Diofantske enačbe

Hugo Trebše (hugo.trebse@gmail.com)

5. avgust 2024

Zapiski sledijo avtorjevem predavanju na pripravah za mednarodna matematična tekmovanja, ki je bilo izvedeno 20. 3. 2024. Za vse napake ter netočnosti je odgovoren avtor sam. Če imate vprašanje ali popravek se obrnite na e-poštni naslov zgoraj.

Zahvaljujem se Luku Horjaku za pomoč pri urejanju ter mnoge nasvete.

Gutta cavat lapidem non vi,
sed saepe cadendo.
Kapljica izvotli kamen ne s silo,
ampak s čestim padanjem.

Latinski pregovor

Kazalo

1 Osnove

V splošnem naloga iz diofantskih enačb od tekmovalca oziroma tekmovalke zahteva, naj najde vse celoštevilske oziroma naravnoštevilske rešitve določene enačbe. Naloga torej sestoji iz dveh delov: v prvem tekmovalec našteje ter preveri veljavnosti rešitev, v drugem pa pokaže, da, z izjemo naštetih, ne obstaja nobena rešitev dane enačbe (dvodelnost dokaza je v tem primeru analogna mnogim nalogam iz funkcijskih enačb). Tipično se pri reševanju diofantske enačbe znajdemo v eni izmed naslednjih treh situacij:

- Množica rešitev diofantske enačbe sestoji iz razmeroma majhnega števila razmeroma majhnih rešitev.
- Diofantska enačba ima neskončno družino rešitev.[1]
- Diofantska enačba nima rešitev.

Daleč najpogostejša izmed naštetih možnosti je prva, a smotrno je imeti v mislih tudi ostali dve, četudi ju lahko pogosto hitro ovržemo. Če posumimo, da ima diofantska enačba morebiti neskončno družino rešitev, smo lahko relativno samozavestni, da lahko to družino podamo parametrično – vse neznanke lahko potem podamo kot funkcije neke nove spremenljivke.

1.1 Kako začeti

Dober prvi korak je preizkusiti nekaj majhnih primerov, kar je sicer tudi odlična praksa pri reševanju problemov v splošnem. Na podlagi teh specifičnih primerov lahko namreč pogosto učeno ugibamo, kako bo videti množica rešitev.

Hkrati si lahko prihranimo čas v prihodnosti, saj lahko določene pristope s protislovjem preprosto ovržemo kot nemogoče, saj bi njihova veljavnost implicirala, da že znana rešitev ne bi smela obstajati. To je dobro imeti v mislih posebej pri nekaterih modularnih argumentih, saj že sam obstoj ene rešitve enačbe onemogoči, da bi prišli do modularnega protislovja, vsaj brez uvedbe dodatnih predpostavk.

Obravnava specifičnih primerov je tudi obetaven prvi korak, tako pri diofantskih enačbah kot splošneje. Do pomembnih ugotovitev lahko pridemo že s preprostimi vprašanji kot so na primer: kaj se zgodi, če so spremenljivke paroma tuje? Kaj pa ko sta specifični dve lihi?

[1] Seveda dopustimo možnost, da ima enačba več neskončnih družin rešitev, a iz vidika rešljivosti takega zapletenega problema je ta možnost zelo majhna.

1.2 Osnovna orodja

Ko menimo, da smo uspešno določili množico rešitev, se lahko lotimo naslednjega koraka – pokazati je treba, da diofantska enačba nima nobenih drugih rešitev.

Nasvet

Tri najosnovnejša orodja, ki nam pomagajo pri tem koraku so:

1. **Modularna aritmetika**
2. **Faktorizacija**
3. **Omejevanje**

Najnazornejše uporabo teh prikažemo na primerih:

Naloga 1.1

Določi vse pare celih števil (x, y), za katere velja $x^2 = 2001 + y!$.

