

МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Алтайский государственный гуманитарно-педагогический университет имени В.М. Шукшина»
(АГГПУ имени В.М. Шукшина)

Кафедра математики, физики, информатики

Утверждаю
проректор по учебной работе
М.В. Довыдова
«26» августа 2022 г.



РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Б1.О.11 АБСТРАКТНАЯ И КОМПЬЮТЕРНАЯ АЛГЕБРА

Направление подготовки	44.03.05 Педагогическое образование (с двумя профилями подготовки)
Профили подготовки	Технология и Информатика
Квалификация выпускника	бакалавр
Форма обучения	очная

Составитель:
канд. физ.-мат. наук, доцент

А.М. Ерёмин

Бийск 2022

РЕКОМЕНДОВАНО К ИСПОЛЬЗОВАНИЮ В УЧЕБНОМ ПРОЦЕССЕ

на заседании кафедры математики, физики, информатики

(протокол от 22 июня 2022 г. № 9)

Заведующий кафедрой

математики, физики, информатики



Т.А. Гусева

1. ЦЕЛЬ И ЗАДАЧИ ДИСЦИПЛИНЫ

Цель дисциплины - формирование систематизированных знаний в области в области абстрактной и компьютерной алгебры, необходимых учителю для глубокого понимания курса информатики

Задачи дисциплины:

- формирование понятийного аппарата абстрактной алгебры, знаний и умений, необходимых для решения типовых задач данной предметной области;
- формирование теоретико-числовой культуры, необходимой будущему учителю для глубокого понимания теоретических основ школьного курса информатики;
- ознакомление учащихся с фундаментальной задачей компьютерной алгебры – представлением математических объектов в ЭВМ;
- формирование профессиональной предметной направленности знаний, умений и навыков, полученных при изучении дисциплины.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Абстрактная и компьютерная алгебра» относится к обязательной части профессионального цикла (Б1.О.11). Областью профессиональной деятельности бакалавров, на которую ориентирует дисциплина, является образование.

Освоение дисциплины готовит к работе со следующими объектами профессиональной деятельности бакалавров:

- обучение;
- воспитание;
- развитие;
- образовательные системы.

Профильной для данной дисциплины является профессиональная деятельность бакалавров.

Для освоения дисциплины студенты используют знания, умения и способы деятельности, сформированные в процессе изучения предметов «Математика» и «Информатика» на предыдущем уровне образования, а также знания, умения, навыки, способы деятельности и установки, полученные и сформированные в ходе изучения дисциплин: «Алгебра и геометрия», «Математический анализ и дифференциальные уравнения», «Программирование».

Освоение данной дисциплины является необходимой основой для изучения по учебному плану смежных с ней и последующих дисциплин: методика обучения информатике, теоретические основы информатики, методы и средства защиты информации, а также различных курсов по выбору, связанных с теоретическими основами информатики и системами компьютерной алгебры.

3. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Процесс изучения дисциплины направлен на формирование следующих **компетенций**:

- Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач (УК-1);
- Способен проектировать и реализовывать программу основного и среднего общего образования по предмету Информатика (ПК-3).

Наименование и код индикаторов достижения компетенций:

В результате изучения дисциплины обучающийся должен:

знать:

- УК-1.1 - знание механизмов и методик поиска, анализа и синтеза информации, включающие системный подход в области образования (З.1);
- УК-1.2 - знание методик постановки цели и способов её достижения, научного представления о результатах обработки информации (З.2);
- ПК-3.1 - знание теоретических основ информатики, принципов функционирования информационных систем и технологий (З.1).

уметь:

- УК-1.3 - умение анализировать задачу, выделять ее базовые составляющие, осуществлять декомпозицию задачи (У.1);
- УК-1.4 - умение находить и критически анализировать информацию, необходимую для решения поставленной задачи (У.2);
- УК-1.5 - умение рассматривать возможные варианты решения задачи, оценивая их достоинства и недостатки (У.3).

владеть:

- УК-1.6 - владение методами установления причинно-следственных связей и определения наиболее значимых среди них (В.1);
- УК-1.7 - владение механизмами поиска информации в том числе с применением современных информационных и коммуникационных технологий (В.2).

4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общая трудоемкость дисциплины составляет 3 зачетные единицы.

