ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ ЛЕНИНГРАДСКОЙ ОБЛАСТИ

**«ЛЕНИНГРАДСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ**

**ИМЕНИ А.С. ПУШКИНА»**

УТВЕРЖДАЮ

Проректор по учебно-методической

работе

\_\_\_\_\_\_\_\_\_\_\_\_ С.Н. Большаков

РАБОЧАЯ ПРОГРАММА

дисциплины

**Б1.О.02.09 АБСТРАКТНАЯ И КОМПЬЮТЕРНАЯ АЛГЕБРА**

Направление подготовки **09.03.03 Прикладная информатика**

Направленность (профиль) **Прикладная информатика в экономике**

(год начала подготовки – 2022)

Санкт-Петербург

2022

**1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ**

Процесс изучения дисциплины направлен на формирование следующих компетенций:

|  |  |  |
| --- | --- | --- |
| Индекс компетенции | Содержание компетенции(или ее части) | Индикаторы компетенций (код и содержание) |
| УК-1 | Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач | ИУК-1.1. Знает понятие «системный подход».ИУК-1.2. Умеет осуществлять поиск, критический анализ и синтез информации.ИУК-1.3. Владеет навыками применения системного подхода для решения поставленных задач. |
| ОПК-1 | Способен применять естественнонаучные и общеинженерные знания, методы математического анализа и моделирования, теоретического и экспериментального исследования в профессиональной деятельности; | ИОПК-1.1. Знает понятийный аппарат естественнонаучных и общеинженерных дисциплин.ИОПК-1.2. Умеет применять методы математического анализа и моделирования в профессиональной деятельности.ИОПК-1.3. Владеет навыками организации теоретического и экспериментального исследования в профессиональной деятельности. |
| ПК-10 | Способен применять системный подход и математические модели в формализации решения прикладных задач | ИПК-10.1. Знает виды математических моделей.ИПК-10.2. Умеет формализовывать решение прикладной задачи.ИПК-10.3. Владеет навыками применения системного подхода и математические моделей в формализации решения прикладных задач. |

**2. Место дисциплины в структуре ОП**

**Цель дисциплины:** ознакомить обучаемых с характеристикой основных понятий абстрактной алгебры.

**Задачи дисциплины:**

* знакомство с алгоритмами символьных преобразований.
* формирование знаний, умений и навыков в области теории кодирования и передачи информации.

Курс «Абстрактная и компьютерная алгебра» входит в состав цикла Б1 и является одной из обязательных дисциплин учебного плана **09.03.03 Прикладная информатика.** Данной дисциплиной закладываются основы решения математических задач путём символьного преобразования математических выражений.

**3. Объем дисциплины и виды учебной работы**

Общая трудоемкость освоения дисциплины составляет 2 зачетных единиц,
72 академических часа *(1 зачётная единица соответствует 36 академическим часам)*.

Очная форма обучения

|  |  |
| --- | --- |
| Вид учебной работы | Трудоемкость в акад.час |
|  |  | Практическая подготовка |
| **Контактная работа (аудиторные занятия) (всего):** | 36 |
| в том числе: |  |
| Лекции | 12 | - |
| Лабораторные работы / Практические занятия (в т.ч. зачет) | 24/- | -/- |
| **Самостоятельная работа (всего)** | 36 |
| **Вид промежуточной аттестации (экзамен):** | - |
| контактная работа | - |
| самостоятельная работа по подготовке к экзамену | - |
| **Общая трудоемкость дисциплины (в час. /з.е.)** | 72/2 |

Заочная форма обучения

|  |  |
| --- | --- |
| Вид учебной работы | Трудоемкость в акад.час |
|  |  | Практическая подготовка |
| **Контактная работа (аудиторные занятия) (всего):** | 12 |
| в том числе: |  |
| Лекции | 4 | - |
| Лабораторные работы/ Практические занятия | 8/- | -/- |
| **Самостоятельная работа (всего)** | 56 | - |
| **Вид промежуточной аттестации (зачет):** | 4 | - |
| контактная работа | 0,25 | - |
| самостоятельная работа по подготовке к зачету | 3,75 | - |
| **Вид промежуточной аттестации (экзамен):** | - |
| контактная работа | - |
| самостоятельная работа по подготовке к экзамену | - |
| **Общая трудоемкость дисциплины (в час. /з.е.)** | 72/2 |

**4. Содержание дисциплины**

При проведении учебных занятий обеспечивается развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств (включая при необходимости проведение интерактивных лекций, групповых дискуссий, ролевых игр, тренингов, анализ ситуаций и имитационных моделей, составленных на основе результатов научных исследований, проводимых организацией, в том числе с учетом региональных особенностей профессиональной деятельности выпускников и потребностей работодателей).