Rešitev. Opazimo, da je $2001 \equiv 6 \pmod 7$ ter za $y \geq 7$ velja $7 \mid y!$, kar implicira $x^2 \equiv 6 \pmod 7$. Zapišimo si, katere ostanke imajo kvadrati celih števil pri deljenju s 7:

$n \pmod 7$	$n^2 \pmod 7$
0	$0^2 \equiv 7^2 \equiv 0$
± 1	$(\pm 1)^2 \equiv 1$
± 2	$(\pm 2)^2 \equiv 4$
± 3	$(\pm 3)^2 \equiv 2$

Ugotovili smo, da je desna stran enačbe kongruentna $6 \pmod 7$, med tem ko je leva stran enačbe kongruentna enemu izmed števil v množici $\{0, 1, 4, 2\}$ po modulu 7, kar je seveda protislovno.

Za $y \leq 6$ najdemo rešitve na manj privlačen način – preverimo vse možnosti, kar poskusimo narediti na učinkovit način, da si zmanjšamo količino dela.

Za $y = 6$ pridemo do protislovja upoštevajoč večkratnost delitelja 3 desne strani, primer $y = 5$ ovržemo na enak način: dobimo $x^2 = 2121$, ter vidimo, da je desna stran kongruentna $6 \pmod 9$. Za $y = 4$ dobimo rešitev $x = 45$, ostale primere pa lahko ovržemo, saj desna stran leži med 44^2 ter 45^2. □

Komentar: Zgornjo nalogo smo rešili z le enim orodjem: modularno aritmetiko, ki je problem reducirala na preverjanje nekaj majhnih primerov. Izbiro modula 7 je težko motivirati; opazka, da za $y \geq 7$ člen $y!$ odpade, je verjetno najboljši razlog.

Kot dodatek pripomnimo, da je ključni korak ločiti primera glede na velikost y, saj nam slednje omogoča, da uporabimo vse kar znamo o modularni aritmetiki. Morda se zdi v tem primeru ta pripomba odvečna, a je pomembno, da pri tvorbi domneve izvzamemo primere, v katerih smo našli rešitve. V nasprotnem primeru bomo namreč neuspešni pri dokazu s protislovjem.

Naloga 1.2: Indija, 1990

Za $x, y \in \mathbb{N} \cup \{0\}$ določi vse rešitve diofantske enačbe

$$(xy - 7)^2 = x^2 + y^2.$$

Rešitev. Enačbo preoblikujemo:

$$\begin{aligned}
(xy-7)^2 &= x^2+y^2 \\
(xy)^2 - 14xy + 7^2 &= x^2+y^2 \\
(xy)^2 - 12xy + 7^2 &= x^2+2xy+y^2 \\
(xy-6)^2 + 13 &= (x+y)^2 \\
(x+y)^2 - (xy-6)^2 &= 13 \\
(x+y-xy+6)(x+y+xy-6) &= 13 \\
(-(x-1)(y-1)+7)((x+1)(y+1)-7) &= 13
\end{aligned}$$

Ker na levi strani dobimo produkt celih števil, na desni pa praštevilo, sledi, da je bodisi

$$((x+1)(y+1)-7, -(x-1)(y-1)+7) = (13, 1),$$

bodisi

$$((x+1)(y+1)-7, -(x-1)(y-1)+7) = (1, 13).$$

Možnosti $(-1, -13)$ in $(-13, -1)$ odpadeta, saj očitno ne moreta obe števili biti hkrati negativni.

V prvem primeru sledi $(x+1)(y+1) = 20$ ter $(x-1)(y-1) = 6$. S kratko obravnavo deliteljev števil 20 ter 6 dobimo edini par rešitev $(x, y) = (y, x) = (3, 4)$.

