Teorija brojeva kroz povijest

Gmajnić, Ana

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Ana Gmajnić

TEORIJA BROJEVA KROZ POVIJEST

Diplomski rad

Voditelj rada:
doc. dr. sc. Filip Najman

Zagreb, 2015.

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

1. _____, predsjednik
2. _____, član
3. _____, član

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Sadržaj

Uvod

Teorija brojeva je grana matematike koja ponajprije proučava svojstva skupa prirodnih, cijelih i ponekad racionalnih brojeva. Za razliku od većine ostalih područja matematike, seže više od 4500 godina u prošlost. Unatoč njenoj starosti, još uvijek postoje pitanja koja čak i do danas nisu odgovorena. Veliki broj načela tog područja otkrivena su eksplicitnim eksperimentima. Od svog osnutka u klasičnom razdoblju, kroz razvoj od 1600. do 1800. godine, teorija brojeva je većinu vremena bila odvojena od ostalih područja matematike. Pitanja teorije brojeve nisu samo bitna matematičarima. Danas, kao i u ranim danima, ovi su problemi privlačni i mnogim laicima te je teorija brojeva zabilježena kao područje matematike u kojemu su prijedlozi i slutnje amatera zaslužne za mnoge cijenjene rezultate.

Cilj ovog rada je pokazati kako se teorija brojeva razvijala kroz povijest i koje teme su bile zanimljive čak i prvim matematičarima, ali i matematičarima danas. Većina od spomenutih tema se provlačila kroz skoro svako razdoblje teorije brojeva. Rani matematičari su otkrili mnoge probleme, no nisu imali potrebne alate kako bi te iste probleme dokazali. Kako se matematika godinama razvijala, tako su i brojni stari teoremi dobili svoje dokaze.

U ovom radu spomenuti su samo neki od glavnih problema koji se javljaju na području teorije brojeva. U izboru su prevagnule teme koje su bile od izrazite povijesne važnosti. Naravno, sve je zapisano u modernom zapisu zbog lakše razumljivosti teorema i dokaza. Rad počinje starom babilonskom pločom Plimpton 322 te završava Dirichletovim teoremom o prostim brojevima u aritmetičkom nizu. Time ne staju otkrića, naprotiv, teorija brojeva se uvukla i u ostale grane matematike te je danas zanimljiva većini matematičara.

Poglavlje 1

Rana povijest

1.1 Babilonci (2500. pr. Kr.)

Bilježenje brojeva postojalo je čak i prije nego bilježenje riječi. Prvi bitan napredak u matematici bilo je uvođenje brojki oko 3500. g. pr. Kr. u Mezopotamiji. Tamo su se iz prvotnih piktograma razvili prvi brojevni sustavi. Stare civilizacije najčešće su koristile nepozicijske brojevne sustave s bazom 10, ali i 60, 20 te 12. Dok se osnovni račun s prirodnim brojevima razvio vrlo rano, svijest o brojevima kao apstraktnim objektima još nije postojala. Prvi tragovi teorije brojeva mogu se pronaći kod Babilonaca na Plimpton 322 ploči. Na toj ploči možemo naći prvi oblik Pitagorinog poučka i to puno prije samog Pitagore. Nađeni su popisi brojeva koje nazivamo Pitagorine trojke.

Definicija 1.1.1. *Uređenu trojku prirodnih brojeva* (x, y, z) *zovemo* Pitagorina trojka *ako su x i y duljine kateta, a z duljina hipotenuze nekog pravokutnog trokuta, tj. vrijedi*

$$x^2 + y^2 = z^2. \tag{1.1}$$

Ako su x, y, z relativno prosti onda kažemo da je (x, y, z) primitivna Pitagorina trojka.

Teorem 1.1.2. *Sve primitivne Pitagorine trojke* (x, y, z) *u kojima je y paran broj dane su formulama*

$$x = m^2 - n^2, \quad y = 2mn, \quad z = m^2 + n^2 \tag{1.2}$$

gdje je $m > n$ *i m, n su relativno prosti prirodni brojevi različite parnosti.*

Dokaz. Jednadžbu (1.1) možemo pisati u obliku $y^2 = (z + x)(z - x)$.
Neka je $y = 2c$. Brojevi $z + x$ i $z - x$ su parni, pa postoje prirodni brojevi a i b takvi da je $z + x = 2a$, $z - x = 2b$.
Sada je

$$c^2 = ab.$$

Iz $z = a+b$, $x = a-b$ zaključujemo da je $(a,b) = 1$ (najveći zajednički djelitelj) pa postoje $m, n \in \mathbb{N}$, $(m,n) = 1$, takvi da je $a = m^2$.
Odavde je

$$x = m^2 - n^2, \quad z = m^2 + n^2, \quad y = 2mn.$$

Brojevi m i n moraju biti različite parnosti jer je broj $x = m^2 - n^2$ neparan. Lako se provjeri da brojevi x, y, z definirani s (1.2) zadovoljavaju (1.1).
Treba još provjeriti da li su relativno prosti. Pretpostavimo da je $(x,z) = d > 1$. Tada je d neparan, $d \mid (m^2 + n^2) + (m^2 - n^2) = 2m^2$ i $d \mid (m^2 + n^2) - (m^2 - n^2) = 2n^2$. Ovo je u kontradikciji s pretpostavkom da su m i n, tj. m^2 i n^2 relativno prosti. □

1.2 Pitagora (571. - 495. pr. Kr.)

Pitagora sa Samosa poznat je kao prvi pravi matematičar, ali se zapravo vrlo malo zna o njegovim matematičkim dostignućima. Naime, niti jedno njegovo djelo nije opstalo. Unatoč tome, smatra se da je upravo on prvi počeo istraživati temeljne principe matematike. Pitagora je zaslužan za osnivanje takozvane Pitagorejske škole koja se bavila geometrijom, glazbom, astronomijom, ali i aritmetikom. Pitagorejci su bili prvi koji su otkrili postojanje iracionalnih brojeva tako što su dokazali da duljina dijagonale kvadrata nije proporcionalna stranici tog istog kvadrata. Također, Pitagorejci su se i bavili traženjem prirodnih brojeva x, y, z koji zadovoljavaju jednakost $x^2 + y^2 = z^2$.

Rano rješenje Pitagorine jednadžbe

Geometrijsko otkriće da su stranice pravokutnog trokuta povezane zakonom koji se može zapisati brojevima vodilo je do pripadajućeg aritmetičkog problema. Proučavanje takvih brojeva je jedan od najranijih problema u teoriji brojeva. On zahtjeva traženje svih pravokutnih trokuta za čije stranice vrijedi $x^2 + y^2 = z^2$. Pitagora je zaslužan za pronalazak relacije koja pronalazi samo neka od rješenja. Ta relacija je

$$x = 2n + 1, \quad y = 2n^2 + 2n, \quad z = 2n^2 + 2n + 1,$$

gdje je $n \geq 1$ proizvoljan cijeli broj. Pitagora je navodno došao do ovog rješenja relacijom iz koje dobivamo kvadratni broj iz manjeg kvadratnog broja

$$(2k - 1) + (k - 1)^2 = k^2. \tag{1.3}$$

Strategija pretpostavlja da je $2k-1$ kvadrat. Ako uzmemo $2k-1 = m^2$ i riješimo jednadžbu po k dobivamo

$$k = \frac{m^2 + 1}{2}, \quad k - 1 = \frac{m^2 - 1}{2}.$$

Kada ove vrijednosti uvrstimo u (1.3) slijedi

$$m^2 + \left(\frac{m^2-1}{2}\right)^2 = \left(\frac{m^2+1}{2}\right)^2,$$

odakle

$$x = m, \quad y = \frac{m^2-1}{2}, \quad z = \frac{m^2+1}{2}, \tag{1.4}$$

zadovoljava Pitagorinu jednakost za bilo koji neparni broj $m > 1$ (m mora biti neparan zbog $m^2 = 2k - 1$).
Kada je $m = 2n + 1$, pri čemu je $n \geq 1$, brojevi u (1.4) postaju

$$x = 2n + 1, \quad y = 2n^2 + 2n, \quad z = 2n^2 + 2n + 1, \tag{1.5}$$

što je upravo Pitagorin rezultat. Ako pogledamo tablicu za prvih nekoliko n, možemo primijetiti da Pitagorina metoda nalazi pravokutne trokute za koje vrijedi da je duljina hipotenuze za 1 veća od duljine jedne katete.

n	x	y	z
1	3	4	5
2	5	12	13
3	7	24	25
4	9	40	41
5	11	60	61

Drugo rješenje ovog problema dao je Platon, on je pronašao trokute čija je duljina hipotenuze za 2 veća od duljine jedne katete. Njegova relacija je oblika

$$x = 2n, \quad y = n^2 - 1, \quad z = n^2 + 1. \tag{1.6}$$

Ovu formulu možemo dobiti uz pomoć relacije (1.3) koju sada primjenjujemo dva puta:

$$\begin{aligned}(k+1)^2 &= k^2 + (2k+1) \\ &= \left[(k-1)^2 + (2k-1)\right] + 2k + 1 \\ &= (k-1)^2 + 4k.\end{aligned}$$

Ako zamjenimo k s n^2 dobivamo Platonovu formulu:

$$(2n)^2 + (n^2-1)^2 = (n^2+1)^2.$$

Iz ove formule dobivamo trojku $(8, 15, 17)$ koju ne možemo dobiti iz Pitagorine formule. Potpuno rješenje Pitagorinog problema nalazimo tek u Euklidovim Elementima (X), ovdje zapisano u Teoremu 1.1.2.

1.3 Euklidovi Elementi (ca. 300. pr. Kr.)

Euklid je bio poznati grčki matematičar iz Atene. Živio je i radio u Aleksandriji gdje je osnovao matematičku školu Museion. Napisao je brojna djela, od kojih neka nisu sačuvana i poznata su samo po naslovu. Iako se Euklid zanimao za geometriju također se bavio teorijom brojeva i to u svojem djelu *Elementi*. Točnije, knjige VII,VIII i IX se sastoje od 102 propozicije posvećene grčkoj aritmetici. Grci (Pitagorejci) su u to vrijeme proučavali samo pozitivne cijele brojeve. Neke od ovih propozicija su bile i ranije poznate, no Euklid je bio prvi koji ih je poredao po logičnom slijedu. To znači da su se novi teoremi dokazivali pomoću prethodno dokazanih teorema i aksioma. Euklida su posebno zanimali problemi djeljivosti te svojstva prostih brojeva.

Djeljivost i prosti brojevi

Djeljivosti i prosti brojevi su osnovni pojmovi kojima se bavi teorija brojeva te pojmovi koji su bili zanimljivi čak i prvim matematičarima.

Definicija 1.3.1. *Za cijeli broj b kažemo da je* djeljiv *cijelim brojem $a \neq 0$ ako postoji cijeli broj c takav da je $b = ac$. To zapisujemo kao $a \mid b$. Ako a ne dijeli b, pišemo $a \nmid b$.*

Definicija 1.3.2. *Za cijeli broj $p > 1$ kažemo da je* prost *ako su mu jedini pozitivni djelitelji 1 i p. Broj koji je veći od jedan i nije prost zovemo složenim brojem.*

Teorem 1.3.3. ***Teorem o dijeljenju s ostatkom.*** *Za proizvoljan prirodni broj a i cijeli broj b postoje jedinstveni cijeli brojevi q i r takvi da je $b = qa + r$, $0 \leq r < a$.*

Dokaz. Promotrimo skup $\{b - am : m \in \mathbb{Z}\}$. Najmanji nenegativni član ovog skupa označimo s r. Tada je po definiciji $0 \leq r < a$ te postoji $q \in \mathbb{Z}$ takav da je $b - qa = r$, tj. $b = qa + r$. Da bi dokazali jedinstvenost od q i r, pretpostavimo da postoji još jedan par q_1 i r_1 koji zadovoljava iste uvjete. Pokažimo najprije da je $r = r_1$. Pretpostavimo da je $r < r_1$. Tada je $0 < r_1 - r < a$, dok je s druge strane $r_1 - r = a(q - q_1) \geq a$. Prema tome je $r_1 = r$ i $q_1 = q$. □

Teorem 1.3.4. ***Euklidov algoritam.*** *Neka su $b, c > 0$, cijeli brojevi. Pretpostavimo da je uzastopnom primjenom teorema o dijeljenju s ostatkom dobiven niz jednakosti*

$$\begin{aligned} b &= cq_1 + r_1, \quad 0 < r_1 < c, \\ c &= r_1q_2 + r_3, \quad 0 < r_2 < r_1, \\ r_1 &= r_2q_3 + r_3, \quad 0 < r_3 < r_2, \\ &\dots \\ r_{j-2} &= r_{j-1}q_j + r_j, \quad 0 < r_j < r_{j-1}, \\ r_{j-1} &= r_jq_{j+1} \end{aligned}$$

Tada je (b, c) *jednak* r_j*, posljednjem ostatku različitom od nule. Vrijednosti od* x_0 *i* y_0 *u izrazu* $(b, c) = bx_0 + cy_0$*, mogu se dobiti izražavanjem svakog ostatka* r_i *kao linearne kombinacije od b i c. Ovaj postupak određivanja najvećeg zajedničkog djelitelja naziva se* Euklidov algoritam*.*

Otkriće ovog algoritma se ponekad pripisuje i Pitagorejcima, no Euklid ga prvi objavljuje u svojim Elementima. Ovaj algoritam su koristili čak i kineski i indijski matematičari u 5. stoljeću.

Dokaz. Dokaz Teorema 1.3.4. može se naći u [3, str. 4, Teorem 1.5.]. □

Teorem 1.3.5. ***Bezoutov identitet.*** *Neka su a i b cijeli brojevi različiti od nula. Postoje brojevi x i y takvi da je* $(a, b) = ax + by$*.*

Dokaz. Dokaz slijedi izravno primjenom Euklidovog algoritma unatrag. □

Teorem 1.3.6. *Neka su a i b cijeli brojevi. Najmanji prirodni broj m za kojeg postoji cjelobrojno rješenje jednadžbe* $ax + by = m$ *je* (a, b)*. Štoviše, jednadžba* $ax + by = m$ *ima cjelobrojno rješenje ako i samo ako* (a, b) *dijeli m.*

Dokaz. Kako $(a, b) \mid a$ i $(a, b) \mid b$, mora vrijediti i $(a, b) \mid ax + by$. Ako jednadžba $ax + by = m$ ima cjelobrojno rješenje, tada $(a, b) \mid m$. Ukoliko je m prirodan broj manji od (a, b), tada m nije djeljiv s (a, b) pa promatrana jednadžba nema rješenja za takav m. Prethodni teorem nam govori kako postoji cjelobrojno rješenje jednadžbe $ax + by = (a, b)$. Neka je $m \in \mathbb{N}$ takav da $(a, b) \mid m$. Tada postoji $d \in \mathbb{N}$ za koji vrijedi $m = (a, b) \cdot d$.
Slijedi

$$adx + bdy = d \cdot (a, b) = m$$

pa je dx, dy traženo cjelobrojno rješenje. □

Ovaj teorem nam pokazuje da su brojevi a i b relativno prosti ako i samo ako postoji cjelobrojno rješenje jednadžbe $ax + by = 1$. Ta tvrdnja nas dovodi do sljedećeg teorema.

Teorem 1.3.7. *Neka su a i b cijeli brojevi različiti od 0. Onda su a i b relativno prosti ako i samo ako postoje cijeli brojevi x i y takvi da je* $ax + by = 1$.

Dokaz. Ako su a i b relativno prosti onda im je najveći zajednički djelitelj $(a, b) = 1$. Prema Teoremu 1.3.5. možemo pronaći brojeve x i y takve da vrijedi $1 = ax + by$.
Pretpostavimo da vrijedi $1 = ax + by$ za neki izbor x i y, i najveći zajednički djelitelj od a i b je $(a, b) = c$. Sada imamo da $c \mid a$ i $c \mid b$, onda mora vrijediti da $c \mid (ax + by)$ ili $c \mid 1$. Kako je c pozitivan cijeli broj, zbog posljednjeg uvjeta mora vrijediti $c = 1$. □

Korolar 1.3.8. *Ako je najveći zajednički djelitelj cijelih brojeva a, b jednak* $(a, b) = c$, *onda je* $(a/c, b/c) = 1$.

Dokaz. Za početak, bitno je primijetiti da su a/c i b/c zapravo cijeli brojevi iako nalikuju na razlomke. Sada imamo da c dijeli i a i b. Kako je $(a, b) = c$, moguće je pronaći cijele brojeve x i y tako da vrijedi $c = ax + by$. Ako podijelimo obje strane jednakosti sa c dobivamo

$$1 = (a/c)x + (b/c)y.$$

Kako su a/c i b/c cijeli brojevi tvrdnja teorema vrijedi. Zaključak je da su a/c i b/c relativno prosti brojevi. □

Korolar 1.3.9. *Ako* $a \mid c$, $b \mid c$ *i* $(a, b) = 1$, *onda* $ab \mid c$.

