Универзитет у Београду

Математички факултет

О неким класичним квадратним Диофантовим једначинама

Мастер рад

ментор: Марко Радовановић

студент: Ивана Фируловић

Београд, 2017.

Садржај

Увод

Диофантов допринос развоју математике, а пре свега аритметике, је веома значајан и због тога је назван „оцем" аритметике. Диофантове једначине су значајне јер обједињују готово све садржаје теорије бројева (дељивост бројева, прости бројеви, конгруенција...), теорије једначина, полинома, неједнакости, математичке логике...

Истраживање квадратних Диофантових једначина развило је многе методе за њихово решавање а неке од њих су: метод минималних решења, Диофантове апроксимације, квадратни остаци, алгебарска раширења. Ове методе биће приказане кроз примере у даљем делу рада.

У овом раду биће речи о Питагориним тројкама. Познато је да су Питагорину теорему, која има значајне везе са Питагориним тројкама у својим грађевинским подвизима поред Египћана користиле и цивилизације у Вавилону, Кини, Индији и Мексику. Први теоријски и логички утемељен доказ Питагорине теореме потиче још од Еуклида. Историја решења Питагорине једначине $x^2 + y^2 = z^2$ познатих као Питагорине тројке (x, y, z), нераздвојива је од историје Питагорине теореме и има такође дугу прошлост. Питагорина тројка $(3,4,5)$ је била позната свим древним културама. На пример, баш та тројка је записана у кинеским документима старим преко три хиљаде година. Древне цивилизације су знале и за друге Питагорине тројке, о чему сведоче глинене плочице исписане клинастим писмом. Иако многи историчари математике, данас општеприхваћену формулу, која генерише све Питагорине тројке: $x = 2mn,\ y = m^2 - n^2,\ z = m^2 + n^2$, приписују Диофанту, та формула је вероватно Еуклидово дело, бар у смислу првог писаног трага. Диофант се једноставно тим формулама веома често користио, а вероватно је и први који је успео да изведе и формалан доказ тог тврђења.

Међу Диофантовим једначинама за које постоји алгоритам за њихово решавање истиче се једначина облика $x^2 - dy^2 = 1$, где d није потпун квадрат. У математичкој литератури ова једначина је позната као Пелова једначина. Савремени историчари математике Ојлера оптужују да је неправедно ову једначину назвао Пеловом. Наиме, Ојлер је читајући Валисову „Алгебру" из 1658. године, очигледно направио грешку и због приличног Валисовог позивања у књизи на Пела и цитирање његових радова, разумео да су Валис и Броункер у својим радовима о једначини $x^2 - dy^2 = 1$, користили неке Пелове резултате. Међутим, том једначином су се интезивно бавили Диофант, Архимед, Баскара, Лагранж,

Ојлер, Гаус. У ресветљавању алгоритма за решавање Пелове једначине могуће је више приступа, али су најуобичајнија два: геометријски и алгебарски.

Писаћу и о једној од најпознатијих теорема у историји математике а то је велика Фермаова теорема. Проблем који је поставио Ферма је такозвана велика Фермаова теорема која тврди да је једначина $x^n + y^n = z^n$ немогућа за целе позитивне вредности x, y, z, ако је природан број $n > 2$. Доказ за $n = 3$ извео је Ојлер, али је протекло преко сто година када је Гаус доказао теоријске основе које је у свом доказу неосновано користио Ојлер. Доказ за $n = 5$ је 1828. године објавио Дирихле, али је он био веома сложен. 1912. године овај доказ је значајно упростио Племељ. Доказ за $n = 7$ извео је Ламе, али је тај доказ касније прилично усавршио Лебег. На крају 20. века, цео свет је признао, да је 360 година после свог настанка велика Фермаова теорема, која је у суштини све то време била хипотеза, постала доказана теорема. Ендру Вајлс (Andrew Wiles) је доказао велику Фермаову теорему и ушао у историју.

Велики немачки математичар Хилберт је 1900. године на међународном математичком конгресу у Паризу формулисао 23 проблема чије је решавање значајно допринело развоју математичких наука у прошлом веку. Од велике важности за овај рад је 10. Хилбертов проблем – проблем решивости Диофантових једначина: „За дату Диофантову једначину са било којим бројем непознатих величина и са целобројним коефицијентима измислити поступак којим се може одлучити да ли та једначина има или нема целобројних решења". Другим речима Хилберт се питао да ли постоји општи алгоритам помоћу којег се за Диофантову једначину одређене класе може рећи да ли она има целобројних решења. Теоријске основе за решавање 10. Хилбертовог проблема у време његове формулације су биле оскудне. Међутим Гедел, Черч, а касније педесетих и шездесетих година Робинсон, Дејвис и Патнам су својим радовима припремили 10. Хилбертов проблем за решење, да би га руски математичар Јурij Матијашевич 1970. године дефинитивно негативно решио. Наиме, он је доказао да поступак за кога се Хилберт интересује у својим проблемима, не постоји.

Негативан одговор на 10. Хилбертов проблем указује да је решавање Диофантових једначина прилично креативан посао који може значајно утицати на интелектуални и научни развој људи.

Глава 1

Линеарне и нелинеарне Диофантове једначине

Основна питања која се постављају везана за сваку Диофантову једначину је наћи решења дате једначине, доказати или отповргнути егзистенцију решења. Када говоримо о линеарној Диофантовој једначини са две променљиве, одговори на ова питања налазе се у наредним примерима и теоремама. Често одговори на задата питања могу бити тешки, што захтева препознавање одговарајућег метода за решавање датог проблема. У овом поглављу биће изложене најчешће методе за решавање Диофантових једначина.

Линеарне Диофантове једначине

Теорема 1. Линеарна Диофантова једначина $ax + by = c$ има решења ако и само ако $d \mid c$, где је $d = (a, b)$. У том случају је опште решење једначине облика

$$x = \frac{c}{d}\alpha + \frac{b}{d}t, \quad y = \frac{c}{d}\beta - \frac{a}{d}t \quad (t \in \boldsymbol{Z}),$$

где се решење (α, β) једначине $a\alpha + b\beta = d$ може добити Еуклидовим алгоритмом.

Специјално, ако су бројеви a и b узајамно прости, тј. ако је $d = (a, b) = 1$, онда је сваки цео број c дељив са d па једначина $ax + by = c$ сигурно има решења.

Доказ: Ако је (x_0, y_0) једно целобројно решење линеарне Диофантове једначине облика $ax + by = c$, тада је $ax_0 + by_0 = c$. Постоје узајамно прости бројеви k и l такви да је $a = kd$ и $b = ld$, што значи да је $kdx_0 + ldy_0 = c$, односно $d(kx_0 + ly_0) = c$. Лева страна једнакости је дељива са d, па мора бити и десна страна, тј. $d \mid c$.

Обрнуто, нека је $d \mid c$, тада постоји цео број m такав да је $c = md$. Како се број d може представити као линеарна комбинација од a и b, то је $d = \alpha a + \beta b$ $(\alpha, \beta \in \boldsymbol{Z})$. Тада је $c = md = m(\alpha a + \beta b)$, па је онда $x = m\alpha$, $y = m\beta$, једно решење дате једначине.

Дакле, ако $d \mid c$, тада једначина $ax + by = c$ има решење $x_1 = \frac{c}{d}\alpha$, $y_1 = \frac{c}{d}\beta$ где је пар (α, β) решење једначине $ax + by = d$. Међутим, у том случају једначина има бесконачно много решења. Претпоставимо да је (u, v) произвољно решење једначине $ax + by = c$. Онда је $au + bv = c$. Са друге стране је $ax_1 + by_1 = c$. Према томе имамо да је

$$au + bv = ax_1 + by_1,$$

одакле је

$$\frac{a}{d}(u - x_1) = \frac{b}{d}(y_1 - v).$$

Како је $d = (a, b)$, то је $(\frac{a}{d}, \frac{b}{d}) = 1$, па

$$\frac{b}{d} | u - x_1, \qquad \frac{a}{d} | y_1 - v$$

одакле је

$$u = x_1 + \frac{b}{d}t, \qquad v = y_1 - \frac{a}{d}t, \qquad t \in \boldsymbol{Z}.$$

Из

$$au + bv = a\left(x_1 + \frac{b}{d}t\right) + b\left(y_1 - \frac{a}{d}t\right) = ax_1 + by_1 = c$$

следи да уређени пар (u, v) за произвољно $t \in \boldsymbol{Z}$ задовољава дату једначину.

