

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ
ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего
образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Методические указания
для проведения практических работ
по дисциплине «Основы модулярной арифметики»
для студентов направления подготовки
01.04.02 Прикладная математика и информатика

Ставрополь, 2026

Оглавление

Введение

Практическое занятие №1: Теоретические основы построения СОК в области целых чисел

Практическое занятие №2: Построение СОК в области целых неотрицательных чисел.

Модульные операции в СОК

Практическое занятие № 3: Отрицательные числа в СОК

Практическое занятие № 4: Представление чисел в многоступенчатой (иерархической) СОК

Практическое занятие № 5-6: Позиционные характеристики кодов СОК и их вычисление

Практическое занятие № 7-8: Методы перевода чисел из СОК в ПСС

Практическое занятие № 9: Контрольное занятие (собеседование)

Практическое занятие № 10: Операции расширения системы оснований и деления на основания СОК

Практическое занятие № 11: Операции расширения системы оснований и деления на основания СОК

Практическое занятие № 12: Деление в системе остаточных классов. Общий случай

Практическое занятие № 13: Корректирующие свойства кодов в СОК

Практическое занятие № 14: Построение системы остаточных классов в комплексной области

Практическое занятие № 15: Построение системы остаточных классов в гиперкомплексных областях

Практическое занятие № 16: Контрольное занятие (коллоквиум)

Введение

Общей фундаментальной стратегией теоретических исследований, осуществляемых в настоящее время, является применение подходов, базирующихся на интенсивном использовании различных форм параллелизма на алгоритмическом, программном и аппаратном уровнях. В свете сказанного исключительно большое значение имеют исследования, ориентированные на применение перспективных способов кодирования числовой информации и соответствующих им параллельных вариантов компьютерной арифметики. Многочисленные исследования отечественных и зарубежных ученых показали, что позиционная система счисления (ПСС) исчерпала свои возможности для построения высокоскоростных параллельных вычислительных структур. Поэтому актуален переход к непозиционным системам счисления, наиболее перспективной из которых является система остаточных классов (СОК), обладающая высоким уровнем естественного параллелизма при выполнении арифметических операций, высокой точностью, надежностью и способностью к самокоррекции. Отмеченные факторы и обусловили включение в учебный план направления подготовки 01.04.02 « Прикладная математика и информатика» дисциплины под названием «Основы модулярной арифметики».

Цель данного курса ознакомить студентов с представлением целых чисел в СОК, научить выполнять модульные и немодульные операции, вычислять позиционные характеристики чисел, изучить условия обнаружения, локализации и исправления ошибок кодами СОК, рассмотреть области применения СОК, перспективы развития данного направления, что должно способствовать подготовке студентов к написанию выпускных квалификационных работ по рассматриваемой тематике.

В результате изучения дисциплины «Основы модулярной арифметики» студент должен обладать следующими компетенциями:

ПК-1- способен проводить научные исследования и получать новые научные и прикладные результаты самостоятельно и в составе научного коллектива на основе существующих методов в конкретной области профессиональной деятельности ;

ПК-7- способен управлять информацией с использованием цифровых средств и алгоритмов обработки данных для решения задач профессиональной деятельности.

При формировании названных компетенций в результате изучения дисциплины студент

- Демонстрирует способность применять знания теоретико-числовые основ построения системы остаточных классов в области целых чисел.

- Способен выполнять обменные операции между модулярным и позиционным кодом.
- Демонстрирует владение навыками выполнения основных операций над числами, представленными в модулярном коде.
- Демонстрирует знание теоретико-числовые основ расширения системы остаточных классов в области вещественных чисел.
- Демонстрирует способность использовать модулярное кодирование данных для реализации алгоритмов цифровой обработки сигналов.
- Демонстрирует владение навыками оценки сложности алгоритмов обработки данных в модулярном коде.

Данное учебно-методическое пособие представляет собой учебно-методические материалы по организации практических занятий по указанной дисциплине для направления подготовки 01.04.02 «Прикладная математика и информатика», направленность (профиль) «Математическое моделирование».

В разработку каждого практического занятия включены вопросы для подготовки к занятию, а также задания, решаемые в аудитории и предлагаемые студентам для самостоятельной работы дома.

Практическое занятие №1.

Тема: Теоретические основы построения СОК в области целых чисел.

Вопросы к занятию:

1. Дайте определение отношению делимости в кольце Z . Приведите примеры.
2. Сформулируйте и докажите основные свойства отношения делимости.
3. Дайте понятие операции деления с остатком. Приведите примеры.
4. Сформулируйте и докажите теорему о делении с остатком.
5. Введите понятия общего делителя чисел, наибольшего общего делителя (НОД) чисел. Перечислите способы отыскания НОДа. Укажите свойства НОДа.
6. Введите понятия взаимно простых и попарно взаимно простых чисел, приведите примеры.
7. Что такое общее кратное чисел? Дайте определение наименьшего общего кратного (НОК) чисел. Перечислите свойства НОК и докажите их. Какова связь между НОК и НОД двух чисел?
8. Дайте определение простых и составных чисел. К какому классу можно отнести единицу?
9. Введите понятие целой части действительного числа $[x]$. Приведите примеры. Постройте график функции $y=[x]$. Перечислите и докажите свойства функции целая часть числа.
10. Дайте определение дробной части действительного числа $\{x\}$. Приведите примеры. Постройте график функции $y=\{x\}$.
11. Дайте определение функции Эйлера $\varphi(m)$. Выведите формулу для нахождения $\varphi(m)$. Чему равна функция Эйлера от простого числа? Сформулируйте и докажите теорему Эйлера. Сформулируйте и докажите малую теорему Ферма.
12. Дайте определение конечной цепной (правильной, непрерывной) дроби. Введите понятие подходящих дробей. Введите формулы для нахождения числителей и знаменателей подходящих дробей.
13. Дайте определение сравнимых чисел. Докажите эквивалентность отношения сравнимости чисел по модулю m и отношения давать одинаковые остатки при делении на m . Сформулируйте и докажите основные свойства сравнений.
14. Введите определения вычета, класса вычетов. Определите операции над классами вычетов. Докажите, что множество классов вычетов по составному модулю относительно операций сложения и умножения классов образуют кольцо, а по простому модулю – поле.

15. Сформулируйте и докажите теорему о числе решений линейного сравнения. Перечислите основные методы решения линейных сравнений.
16. Дайте определение системы линейных сравнений с одним неизвестным. По какому модулю будет решение совместной системы линейных сравнений $x \equiv b_i \pmod{m_i}$, где $i=1, 2, \dots, n$.
17. Сформулируйте и докажите Китайскую теорему об остатках. Какова её роль в решении систем линейных сравнений?

Задания, решаемые в аудитории

1. Число $a=42157$ при делении на некоторое целое положительное число b даёт в частном $q=231$. Найдите делитель b и частное q .
2. Делимое 100, остаток 6. Найдите делитель b и частное q .
3. Докажите, что сумма квадратов пяти последовательных чисел не может быть точным квадратом.
4. Между цифрами числа 16 вписывают 15, в середину числа 1156 опять вписывают 15 и т.д. Докажите, что все полученные числа будут точными квадратами.
5. С помощью алгоритма Евклида найдите наибольший общий делитель чисел и его линейное представление
 - а) 546 и 231; б) 6919 и 1443.
6. Найдите $[-3]; [5,4]; \left[-\frac{7}{9}\right]; [\sqrt{31}]; [\sqrt{715}+1]; \left[4+\cos\frac{101\pi}{204}\right]; [2+\lg 0,3]$.
7. Разложите данные обыкновенные дроби в непрерывные. Замените полученные дроби подходящими дробями четвертого порядка и определите погрешность замены
 - а) $\frac{163}{159}$; б) $\frac{1882}{1651}$.
8. С помощью преобразования коэффициентов найдите решения сравнений
 - а) $3x \equiv 7 \pmod{13}$; б) $7x \equiv 15 \pmod{21}$; в) $16x \equiv 12 \pmod{28}$.
9. С помощью метода Эйлера решите сравнения
 - а) $8x \equiv 18 \pmod{10}$; б) $25x \equiv 4 \pmod{28}$.
10. Решите сравнения методом цепных дробей
 - а) $124x \equiv 32 \pmod{216}$; б) $543x \equiv 421 \pmod{635}$;
 - в) $361x \equiv 38 \pmod{541}$.
11. Решите системы сравнений

$$\begin{array}{lll} \text{а) } \begin{cases} x \equiv 6 \pmod{15} \\ x \equiv 18 \pmod{21}; \\ x \equiv 3 \pmod{12} \end{cases} & \text{б) } \begin{cases} x \equiv 1 \pmod{25} \\ x \equiv 2 \pmod{4} \\ x \equiv 3 \pmod{7} \\ x \equiv 4 \pmod{9} \end{cases} & \text{в) } \begin{cases} 4x \equiv 3 \pmod{7} \\ 5x \equiv 4 \pmod{11} \\ 11x \equiv 8 \pmod{13} \end{cases} \end{array}$$

Задания для самостоятельной работы дома

- Докажите, что из двух последовательных чётных чисел одно делится на 4, а из пяти последовательных натуральных чисел одно делится на 5.
- Докажите, что если остаток от деления некоторого числа на 9 есть одно из чисел 2, 3, 5, 6, 8, то это число не может быть точным квадратом.
- С помощью алгоритма Евклида найдите наибольший общий делитель чисел и его линейное представление
а) 903 и 731; б) 4543 и 885.
- Найдите НОД и НОК чисел 3059, 2737, 943.
- Сумма двух чисел 667, а отношение НОК к их НОД равно 120. Найдите эти числа.
- Найдите $\left[\frac{8}{3}\right]$; $[-2,7]$; $[\sqrt{15}]$; $[\sqrt[4]{200}]$; $\left[\frac{\sqrt{542}+2}{3}\right]$; $[2 - \lg 2512]$; $[1 + \ln 50]$.
- Сколько чисел в интервале от 50 до 200 не взаимно простых с числом 24?
- Дано $\varphi(a) = 11424$ и $a = p^2 q^2$, где p и q – различные простые числа. Найдите a .
- Найдите число всех положительных правильных несократимых дробей со знаменателями от 2 до 10.
- Сколько чисел в интервале от 1 до 120 не взаимно простых с числом 30?
- Дано $\varphi(a) = 3600$ и $a = 3^\alpha \cdot 5^\beta \cdot 7^\gamma$. Найдите a .
- Найдите количество правильных несократимых дробей со знаменателем 16.
- С помощью непрерывных дробей решите следующие неопределённые уравнения
а) $122x + 129y = 2$; б) $258x - 175y = 113$; в) $41x + 114y = 5$.
- С помощью преобразования коэффициентов найдите решения сравнений
а) $11x \equiv 15 \pmod{18}$; б) $24x \equiv 36 \pmod{54}$; в) $15x \equiv 17 \pmod{21}$.
- С помощью метода Эйлера решите сравнения
а) $16x \equiv 4 \pmod{25}$; б) $18x \equiv 26 \pmod{42}$.
- Решите сравнения методом цепных дробей

- а) $37x \equiv 25 \pmod{117}$; б) $91x \equiv 143 \pmod{222}$;
 в) $271x \equiv 25 \pmod{119}$; г) $375x \equiv 195 \pmod{501}$.

