

# Number Theory. IMO

Данный листок содержит задачи по теории чисел, которые в разные годы предлагались на Международной математической олимпиаде (IMO). Для каждой задачи приведена последовательность шагов (Steps), ведущая к решению.

## 1 Делимость

### IMO Problems

**Problem 1.1.** (1998) Determine all pairs  $(a, b)$  of positive integers such that  $ab^2 + b + 7$  divides  $a^2b + a + b$ .

→ [Steps](#)

**Problem 1.2.** (1994) Determine all ordered pairs  $(m, n)$  of positive integers such that

$$\frac{n^3 + 1}{mn - 1}$$

is an integer.

→ [Steps](#)

**Problem 1.3.** (2003) Determine all pairs  $(a, b)$  of positive integers such that

$$\frac{a^2}{2ab^2 - b^3 + 1}$$

is a positive integer.

→ [Steps](#)

### Steps

**Problem 1.1.** Determine all pairs  $(a, b)$  of positive integers such that  $ab^2 + b + 7$  divides  $a^2b + a + b$ .

---

*Step 1.* Если  $ab^2 + b + 7 \mid a^2b + a + b$ , то  $ab^2 + b + 7 \mid b^2 - 7a$ .

*Step 2.* Случай  $b^2 - 7a > 0$  невозможен. Почему?

*Step 3.* Пусть  $b^2 - 7a = 0$ . Получите серию пар  $(7t^2, 7t)$ ,  $t \in \mathbb{N}$ .

*Step 4.* Пусть  $7a - b^2 > 0$ . Из условия  $ab^2 + b + 7 \mid 7a - b^2$  выведите  $b \leq 2$ .

*Step 5.* Исследуйте случаи  $b = 1$  и  $b = 2$ . Получатся ещё две пары.

ОТВЕТ:  $(11, 1)$ ;  $(49, 1)$ ;  $(7t^2, 7t)$ ,  $t \in \mathbb{N}$ .

\* \* \*

**Problem 1.2.** Determine all ordered pairs  $(m, n)$  of positive integers such that

$$\frac{n^3 + 1}{mn - 1}$$

is an integer.

---

*Step 1.* Заметьте, что  $mn - 1$  и  $m$  взаимно просты. Выведите отсюда, что число  $z = \frac{n^3+1}{mn-1}$  является целым тогда и только тогда, когда  $\frac{m^3+1}{mn-1}$  — целое (следовательно, имеется симметрия).

*Step 2.* Рассмотрите случаи  $n = 1$  и  $m = n$ , получив пять пар  $(m, n)$ . Далее полагаем  $m > n \geq 2$ .

*Step 3.* Объясните, почему должно быть  $z = nt - 1$ ,  $t \in \mathbb{Z}$ .

*Step 4.* Получите оценку  $z < n + \frac{1}{n-1} \leq 2n - 1$ . Найдите отсюда единственное  $t$  и ещё четыре пары  $(m, n)$ .

ОТВЕТ:  $(1, 2)$ ;  $(2, 1)$ ;  $(1, 3)$ ;  $(3, 1)$ ;  $(2, 2)$ ;  $(2, 5)$ ;  $(5, 2)$ ;  $(3, 5)$ ;  $(5, 3)$ .

\* \* \*

**Problem 1.3.** Determine all pairs  $(a, b)$  of positive integers such that

$$\frac{a^2}{2ab^2 - b^3 + 1}$$

is a positive integer.

---

*Step 1.* Начните со случая  $b = 1$  и получите серию  $(2t, 1)$ ,  $t \in \mathbb{N}$ . Далее  $b \geq 2$ .

*Step 2.* Из условия положительности числа  $z = \frac{a^2}{2ab^2 - b^3 + 1}$  выведите  $2a \geq b$ .

*Step 3.* Рассмотрите случай  $b = 2a$  и получите серию  $(t, 2t)$ . Далее  $2a > b$ .

*Step 4.* Из условий  $2a > b$  и  $z \in \mathbb{N}$  выведите  $a > b$ . Заметьте, что тогда из  $a \leq b$  следует  $a = b/2$ .

*Step 5.* Рассмотрите квадратное уравнение относительно  $a$  с параметрами  $b$  и  $z$ . Убедитесь, что оно имеет два положительных корня  $a_1$  и  $a_2$  ( $a_1 \leq a_2$ ).