Вид учебной работы	Всего часов	Семестр	
		3	4
Аудиторные занятия (всего)	40	16	24
В том числе:			
Лекции (Л)	14	6	8
Практические занятия (ПЗ)	26	10	16
Самостоятельная работа студентов (СРС) (всего)	41	20	21
В том числе:			
Подготовка к лекционным занятиям	8	4	4
Подготовка к практическим занятиям	12	6	6
Подготовка к теоретическим опросам	8	4	4
Подготовка к аудиторной контрольной работе	13	6	7
Выполнение индивидуальных домашних заданий и домашних контрольных работ	-	-	-
Подготовка к итоговому (семестровому) тесту	-	-	-
Вид промежуточной аттестации – Экзамен	Экзамен	-	Экзамен
Общая трудоемкость в часах:	108	36	72
Общая трудоемкость в зачетных единицах:	3	1	2

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

5.1. Содержание разделов (модулей) дисциплины

№ п/п	Наименование раздела (модуля) дисциплины	Содержание
1.	Алгебры	Алгебры с одной бинарной алгебраической операцией: полугруппы, группы. Бинарные алгебраические операции; виды бинарных операций. Понятие алгебры, алгебраической системы. Алгебры с одной бинарной алгебраической операцией. Полугруппы. Моноиды. Группы, примеры групп; аддитивная и мультипликативная формы записи групп. Простейшие свойства группы. Подгруппа; примеры подгрупп; критерий подгруппы. Алгебры с двумя бинарными алгебраическими операциями: кольца, поля. Кольцо; примеры колец. Простейшие свойства кольца. Подкольцо данного кольца. Определение поля; примеры полей. Простейшие свойства поля.
2.	Теория делимости в кольце целых чисел	Делимость целых чисел. НОД. Алгоритм Евклида. Отношение делимости в кольце целых чисел и его простейшие свойства; теорема о делении с остатком. Наибольший общий делитель. Алгоритм Евклида и его сложность; теорема Ламе. Линейное представление НОД; расширенный алгоритм Евклида. Взаимно простые числа. Наименьшее общее кратное; связь НОК и НОД. Линейные диофантовы уравнения. Простые и составные числа. Определение и свойства простых чисел. Признак простого числа. Основная теорема арифметики. Бесконечность множества простых чисел. Системы счисления. Систематические числа; операции над ними, перевод из одной системы в другую.

3.	Теория сравнений в кольце целых чисел	Отношение сравнения в кольце целых чисел. Теоремы Эйлера и Ферма Отношение сравнения в кольце целых чисел, его свойства. Кольцо классов вычетов Z_m. Поле классов вычетов по простому модулю Z_p. Функция Эйлера. Теоремы Эйлера и Ферма. Решение линейных сравнений. Китайская теорема об остатках. Модулярная арифметика. Точные вычисления, использующие модулярную арифметику. Представление больших целых чисел в памяти компьютера. Операции над большими целыми числами. Извлечение корней из больших целых чисел.
4.	Многочлены над полем	Кольцо многочленов от одной переменной над полем. Построение кольца многочленов от одной переменной над полем. Отношение делимости в кольце многочленов над полем. Теорема о делении с остатком. Деление на двучлен, теорема Безу, схема Горнера, формула Тейлора. Корни многочлена. НОД и НОК многочленов. Алгоритм Евклида. НОД и НОК многочленов. Алгоритм Евклида. Взаимно простые многочлены. Приводимые и неприводимые над данным полем многочлены. Разложение многочлена в произведение нормированных неприводимых множителей, единственность разложения. Многочлены над полями C, R, Q. Алгебраическая замкнутость поля комплексных чисел. Разложение многочлена над полем комплексных чисел в произведение линейных множителей. Формулы Виета. Сопряжённость мнимых корней многочлена с действительными коэффициентами. Решение уравнений третьей и четвертой степени. Рациональные корни многочлена с целыми коэффициентами. Компьютерное представление многочленов. Алгоритмы операций над многочленами. Полиномиальная арифметика: представление многочленов в виде списков; сложение, умножение и деление многочленов; разложение многочленов на множители; вычисление степеней; вычисление многочленов.

5.	Введение в теорию кодирования	Алфавитное кодирование. Помехоустойчивое кодирование. Алфавитное кодирование. Разделимые и префиксные схемы. Кодовое дерево. Неравенство Макмиллана. Помехоустойчивое кодирование. Кодирование с минимальной избыточностью. Кодовое расстояние. Коды с обнаружением и исправлением ошибок. Введение в криптографию. Симметричные и асимметричные криптосистемы. Криптосистемы с открытым и закрытым ключом. Электронная подпись.
----	--------------------------------------	---

