ПРостой стрим. Теория чисел. 12 часов с ДА. Сравнения по модулю

25 октября

Определение 1. Число a делится на натуральное b с остатком r, если $a = bk + r$, причем $0 \leqslant r < b$.

Определение 2. Целые числа, разность которых делится на m, называются *сравнимыми по модулю* m. Запись: $a \equiv b \pmod{m}$.

Свойства сравнений.

- $a \equiv b \pmod{m} \Leftrightarrow$ числа a и b дают одинаковые остатки по модулю m.
- $a \equiv b \pmod{m} \Rightarrow ka \equiv kb \pmod{m}$.
- $a \equiv b \pmod{m}$, $c \equiv d \pmod{m} \Rightarrow a \pm c \equiv b \pm d \pmod{m}$.
- $a \equiv b \pmod{m}$, $c \equiv d \pmod{m} \Rightarrow ac \equiv bd \pmod{m}$.
- $a \equiv b \pmod{m} \Rightarrow a^k \equiv b^k \pmod{m}$.

1. Докажите, что число $1000 \times 1001 \times 1002 \times 1003 - 24$ делится

(a) на 999;

(b) на 1004.

2. Найдите остаток от деления:

(a) 4^{2018} на 3; **(b)** 6^{2017} на 7; **(c)** 13^{555} на 9.

3. Известно, что $a - 2b$ делится на m и $c - 3d$ делится на m. Докажите, что $ac - 6bd$ делится на m.

4. Какой остаток дает $x + y$ при делении на 17, если

(a) $x - 16y \equiv 2 \pmod{17}$;

(b) $3x \equiv 5 + 14y \pmod{17}$?

5. Докажите, что если при некоторых натуральных числах a и b сумма $a^2 + b^2 \vdots 7$, то она делится и на 49.

6. Дано простое число p и его некоторый ненулевой остаток a.

(a) Докажите, что в последовательности $0 \cdot a, 1 \cdot a, 2 \cdot a, \ldots, (p-1) \cdot a$ все числа дают разные остатки по модулю p.

(b) Докажите, что существует и при том единственный обратный остаток b.

(c) Какие остатки совпадают со своими обратными остатками?

7. Преобразуем сумму $\frac{1}{1} + \frac{1}{2} + \ldots + \frac{1}{100}$ в дробь $\frac{m}{n}$. Докажите, что m делится на 101.

8. Докажите, что

(a) число $9^{2015} + 7^{2016}$ делится на 10;

(b) $5^{70} + 6^{70}$ делится на 61.

9. Теорема Вильсона. Пусть p — некоторое простое число. Докажите, что

$$(p-1)! \equiv -1 \pmod{p}.$$

10. Про натуральные числа a, b, c известно, что $a^2 + b^2 = c^2$. Докажите, что abc делится на 60.

11. Докажите, что число $5^{2016} + 28$ — составное.

12. Докажите, что если $2^k - 1$ делится на 11, то оно делится и на 31.

ПРостой стрим. Теория чисел. 12 часов с ДА. Функция Эйлера

25 октября

Упр. 1. Рассмотрим сравнение $ak \equiv bk \pmod m$. При каком условии на k и m из этого следует, что $a \equiv b \pmod m$?

Определение 3. Значение *функции Эйлера* $\varphi(m)$ равно количеству натуральных чисел, не превосходящих m и взаимно простых с m.

Упр. 2. Чему равно $\varphi(p^k)$ при простом p?

Замечание. Функция Эйлера *мультипликативна*, то есть при взаимно простых a и b выполнено $\varphi(a)\varphi(b) = \varphi(ab)$. Это позволяет вывести для нее явную формулу, зная разложение числа на простые множители.

Теорема. Пусть $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, где p_i — различные простые числа. Тогда

$$\varphi(m) = m\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\dots\left(1 - \frac{1}{p_k}\right).$$

Теорема Эйлера. Если НОД$(a, m) = 1$, то $a^{\varphi(m)} \equiv 1 \pmod m$.

Доказывается эта теорема, например, через *приведенную систему вычетов*.

1. Докажите, что при $m > 2$ число $\varphi(m)$ четно.

2. Докажите, что к числу 2^{2018} можно приписать слева несколько цифр так, чтобы снова получилась степень двойки.

