Пелова једначина

Душан Ђукић

0° Увод

Често смо се сретали са линеарним диофантским једначинама, и овакве једначине знамо да решавамо помоћу једноставног алгоритма. Диофантске једначине се појављују у много различитих облика, међу којима се могу издвојити полиномске као најизучаваније. То су једначине облика $P(x_1, x_2, \dots, x_k) = 0$, где је P неконстантан полином, а x_i непознате - најчешће цели или рационални бројеви. Тако су линеарне диофантске једначине дате полиномима првог степена. Још је енглески математичар Хилберт почетком 20. века поставио чувено питање постојања алгоритма којим се може решити ма која полиномска диофант ска једначина. Одговор је дао руски математичар Матијасевич 1976, и тај одговор је негативан. Ипак, за одређене класе диофантских једначина алгоритам постоји. То је случај са *квадратним* диофантским једначинама, задатим полиномом P другог степена.

Квадратне диофантске једначине смо такође виђали. Вероватно најпознатији пример је Питагорина једначина $x^2 + y^2 = z^2$ са три непознате, чија су сва решења дата у облику $(x, y, z) = (t(x^2 - y^2), 2txy, t(x^2 + y^2))$, где су $x, y \in \mathbb{Z}$ и $t \in \mathbb{Q}$.

Испоставља се да се код квадратних једначина са само две променљиве ситуација усложњава.

Пример. Посматрајмо једначину

$$x^2 + xy - y^2 + x - y - 1 = 0$$

са целим непознатим x, y. Допуњавање до квадрата даје $(x + \frac{1}{2}y)^2 - \frac{5}{4}y^2 + x - y - 1 = 0$. Сменом $z = 2x + y$ добијамо $z^2 - 5y^2 + 2z - 6y - 4 = 0$. Опет допуњавамо до квадрата: $(z+1)^2 - 5(y + \frac{3}{5})^2 - \frac{16}{5} = 0$, што уз смену $u = z + 1 = 2x + y + 1$ и $v = 5y + 3$ постаје

$$v^2 - 5u^2 = -16.$$

Решења ове једначине су $(v, u) = (\pm 2, \pm 2), (\pm 8, \pm 4), (\pm 22, \pm 10)$, итд. Да би $y = \frac{v-3}{5}$ и $x = \frac{5u-v-2}{10}$ били цели бројеви, потребно је да буде $v \equiv 3 \pmod 5$, па тако само $v = -2, 8, -22$, итд. долазе у обзир. Тако добијамо (нека) решења полазне једначине: $(x, y) = (\pm 1, -1)$, $(-3, 1)$, $(1, 1)$, $(-3, -5)$, $(7, -5)$, итд.

У претходном примеру смо се суочили са једначином $v^2 - 5u^2 = -16$. Испоставиће се да ова једначина има бесконачно много решења у $\mathbb{Z}$, од којих смо навели само неколико. Каснија решења брзо расту.

Дефиниција. Пелова једначина је диофантска једначина облика $x^2 - dy^2 = 1$, $x, y \in \mathbb{Z}$, за дато $d \in \mathbb{N}$ које није потпун квадрат.

Једначину облика $x^2 - dy^2 = a$, где је a цео број, зовемо *једначином Пеловог типа.*

Сличним поступком као у примеру, свака квадратна диофантска једначина са две непознате се може свести на једначину Пеловог типа. Заиста, полазећи од опште квадратне диофантске једначине $ax^2 + bxy + cy^2 + dx + ey + f = 0$, допуњавањем до квадрата и сменама $X = 2ax + by + d$, $Y = (4ac - b^2)y + 2ae$ је сводимо на жељени облик

$$Y^2 - PX^2 = Q,$$

где је $P = b^2 - 4ac$ и $Q = 4a^2e^2 + P(4af - bd - d^2)$.

Добијене изразе нећемо ни покушавати да запамтимо, али треба да запамтимо поступак. Да истакнемо ово што смо управо показали:

Теорема 0. Произвољна квадратна диофантска једначина са две непознате се може свести на једначину Пеловог типа. □

Како наћи сва решења овакве једначине? Подсетимо се да је опште решење линеарне диофантске једначине линеарно у односу на параметре. То није случај са квадратним диофантским једначинама. Ипак, касније ћемо видети да се и оваквим једначинама може наћи опште решење изражено релативно једноставном формулом.

1° Бројеви облика $x + y\sqrt{d}$

Зашто је у дефиницији Пелове једначине важан услов да d није потпун квадрат? Ако јесте, рецимо $d = c^2$, онда се једначина $x^2 - dy^2 = a$ може факторисати као $(x-cy)(x+cy) = a$, а овакве једначине умемо да тривијално решавамо. Зато у наставку текста подразумевамо да d није квадрат.

Једначину $x^2 - dy^2 = a$ још увек можемо да разложимо на чиниоце:

$$(x + y\sqrt{d})(x - y\sqrt{d}) = a.$$

Да бисмо искористили овакво разлагање, морамо да радимо са скупом свих бројева облика $x + y\sqrt{d}$, где су $x, y \in \mathbb{Z}$. Овај скуп означавамо са $\mathbb{Z}[\sqrt{d}]$. Важно је да приметимо да збир, разлика и производ два елемента скупа остају у скупу:

$$\begin{aligned}(x + y\sqrt{d}) \pm (u + v\sqrt{d}) &= (x \pm u) + (y \pm v)\sqrt{d},\\ (x + y\sqrt{d})(u + v\sqrt{d}) &= (xu + dyv) + (xv + yu)\sqrt{d}.\end{aligned}$$

Такође је веома битно да су за дато $z \in \mathbb{Z}[\sqrt{d}]$ цели бројеви x, y за које је $z = x + y\sqrt{d}$ једнозначно одређени - заиста, из $x + y\sqrt{d} = x_1 + y_1\sqrt{d} = z$ и $y \neq y_1$ би следило $\sqrt{d} = \frac{x_1 - x}{y - y_1}$, што је немогуће јер је $\sqrt{d}$ ирационално.

