kaspersky.academy

Арифметика

Лекция 4. Первообразные элементы

Математика в кибербезопасности

Лекция 4. Первообразные элементы

Малая теорема Ферма

Пусть p – простое число и $a \not\vdots\, p$

Тогда:

$$(a^{p-1} - 1) \vdots\, p$$

или

$$a^{p-1} \equiv 1 \bmod p$$

Тестирование числа на простоту

Возьмем какое-нибудь число p и проверим его на простоту.
Что, если $a^{p-1} \not\equiv 1 \bmod p$?
Тогда число p – точно составное!

А наоборот работает?
К сожалению, нет. Даже если равенство $a^{p-1} \equiv 1 \bmod p$ выполняется, то это еще не факт, что p – просто число.

Пример:

$a = 2$, $p = 5$

Тогда:

$$a^{p-1} - 1 = 2^4 - 1 = 16 - 1 = 15$$

$$15 = 3 \cdot 5$$

Значит,

$a^{p-1} - 1 \vdots\, p$, или $a^{p-1} \equiv 1 \bmod p$

Теорема выполняется. Это означает, что число p может быть как простым, так и составным.

Протестируем число 1727 на простоту.

Задача: $12^{1726} \equiv 1 \bmod 1727$?

$$12^3 \equiv 1728 \bmod 1727 \equiv 1 \bmod 1727$$

$$12^{1726} \bmod 1727 \equiv 12^3 \cdot 12^3 \cdot \ \dots \ \cdot 12^3 \cdot 12^1 \bmod 1727 \equiv 1 \cdot \dots \cdot 1 \cdot 12 \bmod 1727 \equiv 12 \bmod 1727$$

$$12^{1726} \equiv 1 \bmod 1727$$

Ответ: 1727 – точно составное число. $1727 = 11 \cdot 157$

Функция Эйлера

Функция Эйлера $\varphi(n)$ показывает, сколько чисел, стоящих до n, будут взаимно простыми с n.

Пример:

$$\varphi(6) = ?$$

$$\underline{1}, \cancel{2}, \cancel{3}, \cancel{4}, \underline{5}, 6$$

$$\varphi(6) = 2$$

Свойства функции Эйлера

1. $\varphi(1) = 1$
2. $\varphi(p) = p - 1$, если p – простое
   $\varphi(3) = 3 - 1 = 2$
3. $\varphi(p^n) = p^n - p^{n-1}$
   $\varphi(9) = \varphi(3^2) = 3^2 - 3^1 = 6$
4. Мультипликативность:
   $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$
   $\varphi(5 \cdot 7) = \varphi(5) \cdot \varphi(7) = (5 - 1)(7 - 1) = 4 \cdot 6 = 24$
   $\varphi(24) = \varphi(3 \cdot 8) = \varphi(3) \cdot \varphi(2 \cdot 3) = (3 - 1) \cdot (23 - 22) = 2 \cdot 4 = 8$

Первообразный корень

Первообразный корень g – это такое число, которое при возведении в степень $\varphi(m)$ даст единицу по модулю m, и не даст единицу при возведении в любую степень, стоящую до $\varphi(m)$

Пример задания:

Пусть $m = 5$, $\varphi(5) = 4$

Найдем такой g, что:

$$g^4 \equiv 1 \bmod 5$$
$$g^1 \not\equiv 1 \bmod 5$$
$$g^2 \not\equiv 1 \bmod 5$$
$$g^3 \not\equiv 1 \bmod 5$$

g - первообразный корень по $\bmod m$, если:

$$g^{\varphi(m)} \equiv 1 \bmod m$$

и

$$g^k \not\equiv 1 \bmod m$$
$$\text{при } 1 \leq k < \varphi(m)$$

Если $m > 2$,
то 0 и 1 – не первообразные корни

При этом всегда $g < m$, потому что мы считаем по $\bmod m$.

Как найти первообразный корень

Перебором.

Пример:

Найти все первообразные корни по mod 5:

$$\varphi(5) = 4$$

$$g^4 \equiv 1 \bmod 5$$

g – первообразный корень, если
не существует $k < 4$, при котором

$$g^k \equiv 1 \bmod 5$$

1. Пусть $g = 2$, тогда первая единица появляется при $k = 4$
   2 – первообразный корень
2. Пусть $g = 3$, тогда первая единица появляется при $k = 4$
   3 – первообразный корень
3. Пусть $g = 4$, тогда первая единица появляется при $k = 2$
   4 – не первообразный корень, т.к.
   $4^2 \equiv 1 \bmod 5$ и $2 < 4$

g \ k	1	2	3	4
2	2	4	3	1
3	3	4	2	1
4	4	1	4	1

Зачем нужны первообразные корни

Если возводить первообразный корень в степень k, где $1 \leq k < \varphi(m)$, мы получим $\varphi(m) - 1$ разных чисел

Пример:

$$p = 5323$$

$$\varphi(m) = 5322$$

Возводя первообразный корень g
в степени от 1 до 5322 мы получим 5322 разных неповторяющихся числа

Таким образом:

g –генератор чисел, стоящих до 5323