17. Решите системы сравнений

$$\text{а) } \begin{cases} x \equiv 4 \pmod{5} \\ x \equiv 1 \pmod{12} \\ x \equiv 7 \pmod{14} \end{cases} ; \text{ б) } \begin{cases} 5x \equiv 1 \pmod{12} \\ 5x \equiv 2 \pmod{8} \\ 7x \equiv 3 \pmod{11} \end{cases} ; \quad \text{в) } \begin{cases} 2x \equiv 7 \pmod{13} \\ 5x \equiv 8 \pmod{17} \\ 3x \equiv 7 \pmod{31} \\ 14x \equiv 35 \pmod{19} \end{cases} .$$

Учебно-методическое и информационное обеспечение дисциплины

Основная литература

Обработка информации в системе остаточных классов (СОК) [Электронный ресурс]: учебное пособие / Н.И. Червяков [и др.]. — Электрон. текстовые данные. — Ставрополь: Северо-Кавказский федеральный университет, 2016. — 225 с. — 2227-8397. Режим доступа: <http://www.iprbookshop.ru/69412.html>

Модулярная арифметика и ее приложения в инфокоммуникационных технологиях: [монография] / Н. И. Червяков и др. — Москва: ФИЗМАТЛИТ, 2017. — 400 с.: ил., табл., портр. — Библиогр. в конце разд. — ISBN 978-5-9221-1716-6

Дополнительная литература

Применение искусственных нейронных сетей и системы остаточных классов в криптографии / Н. И. Червяков [и др.]. — М. : ФИЗМАТЛИТ, 2012. — 280 с. : ил., прил. — ISBN 978-5-9221-1386-1

Интернет-ресурсы

<http://www.elibrary.ru>
www.biblioclub.ru
www.iprbookshop.ru
www.distant.msu.ru

Практическое занятие № 2

Тема: Построение СОК в области целых неотрицательных чисел. Модульные операции в СОК

Вопросы к занятию

1. Какие требования предъявляются к любой кодовой системе?
2. Дайте определение позиционной системы счисления и систематической записи числа. Как выполняются арифметические действия над систематическими числами.
3. Расскажите о способах перевода чисел из одной позиционной системы счисления в другую.
4. Дайте определение обобщенной позиционной системы счисления.
5. Назовите недостатки позиционной системы счисления.
6. Какие системы счисления относят к непозиционным системам. Приведите примеры непозиционных систем..
7. Дайте определение системы остаточных классов. Введите понятие диапазона представления чисел.
8. Почему при построении СОК к основаниям предъявляются требования взаимной простоты? Постройте пример СОК с основаниями не обладающими этим свойством. Какая задача при этом не может быть решена?
9. Какие требования могут предъявляться к СОК при определении набора модулей (оснований)? Расскажите о критериях выбора оснований СОК.
10. Сформулируйте критерий оптимального выбора оснований СОК для данного диапазона..
11. Расскажите о числах Мерсенна и Ферма.
12. Введите операцию сложения в СОК и докажите возможность определения цифр суммы по указанному Вами правилу.
13. Введите операцию умножения чисел в СОК и докажите возможность определения цифр произведения по указанному Вами правилу.
14. Введенные Вами операции к числу каких операций в СОК относятся и почему их так называют?
15. Если сумма или произведение чисел превысит диапазон, то в результате какое число будет получено, как оно соотносится с правильным результатом?
16. Введите понятия индекса и анииндекса числа. Приведите примеры.

17. Покажите как индексирование может быть использовано при выполнении операции умножения. Какое требование необходимо предъявлять к системе оснований, чтобы предусмотреть возможность индексирования?
18. Перечислите достоинства СОК.
19. Назовите недостатки СОК. Каковы возможности их преодоления.
20. Назовите основоположников системы остаточных классов, перечислите их основные работы и охарактеризуйте их вклад в развитие модулярной арифметики

Задания, решаемые в аудитории

1. Постройте систему остаточных классов с основаниями 2, 5, 7, 13, 19. Определите ее диапазон.
2. Проверьте, удовлетворяет ли построенная система рассмотренному Вами критерию оптимальности. Приведите примеры других наборов оснований, закрывающих тот же диапазон. Какая из них будет удовлетворять критерию оптимальности?
3. Представьте в предложенной в задании 1 системе числа 21, 45, 98, 115, 237, 1347.
4. Найдите попарную сумму предложенных в задании 3 чисел. Сложите все числа. Был ли выход при выполнении этих действий выход за границы диапазона? Проверьте результаты в позиционной системе.
5. Найдите произведение попарное произведение чисел из задания 3? В каком случае был выход за границы диапазона? Какое число получили при выходе за границы диапазона в позиционном представлении, как оно соотносится с истинным результатом? Проверьте результаты в позиционной системе.

Задания для самостоятельной работы дома

1. Пусть дана система оснований 3, 5, 11, 19, 23. Решите задания предложенные в аудитории для этой системы.
2. Пусть дана система оснований 4, 13, 15, 23, 77. Решите задания предложенные в аудитории для этой системы.

Учебно-методическое и информационное обеспечение дисциплины

Основная литература

Обработка информации в системе остаточных классов (СОК) [Электронный ресурс]: учебное пособие / Н.И. Червяков [и др.]. — Электрон. текстовые данные. — Ставрополь: Северо-Кавказский федеральный университет, 2016. — 225 с. — 2227-8397. Режим доступа: <http://www.iprbookshop.ru/69412.html>

Модулярная арифметика и ее приложения в инфокоммуникационных технологиях:

[монография] / Н. И. Червяков и др. – Москва: ФИЗМАТЛИТ, 2017. – 400 с.: ил., табл., портр. – Библиогр. в конце разд. – ISBN 978-5-9221-1716-6

Дополнительная литература

Применение искусственных нейронных сетей и системы остаточных классов в криптографии / Н. И. Червяков [и др.]. – М. : ФИЗМАТЛИТ, 2012. – 280 с. : ил., прил. – ISBN 978-5-9221-1386-1

Интернет-ресурсы

<http://www.elibrary.ru>

www.biblioclub.ru

www.iprbookshop.ru

www.distant.msu.ru

Практическое занятие №3

Тема: Отрицательные числа в СОК

Вопросы к занятию

1. Расскажите, какие существуют способы введения знака числа в СОК?
2. Введите знак числа в СОК в неявном виде в СОК с четным основанием? Дайте определение искусственной формы представления числа.
3. Введите операцию сложения для чисел разных знаков в построенной СОК.
4. Введите операцию умножения в построенной СОК
5. Постройте модулярную арифметику для СОК с нечетными модулями, позволяющую оперировать с числами разных знаков.

Задания, решаемые в аудитории

1. В СОК с основаниями 2, 5, 11, 17, 19, 23 предусмотрите возможность введения знака и представьте следующие числа: 38, -38, 54, -54, 25, -25, 111, -111.
2. В построенной СОК выполните сложение чисел и результат проверьте в позиционной системе:
а) $38+54$; б) $-38+54$; в) $-38-54$; г) $-38+25$; д) $-38-25$; е) $38+111$; ж) $54-111$; з) $-25+111$.
3. В построенной СОК найдите произведения указанных чисел и результат проверьте в позиционной системе:
а) $38 \cdot 54$; б) $-38 \cdot 54$; в) $-38 \cdot (-54)$; г) $-38 \cdot 25$; д) $-38 \cdot (-25)$; е) $25 \cdot 111$; ж) $25 \cdot (-111)$; з) $-25 \cdot (-111)$; и) $-25 \cdot 111$.
4. Решите предложенные выше задачи для СОК с основаниями 4, 5, 7, 13, 19, 23, 29.
5. Решите задания 1-3 для СОК с основаниями 3, 5, 11, 13, 19, 29.

Задания для самостоятельной работы дома

1. Решите задания, решаемые в аудитории для СОК с основаниями 2, 7, 13, 15, 19, 31.
2. Решите задания, решаемые в аудитории для СОК с основаниями 5, 7, 9, 11, 17, 31.

Учебно-методическое и информационное обеспечение дисциплины

Основная литература

Обработка информации в системе остаточных классов (СОК) [Электронный ресурс]: учебное пособие / Н.И. Червяков [и др.]. — Электрон. текстовые данные. — Ставрополь: Северо-Кавказский федеральный университет, 2016. — 225 с. — 2227-8397. Режим доступа: <http://www.iprbookshop.ru/69412.html>

Модулярная арифметика и ее приложения в инфокоммуникационных технологиях:

[монография] / Н. И. Червяков и др. – Москва: ФИЗМАТЛИТ, 2017. – 400 с.: ил., табл., портр. – Библиогр. в конце разд. – ISBN 978-5-9221-1716-6

Дополнительная литература

Применение искусственных нейронных сетей и системы остаточных классов в криптографии / Н. И. Червяков [и др.]. – М. : ФИЗМАТЛИТ, 2012. – 280 с. : ил., прил. – ISBN 978-5-9221-1386-1

Интернет-ресурсы

<http://www.elibrary.ru>

www.biblioclub.ru

www.iprbookshop.ru

www.distant.msu.ru

Практическое занятие № 4

Тема «Представление чисел в многоступенчатой (иерархической) СОК»

Вопросы к занятию

1. Расскажите о задаче оптимизации набора модулей при построении СОК.
2. В чем заключается критерий минимальности количества двоичных разрядов, которые используются при построении арифметического устройства?
3. Введите понятие логарифмического дефекта.
4. В чем заключается алгоритм выбора оснований СОК при заданном числовом диапазоне?
5. В чем заключается подход к оптимизации набора оснований, опирающийся на условие сохранения ранга системы?
6. Как построить многоступенчатую СОК? По каким критериям выбираются основания первого, второго и последующих ярусов для многоступенчатой СОК.
7. Приведите пример многоступенчатой СОК, обеспечивающей диапазон 10^8 .
8. Введите модульные операции в многоступенчатой СОК.

Задания, решаемые в аудитории

1. Постройте многоступенчатую систему СОК, обеспечивающую диапазон 10^{10} . Приведите примеры выполнения модульных операций в этой системе. Результаты проверьте в позиционной системе.
2. Охарактеризуйте построенную в задании 1 систему с точки зрения критериев оптимальности.

Задания для самостоятельной работы дома

1. Постройте многоступенчатую систему СОК, обеспечивающую диапазон 10^{12} . Приведите примеры выполнения модульных операций в этой системе. Результаты проверьте в позиционной системе.
2. Охарактеризуйте построенную в задании 1 систему с точки зрения критериев оптимальности.
3. Введите знак числа в построенной Многоступенчатой СОК. Приведите примеры оперирования с числами разных знаков.

