Функция Эйлера (лекция).

Деление. На прошлой лекции мы научились делить в $\mathbb{Z}_p$. А вот в $\mathbb{Z}_6$ обнаружили некоторые проблемы. Оказывается, что можно делить и по непростому модулю, но не все числа.

Рассмотрим **множество $\mathbb{Z}_m^*$ всех чисел, взаимно простых с m и не превосходящих m. Количество элементов в этом множестве** обозначается $\varphi(m)$ и называется **функцией Эйлера**. Пусть f – отображение $\mathbb{Z}_m^* \to \mathbb{Z}_m^*$, заданное как: $f(x) = ax$, где a элемент $\mathbb{Z}_m^*$. На множестве $\mathbb{Z}_m^*$ f будет биекцией, а в $\mathbb{Z}_m^*$ возможно деление. Например $\mathbb{Z}_6^* = \{1, 5\}$ и в нём $1 : 5 = 5$, так как $5 \cdot 5 \equiv 1 (mod\ 6)$.

Задачка 1. Докажите, что f биекция.

Теорема Эйлера. А не получится ли в $\mathbb{Z}_m^*$ что-нибудь похожее на малую теорему Ферма? Попробуем провести рассуждения, аналогичные доказательству из предыдущей лекции.

Из задачи 1 следует, что множество $\{x_1, x_2, ..., x_{\varphi(m)}\}$ всевозможных элементов $\mathbb{Z}_m^*$ совпадает с множеством $\{a \cdot x_1, a \cdot x_2, ..., a \cdot x_{\varphi(m)}\}$. Поэтому совпадает и произведение всех элементов этих множеств. То есть $x_1 \cdot x_2 \cdot ... \cdot x_{\varphi(m)} \equiv a \cdot x_1 \cdot a \cdot x_2 \cdot ... \cdot a \cdot x_{\varphi(m)}$. Вспомним, что все x_i взаимнопросты с m. Поэтому мы можем сократить на них обе части равенства и получить, что $a^{\varphi(m)} \equiv 1 (mod\ m)$. Это утверждение - **теорема Эйлера**.

Ну и что? – спросите вы. Что может дать утверждение про совершенно неизвестную нам функцию? Ну как, попробуем о ней что-нибудь разведать?

Функция Эйлера. Для начала, посмотрим, как ведёт себя эта функция при маленьких значениях аргумента.

$\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$, $\varphi(6) = 2$, $\varphi(7) = 6$, $\varphi(8) = 4$, $\varphi(9) = 6$, $\varphi(10) = 4$. Пока никакой закономерности не видно.. Но вспомните, в случае простых чисел до сих пор ситуация была проще, чем в случае составных. Что же на этот раз? $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(5) = 4$, $\varphi(7) = 6$,... Кажется, нам опять повезло. Теперь легко построить гипотезу, чему равна наша функция для простых чисел: $\varphi(p) = p - 1$. А чётко сформулированную гипотезу ничего не стоит доказать. Ясно, что все числа, меньшие p, взаимно просты с ним. Поэтому $\varphi(p) = p - 1$. А что, если взять случай посложнее когда $m = p^n$? Среди чисел, меньших p^n, каждое p-ое число не взаимно просто с p^n. А, значит, $\varphi(p^n) = p^n - p^n/p = p^n - p^{n-1}$.

Перед тем как переходить к общему случаю, докажем, что **для взаимно простых чисел n и m :** $\varphi(nm) = \varphi(n)\varphi(m)$. Запишем все числа от 1 до nm в таблицу $n * m$:

1	2	3	...	m-1	m
m+1	m+2	m+3	...	2m-1	2m
...	...	...	...	...	...
(n-1)m+1	(n-1)m+2	(n-1)m+3	...	nm-1	nm

Во-первых, посмотрим сколько *чисел, взаимно простых с m* может быть *в произвольном столбце* таблицы может быть. Пусть в столбце есть число k, взаимно простое с m. Тогда все остальные числа в этом столбце имют вид $\pm mb + k$ и поэтому также взаимно просты с m. Таким образом, *либо все* числа в столбце взаимно просты с m, *либо ни одного*.

Во-вторых, попробуем понять, сколько в таблице *столбцов, в которых все числа взаимно просты с m*. Но из только что доказанного следует, что их столько же, сколько столбцов, в которых верхнее число взаимно просто с m. А значит их *в точности* $\varphi(m)$.

В-третьих, убедимся в том, что *для любого столбца множество его элементов по модулю n совпадает с множеством* $\mathbb{Z}_n$. А вот почему. Каждый столбец выглядит, как начало бесконечной последовательности $a, a+m, a+2m, ..., a+km, ...$ Что можно сказать о такой последовательности? 1. У неё нет предпериода, потому что по числу b всегда можно восстановить предыдущее число $b-m$. 2. Она содержит конечное число значений, а значит, зациклится. Причём внутри периода не может быть двух одинаковых элементов (догадываетесь, с чем это связно?). 3. В ней есть любой наперёд заданный элемент b из $\mathbb{Z}_n$, потому что уравнение $nx+my=b$ для взаимно простых n и m всегда имеет решение. Таким образом, первые n элементов нашей последовательности (а значит, и все элементы столбца) суть все элементы $\mathbb{Z}_n$.

Наконец, в-четвёртых, определим сколько *в каждом столбце чисел взаимно простых с* n. Из вышесказанного следует, что их столько же, сколько в множестве $\mathbb{Z}_n$ существует чисел, взаимно простых с n – то есть, *в точности,* $\varphi(n)$.

Теперь ясно, что числа взаимно простые с mn (то есть взаимно простые и с n, и с m), лежат в тех столбцах, где есть числа, взаимно простые с m. Напомним, что таких столбцов ровно $\varphi(m)$. При этом в каждом столбце нас интересуют только числа взаимно простые с n (а их в каждом столбце ровно $\varphi(n)$ штук). Следовательно, всего чисел меньших nm и взаимно простых с nm $\varphi(nm) = \varphi(n)\varphi(m)$. Итак, мы доказали два свойства функции Эйлера:

Свойство 1. Для простого p верно, что $\varphi(p^n) = p^n - p^{n-1}$

Свойство 2. Для n, m, таких что НОД$(n,m)=1$ верно, что $\varphi(nm) = \varphi(n)\varphi(m)$.

Задачка 2. Выведите из доказанных свойств, что для произвольного $m = p_1^{n_1} \cdot p_2^{n_2} \cdot ... \cdot p_k^{n_k}$ верно, что

а) $\varphi(m) = (p_1^{n_1} - p_1^{n_1-1}) \cdot (p_2^{n_2} - p_2^{n_2-1}) \cdot ... \cdot (p_k^{n_k} - p_1^{n_k-1})$.

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