МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«УЛЬЯНОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ФАКУЛЬТЕТ МАТЕМАТИКИ, ИНФОРМАЦИОННЫХ
И АВИАЦИОННЫХ ТЕХНОЛОГИЙ
КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ТЕОРИИ УПРАВЛЕНИЯ

Рацеев С.М.

Методические указания для самостоятельной работы студентов по дисциплине «Вычислительные методы в алгебре и теории чисел»

для студентов специальностей
10.05.01 «Компьютерная безопасность» и
10.05.03 «Информационная безопасность автоматизированных систем»

Ульяновск
2019

Рацеев С.М. Методические указания для самостоятельной работы студентов по дисциплине «Вычислительные методы в алгебре и теории чисел» для студентов специальностей 10.05.01 «Компьютерная безопасность» и 10.05.03 «Информационная безопасность автоматизированных систем». – Ульяновск: УлГУ, 2019.

Методические указания рекомендованы к введению в образовательный процесс решением Ученого Совета ФМИАТ УлГУ (протокол № 2/19 от 19 марта 2019г.).

Раздел 1. Теория делимости

Тема 1. Разложение по модулю.

Основные вопросы темы:

Теорема о разложении одного целого числа по модулю другого (основная теорема делимости целых чисел). q-ичные системы счисления (представление и единственность). Отношение делимости в кольце целых чисел и его свойства. Наибольший общий делитель и его свойства. Алгоритм Евклида. Обобщенный алгоритм Евклида. Взаимно простые числа и их свойства.

Рекомендации по изучению темы:

Все вопросы изложены в параграфах 1.1, 1.2 учебного пособия [4].

Контрольные вопросы:

1. Теорема о делении с остатком. 2. q-ичные системы счисления (представление и единственность). 3. Отношение делимости в кольце целых чисел и его свойства. 4. Наибольший общий делитель и его свойства. 5. Алгоритм Евклида. Бинарный алгоритм Евклида. 6. Обобщенный алгоритм Евклида. 7. Взаимно простые числа и их свойства.

Задачи для самостоятельной работы:

1. Найти значения выражений в заданной системе счисления:

а) $(30234)_5 + (14024)_5$, б) $(465)_7 \cdot (36)_7$,

в) $(445022)_7 - (3103)_7$, г) $(200111120)_3/(110)_3$.

2. Доказать, что для любого целого n число $n^7 - n$ делится на 7.

3. Доказать, что все числа вида $2^{2^n} + 1$ оканчиваются цифрой 7, $n \geqslant 2$.

4. Доказать, что все числа вида $2^{4^n} - 5$ оканчиваются цифрой 1, $n \geqslant 1$.

5. Доказать, что все числа вида $4^n + 15n - 1$ делятся на 9, $n \geqslant 1$.

6. Вычислить НОД: а) $(198, 294, 780)$, б) $(176, 288, 394)$.

7. С помощью обобщенного алгоритма Евклида найти частные решения уравнений:

а) $48x - 17y = (48, -17)$, б) $98x + 58y = (98, 58)$, в) $50x + 19y = (50, 19)$.

Тема 2. Диофантовы уравнения первой степени.

Основные вопросы темы:

Линейные диофантовы уравнения первой степени. Критерий существования решения. Формула общего решения. Наименьшее общее кратное и его свойства. Формула для наименьшего общего кратного пары целых чисел.

Рекомендации по изучению темы:

Все вопросы изложены в параграфах 1.3, 1.4 учебного пособия [4].

Контрольные вопросы:

1. Наименьшее общее кратное и его свойства. 2. Диофантовы уравнения первой степени. Теорема о существовании решения для уравнений вида $a_1x_1 + \ldots + a_nx_n = (a_1, \ldots, a_n)$. 3. Критерий существования решения диофантова уравнения первой степени. 4. Описание всех решений уравнения вида

Задачи для самостоятельной работы:

1. Вычислить НОК: а) $[106, 168, 172]$, б) $[102, 165, 221]$.

2. Диофантовы уравнения первого порядка. Найти общее решение следующих уравнений:

а) $44x + 27y = 1$, б) $43x + 28y = 5$, г) $45x - 17y = 3$.

Тема 3. Простые числа. Факторизация.