**4.1. Разделы (блоки) дисциплины**

|  |  |
| --- | --- |
| **№** | **Наименование блока (раздела) дисциплины** |
| 1 | Группы, кольца, идеалы, фактор кольца |
| 2 | Кольцо целых чисел. Теория делимости в кольце целых чисел. |
| 3 | Кольцо многочленов от одной переменной. Теория делимости |
| 4 | Алгебраические методы в теории кодирования и защиты информации. |
| 5 | Поля. Расширения полей. Алгебраические и конечные расширения |

**4.2. Примерная тематика курсовых работ (проектов):**

Курсовая работа по дисциплине не предусмотрена учебным планом.

**4.3. Перечень занятий, проводимых в активной и интерактивной формах, обеспечивающих развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств**

| **№ п/п** | **Наименование блока (раздела) дисциплины** | **Занятия, проводимые в активной и интерактивной формах** | **Практическая подготовка** |
| --- | --- | --- | --- |
| **Форма проведения занятия** | **Наименование видов занятий** |
| 1. | Группы, кольца, идеалы, фактор кольца | лекционное занятие | Использование презентаций |  |
| лабораторное занятие | Решение ситуационных задач, работа в группах |  |
| 2 | Кольцо целых чисел. Теория делимости в кольце целых чисел | лекционное занятие | Использование презентаций |  |
| лабораторное занятие | Решение ситуационных задач, работа в группах |  |
| 3 | Кольцо многочленов от одной переменной. Теория делимости | лекционное занятие | Использование презентаций |  |
| лабораторное занятие | Решение ситуационных задач, работа в группах |  |
| 4 | Алгебраические методы в теории кодирования и защиты информации | лекционное занятие | Использование презентаций |  |
| лабораторное занятие | Решение ситуационных задач, работа в группах |  |
| 5 | Поля. Расширения полей. Алгебраические и конечные расширения | лекционное занятие | Использование презентаций |  |
| лабораторное занятие | Решение ситуационных задач, работа в группах |  |

**5. Учебно-методическое обеспечение для самостоятельной работы обучающихся по дисциплине**

**5.1. Темы для творческой самостоятельной работы обучающегося**

Темы для творческой самостоятельной работы студента формулируются обучающимся самостоятельно, исходя из перечня тем занятий текущего семестра.

**5.2. Темы конспектов**

1. Определение бинарной алгебраической операции. Алгебраические структуры с одной бинарной операцией.
2. Понятие группы. Примеры и свойства групп.
3. Подгруппы. Нормальные подгруппы и факторгруппы.
4. Гомоморфизмы групп. Изоморфизмы.
5. Алгебраические структуры с двумя бинарными алгебраическими операциями.
6. Понятие кольца. Примеры и свойства колец.
7. Подкольца. Идеалы кольца. Фактор-кольца.
8. Понятие поля. Числовые поля.
9. Кольцо целых чисел. Отношение делимости, его простейшие свойства.
10. Теорема о делении с остатком.
11. Кольцо классов вычетов.
12. НОД, НОК: Алгоритм Евклида и теорема Ламе; расширенный алгоритм Евклида; Алгоритм Евклида и цепные дроби.
13. Простые числа. Разложение целых чисел на множители; разложение больших целых чисел на множители.
14. Точные вычисления, использующие модулярную арифметику.
15. Представление больших целых чисел в памяти компьютера.
16. Извлечение корней из больших целых чисел.
17. Проверка свойств больших целых чисел.
18. Построение кольца многочленов над полем. Отношение делимости многочленов.
19. Теорема о делении с остатком.
20. Деление на двучлен, схема Горнера, формула Тейлора.
21. Корни многочлена, теорема Безу.
22. НОД и НОК многочленов. Алгоритм Евклида и его следствия.
23. Взаимно простые многочлены. Приводимые и неприводимые многочлены.
24. Разложение на неприводимые множители, единственность разложения.
25. Понятие о многочленах от нескольких переменных.
26. Криптология. Два семейства кодов. Модель системы связи.
27. Понятие кодирования. Скорость передачи информации кода.
28. Определение (n,k)-кода. Вектор ошибок.
29. Расстояние Хэмминга. Вес Хэмминга. Лемма об исправлении ошибок.
30. Кодовое расстояние двоичного кода. Теорема о кодовом расстоянии.
31. Теорема (верхняя граница Хэмминга числа кодовых слов).
32. Код с одной проверкой на чётность. Проверочные уравнения. Проверочная матрица. Порождающая матрица.
33. Упорядоченный код. Теорема о проверочной матрице.
34. Теорема о минимальном весе.
35. Синдром вектора.
36. Нахождение ошибки в сообщении, используя код Хэмминга с проверочной матрицей.
37. БЧХ-коды. Принцип построения циклических кодов.
38. Матричное представление циклических кодов. Нахождение порождающей матрицы. Получение разрешённых кодовых комбинаций. Матричное представление циклических кодов. Выбор образующего полинома.
39. Обнаружение и исправление ошибочной цифры.
40. Алгоритмы символьных преобразований
41. Определение алгебраических и трансцендентных чисел над полем.
42. Конечные расширения поля.
43. Конечные поля.

