\beta_2} \cdots {p_k}^{\beta_k}$ gdje $0 \leq \beta_i \leq \alpha_i$, $i = 1, \ldots, k$. Tada primjenom Teorema 2.1.8 slijedi:

$$\sum_{d \mid n} \varphi(d) = \prod_{i=1}^{k} \left(1 + \varphi(p_i) + \varphi({p_i}^2) + \cdots \varphi({p_i}^{\alpha_i})\right). \tag{2.2}$$

Tada, koristeći da su $p_1, p_2, \ldots, p_k$ prosti brojevi, koristeći Propoziciju 2.1.9 slijedi:

$$\sum_{d \mid n} \varphi(d) = \prod_{i=1}^{k} (1 + (p_i - 1) + ({p_i}^2 - p_i) + \cdots + ({p_i}^{\alpha_i} - {p_i}^{\alpha_i - 1})) = \prod_{i=1}^{k} {p_i}^{\alpha_i} = n.$$

□

Propozicija 2.1.12. *Za svaki prirodan broj m postoji konačno mnogo prirodnih brojeva n takvih da vrijedi $\varphi(n) = m$.*

Dokaz. Neka je $m = {p_1}^{\alpha_1} {p_2}^{\alpha_2} \cdots {p_k}^{\alpha_k}$ gdje su $\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{N}$, a $p_1, p_2, \ldots, p_k$ prosti brojevi. Ako neka potencija prostog broja p dijeli n, odnosno $p^\alpha \mid n$, tada prema Propoziciji 2.1.10 slijedi $\varphi(p^\alpha) \mid \varphi(n)$, odnosno vrijedi $p^{\alpha-1}(p-1) \mid \varphi(n) = m$. Onda je

$$p^\alpha \leq \frac{mp}{p-1} \leq 2m$$

Kako postoji samo konačno mnogo brojeva p^α takvih da vrijedi $p^\alpha \leq 2m$, slijedi da postoji i konačno mnogo produkata takvih potencija prostih brojeva. Stoga postoji i konačno mnogo prirodnih brojeva s danim svojstvom. □

Ocjene Eulerove funkcije

Propozicija 2.1.13. *Za svaki n složen prirodan broj vrijedi:*

$$\varphi(n) \leq n - \sqrt{n}.$$

Dokaz. Budući da je n složen prirodan broj, slijedi da n sadrži prosti faktor p_j takav da vrijedi $p_j \leq \sqrt{n}$. Sada prema 2.1 imamo:

$$\varphi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right) \leq n \left(1 - \frac{1}{p_j}\right) \leq n \left(1 - \frac{1}{\sqrt{n}}\right) = n - \sqrt{n}$$

□

Propozicija 2.1.14. *Za sve prirodne brojeve $n \neq 2, 6$ vrijedi*

$$\varphi(n) \geq \sqrt{n}.$$

Dokaz. Neka je $n = p^m$, gdje je p prost broj i $m \geq 2$, tada vrijedi $\frac{m}{2} \leq m - 1$. Slijedi:

$$\varphi(n) = p^{m-1}(p-1) \geq p^{m-1} \geq p^{\frac{m}{2}} = \sqrt{p^m} = \sqrt{n}. \tag{2.3}$$

Ako je $p \neq 2$ dodatno vrijedi:

$$\varphi(n) = p^{m-1}(p-1) \geq p^{m-1} \cdot 2 \geq p^{m-1}\sqrt{2} \geq \sqrt{2p^m} = \sqrt{2n}. \tag{2.4}$$

Neka je $m = 1$, tada je $n = p$. Promotrimo kvadratnu funkciju $f(x) = x^2 - x - 1$. Uočimo da je funkcija $f(x)$ pozitivna za $x > \frac{1+\sqrt{5}}{2}$. Uvedimo supstituciju $x = \sqrt{t}$ pa slijedi da je $t > \left(\frac{1+\sqrt{5}}{2}\right)^2$, odnosno vrijedi $\sqrt{t} < t - 1$. Stoga za $p \geq 3$ vrijedi $\sqrt{p} < p - 1$, pa slijedi:

$$\varphi(n) = p - 1 > \sqrt{p} = \sqrt{n}. \tag{2.5}$$

Analogno, za $p \geq 5$ slijedi:

$$\varphi(n) = p - 1 \geq \sqrt{2p} = \sqrt{2n}. \tag{2.6}$$

Ako je n neparan ili $4 \mid n$, iz 2.3 i 2.5 slijedi:

$$\varphi(n) = \varphi({p_1}^{\alpha_1}) \cdots \varphi({p_k}^{\alpha_k}) \geq \sqrt{{p_1}^{\alpha_1}} \cdots \sqrt{{p_k}^{\alpha_k}} = \sqrt{n}.$$

Ako je $n = 2k$, gdje je k neparan broj, tada za $n \neq 6$ slijedi da 9 dijeli k ili k ima barem jedan prost faktor $p \geq 5$. Iz 2.3, 2.4, 2.5 slijedi:

$$\varphi(n) = \varphi(k) \geq \sqrt{2k} = \sqrt{n}.$$

□

2.2 Eulerov teorem

Jednim od najvažnijih teorema u teoriji brojeva smatra se Eulerov teorem čiji je sastavni dio Eulerova funkcija.

Teorem 2.2.1. *Ako je* $\text{nzd}(a, m) = 1$*, tada vrijedi* $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Dokaz. Neka je $\{r_1, r_2, \ldots, r_{\varphi(m)}\}$ reducirani sustav ostataka modulo m, tada po teoremu 2.1.5 vrijedi da je i $\{ar_1, ar_2, \ldots, ar_{\varphi(m)}\}$ reducirani sustav ostataka modulo m. Prema tome slijedi:

$$\prod_{j=1}^{\varphi(m)} ar_j \equiv \prod_{i=1}^{\varphi(m)} r_i \pmod{m},$$

odnosno

$$a^{\varphi(m)} \prod_{j=1}^{\varphi(m)} r_j \equiv \prod_{i=1}^{\varphi(m)} r_i \pmod{m}$$

Budući da je $\text{nzd}(r_i, m) = 1$, $i = 1, \ldots, m$ imamo $r_i \equiv 1 \pmod{m}$ pa je $\prod_{i=1}^{\varphi(m)} r_i \equiv 1 \pmod{m}$ iz čega slijedi:

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

□

Kao što smo već spomenuli, Fermat je svojim radom iznio čitav niz tvrdnji. Tako je u jednom pismu 1640. godine iznio tvrdnju: "*ako je p prost broj i a prirodan broj koji nije djeljiv s p, onda je* $a^{p-1} - 1$ *djeljiv s p.* Navedena tvrdnja danas je poznata kao **Mali Fermatov teorem**.

Teorem 2.2.2. *(***Mali Fermatov teorem u Eulerovoj formulaciji***) Ako p označava neparan prost broj, onda je broj* $a^{p-1} - 1$ *uvijek djeljiv s p, osim ako je sam a djeljiv s p.*

Prethodan teorem još možemo iskazati i kao: "*Neka je p prost broj. Ako* $p \nmid a$*, onda je* $a^{p-1} \equiv 1 (\text{mod } p)$."

Dokaz. Neka je p prost broj i $p \nmid a$, tada očito vrijedi $\text{nzd}(a, p) = 1$. Tada prema Teoremu 2.2.1 vrijedi $a^{\varphi(p)} \equiv 1 (\text{mod } p)$. Zbog $\varphi(p) = p - 1$ slijedi:

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

□

Euler je dokazom Malog Fermatovog teorema zapravo dokazao jedan smjer kineske hipoteze stare 2000 godina koja nam govori da je broj p prost ako i samo ako je broj $2^p - 2$ djeljiv s p. Tek je 1819. godine dokazano da drugi smjer ne vrijedi, odnosno pronađen je kontraprimjer: $2^{341} \equiv 2 \pmod{341}$.

2.3 Kvadratni zakon reciprociteta

Kvadratni zakon reciprociteta jedan je od najvažnijih rezultata teorije brojeva. Do prvih zaključaka, vezanih uz njega, stigli su Euler i Lagrange, no prvi je teorem kvadratnog zakon reciprociteta iskazao Gauss. Zanimljivo je da je Gauss dao čak osam različitih dokaza vezanih za taj teorem, dok je danas poznato više od 240 različitih dokaza.
Kako bismo mogli razumjeti sam kvadratni zakon reciprociteta, upoznajmo se najprije s pojmovima koji su nam potrebni za samu njegovu izgradnju.

