Predavanje 12

O DIOFANTSKIM JEDNAČINAMA

Podsetimo se, *diofantska jednačina* je jedančina oblika

$$f(x_1, \ldots, x_k) = 0,$$

gde je f polinom (od k promenljivih $x_1, \ldots, x_k$) sa celim koeficijentima, čija rešenja tražimo isključivo u skupu celih brojeva. 1970. godine, Jurij V. Matijašević je pokazao da ne postoji algoritam koji bi za svaku diofantsku jednačinu odlučivao da li ona ima rešenja; na taj način je negativno rešen 10. Hilbertov problem iz 1900. godine. Međutim, upravo zbog toga diofantske jednačine i jesu fascinantno polje istraživanja u teoriji brojeva. Ovde ćemo se osvrnuti na samo nekoliko odabranih tipova.

Linearne jednačine.

Neka su $a, b, c \in \mathbb{Z}$, pri čemu bar jedan od a, b nije 0. Posmatramo jednačinu

$$ax + by = c. \tag{12.1}$$

Teorema 12.1.

(i) *Jednačina* (12.1) *ima rešenja ako i samo ako* $(a, b) \mid c$.

(ii) *Ako je* (x_0, y_0) *jedno rešenje jednačine* (12.1)*, tada su sva njena rešenja data sa*

$$x = x_0 + \frac{b}{(a,b)}t, \quad y = y_0 - \frac{a}{(a,b)}t,$$

gde je $t \in \mathbb{Z}$.

Dokaz. Deo (i) je samo reformulacija Tvrđenja 2.4, tako da dokazujemo deo (ii). Zaista, neposredno se proverava da za sve $t \in \mathbb{Z}$ dati brojevi (x, y) čine rešenje od (12.1). Obratno, pretpostavimo da (x', y') jeste jedno od rešenja. Tada važi

$$ax' + by' = c = ax_0 + by_0,$$

odakle je

$$a(x' - x_0) + b(y' - y_0) = 0.$$

Prema tome, važi

$$\frac{a}{(a,b)}(x' - x_0) = \frac{b}{(a,b)}(y_0 - y').$$

Pošto su brojevi $a/(a, b)$ i $b/(a, b)$ uzajamno prosti, sledi da $b/(a, b)$ deli $x' - x_0$, tj.

$$x' = x_0 + \frac{b}{(a,b)}t$$

za neko $t \in \mathbb{Z}$. Uvrštavajući ovo u prethodnu jednakost dobijamo traženi oblik za y'. □

Partikularno rešenje (x_0, y_0) se može lako dobiti primenom Euklidovog algoritma: ako je $a, b, r_1, r_2, \ldots, r_m = (a, b)$ niz ostataka koji taj algoritam generiše, tada se jednačina $ax + by = c$ $(a \geqslant b)$ može redom svesti na jednačine

$$\begin{aligned} r_1x_1 + by_1 &= c_1, \\ r_1x_2 + r_2y_2 &= c_2, \\ &\vdots \end{aligned}$$

za neke cele brojeve $c_1, c_2, \ldots$, pri čemu je poslednja jednačina oblika $(a, b)x_m + r_{m-1}y_m = c_m$ ili $r_{m-1}x_m + (a, b)y_m = c_m$, te se ona može neposredno rešiti, imajući u vidu da $(a, b) \mid r_{m-1}$ i $(a, b) \mid c_m$. Uvrštavanjem njenog rešenja (opšteg ili partikularnog) u prethodne jednačine, dobija se odgovarajuće rešenje za $ax + by = c$.