Дефиниција. Конјугат броја $z = x + y\sqrt{d}$ се дефинише као $\overline{z} = x - y\sqrt{d}$, а *норма* броја z као $N(z) = z\overline{z} = x^2 - dy^2 \in \mathbb{Z}$.

Т.1 Норма и конјугат су мултипликативни: $N(z_1 z_2) = N(z_1)N(z_2)$ и $\overline{z_1 z_2} = \overline{z_1} \cdot \overline{z_2}$.

Доказ. Ако је $z_1 = x_1 + y_1\sqrt{d}$ и $z_2 = x_2 + y_2\sqrt{d}$, директно из дефиниције следи $\overline{z_1 z_2} = (x_1 - y_1\sqrt{d})(x_2 - y_2\sqrt{d}) = (x_1x_2 + dy_1y_2) - (x_1y_2 + x_2y_1)\sqrt{d} = \overline{(x_1x_2 + dy_1y_2) + (x_1y_2 + x_2y_1)\sqrt{d}} = \overline{z_1 z_2}$, и одатле $N(z_1z_2) = z_1z_2\overline{z_1z_2} = z_1\overline{z_1}z_2\overline{z_2} = N(z_1)N(z_2)$. □

Пример. У прстену $\mathbb{Z}[\sqrt{2}]$, елемент $z = 5 + 4\sqrt{2}$ има конјугат $\overline{z} = 5 - 4\sqrt{2}$ и норму $N(z) = 5^2 - 2 \cdot 4^2 = -7$.

Исти број можемо да посматрамо и као елемент прстена $\mathbb{Z}[\sqrt{8}]$, јер је $z = 5 + 2\sqrt{8}$. И сада је $\overline{z} = 5 - 2\sqrt{8} = 5 - 4\sqrt{2}$ и $N(z) = 5^2 - 8 \cdot 2^2 = -7$.

Нека је $z' = 4 - \sqrt{2}$. Тада је $N(z) = 4^2 - 2(-1)^2 = 14$. Како је $zz' = 12 + 11\sqrt{2}$, важи $N(zz') = 12^2 - 2 \cdot 11^2 = -98 = N(z)N(z')$.

Задатак. Доказати да не постоје природни бројеви m и n такви да је

$$(5 + 3\sqrt{2})^m = (7 + 4\sqrt{2})^n.$$

Решење. Конјуговање дате једначине даје $(5 - 3\sqrt{2})^m = (7 - 4\sqrt{2})^n$. Међутим, лева страна је мања од 1, док је десна је већа од 1, јер је $|5 - 3\sqrt{2}| < 1 < 7 - 4\sqrt{2}$, па је добијена једнакост немогућа. △

Појам норме нам омогућује да једначину $x^2 - dy^2 = a$ запишемо у еквивалентном облику

$$N(z) = a, \quad \text{где је } z = x - y\sqrt{d} \in \mathbb{Z}[\sqrt{d}].$$

Специјално, Пелова једначина је еквивалентна једначини $N(z) = 1$, $z \in \mathbb{Z}[\sqrt{d}]$. Надаље ћемо често користити ове ознаке.

Како су z и $-z$ истовремено решења једначине Пеловог типа, убудуће подразумевамо без смањења општости да је $z > 0$.

2° Решења Пелове једначине $x^2 - dy^2 = 1$

Пелова једначина има тривијално решење $(x, y) = (1, 0)$, које одговара решењу $z = 1$ једначине $N(z) = 1$. Ако знамо и најмање *нетривијално* решење, онда знамо сва решења. То показује следеће тврђење:

Т.2. Ако је ζ најмањи елемент скупа $\mathbb{Z}[\sqrt{d}]$ такав да је $\zeta > 1$ и $N(\zeta) = 1$, онда су сви елементи $z \in \mathbb{Z}[\sqrt{d}]$ за које је $N(z) = 1$ дати са $z = \pm\zeta^n$, $n \in \mathbb{Z}$.

Доказ. Претпоставимо да је $N(z) = 1$ за неко $z > 0$. Постоји тачно један цео број k за који је $\zeta^k \leq z < \zeta^{k+1}$. Тада за број $z' = z\zeta^{-k} = z\overline{\zeta}^k$ важи $1 \leq z' < \zeta$ и $N(z') = N(z)N(\zeta)^{-k} = N(z) = 1$. Из минималности ζ следи да је $z' = 1$, тј. $z = \zeta^k$. □

Последица. Ако је (ξ, η) најмање решење Пелове једначине за дато d, онда су сва природна решења $(x, y) = (x_n, y_n)$ те једначине дата са $x_n + y_n\sqrt{d} = (\xi + \eta\sqrt{d})^n$, $n \in \mathbb{N}$.

Приметимо да су x и y одређени из $z = x + y\sqrt{d}$ формулама $x = \frac{z+\overline{z}}{2}$ и $y = \frac{z-\overline{z}}{2\sqrt{d}}$. Тако су сва решења Пелове једначине дата са $(x, y) = (x_n, y_n)$, где је

$$x_n = \frac{\zeta^n + \overline{\zeta}^n}{2} \quad \text{и} \quad y_n = \frac{\zeta^n - \overline{\zeta}^n}{2\sqrt{d}}.$$

Пример. Нађимо сва решења једначине $x^2 - 3y^2 = 1$ у скупу природних бројева.

Најмање нетривијално решење ове једначине је $(\xi, \eta) = (3, 2)$. Према томе, за свако решење (x, y) постоји природан број n такав да је $x + y\sqrt{d} = (3 + 2\sqrt{2})^n$, одакле је

$$x = \frac{(3 + 2\sqrt{2})^n + (3 - 2\sqrt{2})^n}{2}, \quad y = \frac{(3 + 2\sqrt{2})^n - (3 - 2\sqrt{2})^n}{2\sqrt{2}}.$$

Тако нпр. за $n = 1, 2, 3, 4$ добијамо решења $(3, 2)$, $(17, 12)$, $(99, 70)$ и $(577, 408)$, и то су четири најмања решења разматране једначине.

