Билет 1. Простые числа, ОТА

Опр: Простое число - натуральное число, имеющее ровно 2 различных натуральных делителя - 1 и самого себя.

Теорема (основная теорема арифметики):

Каждое натуральное число $n > 1$ можно разложить в виде $n = p_1 \cdot \ldots \cdot p_k$, где $p_1 \ldots p_k$ - простые числа, причём такое представление единственно, если не учитывать порядок следования множителей.

▲ Док-во существования по индукции:

База: $2 = 2^1$

Переход: Пусть $\forall k \in \mathbb{N} : k < n$ разложение сущ-ет. Тогда если n - простое, то сущ-ие доказано; если n - составное, то $\exists a, b \in \mathbb{N} : 1 < a, b < n$ такие, что $n = a \cdot b$. Для a, b - верно ~~перо~~ предположение индукции ■

Билет 2-3. НОК, НОД, алгоритм Евклида

Опр: НОК двух натуральных чисел $[a, b]$ - такое наименьшее натуральное число l, что l делится на a и b без остатка.

Опр: НОД двух натуральных чисел (a, b) - такое наибольшее натуральное число d, что a и b делятся на d без остатка.

Теорема (алгоритм Евклида)

$\exists d = НОД(a, b)$, причём $\exists u, v : d = au + bv$

(линейное представление / комбинация a и b)

▲ Пусть б.о.о. $a=0,\ b\neq 0 \Rightarrow (a,b)=b \Rightarrow 0\cdot a+1\cdot b=b$

Теперь пусть $a\neq 0$ и $b\neq 0$ и r_n - последний член $\neq 0$.

$1:\ a = q_1 b + r_1$
$2:\ b = q_2 r_1 + r_2$
$3:\ r_1 = q_3 r_2 + r_3$
$\dots\dots\dots$
$n:\ r_{n-2} = q_n r_{n-1} + r_n$
$n+1:\ r_{n-1} = q_{n+1} r_n + 0$

Заметим, что последовательность $\{r_i\}_{i=1}^{n}$ монотонно убывает т.к. $r_k < r_{k-1} \Rightarrow$ у неё очевидно есть конец, поэтому алгоритм остановится.

Покажем, что $r_n = (a,b)$: (поднимаемся по лестнице)

а) $r_{n-1} \vdots r_n \Rightarrow r_{n-2} \vdots r_n \Rightarrow \dots \Rightarrow a \vdots r_n$ и $b \vdots r_n$

б) если $a \vdots d'$ и $b \vdots d'$, то $r_n \vdots d'$ т.к. (спускаемся)

$$\begin{cases} 1.\ r_1 = a - q_1 b \ \vdots d' \\ 2.\ r_2 = b - q_2 r_1 \ \vdots d' \end{cases} \Rightarrow \dots \Rightarrow r_n \vdots d' \quad \Rightarrow (a,b) = r_n$$

Докажем линейную комбинацию индукцией по кол-во строк в алгоритме Евклида:

заметим, что $НОД(a,b) = НОД(b,r_1) = НОД(r_1,r_2) = \dots = r_n$

т.к. можно вычёркивать строки у алгоритма

База: б.о.о. $b=0 \Rightarrow НОД(a,0) = d = 1\cdot a + 0\cdot b$

предположение: $d = u'\cdot b + v'\cdot r_1$

переход: $d = u'\cdot b + v'\cdot(a - q_1\cdot b) = v'\cdot a + (u' - v'q_1)b$

$\Rightarrow v' = u$ и $u' - v'q_1 = v \Rightarrow d = a\cdot u + b\cdot v$ ■

Билет 4. Лемма Евклида

Лемма: Если простое число p делит без остатка произведение двух целых чисел $x\cdot y$, то p делит x или y

т.е. если $x\cdot y \vdots p \Rightarrow x \vdots p$ или $y \vdots p$.

▲ (От противного) Пусть $x \not\vdots\, p$ и $y \not\vdots\, p$, тогда $НОД(x,p) = НОД(y,p) = 1$. Значит $\exists a_1, a_2, a_3, a_4$ т.ч.

$$\left.\begin{matrix} a_1 x + a_2 \cdot p = 1 \\ a_3 \cdot y + a_4 \cdot p = 1 \end{matrix}\right| \cdot \Rightarrow a_1 a_3 xy + a_1 a_4 xp + a_2 a_3 yp + a_2 a_4 p^2 = 1$$

т.к. $xy \,\vdots\, p \Rightarrow$ левая часть кратна p

но $1 \not\vdots\, p \Rightarrow$ противоречие ■

Билет 5. Единственность в ОТА

Теорема: $\forall n \in \mathbb{N} \setminus \{1\}$ верно, что существует и единственно его каноническое разложение

▲ Сущ-ие уже было доказано. Покажем единственность с помощью леммы Евклида по индукции.

