Лекция №2
Квадратичные вычеты и невычеты

Лектор: Н.Ю. Золотых Записал: Е. Замараева

?? сентября 2008

Содержание

1. Квадратичные вычеты и невычеты

Определение 1. Пусть p — простое нечетное число. Тогда число a, такое, что НОД$(a, p) = 1$, называется *вычетом степени* n, если

$$\exists(x) : x^n \equiv a \pmod{p}.$$

В обратном случае число a называется невычетом степени n. При $n = 2$ вычет (невычет) a называется *квадратичным*, при $n = 3$ — *кубическим*, а при $n = 4$ — *биквадратичным*. При $n = 2$ слово квадратичный опускают и называют a просто вычетом (невычетом).

Рассмотрим группу $\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}$ с заданной операцией умножения по модулю p. Элементы, являющиеся квадратами какого-то числа в $\mathbb{Z}_p^*$, — вычеты.

Пример 1. Пусть $p = 7, \mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$.
$1^2 = 1 \pmod 7$,
$2^2 = 4 \pmod 7$,
$3^2 = 2 \pmod 7$,
$4^2 = 2 \pmod 7$,
$5^2 = 4 \pmod 7$,
$6^2 = 1 \pmod 7$.

Числа $1, 2, 4$ будут являться квадратичными вычетами, а числа $3, 5, 6$ — квадратичными невычетами.

Утверждение 2. *В $\mathbb{Z}_p^*$ существует ровно $\frac{p-1}{2}$ квадратичных вычетов, сравнимых с числами:*

$$1^2, 2^2, \ldots, \frac{p-1}{2}^2.$$

Доказательство. Сначала покажем, что приведенный список чисел содержит квадраты всех элементов из $\mathbb{Z}_p^*$. Это становится очевидно, если представить $\mathbb{Z}_p^*$ как $\{-\frac{p-1}{2}, \dots, -2, -1, 1, 2, \dots, \frac{p-1}{2}\}$. Теперь пусть $\exists i, j \in \mathbb{Z}_p^* : i^2 \equiv j^2 \pmod p, 0 < i < j \leq \frac{p-1}{2}$. Тогда сравнению $x^2 \equiv i^2 \pmod p$ удовлетворяло бы 4 корня: $x = \pm i, \pm j$, чего быть не может, а значит все числа из списка $1^2, 2^2, \dots, \frac{p-1}{2}^2$ различны по модулю p. Таким образом, приведенный список $1^2, 2^2, \dots, \frac{p-1}{2}^2$ состоит из $\frac{p-1}{2}$ различных по модулю p чисел, представляющих все вычеты в группе $\mathbb{Z}_p^*$. □

Утверждение 3. *Если $\mathbb{Z}_p^* = \{1, \theta, \theta^2, \dots, \theta^{p-2}\}$, где θ — порождающий элемент, то справедливо следующее:*

$$a = \theta^j \text{ — квадратичный вычет} \Leftrightarrow j \text{ — четное.}$$

Доказательство. Пусть $a = \theta^j$ — квадратичный вычет. Тогда $\exists x : x^2 \equiv a \pmod p$. Так как θ — порождающий элемент, значит $\exists i : x = \theta^i$, откуда следует, что $\theta^{2i} = \theta^j$, то есть j — четное.

В обратную сторону, пусть j — четное. Тогда $j = 2i$ для некоторого i, то есть $a = \theta^{2i}$. Это значит, что $\exists x = \theta^i : x^2 \equiv a \pmod p$, то есть a — квадратичный вычет. □

2. Символ Лежандра

Определение 2. Для любого простого нечетного p и целого a символ Лежандра определяется следующим образом:

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{если } a \equiv 0 \pmod p; \\ 1, & \text{если } a \text{ — вычет} \pmod p; \\ -1, & \text{если } a \text{ — невычет} \pmod p; \end{cases}$$

2.1. Свойства символа Лежандра

Утверждение 4.

$$a_1 \equiv a \pmod p \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{a_1}{p}\right).$$

Утверждение 5 (Критерий Эйлера)**.**

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p.$$

Доказательство. Для $a \equiv 0 \pmod p$ утверждение очевидно. Далее малая теорема Ферма гласит:

$$a \neq 0 \pmod p \Rightarrow a^{p-1} \equiv 1 \pmod p.$$

Рассмотрим 2 случая:

1. a — квадратичный вычет, то есть $\exists x : x^2 \equiv a \pmod p$. Тогда $a^{\frac{p-1}{2}} = x^{p-1} \equiv 1 \pmod p$. Последнее сравнение вытекает из малой теоремы Ферма. Но из того, что a — квадратичный вычет, вытекает, что $\left(\frac{a}{p}\right) = 1$, следовательно $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$.

