

Лекция 6

Кольца и поля

- 1. Понятие кольца. Кольцо вычетов по модулю n .
- 2. Функция Эйлера. Теорема Эйлера.
- 3. Малая теорема Ферма.
- 4. Понятие поля. Конечные поля.

Литература

1. Белоусов А.И., Ткачев С.Б. Дискретная математика. М., 2002.
2. Бухштаб А.А. Теория чисел: учебное пособие. СПб., 2020.
3. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. М., 2003.

1. Понятие кольца.

Кольцо вычетов по модулю n

Определение 1

Кольцом называется алгебра $R = \langle X, +, \cdot, 0, 1 \rangle$ с двумя бинарными и двумя нульарными операциями, которая удовлетворяет аксиомам:

- (1) $\langle X, +, 0 \rangle$ – коммутативная группа;
- (2) $\langle X, \cdot, 1 \rangle$ – моноид;
- (3) $\forall x, y, z \in X$ имеет место дистрибутивность:

$$z \cdot (x + y) = z \cdot x + z \cdot y$$

$$(x + y) \cdot z = x \cdot z + y \cdot z$$

Операция $+$ называется операцией
сложения кольца;

Операция \cdot называется операцией
умножения кольца;

Элемент 0 – *нулем* кольца;

Элемент 1 – *единицей* кольца.

Группа (1) называется **аддитивной группой** кольца R ;

Моноид (2) называется **мультипликативным моноидом** кольца R ;

Аксиома (3) устанавливает дистрибутивность операции умножения относительно операции сложения.

Если операция умножения коммутативна, то кольцо называют **коммутативным**.

Аксиомы кольца (1)-(3) называются **основными тождествами кольца**.

СР

Выпишите полный список аксиом
кольца.

Пусть $x, y, z \in X$.

Теорема 1

В любом *кольце* выполняются тождества:

$$1. \mathbf{0} \cdot x = x \cdot \mathbf{0} = \mathbf{0}$$

$$2. (-x) \cdot y = -(x \cdot y) = x \cdot (-y)$$

$$3. z \cdot (x - y) = z \cdot x - z \cdot y, \quad (x - y) \cdot z = x \cdot z - y \cdot z$$

Тождества в п.1 выражают **аннулирующее свойство нуля** в кольце.

Следствие

В любом *кольце* справедливо
тождество:

$$(-1) \cdot x = x \cdot (-1) = -x$$

Ненулевые элементы x и y кольца R
называются **делителями нуля**, если
 $x \cdot y = 0$ или $y \cdot x = 0$.

Например, $\forall a \neq 0, b \neq 0$

$$\begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} \bullet \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Пример 1 $\langle \mathbf{Z}, +, \cdot, 0, 1 \rangle$

(1) $\langle \mathbf{Z}, +, 0 \rangle$ – коммутативная группа

(2) $\langle \mathbf{Z}, \cdot, 1 \rangle$ – моноид

(3) $\forall x, y, z \in \mathbf{Z}$ выполняется дистрибутивность:

$$z \cdot (x + y) = z \cdot x + z \cdot y$$

$$(x + y) \cdot z = x \cdot z + y \cdot z.$$

- коммутативность умножения:

$$\forall x, y \in \mathbf{Z} \quad x \cdot y = y \cdot x.$$

Алгебра $R = \langle \mathbf{Z}, +, \cdot, 0, 1 \rangle$ – коммутативное кольцо.

Модулярная арифметика

Пусть $x, y \in \mathbf{Z}$, $n \in \mathbf{N}$.

$$\mathbf{Z}_{[n]} = \{ [0], [1], \dots, [n - 1] \}$$

– множество классов вычетов по модулю n .

Операции на $\mathbf{Z}_{[n]}$

- *Сложение по модулю n :*

$$[a] \oplus [b] = [a + b]$$

- *Умножение по модулю n :*

$$[a] \otimes [b] = [a \cdot b]$$

Определим класс:

$$- [a] = [n - a]$$

Пример 2 $\langle \mathbf{Z}_{[n]}, \oplus, \otimes \rangle$

(1) $\langle \mathbf{Z}_{[n]}, \oplus \rangle$ – коммутативная группа

(2) $\langle \mathbf{Z}_{[n]}, \otimes \rangle$ – моноид

(3) $\forall [a], [b], [c] \in \mathbf{Z}_{[n]}$ дистрибутивность:

$$[c] \otimes ([a] \oplus [b]) = [c] \otimes [a] \oplus [c] \otimes [b]$$

$$([a] \oplus [b]) \otimes [c] = [a] \otimes [c] \oplus [b] \otimes [c]$$

- коммутативность умножения:

$$\forall a, b \in \mathbf{Z}_{[n]} \quad [a] \otimes [b] = [b] \otimes [a]$$

Алгебра $R = \langle \mathbf{Z}_{[n]}, \oplus, \otimes \rangle$ – коммутативное

кольцо.

