Решение сравнений

Сравнение с одним неизвестным x имеет вид

$$a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \equiv 0 \pmod{m}, \qquad (2.1)$$

где $m \in \mathbb{N}$, $m > 1$. Если a_n не делится на m, то n называется *степенью* сравнения (2.1).

Решением сравнения (2.1) называется всякое целое число x_0, для которого $a_n x_0^n + a_{n-1}x_0^{n-1} + \ldots + a_0 \equiv 0 \pmod{m}$. Если x_0 удовлетворяет сравнению (2.1), то, согласно свойству 9 сравнений, этому сравнению будут удовлетворять все целые числа, сравнимые с x_0 по модулю m. Поэтому все решения сравнения (2.1), принадлежащие одному классу вычетов по модулю m, будем рассматривать как одно решение. Таким образом, сравнение (2.1) имеет столько решений, сколько элементов полной системы вычетов ему удовлетворяет.

Сравнения, множества решений которых совпадают, называются *равносильными*.

2.2.1. Сравнения первой степени

Сравнение первой степени с одним неизвестным x имеет вид

$$ax \equiv b \pmod{m}. \qquad (2.2)$$

Теорема 2.4. Для того чтобы сравнение (2.2) имело хотя бы одно решение, необходимо и достаточно, чтобы число b делилось на НОД(a, m).

Пример 2.10. Сравнение $9x \equiv 6 \pmod{12}$ имеет решение, так как НОД(9, 12) = 3 и 6 делится на 3. □

Пример 2.11. Сравнение $6x \equiv 9 \pmod{12}$ не имеет решений, так как НОД(6, 12) = 6, а 9 не делится на 6. □

Теорема 2.5. Пусть сравнение (2.2) разрешимо и $d = \text{НОД}(a, m)$. Тогда множество решений сравнения (2.2) состоит из d классов вычетов по модулю m, а именно, если x_0 — одно из решений, то все другие решения — это $x_0 + m_1, x_0 + 2m_1, \ldots, x_0 + (d-1)m_1$, где $m_1 = \dfrac{m}{d}$.

Пример 2.12. Сравнение $9x \equiv 6 \pmod{12}$ имеет ровно три решения, так как НОД(9, 12) = 3. Эти решения: $x_0 = 2$, $x_0 + 4 = 6$, $x_0 + 2 \cdot 4 = 10$. □

Пример 2.13. Сравнение $11x \equiv 2 \pmod{15}$ имеет единственное решение $x_0 = 7$, так как НОД(11, 15) = 1. □

Покажем, как решать сравнение первой степени. Не умаляя общности, будем считать, что НОД$(a, m) = 1$. Тогда решение сравнения (2.2) можно искать, например, по алгоритму Евклида. Действительно, используя расширенный алгоритм Евклида, представим число 1 в виде линейной комбинации чисел a и m:

$$1 = aq + mr.$$

Умножим обе части этого равенства на b, получим: $b = abq + mrb$, откуда $abq - b = -mrb$, то есть $a \cdot (bq) \equiv b \pmod{m}$ и bq — решение сравнения (2.2).

Еще один путь решения — использовать теорему Эйлера. Опять считаем, что НОД$(a, m) = 1$. Применяем теорему Эйлера: $a^{\varphi(m)} \equiv 1 \pmod{m}$. Умножим обе части сравнения на b: $a^{\varphi(m)}b \equiv b \pmod{m}$. Переписывая последнее выражение в виде $a(a^{\varphi(m)-1}b) \equiv b \pmod{m}$, получаем, что $a^{\varphi(m)-1}b$ — решение сравнения (2.2).

Пусть теперь НОД$(a, m) = d > 1$. Тогда $a = a_1d$, $m = m_1d$, где НОД$(a_1, m_1) = 1$. Кроме того, необходимо $b = b_1d$, для того чтобы сравнение было разрешимо. Если x_0 — решение сравнения $a_1x \equiv b_1 \pmod{m_1}$, причем единственное, поскольку НОД$(a_1, m_1) = 1$, то x_0 будет решением и сравнения $a_1dx \equiv b_1d \pmod{m_1d}$, то есть исходного сравнения (2.2). Остальные $d - 1$ решений находим по теореме 2.5.