2. a — квадратичный невычет, тогда из Утверждения 3 следует, что $\exists j : a = \theta^{2j+1}$, где θ — порождающий элемент. Тогда

$$\begin{aligned} a^{\frac{p-1}{2}} &= \theta^{\frac{(2j+1)(p-1)}{2}} = \theta^{\frac{(2jp-2j+p-1)}{2}} \\ &= \theta^{j(p-1)+\frac{p-1}{2}} = \theta^{\frac{p-1}{2}} = \theta^{(p-1)\frac{1}{2}} = 1^{\frac{1}{2}}. \end{aligned}$$

Сравнение $x^2 \equiv 1 \pmod p$ может иметь только 2 решения: $x = \pm 1$, но, так как θ — порождающий элемент, то только одна ее степень от 0 до $p-1$ может давать 1, и это — степень $p-1$. Следовательно $\theta^{\frac{p-1}{2}} \equiv -1 \pmod p$, а значит

$$a^{\frac{p-1}{2}} \equiv -1 \pmod p.$$

Вспомним, что a — квадратичный невычет, и получим требуемое:

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p.$$

□

Утверждение 6.

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \times \left(\frac{b}{p}\right).$$

Доказательство. По Критерю Эйлера:

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \times \left(\frac{b}{p}\right) \pmod p.$$

Из области допустимых значений символа Лежандра следует, что полученное сравнение можно обратить в равенство. □

Утверждение 7. *Если* НОД$(a, p) = 1$*, то справедливо равенство:*

$$\left(\frac{a^2 b}{p}\right) = \left(\frac{b}{p}\right).$$

Доказательство. Согласно Утверждению 6:

$$\left(\frac{a^2 b}{p}\right) = \left(\frac{a^2}{p}\right)\left(\frac{b}{p}\right).$$

Так как НОД$(a, p) = 1$, то a^2 — квадратичный вычет, и утверждение очевидно. □

Утверждение 8.

$$\left(\frac{1}{p}\right) = 1;$$
$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

Доказательство. 1. Так как $1^2 \equiv 1 \pmod p$, то 1 является квадратичным вычетом, что доказывает первую формулу.

2. Для доказательства второй формулы в критерий Эйлера достаточно подставить -1 в качестве a.

□

Утверждение 9.

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & p \equiv \pm 1 \pmod 8; \\ -1, & p \equiv \pm 3 \pmod 8. \end{cases}$$

Свойство приводится без доказательства.

2.2. Квадратичный закон взаимности

Теорема 10. *Для любых простых нечетных p и q справедливо:*

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{q}{p}\right).$$

Впервые теорема была сформулирована Эйлером в 1783 году, а впоследствии доказана Гауссом в 1796, и имела следующую формулировку:

$$\left(\frac{p}{q}\right) \neq \left(\frac{q}{p}\right) \Leftrightarrow \begin{cases} p \equiv 3 \pmod 4; \\ q \equiv 3 \pmod 4. \end{cases}$$

Теорема приводится без доказательства.

2.3. Алгоритм вычисления символа Лежандра

Алгоритм вычисления символа Лежандра является рекурсивным. На практике он неприменим для больших чисел, так как требует разложения числа на простые сомножители.

Алгоритм

1. Если $a < 0$, то, применяя Утверждения 6 и 8, получаем $\left(\frac{a}{p}\right) = \left(\frac{-a}{p}\right) \times (-1)^{\frac{p-1}{2}}$.

   Переобозначаем $a := -a$.

2. $a := a \mod p$ (операцией mod без скобок мы будем обозначать взятие остатка).

3. Раскладываем a на простые сомножители:

   $$a = p_1^{k^1} \times \cdots \times p_s^{k^s}, \text{ где } p_j \text{ — простые числа для } j = 1, \ldots, s.$$

   Тогда согласно Утверждению 6

   $$\left(\frac{a}{p}\right) = \left(\frac{p_1}{p}\right)^{k_1} \times \cdots \times \left(\frac{p_s}{p}\right)^{k_s}$$

   Множители в четной степени k_j можно удалить, так как они все равны 1.

4. Для всех $p_j = 2$ и нечетных k_j вычисляем $\left(\frac{2}{p}\right)$ по Утверждению 9.

5. Для всех $p_j \neq 2$ и нечетных k_j применяем квадратичный закон взаимности:

   $$\left(\frac{p_j}{p}\right) = (-1)^{\frac{p-1}{2}\frac{p_j-1}{2}} \left(\frac{p}{p_j}\right).$$

   Применяем алгоритм для каждого $\left(\frac{p}{p_j}\right)$.

