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 $R = < X, +, \cdot, \mathbf{0}, \mathbf{1} >$ с двумя бинарными и двумя нульарными операциями, которая удовлетворяет аксиомам:

(1) $< X, +, \mathbf{0} >$ – коммутативная группа;

(2) $< X, \cdot, \mathbf{1} >$ – 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 $\mathbf{0}$ – *нулем* кольца;

Элемент $\mathbf{1}$ – *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.

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

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

Ненулевые элементы x и y кольца R называются делителями нуля, если

$$x \cdot y = \mathbf{0} \text{ или } y \cdot x = \mathbf{0}.$$

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*.

Пример 2 $< \mathbf{Z}_{[n]}, \oplus, \otimes >$

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

(2) $< \mathbf{Z}_{[n]}, \otimes >$ – 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 $R = < \mathbf{Z}_{[n]}, \oplus, \otimes >$ – *коммутативное кольцо*.

$< \mathbf{Z}_{[n]}, \oplus >$ – *аддитивная группа вычетов* по модулю n. Порядок группы равен n.

$< \mathbf{Z}_{[n]}, \otimes >$ – *мультипликативный моноид* по модулю n.

Кольцо $R = < \mathbf{Z}_{[n]}, \oplus, \otimes >$ называется кольцом вычетов по модулю n.

2. Функция Эйлера. Теорема Эйлера

$\boldsymbol{Z_{[n]}} = \{[0], [1], \ldots, [n-1]\}$ – 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 :

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

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

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

Свойства функции Эйлера

Пусть $a, b, p \in \mathbf{N}$

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

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

3. Функция Эйлера мультипликативна:

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

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

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

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.

Пример:

$\varphi(18)=\varphi(2^1 \cdot 3^2)= 2^0\,(2-1)\cdot 3^1(3-1)=6$

$\mathbf{Z}_{[n]} = \{[0], [1], \ldots, [n-1]\}$ – множество классов вычетов по модулю n.

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

Рассмотрим $a, a^2, a^3 \ldots$

Возьмем $a^s = a^t (mod\ n)$, $s > t \geq 1$.

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

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

Вместе с тем $\forall m\in \boldsymbol{N}$ имеем $a^{km}=1(mod\ n)$.

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:

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

Пример 3

Во множестве $\boldsymbol{Z}_{[n]}$ 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

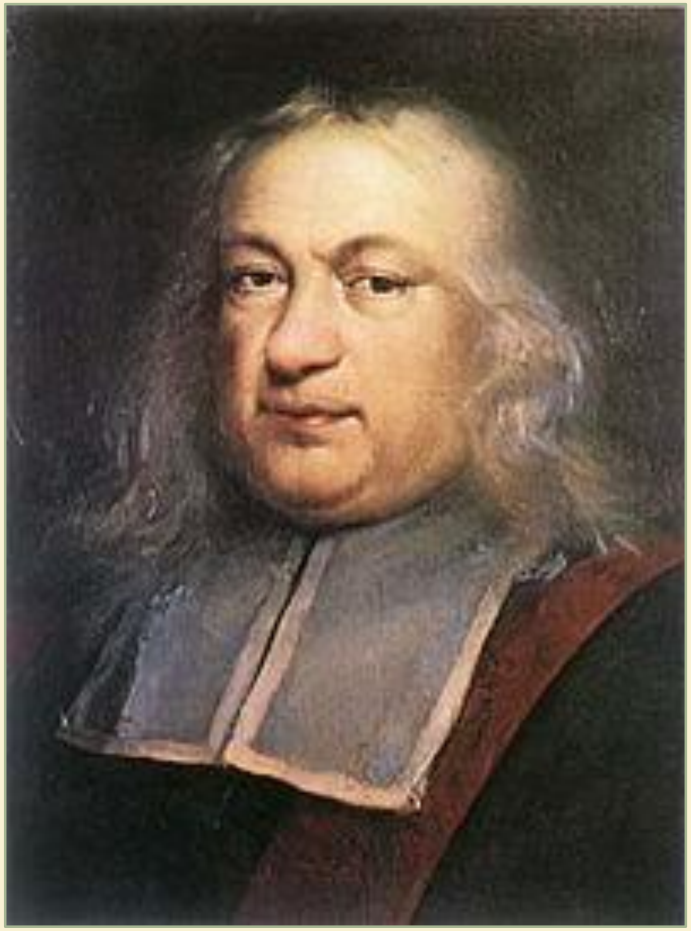
Элемент a кольца $< \mathbf{Z}_{[n]}, \oplus, \otimes >$ имеет обратный a^{-1} $\Leftrightarrow$ НОД$(a,n)=1$.

3. Малая теорема Ферма

Пусть модуль p – *простое* число.

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

Число классов, взаимно простых с p, равно $p-1$.



Пьер де Ферма

(1601 – 1665)

Малая теорема Ферма

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

$$a^{p-1} = 1\ (mod\ p)$$

Если p – *простое число*, то $\forall a \in \boldsymbol{N}$ выполняется сравнение:

$$a^{p} = a\ (mod\ p)$$

$\boldsymbol{Z_{[p]}}$ – множество классов вычетов по модулю p.

Следствие из Т. Ферма

Если p – простое, то в кольце $< \boldsymbol{Z_{[p]}}, \oplus, \otimes >$ выполняется равенство:

$$a^{-1} = a^{p-2} (mod\ p)$$

Пример 4 $< Z^*_{[p]}, \otimes >$,

где $Z^*_{[p]}$ – 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.

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

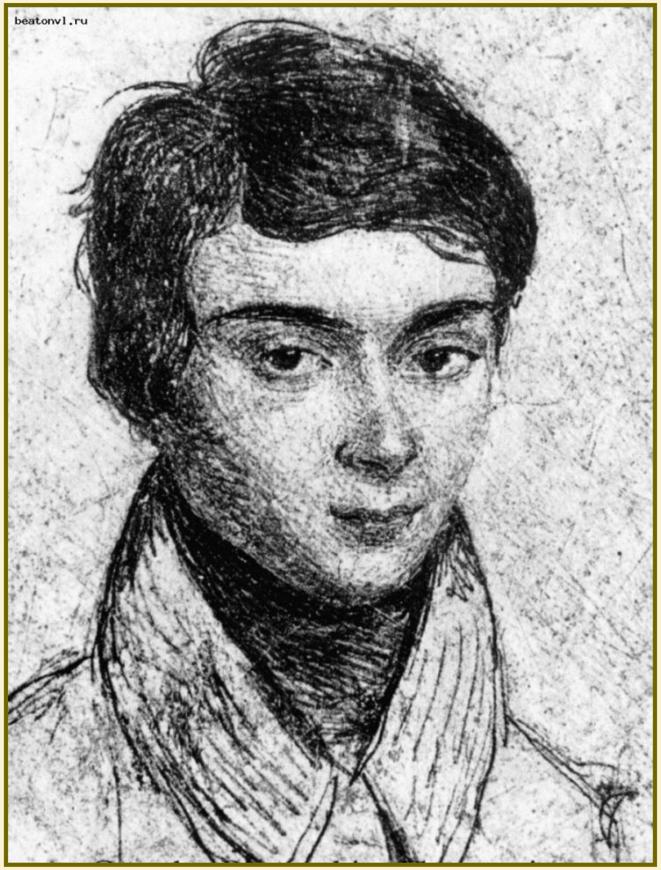
Порядок группы равен $p-1$

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 $< \boldsymbol{Z}_{[n]}, \oplus, \otimes >$ является полем $\Leftrightarrow$ n – простое число.