Пусть $n = p_1 \cdot p_2 \cdot \ldots \cdot p_l = q_1 \cdot q_2 \cdot \ldots q_m$

База: $l = 1$: $n = p_1$ - простое $\Rightarrow m = 1$ и $p_1 = q_1$

переход: пусть доказано для чисел разлагающихся в произведение менее l простых чисел.

$q_1 \cdot \ldots \cdot q_m \,\vdots\, p_l \Rightarrow$ (по лемме Евкл) $\exists i : q_i \,\vdots\, p_l$

$\Rightarrow$ $q_i = p_l$

Значит: $p_1 \ldots p_l = q_1 \ldots \hat{q}_i \ldots q_m \cdot p_l \Rightarrow$

$\Rightarrow p_1 \ldots p_{l-1} = q_1 \ldots \hat{q}_i \ldots q_m \Rightarrow l - 1 = m - 1$

(верно по предполож. индукции) $\Rightarrow l = m$ и

$\exists \sigma : \{1, 2, \ldots l-1\} \to \{1, 2, \ldots l-1\}$ ← перестановка чисел

Положим $\sigma(l) = i$ и σ - биекция ■

Билет 6. Теория сравнений, системы вычетов.

Опр: Пусть $a, b \in \mathbb{Z}$, $m \in \mathbb{N}_+$.

Тогда $a \equiv b \pmod m \Leftrightarrow (a-b) \vdots m$

Опр: Вычетом по модулю m называется произвольный представитель класса эквивалентности „сравнимость по модулю"

Свойства: 1) $a \equiv b(m) \Rightarrow b \equiv a(m)$

2) $a \equiv b(m)$ и $b \equiv c(m) \Rightarrow a \equiv c(m)$

3) $a \equiv b(m) \Rightarrow a+c \equiv b+c(m)$

4) $a \equiv b(m)$ и $c \equiv d(m) \Rightarrow a \pm c \equiv b \pm d(m)$ т.к. $\underbrace{(a-b)+(c-d)}_{\vdots m} \vdots m$

5) $a \equiv b(m) \underset{\text{но } \Leftarrow \text{ только если НОД}(n,m)=1}{\Rightarrow} an \equiv bn(m)$ т.к. $n(a-b) \vdots m$

6) $a \equiv b(m)$ и $c \equiv d(m) \Rightarrow ac \equiv bd(m)$ т.к. $ac-bd = c(a-b)+b(c-d) \vdots m$

7) $a \equiv b(m) \Rightarrow a^n \equiv b^n(m)$

Опр: Полная система вычетов по модулю m - это любой набор из m попарно несравнимых по модулю m целых чисел

Опр: Приведённой системой вычетов по модулю m называется совокупность всех вычетов из полной системы, взаимно простых с модулем m.

Например: $m=10$ Полная система: $\{0, 1, \dots 9\}$
Приведённая: $\{1, 3, 7, 9\}$

Арифметические операции в системе вычетов определены так:

1. $a(m) + b(m) \equiv (a+b) \bmod m$
2. $(a \bmod m)(b \bmod m) \equiv ab\ (m)$

Опр: Элемент a - делитель нуля $\Leftrightarrow a \not\equiv 0(m)$ $\exists b \not\equiv 0(m)$ т.ч. $ab \equiv 0(m)$

2 и 3 $(m=6)$

Опр: Элемент a - обратимый $\Leftrightarrow \exists a^{-1} : a \cdot a^{-1} \equiv 1 (m)$

Опр: Мн-во $\mathbb{Z}_m^*$ - мн-во обратимых эл-тов.

Утверждение: a - обратим $\Leftrightarrow$ a - не делитель нуля.

▲ ($\Rightarrow$) $\exists a^{-1} : a \cdot a^{-1} \equiv 1 (m)$; $\exists b \not\equiv 0 (m) : ab \equiv 0 (m)$

тогда $a \cdot a^{-1} b \equiv b (m)$ и $a b a^{-1} \equiv 0 (m)$

$\Rightarrow$ по транзитивности $b \equiv 0 (m) \Rightarrow$ противоречие

($\Leftarrow$) $\nexists b \not\equiv 0 (m) : a \cdot b \equiv 0 (m)$

Полная система вычетов: $\{0, 1, \dots m-1\}$ $/ \cdot a$

$\Rightarrow \{0, a, 2a, \dots (m-1)a\}$ - пусть не все разные

значит $ka \equiv la (m) \Rightarrow (k-l)a \equiv 0 (m) \Rightarrow k = l$ (т.к. a - не явл. делит. нуля)

Т.о. вторая система - это перестановка первой

$\Rightarrow \exists k : a \cdot k \equiv 1 (m)$ т.к там есть 1. $\Rightarrow a$ - обратим ■

Следствие: a - обратим $\Leftrightarrow (a, m) = 1$.