$\langle \mathbb{Z}_{[n]}, \oplus \rangle$ – аддитивная группа вычетов по модулю n . Порядок группы равен n .

$\langle \mathbb{Z}_{[n]}, \otimes \rangle$ – мультипликативный моноид по модулю n .

Кольцо $R = \langle \mathbb{Z}_{[n]}, \oplus, \otimes \rangle$ называется **кольцом вычетов по модулю n** .

2. Функция Эйлера. Теорема Эйлера

$Z_{[n]} = \{[0], [1], \dots, [n-1]\}$ – множество классов вычетов по модулю n .

Определение 2

Функцией Эйлера называется число классов по модулю n , взаимно простых с этим модулем.

Обозначение: $\varphi(n)$

Функцией Эйлера называется число натуральных чисел, не превосходящих n , и взаимно простых с n :

$$\varphi(n) = |\{ x \in \mathbb{N}: x \leq n, \text{НОД}(x, n) = 1 \}|$$

$$\varphi(1)=1 \quad \varphi(2)=1 \quad \varphi(3)=2 \quad \varphi(4)=2 \quad \varphi(5)=4$$

$$\varphi(6)=2 \quad \varphi(8)=4$$

Свойства функции Эйлера

Пусть $a, b, p \in \mathbb{N}$

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

2. $\forall \alpha \in \mathbb{N} \quad \varphi(p^\alpha) = p^{\alpha-1}(p-1)$

3. Функция Эйлера мультипликативна:

$$\text{НОД}(a, b) = 1 \Rightarrow \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$$

4. Если $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}$ – каноническое разложение числа n , то

$$\varphi(n) = p_1^{\alpha_1-1} \cdot p_2^{\alpha_2-1} \cdot \dots \cdot p_k^{\alpha_k-1} \cdot (p_1 - 1) \cdot (p_2 - 1) \cdot \dots \cdot (p_k - 1).$$

5. При $n > 1$

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right),$$

где $p|n$ означает, что множители произведения \prod берутся при всех возможных простых делителях числа n .

6. Тождество Гаусса:

$$\sum_{d|n} \varphi(d) = n,$$

где $d|n$ означает, что суммирование производится по всем положительным делителям числа n .

Примеры:

$$\varphi(18) = \varphi(2 \cdot 9) = \varphi(2) \cdot \varphi(3^2) = 3^1(3-1) = 6$$

$$\varphi(200) = \varphi(2^3 \cdot 5^2) = 2^2(2-1) \cdot 5(5-1) = 80$$

$Z_{[n]} = \{[0], [1], \dots, [n-1]\}$ – множество классов вычетов по модулю n .

Пусть $a \in N$, $\text{НОД}(a, n) = 1$.

Рассмотрим $a, a^2, a^3 \dots$

Возьмем $a^s = a^t \pmod n$, $s > t \geq 1$.

$\text{НОД}(a, n) = 1 \Rightarrow \text{НОД}(a^t, n) = 1$ и $a^{s-t} = 1 \pmod n$.

Обозначим $k = s - t$, тогда $a^k = 1 \pmod n$, $k \geq 1$.

Вместе с тем $\forall m \in \mathbb{N}$ имеем $a^{km} = 1 \pmod n$.

Вывод: существует бесконечно много степеней числа a , принадлежащих классу $[1]$.



Леонард Эйлер
(1707 – 1783)

Теорема Эйлера

Для любого модуля n и $\forall a \geq 1$,
взаимно простого с n , выполняется
сравнение:

$$a^{\varphi(n)} = 1 \pmod{n}$$

Пример 3

В $\mathbb{Z}_{[n]}$ рассмотрим классы вычетов $[a]$, взаимно простые с n , и операцию \otimes .

$\forall [a]$ существует *обратный класс* по \otimes :

$$[a]^{-1} = [a^{\varphi(n)-1}]$$

Действительно,

$$[a] \otimes [a^{\varphi(n)-1}] = [a \cdot a^{\varphi(n)-1}] = [a^{\varphi(n)}] = [1]$$

$$[a^{\varphi(n)-1}] \otimes [a] = [a^{\varphi(n)-1} \cdot a] = [a^{\varphi(n)}] = [1]$$

В кольце вычетов по модулю n обратимыми вычетами (делителями единицы) являются вычеты, взаимно простые с модулем.

Теорема 2

Элемент a кольца $\langle \mathbf{Z}_{[n]}, \oplus, \otimes \rangle$ имеет обратный $a^{-1} \Leftrightarrow \text{НОД}(a, n) = 1$.

