КОММУТАТИВНАЯ АЛГЕБРА, АСИММЕТРИЧНОЕ ШИФРОВАНИЕ И ПРЕДСТАВЛЕНИЕ ЧИСЕЛ В ВИДЕ СУММЫ ДВУХ КВАДРАТОВ

Н.В. Тимофеева, С.А. Игонин

Аннотация.

Настоящий конспект основан на миникурсе из двух лекций, прочитанных в ЯрГУ в марте 2019 года. Видео лекций доступно на странице `https://cis.uniyar.ac.ru/event/172`

Коммутативная алгебра является основой нескольких областей современной математики (включая алгебраическую геометрию и теорию чисел) и имеет приложения в информационных технологиях, включая защиту информации. Цель этих лекций – показать и мотивировать (как устроены, почему введены именно так, а не иначе) базовые понятия коммутативной алгебры и продемонстрировать некоторые приложения.

Краткое содержание лекций. Целые числа и многочлены. Кольцо вычетов по модулю натурального числа. Группа обратимых элементов кольца вычетов. Асимметричное шифрование информации с использованием колец вычетов. Деление с остатком для целых чисел и многочленов одной переменной над полем. Целые гауссовы числа и алгоритм Евклида для них. Норма гауссова числа и представление простого натурального числа вида 4n+1 в виде суммы двух квадратов.

Этот конспект покрывает не все содержание лекций, но достаточен для решения задач тестирования. Задачи и процедура тестирования описаны на странице 10.

1. Предварительные наблюдения и замечания. Предмет коммутативной алгебры

Целые числа можно складывать, вычитать и умножать. При этом указанные операции обладают хорошими свойствами (*сложение коммутативно и ассоциативно, вычитание в понятном смысле обратно к сложению, умножение коммутативно и ассоциативно, а также дистрибутивно относительно сложения*). Аналогичные факты имеют место для многочленов, скажем, от одной переменной, если коэффициенты многочленов предполагаются целыми или, например, вещественными числами.

Очень важно, что после выполнения любой операции или конечной последовательности операций (сложений, вычитаний и умножений) над целыми числами получается целое число, а при выполнении конечной последовательности аналогичных операций над многочленами с вещественными коэффициентами получается снова многочлен с вещественными коэффициентами.

Определение 1. Множество R с двумя операциями – сложением

$$+ : R \times R \to R : \quad (a, b) \mapsto a + b$$

и умножением

$$\cdot : R \times R \to R : \quad (a, b) \mapsto a \cdot b,$$

– называется (*ассоциативным*) *коммутативным кольцом*, если эти операции обладают следующими свойствами:

(1) сложение *ассоциативно*: для любых $a, b, c \in R$ выполнено равенство $(a + b) + c = a + (b + c)$;
(2) сложение *коммутативно*: для любых $a, b \in R$ выполнено равенство $a + b = b + a$;
(3) сложение *обратимо*: для любых $a, b \in R$ уравнение $a + x = b$ имеет единственное решение $x \in R$;
(4) умножение *ассоциативно*: для любых $a, b, c \in R$ выполнено равенство $(a \cdot b) \cdot c = a \cdot (b \cdot c)$;
(5) умножение *коммутативно*: для любых $a, b \in R$ выполнено равенство $a \cdot b = b \cdot a$;
(6) умножение *дистрибутивно* относительно сложения: для любых $a, b, c \in R$ выполнено равенство $(a + b) \cdot c = a \cdot c + b \cdot c$.

Нетрудно заметить, что свойства (1) – (6) аналогичны свойствам сложения и умножения целых чисел или многочленов с вещественными коэффициентами. Обратимость сложения, в частности, означает при $a = b$ существование специального элемента (*нуля*, или *нейтрального по сложению элемента*) $0 \in R$ такого, что для любого $a \in R$ выполнено $0 + a = a + 0 = a$.

Положив $b = 0$ в уравнении $a + x = b$, получим *существование противоположного элемента* $x = -a$ для каждого $a \in R$. Это означает, что $a + (-a) = (-a) + a = 0$. Решение уравнения $a + x = b$ можно интерпретировать как новую операцию *вычитания* элемента a из элемента b, обозначаемую как «$-$», $x = b - a$, и определяемую выражением $b - a = b + (-a)$.

Замечание 1. Нетрудно доказать, что наличие нуля и существование противоположных элементов для всех $a \in R$ гарантирует обратимость сложения.

Если кольцо содержит только один элемент, то он равен нулю. Такое тривиальное кольцо не интересно.

В дальнейшем предполагается, что каждое из рассматриваемых колец содержит не меньше двух элементов. Из этого следует, что в кольце есть ненулевой (не равный 0) элемент.

Многие естественно возникающие кольца обладают также *единицей*, или *нейтральным по умножению элементом* 1 таким, что для всех $a \in R$ выполнено $1 \cdot a = a \cdot 1 = a$. Кольцо, содержащее единицу, называется *кольцом с единицей,* или *унитарным кольцом.*

Пусть R – кольцо с единицей 1. Как сказано выше, мы предполагаем, что R содержит не меньше двух элементов и, следовательно, существует элемент $b \in R$, не равный 0. По свойствам единицы и нуля, имеем $1 \cdot b = b$ и $0 \cdot b = 0$. Поскольку $b \neq 0$, получаем $1 \neq 0$.

В дальнейшем предполагается, что каждое из рассматриваемых колец содержит единицу.

Замечание 2. Существуют более широкие классы колец; например, если не требовать коммутативности умножения, но добавить требование дистрибутивности относительно суммы во втором сомножителе, то получим ассоциативное, но (возможно) некоммутативное кольцо. Такое кольцо составляют, например, квадратные матрицы фиксированного размера, большего 1, с вещественными элементами.

