1 Квадратичные вычеты. Символы Лежандра и Якоби. Квадратичный закон взаимности.

Пусть m - натуральное число, $a_0, a_1, a_2 \in \mathbb{Z}$, $a_2 \neq 0$. Рассмотрим квадратичное сравнение $a_2x^2 + a_1x + a_0 \equiv 0(\text{mod } m)$ относительно переменной x с помощью выделения полного квадрата, применения теоремы Эйлера и китайской теоремы об остатках может быть приведено к виду

$$x^2 \equiv a(\text{mod } m),$$

где $a \in \mathbb{Z}$.

Будем далее рассматривать квадратичные сравнения вида $x^2 \equiv a(\text{mod } m)$. Понятно, что не для всех a, m данное сравнение имеет решение.

Замечание 1. Для $a = 3$ и $m = 4$. Квадратичное сравнение $x^2 \equiv a(\text{mod } m)$ не имеет решений. В чем несложно убедиться небольшим перебором.

Определение 1. Если сравнение $x^2 \equiv a(\text{mod } m)$ имеет решение, то a называется *квадратичным вычетом* по модулю m, в противном случае число a называется *квадратичным невычетом* по модулю m.

Теорема 1. *Для простого числа $p > 2$ существует ровно $\frac{p-1}{2}$ квадратичных вычетов и $\frac{p-1}{2}$ невычетов.*

Доказательство. Заметим, что $x^2 \equiv (p-x)^2(\text{mod } p)$. Т.е. квадратичных вычетов не более чем $\frac{p-1}{2}$. Покажем, что среди чисел $1^2, \ldots, \left(\frac{p-1}{2}\right)^2$ нет сравнимых по модулю p. Пусть $x^2 \equiv y^2(\text{mod } p)$. Тогда $(x-y)(x+y)|p$ что невозможно так как $x \neq y$ и $x + y < p$. Таким образом, мы нашли $\frac{p-1}{2}$ квадратичных вычетов. □

Вальтер Стангл в 1996 году представил формулу, позволяющую вычислить количество квадратичных вычетов по произвольному модулю n.

Теорема 2. *Пусть $n = 2^t p_1^{d_1} \ldots p_k^{d_k}$ - каноническое разложение числа n. Тогда количество квадратичных вычетов по модулю n равно*

$$\left\lfloor \frac{2^{t-1}+5}{3} \right\rfloor \prod_{i=1}^{k} \left\lfloor \frac{p_i^{d_i+1} + 2p_i + 2}{2(p_i+1)} \right\rfloor$$

если $t = 0$, то левая часть формулы не учитывается.

Теорема 3 (Критерий Эйлера)**.** *Пусть $p > 2$ - простое. Число a, взаимнопростое с p, является квадратичным вычетом тогда и только тогда, когда*

$$a^{(p-1)/2} \equiv 1(mod\ p)$$

Доказательство. Пусть a является квадратичным вычетом по модулю p. Тогда $x^2 \equiv a(\text{mod } p)$. Следовательно, $a^{(p-1)/2} \equiv x^{p-1} \equiv 1(\text{mod } p)$.

Рассмотрим многочлен $x^{(p-1)/2} - 1 \bmod p$. Как показано выше, любой квадратичный вычет является его корнем. Так как p - простое, что данный многочлен имеет не более $(p-1)/2$ корней. С другой стороны количество квадратичных вычетов равно $(p-1)/2$. Следовательно, это корни многочлена $x^{(p-1)/2} - 1 \bmod p$. Таким образом теорема выполнена. □

Определение 2. Символ Лежандра $\left(\frac{a}{p}\right)$ для целого a и простого p определяется следующим образом

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

Приведем основные свойства символа Лежандра. Считаем, что $a, b \in \mathbb{Z}$, $(a, p) = 1$, $(b, p) = 1$, q - нечетное простое число, $(p, q) = 1$.

- $a \equiv b(\text{mod } p) \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$;
- $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2}(\text{mod } p)$(Критерий Эйлера);
- $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$;

- $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$;
- $\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right)$ (квадратичный закон взаимности).

Замечание 2. Если a - квадратичный вычет по простому модулю p и число p имеет вид $4k+3$, $k \in \mathbb{Z}$, то решения сравнения $x^2 \equiv a(\mathrm{mod}\ p)$ задаются формулой $x \equiv \pm a^{(p+1)/4}(\mathrm{mod}\ p)$.