Dokaz. Kako $a \mid c$ i $b \mid c$, postoje cijeli brojevi r i s za koje vrijedi $c = ar = bs$. Kako je $(a, b) = 1$ možemo pisati i $1 = ax + by$, za odgovarajuće cijele brojeve x i y. Pomnožimo li sada tu jednakost sa c dobivamo

$$c = c \cdot 1 = c(ax + by) = acx + bcy.$$

Ako primijenimo odgovarajuću supstituciju s desne strane dobivamo

$$c = a(bs)x + b(ar)y = ab(sx + ry),$$

to jest $ab \mid c$. □

Teorem 1.3.10. *Ako je* $(a, m) = (b, m) = 1$, *onda je* $(ab, m) = 1$.

Dokaz. Dokaz Teorema 1.3.10. može se naći u [3, str. 3 , Propozicija 1.3.]. □

Teorem 1.3.11. ***Euklidova lema.*** *Ako* $a \mid bc$ *i* $(a, b) = 1$, *onda* $a \mid c$.

Dokaz. Započinjemo opet s $1 = ax + by$ pri čemu su x i y cijeli brojevi. Množenjem ove jednadžbe sa c dobivamo

$$c = c \cdot 1 = (ax + bx)c = acx + bcy.$$

Kako $a \mid ac$ i $a \mid bc$ slijedi da $a \mid (acx + bcy)$, to jest $a \mid c$. □

Teorem 1.3.12. *Neka je p prost broj i $p \mid ab$, onda $p \mid a$ ili $p \mid b$. Općenito, ako $p \mid a_1 a_2 \cdots a_n$, onda p dijeli barem jedan od faktora a_i.*

Dokaz. Ako $p \mid a$ nemamo što dokazivati. Pretpostavimo da $p \nmid a$. Kako p ima samo dva djelitelja, 1 i p slijedi $(a, p) = 1$. Sada Euklidova lema povlači da $p \mid b$.
Općenitiju tvrdnju dokazujemo indukcijom. Pretpostavimo da tvrdnja vrijedi za produkte s manje od n faktora. Sada ako $p \mid a_1(a_2 \cdots a_n)$, onda $p \mid a_1$ ili $p \mid a_2 a_3 \cdots a_n$. Ako $p \mid a_2 a_3 \cdots a_n$, onda po induktivnoj pretpostavci $p \mid a_i$ za neki $i = 2, \ldots, n$. □

Teorem 1.3.13. ***Osnovni teorem aritmetike.*** *Svaki prirodni pozitivni broj $n > 1$ je ili prost ili se može zapisati kao produkt prostih brojeva. Taj zapis je jedinstven do na poredak prostih faktora.*

Dokaz. Egzistencija. Tvrdnju da postoji rastav broja $a > 1$ na proste faktore dokazujemo indukcijom. Za $a = 2$ nemamo što dokazivati. Pretpostavimo da svi brojevi iz skupa $\{2, \ldots, a-1\}$ imaju barem jedan rastav na proste faktore. Ako je a prost opet nemamo što dokazivati. Uzmimo da je $p > 1$ najmanji netrivijalni djelitelj broja a. Očito, p mora biti prost jer bi u suprotnom a imao djelitelja manjeg od p što je u suprotnosti s izborom p.
Vrijedi $a = pa'$, gdje je $1 < a' < a$. Sada induktivnu pretpostavku možemo primijeniti na a', tj. $a' = p_1 \cdot \ldots \cdot p_m$.
No tada je

$$a = p \cdot p_1 \cdot \ldots \cdot p_m,$$

čime smo završili dokaz.
Jedinstvenost. Pretpostavimo da je $a = p_1 \cdot p_2 \cdot \ldots \cdot p_r = q_1 \cdot q_2 \cdot \ldots \cdot q_s$. Bez smanjenja općenitosti pretpostavimo da je $r \leq s$. Kako $p_1 \mid q_1 \cdot q_2 \cdot \ldots \cdot q_s$ i p_1 je prost broj, zaključujemo da $p_1 | q_{j_1}$ za neki j_1, međutim i q_{j_1} je, kao i p_1, prost broj pa je $p_1 = q_{j_1}$.
Isto zaključivanje možemo ponoviti i za $p_2, \ldots, p_r$ pa za svaki $1 \leq i \leq r$ postoji indeks j_i takav da $p_i = q_{j_i}$. Pri tome su svi indeksi $j_1, \ldots, j_r$ međusobno različiti. Ako bi bilo $r < s$ tada bismo po označavanju $\{k_1, \ldots, k_{s-r}\} = \{1, \ldots, s\} \setminus \{j_1, \ldots, j_r\}$ dobili da je $1 = q_{k_1} \cdot \ldots \cdot q_{k_{s-r}}$ što je očito nemoguće. Znači mora biti $r = s$. □

Iz teorema vidimo da su prosti brojevi temelj pomoću kojih se može prikazati svaki prirodni broj i to na jedinstven način (do na poredak). Iako se Osnovni teorem aritmetike ponekad pripisuje Euleru, prvi koji ga je u potpunosti dokazao je bio Gauss početkom 19. stoljeća.

Teorem 1.3.14. *Postoji beskonačno mnogo prostih brojeva.*

Dokaz. Pretpostavimo suprotno, postoji konačno mnogo prostih brojeva i p je najveći takav broj. Zapišimo sada proste brojeve $2, 3, 5, 7, 11, \ldots$ u rastućem poretku. Neka je

$$N = (2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot \ldots \cdot p) + 1,$$

za prost broj p. Kako je $N > 1$ možemo koristiti Osnovni teorem aritmetike kako bi zaključili da je N djeljiv nekim prostim brojem q. Niti jedan od prostih brojeva $2, 5, \ldots, p$ ne dijeli N. Ako bi q bio jedan od ovih prostih projeva, onda kombiniranjem relacije $q \mid 2 \cdot 3 \cdot 5 \cdot \ldots \cdot p$ s $q \mid N$, dobili bi $q \mid (N - 2 \cdot 3 \cdot \ldots \cdot p)$, tj. $q \mid 1$. Jedini pozitivni djelitelj broja 1 je sam 1, a kako je $q > 1$ kontradikcija je očita. Zaključujemo da postoji prost broj q veći od p, dakle ne postoji najveći prosti broj. □

1.4 Diofant (ca. 200. pr. Kr.)

Diofant iz Aleksandrije, koji se još naziva ocem algebre, bio je grčki matematičar koji je povratio Museionu izgubljenu slavu. Autor je serije knjiga pod imenom *Aritmetika* u kojima se problemima iz teorije brojeva pristupa i algebarski. Diofant je tražio cjelobrojna i racionalna rješenja algebarskih jednadžbi te se zbog njegovog ranog doprinosa takve jednadžbe nazivaju Diofantskim jednadžbama. Diofantskom jednadžbom nazivamo općenito neodređenu polinomnu jednadžbu ili neodređenu jednadžbu nekog drugog oblika koja, međutim, nalazi rješenja u domeni pozitivnih racionalnih brojeva. U takve probleme ubrajamo i probleme nalaženja Pitagorinih trojki. Diofant, naravno, nije znao formule za traženje rješenja takvih jednadžbi, no uspio je riješiti veliki broj takvih problema. Ovdje je spomenuto njih nekoliko u modernom zapisu.

Problem 1 u knjizi **II** kaže:
Nađi dva racionalna broja takva da je njihov zbroj proporcionalan zbroju njihovih kvadrata.
U modernom zapisu bi pisali

$$\frac{x^2 + y^2}{x + y} = p \tag{1.7}$$

gdje su x i y brojevi koje tražimo, a p nam je zadan koeficijent proporcionalnosti. Jednakost (1.7) možemo pisati kao

$$x^2 - xp + y^2 - yp = 0.$$

Rješenja ove kvadratne jednadžbe su

$$x = \frac{p}{2} \pm \sqrt{\frac{p^2}{4} - y^2 + py}. \tag{1.8}$$

Kako tražimo racionalna rješenja, broj ispod korijena mora biti kvadrat. Tvrdnja koja će nam ovdje pomoći je da se svaki racionalan broj može iskazati u obliku

$$r = \frac{p}{2} + ty$$

za pogodan racionalan broj t. Sada (1.8) možemo zapisati kao

$$\frac{p^2}{4} - y^2 + py = \left(\frac{p}{2} + ty\right)^2. \tag{1.9}$$

Sređivanjem ove jednakosti dobivamo

$$y = p\frac{1-t}{1+t^2}. \tag{1.10}$$

Za svaku racionalnu vrijednost broja t, odgovarajući y u (1.10) čini jednakost (1.9) kvadratom

$$\frac{p^2}{4} - y^2 + py = \left[\frac{p}{2}\frac{(1+2t-t^2)}{1+t^2}\right]^2.$$

Kada ovu jednakost uvrstimo u (1.8), za x imamo dva rješenja:

$$x = p\frac{1+t}{1+t^2}, \quad x = p\frac{t(t-1)}{1+t^2}. \tag{1.11}$$

Općenito rješenje ovog problema je dano s (1.10) i s (1.11) za racionalni t. Diofant nije znao ove formule, ali je demonstrirao metodu za $p = 10$. Njegovo rješenje $x = 12$, $y = 6$ odgovara $t = \frac{1}{3}$.

Problem 22 u knjizi **IV** se svodi na pronalaženje Pitagorinih trojki:
Pronađi tri broja x, y, z; $x > y > z$ takvih da vrijedi

$$x - y = a^2, \quad y - z = b^2, \quad x - z = c^2$$

i tako da je jedan od tih brojeva geometrijska sredina prestala dva. Prethodne jednakosti možemo zapisati kao

$$x = y + a^2, \quad z = y - b^2 \tag{1.12}$$

s proizvoljnim a i b, ali kada ove vrijednosti uvrstimo u treću jednakost dobivamo

$$a^2 + b^2 = c^2.$$

Ako jednakost (1.6) pomnožimo s racionalnim brojem r dobivamo izraze za opće rješenje

$$a = 2nr, \quad b = (n^2-1)r, \quad c = (n^2+1)r \tag{1.13}$$

gdje su r i n racionalni brojevi. Preostaje pokazati da je y geometrijska sredina od x i z, tj.

$$y^2 = xz.$$

Prema (1.12) to možemo pisati kao

$$y^2 = (y + a^2)(y - b^2)$$

što se svede na

$$y^2 = \frac{a^2 b^2}{a^2 - b^2}.$$

Iz (1.12) još slijedi

$$x = \frac{a^4}{a^2 - b^2}, \quad z = \frac{b^4}{a^2 - b^2}.$$

Da bi našli općenito rješenje moramo zamijeniti vrijednosti (1.13) za a, b i c. Kako su nam rješenja pozitivni cijeli brojevi tražimo stranice Pitagorinog trokuta u kojemu je $a > b$. Za $b = 3$, $a = 4$, $c = 5$ imamo

$$x = \frac{256}{7}, \quad y = \frac{144}{7}, \quad z = \frac{81}{7}.$$

Poglavlje 2

Fermatovo doba

2.1 Marin Mersenne (1588. - 1648.)

Marin Mersenne je bio francuski teolog, matematičar i teoretičar glazbe. Za matematiku je posebno značajan zbog dopisivanja sa svim važnim matematičarima svoga doba (kojih je bilo vrlo malo u to vrijeme), čime je omogućena razmjena ideja u doba u koje nisu postojali mnogi drugi načini komunikacije. Sam nije imao mnogo matematičkih postignuća, no znao ih je prepoznati kod drugih matematičara.

Savršeni i Mersennovi brojevi.

Mersenne je najpoznatiji po tome što je pokušao naći sve savršene brojeve.

Definicija 2.1.1. *Pozitivan cijeli broj n je* savršen *ako se može zapisati kao zbroj svih svojih pozitivnih djelitelja ne uključujući n.*

Primjer savršenih brojeva su $6 = 1+2+3$ i $28 = 1+2+4+7+14$ koji su bili poznati još i Pitagorejcima. Pretpostavlja se da su svi savršeni brojevi parni iako nikada nije dokazano da ne postoji neparni savršen broj.

Ako nam $\sigma(n)$ označava zbroj svih pozitivnih djelitelja broja n, onda je zbroj pozitivnih brojeva manjih od n dana sa $\sigma(n) - n$. Dakle, uvjet "n je savršen" se svodi na jednakost $\sigma(n) - n = n$, tj.

$$\sigma(n) = 2n.$$

Na primjer, imamo

$$\sigma(6) = 1 + 2 + 3 + 6 = 2 \cdot 6$$

i

$$\sigma(28) = 1 + 2 + 4 + 7 + 14 + 28 = 2 \cdot 28.$$

Teorem 2.1.2. *Paran broj n je savršen ako i samo ako se može prikazati u obliku* $n = 2^{k-1}(2^k - 1)$*, pri čemu je* $2^k - 1$ *prost broj.*

Dokaz. Neka je $n = 2^{k-1}(2^k - 1)$, gdje je $2^k - 1$ prost. Izravno slijedi

$$\sigma(2^{k-1}) = 1 + 2 + 4 + \ldots + 2^{k-1} = \frac{2^{k-1+1} - 1}{2 - 1} = 2^k - 1$$

te

$$\sigma(2^k - 1) = 1 + 2^k - 1 = 2^k.$$

Kako su 2^{k-1} i $2^k - 1$ relativno prosti, multiplikativnost funkcije σ povlači

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

pa je broj n savršen.

Obratno, neka je n savršen. Zapišimo ga u obliku $n = 2^k \cdot m$, gdje je $k \geq 0$ i m neparan. Kako je $\sigma(n) = 2n$ dobivamo

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

Iz prethodnih jednakosti zaključujemo da je $2^{k+1} - 1$ dijeli $2^{k+1} \cdot m$. Kako su 2^{k+1} i $2^{k+1} - 1$ relativno prosti, $2^{k+1} - 1$ dijeli m. Zapišimo sada m u obliku $m = (2^{k+1} - 1)m'$.
Dobivamo da je

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

te

$$n = (2^{k+1} - 1)2^k m'$$

Preostaje dokazati da je $m' = 1$ i da je $2^{k+1} - 1$ prost broj. Ako je $m' \neq 1$, slijedi $\sigma(m) \geq 1 + m' + m$. No vidjeli smo da je

$$\sigma(m) = 2^{k+1}m' = (2^{k+1} - 1)m' + m' = m + m' < 1 + m' + m.$$

Prema tome, $m' = 1$ te $m = 2^{k+1} - 1$. S druge strane, $\sigma(m) = m + m' = m + 1$ pa je m (tj. $2^{k+1} - 1$) prost broj. □

Dokaz ovog teorema prvi je dao Leonhard Euler.

Definicija 2.1.3. *Brojevi oblika* $M_n = 2^n - 1$*,* $n \geq 1$*, se nazivaju* Mersennovi brojevi. *Mersennove brojeve koji su prosti nazivamo* Mersennovim prostim brojevima.

Neki Mersennovi brojevi su prosti naprimjer $M_7 = 127$, a neki su složeni, kao npr. $M_{11} = 2047$. Hipoteza je da Mersennovih brojeva koji su prosti ima beskonačno mnogo. Najveći poznat Mersennov broj je $M_{43112609}$. To je ujedno i danas najveći poznati prosti broj.

Propozicija 2.1.4. *Ako je Mersennov broj M_n prost, tada je i n prost broj.*

Dokaz. Ako je broj n složen, tada ga možemo zapisati u obliku $n = kl$, za neke prirodne brojeve k, l koja su oba veća od 1. Tada je

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

te je M_n djeljiv s $2^l - 1$, dakle M_n je složen. □

2.2 Pierre de Fermat (1601. - 1665.)

Pierre de Fermat je bio francuski matematičar i pravnik. Za njega kažemo da je uz Descartesa bio jedan od najznačajnijih matematičara 17. stoljeća. Vjeruje se da nije objavio niti jedan od svojih radova, već je to napravio njegov sin Samuel nakon očeve smrti. Unatoč njegovoj skromnosti, Fermat je stekao veliki ugled za svoja matematička postignuća. Postavio je temelje teorije vjerojatnosti te ga se smatra začetnikom infinitezimalnog računa. Bavio se i analitičkom geometrijom i algebrom, no unatoč tome, Fermat je najviše volio teoriju brojeva. Vraćao se problemima iz teorije brojeva u svakom svoj radu, volio je pronalaziti nove probleme, ali i davati odgovore na stare. Fermat niti jedan od svojih teorema nije dokazao što je pravdao time da su dokazi predugi i da ih nema gdje zapisati. Na žalost, Fermatovi suvremenici nikad nisu zahtjevali dokaze Fermatovih teorema. To je pridonijelo činjenici da ga se nazove ”princom matematičara amatera”.

Fermatova metoda faktorizacije

Fermatova metoda faktorizacije je jedna od najučinkovitijih metoda faktorizacije. Nađena je u pismu bez datuma najvjerojatnije poslanog Mersenneu. Metoda je utemeljena na sljedećem:
Ako broj n možemo napisati kao razliku između dva kvadrata onda n ima očitu faktorizaciju $n = x^2 - y^2 = (x - y)(x + y)$.