Упражнение 1. Будут ли коммутативными кольцами

- множество многочленов одной переменной с рациональными коэффициентами,
- множество многочленов одной переменной с натуральными (т.е. целыми положительными) коэффициентами,
- множество многочленов двух переменных с целыми коэффициентами?

Коммутативная алгебра – это теория коммутативных колец и других математических объектов, связанных с коммутативными кольцами.

Приложения коммутативной алгебры широки и разнообразны. Результаты коммутативной алгебры используются в теории чисел, алгебраической геометрии, дифференциальной геометрии, теориях дифференциальных уравнений и интегрируемых систем, математической физике, криптографии и многих других областях.

Зачем изучать коммутативную алгебру? – Чтобы

знать	**уметь**
закономерности строения и поведения математических структур и объектов	применять результаты в различных разделах математики и физики, а также для обработки и защиты информации
(фундаментальный аспект)	**(прикладной аспект)**

Модельными примерами для коммутативной алгебры служат числовые кольца, кольца многочленов одной или нескольких переменных, а также кольца, получаемые из них с помощью различных конструкций.

Для нас основными примерами будут кольцо целых чисел $\mathbb{Z}$ и так называемые *кольца вычетов*, связанные с ним. Также мы рассмотрим кольцо *целых гауссовых чисел*, состоящее из комплексных чисел вида $x + yi$, где $x, y \in \mathbb{Z}$ и $i^2 = -1$.

В настоящем конспекте некоторые факты даны без доказательств, но почти все доказательства легко найти в стандартных учебниках алгебры и теории чисел.

2. Кольца вычетов и обратимые элементы в них

Выберем произвольным образом и зафиксируем натуральное число $n > 1$. Тогда для каждого целого числа m однозначно определено представление

$$m = nq + r, \qquad q, r \in \mathbb{Z}, \qquad 0 \leq r \leq n - 1. \tag{1}$$

Процедура, ставящая в соответствие целому числу m такое представление, называется *делением с остатком* числа m на n. Число r называется *остатком* от деления m на n.

Определение 2. Целые числа a и b *сравнимы по модулю* n (обозначение: $a \equiv b \mod n$), если a и b дают равные остатки при делении на n.

Напомним, что ненулевое целое число d является *делителем* целого числа m, если существует $k \in \mathbb{Z}$ такое, что $m = dk$. Заметим, что $a \equiv b \mod n$ тогда и только тогда, когда n является делителем числа $a - b$.

Предложение 1. *Отношение сравнимости по модулю n разбивает все множество целых чисел на n непересекающихся классов, каждый из которых состоит из всех чисел, имеющих остаток, равный r; $r = 0, 1, \ldots, n-1$.*

Определение 3. Классы, указанные в предложении 1, называются *классами вычетов по модулю n.*

Класс вычетов целого числа m по модулю n обозначается $m \bmod n$ или $(m \bmod n)$. То есть, $(m \bmod n)$ – это класс чисел вида $m + nk$ для всех целых k. Другими словами, подмножество $(m \bmod n) \subset \mathbb{Z}$ состоит из чисел вида $m + nk$ для всех целых k.

Предложение 1 можно переформулировать так. Для любого $m \in \mathbb{Z}$ существует единственное число $r \in \{0, 1, \ldots, n-1\}$ такое, что $(m \bmod n) = (r \bmod n)$. Для целых m и $\tilde{m}$ имеем $(m \bmod n) = (\tilde{m} \bmod n)$ тогда и только тогда, когда $m \equiv \tilde{m} \mod n$.

Классы вычетов по модулю n можно складывать и умножать друг на друга в следующем смысле. Возьмем, например, два числа $m_1 = nq_1 + r_1$ и $m_2 = nq_2 + r_2$, представленные в виде (1). Сложение даст $m_1 + m_2 = n(q_1 + q_2) + (r_1 + r_2)$. Выполнив деление с остатком суммы $r_1 + r_2 = nq' + r'$, получим соответствие $(r_1, r_2) \mapsto r'$. Поскольку оно определяется делением с остатком суммы остатков $r_1 + r_2$ на n, его вычисление не зависит от выбора конкретных представителей $m_1 = nq_1 + r_1$ и $m_2 = nq_2 + r_2$ из соответствующих классов вычетов. Таким образом, определено сложение классов вычетов по модулю n. Аналогичным образом можно определить операцию умножения.

Заметим, что эти операции на классах вычетов по модулю n можно определить так

$$(m_1 \mod n) + (m_2 \mod n) = (m_1 + m_2 \mod n),$$
$$(m_1 \mod n) \cdot (m_2 \mod n) = (m_1 m_2 \mod n).$$

Легко убедиться, что это определение корректно.

Предложение 2. *Классы вычетов по модулю натурального числа $n > 1$ с указанными операциями сложения и умножения составляют кольцо. Нулем и единицей в этом кольце являются классы* $(0 \bmod n)$ *и* $(1 \bmod n)$ *соответственно.*

Определение 4. Кольцо, образованное классами вычетов по модулю n, называется *кольцом классов вычетов по модулю n* и обозначается $\mathbb{Z}_n$.

Замечание 3. Полезно обратить внимание на то, что, например, в кольце $\mathbb{Z}_6$ есть пара ненулевых элементов, при умножении дающих 0:

$$(2 \mod 6) \cdot (3 \mod 6) = (6 \mod 6) = (0 \mod 6).$$

Определение 5. Пусть R – коммутативное кольцо. Элемент $a \in R$ называется *делителем нуля*, если существует ненулевой элемент $b \in R$ такой, что $ab = 0$.