Definicija 2.3.1. *Neka je* $\text{nzd}(a, m) = 1$ *te neka kongruencija* $x^2 \equiv a \pmod{m}$ *ima rješenje. Tada kažemo da je a* ***kvadratni ostatak modulo*** *m. Ako kongruencija nema rješenje, tada je a* ***kvadratni neostatak modulo*** *m.*

Primijetimo da kongruencija $x^2 \equiv 0 (\text{mod } m)$ uvijek ima rješenja, no 0 nije ni kvadratni ostatak ni kvadratni neostatak modulo m jer nije ispunjen uvjet $\text{nzd}(a, m) = 1$.

Definicija 2.3.2. *Neka je p neparni prosti broj.* ***Legendreov simbol*** $\left(\frac{a}{b}\right)$ *jednak je* 1 *ako je a kvadratni ostatak modulo p,* -1 *ako je a kvadratni neostatak modulo p i 0 ako vrijedi* $p \mid a$.

Euler je korištenjem Malog Fermatovog teorema odredio formulu za određivanje Legendreova simbola. Danas tu relaciju poznajemo kao *Eulerov kriterij*. U dokazu Eulerovog kriterija koristiti ćemo slijedeće teoreme.

Teorem 2.3.3. (Lagrangeov teorem) *Ako je p prost broj i $P(x)$ polinom stupnja n s cjelobrojnim koeficijentima, koji nisu svi djeljivi s p, tada kongruencija $P(x) \equiv 0 \pmod{p}$ ima najviše n rješenja modulo p.*

Dokaz. Dokaz teorema nalazi se u [13]. □

Teorem 2.3.4. (Eulerov kriterij) *Ako je a cijeli broj i p neparan prost broj, tada vrijedi:*

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

Dokaz. Očito je da $a^{\frac{p-1}{2}} \equiv 0 (\text{mod } p)$ ako i samo ako $p \mid a$, odnosno ako i samo ako vrijedi $\left(\frac{a}{p}\right) = 0$.
Neka je sada a kvadratni ostatak modulo p. Tada postoji $x_0 \in \mathbb{Z}$ takav da vrijedi ${x_0}^2 \equiv a \pmod{p}$. Budući da su a i p relativno prosti, tada su i a i x_0 i p relativno prosti pa prema Teoremu 2.2.2 slijedi:

$$a^{\frac{p-1}{2}} \equiv {x_0}^{p-1} \equiv 1 \equiv \left(\frac{a}{p}\right) (\text{mod } p).$$

Preostaje nam još provjeriti slučaj kada je a kvadratni neostatak modulo p. Uočimo da vrijedi $\left(a^{\frac{p-1}{2}}\right)^2 \equiv a^{p-1} \equiv 1 (\text{mod } p)$. Kako kongruencija $x^2 \equiv 1 \pmod{p}$ prema Teoremu 2.3.3 ima točno dva rješenja, tada vrijedi $x \equiv \pm 1 \pmod{p}$. Dakle, dovoljno je pokazati da $a^{\frac{p-1}{2}} \not\equiv 1 \pmod{p}$ kada je a kvadratni neostatak modulo p, odnosno iz toga slijedi da je $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.
Prema istome teoremu slijedi da kongruencija $a^{\frac{p-1}{2}} \equiv 1 (\text{mod } p)$ ima najviše $\frac{p-1}{2}$ rješenja. U rješenjima se nalaze $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$ jer se, prema već dokazanome u slučaju kada je a kvadratni ostatak modulo p, u rješenjima nalaze svi kvadratni ostaci modulo p. Sada želimo dokazati da su sva ova rješenja nekongruentna modulo p.
Neka su dani x i y takvi da vrijedi $x \neq y$ i $x^2 \equiv y^2 \pmod{p}$. Tada zbog $x^2 - y^2 \equiv 0 \pmod{p}$ slijedi $p \mid x^2 - y^2$, odnosno $p \mid x - y$ ili $p \mid x + y$. Zbog $1 < x + y < p$ slijedi $x = y$, odnosno sva rješenja kongruencije $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ su dana navedenim nizom koji uključuje samo kvadratne ostatke modulo p.
Dakle, ako je a kvadratni neostatak modulo p, odnosno $\left(\frac{a}{p}\right) = -1$, onda vrijedi $a^{\frac{p-1}{2}} \equiv -1 (\text{mod } p)$. □

Propozicija 2.3.5. *Za svaka dva cijela broja a i b te neparan prost broj p vrijedi:*

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

Dokaz. Koristeći Eulerov kriterij slijedi:

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

□

Iako koristeći Eulerov kriterij možemo izračunati neke Legendreove simbole, taj postupak nam nije efikasan za velike brojeve. Npr. želimo odrediti $\left(\frac{103}{227}\right)$. Uočimo da su i 103 i 227 prosti brojevi te si račun ne možemo olakšati koristeći Propoziciju 2.3.5. Račun je olakšao Gauss svojim iskazom i dokazom kvadratnog reciprociteta. Za iskaz i dokaz kvadratnog zakona reciprociteta, potreban nam je sljedeći teorem:

Teorem 2.3.6. *Ako je p neparan prost broj i* $\text{nzd}(a, 2p) = 1$*, onda je* $\left(\frac{a}{p}\right) = (-1)^t$*, gdje je*

$$t = \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{ja}{p} \right\rfloor$$

Dokaz. Dokaz teorema nalazi se u [5] □

Teorem 2.3.7. ***(Gaussov kvadratni zakon reciprociteta)*** *Ako su p i q različiti neparni prosti brojevi, onda vrijedi:*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} = \begin{cases} 1, \text{ako je } p \equiv 1 \pmod 4 \text{ ili } q \equiv 1 \pmod 4 \\ -1, \text{ako je } p \equiv q \equiv 3 \pmod 4 \end{cases}$$

Drugim riječima, ako su p i q oblika $4k+3$ onda jedna od kongruencija $x^2 \equiv p \pmod q$, $x^2 \equiv q \pmod p$ ima rješenja, a druga nema. Ako barem jedan od brojeva p i q ima oblik $4k+1$, onda ili obje ove kongruencije imaju rješenje, ili nijedna nema rješenje.

Dokaz. Definirajmo skup S kao $S = \left\{(x, y) : x, y \in \mathbb{Z}, 1 \le x \le \frac{p-1}{2}, 1 \le y \le \frac{q-1}{2}\right\}$. Uočimo da tada skup S ima $\frac{p-1}{2} \cdot \frac{q-1}{2}$ članova. Podijelimo sada taj skup na dva disjunktna podskupa S_1 i S_2, ovisno o tome je li $qx > py$ ili $qx < py$. Iz $\frac{qx}{p} \le \frac{q(p-1)}{2p} \le \frac{q}{2}$ slijedi da je $\left\lfloor \frac{qx}{p} \right\rfloor \le \frac{q-1}{2}$. Analogno dobivamo i $\left\lfloor \frac{py}{q} \right\rfloor \le \frac{p-1}{2}$.
Sada skup S_1 možemo definirati kao skup svih parova (x, y) takvih da je $1 \le x \le \frac{p-1}{2}$ i $1 \le y \le \left\lfloor \frac{qx}{p} \right\rfloor$. Uočimo da takvih parova ima $\sum_{x=1}^{\frac{p-1}{2}} \left\lfloor \frac{qx}{p} \right\rfloor$. Analogno, skup S_2 možemo definirati kao skup svih parova (x, y) takvih da je $1 \le x \le \frac{q-1}{2}$ i $1 \le y \le \left\lfloor \frac{py}{q} \right\rfloor$. Uočimo da

takvih parova ima $\sum_{y=1}^{\frac{q-1}{2}} \left\lfloor \frac{py}{q} \right\rfloor$.
Budući da su skupovi disjunktni vrijedi:

$$\sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{jq}{p} \right\rfloor + \sum_{j=1}^{\frac{q-1}{2}} \left\lfloor \frac{jp}{q} \right\rfloor = \frac{p-1}{2} \cdot \frac{q-1}{2}.$$

Tada prema Teoremu 2.3.6 slijedi:

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

□

2.4 Ostali Eulerovi doprinosi u teoriji brojeva

Savršeni brojevi

Potraga za savršenim brojevima smatra se jednim od najstarijih problema u teoriji brojeva. Kako bismo mogli razumjeti Eulerov doprinos savršenim brojevima, upoznajmo se najprije s pojmovima vezanim uz savršene brojeve.

