Подсказки и решения задач пунктов A и B

♦ **A 1.** a) $x = 2a$;

b) $x^2 = (2a-1)^2$;

c) $x = a^2$;

d) $x = a^3$.

♦ **A 2.** Пусть система уравнений такова: $D_1 = 0, \ldots, D_n = 0$. Она эквивалентна одному уравнению $D_1^2 + \cdots + D_n^2 = 0$.

♦ **A 3.** Чтобы пересечь два диофантовых множества, объединим уравнения первого и второго в систему, которая, как мы знаем, эквивалентна одному уравнению. Чтобы объединить два множества, просто перемножим уравнения.

♦ **A 4.** Чтобы показать, что это множество диофантово, рассмотрим то же самое уравнение, но уже относительно параметров $a_1, \ldots, a_m$.

♦ **A 5.** a) $a - b = x + 1$;

b) $a = bx$;

c) $(a-b)^2 = c^2 x$, $0 \leqslant a < c$;

d) Воспользуемся предыдущими пунктами: $a = min\{x, y\}$, $x = bmod(c)$, $y = (c-b)mod(c)$. Реализуем минимум: $a \leqslant x$, $a \leqslant y$, $(a-x)(a-y) = 0$.

e) $ac \leqslant b < (a+1)c$.

♦ **A 6.** Отношение взаимной простоты из алгоритма Евклида выражается уравнением $a(x_1 - x_2) + b(y_1 - y_2) = 1$. $a = (b, c)$, если $b = ax$, $c = ay$, x и y взаимно просты. Чтобы получить НОК, воспользуемся тем, что умеем выразить НОД, и $a \cdot b = (a, b) \cdot (a, b)$.

♦ **A 7.** a) $x^2 < a < (x+1)^2$.

♦ **A 8.** a) $x^2 - n^2 y^2 = 1$. Тогда целые числа $x + ny$ и $x - ny$ равны, поэтому $y = 0$, поэтому $x = \pm 1$.

b) Получаем по определению $u_3 = u_1 u_2 + d v_1 v_2$, $v_3 = u_1 v_2 + u_2 v_1$. Подставим в уравнение: $u_1^2 u_2^2 + d^2 v_1^2 v_2^2 + 2d u_1 u_2 v_1 v_2 - d u_1^2 v_2^2 - d u_2^2 v_1^2 - 2d u_1 u_2 v_1 v_2 = u_2^2(u_1^2 - d v_1^2) - d v_1^2 (u_2^2 - d v_2^2) = 0$;

c) Заметим, что на решение уравнения можно не только умножать, как в предыдущем пункте, но и делить. Это легко проверить. Если рассмотреть уравнение на всей плоскости, то мы получим гиперболу, где наши решения

– еч целые точки. Заметим, что умножение, а потому и деление на сохраняют порядок точек на гиперболе. Рассмотрим только правую ветку, только положительную часть, ибо можно считать переменные неотрицательными. Пусть есть решение, которое не степень минимального. Будем делить на минимальное. По предположению мы не получим тривиальное решение, тогда получим нетривиальное решение, по модулю меньшее, чем минимальное. Противоречие.

♦ **A 9.** a) Если увеличить 1, то и k увеличится, то есть не получится меньшее решение, а уменьшив единицу, мы получим лишь 0.

b) Получаем индукцией по n, ибо $x_n \equiv 1 mod(k-1)$.

c)Задача сводится к следующей за ней: $1 = x^2 - (\frac{b^2}{4} - 1)y^2 = (x + \frac{b}{2}y)^2 - b(x + \frac{b}{2}y)y + y^2$

♦ **A 10.** Рассмотрим отображение $(x, y) \mapsto (y, by - x)$. Оно увеличивает сумму координат. Будем приминять обратное отображение, которое также целочисленно. Поскольку решения целочисленны, бесконечно уменьшатся сумма модулей координат не может. Легко проверить, что, если она не уменьшается, то $y = 0, x = 1$, так что решение получается нашим преобразованием из тривиального.

♦ **A 11.** Это получается по индукции, ибо $n + 2 = 2(n-1) - n$.

♦ **A 12.** Это проверяется индукцией по l. Для $l = 0$ это тривиально следует из того, что $\alpha_0 = 0$, $\alpha_1 = 1$, для $l = 1$ это следует из рекуррентного определния последовательности α_i.