▲ $ax + my = 1$. Пусть a - делитель нуля, тогда

$\exists b \not\equiv 0 (m) : a \cdot b \vdots m \Rightarrow b \vdots m \overset{\text{противоречие}}{\Rightarrow} a$ - обратим

Обратно: $\exists b = \frac{m}{(a,m)} \not\equiv 0 (m) : ab = \frac{a \cdot m}{(a,m)} \equiv 0 (m) \Rightarrow a$ - дел. нуля. ■

(контрпозиция) т.г. $(a,m) \neq 1$

Билет 7. Малая теорема Ферма

Лемма: Если $(a, p) = 1$, то $\{a, 2a, \dots, (p-1)a\}$ - привед. сист.

▲ (от противного) $\exists x \not\equiv y (p)$ т.г. $ax \equiv ay (p)$.

Тогда $a(x-y) \equiv 0 (p) \underset{(a,p)=1}{\Rightarrow} x - y \equiv 0 (p) \Rightarrow x \equiv y (p)$! ■

Теорема (МТФ): Если p - простое, a - целое: $a \not\vdots p$,

тогда $a^{p-1} \equiv 1 (\mathrm{mod}\, p)$ $(\Leftrightarrow a^p \equiv a (p))$

▲ Заметим: $(a, p) = 1$. Рассмотрим полную сист. вычетов.

По лемме: $1 \cdot 2 \cdot \dots \cdot (p-1) \equiv a \cdot 2a \cdot \dots \cdot a(p-1) \Rightarrow a^{p-1} \equiv 1 (p)$ ■

т.к. $(p-1)! \equiv a^{p-1} (p-1)!$ и $\text{НОД}(p, (p-1)!) = 1 \Rightarrow$ можем поделить

Билет 8. Теорема Эйлера

Опр: Функция Эйлера $\varphi(m)$ равна количеству натуральных чисел, меньших m и взаимно простых с ним.

Теорема: $\forall a, m; (a,m)=1$ верно, что $a^{\varphi(m)} \equiv 1\ (m)$

▲ Рассмотрим произвольную приведённую систему вычетов:

$\{x_1, x_2, \dots x_{\varphi(m)}\}$ - привед. т.к. $\varphi(m) < m$. Тогда

$\{ax_1, ax_2, \dots ax_{\varphi(m)}\}$ - тоже привед. т.к. $(a,m)=1$.

Значит $x_1 \cdot \ldots \cdot x_{\varphi(m)} = ax_1 \cdot \ldots \cdot ax_{\varphi(m)}\ (m) \Rightarrow a^{\varphi(m)} \equiv 1\ (m)$

т.к. $x_1 \cdot \ldots x_{\varphi(m)}$ взаимно просто с m ■

Билет 9. Теорема Лагранжа и теорема Вильсона

Теорема Лагранжа (о числе корней многочлена по mod p):

Пусть $P(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$, где $a_i \in \mathbb{Z}_p$ и p- простое число. Тогда у сравнения $P(x) \equiv 0 \pmod p$ не больше n решений.

Теорема Вильсона (с использование т. Лагранжа)

$p \in \mathbb{N}, p > 1$ - простое $\Leftrightarrow (p-1)! \equiv -1 \pmod p$

▲ $(\Rightarrow)$ Рассмотрим $f(x) = (x-1) \cdot \ldots \cdot (x-(p-1))$ и $g(x) = x^{p-1} - 1$.

Корни обоих мн-нов: $1, 2, \dots p-1$ (для $g(x)$ по МТФ)

Заметим, что при x^{p-1} коэффициенты $f(x)$ и $g(x)$ равны 1.