Definicija 2.4.1. *Neka je n prirodni broj. Kažemo da je n* ***savršen broj*** *je jednak zbroju svih svojih pravih djelitelja.*

Definicija 2.4.2. *Za prirodni broj n definiramo funkciju*

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

kao zbroj svih pozitivnih djelitelja broja n.

Teorem 2.4.3. *Neka su m i n relativno prosti brojevi, tada su sljedeće tvrdnje ekvivalentne:*

(1) *Funkcija $\sigma(n)$ je multiplikativna.*

(2) *Ako je $n = p$ prost broj, tada je $\sigma(p)=p+1$. U općem slučaju vrijedi: $\sigma(p^\alpha) = \frac{p^{\alpha+1}-1}{p-1}$*

(3) *Ako je $n = p^{\alpha_1}p^{\alpha_2}\cdots p^{\alpha_k}$ rastav broja na proste faktora, onda je:*

$$\sigma(n) = \prod_{i=1}^{k} \frac{{p_i}^{\alpha+1} - 1}{p_i - 1}$$

Dokaz. Dokaz se nalazi u [10]. □

Iz prethodne definicije očigledno slijedi da je prirodan broj n savršen ako vrijedi $\sigma(n) = 2n$ ili $n = \sigma(n) - n$.
Pojam savršenog broja je definirao sam Euklid u sedmoj knjizi *Euklidovih elemenata*, a u devetoj knjizi je dao i metodu pomoću koje možemo odrediti savršene brojeve:
"*Neka je dan geometrijski red* $1+2+4+8+16+\ldots$. *Promotrimo niz parcijalnih suma tog geometrijskog reda* $1, 3, 7, 15, 31, \ldots$ *i uočimo članove tog niza koji su prosti brojevi. Ako pomnožimo posljednji pribrojnik te parcijalne sume sa samom parcijalnom sumom, dobiti ćemo savršen broj.*"
Npr. $S_1 = 1 + 2 = 3$ je prost broj. Ako pomnožimo S_1 sa njegovim zadnjim pribrojnikom, dobijemo rezultat $3 \cdot 2 = 6$. Djelitelji broja 6 su $1, 2, 3, 6$ pa vrijedi $\sigma(6) = 1 + 2 + 3 + 6 = 12 = 2 \cdot 6$, odnosno 6 je savršen broj. Analogno slijedi da su savršeni brojevi i 28 i 496.
Euklid je uočio da vrijedi $6 = 2 \cdot (2^2 - 1)$, $28 = 2^2 \cdot (2^3 - 1)$ i $496 = 2^4 \cdot (2^5 - 1)$ pa je na temelju toga iznio teorem:

Teorem 2.4.4. *Ako je broj* $2^n - 1$ *prost, onda je broj* $N = 2^{n-1}(2^n - 1)$ *savršen broj.*

Kako bismo dokazali navedeni teorem potrebna nam je slijedeća lema:

Lema 2.4.5. *Neka je k prirodan broj. Tada su brojevi* $2^k - 1$ *i* 2^{k-1} *relativno prosti brojevi.*

Dokaz. Dokaz se nalazi u [10]. □

Dokaz. Budući da je $2^n - 1$ prost, očito vrijedi $\sigma(2^n - 1) = 1 + (2^n - 1) = 2^n$. Prema Teoremu 2.4.3 i Teoremu 2.4.5 vrijedi:

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

□

Teorem 2.4.6. *Ako je broj p prirodan broj i* $2^p - 1$ *prost broj, onda je i p prost broj.*

Dokaz. Dokažimo ekvivalentnu tvrdnju, tj. da je $2^p - 1$ složen broj ako je p složen broj. Neka je $p = rs$, $r > 1$, $s > 1$. Slijedi:

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

pa je broj $2^p - 1$ složen. □

Dvije tisuće godina nakon Euklidovog otkrića o savršenim brojevima, Euler je dokazao da su svi savršeni brojevi oblika $2^{n-1}(2^n - 1)$ gdje je $2^n - 1$ prost broj.

Teorem 2.4.7. *Ako je N paran savršen broj, tada je N oblika* $2^{n-1}(2^n - 1)$ *gdje je* $2^n - 1$ *prost broj.*

Dokaz. Pretpostavimo da je broj n savršen broj oblika $n = 2^k \cdot m$, gdje su k i m prirodni brojevi, uz dodatan uvjet da je m neparan. Budući da su brojevi 2^k i m neparni, te da je funkcija σ multiplikativna slijedi:

$$\sigma(n) = \sigma(2^k) \cdot \sigma(m) = (2^{k+1} - 1) \cdot \sigma(m) \tag{2.7}$$

Budući da je n savršen slijedi:

$$\sigma(n) = 2n = 2 \cdot 2^k \cdot m = 2^{k+1} \cdot m \tag{2.8}$$

Sada iz (2.7) i (2.8) slijedi:

$$(2^{k+1} - 1) \cdot \sigma(m) = 2^{k+1} \cdot m$$

pa vrijedi:

$$\sigma(m) = 2^{k+1} \cdot l \tag{2.9}$$

i

$$m = (2^{k+1} - 1) \cdot l \tag{2.10}$$

za neki neparan broj l. Pretpostavimo da je $l > 1$, pa iz (2.10) slijedi da m ima barem 4 djelitelja i to su $1, mil$ pa sigurno vrijedi $\sigma(m) \geq 1 + m + l$.
Sada slijedi: $\sigma(m) \geq 1 + m + l = 1 + (2^{k+1} - 1) \cdot l + l = 1 + 2^{k+1} \cdot l \geq 2^{k+1} \cdot l = \sigma(m)$ što je kontradikcija pa vrijedi $l = 1$.
Sada iz (2.9) i (2.10) slijedi $\sigma(m) = m + 1$, odnosno možemo zaključiti da je $m = 2^{k+1} - 1$ prost broj. Koristeći Teorem 2.4.7 slijedi da je $k + 1 = p$ također prost pa vrijedi:

$$n = 2^k \cdot m = 2^{p-1} \cdot (2^{k+1} - 1) = 2^{p-1} \cdot (2^p - 1)$$

□

Do danas je poznato 47 savršenih brojeva.

Prijateljski brojevi

Osim potrage za savršenim brojevima, kao jedan od najstarijih i najpoznatijih problema teorije brojeva smatra se i potraga za prijateljskim brojevima. Prijateljski brojevi spominju se još u neohelenističkom razdoblju kod pitagorejaca te su oni poznavali prvi par prijateljskih brojeva$(220, 284)$. Prvi teorem vezan uz njih nalazimo u devetom stoljeću kojeg je iznio i dokazao arapski matematičar Thābit ibn Kurra.

Definicija 2.4.8. *Uređeni par brojeva (m, n) gdje su m i n prirodni brojevi takvi da $m < n$ nazivamo **prijateljski brojevima** ako vrijedi $\sigma(m) = m + n = \sigma(n)$, odnosno $\sigma(n) - n = m$ i $\sigma(m) - m = n$.*

Teorem 2.4.9. (Thābitovo pravilo) *Par brojeva $2^n pq$ i $2^n r$ je prijateljski ako su brojevi $p = 3 \cdot 2^{n-1} - 1$, $q = 3 \cdot 2^n - 1$ i $r = 9 \cdot 2^{2n-1} - 1$ neparni i prosti te $n > 1$.*

Ovo pravilo daje tri para prijateljskih brojeva i to za $n = 2, 4, 7$. Za $n = 2$ dobije se već navedeni uređeni par brojeva $(220, 284)$. Smatra se da je drugi par prijateljskih brojeva pronašao sam Thābit, odnosno za $n = 4$ dobijemo uređeni par brojeva $(17296, 18416)$ kojeg je u 17. stoljeću ponovno otkrio de Fermat. Za $n = 7$ dobijemo prijateljske brojeve 9363584 i 9437056 koje je otkrio Descartes.
Thābitovo pravilo je generalizirao Leonhard Euler na pravilo koje pronalazi sve uređene parove prijateljskih brojeva oblika $(2^n pq, 2^n r)$.