Пример 1. Решити једначину $155x - 95y = 100$.

Решење: Дата једначина има решење, јер је $(155, 95) = 5$, а $5|100$. Према томе једначина се дељењем са 5 може упростити, тако да се добије $31x - 19y = 20$. Како је $(31, 19) = 1$, то постоје цели бројеви α и β такви да је $31\alpha - 19\beta = 1$. Бројеви α и β се одређују Еуклидовим алгоритмом:

$$31 = 1 \cdot 19 + 12$$

$$19 = 1 \cdot 12 + 7$$

$$12 = 1 \cdot 7 + 5$$

$$7 = 1 \cdot 5 + 2$$

$$5 = 2 \cdot 2 + 1.$$

Сада је $1 = 5 - 2 \cdot 2 = 5 - 2(7 - 1 \cdot 5) = 3 \cdot 5 - 2 \cdot 7 = 3(12 - 1 \cdot 7) - 2 \cdot 7 = 3 \cdot 12 - 5 \cdot 7 = 3 \cdot 12 - 5(19 - 1 \cdot 12) = 8 \cdot 12 - 5 \cdot 19 = 8(31 - 1 \cdot 19) - 5 \cdot 19 = 8 \cdot 31 - 13 \cdot 19.$

Дакле, $\alpha = 8$ и $\beta = 13$. Како је $31\alpha - 19\beta = 1$, то је $20(31\alpha - 19\beta) = 20$, па је $31 \cdot 20\alpha - 19 \cdot 20\beta = 20$. Даље добијамо да је $x_0 = 20\alpha = 20 \cdot 8 = 160$ и $y_0 = 20\beta = 20 \cdot 13 = 260$. Према томе, опште решење дате једначине је дато формулом :

$$x = 160 + 19k,\ y = 260 + 31k \ (k \text{ је цео број}).$$

Пример 2. Решити једначину $27x + 59y = 20$.

Решење: Дата једначина има решења јер је $(27,\ 59) = 1$ и $1|20$. Како је $d = 1$, то постоје цели бројеви α и β такви да је $27\alpha + 59\beta = 1$. Бројеви α и β се одређују Еуклидовим алгоритмом:

$$59 = 2 \cdot 27 + 5$$

$$27 = 5 \cdot 5 + 2$$

$$5 = 2 \cdot 2 + 1.$$

Сада је $1 = 5 - 2 \cdot 2 = 5 - 2(27 - 5 \cdot 5) = 11 \cdot 5 - 2 \cdot 27 = 11(59 - 2 \cdot 27) - 2 \cdot 27 = 11 \cdot 59 - 24 \cdot 27$. Дакле, $\alpha = -24$ и $\beta = 11$.

Знамо да је

$$x = \frac{c}{d}\alpha + \frac{b}{d}t \qquad y = \frac{c}{d}\beta - \frac{a}{d}t \ (t \in \boldsymbol{Z}).$$

Даље имамо

$$x = \frac{20}{1} \cdot (-24) + \frac{59}{1} \cdot t \qquad y = \frac{20}{1} \cdot 11 - \frac{27}{1} \cdot t,$$

па је решење

$$x = -480 + 59t \qquad y = 220 - 27t \ (t \in \boldsymbol{Z}).$$

Пример 3. Доказати да Диофантова једначина $28x + 70y = 39$ нема решења у скупу целих бројева.

Решење: Како је $(28, 70) = 14$ и како 14 није делитељ броја 39, дата Диофантова једначина нема решења у скупу целих бројева.

Нелинеарне Диофантове једначине

Познато је да не постоји „општи поступак'' за решавање Диофантових једначина, али зато постоје методе којима се могу решавати неке специјалне класе ових једначина. У даљем делу рада видећемо неке од тих метода који су корисни за решавање квадратних Диофантових једначина.

Метод производа

Ако су $I_1(x, y, \dots), \dots, I_m(x, y, \dots)$ цели алгебарски изрази, тада је једначина

$$I_1(x, y, \dots) \cdot \dots \cdot I_m(x, y, \dots) = \mathrm{a},$$

за неки цео број a, еквивалентна дисјункцији система једначина:

$$I_1(x, y, \dots) = c_1 \ \dots \ I_m(x, y, \dots) = c_m \quad \text{или}$$

$$I_1(x, y, \dots) = d_1 \dots I_m(x, y, \dots) = d_m \quad \text{или} \dots$$

при чему је $\mathrm{a} = c_1 \cdot \dots \cdot c_m = d_1 \cdot \dots \cdot d_m = \dots$ представљено на све могуће начине као производ m целих бројева.

Пример 4. Решити у скупу природних бројева једначину $x^2 - y^2 = 31$.

Решење: Пошто је 31 прост број и важи $x^2 - y^2 = (x - y)(x + y)$ имамо да је

$$x - y = 1 \quad \text{и} \quad x + y = 31$$

или

$$x - y = 31 \quad \text{и} \quad x + y = 1.$$

Решење првог система је $x = 16,\ y = 15,$ док други систем нема решења у скупу природних бројева (што се може закључити и без рачуна јер ако $x,\ y \in \boldsymbol{N}$ онда је $x + y > x - y$).

Пример 5. Решити једначину $xy - 2x + 3y = 13$ у скупу целих бројева.

Решење: Како је $xy - 2x + 3y = 13 \Leftrightarrow xy - 2x + 3y - 6 = 7 \Leftrightarrow x(\mathrm{y} - 2) + 3(\,\mathrm{y} - 2) = 7 \Leftrightarrow (x + 3)(y - 2) = 7$, разликујемо следеће случајеве:

1) $x + 3 = 1,\ y - 2 = 7$

2) $x + 3 = 7,\ y - 2 = 1$

3) $x + 3 = -1,\ y - 2 = -7$

4) $x + 3 = -7,\ y - 2 = -1$

Дакле, решења дате једначине су: $(-2, 9\,),\ (4, 3),\ (-4, -5),\ (-10, 1).$

Пример 6. Одредити све природне бројеве x такве да је $2^x + 1$ квадрат природног броја.

Решење: Ако је $2^x + 1 = y^2$, онда је $y^2 - 1 = 2^x$. Односно $(y - 1)(y + 1) = 2^x$. Нека је $2^x = 2^a \cdot 2^b\ (a \geq b)$, где је $a + b = x$. Тада је $y + 1 = 2^a$ и $y - 1 = 2^b$, па је $2^a - 2^b = y + 1 - y + 1$ односно $2^a - 2^b = 2$. Даље следи да је $2^b(2^{a-b} - 1) = 2$. Јасно је да је $2^b = 2$ и $2^{a-b} - 1 = 1$, па је $b = 1$ и $a - b = 1$. Дакле $a = 2,\ b = 1,\ a + b = 3$. Према томе имамо да је $2^3 + 1 = 9$ односно $x = 3$.

Пример 7. Одредити све просте бројеве p тако да је $2p + 1$ седми степен неког природног броја.

Решење: Нека је тражени природни број n. Према условима задатка је:

$$2p + 1 = n^7$$

$$n^7 - 1 = 2p$$

$$(n - 1)(n^6 + n^5 + n^4 + n^3 + n^2 + n + 1) = 2p.$$

Како су $1, 2, p$ и $2p$ једини чиниоци броја $2p$, то су могући следећи случајеви:

1) Ако је $n-1=1$, онда је $n=2$, па је $n^6+n^5+n^4+n^3+n^2+n+1=2p=127$, што није могуће, јер је $2p$ паран, а 127 непаран број.
2) Ако је $n-1=2$, онда је $n=3$, па је $n^6+n^5+n^4+n^3+n^2+n+1=1093=p$. Како је 1093 прост број, то је $(n,p)=(3,1093)$ једно решење проблема.
3) Ако је $n-1=p$, онда је $n=p+1\geq 3$, па је $n^6+n^5+n^4+n^3+n^2+n+1\geq n+1\geq 3$, што значи да у овом случају нема решења.
4) Ако је $n-1=2p$, онда је $n^6+n^5+n^4+n^3+n^2+n+1=1$, па је $n^6+n^5+n^4+n^3+n^2+n=0$. Претходна једначина нема решења у скупу природних бројева.