Пример 2.14. Решим сравнение $12x \equiv 9 \pmod{21}$. Вычисляем НОД(12, 21) = 3. Число 9 делится на 3, поэтому сравнение разрешимо, и у него три решения. Поделим обе части сравнения и модуль на их наибольший общий делитель: $4x \equiv 3 \pmod 7$. Поскольку НОД(4, 7) = 1, можем воспользоваться теоремой Эйлера: $x_0 = 4^{\varphi(7)-1} \cdot 3 \equiv 4^5 \cdot 3 \equiv 6 \pmod 7$. Таким образом, 6 — это одно из решений сравнения $12x \equiv 9 \pmod{21}$. Находим остальные решения:

$$6+\frac{21}{3}=6+7=13, \quad 6+2\cdot\frac{21}{3}=6+14=20.$$

Проверка: $12\cdot 6-9=63=21\cdot 3$; $12\cdot 13-9=147=21\cdot 7$; $12\cdot 20-$ $-9=231=21\cdot 11$. □

Замечание. Следует особо отметить сравнение первой степени вида $ax \equiv 1 \pmod m$. Оно разрешимо тогда и только тогда, когда НОД$(a, m) = 1$, и при условии разрешимости имеет единственное решение. Это решение x_0 обозначается a^{-1} и называется *мультипликативно обратным* к числу a по модулю m. Таким образом, число a^{-1}, мультипликативно обратное к a по модулю m, — это такое число, при умножении которого на a получается единица по модулю m.

Пример 2.15. Найдем число, мультипликативно обратное к 26 по модулю 49. Числа 26 и 49 взаимно просты, значит, искомое число существует. Реализуем расширенный алгоритм Евклида для чисел 26 и 49, промежуточные результаты занесем в таблицу:

i	r_i	x_i	y_i	q_i
1	49	1	0	
2	26	0	1	1
3	23	1	−1	1
4	3	−1	2	7

i	r_i	x_i	y_i	q_i
5	2	8	-15	1
6	1	-9	17	

Таким образом, $49 \cdot (-9) + 26 \cdot 17 = 1$. Приводим обе части этого равенства по модулю 49: $26 \cdot 17 \equiv 1 \pmod{49}$. Таким образом, число 17 является мультипликативно обратным к числу 26 по модулю 49, то есть $26^{-1} \equiv 17 \pmod{49}$. Точно так же число 26 является мультипликативно обратным к числу 17 по модулю 49, то есть $17^{-1} \equiv 26 \pmod{49}$. □

Отметим, что если число p простое, то сравнение $ax \equiv 1 \pmod{p}$ разрешимо для любого числа a, не делящегося на p, то есть для любого такого a существует мультипликативно обратное по модулю p. Значит, кольцо классов вычетов $\mathbb{Z}/p\mathbb{Z}$ является полем. Это поле часто обозначают $\mathbb{F}_p$ и называют *конечным полем из p элементов* (см. главу 7).

2.2.2. Китайская теорема об остатках

Рассмотрим систему сравнений первой степени:

$$x \equiv a_1 \pmod{m_1},\ x \equiv a_2 \pmod{m_2},\ \ldots,\ x \equiv a_r \pmod{m_r}, \tag{2.3}$$

где числа $m_1, m_2, \ldots, m_r$ попарно взаимно простые, и найдем значение $x_0 \in \mathbb{Z}$, удовлетворяющее всем r сравнениям.

Теорема 2.6 (китайская теорема об остатках). Пусть числа $m_1, m_2, \ldots, m_r$ попарно взаимно простые и числа $a_1, a_2, \ldots, a_r$ произвольные целые. Тогда существует такое целое число x_0, что $0 \le x_0 < m_1 m_2 \ldots m_r$ и $x_0 \equiv a_1 \pmod{m_1}$, $x_0 \equiv a_2 \pmod{m_2}$, $\ldots$, $x_0 \equiv a_r \pmod{m_r}$.