Teorem 2.4.10. (Eulerovo pravilo) *Brojevi $2^n pq$ i $2^n r$ su prijateljski brojevi ako su brojevi $p = 2^{n-l} f - 1$, $q = 2^n f - 1$ i $r = 2^{2n-l} f^2 - 1$ prosti,gdje vrijedi $f = 2^l + 1$ i $k > l \geq 1$.*

Dokaz. Prema definiciji prijateljskih brojeva, n, p, q i r moraju zadovoljavati slijedeće jednadžbe: $(p + 1)(q + 1) = (r + 1)$ i $(2^{k+1} - 1)(p + 1)(q + 1) = 2^k(pq + r)$.
Iz toga slijedi da je $r = pq + p + q$ i

$$\left[p - (2^k - 1)\right]\left[q - (2^k - 1)\right] = 2^{2k}. \tag{2.11}$$

Zapišimo desnu stranu prethodne jednadžbe kao AB, gdje je $A = 2^{k-l}$ i $B = 2^{k+l}$ za neki cijeli broj $l \in [1, k - 1]$. Tada sva rješenja jednadžbe (2.11) možemo zapisati kao:

$$p = 2^k - 1 + 2^{k-l}, q = 2^k - 1 + 2^{k+l}.$$

Ako su brojevi $p = 2^{n-l}(2^l + 1) - 1$, $q = 2^n(2^l + 1) - 1$ i $r = pq + p + q = 2^{2k-l}(2^l + 1)^2 - 1$ svi prosti, tada su $2^n pq$ i $2^n r$ prijateljski brojevi. □

Do Eulerovog otkrića bila su poznata samo tri para prijateljskih brojeva. Euler je za svog života otkrio 58 novih parova prijateljskih brojeva, a danas poznajemo više od 7500 parova prijateljskih brojeva.

Poglavlje 3

Matematička analiza

Glavnim područjem djelovanja matematičara 18. stoljeća smatra se matematička analiza. Velik doprinos razvitku matematičke analize dala je obitelj Bernoulli. Eulerova bliskost s obitelji Bernoulli potaknula je Eulerovo zanimanje za navedenom matematičkom disciplinom. Matematička analiza je dugo vremena bila centar Eulerova zanimanja pa je tako 1747. godine napisao svoju poznatu knjigu *Uvod u analizu beskonačnosti*. Prvi dio ovog djela bavi se beskonačnim procesima, gdje su prikazane funkcije u obliku beskonačnih redova, limesi nekih beskonačnih umnožaka, razni algebarski i trigonometrijski redovi itd.

3.1 Eulerova zeta funkcija

Pietro Mengoli, talijanski matematičar, je 1650. godine u svojoj knjizi o sumi redova *Nove aritmetičke kvadrature* predstavio poznati problem pronalaska zatvorenog oblika beskonačnog reda, danas poznatog pod nazivom baselski problem. O samoj zahtjevnosti problema svjedoči činjenica da problem nisu uspjeli riješiti poznati matematičari poput Jacoba Bernoullija, Johanna Bernoullija, Daniela Bernoullija, Leibniza, de Moivrea itd. Problem je riješio Leonhard Euler 1735. godine, odnosno pokazao je da vrijedi:

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}, n \in \mathbb{N}.$$

Dokaz. Euler je, koristeći činjenicu da se svaka algebarska jednadžba n tog stupnja može zapisati u obliku:

$$a(x - x_1)(x - x_2) \cdots (x - x_n) = 0, a \in \mathbb{R}$$

gdje su $(x_1, \ldots, x_n)$ rješenja algebarske jednadžbe te činjenicu da se funkcija sinus može prikazati u obliku beskonačnog reda:

$$\sin x = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \cdots, \tag{3.1}$$

prikazao funkciju sinus kao beskonačan polinom. Budući da jednadžba $\sin x = 0$ ima beskonačno mnogo rješenja oblika $(0, \pm\pi, \pm 2\pi, \dots)$, Euler je funkciju sinus zapisao kao:

$$\begin{aligned} \sin x &= a(x-0)(x-\pi)(x+\pi)(x-2\pi)(x+2\pi)\cdots \\ &= ax(x-\pi^2)(x-4\pi^2)(x-9\pi^2)\cdots \\ &= a_1 x\left(1-\frac{x^2}{\pi^2}\right)\left(1-\frac{x^2}{4\pi^2}\right)\left(1-\frac{x^2}{9\pi^2}\right)\cdots . \end{aligned} \tag{3.2}$$

Dijeleći jednadžbu (3.2) sa x dobivamo:

$$\frac{\sin x}{x} = a_1\left(1-\frac{x^2}{\pi^2}\right)\left(1-\frac{x^2}{4\pi^2}\right)\left(1-\frac{x^2}{9\pi^2}\right)\cdots . \tag{3.3}$$

Koristeći da vrijedi $\lim\limits_{x\to 0}\frac{\sin x}{x} = 1$ te djelujući na jednadžbu (3.3) limesom gdje x teži prema 0, slijedi da je $a_1 = 1$ pa vrijedi:

$$\begin{aligned} \frac{\sin x}{x} &= \left(1-\frac{x^2}{\pi^2}\right)\left(1-\frac{x^2}{4\pi^2}\right)\left(1-\frac{x^2}{9\pi^2}\right)\cdots \\ &= 1 - x^2\left(\frac{1}{\pi^2}+\frac{1}{4\pi^2}+\frac{1}{9\pi^2}+\cdots\right) + x^4(\cdots) - x^6(\cdots) + \cdots \end{aligned} \tag{3.4}$$

Dijeleći jednadžbu (3.1) s x dobivamo:

$$\frac{\sin x}{x} = 1 - \frac{x^2}{3!} + \frac{x^4}{5!} - \frac{x^6}{7!} + \cdots . \tag{3.5}$$

Sada iz jednadžbi (3.4) i (3.5) slijedi:

$$1 - x^2\left(\frac{1}{\pi^2}+\frac{1}{4\pi^2}+\frac{1}{9\pi^2}+\cdots\right) + x^4(\cdots) - x^6(\cdots) + \cdots = 1 - \frac{x^2}{3!} + \frac{x^4}{5!} - \frac{x^6}{7!} + \cdots .$$

Izjednačavajući koeficijente uz x^2 dobivamo:

$$\begin{aligned} -\left(\frac{1}{\pi^2}+\frac{1}{4\pi^2}+\frac{1}{9\pi^2}+\cdots\right) &= -\frac{1}{3!} \quad \Big/ \cdot \pi^2 \\ 1+\frac{1}{4}+\frac{1}{9}+\cdots &= \frac{\pi^2}{6} \\ 1+\frac{1}{2^2}+\frac{1}{3^2}+\cdots &= \frac{\pi^2}{6} \\ \sum_{n=1}^{\infty}\frac{1}{n^2} &= \frac{\pi^2}{6}, n \in \mathbb{N} \end{aligned} \tag{3.6}$$

□

Osim dokaza da vrijedi $\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$, Euler je također dokazao da vrijedi:

$$\sum_{n=1}^{\infty} \frac{1}{n^4} = \frac{\pi^4}{90}, \quad \sum_{n=1}^{\infty} \frac{1}{n^6} = \frac{\pi^6}{945}, \quad \sum_{n=1}^{\infty} \frac{1}{n^8} = \frac{\pi^8}{9450}, \quad \sum_{n=1}^{\infty} \frac{1}{n^{10}} = \frac{\pi^{10}}{93555}.$$

Euler je zatim promatrao red

$$\sum_{i=1}^{\infty} \frac{1}{n^s}, s \in \mathbb{R} \tag{3.7}$$

i njegovu konvergenciju u ovisnosti o s. U tome će nam pomoći Cauchyev integralni kriterij konvergencije reda.