Учебно-методическое и информационное обеспечение дисциплины

Основная литература

Обработка информации в системе остаточных классов (СОК) [Электронный ресурс]:

учебное пособие / Н.И. Червяков [и др.]. — Электрон. текстовые данные. — Ставрополь:

Северо-Кавказский федеральный университет, 2016. – 225 с. – 2227-8397. Режим доступа:
<http://www.iprbookshop.ru/69412.html>

Модулярная арифметика и ее приложения в инфокоммуникационных технологиях:
[монография] / Н. И. Червяков и др. – Москва: ФИЗМАТЛИТ, 2017. – 400 с.: ил., табл.,
портр. – Библиогр. в конце разд. – ISBN 978-5-9221-1716-6

Дополнительная литература

Применение искусственных нейронных сетей и системы остаточных классов в
криптографии / Н. И. Червяков [и др.]. – М. : ФИЗМАТЛИТ, 2012. – 280 с. : ил., прил. –
ISBN 978-5-9221-1386-1

Интернет-ресурсы

<http://www.elibrary.ru>

www.biblioclub.ru

www.iprbookshop.ru

www.distant.msu.ru

Практическое занятие № 5-6.

Тема: Позиционные характеристики кодов СОК и их вычисление

Вопросы к занятию

1. Сформулируйте Китайскую операцию об остатках.
2. Дайте определение ортогональных базисов и запишите формулу перевода числа из СОК в ПСС с помощью ортогональных базисов.
3. Введите понятие ранга числа.
4. Сформулируйте теорему о ранге суммы и доказите ее.
5. Укажите, какое применение имеет теорема о ранге суммы.
6. Расскажите алгоритм вычисления ранга числа, основанный на теореме о ранге суммы.
7. Введите понятия истинного и расчетного ранга числа.
8. Расскажите о расширенном представлении числа в СОК.
9. Введите определение ключа инверсного представления.
10. Какая система оснований СОК называется нормированной.
11. Введите понятия ортогональных, псевдоортогональных и минимальных псевдоортогональных чисел, следа псевдоортогонального числа.
12. Дайте определение минимального следа числа.
13. Дайте определение минимальной формы числа.
14. Запишите формулы для вычисления ранга и следа минимальных псевдоортогональных чисел в нормированной системе оснований.
15. Дайте определения понятиям: ядро ранга, коррекция ранга.
16. Сформулируйте теорему о нахождении ранга числа по рангам минимальных псевдоортогональных чисел.
17. Введите понятие характера числа.

Задания, решаемые в аудитории

1. Пусть в системе оснований 2; 3; 5; 11; 23 задано число $(0;2;3;8;17)$. Найдите истинный и расчетный ранг этого числа.
2. В системе оснований 2; 3; 5; 11; 23 заданы числа $(0;2;3;8;17)$ и $(1; 2; 4; 7; 6)$. Найдите сумму этих чисел. По теореме о ранге суммы определите был ли выход за границы диапазона. Результат проверьте переводом в ПСС (перевод осуществите методом ортогональных базисов).

Задания для самостоятельной работы дома

Для СОК с основаниями 2; 7; 13; 17; 29 решите задачи, предложенные в аудитории, для чисел (0;2;3;8;17) и (1; 2; 4; 7; 6).

Учебно-методическое и информационное обеспечение дисциплины

Основная литература

Обработка информации в системе остаточных классов (СОК) [Электронный ресурс]: учебное пособие / Н.И. Червяков [и др.]. — Электрон. текстовые данные. — Ставрополь: Северо-Кавказский федеральный университет, 2016. — 225 с. — 2227-8397. Режим доступа: <http://www.iprbookshop.ru/69412.html>

Модулярная арифметика и ее приложения в инфокоммуникационных технологиях: [монография] / Н. И. Червяков и др. — Москва: ФИЗМАТЛИТ, 2017. — 400 с.: ил., табл., портр. — Библиогр. в конце разд. — ISBN 978-5-9221-1716-6

Дополнительная литература

Применение искусственных нейронных сетей и системы остаточных классов в криптографии / Н. И. Червяков [и др.]. — М. : ФИЗМАТЛИТ, 2012. — 280 с. : ил., прил. — ISBN 978-5-9221-1386-1

Интернет-ресурсы

<http://www.elibrary.ru>

www.biblioclub.ru

www.iprbookshop.ru

www.distant.msu.ru

Практическое занятие № 7-8.

Методы перевода чисел из СОК в ПСС

Вопросы к занятию

1. Сформулируйте китайскую теорему об остатках.
2. Каков алгоритм перевода числа из СОК в ПСС с помощью метода ортогональных базисов?
3. Как вычисляется объем диапазона?
4. По какой формуле определяются ортогональные базисы?
5. По какой формуле определяется число A по методу ортогональных базисов?
6. В каком виде представляется число в ОПСС?
7. Назовите преимущество метода перевода числа в ОПСС перед методом ортогональных базисов?
8. Перечислите условия завершения процесса перевода числа в ОПСС до выполнения последнего шага?
9. Какие модификации метода ортогональных базисов вам известны?
10. Запишите формулу вычисления констант α_{kj} .
11. Что является основной характеристикой интервального метода?
12. Назовите формулу для определения номера интервала.
13. Сформулируйте теорему Эйлера.
14. Какой модуль целесообразно выбирать в качестве дробящего?
15. Формула для перевода числа из СОК в ПСС с помощью интервального метода.
16. Суть интервального метода для применения формулы для пар оснований СОК.
17. Изобразите схему объединения модулей при $n = 2k$.
18. Изобразите схему объединения модулей при $n = 2k + 1$.
19. Формула для перевода числа из СОК в ПСС с помощью интервального метода для пар оснований.
20. Проведите сравнительный анализ методов перевода чисел из СОК в ПСС.

Задания, решаемые в аудитории

1. Пусть дана система оснований $p_1 = 2, p_2 = 3, p_3 = 5$. Перевести число $A = (1, 1, 0)$ в позиционную систему.
2. Пусть дана система оснований $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, p_5 = 11$, объем диапазона $P = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 = 2310$. Даны числа $A = (0, 2, 3, 2, 1)$ и $B = (1, 1, 2, 4, 8)$. Найти сумму $A+B$ и перевести результат в ПСС методом ортогональных базисов.
3. Пусть дана система оснований $p_1 = 2, p_2 = 3, p_3 = 5$. Объем диапазона $P = 2310$. Переведем число $A = (1, 1, 4)$ в ОПС.

4. Пусть основания системы $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, p_5 = 11$, объём диапазона $P = 2310$. Перевести числа $A = (0,2,3,2,1)$ и $B = (1,1,2,4,8)$ в ОПС.
5. Пусть основания системы $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, p_5 = 11$, объём диапазона $P = 2310$. Даны числа $A = (0,2,3,2,1)$ и $B = (1,1,2,4,8)$. Найти сумму $A+B$ и перевести результат в ОПС.
6. Пусть основания системы $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, p_5 = 11$, объём диапазона $P = 2310$. Даны числа $A = (0,2,3,2,1)$ и $B = (1,1,2,4,8)$. Найти разность $A-B$ и перевести результат в ОПС.
7. Пусть дана система оснований $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7$, тогда $P = 210$. Переведите число $A = (1,1,4,5)$ в ПСС с помощью интервального метода.
8. Пусть основания системы $p_1 = 2, p_2 = 3, p_3 = 5$. Даны числа $A = (0,2,3)$ и $B = (1,1,2)$. Найти сумму $A+B$ и перевести результат в ПСС с помощью интервального метода.
9. Пусть основания системы $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, p_5 = 11$, объём диапазона $P = 2310$. Даны числа $A = (0,2,3,2,1)$ и $B = (1,1,2,4,8)$. Найти произведение $A*B$ и перевести результат в ПСС с помощью интервального метода.
10. Пусть дана система оснований $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7$, тогда $P = 210$. Переведите число $A = (1,1,4,5)$ в ПСС с помощью интервального метода для пар оснований.

Задания для самостоятельной работы дома

1. Пусть дана система оснований $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, p_5 = 11$, объём диапазона $P = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 = 2310$. Перевести число $A = (1, 1, 0, 2, 7)$ в позиционную систему.
2. Пусть дана система оснований $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, p_5 = 11$. Объём диапазона $P = 2310$. Переведём число $A = (1, 0, 1, 4, 7)$ в ОПС.
3. Пусть основания системы $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7$, объём диапазона $P = 2310$. Перевести числа $A = (1,2,3,2)$ и $B = (1,0,2,4)$ в ОПС.
4. Пусть основания системы $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, p_5 = 11$, объём диапазона $P = 2310$. Даны числа $A = (0,2,3,2,1)$ и $B = (1,1,2,4,8)$. Найти произведение AB и перевести результат в ОПС.

5. Пусть основания системы $p_1 = 2, p_2 = 3, p_3 = 5$. Даны числа $A = (0,2,3)$ и $B = (1,1,2)$. Найти произведение $A \cdot B$ и перевести результат в ПСС с помощью интервального метода.
6. Пусть основания системы $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, p_5 = 11$, объём диапазона $P = 2310$. Даны числа $A = (0,2,3,2,1)$ и $B = (1,1,2,4,8)$. Найти сумму $A+B$ и перевести результат в ПСС с помощью интервального метода.
7. Пусть основания системы $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, p_5 = 11$, объём диапазона $P = 2310$. Даны числа $A = (0,2,3,2,1)$ и $B = (1,1,2,4,8)$. Найти разность $A-B$ и перевести результат в ПСС с помощью интервального метода.
8. Пусть основания системы $p_1 = 2, p_2 = 3, p_3 = 5$. Даны числа $A = (0,2,3)$ и $B = (1,1,2)$. Найти произведение $A \cdot B$ и перевести результат в ПСС с помощью интервального метода для пар оснований.
9. Пусть основания системы $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, p_5 = 13$. Даны числа $A = (0,2,3,2,1)$ и $B = (1,1,2,4,8)$. Найти произведение $A \cdot B$ и перевести результат в ПСС с помощью интервального метода для пар оснований.
10. Пусть основания системы $p_1 = 2, p_2 = 3, p_3 = 5$. Даны числа $A = (0,2,3)$ и $B = (1,1,2)$. Найти сумму $A+B$ и перевести результат в ПСС с помощью интервального метода для пар оснований.