*Step 6.* Покажите, что  $a_1 < b$ , откуда  $a_1 = b/2$ . Получите серию  $(8t^4 - t, 2t)$ .

ОТВЕТ:  $(2t, 1)$ ;  $(t, 2t)$ ;  $(8t^4 - t, 2t)$ ;  $t \in \mathbb{N}$ .

## 2 Принцип крайнего

Так называемый *принцип крайнего* заключается в рассмотрении «крайнего» объекта — скажем, наименьшего или наибольшего числа, обладающего заданным свойством. Часто встречающимся примером служит рассмотрение наименьшего простого делителя данного числа.

### IMO Problems

**Problem 2.1.** (1999) Determine all pairs  $(n, p)$  of positive integers such that

- $p$  is a prime,
- $n \leq 2p$ ,
- $(p - 1)^n + 1$  is divisible by  $n^{p-1}$ .

→ [Steps](#)

### Steps

**Problem 2.1.** Determine all pairs  $(n, p)$  of positive integers such that

- $p$  is a prime,
- $n \leq 2p$ ,
- $(p - 1)^n + 1$  is divisible by  $n^{p-1}$ .

---

*Step 1.* Рассмотрите очевидные случаи  $n = 1, 2$  и  $p = 2$ .

*Step 2.* Пусть  $p \geq 3$ . Тогда  $n \geq 3$  нечётно.

*Step 3.* Пусть  $q$  — наименьший простой делитель  $n$ . Покажите, что  $(p - 1)^n \equiv -1 \pmod{q}$ .

*Step 4.* Верно  $(p - 1)^{q-1} \equiv 1 \pmod{q}$ . Почему?

*Step 5.* Для некоторых целых  $x$  и  $y$  верно  $nx = (q - 1)y + 1$ . Почему?

*Step 6.* Из предыдущего шага выведите сравнение  $(p - 1)^{(q-1)y+1} \equiv -1 \pmod{q}$ . Заключите отсюда, что  $p = q$ .

*Step 7.* Тогда верно  $n = p$ . Почему?

*Step 8.* Имеем:  $p^{p-1} \mid (p - 1)^p + 1$ . Выведите отсюда  $p = 3$ .

ОТВЕТ:  $(2, 2)$ ;  $(3, 3)$ ;  $(1, p)$ , где  $p$  — простое число.

### 3 Lifting The Exponent Lemma

Для простого числа  $p$  и целого числа  $x$  обозначение  $\|x\|_p$  есть максимальная степень  $p$  (с целым неотрицательным показателем), на которую делится  $x$ :

$$\|x\|_p = \alpha \Leftrightarrow p^\alpha \mid x \text{ и } p^{\alpha+1} \nmid x.$$

В этом случае также используется обозначение  $p^\alpha \parallel x$ .

Очевидно, что  $\|x\|_p \geq 0$ . Случай  $x = 0$  здесь интереса не представляет, поэтому далее под знаком  $\|\cdot\|_p$  подразумеваются ненулевые целые числа.

1. (Формула Лежандра) Докажите, что

$$\|n!\|_p = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \dots$$

2. Докажите, что

$$\|C_n^k\|_p > \|n\|_p - \frac{k}{p-1}. \quad (1)$$

3. Пусть  $n$  нечётно и  $3^\alpha \parallel n$ . Докажите, что  $3^{\alpha+1} \parallel 2^n + 1$ . Сделайте это двумя способами:

- 1)  $2 = -1 + 3$ , бином Ньютона и оценка (1);
- 2) индукцией по  $\alpha$ , не используя бином Ньютона.

Утверждение задачи 3 является частным случаем так называемой *леммы о лифтинге* (в оригинале — **Lifting The Exponent Lemma**, сокращённо LTE), которая нередко фигурирует в олимпиадных задачах по теории чисел.

ТЕОРЕМА LTE-1. Пусть  $x$  и  $y$  — различные целые числа,  $p$  — нечётное простое число, не являющееся делителем  $x$  и  $y$  и такое, что  $p \mid x - y$ . Тогда для любого натурального  $n$  выполнено

$$\|x^n - y^n\|_p = \|x - y\|_p + \|n\|_p.$$

СЛЕДСТВИЕ 1. Пусть числа  $a \geq 2$ ,  $\alpha$  и  $n$  — натуральные,  $\beta \geq 0$  — целое,  $p \geq 3$  — простое. Если  $p^\alpha \parallel a - 1$  и  $p^\beta \parallel n$ , то  $p^{\alpha+\beta} \parallel a^n - 1$ .

*Примечание.* Почему «лифтинг»? В формулировке следствия 1 положим  $n = p^\beta$ . Тогда получим:  $p^\alpha p^\beta \parallel a^{p^\beta} - 1$ , т. е.  $p^\beta$  «отправляется наверх» в показатель степени.

ТЕОРЕМА LTE-2. Пусть  $x$  и  $y$  — различные целые числа,  $p$  — нечётное простое число, не являющееся делителем  $x$  и  $y$  и такое, что  $p \mid x + y$ . Тогда для любого нечётного натурального  $n$  выполнено

$$\|x^n + y^n\|_p = \|x + y\|_p + \|n\|_p.$$

СЛЕДСТВИЕ 2. Пусть числа  $a$ ,  $\alpha$ ,  $\beta \geq 0$  — целое,  $p \geq 3$  — простое. Если  $p^\alpha \parallel a + 1$  и  $p^\beta \parallel n$  для нечётного натурального  $n$ , то  $p^{\alpha+\beta} \parallel a^n + 1$ .

4. Докажите теоремы LTE-1 и LTE-2, используя биномиальную оценку (1).

Дополнительно потренироваться в подобных «биномиальных» доказательствах можно на примере следующих двух задач.

5. (Всеросс., 1996, финал, 9) Пусть натуральные числа  $x, y, p, n$  и  $k$  таковы, что  $x^n + y^n = p^k$ . Докажите, что если число  $n$  ( $n > 1$ ) нечётное, а число  $p$  нечётное простое, то  $n$  является степенью числа  $p$  (с натуральным показателем).

6. (Всеросс., 1996, финал, 10) Найдите все такие натуральные  $n$ , что при некоторых взаимно простых  $x$  и  $y$  и натуральном  $k, k > 1$ , выполняется равенство  $3^n = x^k + y^k$ .

$\boxed{z = u}$

В теоремах LTE-1 и LTE-2 существенную роль играет условие  $p \geq 3$ . Случай  $p = 2$  будет рассмотрен отдельно (Problem 3.3).

## IMO Problems

**Problem 3.1.** (1990) Determine all integers  $n > 1$  such that  $\frac{2^n + 1}{n^2}$  is an integer.

→ [Steps](#)

**Problem 3.2.** (1997, Short List) Let  $b, m, n$  be positive integers such that  $b > 1$  and  $m \neq n$ . Prove that if  $b^m - 1$  and  $b^n - 1$  have the same prime divisors, then  $b + 1$  is a power of 2.

→ [Steps](#)

**Problem 3.3.** (1989, Short List) Let  $m$  be a positive odd integer,  $m \geq 3$ . Find the smallest positive integer  $n$  such that  $2^{1989}$  divides  $m^n - 1$ .

→ [Steps](#)

**Problem 3.4.** (1991, Short List) Find the highest degree  $k$  of 1991 for which  $1991^k$  divides the number

$$1990^{1991^{1992}} + 1992^{1991^{1990}}.$$

→ [Steps](#)

**Problem 3.5.** (2014, Short List) Find all triples  $(p, x, y)$  consisting of a prime number  $p$  and two positive integers  $x$  and  $y$  such that  $x^{p-1} + y$  and  $x + y^{p-1}$  are both powers of  $p$ .

→ [Steps](#)

## Steps

**Problem 3.1.** Determine all integers  $n > 1$  such that  $\frac{2^n + 1}{n^2}$  is an integer.

---

### Первое решение

*Step 1.* Через  $(a, b)$  обозначаем наибольший общий делитель целых чисел  $a$  и  $b$ . Пусть  $a > b$ . Докажите, что  $(a, b) = (a - b, b)$ . Объясните, как работает алгоритм Евклида нахождения НОД.

*Step 2.* Пусть  $a > 1, m, n$  — натуральные числа. Докажите, что  $(a^m - 1, a^n - 1) = a^{(m, n)} - 1$ .