5.2. Разделы дисциплин и виды занятий

№ п/п	Наименование раздела дисциплины	Лекц.	Практ. зан.	В том числе в интерактивной форме (час)	СРС	Всего
1.	Алгебры	2	4	Интерактивная лекция – 2 ч. Работа в малых группах – 2 ч.	10	16
2.	Теория делимости в кольце целых чисел	2	4	Интерактивная лекция – 2 ч. Работа в малых группах – 2 ч.	10	16
3.	Теория сравнений в кольце целых чисел	2	6	Интерактивная лекция – 2 ч. Работа в малых группах – 2 ч.	10	18
4.	Многочлены над полем	4	6	Интерактивная лекция – 2 ч. Работа в малых группах – 2 ч.	6	16
5.	Введение в теорию кодирования	4	6	Работа в малых группах – 2 ч.	5	15
	Экзамен	-	-	-	-	27
	Всего:	14	26	18	41	108
В том числе, использование интерактивных форм, технологий				Лек. 8	Прак. 10	

Лекции

№ п/п	Наименование раздела (модуля) дисциплины	Содержание
1-2	Алгебры	Алгебры с одной бинарной алгебраической операцией: полугруппы, группы. Бинарные алгебраические операции; виды бинарных операций. Понятие алгебры,

		алгебраической системы. Алгебры с одной бинарной алгебраической операцией. Полугруппы. Моноиды. Группы, примеры групп; аддитивная и мультипликативная формы записи групп. Простейшие свойства группы. Подгруппа; примеры подгрупп; критерий подгруппы. Алгебры с двумя бинарными алгебраическими операциями: кольца, поля. Кольцо; примеры колец. Простейшие свойства кольца. Подкольцо данного кольца. Определение поля; примеры полей. Простейшие свойства поля.
3-4	Теория делимости в кольце целых чисел	Делимость целых чисел. НОД. Алгоритм Евклида. Отношение делимости в кольце целых чисел и его простейшие свойства; теорема о делении с остатком. Наибольший общий делитель. Алгоритм Евклида и его сложность; теорема Ламе. Линейное представление наибольшего общего делителя. Взаимно простые числа. Наименьшее общее кратное; связь НОК и НОД. Простые и составные числа. Определение и свойства простых чисел. Признак простого числа. Основная теорема арифметики. Бесконечность множества простых чисел. Системы счисления. Систематические числа; операции над ними, перевод из одной системы в другую – <i>самостоятельно</i>
5-7	Теория сравнений в кольце целых чисел	Отношение сравнения в кольце целых чисел. Теоремы Эйлера и Ферма Отношение сравнения в кольце целых чисел, его свойства. Кольцо классов вычетов Z_m. Поле классов вычетов по простому модулю Z_p. Функция Эйлера. Теоремы Эйлера и Ферма. Решение линейных сравнений. Китайская теорема об остатках. Модулярная арифметика. Точные вычисления, использующие модулярную арифметику. Представление больших целых чисел в памяти компьютера. Операции над большими целыми числами. Извлечение корней из больших целых чисел.
8-10	Многочлены над полем	Кольцо многочленов от одной переменной над полем. Построение кольца многочленов от одной переменной над полем. Отношение делимости в кольце многочленов над полем. Теорема о делении с остатком. Деление на двучлен, теорема Безу, схема Горнера, формула Тейлора. Корни многочлена. НОД и НОК многочленов. Алгоритм Евклида. НОД и НОК многочленов. Алгоритм Евклида.

		Взаимно простые многочлены. Приводимые и неприводимые над данным полем многочлены. Разложение многочлена в произведение нормированных неприводимых множителей, единственность разложения. Многочлены над полями C, R, Q. Компьютерное представление многочленов. Алгоритмы операций над многочленами. Полиномиальная арифметика: представление многочленов в виде списков; сложение, умножение и деление многочленов; разложение многочленов на множители; вычисление степеней; вычисление многочленов.
11-13	Введение в теорию кодирования	Алфавитное кодирование. Помехоустойчивое кодирование. Алфавитное кодирование. Разделимые и префиксные схемы. Кодовое дерево. Неравенство Макмиллана. Помехоустойчивое кодирование. Кодирование с минимальной избыточностью. Кодовое расстояние. Коды с обнаружением и исправлением ошибок. Введение в криптографию. Симметричные и асимметричные криптосистемы. Криптосистемы с открытым и закрытым ключом. Введение в криптографию. Криптосистемы с открытым и закрытым ключом. Электронная подпись.

