МАЛАЯ ТЕОРЕМА ФЕРМА (МТФ). ЧАСТЬ 2

ВТОРОЕ ДОКАЗАТЕЛЬСТВО МТФ

Итак, мы доказываем малую теорему Ферма через формулу бинома Ньютона.

МАЛАЯ ТЕОРЕМА ФЕРМА (МТФ).

Пусть p — простое, a — любое целое.
Тогда $a^p - a \vdots p$.

Запишем бином Ньютона для степени p:

$$(a+b)^p = \sum_{k=0}^{p} C^k_p a^{p-k} b^k,$$

где $C^k_p = \dfrac{p!}{k!(p-k)!}$.

УТВЕРЖДЕНИЕ

$\forall\, k = 1, 2, \ldots, p-1$ C^k_p делится на p.

ДОКАЗАТЕЛЬСТВО

Запишем C^k_p в виде $C^k_p = \dfrac{p(p-1)!}{k!(p-k)!}$

C^k_p — целое $\Rightarrow$ $p(p-1)!$ делится на $k!(p-k)!$.

Но НОД$(p, k!(p-k)!) = 1$, т.к. в произведении $k!(p-k)!$ присутствуют только множители, меньшие p, а p — простое.

А значит, $(p-1)!$ делится на $k!(p-k)!$ $\Rightarrow$

$$\frac{(p-1)!}{k!(p-k)!} = l \in \mathbb{Z} \Rightarrow C^k_p = pl,$$

что и требовалось доказать.

Из утверждения следует, что $(a+b)^p \equiv a^p + b^p \bmod p$.

Тогда: $2^p = (1+1)^p \equiv (1^p + 1^p) \bmod p \equiv 2 \bmod p$;
$3^p = (2+1)^p \equiv (2^p + 1^p) \bmod p \equiv 3 \bmod p$;
...

По индукции можем заключить, что

$a^p = ((a-1)+1)^p \equiv ((a-1)^p + 1^p) \bmod p \equiv$
$\equiv (a - 1 + 1) \bmod p \equiv a \bmod p$.

МТФ доказана.

ТРЕТЬЕ ДОКАЗАТЕЛЬСТВО МТФ (ГРАФЫ)

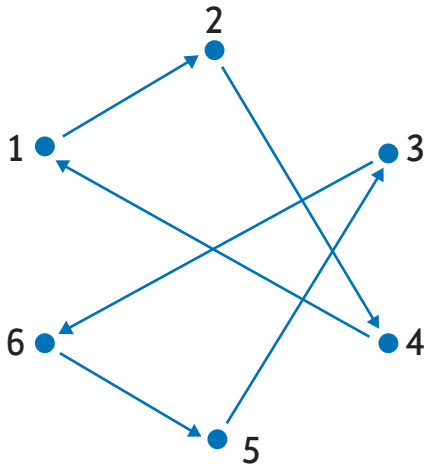
Следующее доказательство МТФ мы проведем с использованием графов.

Графами называются диаграммы, состоящие из вершин (точек) и ребер (отрезков, которые могут соединять вершины).

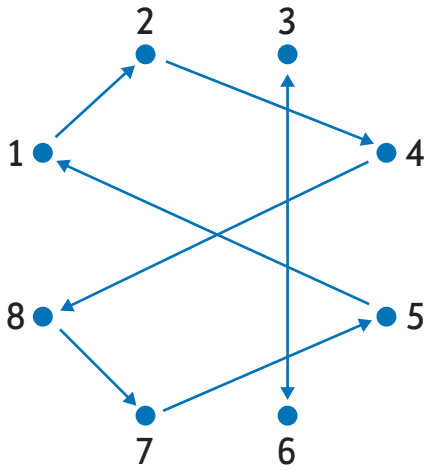
Графы называются **ориентированными**, если их ребра — направленные, т.е. показывают стрелочкой направление от одной вершины к другой.

Возьмем несколько значений модуля p и рассмотрим графы, вершинами которых являются соответствующие ненулевые остатки, а стрелочками отмечены переходы $x \to ax$.

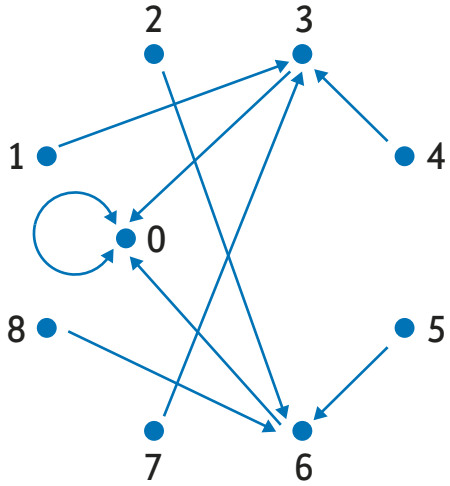
Пусть $p = 7$, $a = 2$. Для каждого из остатков 1-6 отметим стрелочками на графе $x \to 2x$. Мы получили два непересекающихся цикла длины 3.



Пусть, например, $p = 9$, $a = 2$. Для каждого из остатков 1-8 отметим стрелочками на графе $x \to 2x$. Мы снова получили два непересекающихся цикла, но разной длины.

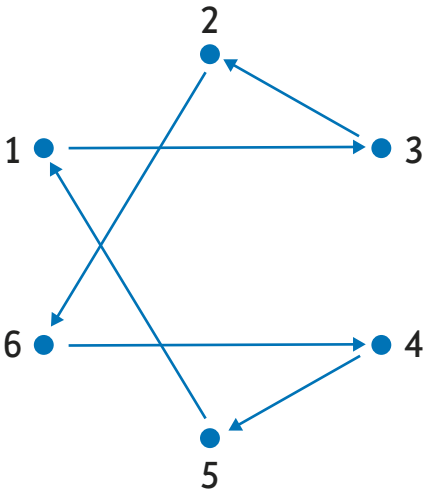


Пусть теперь $p = 9$, $a = 3$. Нам придется добавить в граф остаток 0:



Видим, что в этом случае все цепочки заканчиваются в 0. Это связано с тем, что 9 — составное число.

Вернемся к простому модулю: $p = 7$, $a = 3$. Получим один большой непересекающийся цикл:



Таким образом, 6 первых степеней числа 3 дают все ненулевые остатки от деления на 7, а потом цикл повторяется:

$3^0 = 1$, $3^1 = 3$, $3^2 = 2$, $3^3 = 6$, $3^4 = 4$, $3^5 = 5$,

а затем снова $3^6 = 1$ по mod 7.

Заметим, что при возведении $a = 2$ в степень мы не получили все остатки ($2^3 \equiv 1 \bmod p$, тем самым, цикл замкнулся).

Остаток, порождающий своими степенями множество всех ненулевых остатков по данному модулю, называется **первообразным корнем**.

В частности, остаток 3 является первообразным корнем по модулю $p = 7$.

На основе наших наблюдений можно сформулировать утверждение, которое будет доказано на следующем уроке:

УТВЕРЖДЕНИЕ

Если p — простое, a не делится на p, то в графе умножения на число a состоит из нескольких циклов равной длины, не пересекающих друг друга.