Модульная арифметика

Определение.

X $\overset{\equiv}{\mathbf{m}}$ **Y** или «**X** сравнимо с **Y** по модулю **m**», если (**X – Y**) ⋮ **m.**

Утверждение.

Если **X** $\overset{\equiv}{\mathbf{m}}$ **Y**,то тогда **X** mod **m = Y** mod **m**

Доказательство:

(X – Y) ⋮ m, следовательно **X – Y = km,** следовательно **X = Y + km**.

Делим **Y** с остатком на **m**: **Y = qm + r**

Тогда **X = qm + r + km = (q + k)m + r,** и, так как 0 ≤ **r** < **m,** то **r = X** mod **m**, а это значит, что **X** mod **m = Y** mod **m**, что и требовалось доказать.

Свойства:

1) *Рефлективность*. **X** $\overset{\equiv}{\mathbf{m}}$ **X** Доказательство: **X – X = 0 ⋮ m**.
2) *Симметричность*. Если **X** $\overset{\equiv}{\mathbf{m}}$ **Y**, то и **Y** $\overset{\equiv}{\mathbf{m}}$ **X** .
   Доказательство: **X – Y ⋮ m**, **X – Y = -(Y – X)**, тогда **–(Y – X) ⋮ m**, а это означает, что **Y-X ⋮ m**, т.е. **Y** $\overset{\equiv}{\mathbf{m}}$ **X**.
3) *Транзитивность.* Если **X** $\overset{\equiv}{\mathbf{m}}$ **Y** и **Y** $\overset{\equiv}{\mathbf{m}}$ **Z**, то тогда **X** $\overset{\equiv}{\mathbf{m}}$ **Z**.
   Доказательство:
   $\begin{cases} \mathbf{X - Y \ \vdots \ m} \\ \mathbf{Y - Z \ \vdots \ m} \end{cases}$ тогда **X – Z = (X – Y) + (Y – Z)**, следовательно, $\mathbf{X - Z \ \vdots \ m}$
4) *Сравнимость с нулём.* Если **X** $\overset{\equiv}{\mathbf{m}}$ 0, то **X ⋮ m**.
   Доказательство: **X – 0 ⋮ m**, следовательно **X ⋮ m**.

Пример:

3 $\overset{\equiv}{\mathbf{4}}$ 15

3 $\overset{\equiv}{\mathbf{4}}$ 3, 7, 11, 15, 19 …

Утверждение. Всё множество ℤ разбивается на **m** «классов эквивалентности».

«Класс эквивалентности» - множество **A :** ∀ **X, Y** ∈ **A** **X** $\overset{\equiv}{\mathbf{m}}$ **Y**

При этом, если **A** и **B** – два разных класса эквивалентности, то ∀ **X** ∈ **A,** ∀ **Y** ∈ **B** **X** $\overset{\neq}{\mathbf{m}}$ **Y**.

Доказательство:

Рассмотрим остатки по модулю **m**:

X mod **m** = 0, 1, … , **m** – 1

$\mathbf{A_0}$ = { **X** $\overset{\equiv}{\mathbf{m}}$ 0 | **X** ∈ ℤ }

$\mathbf{A_1}$ = { **X** $\overset{\equiv}{\mathbf{m}}$ 1 | **X** ∈ ℤ }

…

$\mathbf{A_{m-1}}$ = { **X** $\overset{\equiv}{\mathbf{m}}$ **m - 1** | **X** ∈ ℤ }

Пример mod 4:

$\mathbf{A_0} = \{ 0, 4, 8, 12 \dots \}$

$\mathbf{A_1} = \{ 1, 5, 9, 13 \dots \}$

$\mathbf{A_2} = \{ 2, 6, 10, 14 \dots \}$

$\mathbf{A_3} = \{ 3, 7, 11, 15 \dots \}$

Проверка:

1) $\forall \mathbf{X} \in \mathbb{Z} \quad \mathbf{X} \in \mathbf{A_0}$ или $\mathbf{A_1}$

$\mathbf{X} \in \mathbf{A_{x \bmod 4}}$

2) Если $\mathbf{A_i} \cap \mathbf{A_j}$, то $\exists \mathbf{X} : \mathbf{X} \in \mathbf{A_i} \Rightarrow \mathbf{X} \bmod \mathbf{m} = \mathbf{i}$, что является противоречием.