Ilustrovaćemo ovo na primeru jednačine

$$26x + 37y = 79.$$

Izražavajući x, sledi

$$x = -y + 3 + \frac{1 - 11y}{26}\,.$$

Dakle, mora biti $26 \mid 1 - 11y$, što vodi ka rešavanju jednačine $26u + 11y = 1$. Odavde izražavamo y, pa dobijamo

$$y = -2u + \frac{1 - 4u}{11}\,.$$

Tako je naredni korak rešavanje jednačine $4u + 11v = 1$. Sada je

$$u = -2v + \frac{1 - 3v}{4}\,,$$

pa zaključujemo da $1 - 3v$ mora biti deljivo sa 4, tj. $4w + 3v = 1$. Konačno,

$$v = -w + \frac{1 - w}{3}\,,$$

odakle je $w = -3t + 1$, $t \in \mathbb{Z}$. Stoga $w = 1$ jeste jedno partikularno rešenje, koje redom daje $v = -1$, $u = 3$, $y = -7$ i $x = 13$. Prema tome, opšte rešenje posmatrane jednačine glasi

$$x = 13 + 37t, \quad y = -7 - 26t,$$

$t \in \mathbb{Z}$, pošto je $(26, 37) = 1$.

Pitagoritne trojke.

Jedna od najpoznatijih nelinearnih diofantskih jednačina je

$$x^2 + y^2 = z^2, \tag{12.2}$$

između ostalog i zbog njene geometrijske interpretacije: njena (pozitivna) rešenja (x, y, z) opisuju sve provougle trouglove sa celobrojnim dužinama strana. Zato se ta rešenja nazivaju *Pitagorine trojke*.

Primetimo: ako je (x, y, z) Pitagorina trojka, onda je to i (xd, yd, zd) za sve $d \in \mathbb{Z}$. Zbog toga je dovoljno da se razmatraju samo pozitivna rešenja od (12.2) kod kojih je $(x, y, z) = 1$; takva rešenja se još zovu i *primitivna rešenja*.

Teorema 12.2. *Sva primitivna rešenja (x, y, z) jednačine (12.2) — pri čemu rešenja dobijena permutovanjem x i y ne smatramo različitim — data su sa*

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

gde su $m, n \in \mathbb{Z}^+$, $m > n$, različite parnosti i $(m, n) = 1$.

Dokaz. Neka je (x, y, z) neko primitivno rešenje jednačine (12.2). Dokažimo najpre da ono mora biti opisanog oblika. Pre svega, brojevi x, y, z moraju biti po parovima uzajamno prosti; u suprotnom, ako bi, na primer, bilo $(x, z) = d > 1$, tada bismo imali $d^2 \mid z^2 - x^2 = y^2$, tj. $d \mid y$, što protivreči pretpostavci $(x, y, z) = 1$. Osim toga, brojevi x, y moraju biti različite parnosti. Zbog $(x, y) = 1$ oni ne mogu biti oboje parni. Ako bi pak x, y bili oboje neparni, tada bismo imali $z^2 = x^2 + y^2 \equiv 2 \pmod 4$, što je nemoguće, jer 2 nije kvadratni ostatak po modulu 4.

Bez ograničenja opštosti, neka je x neparan, a y paran. Tada je i z neparan broj, pa imamo

$$\left(\frac{y}{2}\right)^2 = \frac{z - x}{2} \cdot \frac{z + x}{2}.$$

Brojevi $(z + x)/2$ i $(z - x)/2$ moraju biti uzajamno prosti, budući da su njihovi zbir i razlika redom (uzajamno prosti brojevi) z i x. Sledi da su oba broja $(z + x)/2$ i $(z - x)/2$ potpuni kvadrati:

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

Odavde odmah dobijamo željeni oblik za x, y, z. Dodatni uslovi za m, n takođe slede na osnovu neparnosti x i primitivnosti posmatranog rešenja.

Obratno, neka je $x = m^2 - n^2$, $y = 2mn$ i $z = m^2 + n^2$ za $m, n \in \mathbb{Z}^+$ koji zadovoljavaju date uslove. Veoma lako se proverava da ovo zaista jeste rešenje jednačine (12.2); prostaje da se vidi da je ono primitivno. Pretpostavimo suprotno: tada x i z imaju zajednički prost faktor p, pa sledi da p deli $2m^2 = (m^2 + n^2) + (m^2 - n^2)$ i $2n^2 = (m^2 + n^2) - (m^2 - n^2)$. Kako je $(m, n) = 1$, to m i n nemaju zajedničkih prostih faktora, pa (npr. po Tvrđenju 3.4) važi $(m^2, n^2) = 1$. Prema tome, jedina mogućnost je da je $p = 2$; međutim, ona je takođe isključena, jer su zbog različite parnosti m i n brojevi x, z neparni. □

Velika Fermaova teorema.

