

ПРОБЛЕМЫ КВАДРАТИЧНОГО ВЫЧЕТА И КВАДРАТНОГО КОРНЯ

1 Квадратичные вычеты. Символы Лежандра и Якоби

Число $a, a \in Z_n^*, 1 \leq a \leq n$ называется *квадратичным вычетом по модулю n* , если существует число x , такое, что, $x^2 \equiv a \pmod{n}$, иначе оно называется *квадратичным невычетом по модулю n* . При этом число x называется *квадратным корнем* числа a по модулю n . Будем обозначать Q_n и \bar{Q}_n множества квадратичных вычетов и квадратичных невычетов по модулю n соответственно.

Если число $a \equiv x^2 \pmod{p}$, где p — простое число, то число $-x$ также удовлетворяет указанному сравнению, то есть квадратичный вычет a по модулю простого числа p имеет два квадратных корня.

Если p — простое число и α — образующий элемент группы Z_p^* , то $a \in Z_p^*$ является квадратичным вычетом тогда и только тогда, когда $a = \alpha^i \pmod{p}$, где i — чётное. Отсюда следует, что $|Q_p| = |\bar{Q}_p| = (p-1)/2$, то есть половина элементов из Z_p^* является квадратичными вычетами, а вторая половина — квадратичными невычетами. Все квадратичные вычеты по модулю простого числа p можно найти возведением в квадрат по модулю p чисел $1, 2, \dots, (p-1)/2$.

Пример Число $\alpha = 6$ является примитивным элементом группы Z_{13}^* . Его степени приведены в таблице

i	0	1	2	3	4	5	6	7	8	9	10	11
$\alpha^i \pmod{13}$	1	6	10	8	9	2	12	7	3	5	4	11

Из таблицы видно, что $Q_{13} = \{1, 3, 4, 9, 10, 12\}$ $\bar{Q}_{13} = \{2, 5, 6, 7, 8, 11\}$.

В общем случае для $n = p_1^{e_1} \cdot \dots \cdot p_k^{e_k}$, где p_1, \dots, p_k — различные нечетные простые числа и $e_i \geq 1, i = 1, \dots, k$, всякий элемент $a \in Q_n$ имеет точно 2^k квадратных корней в Z_n^* .

Пример а) Квадратными корнями числа 12 по модулю 37 являются числа 7 и 30.

б) Число 121 имеет 8 квадратных корней по модулю 315:

$$11, 74, 101, 151, 164, 214, 241, 304.$$

Символ Лежандра для целого a и простого p определяется следующим образом:

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{если } p \text{ делит } a, \\ 1, & \text{если } a \pmod{p} - \text{квадратичный вычет по модулю } p, \\ -1, & \text{если } a \pmod{p} - \text{квадратичный невычет по модулю } p, \end{cases}$$

Легко показать, что имеет место *критерий Эйлера*:

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

Символ Якоби является обобщением символа Лежандра (поэтому обозначается так же). Он определяется для целого a и нечетного $n, n > 2$. Пусть n

разлагается на простые множители:

$$n = p_1^{e_1} \cdots p_k^{e_k}.$$

Тогда символ Якоби определяется как произведение соответствующих символов Лежандра:

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{e_1} \cdots \left(\frac{a}{p_k}\right)^{e_k}.$$

Для некоторых значений a символ Якоби вычисляется следующим образом:

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

то есть $\left(\frac{2}{n}\right) = 1$ если $n \equiv 1$ или $7 \pmod{8}$, и $\left(\frac{2}{n}\right) = -1$ если $n \equiv 3$ или $5 \pmod{8}$.

Значение символа Якоби для нечетных чисел m и n , больших 2, можно вычислять на основе *закона взаимности*

$$\left(\frac{m}{n}\right) = (-1)^{(n-1)(m-1)/4} \cdot \left(\frac{n}{m}\right).$$

Можно показать, что это свойство эквивалентно следующему:

$$\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right),$$

если только не выполняется $m \equiv n \equiv 3 \pmod{4}$.

В последнем случае

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

"Числитель" в символе Якоби можно заменять любым сравнимым с ним по модулю "знаменателя" числом, используя следующее свойство символа Якоби: Если $a \equiv b \pmod{n}$, то $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$

Это позволяет с учетом закона взаимности вычислять символ Якоби по алгоритму, подобному алгоритму Евклида и имеющему ту же сложность.

