Способы решения сравнения второй степени по составному модулю

Теорема 2.11. Пусть число p простое, $p \neq 2$, целое число a не делится на p и $n \in \mathbb{N}$, $n \geq 1$. Для того чтобы сравнение

$$x^2 \equiv a \pmod{p^n} \qquad (2.12)$$

было разрешимо, необходимо и достаточно, чтобы было разрешимо сравнение

$$x^2 \equiv a \pmod{p}. \qquad (2.13)$$

Определение 2.8. *Порядком* числа a, $1 \leq a < m$, НОД$(a, m) = 1$, по модулю m называется наименьшее натуральное число d, для которого $a^d \equiv 1 \pmod{m}$.

Определение 2.9. Число a, $1 \leq a < m$, порядка $\varphi(m)$ по модулю m называется *первообразным корнем по модулю m*.

Лемма 2.12. Для числа a, имеющего порядок d по модулю m, сравнение $a^{\gamma_1} \equiv a^{\gamma_2} \pmod{m}$ выполняется тогда и только тогда, когда $\gamma_1 \equiv \gamma_2 \pmod{d}$.

Лемма 2.13. Если число a имеет порядок $d_1 d_2$ по модулю m, то число a^{d_1} имеет порядок d_2 по модулю m.

Лемма 2.14. Если числа a_1, a_2 имеют по модулю m порядки d_1, d_2 соответственно, причем НОД$(d_1, d_2) = 1$, то число $a_1 a_2$ имеет по модулю m порядок $d_1 d_2$.

Теорема 2.15. Для любого простого $p \neq 2$ существует первообразный корень по модулю p.

Пример 2.30. Число 2 является первообразным корнем по модулю 13, поскольку $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 16 \equiv 3 \pmod{13}$, $2^5 \equiv 6$

$\pmod{13}$, $2^6 \equiv 12 \pmod{13}$, $2^7 \equiv 11 \pmod{13}$, $2^8 \equiv 9 \pmod{13}$, $2^9 \equiv 5$ $\pmod{13}$, $2^{10} \equiv 10 \pmod{13}$, $2^{11} \equiv 7 \pmod{13}$, $2^{12} \equiv 1 \pmod{13}$ и $\varphi(13) = 12$.□

Теорема 2.16. Для любого простого $p \neq 2$ существует первообразный корень по модулю p^2.

Пример 2.31. Число 3 является первообразным корнем по модулю 7 и $3^6 = 729 \equiv 43 \quad 1 \pmod{7^2}$. Значит, согласно доказательству теоремы 2.16, число 3 является первообразным корнем по модулю 7^2. Проверяем: $3^1 = 3$, $3^2 = 9$, $3^3 = 27$, $3^4 \equiv 32 \pmod{7^2}$, …, $3^{21} \equiv 48 \equiv -1$ $\pmod{7^2}$, …, $3^{39} \equiv 20 \pmod{7^2}$, $3^{40} \equiv 11 \pmod{7^2}$, $3^{41} \equiv 33 \pmod{7^2}$, $3^{42} \equiv 1$ $\pmod{7^2}$. □

Теорема 2.17. Если сравнение (2.12) разрешимо, то оно имеет ровно два решения.

Следствие. Число квадратичных вычетов по модулю p^n, где p — простое число, $p \neq 2$, равно числу квадратичных невычетов по модулю p^n.

Пример 2.32. Решим сравнение $x^2 \equiv 3 \pmod{11^3}$. Оно разрешимо, поскольку $\left(\frac{3}{11}\right) = 1$ и сравнение $x^2 \equiv 3 \pmod{11}$ разрешимо. Поскольку $11 \equiv 3 \pmod 4$, находим решение сравнения $x^2 \equiv 3 \pmod{11}$ как $x \equiv 3^{2+1} = 27 \equiv 5 \pmod{11}$, то есть $x = 5 + 11k_1$. Вычисляем: $x^2 = 25 + 2 \cdot 5 \cdot 11k_1 \equiv 3 \pmod{11^2}$. Отсюда

$$2 \cdot 5 \cdot 11k_1 \equiv -22 \pmod{11^2},$$

$$2 \cdot 5 \cdot k_1 \equiv -2 \pmod{11},$$

$$k_1 \equiv -2 \cdot (2 \cdot 5)^{-1} \equiv -2 \cdot (-1)^{-1} \equiv -2 \cdot (-1) = 2 \pmod{11},$$

то есть $k_1 = 2 + 11k_2$, $x = 5 + 11 \cdot 2 + 11^2 k_2 = 27 + 11^2 k_2$.

Ищем коэффициент k_2. Возводим x в квадрат по модулю 11^3: $x^2 = 27^2 + 2 \cdot 27 \cdot 11^2 k_2 \equiv 3 \pmod{11^3}$. Отсюда

$$2 \cdot 27 \cdot 11^2 k_2 \equiv -726 \pmod{11^3},$$

$$2 \cdot 27 \cdot k_2 \equiv -6 \pmod{11},$$

$$k_2 \equiv -6 \cdot (2 \cdot 27)^{-1} \equiv -6 \cdot (-1)^{-1} \equiv -6 \cdot (-1) = 6 \pmod{11},$$

то есть $k_2 = 6 + 11k_3$, $x_3 = 27 + 11^2 \cdot 6 + 11^3 k_3 \equiv 753 \pmod{11^3}$.

