Московский институт электроники и математики им. А.Н. Тихонова

Кафедра информационной безопасности киберфизических систем

Москва 2024

Криптографические методы защиты информации

Квадратичные вычеты

Квадратичные вычеты

Квадратичные вычеты

- **Сравнение второй степени** с одним неизвестным:
  $$x^2 \equiv a \pmod p, p > 2, a \in \{1, 2, \dots, p-1\}.$$
- Число a называется квадратичным вычетом по модулю p, если данное сравнение разрешимо (имеет два решения).
- Число a называется квадратичным невычетом по модулю p, если данное сравнение не имеет решений.
- Если a является квадратичным вычетом по модулю p, то любой элемент из класса вычетов $\bar{a} \in \mathbb{Z}_p$ также является квадратичным вычетом.
- **Примеры:**
  - $5 \pmod{11}$ — квадратичный вычет;
  - $2 \pmod{11}$ — квадратичный невычет.

Свойства квадратичных вычетов

- **Теорема.** Для любого простого числа $p > 2$ число классов квадратичных вычетов по модулю p равно числу классов квадратичных невычетов по модулю p.
- **Теорема.** Числа $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$ образуют систему представителей всех классов квадратичных вычетов по простому модулю $p > 2$.

- **Пример** для $p = 11$:
  - $\mathbb{Z}_p^* = \{\pm1, \pm2, \pm3, \pm4, \pm5\}$;
  - $(\pm1)^2 = 1$; $(\pm2)^2 = 4$; $(\pm3)^2 = 9$; $(\pm4)^2 = 5$; $(\pm5)^2 = 3$;
  - квадратичные вычеты по модулю 11: $\{1, 3, 4, 5, 9\}$;
  - квадратичные невычеты по модулю 11: $\{2, 6, 7, 8, 10\}$.

Символ Лежандра

- **Символ Лежандра** $\left(\frac{a}{p}\right)$ — это функция, указывающая на то, является $a \in \{1, 2, \dots, p-1\}$ квадратичным вычетом или невычетом по модулю $p > 2$:
  - $\left(\frac{a}{p}\right) = +1$, если a — квадратичный вычет по модулю p;
  - $\left(\frac{a}{p}\right) = -1$, если a — квадратичный невычет по модулю p.
- Свойства символа Лежандра:
  - если $a \equiv b \pmod p$, то $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$;
  - $\left(\frac{a^2}{p}\right) = 1$;
  - $\left(\frac{-1}{p}\right) = p \pmod 4$;
  - $\left(\frac{2}{p}\right) = \begin{cases} +1, \text{если } p \equiv \pm 1 \pmod 8, \\ -1, \text{если } p \equiv \pm 3 \pmod 8; \end{cases}$
  - $\left(\frac{a}{p}\right) = \left(\frac{a_1 a_2 \cdots a_k}{p}\right) = \left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right) \cdots \left(\frac{a_k}{p}\right)$.

Способы вычисления символа Лежандра

- **Критерий Эйлера.** Символ Лежандра $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \pmod p$.
- **Критерий Гаусса**. Символ Лежандра $\left(\frac{a}{p}\right) = (-1)^l$, где l представляет собой количество чисел из множества a, $2a$, …, $\left(\frac{p-1}{2}\right)a$, у которых наименьший по абсолютной величине вычет по модулю p отрицателен.
- **Квадратичный закон взаимности**. Для двух любых нечетных простых чисел p и q верно следующее:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} +1, & \text{если } p \equiv 1 \pmod 4 \text{ или } q \equiv 1 \pmod 4, \\ -1, & \text{если } p \equiv 3 \pmod 4 \text{ и } q \equiv 3 \pmod 4. \end{cases}$$

Пример вычисления символа Лежандра

- Найти $\left(\frac{168}{197}\right)$:
  - $\left(\frac{168}{197}\right) = \left(\frac{2^3 \cdot 3 \cdot 7}{197}\right) = \left(\frac{2^2}{197}\right) \cdot \left(\frac{2}{197}\right) \cdot \left(\frac{3}{197}\right) \cdot \left(\frac{7}{197}\right)$;
  - $\left(\frac{2^2}{197}\right) = +1$ по свойству;
  - $\left(\frac{2}{197}\right) = -1$, так как $197 \equiv -3 \pmod 8$;
  - $\left(\frac{3}{197}\right)\left(\frac{197}{3}\right) = 1$ по квадратичному закону взаимности, следовательно $\left(\frac{3}{197}\right) = \left(\frac{197}{3}\right) = \left(\frac{2}{3}\right) = -1$;
  - $\left(\frac{7}{197}\right)\left(\frac{197}{7}\right) = 1$ по квадратичному закону взаимности, следовательно $\left(\frac{7}{197}\right) = \left(\frac{197}{7}\right) = \left(\frac{1}{7}\right) = +1$;
  - $\left(\frac{168}{197}\right) = +1 \cdot (-1) \cdot (-1) \cdot (+1) = +1$.