**5.3. Вопросы для подготовки к устным собеседованиям (опросам):**

**Тема 1. Группы, кольца, идеалы, фактор кольца**

1. Определение бинарной алгебраической операции. Алгебраические структуры с одной бинарной операцией.
2. Понятие группы. Примеры и свойства групп.
3. Подгруппы. Нормальные подгруппы и факторгруппы.
4. Гомоморфизмы групп. Изоморфизмы.
5. Алгебраические структуры с двумя бинарными алгебраическими операциями.
6. Понятие кольца. Примеры и свойства колец.
7. Подкольца. Идеалы кольца. Фактор-кольца.
8. Понятие поля. Числовые поля.

**Тема 2. Кольцо целых чисел. Теория делимости в кольце целых чисел**

1. Кольцо целых чисел. Отношение делимости, его простейшие свойства.
2. Теорема о делении с остатком.
3. Кольцо классов вычетов.
4. НОД, НОК: Алгоритм Евклида и теорема Ламе; расширенный алгоритм Евклида; Алгоритм Евклида и цепные дроби.
5. Простые числа. Разложение целых чисел на множители; разложение больших целых чисел на множители.
6. Точные вычисления, использующие модулярную арифметику.
7. Представление больших целых чисел в памяти компьютера.
8. Извлечение корней из больших целых чисел.
9. Проверка свойств больших целых чисел.

**Тема 3. Кольцо многочленов от одной переменной. Теория делимости.**

1. Построение кольца многочленов над полем. Отношение делимости многочленов.
2. Теорема о делении с остатком.
3. Деление на двучлен, схема Горнера, формула Тейлора.
4. Корни многочлена, теорема Безу.
5. НОД и НОК многочленов. Алгоритм Евклида и его следствия.
6. Взаимно простые многочлены. Приводимые и неприводимые многочлены.
7. Разложение на неприводимые множители, единственность разложения.
8. Понятие о многочленах от нескольких переменных.

**Тема 4. Алгебраические методы в теории кодирования и защиты информации.**

1. Криптология. Два семейства кодов. Модель системы связи.
2. Понятие кодирования. Скорость передачи информации кода.
3. Определение (n,k)-кода. Вектор ошибок.
4. Расстояние Хэмминга. Вес Хэмминга. Лемма об исправлении ошибок.
5. Кодовое расстояние двоичного кода. Теорема о кодовом расстоянии.
6. Теорема (верхняя граница Хэмминга числа кодовых слов).
7. Код с одной проверкой на чётность. Проверочные уравнения. Проверочная матрица. Порождающая матрица.
8. Упорядоченный код. Теорема о проверочной матрице.
9. Теорема о минимальном весе.
10. Синдром вектора.
11. Нахождение ошибки в сообщении, используя код Хэмминга с проверочной матрицей.
12. БЧХ-коды. Принцип построения циклических кодов.
13. Матричное представление циклических кодов. Нахождение порождающей матрицы. Получение разрешённых кодовых комбинаций. Матричное представление циклических кодов. Выбор образующего полинома.
14. Обнаружение и исправление ошибочной цифры.
15. Алгоритмы символьных преобразований

**Тема 5. Поля. Расширения полей. Алгебраические и конечные расширения.**

1. Определение алгебраических и трансцендентных чисел над полем.
2. Конечные расширения поля.
3. Конечные поля.

