Решения на задачите по теория на числата

Този материал е изготвен със съдействието на школа Sicademy

NT1. Четворка цели ненулеви числа $\{a, b, c, d\}$ ще наричаме $(2,3)$-специална, ако едновременно са изпълнени:

1. $a^2 + b^2 = c^3 + d^3 =: n$;
2. не съществува четворка цели числа $\{x, y, z, t\}$, такава че $x^6 + y^6 + z^6 + t^6 = n$.

а) Да се намери най-малката възможна стойност на $k := c + d$ в $(2,3)$-специална четворка.

б) Да се докаже, че съществуват безброй много $(2,3)$-специални четворки, за които минимумът $k = c + d$ от а) се достига.

Решение. Ще покажем, че търсеният минимум е $k = 1$. Тъй като $a, b \neq 0$, имаме, че $n = a^2 + b^2 > 0$. Тогава от $n = (c+d)(c^2 - cd + d^2)$ следва, че $c + d > 0$. Следователно $c + d \geq 1$. Ще покажем, че съществуват безброй много $(2,3)$-специални четворки от вида $\{a, a-1, c, 1-c\}$, $a, c \geq 2$, с което задачата ще бъде решена. От равенството

$$a^2 + (a-1)^2 = c^3 + (1-c)^3$$

последователно получаваме

$$2a^2 - 2a = 3c^2 - 3c \Leftrightarrow (2a-1)^2 = 6c^2 - 6c + 1 \Leftrightarrow 6c^2 - 6c + 1 - t^2 = 0,$$

където сме положили $2a - 1 = t$ за краткост. Дискриминантата на последното квадратно (относно c) уравнение е точен квадрат: $D = 9 - 6 + 6t^2 = (3m)^2$ и положителното решение на това уравнение е $c = (1+m)/2$. Относно променливите m и t получихме следното диофантово уравнение (на Пел):

$$3m^2 - 2t^2 = 1, \quad t, m > 1,$$

$$a = \frac{t+1}{2}, \quad c = \frac{m+1}{2}.$$

За всяко естествено n дефинираме редиците $\{M_n\}$ и $\{T_n\}$ от естествени числа чрез равенствата

$$(\sqrt{3} - \sqrt{2})^{2n-1} = M_n\sqrt{3} - T_n\sqrt{2},$$

$$(\sqrt{3} + \sqrt{2})^{2n-1} = M_n\sqrt{3} + T_n\sqrt{2}.$$

Имаме $3M_n^2 - 2T_n^2 = 1$, $M_1 = T_1 = 1$ и

$$\begin{aligned} T_{n+1} &= 5T_n + 6M_n \\ M_{n+1} &= 4T_n + 5M_n \end{aligned}$$

$$\Rightarrow \begin{aligned} a_{n+1} &= 5a_{n-1} + 6c_n \\ c_{n+1} &= 4a_{n-1} + 5c_n, \end{aligned}$$

където $T_i = 2a_i - 1$, $M_i = 2c_i - 1$. От полагането следва, че $a_{n+1}^2 + (a_{n+1} - 1)^2 = c_{n+1}^3 + (1 - c_{n+1})^3$, т.е. четворките $\{a_n, a_n - 1, c_n, 1 - c_n\}, n \geq 2$ от цели неотрицателни числа, изпълняват условие (1). Тъй като $x^6 \equiv 0, 1 \pmod 7$, то никое число от вида $7\ell + 5$ не може да се представи като сума на четири шести степени. Непосредствена проверка ни дава $c^3 + (1-c)^3 \equiv 5 \pmod 7$, когато $c \equiv 3, 5 \pmod 7$, следователно, ако в редицата $\{c_n\}$ има безброй много членове, даващи остатък 3 или 5 по модул 7, условие (2) е изпълнено за тях и задачата е решена.