Основные вопросы темы:

Простые числа и их свойства. Теорема Евклида. Простейшие проверки целого числа на простоту. Решето Эратосфена. Основная теорема арифметики (о разложении целых чисел в произведение простых). Каноническое разложение целого числа. Формулы для наибольшего общего делителя и для наименьшего общего кратного набора целых чисел на основе их канонических разложений. Факторизация числа n!.

Рекомендации по изучению темы:

Все вопросы изложены в параграфах 1.6, 1.7 учебного пособия [4].

Контрольные вопросы:

1. Простые числа и их свойства. 2. Простейшие проверки целого числа на простоту. Решето Эратосфена. 3. Основная теорема арифметики. Каноническое разложение целого числа. 4. Вычисление н.о.д. и н.о.к. на основе канонического разложения чисел. Нахождение всех делителей целого числа при известном каноническом разложении. 5. Целая часть числа. Каноническое разложение числа $n!$.

Задачи для самостоятельной работы:

1. Разложить на простые множители числа: 7623, 1768.

2. Найти все делители числа 180.

3. Вычислить НОД и НОК на основе факторизации: $(198, 308, 726)$, $[198, 308, 726]$.

4. С помощью решета Эратосфена выписать все простые числа от 2 до 100.

5. Выяснить, являются ли числа 2561, 2669, 2677 простыми, используя предыдущую задачу.

6. Найти каноническое представление факториала числа: 14!, 16!, 17!.

Тема 4. Цепные дроби.

Основные вопросы темы:

Конечные цепные дроби. Представление рационального числа конечной цепной дробью. Подходящие дроби, их вычисление и основные свойства. **Рекомендации по изучению темы:**

Все вопросы изложены в параграфе 1.8 учебного пособия [4].

Контрольные вопросы:

1. Конечные цепные дроби. Представление рационального числа конечной цепной дробью. 2. Подходящие дроби и их вычисление с помощью рекуррентных последовательностей $\{P_k\}_{k\geqslant -1}$ и $\{Q_k\}_{k\geqslant -1}$. 3. Свойства подходящих

дробей: разность соседних подходящих дробей, несократимость подходящих дробей. 4. Свойство монотонности последовательностей $\{P_k\}_{k\geqslant -1}$, $\{Q_k\}_{k\geqslant -1}$ и поведение четных и нечетных подходящих дробей.

Задачи для самостоятельной работы:

1. Разложить в конечную цепную дробь рациональные числа: 83/30, 76/53.

2. Найти значение конечной цепной дроби: а) $[1; 1, 1, 2, 3, 1, 2]$, б) $[1; 2, 2, 3, 2, 3]$.

3. Сократить дробь, пользуясь их разложением в цепную дробь: 1961/1537, 1376/1505.

Тема 5. Бесконечные цепные дроби.

Основные вопросы темы:

Бесконечные цепные дроби. Представление действительных чисел бесконечными цепными дробями.

Рекомендации по изучению темы:

Все вопросы изложены в параграфе 1.8 учебного пособия [4].

Контрольные вопросы:

1. Бесконечные цепные дроби. 2. Сходимость бесконечных цепных дробей. 3. Разложение действительных чисел в цепные дроби.

Задачи для самостоятельной работы:

1. Найти значение бесконечной цепной дроби:

а) $[1; 1, 4, \underbrace{\mathbf{1}, \mathbf{1}, \mathbf{2}}, 1, 1, 2, \ldots]$, б) $[4; 1, 1, \underbrace{\mathbf{2}, \mathbf{1}, \mathbf{1}}, 2, 1, 1, \ldots]$, в) $[1; 2, 1, \underbrace{\mathbf{1}, \mathbf{4}, \mathbf{1}}, 1, 4, 1, \ldots]$.

2. Разложить в бесконечную цепную дробь:

а) $\dfrac{9-\sqrt{3}}{6}$, б) $3+\sqrt{3}$, в) $\dfrac{4+\sqrt{2}}{2}$.

Тема 6. Мультипликативные функции.

Основные вопросы темы:

Мультипликативные функции и их свойства. Примеры мультипликативных функций. Леммы о мультипликативных функциях. Формулы для количества и суммы делителей целого числа. Функция Мебиуса и ее свойства. Функция Эйлера и формула для ее вычисления.

Рекомендации по изучению темы:

Все вопросы изложены в параграфе 1.9 учебного пособия [4].

Контрольные вопросы:

1. Мультипликативные функции и их свойства. Примеры мультипликативных функций. 2. Леммы о мультипликативных функциях. 3. Формула суммы и числа делителей целого числа. 4. Функция Мебиуса и ее свойства. 5. Функция Эйлера и ее вычисление.

