(Кор)

Билет 1. Лемма Евклида через алгоритм Евклида

Линейная выразимость НОД

$\exists x, y \in \mathbb{Z} : \text{НОД}(a,b) = ax + by$

Лемма Евклида:

Если $x \cdot y \vdots p \Rightarrow x \vdots p$ или $y \vdots p$

▲ (Аналогично билету 4 ну удовл.)

(от противного) $\text{НОД}(x,p) = \text{НОД}(y,p) = 1 \Rightarrow \begin{matrix} a_1 x + a_2 p = 1 \\ a_3 y + a_4 p = 1 \end{matrix} \Big| \cdot$

$\Rightarrow Axy + Bxp + Cyp + Dp^2 = 1$

левая часть $\not\vdots p$, а правая – нет $\Rightarrow$ противоречие ■

Билет 2. Лемма Евклида через "идеалы"

Опр: Идеалом в $\mathbb{Z}$ назовем мн-во $M = \{a \in \mathbb{Z} : an \equiv 0 (p)\}$ (*)

Замечание: Идеалы замкнуты относительно сложения и домножения на целое число.

а) $a, b \in M \Rightarrow a+b \in M$ т.к. $an \vdots p$, $bn \vdots p \Rightarrow an+bn \vdots p$

б) $a \in M, b \in \mathbb{Z} \Rightarrow ab \in M$ т.к. $an \vdots p \Rightarrow abn \vdots p$ (кашу маслом не испортишь)

Св-во: $\exists d \in \mathbb{Z}$ т.ч. $M = \{kd : k \in \mathbb{Z}\} = d\mathbb{Z}$ – идеал

▲ d – минимальное положительное число из M

Пусть $a \in M$ и $a = cd + r \Rightarrow r = a + (-c) \cdot d$

при этом $a \in M$ и $d \in M$ и по св-ву $(-c) \cdot d \in M$

и по св-ву суммы $r = a + (-c) \cdot d \in M$

Противоречие с тем, что d – минимальное, ведь $r < d$

$\Rightarrow a = cd$ (т.е. $\forall a \in M \ a \vdots d$) ■

(*) для некоторых n, p – фикс. Они потом будут в л Евклида

Утверждение: $p : d$

▲ $M := \{a \in \mathbb{N} : an \vdots p\}$. Если положить $a = p \Rightarrow pn \vdots p$

Значит $p \in M \Rightarrow p : d$

Более того, из определения простого числа $d = \left[\frac{1}{p}\right.$ ■

Лемма Евклида: $n \cdot m \vdots p \Rightarrow n \vdots p$ или $m \vdots p$

▲ Докажем, что $m : d$, откуда следует лемма Евклида

Если $d = 1$, то $n \vdots p$ т.к. $M = \mathbb{N}$ ($a = 1 : 1 \cdot n \vdots p$ из опред M)

Если $d = p$, то верно

$m \cdot n \vdots p \Rightarrow m \in M \Rightarrow m : d$ (т.к. на d делятся все элементы из M по св-ву)
по опред M

следовательно $m \vdots p$ ■

Билет 3. Единственность в ОТА

▲ (от противного)

Пусть есть числа, разложимые двумя способами.

Выберем минимальное из них $N = p_1 \cdot \ldots \cdot p_k = q_1 \cdot \ldots \cdot q_l$

Все p_i и q_j различны (иначе можно сократить и получить число меньшее N).

Пусть $p_1 < q_1$ и $M = (q_1 - p_1) \cdot q_2 \ldots q_l \Rightarrow M < N$

Заметим, что $M = q_1 \cdot q_2 \ldots q_l - p_1 \cdot q_2 \ldots q_l =$ (по опред N)

$= p_1 \ldots p_k - p_1 \cdot q_2 \ldots q_l = p_1 (p_2 \ldots p_k - q_2 \ldots q_l) \Rightarrow M \vdots p_1$

При этом $(q_1 - p_1) \not\vdots p_1$ и $q_2, \ldots q_l$ отличны от p_1,

сл-но, в разложении M отсутствует $p_1 \Rightarrow$

$\Rightarrow$ у M есть два различных разложения

Значит, противоречие с тем, что N – минимальное такое число. ■

Билет 4. Малая теорема Ферма (4 док-ва)

Смотри билеты 6-7 ну удовл → системы вычетов и МТФ
Приведём ещё 3 док-ва МТФ

Теорема (МТФ): Если a - целое, p - простое $a \nmid p$, тогда $a^{p-1} \equiv 1 \pmod p$

⚠

1 способ: $a = 1+1+\dots 1$ ← a штук

$\Rightarrow a^p = (1+1+\dots+1)^p$ используем полиномиальный коэффициент

$$a^p = \sum_{k_1+\dots k_a=p} \frac{p!}{k_1!\dots k_a!} 1^{k_1}\dots 1^{k_a} = \sum_{k_1+\dots k_a=p} \frac{p!}{k_1!\dots k_a!} \equiv$$

$$\equiv 1+\dots+1 \equiv a \pmod p$$

если $\nexists k_i = p$, то p в числителе не сократится $\Rightarrow$ слагаемое $\vdots p$

2 способ: Рассмотрим все строки длины p из алфавита мощности a. Уберём строки, состоящие из одинаковых букв $\Rightarrow$ осталось $a^p - a$ строк.
Оставшиеся строки можно разбить на классы эквивалентности по отношению „явл циклическим сдвигом". С учётом того, что строка → $p : d$ ← период (по св-вам) получаем, что длина периода это p $\Rightarrow$ размер класса эквивалент. есть p $\Rightarrow$ $a^p - a \equiv 0 \pmod p$.

