Zbroj dva cjelobrojna kvadrata

Stjepanović, Josipa

SVEUČILIŠTE U ZAGREBU
PRIRODOSLOVNO-MATEMATIČKI FAKULTET
MATEMATIČKI ODSJEK

Josipa Stjepanović

ZBROJ DVA CJELOBROJNA KVADRATA

Diplomski rad

Zagreb, 2022.

SVEUČILIŠTE U ZAGREBU
PRIRODOSLOVNO-MATEMATIČKI FAKULTET
MATEMATIČKI ODSJEK

Josipa Stjepanović

ZBROJ DVA CJELOBROJNA KVADRATA

Diplomski rad

Voditelj rada:
prof. dr. sc. Juraj Šiftar

Zagreb, 2022.

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. _____

Zahvaljujem se mentoru prof. dr. sc. Juraju Šiftaru na strpljivosti i razumijevanju te nesebičnom dijeljenju znanja i vremena. Veliko hvala i mojim prijateljicama, kolegicama, koje su mi pružale potporu ne samo tijekom izrade ovog rada već kroz cjelokupno studiranje. Da se nismo upoznale, možda bismo ranije završile sa studiranjem.
Posebna zahvalnost ide mom suprugu te naravno mojim roditeljima i braći koji su mi omogućili učenje, pratili moje pogreške i uz bezuvjetnu ljubav bili najveća podrška u svemu.

Moje školovanje pratio je ovaj citat:
„Molite i dat će vam se, tražite i naći ćete, kucajte i otvorit će vam se.“
Mt 7,7

Sadržaj

Sadržaj **iii**

Uvod **1**

1 Klasični dokaz **4**

2 Zagierov dokaz **9**
2.1 Geometrijska interpretacija Zagierovog dokaza 12

3 D. R. Heath-Brownov dokaz **14**

4 Elsholtzov kombinatorni pristup zbroju dva kvadrata **16**
4.1 Elsholtzov opis Zagierova dokaza 16
4.2 Dijkstrin opis Zagierova dokaza 19
4.3 Elsholtzova generalizacija metode 21
4.4 Elsholtzova kratka verzija teorema 24

5 A. D. Christopherov dokaz **26**

6 Zaključak **30**

Literatura **32**

Uvod

Fermatov teorem o zbroju dva cjelobrojna kvadrata pripada klasičnim rezultatima teorije brojeva, a jedna je njegova osobitost u tome što povezuje proste brojeve, čija je definicija zasnovana na operaciji množenja, s aditivnom strukturom skupa cijelih brojeva. Taj teorem već blizu četiri stoljeća motivira matematičare na nove pristupe i ideje u dokazivanju, a neke primjere takvih dokaza prikazat ćemo u ovom radu.

Opis prirodnih brojeva, ne nužno prostih, koji se mogu izraziti kao zbroj dva cjelobrojna kvadrata objavio je bez dokaza još 1625. godine istaknuti francuski matematičar Albert Girard[1], no osnovni iskaz uobičajeno se pripisuje jednom od najvećih matematičara u povijesti, Pierreu de Fermatu, koji je detaljno proučavao tematiku prikaza prirodnih brojeva pomoću zbroja kvadrata i srodnih kvadratnih formi.

Pierre de Fermat (1601.-1665.) odlikovao se širokim obrazovanjem, posebno dobrim poznavanjem antičke povijesti i kulture, a osim grčkim i latinskim tečno se služio s još nekoliko jezika. Školovao se za pravnika te je glavninu života proveo u toj struci u državnoj službi, napredujući do visokih pozicija u pravosuđu kraljevine Francuske. Premda matematika nije bila njegovo osnovno zanimanje, a što je zapravo karakteristično za mnoge matematičare toga vremena, Fermatova bogata i vrijedna matematička ostavština sadrži niz ključnih doprinosa različitim područjima kao što su teorija brojeva, infinitezimalni račun, teorija vjerojatnosti, analitička geometrija i druge. Uspješno se bavio i fizikom, posebno optikom. Jako malo njegovih radova objavljeno je za njegova života, ne samo zato što još nije bilo znanstvenih časopisa, nego i zbog njegove nesklonosti pisanju formalno dorađenih matematičkih tekstova. Fermatov opus velikim je dijelom sadržan u korespondenciji s drugim matematičarima, primjerice Blaiseom Pascalom i Marinom Mersenneom. Fermat se s osobitim žarom bavio teorijom brojeva, motiviran čitanjem Diofantove *Aritmetike*. U tom području dao je niz tvrdnji, od kojih mnoge bez dokaza, čija se istinitost potvrdila desecima godina pa čak i stoljećima kasnije (tzv. Veliki Fermatov teorem). Posebnu ulogu u tome imao je veliki švicarski matematičar Leonhard Euler[2]. Fermatov rad nije imao osobit odjek kod njegovih suvremenika, ali se pokazao iznimno utjecajnim na kasnije generacije matematičara.

[1] Albert Girard (1595.-1632.), francuski matematičar i glazbenik

[2] Leonhard Euler (1707.-1783.), švicarski matematičar, fizičar i astronom

Teorem (Frematov teorem o zbroju dva kvadrata). Prost broj p jednak je zbroju kvadrata dvaju cijelih brojeva ako i samo ako je $p = 2$ ili je p oblika $4k + 1,\ k \in \mathbb{N}$.

Napomenimo da je prikaz o kojem govori teorem jedinstven, ako postoji (ne uzimajući u obzir redoslijed pribrojnika u zbroju).

Katkad se ovaj teorem naziva Fermatov božićni teorem, jer ga je Fermat iskazao 25. prosinca 1640. godine u pismu Mersenneu[3]. Fermatov dokaz nikada nije pronađen, premda je autor tvrdio da ga poznaje. U jednom pismu Christiaanu Huygensu[4] dao je naznake kako je za dokaz ovog teorema koristio metodu neprekidnog (ili beskonačnog) silaska, ali sa sigurnošću možemo reći kako je prvi poznat dokaz teorema tek Eulerov dokaz iz 1747. godine.

Objavljeno je više od 50 različitih dokaza Fermatovog teorema, a većina njih koristi se činjenicom da za proste brojeve $p \equiv 1 (\mathrm{mod}\ 4)$, jednadžba $x^2 = -1$ ima rješenje u $\mathbb{Z}_p$, odnosno u polju ostataka modulo p. Dok za drugu mogućnost prost, neparan broj $p \equiv 3 (\mathrm{mod}\ 4)$ jednadžba nema rješenje. U ovom radu bavit ćemo se modernijim i novijim dokazima ovog teorema na temelju različitih pristupa. Primjerice, Zagierov[5] „dokaz u jednoj rečenici“, kojim su čitatelju ipak prepušteni elementarni izračuni, iz 1990. godine privukao je veliku pozornost matematičara. Tako ćemo u radu opisati objašnjenje Zagierovog dokaza kojeg je dao moderni matematičar Christian Elsholtz[6]. On u svome članku [8] iznosi i objašnjenja drugih matematičara kao što je Dijkstra[7] te izvodi generalizaciju metode. Potaknut Zagierovom kratkoćom i jasnoćom daje po svome sudu jasniji i lakše pamtljiv kratki dokaz teorema o zbroju dva cjelobrojna kvadrata. Ukratko ćemo opisati ideju dokaza Heath-Browna[8], u kojoj je upravo Zagier pronašao inspiraciju za svoj dokaz. Ključan je domišljat izbor skupa koji omogućuje podjelu na orbite duljine 1 ili 2. Na taj način jednostavna provjera parnosti jamči rastavljanje na dva kvadrata.

[3]Marin Mersenne (1588.-1648.), francuski matematičar, fizičar, filozof i glazbeni teoretičar

[4]Christiaan Huygens (1629.-1695.), nizozemski astronom, matematičar i fizičar

[5]Don Zagier, rođen 1951., američko-njemački matematičar

[6]Christian Elsholtz, rođen 1971. godine, austrijsko-njemački matematičar

[7]Edsger Dijkstra (1930.-2002.), nizozemski računalni znanstvenik

[8]Roger Heath-Brown, rođen 1952., britanski matematičar

Na kraju ćemo pokazati A. D. Christopherov dokaz pomoću teorije particija iz 2015. godine, koji ima sasvim drugačiji pristup od prethodnika. Prije nego krenemo s modernijim dokazima osvrnut ćemo se na Eulerov dokaz, jer to je klasični primjer dokaza pomoću metode neprekidnog silaska.

1 Klasični dokaz

U ovom poglavlju pokazat ćemo koji se prirodni brojevi mogu prikazati kao zbroj kvadrata dvaju cijelih brojeva. Za to će nam biti potreban i rezultat Fermatovog teorema o zbroju dva kvadrata, a za dokaz istog koristit ćemo najčešće viđenu vrstu dokaza koja koristi metodu neprekidnog silaska i elementarnu teoriju brojeva. Fermat je metodu neprekidnog ili beskonačnog silaska primjenjivao na nekoliko dokaza teorema iz teorije brojeva. Tvrdnju želimo dokazati za pozitivne cijele brojeve, a niz pozitivnih cijelih brojeva ne može beskonačno padati, pa je to argument kontradikcije. Dakle, ako želimo da ne postoji pozitivan cijeli broj koji neko svojstvo zadovoljava, pokažemo da iz pretpostavke da neki pozitivan cijeli broj zadovoljava to svojstvo, slijedi da postoji i manji pozitivan cijeli broj s istim svojstvom, a takvo neprekidno spuštanje ne dozvoljava struktura skupa pozitivnih cijelih brojeva. Time smo došli do kontradikcije, moglo bi se reći kako je ova metoda vrsta indukcije.

Taj dokaz slijedit će nam iz nekoliko propozicija (prema [10], [7]).

Teorem 1.1. *Prost broj p jednak je zbroju kvadrata dvaju cijelih brojeva ako i samo ako je $p = 2$ ili je p oblika $4k + 1,\ k \in \mathbb{N}$.*

Propozicija 1.1. *Neka je p prost broj oblika $4k+1$. Tada postoji $x \in \mathbb{N}$, takav da $p \mid x^2 + 1$.*

Za dokaz ove tvrdnje primijenit ćemo Wilsonov teorem $(p-1)!+1 \equiv 0 \ (\mod\ p)$.

$$\begin{aligned}
&(p-1)! \equiv -1 (\text{mod } p)\\
&(p-1)! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot \frac{p-1}{2} \cdot \frac{p+1}{2} \cdot \ldots \cdot (p-3)(p-2)(p-1)\\
&\qquad \equiv (-1)^{\frac{p-1}{2}} \left(1 \cdot 2 \cdot 3 \cdot \ldots \cdot \frac{p-1}{2}\right)^2 (\text{mod } p)
\end{aligned}$$

Ako sada za x uzmemo $x = \left(\frac{p-1}{2}\right)!$ dobivamo $(p-1)! \equiv x^2 (\text{mod } p)$, odnosno $-1 \equiv x^2 (\text{mod } p)$ pa slijedi da $p \mid x^2 + 1$. Na temelju ove propozicije očito vrijedi i sljedeća tvrdnja:

Neka je p prost broj oblika $4k+1$. Tada postoje prirodni brojevi x, y, takvi da $\text{nzd}(x, y) = 1$ i $p \mid x^2 + y^2$. Naime, uzmemo li $x = \left(\frac{p-1}{2}\right)!$ i $y = 1$, zadovoljeno je $\text{nzd}(x, y) = 1$ i $p \mid x^2 + y^2$.