Teorem 2.2.1. *Svaki prirodni neparni broj n možemo zapisati kao razliku dva kvadrata.*

Dokaz. Kada je $n = a \cdot b, b \geq a$ onda je $n = x^2 - y^2$, pri čemu je $x = \frac{a+b}{2}$, $y = \frac{a-b}{2}$. Ako su a i b bliski brojevi, onda je y malo manji, a x malo veći od $\sqrt{n}$. Znamo da je n neparan. Iz toga slijedi da su a i b neparni i x i y su cijeli brojevi. Možemo pisati $x^2 = n + y^2$. Pošto

je $x^2 \geq n$, slijedi da je $x \geq \sqrt{n}$. Postupak se sastoji od uzastopnog mijenjanja vrijednosti broja x koji su veći od $\sqrt{n}$ i provjeravanja je li $\Delta(x) = x^2 - n$ jednak y^2. □

Metodu je najbolje ilustrirati na primjeru.

Primjer 2.2.2. *Faktoriziraj* $n = 13837$.

$\sqrt{n}$ leži između 117 i 118.
$\Delta(118) = 118^2 - 13837 = 87$ što nije kvadrat.
$\Delta(119) = 119^2 - 13837 = 324 = 18^2$.
Našli smo faktorizaciju $13837 = (119 - 18)(119 + 18) = 101 \cdot 137$

Teorem 2.2.3. *Svaki prost broj oblika* $4n + 1$ *može se pokazati kao zbroj kvadrata dvaju cijelih brojeva.*

Ovaj teorem je još poznat pod imenom Fermatov teorem o kvadratima. Dokazao ga je Euler 1749. godine, Lagrange 1775. godine, koristeći kvadratne forme, te Dedekind 1877. godine.

Dokaz. Dokaz je ovdje zapisan kod Teorema 4.2.24. □

Fermatovi brojevi

Fermatovi prosti brojevi su brojevi oblika $F_n = 2^{2^n} + 1$, za $n \in \mathbb{N}_0$. Posebnost Fermatovih brojeva je ta da oni zadovoljavaju nekoliko rekurzivnih relacija koje se mogu dokazati matematičkom indukcijom. Ovdje navodim njih par bez dokaza. Dokaz relacija se može pronaći u [2].

1. $F_n = (F_{n-1} - 1)^2 + 1$
2. $F_n = F_{n-1} + 2^{2n-1} F_0 F_1 \cdots F_{n-2}$
3. $F_n = F_{n-1}^2 - 2(F_{n-2} - 1)^2$
4. $F_n = F_0 F_1 \cdots F_{n-1} + 2$.

Fermat je pretpostavio da su svi brojevi tog oblika prosti. Ako pogledamo redom brojeve vidimo da je prvih pet zaista prosto. $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$, no već F_5 nije prost. To je dokazao Euler 1732. godine.
Pogledajmo kratak dokaz:

$$\begin{aligned} F_5 &= 2^{32} + 1 \\ &= 2^4 \cdot 2^{28} + 1 \\ &= (641 - 5^4) \cdot 2^{28} + 1 \\ &= 641 \cdot 2^{28} - (5 \cdot 2^{7^4}) + 1 \\ &= 641 \cdot 2^{28} - (641 - 1)^4 + 1 \\ &= 641 \cdot (2^{28} - 641^3 + 4 \cdot 641^2 - 6 \cdot 641^2 - 6 \cdot 641 + 4) \end{aligned}$$

Dakle, F_5 je složen broj jer je djeljiv sa 641.
Fermatovi brojevi su naizgled izgubili važnost, no novi problem je taj da se pokaže da postoji konačan broj Fermatovih brojeva koji jesu prosti. Gauss je sveo problem traženja svih pravilnih poligona koji se mogu konstruirati ravnalom i šestarom na problem postojanja Fermatovih prostih brojeva.

Teorem 2.2.4. *Neka su $i, j \in \mathbb{Z}$, $i, j \geq 0$. Ako je $i \neq j$, onda je $(F_i, F_j) = 1$.*

Dokaz. Bez smanjenja općenitosti možemo pretpostaviti kako je $i > j$. Prema četvrtoj relaciji s početka potpoglavlja, vrijedi $F_i = F_0 \cdots F_j \cdots F_{i-2} + 2$. Kako $(F_i, F_j) \mid F_i$ i $(F_i, F_j) \mid F_0 \cdots F_j \cdots F_{i-2}$, slijedi $(F_i, F_j) \mid 2$. Kako su po definiciji svi Fermatovi brojevi neparni, slijedi $(F_i, F_j) = 1$. □

Fermatov mali teorem

Teorem 2.2.5. *Ako je p prost broj, onda je $a^p - a$ djeljiv s p za bilo koji cijeli broj a.*

Dokaz ovog teorema se temelji na činjenici da ako je p prost broj, onda je binomni koeficijent $\binom{p}{k}$ dijeljiv s p za $k = 1, 2, \ldots, p-1$ gdje je

$$\binom{p}{k} = \frac{p(p-1)(p-2)\cdots(p-k+1)}{1 \cdot 2 \cdot 3 \cdots k}.$$

Iz definicije od $\binom{p}{k}$ imamo

$$1 \cdot 2 \cdot 3 \cdots k \binom{p}{k} = p(p-1)(p-2)\cdots(p-k+1).$$

Ovdje p dijeli desnu stranu, dakle mora dijeliti i lijevu. Očito je da produkt $1 \cdot 2 \cdot 3 \cdots k$ ne može biti djeljiv s p jer su svi faktori manji od p. Zaključujemo da onda p mora dijeliti $\binom{p}{k}$

Dokaz. Teorem ćemo dokazati matematičkom indukcijom.
1. Baza indukcije. Kada je $p = 2$ teorem se da provjeriti jednostavno. Imamo $a^p - a = a^2 - a = a(a-1)$, gdje su a i $a-1$ uzastopni brojevi. Znamo da jedan od njih mora biti djeljiv s 2, dakle cijeli umnožak je djeljiv s 2.
Činjenica da je $a^p - a$ dijeljiv s bilo kojim prostim brojem p koristi indukciju broja a. Ako je $a = 0$ ili 1, onda je vrijednost broja $a^p - a$ jednaka nuli, što je djeljivo s p. Dakle, moramo pretpostaviti da je $a > 1$.
2. Pretpostavka indukcije. Pretpostavimo da teorem vrijedi za a.
3. Korak indukcije.

$$(a+1)^p = a^p + \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + \cdots + \binom{p}{p-1}a + 1.$$

Sređivanjem izraza dobivamo

$$(a+1)^p - a^p - 1 = \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + \cdots + \binom{p}{p-1}a.$$

Kako p dijeli svaki binomni koeficijent s desne strane, mora dijeliti i cijelu desnu stranu. Dakle, zaključujemo da p dijeli i $(a+1)^p - a^p - 1$. Ova činjenica i početna pretpostavka da p dijeli $a^p - a$ nas vodi do zaključka da p dijeli

$$[(a+1)^p - a^p - 1] + (a^p - a) = (a+1)^p - (a+1).$$

U slučaju da je a negativan cijeli broj, dokaz je jednostavan. Uzmimo da je $a = -b$, $b > 0$ pa slijedi

$$a^p - a = (-b)^p - (-b) = -(b^p - b).$$

Kako je b pozitivan, već znamo da p dijeli $b^p - b$. □

Fermatova metoda neprekidnog silaska

Glavna metoda kojom je Fermat dokazivao teže teoreme je metoda neprekidnog silaska. Nažalost, Fermat većinu svojih dokaza nije zapisivao na papir već ih je prenosio usmeno. Smatra se kako je on vjerovao u svoju metodu više nego u ispisivanje detalja dokaza. Metodu opisuje na sljedeći način.
Pretpostavimo da postoji pozitivan cijeli broj n koji ima svojstvo P. Moguće je pretpostaviti da postoji još neki pozitivan broj $n_1 < n$ tako da n_1 ima to isto svojstvo P. Istim postupkom možemo zaključiti da postoji još neki broj $n_2 < n_1$ koji također ima to svojstvo. Postupak bi mogli ponavljati u beskonačnost, no to je nemoguće s obzirom da postoji konačan broj pozitivnih cijelih brojeva koji su manji od danog broja n. Zaključujemo da ne postoji niti jedan pozitivan cijeli broj koji sadrži svojstvo P. Metodu je lakše shvatiti ako pogledamo sljedeći primjer.

Primjer 2.2.6. *Pokažimo da je* $\sqrt{2}$ *iracionalan broj.*

Pretpostavimo suprotno, $\sqrt{2}$ je racionalan i može se zapisati kao $\sqrt{2} = \frac{a}{b}$, gdje su a, b pozitivni cijeli brojevi. Sada izraz

$$\sqrt{2} + 1 = \frac{1}{\sqrt{2} - 1}$$

implicira

$$\frac{a}{b} + 1 = \frac{1}{\frac{a}{b} - 1} = \frac{b}{a - b},$$

pa imamo

$$\sqrt{2} = \frac{a}{b} = \frac{b}{a - b} - 1 = \frac{2b - a}{a - b} = \frac{a_1}{b_1},$$

pri čemu nam je $a_1 = 2b - a$ i $b_1 = a - b$. Kako je $1 < \sqrt{2} < 2$, tj. $1 < \frac{a}{b} < 2$, možemo množiti nejednakost s b kako bi dobili $b < a < 2b$. Sada implikacija $0 < 2b - a = a_1$, dok je $2b < 2a$ daje

$$a_1 = 2b - a < a.$$

Počeli smo s $\sqrt{2} = \frac{a}{b}$, a završili s $\sqrt{2} = \frac{a_1}{b_1}$, gdje je $0 < a_1 < a$. Ako cijeli postupak ponovimo dobit ćemo $\sqrt{2} = \frac{a_2}{b_2}$ pri čemu je a_2 pozitivan cijeli broj manji od a_1. Nastavljajući postupak dobit ćemo niz $a_1, a_2, a_3, \cdots$ takav da je

$$a > a_1 > a_2 \cdots > 0.$$

Ovo je, naravno, nemoguće. Pozitivni cijeli brojevi se ne mogu beskonačno smanjivati. Dobiveno povlači da je početna pretpostavka pogrešna, $\sqrt{2}$ se ne može napisati kao razlomak. Zaključujemo da je $\sqrt{2}$ iracionalan broj.

Fermatov posljednji teorem

Fermatov posljednji teorem poznat kao i Fermatov veliki teorem je jedan od najpoznatijih teorema u povijesti matematike. Teorem se, prije nego što je dokazan, nalazio u Guinessovoj knjizi rekorda kao najteži matematički problem na svijetu. Prvi uspješan i potpun dokaz ovog teorema dao je Andrew Wiles tek 1994. godine, nakon 358 godina truda brojnih matematičara. Wilesov je dokaz, prema mnogima najveći matematički rezultat prethodnog stoljeća, ohrabrio matematičare da se uhvate u koštac s mnogim drugim velikim neriješenim matematičkim problemima. Ipak, teško da će išta uspjeti zamijeniti Fermatov poslijednji teorem. S obzirom da dokaz teorema uključuje teoriju grupa i vrlo je složen, ovdje je naveden samo teorem bez dokaza.

Teorem 2.2.7. *Ne postoje tri pozitivna cijela broja a, b, c za koje vrijedi* $a^n + b^n = c^n$ *za bilo koji prirodni broj* $n > 2$.

Poglavlje 3

Eulerovo doba

3.1 Leonhard Euler (1707. - 1783.)

Leondard Euler je matematičar koji je doprinio mnogim područjima matematike, uključujući teoriju brojeva. Bio je švicarski matematičar, no većinu života je proveo u Rusiji. Njegov matematički talent zapazio je Johann Bernoulli koji ga je i matematički poučavao. Euler je prvi matematičar koji je zapazio da se teorija brojeva može proučavati metodama matematičke analize i time je postao osnivač analitičke teorije brojeva. Euler je jedan od najplodonosnijih matemtičara u povijesti, napisao je čak preko 700 radova.

Teorija kongruencija predstavlja naslijeđe "Princa matematike", Carl Friedricha Gaussa. On je ovu tehniku, poznatu i pod nazivom modularna aritmetika, zasnovao u svom djelu *Disquisitiones Arithmeticae*, objavljenom 1801. Spomenuta knjiga se sastojala od sedam poglavlja, od kojih je prvih šest bilo posvećeno teoriji brojeva. Iako Gauss kronološki dolazi nakon Eulera, ovdje su spomenuti najbitniji pojmovi vezani uz teoriju kongruencija. Ti pojmovi su nam korisni za dokaze bitnih Eulerovih postignuća.

Kongruencije

Definicija 3.1.1. *Ako cijeli broj $n \neq 0$ dijeli razliku $a-b$, onda kažemo da je a* kongruentan *b* modulo *n i pišemo $a \equiv b \pmod{n}$. U protivnom, kažemo da a nije kongruentan b modulo n i pišemo $a \not\equiv b \pmod{n}$.*

Propozicija 3.1.2. *Neka je n prirodan broj. Biti kongruentan modulo n je relacija ekvivalencije na skupu $\mathbb{Z}$.*

Dokaz. Najprije treba pokazati da je a kongruentno b modulo n ako i samo ako a i b daju isti ostatak pri djeljenju s n.

Pretpostavimo da je a kongruentno b modulo n te korištenjem Teorema o dijeljenju s ostatkom napišimo $a = q_1 \cdot n + r_1$ i $b = q_2 \cdot n + r_2$, pri čemu vrijedi $0 \leq r_1, r_2 \leq n-1$. Sada je $a - b = (q_1 - q_2)n + r_1 - r_2$. Kako n dijeli $a - b$, dobivamo da n dijeli i $r_1 - r_2$ te iz

$$-n + 1 \leq r_1 - r_2 \leq n - 1$$

slijedi

$$r_1 - r_2 = 0, \quad tj. \quad r_1 = r_2.$$

S druge strane, ako a i b daju isti ostatak pri djeljenju s n, analogno slijedi da n dijeli $a - b$, tj. $a \equiv a \pmod{n}$. Iz dokazanog sada očito slijedi $a \equiv a \pmod{n}$. Također, kako $n \mid a - b$ ako i samo ako $n \mid b - a$, vrijedi i $a \equiv b \pmod{n}$ ako i samo ako $b \equiv a \pmod{n}$.
Neka su sada a, b i c cijeli brojevi i neka vrijedi $a \equiv b \pmod{n}$ i $b \equiv c \pmod{n}$. Iz toga zaključujemo kako a i b te b i c daju isti ostatak pri dijeljenju s n pa je $a \equiv c \pmod{n}$. □

U idućoj propoziciji su navedena osnovna svojstva kongruencija.

Propozicija 3.1.3. *Neka su a, a', b, b' i c cijeli brojevi te n prirodan broj.*

1. *Ako je $a \equiv a' \pmod{n}$ i $b \equiv b' \pmod{n}$, tada vrijedi i*

$$\begin{aligned} a + b &\equiv a' + b' \pmod{n}, \\ a - b &\equiv a' - b' \pmod{n} \ te \\ a \cdot b &\equiv a' \cdot b' \pmod{n}. \end{aligned}$$

2. *Neka su a i n relativno prosti. Ako je $ab \equiv ac \pmod{n}$, tada vrijedi i $b \equiv c \pmod{n}$.*

Dokaz. 1. Dokazati ćemo treću tvrdnju, prve dvije se mogu dokazati analogno. Prema uvjetima propozicije, postoje cijeli brojevi m' i m takvi da je $a - a' = mn$ i $b - b' = m'n$. Odavde slijedi

$$ab - a'b' = ab - ab' + ab' - a'b' = a(b - b') + (a - a')b' = am'n + b'm'n.$$

Dakle, n dijeli $ab - a'b'$ pa je $ab \equiv a'b' \pmod{n}$.

2. Kako su a i n relativno prosti, prema Teoremu 1.3.6. postoje brojevi x i y takvi da je $ax + ny = 1$. Iz kongruencije $ab \equiv ac \pmod{n}$ slijedi da postoji cijeli broj k takav da je $a(b - c) = nk$. Množenjem prethodne jednakosti s x, iz $ax = 1 - ny$ dobivamo

$$(b - c) - ny(b - c) = nkx.$$

Sada je očito da n dijeli $b - c$ pa je $b \equiv c \pmod{n}$.

□

Primijetimo kako tvrdnja 2. ne vrijedi općenito, tj. ukoliko cijeli brojevi a i n nisu relativno prosti.

Teorem 3.1.4. *Vrijedi:* $ax \equiv ay \pmod{m}$ *ako i samo ako* $x \equiv y \pmod{\frac{m}{(a,m)}}$. *Specijalno, ako je* $ax \equiv ay \pmod{m}$ *i* $(a, m) = 1$, *onda je* $x \equiv y \pmod{m}$.

Dokaz. Dokaz Teorema 3.1.4. može se naći u [3, str. 13, Teorem 2.4.]. □

Definicija 3.1.5. *Neka je* $n \in \mathbb{N}$, $n > 1$. *Skup* $S = \{a_1, a_2, \ldots, a_n\}$ *se naziva* potpuni sustav ostataka modulo n *ako za svaki* $b \in \mathbb{Z}$ *postoji jedinstveni* $a_i \in S$ *za koji vrijedi* $b \equiv a_i \pmod{n}$.

Možemo primijetiti kako svaki potpuni sustav ostataka modulo n ima točno n elemenata. Također i svaki n-teročlani skup koji se sastoji od cijelih brojeva koji su međusobno kongruentni modulo n predstavlja potpuni sustav ostataka modulo n.