3. Найдите три последние цифры числа $2008^{2007^{\dots^{2^1}}}$.

4. Для скольких значений числа i, где $1 \leqslant i \leqslant 1000$, существует число j, $1 \leqslant j \leqslant 1000$, такое, что $2^j - 1$ делится на i?

5. Докажите, что для любого натурального числа n найдется число с суммой цифр, равной n, делящееся на n.

6. Дано натуральное $n \geqslant 3$. Докажите, что число

$$n^{n^{n^n}} - n^{n^n}$$

делится на 1989.

7. Дано простое число $p = 3k + 2$. Докажите, что сравнение $y^2 - x^3 \equiv 1 \pmod p$ имеет не более p решений по модулю p.

8. Докажите, что $2^{2^{\dots^2}} - 2^{2^{\dots^2}}$ (в первом слагаемом n двоек, во втором — $n - 1$) делится на все числа от 1 до n.

9. Найдите наименьшее простое p такое, что $2^{120!} - 1$ делится на p, но не делится на p^2.

10. Даны натуральные a и b. Известно, что для любого натурального n число $a^n + n$ делится на $b^n + n$. Докажите, что $a = b$.

ПРостой стрим. Теория чисел. 12 часов с ДА. КТО это начал?

25 октября

1. Докажите, что для взаимно простых чисел a и b и любой пары остатков $n < a$ и $k < b$ найдется число c такое, что при делении на a число c даёт в остатке n, а при делении на b даёт в остатке k.

2. Генерал построил солдат в колонну по 4, но при этом солдат Иванов остался лишним. Тогда генерал построил солдат в колонну по 5. И снова Иванов остался лишним. Когда же и в колонне по 6 Иванов оказался лишним, генерал посулил ему наряд вне очереди, после чего в колонне по 7 Иванов нашел себе место и никого лишнего не осталось. Какое наименьшее число солдат могло быть у генерала?

3. Найдите наименьшее натуральное число, дающее остаток 2 при делении на 3, остаток 3 при делении на 4, остаток 4 при делении на 5, остаток 5 при делении на 6 и остаток 6 при делении на 7.

4. Диме выдали натуральное число N. Он разделил его на 101 и получил в остатке $m > 0$. Затем Дима разделил N на m и получил в остатке p. Найдите наибольшее значение p, которое могло получиться, а затем — наименьшее N, при котором это значение p достигается.

5. (a) Сколько четырёхзначных чисел подходит под условие $x^2 \equiv x \pmod{10000}$?

(b) Сколько чисел от 1 до n подходит под условие $x^2 \equiv x \pmod{n}$?

6. Числа a и b взаимно просты. Докажите, что любую правильную дробь со знаменателем ab можно получить как алгебраическую сумму двух правильных дробей со знаменателями a и b (иначе говоря, для любого натурального $k < ab$ найдутся такие целые неотрицательные $m < a$ и $n < b$, что $\frac{k}{ab} = \pm\frac{m}{a} \pm \frac{n}{b}$).

7. Пятнадцать простых чисел образуют возрастающую арифметическую прогрессию с разностью d. Докажите, что $d > 30000$.

8. Докажите, что натуральные n, для которых $n^n + 1$ делится на 30, образуют арифметическую прогрессию.

ПРостой стрим. Теория чисел. 12 часов с ДА. КТО это закончит?

25 октября

1. Китайская теорема об остатках. Пусть числа $m_1, m_2, \ldots, m_n$ попарно взаимно просты. Тогда для любых целых $a_1, a_2, \ldots, a_n$ найдется целое число x такое, что $x \equiv a_i \pmod{m_i}$ для всех i. Более того, x определен однозначно с точностью до прибавления кратного $M = m_1 m_2 \ldots m_n$.

2. Существует ли такое целое n кратное 4, что $n + 4$ кратно 9, а $n + 9$ кратно 25?

3. (a) Сколько четырёхзначных чисел подходит под условие $x^2 \equiv x \pmod{10000}$?

(b) Сколько чисел от 1 до n подходит под условие $x^2 \equiv x \pmod{n}$?

4. Докажите, что для каждого натурального n существуют натуральные a и b такие, что $4a^2 + 9b^2 - 1$ делится на n.

