Способы решения сравнения второй степени по модулю простого числа

Рассмотрим сравнение

$$x^2 \equiv a \pmod{p}, \qquad (2.11)$$

где число $p \neq 2$ простое и целое число a не делится на p.

Для того чтобы узнать, разрешимо ли сравнение, достаточно вычислить символ Лежандра $\left(\frac{a}{p}\right)$. При $\left(\frac{a}{p}\right) = -1$ сравнение (2.11) решений не имеет.

При $\left(\frac{a}{p}\right) = 1$ сравнение (2.11) разрешимо и имеет ровно два решения. Действительно, если $\left(\frac{a}{p}\right) = 1$, то по определению символа Лежандра сравнение (2.11) имеет хотя бы одно решение $x_1 \pmod{p}$. Пусть x_2 — другое решение сравнения (2.11). Тогда $x_1^2 \equiv a \pmod{p}$, $x_2^2 \equiv a \pmod{p}$, то есть $x_1^2 - x_2^2 \equiv 0 \pmod{p}$. Значит хотя бы одно из выражений $x_1 - x_2$, $x_1 + x_2$ должно делиться на p. В первом случае получаем уже имеющееся решение x_1, во втором случае — решение $x_2 \equiv -x_1 \pmod{p}$. При этом значения x_1 и $-x_1$ различны, в противном случае выполнялось бы соотношение $2x_1 \equiv 0 \pmod{p}$, что невозможно, поскольку $p \neq 2$ и НОД(x_1, p) = НОД(a, p) = 1. Кроме того, согласно теореме 2.8, сравнение (2.11) не может иметь более двух решений.

Рассмотрим некоторые способы решения сравнения (2.11) в зависимости от вида модуля.

Пусть $p \equiv 3 \pmod{4}$, то есть $p = 4m + 3$, где $m \in \mathbb{Z}$. Разрешимость сравнения (2.11) означает, что $\left(\frac{a}{p}\right) = 1$. По свойству 3 символа Лежандра $1 = \left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} = a^{2m+1} \pmod{p}$. Тогда

$$(a^{m+1})^2 = a^{2m+2} = a^{2m+1} \cdot a \equiv a \pmod{p}.$$

Таким образом, решение имеет вид $x \equiv \pm a^{m+1} \pmod{p}$.

Пример 2.26. Решим сравнение $x^2 \equiv 7 \pmod{31}$. Вычисляем символ Лежандра: $\left(\frac{7}{31}\right) = 1$, значит, сравнение разрешимо. Число 31 представляем в виде $31 = 4 \cdot 7 + 3$, то есть $m = 7$. Находим решение: $x \equiv \pm 7^8 = \pm 7^3 7^3 7^2 \equiv \pm 2 \cdot 2 \cdot 18 \equiv \pm 10 \pmod{31}$.

Проверка: $(\pm 10)^2 - 7 = 100 - 7 = 93 = 31 \cdot 3$. □

Пусть $p \equiv 5 \pmod 8$, то есть $p = 8m + 5$, где $m \in \mathbb{Z}$. Разрешимость сравнения (2.11) означает, что $\left(\frac{a}{p}\right) = 1$. По свойству 3 символа Лежандра $1 = \left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} = a^{4m+2} = (a^{2m+1})^2 \pmod p$. Отсюда $a^{2m+1} \equiv 1 \pmod p$ или $a^{2m+1} \equiv -1 \pmod p$. В первом случае, умножая обе части сравнения на a, получаем $a^{2m+2} \equiv a \pmod p$, то есть решение имеет вид $x \equiv \pm a^{m+1} \pmod p$.

При $a^{2m+1} \equiv -1 \pmod p$ ситуация немного сложнее. Заметим, что при $p \equiv 5 \pmod 8$ число 2 является квадратичным невычетом по модулю p. Действительно, $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = (-1)^{\frac{64m^2+80m+24}{8}} = (-1)^{8m^2+10m+3} = -1$. По свойству 3 символа Лежандра $\left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}} = 2^{4m+2} = (2^{2m+1})^2 \pmod p$. Таким образом, $(2^{2m+1})^2 \equiv -1 \pmod p$. Тогда

$$a^{2m+1} \cdot (2^{2m+1})^2 \equiv 1 \pmod p.$$

Умножая обе части этого сравнения на a, получаем решение сравнения (2.11): $x \equiv \pm a^{m+1} \cdot 2^{2m+1} \pmod p$.

Здесь вместо числа 2 можно брать любой другой квадратичный невычет по модулю p.

Пример 2.27. Решим сравнение $x^2 \equiv 10 \pmod{53}$. Вычисляем символ Лежандра: $\left(\frac{10}{53}\right)=1$, значит, сравнение разрешимо. Число 53 представляем в виде $53 = 8 \cdot 6 + 5$, то есть $m = 6$. Поскольку $10^{2 \cdot 6+1} \equiv 1 \pmod{53}$, находим решение: $x \equiv \pm 10^7 \equiv \pm 13 \pmod{53}$.

