# Модульная арифметика

Определение.

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

Утверждение.

Если **X** $\overbar{\overbar{\overbar{m}}}$ **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** $\overbar{\overbar{\overbar{m}}}$ **X** Доказательство:  **X – X = 0** ⋮ **m**.
2. *Симметричность*. Если **X** $\overbar{\overbar{\overbar{m}}}$ **Y**,то и **Y** $\overbar{\overbar{\overbar{m}}}$ **X** .

Доказательство: **X – Y** ⋮ **m**, **X – Y = -**(**Y – X**), тогда **–(Y – X)** ⋮ **m**, а это означает,

что **Y-X** ⋮ **m**, т.е. **Y** $\overbar{\overbar{\overbar{m}}}$ **X**.

1. *Транзитивность.* Если **X** $\overbar{\overbar{\overbar{m}}}$ **Y** и **Y** $\overbar{\overbar{\overbar{m}}} $**Z**, то тогда **X** $\overbar{\overbar{\overbar{m}}}$ **Z**.

Доказательство:

$\left\{\begin{array}{c}X-Y \vdots m\\Y-Z \vdots m\end{array}\right.$ тогда **X – Z =** (**X – Y**) + (**Y** – **Z**), следовательно, **X – Z** ⋮ **m**

1. *Сравнимость с нулём.* Если **X** $\overbar{\overbar{\overbar{m}}}$ 0, то **X** ⋮ **m**.
Доказательство: **X – 0** ⋮ **m**, следовательно **X** ⋮ **m**.

Пример:

3 $\overbar{\overbar{\overbar{4}}}$ 15

3 $\overbar{\overbar{\overbar{4}}}$ 3, 7, 11, 15, 19 …

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

«Класс эквивалентности» - множество **А :** $∀$ **Х**, **Y** $\in $ **A X** $\overbar{\overbar{\overbar{m}}}$ **Y**

При этом, если **A** и **B –** два разных класса эквивалентности, то $∀$ **X** $\in $ **A,** $∀$ **Y** $\in $ **B X**$\begin{matrix}≢\\m\end{matrix}$**Y**.

Доказательство:

Рассмотрим остатки по модулю **m**:

**X** mod **m** = 0, 1, … , **m** – 1

$A\_{0} $= { **X** $\overbar{\overbar{\overbar{m}}}$ 0 **|** **X** $\in $$Z$ }

$A\_{1}$= { **X** $\overbar{\overbar{\overbar{m}}}$ 1 **|** **X** $\in $$Z$ }

**…**

$A\_{m-1}$= { **X** $\overbar{\overbar{\overbar{m}}}$ **m** - **1** **|** **X** $\in $$Z$ }

Пример mod 4:

$$A\_{0}=\{ 0, 4, 8, 12…\}$$

$$A\_{1}=\left\{ 1, 5, 9, 13…\right\}$$

$$A\_{2}=\{ 2, 6, 10, 14…\}$$

$A\_{3}=\{ 3, 7, 11, 15…\}$

Проверка:

$$1) ∀ X \in Z X \in A\_{0} или A\_{1}$$

$ X \in A\_{x mod 4} $

2) Если $A\_{i} ∩ A\_{j} $, то $∃ X :X \in A\_{i} ⇒X mod m=i $**,** что является противоречием.

$X \in A\_{j} ⇒X mod m=j $

**1**  и **2** пункты вместе демонстрируют, что множество $A\_{i}$ **–** разложение **Z**

3) $∀ X, Y \in A\_{i}$надо проверить, что **X** $\overbar{\overbar{\overbar{m}}}$ **Y**

 **X** mod **m = i**

 **Y** mod **m = i**

Следовательно, **X** $\overbar{\overbar{\overbar{m}}}$ **Y**

Арифметические свойства сравнимости:

Пусть **a** $\overbar{\overbar{\overbar{m}}}$ **b** и **с** $\overbar{\overbar{\overbar{m}}}$ **d**.Тогда:

1. **a + c** $\overbar{\overbar{\overbar{m}}}$ **b + d** Доказательство: т.к. $a-b\vdots m$ и $c- d \vdots m$, то тогда

$$a-b+c-d=\left(\left(a+c\right)-\left(b+d\right)\right) \vdots m$$

1. **a – c** $\overbar{\overbar{\overbar{m}}}$ **b – d** Доказательство аналогично п.1.
2. **a** $\*$ **c** $\overbar{\overbar{\overbar{m}}}$ **b** $\*$ **d**

Доказательство:

**a** $\*$ **c** $\overbar{\overbar{\overbar{m}}}$ **b** $\*$ **c** (т.к. (**a – b)** $\*$ **c** $\vdots $ **m**) и

**b** $\*$ **c** $\overbar{\overbar{\overbar{m}}}$ **b** $\*$ **d** (т.к. (**c – d**) $\*$ **b** $\vdots $ **m** ), следовательно **a** $\*$ **c** $\overbar{\overbar{\overbar{m}}}$ **b** $\*$ **d**

1. Если **a** $\*$ **c** $\overbar{\overbar{\overbar{m}}}$ **b** $\*$ **d**,то **a** $\overbar{\overbar{\overbar{\frac{m}{(m, c)}}}}$ **b**

Доказательство:

$$a\*c-b\*c \vdots m ⇒\left(a-b\right)\*c \vdots m ⇒\left(a-b\right)\*c=k\*m ⇒$$

$$⇒\left(a-b\right)\*\frac{c}{\left(m, c\right)}=k\*\frac{m}{(m, c)}$$

Так как$ \frac{C}{(m, c)}$и $\frac{m}{(m, c)}$взаимопросты, то $a-b\vdots \frac{m}{\left(m, c\right)} ⇒$ **a** $\overbar{\overbar{\overbar{\frac{m}{(m, c)}}}}$ **b**

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

 **a** $\overbar{\overbar{\overbar{m}}}$ **b**

 4’’) Если $a\*c \overbar{\overbar{\overbar{m}}} b\*d$ и $c \overbar{\overbar{\overbar{m}}} d$, то $a \overbar{\overbar{\overbar{\frac{m}{\left(m, c\right)}}}} b$

## Арифметические действия с классами эквивалентности

Определение. $A\_{i} \pm A\_{j} , A\_{i}\*A\_{j}$ — класс, содержащий **x** $\pm $ **y**, **x** $\*$ **y**, где $x \in A\_{i} , y\in A\_{j} $

Корректность определения.
Независимо от выбора **x, y** получается один класс $x\_{1}\pm y\_{1 }\overbar{\overbar{\overbar{m}}} x\_{2} \pm  y\_{2}$,

$x\_{1}\*y\_{1 }\overbar{\overbar{\overbar{m}}} x\_{2}\* y\_{2}$– т.е. $x\_{1}\pm y\_{1 }, x\_{1}\*y\_{1 }$и $x\_{2} \pm  y\_{2} , x\_{2}\* y\_{2}$ **–** один класс.

Переобозначим классы более красиво:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| + | 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 |

$A\_{0}$ = 0

$A\_{1}$ = 1

$A\_{2}$ = 2

$A\_{3}$ = 3

(для mod **4**)