Практические занятия

№ п/п	Наименование раздела (модуля) дисциплины	Содержание
1-2	Алгебры	Алгебры с одной бинарной алгебраической операцией: полугруппы, группы. Алгебры с двумя бинарными алгебраическими операциями: кольца, поля.
3-6	Теория делимости в кольце целых чисел	Делимость целых чисел. НОД и НОК. Алгоритм Евклида. Простые и составные числа. Основная теорема арифметики. Системы счисления. Арифметические операции над систематическими числами. Перевод чисел из одной системы счисления в другую. Контрольная работа
7-9	Теория сравнений в кольце целых чисел	Отношение сравнения в кольце целых чисел. Функция Эйлера. Теоремы Эйлера и Ферма. Решение линейных сравнений. Китайская теорема об остатках. Модулярная арифметика. Точные вычисления, использующие модулярную арифметику.

10-12	Многочлены над полем	Теорема о делении с остатком. Деление на двучлен, теорема Безу, схема Горнера.
		НОД и НОК многочленов. Алгоритм Евклида. Многочлены над полями $\mathbb{C}, \mathbb{R}, \mathbb{Q}$.
		Полиномиальная арифметика: представление многочленов в виде списков; сложение, умножение и деление многочленов; разложение многочленов на множители; вычисление степеней; вычисление многочленов.
13-14	Введение в теорию кодирования	Криптосистемы с открытым и закрытым ключом. Электронная подпись.
		Итоговое тестирование по всем разделам дисциплины

6. ЛАБОРАТОРНЫЙ ПРАКТИКУМ

Лабораторный практикум по абстрактной и компьютерной алгебре учебным планом не предусмотрен

7. ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ ПРОЕКТОВ (РАБОТ)

Курсовой проект (работа) по абстрактной и компьютерной алгебре учебным планом не предусмотрен

8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) основная литература:

1. Смолин, Ю.Н. Алгебра и теория чисел [Текст]: учебное пособие / Ю.Н. Смолин. – М.: Флинта: Наука, 2016. – 464 с. **В библиотеке 2006 год!**
2. Смолин, Ю.Н. Алгебра и теория чисел [Электронный ресурс] учебное пособие для студентов физико-математических факультетов высших педагогических вузов / Ю. Н. Смолин. - 4-е изд., стер. - Электрон. текстовые дан. - М. : Флинта : Наука, 2012. - 464 с. **Если это электронный ресурс, должна быть рабочая ссылка на источник, который есть в библиотеке вуза.**
3. Шнеперман, Л.Б. Сборник задач по алгебре и теории чисел [Текст]: учебное пособие. 3-е изд., стер./ Л.Б. Шнеперман. - СПб.: Издательство «Лань», 2018.- 224 с.

1 и 2 книги подходят только для дополнительной литературы.

б) дополнительная литература:

4. Бухштаб, А.А. Теория чисел. [Текст]: учебное пособие для студентов вузов / А. А. Бухштаб. - 3-е изд., стер. - СПб. : Лань, 2008. - 384 с
5. Кострикин, А.И. Введение в алгебру. Часть I. Основы алгебры. [Текст]: учебник для вузов. / А.И. Кострикин. 2-е изд. испр.- М.: Физматлит, 2004.- 272с.
6. Крючков, Н.И. Крюčkова, В.В. Сборник заданий по алгебре. [Текст]: учебное пособие для вузов/ Н. И. Крючков, В. В. Крюčkова. – М.: Академия, 2007. – 192 с.
7. Матрос, Д.Ш. Элементы абстрактной и компьютерной алгебры [Текст]: учебное пособие для вузов по специальности 050202 (030100) "Информатика"/ Д. Ш. Матрос, Г. Б. Поднебесова. - М. : Академия, 2004. - 240 с.

8. *Нечаев, В.И.* Элементы криптографии: основы защиты информации [Текст]: учебное пособие для вузов / В. И. Нечаев. - М. : Высшая школа, 1999. - 109 с.
9. *Новиков, Ф.А.* Дискретная математика [Электронный ресурс]: учебник для вузов. 2-е изд. Стандарт третьего поколения/ Новиков Ф.А. – СПб.: Изд-во «Питер», 2013. – 400 с., УМО.
Новиков, Федор Александрович. Дискретная математика для программистов : учебное пособие для вузов по специальности "Информатика и вычислительная техника" / Ф. А. Новиков. - 3-е изд. - СПб. : Питер, 2008. - 384 с. - (Учебник для вузов). - ISBN 978-5-91180-759-7
10. Самсонов, Борис Борисович. Компьютерная математика [Текст] : основания информатики : учебное пособие для вузов / Б. Б. Самсонов, Е. М. Плохов, А. И. Филоненков. - Ростов н/Д : Феникс, 2002. - 512 с. : ил. - (Учебники и учебные пособия). - ISBN 5-222-02239-0
11. *Самсонов, Б.Б.* Теория информации и кодирование [Текст]: пособие для студентов вузов/ Б.Б. Самсонов, Е.М. Плохов, А.И. Филоненков. Т.В. Кречет. – Ростов-на-Дону: «Феникс», 2002. – 288 с.
12. *Сизый, С.В.* Лекции по теории чисел [Текст]: учебное пособие для студентов вузов/ С.В. Сизый- М.: ФИЗМАТЛИТ, 2007. – 192 с.