Propozicija 1.2. *Ako prost broj p dijeli zbroj dvaju kvadrata $x^2 + y^2$, gdje je $nzd(x, y) = 1$, onda je i p sam zbroj dvaju kvadrata.*

U dokazu ove propozicije koristit ćemo metodu silaska. Kao što smo već pokazali u prethodnoj propoziciji, postoje prirodni brojevi x, y takvi da $\text{nzd}(x, y) = 1$ i $p \mid x^2 + y^2$. Drugim riječima, postoji prirodan broj k takav da vrijedi $pk = x^2 + y^2$, pri čemu je pk najmanji takav višekratnik broja p. Za $k = 1$ propozicija vrijedi trivijalno. Sada pretpostavimo $k > 1$. Pogledajmo donju granicu za k ako izaberemo a i b, tako da bude $x \equiv a(\bmod\ p)$, $y \equiv b(\bmod\ p)$ i $|a|,\ |b| \leq \frac{p}{2}$. Tada vrijedi $x^2+y^2 \equiv a^2+b^2 \equiv 0(\bmod\ p)$ i $a^2+b^2 \leq \frac{p^2}{4}+\frac{p^2}{4} = p\cdot\frac{p}{2}$ pa slijedi da $1 \leq k \leq \frac{p}{2}$.

Nadalje izaberimo $x \equiv u(\text{mod } k)$ i $y \equiv v(\text{mod } k)$, $|u|, |v| \leq \frac{k}{2}$ pa opet zaključujemo $x^2+y^2 \equiv u^2+v^2 \equiv 0(\bmod\ k)$ iz čega postoji prirodan broj l takav da vrijedi $kl = u^2+v^2$. Pritom, $u^2+v^2 \leq \frac{k^2}{4}+\frac{k^2}{4} = k\cdot\frac{k}{2}$ odakle $1 \leq l \leq \frac{k}{2} < k$.

Potom, $pk\cdot kl = (x^2+y^2)\cdot(u^2+v^2) = (xu+yv)^2+(xv-yu)^2$. Primijetimo kako vrijedi $xu+yv \equiv x^2+y^2 \equiv 0(\bmod\ k)$ i $xv-yu \equiv xy-xy \equiv 0(\bmod\ k)$. Stoga postoje cijeli brojevi x_1, y_1, takvi da $xu+yv = x_1k$ i $xv-yu = y_1k$. Uvrstimo dobivene jednakosti u $pk \cdot kl = (x^2 + y^2) \cdot (u^2 + v^2) = (xu + yv)^2 + (xv - yu)^2$ čime dobivamo $(x_1k)^2 + (y_1k)^2 = pk^2l$.

Neka je $\text{nzd}(x_1, y_1) = d$, $x_1 = dx_2$, $y_1 = dy_2$ i $\text{nzd}(x_2, y_2) = 1$. Slijedi $x_2^2 + y_2^2 = p\frac{1}{d^2}$. Iz ove jednakosti dobili smo da postoji prirodan broj $k_1 = \frac{1}{d^2}$ takav da $k_1 \leq l \leq \frac{k}{2} < k$ i da višekratnik pk_1 ima prikaz kao zbroj dva kvadrata. To je u kontradikciji s minimalnosti višekratnika pk. Konačno, $k = 1$ i $p = x^2 + y^2$.

Još nam preostaje dokazati da je prikaz prostog broja u obliku zbroja dva kvadrata, ako postoji, jedinstven.

Pretpostavimo suprotno, da prikaz prostog broja u obliku zbroj dva kvadrata nije jedinstven, odnosno $p = a^2 + b^2 = c^2 + d^2$. Pri tome su nam a, c i b, d iste parnosti. Vrijedi $a^2 - c^2 = d^2 - b^2$, odnosno $\frac{a-c}{2}\cdot\frac{a+c}{2} = \frac{d-b}{2}\cdot\frac{d+b}{2}$. Neka je $\text{nzd}\left(\frac{a-c}{2}, \frac{d-b}{2}\right) = s$. Tada postoje m, n relativno prosti cijeli brojevi takvi da $\frac{a-c}{2} = ms$ i $\frac{d-b}{2} = ns$. Jednakost $\frac{a-c}{2}\cdot\frac{a+c}{2} = \frac{d-b}{2}\cdot\frac{d+b}{2}$ možemo zapisati kao $ms\cdot\frac{a+c}{2} = ns\cdot\frac{d+b}{2}$, kraće $m\cdot\frac{a+c}{2} = n\cdot\frac{d+b}{2}$. Kako su m, n relativno prosti cijeli brojevi, vrijedi $\frac{a+c}{2} = n\cdot t$ i $\frac{d+b}{2} = m\cdot t$. Odavde slijedi vrlo jednostavan sustav

četiri jednadžbe s četiri nepoznanice:

$$\begin{cases} a - c = 2ms \\ d - b = 2ns \\ a + c = 2nt \\ d + b = 2mt, \end{cases}$$

iz čega lako dobivamo $a = ms + nt$ i $b = mt - ns$. Prema identitetu $a^2 + b^2 = (ms + nt)^2 + (mt - ns)^2$, zbroj dva kvadrata jednak je produktu dvaju brojeva od kojih je svaki zbroj dvaju kvadrata, slijedi $a^2 + b^2 = (m^2 + n^2)(s^2 + t^2)$. Time smo dobili kontradikciju s pretpostavkom da je p prost broj. Dakle, ako se prost broj može zapisati u obliku zbroja dvaju kvadrata, onda je taj zapis jedinstven.

Fermat nam je ostavio još nekoliko zanimljivih tvrdnji vezanih uz proste brojeve koje također nije dokazao (vidi [7]). Ti teoremi dovest će nas do odgovora koji se prirodni brojevi mogu prikazati kao zbroj kvadrata dvaju cijelih brojeva. U nastavku ćemo dokazati nekoliko propozicija koje su nam neophodne za odgovor na to pitanje.

Propozicija 1.3. *Prost broj p oblika $4k + 3$, $k \in \mathbb{N}$, ne može se zapisati kao zbroj dvaju kvadrata.*

Dokaz je vrlo jednostavan, proučava kvadratne ostatke i na osnovu njih dolazimo do zaključka kojeg želimo dokazati. Neka su $x, y \in \mathbb{Z}$ pri čemu $p = x^2 + y^2$. Brojevi x i y mogu biti oblika $4k$, $4k + 1$, $4k + 2$ ili $4k + 3$. Tada $x^2, y^2 \equiv 0$ ili $1 (\mathrm{mod}\ 4)$, pa iz toga $p \equiv 0, 1$ ili $2 (\mathrm{mod}\ 4)$. Ovime smo pokazali da zbroj dvaju kvadrata nikako ne može biti oblika $4k + 3$.

Propozicija 1.4. *Neka su m i n sume dvaju kvadrata. Tada je i njihov produkt $m \cdot n$ također suma dvaju kvadrata.*

Dokaz: Neka je $m = x_1^2 + y_1^2$ i $n = x_2^2 + y_2^2$. Tada je njihov produkt

$$\begin{aligned} m \cdot n &= (x_1^2 + y_1^2)(x_2^2 + y_2^2) \\ &= (x_1x_2)^2 + (y_1y_2)^2 + (x_1y_2)^2 + (y_1x_2)^2 + 2x_1x_2y_1y_2 - 2x_1x_2y_1y_2 \\ &= (x_1x_2 + y_1y_2)^2 + (x_1y_2 - y_1x_2)^2 \\ &= (x_1x_2 - y_1y_2)^2 + (x_1y_2 + y_1x_2)^2. \end{aligned}$$

Dakle, $m \cdot n$ također se može prikazati kao suma dvaju kvadrata.

Propozicija 1.5. *Neka je p prost broj oblika $4k+3$, $k \in \mathbb{N}$. Ako $p \mid x^2+y^2$, onda $p \mid x$ i $p \mid y$.*

Dokaz: Pretpostavimo suprotno, odnosno $p \mid x^2+y^2$ i $p \nmid x$, $p \nmid y$. Budući da $p \mid x^2+y^2$ onda vrijedi $x^2 \equiv -y^2 (\mod p)$. Ovako zapisanu kongruenciju potencirajmo eksponentom $\frac{p-1}{2}$ pa dobivamo $x^{p-1} \equiv (-1)^{\frac{p-1}{2}} y^{p-1} (\mod p)$. Primjenom Malog Fermatovog teorema i iz pretpostavki slijedi da je $1 \equiv -1 (\mod p)$, što je nemoguće. Dakle, ako $p \mid x^2+y^2$, onda $p \mid$ i $p \mid y$.

Teorem 1.2. *Prirodan broj n može se prikazati kao zbroj dvaju kvadrata ako i samo ako se u rastavu na proste faktore prosti brojevi p oblika $4k+3$, $k \in \mathbb{N}$ pojavljuju samo s parnim eksponentom.*

Dokaz: Prvo ćemo pokazati nužnost. Neka je $n = x^2+y^2$. Naime, ako je $p = 4k+3$, prema Propoziciji 1.5. imamo $p \mid x$ i $p \mid y$, stoga $p^2 \mid x^2$ i $p^2 \mid y^2$, tj. $p^2 \mid x^2+y^2 = n$, to možemo zapisati $n = p^2 \cdot n_1$. Ako sada $n = x^2+y^2$ podijelimo s p^2, dobivamo $n_1 = \left(\frac{x}{p}\right)^2 + \left(\frac{y}{p}\right)^2$. Nadalje, ako $p \mid n_1$, za koji smo pokazali da je zbroj kvadrata dvaju cijelih brojeva, analogno zaključujemo $p^2 \mid n_1$. Nastavimo li ovaj postupak, dolazimo do zaključka kako je n djeljiv samo parnim potencijama od p pa slijedi tvrdnja.

Sada pokažimo dovoljnost. Prirodan broj n kojemu se u rastavu na proste faktore prosti faktori oblika $4k+3$ pojavljuju s parnom potencijom možemo zapisati kao $n = m^2 l$, pri čemu je m najveći prirodni broj takav da $m^2 \mid n$. U ovom zapisu l je produkt prostih brojeva oblika $4k+1$ i eventualno broja 2. Prema Fermatovom teoremu o zbroju dva kvadrata i prema Propoziciji 1.4., slijedi da je l zbroj dvaju kvadrata, no tada je n također zbroj dvaju kvadrata, $n = m^2 l = m^2(a^2+b^2) = (ma)^2 + (mb)^2$.
Sada kad imamo nekoliko pomoćnih tvrdnji i teorema nije teško doći do odgovora za sve prirodne brojeve.