Учебно-методическое и информационное обеспечение дисциплины

Основная литература

Обработка информации в системе остаточных классов (СОК) [Электронный ресурс]: учебное пособие / Н.И. Червяков [и др.]. — Электрон. текстовые данные. — Ставрополь: Северо-Кавказский федеральный университет, 2016. — 225 с. — 2227-8397. Режим доступа: <http://www.iprbookshop.ru/69412.html>

Модулярная арифметика и ее приложения в инфокоммуникационных технологиях: [монография] / Н. И. Червяков и др. — Москва: ФИЗМАТЛИТ, 2017. — 400 с.: ил., табл., портр. — Библиогр. в конце разд. — ISBN 978-5-9221-1716-6

Дополнительная литература

Применение искусственных нейронных сетей и системы остаточных классов в криптографии / Н. И. Червяков [и др.]. — М. : ФИЗМАТЛИТ, 2012. — 280 с. : ил., прил. — ISBN 978-5-9221-1386-1

Интернет-ресурсы

<http://www.elibrary.ru>

www.biblioclub.ru

www.iprbookshop.ru

www.distant.msu.ru

Практическое занятие № 9.
Контрольное занятие (собеседование)
Вопросы для собеседования
Базовый уровень

Теоретико-числовое обоснование построения системы остаточных классов (СОК) в области целых чисел

1. Дайте определение отношению делимости в кольце Z . Приведите примеры.
2. Сформулируйте и докажите основные свойства отношения делимости.
3. Дайте понятие операции деления с остатком. Приведите примеры.
4. Сформулируйте и докажите теорему о делении с остатком.
5. Введите понятия общего делителя чисел, наибольшего общего делителя (НОД) чисел. Перечислите способы отыскания НОДа. Укажите свойства НОДа.
6. Введите понятия взаимно простых и попарно взаимно простых чисел, приведите примеры.
7. Что такое общее кратное чисел? Дайте определение наименьшего общего кратного (НОК) чисел. Перечислите свойства НОК и докажите их. Какова связь между НОК и НОД двух чисел?
8. Дайте определение простых и составных чисел. К какому классу можно отнести единицу?
9. Введите понятие целой части действительного числа $[x]$. Приведите примеры. Постройте график функции $y=[x]$. Перечислите и докажите свойства функции целая часть числа.
10. Дайте определение дробной части действительного числа $\{x\}$. Приведите примеры. Постройте график функции $y=\{x\}$.
11. Дайте определение функции Эйлера $\varphi(m)$. Выведите формулу для нахождения $\varphi(m)$. Чему равна функция Эйлера от простого числа? Сформулируйте и докажите теорему Эйлера Сформулируйте и докажите малую теорему Ферма.
12. Дайте определение конечной цепной (правильной, непрерывной) дроби. Введите понятие подходящих дробей. Введите формулы для нахождения числителей и знаменателей подходящих дробей.
13. Дайте определение сравнимых чисел. Докажите эквивалентность отношения сравнимости чисел по модулю m и отношения давать одинаковые остатки при делении на m . Сформулируйте и докажите основные свойства сравнений.

14. Введите определения вычета, класса вычетов. Определите операции над классами вычетов. Докажите, что множество классов вычетов по составному модулю относительно операций сложения и умножения классов образуют кольцо, а по простому модулю – поле.
15. Сформулируйте и докажите теорему о числе решений линейного сравнения. Перечислите основные методы решения линейных сравнений.
16. Дайте определение системы линейных сравнений с одним неизвестным. По какому модулю будет решение совместной системы линейных сравнений $x \equiv b_i \pmod{m_i}$, где $i=1, 2, \dots, n$.
17. Сформулируйте и докажите Китайскую теорему об остатках. Какова её роль в решении систем линейных сравнений?
18. Какие требования предъявляются к любой кодовой системе?
19. Дайте определение позиционной системы счисления и систематической записи числа. Как выполняются арифметические действия над систематическими числами.
20. Расскажите о способах перевода чисел из одной позиционной системы счисления в другую.
21. Дайте определение обобщенной позиционной системы счисления.
22. Назовите недостатки позиционной системы счисления.
23. Какие системы счисления относят к непозиционным системам. Приведите примеры непозиционных систем..
24. Дайте определение системы остаточных классов. Введите понятие диапазона представления чисел.
25. Какие требования могут предъявляться к СОК при определении набора модулей (оснований)? Расскажите о критериях выбора оснований СОК.

Модульные операции в СОК

1. Введите операцию сложения в СОК и докажите возможность определения цифр суммы по указанному Вами правилу.
2. Введите операцию умножения чисел в СОК и докажите возможность определения цифр произведения по указанному Вами правилу.
3. Введенные Вами операции к числу каких операций в СОК относятся и почему их так называют?
4. Если сумма или произведение чисел превысит диапазон, то в результате какое число будет получено, как оно соотносится с правильным результатом?
5. Перечислите достоинства СОК.

6. Назовите недостатки СОК. Каковы возможности их преодоления.
7. Назовите основоположников системы остаточных классов, перечислите их основные работы и охарактеризуйте их вклад в развитие модулярной арифметики.
8. Расскажите, какие существуют способы введения знака числа в СОК?
9. Введите знак числа в СОК в неявном виде в СОК с четным основанием? Дайте определение искусственной формы представления числа.

Немодульные операции в СОК. Методы перевода из ПСС в СОК и обратно

1. Расскажите о методах перевода из ПСС в СОК: метод деления, метод непосредственного модульного перевода двоичного кода в СОК, метод Горнера, метод рекурсивного сдвигания, метод понижения разрядности исходного позиционного кода, метод преобразования полиадического кода в код системы остаточных классов. Сравните эти методы.
2. Каков алгоритм перевода числа из СОК в ПСС с помощью метода ортогональных базисов? На какой теореме он основан?
3. В каком виде представляется число в ОПСС?
4. Назовите преимущество метода перевода числа в ОПСС перед методом ортогональных базисов?
5. Перечислите условия завершения процесса перевода числа в ОПСС до выполнения последнего шага?
6. Какие модификации метода ортогональных базисов вам известны?
7. Запишите формулу вычисления констант τ_{kj} .
8. Что является основной характеристикой интервального метода? Назовите формулу для определения номера интервала. Сформулируйте теорему Эйлера. Какой модуль целесообразно выбирать в качестве дробящего?

Повышенный уровень

Теоретико-числовое обоснование построения системы остаточных классов (СОК) в области целых чисел

1. Расскажите о числах Мерсенна и Ферма.
2. Почему при построении СОК к основаниям предъявляются требования взаимной простоты? Постройте пример СОК с основаниями не обладающими этим свойством. Какая задача при этом не может быть решена?
3. Сформулируйте критерий оптимального выбора оснований СОК для данного диапазона..
4. Расскажите о задаче оптимизации набора модулей при построении СОК.

5. В чем заключается критерий минимальности количества двоичных разрядов, которые используются при построении арифметического устройства?
6. Введите понятие логарифмического дефекта.
7. В чем заключается алгоритм выбора оснований СОК при заданном числовом диапазоне?
8. В чем заключается подход к оптимизации набора оснований, опирающийся на условие сохранения ранга системы?

Модульные операции в СОК

1. Как построить многоступенчатую СОК? По каким критериям выбираются основания первого, второго и последующих ярусов для многоступенчатой СОК.
2. Приведите пример многоступенчатой СОК, обеспечивающей диапазон 10^8 .
3. Введите модульные операции в многоступенчатой СОК.
4. Введите понятия индекса и анииндекса числа. Приведите примеры.
5. Покажите как индексирование может быть использовано при выполнении операции умножения. Какое требование необходимо предъявлять к системе оснований, чтобы предусмотреть возможность индексирования?
6. Введите операцию сложения для чисел разных знаков в построенной СОК.
7. Введите операцию умножения в построенной СОК
8. Постройте модулярную арифметику для СОК с нечетными модулями, позволяющую оперировать с числами разных знаков.

Немодульные операции в СОК. Методы перевода из ПСС в СОК и обратно

1. Введите понятие ранга числа.
2. Сформулируйте теорему о ранге суммы и докажите ее.
3. Укажите, какое применение имеет теорема о ранге суммы.
4. Расскажите алгоритм вычисления ранга числа, основанный на теореме о ранге суммы.
5. Введите понятия истинного и расчетного ранга числа.
6. Расскажите о расширенном представлении числа в СОК.
7. Введите определение ключа инверсного представления.
8. Какая система оснований СОК называется нормированной.
9. Введите понятия ортогональных, псевдоортогональных и минимальных псевдоортогональных чисел, следа псевдоортогонального числа.
10. Дайте определение минимального следа числа.

11. Дайте определение минимальной формы числа.
12. Запишите формулы для вычисления ранга и следа минимальных псевдоортогональных чисел в нормированной системе оснований.
13. Дайте определения понятиям: ядро ранга, коррекция ранга.
14. Сформулируйте теорему о нахождении ранга числа по рангам минимальных псевдоортогональных чисел.
15. Введите понятие характера числа.
16. Формула для перевода числа из СОК в ПСС с помощью интервального метода.
17. Суть интервального метода для применения формулы для пар оснований СОК.
18. Изобразите схему объединения модулей при $n = 2k$.
19. Изобразите схему объединения модулей при $n = 2k + 1$.
20. Формула для перевода числа из СОК в ПСС с помощью интервального метода для пар оснований.
21. Проведите сравнительный анализ методов перевода чисел из СОК в ПСС.

1. Критерии оценивания компетенций

Оценка "*отлично*" выставляется, если студент при ответе на вопросы как базового так и повышенного уровня показывает глубокое и всестороннее знание предмета, обязательной и дополнительной литературы, аргументировано и логически стройно излагает материал, пользуясь математической символикой, может применять знания для анализа конкретных ситуаций, свободно ориентируется в межпредметных связях.

Оценка «*хорошо*» ставится, если при ответе на вопросы базовой части студент показывает знание предмета, обязательной литературы, знакомстве с дополнительной литературой, аргументировано излагает материал, умеет применять знания для анализа конкретных ситуаций, однако незначительно нарушает последовательность изложения материала, дает недостаточно полное, хотя и верное определение понятий.

Оценка «*удовлетворительно*» ставится, если студент при ответе на вопросы базовой части показал, что он в основном знает предмет, обязательную литературу, может практически применять свои знания, но программный материал излагает фрагментарно и непоследовательно, допускает отдельные ошибки и погрешности при применении математической символики и понятий, слабо ориентируется в межпредметных связях;.

Оценка «*неудовлетворительно*» ставится, если студент не отвечает на предлагаемые ему вопросы базовой или его ответ показывает, что не усвоено основное содержание предмета, обнаруживается незнание большей части учебного материала, допускаются грубые ошибки

при формулировке теорем, определении основных понятий, неправильно используется математическая символика.

2. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедура проведения данного оценочного мероприятия включает в себя собеседование по представленным вопросам. Допуском к собеседованию является правильное выполнение не менее 60% домашних заданий, по темам представленным к собеседованию. Каждому студенту предлагается по одному вопросу из каждой темы. Сначала студент отвечает на вопросы базового уровня. При успешном ответе ему предлагается один-два вопроса из вопросов повышенного уровня, что позволяет преподавателю определить уровень владения материалом.

Предлагаемые студенту задания позволяют проверить компетенцию ПК-1, ПК-7. Для подготовки к данному оценочному мероприятию необходимо прочитать лекционный материал, выполнять домашние задания, которые выдаются на практических занятиях и сдать их на проверку не позднее чем за неделю до контрольного мероприятия, найти ответы на поставленные вопросы, изучить дополнительную литературу, установить взаимосвязи между изучаемыми понятиями, запомнить основные определения, свойства, теоремы, продумать, где они могут применяться. Рекомендуется готовиться к данному контрольному мероприятию в течение семестра, разбирая теоретические задания для оценки сформированности компетенций к каждому практическому занятию, вовремя выполняя домашние задания.