Step 3. Докажите малую теорему Ферма: если  $a$  не делится на простое число  $p$ , то

$$a^{p-1} \equiv 1 \pmod{p}.$$

Рассмотрите остатки от деления  $a, 2a, \dots, (p-1)a$

Step 4. Пусть  $n$  нечётно и  $p$  — наименьший простой делитель  $n$ . Найдите  $(2n, p-1)$ .

Step 5. Пусть  $2^n + 1$  делится на  $n$ . Комбинируя результаты шагов 2–4, докажите, что наименьший простой делитель  $n$  равен 3.

Step 6. Пусть  $2^n + 1$  делится на  $n^2$ . С помощью LTE докажите, что  $3 \parallel n$ .

Step 7. Пусть  $2^n + 1$  делится на  $m$ , причём  $m > 1$  и  $3 \nmid m$ . Докажите, что наименьший простой делитель числа  $m$  равен 7.

Step 8. Какие остатки может давать степень двойки при делении на 7?

ОТВЕТ:  $n = 3$ .

## Второе решение

ОПРЕДЕЛЕНИЕ. Функция Эйлера  $\varphi(n)$  натурального числа  $n$  есть количество натуральных чисел, меньших  $n$  и взаимно простых с  $n$ .

Step 1. Для простого числа  $p$  найдите: а)  $\varphi(p)$ ; б)  $\varphi(p^k)$ , где  $k \in \mathbb{N}$ .

$$1 - \varphi^d - \varphi^d (9 : 1 - d (e$$

Step 2. Докажите теорему Эйлера: если  $a$  и  $m$  взаимно просты, то  $a^{\varphi(m)} \equiv 1 \pmod{m}$ .

ОПРЕДЕЛЕНИЕ. Пусть  $a$  и  $m$  взаимно просты. *Порядком* числа  $a$  по модулю  $m$  называется наименьшее натуральное  $r$ , для которого  $a^r \equiv 1 \pmod{m}$ .

Step 3. Покажите, что если  $a^s \equiv 1 \pmod{m}$ , то  $r \mid s$ . В частности,  $r \mid \varphi(m)$ .

Step 4. Предположим, что  $2^n + 1$  делится на  $n$ . Пусть  $p$  — наименьший простой делитель  $n$ . Обозначим  $r$  порядок 2 по модулю  $p$ . Покажите, что  $r \mid 2n$ . Выведите отсюда, что  $r = 2$  и  $p = 3$ .

ОПРЕДЕЛЕНИЕ. Число  $a$ , взаимно простое с  $m$ , называется *первообразным корнем* по модулю  $m$ , если порядок  $a$  по модулю  $m$  равен  $\varphi(m)$ .

Step 5. Докажите, что 2 — первообразный корень по модулю  $3^n$  для любого  $n \in \mathbb{N}$ .

Step 6. Пользуясь предыдущим утверждением, докажите, что если  $2^n \equiv -1 \pmod{3^{k+1}}$ , то  $3^k \mid n$ . Выведите отсюда, что если  $2^n + 1$  делится на  $n^2$  и  $3^k \parallel n$ , то  $k \leq 1$ .

Step 7. Предположим, что  $n$  имеет простой делитель, больший 3. Пусть  $q$  — наименьший такой делитель, и пусть  $r$  — порядок 2 по модулю  $q$ . Снова убедитесь, что  $r \mid 2n$ . Предположив, что  $r$

нечётно, придите к противоречию.

*Step 8.* Пусть  $r$  чётно. Покажите, что тогда  $r = 2$  или  $r = 6$ . Выведите отсюда, что  $q = 7$ . А чему равен порядок 2 по модулю 7?

\* \* \*

**Problem 3.2.** Let  $b, m, n$  be positive integers such that  $b > 1$  and  $m \neq n$ . Prove that if  $b^m - 1$  and  $b^n - 1$  have the same prime divisors, then  $b + 1$  is a power of 2.

---

*Step 1.* Для натуральных чисел  $x$  и  $y$  обозначаем  $x \sim y$ , если  $x$  и  $y$  имеют одинаковые простые делители. Убедитесь, что:

- а) это отношение эквивалентности;
- б) если  $x \sim y$ , то  $x \sim (x, y)$ .