Метод збира

Ако су $I_1(x,y,\dots),\dots,I_m(x,y,\dots)$ цели алгебарски изрази, тада је једначина

$$(I_1(x,y,\dots))^2+\cdots+(I_m(x,y,\dots))^2=a,$$

за неки природан број a, еквивалентна дисјункцији система једначина:

$$(I_1(x,y,\dots))^2=s_1\ .\ .\ .(I_m(x,y,\dots))^2=s_m \text{ или}$$

$$(I_1(x,y,\dots))^2=t_1\ .\ .\ .(I_m(x,y,\dots))^2=t_m \text{ или...}$$

при чему је $a=s_1+\ .\ .\ .+s_m=t_1+.\ .\ .+t_m=\cdots$ представљено на све могуће начине као збир m потпуних квадрата.

Пример 8. У скупу целих бројева решити једначину $x^4+y^{2006}=2x^2-1$.

Решење: Како је дата једначина $x^4+y^{2006}=2x^2-1$ еквивалентна са једначином

$$x^4-2x^2+1+y^{2006}=0$$

односно

$$(x^2-1)^2+(y^{1003})^2=0.$$

Како је збир квадрата два цела броја једнак 0 ако и само ако су оба броја једнака 0, па је зато могућ само један случај:

$$x^2-1=0 \text{ и } y=0$$

$$(x-1)(x+1)=0 \text{ и } y=0.$$

Дакле решења дате једначине су: $(1, 0)$ или $(-1, 0)$.

Пример 9. У скупу целих бројева решити једначину $4x^2 + y^2 = 12x + 4y - 12$.

Решење: Трансформишимо једначину у збир квадрата $(2x - 3)^2 + (y - 2)^2 = 1$. Пошто се у задатку траже само решења у скупу целих бројева, разликујемо следећа два случаја:

1) $2x - 3 = 1$ и $y - 2 = 0$ тј.
   $x = 2$ и $y = 2$
2) $2x - 3 = -1$ и $y - 2 = 0$ тј.
   $x = 1$ и $y = 2$.

Дакле решења дате једначине су: $(2, 2);\ (1, 2)$.

Пример 10. Постоје ли цели бројеви x и y који задовољавају једнакост $x^2 + xy + y^2 = 1$?

Решење: Ако се дата једначина помножи са 2 добија се еквивалентна једначина $2x^2 + 2xy + 2y^2 = 2$, односно $x^2 + (x + y)^2 + y^2 = 2$. Збир квадрата три броја је једнак 2, ако су два од тих бројева по 1, а трећи 0, па разликујемо три могућности:

1) $x^2 = 1,\ (x + y)^2 = 1$ и $y^2 = 0$. Следи да је $y = 0,\ (x - 1)(x + 1) = 0$ односно $x = 1$ или $x = -1$, па су решења $(1, 0)$ или $(-1, 0)$.
2) $x^2 = 1,\ (x + y)^2 = 0$ и $y^2 = 1$. Како је $x + y = 0$, а $|x| = 1$ и $|y| = 1$, то су решења $(1, -1)$ или $(-1, 1)$.
3) $x^2 = 0,\ (x + y)^2 = 1$ и $y^2 = 1$. Следи да је $x = 0$, док је $y = 1$ или $y = -1$, па су решења $(0, 1)$ или $(0, -1)$.

Сва решења дате једначине су : $(1, 0);\ (-1, 0);\ (1, -1);\ (-1, 1);\ (0, 1);\ (0, -1)$.

Пример 11. У скупу целих бројева решити једначину

$$x^2 + 5y^2 + 5z^2 - 4xz - 2y - 4yz + 1 = 0.$$

Решење: Трансформишимо једначину на следећи начин

$$(x^2 - 4xz + 4z^2) + (z^2 - 4yz + 4y^2) + (y^2 - 2y + 1) = 0.$$

Одавде је

$$(x-2z)^2+(z-2y)^2+(y-1)^2=0.$$

Следи да је

$$x-2z=0,\ z-2y=0 \text{ и } y-1=0$$

па је $y=1,\ z=2y=2$ и $x=2z=4.$

Метод количника

Једначине које су линеарне, односно квадратне по једној од променљивих чине класу једначина које често можемо решавати комбиновањем метода из теорије обичних алгебарских једначина и теорије целих бројева.

На пример једначина $A(x)y+B(x)=0$, при чему су $A(x)$ и $B(x)$ неки цели алгебарски изрази по x, може се решавати анализом рационалног алгебарског израза $\frac{A(x)}{B(x)}$.

Пример 12. Решити једначину $xy+7x-3y=23$ у скупу целих бројева.

Решење: Дату једначину можемо записати као $x(y+7)=23+3y$.

За $y=-7$ једначина нема решења, а за $y\neq -7$ је:

$$x=\frac{23+3y}{y+7}=3+\frac{2}{y+7}.$$

Да би решење x било целобројно, мора $y+7\in\{1,-1,2,-2\}$ тј. $y\in\{-6,-8,-5,-9\}$.

Скуп решења је: $R=\{(5,-6),(1,-8),(4,-5),(2,-9)\}$.

Пример 13. Одредити све целе бројеве x и y који задовољавају једнакост

$$x^2-xy+2x-3y=6.$$

Решење: Дату једначину можемо трансформисати тако да она има следећи облик:

$x^2+2x-6=xy+3y$ односно $x^2+2x-6=y(x+3)$.

За $x = -3$ једначина нема решења, док за $x \neq -3$ имамо да је:

$$y = \frac{x^2 + 2x - 6}{x + 3} = x - 1 - \frac{3}{x + 3}.$$

Како y мора бити цео број разликују се следеће могућности:

1) $x + 3 = 1 \Rightarrow x = -2,\ y = -6$
2) $x + 3 = -1 \Rightarrow x = -4,\ y = -2$
3) $x + 3 = 3 \Rightarrow x = 0,\ y = -2$
4) $x + 3 = -3 \Rightarrow x = -6,\ y = -6.$

Пример 14. Одредити све двоцифрене природне бројеве који су једнаки квадрату збира својих цифара.

Решење: Нека је тражени број $\overline{xy} = 10x + y$. Из услова задатка се добија да је $10x + y = (x + y)^2$ или $9x + (x + y) = (x + y)^2$. Како је $x \neq 0$, то је и $(x + y) \neq 0$. Дељењем добијене једнакости са $x + y$ добија се једнакост $\frac{9x}{x+y} + 1 = x + y$.

Ако је највећи заједнички делилац за x и y једнак d, онда постоје узајамно прости бројеви a и b такви да је $1 \leq x = ad \leq 9$ и $0 \leq y = bd \leq 9$. Тада једначина постаје:

$$\frac{9ad}{(a + b)d} + 1 = (a + b)d$$

односно

$$\frac{9a}{a + b} + 1 = (a + b)d.$$

Прво ћемо показати да су a и $(a + b)$ узајамно прости.

Претпоставимо супротно да a и $(a + b)$ нису узајамно прости. Тада $\exists\ k,\ k > 1$ тако да је $a = a_1 k$ и $a + b = c_1 k$. Из $a + b = c_1 k$ имамо да је $b = c_1 k - a$ односно $b = c_1 k - a_1 k$, $b = k(c_1 - a_1)$. Дакле имамо $a = a_1 k,\ b = k(c_1 - a_1)$ а то је немогуће јер су a и b узајамно прости.

Како количник $\frac{9a}{a+b}$ мора бити природан број и како су a и $(a + b)$ узајамно прости и пошто 9 мора бити дељив са $a + b$, могућа су следећа три случаја:

1) Ако је $a+b=1$, онда је $9a+1=d$. Овај случај је немогућ, јер из $a+b=1$ следи, због $x\neq 0$, да је $a=1,\ b=0$. У том случају је $d=10$, што није могуће, јер је $d\leq 9$.
2) Ако је $a+b=3$, онда је $3a+1=3d$. Односно $3a-3d=-1,\ 3(a-d)=-1$. Одавде имамо да је лева страна дељива са 3 а десна није, па овај случај није могућ.
3) Ако је $a+b=9$, онда је $a+1=9d$ или $a=9d-1$. Како је $1\leq x\leq 9$, то је $1\leq x=ad=(9d-1)d\leq 9$, онда је $d=1$. То значи да је $a=8$ и $b=1$.

