Опште квадратне Диофантове једначине

Општа теорија Диофантових једначина садржи велики број отворених питања. Питање постојања алгоритма којим се за сваку полиномску Диофантову једначину може одредити да ли она има или нема целобројних или рационалних решења је један од чувених Хилбертових[1] проблема, и одговор на њега је на жалост негативан. С друге стране, теорија квадратних Диофантових једначина је готово у потпуности испитана. Наводимо следеће тврђење чији је доказ изван оквира ове књиге.

Теорема (Хасе[2]-Минковски[3]). *Квадратна Диофантова једначина има решења у скупу рационалних бројева ако и само има решења по сваком простом модулу и у скупу реалних бројева.*

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

$$p(x, y, z) = Ax^2 + By^2 + Cz^2 + Dyz + Ezx + Fxy = 0, \tag{6}$$

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

Метод се заснива на следећем. Ако је (x, y, z) рационално решење једначине (6), онда је и (kx, ky, kz) решење за свако $k \in \mathbf{Q}$. Ако је $z \neq 0$, за погодно k је $kz = 1$, па можемо без смањења општости претпоставити да је $z = 1$. Тада једначина (6) постаје

$$P(x, y) = p(x, y, 1) = Ax^2 + By^2 + Fxy + Ex + Dy + C = 0. \tag{7}$$

Скуп свих решења једначине $P(x, y) = 0$ је нека крива која садржи тачку са рационалним координатама $M(x_1, y_1) = (x_0/z_0, y_0/z_0, z_0)$ -- заиста, $P(x_1, y_1) = p(x_1, y_1, 1) = p(x_0, y_0, z_0)/z_0^2 = 0$. 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 (7).

---

[1] D. Hilbert (1862–1943), немачки математичар

[2] H. Hasse (1898–1979), немачки математичар

[3] H. Minkowski (1864–1909), немачки математичар

Задатак 3. 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 $t=\dfrac{2q}{2p^2-q^2}$. Сада добијамо

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

Пример 4. Једначина $x^2+4xy+4y^2=1$ у скупу рационалних бројева се не може решити горњом методом (проверите!). Разлог је растављивост полинома $P(x,y)=x^2+4xy+4y^2-1$: $P(x,y)=(x+2y+1)(x+2y-1)$, што ионако чини задату једначину готово тривијалном. $\triangle$

Следећи задатак се не би могао једноставно решити на исти начин као Питагорина једначина.

Задатак 4. Решити једначину $2a^2+7b^2=c^2$ у скупу: (а) рационалних; (б) целих бројева.

Решење. Приметимо 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 $x=a/c$ и $y=b/c$, сводимо једначину на $2x^2+7y^2=1$ у скупу рационалних бројева, чија решења образују неку криву (елипсу). Тројка $(a,b,c)=(1,1,3)$ нам даје решење $(x_1,y_1)=(1/3,1/3)$. Нека је (x,y) неко решење једначине и нека су $t\in\mathbf{Q}$ и $p,q\in\mathbf{Z}$ не оба једнака нули, такви да је $x=1/3+pt$, $y=1/3+qt$. Заменом ових вредности у полазну једначину добијамо $2(1/3+pt)^2+7(1/3+qt)^2=1$, што се своди на $4pt/3+14qt/3+(2p^2+7q^2)t^2=0$. Скраћивањем са t добијамо $-2(2p+7q)=3(2p^2+7q^2)t$, одакле је $t=-\dfrac{2(2p+7q)}{3(2p^2+7q^2)}$,

$$x=\frac{1}{3}+pt=\frac{-2p^2-14pq+7q^2}{3(2p^2+7q^2)},\qquad y=\frac{1}{3}+qt=\frac{2p^2-4pq-7q^2}{3(2p^2+7q^2)}. \tag{8}$$

С друге стране, за свако рационално решење, тј. тачку N са рационалним координатама, права $l=MN$ има рационалан нагиб, што значи да су сва рационална решења наше једначине обухваћена формулом (8).