Полезно использовать также свойство мультипликативности

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

Это свойство влечет

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

Пример 4.

$$\begin{aligned}
\left(\frac{2001}{2773}\right) &= \left(\frac{2773}{2001}\right) = \left(\frac{772}{2001}\right) = \left(\frac{193}{2001}\right) = \left(\frac{2001}{193}\right) = \left(\frac{71}{193}\right) = \\
&= \left(\frac{193}{71}\right) = \left(\frac{51}{71}\right) = -\left(\frac{71}{51}\right) = -\left(\frac{20}{51}\right) = -\left(\frac{5}{51}\right) = \\
&= -\left(\frac{51}{5}\right) = -\left(\frac{1}{5}\right) = -1.
\end{aligned}$$

Используя свойства символа Якоби, при нечётном $n \geq 3$ и $a = 2^e a_1$, где a_1 нечётно, можно заключить, что

$$\left(\frac{a}{n}\right) = \left(\frac{2^e}{n}\right) \cdot \left(\frac{a_1}{n}\right) = \left(\frac{2}{n}\right)^e \cdot \left(\frac{n \bmod a_1}{a_1}\right) (-1)^{(a_1-1)(n-1)/4}.$$

Отсюда можно получить следующий рекурсивный алгоритм для вычисления символа Якоби $\left(\frac{a}{n}\right)$, не требующий факторизации n .

ЯСОВИ(a,n)

ВХОД: нечётное целое $n \geq 3$, и целое $a \in Z_n^*$.

ВЫХОД: символ Якоби (Лежандра, если n – простое число) $\left(\frac{a}{n}\right)$

1. Если $a = 1$, то вернуть 1.

2. Если $2|a$
если $2|(n^2 - 1)/8$ вернуть ЯСОВИ $(a/2, n)$,
иначе вернуть $-\text{ЯСОВИ}(a/2, n)$;

(*теперь a – нечетное*)

3. Если $2|(a-1)(n-1)/4$ вернуть ЯСОВИ $(n \bmod a, a)$;

4. вернуть $-\text{ЯСОВИ}(n \bmod a, a)$.

Сложность алгоритма $O((\log n)^3)$. Символ Лежандра лучше вычислять по этому алгоритму, чем возведением в степень.

Пример Для $a = 158$ и $n = 235$ алгоритм вычисляет символ Якоби $\left(\frac{158}{235}\right)$ следующим образом:

$$\left(\frac{158}{235}\right) = -\left(\frac{79}{235}\right) = \left(\frac{77}{79}\right) = \left(\frac{2}{77}\right) = -\left(\frac{1}{77}\right) = -1.$$

Здесь учтено, что 2 не делит $(235^2 - 1)/8$, 2 не делит $(78 \cdot 234)/4$, $2|(76 \cdot 78)/4$, 2 не делит $(77^2 - 1)/8$. Заметим, что если n – простое число, то символ Якоби, просто вычисляемый описанным способом, указывает, является ли m квадратичным вычетом по модулю n .

Если же n – составное, например, $n = pq$, то m является квадратичным вычетом по модулю n тогда и только тогда, когда $\left(\frac{m}{p}\right) = 1$ и $\left(\frac{m}{q}\right) = 1$. Но эти два условия не следуют из равенства 1 символа Якоби числа m по модулю n ,

так как $\left(\frac{m}{n}\right) = 1$ и в том случае, когда $\left(\frac{m}{p}\right) = -1$ и $\left(\frac{m}{q}\right) = -1$. (Такие вычеты m называются *псевдоквадратами* по модулю $n = pq$).

Но не известно, как различить эти два случая, не разлагая число n на простые множители. То есть из равенства $\left(\frac{a}{n}\right) = 1$ ещё не следует, что число a является квадратичным вычетом.

Проблема квадратичного вычета в том и состоит, что требуется узнать, является ли число m , символ Якоби по модулю составного числа $n = pq$ которого равен 1, квадратичным вычетом. В настоящее время неизвестен алгоритм ее решения, не предполагающий факторизации числа n .

Пример Множество квадратичных вычетов по модулю $n = 21 : Q_{21} = \{1, 4, 16\}$; множество квадратичных невычетов по модулю $n = 21 : \bar{Q}_{21} = \{2, 5, 8, 10, 11, 13, 17, 19, 20\}$. Последнее включает три псевдоквадрата 5, 17 и 20.

Если разложение $n = pq$ известно, то можно извлечь квадратный корень из квадратичного вычета.

Действительно, если $0 < a < n$ – квадратичный вычет по модулю $n = pq$, то $a \bmod p$ является квадратичным вычетом по модулю p , и $a \bmod q$ является квадратичным вычетом по модулю q . то есть при существовании $x, x^2 \equiv a \pmod{n}$ существуют такие y и z , что

$$(\pm y)^2 \equiv a \pmod{p}, \quad (\pm z)^2 \equiv a \pmod{q}.$$

При известных p и q числа y и z могут быть найдены за полиномиальное время по алгоритму, приведенному ниже.

Тогда из сравнений

$$x \equiv \pm y \pmod{p} \quad x \equiv \pm z \pmod{q}$$

по китайской теореме об остатках¹ можно получить четыре квадратных корня x по модулю n . Обозначим их $\pm s$ и $\pm t$, где $s \not\equiv t \pmod{n}$. (Такие s и t называются *различными* квадратными корнями).

Таким образом, знание разложения $n = pq$ позволяет вычислить различные квадратные корни.

Проблема квадратного корня заключается в том, что требуется найти квадратный корень из квадратичного вычета по модулю составного числа $n = pq$. В

¹Китайская теорема об остатках. Если модули m_i взаимно просты, то система сравнений

$$x \equiv a_i \pmod{m_i}, \quad i = 1, \dots, t,$$

имеет в интервале $[0, m - 1]$, $m = m_1 \cdot m_2 \cdot \dots \cdot m_t$ единственное решение x вида

$$x = \sum_{i=1}^t a_i \cdot N_i \cdot M_i \bmod m,$$

где $M_i = \frac{m}{m_i}$, $N_i = (M_i)^{-1} \pmod{m_i}$, $i = 1, \dots, t$.

При $t = 2$ $m = n = pq$, $m_1 = p$, $m_2 = q$, $M_1 = q$, $M_2 = p$, $N_1 = q^{-1} \bmod p$, $N_2 = p^{-1} \bmod q$. $N_2 p + N_1 q = 1$, то есть N_1 и N_2 можно найти посредством расширенного алгоритма Евклида. После этого вычисляем корни $x = yqN_1 \pm zpN_2$.

настоящее время неизвестен метод решения этой проблемы, не предполагающий факторизации числа n .

Проблема квадратного корня эквивалентна по сложности проблеме факторизации: как показано выше, знание факторизации составного модуля позволяет извлечь квадратный корень из квадратичного вычета; знание различных квадратных корней позволяет разложить $n = pq$ на простые множители за полиномиальное время. Действительно,

$$s^2 - t^2 = (s + t)(s - t) \equiv 0 \pmod{n}.$$

Это означает, что n делит $(s + t)(s - t)$.

Но по выбору s и t число n не делит ни $(s + t)$, ни $(s - t)$. Отсюда, число $s + t$ кратно числу p или q , и НОД($s + t, n$) есть p или q . Так что применяя алгоритм Евклида, можно разложить n .

2 Извлечение квадратного корня по модулю простого числа

Пусть p – простое число и $p - 1 = 2^s t$, где t – нечетное число, $s \geq 1$. Циклическая группа Z_p^* имеет единственную циклическую подгруппу G порядка 2^s . Квадратичные вычеты по модулю p из G имеют порядки, равные степени 2, поскольку они делят 2^{s-1} . Если $a \in Q_p$, то $a^t \in Q_p$ и $a^t \in G$, последнее – поскольку

$$a^{(p-1)/2} \equiv (a^t)^{2^{s-1}} \equiv 1 \pmod{p}.$$

Следовательно, существует четное k , $1 \leq k \leq 2^s$ такое, что

$$a^t g^k \equiv 1 \pmod{p}, \quad (*)$$

где g – образующий элемент подгруппы G .

Пусть найдены образующий элемент $g \in G$ и четное k . Определим

$$x = a^{(t+1)/2} g^{k/2}. \quad (**)$$

Легко проверить, что $x^2 \equiv a \pmod{p}$.

Таким образом, задача разбита на две части:

- (1) нахождение образующего элемента $g \in G$,
 - (2) нахождение наименьшего четного k , удовлетворяющего соотношению (*).
- Приведем алгоритм извлечения квадратного корня по модулю простого числа.