Нуль 0 называют *тривиальным делителем нуля*, а остальные делители нуля – *нетривиальными.*

Нетрудно заметить, что множества рациональных $\mathbb{Q}$ и вещественных чисел $\mathbb{R}$ также являются кольцами. Однако в алгебраической структуре этих колец есть существенное отличие от строения, например, кольца $\mathbb{Z}$. Это *возможность деления* на любой отличный от нуля элемент, или, иными словами, *обратимость ненулевых элементов*: в кольцах $\mathbb{Q}$ и $\mathbb{R}$ все ненулевые элементы обратимы (в смысле определения 6 ниже). В кольце $\mathbb{Z}$ обратимых элементов всего два: это ± 1.

Как сказано на странице 2, мы предполагаем, что каждое из рассматриваемых колец содержит не меньше двух элементов, среди которых есть единица. Из этого следует, что единица не равна нулю.

Определение 6. Элемент u коммутативного кольца R называется *обратимым*, если существует такой элемент $u' \in R$, что $uu' = 1$, где 1 – единица кольца R. Элемент u' называется *обратным* к элементу u и обозначается как u^{-1}.

Обратимость элемента u в коммутативном кольце R означает, в частности, разрешимость в нем уравнений вида $ux = a$ для любого $a \in R$. Если u обратим, то уравнение $ux = a$ имеет решение $x = u^{-1}a$.

Напомним, что два целых числа называются *взаимно простыми*, если они не имеют никаких общих делителей, кроме ± 1.

Лемма 1. *Числа $a, b \in \mathbb{Z}$ взаимно просты тогда и только тогда, когда существуют $m_1, m_2 \in \mathbb{Z}$ такие, что $m_1 a + m_2 b = 1$.*

Доказательство. Пусть $m_1 a + m_2 b = 1$. Тогда любой общий делитель d чисел a и b также является делителем числа 1, т.е. $d = \pm 1$. Следовательно, a и b взаимно просты.

Если $a, b \in \mathbb{Z}$ взаимно просты, то существование требуемых чисел $m_1, m_2 \in \mathbb{Z}$ следует из алгоритма Евклида, как показано в замечании 11 на странице 9. □

Как сказано выше, мы предполагаем $n > 1$. Возвращаясь к кольцу $\mathbb{Z}_n$, имеем

Предложение 3. *Пусть $a \in \mathbb{Z}$. Элемент $(a \bmod n)$ обратим в кольце $\mathbb{Z}_n$ тогда и только тогда, когда число a взаимно просто с n.*

Доказательство. Пусть $(a \bmod n)$ обратим в кольце $\mathbb{Z}_n$. Это значит, что существует число $\tilde{a} \in \mathbb{Z}$ такое, что

$$(a \mod n) \cdot (\tilde{a} \mod n) = (1 \mod n). \tag{2}$$

Другими словами, $(\tilde{a} \bmod n) = (a \bmod n)^{-1}$ в кольце $\mathbb{Z}_n$.

Поскольку $(a \bmod n) \cdot (\tilde{a} \bmod n) = (a\tilde{a} \bmod n)$, равенство (2) говорит, что $a\tilde{a} \equiv 1 \bmod n$. То есть, существует $k \in \mathbb{Z}$ такое, что

$$a\tilde{a} - 1 = nk. \tag{3}$$

Из (3) следует, что, если d – делитель чисел a и n, то d также является делителем числа 1, т.е. $d = \pm 1$. Таким образом, числа a и n взаимно просты.

Теперь докажем, что, если a и n взаимно просты, то элемент $(a \bmod n)$ обратим. По лемме 1, если a и n взаимно просты, то существуют $m_1, m_2 \in \mathbb{Z}$ такие, что

$$m_1 a + m_2 n = 1. \tag{4}$$

Из (4) получаем $(m_1 \bmod n) \cdot (a \bmod n) = (1 \bmod n)$, т.е. $(a \bmod n)$ обратим и $(m_1 \bmod n) = (a \bmod n)^{-1}$ в кольце $\mathbb{Z}_n$. □

Напомним, что *простое число* – это натуральное число, больше единицы, имеющее ровно два натуральных делителя: 1 и само себя.

Число 2 простое и четное. Все другие простые числа – нечетные.

Из предложения 3 получаем

Следствие 1. *Если n – простое число, то в кольце $\mathbb{Z}_n$ каждый ненулевой элемент обратим.*

Очевидно, что в коммутативном кольце нулевой элемент не является обратимым.

Определение 7. Коммутативное кольцо, в котором каждый ненулевой элемент обратим, называется *полем.* (Как сказано выше, предполагается, что кольцо содержит хотя бы один ненулевой элемент.)

Например, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$ – поля. Из следствия 1 получаем

Следствие 2. *Если n – простое число, то кольцо $\mathbb{Z}_n$ является полем.*

Замечание 4. Если $n > 1$ – не простое, то в $\mathbb{Z}_n$ имеются ненулевые элементы, не являющиеся обратимыми. Из предложения 3 следует, что каждый из них имеет вид

$$(kq \mod n), \qquad \text{где } q \text{ – делитель числа } n, \qquad 2 \le q \le n-1, \qquad k \in \mathbb{Z}, \qquad 1 \le k \le \frac{n}{q} - 1. \tag{5}$$

Упражнение 2. Докажите, что

- в коммутативном кольце любой делитель нуля не является обратимым;
- нетривиальные делители нуля в $\mathbb{Z}_n$ имеют вид (5);
- элемент кольца $\mathbb{Z}_n$ не обратим тогда и только тогда, когда он является делителем нуля;
- в кольце многочленов $\mathbb{R}[x]$ от переменной x с вещественными коэффициентами любой многочлен

  $$a_0 + a_1 x + a_2 x^2 + \ldots + a_k x^k, \qquad a_i \in \mathbb{R}, \qquad a_k \neq 0,$$

  положительной степени $k > 0$ не обратим и не является делителем нуля.

Определение 8. *Функция Эйлера $n \mapsto \varphi(n)$* определена на множестве натуральных чисел следующим образом.