V drugem primeru sledi $(x+1)(y+1) = 8$ ter $(x-1)(y-1) = -6$. Ponovno obravnavamo delitelje (tako negativne kot pozitivne) števil 8 in -6, ter dobimo še drugi par rešitev $(x, y) = (y, x) = (7, 0)$. □

Komentar: Zgornja faktorizacija ni popolnoma očitna, a princip »dopolnitve« do popolnega kvadrata je razmeroma pogost ter si ga je vredno zapomniti. Prav tako je pri reševanju diofantskih enačb zelo pogosta ideja, da enačbo pretvorimo v tako, ki ima na eni strani produkt izrazov, ki vsebujejo spremenljivke, na drugi strani pa so zgolj parametri oziroma konstante. Če se na eni strani pojavijo samo števila, smo uspešno pretvorili problem na preverjanje končno mnogo primerov, saj so lahko izrazi le delitelji števila, ki

nastopa drugi strani. Vse to je mogoče zaradi osnovnega izreka aritmetike, ki pravi, da lahko vsako naravno število večje od 1 zapišemo na enoličen način kot produkt potenc praštevil, do vrstnega reda faktorjev natančno.

1.2.1 Še nekaj o faktorizaciji

Nasvet

Podobni izrazi, za katere je faktorizacija zelo uporabna so:

$$xy + ax + by + c = (x + b)(y + a) + c - ab$$
$$x^2 + x + c = \frac{1}{4}((2x + 1)^2 + (4c - 1))$$

ter klasični načini faktorizacije razlike enakih potenc ter vsote enakih lihih potenc.

Manj očitna je naslednja enakost:

Lema 1.3: Identiteta Sophie Germain

Za realna števila a in b velja enakost

$$a^4 + 4b^4 = (a^2 + 2b^2)^2 - (2ab)^2 = (a^2 + 2ab + 2b^2)(a^2 - 2ab + 2b^2).$$

Zavoljo celovitosti ilustrirajmo še primer uporabe *omejevanja*.

Naloga 1.4

V naravnih številih reši enačbo

$$y^2 = x^4 + 2x^3 + 1.$$

Rešitev. Uporabimo metodo omejevanja med zaporedne kvadrate. Opazimo, da velja

$$(x^2 + x)^2 = x^4 + 2x^3 + x^2 \geq x^4 + 2x^3 + 1 > x^4 + 2x^3 - x^2 - 2x + 1 = (x^2 + x - 1)^2.$$

Desna neenakost je stroga za vse $x \in \mathbb{N}$, med tem ko je leva stroga le za $x > 1$. Ker je seveda nemogoče, da bi med dvema zaporednima popolnima kvadratoma obstajal tretji popolni kvadrat, sledi, da za $x > 1$ ni rešitev diofantske enačbe.

Če je $x = 1$, jasno dobimo rešitev $(x, y) = (1, 2)$. □

Komentar: V rešitvi zgornje naloge smo uporabili princip omejevanja med zaporedne kvadrate, ki se jasno posploši na princip omejevanja med poljubne zaporedne potence.

To še zdaleč ni edini način kako lahko uporabimo omejevanje pri reševanju diofantskih enačb. Že zelo osnovne ugotovitve, kot na primer katera izmed nastopajočih spremenljivk bi lahko bila največja, so lahko pogosto ključne – dober primer je 5. naloga z Mednarodne

matematične olimpijade 2022, pri kateri je osrednji korak obravnavati velikost spremenljivke b glede na p in $2p$.

Pri medsebojnem omejevanju spremenljivk so lahko uporabne neenakosti med potenčnimi sredinami ter kvadratna enačba.

Predstavili smo nekaj osnovnih prijemov pri reševanju diofantskih enačb. Kot zaključek poglavja pa navedimo ter dokažimo še dve občasno uporabni lemi.

Lema 1.5: Delitelji vsote kvadratov

Naj bosta a in b celi števili ter $p \equiv 3 \pmod 4$ praštevilo. Če velja

$$p \mid (a^2 + b^2),$$

potem sledi $p \mid a$ ter $p \mid b$.[2]

Dokaz. Če p deli enega izmed a in b, potem seveda deli tudi drugega. Predpostavimo, da p ne deli nobenega izmed a in b, ter poiščimo protislovje.

$$\begin{aligned} a^2 + b^2 &\equiv 0 \pmod p \\ (ab^{-1})^2 &\equiv -1 \pmod p \\ (ab^{-1})^{p-1} &\equiv (-1)^{\frac{p-1}{2}} \pmod p \end{aligned}$$