Teorem 3.1.1. (Cauchy) *Neka je $f : [a, +\infty] \to [0, +\infty]$ neprekidna i padajuća funkcija, gdje je $a > 0$. Tada:*

$$\text{red } \sum f(n) \text{ konvergira} \Leftrightarrow \text{nepravi integral } \int_a^{+\infty} f(x)\, dx \text{ konvergira}$$

Funkcija $f : [1, \infty\rangle \to \mathbb{R}, f(x) = \frac{1}{x^s}$ je padajuća na intervalu $[1, \infty\rangle$ jer je na tom intervalu $f'(x) = \frac{-s}{x^{s+1}} < 0$. Dakle, prema Teoremu 3.1.1 slijedi da promatrani red (3.7) konvergira ako i samo ako nepravi integral

$$\int_1^{\infty} \frac{dx}{x^s}$$

konvergira. Dakle vrijedi:

$$\int_1^{\infty} \frac{dx}{x^s} = \lim_{a \to +\infty} \int_1^a \frac{dx}{x^s} = \lim_{a \to +\infty} \left(\frac{x^{1-s}}{1-s} \right) \Bigg|_1^a = \lim_{a \to +\infty} \left(\frac{a^{1-s}}{1-s} - \frac{1^{-s}}{1-s} \right)$$

Koristeći da je $\lim_{x \to +\infty} \frac{a^x}{x} = 1$ slijedi da promatrani nepravi integral konvergira k broju $\frac{1}{s-1}$ kada je $s > 1$, a divergira kada je $s \leq 1$.
Koristeću dobivenu činjenicu, Euler je definirao zeta funkciju.

Definicija 3.1.2. *Neka je s realan broj takav da je $s > 1$.* ***Eulerova zeta funkcija*** *definira se kao:*

$$\zeta(s) = \sum_{i=1}^{\infty} \frac{1}{n^s} = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \cdots .$$

U prethodnoj definiciji lako možemo vidjeti da je Baselski problem zapravo generalizacija Eulerove zeta funkcije.

Euler je dokazao da se vrijednost zeta funkcije za parne prirodne brojeve može izračunati pomoću formule

$$\zeta(2k) = (-1)^{k+1}\frac{(2\pi)^{2k}}{2(2k)!}B_{2k}$$

pri čemu B_{2k} označava Bernoullijev broj.

Teorem 3.1.3. *Bernoullijevi brojevi zadovoljavaju slijedeću rekurziju:*

$$\begin{cases} B_0 = 1, \\ B_m = 1 - \sum_{k=0}^{m-1} \frac{B_k(n)}{m-k+1} \end{cases}$$

Iako je uspio izračunati sume s parnim eksponentima, Euler nije uspio izračunati sume s neparnim eksponentima. Eulerovu zeta funkciju, u 19. stoljeću, poopćio je njemački matematičar Bernhard Riemann. Dok je Euler za svoju zeta funkciju smatrao da je to funkcija isključivo realne varijable, Riemann je u svojoj zeta funkciji uzimao kompleksnu varijablu s. Danas funkciju kompleksne varijable s definiranu kao

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

nazivamo Riemannova zeta funkcija.

3.2 Eulerova produktna formula

Osim otkrivanja zeta funkcije, Euler je pronašao i vezu između zeta funkcije i prostih brojeva, odnosno pokazao je da vrijedi:

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p} \left(1 - \frac{1}{p^s}\right)^{-1} = \frac{1}{1-\frac{1}{2^s}} \cdot \frac{1}{1-\frac{1}{3^s}} \cdot \frac{1}{1-\frac{1}{5^s}} \cdots ; \tag{3.8}$$

pri čemu je p prost broj. Promotrimo sada Eulerovu zeta funkciju:

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} + \cdots . \tag{3.9}$$

Množeći (3.9) s $\frac{1}{2^s}$ dobivamo

$$\frac{1}{2^s}\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{4^s} + \frac{1}{6^s} + \cdots . \tag{3.10}$$

Oduzimajući (3.10) od (3.9) slijedi

$$\left(1-\frac{1}{2^s}\right)\zeta(s) = 1+\frac{1}{3^s}+\frac{1}{5^s}+\frac{1}{7^s}+\cdots. \tag{3.11}$$

Ako (3.11) pomnožimo s $\frac{1}{3^s}$ dobivamo

$$\frac{1}{3^s}\left(1-\frac{1}{2^s}\right)\zeta(s) = \frac{1}{3^s}+\frac{1}{9^s}+\frac{1}{21^s}+\cdots. \tag{3.12}$$

Oduzimajući (3.12) od (3.11) dobivamo:

$$\left(1-\frac{1}{3^s}\right)\left(1-\frac{1}{2^s}\right)\zeta(s) = 1+\frac{1}{5^s}+\frac{1}{7^s}+\frac{1}{11^s}+\frac{1}{13^s}+\cdots.$$

Nastavljajući postupak analogno, dobivamo:

$$\cdots\left(1-\frac{1}{11^s}\right)\left(1-\frac{1}{7^s}\right)\left(1-\frac{1}{5^s}\right)\left(1-\frac{1}{3^s}\right)\left(1-\frac{1}{2^s}\right)\zeta(s) = 1.$$

Dakle, vrijedi

$$\zeta(s) = \prod_p \left(1-p^{-s}\right)^{-1}$$

te smo time dokazali sljedeći teorem.

Teorem 3.2.1. (Eulerova produktna formula) *Vrijedi*

$$\zeta(s) = \sum_{n=1}^{\infty}\frac{1}{n^s} = \prod_p\left(1-\frac{1}{p^s}\right)^{-1}$$

za sve $s \in \mathbb{R}$, $s > 1$.

3.3 Razvoj funkcija sinus i kosinus

Euler je u svojim radovima često koristio poznati De Moivreov teorem koji nam govori da vrijedi jednakost:

$$(\cos(x) + i\sin(x))^n = \cos(nx) + i\sin(nx).$$

U svom djelu *Uvod u analizu beskonačnosti*, Euler je iskoristio navedeni teorem kako bi odredio razvoj funkcija sinus i kosinus u redove potencija.

Teorem 3.3.1. *Za svaki $x \in \mathbb{R}$ vrijedi:*

$$\cos(x) = 1 - \frac{x^2}{1\cdot 2} + \frac{x^4}{1\cdot 2\cdot 3\cdot 4} - \frac{x^6}{1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6} + \cdots$$

$$\sin(x) = x - \frac{x^3}{1\cdot 2\cdot 3} + \frac{x^5}{1\cdot 2\cdot 3\cdot 4\cdot 5} - \cdots$$

Dokaz. Euler je znao da za svaki $n \geq 1$ vrijedi:

$$(\cos\theta + i\sin\theta)^n = \cos n\theta + i\sin n\theta \quad \text{i} \quad (\cos\theta - i\sin\theta)^n = \cos n\theta - i\sin n\theta. \tag{3.13}$$

Zbrajajući ove dvije jednakosti i dijeleći ih s 2, zaključio je da vrijedi:

$$\cos n\theta = \frac{(\cos\theta + i\sin\theta)^n + (\cos\theta - i\sin\theta)^n}{2}.$$

Zatim je Euler, koristeći se binomnim teoremom, proširio izraz na desnoj strani i dobio:

$$\begin{aligned}
\cos n\theta = \frac{1}{2}\Bigg[&\cos^n\theta + \frac{ni\cos^{n-1}\theta\sin\theta}{1} - \frac{n(n-1)\cos^{n-2}\theta\sin^2\theta}{1\cdot 2} \\
&- \frac{n(n-1(n-2)i\cos^{n-3}\theta\sin^3\theta)}{1\cdot 2\cdot 3} + \cdots\Bigg] \\
&+ \frac{1}{2}\Bigg[\cos^n\theta + \frac{ni\cos^{n-1}\theta\sin\theta}{1} - \frac{n(n-1)\cos^{n-2}\theta\sin^2\theta}{1\cdot 2} \\
&- \frac{n(n-1(n-2)i\cos^{n-3}\theta\sin^3\theta)}{1\cdot 2\cdot 3} + \cdots\Bigg] \\
= \Bigg[&\cos^n\theta - \frac{n(n-1)\cos^{n-2}\theta\sin^2\theta}{1\cdot 2} \\
&+ \frac{n(n-1)(n-2)(n-3)\cos^{n-4}\theta\sin^4\theta}{1\cdot 2\cdot 3\cdot 4}\Bigg]
\end{aligned}$$

Nakon toga je Euler uveo supstituciju, odnosno stavio je da vrijedi $x = n\theta$, gdje je n beskonačno velik, odnosno $\theta = \frac{x}{n}$ beskonačno malen. Budući da je n beskonačno velik, Euler je smatrao da nema razlike između $n-1$, $n-2$, $n-3$ itd. pa ih je Euler zamjenio s n. Sada je Euler dobio izraz:

$$\begin{aligned}
\cos n &= 1^n - \frac{n\cdot n\cdot 1^{n-2}\left(\frac{x}{n}\right)^2}{1\cdot 2} + \frac{n\cdot n\cdot n\cdot n\cdot 1^{n-4}\left(\frac{x}{n}\right)^4}{1\cdot 2\cdot 3\cdot 4} - \cdots \\
&= 1 - \frac{x^2}{1\cdot 2} + \frac{x^4}{1\cdot 2\cdot 3\cdot 4} - \frac{x^6}{1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6} + \cdots.
\end{aligned}$$

Koristeći se sličnom metodom, prvo oduzimajući jednadžbe u (3.13), Euler je zaključio da vrijedi:

$$\sin n\theta = \frac{(\cos\theta + i\sin\theta)^n - (\cos\theta - i\sin\theta)^n}{2i}$$

iz čega je dokazao da vrijedi:

$$\sin x = x - \frac{x^3}{1\cdot 2\cdot 3} + \frac{x^5}{1\cdot 2\cdot 3\cdot 4\cdot 5} - \frac{x^7}{1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6\cdot 7} + \cdots$$

□

3.4 Eulerov identitet

Eulerova upotreba De Moivreovog teorema očituje se i u formuli koju mnogi smatraju najljepšom jednakošću cijele matematičke znanosti.