3. Малая теорема Ферма

Пусть модуль p – простое число.

Условие $\text{НОД}(a, p) = 1 \Leftrightarrow a$ не делится на p .

Число классов вычетов по модулю p ,
взаимно простых с p :

$$\varphi(p) = p - 1.$$



Пьер де Ферма
(1601 – 1665)

Малая теорема Ферма

(1) Если p – простое число, то $\forall a \geq 1, p \nmid a$, выполняется сравнение:

$$a^{p-1} \equiv 1 \pmod{p}$$

(2) Если p – простое число, то $\forall a \in \mathbb{N}$ выполняется сравнение:

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

СР

Доказательство Т. Ферма:

Замечание:

Т. Ферма дает только *необходимое*,
но не достаточное условие того, что
число p – простое.

$\mathbb{Z}_{[p]}$ – множество классов вычетов по модулю p .

Следствие из Т. Ферма

Если p – простое, то в кольце $\langle \mathbb{Z}_{[p]}, \oplus, \otimes \rangle$ выполняется равенство:

$$a^{-1} = a^{p-2}$$

Пример 4

$$p=5, \mathbf{Z}_{[5]} = \{[0], [1], [2], [3], [4]\}$$

$$a=2 \quad 2^{-1} = 2^{5-2} \pmod{5}$$

$$2^{-1} = 2^3 \pmod{5} = 8 \pmod{5} = 3 \pmod{5}$$

$$\text{Ответ: } 2^{-1} = 3 \text{ в } \mathbf{Z}_{[5]}$$

Вывод: теорема Ферма позволяет находить обратные элементы по операции \otimes в кольце $\mathbf{Z}_{[p]}$

Пример 5 $\langle \mathbb{Z}_{[p]}^*, \otimes \rangle$

$\mathbb{Z}_{[p]}^*$ – множество классов вычетов, взаимно простых с p .

(1) операция \otimes ассоциативна

(2) $\exists!$ нейтральный элемент – класс $[1]$

(3) $\forall a \exists!$ обратный элемент

$$a^{-1} = a^{p-2}$$

- операция \otimes коммутативна

$\langle \mathbb{Z}_{[p]}^*, \otimes \rangle$ – мультипликативная группа кольца вычетов по модулю p .

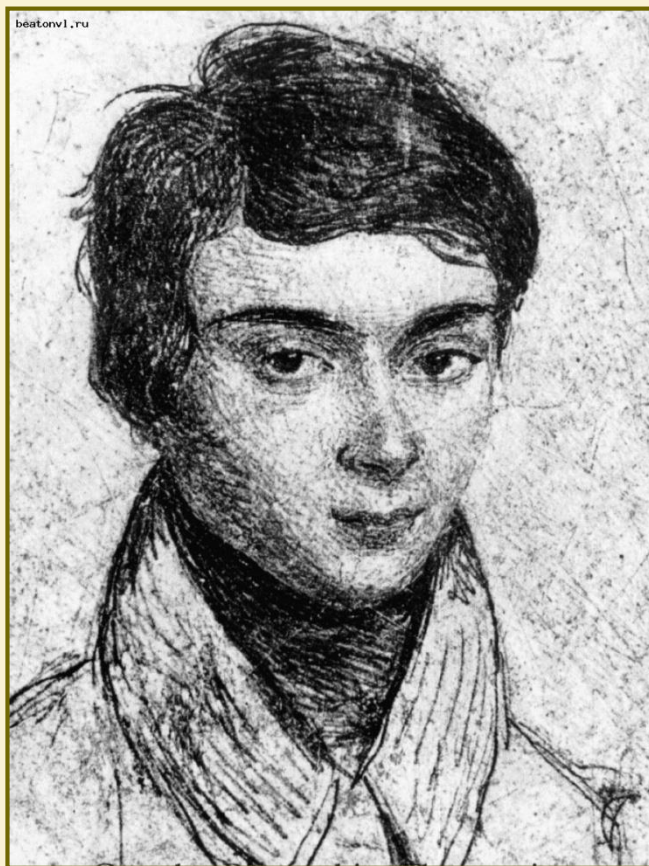
Порядок группы равен $p - 1$

4. Понятие поля. Конечные поля

Определение 2

Коммутативное кольцо, в котором для каждого *ненулевого* элемента существует обратный относительно операции умножения, называется **полем**.

Конечные поля называются **полями Галуа**.



Эварист Галуа
(1811-1832)

Теорема 3

Кольцо вычетов $\langle \mathbf{Z}_{[n]}, \oplus, \otimes \rangle$
является полем $\Leftrightarrow n$ – простое число.

CP

Аксиомы поля: