Решения

1. Существует ли возрастающая последовательность натуральных чисел $\{a_n\}_{n=1}^{\infty}$, такая что для всякого $k \in \mathbb{Z}$ последовательность $\{a_n + k\}_{n=1}^{\infty}$ содержит лишь конечное число простых чисел?

   Ответ: да, существует.

   Решение. Например, можно взять $a_n = (2n)! + n$, поскольку $a_n + k$ делится на $n + k > 1$ при $n > |k| + 1$ (и $a_n + k > n + k$).

   Другое решение. Можно взять $a_n = n!^3$. (Случай $k = 0$ тривиален. Если $|k| \geqslant 2$, то $a_n + k$ делится на k при $n \geqslant |k|$. Кроме того, $a_n \pm 1$ делится на $n! \pm 1$.)

   Третье решение. Для каждого $k \in \mathbb{Z}$ выберем составное натуральное число m_k, так чтобы все числа m_k были попарно взаимно просты (например, можно взять $m_0 = p_1 p_2$, $m_1 = p_3 p_4$, $m_{-1} = p_5 p_6$, $m_2 = p_7 p_8$, $m_{-2} = p_9 p_{10}$ и т. д., где p_k — k-е простое число).

   Обозначим $a_0 = 0$.

   Пусть $n \geqslant 1$, причём $a_0, a_1, \ldots, a_{n-1}$ уже определены. С помощью китайской теоремы об остатках построим $a_n > a_{n-1}$, удовлетворяющее системе сравнений

   $$a_n + k \equiv 0 \pmod{m_k}, \quad |k| \leqslant n.$$

   Полученная последовательность $\{a_n\}_{n=1}^{\infty}$ удовлетворяет условиям задачи, поскольку $a_n + k$ делится на m_k при $n \geqslant |k|$.

2. Рассмотрим последовательность $a_n = \lfloor \alpha^n \rfloor$, где $\alpha = 3 + \sqrt{5}$, $\lfloor x \rfloor$ — целая часть числа x. Докажите, что для всякого $n \in \mathbb{N}$ справедливо сравнение $a_n \equiv -1 \pmod{2^n}$.

   Решение. Рассмотрим последовательность

$$b_n = \left(\frac{3+\sqrt{5}}{2}\right)^n + \left(\frac{3-\sqrt{5}}{2}\right)^n.$$

   Она удовлетворяет рекуррентному соотношению

$$b_{n+2} - 3b_{n+1} + b_n = 0,$$

   причём $b_0 = 2$, $b_1 = 3$. Следовательно, $b_n \in \mathbb{Z}$ при всех n.

   Заметим, что

$$2^n b_n = \left(3+\sqrt{5}\right)^n + \left(3-\sqrt{5}\right)^n.$$

   Поскольку $0 < 3 - \sqrt{5} < 1$, получаем $a_n = 2^n b_n - 1$, откуда следует требуемое.

3. Найдите все целые числа x, y, такие что

$$\frac{x^2+x+2}{y^6-2} \in \mathbb{Z}.$$

Ответ: $y \in \{0, 1, -1\}$, x — любое.

Решение. Заметим, что при $y \in \{0, 1, -1\}$ сгодится любое x.

Пусть $|y| > 1$. Тогда $y^6 - 2 > 0$, причём $y^6 - 2 \equiv -1 \pmod 7$ или $y^6 - 2 \equiv -2 \pmod 7$.

Поскольку $\left(\frac{-1}{7}\right) = \left(\frac{-2}{7}\right) = -1$, то $\left(\frac{y^6-2}{7}\right) = -1$, поэтому $y^6 - 2$ имеет простой делитель p, такой что $\left(\frac{p}{7}\right) = -1$ (в частности, $p \neq 2$).

Но для таких p сравнение $x^2 + x + 2 \equiv 0 \pmod p$ неразрешимо, поскольку $p > 2$ и

$$\left(\frac{D}{p}\right) = \left(\frac{-7}{p}\right) = (-1)^{\frac{p-1}{2}+3\frac{p-1}{2}}\left(\frac{p}{7}\right) = \left(\frac{p}{7}\right) = -1.$$

Следовательно, для любых x значение дроби будет нецелым.

4. Пусть p — простое число, $n \in \mathbb{N}$, причём $p \mid \varphi(n)$ (где φ — функция Эйлера). Докажите, что количество натуральных чисел, не превосходящих n/p и взаимно простых с n, равно $\varphi(n)/p$.

   Решение. Поскольку $\varphi(n)$ делится на p, то либо n делится на p^2, либо n имеет простой делитель $q \equiv 1 \pmod{p}$.

   В первом случае выполнено

$$\text{н.о.д.}(a, n) = 1 \iff \text{н.о.д.}(a + n/p, n) = 1,$$

   поэтому каждый отрезок $[kn/p + 1, (k+1)n/p]$, $k = 0, 1, \ldots, p-1$, содержит одно и то же количество чисел, взаимно простых с n, откуда следует требуемое.

   Рассмотрим второй случай. Искомое количество равно

$$\sum_{k \leqslant n/p} \sum_{d \mid \text{н.о.д.}(k,n)} \mu(d) = \sum_{d \mid n} \sum_{\substack{k \leqslant n/p, \\ k \equiv 0 \pmod{d}}} \mu(d) = \sum_{d \mid n} \mu(d) \left\lfloor \frac{n/p}{d} \right\rfloor.$$

   Обозначим это количество через N. Тогда

$$\frac{\varphi(n)}{p} - N = \sum_{d \mid n} \mu(d) \left(\frac{n}{pd} - \left\lfloor \frac{n}{pd} \right\rfloor \right) = \sum_{d \mid n} \mu(d) \left\{ \frac{n}{pd} \right\}.$$

   Из-за присутствия функции Мёбиуса достаточно суммировать по бесквадратным d. Все такие делители можно разбить на пары вида d_1 и qd_1, где $d_1 \mid nq^{-\nu_q(n)}$. При этом выполнено $\mu(d_1) = -\mu(qd_1)$. Более того,

$$\frac{n}{pd_1} - \frac{n}{pqd_1} = \frac{n}{qd_1} \cdot \frac{q-1}{p} \in \mathbb{Z},$$

   откуда

$$\left\{ \frac{n}{pd_1} \right\} = \left\{ \frac{n}{pqd_1} \right\}.$$

   Следовательно, соответствующие слагаемые уничтожаются, поэтому сумма равна 0.

   Замечание. Аналогично можно доказать, что каждый промежуток $(kn/p, (k+1)n/p]$, $k = 0, 1, \ldots, p-1$, содержит $\varphi(n)/p$ чисел, взаимно простых с n.

5. Докажите, что уравнение
$$a^{ab} + 1 = c^{cd}$$
не имеет решений в натуральных числах a, b, c, d.

Решение. Предположим противное. Заметим, что $a > 1$, $c > 1$, н.о.д.$(a, c) = 1$.

Обозначим $N = a^{ab} + 1 = c^{cd}$. Тогда
$$a^{ab} \equiv -1 \pmod{N} \implies a^{2ab} \equiv 1 \pmod{N}.$$
Пусть $\delta = \operatorname{ord}_N a$. Тогда $\delta \mid 2ab$, причём $\delta > ab$, поскольку
$$a^{\delta} \geqslant N + 1 > a^{ab}.$$
Следовательно, $\delta = 2ab$ (поскольку $2ab/\delta \in \mathbb{N}$ и $2ab/\delta < 2$). При этом
$$\delta \mid \varphi(N) = \varphi\left(c^{cd}\right) = c^{cd-1}\,\varphi(c).$$
Поскольку н.о.д.$(a, c) = 1$, отсюда следует, что $a \mid \varphi(c)$, поэтому
$$a \leqslant \varphi(c) < c. \tag{1}$$
Аналогично, положим $M = c^{cd} - 1 = a^{ab}$, $\gamma = \operatorname{ord}_M c$. Поскольку $c^{cd} \equiv 1 \pmod{M}$ и $c^{\gamma} \geqslant M + 1 = c^{cd}$, то $\gamma = cd$. Следовательно,
$$c \mid \varphi(M) = a^{ab-1}\,\varphi(a),$$
откуда $c \mid \varphi(a)$, в частности $c < a$, что противоречит неравенству (1).

