Vsote dveh kvadratov

Lovro Kastelic, Marsela Supé Vide, Tija Vidmar
Mentor: Izak Jenko

Povzetek

V članku smo raziskovali, katera naravna števila so predstavljiva – jih je mogoče zapisati kot vsoto dveh popolnih kvadratov. Osredotočili smo se predvsem na praštevila. Definirali smo kongruentnost ter podrobno pojasnili in dokazali mali Fermatov izrek. Predstavljivost praštevil smo predstavili geometrijsko s pomočjo krilatih kvadratov. Dokazano smo nato uporabili za odgovor na vprašanje o predstavljivosti sestavljenih naravnih števil.

1 Uvod

Za vse so krivi Francozi. Mogoče se sprašujete, kaj imajo Francozi skupnega z vsotami dveh kvadratov, vendar vam zagotavljamo, da boste kmalu izvedeli, zakaj sta Fermat in Pascal pomembna.

Vsote dveh kvadratov predstavljajo zanimiv matematični koncept, ki spada v matematično področje, imenovano teorija števil. Že antični matematiki so se ukvarjali s to temo, ki se je skozi zgodovino razvila v eno najbolj fascinantnih področij matematike.

Definicija 1. *Pravimo, da je število $n \in \mathbb{N}$* ***predstavljivo****, če ga lahko zapišemo kot vsoto dveh popolnih kvadratov, torej če obstajata taki celi števili $x,\ y \in \mathbb{Z}$, da je*

$$n = x^2 + y^2.$$

Opomba. Celo število je *popoln kvadrat*, če je oblike k^2 za neko celo število $k \in \mathbb{Z}$. V nadaljevanju bomo zavoljo jedrnatosti pridevnik *popoln* pogosto izpuščali in popolne kvadrate imenovali samo kvadrati.

Poglejmo naravna števila do 20 in jih poskusimo zapisati kot vsoto dveh kvadratov. Ugotovimo, da tak zapis ni mogoč za vsa števila, kot nas prepriča tabela 1. Naiven način, kako za naravno število n preverimo, ali je predstavljivo ali ne, je sledeč. Zapišemo si vse kvadrate pozitivnih celih števil, ki so manjši ali enaki n, in si ogledamo njihove razlike od n. Če je kakšna od teh razlik popoln kvadrat, smo našli zapis števila n kot vsoto dveh kvadratov in je torej predstavljivo, sicer pa ni predstavljivo. Na primer popolni kvadrati manjši ali enaki številu 19 so $0,\ 1,\ 4,\ 9$ in 16, njihove razlike do 19 pa so zaporedoma $19,\ 18,\ 15,\ 10$ in 3. Ker nobeno od teh *ni* popoln kvadrat, število 19 ni predstavljivo.

Tekom tega članka bomo spoznali izrek, ki nam bo brez intenzivnega računanja povedal, kdaj je naravno število n predstavljivo, če le poznamo njegov praštevilski razcep.

Tabela 1: Števila kot vsote dveh kvadratov.

$1 = 1^2 + 0^2$	$6 \neq$	$11 \neq$	$16 = 4^2 + 0^2$
$2 = 1^2 + 1^2$	$7 \neq$	$12 \neq$	$17 = 4^2 + 1^2$
$3 \neq$	$8 = 2^2 + 2^2$	$13 = 3^2 + 2^2$	$18 = 3^2 + 3^2$
$4 = 2^2 + 0^2$	$9 = 3^2 + 0^2$	$14 \neq$	$19 \neq$
$5 = 2^2 + 1^2$	$10 = 3^2 + 1^2$	$15 \neq$	$20 = 4^2 + 2^2$

1.1 Produkt kot vsota dveh kvadratov

Prvo splošno opazko o predstavljivih številih povzame naslednja trditev, ki pove, da je produkt predstavljivih števil spet predstavljivo število.

Trditev 1. *Če lahko dve naravni števili $n = x^2 + y^2$ in $m = z^2 + w^2$ napišemo kot vsoto dveh kvadratov, lahko tudi njun produkt zapišemo kot vsoto dveh kvadratov.*

Dokaz. Izračunamo

$$\begin{aligned} n \cdot m &= (x^2 + y^2)(z^2 + w^2) \\ &= x^2z^2 + x^2w^2 + y^2z^2 + y^2w^2 \\ &= x^2z^2 + x^2w^2 + y^2z^2 + y^2w^2 + 2xyzw - 2xyzw \\ &= (xz + yw)^2 + (xw - yz)^2. \end{aligned}$$

V tretji vrstici smo prišteli in odšteli $2xyzw$ in s tem dopolnili po dva člena iz druge vrstice do dveh popolnih kvadratov. □

2 Osnove teorije števil

2.1 Praštevila

Eden izmed najbolj osnovnih objektov v teoriji števil so *praštevila*. Praštevilo je naravno število večje od 1, katerega edina delitelja sta 1 in število samo. Njihovo pomembnost poudarja znameniti osnovni izrek aritmetike.

