ТЕОРЕТИКО-ЧИСЛОВЫЕ МЕТОДЫ В КРИПТОГРАФИИ

Лекция 12

Символы Лежандра и Якоби. Разрешимость сравнений второй степени

Дисциплина: «Теоретико-числовые методы в криптографии».

Объём по рабочей программе: 1 академический час. Материал развивает практическую тему 11: ранее применённые свойства символов теперь получают теоретическое обоснование. Доказательство через целочисленные точки и раздел 7 можно использовать для углублённого самостоятельного изучения.

Цель: научиться обосновывать вычисление квадратичных символов, устанавливать разрешимость квадратных сравнений и различать свойства простого и составного модуля.

Необходимая подготовка: поле вычетов по простому модулю, малая теорема Ферма, число корней многочлена над полем, китайская теорема об остатках.

1 Квадратичные вычеты и символ Лежандра

Пусть p — нечётное простое число. Ненулевой класс a называется **квадратичным вычетом** по модулю p, если существует x, для которого $x^2 \equiv a \pmod p$. Если такого x нет, класс является **квадратичным невычетом**. Ноль рассматривается отдельно.

Определение. Символ Лежандра задаётся формулой

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & p \mid a, \\ 1, & a \text{ — ненулевой квадратичный вычет}, \\ -1, & a \text{ — квадратичный невычет}. \end{cases}$$

Символ зависит только от класса $a \bmod p$. Скобки обозначают специальную арифметическую функцию; это не обычная дробь.

Число вычетов. Если $x^2 = y^2$ в поле $\mathbb{F}_p$, то $(x-y)(x+y) = 0$, откуда $y = x$ или $y = -x$. Для ненулевого x эти два значения различны, поскольку $p \neq 2$. Следовательно, каждое ненулевое квадратное значение получается ровно дважды. Из $p-1$ ненулевых классов ровно $(p-1)/2$ являются вычетами и столько же — невычетами.

Отсюда число различных решений сравнения $x^2 \equiv a \pmod p$ равно

$$N_p(a) = 1 + \left(\frac{a}{p}\right).$$

Формула охватывает все случаи: два корня для ненулевого вычета, один корень для нуля и отсутствие корней для невычета.

Пример 1. По модулю 11 достаточно возвести в квадрат числа от 1 до 5. Получим 1,4,9,5,3. Поэтому $(5/11) = 1$, $(2/11) = -1$, $(22/11) = 0$. У сравнения $x^2 \equiv 5 \pmod{11}$ два корня: 4 и 7.

2 Критерий Эйлера и мультипликативность

Теорема — критерий Эйлера. Для любого целого a выполнено

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

Доказательство. Обозначим $h = (p-1)/2$. Для ненулевого квадрата $a = x^2$ малая теорема Ферма даёт $a^h = x^{p-1} = 1$. Таких квадратов ровно h. Многочлен $X^h - 1$ над полем имеет не более h корней, поэтому другие классы его корнями быть не могут. Для любого ненулевого a равенство $a^{p-1} = 1$ означает $(a^h)^2 = 1$. Следовательно, a^h равно 1 или -1, причём для невычета остаётся только -1. Для $a \equiv 0$ обе части критерия равны нулю. Теорема доказана.

В программе значение -1 представляется остатком $p-1$. Поэтому результат модульного возведения в степень необходимо преобразовать в знак.

Следствие — мультипликативность. Для любых целых a, b справедливо

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

По критерию Эйлера обе части сравнимы по модулю p. Они принадлежат множеству $\{-1,0,1\}$, элементы которого различны по нечётному простому модулю; следовательно, они равны как целые числа. В частности, произведение двух невычетов является вычетом, а произведение вычета и невычета — невычетом.

3 Лемма Гаусса и дополнительные законы

3.1 Лемма Гаусса

Пусть $p \nmid a$, $h = (p-1)/2$. Возьмём наименьшие положительные остатки

$$r_i \equiv ai \pmod p, \qquad 1 \le i \le h,$$

и обозначим через ν число тех остатков, которые больше $p/2$.