Што се тиче целобројних решења, с обзиром да је $x=a/c$ и $y=b/c$, можемо узети $a=k(-2p^2-14pq+7q^2)$, $b=k(2p^2-4pq-7q^2)$, $c=3k(2p^2+7q^2)$, при чему су p и q цели, а k рационалан број за који су горње вредности a,b,c целе. Напоменимо да се не можемо ограничити само на целобројне вредности k, јер онда нпр. решење $(a,b,c)=(3,1,5)$ не би могло да буде добијено. Па ипак, може се показати да је у овом случају довољно захтевати да $42k$ буде цео број (покажите!). $\triangle$

Задатак 5. Наћи све тројке целих бројева (a, b, c) за које је

$$a^2 + b^2 + c^2 = 3(a + 2b)c.$$

Решење. Лако проналазимо нетривијално решење $(a_0, b_0, c_0) = (4, 5, 1)$.

За $c = 0$ нема решења осим тривијалног $(0, 0, 0)$. Нека је $c \neq 0$ и $x = a/c$, $y = b/c$. Једначина постаје $x^2 + y^2 + 1 = 3x + 6y$, са једним решењем $(x_1, y_1) = (4, 5)$. Ставимо $x = 4 + pt$, $y = 5 + qt$, где су $p, q \in \mathbf{Z}$ и $t \in \mathbf{Q}$. Добијамо $5pt+4qt+p^2t^2+q^2t^2 = 0$, одакле је $t = \dfrac{-5p - 4q}{p^2 + q^2}$. Сада је $x = \dfrac{-p^2 + 4q^2 - 4pq}{p^2 + q^2}$ и $y = \dfrac{5p^2 - 5pq + q^2}{p^2 + q^2}$. Одавде лако добијамо опште решење $a = k(-p^2-4pq+4q^2)$, $b = k(5p^2 - 5pq + q^2)$, $c = k(p^2 + q^2)$, где је $k \in \mathbf{Q}$. △

Велика Фермаова теорема

Познати француски математичар Пјер Ферма био је један од оснивача савремене теорије бројева. Поставио је низ проблема чије је решавање довело до значајних достигнућа. Но, свакако је највише напора уложено и највише покушаја учињено да се докаже (или оповргне) његово тврђење које је названо **„великом“** (некад и **„последњом“**) **Фермаовом теоремом**. Ферма га је исказао у краткој ноти на маргинама једне Диофантове књиге и гласи:

Немогуће је да се куб напише као збир два куба, нити да се четврти степен напише као збир четвртих степена и, уопште, да се било који број који је степен већи од другог напише као збир два иста таква степена.

У савременим ознакама:

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

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

Ферма је дописао: „Нашао сам заиста изванредан доказ овог тврђења, али је ова маргина сувише уска да би се доказ могао сместити.“ Овом тврђењу, записаном средином XVII века, многи велики научници посвећивали су много времена и труда. Напори су дали много корисних резултата, посебно у теорији алгебарских бројева. Сама теорема доказана је за многе посебне вредности изложиоца n. Доказ за специјалан случај $n = 4$ (који потиче од самог Фермаа) дајемо у задатку 6 наредног одељка. Занимљиво је да је доказ за случај $n = 3$ много тежи и њега је извео Ојлер. Гаусов доказ за овај случај дајемо у теореми 10 седме главе.

Фермаова велика теорема је коначно ипак доказана 1995. године. (У ствари, решење је најављено две године раније, али саопштења такве врсте увек се примају са резервом, јер је било много случајева да су објављивани „докази“ за које се

касније испоставило да нису коректни.) Заслуга за то приписује се неколицини математичара, при чему је завршни „ударац“ извео енглески математичар Ендру Вајлс (Andrew Wiles).

Занимљиво је поменути да је Ојлер, покушавајући да докаже Фермаову теорему, поставио хипотезу да ни једначина

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

нема решења у скупу природних бројева. За ово тврђење се такође дуго није знало да ли је тачно или не, док није Ноам Елкис (Noam Elkies) 1988. године нашао контрапример

$$2\,682\,440^4 + 15\,365\,639^4 + 18\,796\,760^4 = 20\,615\,673^4.$$

Касније је нађено и мање решење

$$95\,800^4 + 217\,519^4 + 414\,560^4 = 422481^4.$$

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 (нпр. минималан је збир $|x| + |y|$). 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**.

Наведену методу илустроваћемо на следећа три задатка, а још примера се може наћи у задацима ове главе, као и међу задацима са међународних олимпијада (глава 8).