Дакле тражени број је $81=(8+1)^2$.

Метод дискриминанте

Природа решења једначине $A(x)y^2+B(x)y+C(x)=0$ зависи од дискриминанте $D(x)=\big(B(x)\big)^2-4A(x)C(x)$.

Пошто тражимо целобројна решења, анализа дискриминанте заснива се на чињеници да је $D(x)\geq 0$, али и више, да је $D(x)=m^2$, за неки цео број m.

Пример 15. Решити једначину $7x+14y=5x^2+5xy+5y^2$ у скупу целих бројева.

Решење: Дату једначину можемо да запишемо у еквивалентном облику

$$5y^2+(5x-14)y+(5x^2-7x)=0,$$

и она је квадратна по y. Како је $D(x)=(5x-14)^2-4\cdot 5(5x^2-7x)=196-75x^2$, ако дата једначина има решења, онда је $x^2\leq \frac{196}{75}=2{,}6133\ldots$, односно $x\,\epsilon\,\{-1,0,1\}$. Имамо следеће могућности:

1) $x=-1\Rightarrow 5\mathrm{y}^2-19\mathrm{y}+12=0\Rightarrow \mathrm{y}=3$
2) $x=0\Rightarrow \mathrm{y}=0$
3) $x=1\Rightarrow \mathrm{y}=2.$

Дакле, $R=\{(-1,3),\ (0,0),\ (1,2)\}$.

Пример 16. Одредити све целе бројеве x и y такве да је $2x^2 + 5x + y^2 = 19$.

Решење: Дату једначину можемо посматрати као квадратну по x, тј. $2x^2 + 5x + (y^2 - 19) = 0$. Како је $D(y) = 5^2 - 4 \cdot 2 \cdot (y^2 - 19) = 177 - 8y^2$, ако дата једначина има решења, онда је $y^2 \leq \frac{177}{8} = 22{,}125$ односно $y \in \{-4, -3, -2, -1, 0, 1, 2, 3, 4\}$.

Испитивањем ових девет случајева за y добијамо да је скуп решења једначине $\{(-3, 4), (-3, -4), (2, 1), (2, -1)\}$.

Остаци квадрата

Већина ученика је имала прилику да решава задатке у којим се користи чињеница да последња цифра (у декадном запису) природног броја који је потпун квадрат (дакле, квадрат неког другог природног броја) не може бити произвољна. Могуће последње цифре квадрата су $0, 1, 4, 5, 6$ и 9, док не постоје потпуни квадрати који се завршавају на $2, 3, 7$ или 8. Ова чињеница се може другачије исказати на следећи начин:

ако $a \in \{0, 1, 2, \ldots, 9\}$, онда конгруенција

$$x^2 \equiv a \pmod{10}$$

има решења (по x) ако и само ако $a \in \{0, 1, 4, 5, 6, 9\}$ или још: могући остаци квадрата природних бројева по модулу 10 су $0, 1, 4, 5, 6$ и 9.

Можемо посматрати остатке квадрата и по осталим малим модулима (не само по модулу 10) и то ћемо видети у наредном примеру.

Пример 17. Могући остаци квадрата природних бројева:

по модулу 3 су: $0, 1$

по модулу 4 су: $0, 1$

по модулу 5 су: $0, 1, 4$

по модулу 6 су: $0, 1, 3, 4$

по модулу 7 су: $0, 1, 2, 4$

по модулу 8 су: $0, 1, 4$

по модулу 9 су: $0, 1, 4, 7.$

Ово се лако проверава конструисањем таблица као што је наредна, за остатке по модулу 7

x	0	1	2	3	4	5	6
x^2	0	1	4	2	2	4	1

Пример 18 . Доказати да $21 \mid a^2 + b^2$ повлачи $441 \mid a^2 + b^2$.

Решење: Ако $21 \mid a^2 + b^2$ онда $3 \mid a^2 + b^2$ и $7 \mid a^2 + b^2$. Остаци квадрата по модулу 3 могу бити 0 или 1, па збир два таква квадрата може бити дељив са 3 само ако су a и b дељиви са 3. Онда је $9 \mid a^2 + b^2$. Слично, остаци квадрата по модулу 7 могу бити $0, 1, 2$ или 4 па збир таква два броја може бити дељив са 7 само ако су оба дељива са 7. Тада и $49 \mid a^2 + b^2$, а одатле и из претходног следи $9 \cdot 49 = 441 \mid a^2 + b^2$.

Метод остатака

Овај метод је користан за доказивање да дата једначина нема решења. Наиме ако за неки природан број $n > 1$ важи $L(x, y, \dots) \equiv r \ (mod\ n)$ при чему $r \in R \subseteq \{0, 1, 2, \dots, n-1\}$, а $D(x, y, \dots) \equiv s \ (mod\ n)$ при чему $s \in S \subseteq \{0, 1, 2, \dots, n-1\}$, тада у случају да је $R \cap S = \emptyset$, једначина $L(x, y, \dots) = D(x, y, \dots)$ нема решења у скупу целих бројева.

Метод остатака при дељењу са 10, често се назива **метод последње цифре**, док метод остатака при дељењу са 2 назива **метод парности**. На примеру $\equiv (mod\ 10)$, илустоваћемо формирање табеле које могу бити од велике користи:

$n \equiv \cdot (mod\ 10)$	0	1	2	3	4	5	6	7	8	9
$n^2 \equiv \cdot (mod\ 10)$	0	1	4	9	6	5	6	9	4	1
$n^4 \equiv \cdot (mod\ 10)$	0	1	6	1	6	5	6	1	6	1
$n(n+1) \equiv \cdot (mod\ 10)$	0	2	6	2	0	0	2	6	2	0

Пример 19. Доказати да једначина $x^2 + y^2 = 2006$ нема решења у скупу целих бројева.

Решење: Квадрати целих бројева при дељењу са 4 дају остатак 0 (када је број паран) или 1 (када је број непаран). Како је $2006 \equiv 2 \ (mod\ 4)$ па онда следи да су x, y непарни. Означимо $x = 2x_1 + 1$, $y = 2y_1 + 1$ где су x_1, y_1 цели бројеви. Тада је:

$$(2x_1 + 1)^2 + (2y_1 + 1)^2 = 2006$$

$$4{x_1}^2 + 4x_1 + 1 + 4{y_1}^2 + 4y_1 + 1 = 2006$$

$$4({x_1}^2 + x_1 + {y_1}^2 + y_1) = 2004$$

дељењем са 4 добијамо: $x_1(x_1 + 1) + y_1(y_1 + 1) = 501.$

С обзиром да је лева страна паран број, а десна непаран, то једначина нема решења у скупу целих бројева.

Пример 20. Доказати да једначина $3x^2 + 8 = y^2$ нема решења у скупу целих бројева.

Решење: Ако би постојали цели бројеви x и y такви да је $3x^2 + 8 = y^2$ онда би из $3x^2 \equiv 0\ (mod\ 3)$ и $8 \equiv 2\ (\ mod\ 3)$, следило да је $y^2 \equiv 2\ (\ mod\ 3)$. Ово је немогуће јер остаци квадрата по модулу 3 могу бити 0 или 1.

Пример 21. Доказати да једначина $x^2 + y^2 + z^2 = 2007$ нема решења у скупу целих бројева.

Решење: Квадрати целих бројева при дељењу са 4 дају остатак 0 (када је број паран) или 1 (када је број непаран). Како је $2007 \equiv 3\ (mod\ 4)$ то сва три броја $x,\ y,\ z$ морају бити непарна. Нека је $x = 2x_1 + 1,\ y = 2y_1 + 1,\ z = 2z_1 + 1$, где су $x_1,\ y_1,\ z_1$ цели бројеви. Тада је

$${x_1}^2 + 4x_1 + 1 + 4{y_1}^2 + 4y_1 + 1 + 4{z_1}^2 + 4z_1 + 1 = 2007,$$ односно

$$x_1(x_1 + 1) + y_1(y_1 + 1) + z_1(z_1 + 1) = 501.$$

Лева стране последње једначине је паран број, а десна непаран, па једначина нема решења у скупу целих бројева.