Leva stran kongruence je $(p-1)$-ta potenca produkta obrnljivih elementov po modulu p, zato po malem Fermatovem izreku sledi, da je kongruentna 1 po modulu p. Ker je $p \equiv 3 \pmod 4$, sledi, da je $\frac{p-1}{2}$ liho število, kar pomeni, da je desna stran kongruentna -1 po modulu p. To je seveda mogoče le, če je $p = 2$, kar pa je v protislovju s predpostavko $p \equiv 3 \pmod 4$. Sledi, da $p \mid a$ ter $p \mid b$. □

Lema 1.6: Bezoutova lema

Naj bosta a in b celi števili ter $\gcd(a, b)$ njun največji skupni delitelj. Obstajata celi števili x ter y, da velja

$$ax + by = \gcd(a, b).$$

Dokaz. Naj bo $S = \{|au + bv| \,;\, u, v \in \mathbb{Z}\}$. Ker je S navzdol omejena neprazna množica celih števil, obstaja najmanjši neničelni element S – označimo ga z m. Očitno velja $\gcd(a, b) \mid m$, kar pomeni $\gcd(a, b) \leq m$. Če $m \nmid a$, obstajata celi števili q in $1 \leq r \leq m-1$, da je $a = qm + r$. Sledi

$$r = a - qm \in S,$$

kar pomeni, da je r manjši kot m ter neničelni element S, kar je protislovno. Sledi $m \mid a$ ter na analogen način $m \mid b$. To pomeni, da je m skupni delitelj a in b, ki je večji ali enak največjemu skupnemu delitelju a in b. Sledi $\gcd(a, b) = m \in S$, kar smo želeli pokazati. □

[2] Pogosto je uporabna naslednja posledica leme: če $p \mid (n^2 + 1)$, potem je $p \equiv 1 \pmod 4$ ali $p = 2$.

1.3 Naloge za vajo

Naloga 1.7

Najdi vse rešitve enačbe $y^5 = x^2 + 4$ v naravnih številih.[3]

Naloga 1.8: ZDA, JMO, 2013

Ali obstjata celi števili a ter b, da sta $a^5b + 3$ in $ab^5 + 3$ obe popolni tretji potenci?

Naloga 1.9: Slovenija, 2024

Določi vse peterice praštevil $p_1 \leq p_2 \leq p_3 \leq p_4 \leq p_5$, za katere vsako izmed teh praštevil deli vsoto preostalih štirih.

Naloga 1.10: Velika Britanija, 2005

Naj bo n naravno število. Obstaja natanko 2005 urejenih parov naravnih števil (x, y), da velja

$$\frac{1}{x} + \frac{1}{y} = \frac{1}{n}.$$

Pokaži, da je n popolni kvadrat.

Naloga 1.11: Iran, 1997

Naj bosta x in y naravni števili, za kateri velja

$$3x^2 + x = 4y^2 + y.$$

Pokaži, da je $x - y$ popolni kvadrat.

Naloga 1.12

Najdi vsa naravna števila n in cela števila $a_1, a_2, \ldots, a_n$, za katera velja

$$a_1 + a_2 + \cdots + a_n = 5n - 4 \quad \text{in} \quad \frac{1}{a_1} + \frac{1}{a_n} + \cdots + \frac{1}{a_n} = 1.$$

[3] Namig: če v diofantski enačbi nastopajo znane potence spremenljivk, je modro opazovati enačbo po takem modulu n, da potence spremenljivk delijo $\varphi(n)$, saj to zmanjša število morebitnih ostankov potenc po modulu n.

2 Funkcije v teoriji števil

2.1 p-adična valuacija ter celi del

Definicija 2.1: p-adična valuacija

Naj bo $p \in \mathbb{P}$ ter $n \in \mathbb{N}$. *p-adična valuacija* števila n je tako nenegativno celo število $\nu_p(n)$, da velja

$$p^{\nu_p(n)} \mid n \quad \text{in} \quad p^{\nu_p(n)+1} \nmid n.$$

Lema 2.2: Alternativna karakterizaicja p-adičnosti

Že omenjeni *osnovni izrek aritmetike* na alternativen način karakterizira p-adično valuacijo, namreč

$$n = \prod_{p \in \mathbb{P}} p^{\nu_p(n)}.$$

Naslednje lastnosti so po alternativni karakterizaciji p-adičniosti očitne.