Лемма Гаусса. При этих условиях

$$\left(\frac{a}{p}\right) = (-1)^{\nu}.$$

Доказательство. Положим $c_i = \min(r_i, p - r_i)$. Все c_i лежат между 1 и h. Если $c_i = c_j$, то $ai \equiv \pm aj \pmod p$. Сократив на ненулевой класс a, получаем $i \equiv \pm j \pmod p$. В указанных пределах первое равенство означает $i = j$, а второе невозможно: $2 \le i + j \le p - 1$. Таким образом, $c_1, \dots, c_h$ — перестановка чисел $1, \dots, h$.

Замена остатка $r_i > p/2$ числом $c_i = p - r_i$ вносит знак минус. Перемножение даёт

$$a^h h! \equiv r_1 \cdots r_h \equiv (-1)^{\nu} c_1 \cdots c_h = (-1)^{\nu} h! \pmod p.$$

Число $h!$ не делится на p, поэтому на него можно сократить. Получаем $a^h \equiv (-1)^{\nu}$; остаётся применить критерий Эйлера.

Пример 2. Для $(11/7)$ рассматриваем $11,22,33$. Их остатки: $4,1,5$. Порог $7/2$ превышают два остатка, значит $\nu = 2$ и $(11/7) = 1$. Это согласуется с $11 \equiv 4 \pmod 7$.

3.2 Символы с числителями −1 и 2

Критерий Эйлера сразу даёт **первый дополнительный закон**:

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

Следовательно, -1 является вычетом ровно при $p \equiv 1 \pmod 4$.

Для $a = 2$ остатки в лемме Гаусса имеют вид $2, 4, \ldots, p-1$. Условие $2i > p/2$ равносильно $i > p/4$. Поэтому

$$\nu = \frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor.$$

Если записать p в одном из видов $8k+1, 8k+3, 8k+5, 8k+7$, получаем соответственно $\nu = 2k, 2k+1, 2k+1, 2k+2$. Это доказывает **второй дополнительный закон**:

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1, & p \equiv 1, 7 \pmod 8, \\ -1, & p \equiv 3, 5 \pmod 8. \end{cases}$$

Пример 3. Для $p = 29$ первый закон даёт $(-1/29) = 1$, второй — $(2/29) = -1$. По мультипликативности $(-2/29) = -1$, поэтому $x^2 \equiv -2 \pmod{29}$ неразрешимо.

4 Квадратичный закон взаимности

Теорема. Если p и q — различные нечётные простые числа, то

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

При перестановке числителя и знаменателя знак меняется ровно тогда, когда оба простых числа сравнимы с 3 по модулю 4. Во всех остальных случаях символы равны.

4.1 Переход от леммы Гаусса к сумме целых частей

Для положительного нечётного a, взаимно простого с p, положим

$$S(a, p) = \sum_{i=1}^{(p-1)/2} \left\lfloor \frac{ai}{p} \right\rfloor.$$

Используем остатки r_i и числа c_i из доказательства леммы Гаусса. Из деления с остатком следует

$$a \sum_{i=1}^{h} i - pS(a, p) = \sum_{i=1}^{h} r_i.$$

Поскольку a, p нечётны, левая часть по модулю 2 равна $\sum i - S(a, p)$. Каждый из ν больших остатков имеет вид $p - c_i$ и по чётности отличается от c_i на 1. Значит, правая часть сравнима с $\sum c_i + \nu = \sum i + \nu$. После сокращения получаем $S(a, p) \equiv \nu \pmod 2$. Поэтому

$$\left(\frac{a}{p}\right) = (-1)^{S(a,p)}.$$

Нечётность a нужна именно в переходе к чётностям. Подставлять сюда произвольное чётное a без дополнительного преобразования нельзя.

4.2 Доказательство закона взаимности подсчётом точек

Обозначим $h = (p-1)/2$, $k = (q-1)/2$ и рассмотрим прямоугольник целочисленных точек $1 \le i \le h$, $1 \le j \le k$. Всего в нём hk точек. Прямая $pj = qi$ не проходит ни через одну из них: из равенства следовало бы $p \mid i$, что невозможно при $0 < i < p$.