Пример 22. Доказати да једначина $3x^2 + 5y^2 = 4444$ нема решења у скупу целих бројева.

Решење: За свако $n \in \boldsymbol{N}$ имамо $n^2 \equiv r(mod\ 10)$, при чему $r \in \{0, 1, 4, 5, 6, 9\}$. Дакле ако је (x, y) једно решење дате једначине имамо: $3x^2 \equiv a\ (mod\ 10),\ a \in \{0, 3, 2, 5, 8, 7\}$ и $5y^2 \equiv b(mod\ 10),\ b \in \{0, 5\}$ па из таблице

$+_{10}$	0	5
0	0	5
2	2	7
3	3	8
5	5	0
7	7	2
8	8	3

закључујемо да је $3x^2 + 5y^2 \equiv c(mod\ 10),\ c\ \epsilon\ \{0, 2, 3, 5, 7, 8\}$, а важи $4444 \equiv 4(mod\ 10)$. Једначина, дакле, нема решења.

Пример 23. Да ли једначина ${x_1}^4 + {x_2}^4 + {x_3}^4 + \ldots + {x_{14}}^4 = 1599$ има решења у скупу целих бројева?

Решење: Ако је x природан број онда су могући остаци при дељењу броја x са 16 из скупа $\{0, 1, 2,\ \ldots, 15\}$. Тада је $x^2 \equiv k(mod\ 16),\ k \in \{0, 1, 4, 9\}$.

Из тога следи да је $x^4 \equiv 0\ (mod\ 16)$ или $x^4 \equiv 1(\ mod\ 16)$. Због тога збир ${x_1}^4 + {x_2}^4 + {x_3}^4 + \ldots + {x_{14}}^4$ при дељењу са 16 може дати било који остатак из скупа $\{0, 1, 2,\ \ldots 13, 14\}$ али не и број 15. Како је $1599 \equiv 15\ (mod\ 16)$ то дата једначина нема решења у скупу целих бројева.

Метода минималног решења

Ова метода се често користи приликом налажења свих решења неких Диофантових једначина, односно доказивања да решења не постоје. Принцип је следећи.

Претпоставимо да дата једначина има целобројних решења и да постоји алгоритам којим се из једног целобројног решења једначине добија друго целобројно решење. Ако једначина има целобројних решења, онда постоји решење које је минимално у неком смислу. Решење које се добија из тог решења није мање, па се тако добијају одређене особине тог минималног решења- оне су понекад довољне да закључимо да такво решење (и, дакле ниједно друго) не постоји.

Друга формулација ове методе је следећа. Претпоставимо да постоји решење једначине у скупу природних бројева и да се може наћи алгоритам којим се из једног природног решења добија друго природно решење, али које је строго мање (у одређеном смислу) од

полазног. То значи да постоји бесконачно много природних бројева мањих од датог природног броја, што је, наравно, немогуће. Дакле, дата једначина нема природних решења. У овом облику ова метода је позната као **Фермаова метода бесконачног смањивања.**

Пример 24. Доказати да једначина

$$x^2 + y^2 + z^2 + 3(x + y + z) + 5 = 0$$

нема решења у скупу рационалних бројева.

Решење: Дата једначина може се написати у облику

$$(2x + 3)^2 + (2y + 3)^2 + (2z + 3)^2 = 7.$$

Претпоставимо супротно, нека једначина има решења у скупу рационалних бројева. Даље имамо да је:

$$\frac{{m_1}^2}{{n_1}^2} + \frac{{m_2}^2}{{n_2}^2} + \frac{{m_3}^2}{{n_3}^2} = 7, \qquad m_i \in \boldsymbol{Z}, n_i \in \boldsymbol{N}$$

па множењем леве и десне стране са ${n_1}^2{n_2}^2{n_3}^2$ добијамо:

$$(m_1n_2n_3)^2 + (m_2n_1n_3)^2 + (m_3n_1n_2)^2 = 7(n_1n_2n_3)^2.$$

Нека је: $m_1n_2n_3 = a,\ m_2n_1n_3 = b,\ m_3n_1n_2 = c,\ n_1n_2n_3 = m$. Коначно добијамо:

$$\mathrm{a}^{\mathbf{2}} + \mathrm{b}^{\mathbf{2}} + \mathrm{c}^2 = 7\mathrm{m}^2.$$

Тада је $m > 0$. Нека је m најмање могуће.

Ако је m паран број, $m = 2n$, тада је $\mathrm{a}^{\mathbf{2}} + \mathrm{b}^{\mathbf{2}} + \mathrm{c}^2$ дељиво са 4. Лако се проверава да бројеви a, b, c морају бити парни, тј. $a = 2a_1,\ b = 2b_1,\ c = 2c_1$ и ${a_1}^2 + {b_1}^2 + {c_1}^2 = 7n^2$, што је контрадикција са претпоставком о минималности m.

Ако је m непаран број, тада је $m^2 \equiv 1\ (mod\ 8)$, па је $\mathrm{a}^{\mathbf{2}} + \mathrm{b}^{\mathbf{2}} + \mathrm{c}^2 \equiv 7\ (\mathrm{mod}\ 8)$, што је немогуће.

Глава 2

Питагорине тројке и велика Фермаова теорема

У овој глави биће речи о Питагориним тројкама које ће бити праћене теоремама, њиховим доказима као и примерима.

Питагорине тројке

Троугао чији су мерни бројеви страница x, y и z природни бројеви који задовољавају релацију $x^2 + y^2 = z^2$ назива се **Питагорин троугао** (на основу Питагорине теореме такав троугао је правоугли). Природни бројеви x, y, z који су решења једначине $x^2 + y^2 = z^2$ представљају **Питагорине тројке**.

Ако нека два од бројева x, y, z који задовољавају дату једначину имају заједнички делилац d (већи од 1), онда је и трећи од њих дељив са d. Зато ћемо даље претпостављати да су бројеви x, y и z узајамно прости у паровима (у противном можемо скратити једначину њиховим заједничким делиоцем d). Такво решење (x, y, z) дате једначине називамо **примитивним решењем**. Јасно је да налажењем свих примитивних решења (x, y, z) налазимо и сва остала, јер су она облика $(\alpha x, \alpha y, \alpha z)$, $\alpha \in \boldsymbol{N}$.

Теорема 2. Ако је производ два узајамно проста природна броја квадрат целог броја, тј. ако је $ab = c^2$, $(a, b) = 1$, тада су и a и b квадрати целих бројева: $a = {a_1}^2$, $b = {b_1}^2$.

Доказ. Да би број био квадрат целог броја, неопходно је и довољно да су му сви експоненти у канонској факторизацији парни. Како су a и b узајамно прости, то они немају заједничких делилаца, па је сваки прост делилац броја c^2 или делилац броја a или делилац броја b, али не и делилац оба ова броја. Зато сви прости фактори броја a и b у канонској факторизацији морају имати парне експоненте, тј. a и b су квадрати целих бројева.

Теорема 3. Да би уређена тројка (x, y, z) представљала примитивно решење једначине $x^2 + y^2 = z^2$ у скупу природних бројева, неопходно је и довољно да се x, y, z изражавају у облику

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

($m, n \in \boldsymbol{N}, (m, n) = 1,\ m > n$ и m, n различите парности)

или

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

($m, n \in \boldsymbol{N}, (m, n) = 1, m > n$ и m, n различите парности).

Доказ: Нека је (x, y, z) примитивно решење једначине $x^2 + y^2 = z^2$. Показаћемо најпре да од бројева x и y један мора бити паран, а други непаран и да z мора бити непаран број. Ако су x и y оба парни, тада је и z паран број, па се једначина може скратити, тј. посматрана тројка није примитивно решење. Ако су x и y оба непарни тада је $z^2 = x^2 + y^2 \equiv 1 + 1 = 2 \pmod 4$, што је немогуће.

