Лекция №4
Извлечение квадратного корня в поле вычетов

Лектор: Н.Ю. Золотых Записал: М. Сморкалов, О. Касаткина

4 октября 2008

1. Алгоритм Шенкса

Пусть p — нечетное простое число. Требуется найти x такое, что:

$$x^2 \equiv a \pmod{p} \tag{1}$$

Так как p — нечетное, то существует нечетное число s, такое что:

$$p - 1 = 2^\alpha \cdot s \tag{2}$$

Пусть нам известен некоторый квадратичный невычет n. Вычислим b, где

$$b = n^s \pmod{p} \tag{3}$$

Замечание 1. b вычисляется за $\log s$.

Рассмотрим 2 случая: $p \equiv 1 \pmod 4$ и $p \equiv 3 \pmod 4$.

1) $p \equiv 3 \pmod 4$. В качестве x берем $a^{\frac{p+1}{4}}$. Очевидно, что в этом случае равенство (1) будет выполнено, т.к. $a^{\frac{p-1}{2}} \equiv 1 \pmod p$ (это следует из того, что a-вычет).

2) $p \equiv 1 \pmod 4$. Рассмотрим число $r = a^{\frac{s+1}{2}}$. Это число в некотором смысле близко к x, а именно:

Утверждение 1. $(a^{-1}r^2)^{2^{\alpha-1}} \equiv 1 \pmod p$.

Доказательство.

$$(a^{-1}r^2)^{2^{\alpha-1}} = (a^s)^{2^{\alpha-1}} = a^{s\cdot 2^{\alpha-1}} = a^{\frac{p-1}{2}} \equiv 1 \pmod p, \text{ так как } p \equiv 1 \pmod 4$$

□

Будем стараться получить $x = \sqrt{a}$ путём домножения r на некоторый корень степени 2^α из 1.

Утверждение 2. *b — первообразный корень из 1 степени 2^α.*

Доказательство. Для доказательства данного утверждения надо показать:
а) b — корень из 1 степени 2^α. Действительно, $b^{2\alpha} = n^{s\cdot 2^\alpha} = n^{p-1} = 1$.
б) b — первообразный корень. Предположим, что это не так. Тогда:

$$\exists j < 2^\alpha : b^j \equiv 1 \pmod p \tag{4}$$

Очевидно, что достаточно рассматриватьлишь те j, которые являются делителями числа 2^α. Если не так, то мы всегда сможем найти $t < j : b^t \equiv 1 \pmod p$, причем t будет являться делителем 2^α. Действительно:

$$2^\alpha = k \cdot j + t, \qquad 0 < t < j$$

$$b^{2^\alpha} = b^{k\cdot j} + b^t$$

Так как $b^{2^\alpha} = 1$ и $b^{k\cdot j} = 1$, то и $b^t = 1$. Повторяем эту процедуру до тех пор, пока t — не будет являться делителем 2^α.

Пусть теперь:

$$j = 2^\beta \qquad 0 \le \beta < \alpha$$

По ранее доказанному утверждению, существует $\theta : Z_p^* = \{1, \theta, \theta^2, \ldots, \theta^{p-2}\}$ и так как n — невычет, то $n = \theta^{2i+1}$. С другой стороны, т.к. $b^j \equiv 1 \pmod p$, то существует $k : b^j = \theta^{k\cdot p}$. Т.о. имеем:

$$\theta^{k\cdot p} = b^j = (n^s)^{2^\beta} = \theta^{(2i+1)\cdot s\cdot 2^\beta}$$

Отсюда

$$k \cdot p = k \cdot s \cdot 2^\alpha = (2i+1) \cdot s \cdot 2^\beta$$
$$k \cdot 2^{\alpha-\beta} = 2i + 1$$

Но в левой части неравенства стоит четное число (т.к. $\beta < \alpha$), а в правой нечетное! Значит предположение (4) не верно, и b — первообразный корень степени 2^α из 1. □

Будем искать x в виде $x = b^j r$, где $b = n^3 \mod p$, $r = a^{\frac{s+1}{2}} \mod p$.
Найдём такое j, что $(b^j r)^2 \equiv a \pmod p$.
Допустим j разложено в двоичной системе исчисления:

$$j = j_0 + 2j_1 + \ldots + 2^{\alpha-2} j_{\alpha-2}, \text{ где } j_k \in \{0, 1\}. \tag{5}$$

Утверждение 3. $j < 2^{\alpha-1}$

Доказательство.

Пусть $j = j' + 2^{\alpha-1}$, тогда подставив j в выражение $(b^j r)^2 \equiv a \pmod p$ получим:
$(b^{j'+2^{\alpha-1}} r)^2 \equiv a \pmod p$
$(b^{j'} b^{2^{\alpha-1}} r)^2 \equiv a \pmod p$
$b^{2^\alpha} \equiv 1 \pmod p \Rightarrow (b^{j'} r)^2 \equiv a \pmod p$.

□

Определим $j_0, j_1, \ldots, j_{\alpha-2}$ в выражении (5).

$$j_0\text{: } (r^2 a^{-1})^{2^{\alpha-1}} \equiv 1 \pmod p \Rightarrow (r^2 a^{-1})^{2^{\alpha-2}} \equiv \begin{cases} 1 \pmod p \\ -1 \pmod p \end{cases} \Rightarrow \text{ полагаем } \begin{cases} j_0 = 0 \\ j_0 = 1. \end{cases}$$

Утверждение 4. $(b^{j_0} r)^2 a^{-1}$ *— корень степени* $2^{\alpha-2}$ *из 1.*

Доказательство.

$$((b^{j_0} r)^2 a^{-1})^{2^{\alpha-2}} = (b^{j_0})^{2^{\alpha-1}} (r^2 a^{-1})^{2^{\alpha-2}} \equiv 1 \pmod p.$$

□

Пусть найдены $j_0, j_1, \ldots, j_{k-1}$, такие что

$$(b^{j_0 + 2j_1 + \ldots + 2^{k-1} j_{k-1}} r)^2 a^{-1} - \text{ корень степени } 2^{\alpha-k-1} \text{ из 1.}$$

Определим j_k.

$$j_k\text{: } ((b^{j_0+2j_1+\ldots+2^{k-1}j_{k-1}} r)^2 a^{-1})^{2^{\alpha-k-1}} \equiv 1 \pmod p \Rightarrow$$
$$\Rightarrow \quad ((b^{j_0+2j_1+\ldots+2^{k-1}j_{k-1}} r)^2 a^{-1})^{2^{\alpha-k-2}} \equiv \begin{cases} 1 \pmod p \\ -1 \pmod p \end{cases} \Rightarrow \text{ полагаем } \begin{cases} j_k = 0 \\ j_k = 1. \end{cases}$$

Утверждение 5. $(b^{j_0+2j_1+\ldots+2^k j_k}r)^2a^{-1}$ *— корень степени* $2^{\alpha-k-2}$ *из 1.*

Доказательство.

$$((b^{j_0+2j_1+\ldots+2^k j_k}r)^2a^{-1})^{2^{\alpha-k-2}} = (b^{j_k})^{2^{\alpha-1}}((b^{j_0+2j_1+\ldots+2^{k-1}j_{k-1}}r)^2a^{-1})^{2^{\alpha-k-2}} \equiv 1 \pmod p.$$

□

При $k = \alpha - 2$ получаем:

$$(b^{j_0+2j_1+\ldots+2^{\alpha-2}j_{\alpha-2}}r)^2a^{-1} - \text{ корень степени 1 из 1.}$$

Таким образом, $b^{j_0+2j_1+\ldots+2^{\alpha-2}j_{\alpha-2}}r = x$, где j_i $(i = 0, \ldots, \alpha-2)$ определяются следущим образом:

$$((b^{j_0+2j_1+\ldots+2^{i-1}j_{i-1}}r)^2a^{-1})^{2^{\alpha-i-2}} \equiv \begin{cases} 1 \pmod p \\ -1 \pmod p \end{cases} \Rightarrow \begin{cases} j_i = 0 \\ j_i = 1. \end{cases}$$

.

Таким образом получаем следующий алгоритм:

Алгоритм Шенкса

Вход: p - нечетное простое число, a - целое число от 0 до $p-1$ (вычет).
Выход: x - целое число, удовлетворяющее условию $x^2 \equiv a\ (mod\ p)$

1: Если $p \equiv 3\ (mod\ 4)$, то $x = a^{\frac{p+1}{4}}$. Выход.
2: Представим $p-1$ в виде $p-1 = 2^\alpha \cdot s$, где s - нечетное натуральное число.
3: Найдем n - некоторый квадратичный невычет.
4: Положим $b = n^s\ (mod\ p)$
5: Положим $r = a^{\frac{s+1}{2}}$
6: **for** $k = 0, \ldots, \alpha-2$ **do**
7: Найти j_k, такое что $(b^{j_0+2j_1+\cdots+2^k j_k}r)^2a^{-1}$ - корень степени $2^\alpha - k - 2$ из 1.
8: $x = b^{j_0+2j_1+\ldots+2^{\alpha-2}j_{\alpha-2}}r$. Выход.

Пример 1. Найти квадратный корень из $a = 186$ по модулю $p = 401$.

$n = 3$ — невычет
$p - 1 = 2^4 \cdot 25$
$b \equiv n^s \pmod p \equiv 3^{25} \pmod{401} \equiv 268 \pmod{401}$
$r \equiv a^{s+1/2} \pmod p \equiv 186^{13} \pmod{401} \equiv 103 \pmod{401}$
$a^{-1} \equiv 235 \pmod{401}$
$r^2a^{-1} \equiv 103^2 \cdot 235 \equiv 98 \pmod{401}$
$98^4 \equiv -1 \pmod{401} \Rightarrow j_0 = 1$
$((br)^2a^{-1})^2 \equiv ((268 \cdot 103)^2 \cdot 235)^2 \equiv 1 \pmod{401} \Rightarrow j_1 = 0$
$(br)^2a^{-1} \equiv (268 \cdot 103)^2 \cdot 235 \equiv -1 \pmod{401} \Rightarrow j_2 = 1$
$j = j_0 + 2j_1 + 4j_2 = 5 \Rightarrow x \equiv b^j r \pmod{401} \equiv 268^5 \cdot 103 \pmod{401} \equiv 304 \pmod{401}.$