При подготовке к ответу студенту разрешается пользоваться своими тетрадями с домашними заданиями, никакими другими справочными материалами пользоваться не разрешается. Для подготовки к ответу на каждый вопрос отводится время до 3-5 минут, в течение которого студент может записать план своего ответа. Для подготовки к ответу на вопросы повышенного уровня предлагается дополнительное время.

Содержание и объем материала, подлежащего проверке, определяется программой дисциплины. При проверке усвоения этого материала производится выявление полноты, прочности усвоения студентами теории и умения применять ее на практике в знакомых и незнакомых ситуациях.

При оценке в первую очередь учитываются показанные студентами знания и умения (их полноту, глубину, прочность, использование). Оценка также зависит от наличия и характера погрешностей. Среди погрешностей выделяют ошибки и недочеты. Погрешность считается ошибкой, если она свидетельствует о том, что студент не овладел основными знаниями, умениями, указанными в программе.

К недочетам относятся погрешности, свидетельствующие о недостаточно полном или недостаточно прочном усвоении основных знаний и умений или о отсутствии знаний не считающихся основными в соответствии с программой. Недочетами также являются: погрешности, которые не привели к искажению смысла полученного студентом задания или способа его выполнения, неаккуратная запись.

Учебно-методическое и информационное обеспечение дисциплины

Основная литература

Обработка информации в системе остаточных классов (СОК) [Электронный ресурс]: учебное пособие / Н.И. Червяков [и др.]. — Электрон. текстовые данные. — Ставрополь: Северо-Кавказский федеральный университет, 2016. — 225 с. — 2227-8397. Режим доступа: <http://www.iprbookshop.ru/69412.html>

Модулярная арифметика и ее приложения в инфокоммуникационных технологиях: [монография] / Н. И. Червяков и др. — Москва: ФИЗМАТЛИТ, 2017. — 400 с.: ил., табл., портр. — Библиогр. в конце разд. — ISBN 978-5-9221-1716-6

Дополнительная литература

Применение искусственных нейронных сетей и системы остаточных классов в криптографии / Н. И. Червяков [и др.]. — М. : ФИЗМАТЛИТ, 2012. — 280 с. : ил., прил. — ISBN 978-5-9221-1386-1

Интернет-ресурсы

<http://www.elibrary.ru>

www.biblioclub.ru

www.iprbookshop.ru

www.distant.msu.ru

Практическое занятие № 10.

Тема: Операции расширения системы оснований и деления на основания СОК

Вопросы к занятию

1. Дайте определение операции расширения системы оснований.
2. В каких случаях необходимо выполнять расширение оснований? К числу каких операций (модульных или немодульных) относится эта операция. Ответ обоснуйте.
3. Расскажите о методе расширения системы оснований, который опирается на позиционные характеристики ранг и след числа.
4. Расскажите о методе расширения системы оснований с помощью алгоритма перевода в ОПС. Объясните почему при этом методе старшая цифра при перевод в ОПС должна быть равна 0..
5. Какую модификацию предложенного алгоритма можете предложить?
6. Сравните предложенные методы расширения системы оснований.
7. Приведите алгоритм деления чисел на основание СОК, опирающийся на операцию расширения системы оснований с помощью перевода в ОПС.
8. Как провести деление на произведение модулей СОК?
9. Как провести деление на степень основания СОК?
10. Расскажите о модификации предложенного алгоритма при введении знака числа.
11. Расскажите об алгоритме деления на основание СОК, опирающемся на позиционную характеристику след числа.
12. Введите операцию масштабирования чисел. Изложите алгоритм выполнения этой операции.

Задания, решаемые в аудитории

1. В СОК с основаниями 2, 5, 13, 19, 23 задано число (1; 3; 10; 11; 17) проведите операцию расширения системы оснований двумя методами, добавив основания 17 и 31.
2. Число 12345 переведите в СОК с основаниями 2, 5, 13, 19, 23. Разделите это число в СОК

а) на 19; б) на 95.

Деление проведите двумя методами и результат проверьте с помощью позиционной системы.

Задания для самостоятельной работы дома

1. В СОК с основаниями 2, 7, 11, 17, 29 задано число (0; 5; 3; 12; 20) проведите операцию расширения системы оснований двумя методами, добавив основания 13 и 41.

2. Число 8547 переведите в СОК с основаниями 2, 7, 11, 17, 29. Разделите это число в СОК

а) на 17; б) на 77.

Деление проведите двумя методами и результат проверьте с помощью позиционной системы.

Учебно-методическое и информационное обеспечение дисциплины

Основная литература

Обработка информации в системе остаточных классов (СОК) [Электронный ресурс]: учебное пособие / Н.И. Червяков [и др.]. — Электрон. текстовые данные. — Ставрополь: Северо-Кавказский федеральный университет, 2016. — 225 с. — 2227-8397. Режим доступа: <http://www.iprbookshop.ru/69412.html>

Модулярная арифметика и ее приложения в инфокоммуникационных технологиях: [монография] / Н. И. Червяков и др. — Москва: ФИЗМАТЛИТ, 2017. — 400 с.: ил., табл., портр. — Библиогр. в конце разд. — ISBN 978-5-9221-1716-6

Дополнительная литература

Применение искусственных нейронных сетей и системы остаточных классов в криптографии / Н. И. Червяков [и др.]. — М. : ФИЗМАТЛИТ, 2012. — 280 с. : ил., прил. — ISBN 978-5-9221-1386-1

Интернет-ресурсы

<http://www.elibrary.ru>

www.biblioclub.ru

www.iprbookshop.ru

www.distant.msu.ru

Практическое занятие № 11.

Тема «Операции расширения системы оснований и деления на основания СОК»

Вопросы к занятию

1. Дайте определение операции расширения системы оснований.
2. В каких случаях необходимо выполнять расширение оснований? К числу каких операций (модульных или немодульных) относится эта операция. Ответ обоснуйте.
3. Расскажите о методе расширения системы оснований, который опирается на позиционные характеристики ранг и след числа.
4. Расскажите о методе расширения системы оснований с помощью алгоритма перевода в ОПС. Объясните почему при этом методе старшая цифра при перевод в ОПС должна быть равна 0..
5. Какую модификацию предложенного алгоритма можете предложить?
6. Сравните предложенные методы расширения системы оснований.
7. Приведите алгоритм деления чисел на основание СОК, опирающийся на операцию расширения системы оснований с помощью перевода в ОПС.
8. Как провести деление на произведение модулей СОК?
9. Как провести деление на степень основания СОК?
10. Расскажите о модификации предложенного алгоритма при введении знака числа.
11. Расскажите об алгоритме деления на основание СОК, опирающемся на позиционную характеристику след числа.
12. Введите операцию масштабирования чисел. Изложите алгоритм выполнения этой операции.

Задания, решаемые в аудитории

3. В СОК с основаниями 2, 5, 13, 19, 23 задано число (1; 3; 10; 11; 17) проведите операцию расширения системы оснований двумя методами, добавив основания 17 и 31.
4. Число 12345 переведите в СОК с основаниями 2, 5, 13, 19, 23. Разделите это число в СОК

а) на 19; б) на 95.

Деление проведите двумя методами и результат проверьте с помощью позиционной системы.

Задания для самостоятельной работы дома

1. В СОК с основаниями 2, 7, 11, 17, 29 задано число (0; 5; 3; 12; 20) проведите операцию расширения системы оснований двумя методами, добавив основания 13 и 41.

2. Число 8547 переведите в СОК с основаниями 2, 7, 11, 17, 29. Разделите это число в СОК

а) на 17; б) на 77.

Деление проведите двумя методами и результат проверьте с помощью позиционной системы.

Учебно-методическое и информационное обеспечение дисциплины

Основная литература

Обработка информации в системе остаточных классов (СОК) [Электронный ресурс]: учебное пособие / Н.И. Червяков [и др.]. — Электрон. текстовые данные. — Ставрополь: Северо-Кавказский федеральный университет, 2016. — 225 с. — 2227-8397. Режим доступа: <http://www.iprbookshop.ru/69412.html>

Модулярная арифметика и ее приложения в инфокоммуникационных технологиях: [монография] / Н. И. Червяков и др. — Москва: ФИЗМАТЛИТ, 2017. — 400 с.: ил., табл., портр. — Библиогр. в конце разд. — ISBN 978-5-9221-1716-6

Дополнительная литература

Применение искусственных нейронных сетей и системы остаточных классов в криптографии / Н. И. Червяков [и др.]. — М. : ФИЗМАТЛИТ, 2012. — 280 с. : ил., прил. — ISBN 978-5-9221-1386-1

Интернет-ресурсы

<http://www.elibrary.ru>

www.biblioclub.ru

www.iprbookshop.ru

www.distant.msu.ru

Практическое занятие № 12.

Тема: Деление в системе остаточных классов. Общий случай.

(семинарское занятие)

Вопросы к семинару.

1. Перечислите случаи деления в СОК.
2. Сформулируйте теорему о делении с остатком.
3. Почему операция деления относится к числу немодульных операций.
4. В каком случае можно осуществить поразрядное деление цифр α_i на β_i .
5. При каком условии деление определит единственным образом цифру $\gamma_i = \frac{\alpha_i + k_i p_i}{\beta_i}$.
6. Почему деление на 2 играет важную роль в СОК.
7. Дайте определение правильной цифры.
8. Какой след имеет четное число $A = (\alpha_1, \alpha_2, \dots, \alpha_n)$ с нечетными основаниями в результате деления на 2.
9. Какой характер имеет четное число $A = (\alpha_1, \alpha_2, \dots, \alpha_n)$ с нечетными основаниями в результате деления на 2.
10. Перечислите возможные случаи Δ_A (характера), учитывая четность α_n .
11. Дайте определение формального деления.
12. Каким соотношением определяется четность или нечетность числа A , если в системе с нечетными основаниями $p_1, p_2, \dots, p_n$ задано число $A = (\alpha_1, \alpha_2, \dots, \alpha_n)$ со следом S_A и характером Δ_A и числом неправильных цифр λ и если задано частное от формального деления A на 2
$$\left(\frac{A}{2}\right)_\phi = (\beta_1, \beta_2, \dots, \beta_n) \text{ со следом } S \frac{A}{2} \text{ и характером } \Delta \frac{A}{2}.$$
13. Дайте определение неправильной цифры.
14. Каким выражением определяется $\Delta \frac{A}{4}$ если в системе с нечетными основаниями $p_1, p_2, \dots, p_n$ задано число $A = (\alpha_1, \alpha_2, \dots, \alpha_n)$ со следом S_A , характером Δ_A , делящееся нацело на четыре, и если частное от деления A на четыре $\frac{A}{4} = (\tilde{\gamma}_1, \tilde{\gamma}_2, \dots, \tilde{\gamma}_n)$ со следом $S \frac{A}{4}$, характером $\Delta \frac{A}{4}$, то для $p_n = 4k + 1$, где k — целое неотрицательное число.
15. Алгоритм деления на фиксированное число.