Primjer 1.1. *Odredimo sve prirodne brojeve n koji se mogu prikazati kao zbroj kvadrata dvaju prirodnih brojeva, to jest da nijedan od pribrojnika ne smije biti* 0.

To su prirodni brojevi kod kojih prosti faktori od n, oblika $4k+3$ imaju parne eksponente te prosti broj 2 ima neparan eksponent ili imaju barem jedan prosti faktor oblika $4k+1$.

Nužnost: Neka je n najmanji prirodni broj koji je zbroj kvadrata dvaju prirodnih brojeva, te u rastavu na proste faktore sadrži prosti faktor 2 s parnim eksponentom $k \geq 0$. Prema prethodnom teoremu, svi se prosti faktori oblika $4k+3$, $k \in \mathbb{N}$ pojavljuju s parnim eksponentom. To možemo zapisati s $n = 2^{2k}m^2 = a^2 + b^2$. Ako je $k > 0$, onda je lijeva strana djeljiva s 4 pa a i b moraju biti parni. Ako sada zapišemo $a = 2a_1$ i $b = 2b_1$ takvi da $a_1,\ b_1 \in \mathbb{N}$, onda imamo

$$\begin{aligned} 2^{2k}m^2 &= (2a_1)^2 + (2b_1)^2 \\ 2^{2(k-1)}m^2 &= a_1^2 + b_1^2 < n. \end{aligned}$$

Dobivena nejednakost u kontradikciji je s minimalnosti od n. Dakle, $k = 0$ i $m^2 = a^2 + b^2$. Iz uvjeta zadatka znamo da m ima prosti faktor p oblika $4k+3$, pa prema Propoziciji 1.5, ako $p \mid a^2 + b^2$, onda $p \mid a$ i $p \mid b$, te je $\left(\frac{m}{p}\right)^2 = \left(\frac{a}{p}\right)^2 + \left(\frac{b}{p}\right)^2$, što je opet u kontradikciji s minimalnosti od n. Time smo pokazali da prirodan broj koji se može prikazati kao zbroj dvaju kvadrata u rastavu na proste faktore ima broj 2 s neparnim eksponentom ili ima barem jedan prosti faktor oblika $4k+1$. Prema prethodnom teoremu znamo da se prosti faktori oblika $4k+3$ u rastavu n na proste faktore javljaju s parnim eksponentom. Time smo dokazali nužnost.

Dovoljnost: Ako pretpostavimo da prirodan broj n možemo prikazati kao zbroj kvadrata dvaju prirodnih brojeva uz gore navedene uvjete imamo dva slučaja:

1. $n = 2m^2$
2. $n = 2^k m^2 l$, gdje je $k = 0$ ili $k = 1$ i l predstavlja produkt prostih faktora oblika $4k+1$, $k \in \mathbb{N}$

U slučaju 1. jasno je vidljivo da tvrdnja vrijedi jer $n = 2m^2 = m^2 + m^2$.
Pogledajmo sada slučaj 2. Broj l je zbroj kvadrata dvaju prirodnih brojeva, to slijedi iz Fermatovog teorema i Propozicije 1.4. Dakle, ako je $l = x^2 + y^2$, $x, y \in \mathbb{N}$, pa je $m^2 l = (mx)^2 + (my)^2$, dok je $m^2 l = (mx + my)^2 + (mx - my)^2$. Kako je $l = x^2 + y^2$ neparan i $x \neq y$ to povlači $mx - my \neq 0$. Tvrdnja je pokazana.

2 Zagierov dokaz

Don Zagier, rođen 1951., američki je matematičar čije je glavno područje rada i interesa teorija brojeva. O njegovoj natprosječnoj inteligenciji govori i činjenica kako je sa samo 16 godina diplomirao i magistrirao na MIT-u, a doktorirao na Sveučilištu u Bonnu s 20 godina. U ovome poglavlju donosimo dokaz koji je pojednostavljenje dokaza Heath-Browna, dok je s druge strane inspiraciju za takvu vrstu dokaza dao Liouville. Dokaz nije konstruktivan, ne daje metodu za pronalaženje prikaza prostog broja kao zbroja dvaju kvadrata. Osnovni princip kojim se koristimo je jednakost pariteta kardinalnosti konačnog skupa i broja fiksnih točaka pod djelovanjem bilo koje involucije na tom skupu.

Dokaz iskazan samo jednom rečenicom (prema [16]) glasi:

Involucija na konačnom skupu $S = \{(x, y, z) \in \mathbb{N}^3 : x^2 + 4yz = p\}$ definirana s

$$(x, y, z) \to \begin{cases} (x + 2z, z, y - x - z) & \text{ako je } x < y - z \\ (2y - x, y, x - y + z) & \text{ako je } y - z < x < 2y \\ (x - 2y, x - y + z, y) & \text{ako je } x > 2y \end{cases}$$

ima točno jednu fiksnu točku pa je $|S|$ neparan i involucija definirana s $(x, y, z) \to (x, z, y)$ također ima fiksnu točku.

Dokaz ćemo detaljno razraditi i provjeriti sve implicitne tvrdnje za koje nam je potrebno dosta rutinskih provjera.

Definicija 2.1. *Preslikavanje $\varphi : S \to S$ naziva se involucija ili involutorno preslikavanje ako i samo ako je $\varphi(\varphi(x)) = x$ za svaki $x \in S$.*

Lako se provjeri kako je svaka involucija bijekcija. Prvo promotrimo injektivnost. $\varphi(x) = \varphi(y) \Rightarrow x = y$. Slijedi:

$$\varphi(\varphi(x)) = \varphi(\varphi(y)) \Rightarrow \varphi(x) = \varphi(y)$$
$$x = y \Rightarrow \varphi(x) = \varphi(y)$$

Da bismo pokazali kako je funkcija surjekcija, želimo pronaći takav x da vrijedi $\varphi(x) = y$.

Neka je $x = \varphi(y)$.Tada vrijedi $\varphi(\varphi(y)) = y$.

Dokazali smo da je involucija bijektivna. Također, Zagierov dokaz govori kako svaka involucija $\varphi : S \to S$, takva da $|S| < \infty$ i $|S|$ je neparan, ima fiksnu točku, $x \in S$ i $\varphi(x) = x,\ (x, \varphi(x))$.

Za konačan skup $S = \{(x, y, z) \in \mathbb{N}^3 : x^2 + 4yz = p\}$ vrijedi $|S| < \infty$. Lako je uočiti zašto to vrijedi. Neka je p neki fiksan broj, a x^2 i $4yz$ su pozitivni pa sigurno vrijedi $|x| \leq \sqrt{p}$, čime je tvrdnja pokazana. Sada definirajmo skupove:

$$\begin{aligned} S_1 &= \{(x, y, z) \in S : x < y - z\} \\ S_2 &= \{(x, y, z) \in S : y - z < x < 2y\} \\ S_3 &= \{(x, y, z) \in S : x > 2y\}. \end{aligned}$$

Tvrdimo: $S = S_1 \cup S_2 \cup S_3$.
Pogledajmo granične vrijednosti u definiciji ovih skupova. Jasno je da vrijedi $y - z \neq 2y$ jer $y + z = 0$ nije moguće. Ako sada promotrimo drugu granicu $x = y - z$, onda je $p = (y - z)^2 + 4yz = (y + z)^2$, što je kontradikcija s činjenicom da je p prost broj. Preostaje provjeriti slučaj kada je $x = 2y$ pa je $p = (2y)^2 + 4yz = 4y(x + z)$ ponovno kontradikcija s činjenicom da je p prost broj. Dakle, skup S možemo prikazati kao uniju disjunktnih podskupova.

$\varphi : S \to S$ je preslikavanje koje možemo prikazati i na sljedeći način:

$$(x, y, z) \to \begin{cases} (x + 2z, z, y - x - z), & (x, y, z) \in S_1 \\ (2y - x, y, x - y + z), & (x, y, z) \in S_2 \\ (x - 2y, x - y + z, y), & (x, y, z) \in S_3 \end{cases}$$

Provjerimo da je preslikavanje involutorno, pri čemu $\varphi(S_1) \subseteq S_3$, $\varphi(S_2) \subseteq S_2$, $\varphi(S_3) \subseteq S_1$ iz čega slijedi $\varphi(S) \subseteq S$.

Neka je $(x, y, z) \in S_1$, onda $\varphi(x, y, z) = (x + 2z, z, y - x - z) = (u, v, w) \in S_3$. Sada imamo

$$\begin{aligned} \varphi(u, v, w) &= (u - 2v, u - v + w, v) \\ &= (x + 2z - 2z, x + 2z - z + y - x - z, z) \\ &= (x, y, z). \end{aligned}$$

Time smo pokazali da φ djeluje involutorno na elemente skupa S_1 i $\varphi(\varphi(S_1)) = S_1$.

Na isti način pokažimo $\varphi(\varphi(S_2)) = S_2$ i $\varphi(\varphi(S_3)) = S_3$.

Prvo pokažimo $\varphi(\varphi(S_2)) = S_2$.

Neka je $(x, y, z) \in S_2$, $\varphi(S_2) = \varphi(x, y, z) = (2y-x, x, x-y+z) = (u, v, w) \in S_2$ onda

$$\begin{aligned}\varphi(\varphi(S_2)) &= \varphi(u, v, w)\\ &= (2v - u, v, u - v + w)\\ &= (2y - 2y + x, y, 2y - x - y + x - y + z)\\ &= (x, y, z).\end{aligned}$$

Ako je $(x, y, z) \in S_3$, $\varphi(S_3) = \varphi(x, y, z) = (x-2y, x-y+z, y) = (u, v, w) \in S_1$ onda

$$\begin{aligned}\varphi(\varphi(S_3)) &= \varphi(u, v, w)\\ &= (u + 2w, w, v - u - w)\\ &= (x - 2y + 2y, y, x - y + z - x + 2y - y)\\ &= (x, y, z).\end{aligned}$$

Preslikavanje je involutorno.

Uočimo da je S neprazan skup, jer za $p = 4k + 1$ točka $(1, 1, k) \in S$. Potom, $(1, 1, k) \in S_2$.

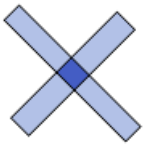
Ako ima fiksnu točku, mora se nalaziti u S_2. Ispitajmo ima li u S_2 fiksnih točaka. Za $(x, y, z) \in S_2$ trebalo bi vrijediti $\varphi(x, y, z) = (2y-x, y, x-y+z) = (x, y, z)$ pa imamo $x = y$. Sada jednadžba $p = x^2+4yz$ izgleda $p = x^2+4xz = x(x + 4z)$. Budući da je p prost broj, onda je $x = 1$ pa $y = 1$, no kako je p oblika $4k + 1$, slijedi $z = k$. Dakle, postoji jedinstvena fiksna točka $(1, 1, k)$. Budući da je fiksna točka u S_2 jedinstvena, slijedi da je $|S_2|$ neparan.