в) программное обеспечение:

1. Работа на компьютере проводится с использованием лицензионных версий операционной системы Microsoft Windows XP Prof.
2. Для работы в библиотеке используется общеузовское лицензионное программное обеспечение «Ирбис-64», в составе которого входят АРМ «Каталогизатор», АРМ «Читатель», АРМ «Администратор», АРМ «Комплектатор», Web-Ирбис (CZ39.50)
3. Лицензионная программа АУП (Шахты) – комплекс «Электронные ведомости»

г) базы данных, информационно-справочные и поисковые системы:

1. Национальный цифровой ресурс Руконт. Режим доступа [<http://www.rucont.ru/>].
2. Университетская библиотека он-лайн. Режим доступа [<http://www.biblioclub.ru/>]. б) интернет-ресурсы 1. <http://www.4p.ru> 2. <http://marketing.com.ru>

д) Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине:

1. Организация самостоятельной работы студентов в учреждении высшего образования [Текст]: методические рекомендации / Сост.Е.Б. Манузина, Е.Э. Норина; Алтайская гос. Академия обр-я им. В.М. Шукшина. – Бийск: ФГБОУ ВПО «АГАО», 2014. – 84 с.

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Учебные аудитории для проведения занятий лекционного типа:

Аудитория, укомплектованная специализированной мебелью, с компьютерами, оснащенными комплектом лицензированного программного обеспечения (лицензионное программное обеспечение: Windows XP, Office2003, Ирбис; Свободно распространяемое программное обеспечение: 7Zip, Adobe Flash Player, Google Chrome, VLC media Player), мультимедиа проектор, экран для представления учебной информации большой аудитории обучающихся.

Учебные аудитории для проведения практических занятий:

Аудитория, укомплектованная специализированной мебелью, с компьютерами, оснащенными комплектом лицензированного программного обеспечения (лицензионное

программное обеспечение: Windows XP, Office2003, Ирбис; Свободно распространяемое программное обеспечение: 7Zip, Adobe Flash Player, Google Chrome, VLC media Player), мультимедиа проектор, экран для представления учебной информации большой аудитории обучающихся.

Учебные аудитории для проведения групповых и индивидуальных консультаций:

Аудитория, укомплектованная специализированной мебелью, с компьютерами, оснащенными комплектом лицензированного программного обеспечения (лицензионное программное обеспечение: Windows XP, Office2003, Ирбис; Свободно распространяемое программное обеспечение: 7Zip, Adobe Flash Player, Google Chrome, VLC media Player), мультимедиа проектор, экран для представления учебной информации большой аудитории обучающихся.

Учебные аудитории для проведения текущего контроля и промежуточной аттестации:

Аудитория, укомплектованная специализированной мебелью, с компьютерами, оснащенными комплектом лицензированного программного обеспечения (лицензионное программное обеспечение: Windows XP, Office2003, Ирбис; Свободно распространяемое программное обеспечение: 7Zip, Adobe Flash Player, Google Chrome, VLC media Player) *с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации.*

Помещения для самостоятельной работы:

Аудитория, укомплектованная специализированной мебелью, с компьютерами, оснащенными комплектом лицензированного программного обеспечения (лицензионное программное обеспечение: Windows XP, Office2003, Ирбис; Свободно распространяемое программное обеспечение: 7Zip, Adobe Flash Player, Google Chrome, VLC media Player) *с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации.*

Читальный зал, оснащенный автоматизированными и обычными рабочими местами, с компьютерами, оснащенными комплектом лицензированного программного обеспечения (Лицензионное программное обеспечение: Windows XP, Office2003, Kaspersky. Свободно распространяемое программное обеспечение: Google Chrome, 7Zip), копировальной машиной, принтерами, сканерами, с наличием автоматизированных рабочих мест для пользователей с проблемами зрения: специальное программное обеспечение, тифлофлешплееры, электронная лупа, читающая машина. Для обучающихся инвалидов и лиц с ОВЗ специализированные сервисы и информационные ресурсы при помощи программно-аппаратных комплексов:

- тифло-флеш-плееров Victor Reader Stream с удобной системой навигации;
- АРМ с проводными гарнитурами Jabra UC VOICE 550 Duo и Windows- приложением для преобразования речи в текст VOCO. Professional .;
- электронного видео-увеличителя Ruby.;
- сканирующего и читающего устройства Eye-Pal Vision;
- специализированного программного обеспечения Easy Converter для создания цифровых говорящих книг в формате DAIZY.