- Если $n > 1$, то $\varphi(n)$ – количество натуральных чисел, меньших n и взаимно простых с n.
- Для $n = 1$ полагают $\varphi(1) = 1$.

Например, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$, $\varphi(6) = 2$. Из предложения 3 следует, что

(6) при $n > 1$ количество обратимых элементов в кольце $\mathbb{Z}_n$ равно $\varphi(n)$.

Произведение двух обратимых элементов коммутативного кольца R есть обратимый элемент. Единица $1 \in R$ является, очевидно, обратимым элементом. Обратный к обратимому элемент тоже является обратимым. Итак, множество обратимых элементов любого коммутативного кольца обладает следующими хорошими свойствами: произведение элементов этого множества снова принадлежит ему же, и множество содержит обратные ко всем своим элементам.

Определение 9. Множество G с операцией $* : G \times G \to G$: $(a, b) \mapsto a * b$ называется *группой*, если

- операция $*$ *ассоциативна*: для любых $a, b, c \in G$ выполнено равенство $a * (b * c) = (a * b) * c$,
- существует *нейтральный элемент* e, т.е. такой, что для любого $a \in G$ выполнены равенства $a * e = e * a = a$,
- все *элементы обратимы*: для каждого $a \in G$ найдется $a^{-1} \in G$ такой, что $a^{-1} * a = a * a^{-1} = e$.

При этом операция $*$ называется *групповой операцией*.

Замечание 5. Определение группы дано в так называемой *мультипликативной записи*. Часто встречаются группы, в которых роль групповой операции играет сложение, нейтральный элемент – нуль 0, а в роли обратного к $a \in G$ выступает *противоположный* элемент $-a$ такой, что $a + (-a) = 0$. В таком случае речь идет об *аддитивной записи* группы.

Если групповая операция коммутативна, то группа называется *коммутативной* или *абелевой*. Обычно таковы группы по сложению. Однако, поскольку рассматриваемые нами кольца коммутативны, обратимые элементы коммутативного кольца с операцией умножения тоже составляют абелеву группу.

Замечание 6. Пример некоммутативной группы – группа невырожденных квадратных матриц фиксированного размера $m > 1$ с вещественными элементами и операцией умножения. Нейтральным элементом в этой группе является единичная матрица размера m.

Упражнение 3. Составляет ли группу относительно сложения множество всех элементов кольца $\mathbb{Z}_4$? Множество всех элементов произвольного коммутативного кольца?

Определение 10. Группа по умножению, образованная обратимыми элементами коммутативного кольца R, называется *группой обратимых элементов* кольца R и обозначается $U(R)$. Единица 1 кольца R является нейтральным элементом группы $U(R)$.

Группу G с операцией $*$ иногда пишут как $(G, *)$. Например, для коммутативного кольца R можно рассмотреть следующие группы.

- Группа $(R, +)$, состоящая из всех элементов кольца R с операцией сложения.
- Группа $(U(R), \cdot)$, состоящая из обратимых элементов кольца R с операцией умножения.

Теперь рассмотрим некоторые черты строения групп. Пусть G – группа.

Определение 11. Если число элементов группы G конечно, то оно называется *порядком* группы G и обозначается как $|G|$. Если множество элементов группы G бесконечно, то говорят, что группа G *имеет бесконечный порядок*.

Например, порядки групп $(\mathbb{Z}_4, +)$ и $(U(\mathbb{Z}_8), \cdot)$ равны 4 (проверьте!), а группа целых чисел по сложению имеет бесконечный порядок. Из (6) получаем, что

(7) при $n > 1$ порядок группы $U(\mathbb{Z}_n)$ дается функцией Эйлера: $|U(\mathbb{Z}_n)| = \varphi(n)$.

Группы конечных порядков называют *конечными*, группы бесконечного порядка – *бесконечными*.

Определение 12. *Подгруппой* группы $(G, *)$ называется подмножество $H \subset G$, являющееся группой относительно операции $*$, т.е. обладающее свойствами:

- подмножество H содержит нейтральный элемент e;
- для любых $a, b \in H$ выполнено $a * b \in H$;
- для любого $a \in H$ его обратный a^{-1} также принадлежит подмножеству H.

Выберем элемент $g \in G$. Тогда множество всех степеней g^k, $k \in \mathbb{Z}$, этого элемента (включая $g^0 = e$) в группе G является подгруппой. Она обозначается $\langle g \rangle$ и называется *циклической подгруппой, порожденной элементом* g. В зависимости от строения группы G и выбора элемента g в ней, циклическая подгруппа $\langle g \rangle$ может оказаться как конечной, так и бесконечной.

Определение 13. *Порядком* элемента g группы G называется порядок циклической подгруппы $\langle g \rangle$, порожденной им в группе G.

Пример 1. Покажем, что порядок элемента $(4 \bmod 7)$ в группе $U(\mathbb{Z}_7)$ равен 3. Имеем

$$(4 \mod 7)^2 = (4 \mod 7) \cdot (4 \mod 7) = (16 \mod 7) = (2 \mod 7),$$
$$(4 \mod 7)^3 = (4 \mod 7)^2 \cdot (4 \mod 7) = (2 \mod 7) \cdot (4 \mod 7) = (8 \mod 7) = (1 \mod 7).$$

Следовательно, для любого $m \in \mathbb{Z}$ имеем

$$(4 \mod 7)^{3m} = \big((4 \mod 7)^3\big)^m = (1 \mod 7)^m = (1 \mod 7),$$
$$(4 \mod 7)^{3m+1} = (4 \mod 7)^{3m} \cdot (4 \mod 7) = (1 \mod 7) \cdot (4 \mod 7) = (4 \mod 7),$$
$$(4 \mod 7)^{3m+2} = (4 \mod 7)^{3m} \cdot (4 \mod 7)^2 = (1 \mod 7) \cdot (2 \mod 7) = (2 \mod 7).$$

Таким образом, циклическая подгруппа, порожденная элементом $(4 \bmod 7) \in U(\mathbb{Z}_7)$, состоит из трех элементов: $(1 \bmod 7)$, $(4 \bmod 7)$, $(2 \bmod 7)$. То есть, порядок этой циклической подгруппы равен 3.