Решение квадратичных сравнений

Сравнение второй степени с одним неизвестным

- Сравнение второй степени с одним неизвестным:
  - частный случай: $x^2 \equiv a \pmod{p}, p > 2, a \in \{1, 2, \dots, p-1\}$.
  - общий случай: $x^2 \equiv a \pmod{n}, n > 1, a \in \{1, 2, \dots, n-1\}$.
- Извлечение квадратного корня по модулю простого числа является простой задачей.
- Извлечение квадратного корня по модулю составного числа $n = p_1 p_2 \dots p_k$:
  - Простая задача, если известно разложение n на простые множители.
  - Сложная задача, если неизвестно разложение n на простые множители.
- *Криптографическое приложение — криптосистема Рабина.*

Извлечение квадратных корней по модулю простого числа

Вход: простое число $p > 2$, $a \in \{1, 2, \dots, p-1\}$.

Выход: два квадратных корня из a по модулю p.

Шаг 1. Вычислить символ Лежандра $\left(\frac{a}{p}\right)$. Если $\left(\frac{a}{p}\right) = -1$, то квадратных корней нет.

Шаг 2. Выбрать целое b, такое, что $\left(\frac{b}{p}\right) = -1$.

Шаг 3. Представить $p - 1 = 2^s \cdot t$, где t — нечетное число.

Шаг 4. Вычислить $a^{-1} \pmod p$ по расширенному алгоритму Евклида.

Шаг 5. Вычислить $C_0 \leftarrow b^t \pmod p$, $r \leftarrow a^{\frac{t+1}{2}} \pmod p$.

Шаг 6. Для $i = \overline{1, s-1}$:

Шаг 6.1. Вычислить $d_i \leftarrow \left(r^2 \cdot a^{-1}\right)^{2^{s-i-1}} \bmod p$.

Шаг 6.2. Если $d_i \equiv -1 \pmod p$, то вычислить $r \leftarrow r \cdot C_0 \pmod p$.

Шаг 6.3. Вычислить $C_0 \leftarrow C_0^2 \pmod p$.

Шаг 7. Возврат $(r;\ -r)$.

Извлечение квадратных корней по модулю составного числа

Вход: простые целые числа $p > 2$, $q > 2$, $a \in \{1, 2, \ldots, pq - 1\}$.

Выход: четыре квадратных корня из a по модулю $n = pq$.

Шаг 1. Вычислить два квадратных корня r и $-r$ из a по модулю p.

Шаг 2. Вычислить два квадратных корня s и $-s$ из a по модулю q.

Шаг 3. Вычислить $cp + dq = 1$ по расширенному алгоритму Евклида.

Шаг 4. Вычислить:

$$x = (rdq + scp) \bmod n;$$

$$y = (rdq - scp) \bmod n.$$

Шаг 5. Возврат $(\pm x;\ \pm y)$.

Алгоритм возведения в степень по модулю

Вход: $a, k \in \mathbb{Z}_n,\ k = \sum_{i=0}^{t} k_i \cdot 2^i$.

Выход: $a^k \bmod n$.

Шаг 1. $b \leftarrow 1$. Если $k = 0$, то переход к шагу 5.

Шаг 2. $A \leftarrow a$.

Шаг 3. Если $k_0 = 1$, то $b \leftarrow a$.

Шаг 4. Для $i = \overline{1, t}$ выполнить следующее:

Шаг 4.1. Вычислить $A \leftarrow A^2 \bmod n$.

Шаг 4.2. Если $k_i = 1$, то $b \leftarrow (A \cdot b) \bmod n$.

Шаг 5. Возврат b.

Пример извлечения квадратных корней по модулю простого числа

Вход: $p = 47, a = 12.$

Шаг 1. Символ Лежандра $\left(\frac{12}{47}\right) = \left(\frac{2^2}{47}\right)\left(\frac{3}{47}\right) = 1 \cdot \left(-\left(\frac{47}{3}\right)\right) = -\left(\frac{2}{3}\right) = -(-1) = 1.$

Шаг 2. $b = -1$, так как $\left(\frac{-1}{47}\right) = -1.$

Шаг 3. $p - 1 = 46 = 2^1 \cdot 23$, то есть $s = 1, t = 23.$

Шаг 4. $12^{-1} (\mathrm{mod}\, 47) = 4.$

Шаг 5. $C_0 = (-1)^{23} \,(\mathrm{mod}\, 47) = -1, r = 12^{\frac{23+1}{2}} \,(\mathrm{mod}\, 47) = 24.$

Шаг 6. Для $i = \overline{1,0}$:

Вход в цикл не выполняется.

Шаг 7. Возврат $(24;\ -24).$

Московский институт электроники и математики им. А.Н. Тихонова

Кафедра информационной безопасности киберфизических систем

Криптографические методы защиты информации

Спасибо за внимание!

Евсютин Олег Олегович
Заведующий кафедрой информационной безопасности киберфизических систем
Канд. техн. наук, доцент

+7 923 403 09 21
oevsyutin@hse.ru