Izrek 2 (Osnovni izrek aritmetike)**.** *Vsako naravno število večje od* 1 *je produkt praštevil, ki je enoličen do vrstnega reda faktorjev natančno.*

V luči našega osnovnega problema, bomo znali s pomočjo faktorizacije odločiti o predstavljivosti sestavljenih števil, ko ugotovimo, katera praštevila so predstavljiva.

2.2 Osnovni izrek o deljenju

Spomnimo se osnovnega izreka o deljenju.

Izrek 3 (Osnovi izrek o deljenju)**.** *Naj bosta a in b poljubni celi števili, pri čemer $b \neq 0$. Če delimo a z b, potem obstajata celi števili q in ostanek r, da velja*

$$a = q \cdot b + r.$$

Ostanek je vedno večji ali enak 0 *in manjši od delitelja* ($0 \leq r < b$).

Številoma q in r iz zgornjega izreka pravimo *količnik* in *ostanek*. Naslednja trditev nam pove, da sta ti dve količini enolično določeni s številoma a in b, zato je na primer smiselno govoriti o *ostanku števila a pri deljenju z b*.

Trditev 4. *Za vsak par* $a,\ b \in \mathbb{Z}$ *sta števili* q *in* r *iz zgornjega izreka o deljenju enolična.*

Dokaz. Če bi za par $a,\ b \in \mathbb{Z}$ obstajal še en par $q',\ r' \in \mathbb{Z}$, za katerega je

$$a = q'b + r' \quad \text{in} \quad 0 \leq r' < b,$$

bi lahko število a zapisali na dva načina

$$q \cdot b + r = a = q' \cdot b + r'.$$

S preurejanjem enačbe dosežemo

$$(q - q')b = r' - r.$$

Ker je $|r' - r| < b$, sledi

$$|q - q'| < 1.$$

Števili q in q' sta celi, zato se slednje lahko to zgodi le, če sta enaki. Od tod sklepamo tudi $r = r'$. □

Definicija 2. *Če vzamemo števili* $a,\ b \in \mathbb{Z}$*, potem število* b ***deli*** *število* a*, ko obstaja število* $k \in \mathbb{Z}$*, da je*

$$a = k \cdot b.$$

Pravimo tudi, da je število a ***večkratnik*** *števila* b*. To označimo z* $b \mid a$*. Kadar število* b ne *deli* a*, pišemo tudi* $b \nmid a$*.*

Opazimo, da število b deli število a natanko tedaj, ko je ostanek a pri deljenju z b enak 0.

Trditev 5. *Denimo, da za* $n \in \mathbb{N}$ *in* $a,\ b \in \mathbb{Z}$ *velja* $n \mid a$ *in* $n \mid b$*, potem velja*

$$n \mid ab \quad in \quad n \mid a + b.$$

Dokaz. Zapišimo $a = a_0 n$ in $b = b_0 n$, kjer sta $a_0,\ b_0 \in \mathbb{Z}$. Potem lahko produkt teh števil zapišemo kot

$$\begin{aligned} ab &= a_0 b_0 n^2 \\ &= (a_0 b_0 n)n, \end{aligned}$$

iz česar je razvidno, da $n \mid ab$. Podobno velja tudi za vsoto dveh števil

$$\begin{aligned} a + b &= a_0 n + b_0 n \\ &= (a_0 + b_0)n, \end{aligned}$$

kar potrdi, da $n \mid a + b$. □

2.3 Kongruence

V nadaljevanju želimo računati z ostanki, kar formaliziramo z vpeljavo pojma *kongruentnosti* števil.

Definicija 3. *Dve števili* $a,\ b \in \mathbb{Z}$ *sta* ***kongruentni*** *po modulu* n*, kadar velja*

$$n \mid a - b.$$

To označimo z

$$a \equiv b \mod n.$$

Trditev 6. *Kongruentni števili imata pri deljenju z* n *isti ostanek.*

Dokaz. Če imamo dve števili $a = q_1 n + r_1$ in $b = q_2 n + r_2$, kjer je $n \in \mathbb{N}$, potem lahko njuno razliko zapišemo kot

$$\begin{aligned} a - b &= q_1 n + r_1 - q_2 n - r_2 \\ &= (q_1 - q_2)n + (r_1 - r_2). \end{aligned}$$

Če iz te enačbe izoliramo razliko ostankov, ugotovimo, da je sestavljena iz razlike dveh celih števil, ki sta deljivi z n.