В группе целых чисел по сложению каждый ненулевой элемент имеет бесконечный порядок.

Из определения порядка элемента группы легко вывести

Предложение 4. *Если элемент g группы G имеет конечный порядок n, то n является минимальным натуральным числом таким, что $g^n = e$, где e – нейтральный элемент группы G.*

В этом случае циклическая подгруппа $\langle g \rangle$ состоит из элементов g^i, $i = 0, 1, \ldots, n-1$. Для $a, b \in \mathbb{Z}$ имеем $g^a = g^b$ тогда и только тогда, когда $a \equiv b \mod n$.

Следующий результат очень важен и имеет многочисленные приложения.

Теорема 1. (Теорема Лагранжа) *Если G – конечная группа, то порядок любой ее подгруппы является делителем порядка группы G. В частности, порядок любого элемента группы G является делителем порядка группы G.*

Следствие 3. *Для любого элемента g конечной группы G справедливо равенство $g^{|G|} = e$.*

Применив следствие 3 к обратимым элементам колец $\mathbb{Z}_p$ и $\mathbb{Z}_n$ для простого p и произвольного натурального $n > 1$, получаем известные теоретико-числовые результаты.

Предложение 5. (Малая теорема Ферма) *Если целое a не делится на простое p, то $a^{p-1} \equiv 1 \bmod p$.*

Предложение 6. (Теорема Эйлера) *Если целое a взаимно просто с натуральным $n > 1$, то $a^{\varphi(n)} \equiv 1 \bmod n$.*

Определение 14. Группа G называется *циклической*, если в ней найдется такой элемент g, что $G = \langle g \rangle$. При этом элемент g называется *образующей* циклической группы G.

Понятно, что в конечной циклической группе $G = \langle g \rangle$ можно рассматривать подгруппы, порожденные различными степенями образующей g. Эти подгруппы могут иметь порядки, отличные от $|G|$.

Используя лемму 1, легко доказать, что элемент g^s имеет порядок, равный $|G|$ (и, тем самым, является образующей в группе G), тогда и только тогда, когда числа s и $|G|$ взаимно просты. Из этого получаем

Предложение 7. *Количество элементов, являющихся образующими в циклической группе порядка n, равно $\varphi(n)$.*

Также полезен следующий результат.

Предложение 8. *Циклическая группа порядка n содержит единственную подгруппу порядка d для каждого натурального делителя d числа n.*

Можно доказать следующее

Предложение 9. *Если p – нечетное простое число, то группа $U(\mathbb{Z}_{p^k})$ является циклической при любом $k \geq 1$.*

При исследовании групп и колец очень полезной оказывается конструкция так называемого *прямого произведения*. Пусть даны группы G и H с операциями $*_G$ и $*_H$ соответственно и нейтральными элементами e_G и e_H соответственно. В каждой группе – своя групповая операция и свой нейтральный элемент; это отражено в обозначениях.

Определение 15. *Прямым произведением* групп $(G, *_G)$ и $(H, *_H)$ называется множество

$$G \times H = \{(g, h) \mid \ g \in G, \ \ h \in H\}$$

с покомпонентно определенной операцией

$$(g, h) \star (g', h') = (g *_G g', \ h *_H h').$$

Предложение 10. *Прямое произведение групп является группой относительно операции $\star$ с нейтральным элементом (e_G, e_H).*

Понятно, что порядок прямого произведения любого конечного набора конечных групп равен произведению порядков сомножителей.

Аналогично прямому произведению групп устроена конструкция прямого произведения колец. Пусть даны кольца $(R, +_R, \cdot_R)$ и $(S, +_S, \cdot_S)$. Символами $+_R$, $\cdot_R$, $+_S$, $\cdot_S$ обозначены операции сложения и умножения в этих кольцах.

Определение 16. *Прямым произведением колец $(R, +_R, \cdot_R)$ и $(S, +_S, \cdot_S)$* называется множество

$$R \times S = \{(r, s) \mid \ r \in R, \ \ s \in S\}$$

с покомпонентно определенными операциями

$$\begin{aligned} (r, s) \boxplus (r', s') &= (r +_R r', s +_S s'), \\ (r, s) \boxdot (r', s') &= (r \cdot_R r', s \cdot_S s'). \end{aligned}$$

Предложение 11. *Прямое произведение колец $R \times S$ является кольцом относительно операций сложения $\boxplus$ и умножения $\boxdot$. Единицей кольца $R \times S$ является элемент $(1_R, 1_S)$, где 1_R – единица кольца R, 1_S – единица кольца S.*

Замечание 7. Нетрудно описать множество обратимых элементов кольца $R \times S$:

$$U(R \times S) = \{(u_R, u_S) \in R \times S \mid u_R \in U(R), \ u_S \in U(S)\}.$$

Некоторые группы, будучи заданными по-разному, обладают аналогичной структурой. Пусть $(G, *_G)$ и $(H, *_H)$ – группы.

Определение 17. Отображение $f\colon G \to H$ называется *изоморфизмом групп*, если оно биективно и сохраняет групповую операцию, т.е. $f(g *_G g') = f(g) *_H f(g')$ для любых $g, g' \in G$. Группы, между которыми существует изоморфизм, называются *изоморфными*.

Нетрудно убедиться в том, что изоморфизм $f\colon G \to H$ переводит нейтральный элемент группы G в нейтральный элемент группы H, и для любого элемента $a \in G$ имеем $f(a^{-1}) = f(a)^{-1}$.