Первая задача решается легко: поскольку t нечетно, для любого $f \in \bar{Q}_n$ $\text{ord}_p(f^t) = 2^s \cdot t/t = 2^s$, поэтому f^t есть образующий элемент подгруппы G . Таким образом, выбирая случайно $f \in Z_n^p$ и проверяя $\left(\frac{f}{p}\right) = -1$, находим f^t – образующий элемент группы G . Вероятность успеха выбора такого элемента f есть $1/2$.

Вторая задача сложнее не на много. Для быстрого поиска k , удовлетворяющего (*), используем тот факт, что порядки не равных единице квадратичных вычетов из G есть степени 2. Так, полагая сначала

$$b = a^t \equiv a^t g^{2^s} \pmod{p}, (**)$$

имеем $b \in G$. Теперь можно найти наименьшее m , $0 \leq m < s$ такое, что

$$b^{2^m} \equiv 1 \pmod{p}$$

и затем преобразовать b следующим образом:

$$b := b g^{2^{s-m}} \equiv a^t g^{2^{s-m}} \pmod{p}.$$

После этого порядок b уменьшается, но остается степенью 2, b остается квадратичным вычетом из G . При повторном редуцировании m строго уменьшается. Когда m станет равным 0, b будет равно 1 и (***) преобразуется в (*).

Поскольку $s < \log_2 p$, временная сложность алгоритма есть $O((\log p)^4)$.

Алгоритм:

ВХОД: простое число p , целое $a \in Q_n$.

ВЫХОД: квадратный корень a по модулю p .

1. (инициализация) Представить $p - 1 = 2^s t$, где t нечетно; присвоить $b = a^t \pmod{p}$; $r := s$, $k := 0$;

2. (первая задача) Найти $f \in \bar{Q}_n$; присвоить $g := f^t \pmod{p}$;

3. (вторая задача, поиск экспоненты k);
пока $b \neq 1$

3.1. Найти наименьшее неотрицательное m такое, что $b^{2^m} \equiv 1 \pmod{p}$;

3.2. Присвоить $b := b g^{2^{r-m}} \pmod{p}$; $k := k + 2^{r-m}$; $r := m$;

4. Вернуть $a^{(t+1)/2} g^{k/2} \pmod{p}$.

Этот алгоритм можно оптимизировать, не прибегая к явному вычислению константы k . 3.34 Algorithm Finding square roots modulo a prime p

ВХОД: нечетное простое p и целое a , $1 \leq a \leq p - 1$.

ВЫХОД: два квадратных корня числа a по модулю p , в предположении, что a есть квадратичный вычет по модулю p .

1. Вычислить символ Лежандра $\left(\frac{a}{p}\right)$. Если $\left(\frac{a}{p}\right) = -1$, то вернуть (a не имеет квадратных корней по модулю p).

2. Выбирать случайно целые b , $1 \leq b \leq p - 1$, пока не будет найдено число b с символом Лежандра $\left(\frac{b}{p}\right) = -1$. (b есть квадратичный невычет по модулю p .)

3. Многократным делением на 2, получить $p - 1 = 2^s t$, где t нечетно.

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

5. Принять $c = b^t \pmod{p}$ и $r = a^{(t+1)/2} \pmod{p}$.

6. Для i от 1 до $s - 1$ выполнить:

6.1 Вычислить $d = (r^2 \cdot a^{-1})^{2^{s-i-1}} \bmod p$.

6.2 Если $d = -1 \pmod p$ то принять $r = r \cdot c \bmod p$.

6.3 Принять $c = c^2 \bmod p$.

7. Вернуть $(r, -r)$.

Этот, как и предыдущий алгоритм вероятностный. Детерминированных алгоритмов вычисления квадратного корня по модулю простого числа не известно.

Временная сложность этого алгоритма $O((\lg p)^4)$ битовых операций. This running time is obtained by observing that the dominant step (step 6) is executed (шаг 6 выполняется $s - 1$ раз, и в каждой итерации осуществляется возведение в степень, что требует $O((\lg p)^3)$ битовых операций. При малых s алгоритм работает быстрее.