16. Сформулируйте теорему о делении на произведение чисел.
17. Алгоритм деления числа A на произведение модулей.
18. Перечислите этапы общего случая деления.
- 19.** Можно ли уменьшить количество итераций при общем случае деления.
Каким может быть делитель, если он фиксированный

Практическое занятие № 13.

Тема: Корректирующие свойства кодов в СОК.

Вопросы к занятию:

1. Дайте определение безызбыточного и избыточного представления чисел в СОК.
2. Что называется корректирующим кодом в СОК.
3. На какие основные классы можно разбить все корректирующие коды.
4. Что такое минимальное кодовое расстояние.
5. Свойства весовых функций.
6. Теоремы, устанавливающие связь между минимальным расстоянием кода, и его корректирующими возможностями.
7. Чему равно минимальное расстояние корректирующего кода в системе остаточных классов.
8. Дайте определение R -кода.
9. Теорема о минимальном расстоянии R -кода.
10. Может ли R – код обнаружить и использовать некоторое число ошибок более высокой кратности, чем та, которая допускается, в соответствии с минимальным расстоянием кода.
11. Меньше какой величины не может быть число контрольных модулей R - кода с минимальным расстоянием d .
12. в каком случае минимальное расстояние кода не единицу больше числа контрольных модулей, т. е. $d = r + 1$.
13. Опишите случай, при котором минимальное расстояние равно числу контрольных модулей, т. е. $d = r$.
14. каким образом можно изменять минимальное расстояние.
15. Как изменится минимальное расстояние кода, если некоторая СОК расширяется путем добавления l модулей, каждый из которых больше модулей исходной системы.
16. . В каком случае представление чисел в СОК всегда избыточно?
17. Корректирующий R – код с минимальным расстоянием 3 используется для исправления ошибок кратности $k=1$. Может ли этот код обнаруживать или даже исправлять хотя бы часть ошибок более высокой кратности

Задания, решаемые в аудитории.

1. Системе остаточных классов с основаниями 3, 4, 9 соответствует L -код, у которого $L = M = 12$. вычислите, чему равно P .
2. Ошибки, какой кратности может исправить корректирующий код, если $d_{\min} = 4$.
4. Какой RL -код соответствует системе с основаниями 3, 5, 7, 11?
5. Имеется СОК с основаниями 3, 4, 5. $L = 12$, данной СОК соответствует R -код. Вычислите R .
6. Ошибки какой кратности может обнаружить корректирующий код, если $d_{\min} = 3$.

Задания для самостоятельной работы дома

1. Постройте геометрическую модель кодов СОК для случая 3-х модулей.
2. Проанализируйте ошибки какой кратности можно обнаруживать и исправлять с помощью этой модели при различном сочетании рабочего и полного диапазонов.

Учебно-методическое и информационное обеспечение дисциплины

Основная литература

Обработка информации в системе остаточных классов (СОК) [Электронный ресурс]: учебное пособие / Н.И. Червяков [и др.]. — Электрон. текстовые данные. — Ставрополь: Северо-Кавказский федеральный университет, 2016. — 225 с. — 2227-8397. Режим доступа: <http://www.iprbookshop.ru/69412.html>

Модулярная арифметика и ее приложения в инфокоммуникационных технологиях: [монография] / Н. И. Червяков и др. — Москва: ФИЗМАТЛИТ, 2017. — 400 с.: ил., табл., портр. — Библиогр. в конце разд. — ISBN 978-5-9221-1716-6

Дополнительная литература

Применение искусственных нейронных сетей и системы остаточных классов в криптографии / Н. И. Червяков [и др.]. — М. : ФИЗМАТЛИТ, 2012. — 280 с. : ил., прил. — ISBN 978-5-9221-1386-1

Интернет-ресурсы

<http://www.elibrary.ru>
www.biblioclub.ru
www.iprbookshop.ru
www.distant.msu.ru

Практическое занятие № 14

Тема «Построение системы остаточных классов в комплексной области» (семинарское занятие)

Вопросы к занятию

1. Дайте определение целого комплексного числа.
2. Введите отношение сравнимости для целых комплексных чисел.
3. Постройте изоморфное отображение целых комплексных чисел на множество целых неотрицательных чисел.
4. Сформулируйте и докажите фундаментальные теоремы Гаусса.
5. Сформулируйте признак, по которому можно судить о принадлежности данного целого комплексного числа к совокупности чисел M , описываемых избранными основаниями.
6. В чем заключается изоморфизм систем комплексных и вещественных вычетов?
7. Расскажите о представлении комплексного числа в виде матрицы.
8. Как построить СОК в области комплексных чисел, опираясь на их представление в виде матрицы?
9. Как отобразить комплексные числа на пары действительных чисел? Как построить обратное отображение.
10. Постройте СОК в комплексной области, отображая комплексные числа на пары действительных чисел.

Учебно-методическое и информационное обеспечение дисциплины

Основная литература

Обработка информации в системе остаточных классов (СОК) [Электронный ресурс]: учебное пособие / Н.И. Червяков [и др.]. — Электрон. текстовые данные. — Ставрополь: Северо-Кавказский федеральный университет, 2016. — 225 с. — 2227-8397. Режим доступа: <http://www.iprbookshop.ru/69412.html>

Модулярная арифметика и ее приложения в инфокоммуникационных технологиях: [монография] / Н. И. Червяков и др. — Москва: ФИЗМАТЛИТ, 2017. — 400 с.: ил., табл., портр. — Библиогр. в конце разд. — ISBN 978-5-9221-1716-6

Дополнительная литература

Применение искусственных нейронных сетей и системы остаточных классов в криптографии / Н. И. Червяков [и др.]. — М. : ФИЗМАТЛИТ, 2012. — 280 с. : ил., прил. — ISBN 978-5-9221-1386-1

Интернет-ресурсы

<http://www.elibrary.ru>

www.biblioclub.ru

www.iprbookshop.ru

www.distant.msu.ru

Практическое занятие № 15

Тема «Построение системы остаточных классов в гиперкомплексных областях» (семинарское занятие)

Вопросы к занятию

1. Дайте определение гиперкомплексной системы.
2. Расскажите о кватернионах. Введите операции сложения для этих чисел.
3. Какую алгебраическую систему образуют кватернионы относительно операций сложения и умножения.
4. Дайте определение бикватернионов. Введите операции сложения для этих чисел.
5. Какую алгебраическую систему образуют кватернионы относительно операций сложения и умножения.
6. Определите октавы. Введите операции сложения для этих чисел.
7. Какую алгебраическую систему образуют кватернионы относительно операций сложения и умножения.
8. Введите понятие квадриплексных чисел. Введите операции сложения для этих чисел.
9. Какую алгебраическую систему образуют кватернионы относительно операций сложения и умножения.
10. Сформулируйте фундаментальную теорему Гаусса.
11. Как определить отношение сравнения в алгебре кватернионов; бикватернионов; октав; квадриплексных чисел.
12. Расскажите о построении СОК в указанных выше гиперкомплексных областях. Как осуществляется отображение указанных числовых множеств на множество целых чисел.

Учебно-методическое и информационное обеспечение дисциплины

Основная литература

Обработка информации в системе остаточных классов (СОК) [Электронный ресурс]: учебное пособие / Н.И. Червяков [и др.]. — Электрон. текстовые данные. — Ставрополь: Северо-Кавказский федеральный университет, 2016. — 225 с. — 2227-8397. Режим доступа: <http://www.iprbookshop.ru/69412.html>

Модулярная арифметика и ее приложения в инфокоммуникационных технологиях: [монография] / Н. И. Червяков и др. — Москва: ФИЗМАТЛИТ, 2017. — 400 с.: ил., табл., портр. — Библиогр. в конце разд. — ISBN 978-5-9221-1716-6

Дополнительная литература

Применение искусственных нейронных сетей и системы остаточных классов в криптографии / Н. И. Червяков [и др.]. – М. : ФИЗМАТЛИТ, 2012. – 280 с. : ил., прил. – ISBN 978-5-9221-1386-1

Интернет-ресурсы

<http://www.elibrary.ru>

www.biblioclub.ru

www.iprbookshop.ru

www.distant.msu.ru

Практическое занятие № 16.
Контрольное занятие (коллоквиум)
Вопросы для коллоквиума
Базовый уровень

Немодульные операции в СОК. Расширение диапазона и деление чисел в СОК

1. Сформулируйте Китайскую операцию об остатках.
2. Дайте определение ортогональных базисов и запишите формулу перевода числа из СОК в ПСС с помощью ортогональных базисов.
3. Дайте определение операции расширения системы оснований.
4. В каких случаях необходимо выполнять расширение оснований? К числу каких операций (модульных или немодульных) относится эта операция. Ответ обоснуйте.
5. Расскажите о методе расширения системы оснований, который опирается на позиционные характеристики ранг и след числа.
6. Расскажите о методе расширения системы оснований с помощью алгоритма перевода в ОПС. Объясните почему при этом методе старшая цифра при перевод в ОПС должна быть равна 0..
7. Какую модификацию предложенного алгоритма можете предложить?
8. Сравните предложенные методы расширения системы оснований.
9. Приведите алгоритм деления чисел на основание СОК, опирающийся на операцию расширения системы оснований с помощью перевода в ОПС.
10. Как провести деление на произведение модулей СОК?
11. Как провести деление на степень основания СОК?
12. Расскажите о модификации предложенного алгоритма при введении знака числа.
13. Расскажите об алгоритме деления на основание СОК, опирающемся на позиционную характеристику след числа.
14. Введите операцию масштабирования чисел. Изложите алгоритм выполнения этой операции.

Корректирующие свойства кодов в СОК

1. Дайте определение безызбыточного и избыточного представления чисел в СОК.
2. Что называется корректирующим кодом в СОК.
3. На какие основные классы можно разбить все корректирующие коды.
4. Что такое минимальное кодовое расстояние.
5. Теоремы, устанавливающие связь между минимальным расстоянием кода, и его корректирующими возможностями.

6. Чему равно минимальное расстояние корректирующего кода в системе остаточных классов.
7. Дайте определение R-кода.
8. Опишите случай, при котором минимальное расстояние равно числу контрольных модулей, т. е. $d = r$.
9. Каким образом можно изменять минимальное расстояние.
10. Как изменится минимальное расстояние кода, если некоторая СОК расширяется путем добавления l модулей, каждый из которых больше модулей исходной системы.
11. В каком случае представление чисел в СОК всегда избыточно?