Аналогичная ситуация может реализоваться и для колец. Пусть $(R, +_R, \cdot_R, 1_R)$ и $(S, +_S, \cdot_S, 1_S)$ – кольца.

Определение 18. Отображение $f\colon R \to S$ называется *изоморфизмом колец*, если оно биективно и сохраняет операции, т.е. для любых $r, r' \in R$

$$f(r +_R r') = f(r) +_S f(r'), \qquad f(r \cdot_R r') = f(r) \cdot_S f(r').$$

Кольца, между которыми существует изоморфизм, называются *изоморфными*.

Замечание 8. Заметим, что изоморфизм колец $f\colon R \to S$ является также изоморфизмом групп, если рассматривать R и S как группы по сложению.

Сохранение единицы $f(1_R) = 1_S$ следует из биективности отображения f и сохранения операции умножения. Кроме того, легко проверить, что для любого $a \in U(R)$ имеем $f(a) \in U(S)$.

Ограничивая отображение f на подмножество $U(R) \subset R$, получаем изоморфизм групп $f\colon U(R) \to U(S)$ с операцией умножения.

Мы будем обозначать изоморфизм символом $\cong$.

Предложение 12. *Если натуральные числа $a > 1$ и $b > 1$ взаимно просты, то имеет место изоморфизм колец $\mathbb{Z}_{ab} \cong \mathbb{Z}_a \times \mathbb{Z}_b$, задаваемый отображением*

$$(r \bmod ab) \mapsto \big((r \bmod a), (r \bmod b)\big), \qquad r = 0, 1, \ldots, ab - 1.$$

Следствие 4. *Пусть натуральное число $n > 1$ разложено в произведение попарно взаимно простых натуральных множителей $n = n_1 \cdot \ldots \cdot n_s$, где $n_i > 1$ для всех $i = 1, \ldots, s$. Тогда имеет место изоморфизм колец*

$$\mathbb{Z}_n \cong \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_s},$$

задаваемый отображением

$$(r \bmod n) \mapsto \big((r \bmod n_1), \ldots, (r \bmod n_s)\big), \qquad r = 0, 1, \ldots, n - 1.$$

Следствие 4 эквивалентно следующему утверждению.

Китайская теорема об остатках. *Если натуральные числа $n_1, \ldots, n_s > 1$ попарно взаимно просты, то для любых $r_1, \ldots, r_s \in \mathbb{Z}$ таких, что $0 \le r_i \le n_i - 1$ при всех $i = 1, \ldots, s$, найдется число $m \in \mathbb{Z}$, которое при делении на n_i дает остаток r_i для всех $i = 1, \ldots, s$.*

Более того, если найдутся два таких числа m_1 и m_2, то $m_1 \equiv m_2 \mod n$, где $n = n_1 \cdot \ldots \cdot n_s$.

Предложение 13. *В условиях следствия 4 описанный в нем изоморфизм колец поставляет изоморфизм их групп обратимых элементов*

$$U(\mathbb{Z}_n) \cong U(\mathbb{Z}_{n_1}) \times \ldots \times U(\mathbb{Z}_{n_s}). \tag{8}$$

Следствие 5. *Функция Эйлера мультипликативна в следующем смысле: если $n = n_1 \cdot \ldots \cdot n_s$, где натуральные числа $n_1, \ldots, n_s$ попарно взаимно просты, то $\varphi(n) = \varphi(n_1) \cdot \ldots \cdot \varphi(n_s)$.*

Доказательство. Поскольку $\varphi(1) = 1$, достаточно рассмотреть случай, когда $n_i > 1$ для всех $i = 1, \ldots, s$. Тогда из (7), (8) имеем

$$\varphi(n) = |U(\mathbb{Z}_n)| = |U(\mathbb{Z}_{n_1})| \cdot \ldots \cdot |U(\mathbb{Z}_{n_s})| = \varphi(n_1) \cdot \ldots \cdot \varphi(n_s).$$

□

Из определения функции Эйлера легко вывести

Предложение 14. *Для простого числа p и натурального числа k имеем $\varphi(p^k) = (p-1)p^{k-1}$.*

Если натуральное n разложено в произведение простых чисел, следствие 5 и предложение 14 позволяют вычислить значение функции Эйлера $\varphi(n)$. Например,

$$\varphi(540) = \varphi(2^2 \cdot 3^3 \cdot 5) = \varphi(2^2) \cdot \varphi(3^3) \cdot \varphi(5) = 2 \cdot 2 \cdot 3^2 \cdot 4 = 144.$$

Пример 2. Найдем две последние цифры в десятичной записи числа 23^{123}, т.е. остаток при делении 23^{123} на 100. Заметим, что числа 23 и 100 взаимно просты, и применим теорему Эйлера:

$$23^{\varphi(100)} \equiv 1 \mod 100.$$

Вычислив $\varphi(100) = \varphi(4) \cdot \varphi(25) = 40$, получаем $23^{40} \equiv 1 \bmod 100$ и, следовательно,

$$23^{123} = 23^{120} \cdot 23^3 = (23^{40})^3 \cdot 23^3 \equiv 23^3 \equiv 23^2 \cdot 23 \equiv 29 \cdot 23 \equiv 67 \mod 100,$$

т.е. искомый остаток равен 67.

3. Евклидовы кольца, алгоритм Евклида и целые гауссовы числа

Символ $\mathbb{N}$ обозначает множество натуральных чисел. Тогда $\mathbb{N} \cup 0$ – множество неотрицательных целых чисел.

Определение 19. Коммутативное кольцо R без нетривиальных делителей нуля называется *евклидовым кольцом*, если на множестве его ненулевых элементов определена функция (*норма*) $N\colon R \setminus 0 \to \mathbb{N} \cup 0$, удовлетворяющая следующему свойству:

(9) для любых $a, b \in R$, $b \neq 0$, существуют $q, r \in R$ такие, что $a = bq + r$ и либо $N(r) < N(b)$, либо $r = 0$.