Решења Пелове једначине се могу написати и као чланови линеарно рекурентног низа. Ако је (ξ, η) минимално решење једначине $x^2 - dy^2 = 1$, онда из једнакости $\zeta^2 - 2\xi\zeta + 1 = 0$ за $\zeta = \xi + \eta\sqrt{d}$ добијамо $\zeta^{n+1} = 2\xi\zeta^n - \zeta^{n-1}$, што по дефиницији x_n, y_n даје рекурентне релације

$$x_{n+1} = 2\xi x_n - x_{n-1}, \quad y_{n+1} = 2\xi y_n - y_{n-1}.$$

Сада ћемо показати да Пелова једначина увек има нетривијално решење. Треба нам једно основно тврђење о апроксимацијама ирационалних бројева рационалним.

Т *(Дирихлеова теорема).* Нека је α ирационалан и n природан број. Тада постоје $p \in \mathbb{Z}$ и $q \in \{1, 2, \ldots, n\}$ такви да је $\left|\alpha - \frac{p}{q}\right| < \frac{1}{(n+1)q}$.

Доказ. Неједнакост из тврђења је еквивалентна неједнакости $|q\alpha - p| < \frac{1}{n+1}$.

Нека, као и обично, $\{x\}$ означава разломљени део реалног броја x. Међу $n+2$ бројева $0, \{\alpha\}, \{2\alpha\}, \ldots, \{n\alpha\}, 1$ у интервалу $[0, 1]$, бар два се разликују за мање од $\frac{1}{n+1}$. Ако су то бројеви $\{k\alpha\}$ и $\{l\alpha\}$, довољно је поставити $q = |k - l|$, а ако су то $\{k\alpha\}$ и 0 или 1, довољно је поставити $q = k$; у оба случаја, p је цео број најближи броју $k\alpha$. □

Л.1. Ако је α произвољан реалан број, онда постоји бесконачно много парова природних бројева (p, q) таквих да је $\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}$.

Доказ. Одмах следи из Дирихлеове теореме. □

Т.3. Пелова једначина има бар једно решење у скупу природних бројева.

Доказ. Тврђење Л.1 примењено на $\alpha = \sqrt{d}$ говори да постоји бесконачно много парова природних бројева (p, q) за које је $\frac{1}{q^2} > \left|\sqrt{d} - \frac{p}{q}\right| = \frac{|p^2-dq^2|}{q^2(p/q+\sqrt{d})}$, што је еквивалентно са $|p^2 - dq^2| < \frac{p}{q} + \sqrt{d}$. Како је $\frac{p}{q} + \sqrt{d} < 2\sqrt{d} + 1$, следи да $|p^2 - dq^2| < 2\sqrt{d} + 1$ важи за бесконачно много парова природних бројева p, q.

Према томе, постоји цео број n, $|n| < 2\sqrt{d} + 1$, такав да једначина $u^2 - dv^2 = n$ има бесконачно много решења (u, v) у скупу $\mathbb{N}$. Међу овим решењима постоје два различита, рецимо (u_1, v_1) и (u_2, v_2), који задовољавају $u_1 \equiv u_2$ и $v_1 \equiv v_2 \pmod{n}$. Означимо $w_1 = u_1 + v_1\sqrt{d}$ и $w_2 = u_2 + v_2\sqrt{d}$, и нека је $w_1 > w_2$. Посматрајмо број $z = w_1/w_2 > 1$. Имамо

$$z = \frac{w_1\overline{w_2}}{n} = \frac{u_1u_2 - dv_1v_2}{n} + \frac{u_1v_1 - u_1v_2}{n}\sqrt{d}.$$

У горњој једнакости коефицијенти $x = \frac{u_1u_2-dv_1v_2}{n}$ и $y = \frac{u_2v_1-u_1v_2}{n}$ су цели бројеви, што следи из конгруенција $u_1u_2 - dv_1v_2 \equiv u_1^2 - dv_1^2 \equiv 0$ и $u_2v_1 - u_1v_2 \equiv u_1v_1 - u_1v_1 = 0 \pmod{n}$. Закључујемо да је z елемент скупа $\mathbb{Z}[\sqrt{d}]$. При том је $N(z) = N(w_1)/N(w_2) = 1$, па z одређује једно решење (x, y) Пелове једначине. □

3° Налажење решења Пелове једначине

Доказали смо да Пелова једначина $x^2 - dy^2 = 1$ увек има нетривијално решење. Међутим, теорема 3 не даје прихватљиву горњу границу за најмање такво решење.

Пример. Најмање решење Пелове једначине $x^2 - 61y^2 = 1$ је $(\xi, \eta) = (1766319049, 226153980)$.

Морамо ли да и оваква решења тражимо "пешачки"? Није неочекивано да формула у затвореном облику не постоји. Ипак, постоје алгоритми којима се ова решења могу наћи релативно брзо. Показаћемо два таква алгоритма.

(*I*) *Метод Чакравала*

Овај метод је изум средњовековних индијских математичара и заснива се на идентитету

$$(x_1^2 - dy_1^2)(x_2^2 - dy_2^2) = (x_1x_2 + dy_1y_2)^2 - d(x_1y_2 + x_2y_1)^2. \qquad (*)$$

За $z_1 = x_1 + y_1\sqrt{d}$ и $z_2 = x_2 + y_2\sqrt{d}$ лева страна у $(*)$ представља $N(z_1)N(z_2)$, а десна $N(z_1z_2)$, тако да је $(*)$ еквивалентно већ познатој једнакости $N(z_1)N(z_2) = N(z_1z_2)$.

Почнимо од произвољног пара (x_1, y_1) са нзд$(x_1, y_1) = 1$ и означимо $x_1^2 - dy_1^2 = k_1$. Главна идеја је да се на место пара (x_2, y_2) стави једноставно $(m, 1)$ са погодно изабраним m. Наиме, $(*)$ даје $(mx_1 + dy_1)^2 - d(x_1 + my_1)^2 = (m^2 - d)k_1$. Одаберимо m тако да

$$k_1 \mid x_1 + my_1 \quad \text{и } |m^2 - d| \text{ је најмање могуће.}$$

Тада из $(-my_1)^2 - dy_1^2 \equiv x_1^2 - dy_1^2 = k_1 \pmod{k_1}$ следи $k_1 \mid m^2 - d$, и одатле $mx_1 + dy_1 \equiv m(x_1 + my_1) \equiv 0 \pmod{k_1}$, дакле $k_1 \mid mx_1 + dy_1$. Према томе, сви сабирци у једнакости

$$\left(\frac{mx_1 + dy_1}{|k_1|}\right)^2 - d\left(\frac{x_1 + my_1}{|k_1|}\right)^2 = \frac{m^2 - d}{k_1}$$

су цели бројеви. Овако смо из тројке (x_1, y_1, k_1) добили нову тројку $(x_2, y_2, k_2) = (\frac{mx_1+dy_1}{|k_1|}, \frac{x_1+my_1}{|k_1|}, \frac{m^2-d}{k_1})$. Настављамо овај поступак све док не добијемо пар $(x_n, y_n, 1)$, тј. решење Пелове једначине. Лагранж је доказао да се овај поступак увек завршава.

