МАЛАЯ ТЕОРЕМА ФЕРМА (МТФ). ЧАСТЬ 3

На этом уроке мы завершим 3-е доказательство МТФ, а также, приведем еще одно красивое доказательство этой важной теоремы.

УТВЕРЖДЕНИЕ О ВИДЕ ГРАФА ОСТАТКОВ ПО МОДУЛЮ p

Итак, докажем утверждение, которое следует из наших рассмотрений на предыдущем уроке:

УТВЕРЖДЕНИЕ

Если p — простое, a не делится на p, то граф умножения на число a есть объединение непересекающихся циклов равной длины.

ДОКАЗАТЕЛЬСТВО

Вспомним свойство, которое мы неоднократно использовали в нашем курсе:

Если $\alpha \not\equiv \beta \bmod p$, то $\alpha a \not\equiv \beta a \bmod p$ при $a \not\equiv 0 \bmod p$.

То есть разные остатки переходят в разные, и ситуация, когда две стрелочки приходят в одну точку, невозможна.

Если мы стартовали из 1, мы попадаем в a, затем в a^2 (которое может быть равным 1, но не может быть равным a). Рано или поздно мы вернемся в 1 и никогда не попадем в какую-то из промежуточных степеней a.

Если все остатки не исчерпаны, мы можем взять другую точку и очевидно получим еще один цикл.

Почему этот цикл будет иметь такую же длину?

Пусть первый цикл имеет вид:
$1 \to a \to a^2 \to a^3 \to \ldots \to a^r \equiv 1 \bmod p$.

Тогда любой другой цикл имеет вид:
$b \to ba \to ba^2 \to ba^3 \ldots ba^r \equiv b \bmod p$.

Цикл не мог закончиться раньше, т.к. иначе можно было сократить на b и получить, что $a^l \equiv 1 \bmod p$, где $l < r$, что невозможно.

Таким образом мы постепенно исчерпываем множество всех ненулевых остатков одинаковыми порциями по r.

Доказано.

ЗАВЕРШЕНИЕ 3-ГО ДОКАЗАТЕЛЬСТВА МТФ

Пусть $1 \to a \to a^2 \to a^3 \to \ldots \to a^r \equiv 1 \bmod p$.

То есть число a в степенях от 0 до $r - 1$ дает различные остатки, a в степени r впервые обращается в 1 по модулю p.

ОПРЕДЕЛЕНИЕ

Порядком ненулевого остатка a по модулю p называется такое минимальное число r, что $a^r \equiv 1 \bmod p$.

Обозначение: $r = Ord(a)$.

Получаем, что мы разбили все $p - 1$ ненулевых остатков на непересекающиеся циклы длины r.

Значит, $(p - 1) \vdots r$.

Имеем $a^{p-1} = a^{rl} \equiv 1^l \bmod p \equiv 1 \bmod p$. МТФ доказана.

СЛЕДСТВИЕ

$a^m \equiv 1 \bmod p \Rightarrow m \vdots Ord(a)$.

ОПРЕДЕЛЕНИЕ

Остаток a по модулю p называется первообразным корнем, если $Ord(a) = p - 1$.

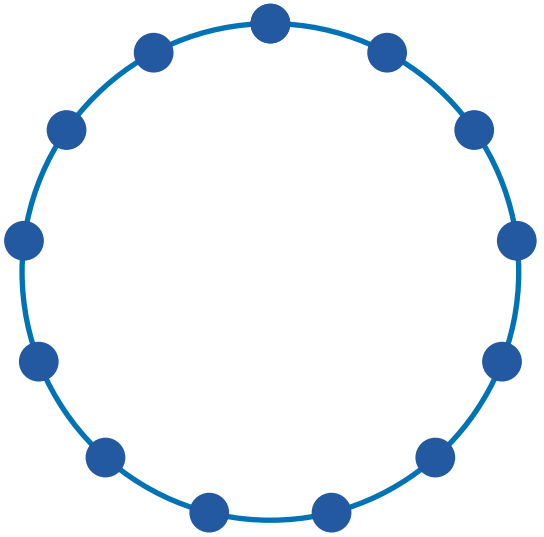
В будущем мы докажем, что для каждого простого модуля существует хотя бы один первообразный корень.

Первообразные корни являются порождающими элементами для группы остатков, которая, таким образом, в случае простого модуля является циклической.

4-Е ДОКАЗАТЕЛЬСТВО МТФ (КАРУСЕЛЬ)

Рассмотрим карусель, а точнее, колесо обозрения с простым числом кабинок p. Например, $p = 13$.

Пусть a — количество красок, в которые мы красим кабинки ($a \not\equiv 0 \bmod p$).



Вопрос: сколько существует различных способов раскрасить это колесо обозрения в a цветов?

Для каждой из кабинок a вариантов, значит, всего получаем a^p раскрасок.

Теперь вспоминаем о том, что колесо можно поворачивать. Каждая раскраска порождает p сдвигов.

Если бы у нас было колесо обозрения с 12 кабинками, раскрашенное в 3 чередующихся цвета — красный, синий, желтый — то сдвиг на 3 такта давал раскраску, совпадающую с первоначальной. И все 12 сдвигов давали бы только три разные раскраски.

УТВЕРЖДЕНИЕ

Если число кабинок p — простое, то все сдвиги дают различные раскраски, либо раскраска одноцветная.

ДОКАЗАТЕЛЬСТВО

Докажем от противного. Пусть сдвиг на m тактов раскраску не меняет. Тогда сдвиг на $2m$, $3m$, … тоже раскраску не меняет. Так как НОД$(p, m) = 1$, то существуют такие n, $s \in \mathbb{Z}$, что $mn + ps = 1$.

Поворачиваем колесо n раз на m, что не меняет раскраску. Но согласно нашему равенству это то же самое, что совершить s полных поворотов (на p тактов) и еще на 1 такт.

Получаем, что тогда сдвиг на 1 раскраску не меняет. А значит, раскраска одноцветная. Утверждение доказано.

Осталось посчитать эти раскраски. Существует a одноцветных раскрасок, а все остальные разбиваются на порции по p различных раскрасок. Таким образом: $a^p = a + p \cdot M$, где M — некоторое целое число. Отсюда $a^p \equiv a \bmod p$. Что и требовалось доказать.

На этом мы завершаем комплекс из 4-х доказательств МТФ.

На следующем уроке мы вернемся к изучению многочленов над конечным полем и будем получать далеко идущие выводы из малой теоремы Ферма.