ОПРЕДЕЛЕНИЕ

Два целых числа, разность которых кратна данному натуральному числу m, называются сравнимыми по модулю m.

Утверждение «a сравнимо с b по модулю m» обычно записывают в виде $a \equiv b \pmod{m}$, и называют сравнением.

Примеры сравнений:

$5 \equiv 1 \pmod{2}$,

$48 \equiv 0 \pmod{6}$,

$14 \equiv 9 \pmod{5}$.

ОПРЕДЕЛЕНИЕ

Если a и b — два целых числа и их разность $a - b$ делится на натуральное число m, то говорят, что a и b сравнимы по модулю m.

$$a \equiv b \pmod{m}$$

Делитель m мы предполагаем натуральным.

Он называется ***модулем сравнения.***

Наше высказывание означает, что

$a - b = mk$, где k — целое число.

ПРИМЕР 1

1) $23 \equiv 8 \pmod 5$, так как $23 - 8 = 15 = 5 \cdot 3$;

2) $47 \equiv 11 \pmod 9$, так как $47 - 11 = 36 = 9 \cdot 4$;

3) $-11 \equiv 5 \pmod 8$, так как $-11 - 5 = -16 = 8 \cdot (-2)$;

4) $81 \equiv 0 \pmod{27}$, так как $81 - 0 = 81 = 27 \cdot 3$.

Последний пример показывает, что вообще, вместо того, чтобы говорить: число a делится на число m, мы можем записать $a \equiv 0 \pmod m$, так как это означает, что $a - 0 = a = mk$, где k — некоторое целое число. Например, вместо того, чтобы сказать, что a — четное число, мы можем записать $a \equiv 0 \pmod 2$.

Таким же образом видно, что нечетное число является числом, удовлетворяющим сравнению $a \equiv 1 \pmod 2$.

СВОЙСТВА СРАВНЕНИЙ

1. $a \equiv b \pmod{m}, b \equiv c \pmod{m}, \Rightarrow a \equiv c \pmod{m}$
2. $a \equiv b \pmod{m} \Leftrightarrow b \equiv a \pmod{m}$
3. $a_1 \equiv b_1 \pmod{m}, a_2 \equiv b_2 \pmod{m},$
$\ldots, a_k \equiv b_k \pmod{m} \Rightarrow a_1 + \ldots + ak \equiv b_1 + \ldots b_k \pmod{m}$
4. $a + b \equiv c \pmod{m} \Rightarrow a \equiv c - b \pmod{m}$
5. $a \equiv b \pmod{m} \Rightarrow a + mt \equiv b + mk \pmod{m}$ $(t, k \in \mathbb{Z})$
6. $a \equiv b \pmod{m}, c \equiv d \pmod{m} \Rightarrow ac \equiv bd \pmod{m}$
7. $a \equiv b \pmod{m} \Rightarrow a^k \equiv b^k \pmod{m}$
8. Если $a \equiv b \pmod{m}$, $(a, b) = c$, $(c, m) = 1 \Rightarrow \dfrac{a}{(a,b)} \equiv \dfrac{b}{(a,b)} \pmod{m}$

СВОЙСТВА СРАВНЕНИЙ

9. $a \equiv b \pmod{m} \Rightarrow ak \equiv bk \pmod{mk}$

10. $a \equiv b \pmod{m}, a = a_1 d, b = b_1 d, m = m_1 d \Rightarrow a_1 \equiv b_1 \pmod{m_1}$

11. $a \equiv b \pmod{m_1}, a \equiv b \pmod{m_2}, \ldots, a \equiv b \pmod{m_k} \Rightarrow$
$a \equiv b \pmod{\text{НОК}(m_1,\ldots,m_k)}$

12. $a \equiv b \pmod{m}, \frac{d}{m} \Rightarrow a \equiv b \pmod{d}$

13. $\frac{d}{a}, \frac{d}{m}, a \equiv b \pmod{m} \Rightarrow \frac{d}{b}$

14. $a \equiv b \pmod{m} \Rightarrow (a, m) = (b, m)$

ЗАДАЧА

Задача нахождения обратного элемента: найти $b = a^{-1} \pmod{n}$, где a и n заданы, b неизвестно.

Элемент b называется обратным к a по модулю n, если $a \cdot b \equiv 1 \pmod{n}$.

Тогда пишут, что $b \equiv a^{-1} \pmod{n}$.