$$\begin{aligned} r_1 - r_2 &= (a-b) - (q_1 - q_2)n \\ &= k \cdot n - (q_1 - q_2)n \end{aligned}$$

Število $a - b$ namreč lahko zapišemo kot večkratnik števila n, kar pomeni, da obstaja $k \in \mathbb{Z}$, da je $a - b = k \cdot n$. Tako ugotovimo, da $n \mid r_1 - r_2$. Ker pa sta oba ostanka manjša od n in brez škode za splošnost predpostavimo še $r_2 \leq r_1$, je možno le, da sta ostanka enaka, torej $r_1 = r_2$. □

Naslednja trditev je zelo pomembna, saj nam bo v nadaljevanju bistveno poenostavila računanje s kongruencami.

Trditev 7. *Imejmo po dva para kongruentnih celih števil* $a \equiv a' \mod n$ *in* $b \equiv b' \mod n$*, pri čemer je* $n \in \mathbb{N}$*. Potem velja*

$$a + b \equiv a' + b' \mod n \quad in \quad ab \equiv a'b' \mod n.$$

Dokaz. Kadar sta števili kongruentni po modulu n, število n deli njuno razliko. Torej lahko v našem primeru zapišemo

$$a - a' = n \cdot v \quad \text{in} \quad b - b' = n \cdot u,$$

za neka $u,\ v \in \mathbb{Z}$. Trdimo, da je $a + b \equiv a' + b' \mod n$. Poglejmo njuno razliko

$$\begin{aligned} a + b - (a' + b') &= a - a' + b - b' \\ &= nv + nu \\ &= n \cdot (v + u). \end{aligned}$$

Torej $n \mid a + b - (a' + b')$, kar dokaže želeno.

Dokažimo še drugi del trditve, ki pravi, da je $ab \equiv a'b' \mod n$. Poglejmo razliko zmnožkov

$$\begin{aligned} ab - a'b' &= ab - a'b' - a'b + a'b \\ &= b(a - a') + a'(b - b') \\ &= b \cdot nv + a' \cdot nu \\ &= n \cdot (bv + a'u). \end{aligned}$$

V prvi vrstici smo odšteli in prišteli isto količino $a'b$ in po izpostavljanju ustreznih členov dobili, da $n \mid ab - a'b'$, kar pokaže zatrjeno. □

3 Krilati kvadrati

Sedaj smo pripravljeni za izrek, ki pove, katera praštevila so predstavljiva. Presenetljivo in precej zvito bomo izrek dokazali z uporabo geometrije. Vpeljali bomo t. i. *krilate kvadrate* in preučili njihovo obnašanje in povezavo s predstavljivostjo praštevil. Sledili bomo dokazu iz knjige [1, Chapter 4], ki ga je našel moskovski matematik Alexander Spivak.

Izrek 8. *Naj bo* $p \in \mathbb{N}$ *praštevilo.*

1. *Če velja* $p = 2$ *ali* $p \equiv 1 \mod 4$*, potem je* p *mogoče zapisati kot vsoto dveh kvadratov.*
2. *Če je* $p \equiv 3 \mod 4$*, praštevila* p *ni mogoče zapisati kot vsoto dveh kvadratov.*

Dokaz. Drugi del izreka je mnogo lažje dokazati kot prvega, zato začnimo z njim. Potrebujemo le lastnosti računanja s kongruencami iz trditve 7.

Trditev pokažimo s protislovjem. Recimo, da je preštevilo p predstavljivo, torej je $p = x^2 + y^2$ za neka $x,\ y \in \mathbb{Z}$. Če na to enakost pogledamo po modulu 4, dobimo

$$3 \equiv x^2 + y^2 \mod 4. \tag{1}$$

Z izračunom kvadratov števil 0, 1, 2 in 3 (to so vsi možni ostanki celega števila pri deljenju s 4) vidimo, da je ostanek kvadrata pri deljenju s 4 lahko le 0 ali 1. Desna stran enačbe (1) torej zavzame le vrednosti 0, 1 ali 2 in *ne* 3. Predpostavka o predstavljivosti praštevila p je torej neresnična, zato p ni mogoče zapisati kot vsoto dveh kvadratov.

Lotimo se še prvega dela. Definirajmo množico

$$S = \{(x, y, z) \in \mathbb{N}^3 \mid 4xy + z^2 = p\}.$$

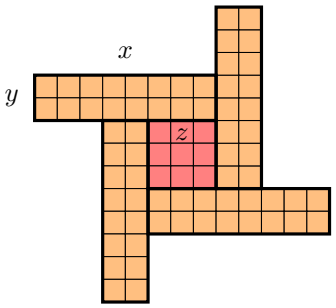
Najprej opazimo, da je množica S neprazna. Po predpostavki je namreč $p \equiv 1 \mod 4$, zato obstaja $k \in \mathbb{N}$, da je $p = 4k + 1$, torej je $(k, 1, 1) \in S$.