Замечание. Эта задача — частный случай знаменитой теоремы Михалеску (известной также как гипотеза Каталана), которая утверждает, что уравнение
$$x^u - y^v = 1$$
имеет единственное решение $3^2 - 2^3 = 1$ в натуральных числах x, y, u, v при условии, что $u > 1$ и $v > 1$.

6. Пусть A — целочисленная квадратная матрица, p — простое число.

а) Докажите, что справедливо сравнение

$$\mathrm{Tr}\big(A^p\big) \equiv \mathrm{Tr}(A) \pmod{p},$$

где $\mathrm{Tr}(M)$ — след матрицы M.

б) Докажите, что для всякого $n \in \mathbb{N}$ справедливо сравнение

$$\mathrm{Tr}\Big(A^{p^n}\Big) \equiv \mathrm{Tr}\Big(A^{p^{n-1}}\Big) \pmod{p^n}.$$

Решение. Пусть $\lambda_1, \lambda_2, \ldots, \lambda_m \in \mathbb{C}$ — собственные числа матрицы A (с учётом кратности), так что

$$(\lambda_1 - \lambda)(\lambda_2 - \lambda)\cdots(\lambda_m - \lambda) = \chi_A(\lambda) = \det(E - \lambda A) \in \mathbb{Z}[\lambda].$$

Тогда

$$\mathrm{Tr}\Big(A^d\Big) = \lambda_1^d + \lambda_2^d + \cdots + \lambda_m^d.$$

Таким образом, утверждение задачи является частным случаем следующей теоремы.

Теорема. *Допустим, что числа $\lambda_1, \ldots, \lambda_m \in \mathbb{C}$ удовлетворяют условию*

$$(x - \lambda_1)\cdots(x - \lambda_m) \in \mathbb{Z}[x]. \tag{2}$$

Далее, пусть $S(x_1, \ldots, x_m)$ — симметрический многочлен с целыми коэффициентами. Тогда для произвольного $d \in \mathbb{N}$ выполнено

$$S\Big(\lambda_1^d, \ldots, \lambda_m^d\Big) \in \mathbb{Z}.$$

Более того, если p — простое число, $n \in \mathbb{N}$, то справедливо сравнение

$$S\Big(\lambda_1^{p^n}, \ldots, \lambda_m^{p^n}\Big) \equiv S\Big(\lambda_1^{p^{n-1}}, \ldots, \lambda_m^{p^{n-1}}\Big) \pmod{p^n}.$$

Первое утверждение теоремы достаточно доказать для $d = 1$. По основной теореме о симметрических многочленах, найдётся многочлен $P(x_1, \ldots, x_m) \in \mathbb{Z}[x_1, \ldots, x_m]$, такой что

$$S(x_1, \ldots, x_m) = P(\sigma_1, \ldots, \sigma_m),$$

где $\sigma_k = \sigma_k(x_1, \ldots, x_m)$ — элементарные симметрические многочлены. Из теоремы Виета и условия (2) следует, что $\sigma_k(\lambda_1, \ldots, \lambda_m) \in \mathbb{Z}$, откуда получаем требуемое.

Второе утверждение теоремы будем доказывать индукцией по n.

Лемма 1. *Пусть p — простое число.*

1) Для любого $M \in \mathbb{N}$ выполняется сравнение

$$(y_1 + \cdots + y_M)^p \equiv y_1^p + \cdots + y_M^p \pmod{p},$$

то есть все коэффициенты многочлена $(y_1 + \cdots + y_M)^p - \big(y_1^p + \cdots + y_M^p\big)$ делятся на p.

2) Для любого многочлена $P(x_1, \ldots, x_m) \in \mathbb{Z}[x_1, \ldots, x_m]$ выполняется сравнение

$$(P(x_1, \ldots, x_m))^p \equiv P\big(x_1^p, \ldots, x_m^p\big) \pmod{p}.$$

Доказательство. Первое утверждение легко доказать индукцией по M (случай $M = 1$ тривиален; при $M = 2$ оно следует из того, что биномиальные коэффициенты $\binom{p}{k}$ делятся на p при $1 \leqslant k \leqslant p-1$).