Teorem 3.4.1. *Za svaki realan broj x vrijedi $e^{ix} = \cos x + i\sin x$.*

Dokaz. Kao i kod razvoja funkcija sinus i kosinus u redove, Euler je i ovdje započeo s:

$$\cos n\theta = \frac{(\cos\theta + i\sin\theta)^n + (\cos\theta - i\sin\theta)^n}{2}.$$

Ponovno je "pustio" da n bude beskonačno velik broj pa je $\theta = \frac{x}{n}$ beskonačno malen i na taj način dobio $\cos\theta = 1$ i $\sin\theta = \theta = \frac{x}{n}$.
Time je došao do jednakosti:

$$\begin{aligned}\cos x = \cos n\theta &= \frac{(\cos\theta + i\sin\theta)^n + (\cos\theta - i\sin\theta)^n}{2} \\ &= \frac{\left(1 + \frac{ix}{n}\right)^n + \left(1 - \frac{ix}{n}\right)^n}{2}\end{aligned} \tag{3.14}$$

Euler je znao da vrijedi $e^{\omega} = 1 + \omega$ kada je ω beskonačno malen. Prema tome, ako je a konačan broj i n beskonačno velik imamo:

$$e^a = \left(e^{\frac{a}{n}}\right)^n = \left(1 + \frac{a}{n}\right)^n.$$

Mijenjajući a s konačnim (iako imaginarnim) vrijednostima ix i $-ix$ Euler je jednadžbu (3.14) transformirao u:

$$\cos x = \frac{e^{ix} + e^{-ix}}{2}.$$

Na analogan način, Euler je pokazao da vrijedi:

$$\sin x = \frac{e^{ix} + e^{-ix}}{2i}.$$

Zbrajajući dobivene rezultate, Euler je dokazao da vrijedi:

$$\cos x + i \sin x = \frac{e^{ix} + e^{-ix}}{2} + \frac{e^{ix - e^{-ix}}}{2i} = e^{ix}. \tag{3.15}$$

□

Jednadžbu (3.15) nazivamo **Eulerovim identitetom**. Primijetimo, ukoliko stavimo $x = \pi$, tada vrijedi:

$$e^{i\pi} = \cos \pi + i \sin \pi = -1 + i \cdot 0 = -1.$$

Odnosno:

$$e^{i\pi} + 1 = 0.$$

Prethodna jednadžba je povezala svih 5 najvažnijih matematičkih konstanti $(0, 1, \pi, e, i)$ pa zbog toga Eulerov identitet smatramo najljepšom matematičkom jednadžbom.

Poglavlje 4

Geometrija

Koliko je velik bio Eulerov doprinos geometriji, može se iščitati u tome što je čak 1600 stranica *Opere omnie* (kompilacija znanstvenih radova Leonharda Eulera) posvećeno geometriji. Od njegovih znamenitijih rezultata, u ovom poglavlju predstavit ćemo Eulerov dokaz da središte opisane kružnice trokuta, središte trokuta i ortocentar trokuta leže na jednom pravcu, kojeg danas nazivamo **Eulerov pravac**. Poznata je i Eulerova formula kojom je Euler povezao udaljenost središta opisane i upisane kružnice trokuta, radijus opisane kružnice i radijus upisane kružnice trokuta. Na kraju ovog poglavlja predstavit ćemo Eulerovu kružnicu kojom je Euler pokazao da se na jednoj kružnici nalaze nožišta visine trokuta i polovišta stranica.

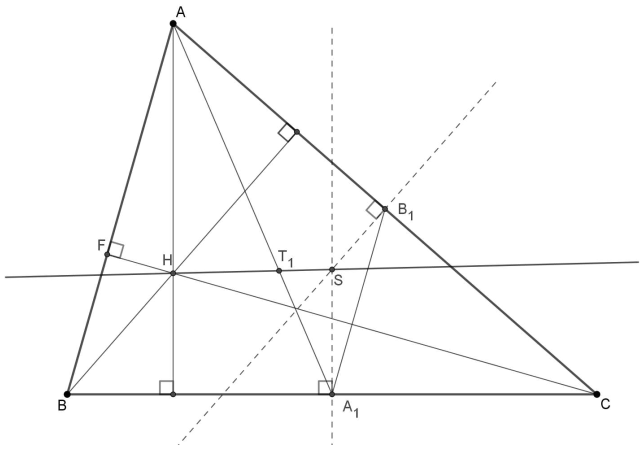
4.1 Eulerov pravac

Lema 4.1.1. *Ako su X i Y točke na dužini $\overline{AB}$ sa svojstvom $\frac{|AX|}{|BX|} = \frac{|AY|}{|BY|}$ tada se točke X i Y podudaraju.*

Dokaz. Iz $\frac{|AX|}{|BX|} = \frac{|AY|}{|BY|}$ slijedi $\frac{|AX|-|BX|}{|BX|} = \frac{|AB|-|BY|}{|BY|}$, pa je $\frac{|AB|}{|BX|} = \frac{|AB|}{|BY|}$. Dakle, $|BX| = |BY|$, odnosno X i Y se podudaraju. □

Teorem 4.1.2. *Središte S opisane kružnice trokuta, težište T i ortocentar H svakog trokuta leže na jednom pravcu, odnosno navedene točke su kolinearne. Dodatno vrijedi, $|TH| = 2\,|TS|$.*

Dokaz. Neka u trokutu ABC točke A_1 i B_1 označavaju polovišta stranica $\overline{BC}$ i $\overline{AC}$ respektivno. Prema tome $\overline{A_1B_1}$ je srednjica trokuta ABC pa slijedi da su pravci A_1B_1 i AB paralelni i $|A_1B_1| = \frac{1}{2}\,|AB|$.



Budući da su pravci AH i A_1S okomiti na BC, slijedi da su pravci AH i A_1S paralelni. Također, pravci B_1S i BH su okomiti na AC pa slijedi da su pravci B_1S i BH paralelni. Dakle, odgovarajuće stranice u trokutima ABH i A_1B_1S su paralelne.

Budući da su šiljasti kutovi $\angle HAB$ i $\angle SA_1B_1$ kutovi s paralelnim kracima, slijedi da su oni međusobno sukladni, kao i kutovi $\angle ABH$ i $\angle A_1B_1S$. Prema K-K-K teoremu o sličnosti trokuta vrijedi da su trokuti ABH i A_1B_1S slični pa vrijedi $\frac{|AH|}{|A_1S|} = \frac{|AB|}{|A_1B_1|} = 2$.

Neka točka T_1 predstavlja presjek pravca HS i AA_1. Budući da su pravci AH i A_1S paralelni, a točke A, A_1 i T_1, odnosno H, S i T_1 kolinearne, slijedi da su trokuti AHT_1 i A_1ST_1 slični prema K-K-K teoremu pa vrijedi $\frac{|AT_1|}{|A_1T_1|} = \frac{|AH|}{|A_1S|} = 2$.