Помещение для хранения и профилактического обслуживания учебного оборудования:

Аудитория, укомплектованная специализированной мебелью: шкаф для хранения учебных наглядных пособий, обеспечивающих тематические иллюстрации; стол, стул, компьютер, принтер, учебно-методические пособия.

10. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

10.1. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ ДЛЯ ПРЕПОДАВАТЕЛЕЙ

Изучение курса абстрактной и компьютерной алгебры является важной частью теоретической и практической подготовки будущего учителя информатики.

Согласно программе дисциплины, курс абстрактной и компьютерной алгебры разделен на 5 разделов, каждый из которых решает определенные задачи.

Изучение учебного содержания этих разделов имеет важное значение в профессионально-предметной подготовке будущего учителя информатики, так как является теоретической основой для изучения ряда дисциплин в области информатики.

При преподавании методически целесообразно в каждом разделе курса выделить наиболее важные моменты и акцентировать на них внимание обучающихся. Предполагается:

- при изучении первого раздела программы добиться точного знания студентами определений основных алгебраических структур компьютерной математики (полугрупп, групп, колец, полей) и умения их распознавать среди различных алгебр;
- при изучении второго и третьего разделов уделить особое внимание усвоению студентами основополагающих фактов теории делимости, а также теории сравнений в кольце целых чисел, положенных в основу построения модулярной арифметики;
- на практических занятиях по четвертому разделу акцентировать внимание на формирование практических навыков работы с многочленами и представление их в компьютере;
- при изучении пятого раздела основное внимание уделить формированию первоначальных представлений о кодировании и показу значения теоретико-числовых знаний для понимания сущности современных методов шифрования (открытый ключ, электронная подпись);
- при чтении лекций по всем разделам программы иллюстрировать теоретический материал большим количеством примеров, что позволяет усилить наглядность изложения и продемонстрировать приемы решения задач;

В соответствии с расставленными приоритетами были определены формы контроля. По первому разделу предполагается провести домашнюю контрольную работу и теоретический опрос на усвоение теоретического материала. По разделу «Теория делимости в кольце целых чисел» предполагается аудиторная контрольная работа, а по разделу «Теория сравнений в кольце целых чисел» - домашняя контрольная работа

проверяющая умения применять полученные знания при решении задач на арифметические приложения теории сравнений.

Индивидуальное домашнее задание по четвертому разделу включают основные типы заданий, выполнение которых направлено на формирование умений применять полученные знания по основам теории многочленов при решении практических задач.

По основным понятиям пятого раздела планируется контрольный опрос. Итоговый тест включает задания по первым пяти дидактическим единицам дисциплины.

Допуск к зачету с оценкой осуществляется только при выполнении всех видов практических работ. Студент, успешно отчитавшийся по всем формам контроля (домашние контрольные работы по первому и третьему разделам, аудиторная контрольная работа по 2-му разделу, ИДЗ по теории многочленов, итоговый тест), по его желанию может быть освобожден от зачета с оценкой с выставлением оценки по рейтингу. Рейтинговая оценка на зачете с оценкой может быть улучшена не более, чем на 30%.

10.2 МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ ДЛЯ СТУДЕНТОВ

Общая трудоемкость дисциплины, в соответствии с учебным планом, составляет 3 зачетные единицы и включает учебное время, отведенное на **лекционные, практические занятия и самостоятельную работу** студента.

Тематика лекционных и практических занятий охватывает все разделы учебной дисциплины и ориентирована на выполнение ее целей и задач в соответствии с требованиями к результатам освоения дисциплины.

На лекционных занятиях рекомендуется внимательно слушать преподавателя, конспектировать материал лекции, принимать участие в интерактивных формах, используемых преподавателем на лекции, задавать вопросы и активно отвечать на поставленные вопросы. При подготовке к лекции необходимо проработать содержание предыдущих лекций, подготовить вопросы. После лекции также следует прочитать свой конспект, ознакомиться с вариантами изложения данной темы в учебниках и учебных пособиях, и если возникают вопросы, то можно с ними обратиться к преподавателю.

Цель **практических занятий** - осмысление студентами теоретического материала, изложенного на лекциях, формирование умения использовать его при

решении практических задач в изучаемой области, развитие навыков самостоятельной работы, умения работать с учебной литературой.

Подготовка к практическому занятию включает выполнение заданий преподавателя по теме предыдущего занятия, а также подготовку к занятию по новой теме – самостоятельное изучение материалов лекционного курса, источников обязательной и дополнительной литературы.

Самостоятельная работа является неотъемлемой частью учебного процесса. Она запланирована и структурирована таким образом, чтобы студент при подготовке к занятиям наиболее эффективно осваивал теоретический материал и получал системные знания по курсу.

Руководство самостоятельной работой студентов со стороны преподавателя заключается в оказании помощи при планировании работы по изучению курса, в разъяснении вопросов, возникающих у студентов при изучении отдельных тем курса, при подготовке к различным формам контроля, запланированным программой дисциплины.

При выполнении индивидуального домашнего задания (ИДЗ) следует обратить внимание на следующие моменты: вариант задания для каждого студента определяется его номером в списке группы; задание выполняется в отдельной тетради с подробным описанием хода решения и ссылками на соответствующий теоретический материал; проверка самостоятельности выполнения ИДЗ осуществляется преподавателем при собеседовании со студентом (защита ИДЗ).

Время, отведенное учебным планом на самостоятельную работу студента по дисциплине, составляет примерно 60% всей ее трудоемкости. Формы самостоятельной работы по каждому разделу дисциплины перечислены в технологической карте в конце программы.

Для оценивания уровня достигнутых результатов освоения студентом каждого раздела дисциплины, а также всей дисциплины в целом, соответствия его заявленным требованиям, используется **балльно-рейтинговая система**, детально описанная в технологической карте дисциплины.

11. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Фонд оценочных средств разработан для проведения промежуточной аттестации обучающихся по дисциплине «Абстрактная и компьютерная алгебра» и входит в состав основной образовательной программы по направлению подготовки: 44.03.05 «Педагогическое образование (с двумя профилями подготовки)» (профили «Технология и Информатика») (квалификация «Бакалавр»), реализуемой при подготовке обучающихся в федеральном государственном бюджетном образовательном учреждении высшего образования «Алтайский государственный гуманитарно-педагогический университет имени В.М. Шукшина». Фонд оценочных средств предназначен для проверки сформированности компетенций, заявленных в программе дисциплины «Абстрактная и компьютерная алгебра» в соответствии с учебным планом 44.03.05 «Педагогическое образование (с двумя профилями подготовки)» (профили «Технология и Информатика») (квалификация «Бакалавр»).

Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

- Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач (УК-1);
- Способен проектировать и реализовывать программу основного и среднего общего образования по предмету Информатика (ПК-3).

Компетенции, этапы	Индикаторы	Оценочные средства
УК-1 2 этап	Знать: - УК-1.1 - знание механизмов и методик поиска, анализа и синтеза информации, включающие системный подход в области образования (З.1); - УК-1.2 - знание методик постановки цели и способов её достижения, научного представления о результатах обработки информации (З.2);	Практико-ориентированное задание: контрольный опрос, контрольная работа, ИДЗ, итоговый тест
	Уметь: - УК-1.3 - умение анализировать задачу, выделять ее базовые составляющие, осуществлять декомпозицию задачи (У.1); - УК-1.4 - умение находить и критически анализировать информацию, необходимую для решения поставленной задачи (У.2); - УК-1.5 - умение рассматривать возможные варианты решения задачи, оценивая их достоинства и недостатки (У.3).	
	Владеть: - УК-1.6 - владение методами установления причинно-следственных связей и определения наиболее значимых среди них (В.1);	

	- УК-1.7 - владение механизмами поиска информации в том числе с применением современных информационных и коммуникационных технологий (В.2).	
ПК-3 2 этап	Знать: - ПК-3.1 - знание теоретических основ информатики, принципов функционирования информационных систем и технологий (3.1).	Практико-ориентированное задание: контрольный опрос, контрольная работа, ИДЗ, итоговый тест
	Уметь: -	
	Владеть: -	

Компетенция УК-1 с указанием этапа формирования в процессе освоения образовательной программы

Компетенция УК-1 (способность осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач) формируется на втором этапе формирования компетенций.

Компетенция УК-1 формировалась в процессе изучения данной дисциплины и продолжит формироваться на следующих курсах в процессе изучения других учебных дисциплин, прохождения практик и итоговой государственной аттестации (Защита выпускной квалификационной работы).