Следующий алгоритм извлечения квадратного корня по модулю простого p предпочтительнее предыдущего в случае, когда $p - 1 = 2^s \cdot t$ при большом s , Например, в случае $p =$

790762591593025597461690248883442887156873251046766537259507420759800756
885340391414355824906001849647163464719568407053284015160383715877576202
972647865599756069611215219841551710680581558897385363619436264520004024
943412577612853634081162952484870437802465588853079668909723314687042262
731110152375813123986025506282051028274131990114843153499921321536353412
123718819495024628444224954859555578112245361254951708505453123399592288
974958667314401447678725215059274302265492268715086929181289632592793450
329368110258606671034730438207904280955657396643455904470057597322823111
798907895051971628799553820312134264392969181087564531492486597943311483
561642257154916441049575213012723975639912768595476399985299565200071580
693336928840870775354909511426182000794770163281734978904607653027709683
874908182534763506636480251502958517442170156106038041467511991876017811
096612039654827801357797752279997987800765547180445349374589823395369823
9585008558258080513959919617=
= $2^{2690} \cdot 134078079299425970995740194528664578858496466637645984662101520887$
 $255159836644537417563868425624270286418470656111680864392527457611739049$
 $57497751170449409 + 1$.

ВХОД: нечетное простое a квадратичный вычет $a \in Q_p$.

ВЫХОД: два квадратных корня a по модулю p .

1. Выбирать случайно b , пока не будет получен квадратичный невычет $b^2 - 4a$ по модулю p т.е. $\left(\frac{b^2 - 4a}{p}\right) = -1$.

2. Пусть $f(X)$ есть полином $X^2 - bX + a$ в $Z_p[X]$.

Вычислить $r = X^{\frac{p+1}{2}} \bmod f(X)$. (r окажется целым.)

4. Вернуть $(r, -r)$.

Временная сложность этого алгоритма $O(\lg p)^3$ битовых операций.

Примечание. Если $p \equiv 3$ или $7 \pmod{4}$, то квадратный корень по модулю p можно получить по формуле

$$x = \pm a^{(p+1)/4} \pmod{p}.$$

Действительно, в этом случае $p+1$ кратно 4. Пусть $x = a^{(p+1)/4} \pmod{p}$. Тогда с учетом того, что $a^{(p-1)/2} \equiv 1 \pmod{p}$, имеем

$$x^2 \equiv a^{(p+1)/2} \equiv a^{(p-1)/2} a \equiv a \pmod{p}.$$

Если $p \equiv 5 \pmod{8}$, то

$$\text{а) } x = \pm a^{(p+3)/8} \pmod{p}, \text{ если } d = 1,$$

$$\text{б) } x = \pm (4a)^{(p+3)/8} / 2 \pmod{p}, \text{ если } d = p - 1,$$

где $d = a^{(p-1)/4} \pmod{p}$.

Действительно, в этом случае $p+3$ кратно 8. Поскольку $(p-1)/2$ нечетно, -1 удовлетворяет критерию Эйлера как квадратичный вычет. Пусть $x = a^{(p+3)/8} \pmod{p}$, $a \in \mathbb{Q}_p$.

Из $a^{(p-1)/2} \equiv 1 \pmod{p}$, с учетом, что 1 в \mathbb{Z}_p^* имеет только два квадратных корня 1 и -1 , получаем $a^{(p-1)/4} \equiv \pm 1 \pmod{p}$.

Следовательно,

$$x^2 \equiv a^{(p+3)/4} \equiv a^{(p-1)/4} \cdot a \equiv \pm a \pmod{p}.$$

Если знак $+$, то это соответствует случаю а).

Если знак $-$, то

$$-x^2 \equiv (\sqrt{-1}x)^2 \equiv a \pmod{p}.$$

Поэтому решением является

$$x = \sqrt{-1} a^{(p+3)/8} \pmod{p}.$$

Задача сведена к вычислению $\sqrt{-1} \pmod{p}$.

Пусть b есть квадратичный невычет по модулю p . Тогда по критерию Эйлера

$$(b^{(p-1)/4})^2 \equiv b^{(p-1)/2} \equiv -1 \pmod{p},$$

отсюда $b^{(p-1)/4} \pmod{p}$ можно взять вместо $\sqrt{-1} \pmod{p}$:

$$x \equiv (\sqrt{-1} a^{(p+3)/8} \pmod{p}) \equiv b^{(p-1)/4} a^{(p+3)/8} \pmod{p}.$$