Međutim, dužina $\overline{AA_1}$ je težišnica trokuta ABC i za težište T tog trokuta vrijedi $\frac{|AT|}{|A_1T|} = 2$. Sada iz $\frac{|AT_1|}{|A_1T_1|} = \frac{|AT|}{|A_1T|}$ prema Lemi 4.1.1 slijedi da se T_1 i T podudaraju, odnosno T leži na pravcu HS pa možemo zaključiti da su točke T, H, S kolinearne. Kako je $\triangle AHT \sim \triangle A_1ST$, to povlači $\frac{|TH|}{|TS|} = \frac{|AT|}{|A_1T|} = 2$. Dakle, vrijedi $|TH| = 2\,|TS|$.

□

Dobiveni pravac nazivamo **Eulerov pravac**

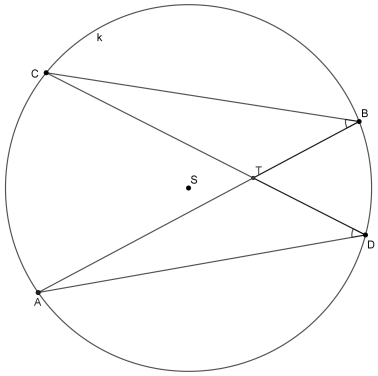
4.2 Eulerov teorem

Teorem 4.2.1. *Neka je k kružnica, a T točka ravnine. Neka je p bilo koji pravac koji prolazi točkom T i siječe kružnicu k u točkama A i B. Tada je vrijednost izraza $|TA| \cdot |TB|$*

konstantna, tj. ne ovisi o izboru pravca p.

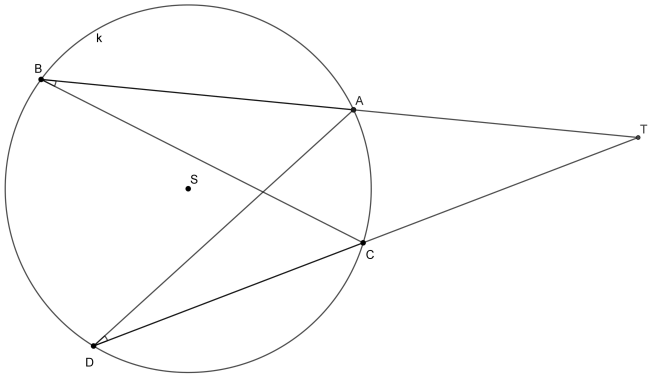
Dokaz. 1° T leži na k.
Tada se T podudara sa jednom od točaka A i B pa vrijedi ili $|TA| = 0$ ili $|TB| = 0$. Dakle, vrijedi $|TA| \cdot |TB| = 0$.

2° T je unutar k.
Budući da su kutovi $\angle ATD$ i $\angle CTB$ vršni kutovi, slijedi $\sphericalangle ATD = \sphericalangle CTB$. Dodatno, ku-



tovi $\angle CBT$ i $\angle TDA$ su obodni kutovi nad kružnim lukom $\overset{\frown}{AC}$ pa vrijedi $\sphericalangle CBT = \sphericalangle TDA$ pa prema K-K-K poučku o sličnosti trokuta slijedi $\triangle ATD \sim \triangle CTB$. Vrijedi $\frac{|TA|}{|TD|} = \frac{|TC|}{|TB|}$, odakle slijedi $|TA| \cdot |TB| = |TC| \cdot |TD|$.

3° T je izvan k



Neka su dana dva pravca koja oba prolaze kroz T. Prvi pravac siječe kružnicu k u točkama A i B, dok drugi pravac siječe kružnicu k u točkama C i D. Uočimo da su kutovi $\angle CBT$ i $\angle TDA$ obodni kutovi nad kružnim lukom $\overset{\frown}{AC}$ pa vrijedi $\sphericalangle CBT = \sphericalangle TDA$. Dodatno, trokuti

ATD i CTB imaju zajednički kut kod vrha T pa su ti trokuti slični prema K-K-K teoremu. Prema tome vrijedi $\frac{|TA|}{|TD|} = \frac{|TC|}{|TB|}$, pa je $|TA| \cdot |TB| = |TC| \cdot |TD|$. □

Definicija 4.2.2. *Za danu točku T i kružnicu k definira se **potencija točke** T s obzirom na kružnicu k:*

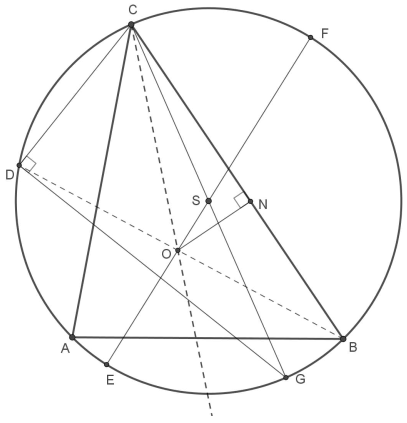
- *za točku T izvan kružnice, potencija je $|TA| \cdot |TB|$,*
- *za točku T unutar kružnice, potencija je $-|TA| \cdot |TB|$,*
- *za točku T na kružnici, potencija je 0.*

Teorem 4.2.3. (Eulerov teorem) *Neka je $k(S, R)$ kružnica opisana, a $k(O, r)$ kružnica upisana trokutu ABC. Tada je $|SO|^2 = R^2 - 2Rr$.*

Dokaz. Neka je pravac BO simetrala kuta $\angle ABC = \beta$, a pravac CO simetrala kuta $\angle BAC = \gamma$. Označimo sjecište pravca BO i kružnice opisane trokutu s D. Neka su E i F sjecišta pravca SO i kružnice opisane trokutu ABC. Tada prema Teoremu 4.2.1 vrijedi:

$$|BO| \cdot |OD| = |EO| \cdot |OF| = (R - |SO|)(R + |SO|) = R^2 - |SO|^2,$$

pa slijedi $|SO|^2 = R^2 - |BO| \cdot |OD|$, dakle želimo dokazati da vrijedi $|BO| \cdot |OD| = 2Rr$



Uočimo da su kutovi $\angle DCA$ i $\angle DBA$ obodni kutovi nad kružnim lukom $\overset{\frown}{AD}$ te je pravac BD simetrala kuta β pa vrijedi $\sphericalangle DBA = \sphericalangle DBC = \frac{\beta}{2}$. Pravac CO je simetrala kuta γ pa vrijedi $\sphericalangle ACO = \sphericalangle BCO = \frac{\gamma}{2}$.
Slijedi $\sphericalangle DCO = \sphericalangle DCA + \sphericalangle ACO = \frac{\beta}{2} + \frac{\gamma}{2}$.
Dodatno, $\angle DOC$ je vanjski kut trokuta BCO pa vrijedi $\sphericalangle DOC = \sphericalangle DBC + \sphericalangle BCO = \frac{\beta}{2} + \frac{\gamma}{2}$, odnosno $\sphericalangle DCO = \sphericalangle DOC$ odakle slijedi $|OD| = |CD|$.
Neka je N nožište okomice iz O na $\overline{BC}$ te neka je G sjecište pravca CS i kružnice opisane

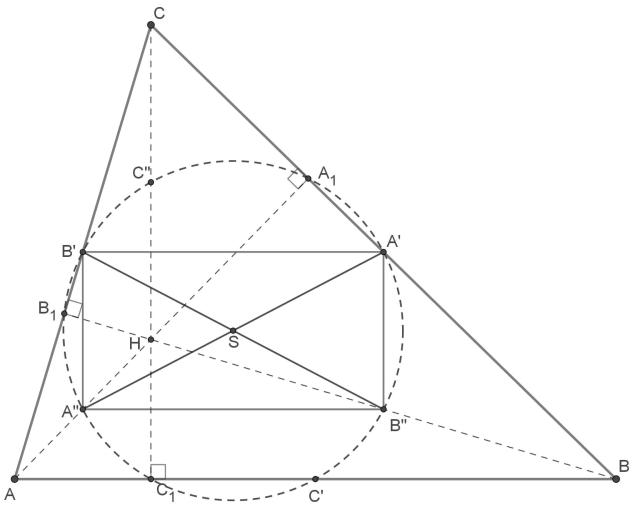
trokutu. Prema Talesovom teoremu slijedi $\sphericalangle CDG = 90°$, odnosno $\sphericalangle CDG = \sphericalangle ONB$.
Kutovi $\angle DGC$ i $\angle DBC$ su obodni kutovi nad kružnim lukom $\overset{\frown}{CD}$ pa vrijedi $\sphericalangle DGC = \sphericalangle DBC$.
Prema K-K-K teoremu o sličnosti trokuta slijedi da su trokuti BNO i GDC slični.
Sada vrijedi $\frac{|BO|}{|GC|} = \frac{|NO|}{|DC|}$, odnosno $\frac{|BO|}{2R} = \frac{r}{|DC|}$, iz čega konačno slijedi:

$$|BO| \cdot |OD| = |BO| \cdot |CD| = 2Rr.$$

□

4.3 Eulerova kružnica

Teorem 4.3.1. *Neka su u trokutu ABC točke A', B', C' polovišta stranica, točke A'', B'', C'' polovišta dužina $\overline{AH}$, $\overline{BH}$, $\overline{CH}$ gdje je H ortocentar, a točke A_1, B_1 i C_1 nožišta visina. Svih devet točaka A', B', C', A'', B'', C'', A_1, B_1, C_1 leže na istoj kružnici.*