Пример. Нађимо решење једначине $x^2 - 67y^2 = 1$ у природним бројевима.

Корак 1. Одаберимо $(x_1, y_1) = (8, 1)$ и $k = 8^2 = 67 \cdot 1^2 = -3$.

Корак 2. Бирамо m тако да $k = -3$ дели $x_1 + my_1 = 8 + m$ и $|m^2 - 67|$ је најмање могуће: то је $m = 7$. Добијамо $(x_2, y_2, k_2) = (\frac{7\cdot8+67\cdot1}{3}, \frac{1\cdot8+7\cdot1}{3}, \frac{7^2-67}{-3}) = (41, 5, 6)$.

Корак 3. Бирамо m тако да $6 \mid 41 + 5m$ и $|m^2 - 67|$ је најмање могуће: то је $m = 5$, па добијамо тројку $(x_3, y_3, k_3) = (\frac{5\cdot41+67\cdot5}{6}, \frac{1\cdot41+5\cdot5}{6}, \frac{5^2-67}{6}) = (90, 11, -7)$.

Корак 4. Избор $m = 9$ даје $(x_4, y_4, k_4) = (\frac{9\cdot90+67\cdot11}{7}, \frac{1\cdot90+9\cdot11}{7}, \frac{9^2-67}{-7}) = (221, 27, -2)$.

Корак 5. $m = 9$, $(x_5, y_5, k_5) = (\frac{9\cdot221+67\cdot27}{2}, \frac{1\cdot221+9\cdot27}{2}, \frac{9^2-67}{-2}) = (1899, 232, -7)$, итд.

Корак 8. $(x_8, y_8, k_8) = (48842, 5967, 1)$, и то је најмање решење: $48842^2 - 67 \cdot 5967^2 = 1$.

Напомена. Алгоритам се могао убрзати. Наиме, коначно решење се могло добити директно после корака 4 - видети теорему 6.

(II) *Верижни разломци*

Ако је (x, y) решење Пелове једначине $x^2 - dy^2 = 1$, разломак $\frac{x}{y}$ је близак $\sqrt{d}$ и у извесном смислу представља оптималну апроксимацију ирационалног броја $\sqrt{d}$ рационалним. Апроксимације ирационалног броја α рационалним су у тесној вези са развојем α у тзв. *верижни разломак.*

Сваки реалан број α се може развити у верижни разломак облика

$$[a_0, a_1, a_2, a_3, \dots] := a_0 + \cfrac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \cdots}}}$$

где је $a_0 \in \mathbb{Z}$ и $a_1, a_2, \dots \in \mathbb{N}$. Овај развој је коначан (и условно јединствен) за рационално α, односно бесконачан (и јединствен) за ирационално α. Верижни разломци $[a_0], [a_0, a_1]$, $[a_0, a_1, a_2], \dots$ су рационални бројеви који теже броју α.

Испоставља се да је развој $\sqrt{d}$ у верижни разломак периодичан почев од a_1, и да се период завршава са $a_n = 2a_0$:

$$\sqrt{d} = [a_0, \overline{a_1, a_2, \dots, a_{n-1}, 2a_0}].$$

Коначан верижни разломак $[a_0, a_1, \dots, a_{n-1}]$ одговара неком рационалном броју $\frac{x}{y}$, $(x, y) = 1$. Тада пар (x, y) задовољава $x^2 - dy^2 = (-1)^n$.

Пример. Нађимо минимално решење Пелове једначине $x^2 - 61y^2 = 1$.

Уз мало рачуна налазимо $\sqrt{61} = [7, \overline{1, 4, 3, 1, 2, 2, 1, 3, 4, 1, 14}]$. Период верижног разломка је 11, па нам $\frac{x}{y} = [7, 1, 4, 3, 1, 2, 2, 1, 3, 4, 1] = \frac{29718}{3805}$ одређује минимално решење $(x, y) = (29718, 3805)$ једначине $x^2 - 61y^2 = (-1)^{11} = -1$. Најзад, најмање решење (ξ, η) одговарајуће Пелове једначине добијамо ако период напишемо двапут, дакле $\frac{\xi}{\eta} = [7, 1, 4, 3, 1, 2, 2, 1, 3, 4, 1, 14, 1, 4, 3, 1, 2, 2, 1, 3, 4, 1]$: то је $(\xi, \eta) = (1766319049, 226153980)$.

4° Једначина $x^2 - dy^2 = a$, за $a \in \{-1, \pm2, \pm4\}$

Произвољна једначина Пеловог типа $x^2 - dy^2 = a$ не мора да има решења (на пример, једначина $x^2 - 3y^2 = 2$ - зашто?). Ипак, онда када има решења, сва решења се могу описати као што ћемо ускоро видети.

Једначина Пеловог типа која је у најдиректнијој вези са Пеловом је једначина $x^2 - dy^2 = N(x - y\sqrt{d}) = -1$. Ни за њу не важи да има решења за свако d. Наиме, да би имала решења, број d мора да дели $x^2 + 1$ за неко x - а знамо да такво x постоји ако и само ако су сви непарни прости делиоци d облика $4k + 1$ и $4 \nmid d$. Касније ћемо видети да ни то није довољан услов за постојање решења.