Izrek 2.3

Za $x, y \in \mathbb{N}$ velja:

- $\nu_p(xy) = \nu_p(x) + \nu_p(y)$
- $\nu_p(x^y) = y \cdot \nu_p(x)$
- $\nu_p(x+y) \geq \min\{\nu_p(x), \nu_p(y)\}$. Če velja $\nu_p(x) \neq \nu_p(y)$, potem sledi enakost.

p-adična valuacija je daleč najuporabnejša pri multiplikativnih problemih – tistih, ki pretežno sestojijo iz množenja ter potenciranja, kar zrcali tudi razlika med prvima dvema ter tretjo točko zgornjega izreka. Šibkost p-adične valuacije leži v seštevanju;[4] pri slednjem je v splošnem najuporabnejši *Evklidov algoritem*.

[4] Vprašanje, kako se spremeni praštevilska faktorizacija celega števila pri prištevanju 1, je zelo kompleksno; nekatere trenutne najučinkovitejše metode obravnavajo prištevanje 1 kot naključno mešanje praštevilskih deliteljev.

Ogrejmo se z naslednjim problemom:

Naloga 2.4

Naj bosta a in b celi števili. Velja

$$a \mid b^2 \mid a^3 \mid b^4 \mid \cdots .$$

Pokaži, da je $a = b$.

Rešitev. Prevedimo problem deljivosti na problem p-adičnosti. Iz osnovnega izreka aritmetike opazimo, da če $x \mid y$, potem za vsa praštevila p velja $\nu_p(x) \leq \nu_p(y)$. Pogoj naloge se tako prevede na: za vse $p \in \mathbb{P}$ in za vse $i \in \mathbb{N}$ velja

$$\nu_p(a^{2i-1}) \leq \nu_p(b^{2i}) \quad \text{in} \quad \nu_p(b^{2i}) \leq \nu_p(a^{2i+1}),$$

kar je ekvivalentno

$$(2i-1) \cdot \nu_p(a) \leq (2i) \cdot \nu_p(b) \quad \text{in} \quad (2i) \cdot \nu_p(b) \leq (2i+1) \cdot \nu_p(a).$$

Tako sledi

$$\frac{2i-1}{2i} = 1 - \frac{1}{2i} \leq \frac{\nu_p(b)}{\nu_p(a)} \leq \frac{2i+1}{2i} = 1 + \frac{1}{2i}$$

Če je kvocient $\frac{\nu_p(a)}{\nu_p(b)}$ različen od 1, lahko seveda najdemo tak indeks i, da je kvocient bodisi manjši od $1 - \frac{1}{2i}$, bodisi večji od $1 + \frac{1}{2i}$, zaradi česar sledi, da je $\frac{\nu_p(a)}{\nu_p(b)} = 1$ za vse $p \in \mathbb{P}$.

Po lemi 2.2 sledi $a = b$. □

Spotoma definirajmo še funkcijo celi del:

Definicija 2.5

Funkcija celi del je funkcija $\lfloor \cdot \rfloor : \mathbb{R} \mapsto \mathbb{Z}$, ki realnemu številu dodeli največje celo število, ki ne presega tega realnega števila. Se pravi, funkcija celi del[5]realnemu številu x pripiše tako celo število $n = \lfloor x \rfloor$, da velja

$$n \leq x < n + 1.$$

Naslednji izrek ponovno prikaže moč p-adične valuacije pri mulitplikativnih problemih.

Izrek 2.6: Legendrova formula

Naj bo $n \in \mathbb{N}$ ter $p \in \mathbb{P}$. Potem velja

$$\nu_p(n!) = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor$$

[5]Pogosto je uporabno definirati funkcijo neceli del, ki zadošča enakosti $\{x\} = x - \lfloor x \rfloor$, saj po definiciji sledi $0 \leq \{x\} < 1$, kar omogoča bolj intuitivno omejevanje vrednosti.