Нека је $x = 2a$ паран, а y непаран број. Тада је z непаран број. Дата једначина се може написати у облику

$$x^2 = z^2 - y^2 = (z - y)(z + y).$$

Оба чиниоца на десној страни су парни бројеви, па су бројеви

$$u = \frac{z + y}{2} \qquad \text{и} \qquad v = \frac{z - y}{2}$$

цели. Тада је $x^2 = 4a^2 = 4uv$, тј. $a^2 = uv$.

Из $z = u + v,\ y = u - v$ закључујемо да је $(u, v) = 1$. На основу **теореме 2** следи да они морају бити квадрати целих бројева: $u = m^2$ и $v = n^2$, при чему m и n немају заједничких делилаца и различите су парности. Дакле, добијамо да је $x = 2a = 2mn,\ y = u - v = m^2 - n^2,\ z = u + v = m^2 + n^2$, при чему су $m, n \in \boldsymbol{N}$, $(m, n) = 1$, $m > n$ и бројеви m и n су различите парности. Лако се проверава да је:

$$(m^2 - n^2)^2 + (2mn)^2 = m^4 + 2m^2n^2 + n^4 = (m^2 + n^2)^2,$$

тј. да тројка (x, y, z) задовољава једначину $x^2 + y^2 = z^2$.

Слично, ако је y паран број добијамо да је тројка (x, y, z) другог од описаних облика.

Пример 25. Ако је полупречник круга непаран прост број, тада се око тог круга могу описати тачно два неподударна примитивна Питагорина троугла. Доказати.

Решење: Ако је $a = m^2 - n^2,\ b = 2mn,\ c = m^2 + n^2$ примитивна Питагорина тројка, полупречник уписаног круга одговарајућег троугла је

$$r = \frac{1}{2}(a + b - c) = n(m - n).$$

Ако је r непаран прост број p, имамо следеће две могућности:

1) $n = 1,\ m = p + 1,\ a = p(p + 2),\ b = 2(p + 1),\ c = p^2 + 2p + 2$
2) $n = p,\ m = p + 1,\ a = 2p + 1,\ b = 2p(p + 1),\ c = 2p^2 + 2p + 1.$

Пример 26. Нађимо све Питагорине тројке за $0 < z < 20,\ x < y$.

Решење: Нађимо најпре све примитивне Питагорине тројке које задовољавају $0 < z < 20,\ x < y$. Све примитивне Питагорине тројке су облика

$$(m^2 - n^2,\ 2mn,\ m^2 + n^2) \text{ или } (2mn,\ m^2 - n^2,\ m^2 + n^2)$$

где је $m > n$ и $m,\ n$ узајамно прости природни бројеви различите парности. Како је по услову задатка $0 < z < 20$, онда посматрамо следеће случајеве:

1) За $n = 1,\ m = 2$ добијамо $m^2 + n^2 = 5,\ m^2 - n^2 = 3, 2mn = 4,$ односно добијамо тројку $(3, 4, 5)$.
2) За $n = 2,\ m = 3$ добијамо $m^2 + n^2 = 13,\ m^2 - n^2 =$5, $2mn = 12$, односно добијамо тројку $(5, 12, 13)$.
3) За $n = 3,\ m = 4$ добијамо $m^2 + n^2 = 25 > 20$.
4) За $n = 1,\ m = 4$ добијамо $m^2 + n^2 = 17,\ m^2 - n^2 =$15, $2mn = 8$, односно добијамо тројку $(8, 15, 17)$.

Тражене Питагорине тројке су: $(3, 4, 5);\ (6, 8, 10);\ (9, 12, 15);\ (5, 12, 13);\ (8, 15, 17)$.

Пример 27. Одредити примитивне Питагорине троуглове чији мерни број обима је једнак мерном броју површине.

Решење: Јасно је да је мерни број обима сваког Питагориног троугла једнак

$$2mn + m^2 - n^2 + m^2 + n^2 = 2mn + 2m^2 = 2m(m + n).$$

Мерни број површине је $mn(m^2-n^2)$. Дакле, $2m(m+n)=mn(m-n)(m+n)$, па је $(m-n)n=2$. Следи да је $n=1,\ m-n=2$ или $n=2$, а $m-n=1$. Према томе постоје два решења: $(m,\ n)=(3,1)$ или $(m,\ n)=(3,2)$.

Пошто се у задатку траже примитивне Питагорине тројке онда прво решење $(m,\ n)=(3,1)$ одбацујемо, јер су m и n оба непарна броја.

Странице троугла су тада: $(12,5,13),\ O=P=30$.

Велика Фермаова теорема

Познати француски математичар **Пјер Ферма (1601-1665)** био је један од оснивача савремене теорије бројева. Поставио је низ проблема чије је решавање довело до значајних достигнућа. Највише напора је уложено да се докаже (или оповргне) његово тврђење које је названо **„великом" Фермаовом теоремом**. Пјер Ферма га је исказао на маргинама једне Диофантове књиге и гласи:

Немогуће је куб разложити на два куба, ни биквадрат на два биквадрата, и уопште никакав степен већи од квадрата, на два степена са истим таквим изложиоцем.

Математичари су се више од три века бавили великом Фермаовом теоремом. Та теорема је коначно доказана 1995. године. Енглески математичар Ендру Вајлс (Andrew Wiles) је доказао велику Фермаову теорему.

Теорема 4. Ако је n ма који природан број већи од 2, онда не постоје природни бројеви x, y и z, такви да је

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

Сама теорема доказана је за многе посебне вредности изложиоца n. Доказ за специјалан случај $n=4$ (који потиче од самог Фермаа) показаћемо на наредном задатку.

Пример 28. Доказати да једначина $x^4+y^4=z^2$ нема решења у скупу природних бројева. Специјално, једначина $x^4+y^4=z^4$ нема природних решења.

Решење: Претпоставимо да решење у $\boldsymbol{N}$ постоји и да је $(x,\ y,\ z)$ такво решење са минималним z. Тада су $(x,\ y,\ z)$ узајамно прости у паровима.

Један од бројева x, y је паран. Пошто је (x^2, y^2, z) примитивна Питагорина тројка, постоје узајамно прости природни бројеви m, n такви да је

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

Тројка (x, n, m) је такође примитивна Питагорина, па постоје узајамно прости $u, v \in \boldsymbol{N}$ такви да је

$$m = u^2 + v^2, \quad x = u^2 - v^2, \quad n = 2uv \quad \text{(јер је } x \text{ непаран).}$$

Једначина $y^2 = 2mn$ се своди на $(\frac{y}{2})^2 = uv(u^2 + v^2)$. Међутим, због $(u, v) = 1$ су бројеви uv и $u^2 + v^2$ узајамно прости, а њихов производ је квадрат, па зато постоје $c, d \in \boldsymbol{N}$ за које је

$$uv = d^2 \quad \text{и} \quad u^2 + v^2 = c^2. \tag{1}$$

Најзад, због $(u, v) = 1$ и $uv = d^2$ постоје $a, b \in \boldsymbol{N}$ такви да важи $u = a^2$ и $v = b^2$, па друга једначина у (1) постаје

$$a^4 + b^4 = c^2.$$

Дакле, (a, b, c) је решење полазне једначине и притом је очигледно $c < z$, што је у контрадикцији са избором решења (x, y, z).

Глава 3

Пелова једначина

Резултати теорије Диофантових апроксимација имају примену и у решавању неких Диофантових једначина. Илуструјмо ово на примеру Пелове једначине

$$x^2 - dy^2 = 1, \qquad d \text{ није потпун квадрат}$$

чија решења тражимо у скупу природних бројева. Наведимо најпре нека једноставна својства ове једначине.

Услов да d није потпун квадрат је неопходан јер у супротном једначина, сем тривијалног $(x_0, y_0) = (1, 0)$ нема друга решења . Претпоставимо да је тај услов испуњен и препишимо једначину у облику

$$\left(x - y\sqrt{d} \right)(x + y\sqrt{d}\,) = 1.$$

Претпоставимо, даље, да знамо једно решење ($x_1,\ y_1$) једначине, тј. да је

$$(x_1 - \ y_1\sqrt{d})\ (x_1 + \ y_1\sqrt{d}) = 1.$$

Степеновањем са n добијамо

$$\left(x_n \ - y_n\sqrt{d}\,\right)(x_n + y_n\sqrt{d}\,) = 1,$$

за неке природне бројеве x_n и y_n. Заправо, применом биномне формуле која гласи:

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

ми смо добили да x_n представља збир свих чланова у случају када је k паран број, док $y_n\sqrt{d}$ када је k непаран број.