Za $\varphi(S_1) = S_3$ i φ je bijekcija slijedi $|S_1| = |S_3|$. Vrijedi $|S|$ je neparan jer $|S| = |S_1| + |S_2| + |S_3| = 2|S_1| + |S_2|$, a $|S_2|$ je neparan.

Preslikavanje $\theta : S \to S$ definirano s $\theta(x, y, z) = (x, z, y)$ očito je involucija te mora imati barem jednu fiksnu točku. Za tu fiksnu točku $y = z$ pa vrijedi $p = x^2 + 4yz = p = x^2 + (2y)^2$. Time smo detaljno razradili dokaz.

2.1 Geometrijska interpretacija Zagierovog dokaza

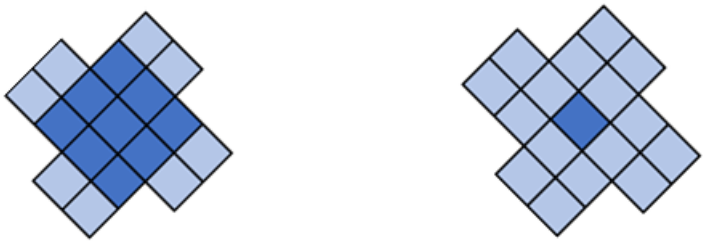
Jako je zanimljiva ideja geometrijske interpretacije Zagierovog dokaza [6]. To je jednostavniji i ljepši način kojime se involucija i njezini slučajevi pojavljuju nekako prirodno. Svaku trojku (x, y, z) interpretiramo „vjetrenjačom“, Tablica 1. Vjetrenjača se sastoji od kvadrata stranice duljine x okruženog četirima pravokutnicima dimenzija $y \times z$, pri čemu je y duljina stranice koja se nalazi duž $x \times x$ kvadrata. Ovako postavljena, vjetrenjača je jedinstvena, do na simetričnu vjetrenjaču. Takve vjetrenjače se mogu svrstati u pet tipova, prema relativnoj veličini y u usporedbi s x i $x + z$. Granični slučajevi $x = 2y$ i $y = x + z$ ne događaju se kada je p prost, što smo i pokazali. Ne trebamo se brinuti ni o slučajevima $x = 0$, $y = 0$ ili $z = 0$.

Tip 1	**Tip 2**	**Tip 3**	**Tip 4**	**Tip 5**
$y < \frac{x}{2}$	$\frac{x}{2} < y < x$	$x = y$	$x < y < x+z$	$x + z < y$
				

Tablica 1: Geometrijska interpretacija Zagierovog dokaza

Ključno je zapažanje da za bilo koji vanjski oblik jedne od ovih vjetrenjača postoje ili jedna ili dvije vjetrenjače koji se uklapaju u njega, Slika 1, Slika 2. Dakle, svakoj vjetrenjači može se pridružiti „dualna“ vjetrenjača. Vjetrenjače koje su dualne same sebi upravo su one vjetrenjače za koje je moguć samo jedan vanjski oblik. Ta dualnost definira involuciju na skupu vjetrenjača određene površine, a djelovanje te involucije na trojku (x, y, z) zadano je preslikavanjima iz Zagierovog teorema. U radu smo to prikazali slikama, Slika 1 i Slika 2, za primjer $p = 17$, prema Zagieru $x^2 + 4yz = p$. Događa se da vjetrenjače tipa 2, 3 i 4 rezultiraju istom jednadžbom, što je razlog zašto Zagierova definicija razlikuje tri slučaja, a ne pet. Time smo opisali geometrijsku interpretaciju Zagierovog dokaza.

Slika 1: Vjetrenjača $(3, 1, 2)$ tipa 1 uparena vjetrenjači $(1, 4, 1)$ tipa 5



Slika 2: Vjetrenjača $(4, 2, 1)$ tipa 2 uparena vjetrenjači $(1, 2, 2)$ tipa 3

3 D. R. Heath-Brownov dokaz

Dokaz koji je dao Zagier zapravo je pojednostavljenje Heath-Brownovog dokaza pa ćemo se ovom prilikom ukratko osvrnuti na njega. David Rodney „Roger“ Heath-Brown, rođen 1952. godine, britanski je matematičar koji se bavi analitičkom teorijom brojeva. Heath-Brown je preformulirao Liouvilleov rad te se njegova verzija [10] pojavila 1984. u studentskom časopisu koji izdaje Dodiplomsko matematičko društvo Sveučilišta u Oxfordu. Budući da je Heath-Brownov dokaz bio malo drugačiji, ukratko opisujemo njegov dokaz (za opširniju verziju vidi [8]). U ovom dokazu koristimo permutacije skupa zadane pomoću grupe regularnih matrica (što je samo drukčiji način zapisa). Ključan je izbor skupa koji omogućuje podjelu na orbite duljine 1 ili 2. Orbita nekog elementa je skup svih slika tog elementa pod djelovanjem grupe, a duljina orbite onda predstavlja broj različitih slika pojedinog elementa. Na taj način jednostavna provjera parnosti jamči rastavljanje na dva kvadrata.

Definirajmo

$$X_1 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \; X_2 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \; X_3 = \begin{pmatrix} 1 & -1 & 1 \\ 0 & 1 & 0 \\ 0 & 2 & -1 \end{pmatrix}, Y = \begin{pmatrix} 0 & 2 & 0 \\ 2 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Skupovi su sad definirani s

$$\begin{aligned} S &= \{v = (x, y, z) \in \mathbb{Z}^3 : p = v^T Y v, \; x, y > 0\}, \\ T &= \{(x, y, z) \in S : z > 0\}, \\ U &= \{(x, y, z) \in S : x + z > y\}. \end{aligned}$$

U ovako definiranim skupovima, v je vektor stupac i $v^T Y v$ samo znači da je $x^2 + 4yz = p$.

Lako se provjeri da je $X_1^2 = X_2^2 = X_3^2 = I$. Kako su ove matrice očito invertibilne, linearna preslikavanja zadana pomoću njih su bijekcije. Također vrijedi i $X_1^T Y X_1 = X_2^T Y X_2 = X_2^T Y X_2 = Y$. Štoviše, X_1 preslikava S na sebe, X_2 preslikava T na sebe, a X_3 preslikava U na sebe. Pokazat ćemo samo posljednji slučaj. Ostali slučajevi pokazuju se analogno. Ako je $v = (x, y, z) \in S$ takav da $x + z > y$, onda $X_3 v = (x - y + z, y, 2y - z) = (x_1, y_1, z_1)$ pa vrijedi

- $x_1 > 0$ jer $x + z > y$

- $y_1 > 0$ jer $y > 0$
- $x_1 + z_1 > y_1$ jer $x > 0$.

Nadalje, $(X_3 v)^T Y (X_3 v) = v^T (X_3^T Y X_3) v = v^T Y v = p$, čime je pokazano da X_3 preslikava U na sebe.

S je disjunktna unija skupova T i $X_1 T$, kao i skupova U i $X_1 U$. Provjerimo posljednju tvrdnju. Ako je $(x, y, z) \in S$ takav da $x + z > y$, znamo da $(x, y, z) \in U$. Ostaje provjeriti slučajeve kada je $x + z = y$ ili je $x + z < y$. Slučaj $x + z = y$ u kontradikciji je s time da je p prost broj, što smo već vidjeli kod Zagiera, da granice ne stvaraju probleme jer se ne postižu za tako definiran p. Neka je p prost i $U_1 = \{(x, y, z) \in S : x + z < y\}$, onda $U_1 = X_1 U$ i ovo nam daje traženi rezultat. Ako je $v = (x, y, z) \in U$, onda $v \in S$ i tada je $X_1 v \in X_1 S = S$. Kako je $X_1 v = (y, x, -z)$, sada imamo $y - z < x$, odakle $X_1 v \in U$. Dakle, $X_1 U_1 \subseteq U$, odakle slijedi $U_1 = X_1^2 U \subseteq X_1 U$. Time smo pokazali kako je $U_1 = X_1 U$.

Budući da je X_1 bijektivno preslikavanje, vrijedi $|T| = |X_1 T|$ i $|U| = |X_1 U|$. Štoviše, kako je $|S|$ disjunktna unija T i $X_1 T$, slijedi da je $|S| = |T| + |X_1 T| = 2|T|$ i slično $|S| = 2|U|$. To implicira $|T| = |U|$. Ako je (x, y, z) fiksna točka od X_3 onda imamo $x - y + z = x$, $y = y$ i $2y - z = z$ pa iz toga slijedi $y = z$ i $p = y(4x + y)$. No, kako je p prost broj i kako vrijedi $p \equiv 1 (\mathrm{mod}\ 4)$, to je zadovoljeno ako i samo ako $y = z = 1$ i $x = \frac{p-1}{4}$. Posljedica toga je da X_3 ima točno jednu fiksnu točku u svome djelovanju na U. Budući da preslikavanje X_3 koje djeluje na U ima točno jednu orbitu duljine 1 (za $y = z = 1$), a budući da sve ostale orbite imaju duljinu 2, nalazimo da $|U|$ mora biti neparan. Dakle, $|T|$ također je neparan, a djelovanje X_2 na T mora imati orbitu duljine 1, tj. postoji fiksna točka takva da $x = y$, $p = 4x^2 + z^2$ što i želimo. Ovo je lijepi primjer kako pravi izbor skupa, djelovanja unutar grupe i brojanje orbite može pojednostaviti postojeće dokaze.

4 Elsholtzov kombinatorni pristup zbroju dva kvadrata i povezani problemi

4.1 Elsholtzov opis Zagierova dokaza

Christian Elsholtz rođen je 1971. godine, a područje njegova interesa su kombinatorna i analitička teorija brojeva, aditivni i multiplikativni problemi, te teorija grafova, kombinatorika i geometrija. Tako se još kao student u jednom radu bavio Zagierovim dokazom, iako je dokaz vrlo kratak ipak za razumijevanje iziskuje bolje znanje matematike, Elsholtz u svome radu detaljno provjerava točnosti Zagierovih tvrdnji i analizira kako je došlo do izbora preslikavanja u Zagierovom dokazu.

Elsholtz opisuje preslikavanje α zadano matricom $B = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}$ s cjelobrojnim koeficijentima. Tada je

$$B \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} ax + by + cz \\ dx + ey + fz \\ gx + hy + iz \end{pmatrix} = \begin{pmatrix} x' \\ y' \\ z' \end{pmatrix}.$$

Budući da zbog invarijantnosti skupa rješenja pod djelovanjem traženog preslikavanja (svako rješenje treba se preslikati opet u neko rješenje) treba vrijediti: $x^2 + 4yz = (x')^2 + 4y'z'$, slijedi

$$(ax + by + cz)^2 + 4(dx + ey + fz)(gx + hy + iz) = x^2 + 4yz.$$

Izjednačavanjem koeficijenata sad dobivamo:

uz x^2 : $a^2 + 4dg = 1$
uz xy : $2ab + 4(dh + ef) = 0$
uz y^2 : $2ab + 4(dh + ef) = 0$
uz xz : $b^2 + 4eh = 0$
uz z^2 : $2ac + 4(di + fg) = 0$
uz yz : $c^2 + 4fi = 0$.