Т.4. Једначина $x^2 - dy^2 = -1$ има решење у скупу целих бројева ако и само ако постоји $z_1 \in \mathbb{Z}[\sqrt{d}]$ такво да је $z_1^2 = \zeta$, где је $z = \zeta$ најмање решење Пелове једначине $N(z) = 1$, $z > 1$.

Доказ. Решење (x, y) једначине $x^2 - dy^2 = -1$ одговара елементу $z = x + y\sqrt{d}$ са $N(z) = -1$. Претпоставимо да овакво $z \in \mathbb{Z}[\sqrt{d}]$ постоји. Тада је $N(z^2) = N(z)^2 = 1$, па је по Т.1 $z = \zeta^n$ за неко $n \in \mathbb{N}$. Број n мора бити непаран, јер у супротном важи $N(z) = N(\zeta)^{n/2} = 1$. Ако напишемо $n = 2k+1$, за $\zeta = z \cdot \zeta^{-k}$ важи $z_1^2 = \zeta$.

С друге стране, ако постоји z_1 са $z_1^2 = \zeta$, имамо $N(z_1) = \pm 1$, па због минималности ζ важи $N(z_1) = -1$. □

Т.5. Ако је p прост број облика $4k+1$ ($k \in \mathbb{N}$), онда једначина $x^2 - py^2 = -1$ има целобројних решења.

Доказ. Пођимо од једнакости $(\xi - 1)(\xi + 1) = p\eta^2$, где је (ξ, η) минимално решење Пелове једначине $x^2 - py^2 = 1$. Ако је ξ парно, онда $\eta^2 + 1 \equiv p\eta^2 + 1 \equiv 0 \pmod 4$ што је немогуће. Значи, ξ је непарно, па важи $(\xi - 1, \xi + 1) = 2$. Следи да је један од бројева $\xi - 1, \xi + 1$ облика $2s^2$, док је други једнак $2pt^2$ за неке целе бројеве s, t.

Претпоставимо да је $\xi + 1 = 2s^2$ и $\xi - 1 = 2pt^2$. Тада је $s^2 - pt^2 = 1$, па је s, t нетривијално решење Пелове једначине $x^2 - py^2 = 1$ мање од (ξ, η) што је контрадикција. Дакле, једина могућност је $\xi - 1 = 2s^2$ и $\xi + 1 = 2pt^2$, што нам даје $s^2 - pt^2 = -1$. □

Тако из сваког решења z једначине $N(z) = -1$ квадрирањем добијамо решење Пелове једначине: $N(z^2) = 1$. На први поглед, својство броја -1 да је $(-1)^2 = 1$ је круцијално. Ипак, решење Пелове једначине можемо добити и из решења једначина $N(z) = \pm 2$ и $N(z) = \pm 4$, тако да су и ове једначине једнако блиске Пеловој.

Т.6. Нека је $d \in \mathbb{N}$, где d није квадрат, и $z = x + y\sqrt{d}$ ($x, y \in \mathbb{Z}$). Тада важи:

(1) Ако је $N(z) = \pm 2$, тада је $\frac{1}{2}z^2 \in \mathbb{Z}[\sqrt{d}]$ и $N(\frac{1}{2}z^2) = 1$.

(2) Ако је $N(z) = \pm 4$ и $4 \mid d$, тада је $\frac{1}{4}z^2 \in \mathbb{Z}[\sqrt{d}]$ и $N(\frac{1}{4}z^2) = 1$.

(3) Ако је $N(z) = \pm 4$ и $4 \nmid d$, тада је $\frac{1}{8}z^3 \in \mathbb{Z}[\sqrt{d}]$ и $N(\frac{1}{8}z^3) = \pm 1$.

Доказ. (1) Имамо $\frac{1}{2}z^2 = \frac{x^2+dy^2}{2} + xy\sqrt{d}$, где је $\frac{x^2+dy^2}{2} = x^2 \pm 1$ цео број, па следи $\frac{1}{2}z^2 \in \mathbb{Z}[\sqrt{d}]$. При том је $N(\frac{1}{2}z^2) = \frac{1}{4}N(z^2) = \frac{1}{4}N(z)^2 = 1$.

(2) У овом случају је x парно, па $\frac{1}{4}z^2 = \frac{x^2+dy^2}{4} + \frac{xy}{2}\sqrt{d}$ има целе коефицијенте и $N(\frac{1}{4}z^2) = \frac{1}{16}N(z)^2 = 1$.

(3) Случај $d \equiv 2 \pmod 4$ је тривијалан, јер тада $2 \mid x, y$. Нека је сада d непарно.

Имамо $\frac{1}{8}z^3 = \frac{x(x^2+3dy^2)}{8} + \frac{y(3x^2+dy^2)}{8}\sqrt{d} = \frac{x(x^2\pm 3)}{2} + \frac{y(dy^2 \mp 3)}{2}\sqrt{d}$, где су коефицијенти очигледно цели бројеви, па следи $\frac{1}{8}z^3 \in \mathbb{Z}[\sqrt{d}]$ и $N(\frac{1}{8}z^3) = \frac{1}{64}N(z)^3 = \pm 1$. □

Пример. У примеру за метод Чакравала решавали смо једначину $x^2 - 67y^2 = 1$ и после корака 4 добили $N(z) = -2$ за $z = 221 + 27\sqrt{67}$. По Т.6 имамо $N(\frac{1}{2}z^2) = 1$, при чему је $\frac{1}{2}z^2 = 48842 + 5967\sqrt{67}$, дакле $(x, y) = (48842, 5967)$ је једно решење Пелове једначине $x^2 - 67y^2 = 1$.

5° Једначина Пеловог типа $x^2 - dy^2 = a$

Посматрајмо сада општу једначину Пеловог типа $N(z) = x^2 - dy^2 = a$. Ако је $z = z_0 \in \mathbb{Z}[\sqrt{d}]$ једно њено решење, а $\zeta = \xi + \eta\sqrt{d}$, као и до сад, најмање решење Пелове једначине $N(z) = 1$, тада је $N(z\zeta^n) = N(z)N(\zeta)^n = a$. Другим речима, $z = z_0\zeta^n$ ($n \in \mathbb{Z}$) такође задовољава једначину $N(z) = a$.