Дакле, дата једначина под наведеним претпоставкама (да d није потпун квадрат и да бар једно решење постоји) има бесконачно много решења (x_n, y_n) и основни проблем је налажење једног од њих. Најмање од таквих решења (прецизније, оно решење код којег је $x_n + \ y_n\sqrt{d}$ најмање) назива се **основним решењем**. Оно што није сасвим тривијално је

да се докаже да ако је (x_e, y_e) основно решење, тада су претходним поступком описана сва решења Пелове једначине.

Када је основно решење (x_e, y_e) познато, одређивање осталих решења (x_n, y_n) може се извршити било описаним поступком степеновања, било формирањем рекурентне везе два узастопна решења. Наиме, из

$$x_{n+1} + y_{n+1}\sqrt{d} = \left(x_n + y_n\sqrt{d}\right)\left(x_e + y_e\sqrt{d}\,\right)$$
$$= (x_e x_n + y_e d y_n) + (x_e y_n + y_e x_n)\sqrt{d}$$

закључујемо да мора да важи

(2) $$x_{n+1} = x_e x_n + y_e d y_n, \qquad y_{n+1} = x_e y_n + y_e x_n.$$

Дакле, низови (x_n) и (y_n) задовољавају систем диференцних једначина (2), уз почетне услове $x_0 = 1,\ y_0 = 0$. Из овог система низови (x_n) и (y_n) се одређују рекурентно.

Лема 1. Ако су за неко $k \in \boldsymbol{Z}$ парови $(x_1,\ y_1)$ и $(x_2,\ y_2)$ решења једначине $x^2 - dy^2 = k$, онда је условом

$$X + Y\sqrt{d} = \left(x_1 + y_1\sqrt{d}\right)\left(x_2 \pm y_2\sqrt{d}\right), \qquad X, Y \in \boldsymbol{Z}$$

(узима се произвољан знак у последњој загради) одређено решење једначине $X^2 - dY^2 = k^2$.

Доказ.

У доказу користимо да из:

$$X + Y\sqrt{d} = \left(x_1 + y_1\sqrt{d}\right)\left(x_2 \pm y_2\sqrt{d}\right), \qquad X, Y \in \boldsymbol{Z}$$

следи

$$X - Y\sqrt{d} = \left(x_1 - y_1\sqrt{d}\right)\left(x_2 \mp y_2\sqrt{d}\right), \qquad X, Y \in \boldsymbol{Z}.$$

Сада је

$$X^2 - dY^2 = (X + Y\sqrt{d})\,(X - Y\sqrt{d})$$
$$= \left(x_1 + y_1\sqrt{d}\right)\left(x_2 \pm y_2\sqrt{d}\right)\left(x_1 - y_1\sqrt{d}\right)\left(x_2 \mp y_2\sqrt{d}\right)$$
$$= ({x_1}^2 - d\,{y_1}^2)({x_2}^2 - d\,{y_2}^2) = k^2.$$

Важан резултат теорије Диофантових апроксимација је следећа **Дирихлеова теорема.**

Теорема 5. Нека је α произвољан реалан број и $t \in \boldsymbol{N}$. Тада постоји рационалан број $\frac{p}{q}$ такав да важи

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{qt} \text{ и } 0 < q \leq t.$$

Доказ: Посматрајмо $t+1$ бројева $\alpha x - \lfloor \alpha x \rfloor$ за $x = 0, 1, \ldots, t$. Сви они припадају интервалу $[0, 1)$. Поделимо тај интервал на t интервала

$$\left[0, \frac{1}{\mathrm{t}}\right), \quad \left[\frac{1}{\mathrm{t}}, \frac{2}{\mathrm{t}}\right), \ \ldots \ , \quad \left[\frac{\mathrm{t}-1}{\mathrm{t}}, 1\right).$$

На основу Дирихлеовог принципа, бар један од тих интервала садржи два од датих бројева; нека су то бројеви $\alpha x_1 - \lfloor \alpha x_1 \rfloor$ и $\alpha x_2 - \lfloor \alpha x_2 \rfloor$ и нека је, на пример, $x_2 > x_1$. Тада је

$$\frac{1}{t} > |(\alpha x_2 - \lfloor \alpha x_2 \rfloor) - (\alpha x_1 - \lfloor \alpha x_1 \rfloor)| = |\alpha(x_2 - x_1) - (\lfloor \alpha x_2 \rfloor - \lfloor \alpha x_1 \rfloor)|.$$

Означимо $q = x_2 - x_1,\ \lfloor \alpha x_2 \rfloor - \lfloor \alpha x_1 \rfloor = p$. Тада важи $0 < q \leq t$ и

$$|\alpha q - p| < \frac{1}{t}, \quad \left|\alpha - \frac{p}{q}\right| < \frac{1}{tq}.$$

Теорема 6. За произвољан природан број d који није потпун квадрат, једначина $x^2 - dy^2 = 1$ има решења.

Доказ: Нека је фиксиран природан број $t_1 > 1$. На основу Дирихлеове теореме постоје природни бројеви p_1 и q_1 за које важи

$$(3) \qquad \left|q_1\sqrt{d} - p_1\right| < \frac{1}{t_1}, \qquad q_1 \leq t_1.$$

Тада је

$$p_1 < q_1\sqrt{d} + \frac{1}{t_1} < q_1\sqrt{d} + 1,$$

па је

(4) $$q_1\sqrt{d} + p_1 < 2q_1\sqrt{d} + 1.$$

Множећи леве и десне стране неједнакости (3) и (4), с обзиром да је $q_1 \leq t_1$, добијамо да је

(5) $$|{p_1}^2 - {q_1}^2 d| < 2\sqrt{d} + 1.$$

Изаберимо сада природан број t_2 тако да важи

$$t_2 > t_1 \qquad \text{и} \qquad \frac{1}{t_2} < |q_1\sqrt{d} - p_1|.$$

На претходно описани начин нађимо нови пар природних бројева (p_2, q_2) за које важи $|{p_2}^2 - {q_2}^2 d| < 2\sqrt{d} + 1$. Затим наставимо овај поступак налазећи низ парова (p_n, q_n) који задовољавају неједначину типа (5).

Посматрајмо вредности ${p_n}^2 - {q_n}^2 d$ за све $n \in \boldsymbol{N}$. Све оне се налазе у интервалу $(-2\sqrt{d} - 1, 2\sqrt{d} + 1)$, па како тај интервал садржи коначно много целих бројева, то постоји цео број $k \neq 0$ у њему такав да је

$${p_n}^2 - {q_n}^2 d = k$$

за бесконачно много вредности n. Међу тако изабраним паровима (p_n, q_n) сигурно ће постојати два, означимо их са (x_1, y_1) и (x_2, y_2), за које важи $x_1 \equiv x_2 \ (mod\ |k|)$ и $y_1 \equiv y_2 (mod\ |k|)$. Означимо са x_0 и y_0 целе бројеве за које важи

$$x_0 + y_0\sqrt{d} = \left(x_1 + y_1\sqrt{d}\right)\left(x_2 - y_2\sqrt{d}\right).$$

На основу **леме 1** важи

(6) $${x_0}^2 - {y_0}^2 d = k^2.$$

При томе је

$$x_0 = x_1x_2 - y_1\,y_2 d \equiv {x_1}^2 - {y_1}^2 d \equiv 0\ (mod\ |k|),$$

$$y_0 = -x_1y_2 + x_2\,y_1 \equiv -x_1y_1 + x_1y_1 \equiv 0\ (mod\ |k|).$$

Због тога је $x_0 = x|k|$, $y_0 = y|k|$ за неке целе бројеве x и y, за које, заменом у (6) добијамо да важи $x^2 - dy^2 = 1$.

Докажимо тврђење према којем су напред описаним рекурентним поступком одређена сва решења Пелове једначине.