Po opazovanju enačbe

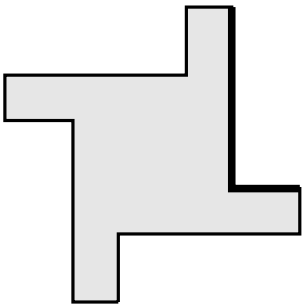
$$4xy + z^2 = p \tag{2}$$

ugotovimo, da lahko vsako od treh spremenljivk (zelo grobo) navzgor omejimo s p. Ker vse spremenljivke zavzamejo vrednosti med naravnimi števili, je tako rešitev enačbe (2) le končno mnogo. Množica S je torej končna.

Sedaj pokažimo, da je moč množice S liha. Naj bo $(x, y, z) \in S$ poljubna rešitev. Tej rešitvi lahko priredimo *krilati kvadrat*, ki je sestavljen iz osrednjega kvadrata, ki ima stranico dolžine z in štirih pravokotnikov z dolžinama stranic x in y, pri čemer se vsi štirje pravokotniki stikajo s sredinskim kvadratom v stranici dolžine x, kot je prikazano na sliki 3.

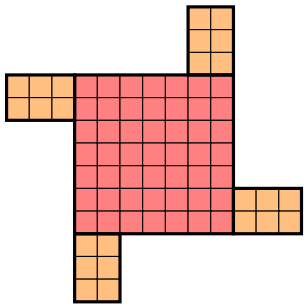


Slika 1: Krilati kvadrat.

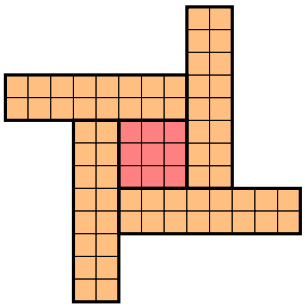


Slika 2: Oblika krilatega kvadrata.

Vsaka od rešitev $(x, y, z) \in S$ tako določa en podobnostni razred krilatih kvadratov (zrcalna slika krilatega kvadrata namreč podaja isto rešitev). Iz vsakega od razredov izberemo tistega, ki ima kotni L v desnem nekonveksnem oglišču vsaj tako visok kot širok (ta je označen na sliki 3). Velja pa tudi obratno, iz vsakega krilatega kvadrat lahko razberemo trojico $(x, y, z) \in \mathbb{N}^3$, tako da preberemo dolžine stranic kvadrata in pravokotnikov, ki ga sestavljajo. Trojica potem zadošča enačbi $4xy + z^2 = p$, saj je to natanko ploščina krilatega kvadrata, zato pripada S. Množico S lahko tako identificiramo z množico vseh krilatih kvadratov, ki imajo kotni L v desnem nekonveksnem oglišču vsaj tako visok kot širok.



(2, 3, 7)

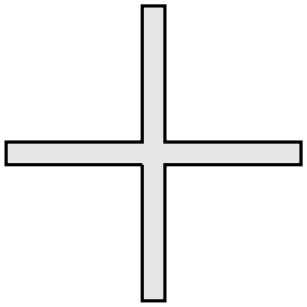


(8, 2, 3)

Slika 3: Dva različna krilata kvadrata za praštevilo $p = 73$ z enako obliko.

Oblika krilatega kvadrata je lik v ravnini, ki ga definira krilati kvadrat, odvisen pa je le od robne krivulje, ki ga obdaja. Oblika krilatega kvadrata s slike 3 je prikazana na sliki 3. Za vsako obliko krilatega kvadrata dobimo bodisi en bodisi dva krilata kvadrata. Na sliki 3 imamo dva različna krilata kvadrata z enako obliko.

Po dva krilata kvadrata oz. trojici iz množice S dobimo iz vsake oblike krilatih kvadratov, razen pri eni in sicer tisti, ki ima kotni L enako visok kot širok (ta je prikazana na sliki 3).



Slika 4: Oblika krilatega kvadrata, ki ima kotni L enako širok kot visok.

Če $(x, y, z) \in S$ pripada krilatemu kvadratu, katerega oblika ima to lastnost, velja $x = z$. Od tod lahko faktoriziramo $p = 4xy + z^2 = x(4y + x)$. Toda p je praštevilo, zato je $x = 1$, kajti za naravni števili x in y je $4y + x > 0$. Opazimo, da ta krilati kvadrat pripada natanko trojici $(1, k, 1)$, ki izhaja iz dejstva, da lahko zapišemo $p = 4k + 1$. Vsaki od oblik krilatih kvadratov lahko torej priredimo dva krilata kvadrata, le eni pa samo enega. To pomeni, da je S množica z liho močjo.

