Малая теорема Ферма, системы вычетов

Малая теорема Ферма

Теорема. **(Малая теорема Ферма, МТФ)** Для любого целого a и простого p выполнено

$$a^p \equiv a \pmod p.$$

Первое доказательство МТФ *(по индукции)*. Докажем для начала утверждение для натуральных a (и нуля). Доказательство будем вести индукцией по a. Все сравнения — по модулю p.

База. $a = 0$: очевидно, $0^p \equiv 0$.

Переход. $a \to a + 1$

Предположение индукции. $a^p \equiv a$.

Нам надо доказать, что $(a+1)^p \equiv a + 1$. Согласно биному Ньютона, имеем:

$$(a+1)^p = a^p + C_p^1 a^{p-1} + \ldots + C_p^{p-1} a + 1 \equiv$$

Нетрудно показать, что при $1 < k < p$ число C_p^k делится на p, то есть сравнимо с 0 по модулю p и

$$\equiv a^p + 1 \equiv a + 1,$$

где последнее сравнение следует из предположения индукции. Переход доказан.

Теперь осталось проверить утверждение для отрицательных a. Для этого достаточно заметить, что для любого простого $p > 2$ выполнено $(-a)^p = -a^p \equiv -a$, а при $p = 2$ утверждение МТФ очевидно. ■

Системы вычетов. Теорема Эйлера

Второе доказательство МТФ *(через приведенную систему вычетов)*. Все сравнения по модулю p.

Пусть, для начала, $(a, p) = 1$. Рассмотрим тогда набор чисел a, $2a$, …, $(p-1)a$. Легко видеть, что ни одно из этих чисел не делится на p. Покажем, что все они дают различные остатки при делении на p. Действительно, если $ai \equiv aj$, то, поскольку $(a, p) = 1$, на a можно сократить и получить $i \equiv j$, чего быть не может (так как $1 \leqslant i,\ j \leqslant p-1$). Тогда a, $2a$, …, $(p-1)a$ дают все ненулевые остатки при делении на p, то есть 1, 2, …, $p-1$.

Значит,

$$\begin{aligned} a \cdot 2a \cdot \ldots \cdot (p-1)a &\equiv 1 \cdot 2 \cdot \ldots \cdot (p-1) \pmod p \\ a^{p-1} \cdot (p-1)! &\equiv (p-1)! \pmod p \\ a^{p-1} &\equiv 1 \pmod p, \end{aligned}$$

где последний переход получается сокращением на $(p-1)!$, мы можем это сделать, поскольку $(p, (p-1)!) = 1$.

Замечание. Итак, мы доказали, что если $(a, p) = 1$, т.е. $a \not\vdots p$, то $a^{p-1} - 1 \vdots p$, а значит и $a^p - a = a \cdot (a^{p-1} - 1) \vdots p$. Если же $a \vdots p$, то $a^p - a = a \cdot (a^{p-1} - 1)$ также делится на p. Учитывая это рассуждение, иногда под малой теоремой Ферма понимают следующее утверждение: если $p \in \mathbb{P}$, $(\mathbf{a}, \mathbf{p}) = \mathbf{1}$, то $a^{p-1} \equiv 1 \pmod p$. ■

Определение. *Полной системой вычетов* по модулю n называется набор целых чисел, в котором каждый остаток при делении на n встречается ровно один раз.

Очевидно, что множество является приведенной системой вычетов по модулю n тогда и только тогда, когда в нем ровно n чисел, дающих попарно различные остатки при делении на n.

Утверждение. Пусть A — полная система вычетов по модулю n. Тогда для любого числа b множество $A + b = \{x + b \mid x \in A\}$ также является полной системой вычетов по модулю n.

Доказательство. Пусть $A = \{a_1, a_2, \ldots, a_n\}$. Покажем, что в множестве $A+b = \{a_1 + b, \ldots, a_n + b\}$ все числа дают попарно различные остатки при делении на n. Из этого, с учетом того, что их ровно n и будет следовать, что $A + b$ — полная система вычетов по модулю n.

Итак, пусть наше предположение не верно и существуют числа, дающие одинаковые остатки при делении на n. Пусть это числа $a_i + b$ и $a_j + b$. Тогда $a_i + b \equiv a_j + b$ и $a_i \equiv a_j$ (все сравнения по модулю n). Однако последнее невозможно, так как A — полная система вычетов по модулю n и в ней не может быть чисел, сравнимых по модулю n. ■

Утверждение. Пусть A — полная система вычетов по модулю n. Тогда для любого числа b, **взаимно простого с n**, множество $bA = \{bx \mid x \in A\}$ также является полной системой вычетов по модулю n.