Для фиксированного i число точек ниже прямой равно $\lfloor qi/p \rfloor$. Эта величина не превышает k, так как $qi/p < q/2$. Поэтому общее число точек ниже прямой равно $S(q, p)$.

Аналогично число точек выше прямой равно $S(p,q)$: при фиксированном j там выполняется $i < pj/q$.

Каждая точка попадает ровно в одну из двух частей, следовательно,

$$S(q,p) + S(p,q) = hk.$$

Применив результат предыдущего подраздела к обоим символам, получаем утверждение теоремы.

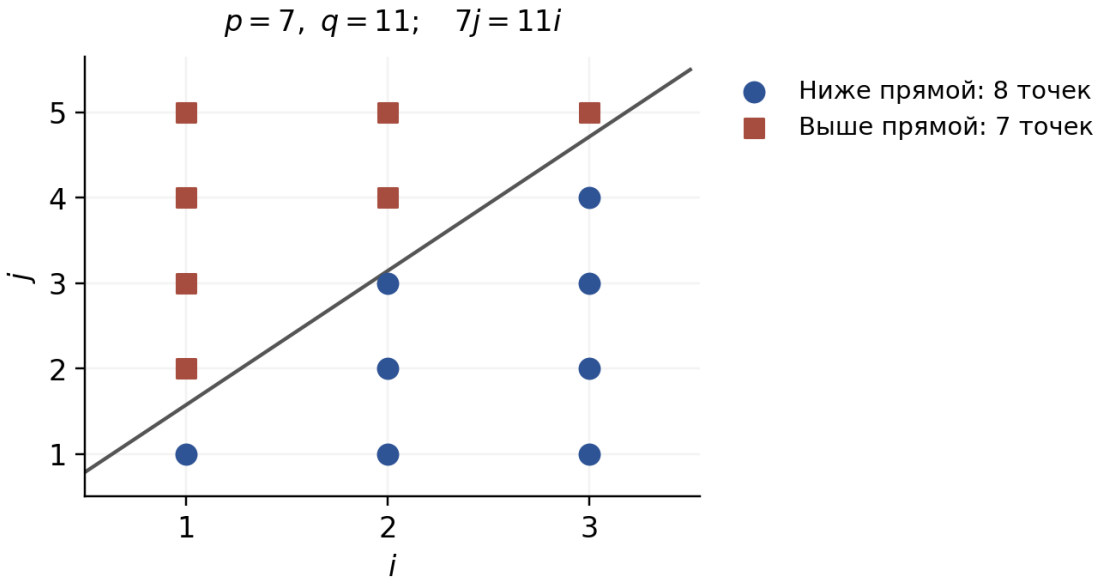


Рисунок 1 — Геометрический подсчёт, лежащий в основе закона взаимности

Пример 4. Для $p = 7$, $q = 11$ получаем

$$S(11,7) = 1 + 3 + 4 = 8, \qquad S(7,11) = 0 + 1 + 1 + 2 + 3 = 7.$$

Сумма равна $3 \cdot 5 = 15$. Поэтому $(11/7) = 1$, $(7/11) = -1$. Произведение символов равно -1, как и требует закон взаимности для двух простых чисел вида $4k + 3$.

Пример 5. Вычислим $(43/59)$. Оба простых числа сравнимы с 3 по модулю 4, поэтому

$$\left(\frac{43}{59}\right) = -\left(\frac{59}{43}\right) = -\left(\frac{16}{43}\right) = -1.$$

Последний символ равен 1, поскольку $16 = 4^2$ и $43 \nmid 4$. Сравнение $x^2 \equiv 43 \pmod{59}$ корней не имеет.

5 Символ Якоби: вычисление и границы вывода

Пусть $n > 1$ — нечётное число с разложением $n = p_1^{e_1} \cdots p_r^{e_r}$. **Символ Якоби** определяется произведением

$$\left(\frac{a}{n}\right) = \prod_{j=1}^{r} \left(\frac{a}{p_j}\right)^{e_j}.$$

Для $n = 1$ принимают $(a/1) = 1$. Здесь используется расширенное определение: при $\gcd(a,n) > 1$ символ равен нулю. Для простого знаменателя это определение совпадает с символом Лежандра.