Проверка: $(\pm 13)^2 - 10 = 169 - 10 = 159 = 53 \cdot 3$. □

Пример 2.28. Решим сравнение $x^2 \equiv 11 \pmod{37}$. Вычисляем символ Лежандра: $\left(\frac{11}{37}\right)=1$, значит, сравнение разрешимо. Число 37 представляем в виде $37 = 8 \cdot 4 + 5$, то есть $m = 4$. Поскольку $11^{2 \cdot 4+1} \equiv -1 \pmod{37}$, находим решение: $x \equiv \pm 11^5 \cdot 2^9 \equiv \pm 14 \pmod{37}$.

Проверка: $(\pm 14)^2 - 11 = 196 - 11 = 185 = 37 \cdot 5$. □

Пусть $p \equiv 1 \pmod 8$. Представим p в виде $p = 2^k \cdot h + 1$, где $k \geq 3$, число h нечетное. Разрешимость сравнения (2.11) означает, что $\left(\frac{a}{p}\right)=1$. По свойству 3 символа Лежандра $1=\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} = a^{2^{k-1} \cdot h} \pmod p$. Отсюда $a^{2^{k-2} \cdot h} \equiv \pm 1 \pmod p$. Пусть N — произвольный квадратичный невычет по модулю p, то есть $-1=\left(\frac{N}{p}\right) \equiv N^{2^{k-1} \cdot h} \pmod p$. Тогда при некотором целом $s_2 \geq 0$ получим $a^{2^{k-2} \cdot h} \cdot N^{2^{k-1} \cdot s_2} \equiv 1 \pmod p$, откуда $a^{2^{k-3} \cdot h} \cdot N^{2^{k-2} \cdot s_2} \equiv \pm 1 \pmod p$. Далее, при некотором целом $s_3 \geq 0$ получим $a^{2^{k-3} \cdot h} \cdot N^{2^{k-2} \cdot s_3} \equiv 1 \pmod p$, откуда $a^{2^{k-4} \cdot h} \cdot N^{2^{k-3} \cdot s_3} \equiv \pm 1 \pmod p$ и т. д. Получив сравнение $a^h \cdot N^{2 s_k} \equiv 1 \pmod p$ для некоторого целого $s_k \geq 0$ и умножив обе его части на a, получаем решение $x \equiv \pm a^{\frac{h+1}{2}} \cdot N^{s_k} \pmod p$.

Алгоритм 2.2. Решение сравнения второй степени по модулю простого числа [4].

Вход. Простое число $p \neq 2$; такие целые числа a и N, что $\left(\frac{a}{p}\right) = -\left(\frac{N}{p}\right) = 1$.

Выход. Решение сравнения $x^2 \equiv a \pmod{p}$.

1. Представить число p в виде $p = 2^k \cdot h + 1$, где число h нечетное.
2. Положить $a_1 \leftarrow a^{\frac{h+1}{2}} \pmod{p}$, $a_2 \leftarrow a^{-1} \pmod{p}$, $N_1 \leftarrow N^h \pmod{p}$, $N_2 \leftarrow 1, j \leftarrow 0$.
3. Для $i = 0, 1, \ldots, k-2$ выполнять следующие действия.
   3.1. Положить $b \leftarrow a_1 N_2 \pmod{p}$.
   3.2. Вычислить $c \leftarrow a_2 b^2 \pmod{p}$.
   3.3. Вычислить абсолютно наименьший вычет $d \leftarrow c^{2^{k-2-i}} \pmod{p}$.
   При $d = 1$ положить $j_i \leftarrow 0$, при $d = -1$ положить $j_i \leftarrow 1$.
   3.4. Положить $N_2 \leftarrow N_2 N_1^{2^i j_i} \pmod{p}$.
4. Результат: $\pm a_1 N_2 \pmod{p}$. □

Сложность этого алгоритма равна $O(\log^4 p)$.

Пример 2.29. Решим сравнение $x^2 \equiv 14 \pmod{193}$. Вычисляем символ Лежандра: $\left(\frac{14}{193}\right) = 1$, значит, сравнение разрешимо. Выбираем $N = 5$, $\left(\frac{5}{193}\right) = -1$. Находим представление $193 = 2^6 \cdot 3 + 1$, то есть $k = 6$, $h = 3$.

Полагаем $a_1 = 14^2 \equiv 3 \pmod{193}$, $a_2 = 14^{-1} \equiv 69 \pmod{193}$, $N_1 = 5^3 \equiv 125 \pmod{193}$, $N_2 = 1, j = 0$.

Результаты вычислений сведем в таблицу:

i	$b \equiv a_1 N_2$	$c \equiv a_2 b^2$	$d \equiv c^{2^{4-i}}$	j_i	N_2
0	3	42	-1	1	125
1	182	50	-1	1	158
2	88	112	1	0	158
3	88	112	-1	1	39
4	117	192	-1	1	122

Тогда решением сравнения будет $x = \pm 3 \cdot 122 \equiv \pm 173 \pmod{193}$.

Проверка: $(\pm 173)^2 - 14 = 29929 - 14 = 29915 = 193 \cdot 155$. □