**5.4. Вопросы для подготовки к коллоквиумам:**

**Коллоквиум №1**

**Тема 1. Группы, кольца, идеалы, фактор кольца**

1. Определение бинарной алгебраической операции. Алгебраические структуры с одной бинарной операцией.
2. Понятие группы. Примеры и свойства групп.
3. Подгруппы. Нормальные подгруппы и факторгруппы.
4. Гомоморфизмы групп. Изоморфизмы.
5. Алгебраические структуры с двумя бинарными алгебраическими операциями.
6. Понятие кольца. Примеры и свойства колец.
7. Подкольца. Идеалы кольца. Фактор-кольца.
8. Понятие поля. Числовые поля.

**Коллоквиум №2**

**Тема 2. Кольцо целых чисел. Теория делимости в кольце целых чисел**

1. Кольцо целых чисел. Отношение делимости, его простейшие свойства.
2. Теорема о делении с остатком.
3. Кольцо классов вычетов.
4. НОД, НОК: Алгоритм Евклида и теорема Ламе; расширенный алгоритм Евклида; Алгоритм Евклида и цепные дроби.
5. Простые числа. Разложение целых чисел на множители; разложение больших целых чисел на множители.
6. Точные вычисления, использующие модулярную арифметику.
7. Представление больших целых чисел в памяти компьютера.
8. Извлечение корней из больших целых чисел.
9. Проверка свойств больших целых чисел.

**Коллоквиум №3**

**Тема 3. Кольцо многочленов от одной переменной. Теория делимости.**

1. Построение кольца многочленов над полем. Отношение делимости многочленов.
2. Теорема о делении с остатком.
3. Деление на двучлен, схема Горнера, формула Тейлора.
4. Корни многочлена, теорема Безу.
5. НОД и НОК многочленов. Алгоритм Евклида и его следствия.
6. Взаимно простые многочлены. Приводимые и неприводимые многочлены.
7. Разложение на неприводимые множители, единственность разложения.
8. Понятие о многочленах от нескольких переменных.

**Коллоквиум №4**

**Тема 4. Алгебраические методы в теории кодирования и защиты информации.**

1. Криптология. Два семейства кодов. Модель системы связи.
2. Понятие кодирования. Скорость передачи информации кода.
3. Определение (n,k)-кода. Вектор ошибок.
4. Расстояние Хэмминга. Вес Хэмминга. Лемма об исправлении ошибок.
5. Кодовое расстояние двоичного кода. Теорема о кодовом расстоянии.
6. Теорема (верхняя граница Хэмминга числа кодовых слов).
7. Код с одной проверкой на чётность. Проверочные уравнения. Проверочная матрица. Порождающая матрица.
8. Упорядоченный код. Теорема о проверочной матрице.
9. Теорема о минимальном весе.
10. Синдром вектора.
11. Нахождение ошибки в сообщении, используя код Хэмминга с проверочной матрицей.
12. БЧХ-коды. Принцип построения циклических кодов.
13. Матричное представление циклических кодов. Нахождение порождающей матрицы. Получение разрешённых кодовых комбинаций. Матричное представление циклических кодов. Выбор образующего полинома.
14. Обнаружение и исправление ошибочной цифры.
15. Алгоритмы символьных преобразований

**Коллоквиум №2**

**Тема 5. Поля. Расширения полей. Алгебраические и конечные расширения.**

1. Определение алгебраических и трансцендентных чисел над полем.
2. Конечные расширения поля.
3. Конечные поля.