$\mathbf{X} \in \mathbf{A_j} \Rightarrow \mathbf{X} \bmod \mathbf{m} = \mathbf{j}$

1 и **2** пункты вместе демонстрируют, что множество $\mathbf{A_i}$ – разложение **Z**

3) $\forall \mathbf{X}, \mathbf{Y} \in \mathbf{A_i}$ надо проверить, что $\mathbf{X} \overset{\equiv}{\mathbf{m}} \mathbf{Y}$

X mod **m = i**

Y mod **m = i**

Следовательно, $\mathbf{X} \overset{\equiv}{\mathbf{m}} \mathbf{Y}$

Арифметические свойства сравнимости:

Пусть $\mathbf{a} \overset{\equiv}{\mathbf{m}} \mathbf{b}$ и $\mathbf{c} \overset{\equiv}{\mathbf{m}} \mathbf{d}$. Тогда:

1) $\mathbf{a + c} \overset{\equiv}{\mathbf{m}} \mathbf{b + d}$ Доказательство: т.к. $\mathbf{a - b} \vdots \mathbf{m}$ и $\mathbf{c - d} \vdots \mathbf{m}$, то тогда
   $\mathbf{a - b + c - d} = \big((\mathbf{a + c}) - (\mathbf{b + d})\big) \vdots \mathbf{m}$
2) $\mathbf{a – c} \overset{\equiv}{\mathbf{m}} \mathbf{b – d}$ Доказательство аналогично п.1.
3) $\mathbf{a} * \mathbf{c} \overset{\equiv}{\mathbf{m}} \mathbf{b} * \mathbf{d}$
   Доказательство:
   $\mathbf{a} * \mathbf{c} \overset{\equiv}{\mathbf{m}} \mathbf{b} * \mathbf{c}$ (т.к. $(\mathbf{a – b}) * \mathbf{c} \vdots \mathbf{m}$) и
   $\mathbf{b} * \mathbf{c} \overset{\equiv}{\mathbf{m}} \mathbf{b} * \mathbf{d}$ (т.к. $(\mathbf{c – d}) * \mathbf{b} \vdots \mathbf{m}$), следовательно $\mathbf{a} * \mathbf{c} \overset{\equiv}{\mathbf{m}} \mathbf{b} * \mathbf{d}$
4) Если $\mathbf{a} * \mathbf{c} \overset{\equiv}{\mathbf{m}} \mathbf{b} * \mathbf{d}$, то $\mathbf{a} \overset{\equiv}{\frac{\mathbf{m}}{(\mathbf{m},\mathbf{c})}} \mathbf{b}$
   Доказательство:
   $\mathbf{a} * \mathbf{c} - \mathbf{b} * \mathbf{c} \vdots \mathbf{m} \Rightarrow (\mathbf{a} - \mathbf{b}) * \mathbf{c} \vdots \mathbf{m} \Rightarrow (\mathbf{a} - \mathbf{b}) * \mathbf{c} = \mathbf{k} * \mathbf{m} \Rightarrow$
   $\Rightarrow (\mathbf{a} - \mathbf{b}) * \frac{\mathbf{c}}{(\mathbf{m}, \mathbf{c})} = \mathbf{k} * \frac{\mathbf{m}}{(\mathbf{m}, \mathbf{c})}$
   Так как $\frac{\mathbf{c}}{(\mathbf{m},\mathbf{c})}$ и $\frac{\mathbf{m}}{(\mathbf{m},\mathbf{c})}$ взаимопросты, то $\mathbf{a} - \mathbf{b} \vdots \frac{\mathbf{m}}{(\mathbf{m},\mathbf{c})} \Rightarrow \mathbf{a} \overset{\equiv}{\frac{\mathbf{m}}{(\mathbf{m},\mathbf{c})}} \mathbf{b}$

4’) Если $\mathbf{a} * \mathbf{c} \overset{\equiv}{\mathbf{m}} \mathbf{b} * \mathbf{c}$ и НОД(**m, c**) = 1 (т.е. если **m** и **c** взаимопросты), то $\mathbf{a} \overset{\equiv}{\mathbf{m}} \mathbf{b}$

4’’) Если $\mathbf{a} * \mathbf{c} \overset{\equiv}{\mathbf{m}} \mathbf{b} * \mathbf{d}$ и $\mathbf{c} \overset{\equiv}{\mathbf{m}} \mathbf{d}$, то $\mathbf{a} \overset{\equiv}{\frac{\mathbf{m}}{(\mathbf{m},\mathbf{c})}} \mathbf{b}$

Арифметические действия с классами эквивалентности

Определение. $\mathbf{A_i} \pm \mathbf{A_j}$, $\mathbf{A_i} * \mathbf{A_j}$ — класс, содержащий $\mathbf{x} \pm \mathbf{y}$, $\mathbf{x} * \mathbf{y}$, где $\mathbf{x} \in \mathbf{A_i}$, $\mathbf{y} \in \mathbf{A_j}$

Корректность определения.

Независимо от выбора **x, y** получается один класс $\mathbf{x_1} \pm \mathbf{y_1} \,\vdots\, \mathbf{x_2} \pm \mathbf{y_2}$,

$\mathbf{x_1} * \mathbf{y_1} \,\vdots\, \mathbf{x_2} * \mathbf{y_2}$ – т.е. $\mathbf{x_1} \pm \mathbf{y_1}$, $\mathbf{x_1} * \mathbf{y_1}$ и $\mathbf{x_2} \pm \mathbf{y_2}$, $\mathbf{x_2} * \mathbf{y_2}$ – один класс.

Переобозначим классы более красиво:

$\mathbf{A}_0 = 0$
$\mathbf{A}_1 = 1$
$\mathbf{A}_2 = 2$
$\mathbf{A}_3 = 3$
(для mod **4**)

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

*	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1