Далее, заметим, что

$$p^2 - 1 = (p+1)(p-1) = (8k+6)(8k+4) = 8(4k+3)(2k+1),$$

и правая часть есть нечетное число, умноженное на 8. Поэтому $2 \in \bar{Q}_p$ (по свойству $\left(\frac{2}{p}\right)$). Таким образом, в этом случае можно использовать $2^{(p-1)/4}$ вместо $\sqrt{-1}$. Таким образом,

$$x \equiv (\sqrt{-1}a^{(p+3)/8} \equiv 2^{(p-1)/4}a^{(p+3)/8} \equiv (4a)^{(p+3)/8}/2 \pmod{p}.$$

Алгоритм извлечения квадратного корня по модулю p , $p \equiv 3$, или $7 \pmod{4}$ или $p \equiv 5 \pmod{8}$.):

ВХОД: простое число p , $p \equiv 3$, или $7 \pmod{4}$ или $p \equiv 5 \pmod{8}$, квадратичный вычет a по модулю p .

ВЫХОД: квадратный корень x числа a по модулю p .

1. Если $p \equiv 3$ или $7 \pmod{8}$ вернуть $a^{(p+1)/4} \pmod{p}$;
2. если $a^{(p-1)/4} \equiv 1 \pmod{p}$ вернуть $a^{(p+3)/8} \pmod{p}$;
3. вернуть $(4a)^{(p+3)/8}/2 \pmod{p}$.

Сложность этого алгоритма есть $O((\log p)^3)$.

Рассмотренные выше алгоритмы могут быть распространены на любые поля F_q нечетного порядка $q = p^m$, p простое, $m \geq 1$. Квадратные корни в полях четного порядка вычисляются в соответствии со следующим фактом:

Каждый элемент $a \in F_{2^m}$ поля четного порядка имеет единственный квадратный корень $a^{2^{m-1}}$.

3 Числа Блума

Особое значение в криптографии имеют числа Блума (Blum numbers). Составное число $n = pq$ называется числом Блума, если p и q – простые числа, сравнимые с 3 по модулю 4. Они имеют следующие свойства:

- 1) $\left(\frac{-1}{p}\right) = \left(\frac{-1}{q}\right) = -1$, следовательно, $\left(\frac{-1}{n}\right) = 1$;
- 2) Для $y \in Z_n^*$, если $\left(\frac{y}{n}\right) = 1$, то либо $y \in Q_n$, либо $y \in \bar{Q}_n$,
- 3) каждый вычет $y \in Q_n$ имеет 4 квадратных корня $t, -t, s, -s$, такие, что
 - а) $\left(\frac{s}{p}\right) = 1$, $\left(\frac{s}{q}\right) = 1$, то есть $t, s \in Q_n$;
 - б) $\left(\frac{-s}{p}\right) = 1$, $\left(\frac{-s}{q}\right) = 1$;
 - в) $\left(\frac{t}{p}\right) = -1$, $\left(\frac{t}{q}\right) = 1$;
 - г) $\left(\frac{-t}{p}\right) = 1$, $\left(\frac{-t}{q}\right) = -1$.
- д) функция $f(x) = x^2 \pmod{n}$ есть перестановка на Q_n ;
- е) для каждого $y \in Q_n$ точно один квадратный корень из y по модулю n , имеющий символ Якоби 1, меньше, чем $n/2$;
- ж) Z_n^* разбивается на четыре класса эквивалентности: мультипликативная группа Q_n и три смежных левых класса: $(-1)Q_n$, $\xi(Q_n)$, $(-\xi)Q_n$, где ξ есть квадратный корень из 1 по модулю n с символом Якоби -1 .

Примечание. По свойствам 3а), 3в) и 3б), 3г) два различных квадратных корня из квадратичного вычета имеют различные символы Якоби по модулю n .

4 Контрольные вопросы

1. Дайте определения квадратичного вычета и квадратичного невычета по заданному модулю.
2. Дайте определения символов Лежандра и символа Якоби.
3. Каковы свойства символа Якоби, позволяющие вычислить его, не прибегая к разложению модуля?
4. Сформулируйте критерий Эйлера для символа Лежандра.
5. Какова связь задач вычисления модульного квадратного корня и факторизации чисел?
6. Для каких мультипликативных групп известны детерминированные алгоритмы извлечения квадратного корня?
7. Какова особенность алгоритма извлечения квадратного корня по простому модулю для общего случая?

Литература.

1. Коблиц Н. курс теории чисел и криптография. –М: Научное издательство ТВП. 2001.
2. Саломаа А. Криптография с открытым ключом. М.: Мир, 1996.
3. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии, МЦН-МО, 2003.