

Лекция 6

Классы вычетов



Класс чисел

*Целые числа, сравнимые с a по модулю m
($m \in \mathbb{N}$, $m > 1$) образуют класс чисел по модулю m
и он обозначается*

$$\bar{a} = \{x \in \mathbb{Z} \mid x \equiv a \pmod{m}\}$$

*Любое число класса называется **вычетом** этого
класса по модулю m*

Например

$$\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$$

$$\bar{0} = \{x \in \mathbb{Z} \mid x \equiv 0 \pmod{6}\} = \{6k \mid k \in \mathbb{Z}\};$$

$$\bar{1} = \{x \in \mathbb{Z} \mid x \equiv 1 \pmod{6}\} = \{1 + 6k \mid k \in \mathbb{Z}\}$$

Свойства классов вычетов

) $a \in \bar{a} (a \equiv a \pmod{m})$

) $\bar{a} = \bar{b} \Leftrightarrow a \equiv b \pmod{m}$

) Если два класса имеют хотя бы один общий элемент, то они совпадают

) По модулю m существует ровно m классов вычетов $\bar{0}, \bar{1}, \bar{2}, \dots, \overline{m-1}$



Полные и приведенные системы вычетов

Определение 1

Полной системой вычетов по модулю m

называется совокупность чисел, взятых по одному из каждого класса вычетов по модулю m

Пример

- $m=6$. Так как остатки при делении на 6 могут быть 0, 1, 2, 3, 4, 5, то по модулю 6 имеется шесть классов вычетов:

$$\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}$$

- 12, 7, 8, -3, 10, 17 – полная система вычетов по модулю шесть, т.к.

$$12 \in \bar{0}, 7 \in \bar{1}, 8 \in \bar{2}, -3 \in \bar{3}, 10 \in \bar{4}, 17 \in \bar{5}$$

Теорема 1 (признак полной системы вычетов)
Любая система t чисел, попарно не сравнимых по модулю t , является полной системой вычетов по модулю t

Доказательство

- По условию числа попарно не сравнимы по модулю t , т.е. взяты из разных классов
- Т.к. чисел t , то вычет каждого класса присутствует в системе
- Значит, это система – полная система вычетов по модулю t



Теорема 2

Если $(a, m) = 1$ и x пробегает полную систему вычетов по модулю m , то $ax + b$, где $b \in \mathbb{Z}$, тоже пробегает полную систему вычетов по модулю m

Определение 2

Пусть

$$m \in \mathbb{N}$$

Функцией Эйлера называется функция натурального аргумента $\varphi(m)$, которая определена как количество натуральных чисел, не превосходящих m и взаимно простых с m

Примеры

$$\varphi(2) = 1, \varphi(3) = 2, \varphi(6) = 2$$

Заметим, что в полной системе вычетов по модулю m : $1, 2, 3, 4, \dots, m$ ровно $\varphi(m)$ вычетов, взаимно простых с m (согласно определению $\varphi(m)$)

Определение 3

Приведённой системой вычетов по модулю m называется совокупность вычетов, взятых по одному из каждого класса, взаимно простого с модулем

Заметим, что если $(a, m) = 1$, то $(\bar{a}, m) = 1$

Примеры

- 1) 1, 2, 3, 4 – приведенная система вычетов по модулю 5
- 2) 1, 3, -3, -1 – приведенная система вычетов по модулю 10



Теорема 3 (признак приведённой системы вычетов)

Совокупность $\varphi(m)$ чисел, попарно не сравнимых по модулю m и взаимно простых с m , образует приведённую систему вычетов по модулю m

Доказательство

- Поскольку числа попарно не сравнимы, то они взяты из различных классов
- Т.к. они взаимно просты с модулем, то взяты из классов, взаимно простых с модулем
- Поскольку их $\varphi(m)$ штук, т.е. столько же, сколько классов вычетов взаимно простых с модулем, то вычет каждого такого класса присутствует в системе
- Значит, это приведённая система вычетов по модулю m

Теорема 4

Пусть $a \in \mathbb{Z}$, $m \in \mathbb{N}$. Если $(a, m) = 1$ и в выражении ax , переменная x пробегает приведённую систему вычетов по модулю m , то и само выражение ax пробегает приведённую систему вычетов по модулю m



Понятие кольца

Не пустое множество K называют кольцом, если на нём определены две бинарные алгебраические операции сложения и умножения, т.е. если $a, b \in K$, то $(a+b) \in K$,

$a \cdot b \in K$ и выполняются свойства:

- . $\forall a, b, c \in K \ a+b=b+a; \ (a+b)+c=a+(b+c)$*
- . $\forall a \in K$ существует относительно сложения нейтральный элемент $- 0$, т.е. $a+0=a$*
- . $\forall a \in K$ существует противоположный (симметричный) элемент $- a'$, т.е. $a+a' = 0$*
- . $\forall a, b, c \in K \ (a \cdot b) \cdot c = a \cdot (b \cdot c)$*
- . $\forall a, b, c \in K \ a \cdot (b+c) = a \cdot b + b \cdot c, \ (a+b) \cdot c = a \cdot c + b \cdot c$*

Примеры:

N – не кольцо; Z – кольцо; Q – кольцо; R – кольцо

Кольцо классов вычетов

Z_m - множество классов вычетов по модулю m

$$Z_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$$

В Z_m определим операции сложения и умножения:

$$\bar{a} + \bar{b} = \overline{a + b}$$

$$\bar{a} \cdot \bar{b} = \overline{a \cdot b}$$

Примеры

По модулю 5

- $\bar{3} + \bar{4} = \bar{2}$, т.к. $3 + 4 = 7 \in \bar{2}$ ($7 \equiv 2 \pmod{5}$)
- $\bar{2} \cdot \bar{4} = \bar{3}$, т.к. $2 \cdot 4 = 8 \in \bar{3}$

Теорема 5

Множество классов вычетов по модулю m , относительно сложения и умножения образует коммутативное кольцо с 1



Доказательство теоремы 5

1. Сложение классов ассоциативно и коммутативно

$$\overline{a} + (\overline{b} + \overline{c}) = \overline{a} + \overline{(b + c)} = \overline{a + (b + c)} = \overline{(a + b) + c} = \overline{(a + b) + c} = \overline{(a + b)} + \overline{c} = \overline{(a + b)} + \overline{c}$$

$$\overline{a} + \overline{b} = \overline{a + b} = \overline{b + a} = \overline{b} + \overline{a}$$

2. Роль нейтрального элемента выполняет класс $\overline{0}$

3. Для каждого класса \overline{a} противоположным классом

является $-\overline{a}$, т.е. класс, содержащий $-a$; $\overline{a} + (-\overline{a}) = \overline{0}$

4. Умножение коммутативно и ассоциативно

$$\overline{a} \cdot \overline{b} = \overline{ab} = \overline{ba} = \overline{b} \cdot \overline{a}$$

$$\overline{a}(\overline{bc}) = \overline{a(bc)} = \overline{a(bc)} = \overline{(ab)c} = \overline{(ab)c} = \overline{(ab)}\overline{c} = \overline{(ab)c}$$

5. Умножение и сложение связаны дистрибутивно

$$\overline{(a + b)c} = \overline{(a + b)c} = \overline{(a + b)c} = \overline{ac + bc} = \overline{ac + bc} = \overline{ac} + \overline{bc}$$

6. Роль единицы играет класс $\overline{1}$

Свойства функции Эйлера



1. Если p – простое, то $\varphi(p) = p - 1$

2. $\varphi(p^n) = p^{n-1}(p - 1)$

3. Функция Эйлера мультипликативна, т.е.

если $(a, b) = 1$ то $\varphi(ab) = \varphi(a) \cdot \varphi(b)$

Определение

Функция, определенная на множестве натуральных чисел, называется **мультипликативной**, если для любых взаимно простых натуральных чисел a и b

$$f(a \cdot b) = f(a) \cdot f(b)$$

Свойства функции Эйлера

4. Пусть $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ каноническое разложение натурального числа, тогда

$$\varphi(n) = \varphi(p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}) = \varphi(p_1^{\alpha_1}) \varphi(p_2^{\alpha_2}) \dots \varphi(p_k^{\alpha_k}) =$$

$$p_1^{\alpha_1-1} (p_1 - 1) p_2^{\alpha_2-1} (p_2 - 1) \dots p_k^{\alpha_k-1} (p_k - 1) = n \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right)$$



Теорема Эйлера

Если $m > 1$ и $(a, m) = 1$, то

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$



*Леона́рд Э́йлер (нем. *Leonhard Euler*; 15 апреля 1707, Базель, Швейцария — 7 (18) сентября 1783, Санкт-Петербург, Российская империя) — швейцарский, немецкий и российский математик и механик*



Пьер де Ферма (1601-1665) – французский математик, один из создателей аналитической геометрии, математического анализа, теории вероятностей и теории чисел. По профессии юрист, советник парламента в Тулузе

Теорема Ферма

Пусть a , p – простое.

Если $(a, p) = 1$ $a^{p-1} \equiv 1 \pmod{p}$

Следствие

Для любого целого a и простого p

$$a^p \equiv a \pmod{p}$$