1637. godine, francuski pravnik, sudija Pjer de Ferma, verovatno najveći matematičar-amater svih vremena, napisao je na margini svog primerka Diofantove *Artimetike* (latinsko izdanje iz 1621. godine) sledeću opasku: "Zbir dva cela kuba nikada nije kub, zbir dva četvrta stepena nikada nije četvrti stepen, etc. Imam čudesan dokaz za ovu tvrdnju, ali je ova margina nažalost suviše mala da ga ovde izložim." Više od tri i po veka matematičari celog sveta — što profesionalci, što

amateri — bezuspešno su pokušavali da otkriju Fermaov "čudesni dokaz" da diofantska jednačina

$$x^n + y^n = z^n \tag{12.3}$$

nema rešenja ni za jedno $n > 2$. Pošto iz pretpostavke da jednačina $x^k + y^k = z^k$ nema rešenja sledi da ni jednačina $x^{kt} + y^{kt} = z^{kt}$ nema rešenja ni za jedno $t \geqslant 1$, dovoljno je ograničiti se na slučajeve kada je $n = 4$, odnosno kada je n neparan prost broj. Dokaz za slučaj $n = 4$ je dao sam Ferma (i mi ćemo ga kasnije ovde navesti), a ceo vek kasnije Ojler je rešio slučaj $n = 3$. U XIX veku nerešivost jednačine (12.3) je dokazana za još neke (neparne proste) vrednosti n, a u XX veku je potraga za dokazima tog tipa nastavljena i uz pomoć računara; ipak, takav pristup je razrešio samo konačno mnogo eksponenata n. 1983. godine nemački matematičar *Gerd Faltings* izazvao je senzaciju sa svojim dokazom da za svako $n > 2$ postoji samo konačno mnogo primitivnih rešenja (kod kojih je $(x, y, z) = 1$). Međutim, ispostavilo se da je to bio samo uvod u pravu "matematičku dramu" koja je usledila. 23. juna 1993., nakon gotovo sedam godina tajnog rada u potkrovlju svoje kuće i tri dana uzastopnih predavanja na seminaru Univerziteta u Kembridžu, britanski matematičar *Endrju Vajls* (Andrew Wiles) obznanio je svetu da je u potpunosti dokazao veliku Fermaovu teoremu. Ali, već te jeseni postalo je jasno da Vajlsov dokaz sadrži ozbiljan, suštinski nedostatak; nakon nekoliko pokušaja da se nastali problemi brzo reše, Vajls je 4. decembra, u i-mejlu upućenom matematičkoj javnosti priznao grešku, uz najavu da će još neko vreme posvetiti pokušajima da popravi dokaz. Te zime, pozvao je svog bivšeg učenika Ričarda Tejlora da mu pomogne u tome. Naredne jeseni, Vajls je bio spreman da odustane. A onda, kada je u ponedeljak ujutro 19. septembra 1994. Vajls odlučio da još jednom, verovatno po poslednji put pogleda svoje beleške, u trenutku nadahnuća došao je do čudesnog uvida: sve "kockice" su se konačno sklopile. Tako je, posle ravno 357 godina pokušaja od strane najbriljantnijih matematičara svog vremena, velika Fermaova teorema konačno dokazana. Kompletan dokaz izložen je na 129 strana, u sklopu dva rada u časopisu *Annals of Mathematics* (jedan u koautorstvu sa Tejlorom). Za ovaj rezultat, Vajls je dobio mnogobrojna vredna priznanja. 1999. godine jedan asteroid je nazvan po njemu, a 2000. godine britanska kraljica Elizabeta II proglasila je Ser Endrjua Vajlsa za Komandujućeg Viteza Britanske Imperije.