Из определения следуют зависимость от остатка числителя, мультипликативность по числителю и по нечётному положительному знаменателю. Дополнительные законы сохраняют вид

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

Для взаимно простых положительных нечётных a, n закон взаимности принимает форму

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

Почему это верно? Разложим числитель и знаменатель на простые множители и применим закон Лежандра к каждой паре. Полученные знаки перемножаются. Для нечётных u, v разность между $(uv-1)/2$ и суммой $(u-1)/2 + (v-1)/2$ чётна. Аналогично чётна разность между $(u^2v^2-1)/8$ и суммой $(u^2-1)/8 + (v^2-1)/8$. Эти тождества объединяют показатели знака в записанные формулы.

Закон взаимности, выделение степеней двойки и переход к остатку позволяют вычислять символ Якоби по схеме алгоритма Евклида, **без предварительной факторизации знаменателя**. Разложение необходимо для определения и доказательства свойств, но не для такого алгоритма вычисления.

Смысл результата. Для взаимно простых a, n наличие квадратного корня влечёт $(a/n) = 1$: по каждому простому делителю a является вычетом. Поэтому значение -1 доказывает отсутствие корней. Значение 1 само по себе разрешимость не доказывает. Значение 0 сообщает об общем делителе и также не решает вопрос о корнях.

Пример 6. По модулю 35 символ $(3/35) = (3/5)(3/7) = (-1)(-1) = 1$. Но уже сравнение $x^2 \equiv 3 \pmod 5$ неразрешимо, следовательно, корней по модулю 35 нет. Для числа 4 тот же символ равен 1, однако корни существуют: 2, 12, 23, 33.

Нулевой символ тоже допускает оба исхода. У сравнения $x^2 \equiv 7 \pmod{21}$ есть корни 7 и 14, а у $x^2 \equiv 3 \pmod{21}$ корней нет, поскольку 3 — невычет по модулю 7. В обоих случаях символ Якоби равен нулю.

6 Сравнение общего вида второй степени

Рассмотрим $Ax^2 + Bx + C \equiv 0 \pmod p$, где p — нечётное простое и $A \not\equiv 0 \pmod p$. После умножения на $4A$ и выделения квадрата получаем

$$(2Ax + B)^2 \equiv \Delta \pmod p, \qquad \Delta = B^2 - 4AC.$$

Отображение $x \mapsto 2Ax + B$ взаимно однозначно, так как $2A$ обратимо. Поэтому число решений равно $1 + (\Delta/p)$. Если $r^2 \equiv \Delta$, то

$$x \equiv (-B \pm r)(2A)^{-1} \pmod p.$$

При $\Delta = 0$ два знака дают один корень. Если $A = 0$, решают линейное сравнение; когда также $B = 0$, остаётся проверить C. По модулю 2 оба класса проверяются отдельно. Эти случаи не входят в выведенную формулу.

Пример 7. Для $2x^2 + 3x + 21 \equiv 0 \pmod{41}$ имеем $\Delta = 9 - 168 \equiv 5$. Закон взаимности даёт $(5/41) = (41/5) = 1$. Таким образом, корней два. Их нахождение алгоритмом Тонелли — Шенкса разобрано в практикуме: квадратные корни из 5 равны 13 и 28, а исходное сравнение имеет корни 23 и 37.

Символ отвечает на вопрос о существовании корня. Сам корень требует отдельного вычисления: формулы для $p \equiv 3 \pmod 4$ или общего алгоритма для нечётного простого модуля.

7 Почему символ Якоби не раскрывает все квадраты

Пусть $n = pq$, где p, q — различные нечётные простые. Рассмотрим только обратимые классы, которых $\varphi(n) = (p-1)(q-1)$. Китайская теорема об остатках сопоставляет каждому из них независимую пару ненулевых классов по модулям p и q.

