01.04.19

***Утверждение***: Для любых a, b, m ϵ Z таких, что (b, m) = 1, существует единственный x ϵ Z такой, что bx = a mod m (x = mod m).

Доказательство:

Как искать х?

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

= -q

a (b, m) = 1

Диофантовы уравнения мы уже умеем решать:

x = x0 + k = x0 + km

= - k

Итого, x = x0 + km ↔ x = x0 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: x0, x0 + , x0 + 2 , …, x0 + ((m, b) – 1), x0 + (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. |

Итак, Zp — поле, если р — простое число.

Доказательство:

Нужно проверить, что есть обратные элементы по умножения для всех кроме 0, т.е. для любого a ϵ Zp , если а ≠ 0 (а ≠ 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**

***Определение***: 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 = {a0, a1, …, am-1}, ai = i mod m

Полная система вычетов 2 = {b0, b1, …, bm-1}, bi = i mod m

Проверим, что (bi, m) = 1 (это значит, что мы вычёркиваем или не вычёркиваем аi, bi одновременно).

Пусть аi ⁝ d, m ⁝ m

bi = аi mod m = i mod m → bi - аi ⁝ m → q: bi - аi = mq → bi = mq + аi → bi ⁝ d

Тогда (bi, m) ⁝ d.

И наоборот, если (bi, m) ⁝ d, то (аi, m) ⁝ d ч.т.д.

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

Примеры: φ(6) = 2, φ(10) = 4

***Утверждение***: Если M — приведённая система вычетов mod m, a ϵ 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 ≠ ay mod m, где x, y ϵ M (x ≠ y)

От противного: ax = ay mod m → ax – ay ⁝ m → a\*(x-y) ⁝ m → (x – y) ⁝ m → x = y mod 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 φ(m). Все взаимно просты с m → a\*M — приведённая система вычетов ч.т.д.

**Как считать φ(m)?**

1) φ(p) - ?

Пусть p — простое число.

0, 1, 2, …, p-1 — взаимно простые.

Итого, φ(p) = p-1

2) φ(pk) - ?

1, 2, 3, …, x, …, pk

Пусть (x, pk) ≠ 1 → (x, pk) ⁝ p → x ⁝ p

Всего чисел делящихся на p (т.е. не взаимно простых с p) pk-1.

φ(pk) = pk-1(p-1)

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

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