*Step 2.* Пусть  $d = (m, n)$ . Положим  $k = m/d$  и  $a = b^d$ . Покажите, что отношение  $b^m - 1 \sim b^n - 1$  равносильно отношению  $a^k - 1 \sim a - 1$ .

*Step 3.* В предположении, что  $a + 1$  есть степень двойки, покажите, что  $b + 1$  есть также степень двойки.

*Step 4.* Пусть  $a^k - 1 \sim a - 1$  и  $r \mid k$ . Покажите, что  $a^r - 1 \sim a - 1$ .

*Step 5.* Пусть  $p \geq 3$  — простой делитель числа  $k$  и  $p^\beta \parallel k$ . Обозначим  $S = 1 + a + a^2 + \dots + a^{p^\beta - 1}$ . Покажите, что каждый простой делитель числа  $S$  делит  $a - 1$ . Выведите отсюда, что  $S$  является степенью  $p$ .

*Step 6.* Коль скоро  $p \mid a - 1$ , положим  $p^\alpha \parallel a - 1$ . С помощью леммы о лифтинге покажите, что  $S = p^\beta$ . Это противоречие. Почему?

*Step 7.* Противоречие порождено предположением, что  $p \geq 3$  — простой делитель числа  $k$ . Следовательно,  $k$  есть степень двойки. Выведите отсюда, что  $a + 1$  также является степенью двойки.

\* \* \*

**Problem 3.3.** Let  $m$  be a positive odd integer,  $m \geq 3$ . Find the smallest positive integer  $n$  such that  $2^{1989}$  divides  $m^n - 1$ .

---

*Step 1.* Проанализируйте доказательство теоремы LTE-1. Где используется требование  $p \geq 3$  и почему не проходит доказательство для  $p = 2$ ?

Ситуацию можно поправить, усилив условие теоремы.

**ТЕОРЕМА LTE-3.** Пусть  $x$  и  $y$  — различные нечётные числа и  $4 \mid x - y$ . Тогда для любого натурального  $n$  выполнено

$$\|x^n - y^n\|_2 = \|x - y\|_2 + \|n\|_2.$$

СЛЕДСТВИЕ 3. Если  $2^\alpha \parallel m - 1$  при  $\alpha \geq 2$  и  $2^\beta \parallel n$ , то  $2^{\alpha+\beta} \parallel m^n - 1$ .

*Step 2.* Следствие 3 ничего не говорит нам о случае  $m \equiv -1 \pmod{4}$ . Но на самом деле имеется более сильное утверждение: если  $2^{\alpha+1} \parallel m^2 - 1$  и  $2^\beta \parallel n$ , то  $2^{\alpha+\beta} \parallel m^n - 1$ . Его мы и будем доказывать.

*Step 3.* Пусть  $n = 2^\beta k$ , где  $k$  нечётно. Покажите, что  $m^n - 1$  и  $m^{2^\beta} - 1$  делятся на одну и ту же степень двойки.

*Step 4.* Раскладывая  $m^{2^\beta} - 1$  на множители (несколько раз применяя формулу разности квадратов), покажите, что  $2^{\alpha+\beta} \parallel m^{2^\beta} - 1$  и тем самым  $2^{\alpha+\beta} \parallel m^n - 1$ .

ОТВЕТ: если  $\alpha < 1988$ , то  $n = 2^{1988-\alpha}$ ; иначе  $n = 1$ .

\* \* \*

**Problem 3.4.** Find the highest degree  $k$  of 1991 for which  $1991^k$  divides the number

$$1990^{1991^{1992}} + 1992^{1991^{1990}}.$$

---

*Step 1.* Пусть  $a \geq 3$  нечётно и  $n$  — целое. Докажите, что  $a^{n+1} \parallel (a+1)^{a^n} - 1$  и  $a^{n+1} \parallel (a-1)^{a^n} + 1$ .

ОТВЕТ:  $k = 1993$ .

\* \* \*

**Problem 3.5.** Find all triples  $(p, x, y)$  consisting of a prime number  $p$  and two positive integers  $x$  and  $y$  such that  $x^{p-1} + y$  and  $x + y^{p-1}$  are both powers of  $p$ .

---

*Step 1.* Случай  $p = 2$  тривиален. Каков будет ответ? Далее полагаем  $p \geq 3$ .