Значит $h(x) = f(x) - g(x)$ имеет те же $p-1$ корней, но $\deg(h(x)) = p-2 \Rightarrow$ по т. Лагранжа $h(x) \equiv 0$

$\Rightarrow f(0) = g(0) \Rightarrow (p-1)! \equiv -1 \pmod p$

$(\Leftarrow)$ Пусть p - составное и $p \neq 4$, тогда $(p-1)! \equiv 0\ (p)$

т.к. $\exists x, y < p : x \cdot y = p$; если $p = 4 \Rightarrow (4-1)! \equiv 2 \pmod 4$ ■

Билет 10. Док-во теоремы Вильсона

Опр: Показателем или порядком $ord_m(x) = ord(x)$ элемента $x \in \mathbb{Z}_m^*$ называется такое минимальное $k \geq 1$, что $x^k \equiv 1 \pmod m$

Опр: Число g называется первообразным корнем по модулю m, если $ord(g) \equiv \varphi(m)$

Утверждение: $\forall p$ - простого $\exists$ первообразный корень

Теорема Вильсона:

$p \in \mathbb{N}, p > 1$ - простое $\Leftrightarrow (p-1)! \equiv -1 \pmod p$

▲ $\Rightarrow$ Пусть g - первообразный корень $(\text{mod } p)$

Тогда $1, g, g^2 \dots g^{p-2}$ - попарно различные т.к.

если $g^x \equiv g^y \Rightarrow g^{x-y} \equiv 1$ ← противоречие

$\Rightarrow$ образуют полную систему вычетов без нуля

Значит: $(p-1)! \equiv 1 \cdot g \cdot g^2 \cdot \dots g^{p-2} = g^{\frac{(p-2)(p-1)}{2}} \pmod p$

Теперь пусть p - простое и нечётное $\Rightarrow p = 2k+1$.

Тогда $k < p-1$; $g^k \not\equiv 1 (p)$, но $g^{2k} \equiv g^{p-1} \equiv 1 (p)$ по МТФ.

$\Rightarrow (g^k - 1)(g^k + 1) \equiv 0 \ (p) \Rightarrow g^k \equiv -1 \ (p)$ следовательно

$$(p-1)! \equiv g^{\frac{(p-2)(p-1)}{2}} \equiv (g^k)^{2k-1} \equiv (-1)^{2k-1} \equiv -1 \ (p)$$

$\Leftarrow$ смотри билет 9 $\left(\begin{matrix} p\text{-составное } p \neq 4 \\ (p-1)! \equiv 0 \ (p) \end{matrix}\right)$ ■

Билет 11. Бесконечность простых вида $3k+2$, $2k \pm 1$

Пусть $p_1, \dots p_n$ - простые числа. Тогда число $p_1 \cdot \dots \cdot p_n \pm 1$ не делится ни на какое из p_i

▲ $(p_1 \cdot \dots \cdot p_n \pm 1) - (p_1 \cdot \dots \cdot p_n) = \pm 1$ при этом $\pm 1 \not\vdots \ p_i$

значит левая скобка $\not\vdots \ p_i$ ■

Лемма: Если n^2+1 делится на нечётное простое p, то p вида $4k+1$.

▲ Заметим, что $(n,p)=1 \Rightarrow$ по МТФ (т.к. $n^2 \equiv -1 \pmod p$)

$1 \equiv n^{p-1} \equiv (n^2)^{(p-1)/2} \equiv (-1)^{(p-1)/2} (p) \Rightarrow \frac{p-1}{2} \equiv 0 \pmod 2$ ■

Утверждение: $\exists\ \infty$ много простых чисел вида $3k+2$ и $4k\pm1$

▲ а) $p=3k+2$:

предположим, что их конечное число $p_1, \dots p_n$. Тогда $A = 3p_1 \cdot \ldots \cdot p_n + 2 \equiv 2 \pmod 3$ при этом все его простые делители, среди которых есть ~~дел~~ делитель вида $3k+2$ (*), отличны от $p_1, \dots p_n$ $\Rightarrow$ противоречие (т.е. нашли ещё один делитель не из списка)

б) $p=4k+1$:

предположим, что их конечное число $p_1, \dots p_n$. Тогда $A = (2 \cdot p_1 \ldots p_n)^2 + 1$ - нечётное, а значит делится на нечётное простое $\Rightarrow$ по лемме A имеет вид $4k+1$, но оно отлично от $p_1, \dots p_n$ $\Rightarrow$ противоречие

в) $p=4k+3$:

предположим, что их конечное число $p_1, \dots p_n$. Тогда $A = 4p_1 \cdot \ldots \cdot p_n + 3 \equiv 3 \pmod 4$ при этом все его простые делители, среди которых есть делитель вида $4k+3$, отличны от $p_1, \dots p_n$ $\Rightarrow$ противоречие (т.е. нашли еще один делитель вида $4k+3$ не из фикс. списка. ■

(*) при делении на 3 остатки: $-1, 0, 1$. (0 - не может быть, иначе $A \vdots 3$)
если все делители $\equiv 1(3) \Rightarrow A \equiv 1(3) \leftarrow$ плохо $\Rightarrow \exists$ хотя бы 1 делитель $3k+2$.