ТЕОРЕМА ОБРАТИМОСТИ

Существует $a^{-1} \pmod{n} \Leftrightarrow (a, n) = 1$.
То есть, обратный элемент для числа существует тогда и только тогда, когда это число взаимно простое с модулем.

АЛГОРИТМ ЕВКЛИДА

Пусть $a > n$; $a, n \in \mathbb{Z}$.

Расширенный алгоритм Евклида находит числа x, y:

$ax + ny = \text{НОД}(a, n)$.

Вычисляется цепочка равенств:

$a = nq_1 + r_1;$

$n = r_1q_2 + r_2;$

$r_1 = r_2q_3 + r_3;$

…

$r_{k-2} = r_{k-1}q_k + r_k;$

$r_{k-1} = r_kq_k + 1.$

Используя эту цепочку, восстанавливаем:

$r_k = r_{k-2} - r_{k-1}q_k = r_{k-2} - (r_{k-3} - r_{k-2}q_{k-1})q_k = \ldots = ax + ny.$

Получаем сравнение $ax + ny \equiv 1 \pmod{n}$.

Поскольку $ny \equiv 0 \pmod{n}$, то $ax \equiv 1 \pmod{n}$,
а значит полученное с помощью расширенного алгоритма Евклида число x как раз и есть искомый обратный элемент к числу a по модулю n.

ПРИМЕР 2

Вычислить элемент,
обратный a по mod n, если $a = 9$; $n = 29$;

Решение:

Воспользуемся расширенным алгоритмом Евклида:

$29 = 9 \cdot 3 + 2$; $9 = 2 \cdot 4 + 1$; $2 = 1 \cdot 2 + 0$

Обратный ход:

$1 = 9 - 2 \cdot 4 = 9 \cdot 1 - (29 - 9 \cdot 3) \cdot 4 = 9 \cdot 13 - 29 \cdot 4.$

Проверка:

$13 \cdot 9 = 117$; $117 \equiv 1 \pmod{29}$.

Ответ: обратный элемент = 13.

$a_1 x + a_0 \equiv 0 \pmod{m}$ — сравнение первой степени

$ax \equiv b \pmod{m}$

Два случая: $(a, m) = 1$ и $(a, m) = d > 1$

Теорема 1: если $(a, m) = 1$, то

сравнение имеет единственное решение.

Теорема 2: если $(a, m) = d > 1$ и число b не делится на d, то

сравнение $ax \equiv b \pmod{m}$ не имеет решений.

Теорема 3: если $(a, m) = d > 1$ и $b \equiv d$, то

сравнение $ax \equiv b \pmod{m}$ имеет d решений.

ЗАДАЧА

Решить сравнение $25\ x \equiv 15 \pmod{17}$

1 способ:

НОД (25, 17) = 1

Значит, сравнение имеет единственное решение.

$25x \equiv 15 \pmod{17}$

$5x \equiv 3 \pmod{17}$

$5x \equiv 3 + 17 \pmod{17}$

$5x \equiv 20 \pmod{17}$

$x \equiv 4 \pmod{17}$

ЗАДАЧА

Решить сравнение $25\ x \equiv 15 \pmod{17}$

2 способ:

НОД (25, 17) = 1

Значит, сравнение имеет единственное решение.

$25x \equiv 15 \pmod{17}$

$5x \equiv 3 \pmod{17}$

Найдем обратный элемент к 5, используя алгоритм Евклида:

$17 = 5 \equiv 3 + 2$

$5 = 2 \cdot 2 + 1$

$2 = 2 \cdot 1 + 0$

$1 = 5 - 2 \cdot 2 = 5 - 2 \cdot (17 - 5 \cdot 3) = 5 \cdot 7 - 17 \cdot 2$

таким образом, обратным для 5 по модулю 17 будет 7.

$5x \equiv 3 \pmod{17}$

$7 \cdot 5x \equiv 7 \cdot 3 \pmod{17}$

$x \equiv 21 \equiv 4 \pmod{17}$

1. $325x \equiv 56(\mod 8)$

Ответ: _____

2. $625x \equiv 15(\mod 7)$

Ответ: _____

3. $646x \equiv 18(\mod 16)$

Ответ: _____

4. $646x \equiv 18(\mod 16)$

Ответ: _____

5. $428x \equiv 14(\mod 2)$

Ответ: _____

Теорема (китайская теорема об остатках). Для натуральных чисел m_1 и m_2 таких что $\text{НОД}(m_1, m_2) = 1$ система сравнений

$$\begin{cases} x \equiv a \pmod{m_1} \\ x \equiv b \pmod{m_2} \end{cases}$$

разрешима и имеет единственное решение по модулю (m_1, m_2).