5. Докажите, что для каждого натурального n существуют n попарно взаимно простых чисел k_1, k_2, …, k_n, больших 1, таких, что число $k_1 k_2 \ldots k_n - 1$ представляется как произведение двух последовательных натуральных чисел.

6. *Полезное следствие.* Докажите, что для любых попарно взаимно простых чисел $m_1, m_2, \ldots, m_n$ и остатков $r_1, r_2, \ldots, r_n$ по модулям $m_1, m_2, \ldots, m_n$ найдутся n последовательных чисел $a + 1, a + 2, \ldots, a + n$ таких, что $a + i \equiv r_i \pmod{m_i}$.

7. Назовем число *хорошим*, если оно делится на квадрат натурального числа > 1. При каких N найдется N последовательных хороших чисел? (Пример для $N = 3$: 48, 49, 50).

8. Докажите, что найдутся 1000 последовательных чисел, каждое из которых не является

(a) простым числом или степенью простого числа;

(b) степенью (не ниже второй) натурального числа.

9. Найдите все натуральные $n > 1$, для которых любое целое число можно представить в виде суммы двух целых чисел, каждое из которых взаимно просто с n.

10. Докажите, что найдутся 2016 последовательных натуральных чисел, каждое из которых имеет не менее трех различных простых делителей.

11. Докажите, что числа натурального ряда можно переставить местами так, чтобы для всех n сумма n первых чисел делилась на n.

ПРостой стрим. Теория чисел. 12 часов с ДА. Показатели

25 октября

Определение 4. Пусть НОД$(a, m) = 1$. *Показателем* числа a по модулю m называется наименьшее натуральное d такое, что $a^d \equiv 1 \pmod m$.

Обозначение $\operatorname{ord}_m a$ происходит от английского слова *order*.

Упр. 3. Докажите, что показатель существует.

Упр. 4. Пусть $\operatorname{ord}_m a = d$. Докажите, что тогда

(a) числа $a, a^2, \ldots, a^d$ попарно не сравнимы по модулю m;

(b) $a^{d_1} \equiv a^{d_2} \pmod m$ тогда и только тогда, когда $d_1 \equiv d_2 \pmod d$;

(c) d является делителем числа $\varphi(m)$.

Упр. 5. Найдите $\operatorname{ord}_{a^n-1}(a)$.

Упр. 6. Докажите, что если для натурального k выполнено $a^k \equiv 1 \pmod m$, то $k \vdots \operatorname{ord}_m a$.

1. Докажите, что показатели взаимно обратных чисел совпадают.

2. Пусть $\operatorname{ord}_m a = d$. Докажите, что тогда

(a) если $d \vdots h$, то показатель числа a^h по модулю m равен $\frac{d}{h}$;

(b) если k является показателем числа b по модулю m и НОД$(k, d) = 1$, то dk является показателем числа ab по модулю m.

3. Рассмотрим все числа вида $10^i - 10^j$ при $0 \leqslant i < j \leqslant 99$. Сколько из них делятся на 1001?

4. Дано нечетное простое число p, а также простые числа q и r. Известно, что $q^r + 1 \vdots p$. Докажите, что либо $p - 1 \vdots 2r$, либо $q^2 - 1 \vdots p$.

5. Сколько делителей от 1 до 200 имеет число $2^{239} - 1$?

6. Пусть N — произведение первых ста простых чисел. Сравнимо ли 2^N с единицей по модулю 17?

7. Дано простое число p. Докажите, что $2^{2^p} - 4$ делится на $2^p - 1$.

8. Даны натуральные числа $a, n > 1$. Докажите, что для каждого нечетного простого делителя p числа $a^{2^n} + 1$ число $p - 1$ делится на 2^{n+1}.

9. Докажите, что при натуральном $n > 1$ число $2^n - 1$ не делится на n.

10. Найдите все пары простых чисел p и q таких, что $(5^p - 2^p)(5^q - 2^q) \vdots pq$.

---

11. Докажите, что для всех натуральных $a, n > 1$ выполнено $\varphi(a^n - 1) \vdots n$.