♦ **A 13.** Используется $\alpha_{2m}(b) = \alpha_m(b)(\alpha_{m+1}(b) - \alpha_{m-1}(b))$, $\alpha_{4m-1}(b) = \alpha_{2m-1}(b)(\alpha_{2m}(b) - \alpha_{2m-2}(b))$ и то, что $\alpha_{4m}(b)$ делится на $\alpha_{2m}(b)$.

♦ **A 14.** Проверяется индукцией из рекуррентного определения последовательности.

♦ **A 15.** Без комментариев

♦ **A 16.** Легко понять, что $\alpha_n(b) (\mathrm{amod}\, v) = \alpha_n(w) (\mathrm{amod}\, v)$ и $n (\mathrm{amod}\, u) = \alpha_n(w) (\mathrm{amod}\, u)$(из задачи 14). Т.к. то, что стоит под amod в правых частях меньше, чем v и u соответственно (т.к. последовательность $\alpha_n(b)$ возрастает), то $\alpha_n(b) = \alpha_n(b) (\mathrm{amod}\, v)$ и $n = n (\mathrm{amod}\, u)$, откуда и следует утверждение задачи.

♦ **A 17.** Без комментариев

♦ **A 18.** Это равносильно тому, что просто $\alpha_k(b) \geqslant k$, то есть что $\alpha_k(b)$ строго возрастает, что очевидно.

♦ **A 19.** Без комментариев.

♦ **A 20.** Индукция по n. При $n = 0, 1$ верно. Пусть верно для n. Покажем для $n+1$. $\alpha_{n+1}(k) = k\alpha_n(k) - alpha_{n-1}(k) \leqslant k\alpha_n(k) \leqslant k^{n+1}$.

$\alpha_{n+1}(k) = k\alpha_n(k) - alpha_{n-1}(k) \geqslant (k-1)\alpha_n(k) + (\alpha_n(k) - \alpha_{n-1}(k)) \geqslant (k-1)\alpha_n(k) \geqslant (k-1)^n$

♦ **A 21.** Индукция по n. Для 0 верно. пусть верно для n. Проверим для $n+1$. $(1+s)^{n+1} = (1+s)^n(1+s) \geqslant (1+ns)(1+s) = 1+(n+1)s+ns^2 \geqslant 1+(n+1)s$

♦ **A 22.** $\frac{\alpha_{c+1}(bn+4)}{\alpha_{c+1}(n)} \leqslant \frac{(bn+4)^c}{(n-1)^c} = b^c \left(\frac{bn+4}{n-1}\right)^c \xrightarrow{n\to\infty} b^c$;
$\frac{\alpha_{c+1}(bn+4)}{\alpha_{c+1}(n)} \geqslant \frac{(bn+3)^c}{n^c} = b^c \left(\frac{bn+3}{n}\right)^c \xrightarrow{n\to\infty} b^c$.

♦ **B 1.** $c = \left[\frac{a}{b^{k-1}}\right] \pmod{b^k}$

♦ **B 2.** a) $b = 2^n$, $a = (2^n+1)^n$
b)

♦ **B 3.** p — простое тогда и только тогда, когда $GCD(p, (p-1)!) = 1$

♦ **B 4.** $(x_0+1)(1 - D(x_0, x_1, \ldots, x_m)^2) - 1 \geqslant 0$ если и только если $1 - D(x_0, x_1, \ldots, x_m)^2 > 0$, т.е. $D(x_0, x_1, \ldots, x_m) = 0$. Поэтому $a = (x_0+1)(1-0) - 1 = x_0$.

♦ **B 5.** следует из двух предыдущих задач

♦ **B 6.** a) Первое слагаемое этой суммы равно числу множителей, делящихся на p, второе — на p^2 и так далее.

b) $\sum(\left[\frac{m+n}{p^k}\right] - \left[\frac{m}{p^k}\right] - \left[\frac{n}{p^k}\right])$ равна искомому числу.

♦ **B 7.** $\binom{x_n p^{n-1}+\ldots+x_1 p+x_0}{y_n p^{n-1}+\ldots+y_1 p+y_0}$ делится на p если и только если существует i, такое что $x_i < y_i$.

♦ **B 8.** $a < e \cdot \frac{p^n-1}{p-1}$

♦ **B 9.** $(y_n b_1^{n-1} + \ldots + y_1 b_1 + y_0) - (y_n b_2^{n-1} + \ldots + y_1 b_2 + y_0) \equiv 0 \pmod{b_2 - b_1}$

♦ **B 10.** $a_1 = a_2 \pmod{b_2 - b_1}$ (ибо $a_1 < b_1^n < b_2 - b_1$)