3 способ: по т. Лагранжа из теории групп:
порядок эл-та ($\min K : a^K =$ нейтр. эл-т) делит порядок конечной группы (число эл-тов в ней).
Сл-но, если $\mathbb{Z}_p$ - привед. сист. вычетов, то $\mathbb{Z}_p$ - группа по умножению с 1 - нейтр. эл-т. Порядок группы: $p-1$.
$\Rightarrow a^{p-1} = 1 \Rightarrow a^{p-1} \equiv 1 (p)$ ▨

Билет 5. Функция Эйлера

билет 7 $\{a, 2a, \dots (m-1)a\}$

Лемма: Пусть $(m, m') = 1$; $\{a\}$ - пробегает приведённую систему вычетов m; $\{a'\}$ - приведённую систему вычетов m'. Тогда числа $a' \cdot m + a \cdot m'$ - образуют приведённую систему вычетов по модулю mm'.

▲ Если $a_1' m + a_1 m' \equiv a_2' m + a_2 m' \pmod{mm'}$

тогда $a_1' m + a_1 m' \equiv a_2' m + a_2 m' \pmod{m} \Rightarrow$

$\Rightarrow a_1 m' \equiv a_2 m' \pmod{m} \Rightarrow a_1 \equiv a_2 \pmod{m}$

Аналогично $a_1' \equiv a_2' \pmod{m'}$

$\Rightarrow$ существует mm' чисел образующих приведённую систему вычетов по модулю mm'. ■

Утв: Ф-ция Эйлера мультипликативна

т.е. $\varphi(mm') = \varphi(m)\varphi(m')$ если $(m, m') = 1$

▲ Из леммы $\Rightarrow \exists a, a' : (a'm + am'; mm') = 1 \Rightarrow$

$\Rightarrow (a'm + am'; m) = 1$ и $(a'm + am'; m') = 1 \Rightarrow$

$\Rightarrow (am'; m) = 1$ и $(a'm; m') = 1 \Rightarrow$

$\Rightarrow (a, m) = 1$ и $(a'; m') = 1$

Поэтому $\varphi(mm')$ чисел (которые по опред ф-ции Эйлера меньше числа mm' и взаимно просты с ними) являются наименьшими положительными вычетами среди $\varphi(m)\varphi(m')$ т.к. они представимы в виде $a'm + am'$. Значит мультипликативность доказана $\Rightarrow \varphi(mm') = \varphi(m)\varphi(m')$ ■

Следствие: p-простое $\varphi(p^n) = p^n - p^{n-1}$

▲ $1 \le p, 2p, 3p, \dots p^{n-1} < p^n$ и все не взаимно просты с p^n.

Всего таких чисел $p^{n-1} \Rightarrow$ # чисел взаимно простых с p^n равно $p^n - p^{n-1}$ ■

Теорема: $\varphi(n) = n \cdot \prod\limits_{p/n} \left(1 - \frac{1}{p}\right)$, $n > 1$, p - простое

△ Из ОТА: $n = p_1^{d_1} \cdot \ldots \cdot p_k^{d_k}$ где $p_1 < \ldots < p_k$ и $d_1, \ldots d_k \in \mathbb{N}$

Тогда $\varphi(n) = \varphi(p_1^{d_1}) \cdot \ldots \cdot \varphi(p_k^{d_k}) =$

$$= \prod_{i=1}^{k} \varphi(p_i^{d_i}) = \prod_{i=1}^{k} (p_i^{d_i} - p_i^{d_i - 1}) = \prod_{i=1}^{k} \left(p_i^{d_i}\left(1 - \frac{1}{p_i}\right)\right) = n \prod_{i=1}^{k}\left(1 - \frac{1}{p_i}\right)$$

(по следствию)

■

Билет 6. Т. Лагранжа о числе корней

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

△ (от противного) Пусть $x_1, \ldots x_{n+1}$ - решения

Тогда $f(x) = c_1 (x - x_1)(x - x_2) \cdot \ldots \cdot (x - x_n) +$

$+ c_2 (x - x_1)(x - x_2) \cdot \ldots \cdot (x - x_{n-1}) +$

$+ \ldots + c_n (x - x_1) + c_{n+1}$

Если подставить x_1, то $f(x_1) = c_{n+1} \equiv 0 (p)$

Если x_2, то $f(x_2) = c_n (x_2 - x_1) + c_{n+1} \equiv c_n (x_2 - x_1) \equiv 0 (p)$

при этом $(x_2 - x_1) \not\equiv 0 (p) \Rightarrow c_n \equiv 0 (p)$ и так далее.

Если подставить x_{n+1}, то первое произведение скобок $\not\equiv 0 (p) \Rightarrow c_1 = c_2 = \ldots = c_{n+1} = 0 \Rightarrow f(x) \equiv 0$

$\Rightarrow$ корней $\leqslant n$ штук

■