Задачи для самостоятельной работы:

1. Найти число и сумму делителей числа, а также значение функции Эйлера: 1224, 7!.

2. Найти количество делителей чисел: 19!, 20!.

Раздел 2. Сравнения

Тема 7. Сравнения.

Основные вопросы темы:

Отношение сравнимости в кольце целых чисел и его свойства. Полная и приведенная системы вычетов и их свойства. Теорема Эйлера. Теорема Ферма (малая).

Рекомендации по изучению темы:

Все вопросы изложены в параграфах 1.10, 1.11 учебного пособия [4].

Контрольные вопросы:

1. Отношение сравнимости в кольце целых чисел и его свойства. 2. Полная система вычетов и ее свойства. 3. Приведенная система вычетов и ее свойства. 4. Теорема Эйлера. Теорема Ферма.

Задачи для самостоятельной работы:

1. Образует ли полную систему вычетов по указанному модулю совокупность чисел:

а) -253, -138, 170, 393, 965, 2000, 47, 1660, модуль 8.

б) -40, -45, 31, 26, -48, -34, модуль 6.

в) 36, 25, -23, 21, -43, -33, 31, модуль 7.

2. Образуют ли приведенную систему вычетов по модулю 12 числа:

а) -349, -193, 231, 401.

б) 385, -247, -133, -197.

3. Записать полную и приведенную системы наименьших неотрицательных и наименьших по абсолютной величине вычетов по модулям 9, 12.

4. Теорема Эйлера. Найти остаток от деления:

а) 99^{402} на 101, б) 177^{567} на 10,

в) 23^{247} на 7, г) 4298^{33} на 17,

д) 71^{167} на 24, е) $5^{50} + 7^{70}$ на 9.

5. Найти две последние цифры в десятичном представлении:

а) 2^{888}, б) 3^{2006}, в) 5^{444},

г) 11^{802} (21), д) 243^{402} (49).

Тема 8. Сравнения первой степени.

Основные вопросы темы:

Сравнения первой степени $ax \equiv b \pmod m$, случай $(a, m) = 1$. Сравнения первой степени $ax \equiv b \pmod m$, случай $(a, m) > 1$. Системы сравнений первой степени. Системы сравнений первой степени и методы их решения.

Рекомендации по изучению темы:

Все вопросы изложены в параграфах 1.12, 1.14 учебного пособия [4].

Контрольные вопросы:

1. Сравнения первой степени $ax \equiv b \pmod m$. Случай $(a, m) = 1$. 2. Сравнения первой степени $ax \equiv b \pmod m$. Случай $(a, m) > 1$. 3. Системы срав-

нений 1-й степени и методы их решения. Китайская теорема об остатках.

Задачи для самостоятельной работы:

1. Найти решения сравнений:

а) $13x \equiv 5 \pmod{18}$, б) $10x \equiv 4 \pmod{17}$, в) $15x \equiv 6 \pmod{27}$, г) $32x \equiv 8 \pmod{44}$.

2. Найти обратный элемент к:

а) 29 по модулю 45, б) 27 по модулю 46,

в) 26 по модулю 49, г)31 по модулю 48.

3. Найти решения систем сравнений:

а) $\begin{cases} x \equiv 5 \pmod{8} \\ x \equiv 1 \pmod{13} \end{cases}$

б) $\begin{cases} x \equiv 3 \pmod{6} \\ x \equiv 2 \pmod{7} \\ x \equiv 5 \pmod{11} \end{cases}$

4. Найти остаток от деления 7^{103} на 220.

5. Найти две последние цифры в десятичной системе счисления числа 23^{72}.

Литература

[1] Бухштаб А.А. Теория чисел. – СПб.: Лань, 2008. – 383 с.

[2] Глухов М.М., Елизаров В.П., Нечаев А.А. Алгебра: в 2 т. – М.: Гелиос АРВ, – 2003.

[3] Нестеренко Ю.В. Теория чисел: Учеб. для студ. высш. учеб. заведений. – М.: издательский центр «Академия», 2008. – 272 с.

[4] Рацеев С.М. Математические методы защиты информации [Электронный ресурс]: Электронное учеб. пособие. – Ульяновск: УлГУ, 2018. 1 CD-R. № гос. регистрации – 0321901084.