Dokaz. Opazimo, da za vse dovolj velike $j \in \mathbb{N}$ velja $p^j > n$, kar pomeni, da so vsi členi vsote z indeksi večjimi od j enaki 0. Sledi, da je vsota na desni končna. Sedaj pokažimo enakost. Obstaja natanko $\left\lfloor \frac{n}{p} \right\rfloor$ števil med 1 in n, ki so deljiva s p. Izmed teh jih je $\left\lfloor \frac{n}{p^2} \right\rfloor$ s p deljivo vsaj dvakrat, $\left\lfloor \frac{n}{p^3} \right\rfloor$ s p deljivo vsaj trikrat in podobno naprej.

Naj množica A_j vsebuje vsa števila med 1 in n, ki imajo p-adičnost vsaj j, sledi $|A_j| = \left\lfloor \frac{n}{p^j} \right\rfloor$. Očitno je

$$A_0 \supsetneq A_1 \supsetneq A_2 \supsetneq A_3 \dots .$$

Za vsako število, ki ima p-adičnost natanko j, velja, da je v množici števil s p-adičnostjo vsaj j ter ni v množici števil p-adičnosti vsaj $j+1$. Sledi, da je število med 1 in n s p-adičnostjo natanko j enako $\left\lfloor \frac{n}{p^j} \right\rfloor - \left\lfloor \frac{n}{p^{j+1}} \right\rfloor$. Števila med 1 in n s p-adičnostjo natanko j tako p-adičnosti fakultete doprinesejo

$$j \cdot \left(\left\lfloor \frac{n}{p^j} \right\rfloor - \left\lfloor \frac{n}{p^{j+1}} \right\rfloor \right)$$

faktorjev p. Sledi, da je

$$\begin{aligned} \nu_p(n!) &= \sum_{i=1}^{\infty} i \cdot \left(\left\lfloor \frac{n}{p^i} \right\rfloor - \left\lfloor \frac{n}{p^{i+i}} \right\rfloor \right) \\ &= \sum_{i=1}^{\infty} i \cdot \left\lfloor \frac{n}{p^i} \right\rfloor - \sum_{i=1}^{\infty} (i-1) \cdot \left\lfloor \frac{n}{p^i} \right\rfloor \\ &= \sum_{i=1}^{\infty} (i - (i-1)) \cdot \left\lfloor \frac{n}{p^i} \right\rfloor \\ &= \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor . \end{aligned}$$

□

2.2 Naloge za vajo

Naloga 2.7

Določi vse $x, y, a, b \in \mathbb{Z}$, za katere velja

$$a^2 + 6b^2 = x^2 \quad \text{ter} \quad b^2 + 6a^2 = y^2.$$

Naloga 2.8

Pokaži, da za vse $n \in \mathbb{N}$ velja

$$\binom{2n}{n} \,\Big|\, \operatorname{lcm}\{1, 2, \ldots, 2n\}\,.$$

Naloga 2.9

Naj bosta $x, y \in \mathbb{N}$ ter naj velja

$$(x - 2y)(1 - 2y) \mid (x^2 - 4y + 1).$$

Pokaži, da je $|x - 2y|$ popolni kvadrat.

Naloga 2.10

Naj bo $n \in \mathbb{N}$. Vsota vseh pozitivnih deliteljev n je popolna potenca 2. Pokaži, da je število deliteljev n prav tako popolna potenca 2.

3 Neskončni spust

Neskončni spust nam pomaga dokazati, da diofantska enačba nima rešitev. Princip je sledeč: predpostavimo obstoj rešitve, ki je na nek način minimalna, ter nato pokažemo, da obstaja rešitev manjša od slednje, kar doseže želeno protislovje.[6] Najpogosteje izberemo rešitev z minimalno vsoto, produktom ali pa eno izmed tistih, ki minimizirajo posamezni člen.