Uočimo da zbog involutornosti treba vrijediti $B^2 = I$. Iz toga slijedi

$$
\begin{aligned}
a^2 + bd + cg &= 1 \\
da + ed + fg &= 0 \\
ga + hd + ig &= 0 \\
ab + be + ch &= 0 \\
db + e^2 + fh &= 1 \\
gb + he + ih &= 0 \\
ac + bf + ci &= 0 \\
dc + ef + fi &= 0 \\
gc + hf + i^2 &= 1.
\end{aligned}
$$

Budući da $\begin{pmatrix} 1 \\ 1 \\ k \end{pmatrix}$ treba biti fiksna točka preslikavanja, neovisno o izboru prirodnog broja k, cjelobrojni koeficijenti matrice B daju nam sljedeće:

$$
\begin{aligned}
a + b + ck &= 1 \\
d + e + fk &= 1 \\
g + h + ik &= k
\end{aligned}
$$

Kako su koeficijenti konstantni dobivamo $c = f = 0$ i $i = 1$. Sada jednadžba $2ac+4(di+fg) = 0$ daje $d = 0$, na isti način dalje dobivamo iz $2bc+4(ei+fh) = 4$ da je $e = 1$. Budući da vrijedi $a^2 + 4dg = 1$, slijedi $a = 1$ ili $a = -1$. Za $a = 1$, rješavanjem preostalih jednadžbi dobivamo $b = 0$, $h = 0$ i $g = 0$. Time smo dobili da iz $a = 1$ slijedi da je matrica B jedinična, ali to ne želimo budući da $\begin{pmatrix} 1 \\ 1 \\ k \end{pmatrix}$ treba biti jedina fiksna točka. Dakle, mora vrijediti $a = -1$ pa je $b = -2$, $h = -1$ i $g = 1$. Stoga vrijedi sljedeće,

$$
B = \begin{pmatrix} -1 & 2 & 0 \\ 0 & 1 & 0 \\ 1 & -1 & 1 \end{pmatrix}.
$$

Kada smo izračunali koeficijenate, vidimo da bismo u tome uspjeli i bez unaprijed postavljenog uvjeta involutornosti, a lako se provjeri da doista vrijedi $B = I^2$. Kako su x', y' i z' prirodni brojevi, mora vrijediti $-x + 2y > 0$ i $x - y + z > 0$. a dobivanje pravila preslikavanja i za ostale slučajeve, $x > 2y$

i $x < y - z$, Zagierovog dokaza trebaju nam drugačije matrice. Za skup A, u kojemu vrijedi $x < y - z$, i skup C, u kojemu vrijedi $x > 2y$, trebamo matrice koje predstavljaju zasebna preslikavanja. Elsholtz prebrojavanjem nekih konkretnih vrijednosti p, koje je razmatrao za primjer kako bi vidio što treba učiniti, uočava da pokušaj da se A i C preslikaju svaki sam u sebe ne prolazi, onda prebrojavanjem za neke konkretne vrijednosti ukazuje da bi bilo šanse ako A i C preslika međusobno. Nalazi dvije matrice A i C za koje vrijedi $AC = I = CA$. Pronađimo matricu X koja okreće uvjete retka B u $(1, -2, 0)$ i $(1, -1, 1)$. Neka je $X = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$.

Matrice $A = BX$ i $C = XB$ pokrivaju sve slučajeve. Neka je

$$A = BX = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 0 & 1 \\ -1 & 1 & -1 \end{pmatrix} \text{ i } C = XB = \begin{pmatrix} 1 & -2 & 0 \\ 1 & -1 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

Vidimo da su uvjeti na retke matrice potpuno usklađeni te induciraju particiju skupa svih rješenja. Elsholtz iz ideje da bi moglo postojati najjednostavnije moguće preslikavanje sa željenim svojstvima dobiva upravo Zagierovo preslikavanje. Uz to je uspio odrediti matrice pridruživanjem jednadžbi za vrlo male proste brojeve $p = 13, 17$ i 29. Primijetivši da su ovdje skupovi rješenja takvi da $-x + 2y < 0$ ili $x - y + z$ imaju samo jedan ili dva elementa. Za $p = 13$, nalazi da $(1, 3, 1)$ mora biti preslikano na $(3, 1, 1)$ i obrnuto. Za $p = 17$ nalazi da $(1, 4, 1)$ mora biti preslikano na $(3, 1, 2)$ i obrnuto. Za $p = 29$ postoje dvije mogućnosti. Jedna uključuje djelomično poznato preslikavanje da je $(1, 7, 1)$ preslikano u $(5, 1, 1)$ i nalazi da je $(1, 7, 1)$ preslikan na $(3, 1, 5)$, iz čega A i C jednoznačno slijede.

U radu sam se osvrnula na Elsholtzovo proširenje i objašnjenje Zagierovog dokaza iz razloga što sam Zagier u svome dokazu govori kako dokaz nije konstruktivan i pokazuje nam postojanje rješanja, ali ne i sama rješenja.

Iako nismo unaprijed znali za particiju skupa S u tri podskupa, imamo preslikavanje $\alpha : S \to S$ takvo da

$$\alpha = \begin{cases} \alpha_1 \text{ opisan matricom } A \text{ ako } -x + y - z > 0 \\ \alpha_2 \text{ opisan matricom } B \text{ ako } -x + 2y > 0 \text{ i } x - y + z > 0 \\ \alpha_3 \text{ opisan matricom } C \text{ ako } x - 2y > 0 \text{ i } x - y + z > 0. \end{cases}$$

To je upravo preslikavanje koje je dao Zagier. Zagierovo drugo preslikavanje, s $\beta : S \to S$ i $(x, y, z) \to (x, z, y)$ odgovara matrici $Y = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$. Kombinirajući dvije involucije α i β, možemo dati konstruktivan dokaz. Počevši s jedinom fiksnom točkom od α, i ponavljanjem β,$\alpha \ldots$ moramo doći do perioda zrcalno simetričnog prema središtu

$$(1, 1, k) \xrightarrow{\beta} (1, k, 1) \xrightarrow{\alpha} (3, 1, k-2) \xrightarrow{\beta} \ldots \xrightarrow{\beta} (3, 1, k-2) \xrightarrow{\alpha} (1, k, 1) \xrightarrow{\beta} (1, 1, k).$$

Budući da je preslikavanje bijektivno, nema pretperioda. Dakle, na kraju se vraćamo na $(1, 1, k)$ s β. Broj elemenata u periodu je paran. Po simetriji, mora postojati još jedna fiksna točka u sredini ciklusa. Budući da postoji samo jedna fiksna točka od α, ova iteracija konstruira fiksnu točku β, to je rješenje $p = x^2 + 4y^2$.

Primjenom ovog algoritma na složeni nekvadratni cijeli broj $n = 4k + 1$ pokazali smo da uz isti argument svaki ciklus koji sadrži $(1, 1, k)$ mora sadržavati i druge fiksne točke. Budući da n više nije prost, mogli bismo doći do druge fiksne točke od α što odgovara faktorizaciji od n. Kako bismo to vidjeli, koncentrirat ćemo se na produkte dvaju različitih prostih brojeva $n = p_1 p_2$ s $p_1 \equiv p_2 \equiv 3 (\mathrm{mod}\ 4)$.

Ovdje β nema fiksnu točku, budući da se n ne može zapisati kao zbroj dva kvadrata. Dakle, u ovom slučaju iteracija $\beta,\ \alpha,\ \beta \ldots$ mora na kraju doći do druge fiksne točke od α koja odgovara $x = y$, tj. faktorizaciji n.

4.2 Dijkstrin opis Zagierova dokaza

Elsholtz iznosi i Dijkstrin nešto drugačiji opis Zagierovog preslikavanja. Edsger Wybe Dijkstra, bio je računalni znanstvenik pa ne čudi da su i njegove bilješke kao i ova o Zagierovom dokazu pisane informatičkim jezikom.
Dijkstra definira dvije involucije, koje naziva inv_0 i inv_1 te zajedničku domenu na kojoj definira S. Koristit će sljedeću strukturu broja fiksnih točaka od inv_0 različitu od nule. Broj fiksnih točaka od inv_0 je neparan, broj elemenata od S je također neparan, a broj fiksnih točaka od inv_1 je neparan i inv_1 ima barem jednu fiksnu točku. Budući da je p neparan broj, jedan od kvadrata je neparan, dok je drugi onda paran broj, što je ekvivalentno rješenju od

$$(x, y) : x^2 + 4y^2 = p. \tag{1}$$

Dijkstra nam daje trivijalnu bijektivnu korespodenciju između rješenja od (1) i

$$(x, y, z) : x^2 + 4yz = p \text{ i } y = z.$$

Neka je $S = \{(x, y, z) : x, y, z \in \mathbb{N} : x^2 + 4yz = p\}$. Koristeći simetriju u y i z, Dijkstra odabire prvu involuciju inv_0 po $S \to S : (x, y, z) \to (x, z, y)$. Fiksne točke od inv_0 zadovoljavaju $y = z$. Stoga je dovoljno pokazati da inv_0 ima barem jednu fiksnu točku. Da bi se to postiglo, konstruira drugu involuciju inv_1 na S, koja ima točno jednu fiksnu točku.

Zatim, Dijkstra prikuplja neke elementarne činjenice:
$x > 0,\ y > 0,\ z > 0,\ x \neq \pm(y - z)$, budući da je p neparan, a ne kvadrat nekog broja.

Sljedeće, zamislimo operatore na (x, y, z) za koje je $x^2 + 4yz = p$ je invarijanta, tj. operator koji preslikava rješenja od S na takva rješenja. Dijkstra zatim proučava operatore tipa $(x, y, z) \to (x + \Delta x, y + \Delta y, z + \Delta z)$, gdje Δx nije nula. Zato što za bilo koje rješenje od $(x, y, z) : x^2 + 4yz = p$ vrijednost od x je neparna, i našu pažnju možemo usmjeriti na parne Δx tako da je recimo $\Delta x = 2b$.

Ovdje Dijkstra implicitno pretpostavlja da je Δ operator, za koji $\Delta f(x) = f(x + \Delta x) - f(x)$ tako da na primjer $\Delta(x^2) = (x + \Delta x)^2 - x^2 = 2x\Delta x + (\Delta x)^2$.

Pretpostavka invarijantnosti $\Delta : S \to S$, tj. $(x')^2 + 4y'z' = p$ znači da $\Delta(x^2 + 4yz) = 0$.

Tako dobiva sljedeće jednakosti:

$$\begin{aligned} \Delta(x^2 + 4yz) &= 0 \\ \Delta(x^2) &= -4\Delta(yz) \\ 2x(\Delta x) + (\Delta x)^2 &= -4((y + \Delta y)(z + \Delta z) - yz) \\ b(x + b) &= -y\Delta z - z\Delta y - \Delta y\Delta z. \end{aligned}$$

Najjednostavniji način da se ovo pojednostavi je eliminirati dva ili tri produkta na desnoj strani jednadžbe.