Теорема 7. Нека је (x_e, y_e) основно решење једначине $x^2 - dy^2 = 1$ (d није потпун квадрат), тј. нека је то решење за које је израз $x + y\sqrt{d}$ најмањи. Тада је свако решење (x, y) те једначине одређено условом

$$(7) \qquad x + y\sqrt{d} = (x_e + y_e\sqrt{d})^n, \quad x, y \in N, \text{ за неко } n \in \boldsymbol{N}.$$

Доказ: Да је пар (x, y) одређен условом (7) решење дате једначине, доказали смо раније. Претпоставимо, супротно тврђењу, да постоји решење (x, y) те једначине за које не важи услов (7). Тада за неко $n \in \boldsymbol{N}$ важи

$$(x_e + y_e\sqrt{d})^n < x + y\sqrt{d} < (x_e + y_e\sqrt{d})^{n+1}.$$

Узимајући у обзир да је $(x_e + y_e\sqrt{d})^{-1} = x_e - y_e\sqrt{d}$, делећи претходну двоструку неједнакост са $(x_e + y_e\sqrt{d})^n$, добијамо

$$(8) \qquad 1 < X + Y\sqrt{d} < x_e + y_e\sqrt{d},$$

где су X и Y цели бројеви одређени једнакошћу

$$X + Y\sqrt{d} = \frac{x + y\sqrt{d}}{(x_e + y_e\sqrt{d})^n} = (x + y\sqrt{d})(x_e - y_e\sqrt{d})^n.$$

На основу **леме 1**, међутим, пар (X, Y) задовољава једначину $X^2 - dY^2 = 1$. При том су бројеви X и Y позитивни, јер из претходне једнакости следи да је $0 < X - Y\sqrt{d} < 1$ а из (8) је $X + Y\sqrt{d} > 1$. На тај начин је (X, Y) решење дате Пелове једначине у скупу природних бројева за које је израз $X + Y\sqrt{d}$ мањи од $x_e + y_e\sqrt{d}$, што противречи минималности избора решења (x_e, y_e). Добијена контрадикција доказује теорему.

Пример 29. Посматрајмо једначину $x^2 - 14y^2 = 1$.

Решење: Примећујемо да је $d = 14$. Пробањем се налази њено основно решење $x_e = 15,\ y_e = 4$ (заиста $15^2 - 14 \cdot 4^2 = 1$). Квадрирањем добијамо:

$$(15 + 4\sqrt{14})^2 = 449 + 120\sqrt{14}, \text{ па је } x_2 = 449,\ y_2 = 120.$$

Даље се може наставити степеновањем, међутим једноставније је искористити систем (2).

Тако је:

$$x_2 = 15^2 + 14 \cdot 4^2 = 449, \qquad x_3 = 15 \cdot 449 + 4 \cdot 14 \cdot 120 = 13455, \qquad \ldots$$

$$y_2 = 2 \cdot 15 \cdot 4 = 120, \qquad y_3 = 15 \cdot 120 + 4 \cdot 449 = 3596, \qquad \ldots$$

Даљим рачуном се може добити

n	x_n	y_n
1	15	4
2	449	120
3	13455	3596
4	403201	107760
5	12082575	3229204
6	362074049	96768360

итд. Видимо да решења врло брзо расту.

Глава 4

Теорема Хасе- Минковски

Општа теорија Диофантових једначина садржи велики број отворених питања међу којима је и питање постојања алгоритма којим се за сваку полиномску Диофантову једначину може одредити да ли она има или нема целобројних или рационалних решења. То је један од чувених Хилбертових проблема, формулисаних на II светском конгресу математичара у Паризу 1900. године. Одговор на то питање је нажалост негативан. С друге стране, теорија квадратних Диофантових једначина је готово у потпуности испитана.

Теорема 8. Квадратна Диофантова једначина има решења у скупу рационалних бројева ако и само ако има решења по сваком простом модулу и у скупу реалних бројева.

Овде ћемо показати један метод налажења општег решења (x, y, z) једначине

(9) $$p(x, y, z) = Ax^2 + By^2 + Cz^2 + Dyz + Ezx + Fxy = 0,$$

где су A, B, C, D, E, F цели бројеви, ако нам је познато једно нетривијално решење (x_0, y_0, z_0) у ком је, рецимо, $z_0 \neq 0$.

Метод се заснива на следећем. Ако је (x, y, z) рационално решење једначине (9), онда је и (kx, ky, kz) рационално решење за свако $k \in \boldsymbol{Q}$. Ако је $z \neq 0$, за погодно k је $kz = 1$, па можемо без смањења општости претпоставити да је $z = 1$. Тада једначина (9) постаје

(10) $$P(x, y) = p(x, y, 1) = Ax^2 + By^2 + Fxy + Ex + Dy + C = 0.$$

Скуп свих решења једначине $P(x, y) = 0$ је нека крива која садржи тачку са рационалним координатама $M(x_1, y_1) = (x_0/z_0,\ y_0/z_0)$, $P(x_1, y_1) = p(x_1, y_1, 1) = p(x_0, y_0, z_0)/{z_0}^2 = 0$.

Свака права l кроз тачку M, ако није цела садржана у кривој, сече криву у још једној тачки N (ако је l тангента, сматрамо да је $N = M$). Ако се права l креће по скупу свих правих које пролазе кроз M и имају рационалан нагиб, скуп добијених пресечних тачака N ће бити управо скуп рационалних решења једначине (10).

Пример 30. Решити једначину $2x^2 + 1 = y^2$ у скупу рационалних бројева.

Решење: Пођимо од решења дате једначине $(x_1, y_1) = (0, 1)$. Сва друга решења су дата са $(x, y) = (pt, 1 + qt)$, где су p, q цели и t рационалан. Ако фиксирамо p и q, једначина $2x^2 + 1 = y^2$ даје једначину по t:

$2p^2t^2 = 2qt + q^2t^2$, одакле је $t = 0$ или $t = \frac{2q}{2p^2 - q^2}$. Сада добијамо

$$x = \frac{2pq}{2p^2 - q^2}, \qquad y = \frac{2p^2 + q^2}{2p^2 - q^2}.$$

Пример 31. Решити једначину $2a^2 + 7b^2 = c^2$ у скупу рационалних бројева.

Решење: Можемо приметити да је једно нетривијално решење једначине $(1, 1, 3)$.

Ако је $c = 0$, једино решење је $(0, 0, 0)$. Надаље сматрамо да је $c \neq 0$. Ако ставимо $x = \frac{a}{c}, y = \frac{b}{c}$ сводимо једначину на $2x^2 + 7y^2 = 1$ у скупу рационалних бројева, чије решење образује неку криву (елипсу). Тројка $(a, b, c) = (1, 1, 3)$ нам даје решење $(x_1, y_1) = \left(\frac{1}{3}, \frac{1}{3}\right)$. Нека је (x, y) неко решење једначине и нека су $t \in \boldsymbol{Q}$ и $p, q \in \boldsymbol{Z}$ не оба једнака нули, такви да је

$$x = \frac{1}{3} + pt, \qquad y = \frac{1}{3} + qt.$$

Заменом ових вредности у полазну једначину добијамо

$$2(\frac{1}{3} + pt)^2 + 7(\frac{1}{3} + qt)^2 = 1,$$

што се своди на

$$4\frac{pt}{3} + 14\frac{qt}{3} + (2p^2 + 7q^2)t^2 = 0.$$

Скраћивањем са t добијамо $-2(2p + 7q) = 3(2p^2 + 7q^2)t$, одакле је

$$t = -\frac{2(2p + 7q)}{3(2p^2 + 7q^2)},$$

па је

$$(11) \qquad x = \frac{1}{3} + pt = \frac{-2p^2 - 14pq + 7q^2}{3(2p^2 + 7q^2)}, \qquad y = \frac{1}{3} + qt = \frac{2p^2 - 4pq - 7q^2}{3(2p^2 + 7q^2)}.$$

С друге стране, за свако рационално решење, тј. тачку N са рационалним координатама, права $l = MN$ има рационални нагиб, што значи да су сва рационална решења наше једначине обухваћена формулом (11).

Литература

1. В. Мићић, З. Каделбург, Д. Ђукић, Увод у теорију бројева, Друштво математичара Србије, Београд, 2013.

2. М. Станић, Н. Икодиновић, Теорија бројева збирка задатака, Београд, 2004.

3. В. Андрић, Мала збирка Диофантових једначина, Ваљево, 2006.