12. Даны натуральные числа a и b, взаимно простые с числом m. При этом оказалось, что $a^x \equiv b^x \pmod m$ и $a^y \equiv b^y \pmod m$. Докажите, что $a^{\text{НОД}(x,y)} \equiv b^{\text{НОД}(x,y)} \pmod m$.

13. Даны взаимно простые числа a и b. Докажите, что для любого нечетного делителя d числа $a^{2^n} + b^{2^n}$ выполнено $d - 1 \vdots 2^{n+1}$.

14. Докажите, что для натурального $n > 1$ число $2^{n-1} + 1$ не делится на n.

15. Найдите все упорядоченные тройки простых чисел (p, q, r) таких, что

$$p^q + 1 \vdots r, q^r + 1 \vdots p, r^p + 1 \vdots q.$$

16. Найдите все пары простых чисел p и q таких, что $5^p + 5^q \vdots pq$.

17. Найдите наименьшее n такое, что $17^n - 1$ делится на 2^{2005}.

18. Дано число $p = 2^n + 1$, где $n \geqslant 2$. Докажите, что если $3^{(p-1)/2} + 1 \vdots p$, то число p — простое.

ПРостой стрим. Теория чисел. 12 часов с ДА. Квадратичные вычеты

25 октября

Попробуем решить сравнение $x^2 \equiv 2 \pmod 7$. Операции извлечения корня как таковой при работе над сравнениями у нас нет, поэтому просто подберем корень $x \equiv 3$.

Определение 5. Говорят, что число a является *квадратичным вычетом* по модулю m, если a взаимно просто с m и существует корень сравнения $x^2 \equiv a \pmod m$.

Упр. 7. Легко видеть, что у изначального сравнения $x^2 \equiv 2 \pmod 7$ есть принципиально два различных корня: 3 и -3. И это вполне оправдывает наши ожидания, что квадратный трехчлен имеет не более двух корней. А всегда ли это так?

Далее везде p — *нечетное* простое число, a обычно не делится на p.

Упр. 8. Квадратичные вычеты — квадраты обычных вычетов, поэтому все они получаются при возведении приведенной системы вычетов в квадрат. Сколько принципиально различных чисел мы получим, другими словами, сколько существует квадратичных вычетов по модулю p?

Определение 6. Вычет, не являющийся квадратичным по модулю p и не делящийся на p, называется *квадратичным невычетом* по модулю p.

Упр. 9. Сколько существует квадратичных невычетов по модулю p?

1. Пусть p — нечетное простое число, a, b, c — вычеты по модулю p, причем a не делится на p, а $D = b^2 - 4ac$. Докажите, что если D — квадратичный вычет по модулю p, то сравнение $ax^2 + bx + c \equiv 0 \pmod p$ имеет два корня, если D — квадратичный невычет по модулю p, то указанное сравнение не имеет корней, а если D делится на p, то это сравнение имеет ровно один корень.

Упр. 10. Почему важно условие, что p — не 2?

2. Решите сравнение $3x^2 - 4x + 1 \equiv 0 \pmod{131}$. Без перебора!

Определение 7. *Символом Лежандра* называется выражение, обозначаемое $\left(\frac{a}{p}\right)$, равное 1, если a — квадратичный вычет по модулю p; -1, если a — невычет по модулю p и 0, если a кратно p.

Свойства символа Лежандра.

3. **(a)** $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod p$ (критерий Эйлера);

(b) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ (мультипликативность).

Другими словами, мы только что доказали, что *вычет на вычет дает вычет, невычет на вычет дает невычет, невычет на невычет дает вычет.*

4. Докажите, что -1 является квадратичным вычетом по модулю $p \iff p = 4k+1$.

5. Докажите, что у сравнения $(x^2 - 2)(x^2 - 3)(x^2 - 6) \equiv 0 \pmod p$ всегда есть решение.

6. Докажите, что число p является делителем числа вида $x^2 - x + 3$ тогда и только тогда, когда оно является делителем числа вида $y^2 - y + 25$.

7. Решите в целых числах уравнение $x^3 + 7 = y^2$.

8. Решите в целых числах уравнение $x^2 = y^3 - 5$.

9. Докажите, что простых чисел вида $4k+1$ бесконечно много.