U svrhu pojednostavljenja Dijkstra ovdje bira $\Delta y = 0$, pri čemu se ne gubi na općenitosti jer se u dva koraka može doći do slučaja kad su $\Delta y \neq 0$ i $\Delta z \neq 0$. Sada, $b(x + b) = -y\Delta z$ sugerira sljedeće 4 mogućnosti:

1. $b = -y,\ x + b = \Delta z$, dajući $(x, y, z) \to (x - 2y, y, z + x - y)$

2. $b = y,\ x + b = -\Delta z$, dajući $(x, y, z) \to (x + 2y, y, z - x - y)$

3. $b = \Delta z,\ x + b = -y$, dajući $(x, y, z) \to (-x - 2y, y, z - x - y)$

4. $b = -\Delta z,\ x + b = y$, dajući $(x, y, z) \to (2y - x, y, z + x - y)$-

Zapišimo slučajeve 1 do 4 u obliku $(x, y, z) \to (x', y', z')$. Budući da je B sastavljen od rješenja u prirpdnim brojevia pa mora biti zadovoljeno $x' > 0$, $y' > 0$, $z' > 0$, vidimo da treći slučaj $x' = -x - 2y$ možemo odbaciti. Do sada još nismo koristili činjenicu da bi inv_1 trebao imati točno jednu fiksnu točku. Sada, za fiksnu točku $(x, y, z) = (x', y', z')$ je $x = x'$, a to u prvom i drugom slučaju implicira $y = 0$ što znači da jedino preostaje slučaj 4. Ovdje $x = 2y - x$ pokazuje da se fiksna točka može pojaviti samo ako je $x = y$ tako da $p = x^2 + 4yz = x(x + 4z)$ implicira da je $z = \frac{p-1}{4}$, dajući jedinstvenu fiksnu točku $\left(1, 1, \frac{p-1}{4}\right)$. Dijkstra zatim dovršava konstrukciju involucije inv_1 za rješenja $y > z + x$ odnosno $x > 2y$.

Elsholtz uspoređujući ove dvije različite konstrukcije Zagierovog dokaza iznosi zadovoljstvo postignutom jedinstvenošću i poopćenjem dokaza. U njegovoj je konstrukciji ključan izbor fiksne točke koja na jednostavan i brz način dovodi do cijelobrojnih koeficijenata c, f i i matrice B, a zatim izjednačavanjem koeficijenata jednadžbe bez korištenja svojstva involutornosti dolazi do ostalih koeficijenata matrice. S druge strane, Dijkstra izborom $\Delta y = 0$ dolazi do koeficijenata d, f i e, a nepromjenjivost oblika i razmatranje fiksne točke do ostalih koeficijenata matrice. Ovi kombinatorni dokazi i činjenica da je broj rješenja (x, y, z) danog za $p = x^2 + 4yz;\ x < y - z$ jednak broju rješenja drugog tipa $x > 2y$ pomogli su Elsholtzu za generalizaciju metode.

4.3 Elsholtzova generalizacija metode

Elsholtz 1996. godine daje generalizaciju jednostavnog dokaza ovog teorema idejom Heath Brown-Zagierovog dokaza. Ukratko ćemo opisati poopćenje prethodnog, a detaljna generalizacija opisana je u [8].

Za generalizaciju Elsholtz traži slične involucije za srodni problem prikaza $p = sx^2 + tyz$, gdje su s i t fiksne konstante.

Sljedeća dva teorema proširenja su opet Fermatovih zaključaka. Naime, Fermat je proučavajući zbroj kvadrata zaključio da bi za proste brojeve oblika $x^2 + ny^2$ mogle vrijediti neke pravilnosti te je tako došao do sljedećih tvrdnji:

- Svaki prost broj oblika $8n + 1$ ili $8n + 3$ može se prikazati kao $x^2 + 2y^2$
- Svaki prost broj oblika $3n + 1$ može se prikazati kao $x^2 + 3y^2$.

Kasnije su matematičari došli do većeg broja srodnih pravilnosti, a neke izrečene u sljedećim teoremima pokazat ćemo kroz ovu generalizaciju.

Teorem 4.1. *Neka je p prost broj.*

a) Za $p = 8k + 3$ postoji rješenje za $p = x^2 + 2y^2$ u pozitivnim cijelim brojevima.

b) Za $p = 8k + 7$ postoji rješenje za $p = x^2 - 2y^2$ u pozitivnim cijelim brojevima.

a) Za $p = 8k + 5$ postoji prikaz kao $p = x^2 - 2y^2$.

Teorem 4.2. *Neka p označuje prost broj.*

a) Za $p = 12k + 7$ postoji rješenje za $p = 3x^2 + 4y^2$ u pozitivnim cijelim brojevima.

b) Za $p = 12k + 11$ postoji rješenje za $p = 3x^2 - 4y^2$ u pozitivnim cijelim brojevima.

Sada matrica $B = \begin{pmatrix} -1 & \frac{2m}{n} & 0 \\ 0 & 1 & 0 \\ \frac{4sm}{tn} & \frac{-4sm^2}{tn^2} & 1 \end{pmatrix}$ preslikava rješenja $p = sx^2 + tyz$ na takva rješenja i ima fiksnu točku (m, n, k'). Ovdje su m, n, s i t fiksni nenegativni cijeli brojevi. Dakle, $k' = \frac{p - sm^2}{tn}$. Opet je zadovoljeno $B^2 = I$.

U općem slučaju, međutim, granice određene retcima matrice B, naime $-x + \frac{2m}{n} > 0$ i $\frac{4sm}{tn}x - \frac{4sm^2}{tn^2}y + z > 0$ ne definiraju tako uravnoteženu particiju skupa rješenja na tri dijela.

Ipak, za $p = x^2 + 2y^2$ i $p = 3x^2 + 4y^2$ moguće je zadati prikladna preslikavanja pomoću daljnjih matrica. One se ponovno dobivaju pomoću B i X, a koncepcija nastavka dokaza ostaje ista.

Možemo pokušati iskoristiti matricu $A = BX$, ne vodeći zasad računa o particiji skupa rješenja i granicama određenima retcima matrice. Pritom, geometrijska intuicija navodi na pretpostavku da je $\det A = 1$ ili $\det A = -1$, budući da ne očekujemo da će se veće područje preslikati u manje i obrnuto. Promatrat ćemo svojstvene vrijednosti λ matrice $A = BX$:

$$A = BX = \begin{pmatrix} -1 & \frac{2m}{n} & 0 \\ 0 & 1 & 0 \\ \frac{4sm}{tn} & \frac{-4sm^2}{tn^2} & 1 \end{pmatrix} \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & \frac{2m}{n} \\ 0 & 0 & 1 \\ \frac{-4sm}{tn} & 1 & \frac{-4sm^2}{tn^2} \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 0 & a \\ 0 & 0 & 1 \\ -c & 1 & -d \end{pmatrix}.$$

Primijetimo da je $ac = 2d$. Znamo da je λ rješenje algebarske jednadžbe $\det(A - \lambda I) = 0$ pa imamo:

$$0 = (1-\lambda)(0-\lambda)(-d-\lambda) - (1-\lambda) - (-c)(0-\lambda)a = (\lambda+1)(\lambda^2+(d-2)\lambda+1).$$

Nalazimo da je $\lambda_1 = -1$ i $\lambda_{2,3} = \frac{-d-2}{2} \pm \sqrt{\left(\frac{d-2}{2}\right)^2 - 1}$.

Za cijele brojeve $d \geq 5$ ili $d \leq -1$, vrijednosti $\lambda_{2,3}$ su realni, ali iracionalni brojevi. Iracionalne vrijednosti ne čine se povoljnima za konstrukciju preslikavanja koje bi bilo sastavljeno od konačno mnogo dijelova. Dakle, promatramo slučajeve $d = 0, 1, 2, 3, 4$ i u tim slučajevima $|\lambda_1| = |\lambda_2| = |\lambda_2| = 1$. Ovime je zadovoljeno i naše očekivanje da je $\det A = 1$.

Budući da je $d = \frac{4sm^2}{tn^2}$, želimo predstaviti proste brojeve s $p = sx^2 + tyz = sm^2 + tnz$. Možemo pretpostaviti da je $\text{nzd}(sm, tn) = 1$. Istaknimo samo prva dva slučaja,

1. Za $d = 0$ imamo $sm = 0$, tako da je $p = tnz$. Ovaj slučaj nije od interesa.

2. Za $d = 1$ i $(s, t) = (s, n) = (t, m) = (m, n) = 1$ imamo dvije mogućnosti:

2.1. $s = m = n = 1$, $t = 4$. Upravo je to slučaj Heath-Brownovog i Zagierovog dokaza.

2.2. $s = m = t = 1$, $n = 2$.

Ovaj slučaj vodi do varijante dokaza za sumu dva kvadrata, pri čemu se promatraju (x, y, z) takvi da su y i z parni te vrijedi $x^2 + yz = p$. Sve je inače slično kao u Zagierovom dokazu te nećemo izložiti pojedinosti. Također ovdje nećemo navesti analizu ostalih slučajeva za vrijednosti d. Ta razmatranja uglavnom su složenija od prethodnih, a kao rezultate daju nove dokaze Teorema 4.1. i 4.2.

4.4 Elsholtzova kratka verzija teorema o zbroju dva cjelobrojna kvadrata

Inspiriran Zagierovom kratkoćom u dokazu, Christian Elsholtz daje svoju verziju kratkog dokaza koju smatra lakše pamtljivom od Zagierove verzije. Dokaz glasi:

Involucija na konačnom skupu $S = \{2 \leq a \leq \frac{p-1}{2}\}$ definirana s

$$a \to \begin{cases} a^{-1}(\text{mod } p), \text{ ako } 2 \leq (a^{-1}(\text{mod } p)) \leq \frac{p-1}{2} \\ a^{-1}(\text{mod } p), \text{ inače} \end{cases}$$

ima barem jednu fiksnu točku z takvu da fundamentalna domena rešetke

$$L_z = \{(x, zx(\text{mod } p)),\ 0 \leq x < p\}$$

ima oblik kvadrata površine p, tako da teorem o zbroju kvadrata slijedi primjenom Pitagorinog teorema.