Второе решение: $-753 \equiv 578 \pmod{11^3}$. Это же решение получается, если строить x_3 из начального значения $x \equiv 6 \pmod{11}$ — второго решения сравнения $x^2 \equiv 3 \pmod{11}$.

Проверка:

$753^2 - 3 = 567006 = 11^3 \cdot 426$, $578^2 - 3 = 334081 = 11^3 \cdot 251$. □

Теорема 2.18. Пусть число a нечетное. Справедливы следующие утверждения.

1. Сравнение $x^2 \equiv a \pmod 2$ разрешимо при любом a.

2. Сравнение $x^2 \equiv a \pmod{2^2}$ разрешимо тогда и только тогда, когда $a \equiv 1 \pmod 4$.

3. Сравнение $x^2 \equiv a \pmod{2^n}$, где $n \geq 3$, разрешимо тогда и только тогда, когда $a \equiv 1 \pmod 8$.

Пример 2.33. Решим сравнение $x^2 \equiv 41 \pmod{64}$, то есть $n = 6$. Поскольку $41 \equiv 1 \pmod 8$, сравнение разрешимо. Представляем решение в виде $x = \pm(1 + 4t_3)$. Тогда

$$(1 + 4t_3)^2 \equiv 41 \pmod{2^4},$$

$$2 \cdot 4t_3 \equiv 40 \pmod{2^4},$$

$$t_3 \equiv 1 \pmod 2,$$

то есть $t_3 = 1 + 2t_4$ и $x = \pm(5 + 8t_4)$.

Далее,

$$(5 + 8t_4)^2 \equiv 41 \pmod{2^5},$$

$$2 \cdot 5 \cdot 8t_4 \equiv -16 \pmod{2^5},$$

$$t_4 \equiv 1 \pmod 2,\ t_4 = 1 + 2t_5,\ x = \pm(13 + 16t_5);$$

$$(13 + 16t_5)^2 \equiv 41 \pmod{2^5},$$

$$2 \cdot 13 \cdot 16t_5 \equiv -128 \pmod{2^5},$$

$$t_5 \equiv 0 \pmod 2,\ t_5 = 2t_6,\ x = \pm(13 + 32t_6).$$

Отсюда получаем четыре решения: $x \equiv \pm 13$, $x \equiv \pm 45 \pmod{64}$.

Проверка: $(\pm 13)^2 - 41 = 169 - 41 = 128 = 64 \cdot 2$; $(\pm 45)^2 - 41 = 2025 - 41 = 1984 = 64 \cdot 31$. □

Теорема 2.19. Пусть $m = m_1 m_2 \ldots m_r$, где числа $m_1, m_2, \ldots, m_r$ попарно взаимно просты. Для того чтобы сравнение (2.7) было разрешимо, необходимо и достаточно, чтобы были разрешимы все сравнения $x^2 \equiv a \pmod{m_1}$, $x^2 \equiv a \pmod{m_2}$, …, $x^2 \equiv a \pmod{m_r}$.

Пример 2.34. Сравнение $x^2 \equiv 13 \pmod{35}$ не имеет решений, хотя

$$\left(\frac{13}{35}\right) = (-1)^{\frac{13-1}{2}\frac{35-1}{2}} \left(\frac{35}{13}\right) = (-1)^{6\cdot 17} \left(\frac{9}{13}\right) = \left(\frac{9}{13}\right) = \left(\frac{3^2}{13}\right) = \left(\frac{1}{13}\right) = 1.$$

Представим этот символ Якоби в виде $\left(\frac{13}{35}\right) = \left(\frac{13}{5}\right)\left(\frac{13}{7}\right)$. Вычисляя символы Лежандра в правой части равенства, получаем

$$\left(\frac{13}{5}\right) = \left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1,$$

$$\left(\frac{13}{7}\right) = \left(\frac{6}{7}\right) = \left(\frac{2}{7}\right)\left(\frac{3}{7}\right) = 1 \cdot (-1)\left(\frac{7}{3}\right) = -\left(\frac{7}{3}\right) = -1 \cdot 1 = -1,$$

то есть число 13 является квадратичным невычетом по модулям 5 и 7. □

Следствие 1. Пусть $m = 2^n p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s}$ — каноническое разложение целого числа m и целое число a взаимно просто с m. Сравнение $x^2 \equiv a \pmod{m}$ разрешимо тогда и только тогда, когда $a \equiv 1 \pmod{4}$ при $n = 2$, $a \equiv 1 \pmod{8}$ при $n \geq 3$ и $\left(\frac{a}{p_1}\right) = \left(\frac{a}{p_2}\right) = \ldots = \left(\frac{a}{p_s}\right) = 1$. Это сравнение имеет 2^s решений при $n = 0$ или $n = 1$; 2^{s+1} решений при $n = 2$; 2^{s+2} решений при $n \geq 3$.

