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 «Теоретико-числовые методы в криптографии»

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 «Теоретико-числовые методы в криптографии» 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.).

Тема 1. Системы линейных диофантовых уравнений

Основные вопросы темы:

Системы линейных диофантовых уравнений. Допустимые преобразования расширенной матрицы. Алгоритм решения систем диофантовых уравнений. Критерий существования решения. Формула общего решения. Сравнения произвольной степени по простому модулю. Сравнения по составному модулю.

Рекомендации по изучению темы:

Все вопросы изложены в параграфах 1.5, 1.15, 1.16 учебного пособия [3].

Контрольные вопросы:

1. Системы диофантовых уравнений первой степени. 2. Допустимые преобразования расширенной матрицы. 3. Алгоритм решения систем диофантовых уравнений. 4. Критерий существования решения. Формула общего решения. 5. Сравнения произвольной степени по простому модулю. 6. Сравнения по составному модулю.

Задачи для самостоятельной работы:

1. Найти общее решение уравнения $6x - 5y + 3z = 1$.

2. Найти общее решение уравнения $-10x_1 - 11x_2 + 9x_3 - 7x_4 = 19$.

3. Найти общее решение уравнения $10x_1 + 6x_2 - 8x_3 + 11x_4 = 25$.

4. Найти общее решение систем линейных диофантовых уравнений:

а) $\begin{cases} 3x_1 - 2x_2 + 4x_3 + 2x_4 = 19, \\ 5x_1 + 6x_2 - 2x_3 + 3x_4 = 23, \end{cases}$ б) $\begin{cases} 4x_1 + 3x_2 + 2x_3 + 8x_4 = 36, \\ 3x_1 - 4x_2 + 7x_3 + 5x_4 = 12 \end{cases}$

5. Найти частное решение уравнения (методом сравнений):

а) $13x_1 + 6x_2 + 18x_3 - 27x_4 = 1$, б) $9x_1 - 6x_2 + 8x_3 + 10x_4 = -11$,

в) $8x_1 - 9x_2 - 7x_3 + 5x_4 = 3$.

6. Найти решения сравнения по простому модулю:

а) $x^3 - 3x^2 - 3x - 1 \equiv 0 \pmod 5$, б) $x^4 - x^2 - 6 \equiv 0 \pmod 5$,

в) $x^3 - 4x^2 - 3x - 2 \equiv 0 \pmod 7$, г) $x^3 - 2x^2 - 6x - 10 \equiv 0 \pmod{11}$.

7. Найти все решения сравнения по составному модулю:

а) $x^3 - 4x^2 - 3x - 23 \equiv 0 \pmod{35}$, б) $x^2 + 4x + 1 \equiv 0 \pmod{15}$,

в) $x^2 + 7x + 10 \equiv 0 \pmod{33}$, г) $x^2 + 7x + 6 \equiv 0 \pmod{33}$.

Тема 2. Степенные вычеты

Основные вопросы темы:

Показатель числа. Свойства показателя. Первообразные корни по простому модулю. Первообразные корни по составному модулю. Критерий, описывающий все случаи существования первообразных корней. Индексы (дискретные логарифмы). Свойства индексов.

Рекомендации по изучению темы:

Все вопросы изложены в параграфах 1.17-1.20 учебного пособия [3].

Контрольные вопросы:

1. Степенные вычеты. Показатель числа. Свойства показателя. 2. Первообразные корни по простому модулю p. 3. Первообразные корни по модулю p^n. 4. Первообразные корни по модулю $2p^n$. 5. Критерий, описывающий все случаи существования первообразных корней.

Задачи для самостоятельной работы:

1. Найти все показатели чисел приведенной системы вычетов по модулю $m = 11$.

2. Найти показатели чисел 4, 7 и 10 по модулю 17.

3. Найти первообразные корни по модулю m: а) $m = 11$, б) $m = 13$, в) $m = 17$.

Тема 3. Сравнения второй степени

Основные вопросы темы:

Квадратичные вычеты и невычеты. Критерий Эйлера. Символ Лежандра. Свойства символа Лежандра. Критерий Гаусса. Квадратичный закон взаимности Гаусса. Символ Якоби. Свойства символа Якоби. Алгоритм эффективного вычисления символа Лежандра на основе символа Якоби. Вычисление квадратного корня. Алгоритм Тонелли-Шенкса.

Рекомендации по изучению темы:

Все вопросы изложены в параграфе 1.21 учебного пособия [3].