U [8] Elsholtz daje i dulju verziju ovog dokaza, odnosno potpuno objašnjenje. Za razumijevanje Elsholtzova dokaza potrebno je znati algoritam za rješavanje linearne kongruencije koji se zasniva na Proširenom Euklidovom algoritmu. Znamo da je kongruencija $ax \equiv 1(\text{ mod } m)$ rješiva ako i samo ako je $\text{nzd}(a, m) = 1$ te u tom slučaju ima jedinstveno rješenje u $\mathbb{Z}_m$. To je rješenje modularni inverz od a, odnosno to je rješenje jedinstveni multiplikativni inverz od $a_0 \in \mathbb{Z}_m$ u prstenu $\mathbb{Z}_m$, gdje vrijedi $a_0 \equiv a(\text{mod } m)$, njegova je oznaka a^{-1}. Promotrimo li preslikavanje $f : S \to S$, f je preslikavanje koje zadovoljava $f(f(a)) = f(a^{-1}) = (a^{-1})^{-1} = a$ i slično $f(f(a)) = f(-a^{-1}) = -(-a^{-1})^{-1} = a$, dakle f je involucija jer za svaki $a \in S : f(f(a)) = a$. Budući da $|S|$ je neparan, mora postojati neparan broj (tj. najmanje jedan) elemenata takav da $a = f(a)$. Budući da $-1, 1 \notin S$, slijedi da $(a+1)(a-1) \equiv 0(\text{mod } p)$ nema rješenja u $|S|$

što implicira da $a \equiv a^{-1} (\text{mod } p)$ nema rješenja. No, tada mora postojati element $a \equiv -a^{-1} (\text{mod } p)$, odnosno taj element zadovoljava $a^2 \equiv -1 (\text{mod } p)$.

Sada treba pobliže razmotriti kako skupovi L_z "popločavaju" skup $\mathbb{Z}_p \times \mathbb{Z}_p$. Ti skupovi sastoje se od međusobno sukladnih paralelograma, razapetih po jednom točkom i s dva od njezina četiri najbliža susjeda, u linearno nezavisnim smjerovima. Svaki paralelogram je jedna fundamentalna domena pojedine rešetke, a rešetaka ima koliko i elementa skupa S, dakle $\frac{p-1}{2} - 1$. Slučaj $a^{-1} \equiv -1 (\text{mod } p)$ znači da su smjerovi stranica paralelograma međusobno okomiti (poznati uvjet za koeficijente okomitih smjerova). Stoga je taj paralelogram pravokutnik. Invarijantnost rešetke pod djelovanjem preslikavanja f znači da je rešetka invarijantna pri rotaciji za pravi kut pa je taj pravokutnik kvadrat. Površinu tog kvadrata dobivamo dijeljenjem p^2 kao površine "ploče" $\mathbb{Z}_p \times \mathbb{Z}_p$ s brojem kongruentnih kvadrata kojima je pokrivena, a taj broj je p. Dakle, površina ove kvadratne fundamentalne domene jednaka je p. Njezina stranica ima duljinu $\sqrt{p}$, a to je hipotenuza pravokutnog trokuta s katetama cjelobrojnih duljina. Time je teorem dokazan.

5 A. D. Christopherov dokaz

U zadnjem dijelu rada predstavit ćemo elementarniji tip dokaza Fermatovog teorema o dva kvadrata pomoću teorije particija. Jednostavno rečeno, particije broja su načini zapisivanja tog broja kao zbroja pozitivnih cijelih brojeva. Primjerice, tri particije broja 3 su 3, $2+1$, $1+1+1$. Naizgled jednostavna misao donijela je brojne rezultate i novitete, zaokupljala je matematičare kroz povijest pa sve do danas. Koncept particije dao je Euler u 18. stoljeću, a teoriju particije su proučavali brojni poznati matematičari. Particije ([14]) u primjenama se može naći gdje god se diskretni objekti trebaju brojati ili klasificirati, bilo u molekularnim i atomskim znanstvenim istraživanjima, statističkoj mehanici, u teoriji brojeva ili u kombinatornim problemima.

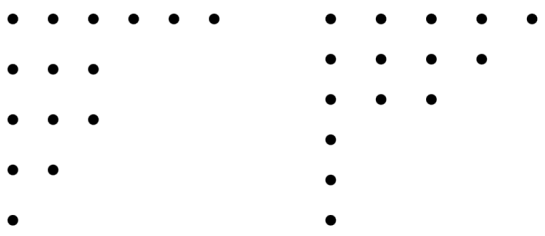
Počinjemo s osnovnim definicijama i oznakama potrebnim u nastavku. Dokaz prema [3].

Definicija 5.1. *Particija pozitivnog cijelog broja je konačan nerastući niz pozitivnih cijelih brojeva $\pi = (x_1, x_2, \ldots, x_m)$ tako da $x_1 + x_2 + \ldots + x_m = n$. Pojedini x_i naziva se dio particije π, a vrijednosti dijelova koje se pojavljuju u particiji nazivaju se veličinama particije π. Više različitih dijelova mogu imati jednaku veličinu. Stoga pišemo, $\pi = (a_1^{f_1} a_2^{f_2} \ldots)$ pri čemu je $a_1 > a_2 > \ldots$, ako se veličina a_i javlja točno f_i puta u particiji π.*

Definicija 5.2. *Neka je $\pi = (a_1^{f_1} a_2^{f_2})$ particija n s točno dvije veličine. Tada se particija $C(\pi) = ((f_1 + f_2)^{a_2} f_i^{a_1 - a_2})$ naziva konjugat particije π.*

Definicija 5.3. *Neka je $\pi = (a_1^{f_1} a_2^{f_2})$ particija n s točno dvije veličine takva da je $f_1 \neq f_2$. Tada se particija $T(\pi) = (f_1^{a_1} f_2^{a_2})$ (odnosno, $(f_2^{a_2} f_a^{a_1})$) kada $f_1 > f_2$ (odnosno, $f_2 > f_1$) naziva transpozicija particije π.*

Posebno je zanimljiv grafički prikaz particija. Postoji više načina kako particiji pridružiti dijagram, najpoznatiji prikaz particije je Ferrerovim dijagramom. Takav prikaz olakšava brojne dokaze različitih kombinatornih identiteta. „Čvorovi“ se mogu brojati u stupcima umjesto u retcima. Dvije particije proizvedene iz takvog grafa su konjugati. Parovi particija za jedan broj čiji se Ferrerovi dijagrami pretvaraju jedan u drugi kada se zrcale oko pravca $y = -x$, s koordinatama gornje lijeve točke uzete kao $(0, 0)$, jesu konjugati (ili transpozicija) particije. Na primjer, Slika 3, gore ilustrirane konjugirane particije odgovaraju particijama $6+3+3+2+1$ i $5+4+3+1+1+1$ od 15. Postoje particije koje su jednake svom konjugatu i njih nazivamo samokonjugirane particije.



Slika 3: Primjer konjugirane particije prikazane Ferrovim dijagramom

Neka je n neparan prost broj i neka P_2^n označava skup particija od n s točno dvije veličine. Tada za svaki $\pi \in P_2^n$, imamo $C(\pi) \in P_2^n$ i za svaki $(a_1^{f_1} a_2^{f_2})$ takav da $f_1 \neq f_2$, imamo $T((a_1^{f_1} a_2^{f_2})) \in P_2^n$.

Za dokaz teorema prvenstveno pokazujemo

$$|P_2^n| \equiv 1 (\text{mod } 2). \tag{2}$$

Promatramo konjugiranje kao preslikavanje $C : P_2^n \to P_2^n$. Budući da vrijedi $C(C(\pi)) = \pi$, iz involutorne prirode preslikavanja slijedi da je C bijekcija. Skup P_2^n sastoji se od samokonjugiranih particija i od parova $(\pi, C(\pi)$ particija takvih da je $\pi \neq C(\pi)$. Stoga je razlika ukupnog broja elemenata od P_2^n i broja samokonjugiranih particija paran broj. Označimo li broj samokonjugiranih particija s $SC_2(n)$, vrijedi:

$$|P_2^n| \equiv SC_2(n) (\text{mod } 2).$$

Tvrdimo da $SC_2(n) = 1$. Ako je $(a_1^{f_1} a_2^{f_2}) \in P_2^n$ samokonjugirana particija, onda $f_1 = a_2$ i $f_2 = a_1 - a_2$ i obrnuto. Dakle, u ovom slučaju mora vrijediti sljedeća jednakost: $n = a_1 a_2 + a_2(a_1 - a_2) = a_2 = (2a_1 - a_2)$. Budući da je n prost broj, iz prethodno spomenute jednakosti slijedi da ili $a_2 = 1$ ili $2a_1 - a_2 = 1$. Sada vidimo da je jednakost $2a_1 - a_2 = 1$ nemoguća; jer ako $2a_1 - a_2 = 1$, onda opet pretpostavka da je n prost implicira da $a_2 = n$, kršeći trivijalnu nejednakost: $a_1 f_1 + a_2 f_2 > a_2$. Nadalje, vidimo da: ako $a_2 = 1$ onda jednostavni izračun daje $a_1 = \frac{n+1}{2}$, $f_1 = 1$ i $f_2 = \frac{n-1}{2}$. Time je utvrđena jedinstvenost samokonjugirane particije.

Odredimo paritet od $|P_2^n|$ na drugi način. Promotrimo skup

$$A = \{(a_1^{f_1} a_2^{f_2}) \in P_2^n : f_1 \neq f_2; f_1 \neq a_1 \text{ ili } f_2 \neq a_2\}$$

i transponiranje kao preslikavanje $T : A \to A$. Jasno je da je T involutorno preslikavanje bez fiksne točke. Zatim slijedi da $|A| \equiv 0 (\text{mod } 2)$. Razmotrimo

skup $P_2^n - A$, za koji će se pojaviti sljedeći slučajevi:

Slučaj 1. $f_1 = f_2$. Budući da je n prost, imamo $f_1 = f_2 = 1$. Dakle, koje pripadaju ovom slučaju jednak je broju načina kojim se n može zapisati kao zbroj dva različita dijela. Jasno, ovaj broj je $\lfloor \frac{n-1}{2} \rfloor$, gdje $\lfloor \cdot \rfloor$ označavamo funkciju najveće cijelo.

Slučaj 2. $f_1 \neq f_2$, s $a_1 = f_1$ i $a_2 = f_2$. S $R_2(n)$ označavamo broj particija koje leže u ovom slučaju. Uočimo da $R_2(n)$ izražava broj načina na koji se n može predstaviti kao zbroj dva različita kvadrata.

Kao posljedicu dobivamo $|P_2^n| = |A| + \lfloor \frac{n-1}{2} \rfloor + R_2(n)$. Budući da $|A| \equiv 0 (\bmod 2)$, imamo sljedeću kongruenciju:

$$|P_2^n| \equiv \lfloor \frac{n-1}{2} \rfloor + R_2(n) (\text{mod } 2) \tag{3}$$

Sada zbrajanjem kongruencija (1?), (2?) dobivamo:

$$\lfloor \frac{n-1}{2} \rfloor + R_2(n) + 1 \equiv 0 (\text{mod } 2) \tag{4}$$

Za $n \equiv 1 (\text{mod } 4)$ slijedi $\lfloor \frac{n-1}{2} \rfloor \equiv 0 (\text{mod } 2)$. Iz (3?) slijedi da $R_2(n) \equiv 1 (\text{mod } 2)$, što implicira $R_2(n) \geq 1$, kada $n \equiv 1 (\text{mod } 4)$. Time je dokaz završen.