То значи да, да бисмо решили једначину Пеловог типа $N(z) = x^2 - dy^2 = a$, морамо прво да решимо одговарајућу Пелову једначину. Сва решења једначине Пеловог типа су генерисана коначним бројем "малих" решења, као што показује следеће тврђење.

Т.7. Нека је a цео број и $z = z_1$ једно решење једначине $N(z) = x^2 - dy^2 = a$. Тада постоје решење $z_0 = x_0 + y_0\sqrt{d}$ једначине $N(z) = a$ и цео број m такви да је

$$z_1 = z_0\zeta^m \quad \text{и} \quad 2x_0^2 \leq |a|(\xi + 1).$$

Доказ. Постоји $m \in \mathbb{Z}$ за које је $\sqrt{|a/\zeta|} \leq \zeta^m z_1 < \sqrt{|a\zeta|}$. Тада је и $z_0 = \zeta^m z_1 = x_0 + y_0\sqrt{d}$ решење једначине $N(z) = 1$ и важи

$$2|x_0| = \left|z_0 + \frac{a}{z_0}\right| \leq \max_{[\sqrt{|a/\zeta|},\sqrt{|a\zeta|})} \left|t + \frac{a}{t}\right| \leq \frac{\zeta + 1}{\sqrt{\zeta}}\sqrt{|a|}.$$

Квадрирањем, узимајући у обзир да је $\zeta + 1/\zeta = 2\xi$, добијамо тражену оцену. □

Напомена. Максимум функције $|t + \frac{a}{t}|$ на посматраном интервалу за $a < 0$ је $\frac{\zeta - 1}{\sqrt{\zeta}}\sqrt{|a|}$, па тако заправо добијамо мало јачу оцену: $2x_0^2 \leq |a|\xi + a$.

Задатак 1. Наћи сва целобројна решења једначине $x^2 - 7y^2 = 2$.

Решење. Најмање решење одговарајуће Пелове једначине је $(\xi, \eta) = (8, 3)$. Нађимо сва решења једначине $x^2 - 7y^2 = 2$ са $2x^2 \leq |a|(\xi + 1) = 18$, дакле са $x \leq 3$ и $y = \sqrt{\frac{x^2-2}{7}} \leq 1$. Једино такво решење је $(x, y) = (3, 1)$. Следи да су сва решења (x, y) задате једначине дата са

$$x + y\sqrt{7} = \pm(3 + \sqrt{7})(8 + 3\sqrt{7})^n, \quad n \in \mathbb{Z}.$$

Задатак 2. Решити једначину $3x^2 - 2y^2 = 1$ у скупу целих бројева.

Решење. Означимо $z = 3x$. Нашу једначину можемо записати у облику $z^2 - 6y^2 = 3$. Најмање решење Пелове једначине $z^2 - 6y^2 = 1$ је $(z, y) = (5, 2)$, па треба да нађемо сва решења једначине $z^2 - 6y^2 = 3$ са $2x^2 \leq 3(5+1) = 18$, тј. $x \leq 3$. Једино такво решење је $(z, y) = (3, 1)$. Следи да су сва решења те једначине дата са $z + y\sqrt{6} = (3 + \sqrt{6})(5 + 2\sqrt{6})^n$. Означимо $z_n + y_n\sqrt{6} = (3 + \sqrt{6})(5 + 2\sqrt{6})^n$. Како је тада $z_n + y_n\sqrt{6} = (5 + 2\sqrt{6})(z_{n-1} + {}$ ${}+y_{n-1}\sqrt{6})$, добијамо систем рекурентних формула

$$z_n = 5z_{n-1} + 12y_{n-1}, \quad y_n = 2z_{n-1} + 5y_{n-1}.$$

Одавде добијамо рекурентну формулу по z_n: $z_{n+1} - 10z_n + z_{n-1} = 0$. Можемо директно да израчунамо да је $z_0 = 3$, $z_1 = 27$, $z_2 = 267$, одакле добијамо да је свако z_n дељиво са 3 и одређује по једно $x_n = z_n/3$.

У општем случају, сасвим је могуће да решење једначине Пеловог типа не буде једнообразно, тј. да имамо више од једне фамилије решења.

Задатак 3. Наћи сва решења једначине $x^2 = 5y^2 + 44$ у скупу целих бројева.

Решење. Најмање решење одговарајуће Пелове једначине $x^2 - 5y^2 = 1$ је $(\xi, \eta) = (9, 4)$. Довољно је пронаћи сва решења дате једначине у којима је $2x^2 \leq |a|(\xi + 1) = 440$, тј. $x \leq 14$. Сва таква решења су $(\pm 7, \pm 1)$, $(\pm 8, \pm 2)$ и $(\pm 13, \pm 5)$. Дакле, тражена решења се изражавају формулама

$$x + y\sqrt{5} = \begin{cases} \pm(7 \pm \sqrt{5})(9 + 4\sqrt{5})^n, \\ \pm(8 \pm 2\sqrt{5})(9 + 4\sqrt{5})^n, \ \text{или} \\ \pm(13 \pm 5\sqrt{5})(9 + 4\sqrt{5})^n, \ \text{за } n \in \mathbb{Z}. \end{cases}$$

6° Задаци

1. За дати цео број d, решити једначину $x^2 - dy^2 = 1$ у скупу *рационалних* бројева.
2. Нека је y природан број. Доказати да је y члан Фибоначијевог низа ако и само ако је један од бројева $5y^2 \pm 4$ потпун квадрат.
3. Пронаћи све $n \in \mathbb{N}$ такве да је $\binom{n}{k-1} = 2\binom{n}{k} + \binom{n}{k+1}$ за неки природан број $k < n$.
4. Претпоставимо да за природан број n постоје цели бројеви x, y такви да је $n = x^2 + 4xy + 2y^2$. Доказати да тада постоје ненегативни цели бројеви x_0, y_0 такви да је $n = x_0^2 + 4x_0y_0 + 2y_0^2$.
5. Нека је $a \in \mathbb{N}$ и $D = a^2 - 1$. Ако су x, y цели бројеви и $m = x^2 - Dy^2$ задовољава $0 < m \leq 2a + 1$, доказати да је m потпун квадрат.
6. Ако је $m = 2 + 2\sqrt{28n^2 + 1}$ цео број за $n \in \mathbb{N}$, доказати да је m потпун квадрат.
7. Ако је разлика два узастопна куба једнака n^2, $n \in \mathbb{N}$, доказати да је $2n - 1$ квадрат.
8. Ако је n цео број такав да су $3n+1$ и $4n+1$ квадрати, доказати да је n дељиво са 56.
9. Ако је p прост број облика $4k + 3$, доказати да једна и само једна од једначина $x^2 - py^2 = \pm 2$ има целобројних решења.
10. Доказати да је $3^n - 2$ потпун квадрат само за $n = 1$ и $n = 3$.
11. Ако је $\dfrac{x^2+1}{y^2} + 4$ потпун квадрат за неке $x, y \in \mathbb{Z}$, доказати да је он једнак 9.