Naloga 3.1

Reši enačbo

$$x^3 + 2y^3 = 4z^3$$

v naravnih številih.

Rešitev. Denimo, da obstaja nekaj rešitev enačbe v naravnih številih ter naj bo (x_0, y_0, z_0) ena izmed rešitev z najmanjšo vsoto. Ker velja

$$x_0^3 + 2y_0^3 = 4z_0^3$$

sledi, da je x_0^3 sod, kar pomeni da je x_0 sod. Sledi, da lahko zapišemo $x_0 = 2x_1$, pri čemer se začetna enačba glasi

$$8(x_1^3) + 2y_0^3 = 4z_0^3.$$

Z analognima argumentoma ugotovimo, da sta $y_0 = 2y_1$ ter $z_0 = 2z_1$ soda, kar pomeni, da velja

$$x_1^3 + 2y_1^3 = 4z_1^3$$

ter $x_0 + y_0 + z_0 = 2(x_1 + y_1 + z_1)$, kar implicira obstoj rešitve, vsota spremenljivk katere pa je manjša od rešitve z najmanjšo vsoto. Dosegli smo protislovje, kar pomeni da enačba nima rešitev. □

Uporabimo metodo *končnega spusta*, da dokažemo znan izrek iz teorije števil.

Izrek 3.2: Fermatov izrek o vsoti dveh kvadratov

Naj bo $p \in \mathbb{P}$ liho praštevilo. Potem je $p \equiv 1 \pmod 4$ natanko tedaj, ko obstajata celi števili x in y, za kateri je

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

Dokaz. Implikacija iz desne proti levi je očitna po lemi 1.5. Dokažimo še implikacijo iz leve proti desni.

Kot prvi korak dokaza pokažemo, da za $p \equiv 1 \pmod 4$ obstaja $a \in \mathbb{Z}$, za katerega je $a^2 \equiv -1 \pmod p$. To storimo z uporabo Wilsonovega izreka, ki pravi, da je p praštevilo natanko tedaj, ko velja $(p-1)! \equiv -1 \pmod p$.

[6] Opisani argument ni uporaben izključno v teoriji števil; pojavlja se tudi v kombinatoriki pod imenom »protislovje z minimalnim protiprimerom«. Kot namiguje ime, predpostavimo obstoj minimalnega protiprimera neki domnevi, potem pa dokažemo obstoj manjšega protiprimera. Sledi, da domneva nima protiprimera, torej je resnična.

Števila v množici $\{1, 2, \ldots, p-1\}$ razdelimo v $\frac{p-1}{2}$ parov oblike $(j, p-j)$. Uporabili bomo naslednjo opazko: produkt komponent vsakega izmed parov je kongruenten $-j^2 \pmod{p}$. Po modulu p velja torej

$$-1 \equiv (p-1)! \equiv \prod_{i=1}^{p-1} i \equiv \prod_{i=1}^{\frac{p-1}{2}} i \cdot (p-i) \equiv \prod_{i=1}^{\frac{p-1}{2}} -i^2 \equiv (-1)^{\frac{p-1}{2}} \cdot \left(\prod_{i=1}^{\frac{p-1}{2}} i \right)^2 \pmod{p}.$$

Ker je $\frac{p-1}{2}$ sodo število, je želeno dokazano.

Naj bo X tako celo število, da velja $X^2 + Y^2 = m_0 p$ za $Y = 1$ ter nek $m_0 \in \mathbb{N}$.

Če je $m_0 = 1$, smo končali, v nasprotnem primeru pa naj bosta u in v taki celi števili, da velja

$$u \equiv X \pmod{m_0}, \quad v \equiv Y \pmod{m_0} \quad \text{in} \quad |u|, |v| \leq \frac{m_0}{2}.$$

Z enostavnimi razmisleki iz modularne aritmetike preverimo, da so $Xu + Yv$, $Xv - Yu$ ter $u^2 + v^2$ vsi deljivi z m_0.