Определение 3. Пусть n - нечетное натуральное число, большее 1, и $n = p_1 \dots p_k$ – разложение числа n на простые множители (не обязательно различные). Для любого целого a, $(a,n) = 1$, *символ Якоби* $\left(\frac{a}{n}\right)$ определяется через символы Лежандра по формуле:

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right) \dots \left(\frac{a}{p_k}\right)$$

Замечание 3. Для символа Якоби равенство $\left(\frac{a}{n}\right) = 1$ является лишь необходимым (но, вообще говоря, не достаточным) условием того, чтобы число a являлось квадратичным вычетом по модулю n. Однако в случае, когда $n = p^k$, p - нечетное простое, равенство $\left(\frac{a}{n}\right) = 1$ является критерием того, что число a – это квадратичный вычет по модулю n.

Приведем основные свойства символа Якоби. Считаем, что $a, b \in \mathbb{Z}$, $(a,P) = 1$, $(b,P) = 1$, Q - нечетное число, большее 1, $(P,Q) = 1$.

- $a \equiv b(\mathrm{mod}\ P) \Rightarrow \left(\frac{a}{P}\right) = \left(\frac{b}{P}\right)$;
- $\left(\frac{ab}{P}\right) = \left(\frac{a}{P}\right)\left(\frac{b}{P}\right)$;
- $a = \pm 1 \Rightarrow \left(\frac{a}{P}\right) = a^{(P-1)/2}$;
- $\left(\frac{2}{P}\right) = (-1)^{(P^2-1)/8}$;
- $\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2}\frac{Q-1}{2}}\left(\frac{P}{Q}\right)$ (квадратичный закон взаимности).

Пример 1.1. *Исследовать на разрешимость сравнение* $x^2 \equiv 983(mod\ 1103)$.
Заметим, что 1101 *- простое число. Вычислим символ Лежандра. Используем квадратичный закон взаимности*

$$\left(\frac{983}{1103}\right) = -\left(\frac{1103}{983}\right) = -\left(\frac{120}{983}\right) =$$
$$-\left(\frac{2}{983}\right)^3\left(\frac{3}{983}\right)\left(\frac{5}{983}\right) =$$
$$\left(\frac{983}{3}\right)\left(\frac{983}{5}\right) = \left(\frac{2}{3}\right)\left(\frac{3}{5}\right) =$$
$$\left(\frac{2}{3}\right)^2 = 1$$

Таким образом сравнение $x^2 \equiv 983(mod\ 1103)$ *разрешимо.*

Пример 1.2. *Исследовать на разрешимость сравнение* $x^2 \equiv 557(mod\ 854)$.
В силу китайской теоремы об остатках исходное сравнение разрешимо тогда и только тогда, когда разрешимо каждое из сравнений $x^2 \equiv 557 \equiv 1(mod\ 2)$, $x^2 \equiv 557 \equiv 4(mod\ 7)$, $x^2 \equiv 557 \equiv 8(mod\ 61)$. *Первое и второе сравнения, очевидно, разрешимы. Вычислим символ Лежандра* $\left(\frac{8}{61}\right)$, *рассматривая его как символ Якоби. Имеем* $\left(\frac{8}{61}\right) = \left(\frac{2}{61}\right) = (-1)^{465} = -1$.
Таким образом, третье сравнение не разрешимо, а значит, и исходное сравнение также не разрешимо.

1.1 Количество решений

Посчитаем количество решений сравнений $x^2 \equiv a(\mathrm{mod}\ m)$.

Теорема 4. *Пусть p - нечетное простое число. Тогда сравнение $x^2 \equiv 1(mod\, p^k)$ имеет только два решения.*

Доказательство. Заметим, что $x \equiv \pm 1(\mathrm{mod}\ p^k)$ являются решением. Таким образом имеется как минимум два решения. Покажем, что это единственные решения.

Пусть x_0 - решение сравнения. Тогда $p^k|(x_0^2 - 1)$. Покажем, что выполнено ровно одно из утверждений $p^k|(x_0 + 1)$ или $p^k|(x_0 - 1)$. Пусть это не так. Тогда $p^k|2$. Противоречие. Получаем, что или $x \equiv 1(\mathrm{mod}\ p^k)$ или $x \equiv -1(\mathrm{mod}\ p^k)$. □

Теорема 5. *Сравнение $x^2 \equiv 1(mod\ 2^k)$ имеет*

- *при $k = 1$ одно решение;*
- *при $k = 2$ два решения;*
- *при $k \geq 3$ четыре решения.*

$$x \equiv \pm 1(mod\ 2^k) \qquad x \equiv \pm(1 + 2^{k-1})(mod\ 2^k)$$

Во всех остальных случаях решений нет.

