Сравнения произвольной степени по простому модулю

Теорема 2.7. Сравнение

$$f(x) \equiv 0 \pmod{p}, \tag{2.6}$$

где $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ и число p простое, равносильно сравнению степени не выше $p - 1$.

Пример 2.18. Найдем сравнение степени ниже 7, которому равносильно сравнение

$$f(x) = 2x^{11} + 5x^{10} + 2x^9 + 4x^8 + 2x^7 + 3x^6 + x^4 + 5x^3 + 3x^2 + 3x + 5 \equiv 0 \pmod{7}.$$

Делим $f(x)$ с остатком на $x^7 - x$: $f(x) = (x^7 - x)q(x) + r(x)$, где

$$q(x) = 2x^4 + 5x^3 + 2x^2 + 4x + 2, \quad r(x) = 3x^6 + 2x^5 + 6x^4 + 7x^3 + 7x^2 + 5x + 5.$$

Приводя коэффициенты полинома $r(x)$ по модулю 7, получаем:

$$f(x) \equiv 3x^6 + 2x^5 + 6x^4 + 5x + 5 \pmod{7}. \qquad \square$$

Теорема 2.8. Если сравнение (2.6) имеет больше чем n решений, то $a_i \equiv 0 \pmod{p}$ для $i = 0, 1, \ldots, n$.

Сравнения второй степени

Будем рассматривать сравнения второй степени вида

$$x^2 \equiv a \pmod{m}, \tag{2.7}$$

где $m \in \mathbb{N}$, $m > 1$, числа a и m взаимно просты. Целое число a представляет соответствующий класс вычетов по модулю m.

Определение 2.5. Если сравнение (2.7) разрешимо, то число a называется *квадратичным вычетом по модулю m*, в противном случае a называется *квадратичным невычетом по модулю m*.

Пример 2.19. Число 5 является квадратичным вычетом по модулю 11, поскольку сравнение $x^2 \equiv 5 \pmod{11}$ имеет очевидное решение $x \equiv 4 \pmod{11}$: $4^2 = 16 \equiv 5 \pmod{11}$. □

Пример 2.20. Число 21 является квадратичным вычетом по модулю $m = 541 \cdot 547 \cdot 563 \cdot 571 \cdot 587$, поскольку сравнение $x^2 \equiv 21 \pmod{m}$ имеет решение $x \equiv 10208002722743 \pmod{m}$. □

Пример 2.21. Число 3 является квадратичным невычетом по модулю 7, поскольку ни одно из чисел $1^2 = 1$, $2^2 = 4$, $3^2 = 9 \equiv 2 \pmod{7}$, $4^2 = 16 \equiv 2 \pmod{7}$, $5^2 = 25 \equiv 4 \pmod{7}$, $6^2 = 36 \equiv 1 \pmod{7}$ не сравнимо с 3 по модулю 7, то есть сравнение $x^2 \equiv 3 \pmod{7}$ не имеет решений. □

Символ Лежандра

Определение 2.6. Рассмотрим сравнение

$$x^2 \equiv a \pmod{p}, \tag{2.8}$$

где число p простое, $p \neq 2$, a не делится на p. Определим для таких a и p *символ Лежандра*

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{если сравнение (2.8) разрешимо,} \\ -1, & \text{если сравнение (2.8) неразрешимо.} \end{cases}$$

Таким образом, если $\left(\frac{a}{p}\right) = 1$, то a — квадратичный вычет по модулю p, если $\left(\frac{a}{p}\right) = -1$, то a — квадратичный невычет по модулю p.

Замечание. Понятие символа Лежандра можно обобщить и на случай, когда a делится на p. Тогда полагают $\left(\frac{a}{p}\right) = 0$.

Символ Лежандра обладает следующими свойствами для любых целых чисел a, b, не делящихся на простое число $p \neq 2$.

1. $\left(\frac{a+kp}{p}\right) = \left(\frac{a}{p}\right)$ для любого $k \in \mathbb{Z}$.

Доказательство. Равенство выполняется, поскольку $a + kp \equiv a \pmod{p}$ для любого $k \in \mathbb{Z}$. Таким образом, если $a \equiv b \pmod{p}$, то $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$. □

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

3. $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$. В частности, $\left(\frac{1}{p}\right) = 1$ для любого простого $p \neq 2$, $\left(\frac{-1}{p}\right) = 1$ при $p \equiv 1 \pmod 4$ и $\left(\frac{-1}{p}\right) = -1$ при $p \equiv 3 \pmod 4$.

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

5. Лемма 2.9 (Гаусс). $\left(\frac{a}{p}\right)=(-1)^{\mu}$, где μ — число отрицательных вычетов среди абсолютно наименьших вычетов чисел $a, 2\cdot a, \ldots, \frac{p-1}{2}\cdot a$.

