01.04.19

<u>Утверждение</u>: Для любых a, b, m ϵ Z таких, что (b, m) = 1, существует единственный x ϵ Z такой, что bx = a mod m ($x = \frac{a}{b}$ mod m).

Доказательство:

Как искать x?

bx = a mod m ↔ bx – a ⋮ m ↔ ∃ q: bx – a = qm ↔ ∃ q: bx – qm = a — диафантово уравнение

$\acute{q}$ = -q

a ⋮ (b, m) = 1

Диофантовы уравнения мы уже умеем решать:

$$\begin{cases} x = x_0 + \frac{m}{(m,b)} k = x_0 + km \\ \acute{q} = \acute{q}_0 - \frac{b}{(m,b)} k \end{cases}$$

Итого, $x = x_0 + km$ ↔ $x = x_0$ mod m.

Замечание:

Если m и b — не взаимно простые числа (т.е. (b, m) ≠ 1), то 1) решения может не быть, если a не делится нацело на (b, m); 2) если решения есть, то их несколько: x_0, $x_0 + \frac{m}{(m,b)}$, $x_0 + 2\frac{m}{(m,b)}$, …, $x_0 + \frac{m}{(m,b)}((m, b) - 1)$, $x_0 + \frac{m}{(m,b)}(m, b)$

Примеры к замечанию:

6x = 4 mod 15 4 не делится нацело на (6, 15) = 3 → решений нет	6x = 3 mod 15 3 делится нацело на (6, 15) = 3 → частные решения: x = 3, x = 8, x = 13 и .т.д.

<u>Итак</u>, Z_p — поле, если p — простое число.

Доказательство:

Нужно проверить, что есть обратные элементы по умножения для всех кроме 0, т.е. для любого a ϵ Z_p , если a ≠ 0 (a ≠ 0 mod p), то существует b такое, что ab = 1 mod p.

Это верно, т.к. (a, p) = 1 ч.т.д.

Приведённая система вычетов

<u>Определение</u>: Приведённая система вычетов — это полная система вычетов mod m без чисел, которые не взаимно простые с m.

Примеры:

{0, 1, 2, 3, 4, 5} — полная система вычетов mod 6

{1, 5} — приведённая система вычетов mod 6

{0, 5, 10, 15, 20, 25} — полная система вычетов mod 6

{5, 25} — приведённая система вычетов mod 6

Утверждение: Все приведённые системы вычетов по mod m имею одинаковое количество элементов.

Доказательство:

Полная система вычетов = $\{a_0, a_1, \dots, a_{m-1}\}$, $a_i = i \bmod m$

Полная система вычетов 2 = $\{b_0, b_1, \dots, b_{m-1}\}$, $b_i = i \bmod m$

Проверим, что $(b_i, m) = 1$ (это значит, что мы вычёркиваем или не вычёркиваем a_i, b_i одновременно).

Пусть $a_i ⋮ d$, $m ⋮ m$

$b_i = a_i \bmod m = i \bmod m \to b_i - a_i ⋮ m \to \exists\, q: b_i - a_i = mq \to b_i = mq + a_i \to b_i ⋮ d$

Тогда $(b_i, m) ⋮ d$.

И наоборот, если $(b_i, m) ⋮ d$, то $(a_i, m) ⋮ d$ ч.т.д.

<u>Обозначение</u>: *φ(n) — функция Эйлера* — количество элементов в приведённой системе вычетов mod m.

Примеры: $\varphi(6) = 2$, $\varphi(10) = 4$

Утверждение: Если M — приведённая система вычетов mod m, $a \in Z$ такое, что $(a, m) = 1$, тогда a*M также приведённая система вычетов.

Доказательство:

1) Проверим, что после умножения все остатки разные, т.е. $ax \neq ay \bmod m$, где $x, y \in M$ $(x \neq y)$

От противного: $ax = ay \bmod m \to ax - ay ⋮ m \to a*(x-y) ⋮ m \to (x - y) ⋮ m \to x = y \bmod m$ — ! противоречие!

2) Почему $(ax, m) = 1$, если $(x, m) = 1$?

От противного:

Пусть $ax ⋮ d$ и $m ⋮ d$

Выберем простой общий делитель p такой, что $ax ⋮ p$, $m ⋮ p$.

Если $ax ⋮ p$, то $a ⋮ p$ ($m ⋮ p$!!) или $x ⋮ p$ (!!$m ⋮ p$).

3) В a*M — количество элементов равно $\varphi(m)$. Все взаимно просты с $m \to$ a*M — приведённая система вычетов ч.т.д.

Как считать φ(m)?

1) $\varphi(p)$ - ?

Пусть p — простое число.

0, 1, 2, …, p-1 — взаимно простые.

Итого, $\varphi(p) = p-1$

2) $\varphi(p^k)$ - ?

$1, 2, 3, \dots, x, \dots, p^k$

Пусть $(x, p^k) \neq 1 \to (x, p^k) ⋮ p \to x ⋮ p$

Всего чисел делящихся на p (т.е. не взаимно простых с p) p^{k-1}.

$\varphi(p^k) = p^{k-1}(p-1)$

3) Утверждение: $\varphi(ab) = \varphi(a) * \varphi(b)$ для взаимно простых a и b (функция Эйлера — мультипликативная).

Пример: $\varphi(10) = \varphi(2) * \varphi(5) = 1*4 = 4$