Математичка гимназија у Београду
Додатна настава, шк.г. 2003/04

Пелова једначина

Основна теорија

Деф. *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, обично зовемо *једначином Пеловог типа.*

Произвољна квадратна диофанцка једначина са две непознате се може свести на једначину Пеловог типа. Како се решавају 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 (са две непознате) може наћи опште решење изражено релативно једноставном формулом.

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:

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

Како бисмо искористили овакво разлагање, важно је 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.

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

Пример. Једначина $x^2 - dy^2 = a$ се еквивалентно записује као $N(z) = a$, где је $z = x - y\sqrt{d}$, $x, y \in \mathbb{Z}$. Специјално, Пелова једначина је еквивалентна једначини $N(z) = 1$, $z \in \mathbb{Z}[\sqrt{d}]$.

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 је директан.

Пелова једначина има два тривијална решења, $(\pm 1, 0)$, која одговарају $z = \pm 1$. Ако знамо и најмање *нетривијално* решење, тврдимо да онда знамо сва решења.

Т.2 Ако је z_0 најмањи број елемент скупа $\mathbb{Z}[\sqrt{d}]$ такав да је $z_0 > 1$ и $Nz_0 = 1$, онда су сви елементи $z \in \mathbb{Z}[\sqrt{d}]$ за које је $Nz = 1$ дати са $z = \pm z_0^n$, $n \in \mathbb{Z}$.

Доказ Претпоставимо да је $Nz = 1$ за неко $z \in \mathbb{Z}[\sqrt{d}]$. Постоји тачно један цео број k за који је $|z_0|^k \leq |z| < |z_0|^{k+1}$. Тада је $z_1 = zz_0^{-k} = z\overline{z_0}^k$ елемент скупа $\mathbb{Z}[\sqrt{d}]$ који задовољава $N(z_1) = N(z)N(z_0)^{-k} == N(z) = 1$. Међутим, из $|z_1| = |z| \cdot |z_0|^{-k}$ следи $1 \leq |z_1| < |z_0|$, а с обзиром на минималност $|z_0|$ добијамо $z_1 = 1$. Дакле, $z = z_0^k$.

Последица. Ако је x_0, y_0 најмање решење Пелове једначине за дато d, онда су сва природна решења (x, y) те једначине дата са $x + y\sqrt{d} = \pm(x_0 + y_0\sqrt{d})^n$, $n \in \mathbb{N}$.

Пример. Најмање нетривијално решење једначине $x^2 - 2y^2 = 1$ је $(x, y) = (3, 2)$. Према томе, за свако решење (x, y) постоји цео број n такав да је $x + y\sqrt{d} = \pm(3 + 2\sqrt{2})^n$. Како је тада и $x - y\sqrt{d} = (3 - 2\sqrt{2})^n$, добијамо формулу

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

Сада ћемо показати да Пелова једначина увек има нетривијално решење.

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

Л.2 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 следи директно из Дирихлеове теореме.

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

Доказ Примењујући Л.2 на $\alpha = \sqrt{d}$ закључујемо да постоји цео број n, $|n| < 2\sqrt{d}+1$ такав да једначина $x^2 - dy^2 = n$ има бесконачно много решења (x, y) у скупу природних бројева. Следи да постоје два различита, рецимо (x_1, y_1) и (x_2, y_2), који задовољавају $x_1 \equiv x_2$ и $y_1 \equiv y_2 \pmod{n}$. Означимо $z_1 = x_1 + y_1\sqrt{d}$ и $z_2 = x_2 + y_2\sqrt{d}$, и нека је $z_1 > z_2$. Тада је $z_0 = z_1/z_2$ елемент $\mathbb{Z}[\sqrt{d}]$ норме 1 (проверите!), тако да одређује једно решење (x_0, y_0) Пелове једначине.

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, постоји алгоритам за проналажење општег 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 $z_1^2 = z_0$.

Доказ "Ако" смер је тривијалан. У другом смеру, посматрамо најмање решење $z = z_1 \in \mathbb{Z}[\sqrt{d}]$ једначине $N(z) = -1$ које задовољава $z > 1$ и на исти начин као у теореми Т.2 показујемо да је $1 \leq z_1 < z_0$, па како је $z = z_1^2 < z_0^2$ решење Пелове једначине $N(z) = 1$, закључујемо да је $z_1^2 = z_0$.

Т.5 Ако је k цео број и $z_1 \in \mathbb{Z}[\sqrt{d}]$ једно решење једначине $N(z) = k$, онда постоји $m \in \mathbb{Z}$ за које је $1 \leq |z_0^m z_1| < z_0$.

Доказ Потпуно иста идеја као у доказу претходног тврђења. Испишите детаље за вежбу!

Задаци за вежбу

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

2. Решити у скупу $\mathbb{Z}$ једначину $x^2 + y^2 - 1 = 4xy$.

3. За дати цео број d, решити једначину $x^2 - 2y^2 = 1$ у скупу *рационалних* бројева.

4. Нека је $(x, y) = (a, b)$, $a, b \in \mathbb{N}$ најмање решење једначине $x^2 - dy^2 = 1$. Посматрајмо низ дат релацијама $y_0 = 0$, $y_1 = b$, $y_{n+1} = 2ay_n - y_{n-1}$ за $n \geq 1$. Доказати да је $ay_n^2 + 1$ потпун квадрат за свако n. Доказати да ако је $ay^2 + 1$ квадрат за неко $y \in \mathbb{N}$, онда је $y = y_n$ за неко n.

5. Доказати да је $5x^2 + 4$ или $5x^2 - 4$ потпун квадрат ако и само ако је x члан Фибоначијевог низа.

6. Пронаћи све $n \in \mathbb{N}$ такве да је $\binom{n}{k+1} = \binom{n}{k} + \binom{n}{k-1}$ за неки природан број $k < n$.

7. Нека је $a \in \mathbb{N}$ и $d = a^2 - 1$. Ако су x, y цели бројеви и $m = x^2 - dy^2$ мање по апсолутној вредности од $2a + 1$, доказати да је $|m|$ потпун квадрат.

8. Ако је $m = 2 + 2\sqrt{28n^2 + 1}$ цео број за $n \in \mathbb{N}$, доказати да је m потпун квадрат.

9. Ако је разлика два узастопна куба једнака n^2, $n \in \mathbb{N}$, доказати да је $2n - 1$ квадрат.

10. Доказати да једначина $x^2 - dy^2 = -1$ има решење у скупу целих бројева ако и само ако га има једначина $x^2 - dy^2 = -4$.

11. Нека је p прост број. Доказати да једначина $x^2 - py^2 = -1$ има целобројних решења ако и само ако је $p = 2$ или $p \equiv 1 \pmod 4$.

12. 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.

13. Доказати да је $3^n - 2$ потпун квадрат само за $n = 1$ и $n = 3$.

14. Ако је $\dfrac{x^2 + 1}{y^2} + 4$ потпун квадрат, доказати да је он једнак 9.

Душан Ђукић