Изразявайки $a_n - 1$ чрез c_n и c_{n-1} и замествайки във формулата за c_{n+1}, получаваме рекурентната връзка $c_{n+1} = 10c_n - c_{n-1} - 4$, откъдето

$$c_{n+1} \equiv 3(c_n + 1) - c_{n-1} \pmod 7, \quad c_1 \equiv 1 \pmod 7, \quad c_2 \equiv 5 \pmod 7.$$

Така, по модул 7 остатъците на c_n образуват следната периодична редица:

$$1, 5, 3, 0, 0, 3, 5, 1, 1, 5, 3, 0, 0, 3, 5, 1, \ldots$$

и, например четворките от вида $\{a_{8\ell+2}, a_{8\ell+2}-1, c_{8\ell+2}, 1-c_{8\ell+2}\}$ са $(2,3)$-специални за всяко естествено число ℓ. Най-малката такава четворка е $\{6, 5, 5, -4\}$.

NT2. Ще казваме, че естественото число q е добро за апроксимиране на реалното число α, ако съществува цяло число p, такова, че

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^2}.$$

За фиксирано $\alpha \in \mathbb{R}$ означаваме с D_α множеството от всички естествени числа, които са добри за апроксимиране на α. Да се докаже, че ако D_α съдържа всички числа от вида $2^k + 1$, където $k \in \mathbb{N}$, то $D_\alpha = \mathbb{N}$.

Решение. Ще докажем, че числото α е цяло, което очевидно води до $D_\alpha = \mathbb{N}$.

Да допуснем първо, че α е ирационално. Тогава за всяко $q \in D_\alpha$ от неравенствата в условието следва, че дробната част $\{q\alpha\}$ принадлежи на някой от интервалите $(0, 1/q)$ и $(1 - 1/q, 1)$. Нека естественото число r е такова, че

$$2^r > \max\left(\frac{1}{\{\alpha\}}, \frac{1}{1 - \{\alpha\}}\right).$$

Ако $0 < \{(2^r + 1)\alpha\} < 1/(2^r + 1)$, то

$$\{\alpha\} > \frac{1}{2^r + 1} > \{(2^r + 1)\alpha\} = \{\{2^r\alpha\} + \{\alpha\}\}.$$

Това означава, че

$$1 - \{\alpha\} < \{2^r\alpha\} < 1 - \{\alpha\} + \frac{1}{2^r + 1}.$$

Ако пък $1 > \{(2^r + 1)\alpha\} > 1 - \frac{1}{2^r+1}$, аналогично получаваме, че

$$1 - \{\alpha\} - \frac{1}{2^r + 1} < \{2^r\alpha\} < 1 - \{\alpha\}$$

(използваме и неравенството $\{2^r\alpha\} + \{\alpha\} < 2 - \frac{1}{2^r+1}$, което следва от избора на r).

Получихме, че за всички достатъчно големи r е са изпълнени неравенствата

$$1 - \{\alpha\} - \frac{1}{2^r + 1} < \{2^r\alpha\} < 1 - \{\alpha\} + \frac{1}{2^r + 1}.$$

Това лесно води до противоречие (с разглеждане поотделно на случаите $\{\alpha\} < 1/2$ и $\{\alpha\} > 1/2$).

Нека сега $\alpha = a/b$ е рационално число, $b \in \mathbb{N}$, $a \in \mathbb{Z}$ и $(a, b) = 1$. Тогава неравенството в условието казва, че за всяко $q_n = 2^{2^n} + 1$ съществува $p_n \in \mathbb{Z}$, такова, че

$$\left|\frac{a}{b} - \frac{p_n}{q_n}\right| \leq \frac{1}{q_n^2},$$

тоест $|aq_n - p_n b| < \frac{b}{q_n}$. Оттук при $q_n > b$ заключаваме $aq_n = p_n b$, което води до $b|q_n$, за всеко $n > b$ и тъй като $(q_n, q_{n+1}) = 1$, заключаваме, че $b = 1$, т.е. α е цяло число.

NT3. Нека P и Q са неконстантни полиноми с цели неотрицателни кофициенти и старши кофициент 1, а k е естествено число. Естествените числа $a_1, a_2, \ldots, a_k; a_i \geq 2$ за $i = 1, 2, \ldots, k$, са такива, че за всяко естествено число n числото

$$(a_1^{P(n)} + Q(n))(a_2^{P(n)} + Q(n)) \cdots (a_k^{P(n)} + Q(n))$$

е точен квадрат. Да се докаже, че числото $a_1 a_2 \ldots a_k$ също е точен квадрат.