Доказательство. Утверждение теоремы несложно проверить перебором для $k = 1, 2, 3, 4$. Это база индукции. Предположим, что сравнение $x^2 \equiv 1(\mathrm{mod}\ 2^k)$ имеет четыре решения для некоторого $k > 2$. Предположим, что x это решение сравнения $x^2 \equiv 1(\mathrm{mod}\ 2^{k+1})$. Тогда x это решение сравнения $x^2 \equiv 1(\mathrm{mod}\ 2^k)$. Тогда x это одно из следующих значений

$$x \equiv \pm 1(\mathrm{mod}\ 2^{k+1}) \qquad x \equiv \pm(1 + 2^k)(\mathrm{mod}\ 2^{k+1})$$
$$x \equiv \pm(1 + 2^{k-1})(\mathrm{mod}\ 2^{k+1}) \qquad x \equiv \pm(1 + 2^{k-1} + 2^k)(\mathrm{mod}\ 2^{k+1})$$

Непосредственной проверкой убеждаемся, что только первые четыре значения являются решениями. □

Теорема 6. *Пусть $m = 2^k p_1^{k_1} \dots p_s^{k_s}$, где p_i - различные нечетные простые числа. Тогда число решений сравнения $x^2 \equiv 1(mod\ m)$, если они существуют, равно*

- 2^s *при $k = 0$ и $k = 1$;*
- 2^{s+1} *при $k = 2$;*
- 2^{s+2} *при $k \geq 3$.*

Доказательство. Воспользуемся великой китайской теоремой об остатках. Тогда для решения сравнения $x^2 \equiv 1(\mathrm{mod}\ m)$ необходимо решить следующую систему

$$\begin{cases} x^2 \equiv 1(\mathrm{mod}\ 2^k) \\ x^2 \equiv 1(\mathrm{mod}\ p_1^{k_1}) \\ \dots x^2 \equiv 1(\mathrm{mod}\ p_s^{k_s}) \end{cases} \tag{1}$$

Каждое из сравнений $x^2 \equiv 1(\mathrm{mod}\ p_i^{k_i})$ имеет ровно два решения. Сравнение $x^2 \equiv 1(\mathrm{mod}\ 2^k)$ имеет 1, 2 или 4 решения в зависимости от k. Используя результаты предыдущих теорем, заключаем, что теорема доказана. □

Можно сформулировать более общие варианты вышеизложенных теорем. Их доказательство уже более сложное.

Теорема 7. *Пусть p - нечетное простое число и $p|a$. Тогда сравнение $x^2 \equiv a(mod\ p^k)$ имеет два решения, если $\left(\frac{a}{p}\right) = 1$ и ни одного решения в противном случае.*

Теорема 8. *Пусть $2 \not| a$ сравнение $x^2 \equiv a(mod\ 2^k)$ имеет*

- *при $k = 1$ одно решение;*
- *при $k = 2, a \equiv 1(mod\ 4)$ два решения;*

- *при* $k \geq 3, a \equiv 1(mod\ 8)$ *четыре решения.*

Во всех остальных случаях решений нет.

Теорема 9. *Пусть* $m = 2^k p_1^{k_1} \dots p_s^{k_s}$, *где* p_i *- различные нечетные простые числа. Пусть* $(a, m) = 1$. *Тогда число решений сравнения* $x^2 \equiv a(mod\ m)$, *если они существуют, равно*

- 2^s *при* $k = 0$ *и* $k = 1$;
- 2^{s+1} *при* $k = 2$;
- 2^{s+2} *при* $k \geq 3$.

2 Приложения

Теорема 10. *Натуральное нечетное число* $n > 1$ *является простым тогда и только тогда, когда для любого* a, $(a, n) = 1$ *выполняется сравнение*

$$a^{\frac{(n-1)}{2}} \equiv \left(\frac{a}{n}\right) (mod\ n)$$

Соловей и Штрассен в 1977 году предложили следующий вероятностный тест проверки простоты чисел, основанный на критерии простоты.

Алгоритм 1 (Тест Соловея-Штрассена)**.** *Дано натуральное число* n.

1. *случайно выбрать число* $a \in \{1, \dots, n-1\}$ *и вычислить* $(a, n) = d$. *Если* $d \neq 1$, *то число составное.*
2. *если* $d = 1$, *то проверить выполнимость сравнения*

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

Если данное сравнение не выполнено, то число составное. В противном случае ответ неизвестно.

Утверждение 1. *Трудоемкость алгоритма оценивается величиной* $O(\log^3 n)$. *Вероятность того, что алгоритм выдаст ответ составное, если* n *составное не менее* $\frac{1}{2}$.