**6. Оценочные средства для текущего контроля успеваемости**

**6.1. Текущий контроль**

|  |  |  |
| --- | --- | --- |
| №пп | № и наименование блока (раздела) дисциплины | Форма текущего контроля |
| 1 | Группы, кольца, идеалы, фактор кольца | Устное собеседованиеОтчёт по лабораторной работеКоллоквиум №1 |
| 2 | Кольцо целых чисел. Теория делимости в кольце целых чисел. | Устное собеседованиеОтчёт по лабораторной работеКонтрольная работа № 1Коллоквиум №2 |
| 3 | Кольцо многочленов от одной переменной. Теория делимости | Устное собеседованиеОтчёт по лабораторной работеКонтрольная работа № 2Коллоквиум №3 |
| 4 | Алгебраические методы в теории кодирования и защиты информации. | Устное собеседованиеОтчёт по лабораторной работеКонтрольная работа № 3Коллоквиум №4 |
| 5 | Поля. Расширения полей. Алгебраические и конечные расширения | Устное собеседованиеОтчёт по лабораторной работеКоллоквиум №5 |

**6.2. Примеры оценочных средств для текущего контроля**

**Темы конспектов**

Представлены в разделе 5.2.

**Вопросы для проведения устных опросов**

Представлены в разделе 5.3.

**Вопросы для сдачи коллоквиумов**

Представлены в разделе 5.4.

**Задания для лабораторных работ**

**Алгебраические действия. Свойства действий. Группы, кольца**

**1.**Используя систему GAP, проверьте свойства таблично заданного действия (коммутативность, ассоциативность, наличие нейтрального элемента, наличие нулевого элемента (*z* — нулевой элемент, если для всех *m*∈*M* выполнено *z* \* *m* = *m* \* *z* = *z*) , обратный элемент):

|  |  |  |  |
| --- | --- | --- | --- |
| **\*** | **1** | **2** | **3** |
| **1** | 1 | 1 | 3 |
| **2** | 2 | 2 | 3 |
| **3** | 3 | 3 | 3 |

**2.**Задайте группоид, в котором коммутативность не выполняется. Найдите все пары, для которых коммутативность не выполняется, и проверьте коммутативность для каждой найденной пары.

**3.** Задайте группоид, обладающий нейтральным элементом. Для каждого элемента множества найдите обратный элемент.

**4.** Задайте группоид, обладающий свойством коммутативности и нулевым элементом.

**5.**Задайте группоид, в котором не выполнено свойство ассоциативности. Найдите все тройки, для которых ассоциативность не выполняется, и проверьте ассоциативность для каждой найденной тройки.

**6.**Задайте группоид, в котором выполнено свойство ассоциативности. Проверьте, является ли он полугруппой и моноидом.

**Теория делимости в кольце целых чисел**

# I. Воспользовавшись стандартными функциями GAP, выполните следующие задания:

**1.** Вычислите наибольший общий делитель чисел 1232 и 786. Укажите коэффициенты линейного выражения НОД.

**2.** Вычислите наименьшее общее кратное чисел 456, 128 и 1286.

**3.** Вычислите 13 простое число.

**4.** Проверьте, является ли число 1345667889 простым.

**5.** Проверьте, является ли число 4567 степенью простого числа.

**6.** Найдите количество делителей числа 128765, выведите их список и вычислите сумму.

**7.** Разложите число 546436 на множители.

# II. Разработайте функции GAP для решения следующих задач:

**1.** Найдите количество натуральных чисел, меньших заданного числа *a* и имеющих с ним наибольшим общим делителем заданное число *b*.

**2.** Разработайте функцию для определения количества делителей натурального числа.

*Указание:* используйте функции **DivisorsInt** и **Length**

**3.** Разработайте собственную функцию для разложения числа на простые множители.

**4.** Напишите программу, которая определяет, можно ли заданное натуральное число *М* представить в виде произведения простого и составного чисел.

**Полиномы. Делимость полиномов**

**I.** Воспользовавшись стандартными функциями GAP, выполните следующие задания:

**1.** Для заданного полинома :

**1.1.** Найдите рациональные корни.

**1.2.** Определите промежутки монотонности.

**1.3.** Определите промежутки выпуклости/вогнутости.

**1.4.** Выполните разложение на множители.

**2.** Для заданных полиномов

:

**2.1.** Найдите частное и остаток от деления.

**2.2.** Найдите НОД и его линейное разложение.

**2.3.** Найдите НОК.

**2.4.** Проверьте ассоциированность.

**II.** Разработайте функции GAP для решения следующих задач:

**1.** Разработайте функцию, которая определяет, положительно ли значение заданного многочлена *f*(*x*) в заданной точке *a*, и в случае отрицательного ответа возвращает значение производной многочлена *f*(*x*) в точке *a*, а в случае положительного — значение многочлена *f*(*x*) в точке *a*.