7° Решења

1. Овде није потребно никакво знање Пелове једначине. За $x \neq 1$ имамо $d\left(\frac{y}{x-1}\right) = \frac{x+1}{y}$. Означимо $\frac{y}{x-1} = t \in \mathbb{Q}$ и добићемо $x = \frac{dt^2+1}{dt^2-1}$ и $y = \frac{2t}{dt^2-1}$.
2. Најмање решење Пелове једначине $x^2 - 5y^2 = 1$ је $(x, y) = (9, 4)$. Према томе, по теореми 7, сва решења једначина $x^2 - 5y^2 = \pm 4$ проишоде из решења у којима је $2x^2 \leq 4(9+1)$, дакле $|x| \leq 4$. Таква решења су $(x, y) \in \{(\pm 4, \pm 2), (\pm 1, \pm 1)\}$ за једначину $x^2 - 5y^2 = -4$, односно $(x, y) = (\pm 3, \pm 1)$ за једначину $x^2 - 5y^2 = 4$. Следи да су сва решења (x, y) једначина $x^2 - 5y^2 = \pm 4$ дата формулама
$$x + y\sqrt{5} \ \in \ \{\pm 2(2+\sqrt{5})^n, \pm(3 \pm \sqrt{5})(2+\sqrt{5})^n, \pm(4 \pm 2\sqrt{5})(2+\sqrt{5})^n \ \mid \ n \in \mathbb{Z}\}.$$
Како је $2 + \sqrt{5} = \phi^3$ и $3 \pm \sqrt{5} = 2\phi^{\pm 2}$, где је $\phi = \frac{1+\sqrt{5}}{2}$, сва ова решења можемо написати у облику $x + y\sqrt{5} = \pm 2\phi^n$, $n \in \mathbb{N}$. Такође важи $x - y\sqrt{5} = \pm 2(-\phi)^{-n}$.
Сада је $y = (\phi^n - (-\phi)^{-n})/\sqrt{5} = F_n$, где F_n означава n-ти Фибоначијев број. Овим је тврђење задатка доказано.
3. Множењем са $\frac{(k+1)!(n-k+1)!}{n!}$ сводимо једначину на $k(k+1) = 2(k+1)(n-k+1) + (n-k)(n-k+1)$, што после сређивања постаје $n^2 + 3n + 2 = 2k^2 + 2k$, тј.
$$(2n+3)^2 + 1 = 2(2k+1)^2.$$
Најмање решење једначине $x^2 - 2y^2 = -1$ је $(1, 1)$, па су сва решења (x_i, y_i) дата са $x_i + y_i\sqrt{2} = (1+\sqrt{2})^{2i+1}$. Примећујемо да су x_i и y_i увек непарни, па је $n = \frac{x_i - 3}{2}$ цео број који задовољава услов задатка. Других решења очигледно нема.

4. Дати услов можемо записати у облику $n = 2z^2 - x^2$, где је $z = x + y$. Можемо узети $z, x \geq 0$. Како је $(r, s) = (3, 2)$ најмање природно решење једначине $r^2 - 2s^2 = 1$, по Т.7 постоји решење (z_0, x_0) једначине $z_0^2 - 2x_0^2 = -n$ такво да је $x_0^2 \leq n$. Тада је и $z_0^2 = x_0^2 + (x_0^2 - n) \leq x_0^2$ па је $y_0 \geq 0$. Јасно је да важи $n = x_0^2 + 4x_0y_0 + 2y_0^2$.

5. Најмање решење Пелове једначине $x^2 - Dy^2 = 1$ је $(x, y) = (a, 1)$. На основу Т.7 постоји решење (x_0, y_0) једначине $x^2 - Dy^2 = b$ такво да је $2x_0^2 \leq b(a+1) < 2(a+1)^2$, тј. $x_0 \leq a$. Одавде је или $y_0 = 1$ и $m = 1$, или $y_0 = 0$ и $m = x_0^2$.

6. Прво нађимо оне n за које је m цео број. Тада је $(\frac{m}{2} - 1, n)$ решење Пелове једначине $x^2 - 28y^2 = 1$ чије је најмање решење $(x_0, y_0) = (127, 24)$, па добијамо $\frac{m}{2} - 1 + n\sqrt{28} = (127 + 24\sqrt{28})^k$ за неко $k \in \mathbb{N}$. Сада је

$$m = 2 + (127 + 24\sqrt{28})^k + (127 - 24\sqrt{28})^k = A_k^2,$$

   при чему је $A_k = (8 + 3\sqrt{7})^k + (8 - 3\sqrt{7})^k$ цео број.

   Напомена. Решење $(127, 24)$ се може одредити посматрањем једначине $x^2 - 7y^2 = 1$ и налажењем решења у коме је y парно.

7. Нека је $(m+1)^3 - m^3 = 3m^2 + 3m + 1 = n^2$. Тада је $(2n)^2 = 3(2m+1)^2 + 1$. Следи да је $(2n, 2m+1)$ решење Пелове једначине $x^2 - 3y^2 = 1$, и као што је већ описано добијамо $2n + (2m+1)\sqrt{3} = (2 + \sqrt{3})^l$. Да би n био цео број, l мора бити непарно. Следи да је $4n = (2 + \sqrt{3})^{2k+1} + (2 - \sqrt{3})^{2k+1}$. Најзад,

$$2n - 1 = \frac{(1 + \sqrt{3})^2(2 + \sqrt{3})^{2k} + (1 - \sqrt{3})^2(2 - \sqrt{3})^{2k} - 8}{4} = N^2,$$

   при чему је N цео: $N = \frac{1}{2}\left((1 + \sqrt{3})(2 + \sqrt{3})^k + (1 - \sqrt{3})(2 - \sqrt{3})^k\right)$.