Dokaz izreka zaključimo z definicijo še enega parjenja krilatih kvadratov. To dosežemo s funkcijo $f\colon S \to S$ definirano s predpisom

$$f(x, y, z) = (y, x, z).$$

Očitno f slika v množico S, saj je (x, y, z) rešitev enačbe $4xy + z^2 = p$ natanko tedaj, ko je (y, x, z) rešitev. Funkcija f tako popari trojico (x, y, z) s trojico (y, x, z). Ker pa je moč množice S liha, mora f vsaj eno od rešitev popariti samo s seboj, kar pomeni, da je ta oblike (x, x, z). Ta trojica nazadnje pokaže, da je praštevilo p predstavljivo kot vsota dveh kvadratov, saj dobimo zapis

$$p = (2x)^2 + z^2.$$

□

4 Števila, ki so vsota dveh kvadratov

Sedaj raziščimo še, kako se predstavljivost praštevil posploši na predstavljivost ostalih sestavljenih števil.

4.1 Mali Fermatov izrek

V nadaljevanju bo koristno poznati mali Fermatov izrek. Za dokaz bomo potrebovali binomski izrek in eno lastnost binomskega simbola, zato najprej raziščimo ta dva koncepta.

Definicija 4. *Za naravni števili $n \in \mathbb{N}$ in $0 \leq k \leq n$ je **binomski simbol** definiran kot*

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

Opomba. Kombinatorično binomski simbol $\binom{n}{k}$ šteje, na koliko načinov lahko iz množice z n elementi izberemo podmnožico s k elementi.

Če pogledamo Pascalov trikotnik, lahko binomski simbol $\binom{n}{k}$ najdemo v n-ti vrstici kot k-ti element te vrstice, pri tem pa pazimo, da prvo število v vrstici štejemo kot 0-ti element.

$n = 0$ 1
$n = 1$ 1 1
$n = 2$ 1 2 1
$n = 3$ 1 3 3 1
$n = 4$ 1 4 6 4 1
$n = 5$ 1 5 10 10 5 1
$n = 6$ 1 6 15 20 15 6 1
$n = 7$ 1 7 21 35 35 21 7 1

Slika 5: Pascalov trikotnik.

Primer 5. Recimo, da nas zanima, na koliko načinov lahko iz množice z močjo 5 izberemo podmnožico moči 3. Pogledamo četrto število v peti vrstici Pascalovega trikotnika, ter vidimo, da je rezultat 10. Pravilnost lahko preverimo tudi z računom

$$\binom{5}{3} = \frac{5!}{3!(5-3)!} = \frac{20}{2} = 10.$$

Izrek 9 (Binomski izrek)**.** *Za polinoma v spremenljivkah x in y velja enakost*

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

Binomski izrek, nam pomaga pri razčlenitvi dvočlenika na poljubno stopnjo. Ugotovimo, da koeficiente v razvoju najdemo v n-ti vrstici Pascalovega trikotnika.

Lema 10. *Naj bo $p \in \mathbb{N}$ praštevilo in $0 < k < p$. Potem $p \mid \binom{p}{k}$.*

Dokaz. Binomski simbol $\binom{p}{k}$ je vedno celo število in ga lahko zapišemo tudi kot

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

V imenovalcu so vsi faktorji manjši od p, ki je praštevilo, zato $k!$ deli produkt $(p-1)\cdots(p-k+1)$, kar pomeni, da je $\frac{(p-1)\cdots(p-k+1)}{k!}$ celo število. Od tod sledi, da $p \mid \binom{p}{k}$. □

Pravkar dokazano je seveda razvidno tudi v Pascalovem trikotniku 5, če pogledamo vrstice pri $n = 2,\ 3,\ 5,\ 7$.

Lema 11 (Brucove sanje)**.** *Naj bosta $a,\ b \in \mathbb{Z}$ in $p \in \mathbb{N}$ praštevilo. Tedaj velja*

$$(a+b)^p \equiv a^p + b^p \mod p.$$

Dokaz. Po binomskem izreku vemo, da je

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

Lema 10 nam pove, da je $\binom{p}{k} \equiv 0 \mod p$ za vse $0 < k < p$, zato po modulu p v zgornji vsoti ostaneta le prvi in zadnji člen, pri indeksih $k = 0$ in $k = p$. Sledi

$$(a+b)^p \equiv a^p + b^p \mod p.$$

□

Izrek 12 (Mali Farmatov izrek)**.** *Naj bo $p \in \mathbb{N}$ praštevilo in $a \in \mathbb{Z}$, potem velja*

$$a^p \equiv a \mod p.$$

Dokaz. Najprej omenimo, da se je dovolj omejiti na $0 \leq a < p$, saj ima vsako celo število ostanek pri deljenju s p vsebovan v množici $\{0, \ldots, p-1\}$. Izrek dokažimo z matematično indukcijo.