Ključna primedba koja je dovela do konačnog rešenja ovog epskog problema potiče od *Gerharda Freja*: naime, polazeći od pretpostavke da za neki prost broj $p > 2$ postoje prirodni brojevi a, b, c tako da je $a^p + b^p = c^p$, Frej je predložio da se posmatra kriva u ravni definisana jednačinom

$$y^2 = x(x - a^p)(x + b^p).$$

Ova kriva pripada klasi tzv. semistabilnih eliptičkih krivih. S druge strane, 1990. godine *Ken Ribet* je pokazao da ova kriva nije modularna; Vajlsov dokaz se zapravo sastoji od dokaza hipoteze (sada: teoreme) Tanijame i Šimure, koja tvrdi da krive sa tim svojstvima ne postoje. Zbog toga, ni hipotetičko rešenje jednačine (12.3) ne može da postoji.

Kao što je najavljeno, razmotrićemo slučaj $n = 4$.

Tvrđenje 12.3. *Jednačina*

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

nema rešenja u skupu celih brojeva.

Dokaz. Dokazaćemo nešto jače tvrđenje, naime, da jednačina

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

nema rešenja. Pretpostavimo suprotno; u tom slučaju, od svih (pozitivnih) rešenja odaberimo ono kod kojeg je z minimalno. Označimo uočeno rešenje sa (x_0, y_0, z_0).

Sada imamo da je (x_0^2, y_0^2, z_0) Pitagorina trojka. Lako se dokazuje da mora biti $(x_0, y_0) = 1$: u suprotnom, ako bi bilo $(x_0, y_0) = d > 1$, tada bismo imali $z_0^2 = d^4(a^4 + b^4)$, gde je $x_0 = ad$ i $y_0 = bd$, odakle bi sledilo $d^2 \mid z_0$, tj. $z_0 = cd^2$. Stoga bi (a, b, c) bilo rešenje, što uz $c < z_0$ daje kontradikciju.

Prema tome, (x_0^2, y_0^2, z_0) je primitivna Pitagorina trojka; ako je, na primer, x_0 neparno, a y_0 parno, po Teoremi 12.2 postoje uzajamno prosti brojevi $m > n$ različite parnosti tako da je

$$\begin{aligned} x_0^2 &= m^2 - n^2, \\ y_0^2 &= 2mn, \\ z_0 &= m^2 + n^2. \end{aligned}$$

Drugim rečima, $x_0^2 + n^2 = m^2$, pa je broj n paran, dok je m neparan. Pišimo $n = 2k$ i $y_0 = 2y_1$; sada je $y_1^2 = mk$, pa zbog $(m, k) = 1$ sledi da su m i k potpuni kvadrati, $m = r^2$, $k = s^2$. S druge strane, (x_0, n, m) je primitivna Pitagorina trojka, pa za neke uzajamno proste brojeve u, v različite parnosti važi $2s^2 = n = 2uv$ i $r^2 = m = u^2 + v^2$. Sada je $s^2 = uv$, pa su u, v potpuni kvadrati, $u = u_1^2$ i $v = v_1^2$, zbog čega je (u_1, v_1, r) novo rešenje jednačine $x^4 + y^4 = z^2$. Međutim, $r \leqslant r^2 = m \leqslant m^2 < z_0$, što je kontradikcija sa minimalnošću z_0. □

Pelove jednačine.

Neka je m pozitivan ceo broj koji *nije* potpun kvadrat (zapravo, ne predstavlja ograničenje opštosti da se pretpostavi da je m *kvadratno slobodan*, tj. da je proizvod različitih prostih brojeva). Tada jednačinu oblika

$$x^2 - my^2 = 1 \tag{12.4}$$

zovemo *Pelova jednačina*. Naravno, $x = \pm 1$, $y = 0$ su rešenja svake Pelove jednačine; ova rešenja su trivijalna, dok su sva druga netrivijalna.

Primetimo da se leva strana jednačine (12.4) može faktorisati na sledeći način:

$$(x + y\sqrt{m})(x - y\sqrt{m}) = 1.$$

Zbog toga, ako je (x, y) jedno netrivijalno rešenje jednačine (12.4) i ako sa x_n, y_n označimo cele brojeve definisane sa

$$x_n + y_n\sqrt{m} = (x + y\sqrt{m})^n$$

za $n \geqslant 1$, tada i (x_n, y_n) predstavlja rešenje. Sva uočena rešenja (x_n, y_n) su različita, pa tako dolazimo do zaključka: ako jednačina (12.4) ima bar jedno netrivijalno rešenje, ima ih beskonačno mnogo. Međutim, netrivijalna rešenja uvek postoje; ovo tvrđenje (koje se zasniva na nekim osnovnim rezultatima iz oblasti diofantskih aproksimacija) dajemo bez dokaza.