Замечание. Легко показать, что условие взаимной просты является необходимым, то есть верно обратное утверждение: если bA — полная система вычетов, то $(b, n) = 1$.

Доказательство. Доказательство аналогично доказательству предыдущего утверждения. Нам достаточно показать, что числа $ba_1, \ldots, ba_n$ дают попарно различные остатки при делении на n. Если $ba_i \equiv ba_j$, то $a_i \equiv a_j$, сокращать на b мы можем из-за того, что $(b, n) = 1$. ■

Определение. *Приведенной системой вычетов* по модулю n называется набор целых чисел, в котором каждый остаток при делении на n, **взаимно простой с n**, встречается ровно один раз.

Определение. Количество элементов в приведенной системе вычетов по модулю n обозначается $\varphi(n)$. $\varphi(n)$ называется *функцией Эйлера*.

Утверждение. Пусть A — приведенная система вычетов по модулю n. Тогда для любого числа b, взаимно простого с n, множество $bA = \{bx \mid x \in A\}$ также является приведенной системой вычетов по модулю n.

Доказательство. Доказательство аналогично доказательству утверждения для полной системы вычетов. Действительно, все числа в множестве bA дают попарно различные остатки при делении на n. Для окончания доказательства осталось заметить, что все они взаимно просты с n. Действительно, если $(ba, n) \vdots p$ для некоторого простого p, то $n \vdots p$ и либо $a \vdots p$, либо $b \vdots p$, но тогда либо $(a, n) \vdots p$, либо $(b, n) \vdots p$, противоречие. ■

Теорема. **(Теорема Эйлера)** Для любого целого n и любого целого a, взаимно простого с n выполнено

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Доказательство. Пусть $B = \{b_1, b_2, \ldots, b_{\varphi(n)}\}$ — приведенная система вычетов по модулю n. Тогда $aB = \{ab_1, ab_2, \ldots, ab_{\varphi(n)}\}$ также является приведенной системой вычетов по модулю n. Значит, произведение чисел в них сравнимы по модулю n:

$$b_1 \cdot b_2 \cdot \ldots \cdot b_{\varphi(n)} \equiv ab_1 \cdot ab_2 \cdot \ldots \cdot ab_{\varphi(n)} \pmod{n}.$$

Откуда, после алгебраических преобразований и сокращения на $b_1 \cdot \ldots \cdot b_{\varphi(n)}$ *(почему оно взаимно просто с n?)* и получаем утверждение теоремы. ■

Обратный элемент. Теорема Вильсона

Мотивация. Нам бы хотелось уметь решать сравнение $ax \equiv c \pmod{m}$.

В случае обычного уравнения $ax = c$ нам было достаточно умножить это уравнение на $a^{-1} = 1/a$ и получить $ax/a = c/a$, то есть $x = c/a$. Соответственно, если существует такое число b, что $ab \equiv 1 \pmod{n}$, то нам достаточно умножить исходное сравнение на него и получить, что $x \equiv bc \pmod{n}$.

Определение. Число b называется *элементом, обратным к элементу a по модулю n*, если $ab \equiv 1 \pmod{n}$.

Утверждение. Для любых целых a и n, таких, что $(a, n) = 1$, существует обратный элемент к a по модулю n.

Доказательство. Пусть $B = \{b_1, b_2, \ldots, b_{\varphi(n)}\}$ — приведенная система вычетов по модулю n. Тогда $aB = \{ab_1, ab_2, \ldots, ab_{\varphi(n)}\}$ также является приведенной системой вычетов по модулю n. Так как $(1, n) = 1$ (остаток 1 лежит в приведенной системе вычетов), то сушествует такое число b_k, что $ab_k \equiv 1 \pmod{n}$, то есть b_k является обратным элементом к a по модулю n. ■

Замечание. 1. Поскольку в любой приведенной системе вычетов существует ровно одно число, дающее остаток 1 при делении на n, то остаток обратного элемента по модулю n определен однозначно.

2. *("Деление на ноль")* Покажем, что если $(a, n) > 1$, то не существует элемента, обратного к a по модулю n. В частности, если $a \underset{n}{\equiv} 0$.

Действительно, если $(a, n) \vdots p$ для некоторого простого p, то для любого целого b число ab делится на p, если же при этом и $ab - 1 \vdots n \vdots p$, то тогда и $1 = ab - (ab - 1) \vdots p$, противоречие.