Dokaz. Uočimo da je $\overline{A'B'}$ srednjica trokuta ABC pa vrijedi $|A'B'| = \frac{1}{2}|AB|$ i $AB \parallel A'B'$.
Dodatno, $\overline{A''B''}$ je srednjica trokuta ABH pa vrijedi $|A''B''| = \frac{1}{2}|AB|$ i $AB \parallel A''B''$. Slijedi da je $|A'B'| = |A''B''|$ i $A'B' \parallel A''B''$. Dakle, četverokut $A'B'A''B''$ je paralelogram pa se njegove dijagonale međusobno raspolavljaju. Presjek tih dijagonala označimo sa S. Budući da je $\overline{A''B'}$ srednjica trokuta AHC, slijedi da je $A''B' \parallel CH$, dakle vrijedi $A''B' \perp AB$, odnosno $A''B' \perp A''B''$. Sada slijedi $\sphericalangle B'A''B'' = 90°$, dakle četverokut $A'B'A''B''$ je pravokutnik pa mu možemo opisati kružnicu $k\left(S, \frac{1}{2}|A'A''|\right)$.
Na analogan način dokazujemo da je $A'C'A''C''$ pravokutnik pa mu možemo opisati kružnicu $k\left(S, \frac{1}{2}|A'A''|\right)$. Dakle, točke A',B',C',A'',B'',C'' leže na istoj kružnici k.
Budući da je trokut $A'A''A_1$ pravokutan s hipotenuzom $\overline{A'A''}$ slijedi da je kružnica opisana

tom trokutu $k\left(S, \frac{1}{2}|A'A''|\right)$ što povlači da i A_1 leži na k. Na analogni način dokazujemo da i B_1 i C_1 pripadaju kružnici k. □

Leonhard Euler je 1765. dokazao da se nožišta visina trokuta i polovišta stranica trokuta nalaze na jednoj kružnici pa se prema tome kružnica iz prethodnog teorema naziva **Eulerova kružnica**. Charles Julien Brianchon i Jean-Victor Poncelet su 1820. godine naveli da se na Eulerovoj kružnici nalaze i polovišta spojnica vrhova trokuta i ortocentra trokuta, dok je Karl Wilhelm Feuerbach 1822. dokazao da Eulerova kružnica dira sve četiri kružnice koje diraju stranice trokuta pa se prema tome Eulerova kružnica još naziva **kružnica devet točaka** ili **Feuerbachova kružnica**.

Bibliografija

[1] R. Ayoub, *Euler and the Zeta Function*, The American Mathematical Monthly **81** (1974.), br. 10, 1067–1086.

[2] D. Bojmić, *Uvod u Riemannovu hipotezu* (Diplomski rad), Zagreb: Sveučilište u Zagrebu, Prirodoslovno matematički fakultet (2014).

[3] M. Bombardelli i D. Ilišević, *Elementarna geometrija*, Zagreb: Sveučilište u Zagrebu, Prirodoslovno matematički fakultet (2007.), https://web.math.pmf.unizg.hr/~ilisevic/Slike/EGskripta.pdf.

[4] F. M. Brückler, *Leonhard Euler*, Osječki matematički list **10** (2010), br. 1, 95–98.

[5] A. Dujella, *Teorija brojeva*, Školska Knjiga, 2019.

[6] M. Garcia, J. Munch Pedersen i H. te Riele, *Amicable Pairs, a Survey*, Fields Institute Communications **41** (2004), 183–184.

[7] A. Golemac, *Teorija Grafova*, Prirodoslovno - matematički fakultet u Splitu, 2022.

[8] A. Golemac, A. Mimica i T. Vučičić, *Od königsberških mostova do kineskog poštara*, (2012), http://e.math.hr/category/klju-ne-rije-i/problem-kineskog-po-tara.

[9] I. Grgić, *Upoznavanje s Bernoullijevim brojevima*, Acta mathematica Spalatensia. Series didactica) **5**, br. 2, 59–70, https://doi.org/10.32817/amssd.5.6.

[10] B. Ibrahimpašić i E. Liđan, *Mersenneovi i savršeni brojevi*, MAT-KOL (Banja Luka) **15**, br. 2, 51–60.

[11] M. Jukić Bokun, *Eulerova funkcija*, Hrvatski matematički elektronički časopis **31** (2017), br. 1, 35–39.

[12] A. Lovrić, *Leonhard Euler - znameniti matematičar 18. stoljeća* (Diplomski rad), Osijek: Sveučilište Josipa Jurja Strossmayera u Osijeku, Odjel za matematiku (2019.).

[13] I. Matić, *Uvod u teoriju brojeva*, Odjel za matematiku Sveučilišta J.J. Strossmayera u Osijeku (2013.), https://www.mathos.unios.hr/images/homepages/mirela/UUTB/uvod_u_teoriju_brojeva.pdf.

[14] G. Šimić, *Riemannova zeta funkcija* (Diplomski rad), Osijek: Sveučilište Josipa Jurja Strossmayera u Osijeku, Odjel za matematiku (2011).

[15] V. Tisanić, *Baselski problem*, Zagreb: Sveučilište u Zagrebu, Prirodoslovno matematički fakultet (2018.).

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

Sažetak

U ovom diplomskom radu opisan je život i znanstveni doprinos Leonharda Eulera.

U prvome poglavlju bavimo se Eulerovim doprinosima u teoriji grafova te prikazujemo zbog čega se Eulera naziva ocem topologije. Između ostalog, spominjemo Eulerove grafove, njihovu primjenu te Eulerovu formulu za poliedre.

U drugome poglavlju ovog rada, opisujemo Eulerov doprinos teoriji brojeva. Uz nadaleko poznatu Eulerove funkciju te Eulerov teorem, bavimo se i kvadratnim zakonom reciprociteta te Eulerovim otkrićima vezanim uz savršene i prijateljske brojeve.

U trećem poglavlju prikazujemo Eulerove rezultate u matematičkoj analizi od kojih se najviše ističu Eulerova zeta funkcija i njen produkt, Eulerov identitet te razvoj funkcija sinus i kosinus.

U posljednjem poglavlju bavimo se Eulerovim doprinosom u geometriji pri čemu spominjemu Eulerov pravac, Eulerov teorem i Eulerovu kružnicu.

Summary

This master's thesis describes the life and scientific contribution of Leonhard Euler.

The first chapter describes his contribution in graph theory and shows why Euler is called the father of topology. Among other things, Euler's graphs are mentioned as is their application. Euler's formula for polyhedra is also discussed.

In the second chapter of this work, Euler's contribution to number theory is described. In addition to widely known Euler function and Euler's theorem, the law of quadratic reciprocity and Euler's discoveries related to perfect and friendly numbers is mentioned.

In the third chapter Euler's result in mathematical analysis is presented, of which I emphasize Euler's zeta function and its product, Euler's identity and the development of the sine and cosine function.

The last chapter of this paper deals with Euler's contribution in geometry, where Euler's line, Euler's theorem and Euler's circle are mentioned.

Životopis

Rođen sam 30. 08. 1996. godine u Zaboku. Od 2003. do 2011. godine pohađam Osnovnu školu Ante Kovačića u Zlataru te nakon toga svoje obrazovanje nastavljam u Srednjoj školi Zlatar, gdje sam 2015. godine završio opću gimnaziju. 2016. godine upisujem preddiplomski sveučilišni studij Matematike, smjer nastavnički na Prirodoslovno-matematičkom fakultetu Sveučilišta u Zagrebu. Isti završavam 2021. godine te zatim upisujem diplomski studij Matematike, nastavnički smjer.