10. Пусть a — квадратичный вычет по простому модулю $p>2$. Докажите, что a — квадратичный вычет по модулю p^n при любом натуральном n.

11. Пусть $p=4k+3$ простое. Докажите, что если

$$\frac{1}{0^2+1}+\frac{1}{1^2+1}+\ldots+\frac{1}{(p-1)^2+1}=\frac{m}{n},$$

где $(m,n)=1$, то $2m-n\vdots p$.

12. Последовательность $\{a_n\}$ целых чисел задаётся следующими соотношениями: $a_1=100$, $a_{n+1}=a_n^{17}+a_n+2$. Докажите, что a_n не делится на 19 ни при каком n.

ПРостой стрим. Теория чисел. 12 часов с ДА. Рождество в октябре

25 октября

Упражнение. Докажите, что в виде суммы двух квадратов целых чисел представляются число 2 и число p^2.

1. Два числа представляются в виде суммы двух квадратов. Докажите, что их произведение представляется в виде двух квадратов.

2. Число n представляется в виде суммы двух квадратов. Докажите, что в разложении n на простые множители все простые делители вида $4k+3$ входят в четной степени.

3. *Лемма Туэ.* Пусть n — натуральное число, а a — целое. Тогда найдутся такие целые x и y, что $(x,y) \neq (0,0)$, $ax - y \vdots n$, и $|x|, |y| \leqslant \sqrt{n}$.

4. С помощью леммы Туэ докажите, что простое $p = 4k+1$ представляется в виде суммы двух квадратов.

5. Опишите все числа, представимые в виде суммы двух квадратов.

6. Докажите, что $p = 4k+1$ представляется в виде суммы двух квадратов единственным способом.

7. Докажите, что уравнение $x^2+y^2 = z^5+z$ имеет бесконечно много целых решений, в которых x, y и z попарно взаимно просты.

8. Какие простые числа p представляются в виде $p = a^2 + 2b^2$?

9. Сколькими способами n представляется в виде суммы двух квадратов?

ПРостой стрим. Теория чисел. 12 часов с ДА. Немного о двойке

25 октября

Сегодня мы узнаем, по каким простым модулям 2 является квадратичным вычетом. Для этого нам достаточно узнать, с чем сравнимо $2^{(p-1)/2}$ по модулю p.

1. Рассмотрим числа 2, 4, 6, ..., $p-1$. Докажите, что их произведение сравнимо с $\pm 1 \cdot 2 \cdot \ldots \cdot \frac{p-1}{2}$ по модулю p.

2. Научитесь определять знак в предыдущей задаче в зависимости от p.

3. Докажите, что 2 — квадратичный вычет по модулю $p \Leftrightarrow p \equiv \pm 1 \pmod 8$.

4. По каким простым модулям -2 является квадратичным вычетом?

5. Докажите, что у числа $2^n + 1$ не может быть простых делителей вида $8k + 7$.

6. Чему равна сумма

$$\left[\frac{1}{2003}\right] + \left[\frac{2}{2003}\right] + \left[\frac{2^2}{2003}\right] + \ldots + \left[\frac{2^{2001}}{2003}\right]?$$

7. Докажите, что простых чисел вида **(a)** $8k + 3$; **(b)** $8k + 5$; **(c)** $8k + 7$ бесконечно много.

8. Докажите, что равенство $x^3 - 3 = 2y^2$ не имеет решений в целых числах.

9. Последовательность $\{x_n\}$ определена рекурсивно: $x_1 = a$ при некотором натуральном a, а также $x_{n+1} = 2x_n + 1$. Пусть $y_n = 2^{x_n} - 1$. Какое максимальное количество подряд идущих простых чисел может быть в последовательности $\{y_n\}$?

ПРостой стрим. Теория чисел. 12 часов с ДА. Примитивные задачи

25 октября

Определение 8. Число называется *первообразным корнем (primitive root)* по модулю m, если его показатель равен в точности $\varphi(m)$.

Теорема. По любому простому модулю p существует первообразный корень.

Ключевая лемма. Пусть p — произвольное простое число. Тогда сравнение $x^n \equiv 1 \pmod p$ имеет не более n решений по модулю p.

Доказательство 1. Пусть $d_1, \ldots, d_{p-1}$ — показатели чисел $1, \ldots, p-1$ соответственно.

