# Модульная арифметика

Определение.

**Х**  **Y** или «**X** сравнимо с **Y** по модулю **m**», если (**X – Y**) ⋮ **m.**

Утверждение.

Если **X**  **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**  **X** Доказательство:  **X – X = 0** ⋮ **m**.
2. *Симметричность*. Если **X**  **Y**,то и **Y X** .

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

что **Y-X** ⋮ **m**, т.е. **Y X**.

1. *Транзитивность.* Если **X**  **Y** и **Y Z**, то тогда **X**  **Z**.

Доказательство:

тогда **X – Z =** (**X – Y**) + (**Y** – **Z**), следовательно, **X – Z** ⋮ **m**

1. *Сравнимость с нулём.* Если **X**  0, то **X** ⋮ **m**.  
   Доказательство: **X – 0** ⋮ **m**, следовательно **X** ⋮ **m**.

Пример:

3 15

3 3, 7, 11, 15, 19 …

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

«Класс эквивалентности» - множество **А : Х**, **Y A X** **Y**

При этом, если **A** и **B –** два разных класса эквивалентности, то **X A,**  **Y B X  Y**.

Доказательство:

Рассмотрим остатки по модулю **m**:

**X** mod **m** = 0, 1, … , **m** – 1

= { **X** 0 **|** **X**  }

= { **X** 1 **|** **X**  }

**…**

= { **X** **m** - **1** **|** **X**  }

Пример mod 4:

Проверка:

2) Если , то **,** что является противоречием.

**1**  и **2** пункты вместе демонстрируют, что множество  **–** разложение **Z**

3) надо проверить, что **X**  **Y**

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

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

Следовательно, **X**  **Y**

Арифметические свойства сравнимости:

Пусть **a**  **b** и **с**  **d**.Тогда:

1. **a + c**  **b + d** Доказательство: т.к. и , то тогда
2. **a – c**  **b – d** Доказательство аналогично п.1.
3. **a c**  **b d**

Доказательство:

**a c**  **b c** (т.к. (**a – b) c m**) и

**b c**  **b d** (т.к. (**c – d**) **b m** ), следовательно **a c**  **b d**

1. Если **a c**  **b d**,то **a**  **b**

Доказательство:

Так каки взаимопросты, то  **a**  **b**

4’) Если и НОД(**m, c**) = 1 (т.е. если **m** и **c** взаимопросты), то

**a**  **b**

4’’) Если и , то

## Арифметические действия с классами эквивалентности

Определение. — класс, содержащий **x**  **y**, **x y**, где

Корректность определения.  
Независимо от выбора **x, y** получается один класс ,

– т.е. и  **–** 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 |

= 0

= 1

= 2

= 3

(для mod **4**)