8. Нађимо све такве бројеве n. Нека је $3n + 1 = a^2$ и $4n + 1 = b^2$. Имамо $(2a)^2 - 3b^2 = 1$.

   Тражимо сва решења једначине $x^2 - 3b^2 = 1$ са парним $x = 2a$. Решења Пелове једначине $u^2 - 3v^2 = 1$ су дата са $(u, v) = (u_k, v_k)$, где је $u_k + v_k\sqrt{3} = (2 + \sqrt{3})^k$. Лако се добија да је u_k парно ако и само ако је k непарно. Дакле, $(x, b) = (u_{2k+1}, v_{2k+1})$, при чему још имамо

$$2u_{2k+1} = (2 + \sqrt{3})^{2k+1} + (2 - \sqrt{3})^{2k+1}.$$

   Следи да је $(a, b) = (\frac{1}{2}u_{2k+1}, v_{2k+1})$ и $n = \frac{1}{3}(a^2 - 1) = \frac{1}{12}(u_{2k+1}^2 - 4)$, што даје

$$\begin{aligned} 48n &= (7 + 4\sqrt{3})^{2k+1} + (7 - 4\sqrt{3})^{2k+1} - 14 \\ &= 2\left(7^{2k+1} - 7 + 48\binom{2k+1}{2}7^{2k-1} + 48^2\binom{2k+1}{2}7^{2k-3} + \cdots\right). \end{aligned}$$

   Одавде одмах видимо да је n дељиво са 7. С друге стране, како је $4n + 1$ непаран квадрат, а сви непарни квадрати су облика $8k + 1$ ($k \in \mathbb{Z}$), n мора да буде парно, а онда је и $3n + 1$ непаран квадрат, одакле следи да $8 \mid n$. Према томе, $7 \cdot 8 = 56 \mid n$.

9. Највише једна од ове две једначине има решења. Сада ако је (x_0, y_0) најмање решење одговарајуће Пелове једначине, ако $x_0 \pm 1$ нису узајамно прости, из једнакости $(x_0 - 1)(x_0 + 1) = py_0^2$ добијамо $x_0 \pm 1 = 2x^2$ и $x_0 \mp 1 = 2py^2$, тј. $x^2 - py^2 = \pm 1$, а и једно и друго је немогуће. Следи да су $x_0 \pm 1$ узајамно прости, што овог пута даје $x_0 \pm 1 = x^2$, $x_0 \mp 1 = py^2$ и $x^2 - py^2 = \pm 2$.

10. За парно n очигледно нема решења. Нека је $n = 2m + 1$, $m \in \mathbb{N}_0$. Тада је

$$x^2 - 3y^2 = -2 \qquad (*)$$

   за $y = 3^m$ и $x \in \mathbb{Z}$. Нађимо сва целобројна решења једначине $(*)$. Како је минимално решење Пелове једначине $x^2 - 3y^2 = 1$ пар $(2, 1)$, по Т.7 довољно је наћи сва решења $(*)$ са $2x^2 \leq 2(2+1) = 6$, тј. $|x| \leq 1$. Једина таква решења су $(x, y) = (\pm 1, \pm 1)$, одакле следи да су сва решења $(*)$ дата релацијом $x+y\sqrt{3}=\pm(\pm 1+\sqrt{3})(2+\sqrt{3})^k$, $k\in\mathbb{Z}$, што се, с обзиром на једнакости $(1+\sqrt{3})^2=2(2+\sqrt{3})$ и $-1+\sqrt{3}=\frac{2}{1+\sqrt{3}}$, своди на

$$x+y\sqrt{3}=\pm\frac{1}{2^k}(1+\sqrt{3})^{2k+1}.$$

Означимо $(1+\sqrt{3})^i=a_i+b_i\sqrt{3}$, тако да је $y=\frac{1}{2^k}a_{2k+1}$ за неко k. Имамо $a_0=0$, $a_1=1$, $a_{i+1}=2a_i+2a_{i-1}$. Претпоставимо да је $n>3$, тј. $m\geq 2$. Видимо да $9\mid a_9=2448=9\cdot 272$ и да $9\mid a_i$ ако и само ако $9\mid i$. Међутим, једноставном индукцијом по i се показује да је $a_{i+9}\equiv a_{10}a_i \pmod{a_9}$, одакле $a_9\mid a_{9j}$ за $j\in\mathbb{Z}$. Следи да $16\cdot 17=272\mid a_{9j}$; дакле, ако је a_i дељиво са 9, онда је дељиво и са 17. Према томе, немогуће је да $y=\frac{1}{2^k}a_{2k+1}$ буде степен тројке већи од 3.

11. Доказујемо да једначина $x^2-(n^2-4)y^2=-1$ нема решења у $\mathbb{N}$ за $n>3$. Пошто је $x<ny$, стављањем $x=ny-z$ $(z>0)$ добијамо $-2nyz+z^2+4y^2=-1$. За $w=2y$ имамо

$$z^2+w^2+1=nzw. \qquad (*)$$

Показаћемо да $(*)$ нема решења у $\mathbb{Z}$ ни за једно цело $n>3$. Претпоставимо супротно и посматрајмо решење (z,w) са најмањим z. Како је $f(w)=f(nz-w)$ за $f(t)=nzt-t^2$, пар $(z,nz-w)$ је такође решење $(*)$, па због минималности z важи $nz-w\geq z$, тј. $z\leq w\leq(n-1)z$. Међутим, тада је $z^2+1=f(w)\geq f(z)=(n-1)z^2$, што за $n>3$ значи да је $z=0$, а $(*)$ нема решења са $z=0$. Према томе, једина могућност је $n=3$, и у том случају имамо решења, нпр. $(x,y)=(2,1)$.

Београд, 2003-2011