Доказательство. По условию $\text{НОД}(m_1, m_2) = 1$. Значит, существует линейное представление с целыми u и v такими, что $m_1 \cdot u + m_2 \cdot v = 1$. Рассмотрим $x = b \cdot m_1 \cdot u + a \cdot m_2 \cdot v$. Легко увидеть, что $x \equiv a \pmod{m_1}$ и $x \equiv b \pmod{m_2}$. Таким образом, решение системы существует. Пусть найдется другое решение $x = x_0$ этой системы: $x_0 \equiv a \pmod{m_1}$ и $x_0 \equiv b \pmod{m_2}$.

Тогда $x - x_0 \equiv 0 \pmod{m_1}$ и $x - x_0 \equiv 0 \pmod{m_2}$, следовательно, $m_1 \mid (x - x_0)$, $m_2 \mid (x - x_0)$. При условии $\text{НОД}(m_1, m_2) = 1$, $m_1 \cdot m_2 \mid (x - x_0)$, значит, $x_0 \equiv x \pmod{m_1 \cdot m_2}$. ■

Теорема. В условиях теоремы, решением системы является $x \equiv b \cdot m_1 \cdot u + a \cdot m_2 \cdot v \pmod{m_1 \cdot m_2}$, где $m_1 \cdot u + m_2 \cdot v = 1$ - линейное представление $\text{НОД}(m_1, m_2) = 1$.

Пример 5. Решить систему сравнений $\begin{cases} x \equiv 2 \pmod 5 \\ x \equiv 8 \pmod{11} \end{cases}$ любым способом.

Решение. Из первого сравнения системы получаем, что $x = 2 + 5t$, где $t \in \square$.

Подставим во второе сравнение системы $2 + 5t \equiv 8 \pmod{11}$. Решим его: $5t \equiv 6 \pmod{11} \equiv -5 \pmod{11}$, $t \equiv 10 \pmod{11}$ или $t = 10 + 11k$, тогда $x = 2 + 5(10 + 11k) = 52 + 55k$.

Ответ: $x \equiv 52 \pmod{55}$.

Пример 6. Решить систему сравнений:

а) $\begin{cases} x \equiv 2 \pmod 5 \\ x \equiv 8 \pmod{11} \end{cases}$;

б) $\begin{cases} 4x \equiv 3 \pmod 5 \\ 3x \equiv 1 \pmod{10} \end{cases}$.

Решение.

а) Рассмотрим систему $\begin{cases} x \equiv 2(\mathrm{mod}5) \\ x \equiv 8(\mathrm{mod}11) \end{cases}$.

Модули обладают свойством НОД (5, 11) = 1, то решить систему можно по следствия китайской теоремы об остатках. Для этого найдем линейное представление НОД (5, 11):

$1 = 5 \cdot (-2) + 11 \cdot 1.$

Тогда по известным формулам имеем

$x = 2 \cdot (11 \cdot 1) + 8 \cdot (5 \cdot (-2))$, или

$x = 22 - 80 = -58;$

$x \equiv -58(\mathrm{mod}55) \equiv 52(\mathrm{mod}55).$

б) $\begin{cases} 4x \equiv 3 (\mathrm{mod}\, 5) \\ 3x \equiv 1 (\mathrm{mod}\, 10) \end{cases}$.

Решим независимо каждое сравнение любым способом:

$$\begin{cases} x \equiv 12 (\mathrm{mod}\, 15) \\ x \equiv 7 (\mathrm{mod}\, 10) \end{cases}$$

Так как модули не взаимно простые, то решение находим по модулю НОК[10, 15] = 30. Из первого сравнения получаем: $x = 12 + 15k$, подставим во второе сравнение системы

$12 + 15k \equiv 7 (\mathrm{mod}\, 10)$; упростим

$15k \equiv -5 (\mathrm{mod}\, 10)$; $3k \equiv -1 (\mathrm{mod}\, 2)$; $k \equiv 1 (\mathrm{mod}\, 2)$, тогда $k = 1 + 2n$, где n - целое число; подставим k в формулу для x:

$$x = 12 + 15(1 + 2n) = 27 + 30n \equiv 27 (\mathrm{mod}\, 30).$$

Ответ: а) $x \equiv 52 (\mathrm{mod}\, 55)$; $x \equiv 27 (\mathrm{mod}\, 30)$.