Следствие 2. Если целое число m имеет хотя бы два взаимно простых делителя, то число квадратичных вычетов по модулю m строго меньше, чем число квадратичных невычетов. Для заданного нечетного числа $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$ произвольное наугад взятое число a, взаимно простое с m, будет квадратичным вычетом с вероятностью $\frac{1}{2^s}$.

Пример 2.35. Решим сравнение $x^2 \equiv 1033 \pmod{2^4 \cdot 3^3 \cdot 19}$.

Это сравнение разрешимо, поскольку $1033 \equiv 1 \pmod 8$ и выполняются равенства для символов Лежандра $\left(\frac{1033}{3}\right) = \left(\frac{1033}{19}\right) = 1$.

В обозначениях следствия 1 $s = 2$, $n = 4$, значит, сравнение имеет $2^{2+2} = 16$ решений.

Решаем сравнение по модулю 19: $x^2 \equiv 1033 \equiv 7 \pmod{19}$. Так как $19 \equiv 3 \pmod 4$, по способу п. 2.3.2 решением будет $x \equiv \pm 7^5 \equiv \pm 8 \pmod{19}$.

Решаем сравнение по модулю 3^3: $x^2 \equiv 1033 \equiv 7 \pmod{3^3}$. Ищем решение в виде $x_0 + 3k_1 + 9k_2$. Находим $x_0 \equiv 1 \pmod 3$ — решение сравнения $x^2 \equiv 7 \equiv 1 \pmod 3$. Далее, $(1 + 3k_1)^2 \equiv 1 + 6k_1 \equiv 7 \pmod{3^2}$, $k_1 \equiv 1 \pmod 3$; $(4 + 9k_2)^2 \equiv 16 + 72k_2 \equiv 7 \pmod{3^3}$, $k_2 \equiv 1 \pmod 3$. Таким образом, нашли решение $x \equiv \pm 13 \pmod{3^3}$.

Решаем сравнение по модулю 2^4: $x^2 \equiv 1033 \equiv 9 \pmod{2^4}$. Отсюда очевидные решения: $x \equiv \pm 3 \pmod{2^4}$, $x \equiv \pm 5 \pmod{2^4}$.

Восстанавливаем решения исходного сравнения по китайской теореме об остатках. Решаем систему $x \equiv 8 \pmod{19}$, $x \equiv 13 \pmod{3^3}$, $x \equiv 3 \pmod{2^4}$:

$$x \equiv 8 \cdot 3^3 \cdot 2^4 \cdot (3^{-3} \cdot 2^{-4} \pmod{19}) + 13 \cdot 19 \cdot 2^4 \cdot (19^{-1} \cdot 2^{-4} \pmod{3^3}) +$$

$$+ 3 \cdot 19 \cdot 3^3 \cdot (19^{-1} \cdot 3^{-3} \pmod{2^4}) \equiv 3456 \cdot 15 + 3952 \cdot 4 + 1539 \cdot 1 \equiv$$

$$\equiv 3523 \pmod{2^4 \cdot 3^3 \cdot 19}.$$

Аналогично находим еще семь решений:

$x \pmod{19}$	$x \pmod{3^3}$	$x \pmod{2^4}$	$x \pmod{2^4 \cdot 3^3 \cdot 19}$
8	13	5	4549
8	−13	3	4739
8	−13	5	5765
−8	13	3	6547
−8	13	5	7573
−8	−13	3	7763
−8	−13	5	581

Остальные восемь решений противоположны найденным по знаку.

Итак, окончательный результат: $x \equiv \pm 445,\ 581,\ \pm 635,\ \pm 1661,\ \pm 2443,\ \pm 3469,\ \pm 3523,\ \pm 3659 \pmod{2^4 \cdot 3^3 \cdot 19}$.

Проверка:

$(\pm 445)^2 - 1033 = 196992 = 2^4 \cdot 3^3 \cdot 19 \cdot 24,$

$(\pm 581)^2 - 1033 = 336528 = 2^4 \cdot 3^3 \cdot 19 \cdot 41,$

$(\pm 635)^2 - 1033 = 402192 = 2^4 \cdot 3^3 \cdot 19 \cdot 49,$

$(\pm 1661)^2 - 1033 = 2757888 = 2^4 \cdot 3^3 \cdot 19 \cdot 336,$

$(\pm 2443)^2 - 1033 = 5967216 = 2^4 \cdot 3^3 \cdot 19 \cdot 727,$

$(\pm 3469)^2 - 1033 = 12032928 = 2^4 \cdot 3^3 \cdot 19 \cdot 1466,$

$(\pm 3523)^2 - 1033 = 12410496 = 2^4 \cdot 3^3 \cdot 19 \cdot 1512,$

$(\pm 3659)^2 - 1033 = 13387248 = 2^4 \cdot 3^3 \cdot 19 \cdot 1631.$