*Step 2.* Покажите, что  $x = y$  невозможно. Покажите также, что  $p \mid x$  невозможно.

*Step 3.* Полагаем  $x < y$  и  $p \nmid x$ . Пусть  $x^{p-1} + y = p^a$  и  $x + y^{p-1} = p^b$ . Покажите, что  $p^a \mid y^p - x^p$  и  $p^{a-1} \mid y - x$ . Пусть  $y = x + p^{a-1}q$ .

*Step 4.* Рассмотрев произведение  $x(x^{p-2} + 1)$ , докажите, что  $x \mid p - q$ .

*Step 5.* Из  $p^b = x + (p^a - x^{p-1})^{p-1}$  выведите, что  $p^a \mid 1 + x^{p(p-2)}$ . С помощью малой теоремы Ферма покажите теперь, что  $x \equiv -1 \pmod{p}$ .

*Step 6.* Из условий  $x \mid p - q$  и  $p \mid x + 1$  выведите, что  $q = 1$  и  $x = p - 1$  (и тогда  $y = p - 1 + p^{a-1}$ ).

*Step 7.* Покажите, что  $a = 2$  и  $p = 3$ .

ОТВЕТ:  $(3, 2, 5)$ ;  $(3, 5, 2)$ ;  $(2, n, 2^k - n)$  при  $0 < n < 2^k$ .

## 4 Китайская теорема об остатках

### IMO Problems

**Problem 4.1.** (2000, Short List) Determine all positive integers  $n \geq 2$  that satisfy the following condition: for all integers  $a, b$  relatively prime to  $n$ ,

$$a \equiv b \pmod{n} \text{ if and only if } ab \equiv 1 \pmod{n}.$$

→ [Steps](#)

**Problem 4.2.** (1992, Short List) Does there exist a set  $M$  with the following properties?

- (i) The set  $M$  consists of 1992 natural numbers.
- (ii) Every element in  $M$  and the sum of any number of elements have the form  $m^k$  ( $m, k \in \mathbb{N}$ ,  $k \geq 2$ ).

→ [Steps](#)

### Steps

**Problem 4.1.** Determine all positive integers  $n \geq 2$  that satisfy the following condition: for all integers  $a, b$  relatively prime to  $n$ ,

$$a \equiv b \pmod{n} \text{ if and only if } ab \equiv 1 \pmod{n}.$$

*Step 1.* Объясните, почему условие (condition) эквивалентно условию  $a^2 \equiv 1 \pmod{n}$  для всех целых  $a$ , взаимно простых с  $n$ .

*Step 2.* Это, в свою очередь, эквивалентно системе (для любого  $a$ , взаимно простого с  $n$ )

$$a^2 \equiv 1 \pmod{p_1^{e_1}}, \quad a^2 \equiv 1 \pmod{p_2^{e_2}}, \quad \dots, \quad a^2 \equiv 1 \pmod{p_s^{e_s}},$$

где  $n = p_1^{e_1} p_2^{e_2} \dots p_s^{e_s}$  — разложение  $n$  на простые множители.

*Step 3.* Если  $p_i \geq 3$ , то берём  $a = 2$  и с необходимостью заключаем, что  $p_i = 3$  и  $e_i = 1$ .

*Step 4.* Если  $p_i = 2$ , то берём  $a = 3$  и с необходимостью заключаем, что  $e_i \leq 3$ .

*Step 5.* Убеждаемся, что все делители 24 годятся.

ОТВЕТ: все делители числа 24.

\* \* \*

**Problem 4.2.** Does there exist a set  $M$  with the following properties?

(i) The set  $M$  consists of 1992 natural numbers.

(ii) Every element in  $M$  and the sum of any number of elements have the form  $m^k$  ( $m, k \in \mathbb{N}$ ,  $k \geq 2$ ).

---

*Step 1.* Для любого натурального  $n$  пусть  $p_1, p_2, \dots, p_n$  — различные простые числа. Рассмотрим число  $a = 2^{p_1 e_2} 3^{p_1 e_3} \dots n^{p_1 e_n}$  с некоторыми целыми неотрицательными  $e_2, e_3, \dots, e_n$  (оно имеет вид  $m^{p_1}$ ).