Задатак 6. 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 $\mathbf{N}$ постоји и да је (x, y, z) такво решење са минималним z. Можемо претпоставити да су (x, y, z) узајамно прости у паровима. Један од бројева x, y је паран -- нека је без смањења општости $2 \mid y$

и $2 \nmid x$. 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 $u, v \in \mathbf{N}$ такви да је

$$m = u^2 + v^2, \qquad x = u^2 - v^2, \qquad n = 2uv.$$

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

$$uv = d^2 \quad \text{и} \quad u^2 + v^2 = c^2. \tag{9}$$

Најзад, због $(u, v) = 1$ и $uv = d^2$ постоје $a, b \in \mathbf{N}$ такви да важи $u = a^2$ и $v = b^2$, па друга једначина у (9) постаје

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

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

Задатак 7. Наћи све парове природних бројева a, b такве да $a \mid b^2 + 1$ и $b \mid a^2 + 1$.

Решење. Јасно је да је $(a, b) = 1$, па је услов задатка еквивалентан са $ab \mid a^2 + b^2 + 1$. Фиксирајмо $n = \dfrac{a^2 + b^2 + 1}{ab} > 2$ и посматрајмо једначину

$$a^2 + b^2 + 1 = nab. \tag{10}$$

Нека је (a, b) решење у $\mathbf{N}$ једначине (10) у коме је $a \geqslant b$ и a најмање могуће. Ако (10) напишемо као квадратну једначину по a,

$$f(a) = a^2 - nb \cdot a + b^2 + 1 = 0,$$

примећујемо да ако је (a, b) њено решење, онда је и $(nb - a, b)$ решење. Због начина избора решења (a, b) и чињенице да је $nb - a > 0$, мора бити $nb - a \geqslant a \geqslant b$. Квадратна функција f је негативна на интервалу $(a, nb-a)$, а ненегативна изван њега. Између осталог, важи $f(b) \geqslant 0$, тј. $-(n-2)b^2 + 1 \geqslant 0$. Следи да је $n = 3$ и $a = b = 1$.

Сва друга решења (a, b) једначине (10) са $a \geqslant b$ се после коначног броја трансформација $(a, b) \mapsto (b, 3b - a)$ своде на најмање решење $(1, 1)$. Идући „уназад“, одавде лако добијамо да је решење (a, b) облика (F_{2n-1}, F_{2n+1}), $n \geqslant 0$, где су F_k чланови Фибоначијевог низа[4] ($F_{-1} = 1$, $F_0 = 0$, $F_{k+1} = F_k + F_{k-1}$). $\triangle$

[4] L. Pisano (Fibonacci), (око 1170--после 1240), италијански математичар. О Фибоначијевим бројевима видети нпр. у свесци 8 ових Материјала [25].

Задатак 8. Ако су m, n природни бројеви исте парности такви да је $m > n$ и $m^2 - n^2 + 1 \mid m^2$, доказати да је $m^2 - n^2 + 1$ потпун квадрат.

Решење. С обзиром на исту парност бројева m и n, уведимо смену $m = a+b$, $n = a-b$. Услов задатка постаје $a^2+2ab+b^2 = k(4ab+1)$ за неко $k \in \mathbf{N}$, тј.

$$f(a) = a^2 - (4k-2)ab + b^2 - k = 0.$$

Нека је (a_0, b_0) решење (a, b) ове једначине у $\mathbf{N}$ са $a \geqslant b$ и најмањим могућим a. Како је $((4k-2)b_0 - a_0, b_0)$ такође решење, мора бити $(4k-2)b_0 - a_0 \geqslant a_0 \geqslant b_0$ или $(4k-2)b_0 - a_0 < 0 \leqslant a_0$ или $(4k-2)b_0 - a_0 = 0$. У првом случају добијамо $f(b_0) \geqslant 0$ што није могуће. У другом случају добијамо $f(-1) \leqslant 0$, одакле је $1 + (4k-2)b_0 + b_0^2 \leqslant k$ што је немогуће. Остаје трећи случај у коме је $f(0) = 0$, одакле је $b_0^2 = k$. Полазна једначина сада постаје $(a+b)^2 = b_0^2(4ab+1)$, па следи да је и $4ab+1$ потпун квадрат. $\triangle$