3. Если b является обратным элементом к a, то a является обратным элементом к b.

Теорема. **(Теорема Вильсона)** Пусть $p \in \mathbb{P}$. Тогда

$$(p-1)! \equiv -1 \pmod{p}.$$

Доказательство. Сопоставим каждому числу от 1 до $p-1$ его обратный элемент (с учетом замечания 1 этот элемент единственный). Тогда, с учетом замечания 3, все числа разобьются на пары, **за исключением тех, для которых обратный элемент совпадает с самим элементом.**

Если для элемента x обратным является он сам, то $x^2 \underset{p}{\equiv} 1$ или $x^2 - 1 \vdots p$. Так как $x^2 - 1 = (x-1)(x+1)$, а p — простое, то либо $x - 1 \vdots p$, либо $x + 1 \vdots p$, или $x \underset{p}{\equiv} 1$ и $x \underset{p}{\equiv} p - 1$, соответственно.

Тогда, имеем:

$$\begin{aligned}(p-1)! &\equiv 1 \cdot (p-1) \cdot (x_1 x_2) \cdot \ldots \cdot (x_{2k-1} x_{2k}) \equiv \\ &\equiv 1 \cdot (-1) \cdot 1 \cdot 1 \cdot \ldots \cdot 1 \equiv \\ &\equiv -1 \pmod{p},\end{aligned}$$

что и требовалось. ■

Еще одно доказательство МТФ

Третье доказательство МТФ *(через циклы)*.[1] Пусть $(a, p) = 1$. Будем доказывать, что $a^{p-1} \underset{p}{\equiv} 1$.

Рассмотрим ориентированный граф, вершинами которого являются остатки при делении на p, а из вершины x в вершину y ведет ребро, если $y \underset{p}{\equiv} ax$. Таким образом, из каждой вершины выходит ровно одно ребро (сколько приходит мы пока не знаем).

Возьмем какую-нибудь вершину b и выйдем из нее по ребру в вершину ba, из нее — в вершину ba^2, оттуда — в ba^3 и т.д. Поскольку вершин конечно, то рано или поздно мы придем в какую-то вершину, в которой уже были.

Может ли эта вершина быть отлична от b? Если да, то существует такая вершина y и хотя бы две такие вершины x_1 и x_2, что и из x_1, и из x_2 ребро ведет в y. Но тогда $ax_1 \underset{p}{\equiv} ax_2 \underset{p}{\equiv} y$. Откуда, после сокращения на a, получаем $x_1 \underset{p}{\equiv} x_2$, чего быть не может, противоречие. (Именно тут мы воспользовались, что $(a, p) = 1$.)

Значит, мы вернемся именно в b. Таким образом, все вершины разбились на несколько непересекающихся *(почему непересекающихся?)* циклов. В частности, вершина 0 представляет из себя цикл длины 1.

Рассмотрим цикл, в котором находится 1. В нем каждый элемент является некоторой степенью a, поэтому существует такое число $d > 0$, что $a^d \underset{p}{\equiv} 1$. Из всех таких d выберем наименьшее. Тогда среди остатков 1, a, a^2, …, a^{d-1} нет одинаковых, то есть цикл, в котором находится 1, имеет длину d.

Какую длину тогда имеют другие циклы? Пусть b — некоторый ненулевой остаток и цикл, в котором он находится, имеет длину d_1. Тогда $ba^{d_1} \underset{p}{\equiv} b$, то есть (после сокращения на b) имеем $a^{d_1} \underset{p}{\equiv} 1$, то есть $d \leqslant d_1$. (Именно тут мы пользуемся, что p — простое и любой ненулевой остаток при делении на p взаимно прост с p.)

С другой стороны, так как $a^d \underset{p}{\equiv} 1$, то $ba^d \underset{p}{\equiv} b$, то есть длина цикла, в котором находится b не может быть больше d, а значит $d_1 \leqslant d$ и $d_1 = d$.

Таким образом, наш граф представляет из себя вершину 0, а также несколько (пусть k) групп вершин, каждая из которых представляет из себя цикл длины d. Значит, $dk = p - 1$. Откуда, возводя сравнение $a^d \underset{p}{\equiv} 1$ в степень k, получаем требуемое утверждение: $a^{p-1} = a^{dk} \underset{p}{\equiv} 1$. ■

[1] Картинки когда-нибудь появятся.

Замечание. Для доказательства теоремы Эйлера ($a^{\varphi(n)} \underset{n}{\equiv} 1$) достаточно рассматривать ориентированный граф, в котором вершины — остатки, взаимно простые с n.