З а м е ч а н и е. Приведем выражение (2.4) к симметричному виду. Для этого сначала покажем, что $m_1^{\varphi(m_2)}+m_2^{\varphi(m_1)}\equiv 1\,(\mathrm{mod}\, m_1m_2)$. Действительно, так как числа m_1, m_2 взаимно просты, можем применить к ним теорему Эйлера: $m_1^{\varphi(m_2)}\equiv 1\,(\mathrm{mod}\, m_2)$, то есть разность $m_1^{\varphi(m_2)}-1$ делится на m_2. Но точно так же $m_2^{\varphi(m_1)}\equiv 1\,(\mathrm{mod}\, m_1)$, то есть разность $m_2^{\varphi(m_1)}-1$ делится на m_1. Тогда выражение $m_1^{\varphi(m_2)}+m_2^{\varphi(m_1)}-1$ делится на m_1m_2.

В общем случае получаем *целочисленный аналог интерполяционной формулы Лагранжа*:

$$x_0 \equiv \sum_{i=1}^{r} a_i M_i N_i \pmod{m_1 m_2 \ldots m_r}, \tag{2.5}$$

где $M_i = m_1 \ldots m_{i-1} m_{i+1} \ldots m_r$ и $N_i \equiv M_i^{-1} \pmod{m_i}$.

Пример 2.16. Решим систему сравнений $x \equiv 2 \pmod 5$, $x \equiv 3 \pmod 6$, $x \equiv 4 \pmod 7$.

Вычисляем: $M_1 = 6 \cdot 7 = 42$, $M_2 = 5 \cdot 7 = 35$, $M_3 = 5 \cdot 6 = 30$. Находим мультипликативно обратные числа:

$$N_1 \equiv 42^{-1} \equiv 2^{-1} \equiv 3 \pmod 5;$$

$$N_2 \equiv 35^{-1} \equiv 5^{-1} \equiv 5 \pmod 6;$$

$$N_3 \equiv 30^{-1} \equiv 2^{-1} \equiv 4 \pmod 7.$$

Подставляем значения в формулу (2.5):

$$x_0 \equiv 2 \cdot 42 \cdot 3 + 3 \cdot 35 \cdot 5 + 4 \cdot 30 \cdot 4 =$$

$$= 252 + 525 + 480 = 1257 \equiv 207 \pmod{210}.$$

Проверка: $207 - 2 = 205 = 5 \cdot 41$, то есть $207 \equiv 2 \pmod 5$; $207 - 3 = 204 = 6 \cdot 34$, то есть $207 \equiv 3 \pmod 6$; $207 - 4 = 203 = 7 \cdot 29$, то есть $207 \equiv 4 \pmod 7$. □

Определение 2.4. Пусть $f(x_1, x_2, \ldots, x_n)$ — полином n-й степени с целыми коэффициентами от переменных $x_1, x_2, \ldots, x_n$. Уравнение вида $f(x_1, x_2, \ldots, x_n) = 0$, которое нужно решить в целых (или рациональных) числах, называется *диофантовым.*

Следствие. Диофантово уравнение $f(x_1, x_2, \ldots, x_n) = 0$ разрешимо в целых числах тогда и только тогда, когда оно разрешимо по модулю любого простого числа.

Пример 2.17. Покажем, что уравнение $x^2 - 7y^3 = 3$ не имеет целочисленных решений, то есть не существует пары целых чисел x, y, удовлетворяющих данному уравнению.

Приведем обе части уравнения по модулю 7, получим

$$x^2 \equiv 3 \pmod 7,$$

то есть если пара целых чисел (x_0, y_0) — решение исходного уравнения, то $x_0^2 \equiv 3 \pmod 7$. Заметим, что число x_0 имеет вид $x_0 = 7q + r$, где число q целое и $r \in \{0, 1, 2, 3, 4, 5, 6\}$. Тогда

$$x_0^2 = (7q + r)^2 = 49q^2 + 14qr + r^2 \equiv r^2 \pmod 7.$$

Число r^2 при делении на 7 дает остатки 0, 1, 4, 2, 4, 1. Таким образом, ни для какого целого числа x_0 сравнение $x_0^2 \equiv 3 \pmod 7$ не выполнено, а значит, и исходное уравнение $x^2 - 7y^3 = 3$ не имеет целочисленных решений. □