Lema 3.1.6. *Neka su a i n prirodni brojevi. Ako su a i n relativno prosti, tada konvergencija* $ax \equiv b \pmod{n}$ *ima jedinstveno rješenje modulo n, tj. ako je* $S = \{a_1, a_2, \ldots, a_n\}$ *potpun sustav ostataka modulo n tada postoji jedinstveni* $a_i \in S$ *takav da je* $x \equiv a_i \pmod{n}$ *rješenje polazne konvergencije.*

Dokaz. Kako su a i n relativno prosti, možemo naći brojeve k, l za koje vrijedi $ak + nl = 1$. Iz toga slijedi $akb + nkb = b$. Sada je očito $akb \equiv b \pmod{n}$ pa je $x = kb$ rješenje polazne kongruencije.
Neka su sada x_1 i x_2 rješenja polazne kongruencije. Kako je $ax_1 \equiv b \pmod{n}$ i $ax_2 \equiv b \pmod{n}$ dobivamo $ax_1 \equiv ax_2 \pmod{n}$. Primjenom Propozicije 3.1.3. dobivamo $x_1 \equiv x_2 \pmod{n}$ što je i trebalo pokazati. □

Lema 3.1.7. *Neka je* $\{x_1, \ldots, x_m\}$ *potpun sustav ostataka modulo m, te neka je* $(a, m) = 1$. *Tada je* $\{ax_1, \ldots, ax_m\}$

Dokaz. Dovoljno je dokazati kako $ax_i \not\equiv ax_j \pmod{m}$ za $i \neq j$. Pretpostavimo da je $ax_i \equiv ax_j \pmod{m}$. Tada Teorem 3.1.4. povlači da je $x_i \equiv x_j \pmod{m}$, tj. $i = j$. □

Eulerova funkcija

Definicija 3.1.8. *Neka je n prirodan broj. Broj prirodnih brojeva u nizu* $1, 2, \ldots, n$ *koji su relativno prosti s n se označava s* $\varphi(n)$*; ovim je definirana funkcija* $\varphi : \mathbb{N} \to \mathbb{N}$ *koja se naziva* Eulerova funkcija.

Primijetimo kako je $\varphi(n)$ upravo broj elemenata reduciranog sustava ostataka modulo n te dalje reducirani sustav ostataka možemo zapisati u obliku $\left\{a_1, a_2, \ldots, a_{\varphi(n)}\right\}$.

Primjer 3.1.9. *Na primjer,* $\varphi(5) = 4$, $\varphi(6) = 2$ *i* $\varphi(1) = 1$. *Ako je* p *prost broj onda je* $\varphi(p) = p - 1$. *Na primjer,* $\varphi(7) = 6$. *Također, ako za neki prirodan broj* n *vrijedi* $\varphi(n) = n - 1$, *zaključujemo kako je* n *relativno prost sa svakim prirodnim brojem koji je manji od njega. Prema tome,* n *mora biti prost broj.*

Lema 3.1.10. *Neka je* $S = \left\{a_1, a_2, \ldots, a_{\varphi(n)}\right\}$ *reducirani sustav ostataka modulo* n. *Tada je i* $\left\{b \cdot a_1, b \cdot a_2, \ldots, b \cdot a_{\varphi(n)}\right\}$ *reducirani sustav ostataka modulo* n, *za svaki broj* b *za koji vrijedi* $(b, n) = 1$.

Dokaz. Direktno iz Leme 3.1.7. i Teorema 1.3.10. □

Teorem 3.1.11. ***Eulerov teorem.*** *Neka je* a *cijeli broj te* n *prirodan broj. Ako su brojevi* a *i* n *relativno prosti, tada je* $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Dokaz. Neka je $S = \left\{a_1, a_2, \ldots, a_{\varphi(n)}\right\}$ reducirani sustav ostataka modulo n. Prema Lemi 3.1.10. je tada i skup $\left\{a \cdot a_1, a \cdot a_2, \cdots, a \cdot a_{\varphi(n)}\right\}$ reducirani skup ostataka modulo n. Prema tome, za svaki a_i, $1 \leq i \leq \varphi(n)$, postoji jedinstveni $a_j \in S$ takav da je $a_i \equiv a \cdot a_j \pmod{n}$. Primjenom Propozicije 3.1.3. (1) dobivamo

$$a_1 \cdot a_2 \cdots a_{\varphi(n)} \equiv aa_1 \cdot aa_2 \cdots aa_{\varphi(n)} \pmod{n},$$

tj.

$$a_1 \cdot a_2 \cdots a_{\varphi(n)} \equiv a^{\varphi(n)} a_1 \cdot a_2 \cdots a_{\varphi(n)} \pmod{n}.$$

Kako je $(a_i, n) = 1$ za sve $a_i \in S$, uzastopnom primjenom propozicije 3.1.3. (2) dobivamo $1 \equiv a^{\varphi(n)} \pmod{n}$, čime je teorem dokazan. □

Ako je p prost broj i a cijeli broj koji nije djeljiv s p, tada su a i p relativno prosti. Euler je dokazao Mali Fermatov teorem upravo zato što je on izravna posljedica Eulerovog teorema.

Teorem 3.1.12. ***Mali Fermatov teorem.*** *Neka je* p *prost broj i* a *cijeli broj. Tada je* $a^p \equiv a \pmod{p}$. *Ako* p *ne dijeli* a, *vrijedi i* $a^{p-1} \equiv 1 \pmod{p}$.

Dokaz. Očito je $\varphi(p) = p - 1$, pa tvrdnja slijedi iz Eulerovog teorema. □

Lema 3.1.13. *Neka je* p *prost broj i* $k \in \mathbb{N}$. *Tada je* $\varphi(p^k) = p^k - p^{k-1}$.

Dokaz. Neka je $1 \leq n \leq p^k$. Ako p ne dijeli n, tada su n i p^k relativno prosti. Prema tome, jedini brojevi u nizu $1, 2, \ldots, p^k$ koji nisu relativno prosti s p^k su $p, 2p, 3p, \ldots, p^k = p^{k-1} \cdot p$ (tj. ima ih p^{k-1}). Odavde slijedi $\varphi(p^k) = p^k - p^{k-1}$. □

Pokažimo da je Eulerova funkcija i multiplikativna. Prije dokaza nam je potreban sljedeći teorem.

Teorem 3.1.14. ***Kineski teorem o ostatcima.*** *Neka su m i n relativno prosti prirodni brojevi. Tada za svaki par cijelih brojeva a i b postoji jedinstveno, modulo mn, rješenje sustava kongruencija $x \equiv a \pmod{m}$, $x \equiv b \pmod{n}$.*

Dokaz. Ovdje imamo sustav dvije kongruencije s jednom nepoznanice. Promatramo preslikavanje

$$i : \{0, 1, \ldots, mn-1\} \to \{0, 1, \ldots, m-1\} \times \{0, 1, \ldots, n-1\}$$

dano s $i(t) = (t \bmod m, t \bmod n)$. Da bi dokazali lemu dovoljno je dokazati da je preslikavanje i bijekcija. Kako skupovi $\{0, 1, \ldots, mn-1\}$ i $\{0, 1, \ldots, m-1\} \times \{0, 1, \ldots, n-1\}$ imaju jednaki broj elemenata, potrebno je pokazati da je preslikavanje i injekcija.
Neka su $t_1, t_2 \in \{0, 1, \ldots, mn-1\}$ takvi da je $i(t_1) = i(t_2)$. Tada je $t_1 \equiv t_2 \pmod{m}$ i $t_1 \equiv t_2 \pmod{n}$. Drugim riječima $m \mid t_1 - t_2$ i $n \mid t_1 - t_2$. Kako su m i n relativno prosti zaključujemo $mn \mid t_1 - t_2$ te zbog $-mn+1 \leq t_1 - t_2 \leq mn-1$ vrijedi $t_1 = t_2$. Zaključujemo, i je injekcija. □

Kinezi su se ovim rezultatom koristili primjenom na probleme iz svakodnevnog života. Ovaj teorem je prvenstveno korišten u vojne svrhe prilikom prebrojavanja preživjelih vojnika nakon bitke. Vojnici bi se postrojili u redove po 3, 4, 5, 7, 11 vojnika, a potom bi se pomoću broja vojnika preostalih u zadnjem redu dobio sustav kongruencija. Rješavanje takvog sustava bi rezultiralo točnim brojem preživjelih vojnika.

Teorem 3.1.15. *Eulerova funkcija je multiplikativna.*

Dokaz. Već smo vidjeli da je $\varphi(1) = 1$. Neka su sada m, n relativno prosti cijeli brojevi. Definiramo skupove

$$\begin{aligned} S_1 &= \{a \in \mathbb{N} : a \leq mn, (a, mn) = 1\}, \\ S_2 &= \{a \in \mathbb{N} : a \leq m, (a, m) = 1\}, \\ S_3 &= \{a \in \mathbb{N} : a \leq n, (a, n) = 1\}. \end{aligned}$$

Očito je $|S_1| = \varphi(mn)$, $|S_2| = \varphi(m)$ te $|S_3| = \varphi(n)$. Za $t \in \{0, 1, \ldots, mn-1\}$, neka je $i(t) = (a, b)$, gdje je i preslikavanje definirano u dokazu Kineskog teorema o ostatcima. Primijetimo da je $(t, mn) = 1$ ako i samo ako je $(a, m) = (b, n) = 1$. Kako je $t = k_1 m + a = k_2 n + b$, slijedi da je svaki zajednički prost djelitelj brojeva t i m (tj. t i n) ujedno i zajednički prost djelitelj brojeva a i m (b i n). Prema tome, restrikcija preslikavanja i na skup S_1 daje bijekciju skupa S_1 na skup $S_2 \times S_3$ što povlači $\varphi(mn) = \varphi(m)\varphi(n)$. □

Eulerova metoda faktorizacije

Eulerova metoda faktorizacije je tehnika faktoriziranja broja zapisivanjem tog broja kao zbroja dva kvadrata i to na dva različita načina. Na primjer, broj 1000009 se može zapisati kao $1000^2 + 3^2$ ili kao $972^2 + 235^2$. Eulerova metoda nam daje faktorizaciju $1000009 =$

$293 \cdot 3413$. Ova metoda je bolja od Fermatove metode za one cijele brojeve čiji faktori nisu blizu i čak učinkovitija od faktorizacije djeljenjem, pod uvjetom da se može naći reprezentacija početnog broja kao zbroja dva kvadrata.

Veliki nedostatak Eulerove metode je taj da se ne može primijeniti na cijeli broj koji ima prosti faktor oblika $4k+3$ na neku neparnu potenciju, jer se takav broj ne može zapisati kao kvadrat. Čak su i neparni složeni brojevi oblika 4k+1 često umnožak dva prosta broja oblika $4k + 3$ pa se ova metoda ne može koristiti.

Za prikaz ove metode koristit ćemo Teorem 2.2.3. i Brahmagupta - Fibonacci identitet.
Brahmagupta - Fibonacci identitet:

1. $(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2$
2. $(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2$.

Sada prijeđimo na samo metodu. Zapišimo broj n kao $n = a^2 + b^2 = c^2 + d^2$. Prvo zaključujemo da vrijedi $a^2 - c^2 = d^2 - b^2$. Kada sredimo tu jednakost dobivamo

$$(a - c)(a + c) = (d - b)(d + b). \tag{3.1}$$

Neka je $k = (a-c, d-b)$ i $h = (a+c, d+b)$ tako da postoje neke konstante l, m, l', m' za koje vrijedi $(a - c) = kl$, $(d - b) = km$, $(a + c) = hm'$ i $(d + b) = hl'$. Najveći zajednički djelitelj od l i m je 1 i najveći zajednički djelitelj od l' i m' je 1. Ako ove jednakosti uvrstimo u (3.1) dobivamo

$$klhm' = kmhl'.$$

Kada prethodnu jednakost podijelimo s kh dobivamo

$$lm' = l'm.$$

Koristeći činjenicu da su (l, m) i (l', m') parovi relativno prostih brojeva dolazimo do zaključka da je $l = l'$ i $m = m'$. Dakle, $(a - c) = kl$, $(d - b) = km$, $(a + c) = hm$ i $(d + b) = hl$. Vidimo sada da je $m = (a + c, d - b)$ i $l = (a - c, d + b)$.

$$\begin{aligned}
(k^2 + h^2)(l^2 + m^2) &= (kl - hm)^2 + (km + hl)^2 \\
&= ((a - c) - (a + c))^2 + ((d - b) + (d + b))^2 \\
&= (2c)^2 + (2d)^2 \\
&= 4n. \\
(k^2 + h^2)(l^2 + m^2) &= (kl + hm)^2 + (km - hl)^2 \\
&= ((a - c) + (a + c))^2 + ((d - b) - (d + b))^2 \\
&= (2a)^2 + (2b)^2 \\
&= 4n.
\end{aligned}$$

Kako je svaki faktor zbroj dva kvadrata, jedan od njih mora sadržavati oba parna broja: ili su to (k,h) ili (l,m). Bez smanjenja općenitosti pretpostavimo da je (k,h) takav par brojeva. Faktorizacija je tada oblika

$$n = \left(\left(\frac{k}{2}\right)^2 + \left(\frac{h}{2}\right)^2\right)\left(l^2 + m^2\right).$$

Pogledajmo sada metodu na početnom primjeru.

Primjer 3.1.16. *Faktoriziraj 1000009.*

Kako je $100009 = 1000^2 + 3^2 = 972^2 + 235^2$ imamo

$a = 1000$	$a - c = 28$	$(a-c, d-b) = k = 4$
$b = 3$	$a + c = 1972$	$(a+c, d+b) = h = 34$
$c = 972$	$d - b = 232$	$l = 7$
$d = 235$	$d + b = 238$	$m = 58$

Dakle,

$$\begin{aligned} 1000009 &= \left[\left(\frac{4}{2}\right)^2 + \left(\frac{34}{2}\right)^2\right] \cdot \left(7^2 + 58^2\right) \\ &= \left(2^2 + 17^2\right) \cdot \left(7^2 + 58^2\right) \\ &= (4 + 289) \cdot (49 + 3364) \\ &= 293 \cdot 3413 \end{aligned}$$

3.2 Christian Goldbach (1690. - 1764.)

Christian Goldbach je bio njemački matematičar i pravnik. Studirao je na sveučilištu Royal Albertus University. Nakon studija je putovao po Europi gdje je susreo mnoge matematičare kao što su Gottfried Leibniz, Leonhard Euler i Nicholas Bernoulli. Bavio se teorijom brojeva, ali i matematičkom analizom. Danas je najpoznatiji po takozvanoj "Goldbachovoj slutnji" koju je zapisao u pismu Euleru 1742. godine.

Goldbachova slutnja

Goldbachova slutnja je jedan od najstarijih i najpoznatijih problema u teoriji brojeva, ali i u ostalim granama matematike. Potječe iz pisma Euleru 7. lipnja 1742. godine. Ona govori:

Svaki cijeli broj veći od dva koji se može zapisati kao zbroj dva prosta broja se može zapisati kao zbroj proizvoljno mnogo cijelih brojeva.

U marginama pisma napisao je još jednu slutnju koja govori:

Svaki cijeli broj veći od 2 se može zapisati kao zbroj tri prosta broja.

Danas znamo da su ove dvije tvrdnje ekvivalentne iako se u ono vrijeme to nije tako činilo. Bitno je napomenuti da je Goldbach smatrao da je 1 prost broj. Moderni i konačan zapis ove slutnje je:

Svaki cijeli broj veći od dva se može zapisati kao zbroj dva prosta broja.

Slutnja je pokazana kao ispravna za brojeve do 4×10^{18}, no teorem nije dokazan u općenitom slučaju. Čak je i Euler izjavio da smatra tvrdnju točnom, no kako ju ne zna dokazati.

Definicija 3.2.1. *Goldbachov broj je pozitivan cijeli broj koji se može prikazati kao zbroj dva neparna prosta broja.*

Ovo je vidimo još jedan oblik Goldbachove slutnje koja kaže da su svi parni brojevi veći od 4 Goldbachovi brojevi.

Poglavlje 4

Lagrangeovo doba

4.1 Joseph Louis Lagrange (1736. - 1813.)

Joseph-Louis Lagrange je bio talijanski matematičar i astronom koji je živio u doba prosvjetiteljstva. Napravio je znatne doprinose na polju matematičke analize i teorije brojeva. Lagrange je s 19 godina postao je profesor matematike na artiljerijskoj školi u Torinu te je poznat po svojoj izjavi: "Da sam bogat, nikada se ne bih bavio matematikom." Leonhard Euler je prepoznao njegov talent te je često pregledavao njegove radove. Veliki dio Lagrangeovog doprinosa teoriji brojeva su dokazi već poznatih teorema.

Wilsonov i Lagrangeov teorem

Definicija 4.1.1. *Neka je p prost broj i $a < p$, prirodan. Tada postoji prirodan broj b za kojeg vrijedi $a \cdot b \equiv 1 \pmod{p}$ i takav broj b se naziva* multiplikativni inverz od a modulo p.