Ideju dokaza proći ćemo kroz primjer kako bi ga približili čitatelju.

Neka je $n = 5$, njega možemo prikazati kao zbroj sljedećih brojeva

$$\begin{aligned} 5 &= 5 \\ 5 &= 4 + 1 \\ 5 &= 3 + 2 \\ 5 &= 3 + 1 + 1 \\ 5 &= 2 + 2 + 1 \\ 5 &= 2 + 1 + 1 + 1 \\ 5 &= 1 + 1 + 1 + 1 + 1 \end{aligned}$$

$\pi = (a_1^{f_1} a_2^{f_2})$ particija n s točno dvije veličine, dakle $\pi_1 = (4^1 1^1)$, $\pi_2 = (3^1 2^1)$, $\pi_3 = (3^1 1^2)$, $\pi_4 = (2^2 1^1)$ i $\pi_5 = (2^1 1^3)$.

Sada imamo, $C(\pi_1) = (2^1 1^3)$, $C(\pi_2) = (2^2 1^1)$, $C(\pi_3) = (3^1 1^3)$, $C(\pi_4) = (3^1 2^1)$ i $C(\pi_5) = (4^1 1^1)$. Lako se uoči kako je $\pi_3 = (3^1 1^2)$ samokonjugirana particija.

$P_2^n = \{(4^1 1^1), (3^1 2^1), (3^1 1^2), (2^2 1^1), (2^1 1^3)\}$ vidimo da je $|P_2^n| = 5 \equiv 1 (\mathrm{mod}\ 2)$.

$SC_2(n)$ označava broj samokonjugiranih particija od $|P_2^n|$, kao što je već rečeno, a samo je jedna samokonjugirana particija, pa je zadovoljeno $|P_2^n| \equiv SC_2(n) (\mathrm{mod}\ 2)$.

Drugi način izvođenja pariteta daje nam

$$A = \{(a_1^{f_1} a_2^{f_2}) \in P_2^n : f_1 \neq f_2 \text{ uz uvjet } f_1 \neq a_1 \text{ ili } f_2 \neq a_2\} = \{(3^1 1^2), (2^1 1^3)\},$$

time je zadovoljeno i $|A| \equiv 0 (\mathrm{mod}\ 2)$.

Broj particija za koje vrijedi $f_1 = f_2$ jednak je $\lfloor \frac{n-1}{2} \rfloor = 2$. To su $\pi_1 = (4^1 1^1)$ i $\pi_2 = (3^1 2^1)$.

Broj particija za koje vrijedi $f_1 \neq f_2$ s $a_1 = f_1$ i $a_2 = f_2$ jednak je $R_2(n) = 1$. To je $\pi_4 = (2^2 1^1)$. Na ovom primjeru prošli smo sve tvrdnje dokaza.

6 Zaključak

Fermatov ili ne, rezultat o prikazu prostog broja kao zbroja dva kvadrata inspirirao je mnoge matematičare i njihova istraživanja odveo u nekoliko smjerova. Teoriju brojeva povezali su s kombinatorikom, pronašli geometrijska tumačenja, primijenili teoriju particija te razmatranja fiksnih točaka domišljato zadanih preslikavanja na načine koji podsjećaju na metode u topologiji. Od metode neprekidnog silaska koju su počeli koristiti veliki matematičari u 17. i 18. stoljeću do vrlo konciznih dokaza krajem 20. stoljeća, generacije matematičara težile su čim elegantnijem, ali i transparentijem pristupu već odavno riješenom osnovnom problemu.

Zagier nam daje profinjen i kratak dokaz „u jednoj rečenici“, ali ta kratkoća ne znači nužno i lakoću. Zato je njegov dokaz privukao pozornost mnogih drugih matematičara koji su nastojali postići još dublji uvid u srž problema. Različiti pristupi mogu potaknuti čitatelja na dodatno učenje, upoznati ga s područjima o kojima možda nije znao gotovo ništa i inspirirati ga na neki njemu svojstven način razmišljanja. Premda je u nekim pristupima potrebno provesti dosta rutinskih koraka uz pažljivu provjeru pojedinih slučajeva, redovito se razabiru nadahnute i inovativne zamisli koje leže u njihovoj osnovi.

Moglo bi se reći „za svakoga ponešto“, a elegancija i ljepota matematike zapravo i leži u jednostavnosti, logičnosti i različitim načinima razmišljanja koji često novim putovima vode prema istom zaključku.

Literatura

[1] G. E. Andrews, *The Theory of Partitions*. Cambridge University Press, SAD, 1998.

[2] J. Cafuk, *O nekim Eulerovim doprinosima u teoriji brojeva*, dostupno na `https://urn.nsk.hr/urn:nbn:hr:217:863766`, siječanj 2022.

[3] A. D. Christopher, *A partition-theoretic proof of Fermat's Two-Squares Theorem*. Discrete Mathematics, 339(2016), str. 1410–1411.

[4] B. Dakić, *Pierre de Fermat (1601.-1665.)*. MIŠ, 10(2001), str. 219–221.

[5] E. W. Dijkstra, *A derivation of a proof by D. Zagier*, dostupno na `https://www.cs.utexas.edu/users/EWD/ewd11xx/EWD1154.PDF`, ožujak 2022.

[6] G. Dubach i F. Han, *Formal verification of Zagier's one-sentence proof*, dostupno na `https://arxiv.org/pdf/2103.11389v2.pdf`, siječanj 2022.

[7] A. Dujella, *Teorija brojeva*. Školska knjiga, Zagreb, 2019.

[8] C. Elsholtz, *A combinatorial approach to sums of two squares and related problems*, dostupno na `https://www.math.tugraz.at/~elsholtz/WWW/papers/papers30nathanson-new-address3.pdf`, siječanj 2022.

[9] C. Elsholtz, *Primzahlen der Form $4k+1$ sind Summe zweier Quadrate*. Mathematiklehren, 62(1994), str. 58–61.

[10] D. R. Heath-Brown, *Fermat's two-squares theorem*. Invariant, 1984., str. 3–5.

[11] M. D. Hirschhorn, *A Simple Proof of Jacobi's Two-Square Theorem*. The American Mathematical Monthly, 92(1985), str. 579–580.

[12] T. Jackson, *A Short Proof That Every Prime $p \equiv 3 (\mathrm{mod}\ 8)$ is of the Form x^2+2y^2*. The American Mathematical Monthly, 107(2000), str. 447.

[13] P. Međimurec, *Algoritmi elementarne teorije brojeva i neke njihove primjene*, dostupno na `https://urn.nsk.hr/urn:nbn:hr:217:301717`, siječanj 2022.

[14] I. Petrić, *Particije Rogers-Ramanujanovog tipa*, dostupno na `https://urn.nsk.hr/urn:nbn:hr:126:210776`, travanj 2022.

[15] V. Plantak, *Fermatov doprinos u teoriji brojeva*, dostupno na `https://urn.nsk.hr/urn:nbn:hr:217:946216`, siječanj 2022.

[16] D. Zagier, *A one-sentence proof that every prime* $p \equiv 1 (\mathrm{mod}\ 4)$ *is a sum of two squares*. The American Mathematical Monthly, 97(1990), str. 144.

Sažetak

Jedan od klasičnih rezultata elementarne teorije brojeva je Fermatov teorem da se svaki prost broj može prikazati kao zbroj dva cjelobrojna kvadrata. Iako se teorem pripisuje Fermatu, tvrdnju je još ranije iskazao Girard, bez dokaza. Nije utvrđeno ni postojanje Fermatovog dokaza te prvi pouzdani dokaz potječe od Eulera. Kasnije su brojni matematičari objavili različite nove dokaze, a glavni je cilj ovog rada prikazati neke od tih dokaza koji su se pojavili u novije vrijeme.

U radu je prvo ponuđena verzija dokaza koja se može smatrati klasičnom i pristupačnom, a nakon toga slijede dokazi za koje je potrebno pristup nadograditi daljnjim pojmovima i idejama . Od modernijih dokaza prikazan je onaj Zagierov, poznat kao „dokaz u jednoj rečenici“. Taj je inspiriran Heath-Brownovim dokazom pa je izložena i njegova ideja. Nadalje, uvršteno je objašnjenje Zagierova dokaza koje je dao Elsholtz, u želji da široj publici pojednostavi i protumači dokaz, sa svim potrebnim provjerama koje su izostavljene u Zagierovu krajnje sažetom članku. Zanimljiva je i geometrijska interpretacija kojom se vizualno vjetrenjačama dočarava Zagierov pristup. U radu je objašnjeno i kako sam dokaz učiniti konstruktivnim, a zatim i Elsholtzova kratka varijanta dokaza Zagierom. Na kraju rada predstavljen je potpuno drugačiji pristup A. D. Christophera koji koristi teoriju particija.

Summary

One of the classic results of elementary number theory is Fermat's theorem that every prime number $p \equiv 1 (\mathrm{mod}\ 4)$ can be represented as the sum of two integer squares. Although the theorem is attributed to Fermat, Girard made the claim even earlier, without proof. The existence of Fermat's proof has not been confirmed, and the first reliable evidence originates from Euler. Later, a number of mathematicians published various new proofs, and the primary objective of this paper is to present some of these proofs that have emerged in recent times.

The paper first offers a version of the proof that can be considered classic and accessible, followed by proof for which the approach needs to be upgraded with further concepts and ideas. Of the modern proofs, Zagier's proof is presented, also known as the „one-sentence proof". The proof from Heath-Brown inspired him, so this idea is also shown. Furthermore, an explanation of Zagier's proof provided by Elsholtz is included, in an aspiration to simplify and interpret the proof to a wider audience, with all the necessary analysis omitted in Zagier's extremely concise article. A geometric interpretation is also interesting, as it visually evokes Zagier's approach using polygons with shapes reminiscent of windmills. It is also explained how to make the proof itself constructive, and furthermore Elsholtz's short version of the proof is presented. At the end of the paper, a completely different approach of A. D. Christopher using partition theory is presented.

Životopis

Rođena sam 10.02.1996. godine u Zagrebu. U razdoblju od 2002./2003. do 2009./2010. pohađala sam Osnovnu školu Sesvetska Sela. Sudjelovala sam 2010. godine na INOVI izložbi inovacija učenika zagrebačkih osnovnih, srednjih škola i studenta s međunarodnim sudjelovanjem na kojoj sam osvojila srebrnu medalju za svoj rad. Zatim sam svoje školovanje nastavila od 2010./2011. do 2013./2014. u Općoj gimnaziji Sesvete. Akademske godine 2014./2015. sam upisala Prirodoslovno - matematički fakultet u Zagrebu, preddiplomski studij, matematika, nastavnički smjer te sam stekla titulu sveučilišnog prvostupnika edukacije matematike. Zatim sam akademske godine 2018./2019. upisala diplomski studij, matematika, nastavnički smjer na istoimenom fakultetu. Osim matematičkog znanja, tijekom svog školovanja kroz volontiranje i radeći brojne studentske poslove stekla sam vještine kao što su prilagođavanje, marljivost i timski rad.