По каждому простому модулю вычетов и невычетов поровну. Поэтому четыре пары знаков символов Лежандра встречаются одинаково часто — по $\varphi(n)/4$ раз.

(a/p)	(a/q)	(a/n)	**Есть ли квадратный корень по модулю n?**
1	1	1	Да, четыре различных корня
1	-1	-1	Нет
-1	1	-1	Нет
-1	-1	1	Нет

Итак, среди обратимых классов ровно $\varphi(n)/2$ имеют символ Якоби 1, но лишь $\varphi(n)/4$ являются квадратами. Среди классов с положительным символом ровно половина — квадраты. Это утверждение доказано для произведения **двух различных** простых; переносить его без проверки на произвольный составной модуль нельзя.

Пример 8. Для $n = 77$ получаем $\varphi(77) = 60$: положительный символ имеют 30 обратимых классов, квадратами являются 15. Число 6 имеет пару знаков $(-1, -1)$ и положительный символ Якоби, но квадратным вычетом по модулю 77 не является.

В криптографии это различие появляется в задачах о квадратичной вычетности по составному модулю. Для простых модулей извлечение корней используется, в частности, в вычислениях с точками эллиптических кривых. Современный пример описания таких подпрограмм — приложение I к RFC 9380 (2023); там приведена также версия алгоритма Тонелли — Шенкса с постоянным временем выполнения.

Упражнения для закрепления

1. По лемме Гаусса вычислите $(5/11)$, выпишите остатки и значение ν.
2. Вычислите $(-2/29)$ с помощью дополнительных законов и определите число корней соответствующего сравнения.
3. Используя закон взаимности, найдите $(43/59)$. Укажите, на каком шаге меняется знак.
4. Сравните $(3/35)$ и $(4/35)$. Для каждого числителя определите разрешимость; для второго найдите все корни с помощью китайской теоремы об остатках.
5. Решите $2x^2 + 3x + 21 \equiv 0 \pmod{41}$, если известно, что $13^2 \equiv 5 \pmod{41}$. Проверьте корни подстановкой.
6. Для модуля 77 найдите число обратимых классов с символом Якоби 1 и число ненулевых обратимых квадратов. Объясните положение числа 6 среди четырёх пар знаков.

Контрольные вопросы

1. Почему ненулевых квадратичных вычетов по простому модулю ровно половина от числа ненулевых классов?
2. Как число корней связано с символом Лежандра, включая случай нулевого числителя?
3. Какая теорема о многочленах используется в доказательстве критерия Эйлера?
4. Что именно считает число ν в лемме Гаусса?
5. Почему в её доказательстве можно сократить на факториал?
6. При каких остатках p по модулю 8 число 2 является вычетом?
7. Когда перестановка простых числителя и знаменателя меняет знак символа?
8. Почему прямая $pj = qi$ не содержит точек рассматриваемого прямоугольника?
9. Для чего в формуле с суммой целых частей требуется нечётность числителя?
10. Почему символ Якоби можно вычислять без разложения знаменателя?
11. Какие выводы о корнях допустимы при значениях символа Якоби -1, 0 и 1?
12. При каких условиях квадратное сравнение сводится к дискриминанту и что делать при нарушении этих условий?

Литература

1. Мартынов Л. М. **Алгебра и теория чисел для криптографии.** 2020. § 7.7.1–7.7.2, с. 237–244: символы Лежандра и Якоби. Использован предоставленный полный текст; страницы указаны по печатной нумерации.
2. Trappe W., Washington L. C. **Introduction to Cryptography with Coding Theory.** 2nd ed. Pearson, 2006. § 3.9–3.10: квадратные корни, символы Лежандра и Якоби.
3. Faz-Hernandez A. et al. **Hashing to Elliptic Curves.** RFC 9380, 2023. Приложение I: извлечение квадратных корней. Дополнительный материал о применении алгоритмов.

Доказательства и численные примеры изложены для данного учебного блока; практикум содержит самостоятельную учебную реализацию общего алгоритма извлечения корней.