Пример 2.22. Вычислим символ Лежандра $\left(\frac{5}{13}\right)$, используя лемму Гаусса. Составляем систему абсолютно наименьших вычетов: 5, $2\cdot 5=10\equiv -3 \pmod{13}$, $3\cdot 5=15\equiv 2 \pmod{13}$, $4\cdot 5=20\equiv -6 \pmod{13}$, $5\cdot 5=25\equiv -1 \pmod{13}$, $6\cdot 5=30\equiv 4 \pmod{13}$. Получили три отрицательных значения, значит, $\left(\frac{5}{13}\right)=(-1)^3=-1$. □

6. $\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$, то есть $\left(\frac{2}{p}\right)=1$ при $p\equiv \pm 1 \pmod 8$; $\left(\frac{2}{p}\right)=-1$ при $p\equiv \pm 3 \pmod 8$.

7. При изменении a от 1 до $p-1$ символ Лежандра принимает значения 1 и -1 одинаково часто.

Теорема 2.10 (квадратичный закон взаимности Гаусса). Пусть p и q — различные простые числа, $p \neq 2$, $q \neq 2$. Тогда

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

Другими словами, $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$, если $p \equiv q \equiv 3 \pmod 4$, и $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ в противном случае.

Пример 2.23. Вычислим символ Лежандра $\left(\frac{88}{347}\right)$. Разложим число 88 на множители: $88 = 2^3 \cdot 11$. Значит, согласно свойству 4,

$$\left(\frac{88}{347}\right) = \left(\frac{2^3 \cdot 11}{347}\right) = \left(\frac{2^3}{347}\right)\left(\frac{11}{347}\right).$$

По свойству 2 имеем: $\left(\frac{2^3}{347}\right) = \left(\frac{2\cdot 2^2}{347}\right) = \left(\frac{2}{347}\right)$. Поскольку $347 \equiv 3 \pmod 8$, по свойству 6 получаем $\left(\frac{2}{347}\right) = -1$.

Для вычисления $\left(\frac{11}{347}\right)$ воспользуемся квадратичным законом взаимности: $\left(\frac{11}{347}\right) = (-1)^{\frac{11-1}{2}\cdot\frac{347-1}{2}}\left(\frac{347}{11}\right) = (-1)^{5\cdot 173}\left(\frac{347}{11}\right) = -\left(\frac{347}{11}\right)$.

Поскольку $347 = 11 \cdot 31 + 6$, по свойству 1 получаем $\left(\frac{347}{11}\right) = \left(\frac{6}{11}\right)$.

Снова применяем свойство 4: $\left(\frac{6}{11}\right) = \left(\frac{2}{11}\right)\left(\frac{3}{11}\right)$. Вычисляем по свойству 6: $\left(\frac{2}{11}\right) = (-1)^{\frac{11^2-1}{8}} = (-1)^{15} = -1$, по свойству 3: $\left(\frac{3}{11}\right) \equiv 3^{\frac{11-1}{2}} = 3^5 = 243 \equiv 1 \pmod{11}$. Таким образом, $\left(\frac{11}{347}\right) = -(-1\cdot 1) = 1$ и $\left(\frac{88}{347}\right) = -1\cdot 1 = -1$. □

Пример 2.24. Используя квадратичный закон взаимности, найдем такие простые числа p, для которых 5 является квадратичным вычетом. Запишем символ Лежандра

$$\left(\frac{5}{p}\right)=(-1)^{\frac{5-1}{2}\cdot\frac{p-1}{2}}\left(\frac{p}{5}\right)=(-1)^{2\cdot\frac{p-1}{2}}\left(\frac{p}{5}\right)=\left(\frac{p}{5}\right)$$

и определим, при каких значениях p он равен 1. По свойству 3 символа Лежандра имеем:

$$\left(\frac{p}{5}\right)\equiv p^{\frac{5-1}{2}}=p^2(\mathrm{mod}\,5).$$

Таким образом, нужно найти такие простые числа p, для которых $p^2\equiv 1\ (\mathrm{mod}\ 5)$. Простое число $p\neq 5$ при делении на 5 может давать в остатке 1, 2, 3 или 4, при этом $1^2\equiv 4^2\equiv 1\ (\mathrm{mod}\ 5)$. Значит, число 5 является квадратичным вычетом по модулю простых чисел вида $5k+1$ и $5k+4$, где число k целое. Другими словами, число p, заданное в десятичной системе счисления, должно оканчиваться на 1 или на 9. Это, например, числа 11, 19, 29, 31 и т. д. □