

Лекция №

Вычисление квадратного корня по модулю p

Лектор: Н.Ю. Золотых

Записал: С. Гагаринова

11 октября 2008

Пусть нужно найти x такое, что

$$x^2 \equiv a \pmod{p} \quad (1)$$

где p — простое нечетное число, a — целое неотрицательное число.

Сначала рассмотрим случай, когда $p \equiv 3 \pmod{4}$.

Тогда $x = a^{\frac{p+1}{4}}$. Действительно,

$$x^2 = a^{2 \cdot \frac{p+1}{4}} = a^{\frac{p+1}{2}} = a \cdot a^{\frac{p-1}{2}},$$

что по критерию Эйлера равно a (так как a — вычет).

Пусть теперь $p \equiv 1 \pmod{4}$.

По малой теореме Ферма $a^{p-1} \equiv 1 \pmod{p}$, поэтому $x^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$. Заметим, что если $x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ и выполнено (1), то

$$\text{НОД}(x^{\frac{p-1}{2}} - 1, x^2 - a) \equiv 0 \pmod{p}.$$

Поэтому будем искать i такое, что $\text{НОД}((x+i)^{\frac{p-1}{2}} - 1, x^2 - a) \neq 1$. В этом случае

$$\text{НОД}((x+i)^{\frac{p-1}{2}} - 1, x^2 - a) = x \pm \sqrt{a} \pmod{p}.$$

Таким образом, если такое i найдено, то x может быть найдено из соотношения $(x+i)^{\frac{p-1}{2}} - 1 \equiv x - \sqrt{a}$.

Пример 1. $a = 23$, $p = 29$

Рассмотрим $i = 1$. Вычислим $(x+1)^{14}$. Вместо $\equiv \pmod{p}$ для краткости будем писать $=$.

$$(x+1)^2 = x^2 + 2x + 1 = 23 + 2x + 1 = 2x + 24$$

$$(x+1)^3 = 2x^2 + 26x + 24 = 26x + 12$$

$$(x+1)^6 = 9x^2 + 15x + 28 = 15x + 3$$

$$(x+1)^7 = 15x^2 + 18x + 3 = 18x$$

$$(x+1)^{14} = 5x^2 = 28$$

$\text{НОД}((x+1)^{\frac{p-1}{2}} - 1, x^2 - a) = 1$, поэтому рассмотрим следующее i .

$i = 2$

$$(x+2)^2 = x^2 + 4x + 4 = 4x + 27$$

$$(x+2)^3 = 4x^2 + 6x + 25 = 6x + 1$$

$$(x+2)^6 = 7x^2 + 12x + 1 = 12x - 12$$

$$(x+2)^7 = 12x^2 + 12x - 24 = 12x + 20$$

$$(x+2)^{14} = -x^2 + 23 + 16x = 16x$$

$$\text{НОД}((x+2)^{\frac{p-1}{2}} - 1, x^2 - a) = 16x - 1 = x - \sqrt{a}$$

Найдем число обратное к 16 с помощью расширенного алгоритма Евклида.

$$29 = 1 \cdot 29 + 0 \cdot 16$$

$$16 = 0 \cdot 29 + 1 \cdot 16$$

$$13 = 1 \cdot 29 - 1 \cdot 16$$

$$3 = (-1) \cdot 29 + 2 \cdot 16$$

$$1 = 5 \cdot 29 - 9 \cdot 16$$

$$16x - 1 = x - 20$$

Итак, $x = \pm 20$.