Za $a = 0$ in $a = 1$, je trditev očitna. Denimo torej, da je $(a-1)^p \equiv a - 1 \mod p$ in pokažimo, da velja $a^p \equiv a \mod p$. Zapišemo lahko

$$a^p \equiv ((a-1)+1)^p \equiv (a-1)^p + 1^p \mod p,$$

kjer drugo kongruenco zagotavlja lema 11. Po indukcijski predpostavki tedaj sledi

$$(a-1)^p + 1^p \equiv a - 1 + 1 \equiv a \mod p,$$

kar dokaže želeno. □

Izrek bomo še malenkost izboljšali, v ta namen se spomnimo, kdaj je funkcija injektivna in surjektivna. Funkcija $g\colon S \to S$ je *injektivna*, kadar za vsaka $x,\ y \in S$ iz $g(x) = g(y)$, sledi $x = y$. Z drugimi besedami je funkcija g injektivna, kadar za neki $y \in S$ obstaja največ en $x \in S$, ki se z g slika v y. Funkcija $g\colon S \to S$ je *surjektivna*, kadar za vsak $y \in S$ obstaja neki $x \in S$, ki se z g slika vanj. Funkcija g je torej surjektivna natanko takrat, ko je za vsak $y \in S$ rešljiva enačba $g(x) = y$.

Lema 13. *Naj bo S končna množica in $g\colon S \to S$ injektivna preslikava, potem je g surjektivna.*

Dokaz te leme ni zahteven, a ga bomo kljub temu izpustili.

Trditev 14. *Naj bo $p \in \mathbb{N}$ praštevilo. Za vsak $a \in \mathbb{Z}$, kjer $p \nmid a$, obstaja neki $b \in \mathbb{Z}$, za katerega velja*

$$ab \equiv 1 \mod p.$$

Dokaz. Naj bo $Z_p = \{0, 1, ..., p-1\}$, ki predstavlja ostanke po modulu p. Potem naj bo funkcija $f\colon Z_p \to Z_p$ podana s predpisom $f(x) = ax \mod p$. Pokažimo, da je f injektivna.

Naj bosta $x,\ y \in Z_p$ poljubna in denimo, da velja $f(x) = f(y)$. Potem drži

$$ax \equiv ay \mod p.$$

Od tod sledi, da $p \mid a(x-y)$. Ker vemo, da p ne deli a, sklepamo, da $p \mid x - y$. Slednje pomeni $x \equiv y \mod p$, ker pa x in y ležita v Z_p, torej sta že ostanka, imamo tudi enakost $x = y$.

Množica Z_p je končna, zato lahko uporabimo lemo 13. Po pravkar dokazanem je f injektivna, zato je tudi surjektivna. Obstaja torej $b \in Z_p$, da je $f(b) = 1 \mod p$, kar pomeni, da b zadošča kongruenci

$$ab \equiv 1 \mod p.$$

□

Sledi manjša izboljšava malega Fermatovega izreka, dokaz katere je uporaba izreka 12 in trditve 14.

Izrek 15. *Naj bo $p \in \mathbb{N}$ praštevilo in $a \in \mathbb{Z}$, tako da $p \nmid a$. Tedaj velja*

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

Dokaz. Ker p ne deli a, obstaja $b \in \mathbb{Z}$, da velja $ab \equiv 1 \mod p$. Če kongruenco $a^p \equiv a \mod p$ z obeh strani pomnožimo z b, dobimo

$$a^p b \equiv ab \mod p.$$

Torej imamo $a^{p-1} \equiv a^{p-1}ab \equiv a^p b \equiv ab \equiv 1 \mod p$, kar dokaže želeno. □

Zgled. Kakšen je ostanek števila 17^{341} pri deljenju s 5? Vemo, da lahko 17 zapišemo kot $17 = 3 \cdot 5 + 2$, kar pomeni, da ima 17 pri deljenju s 5 ostanek 2, torej je $17 \equiv 2 \mod 5$. To pomeni, da velja $17^{341} \equiv 2^{341} \mod 5$. Ker 5 ne deli 2, po izboljšavi malega Fermatovega izreka velja

$$2^4 \equiv 1 \mod 5.$$

Slednje je preprosto opaziti tudi s kratkim računom. Dalje sklepamo, da velja

$$2^{341} \equiv 2^{85 \cdot 4 + 1} \equiv (2^4)^{85} \cdot 2 \equiv 2 \mod 5.$$

To pomeni, da je $17^{341} \equiv 2 \mod 5$.