Контрольные вопросы:

1. Сравнения второй степени. Квадратичный вычет. Критерий Эйлера квадратичного вычета по простому модулю. 2. Квадратичный невычет. Критерий квадратичного невычета по простому модулю. 3. Символ Лежандра и его свойства. 4. Алгоритм вычисления символа Лежандра, использующий факторизацию. 5. Символ Якоби и его свойства. 6. Эффективный алгоритм вычисления символа Лежандра на основе символа Якоби.

Задачи для самостоятельной работы:

1. Вычислить значение символа Лежандра:

$$\left(\frac{24}{47}\right), \quad \left(\frac{42}{47}\right), \quad \left(\frac{29}{53}\right), \quad \left(\frac{46}{97}\right), \quad \left(\frac{75}{101}\right), \quad \left(\frac{69}{107}\right).$$

2. Вычислить значение символа Лежандра на основе символа Якоби:

$$\left(\frac{180}{307}\right), \quad \left(\frac{328}{421}\right), \quad \left(\frac{572}{971}\right), \quad \left(\frac{582}{983}\right), \quad \left(\frac{524}{727}\right), \quad \left(\frac{724}{1031}\right).$$

Тема 4. Тесты на простоту

Основные вопросы темы:

Тест на простоту на основе малой теоремы Ферма. Псевдопростые числа по заданному основанию. Числа Кармайкла и их свойства. Критерий Корсельта. Критерий Эйлера простоты числа. Эйлеровы псевдопростые числа по заданному основанию. Тест на простоту Соловея-Штрассена. Теорема Мил-

лера. Теорема Рабина. Тест на простоту Миллера-Рабина. Генерация простых чисел. $N-1$ методы доказательства простоты. Метод Поклингтона проверки на простоту. Теорема Лемера. Алгоритм построения простых чисел p с известным простым делителем q числа $p-1$.

Рекомендации по изучению темы:

Все вопросы изложены в параграфе 1.23 учебного пособия [3].

Контрольные вопросы:

1. Тест на простоту на основе малой теоремы Ферма. 2. Псевдопростые числа по заданному основанию. 3. Критерий Эйлера простоты числа. 4. Эйлеровы псевдопростые числа по заданному основанию. 5. Тест на простоту Соловея-Штрассена. 6. Теорема Миллера. Теорема Рабина. Тест на простоту Миллера-Рабина. 7. Генерация простых чисел. 8. Метод Поклингтона проверки на простоту.

Тема 5. Задача факторизации

Основные вопросы темы:

Задача факторизации. ρ-метод Полларда. $(p-1)$-метод Полларда.

Рекомендации по изучению темы:

Все вопросы изложены в параграфе 1.24 учебного пособия [3].

Контрольные вопросы:

1. Задача факторизации.
2. ρ-метод Полларда.
3. $(p-1)$-метод Полларда.

Тема 6. Методы дискретного логарифмирования

Основные вопросы темы:

Метод Гельфонла-Шенкса. ρ-метод Полларда. Метод исчисления порядка. Решение систем сравнений, возникающих в методе исчисления порядка.

Рекомендации по изучению темы:

Все вопросы изложены в параграфе 1.25 учебного пособия [3].

Контрольные вопросы:

1. Методы дискретного логарифмирования. Метод Гельфонла-Шенкса. 2. Методы дискретного логарифмирования. ρ-метод Полларда. 3. Методы дискретного логарифмирования. Метод исчисления порядка.

Задачи для самостоятельной работы:

Найти решение систем сравнений:

а) $\begin{cases} 7x+5y+6z \equiv 7 \pmod{10}, \\ 9x+2y+7z \equiv 2 \pmod{10}, \\ 2x+3y+4z \equiv 8 \pmod{10}, \end{cases}$ б) $\begin{cases} 4x+3y+4z \equiv 4 \pmod{16}, \\ 10x+5y+11z \equiv 6 \pmod{16}, \\ 11x+9y+13z \equiv 14 \pmod{16}, \end{cases}$

в) $\begin{cases} 2x+14y+7z \equiv 16 \pmod{22}, \\ 10x+21y+20z \equiv 11 \pmod{22}, \\ 7x+7y+18z \equiv 19 \pmod{22}. \end{cases}$

Литература

[1] Маховенко Е.Б. Теоретико-числовые методы в криптографии. Учеб. пособие для вузов. М.: Гелиос АРВ, 2006. 320 с.

[2] Нестеренко А.Ю. Теоретико-числовые методы в криптографии: учеб. пособие. Моск. гос. ин-т электроники и математики. 2012. 224 с.

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