Свойство (9) называют *делением элемента a на элемент b с остатком r* в евклидовом кольце R с нормой N.

Норма в кольце целых чисел $\mathbb{Z}$ задается абсолютной величиной целого числа, а в кольце $\mathbb{K}[x]$ многочленов от одной переменной x над полем $\mathbb{K}$ – степенью многочлена.

Замечание 9. Для данных элементов $a, b \in R$, $b \neq 0$, евклидова кольца R с нормой N представление

$$a = bq + r, \qquad q, r \in R, \qquad N(r) < N(b) \text{ или } r = 0, \tag{10}$$

может быть не единственным. (Пример такой ситуации обсуждается в замечании 12 ниже.)

Если $R = \mathbb{Z}$ и норма N задается абсолютной величиной целого числа, то для данных $a, b \in \mathbb{Z}$ существует единственное представление (10) с $q, r \in \mathbb{Z}$, удовлетворяющее дополнительному условию $r \geq 0$.

Заметим, что для произвольного евклидова кольца R и элемента $r \in R$ условие $r \geq 0$ не имеет смысла.

Говорят, что ненулевой элемент d кольца R является *делителем* элемента $m \in R$, если существует $q \in R$ такой, что $m = dq$.

Определение 20. *Наибольшим общим делителем* (*НОД*) элементов a, b в евклидовом кольце R называется элемент $d = \text{НОД}(a, b)$ такой, что

- d – общий делитель a и b, т.е. найдутся $s, t \in R$ такие, что $a = ds$ и $b = dt$;
- любой общий делитель d' элементов a и b является делителем элемента d.

Замечание 10. Вообще говоря, наибольший общий делитель двух элементов a, b евклидова кольца R определен *не единственным образом*: если d – наибольший общий делитель элементов a, b кольца R и u – обратимый элемент этого кольца, то ud – тоже наибольший общий делитель для a, b.

При этом все наибольшие общие делители для данных $a, b \in R$ могут быть получены умножением какого-нибудь наибольшего общего делителя на всевозможные $u \in U(R)$.

Если $R = \mathbb{Z}$, наибольший общий делитель $d \in \mathbb{Z}$ для данных чисел $a, b \in \mathbb{Z}$ можно выбрать однозначно, наложив дополнительное условие $d > 0$. (Для произвольного евклидова кольца R так сделать нельзя, поскольку для $d \in R$ условие $d > 0$ не имеет смысла.)

В евклидовых кольцах реализуется *алгоритм Евклида*, вычисляющий наибольший общий делитель двух элементов путем последовательного деления с остатком. Искомый наибольший общий делитель получается как последний ненулевой элемент в цепи последовательно получаемых остатков с убывающими нормами:

$$\begin{aligned}
a &= bq_1 + r_1, && N(r_1) < N(b),\\
b &= r_1q_2 + r_2, && N(r_2) < N(r_1),\\
r_1 &= r_2q_3 + r_3, && N(r_3) < N(r_2),\\
&\ldots\ldots\ldots && \ldots\ldots\ldots\\
r_{\ell-2} &= r_{\ell-1}q_\ell + r_\ell, && N(r_\ell) < N(r_{\ell-1}),\\
r_{\ell-1} &= r_\ell\, q_{\ell+1} + 0, && \text{НОД}(a, b) = r_\ell.
\end{aligned}$$

Рассматривая выписанные равенства снизу вверх, легко показать, что элемент $r_\ell \in R$ является делителем элементов

$$r_{\ell-1}, \quad r_{\ell-2}, \quad \ldots, \quad r_1, \quad b, \quad a,$$

и найти $m_1, m_2 \in R$ такие, что $r_\ell = m_1a + m_2b$. Из этого легко вывести, что r_ℓ является наибольшим общим делителем элементов a и b.

При применении алгоритма Евклида к данной паре элементов $a, b \in R$ мы последовательно выбираем $q_j, r_j \in R$ для $j = 1, 2, \ldots, \ell$ так, чтобы выполнялись указанные свойства. Согласно замечанию 9, вообще говоря, элементы q_j, r_j, определены не единственным образом.

Если $R = \mathbb{Z}$, числа $q_j, r_j \in \mathbb{Z}$ можно выбрать однозначно, наложив дополнительное условие $r_j \geq 0$.

Замечание 11. Пусть $R = \mathbb{Z}$ и $a, b \in \mathbb{Z}$. Как сказано выше, применяя алгоритм Евклида к $a, b \in \mathbb{Z}$, мы можем предполагать $r_j \geq 0$ для всех j и найти числа $m_1, m_2 \in \mathbb{Z}$ такие, что $r_\ell = m_1a + m_2b$.

Рассмотрим случай, когда числа $a, b \in \mathbb{Z}$ взаимно просты. Тогда $r_\ell = \text{НОД}(a, b) = 1$. Следовательно, в этом случае существуют $m_1, m_2 \in \mathbb{Z}$ такие, что $m_1a + m_2b = 1$.

Кольцо *целых гауссовых чисел* определяется как множество

$$\mathbb{Z}[i] = \{x + yi \mid \ x, y \in \mathbb{Z}, \ \ i^2 = -1\}$$

с обычными сложением и умножением для комплексных чисел. Это евклидово кольцо; норма целого гауссова числа $x + yi$ определяется выражением $N(x + yi) = x^2 + y^2$.

Пример 3. Применим алгоритм Евклида для нахождения наибольшего общего делителя целых гауссовых чисел $11 + 3i$ и $1 + 8i$.