Построение системы остаточных классов в комплексной области

1. Дайте определение целого комплексного числа.
2. Введите отношение сравнимости для целых комплексных чисел.
3. Постройте изоморфное отображение целых комплексных чисел на множество целых неотрицательных чисел.
4. Сформулируйте и докажите фундаментальные теоремы Гаусса.
5. Сформулируйте признак, по которому можно судить о принадлежности данного целого комплексного числа к совокупности чисел M , описываемых избранными основаниями.
6. В чем заключается изоморфизм систем комплексных и вещественных вычетов?
7. Расскажите о представлении комплексного числа в виде матрицы.
8. Как построить СОК в области комплексных чисел, опираясь на их представление в виде матрицы?
9. Как отобразить комплексные числа на пары действительных чисел? Как построить обратное отображение.
10. Постройте СОК в комплексной области, отображая комплексные числа на пары действительных чисел.

Области применения модулярной арифметики

1. В чем состоит сущность цифровой обработки сигнала? Что такое сигнал? Что такое аналоговый сигнал? Что такое дискретный сигнал?
2. Что называют отсчетом сигнала? Что такое интервал дискретизации? Что такое частота дискретизации?
3. Рассказать о нормированной частоте?

4. Что такое цифровой сигнал?
5. Сформулируйте китайскую теорему для многочленов.
6. Расскажите о квантовании числа. Что называют шагом квантования? Какие два способа используются при квантовании?
7. Расскажите о нелинейные и линейные модели процесса квантования.
8. Какие основные операции выполняет АЦП?
9. Использование нейросетевых технологий в задачах обработки сигналов.
10. Основные подходы к реализации нейронных сетей.
11. Что называют линейным пороговым элементом?
12. Соотношение, связывающее вход и выход m -го ЛПЭ j -слоя сети?
13. Что собой представляет вычислительная модель нейронной сети?
14. Причины целесообразности приближения нейронных сетей к СОК.
15. Какая связь существует между нейронной сетью и системой остаточных классов?

Повышенный уровень

Немодульные операции в СОК. Расширение диапазона и деление чисел в СОК

1. Перечислите случаи деления в СОК.
2. Сформулируйте теорему о делении с остатком.
3. Почему операция деления относится к числу немодульных операций.
4. В каком случае можно осуществить поразрядное деление цифр α_i на β_i .
5. При каком условии деление определит единственным образом цифру $\gamma_i = \frac{\alpha_i + k_i p_i}{\beta_i}$.
6. Почему деление на 2 играет важную роль в СОК.
7. Дайте определение правильной цифры.
8. Какой след имеет четное число $A = (\alpha_1, \alpha_2, \dots, \alpha_n)$ с нечетными основаниями в результате деления на 2.
9. Какой характер имеет четное число $A = (\alpha_1, \alpha_2, \dots, \alpha_n)$ с нечетными основаниями в результате деления на 2.
10. Перечислите возможные случаи Δ_A (характера), учитывая четность α_n .
11. Дайте определение формального деления.
12. Каким соотношением определяется четность или нечетность числа A , если в системе с нечетными основаниями $p_1, p_2, \dots, p_n$ задано число $A = (\alpha_1, \alpha_2, \dots, \alpha_n)$ со

следом S_A и характером Δ_A и числом неправильных цифр λ и если задано частное от формального деления A на 2

$$\left(\frac{A}{2}\right)_\phi = (\beta_1, \beta_2, \dots, \beta_n) \text{ со следом } S \frac{A}{2} \text{ и характером } \Delta \frac{A}{2}.$$

13. Дайте определение неправильной цифры.

14. Каким выражением определяется $\Delta \frac{A}{4}$ если в системе с нечетными основаниями

$p_1, p_2, \dots, p_n$ задано число $A = (\alpha_1, \alpha_2, \dots, \alpha_n)$ со следом S_A , характером Δ_A ,

делящееся нацело на четыре, и если частное от деления A на четыре $\frac{A}{4} =$

$(\tilde{\gamma}_1, \tilde{\gamma}_2, \dots, \tilde{\gamma}_n)$ со следом $S \frac{A}{4}$, характером $\Delta \frac{A}{4}$, то для $p_n = 4k + 1$, где k — целое

неотрицательное число.

15. Алгоритм деления на фиксированное число.

16. Сформулируйте теорему о делении на произведение чисел.

17. Алгоритм деления числа A на произведение модулей.

18. Перечислите этапы общего случая деления.

19. Можно ли уменьшить количество итераций при общем случае деления.

20. Каким может быть делитель, если он фиксированный.

Корректирующие свойства кодов в СОК

1. Теорема о минимальном расстоянии R -кода.
2. Может ли R – код обнаружить и использовать некоторое число ошибок более высокой кратности, чем та, которая допускается, в соответствии с минимальным расстоянием кода.
3. Меньше какой величины не может быть число контрольных модулей R - кода с минимальным расстоянием d .
4. В каком случае минимальное расстояние кода не единицу больше числа контрольных модулей, т. е. $d = r + 1$.
5. Корректирующий R – код с минимальным расстоянием 3 используется для исправления ошибок кратности $k=1$. Может ли этот код обнаруживать или даже исправлять хотя бы часть ошибок более высокой кратности.

Построение системы остаточных классов в комплексной области

1. Дайте определение гиперкомплексной системы.

2. Расскажите о кватернионах. Введите операции сложения для этих чисел.
3. Какую алгебраическую систему образуют кватернионы относительно операций сложения и умножения.
4. Дайте определение бикватернионов. Введите операции сложения для этих чисел.
5. Какую алгебраическую систему образуют кватернионы относительно операций сложения и умножения.
6. Определите октавы. Введите операции сложения для этих чисел.
7. Какую алгебраическую систему образуют кватернионы относительно операций сложения и умножения.
8. Введите понятие квадриплексных чисел. Введите операции сложения для этих чисел.
9. Какую алгебраическую систему образуют кватернионы относительно операций сложения и умножения.
10. Сформулируйте фундаментальную теорему Гаусса.
11. Как определить отношение сравнения в алгебре кватернионов; бикватернионов; октав; квадриплексных чисел.
12. Расскажите о построении СОК в указанных выше гиперкомплексных областях. Как осуществляется отображение указанных числовых множеств на множество целых чисел.

Области применения модулярной арифметики

1. Расскажите об алгоритме перекрытия с суммированием.
2. Расскажите об алгоритме перекрытия с накоплением.
3. Расскажите об алгоритме Кука – Тоома.
4. Расскажите об алгоритме Винограда вычисления коротких сверток. Какой вид имеет Z-передаточная функция простейшего z-фильтра?
5. Как можно достигнуть улучшения качества обработки в z-фильтре?
6. На чем базируется разработка адаптивных структур?
7. Что показывают проведенные исследования в области создания отказоустойчивых специализированных процессоров ЦОС?
8. Что обеспечивает избыточное кодирование в СОК?
9. Реализация алгоритмов ЦОС на основе нейроподобной сети (НПС).

1. Критерии оценивания компетенций

Оценка "**отлично**" выставляется, если студент при ответе на вопросы как базового так и повышенного уровня показывает глубокое и всестороннее знание предмета, обязательной и дополнительной литературы, аргументировано и логически стройно излагает материал, пользуясь математической символикой, может применять знания для анализа конкретных ситуаций, свободно ориентируется в межпредметных связях.

Оценка **«хорошо»** ставится, если при ответе на вопросы базовой части студент показывает знание предмета, обязательной литературы, знакомстве с дополнительной литературой, аргументировано излагает материал, умеет применять знания для анализа конкретных ситуаций, однако незначительно нарушает последовательность изложения материала, дает недостаточно полное, хотя и верное определение понятий.

Оценка **«удовлетворительно»** ставится, если студент при ответе на вопросы базовой части показал, что он в основном знает предмет, обязательную литературу, может практически применять свои знания, но программный материал излагает фрагментарно и непоследовательно, допускает отдельные ошибки и погрешности при применении математической символики и понятий, слабо ориентируется в межпредметных связях;.

Оценка **«неудовлетворительно»** ставится, если студент не отвечает на предлагаемые ему вопросы базовой или его ответ показывает, что не усвоено основное содержание предмета, обнаруживается незнание большей части учебного материала, допускаются грубые ошибки при формулировке теорем, определении основных понятий, неправильно используется математическая символика.

2. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедура проведения данного оценочного мероприятия включает в себя устный опрос студентов в форме индивидуального собеседования на вопросы коллоквиума. Каждому студенту предлагается по одному вопросу из каждой темы. Сначала студент отвечает на вопросы базового уровня. При успешном ответе ему предлагается один-два вопроса из вопросов повышенного уровня, что позволяет преподавателю определить уровень владения материалом.

Предлагаемые студенту задания позволяют проверить компетенции ПК-1, ПК-7. Для подготовки к данному оценочному мероприятию необходимо прочитать лекционный материал, найти ответы на поставленные вопросы, изучить дополнительную литературу, установить взаимосвязи между изучаемыми понятиями, запомнить основные определения, свойства, теоремы, продумать, где они могут применяться. Запомнить методы доказательства основных теорем, свойств и провести самостоятельно доказательство оставшихся положений,

включённых в вопросы для подготовки к данному мероприятию. Рекомендуется готовиться к данному контрольному мероприятию в течение семестра, разбирая теоретические задания для оценки сформированности компетенций к каждому практическому занятию.

При подготовке к ответу студенту не разрешается пользоваться никакими справочными материалами. Для подготовки к ответу даётся время на подготовку до 10-15 минут, в течение которого студент может записать план своего ответа, основные формулы, план доказательства теорем. Для подготовки к ответу на вопросы повышенного уровня предлагается дополнительное время.

Содержание и объем материала, подлежащего проверке, определяется программой дисциплины. При проверке усвоения этого материала производится выявление полноты, прочности усвоения студентами теории и умения применять ее на практике в знакомых и незнакомых ситуациях.

При оценке в первую очередь учитываются показанные студентами знания и умения (их полноту, глубину, прочность, использование). Оценка также зависит от наличия и характера погрешностей. Среди погрешностей выделяют ошибки и недочеты. Погрешность считается ошибкой, если она свидетельствует о том, что студент не овладел основными знаниями, умениями, указанными в программе.

К недочетам относятся погрешности, свидетельствующие о недостаточно полном или недостаточно прочном усвоении основных знаний и умений или о отсутствии знаний не считающихся основными в соответствии с программой. Недочетами также являются: погрешности, которые не привели к искажению смысла полученного студентом задания или способа его выполнения, неаккуратная запись, небрежная формулировка основных определений, теорем, свойств.

