1

Десятая проблема Гильберта

Ю. В. Матиясевич, Я. Абрамов, А. Я. Белов-Канель,
И. А. Иванов-Погодаев, А. С. Малистов

Уравнение Пелля

Определение. *Уравнением Пелля* называется уравнение вида $x^2 - dy^2 = 1, d \in \mathbb{N}$.

♦ **A8.** *Уравнение Пелля.*
а) *Решение (x, y) назовчм нетривиальным, если $y \neq 0$. Пусть d – квадрат. Докажите, что нет нетривиальных решений.*
б) *Пусть (u_1, v_1) и (u_2, v_2) – решения уравнения Пелля $x^2 - dy^2 = 1$. Докажите, что если $u_3 + \sqrt{d}v_3 = (u_1+\sqrt{d}v_1)\cdot(u_2+\sqrt{d}v_2)$, то (u_3, v_3) — также решение. В частности, если (x, y) — решение, то (x_n, y_n) — решение, где $x_n + \sqrt{d}y_n = (x + \sqrt{d}y)^n$.*
в) *Решение назовчм минимальным, если оно нетривиально, и среди нетривиальных $|x+y|$ минимально. Докажите, что любое решение — степень минимального.*

Известно, что если d не квадрат, то существует нетривиальное решение. Это достаточно сложное утверждение, поэтому мы не приводим его доказательство и не включаем его в список задач. Доказательство см., например, в книге В. О. Бугаенко «Уравнение Пелля».

♦ **A9.** *Специальный случай уравнения Пелля*
а) *$d = k^2 - 1$. Докажите, что $(k, 1)$ — минимальное решение.*
б) *$d = k^2 - 1$, (x_1, y_1) — минимальное решение, $(x_n, y_n) = (x_1, y_1)^n$. Докажите, что $y_n \equiv n \pmod{(k-1)}$.*
с) *Другие виды уравнения Пелля. Решите уравнение $x^2 - (\frac{b^2}{4} - 1)y^2 = 1$*

Диофантовость степени

Сейчас мы будем рассматривать решения специального семейства диофантовых уравнений, называемых уравнениями Пелля. Решения этих уравнений получаются из частного их решения с помощью последовательног многократного применения одного и того же преобразования плоскости.

Рассмотрим последовательность, заданную так: $\alpha_0(b) = 0$, $\alpha_1(b) = 1$, $\alpha_{n+2}(b) = b\alpha_{n+1}(b) - \alpha_n(b)$, где $b \geqslant 2$.

♦ **A10.** *Докажите, что $x^2 - bxy + y^2 = 1, x, y \geqslant 0$, тогда и только тогда, когда*

$$\text{либо} \begin{cases} x = \alpha_{m+1}(b), \\ y = \alpha_m(b), \end{cases} \qquad \text{либо} \begin{cases} x = \alpha_m(b), \\ y = \alpha_{m+1}(b), \end{cases}$$

для некоторого m.

♦ **A11.** *Докажите, что $\alpha_n(2) = n$;*

♦ **A12.** *Докажите, что $\alpha_{k+\ell}(b) = \alpha_k(b) \cdot \alpha_{\ell+1}(b) - \alpha_{k-1}(b) \cdot \alpha_\ell(b)$.*

♦ **A13.** *Докажите, что $\alpha_n(b) \equiv \alpha_{n+4m}(b) \pmod{v}$, где $v = \alpha_{m+1}(b) - \alpha_{m-1}(b)$;*

♦ **A14.** *Докажите, что если $b_1 \equiv b_2 \pmod{q}$, то $\alpha_n(b_1) \equiv \alpha_n(b_2) \pmod{q}$.*

Через $b \ (\mathrm{amod}\ c)$ обозначается расстояние от b до ближайшего числа, делящегося на c.

♦ **A15.** *Докажите, что наименьшим числом k, таким что при фиксированном n*

$$\alpha_n(w) \pmod{\!\!}\ \text{(amod } v) = \alpha_{n+k}(w) \quad (\text{amod } v),$$

$$\text{где} \quad w \equiv b \pmod{v}, \quad v = \alpha_{m+1}(b) - \alpha_{m-1}(b),$$

является $2m$.

♦ **A16.** *Докажите, что если*

$$w \equiv b \pmod{v}, \quad w \equiv 2 \pmod{u}, \qquad \text{где } v > 2\alpha_k(b),\ u > 2k,$$

то первые k членов последовательности

$$\big(\alpha_0(b), 0\big), \ldots, \big(\alpha_n(b), n\big), \ldots$$

совпадают с первыми k членами последовательности

$$\Big(\alpha_0(w) \quad (\text{amod } v), \alpha_0(w) \quad (\text{amod } u)\Big), \ldots, \Big(\alpha_n(w) \quad (\text{amod } v), \alpha_n(w) \quad (\text{amod } u)\Big), \ldots$$

♦ **A17.** *Докажите, что если $\alpha_m(b)$ делится на $(\alpha_k(b))^2$, то m делится на $\alpha_k(b)$.*

♦ **A18.** *Докажите, что если $2\alpha_k(b) < u$, то $2k < u$.*

♦ **A19.** *Докажите, что множество $\{(a,\ b,\ c) \mid\ a = \alpha_c(b),\ b > 3\}$ диофантово.*

♦ **A20.** *Докажите, что $(k-1)^n \leqslant \alpha_{n+1}(k) \leqslant k^n$;*

♦ **A21.** *Докажите, что $(1+s)^n \geqslant 1 + ns$ при $s \in \mathbb{R}$, $s > -1$, n — целое неотрицательное;*

♦ **A22.** *Докажите, что $b^c = \lim\limits_{n\to\infty} \dfrac{\alpha_{c+1}(bn+4)}{\alpha_{c+1}(n)}$.*

♦ **A23.** *Докажите, что диофантово уравнение, в котором разрешено возводить в степень (экспоненциально диофантовое уравнение), сводится к обычному диофантову уравнению, быть может, с большим числом неизвестных.*