Teorema 12.4. *Neka je m pozitivan ceo broj koji nije potpun kvadrat. Tada jednačina* (12.4) *ima beskonačno mnogo rešenja.*

Štaviše, moguće je opisati skup svih rešenja Pelove jednačine (12.4).

Teorema 12.5. *Neka je m pozitivan ceo broj koji nije potpun kvadrat i neka je (x_0, y_0) ono pozitivno rešenje ($x_0 > 0$, $y_0 > 0$) jednačine* (12.4) *za koje je $x_0 + y_0\sqrt{m}$ minimalno. Tada su sva rešenja (x, y) od* (12.4) *određena sa*

$$x + y\sqrt{m} = \pm(x_0 + y_0\sqrt{m})^n,$$

$n \in \mathbb{Z}$.

Dokaz. Po prethodnim primedbama, ako je (x_0, y_0) rešenje od (12.4), onda je to i svaki par (x, y) određen uslovom iz formulacije teoreme. Dokazaćemo da drugih rešenja nema. Pretpostavimo suprotno: da postoji neko rešenje (x, y) koje nije zadatog oblika. Pri tome, ne predstavlja nikakvo umanjenje opštosti ako pretpostavimo da je $x + y\sqrt{m} > 0$. Pošto je $\lim_{n\to-\infty}(x + y\sqrt{m})^n = 0$ i $\lim_{n\to+\infty}(x + y\sqrt{m})^n = +\infty$, sledi da postoji $k \in \mathbb{Z}$ tako da je

$$(x_0 + y_0\sqrt{m})^k < x + y\sqrt{m} < (x_0 + y_0\sqrt{m})^{k+1}.$$

Množeći ovu dvostruku nejednakost sa $(x_0 - y_0\sqrt{m})^k > 0$ i imajući u vidu da je $x_0^2 - my_0^2 = 1$, dobijamo

$$1 < (x + y\sqrt{m})(x_0 - y_0\sqrt{m})^k < x_0 + y_0\sqrt{m}. \tag{12.5}$$

Ako sada definišemo $x', y' \in \mathbb{Z}$ sa $x' + y'\sqrt{m} = (x + y\sqrt{m})(x_0 - y_0\sqrt{m})^k$, sledi da važi

$$\begin{aligned}(x')^2 - m(y')^2 &= (x' + y'\sqrt{m})(x' + y'\sqrt{m}) \\ &= (x + y\sqrt{m})(x_0 - y_0\sqrt{m})^k(x - y\sqrt{m})(x_0 + y_0\sqrt{m})^k \\ &= (x^2 - my^2)(x_0^2 - my_0^2)^k = 1,\end{aligned}$$

pa i (x', y') predstavlja rešenje jednačine (12.4). Nejednakosti (12.5) možemo sada prepisati u obliku

$$1 < x' + y'\sqrt{m} < x_0 + y_0\sqrt{m}, \tag{12.6}$$

odakle je

$$0 < x' - y'\sqrt{m} < 1.$$

Zbog poslednjih nejednakosti, nemogući su slučajevi $y' = 0$, zatim $x' > 0$, $y' < 0$, kao i $x' < 0$, $y' > 0$, dok je zbog (12.6) ne može biti $x', y' < 0$. Prema tome, važi $x', y' > 0$. Ali, sada druga nejednakost iz (12.6) čini kontradikciju sa pretpostavljenim minimalnim svojstvima rešenja (x_0, y_0). □

Prethodna dva dokaza ilustruju ono što se u teoriji diofantskih jednačina zove *Fermaov metod beskonačnog spuštanja*: pod pretpostavkom da posmatrana jednačina ima rešenja (određenog tipa), uoči se rešenje koje je u izvesnom smislu "minimalno". S druge strane, svojstva jednačine omogućavaju da se, polazeći od minimalnog rešenja, konstruiše "manje", što daje kontradikciju i pokazuje da dotična rešenja zapravo ne postoje.