Решение. Ще използваме следната лема.

Лема. Нека f е неконстантен полином с цели коефициенти и нека A е множеството от прости числа p, за които $v_p(f(n))$ е нечетно за някое $n \in \mathbb{N}$. Ако множеството A е крайно, то съществуват полином g с цели коефициенти и константа c, такива, че $f = cg^2$.

Доказателство. Можем да считаме, че полиномът f е свободен от квадрати (т.е. не се дели на квадрат на полином с цели коефициенти). От условието следва, че множеството от простите числа, които делят точно в четни степени стойности на f, е безкрайно. Нека p е такова просто число и $p^{2k} \parallel f(n)$ за някои естествени числа n и k.

Да разгледаме $f(n + \ell p^{k+1})$, където $\ell \in \mathbb{N}$. Лесно се вижда, че

$$f(n + \ell p^{k+1}) \equiv f(n) + \ell p^{k+1} f'(n) \pmod{p^{2k+2}}.$$

Ако $(p, f'(n)) = 1$, то сравнението $\ell f'(n) + \frac{f(n)}{p^{k+1}} \equiv p^k \pmod{p^{k+1}}$ има решение. Това означава, че съществува естествено число n_1, за което $p^{2k+1} \| f(n_1)$, т.е. $p \in A$, което е противоречие. Следователно съществуват безбройно много прости числа p, за които съществува естествено число n, такова, че $p|(f(n), f'(n))$. Сега от лемата на Безу за полиноми следва, че съществуват полиноми $u, v \in \mathbb{Z}[x]$, такива че $uf + vf' = T$, където $T \in \mathbb{Z}[x]$ е най-големият общ делител на f и f', като при това T не е константа. Нека R е неразложим делител на T и нека z е негов (комплексен) корен. Тъй като z е общ корен на f и f', то z е кратен корен на f. Тъй като R няма кратни корени (защото е неразложим), всеки негов корен е корен и на f/R, тоест $R^2|f$, което противоречи на избора на f в началото. Следователно $f = cg^2$ за някои $c \in \mathbb{Z}$ и $g \in \mathbb{Z}[x]$, с което лемата е доказана.

Обратно към решението да отбележим първо, че можем да считаме, че числата $a_1, a_2, \ldots, a_k$ са две по две различни. Нека $c = P(1) > 0$ и да разгледаме полинома $g(x) = Q(x) + a_1^c$. Да допуснем, че $g(x)$ не е точен квадрат на полином с цели коефициенти. Тогава от горната лема и от лемата на Шур следва, че съществуват безбройно много прости числа p, за които съществува естествено число n_0, за което $v_p(g(n_0)) = 2k + 1$ е нечетно число. За всяко такова p по Китайската теорема за остатъците можем да изберем естествено число n, за което $n \equiv 1 \pmod{p-1}$ и $n \equiv n_0 \pmod{p^{2k+2}}$. Тогава $p^{2k+1} \| g(n) = Q(n) + a_1^{P(n)}$. Последното означава, че $p|a_i^{P(n)} + Q(n)$ за някое $i \neq 1$, откъдето $p|a_1^c - a_i^c$. Тъй като можем да изберем $p > \max\{|a_1^c - a_i^c| : i = 2, 3, \ldots, k\}$, заключаваме, че $a_1^c = a_i^c$ за някое $i \neq 1$, т.е. $a_1 = a_i$, противоречие.

Нека $Q(x) + a_1^c = R_1^2(x)$ е точен квадрат на неконстантен полином с цели коефициенти. С $d = P(2) > P(1) = c$ и разсъждения както по-горе заключаваме, че и $Q(x) + a_1^d = R_2^2(x)$ е точен квадрат на неконстантен полином с цели коефициенти. Тогава

$$a_1^c - a_1^d = (R_1(x) - R_2(x))(R_1(x) + R_2(x)),$$

откъдето лесно следва, че $R_1 \equiv R_2$ и $a_1^c = a_1^d$, т.е. $a_1 = 1$.