Алгоритм можно рассматривать как свод правил, руководствуясь которыми, можно вычислить символ Лежандра.

Пример 11. Вычислить $\left(\frac{126}{53}\right)$. Применим к этому выражению описанные выше правила (над знаками равенства указываются номера соответствующих шагов алгоритма):

$$\begin{aligned} \left(\frac{126}{53}\right) &\overset{2}{=} \left(\frac{20}{53}\right) \overset{3}{=} \left(\frac{2}{53}\right)^2 \times \left(\frac{5}{53}\right) = \left(\frac{5}{53}\right) \overset{5}{=} \left(\frac{53}{5}\right) (-1)^{\frac{53-1}{2}\frac{5-1}{2}} \\ &= \left(\frac{53}{5}\right) \overset{2}{=} \left(\frac{3}{5}\right) \overset{5}{=} \left(\frac{5}{3}\right) (-1)^{\frac{3-1}{2}\frac{5-1}{2}} \overset{2}{=} \left(\frac{2}{3}\right) \overset{\text{утв-ие 9}}{=} (-1)^{\frac{9-1}{8}} \\ &= -1. \end{aligned}$$

3. Символ Якоби

Определение 3. Пусть n — нечетное, больше единицы и $n = p_1^{k_1} \dots p_s^{k_s}$, где $p_1, \dots, p_s$ — простые числа. Тогда символ Якоби $\left(\frac{a}{n}\right)$ определяется следующим равенством:

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{k_1} \times \dots \times \left(\frac{a}{p_s}\right)^{k_s}.$$

Символ Якоби является обобщением символа Лежандра, а символ Лежандра является частным случаем символа Якоби.

3.1. Свойства символа Якоби

Свойства символа Якоби прямо вытекают из соответствующих свойств символа Лежандра. Их доказательство оставляется читателю в качестве самостоятельного упражнения.

Утверждение 12.

$$a_1 \equiv a \pmod{n} \Rightarrow \left(\frac{a_1}{n}\right) = \left(\frac{a}{n}\right).$$

Утверждение 13.

$$\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right).$$

Утверждение 14.

$$\text{НОД}(a, n) = 1 \Rightarrow \left(\frac{a^2 b}{n}\right) = \left(\frac{b}{n}\right).$$

Утверждение 15.

$$\left(\frac{1}{n}\right) = 1;$$
$$\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}.$$

Утверждение 16.

$$\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}.$$

3.2. Обобщение квадратичного закона взаимности

Квадратичный закон взаимности для символа Лежандра обобщается на символ Якоби следующим уравнением:

Теорема 17. *Для любых нечетных m и n справедливо:*

$$\left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}} \left(\frac{n}{m}\right).$$

3.3. Алгоритм вычисления символа Якоби

Для вычисления символа Якоби в алгоритм вычисления символа Лежандра добавляется нулевой шаг, заключающийся в разложении символа Якоби в произведение символов Лежандра согласно определению.

Пример 18. Вычислить символ Якоби $\left(\frac{131}{255}\right)$. Воспользуемся предложенным алгоритмом вычисления символа Лежандра и его расширением на вычисление символа Якоби. Над знаками равенства будут указываться номера шагов алгоритма. Нам понадобится разложение числа 255 на простые сомножители:

$$255 = 3 \times 5 \times 17.$$

Начинаем применять алгоритм с его нулевого шага:

$$\left(\frac{131}{255}\right) \overset{0}{=} \left(\frac{131}{3}\right) \times \left(\frac{131}{5}\right) \times \left(\frac{131}{17}\right).$$

Вычисляем сомножители:

$$\left(\frac{131}{3}\right) \overset{2}{=} \left(\frac{2}{3}\right) \overset{4}{=} (-1)^{\frac{3^2-1}{8}} = -1;$$

$$\left(\frac{131}{5}\right) \overset{2}{=} \left(\frac{1}{5}\right) \overset{\text{утв-ие 8}}{=} 1;$$

$$\left(\frac{131}{17}\right) \overset{2}{=} \left(\frac{12}{17}\right) \overset{3}{=} \left(\frac{2}{17}\right)^2 \times \left(\frac{3}{17}\right) = \left(\frac{3}{17}\right) \overset{5}{=} \left(\frac{17}{3}\right) \times (-1)^{\frac{17-1}{2}\frac{3-1}{2}} = \left(\frac{17}{3}\right) \overset{2}{=} \left(\frac{2}{3}\right) \overset{4}{=} -1.$$

Перемножаем полученные величины и получаем решение:

$$\left(\frac{131}{255}\right) = (-1) \times 1 \times (-1) = 1.$$

Список литературы

[1] *Виноградов И.М.* Основы теории чисел. — М.–Л., Гостехиздат, 1952.