*Step 2.* Подберём  $e_2$  как решение системы сравнений

$$p_1 e_2 \equiv -1 \pmod{p_2}, \quad p_1 e_2 \equiv 0 \pmod{p_3}, \quad \dots, \quad p_1 e_2 \equiv 0 \pmod{p_n}$$

(почему это возможно?).

*Step 3.* Подберём  $e_3, \dots, e_n$  как решения систем

$$\begin{aligned} p_1 e_3 &\equiv 0 \pmod{p_2}, & p_1 e_3 &\equiv -1 \pmod{p_3}, & \dots, & p_1 e_3 &\equiv 0 \pmod{p_n}; \\ &\dots & & & & & \\ p_1 e_n &\equiv 0 \pmod{p_2}, & p_1 e_n &\equiv 0 \pmod{p_3}, & \dots, & p_1 e_n &\equiv -1 \pmod{p_n}. \end{aligned}$$

*Step 4.* Тогда оказывается, что  $2a$  есть  $p_2$ -я степень целого числа,  $3a$  —  $p_3$ -я степень,  $\dots$ ,  $na$  —  $p_n$ -я степень.

*Step 5.* Возьмите  $M = \{a, 2a, \dots, 1992a\}$  и  $n = 1992 \cdot 1993/2$ .

ОТВЕТ: существует.

## 5 Уравнения в целых числах

### IMO Problems

**Problem 5.1.** (2006) Determine all pairs  $(x, y)$  of integers such that

$$1 + 2^x + 2^{2x+1} = y^2.$$

→ [Steps](#)

**Problem 5.2.** (1997) Find all pairs  $(a, b)$  of integers  $a, b \geq 1$  that satisfy the equation

$$a^{b^2} = b^a.$$

→ [Steps](#)

### Steps

**Problem 5.1.** Determine all pairs  $(x, y)$  of integers such that

$$1 + 2^x + 2^{2x+1} = y^2.$$

---

*Step 1.* Покажите, что  $x < 0$  невозможно.

*Step 2.* Непосредственно проверьте  $x = 0, 1, 2$  (две пары решений). Далее  $x \geq 3$  и  $y > 0$ .

*Step 3.* Запишите уравнение в виде  $(y - 1)(y + 1) = 2^x(1 + 2^{x+1})$ .

*Step 4.* Одно из чисел  $y \pm 1$  делится на 2, но не на 4, а второе — на  $2^{x-1}$ , но не на  $2^x$ .

*Step 5.* Пусть  $y - 1 = 2^{x-1}m$ , где  $m$  нечётно. Получите соотношение  $2^{x-2}(m^2 - 8) = 1 - m$ . Есть решения?

*Step 6.* Аналогично, пусть  $y + 1 = 2^{x-1}m$ . Получите ещё две пары решений.

ОТВЕТ:  $(0, \pm 2); (4, \pm 23)$ .

\* \* \*

**Problem 5.2.** Find all pairs  $(a, b)$  of integers  $a, b \geq 1$  that satisfy the equation

$$a^{b^2} = b^a.$$

---

*Step 1.* Пусть  $a = p_1^{\alpha_1} \dots p_s^{\alpha_s}$  и  $b = p_1^{\beta_1} \dots p_s^{\beta_s}$  с простыми  $p_1, \dots, p_s$ . Покажите, что  $\frac{\alpha_i}{\beta_i} = \frac{a}{b^2} = \frac{m}{n}$  для некоторых взаимно простых  $m$  и  $n$ . Выведите отсюда, что  $a$  и  $b$  являются степенями одного целого числа:  $a = c^m, b = c^n$ .

*Step 2.* Получите решение для  $c = 1$ . Далее  $c \geq 2$ .

*Step 3.* Выведите уравнение  $mc^{2n} = nc^m$ .

*Step 4.* Пусть  $m > n$ , откуда  $m > 2n$ . Обозначаем  $d = m - 2n$ . Выведите  $d = n(c^d - 2)$ .

*Step 5.* Докажите, что  $c^d - 2 > d$  при  $d \geq 3$ .

*Step 6.* Следовательно,  $d \leq 2$ . Получите два решения.

*Step 7.* Пусть теперь  $m < n$ . Действуя аналогично, покажите, что решений нет.

ОТВЕТ:  $(1, 1)$ ;  $(16, 2)$ ;  $(27, 3)$ .