**2.**Разработайте функцию, которая определяет, равен ли единице старший коэффициент заданного многочлена *f*(*x*), и в случае положительного ответа возвращает исходный многочлен, а в случае отрицательного — многочлен, полученный из многочлена *f*(*x*) делением его на свой старший коэффициент.

**3.** Разработайте функцию, которая определяет, отличаются ли степени заданных многочленов *f*(*x*) и *g*(*x*) на 1, и в случае отрицательного ответа возвращает сумму многочленов, а в случае положительного — произведение.

**Алгебраические методы в теории кодирования и защиты информации**

**1.** Построить самокорректирующийся код Хэмминга для слов длины 4.

**2.** Обнаружить и исправить ошибку при передаче кодовых слов  из кода Хэмминга :



**3.** Дана порождающая матрица G.



**1.** Приведите порождающую матрицу G к виду G=(IkP).

**2.** Найдите кодовые слова. Сколько их должно быть?

**3.** Найдите проверочную матрицу.

**4.** Полученный вектор имеет вид: v=(0,0,1,1,0). Найдите переданный вектор.

**4.** Пусть *g(х)=x3+х2+1 —* порождающий полином кода (7,4). Найдите код сообщения (1,0,1,0).

**Поля. Расширения полей**

**1.**Найдите неприводимый примитивный многочлен степени *n*=2 с наименьшим лексикографическим номером над полем *F*5.

**2.**Убедитесь в том, что многочлен  является неприводимым и примитивным над полем *F*5.

# Задания для контрольной работы №1

**1.**Используя функции GAP, проверьте справедливость следующих утверждений:

|  |  |  |
| --- | --- | --- |
| 1) 12∈N;2) -100∈Z; | 3) -11∈Q+;4) 2,5∈Q-; | 5) 0∈N;6) -5∈Q; |

**2.** Вычислите значение следующей функции:



**3.**Используя систему GAP, проверьте свойства таблично заданного действия (коммутативность, ассоциативность, наличие нейтрального элемента, наличие нулевого элемента (*z* — нулевой элемент, если для всех *m*∈*M* выполнено *z* \* *m* = *m* \* *z* = *z*) , обратный элемент):

|  |  |  |  |
| --- | --- | --- | --- |
| **\*** | **1** | **2** | **3** |
| **1** | 1 | 1 | 1 |
| **2** | 1 | 2 | 3 |
| **3** | 3 | 2 | 1 |

**4.**Вычислите наибольший общий делитель чисел 5432 и 867. Укажите коэффициенты линейного выражения НОД.

**5.**Вычислите наименьшее общее кратное чисел 561, 1284 и 786.

**6.**Вычислите 30 простое число.

**7.** Проверьте, является ли число 77668899 простым.

**8.**Найдите количество делителей числа 8765, выведите их список и вычислите сумму.

**9.**Разложите число 89765 на множители.

**10.**Найдите первую степень числа 5, превышающую данное целое число *a*.

**Задания для контрольной работы №2**

**1.**Проверьте, сравнимы ли 54389 и 7856 по модулю 12.

**2.** Найдите наименьший примитивный корень по модулю 29.

**3.**Дано натуральное число *n*. Найдите произведение простых чисел из промежутка [1..*m*], не сравнимых с числом *n* по указанному модулю.

**4.** Вычислите 4-1(mod 13).

**5.** Задано кольцо Z11.

**5.1.** Найдите группу обратимых элементов кольца (U11).

**5.2.** Определите количество примитивных корней по модулю 11.

**5.3.** Найдите примитивные корни по модулю 11.

**6.** Решите систему сравнений:

****

**7.** Разработайте функцию, которая определяет, четна ли степень произведения заданных многочленов *f*(*x*) и *g*(*x*), и в случае отрицательного ответа возвращает НОД многочленов, а в случае положительного — НОК.