Билет 12. Сравнения 2ой степени. Квадр. вычеты/невычеты

Опр: $ax^2+bx+c \equiv 0 \pmod m$ – сравнение $2^{го}$ порядка

Опр: Пусть p – нечётное простое число, тогда если $(a,p)=1$ и $\exists x: x^2 \equiv a \pmod p$, то a – квадратичный вычет, иначе – невычет (0 – не явл ни выч, ни невыч.)

Утв: Пусть p – нечётное простое число, тогда число вычетов, как и невычетов, равно $\frac{p-1}{2}$.

▲ Так как $x^2 \equiv (p-x)^2$, то достаточно показать, что вычеты $1^2, 2^2, \dots ((p-1)/2)^2$ различны

Предположим, что $\exists x,y \in (0, \frac{p-1}{2}]: x^2 \equiv y^2 \pmod p$

Тогда $(x-y)(x+y) \equiv 0 (p)$ и $0 < |x-y| < p$

Значит, $(x+y) \equiv 0 \pmod p$, но $x+y \leq p-1$

Следовательно, противоречие и кв. вычетов $\frac{p-1}{2}$.

Все остальные элементы F_p – кв. невычеты, и их $(p-1) - \frac{p-1}{2} = \frac{p-1}{2}$ ← столько же ■

Билет 13. Символ Лежандра, формулы

Опр: Символом Лежандра называют (p – простое, нечётное)

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & a \text{ - вычет} \\ -1, & a \text{ - невычет} \end{cases} \text{ и } \left(\frac{a}{p}\right) = 0, \text{ если } a \,\vdots\, p$$

Теорема: $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$

▲ Если $(a,p) \neq 1$, то тривиально. Теперь $(a,p)=1$, тогда по МТФ $a^{p-1} \equiv 1 (p) \Rightarrow (a^{\frac{p-1}{2}}-1)(a^{\frac{p-1}{2}}+1) \equiv 0 \pmod p$ При этом оба множителя не могут одновременно делится на p, т.к. иначе делилась бы их разность, а $2 \not\vdots\, p$.

Пусть a - вычет $\Rightarrow \exists x: a \equiv x^2 (p) \Rightarrow a^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} = x^{p-1} \underset{МТФ}{\equiv} 1 \ (p)$

следовательно $a^{\frac{p-1}{2}} \equiv 1 \pmod p$

Если a - невычет, то $a^{\frac{p-1}{2}} \equiv -1 \pmod p$ } совпадает с символом лежандра

Следствие: Символ лежандра мультипликативен

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod p$$

значит $\left(\frac{a_1 \dots a_n}{p}\right) = \left(\frac{a_1}{p}\right) \dots \left(\frac{a_n}{p}\right)$ (по индукции)

Билет 14. Умение вычислить символ лежандра

1° $\left(\frac{1}{p}\right) = 1$; $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} \Rightarrow$ $p=8k+1: 1$; $p=8k+3: -1$; $p=8k+5: -1$; $p=8k+7: 1$

2° $\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{q}{p}\right) \Rightarrow \begin{cases} \text{если } p=4k+3,\ q=4m+3 \text{ то } \left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right) \\ \text{иначе } \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \end{cases}$

(это кв. закон взаимности)

3° Если $a \equiv b (p)$, то $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ 4° Если $a \not\vdots\, p$, то $\left(\frac{a^2}{p}\right) = 1$

Задача: а) $\left(\frac{102}{103}\right) = \left(\frac{-1}{103}\right) = (-1)^{\frac{p-1}{2}} = -1$ т.к. $103 = 4k+3$; 1 если $p = 4k+1$

б) $\left(\frac{113}{79}\right) = \left(\frac{34}{79}\right) = \underbrace{\left(\frac{2}{79}\right)}_{1}\left(\frac{17}{79}\right) = \left(\frac{79}{17}\right) = \left(\frac{11}{17}\right) = \left(\frac{17}{11}\right) = \left(\frac{6}{11}\right) = \underbrace{\left(\frac{2}{11}\right)}_{-1}\left(\frac{3}{11}\right) = -1$ $5^2 \equiv 3 (11) \leftarrow$ вычет

в) $\left(\frac{5}{73}\right) = \left(\frac{73}{5}\right) = \left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1$