Preden lahko odgovorimo na prvotno vprašanje, vpeljimo še pojem *reda* nekega elementa po modulu preštevila p.

Definicija 6. *Naj bo praštevilo $p \in \mathbb{N}$ in $a \in \mathbb{Z}$. Poleg tega naj velja $p \nmid a$. Definirajmo* ***red*** *elementa a po modulu p kot* najmanjše *naravno število $r \in \mathbb{N}$, za katerega velja*

$$a^r \equiv 1 \mod p.$$

Trditev 16. *Imejmo praštevilo $p \in \mathbb{N}$, število $a \in \mathbb{Z}$ in denimo, da drži $p \nmid a$. Naj bo $r \in \mathbb{N}$ red elementa a. Če za $m \in \mathbb{N}$ velja $a^m \equiv 1 \mod p$, potem $r \mid m$.*

Dokaz. Zaradi osnovnega izreka o deljenju vemo, da obstajata $q,\ t \in \mathbb{Z}$, za kateri velja $0 \leq t < r$ in

$$m = qr + t.$$

S tem lahko preoblikujemo $a^m \equiv 1 \mod p$ v $a^{qr+t} \equiv 1 \mod p$, kar je enako tudi $(a^r)^q \cdot a^t \equiv 1 \mod p$. Po naši definiciji je $a^r \equiv 1 \mod p$. Dobimo $1^q \cdot a^t \equiv 1 \mod p$. Ker je r najmanjše število za katerega $a^r \equiv 1 \mod p$, mora biti $t = 0$. Ker pa je t ostanek pri deljenju m s številom r, velja $r \mid m$. □

4.2 Glavni izrek

Najprej dokažimo pomožno lemo, ki bo koristna pri dokazu glavnega izreka.

Lema 17. *Vzemimo praštevilo $p \in \mathbb{N}$. Če je $x^2 \equiv -1 \mod p$, kjer je $x \in \mathbb{Z}$, potem je $p = 2$ ali pa je $p \equiv 1 \mod 4$.*

Dokaz. Predpostavimo, da je $p > 2$ in pokažimo, da je red elementa x po modulu p enak 4.

Očitno je $x^4 \equiv 1 \mod p$. Red elementa x ne more biti 1, saj bi moralo držati $x \equiv 1 \mod p$, kar pa ne more biti res, saj $1^2 \not\equiv -1 \mod p$. Prav tako red ne more biti 2, saj vemo $x^2 \equiv -1 \not\equiv 1 \mod p$. S protislovjem pokažimo še, da tudi 3 ni red elementa x. Predpostavimo, da je 3 red elementa x po modulu p. Potem velja

$$x^3 \equiv 1 \mod p.$$

Z upoštevanjem predpostavke $x^2 \equiv -1 \mod p$, sledi

$$1 \equiv x^3 \equiv x \cdot x^2 \equiv -x \mod p.$$

Toda potem je $x^2 \equiv (-x)^2 \equiv 1 \mod p$, kar je v nasprotju s predpostavko, saj $1 \not\equiv -1 \mod p$.

Najmanjše naravno število $r \in \mathbb{N}$, za katerega je $x^r \equiv 1 \mod p$, je tako $r = 4$, ki je torej red elementa x po modulu p.

Posebej opomnimo, da velja $p \nmid x$, saj bi v nasprotnem imeli $x \equiv 0 \mod p$ in tako tudi $x^2 \equiv 0 \mod p$, kar nasprotuje predpostavki leme. Zato lahko uporabimo izboljšavo malega Fermatovega izreka 15, ki nam pove, da je $x^{p-1} \equiv 1 \mod p$. Po trditvi 16, tako dobimo, da $4 \mid p-1$. Od tod sledi $p - 1 \equiv 0 \mod 4$. Po preureditvi te kongruence pa dobimo $p \equiv 1 \mod 4$, kar dokaže našo trditev. □

Kako zdaj vse te izreke povežemo na naše vprašanje, katera naravna števila je mogoče zapisati kot vsoto dveh kvadratov? Uporabili bomo osnovni izrek aritmetike, ki pravi, da lahko vsako naravno število zapišemo kot produkt praštevil. Poleg tega pa bo koristno tudi dejstvo, da lahko z izjemo števila 2 praštevila razdelimo v dve skupini, in sicer na praštevila, ki so kogruentna 1, in tista, ki so kongruenta 3 po modulu 4. Sedaj smo pripravljeni za glavni izrek.