Учебно-методическое и информационное обеспечение дисциплины

Основная литература

Обработка информации в системе остаточных классов (СОК) [Электронный ресурс]: учебное пособие / Н.И. Червяков [и др.]. — Электрон. текстовые данные. — Ставрополь: Северо-Кавказский федеральный университет, 2018. — 225 с. — 2227-8397. Режим доступа: <http://www.iprbookshop.ru/69412.html>

Модулярная арифметика и ее приложения в инфокоммуникационных технологиях: [монография] / Н. И. Червяков и др. — Москва: ФИЗМАТЛИТ, 2020. — 400 с.: ил., табл., портр. — Библиогр. в конце разд. — ISBN 978-5-9221-1716-6

Дополнительная литература

Применение искусственных нейронных сетей и системы остаточных классов в криптографии / Н. И. Червяков [и др.]. – М. : ФИЗМАТЛИТ, 2019. – 280 с. : ил., прил. – ISBN 978-5-9221-1386-1

Интернет-ресурсы

<http://www.elibrary.ru>

www.biblioclub.ru

www.iprbookshop.ru

www.distant.msu.ru

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ
ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего
образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Методические указания
по организации самостоятельной работы студентов
по дисциплине " Основы модулярной арифметики "

Направление подготовки 01.04.02 - Прикладная математика и информатика.

Профиль подготовки «Математическое моделирование».

Квалификация выпускника - магистр. Очная форма обучения.

Ставрополь, 2023

Оглавление.

Введение

1. Методические рекомендации по изучению теоретического материала, подготовке к практическим занятиям.
2. Вопросы для собеседования
3. Методические рекомендации по подготовке реферата.
4. Темы рефератов.

Введение.

Самостоятельная работа – планируемая учебная, учебно-исследовательская, научно-исследовательская работа студентов, выполняемая во внеаудиторное (аудиторное) время по заданию и при методическом руководстве преподавателя, но без его непосредственного участия (при частичном непосредственном участии преподавателя, оставляющем ведущую роль за работой студента).

Самостоятельная работа студента является важным видом учебной деятельности студента. Федеральным государственным образовательным стандартом предусматривается значительный объем времени из общей трудоемкости дисциплины на самостоятельную работу. В связи с этим, обучение включает в себя две, практически одинаковые по объему и взаимовлиянию части – процесса обучения и процесса самообучения. Поэтому самостоятельная работа должна стать эффективной и целенаправленной работой студента.

Концепцией модернизации российского образования определены основные задачи профессионального образования – подготовка квалифицированного работника соответствующего уровня и профиля, конкурентоспособного на рынке труда, компетентного, ответственного, свободно владеющего своей профессией и ориентированного в смежных областях деятельности, способного к эффективной работе по специальности на уровне мировых стандартов, готового к постоянному профессиональному росту, социальной и профессиональной мобильности.

Решение этих задач невозможно без повышения роли самостоятельной работы студентов над учебным материалом.

Самостоятельная работа студента предполагает, прежде всего, его практическую деятельность, поскольку именно этот вид учебной работы в первую очередь готовит к самостоятельному выполнению профессиональных задач. Конечной целью самостоятельной работы является организация самостоятельной познавательной деятельности, формирование умения самостоятельно анализировать информацию, выделять главное и второстепенное.

Основными формами самостоятельной работы студентов по дисциплине «Основы модулярной арифметики» являются:

- подготовка к практическому занятию,
- выполнение разноуровневых заданий, решение разноуровневых задач,
- самостоятельное изучение литературы,

- подготовка реферата.

В процессе изучения дисциплины у обучающихся формируются следующие компетенции (в соответствии с образовательным стандартом):

ПК-1- способен проводить научные исследования и получать новые научные и прикладные результаты самостоятельно и в составе научного коллектива на основе существующих методов в конкретной области профессиональной деятельности.

ПК-7- способен управлять информацией с использованием цифровых средств и алгоритмов обработки данных для решения задач профессиональной деятельности.

1. Методические рекомендации по изучению теоретического материала, подготовке к практическим занятиям.

Для подготовки к текущему практическому занятию

Дома

1. Прочитайте конспект лекции, соответствующий теме занятия. Запомните основные определения и теоремы.
2. Изучите рекомендуемую литературу по вопросам, выносимым на обсуждение.
3. Найдите ответы на теоретические задания. Подготовьтесь к ответам на эти вопросы на занятии.
4. Законспектируйте ответы на теоретические задания, которые не содержатся в Вашем конспекте лекции по указанной проблеме.
5. Изучите разобранные примеры решения типовых задач и законспектируйте их решение в рабочую тетрадь.

На занятии

6. Дайте ответы на вопросы из теоретических заданий и в рабочей тетради решите практические задания из заданий, решаемых в аудитории.

Дома

7. Закрепите полученные практические умения и навыки, решая практические задания из заданий для самостоятельной работы дома.

Для подготовки к итоговому практическому занятию по теме

Дома:

1. Подготовьтесь к собеседованию по теме по указанным теоретическим вопросам базового и повышенного уровня.
2. Подготовьтесь к собеседованию по выполненным домашним заданиям по теме.

2. Вопросы для собеседования

1. Систематические числа.
2. Обобщенно-позиционная система счисления.
3. Теоретико-числовые основы построения системы остаточных классов.
4. Способы введения отрицательных чисел в системе остаточных классов.
5. Введение знака в системе остаточных классов при одном из оснований равном 2.
6. Правило сложения чисел разных знаков в системе остаточных классов.
7. Правило умножения чисел разных знаков в системе остаточных классов.
8. Введение знака в системе остаточных классов с нечетными основаниями.
9. Оптимальный выбор системы оснований системы остаточных классов.
10. Построение многоступенчатой системы остаточных классов.
11. Позиционные характеристики модулярного кода.
12. Ранг числа и его свойства.
13. Теорема о ранге суммы.
14. Вычисление ранга числа.
15. Расширенное представление числа. Ключ инверсного представления.
16. Ортогональные и псевдоортогональные числа.
17. Ядро, коррекция ранга и характер числа.
18. Перевод чисел из модулярного кода в позиционный методом ортогональных базисов.
19. Перевод чисел из модулярного кода в обобщенную позиционную систему счисления.
20. Интервальные методы перевода из модулярного кода в позиционный.
21. Расширение системы оснований, опирающееся на ранг и след числа.
22. Расширение системы оснований с помощью характеристик обобщенной позиционной системы.
23. Алгоритм деления чисел на основания модулярного кода с помощью перевода в обобщенной позиционной системы.
24. Алгоритм деления с помощью характеристик ранг и след числа.
25. Масштабирование чисел в системе остаточных классов.
26. Формальное деление в системе остаточных классов.
27. Деление на фиксированное число.
28. Деление на основание модулярного кода.
29. Общий случай деления.
30. Основные факты, характеризующие корректирующие свойства кодов

31. Корректирующие свойства кодов в СОК.
32. Корректирующие свойства R – кодов.
33. Геометрическая модель избыточного кода в СОК.
34. Обнаружение и локализация ошибок в СОК
35. Построение СОК в комплексной области на основе теоремы Гаусса.
36. Отображение комплексного числа на пары действительных чисел.
37. Метод представления комплексных чисел в СОК, опирающийся на их представление в виде матрицы
38. Построение системы остаточных классов для гиперкомплексных чисел.
39. Применение системы остаточных классов в цифровой обработке сигналов.
40. Применение системы остаточных классов в задачах защиты информации.

Критерии оценивания

Оценка «отлично» выставляется студенту, если теоретическое содержание курса освоено полностью, без пробелов; исчерпывающе, последовательно, четко и логически стройно излагает материал; свободно справляется с задачами, вопросами и другими видами применения знаний; использует в ответе дополнительный материал все предусмотренные программой задания выполнены, качество их выполнения оценено числом баллов, близким к максимальному; анализирует полученные результаты; проявляет самостоятельность при выполнении заданий.

Оценка «хорошо» выставляется студенту, если теоретическое содержание курса освоено полностью, необходимые практические компетенции в основном сформированы, все предусмотренные программой обучения учебные задания выполнены, качество их выполнения достаточно высокое. Студент твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос.

Оценка «удовлетворительно» выставляется студенту, если теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, большинство предусмотренных программой заданий выполнено, но в них имеются ошибки, при ответе на поставленный вопрос студент допускает неточности, недостаточно правильные формулировки, наблюдаются нарушения логической последовательности в изложении программного материала.

Оценка «неудовлетворительно» выставляется студенту, если он не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы, необходимые практические компетенции не сформированы, большинство предусмотренных

программой обучения учебных заданий не выполнено, качество их выполнения оценено числом баллов, близким к минимальному.

3.Методические рекомендации по подготовке реферата.

Для подготовки реферата по дисциплине необходимо:

1. Составить план работы. Правильно составленный план работы помогает систематизировать материал, обеспечивает последовательность его изложения. План работы составляется самостоятельно, с учетом замысла и индивидуального подхода. В процессе работы план работы может уточняться.

2. Грамотно подобрать литературные источники. Реферат выполняется на основе глубокого изучения литературных источников. Литература по теме реферата может быть подобрана студентом при помощи предметных и алфавитных каталогов библиотек. Для этих целей могут быть использованы каталоги книг, указатели журнальных статей, специальные библиографические справочники, тематические сборники литературы, периодически выпускаемые отдельными издательствами, интернет-сайты официальных организаций.

Проработка источников сопровождается выписками, конспектированием. Выписки из текста делают обычно в виде цитаты. После каждой цитаты приводится ссылка на автора и источник. Поэтому при выписке цитат и конспектировании следует делать ссылки: автор, название издания, место издания, издательство, год издания, номер страницы. Конспект может содержать в себе факты, доказательства, примеры, основные положения и выводы автора, а также личное отношение студента к изученному материалу.

Рациональной и эффективной организации исследовательской деятельности способствует составление студентом собственной картотеки проработанных по теме и смежным вопросам литературных источников. Картотека не только помогает получить представление о степени изученности данной проблемы, но и позволяет работать с литературой более целеустремленно.

3.Оформление реферата осуществляется в соответствии с требованиями государственных стандартов.

4. Темы рефератов.

1. Полиномиальная система классов вычетов.
2. Применение модулярной арифметики в задачах распараллеливания алгоритмов вычисления свертки.
3. Применение модулярной арифметики в задачах распараллеливания алгоритмов ортогональных преобразований цифровой обработки сигналов.
4. Сравнительная характеристика различных методов обменных операций между модулярным и позиционным кодом.
5. Оценка избыточности модулярного кода.
6. Оценка сложности алгоритмов модулярной арифметики.

Критерии оценки:

Оценка «отлично» выставляется студенту, если: он безукоризненно изложил теоретический материал реферата, достиг целей, поставленных в реферате, оформил его в соответствии со стандартами. Возможны одна - две неточности при освещении второстепенных вопросов или выкладках, которые студент легко исправил после замечания преподавателя

Оценка «хорошо» выставляется студенту, если: он показал систематический характер знаний материала реферата, достиг целей, поставленных в реферате, но не соблюдал правил оформления в соответствии со стандартами. Допускал неточности в изложении материала.

Оценка «удовлетворительно» выставляется студенту, если: он допустил погрешности в докладе, не достиг всех целей реферата, слабо осветил поставленную тематику. Не соблюдал требований стандартов для оформления работы.

Оценка «неудовлетворительно» выставляется студенту, если: он обнаружил пробелы в знаниях, не достиг целей реферата, не раскрыл тему реферата. Оформление реферата вне соответствий требованиям государственных стандартов.