**8.** Для заданных полиномов

:

**8.1.** Найдите частное и остаток от деления.

**8.2.** Найдите НОД и его линейное разложение.

**8.3.** Найдите НОК.

**8.4.** Найдите рациональные корни.

**8.5.** Выполните разложение на множители.

**9.**Даны матрицы  Выполните следующие действия:

**9.1.** Вычислите *A*+*B*, *A*-*B*, *A*\**B*, 2\**A*, *B*-5.

**9.2.** Найдите обратную матрицу для *А*.

**9.3.** Транспонируйте матрицу *B*.

**9.4.** Вычислите ранг матрицы *А*.

**9.5.** Решите матричные уравнения .

**Задания для контрольной работы №3**

**1.** Построить самокорректирующийся код Хэмминга для слов длины 4.

**2.** Обнаружить и исправить ошибку при передаче кодовых слов  из кода Хэмминга :



**3.** Дана порождающая матрица G.



**1.** Приведите порождающую матрицу G к виду G=(IkP).

**2.** Найдите кодовые слова. Сколько их должно быть?

**3.** Найдите проверочную матрицу.

**4.** Полученный вектор имеет вид: v=(0,0,1,1,0). Найдите переданный вектор.

**4.** Пусть *g(х)=x3+х2+1 —* порождающий полином кода (7,4). Найдите код сообщения (1,0,1,0).

**7. ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ**

| **№ п/п** | **Наименование** | **Авторы** | **Место издания** | **Год издания** | **Наличие** |
| --- | --- | --- | --- | --- | --- |
| **печатные издания** | **ЭБС (адрес в сети Интернет)** |
| 1. | Элементы абстрактной и компьютерной алгебры: учебное пособие | Царев А. В., Шеина Г. В. | М.: Московский педагогический государственный университет (МПГУ) | 2016 |  | <https://biblioclub.ru> |
| 2. | Компьютерная алгебра в задачах: учебное пособие | Шилин И. А. | М.: Московский педагогический государственный университет (МПГУ) | 2018 |  | <https://biblioclub.ru> |
| 3. | Числовые системы: учебное пособие | Смолин Ю. Н. | Москва: ФЛИНТА | 2021 |  | <https://biblioclub.ru> |

**8. Ресурсы информационно-телекоммуникационной сети «Интернет»**

***Информационно-справочные ресурсы сети интернет:***

1. GAP System for Computational Discrete Algebra: [сайт]. URL: http://www.gap-system.org/

2. Образовательный математический сайт EXPonenta.ru: [сайт]. URL: http://www.exponenta.ru/

***Электронные библиотеки:***

1. «НЭБ». Национальная электронная библиотека. – Режим доступа: http://нэб.рф/

2. «eLibrary». Научная электронная библиотека. – Режим доступа: https://elibrary.ru

3. «КиберЛенинка». Научная электронная библиотека. – Режим доступа: https://cyberleninka.ru/

4. ЭБС «Университетская библиотека онлайн». – Режим доступа: http://www.biblioclub.ru/

5. Российская государственная библиотека. – Режим доступа: http://www.rsl.ru/

**9. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, ИСПОЛЬЗУЕМЫЕ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ**

В ходе осуществления образовательного процесса используются следующие информационные технологии:

- средства визуального отображения и представления информации (LibreOffice) для создания визуальных презентаций как преподавателем (при проведении занятий) так и обучаемым при подготовке докладов для семинарского занятия.

- средства телекоммуникационного общения (электронная почта и т.п.) преподавателя и обучаемого.

- использование обучаемым возможностей информационно-телекоммуникационной сети «Интернет» при осуществлении самостоятельной работы.

**9.1. Требования к программному обеспечению учебного процесса**

Для успешного освоения дисциплины, обучающийся использует следующие программные средства:

* Windows 10 x64
* MicrosoftOffice 2016
* LibreOffice
* Mozilla Firefox
* Система компьютерной алгебры GAP

**9.2. Информационно-справочные системы (при необходимости)**

Не используются.

**10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ:**

Для проведения занятий лекционного типа предлагаются наборы демонстрационного оборудования и учебно-наглядных пособий.

Для изучения дисциплины используется следующее оборудование: аудитория, укомплектованная мебелью для обучающихся и преподавателя, доской, ПК с выходом в интернет, мультимедийным проектором и экраном.

Для самостоятельной работы обучающихся используется аудитория, укомплектованная специализированной мебелью и техническими средствами (ПК с выходом в интернет и обеспечением доступа в электронно-информационно-образовательную среду организации).