Докажем второе утверждение. Пусть

$$P(x_1, \ldots, x_m) = \sum_{k_1,\ldots,k_m} c_{k_1,\ldots,k_m} x_1^{k_1} \cdots x_m^{k_m}.$$

Воспользуемся пунктом 1, взяв в качестве $y_1, \ldots, y_M$ одночлены $c_{k_1,\ldots,k_m} x_1^{k_1} \cdots x_m^{k_m}$.

Получим (сравнения по модулю p)

$$\begin{aligned}(P(x_1, \ldots, x_m))^p &\equiv \sum_{k_1,\ldots,k_m} c_{k_1,\ldots,k_m}^p x_1^{k_1 p} \cdots x_m^{k_m p} \\ &\equiv \sum_{k_1,\ldots,k_m} c_{k_1,\ldots,k_m} x_1^{k_1 p} \cdots x_m^{k_m p} = P\bigl(x_1^p, \ldots, x_m^p\bigr),\end{aligned}$$

где во втором сравнении мы применили малую теорему Ферма.

Лемма доказана. □

Таким образом, справедливо равенство

$$S\bigl(x_1^p, \ldots, x_m^p\bigr) = (S(x_1, \ldots, x_m))^p + pT(x_1, \ldots, x_m), \tag{3}$$

где $T(x_1, \ldots, x_m) \in \mathbb{Z}[x_1, \ldots, x_m]$, причём многочлен T симметрический.

Возьмём $x_j = \lambda_j$, $1 \leqslant j \leqslant m$. Поскольку $S(\lambda_1, \ldots, \lambda_m) \in \mathbb{Z}$ и $T(\lambda_1, \ldots, \lambda_m) \in \mathbb{Z}$, то

$$S\bigl(\lambda_1^p, \ldots, \lambda_m^p\bigr) \equiv (S(\lambda_1, \ldots, \lambda_m))^p \equiv S(\lambda_1, \ldots, \lambda_m) \pmod{p},$$

где мы снова применили малую теорему Ферма. Это доказывает второе утверждение теоремы при $n = 1$ (и одновременно пункт а задачи).

Предположим, что утверждение доказано для некоторого $n \in \mathbb{N}$ (и произвольного симметрического многочлена S). Тогда справедливы сравнения

$$\begin{aligned}S\left(\lambda_1^{p^n}, \ldots, \lambda_m^{p^n}\right) &\equiv S\left(\lambda_1^{p^{n-1}}, \ldots, \lambda_m^{p^{n-1}}\right) \pmod{p^n}, \\ T\left(\lambda_1^{p^n}, \ldots, \lambda_m^{p^n}\right) &\equiv T\left(\lambda_1^{p^{n-1}}, \ldots, \lambda_m^{p^{n-1}}\right) \pmod{p^n}.\end{aligned}$$

Отсюда получаем сравнения

$$\left(S\left(\lambda_1^{p^n}, \ldots, \lambda_m^{p^n}\right)\right)^p \equiv \left(S\left(\lambda_1^{p^{n-1}}, \ldots, \lambda_m^{p^{n-1}}\right)\right)^p \pmod{p^{n+1}}, \tag{4}$$

$$pT\left(\lambda_1^{p^n}, \ldots, \lambda_m^{p^n}\right) \equiv pT\left(\lambda_1^{p^{n-1}}, \ldots, \lambda_m^{p^{n-1}}\right) \pmod{p^{n+1}}, \tag{5}$$

где в (4) мы воспользовались следующим простым утверждением.

Лемма 2. *Пусть $a, b \in \mathbb{Z}$, $p, n \in \mathbb{N}$, причём $a \equiv b \pmod{p^n}$. Тогда $a^p \equiv b^p \pmod{p^{n+1}}$.* □

Складывая сравнения (4) и (5), с учётом равенства (3) получаем

$$S\left(\lambda_1^{p^{n+1}}, \ldots, \lambda_m^{p^{n+1}}\right) \equiv S\left(\lambda_1^{p^n}, \ldots, \lambda_m^{p^n}\right) \pmod{p^{n+1}}.$$

Таким образом, шаг индукции проверен и теорема доказана.