Положим $a = 11+3i$, $b = 1+8i$. Поскольку $11+3i = (1+8i)(1-i)+2-4i$ и $N(2-4i)=20 < N(1+8i)=65$, можно взять $q_1 = 1 - i$ и $r_1 = 2 - 4i$.

Далее, поскольку $1 + 8i = (2 - 4i)(-1 + i) + (-1 + 2i)$ и $N(-1 + 2i) < N(2 - 4i)$, можно взять $q_2 = -1 + i$ и $r_2 = -1 + 2i$.

Имеем $2-4i = (-1+2i)(-2)$. Следовательно, $r_2 = -1+2i$ является наибольшим общим делителем чисел $a = 11 + 3i$ и $b = 1 + 8i$.

Заметим, что для любых $x, y \in \mathbb{Z}$ имеем $x^2 + y^2 = (x + yi)(x - yi)$. Используя эту формулу и свойства разложения на множители в кольце $\mathbb{Z}[i]$, можно доказать

Предложение 15. *Пусть p – простое натуральное число, имеющее вид $p = 4n+1$ для некоторого $n \in \mathbb{N}$. Тогда существуют $x, y \in \mathbb{N}$ такие, что $p = x^2 + y^2$.*

Замечание 12. Пусть $R = \mathbb{Z}[i]$. Покажем, что для данных чисел $a, b \in \mathbb{Z}[i]$ представление (10) может быть не единственным.

Например, для $a = 7 + 2i$ и $b = 3 - i$ существуют три различных представления типа (10)

$$7 + 2i = (3 - i)(2 + i) + i, \qquad 7 + 2i = (3 - i)(1 + i) + 3, \qquad 7 + 2i = (3 - i)(2 + 2i) + (-1 - 2i).$$

При применении алгоритма Евклида к числам $a = 7 + 2i$ и $b = 3 - i$ можно использовать любое из этих трех представлений.

Задачи для тестирования

При решении задач можно пользоваться всеми утверждениями этого конспекта, не доказывая их.

Задача 1. (1 балл) Составьте таблицы сложения и умножения в кольце $\mathbb{Z}_6$.

Задача 2. (2 балла) Покажите, что элемент $(3 \bmod 7)$ является образующей для циклической группы $U(\mathbb{Z}_7)$.

Задача 3. (2 балла) Вычислите $\varphi(15750)$, где φ – функция Эйлера.

Задача 4. (4 балла) Используя теорему Эйлера, найдите остаток от деления числа 9977^{2019} на 90.
(*Подсказка*: можно рассуждать аналогично примеру 2 со страницы 8.)

Задача 5. (6 баллов) Используя алгоритм Евклида, найдите наибольший общий делитель целых гауссовых чисел $40 + 6i$ и $1 + 23i$. Выпишите все шаги алгоритма Евклида для этих чисел.

Задача 6. (3 балла) Пусть R и S – коммутативные кольца, не содержащие нетривиальных делителей нуля. Опишите все делители нуля в кольце $R \times S$.

Задача 7. (10 баллов) Пусть a – нечетное простое число; l, m – натуральные числа, $l < m$.
Сколько в группе $U(\mathbb{Z}_{a^m})$ элементов, имеющих порядок, равный a^l?

Задача 8. (11 баллов) Пусть q – нечетное простое число. Рассмотрим число $8q$, кольцо $\mathbb{Z}_{8q}$ и группу $U(\mathbb{Z}_{8q})$.
Докажите, что группа $U(\mathbb{Z}_{8q})$ не является циклической.

Задача 9. (11 баллов) Пусть q – простое число, $q \geq 5$. Положим $\ell = \dfrac{q-1}{2}$. Пусть целые числа a, b, c таковы, что

- произведение $ab(b-1)(b^2-1)\dots(b^\ell-1)$ не делится на q,
- $a \equiv c^2 \mod q$.

Докажите, что существует четное натуральное число r такое, что $b^r \equiv a \mod q$.

Решения задач нужно записать и сдать Надежде Владимировне Тимофеевой **не позднее 12:30 11-го апреля (четверг)**. Решения должны содержать описание и обоснование рассуждений/вычислений. Ответы, приведенные без обоснований, засчитаны не будут.

При наличии ошибок или неполном решении задачи ее решение будет оценено частью общего количества баллов, соответствующего этой задаче.

Предполагается, что каждый студент будет решать задачи самостоятельно, не советуясь с другими людьми.

Вопросы по конспекту и условиям задач можно задавать Надежде Владимировне Тимофеевой <ntimofeeva@list.ru> и Сергею Александровичу Игонину <s-igonin@yandex.ru>.

Н.В. Тимофеева бывает в 7-м корпусе по средам (3-4 пары, ауд. 418) и четвергам (1-2 пары, ауд. 320). В перерывах между парами ее обычно можно найти в ауд. 334. В частности, 11 апреля с 12:20 до 12:30 Н.В. Тимофеева будет в ауд. 334.

Настоящий конспект основан на миникурсе из двух лекций, прочитанных в ЯрГУ в марте 2019 года. Видео лекций доступно на странице https://cis.uniyar.ac.ru/event/172

Авторы считают, что содержание конспекта достаточно для решения задач тестирования, но конспект покрывает не все содержание миникурса. Более полное и подробное изложение материала лекций можно найти в книге:

С.В. Фролов, А.Ш. Багаутдинова. “Высшая математика. Этюды по теории и ее приложениям.” (СПб.: ГИОРД, 2012). Тема 7 (стр. 53–66) и Тема 27 (стр. 161–170).

В этой книге описаны основные идеи многих областей математики и их приложения, в том числе асимметричное шифрование информации с использованием колец вычетов. Кольцо целых гауссовых чисел в книге обозначено как K_1 и возникает в серии мнимых решеточных колец.

Надежда Владимировна Тимофеева, Сергей Александрович Игонин
E-mail address: ntimofeeva@list.ru, s-igonin@yandex.ru