Zaista, kako su a i p relativno prosti prema Teoremu 1.3.6. postoje cijeli brojevi x, y za koje vrijedi $ax + py = 1$. Slijedi, $ax \equiv 1 \pmod{p}$ te možemo uzeti $b = x$. Možemo primijetiti kako iz Leme 3.1.6. slijedi da su svaka dva multiplikativna inverza od a modulo p međusobno kongruentni modulo p, pa postoji jedinstveni multiplikativni inverz od a modulo p koji je prirodan broj manji od p.
Općenito ako je a prirodan broj i p ne dijeli a, tada postoji multiplikativni inverz od a modulo p. Najistaknutija primjena multiplikativnih inverza pojavljuje se prilikom evaluacije produkta $(p-1)! = 1 \cdot 2 \cdot 3 \cdots (p-1)$ modulo p, pri čemu je p prost broj. O tome nam više govori sljedeći teorem engleskog matematičara Johna Wilsona. Wilsonov teorem je jedan od poznatijih teorema iz teorije brojeva. Ovaj teorem je dokazan tek 1771. godine od strane Lagrangea. Vrlo je bitan jer za razliku od Fermatovog malog teorema, vrijedi i njegov obrat te nam tako daje nužan i dovoljan uvijet da bi broj bio prost.

Teorem 4.1.2. ***Wilsonov teorem.*** *Ako je p prost broj tada je* $(p-1)! \equiv -1 \pmod{p}$.

Dokaz. Prema prethodnoj diskusiji, za svaki broj $1, 2, \ldots, p-1$ postoji multiplikativni inverz modulo p. Dakle, svaki od faktora u $(p-1)! = 1 \cdot 2 \cdots (p-1)$ daje 1 modulo p u umnošku sa svojim multiplikativnim inverzom, osim faktora koji su sami sebi inverzni. Odredimo sada takve faktore.
Neka je $x \in \{1, 2, \ldots, p-1\}$ takav da vrijedi $x^2 \equiv 1 \pmod{p}$. Tada $p \mid x^2-1 = (x-1)(x+1)$. Kako je p prost i $1 \leq x \leq p-1$, slijedi da je ili $x-1 = 0$ ili $x+1 = p$. Dakle, jedini faktori u $(p-1)!$ koji su sami sebi inverzni su 1 i $p-1$. Iz toga dobivamo $(p-1)! \equiv 1 \cdot (p-1) \pmod{p}$ te $(p-1)! \equiv -1 \pmod{p}$. □

Pogledajmo sada obrat Wilsonovog teorema.

Teorem 4.1.3. *Ako prirodan broj n zadovoljava* $(n-1)! \equiv -1 \pmod{n}$*, tada je on prost.*

Dokaz. Iz $(n-1)! \equiv -1 \pmod{n}$ slijedi $(n-1)! \equiv -1 \pmod{m}$ za svaki m koji dijeli n. Ako $m < n$, tada se m pojavljuje kao faktor od $(n-1)!$ pa je $(n-1)! \equiv 0 \pmod{m}$ i $-1 \equiv 0 \pmod{m}$. Iz ovoga slijedi da je $m = 1$ te n nema pozitivnih djelitelja različitih od 1. Slijedi, n je prost. □

Teorem 4.1.4. *Neka je p prost broj. Tada kongruencija $x^2 \equiv -1 \pmod{p}$ ima rješenja ako i samo ako je $p = 2$ ili $p \equiv 1 \pmod{4}$.*

Dokaz. Za $p = 2$ je $x = 1$ jedno rješenje. Ako je $p \equiv 1 \pmod{4}$, onda iz Wilsonovog teorema slijedi:

$$\left[1 \cdot 2 \cdots \frac{p-1}{2}\right] \cdot \left[(p-1)(p-2)\cdots\left(p - \frac{p-1}{2}\right)\right] \equiv \left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv -1 \pmod{p},$$

pa je $x = \left(\frac{p-1}{2}\right)!$ jedno rješenje.
Neka je $p \equiv 3 \pmod{4}$. Pretpostavimo da postoji $x \in \mathbb{Z}$ takav da je $x^2 \equiv -1 \pmod{p}$. Tada je $x^{p-1} \equiv (-1)^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ što je kontradikcija s malim Fermatovim teoremom. □

Teorem 4.1.5. ***Lagrangeov teorem.*** *Ako je p prost broj i $P(x)$ polinom stupnja n s cjelobrojnim koeficijentima koji nisu djeljivi s p, tada kongruencija $P(x) \equiv 0 \pmod{p}$ ima najviše n rješenja modulo p.*

Dokaz. Dokaz se provodi indukcijom po stupnju polinoma $P(x)$. Ako je stupanj polinoma 1, tvrdnja teorema slijedi iz Leme 3.1.6. Pretpostavimo kako tvrdnja vrijedi za polinome stupnja manjeg od n i neka je $P(x)$ polinom stupnja n. Ako kongruencija $P(x) \equiv 0 \pmod{p}$ nema rješenja, tada nemamo što dokazivati. Nasuprot, pretpostavimo kako je $P(x_0) \equiv 0 \pmod{p}$, za neki cijeli broj x_0 te neka je

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0,$$

gdje su $a_0, a_1, \ldots, a_n$ cijeli brojevi. Odavde slijedi da je $P(x) \equiv P(x) - P(x_0) \pmod{p}$, tj.

$$P(x) \equiv a_n(x^n - x_0^n) + a_{n-1}(x^{n-1} - x_0^{n-1}) + \ldots + a_1(x - x_0) \pmod{p}.$$

Kako za $k \in \mathbb{N}$ vrijedi

$$x^k - x_0^k = (x - x_0)(x^{k-1} + x^{k-2}x_0 + \ldots + xx_0^{k-2} + x_0^{k-1}),$$

desnu stranu možemo zapisati kao $(x - x_0)Q(x)$, pri čemu je $Q(x)$ polinom stupnja $n - 1$ s cjelobrojnim koeficijentima.
Kako je p prost, kongruencija $P(x) \equiv 0 \pmod{p}$ pokazuje kako je $x - x_0 \equiv 0 \pmod{p}$ ili $Q(x) \equiv 0 \pmod{p}$. Prema pretpostavci indukcije kongruencija $Q(x) \equiv 0 \pmod{p}$ ima najviše $n - 1$ rješenja pa kongruencija $P(x) \equiv 0 \pmod{p}$ ima najviše n rješenja što je i trebalo pokazati. □

Pellove jednadžbe

Definicija 4.1.6. *Neka je d prirodan broj koji nije potpuni kvadrat. Diofantska jednadžba oblika $x^2 - dy^2 = 1$ naziva se* Pellova jednadžba*. Jednadžba oblika $x^2 - dy^2 = N$, pri čemu je N cijeli broj naziva se* pellovska jednadžba*.*

Pellova jednadžba pripada među najstarije i najvažnije diofantske jednadžbe drugog reda. Jedini suparnik joj je bila Pitagorina jednadžba koja je ovdje spomenuta u prvom poglavlju. Pellova jednadžba je poznata još od antike gdje je korištena za aproksimaciju broja $\sqrt{2}$. Spomenuta jednadžba je dobila ime nakon Eulerovog susreta s Wallisovim djelom *Opera Mathematica* koji je zabunom proglasio Johna Pella kao osobu koja se prva bavila ovakvim tipom jednadžbi. Do danas ne postoje dokazi da se John Pell ikada bavio ovakvim tipom jednadžbi. Posljednji koji se prije Eulera bavio ovakvim jednadžbama je Fermat.

Teorem 4.1.7. ***Dirichletov teorem o aproksimaciji.*** *Za svaki iracionalni broj oblika $\sqrt{n}$ i prirodan broj B postoje cijeli brojevi a i b, $0 < b < B$ takvi da je*

$$|a - b\sqrt{n}| < \frac{1}{B}.$$

Dokaz. Neka je prirodan broj B proizvoljan i fiksiran. Promotrimo $B - 1$ brojeva $\sqrt{n}, 2\sqrt{n}, \ldots, (B-1)\sqrt{n}$. Za svaki $k \in \{1, 2, \ldots, B-1\}$ odaberemo broj A_k takav da je $0 \leq A_k - k\sqrt{n} \leq 1$.
Kako je $\sqrt{n}$ iracionalan, niti jedan od brojeva $A_k - k\sqrt{n}$ ne može biti jednak 0 ili 1. Također za $k_1 \neq k_2$ vrijedi $A_{k_1} - k_1\sqrt{n} \neq A_{k_2} - k_2\sqrt{n}$ (jer bi u suprotnom vrijedilo $\sqrt{n} = \frac{A_{k_1} - A_{k_2}}{k_2 - k_1}$). Dakle, u segmentu $[0, 1]$ imamo $B + 1$ različitih brojeva

$$0, A_1 - \sqrt{n}, A_2 - 2\sqrt{n}, ..., A_{B-1} - (B-1)\sqrt{n}, 1.$$

Podijelimo li spomenuti segment na B podintervala duljine $\frac{1}{B}$ prema Dirichletovom principu barem jedan od tih podintervala sadrži bar dva navedena broja. Neka su to $A_i - i\sqrt{n}$ i $A_j - j\sqrt{n}$, $i \neq j$. Tada je $|A_i - i\sqrt{n} - A_j + j\sqrt{n}| < \frac{1}{B}$ te za $a = A_i - A_j$ i $b = j - i$ vrijedi $|a - b\sqrt{n}| < \frac{1}{B}$. Iz $1 \leq i \leq j \leq B - 1$ slijedi $0 < b < B$. □

Ovaj teorem ima nekoliko bitnih posljedica:

1. Kako prethodni teorem vrijedi za sve brojeve $B < 0$, možemo naći proizvoljno mali broj $\frac{1}{B}$, čime dobivamo nove vrijednosti za a i b. Dakle, postoji beskonačno mnogo parova cijelih brojeva (a, b) takvih da vrijedi $|a - b\sqrt{n}| < \frac{1}{B}$. Iz $0 < b < B$ slijedi $|a - b\sqrt{n}| < \frac{1}{b}$.

2. Očito vrijedi $|a + b\sqrt{n}| \leq |a - b\sqrt{n}| + |2b\sqrt{n}| \leq |3b\sqrt{n}|$ i $|a^2 - b^2 n| \leq \frac{1}{b} \cdot 3b\sqrt{n} = 3\sqrt{n}$. Prema tome možemo pronaći beskonačno mnogo cijelih brojeva (a, b) takvih da vrijedi $|a^2 - nb^2| \leq 3\sqrt{n}$. Posebno, postoji beskonačno mnogo parova prirodnih brojeva (a_i, b_i) takvih da je $a_i^2 - nb_i^2 = N$, za neki prirodan broj N, pri čemu je $N < 3\sqrt{n}$.

3. Postoje različiti parovi (a_1, b_1) i (a_2, b_2) za koje vrijedi $a_1^2 - nb_1^2 = a_2^2 - nb_2^2 = N$, $a_1 \equiv a_2 \pmod{N}$ i $b_1 \equiv b_2 \pmod{N}$.

Iz ovoga se može dokazati egzistencija rješenja Pellove jednadžbe.

Teorem 4.1.8. *Neka je $n \in \mathbb{N}$ i n nije potpun kvadrat. Tada Pellova jednadžba $x^2 - dy^2 = 1$ ima rješenja u prirodnim brojevima $(x, y) \neq (1, 0)$.*

Dokaz. Neka je $a - b\sqrt{n}$ kvocijent brojeva $a_1 - b_1\sqrt{n}$ i $a_2 - b_2\sqrt{n}$ dobivenih prije iskaza teorema. Tada je

$$a - b\sqrt{n} = \frac{a_1 - b_1\sqrt{n}}{a_2 - b_2\sqrt{n}} = \frac{(a_1 - b_1\sqrt{n})(a_2 + b_2\sqrt{n})}{a_2^2 - nb_2^2} = \frac{a_1a_2 - nb_1b_2}{N} + \frac{a_1b_2 - b_1a_2}{N}\sqrt{n}.$$

Očito je $a - b\sqrt{n} \neq \pm 1$.
Kako N dijeli $a_1^2 - nb_1^2$, dobivamo $a_1^2 - nb_1^2 \equiv 0 \pmod{N}$, odakle iz $a_1 \equiv a_2 \pmod{N}$ i $b_1 \equiv b_2 \pmod{N}$ slijedi $a_1a_2 - nb_1b_2 \equiv 0 \pmod{N}$. Na isti način je i $a_1b_2 - b_1a_2 \equiv 0 \pmod{N}$ pa su $\frac{a_1a_2 - nb_1b_2}{N}$ i $\frac{a_1b_2 - b_1a_2}{N}$ cijeli brojevi. Korištenjem $a_1^2 - nb_1^2 = a_2^2 - nb_2^2 = N$ dobivamo $a^2 - nb^2 = 1$ pa je (a, b) traženo rješenje. □

Rješenje Pellove jednadžbe (x_1, x_2) u prirodnim brojevima nazivamo najmanjim netrivijalnim rješenjem ako za svako drugo rješenje (x_2, y_2) vrijedi $x_1 < x_2$. U tom slučaju će vrijediti i $y_1 < y_2$ te $x_1 + \sqrt{n}y_1 < x_2 + \sqrt{n}y_2$. Takvo najmanje netrivijalno rješenje najčešće nije jednostavno naći, no njegova važnost leži u tome što ono odmah daje beskonačno mnogo rješenja.

Propozicija 4.1.9. ***Brahmaguptino kompozicijsko pravilo.*** *Ako su* (x_1, y_1) *i* (x_2, y_2) *rješenja Pellove jednadžbe* $x^2 - ny^2 = 1$*, tada je i* $(x_3, y_3) = (x_1x_2 + ny_1y_2, x_1y_2 + x_2y_1)$ *također rješenje.*

Dokaz. Vrijedi $(x_1 + \sqrt{n}y_1)(x_2 + \sqrt{n}y_2) = x_1x_2 + ny_1y_2 + \sqrt{n}(x_1y_2 + x_2y_1)$. Kako su (x_1, y_1),(x_2, y_2) rješenja Pellove jednadžbe očito je $(x_1^2 - ny_1^2)(x_2^2 - ny_2^2) = 1$.
Sada imamo

$$\begin{aligned} 1 &= (x_1 - \sqrt{n}y_1)(x_1 + \sqrt{n}y_1)(x_2 - \sqrt{n}y_2)(x_2 + \sqrt{n}y_2) \\ &= (x_1 - \sqrt{n}y_1)(x_2 - \sqrt{n}y_2)(x_1 + \sqrt{n}y_1)(x_2 + \sqrt{n}y_2) \\ &= (x_1x_2 + ny_1y_2 - \sqrt{n}(x_1y_2 + x_2y_1))(x_1x_2 + ny_1y_2 + \sqrt{n}(x_1y_2 + x_2y_1)) \\ &= (x_1x_2 + ny_1y_2)^2 - n(x_1y_2 + x_2y_1)^2 \\ &= x_3^2 - ny_3^2 \end{aligned}$$

pa je i par (x_3, y_3) rješenje Pellove jednadžbe. □

Netrivijalna rješenja Pellove jednadžbe najlakše se mogu odrediti korištenjem razvoja broja $\sqrt{n}$ u verižni razlomak.

Definicija 4.1.10. *Za beskonačni verižni razlomak* $[a_1, a_2, \ldots]$ *kažemo da je* periodski *ako postoje prirodni brojevi* k *i* m *takvi da je* $a_{m+n} = a_n$ *za svaki* $n \geq k$*. Najmanji takav broj* m *nazivamo* periodom *verižnog razlomka* $[a_1, a_2, \ldots]$ *te pišemo*

$$[a_1, a_2, \ldots] = [a_1, a_2, \ldots, a_{k-1}, \overline{a_k, a_{k+1}, \ldots, a_{k+m-1}}].$$

Pogledajmo sada algoritam za određivanje razvoja u jednostavni verižni razlomak:

1. Najprije odredimo a_1, $a_1 = \lfloor \sqrt{n} \rfloor$, te neka je $s_1 = a_1$ i $t_1 = n - s_1^2$.
2. U idućem koraku stavimo $\alpha_1 = \frac{s_1 + \sqrt{n}}{t_1}$.
3. U svakom sljedećem koraku uzmemo $a_i = \lfloor \alpha_{i-1} \rfloor$, $s_i = a_i t_{i-1} - s_{i-1}$ te $t_i = \frac{n - s_i^2}{t_{i-1}}$.
4. Nakon toga $\alpha_i = \frac{s_i + \sqrt{n}}{t_i}$.

Možemo primijetiti kako je razvoj periodski ako postoje brojevi $i, j \in \mathbb{N}$, $i \neq j$, takvi da je $(s_i, t_i) = (s_j, t_j)$. Može se pokazati kako vrijedi nejednakost $t_i < s_j + \sqrt{n} < 2\sqrt{n}$, iz koje slijedi kako brojevi s_i, t_i mogu poprimiti konačan broj vrijednosti.

Definicija 4.1.11. *Iracionalni broj* α *zovemo* kvadratna iracionalnost *ako je* α *korijen kvadratne jednadžbe s racionalnim koeficijentima.*

Teorem 4.1.12. ***Euler, Lagrange.*** *Iracionalan broj α ima periodski razvoj u jednostavni verižni razlomak ako i samo ako je α kvadratna iracionalnost.*

Dokaz. Periodičnost zapisa će slijediti isto kao i u slučaju razvoja drugog korijena iz prirodnog broja koji nije potpun kvadrat. Pogledajmo sada koja je veza periodskih zapisa i kvadratnih iracionalnosti.
Neka je $\alpha = [a_1, a_2, \ldots, a_k, \overline{a_{k+1}, \ldots, a_{k+m-1}}]$ razvoj iracionalnog broja α u periodski verižni razlomak. Pokažimo da je α kvadratna iracionalnost. Neka je sada $\beta = [\overline{a_{k+1}, \ldots, a_{k+m-1}}]$. Sada vrijedi

$$\beta = a_{k+1} + \cfrac{1}{\ddots + \cfrac{1}{a_{k+m-1} + \frac{1}{\beta}}},$$

odakle dobivamo da postoje cijeli brojevi a, b, a', b' takvi da je

$$\beta = \frac{a\beta + b}{a'\beta + b'},$$

što daje kvadratnu jednadžbu za β. Dakle, β je kvadratna iracionalnost i njen oblik je $\beta = \frac{c+\sqrt{d}}{e}$. S obzirom da je $\alpha = [a_1, a_2, \ldots, a_k, \beta]$ izravno slijedi da je i α kvadratna iracionalnost. Prema tome, α je oblika $\frac{c'+\sqrt{d'}}{e'}$ za $d' \in \mathbb{N}$ koji nije potpun kvadrat. □

Teorem o četiri kvadrata

Teorem 4.1.13. ***Teorem o četiri kvadrata.*** *Svaki prirodan broj n se može prikazati u obliku zbroja kvadrata četiri cijela broja:*

$$n = x^2 + y^2 + z^2 + w^2, x, y, z, w \in \mathbb{Z}.$$

Dokaz. Uočimo da vrijedi

$$\begin{aligned}(x^2 + y^2 + z^2 + w^2)(a^2 + b^2 + c^2 + d^2) = (ax + by + cz + dw)^2 + (ay - bx + dz - cw)^2 \\ + (az - cx + bw - dy)^2 + (aw - dx + cy - bz)^2.\end{aligned} \tag{4.1}$$

Stoga je tvrdnju teorema dovoljno provjeriti samo za proste brojeve. Očito je da 2 možemo zapisati kao $2 = 1^2 + 1^2 + 0^2 + 0^2$, pa pretpostavimo da je p neparan.
Promotrimo brojeve oblika

$$0^2, 1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2. \tag{4.2}$$

Nikoja dva broja nisu kongruentna modulo p. Isto vrijedi i za

$$-1-0^2, -1-1^2, -1-2^2, \ldots, -1-\left(\frac{p-1}{2}\right)^2. \tag{4.3}$$

U (4.2) i (4.3) imamo ukupno $p+1$ brojeva. Po Dirichletovom principu, dva među njima moraju dati isti ostatak pri dijeljenju s p. To znači da možemo pronaći cijele brojeve x i y takve da je $x^2 \equiv -1-y^2 \pmod{p}$ i vrijedi $x^2+y^2+1 < 1+2\cdot\left(\frac{p}{2}\right)^2 < p^2$. Dakle, dobili smo da je $mp = x^2+y^2+1$ za neki cijeli broj m, $0 < m < p$.
Neka je sada l najmanji prirodan broj takav da je $lp = x^2+y^2+z^2+w^2$ za neke $x, y, z, w \in \mathbb{Z}$. Tada je $l \leq m < p$. Dalje, l je neparan. Naime, kada bi l bio paran, onda bi među brojevima x, y, z, w imali parno mnogo neparnih brojeva. U tom slučaju mogli bi pretpostaviti da su brojevi $x+y$, $x-y$, $z+w$, $z-w$ parni. Tada bi iz

$$\frac{1}{2}lp = \left(\frac{x+y}{2}\right)^2 + \left(\frac{x-y}{2}\right)^2 + \left(\frac{z+w}{2}\right)^2 + \left(\frac{xz-w}{2}\right)^2$$

dobili kontradikciju s činjenicom da je l najmanji prirodni broj za kojeg vrijedi gornja tvrdnja. Kako bi dokazali teorem potrebno je pokazati da je $l = 1$.
Pretpostavimo da je $l > 1$. Neka su x', y', z', w' najmanji ostatci po apsolutnoj vrijednosti pri dijeljenju brojeva x, y, z, w sa l, te neka je

$$n = x'^2 + y'^2 + z'^2 + w'^2.$$

Tada slijedi $n \equiv 0 \pmod{l}$ i $n > 0$, jer bi inače l dijelio p. Dalje, budući da je l neparan, imamo da je $n < 4\cdot\left(\frac{l}{2}\right)^2 = l^2$. Stoga je $n = kl$ za neki cijeli broj k, $0 < k < l$. Iz (4.1) slijedi da se broj $(kl)(lp)$ može pokazati kao zbroj kvadrata četiri cijela broja i čak svaki od tih kvadrata je djeljiv s l^2. Odavde slijedi da se broj kp može prikazati kao zbroj četiri kvadrata, no to je kontradikcija s minimalnošću od l. □

4.2 Johann Carl Friedrich Gauss (1777. - 1855.)

Johann Carl Friedrich Gauss je bio njemački matematičar najpoznatiji po tome da se još u osnovnoj školi iskazao iznenađujuće brzim zbrajanjem prirodnih brojeva od 1 do 100. Pridonio je otkriću zakona kvadratnog reciprociteta te teorema prostih brojeva. Poznat je i po tome što je prvi dokazao Osnovni teorem algebre, jedan od najbitnijih teorema u matematici. Pokušao je konstruirati pravilni sedmerokut pomoću ravnala i šestara. Ne samo da je došao do zaključka da je to nemoguće, već je otkrio metode konstrukcije pravilnog 17, 257, 65537 – terokuta. Tako je dokazao da je konstrukcija pravilnog mnogokuta, ravnalom i šestarom, moguća samo kada su stranice prosti brojevi serije 3, 5, 17, 257, 65537 i tako dalje. To je opisao u knjizi o teoriji brojeva, *Disqvisitiones Arithmeticae* (Pitanja o aritmetici, 1801.).

Kvadratni ostatci i kvadratni zakon reprociteta

Euler je bio prvi matematičar koji je izrekao zakon kvadratnog reprociteta, no nije ga znao dokazati. Izrekao ga je i Legendre, te ga je probao dokazati, no dokaz nije bio u potpunosti točan. Prvi koji ga je uspio ispravno dokazati bio je Gauss.

Definicija 4.2.1. *Neka je* $(a, m) = 1$. *Ako kongruencija* $x^2 \equiv a \pmod{m}$ *ima rješenja, onda kažemo da je* a kvadratni ostatak modulo m.

Primjer 4.2.2. *Kvadratni ostatci modulo 5 su 1 i 4, a neostatci su 2 i 3.*

Teorem 4.2.3. *Neka je* p *neparni prost broj. Reducirani sustav ostataka modulo* p *sastoji se od* $\frac{p-1}{2}$ *kvadratnih ostataka i* $\frac{p-1}{2}$ *kvadratnih neostataka.*

Dokaz. Dokaz Teorema 4.2.3. može se naći u [3, str. 29, Teorem 3.1.]. □

Definicija 4.2.4. *Neka je* p *neparan prost broj,* a *cijeli broj.* Legendrov simbol $\left(\frac{a}{p}\right)$ *je definiran sa*

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

U slučaju da su a i p relativno prosti brojevi, p neparan prost broj, po Malom Fermatovom teoremu vrijedi $a^{p-1} \equiv 1 \pmod{p}$. Ovu relaciju je iskoristio Euler kako bi dobio sljedeću formulu.

Teorem 4.2.5. ***Eulerov kriterij.*** *Ako je* p *neparan i prost broj, vrijedi* $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$. *Prema tome,* a *je kvadratni ostatak modulo* p *ako i samo ako je* $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

Dokaz. U slučaju da je $\left(\frac{a}{p}\right) = 0$, $p \mid a$ pa je tvrdnja zadovoljena. Ako je $\left(\frac{a}{p}\right) = 1$, onda je moguće pronaći $x_0 \in \mathbb{Z}$ takav da je $x_0^2 \equiv a \pmod{p}$. Sada iz Malog Fermatovog teorema slijedi $a^{\frac{p-1}{2}} \equiv x_0^{p-1} \equiv 1 \equiv \left(\frac{a}{p}\right) \pmod{p}$. Neka je $\left(\frac{a}{p}\right) = -1$ Za svaki $i \in \{1, \ldots, p-1\}$ odaberimo $j \in \{1, \ldots, p-1\}$ tako da je $i \cdot j \equiv a \pmod{p}$. Uočimo da je $i \neq j$, s obzirom da $x^2 \equiv a \pmod{p}$ nema rješenja. Dakle, skup $\{1, \ldots, p-1\}$ se raspada na $\frac{p-1}{2}$ parova (i, j) za koje vrijedi $i \cdot j \equiv a \pmod{p}$. Množenjem $\frac{p-1}{2}$ kongruencija i koristeći Wilsonov teorem dobivamo

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

□

Propozicija 4.2.6. *Za neparan prost broj* p *vrijedi*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{ako je } p \equiv 1 \pmod{4}, \\ -1, & \text{ako je } p \equiv 3 \pmod{4}. \end{cases}$$

Dokaz. Prema Eulerovom kriteriju imamo $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$. Ako je $p \equiv 1 \pmod 4$, tada je $\frac{p-1}{2}$ paran te slijedi $\left(\frac{-1}{p}\right) = 1$. Ako je $p \equiv 3 \pmod 4$, tada je $\left(\frac{p-1}{2}\right)$ neparan pa je $\left(\frac{-1}{p}\right) = -1$. □

Propozicija 4.2.7. *Za neparan prost broj p vrijedi*

$$\left(\frac{2}{p}\right) = \begin{cases} 1, \text{ ako je } p \equiv 1 \pmod 8 \text{ ili } p \equiv 7 \pmod 8, \\ -1, \text{ako je } p \equiv 3 \pmod 8 \text{ ili } p \equiv 5 \pmod 8. \end{cases}$$

Dokaz. Dokaz Propozicije 4.2.7. možemo naći u [6, str. 43, Teorem 4.1.5.] □

Teorem 4.2.8. ***Gaussova lema.*** *Neka je p neparan broj i $(a, p) = 1$. Promotrimo brojeve $a, 2a, 3a, \ldots, \frac{p-1}{2}a$ i njihove najmanje nenegativne ostatke pri dijeljenju s p. Označimo s n broj ostataka koji su veći od $\frac{p}{2}$. Tada je*

$$\left(\frac{a}{p}\right) = (-1)^n$$

Dokaz. Neka su $r_1, \ldots, r_n$ ostatci koji su veći od $\frac{p}{2}$ i $s_1, \ldots, s_k$ preostali ostatci. Brojevi $r_1, \ldots, r_n$ i $s_1, \ldots, s_k$ su međusobno različiti po Lemi 3.1.7. te niti jedan od njih nije 0. Dalje, $n + k = \frac{p-1}{2}$. Brojevi $p - r_i$ su međusobno različiti i $0 < p - r_i < \frac{p}{2}$, za $i = 1, \ldots, n$. Također niti jedan od $p - r_i$ nije jednak nekom s_j. Ako je $p - r_i = s_j$, onda je $r_i \equiv \alpha a \pmod p$, $s_j \equiv \beta a \pmod p$ za neke $1 \leq \alpha, \beta \leq \frac{p-1}{2}$, pa iz $a(\alpha + \beta) \equiv 0 \pmod p$ i $(a, p) = 1$ slijedi da je $\alpha + \beta \equiv 0 \pmod p$, što je nemoguće jer je $2 \leq \alpha + \beta \leq p - 1$.
Dakle, brojevi $p - r_i, \leq, p - r_n, s_1, \ldots, s_k$ su svi međusobno različiti, ima ih točno $\frac{p-1}{2}$ i elementi su skupa $\left\{1, \ldots, \frac{p-1}{2}\right\}$. Stoga su to upravo brojevi $1, 2, \ldots, \frac{p-1}{2}$ u nekom poretku. Množenjem dobivamo

$$(p - r_1) \cdots (p - r_n) s_1 \cdots s_k = 1 \cdot 2 \cdot \cdots \left(\frac{p-1}{2}\right).$$

Odavde je

$$1 \cdot 2 \cdots \frac{p-1}{2} \equiv (-r_1) \cdots (-r_n) s_1 \cdots s_k \equiv (-1)^n a \cdot 2a \cdot 3a \cdots \left(\frac{p-1}{2}\right) a \pmod p.$$

Sada ako skratimo ovu kongruenciju s $\left(\frac{p-1}{2}\right)!$, dobivamo $1 \equiv (-1)^n a^{\frac{p-1}{2}} \pmod p$ pa je po Eulerovom kriteriju

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

□

Teorem 4.2.9. *Ako je p neparan prost broj i $(a, 2p) = 1$, onda je $\left(\frac{a}{p}\right) = (-1)^t$, gdje je*

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

Također je

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

Drugim riječima p je kvadratni ostatak modulo p ako i samo ako je p oblika $8k \pm 1$.

Dokaz. Neka su r_i i s_i ostatci pri dijeljenju brojeva ja s p, $j = 1, \ldots, \frac{p-1}{2}$ definirani kao u dokazu prethodne leme. Kvocijenti pri tom dijeljenju su brojevi $\left\lfloor \frac{ja}{p} \right\rfloor$. Sada, ako je $(a, p) = 1$ onda imamo

$$\sum_{j=1}^{\frac{p-1}{2}} ja = \sum_{j=1}^{\frac{p-1}{2}} p \left\lfloor \frac{ja}{p} \right\rfloor + \sum_{i=1}^{n} r_i + \sum_{i=1}^{k} s_i,$$

te

$$\sum_{j=1}^{\frac{p-1}{2}} j = \sum_{i=1}^{n} (p - r_i) + \sum_{i=1}^{k} s_i = np - \sum_{i=1}^{n} r_i + \sum_{i=1}^{k} s_i.$$

Ako sada oduzmemo ova dva izraza dobivamo

$$(a-1) \sum_{j=1}^{\frac{p-1}{2}} j = p \left(\sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{ja}{p} \right\rfloor - n \right) + 2 \sum_{i=1}^{n} r_i.$$

Dalje imamo

$$\sum_{j=1}^{\frac{p-1}{2}} j = \frac{\frac{p-1}{2} \cdot \frac{p+1}{2}}{2} = \frac{p^2 - 1}{8},$$

pa slijedi

$$(a-1)\frac{p^2-1}{8} \equiv \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{ja}{p} \right\rfloor - n \pmod 2.$$

Ako je a neparan i $(a, 2p) = 1$ onda dobivamo da je $n \equiv \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{ja}{p} \right\rfloor \pmod 2$, a ako je $a = 2$ dobivamo $n \equiv \frac{p^2-1}{8} \pmod 2$ jer je $\left\lfloor \frac{2j}{p} \right\rfloor = 0$ za $j = 1, \ldots, \frac{p-1}{2}$. Sada tvrdnja teorema slijedi iz Gaussove leme. □

Teorem 4.2.10. ***Gaussov kvadratni zakon reprociteta.*** *Ako su p i q različiti neparni prosti brojevi, onda je*

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

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

Dokaz. Neka je

$$S = \left\{(x,y) : x, y \in \mathbb{Z},\ \ 1 \le x \le \frac{p-1}{2},\ \ 1 \le y \le \frac{q-1}{2}\right\}.$$

Skup S ima $\frac{p-1}{2} \cdot \frac{q-1}{2}$ članova. Dijelimo S na dva podskupa koja su disjunktna, S_1 i S_2 prema tome je li $qx > py$ ili je $qx < py$. Uočimo da ne može biti $qx = py$. Skup S_1 je skup svih parova (x,y) takvih da je $1 \le x \le \frac{p-1}{2}$ i $1 \le y < \frac{qx}{p}$. Takvih parova ima

$$\sum_{x=1}^{\frac{p-1}{2}} \left\lfloor \frac{qx}{p} \right\rfloor.$$

Slično, S_2 se sastoji od svih parova (x,y) takvih da je $1 \le y \le \frac{q-1}{2}$ i $1 \le x < \frac{px}{q}$, a takvih parova ima

$$\sum_{y=1}^{\frac{q-1}{2}} \left\lfloor \frac{py}{q} \right\rfloor.$$

Prema tome je

$$\sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{qj}{p} \right\rfloor + \sum_{j=1}^{\frac{q-1}{2}} \left\lfloor \frac{pj}{q} \right\rfloor = \frac{p-1}{2} \cdot \frac{q-1}{2},$$

pa je po Teoremu 4.2.9.

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

□

Napomena 4.2.11. *Ako su p i q različiti prosti brojevi koji nisu istovremeno kongruentni s 3 modulo 4, tada je $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$, dok je u protivnom $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$. Ovaj zakon često koristimo za računanje Legendreovog simbola.*

Gaussovi cijeli brojevi

Gaussovi cijeli brojeve predstavljaju proširenje skupa cijelih brojeva. Proširenje je uveo Gauss proučavajući diofantske jednadžbe oblika $x^2 + y^2 = n$ zbog toga što lijeva strana navedene jednadžbe omogućuje faktorizaciju. Skup Gaussovih cijelih brojeva posjeduje i brojna svojstva skupa cijelih brojeva koja omogućavaju primjenu na rješavanje različitih problema.

Definicija 4.2.12. Gaussovi cijeli brojevi *su kompleksni brojevi oblika $a + bi$, pri čemu su a i b cijeli brojevi. Skup Gausovih cijelih brojeva označava se sa* $\mathbb{Z}[i]$.

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}.$$

Možemo primijetiti kako je svaki cijeli broj također i Gaussov cijeli broj jer je $\mathbb{Z}[i]$ proširenje skupa cijelih brojeva. Svaki prirodan broj n koji se može prikazati u obliku zbroja kvadrata dva cijela broja x i y se može zapisati u obliku umnoška dva Gaussova cijela broja. Vrijedi $x^2 + y^2 = (x + yi)(x - yi)$.

Definicija 4.2.13. *Na skupu $\mathbb{Z}[i]$ definiramo* normu $N(\alpha)$, *za $\alpha = a + bi \in \mathbb{Z}[i]$ sa*

$$N(\alpha) = \alpha \cdot \overline{\alpha} = (a + bi)(a - bi) = a^2 + b^2.$$

$N(\alpha)$ je uvijek nenegativan i cijeli broj. On će biti jednak nuli ako i samo ako je $\alpha = 0$. Osnovno svojstvo norme je njena multiplikativnost.

Lema 4.2.14. *Za $\alpha, \beta \in \mathbb{Z}[i]$ vrijedi $N(\alpha \cdot \beta) = N(\alpha)N(\beta)$*

Dokaz. $N(\alpha \cdot \beta) = (\alpha \cdot \beta)(\overline{\alpha \cdot \beta}) = (\alpha \cdot \beta)(\overline{\alpha} \cdot \overline{\beta}) = (\alpha \cdot \overline{\alpha})(\beta \cdot \overline{\beta}) = N(\alpha)N(\beta)$. □

Iz ove leme slijedi i Diofantov identitet:

$$(a_1^2 + b_1^2)(a_2^2 + b_2^2) = (a_1a_2 - b_1b_2)^2 + (a_1b_2 + b_1a_2)^2. \tag{4.4}$$

Definicija 4.2.15. *Element $\alpha \in \mathbb{Z}[i]$ nazivamo* invertibilnim *ukoliko postoji $\beta \in \mathbb{Z}[i]$ takav da je $\alpha \cdot \beta = 1$. Takav element β, u slučaju da postoji, se označava s α^{-1}.*

Propozicija 4.2.16. *Gaussov cijeli broj α je invertibilan ako i samo ako mu je norma jednaka 1. Dakle, jedini invertibilni brojevi su* $1, -1, i, -i$.

Dokaz. Neka je $\alpha \in \mathbb{Z}[i]$ invertibilan. Sada je očito $\alpha \neq 0$. Tada postoji $\alpha^{-1} \in \mathbb{Z}[i]$ takav da je $\alpha \cdot \alpha^{-1} = 1$. Koristeći prethodnu lemu slijedi $N(\alpha)N(\alpha^{-1}) = 1$. Kako su $N(\alpha)$ i $N(\alpha^{-1})$ prirodni brojevi, slijedi $N(\alpha) = 1$. Ako je sada α cijeli broj čija je norma 1, tada je $\alpha \cdot \overline{\alpha} = N(\alpha) = 1$ pa slijedi da je α invertibilan. Ako je $\alpha = a + bi$ Gaussov cijeli broj norme 1, tada je $a^2 + b^2 = 1$. Sada možemo zaključiti da je $a, b \in \{0, 1, -1\}$, $a \neq b$ i $a \cdot b = 0$. Iz ovoga slijedi posljednja tvrdnja propozicije. □

Definicija 4.2.17. *Kažemo da Gaussov cijeli broj $\alpha \neq 0$* dijeli *Gaussov cijeli broj β ako postoji Gaussov cijeli broj γ takav da vrijedi $\beta = \alpha \cdot \gamma$.*

Definicija 4.2.18. *Gaussov cijeli broj je* prost *ako se ne može prikazati u obliku produkta Gaussovih cijelih brojeva manje norme.*

Propozicija 4.2.19. *Svaki Gaussov cijeli broj se može prikazati kao produkt prostih Gaussovih cijelih brojeva.*

Dokaz. Neka je α Gaussov cijeli broj. Ako je α prost, nemamo što dokazivati. Ako α nije prost, tada postoje $\beta, \gamma \in \mathbb{Z}[i]$, norme manje od α i to takvi da je $\alpha = \beta \cdot \gamma$. Ako β i γ oboje nisu prosti, na isti način ih prikažemo u obliku produkta Gaussovih cijelih brojeva manje norme. Kako su norme prirodni brojevi i smanjuju se u svakom koraku ovaj postopak mora stati. Time smo dobili traženu faktorizaciju od α. □

Preostaje ispitati je li ovakva faktorizacija jedinstvena. U slučaju prirodnih brojeva znamo da vrijedi Osnovni teorem aritmetike. Faktorizacija u $\mathbb{Z}[i]$ je jedinstvena do na poredak faktora i množenje faktora invertibilnim elementima. Osim toga, najveći zajednički djelitelj Gaussovih cijelih brojeva α i β je svaki Gaussov cijeli broj γ sa svojstvom da iz $\delta \mid \alpha$ i $\delta \mid \beta$ slijedi $\delta \mid \gamma$. Ukoliko je $\gamma = (\alpha, \beta)$ direktno iz definicije slijedi da su $-\gamma$, $i \cdot \gamma$ i $(-i) \cdot \gamma$ također najveći zajednički djelitelji od α i β. Za dokaz jedinstvenosti nam je potreban sljedeći teorem, koji je ujedno i analogon Teorema o dijeljenju s ostatkom za Gaussove cijele brojeve.

Teorem 4.2.20. *Za $\alpha, \beta \in \mathbb{Z}[i]$, $\beta \neq 0$ postoje γ, $\delta \in \mathbb{Z}[i]$ takvi da je $\alpha = \gamma \cdot \beta + \delta$ te $N(\delta) < N(\beta)$.*

Dokaz. Gaussov cijeli broj γ definiramo kao najbolju aproksimaciju kompleksnog razlomka $\frac{\alpha}{\beta}$ koji je dobiven zaokruživanjem realnog i imaginarnog dijela na najbliži cijeli broj. Posebno 0.5 na 1 i -0.5 na 0. Sada definiramo $\delta = \alpha - \beta \cdot \gamma$. Primijetimo da je $\frac{\alpha}{\beta} - \gamma = x + yi$, gdje je $|x|, |y| \leq \frac{1}{2}$. Iz definicije od δ slijedi $N(\delta) = N(\alpha - \beta \cdot \gamma) = N(\frac{\alpha}{\beta} - \gamma)N(\beta)$, pa je $\frac{N(\delta)}{N(\beta)} = N(\frac{\alpha}{\beta} - \gamma) = N(x + yi) = x^2 + y^2 \leq \frac{1}{2}$. Odavde je

$$N(\delta) \leq \frac{N(\beta)}{2} < N(\beta).$$

□

Korištenjem ovog teorema možemo dobiti Euklidov algoritam za Gaussove cijele brojeve.

Propozicija 4.2.21. *Prost prirodan broj p je prost Gaussov cijeli broj ako i samo ako p nije zbroj dva kvadrata.*

Dokaz. Ako je p oblika $p = a^2 + b^2$, za neke a i b iz $\mathbb{Z}$, tada je $p = (a - bi)(a + bi)$. Kako je $N(a \pm bi) = p < N(p) = p^2$, p nije prost Gaussov cijeli broj. Neka je sada p prost prirodan broj koji nije prost u $\mathbb{Z}[i]$. Tada postoji faktorizacija $p = (a+bi)\gamma$, gdje su $a+bi$ i γ Gaussovi cijeli brojevi norme manje od p^2. Konjugiranjem dobivamo $p = (a - bi)\overline{\gamma}$. Množenjem prethodinih izraza dobivamo $p^2 = (a^2 + b^2)N(\gamma)$. Kako su $a^2 + b^2$ i $N(\gamma)$ prirodni brojevi koji su veći od 1, a p prost, slijedi $p = a^2 + b^2$. □

Propozicija 4.2.22. *Svaki prost Gaussov cijeli broj je oblika $a + bi$, gdje je $a \cdot b \neq 0$, je djelitelj prostog prirodnog broja p oblika $a^2 + b^2$.*

Dokaz. Ako je $a + bi$ prost Gaussov cijeli broj, tada je i $a - bi$ prost. Dalje, $(a + bi)(a - bi)$ je jedinstven rastav od $p = a^2 + b^2 = (a + bi)(a - bi)$ u produkt prostih Gaussovih cijelih brojeva. U slučaju da p nije prost, postoji i rastav $p = rs$, r, $s \in \mathbb{N}$, $1 < r$, $s < p$, što nije moguće. Na taj način bi dobili još neki rastav u produkt Gaussovih cijelih brojeva što nije moguće zbog jedinstvenosti rastava na proste Gaussove cijele brojeve. □

Korištenjem Gaussovih cijelih brojeva možemo komentirati prikaze prirodnih brojeva u obliku $x^2 + y^2$. Ukoliko je p prost i prirodan broj oblika $4k + 3$, korištenjem kongruencija modulo 4 može se vidjeti kako se p ne može prikazati u obliku zbroja dva kvadrata. Preostaje pogledati što možemo reći za proste brojeve oblika $4k + 1$. Korištenjem Guassovih otkrića dolazimo do vrlo jednostavnih dokaza problema poznatih još i Babiloncima.

Lema 4.2.23. ***Lagrange.*** *Prost broj $p \in \mathbb{N}$ oblika $4k + 1$ dijeli $n^2 + 1$ za neki cijeli broj n.*

Dokaz. Ovaj teorem ćemo dokazati primjenom Wilsonova teorema.

$$\begin{aligned}
-1 &\equiv (p-1)! \pmod{p} \\
&\equiv 1 \cdot 2 \cdot 3 \cdots 4k \pmod{p} \\
&\equiv (1 \cdot 2 \cdots 2k)((2k+1) \cdot (2k+2) \cdots 4k) \pmod{p} \\
&\equiv (1 \cdot 2 \cdots 2k)((-2k) \cdot (-2k-1) \cdots (-1)) \pmod{p} \\
&\equiv (1 \cdot 2 \cdots 2k)^2(-1)^{2k} \pmod{p} \\
&\equiv (1 \cdot 2 \cdots 2k)^2 \pmod{p}.
\end{aligned}$$

U slučaju $n = (2k)!$, dobivamo $n^2 \equiv -1 \pmod{p}$ pa p dijeli $n^2 + 1$. □

Teorem 4.2.24. ***Fermat.*** *Svaki prosti broj oblika $4k + 1$ se može prikazati u obliku zbroja kvadrata dvaju cijelih brojeva.*

Dokaz. Neka je $n \in \mathbb{Z}$ takav da p dijeli $n^2 + 1$. Prethodna lema nam osigurava pronalazak takvog broja n. Znamo da u $\mathbb{Z}[i]$ vrijedi $n^2 + 1 = (n - i)(n + i)$.
Iako p dijeli $n^2 + 1$, p ne dijeli niti jedan od faktora $n - i$, $n + i$ jer $\frac{n}{p} - \frac{i}{p}$ i $\frac{n}{p} + \frac{i}{p}$ nisu Gaussovi cijeli brojevi. U tom slučaju p tada nije prost Gaussov cijeli broj. Sada Propozicija 4.2.21. pokazuje da je p oblika $p = a^2 + b^2$ za neke cijele brojeve a i b. □

Teorem 4.2.25. *Prirodan broj n može se prikazati u obliku zbroja kvadrata dvaju cijelih brojeva ako i samo ako se svaki prost faktor oblika* $4k + 3$ *u rastavu od n pojavljuje s parnom potencijom.*

Dokaz. Najprije neka je $n = x^2 + y^2$ te $p \in \mathbb{N}$ je prost faktor od n oblika $4k + 3$. Tada je $x^2 \equiv -y^2 \pmod{p}$. Pretpostavimo da p ne dijeli y, tada je Legendreov simbol $\left(\frac{-y^2}{p}\right)$ jednak 1 te i $\left(\frac{-1}{p}\right) = 1$. To nije moguće prema Propoziciji 4.2.6. Prema tome, $p \mid y$ pa $p^2 \mid x^2 + y^2 = n$. Dijeljenjem s p^2 dobivamo

$$\left(\frac{x}{p}\right)^2 + \left(\frac{y}{p}\right)^2 = \frac{n}{p^2}$$

te induktivno slijedi da se p pojavljuje u rastavu broja n na proste faktore i to one s parnom potencijom.
Sada pretpostavimo kako se svaki prost broj oblika $4k + 3$ u rastavu od n pojavljuje s parnom potencijom. Dakle, n možemo zapisati kao $n = p_1 p_2 \cdots p_l n_1^2$, gdje su $p_1, p_2, \ldots, p_l$ međusobno različiti prosti brojevi. Najviše jedan od tih prostih brojeva je jednak 2, a za ostale vrijedi $p_i \equiv 1 \pmod{4}$. Iz Teorema 4.2.24. i $2 = 1^2 + 1^2$ slijedi da se svaki od prostih brojeva $p_1, p_2, \ldots, p_l$ može prikazati u obliku zbroja kvadrata dvaju cijelih brojeva pa iz Diofantova identiteta (4.4) slijedi da se i broj n može prikazati kao zbroj kvadrata dva cijela broja. □

Poglavlje 5

Legendreovo doba

5.1 Adrien - Marie Legendre (1752. - 1833.)

Adrien-Marie Legendre je bio francuski matematičar rođen u Parizu. Bavio se geometrijom, primjenama matematike u fizici i astronomiji, ali i teorijom brojeva. U prvom izdanju svoje knjige *Théorie des Nombres* 1785. godine izrekao je i dokazao (samo neke slučajeve) zakon kvadratnog reprociteta. Konačan dokaz teorema dao je Gauss pa se taj dokaz nalazi u prethodnom poglavlju.

Teorem o prostim brojevima

Teorem o prostim brojevima opisuje asimptotsku distribuciju prostih brojeva među pozitivnim cijelim brojevima. Teorem formalizira intuitivnu ideju da se gustoća prostih brojeva smanjuje kako oni postaju veći i točno kvantificira stopu po kojoj se to događa. Prvu sumnju o ovom problemu predstavili su, nezavisno jedno o drugome, Gauss i Legendre. Teorem su konačno dokazali Jacques-Salomon Hadamard i Charles Jean de la Vallée-Poussin 1896. godine.

Definicija 5.1.1. *S $\pi(x)$ je definirana funkcija $\pi : [2, +\infty\rangle \to \mathbb{N}$.*

$$\pi(x) = card\,\{p \in \mathrm{P} \mid p \leq x\},$$

pri čemu je p prost broj.

Definicija 5.1.2. *Definiramo funkciju $\vartheta(x) = \sum_{p \leq x} \ln p$, pri čemu je p iz skupa prostih brojeva.*

Definicija 5.1.3. *Neka su f i g funkcije realne varijable. Kažemo da je $f(x) = O(g(x))$, ako postoje konstante C, $B \in \mathbb{R}$ takve da vrijedi $|f(x)| \leq Cg(x)$, $\forall x \geq B$.*

Lema 5.1.4. *Vrijedi $\vartheta(x) = O(x)$, odnosno $\vartheta(x) \leq Cx$, $\forall x \geq 1$.*

Dokaz. Dokaz Leme 5.1.4. se može naći u [4, str. 7, Lema 5.] □

Teorem 5.1.5. *Neka je $\pi(x)$ funkcija koja prebrojava proste brojeve te koja daje broj prostih brojeva koji su manji ili jednaki x, za bilo koji realni broj x. Tada je*

$$\pi(x) \approx \frac{x}{\ln x}$$

što možemo pisati i kao

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

Dokaz. Funkcija $\vartheta(x)$ je definirana kao $\vartheta(x) = \sum_{p\leq x} \ln p$, pri čemu je p prost broj. Imamo da vrijedi

$$\vartheta(x) = \sum_{p\leq x} \ln p \geq \sum_{x^{1-\epsilon}<p\leq x} \ln p, \forall \epsilon > 0.$$

Zbog strogog rasta funkcije ln vrijedi

$$x^{1-\epsilon} \leq p \leq x \Rightarrow \ln x^{1-\epsilon} \leq \ln p \leq \ln x.$$

Primjenom prethodnog imamo

$$\vartheta(x) \geq \sum_{x^{1-\epsilon}<p\leq x} (1-\epsilon)\ln x = \left(\pi(x) - \pi\left(x^{1-\epsilon}\right)\right)(1-\epsilon)\ln x.$$

Kako očito vrijedi $\pi\left(x^{1-\epsilon}\right) \leq x^{1-\epsilon}$, $\forall x \geq 0$, imamo

$$\vartheta(x) \geq \left(\pi(x) - x^{1-\epsilon}\right)(1-\epsilon)\ln x.$$

Također,

$$\vartheta(x) \leq \sum_{p\leq x} \ln x = \pi(x)\ln x,$$

pa iz svega vrijedi

$$\left(\pi(x) - x^{1-\epsilon}\right)(1-\epsilon)\ln x \leq \vartheta(x) \leq \pi(x)\ln x.$$

Tj. djeljenjem obje strane s $x > 0$ dobivamo

$$(1-\epsilon)\left(\frac{\pi(x)\ln x}{x} - \frac{\ln x}{x^{\epsilon}}\right) \leq \frac{\vartheta(x)}{x} \leq \frac{\pi(x)\ln x}{x}.$$

Sada uzmimo u obzir da $x \to \infty$ u obje jednakosti.

Kažemo da su dvije funkcije asimptotski jednake ($f(x) \sim g(x)$) ako $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$. Iz toga vrijedi da je $\lim_{x\to\infty} \frac{\vartheta(x)}{x} = 1$ (jer je $\vartheta(x) \sim x$, Lema 8. u [4]) i kako je po L'Hopitalovom pravilu

$$\lim_{x\to\infty} \frac{\ln x}{x^\epsilon} = \lim_{x\to\infty} \frac{1}{\epsilon x^\epsilon} = 0,$$

slijedi

$$\lim_{x\to\infty}(1-\epsilon)\frac{\pi(x)\ln x}{x} \leq 1 \leq \lim_{x\to\infty} \frac{\pi(x)\ln x}{x}, \forall \epsilon > 0,$$

pa iz prve nedjednakosti vrijedi

$$\limsup_{x\to\infty} \frac{\pi(x)\ln x}{x} \leq 1,$$

iz druge vrijedi

$$\liminf_{x\to\infty} \frac{\pi(x)\ln x}{x} \geq 1.$$

Na temelju toga možemo zaključiti da je

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

□

5.2 Peter Gustav Lejeune Dirichlet (1805. - 1859.)

Peter Gustav Lejeune Dirichlet je bio jedan od najdarovitijih njemačkih matematičara, nakon Gaussa, koji je mnogo doprinio teoriji brojeva (uključujući stvaranje područja analitičke teorije brojeva). Bavio se i matematičkom analizom te je bio prvi koji je dao modernu definiciju funkcije. Prvi rad je objavio o Fermatovom posljednjem teoremu, gdje je ponudio djelomični dokaz za slučaj n = 5, kojeg je dovršio Adrien-Marie Legendre.

Dirichletov teorem o prostim brojevima u aritmetičkom nizu

Do teorema o prostim brojevima u aritmetičkom nizu Dirichlet je došao 1837. godine. Teorem je otkrio i Legendre, no nije ga znao dokazati.

Teorem 5.2.1. *Neka su a, b > 0 cijeli brojevi takvi da je (a,b)=1. Tada beskonačni aritmetički niz ak + b, k= 0, 1, 2, ... sadrži beskonačno mnogo prostih brojeva.*

Dokaz. Potpun dokaz Teorema 5.2.1. može se naći u [11]. □

Pogledajmo tablicu prostih brojeva u aritmetičkim nizovima.

Aritmetički niz	Prvih 10 prostih brojeva u nizu
$1 + 2n$	3, 5, 7, 11, 13, 17, 19, 23, 29, 31, ...
$1 + 4n$	5, 13, 17, 29, 37, 41, 53, 61, 73, 89, ...
$3 + 4n$	3, 7, 11, 19, 23, 31, 43, 47, 59, 67, ...
$1 + 6n$	7, 13, 19, 31, 37, 43, 61, 67, 73, 79, ...
$5 + 6n$	5, 11, 17, 23, 29, 41, 47, 53, 59, 71, ...
$1 + 8n$	17, 41, 73, 89, 97, 113, 137, 193, 233, 241, ...
$3 + 8n$	3, 11, 19, 43, 59, 67, 83, 107, 131, 139, ...
$5 + 8n$	5, 13, 29, 37, 53, 61, 101, 109, 149, 157, ...
$7 + 8n$	7, 23, 31, 47, 71, 79, 103, 127, 151, 167, ...
$1 + 10n$	11, 31, 41, 61, 71, 101, 131, 151, 181, 191, ...
$3 + 10n$	3, 13, 23, 43, 53, 73, 83, 103, 113, 163, ...
$7 + 10n$	7, 17, 37, 47, 67, 97, 107, 127, 137, 157, ...
$9 + 10n$	19, 29, 59, 79, 89, 109, 139, 149, 179, 199, ...

Sada ćemo dokazati dva specijalna slučaja prethodnog teorema:

1. Postoji beskonačno mnogo prostih brojeva oblika $4k + 3$.
2. Postoji beskonačno mnogo prostih brojeva oblika $4k + 1$.

Dokaz. 1. Postoji beskonačno mnogo prostih brojeva oblika $4k + 3$. Pretpostavimo da postoji samo konačno mnogo prostih brojeva $p_1 = 3, \ldots, p_r$ koji daju ostatak 3 pri dijeljenju s 4. Promatrajmo sada broj

$$A = 4p_1 \cdots p_r - 1.$$

Očito, A nije dijeljiv nijednim od prostih brojeva $p_1, \ldots, p_r$, kao ni s 2. Dakle, svi prosti faktori q_i, broja $A = q_1 \cdots q_s$ su oblika $4k + 1$. Odavde lako slijedi da je $-1 \equiv A \equiv 1 \pmod 4$ kontradikcija.

2. Postoji beskonačno mnogo prostih brojeva oblika $4k + 1$. Pretpostavimo da postoji konačno mnogo prostih brojeva $p_1 = 5, \ldots, p_r$ koji daju ostatak 1 pri dijeljenju s 4. Sada ćemo promatrati broj

$$A = (2p_1 \cdots p_r)^2 + 1.$$

On nije djeljiv brojevima $2, p_1, \ldots, p_r$ pa slijedi da svi njegovi prosti faktori moraju biti oblika $4k + 3$. Neka je q jedan od njih. Tada uz osnovu da $q \mid A$ slijedi

$$(2p_1 \cdots p_r)^2 \equiv -1 \pmod q.$$

Dakle, -1 je kvadratni ostatak modulo q, što je moguće ako i samo ako je $q \equiv 1 \pmod 4$. Time smo dobili kontradikciju.

□

Snažnija posljedica Dirichletovog teorema je tvrdnja da red recipročnih prostih brojeva oblika

$$\frac{1}{3}+\frac{1}{7}+\frac{1}{11}+\frac{1}{19}+\frac{1}{23}+\frac{1}{31}+\frac{1}{43}+\frac{1}{47}+\frac{1}{59}+\cdots$$

divergira.

Teorem 5.2.2. *Za svaki realni broj $y \geq 2$ vrijedi*

$$\sum_{p\leq y}\frac{1}{p} > \ln\ln y - 1.$$

Odavde neposredno slijedi da red

$$\sum_{p\geq 2}^{\infty}\frac{1}{p},$$

pri čemu je p prost, divergira.

Dokaz. S $\aleph$ označimo skup svih prirodnih brojeva n koji su sastavljeni samo od prostih faktora p, $p \leq y$, uključujući broj 1. Kako imamo samo konačno mnogo brojeva koji su manji ili jednaki y, u apsolutno konvergentnom redu možemo permutirati članove pa imamo:

$$\prod_{p\leq y}\left(1+\frac{1}{p}+\frac{1}{p^2}+\frac{1}{p^3}+\cdots\right)=\sum_{n\in\aleph}\frac{1}{n}.$$

Odnosno,

$$\prod_{p\leq y}\left(\frac{1}{1-\frac{1}{p}}\right)=\sum_{n\in\aleph}\frac{1}{n} \tag{5.1}$$

Očito su svi prirodni brojevi koji su manji ili jednaki od y elementi skupa $\aleph$. Neka je $N = \lfloor y \rfloor$, najveći cijeli broj manji ili jednak y. Usporedbom gornje Darbouxove sume i integrala dobivamo

$$\sum_{n=1}^{N}\frac{1}{n} \geq \int_{1}^{N+1}\frac{dx}{x} = \ln(N+1) > \ln y.$$

Prema tome, iz (5.1) dobivamo

$$\prod_{p\leq y}\left(1-\frac{1}{p}\right)^{-1} > \ln y. \tag{5.2}$$

Dokažimo sada da za sve realne brojeve v, takve da je $0 \leq v \leq \frac{1}{2}$, vrijedi

$$e^{v+v^2} \geq (1-v)^{-1}. \tag{5.3}$$

Da bi dokazali (5.3) moramo definirati funkciju:

$$f(v) = (1 - v)e^{v+v^2}.$$

Tada je

$$f'(v) = -e^{v+v^2} + (1 - v)(1 + 2v)e^{v+v^2} = v(1 - 2v)e^{v+v^2}.$$

Budući da je $f'(v) \geq 0$ za $v \in \left[0, \frac{1}{2}\right]$, radi se o rastućoj funkciji za koju vrijedi $f(0) = 1$, pa je $f(v) \geq 1$ za $v \in \left[0, \frac{1}{2}\right]$. Nakon uvrštavanja (5.3) u (5.2) dobivamo

$$\prod_{p \leq y} e^{\frac{1}{p} + \frac{1}{p^2}} > \ln y.$$

Logaritmirajući obje strane nejednakosti te nakon transformacije logaritma umnoška u zbroj logaritma, dobivamo

$$\sum_{p \leq y} \frac{1}{p} + \sum_{p \leq y} \frac{1}{p^2} > \ln \ln y.$$

Očito je da $\sum_{p \leq y} \frac{1}{p^2}$ konvergira jer je usporediv s harmonijskim redom $\sum_{n=2}^{\infty} \frac{1}{n^2}$ pa

$$\sum_{n=2}^{\infty} \frac{1}{n^2} < \int_1^{\infty} \frac{dx}{x^2} = 1.$$

Od tuda slijedi tvrdnja $\sum\limits_{p \leq y} \frac{1}{p} > \ln \ln y - 1$. Kada $y \to \infty$, zaključujemo da red recipročnih prostih brojeva divergira. □

Bibliografija

[1] D. M. Burton, *The History of Mathematics*, McGraw-Hill, New York, 2011.,

[2] Lj. Baćić, *Fermatovi brojevi*, Osječki matematički list, Vol 13., Osijek, 2013.

[3] A. Dujella, *Uvod u teoriju brojeva*
http://web.math.pmf.unizg.hr/~duje/utb/utblink.pdf,
(lipanj, 2015.)

[4] Z. Durmiš, *Teorem o prostim brojevima*, Završni rad, Rijeka, 2012. https://teoremoprostimbrojevima.files.wordpress.com/2012/09/primenumbertheorem.pdf (kolovoz, 2015.)

[5] I. Ilišević, *Wilsonov teorem*, Osječki matematički list, Vol. 4, Osijek, 2004.

[6] I. Matić, *Uvod u teoriju brojeva*, Osijek, 2014.
http://www.mathos.unios.hr/~imatic/uvod%20u%20teoriju%20brojeva.pdf

[7] O. Ore, *Number theory and its history*, McGraw-Hill, New York, 1948.

[8] S. Slijepčević, *Veliki Fermatov teorem*, Matematika i škola, Zagreb, 2000.
http://mis.element.hr/fajli/513/03-08.pdf
(srpanj, 2015.)

[9] A. Weil, *Number theory - An approach through history from Hammurapi to Legendre*, Birkhäuser, Boston, 2001.

[10] F. M. Brueckler, Povijest matematike - prezentacije,
http://prelog.chem.pmf.hr/~fmbruckler/PovMat/povijest.html
(lipanj, 2015.)

[11] Dirichletov teorem o prostim brojevima u aritmetičkom nizu
http://math.uga.edu/~pete/4400DT.pdf
(kolovoz, 2015.)

[12] Osnovni teorem aritmetike,
http://people.dmi.uns.ac.rs/~dockie/tb/lnotes/tb03.pdf
(lipanj, 2015.)

[13] Prosti brojevi, seminar
https://www.fer.unizg.hr/_download/repository/Seminar_Prosti_brojevi.pdf
(kolovoz, 2015.)

[14] Teorem o prostim brojevima,
http://bs.matematika.wikia.com/wiki/Teorema_o_prostim_brojevima
(kolovoz, 2015.)

[15] https://en.wikipedia.org
(lipanj, srpanj, kolovoz 2015.)

Sažetak

Teorija brojeva je grana matematike koja seže čak i do 4500 godina u prošlost te je jedna od najstarijih područja matematike. Rana povijest započinje Plimpton 322 pločom koja je dokument na kojem pronalazimo prve tragove teorije brojeva. Nakon toga, mnoge teoreme pronalazimo kod Pitagore (ca 500 g. pr. Kr.) koji se bavio pronalaskom prirodnih brojeva x, y, z za koje vrijedi $x^2 + y^2 = z^2$. U Euklidovim Elementima (ca. 300. g. pr. Kr.) pronalazimo mnoge teoreme vezane uz djeljivost i proste brojeve. Pronalazimo i Euklidov algoritam koji se i danas koristi kao alat za pronalaženje najvećeg zajedničkog djelitelja. Također, Euklid spominje i Osnovni teorem aritmetike, kojeg je dokazao Gauss tek u 19. stoljeću. Nakon Euklida slijedi mračno razdoblje teorije brojeva te ona počinje biti zanimljiva tek matematičarima 16. stoljeća. Najpoznatiji matematičari u tom razdoblju su Marin Mersenne i Pierre de Fermat koji su proučavali svojstva prostih brojeva. Fermat je zaslužan za dva velika teorema tog razdoblja pod imenom Mali i Veliki Fermatov teorem. Mali Fermatov teorem je dokazao Leonhard Euler 1736., dok je Veliki Fermatov teorem dokazao Andrew Wiles tek 1994. godine. Leonhard Euler je jedan od najplodonosnijih matematičara u povijesti te je zaslužan za proučavanje teorije brojeva metodama matematičke analize. Također, mnogi ga smatraju najboljim matematičarem u povijesti. Eulerov suvremenik Christian Goldbach je iznio slutnju da se svaki broj veći od dva može zapisati kao zbroj dva prosta broja. Ta slutnja još uvijek nije dokazana. Bitni matematičari 18. stoljeća su bili i Joseph Louis Lagrange i Johann Friedrich Gauss. Lagrange je zaslužan za dokaz mnogih teorema, uključujući Wilsonov teorem te teorem o četiri kvadrata. Gauss je zaslužan za osnivanje teorije kongruencija te za dokaz zakona o kvadratnom reprocitetu. Također, proširio je skup cijelih brojeva na skup takozvanih Gaussovih cijelih brojeva. Konačno, u 19. stoljeću imamo dva bitna matematičara, a to su Legendre i Dirichlet. Legendre je, između ostalog, poznat po teoremu o gustoći prostih brojeva, dok je Dirichlet poznat po teoremu o prostim brojevima u aritmetičkom nizu.

Summary

Number theory is one of the oldest branches of mathmatics, and there is evidence that it has been around for some 4500 years. Early history starts with Plimpton 322 tablet on which we can find the first traces of number theory. After that, many theorems can be found in Pythagoras work (500 BC). Pythagoras was trying to find positive integers x, y, z for which $x^2 + y^2 = z^2$ is valid. In Euclids Elements (300 BC) we can find many theorems that are related to divisibility and prime numbers. Also, we can find the Euclidean algorithm which is used, even today, for finding greatest common divisors. Euclid also mentions the fundamental theorem of arithmetic, which is proven by Gauss in the 19th century. After Euclid, number theory enters a dormant period which lasts until the 16th century, when it once again peaks interest amongst mathematicians. Noteworthy mathematicians in this period are Marin Mersenne and Pierre de Fermat who studied the properties of prime numbers. Fermat was responsible for two great theorems of that time, Fermat's little theorem and Fermat's last theorem. Fermat's little theorem was proven by Leonhard Euler in 1736., and Fermat's last theorem was proven by Andrew Wiles in 1994. Leonhard Euler is considered to be one of the most prolific mathematicians in history, and is responsible for studying number theory trough the methods of mathematical analysis. Eulers contemporary Christian Goldbach came forward with a conjecture that stated: Any number greater than two can be written as the sum of two prime numbers. This conjecture has not yet been proven. Important mathematicians of the 18th century were Joseph Louis Lagrange and Johann Friedrich Gauss. Lagrange is responsible for proofs of many theorems, including Wilson's theorem and the theorem of four squares. Gauss is responsible for establishing the theory of congruences and for the proof of the Law of Quadratic Reciprocity. Also, he expanded the set of integers to the set of so-called Gaussian integers. Finally, in the 19th century we have two important mathematicians, Legendre and Dirichlet. Legendre, among other things, is known for the the prime number theorem, while Dirichlet is known for Dirichlet theorem on primes in arithmetic progression .

Životopis

Ana Gmajnić rođena je 18.11.1990. godine u Zagrebu. Pohađala je Osnovnu školu Luka u Sesvetama te Opću gimnaziju Sesvete. Obrazovanje je nastavila na Matematičkom odsjeku Prirodoslovno matematičkog fakulteta u Zagrebu, na kojem upisuje preddiplomski studij 2009. godine te diplomski studij Matematika; smjer nastavnički 2013. godine. Završila je diplomski studij u rujnu 2015. godine.