Izrek 18. *Recimo, da je n poljubno naravno število, $p_1, \ldots, p_k$ in $q_1, \ldots, q_m$ pa njegovi različni praštevilski faktorji, pri čemer za vse i in j velja*

$$p_i \equiv 1 \mod 4 \quad \textit{in} \quad q_j \equiv 3 \mod 4.$$

Zapišimo

$$n = 2^t \cdot p_1^{e_1} \ldots p_k^{e_k} \cdot q_1^{f_1} \ldots q_m^{f_m}, \tag{3}$$

za neka naravna števila $t \in \mathbb{N}_0,\ e_1, \ldots, e_k \in \mathbb{N}$ in $f_1, \ldots, f_m \in \mathbb{N}$.

Tedaj je število n predstavljivo kot vsota dveh kvadratov, če in samo če so vsi eksponenti f_j sodi.

Dokaz. ($\Leftarrow$) V začetku članka smo že opazili, da lahko število napišemo kot vsoto kvadratov dveh števil, kadar lahko to storimo za vsa števila v neki njegovi faktorizaciji. To pove trditev 1. Poglejmo, zakaj so vsi faktorji iz faktorizacije (3) predstavljivi.

Začnimo z 2. Če je eksponent t sod, je oblike $t = 2u$ za neki $u \in \mathbb{N}_0$. Potem je 2^t kvadrat nekega števila in zato tudi predstavljiv, saj velja

$$2^{2u} = (2^u)^2 + 0^2.$$

Če pa je eksponent t lih, je oblike $t = 2u + 1$ za neki $u \in \mathbb{N}$, in velja

$$2^{2u+1} = 2 \cdot (2^u)^2 = (2^u)^2 + (2^u)^2,$$

ki je vsota dveh kvadratov.

Za praštevila p_i smo v izreku 8 dokazali, da jih lahko vedno zapišemo kot vsoto dveh kvadratov, praštevila q_j pa se pojavijo s sodimi eksponenti, zato so že sami kvadrati in zato predstavljivi. Sledi, da je n predstavljivo.

($\Rightarrow$) Sedaj denimo, da je n mogoče zapisati kot vsoto dveh kvadratov

$$n = x^2 + y^2 \quad \text{za } x,\ y \in \mathbb{Z}$$

in pokažimo, da so vsi eksponenti f_j sodi.

Naj bo q eno od praštevil q_j iz praštevilskega razcepa števila n. Pokažimo, da $q^2 \mid n$. Slednje bomo dokazali tako, da pokažemo, da $q \mid x$ in $q \mid y$.

Predpostavimo, da $q \nmid x$. Naj bo $z \in \mathbb{Z}$ tako, da bo veljalo $xz \equiv 1 \mod q$. Praštevilo q je delitelj n, zato je $n \equiv 0 \mod q$. Potem velja

$$0 \equiv z^2 n \equiv z^2 x^2 + z^2 y^2 \equiv 1 + (zy)^2 \mod q.$$

Če to preuredimo, dobimo $(zy)^2 \equiv -1 \mod q$. Lema 17 nam pove, da je $q \equiv 1 \mod 4$. Toda, ker smo predpostavili $q \equiv 3 \mod 4$ pridemo v protislovje. Po enakem postopku lahko dokažemo tudi $q \mid y$.

Ker velja $q \mid x$ in $q \mid y$, mora veljati tudi

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

Vidimo, da je število $\frac{n}{q^2}$ možno zapisati kot vsoto dveh kvadratov, zato lahko ta postopek nadaljujemo in na vsakem koraku opazimo, da v primeru, ko praštevilo q z $q \equiv 3 \mod 4$ deli n, tudi q^2 deli n. Torej imajo vsi prafaktorji q_j v praštevilskem razcepu n sode eksponente, tj. f_j so vsi sodi. □

5 Zaključek

V članku smo se spraševali, kaj mora držati, da lahko neko poljubno naravno število zapišemo kot vsoto kvadratov dveh celih števil. Naprej nam je to uspelo dokazati za poljubno praštevilo, za katerega je bilo potrebno samo, da ima pri deljenju s 4 ostanek 1, oz. $p \equiv 1 \mod 4$. Od tod smo nazadnje izpeljali, da lahko število zapišemo kot vsoto dveh kvadratov, če in samo če lahko to naredimo za vse prafaktorje, ki ga sestavljajo in imajo tisti, ki jih ne moremo samih po sebi zapisati kot vsoto dveh kvadratov, sodo potenco.

Literatura

[1] M. Aigner, G. M. Ziegler, *Proofs from THE BOOK*, 6th edition Springer, Berlin, 2018.

[2] *Fermatov mali izrek*, v: Wikimedie, S. P. (2022, August 23). Fermatov mali izrek. Wikipedija, Prosta Enciklopedija. `https://sl.wikipedia.org/wiki/Fermatov_mali_izrek`

[3] K. Šivic, *Funkcije in funkcijske enačbe*, `https://www.dmfa.si/Tekmovanja/MaSSA/Dokumenti/funkcijske_predavanje.pdf`