S krajšim računom lahko preverimo, da velja[7]

$$(u^2 + v^2)(X^2 + Y^2) = (Xu + Yv)^2 + (Xv - Yu)^2.$$

Ker je $X^2 + Y^2$ večkratnik p, je desna stran deljiva s p. Vsak izraz v oklepajih je prav tako deljiv z m_0, zato sledi

$$\left(\frac{Xu + Yv}{m_0} \right)^2 + \left(\frac{Xv - Yu}{m_0} \right)^2 = m_1 p,$$

kjer velja $m_1 \in \mathbb{N}$ ter

$$m_1 = \frac{u^2 + v^2}{m_0} \leq \frac{1}{m_0} \cdot \left(\frac{m_0^2}{4} + \frac{m_0^2}{4} \right) = \frac{m_0}{2}.$$

Če je $u = v = 0$ bi sledilo, da je $m_1 = 0$, kar poruši naš argument. Pokažimo, da se to ne zgodi za $m_0 > 1$. Denimo, da sta u ter v oba ničelna. Sledi, da sta X ter Y oba deljiva z m_0, od koder sledi

$$m_0^2 \mid X^2 + Y^2 = m_0 p,$$

oziroma $m_0 \mid p$. Ker je $m_0 \neq 1$ in je p praštevilo, sledi $m_0 = p$. Potemtakem velja $X^2 + Y^2 = p^2$, kjer sta X in Y naravni števili, ki sta deljivi s p. To je seveda protislovno, saj je $X^2 + Y^2 \geq 2p^2$.

Uspelo nam je pretvoriti enačbo oblike $X^2 + Y^2 = m_0 p$ v enačbo oblike $X_1^2 + Y_1^2 = m_1 p$, kjer sta $m_0 > 1$ in m_1 naravni števili, za kateri velja $m_1 < m_0$. Postopek ponavljamo, dokler ne dosežemo $m_i = 1$, ki je naša želena ugotovitev. Postopek pa se seveda konča, saj se koeficienti m_i na vsakem koraku strogo manjšajo ter zavzamejo le naravne vrednosti. □

[7] Gre pravzaprav za poseben primer *identitete Brahmagupte*. V splošnem za vsa realna števila a, b, c, d in n velja $(a^2 + nb^2)(c^2 + nd^2) = (ac \pm n \cdot bd)^2 + n \cdot (ad \mp bc)^2$.

3.1 Naloge za vajo

Naloga 3.3: Domača naloga za MMO, 2022

Naj bodo a, b, c ter d naravna števila za katera velja:

$$a^2 + b^2 + c^2 + d^2 = 2022!$$

Pokaži, da so vse spremenljivke večje od 10^{270}.

Naloga 3.4

Upoštevajoč izrek 3.2 ali drugače pokaži, da lahko vsako naravno število zapišemo kot vsoto štirih kvadratov celih števil.

Naloga 3.5: Madžarska, 2000

Najdi vsa praštevila p, za katera obstajajo naravna števila x, y in n, tako da velja

$$p^n = x^3 + y^3.$$

Naloga 3.6: MMO, 2007

Naj sta a in b naravni števili za kateri velja

$$(4ab - 1) \mid (4a^2 - 1)^2.$$

Pokaži, da sledi $a = b$.

Literatura

[1] David Arthur. *Number Theory Tips and Tricks*. 2009. URL: https://olympiadtraining.files.wordpress.com/2014/10/arthur-number-theory-tips-and-tricks.pdf (pridobljeno 9. 4. 2024).

[2] Neil Donaldson. *Fermat's method of descent*. 2021. URL: https://www.math.uci.edu/~ndonalds/math180b/5descent.pdf (pridobljeno 9. 4. 2024).

[3] Alexander Remorov. *Exponents and Primes*. 2010. URL: https://alexanderrem.weebly.com/uploads/7/2/5/6/72566533/exponentsprimes.pdf (pridobljeno 7. 4. 2024).

[4] Navid Safaei. *Exponent of primes: a closer look*. 2021. URL: https://www.researchgate.net/publication/353393715_Exponent_of_primes_a_closer_look_Arhimode_journal_2021_0801_55-80 (pridobljeno 9. 4. 2024).