(a) Докажите, что если показатели каких-то двух чисел равны a и b, то существует число, показатель которого равен $\text{НОК}(a, b)$.

Подсказка. Вспомните задачу **2** из показателей–1.

(b) Рассмотрим сравнение $x^{\text{НОК}(d_1,\ldots,d_{p-1})} \equiv 1 \pmod p$. Докажите, пожалуйста, что $\text{НОК}(d_1, \ldots, d_{p-1}) = p - 1$.

(c) Докажите, что первообразные корни по модулю p существуют.

Важная мысль. Первообразный корень g прекрасен тем, что g^1, g^2, …, g^{p-1} дают все ненулевые остатки по модулю p.

Упр. 11. Пусть g — первообразный корень по модулю $m > 2$. Докажите, что $g^{\varphi(m)/2} \equiv -1 \pmod m$. Верно ли это в обратную сторону?

1. Докажите, что при простом p сравнение $x^4 \equiv -1 \pmod p$ имеет решение тогда и только тогда, когда $p = 8k + 1$.

2. Найдите сумму всех квадратичных вычетов по простому модулю $p > 3$.

3. Докажите, что натуральные числа 1, 2, …, 238 можно расставить по кругу так, чтобы для любых трех подряд идущих по часовой стрелке чисел a, b, c число $b^2 - ac$ делилось на 239.

4. Докажите, что 2 является первообразным корнем любого простого числа вида $p = 4q + 1$, где q — простое.

5. Найдите остаток суммы всех выражений вида ij, где $1 \leqslant i < j \leqslant p - 1$ по простому модулю p.

6. Дано простое число p и натуральное число $0 < i \leqslant p - 2$. Докажите, что

$$1^i + 2^i + \ldots + (p-1)^i \vdots p.$$

Докажем существование первообразного корня еще двумя способами.

Доказательство 2. Пусть d — делитель числа $p - 1$.

(a) Пусть показатель числа a равен d. Докажите, что все решения сравнения $x^d \equiv 1 \pmod p$ суть вычеты $a^1, a^2, \ldots a^d$.

(b) Докажите, что существует не более $\varphi(d)$ вычетов, показатель которых равен d.

(c) Пусть $d_1, d_2, \ldots, d_k$ — все делители натурального числа n (включая n). Докажите тождество Гаусса

$$\varphi(d_1) + \varphi(d_2) + \ldots + \varphi(d_k) = n.$$

(d) Докажите, что существует в точности $\varphi(d)$ вычетов, показатель которых равен d.

Доказательство 3. Рассмотрим разложение числа $p-1 = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_k^{\alpha_k}$ на простые множители. Далее найдём такие числа g_i, что $g_i^{(p-1)/q_i^{\alpha_i}} \not\equiv 1 \pmod{p}$.

(a) Докажите, что такие числа g_i действительно найдутся.

(b) Докажите, что если через h_i обозначить $\dfrac{p-1}{q_i^{\alpha_i}}$ степень числа g_i, то показатель числа h_i равен $q_i^{\alpha_i}$.

(c) Докажите, что произведение всех чисел h_i является первообразным корнем.

7. Докажите, что 2 является первообразным корнем по модулю 3^n при любом натуральном n.

8. Докажите, что если $n = 3^{k-1}$, то $2^n + 1 \vdots 3^k$.

9. Докажите, что если у числа n есть два различных нечетных простых делителя p и q, то по модулю n нет первообразных корней.

10. Докажите, что по модулю $2^k p$, где $k \geqslant 2$, а p — простое, нет первообразных корней.

11. Пусть g — первообразный корень по простому модулю p. Докажите, что либо g, либо $g+p$ является первообразным корнем по модулю p^2.

12. Пусть g — первообразный корень по модулю p^k, где p — простое, $k \geqslant 2$. Докажите, что тогда g — первообразный корень по модулю p^{k+1}.

13. Дано некоторое натуральное число m. Все числа, не превосходящие m и взаимно простые с ним, перемножили, получив число P. Докажите, что $P \equiv \pm 1 \pmod{m}$, причем сравнимо с -1 тогда и только тогда, когда по модулю m есть первообразный корень.