Типовое контрольное задание для оценки сформированности данной компетенции направлено на демонстрацию готовности осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач.

Компетенция ПК-3 с указанием этапа формирования в процессе освоения образовательной программы

Компетенция ПК-3 (способность проектировать и реализовывать программу основного и среднего общего образования по предмету) формируется на втором этапе формирования компетенций.

Компетенция ПК-3 формировалась в процессе изучения данной дисциплины и продолжит формироваться на следующих курсах в процессе изучения других учебных дисциплин, прохождения практик и итоговой государственной аттестации (Защита выпускной квалификационной работы).

Типовое контрольное задание для оценки сформированности данной компетенции направлено на демонстрацию готовности проектировать и реализовывать программу основного и среднего общего образования по предмету.

1. Типовое контрольное задание на этапе формирования УК-1 и ПК-3:

Контрольные опросы

Контрольный опрос по разделу «Алгебры»

1. Сформулируйте определение бинарной алгебраической операции. Приведите примеры.

2. Какая бинарная алгебраическая операция называется коммутативной? Приведите примеры коммутативных бинарных алгебраических операций и бинарных алгебраических операций, не являющихся таковыми.
3. Какая бинарная алгебраическая операция называется ассоциативной? Приведите примеры ассоциативных бинарных алгебраических операций.
4. В каком случае говорят, что бинарная алгебраическая операция $\circ$ дистрибутивна относительно бинарной алгебраической операции $*$? Приведите примеры.
5. Как определяется нейтральный относительно бинарной алгебраической операции $*$ элемент? Как называется и чему равен нейтральный элемент по сложению? – по умножению?
6. Как определяется элемент, симметричный для a относительно бинарной алгебраической операции $*$? Как называется и чему равен симметричный элемент по сложению? – по умножению?
7. Сформулируйте определения моноида и группы. Приведите примеры группы и моноида, не являющегося группой.
8. Перечислите основные свойства группы.
9. Сформулируйте определение подгруппы данной группы. Приведите примеры подгрупп. Сформулируйте критерий подгруппы.
10. Сформулируйте определение кольца. Приведите примеры колец.
11. Сформулируйте определение подкольца данного кольца, укажите его критерий; приведите примеры подколец.
12. Сформулируйте определение поля. Перечислите основные свойства полей.
13. Приведите пример кольца, не являющегося полем и кольца, являющегося полем.
14. Опишите кольцо классов вычетов Z_m . Какие классы являются обратимыми в этом кольце?
15. Опишите поле классов вычетов Z_p .

Контрольный опрос по разделу «Введение в теорию кодирования»

1. Что понимают под кодированием?
2. Приведите примеры способов кодирования.
3. Какие требования должны выполняться при кодировании?
4. Что является существенным условием при выборе алфавита кодирования?
5. Почему в устройствах хранения и обработки дискретной информации используется двоичная система кодирования?
6. Как задается алфавитное кодирование?
7. Какая схема будет называться разделимой? префиксной?
8. Является ли префиксная схема разделимой?
9. Является ли схема алфавитного кодирования $\langle a \rightarrow 0, b \rightarrow 10, c \rightarrow 011, d \rightarrow 1011, e \rightarrow 1111 \rangle$ разделимой? префиксной?
10. В чем состоит задача кодирования при передаче информации по каналу с помехами?
11. Что понимают под кодовым расстоянием?
12. Чему равно минимальное кодовое расстояние, необходимое для различения двух кодов?
13. Сколько можно обнаружить и исправить ошибок, если кодовое расстояние равно 4?
14. В чем заключается метод кодирования «проверка на четность»?
15. В чем состоит процесс шифрования?
16. Чем занимается область знаний «криптография»?
17. В чем заключается принцип перемешивания Шеннона?
18. В чем состоят отличия между рассеивающими и перемешивающими преобразованиями при шифровании информации?
19. Какой параметр в криптосистеме RSA является секретным?
20. Как может быть вычислен секретный ключ в RSA?

Критерии оценки контрольного опроса:

1. Каждый вопрос оценивается в 1 балл.
2. Итоговая оценка за весь опрос соответствует проценту правильных ответов по отношению к общему числу всех вопросов.
3. Оценка за опрос считается положительной, если студент ответил правильно не менее, чем на 60% всех вопросов.

2. Типовое контрольное задание на этапе формирования УК-1 и ПК-3:

Контрольные работы

Критерии оценки контрольной работы:

1. Каждое задание работы оценивается в баллах; при допущенных ошибках оценка за задание снижается.
2. «Стоимость» каждого задания и максимально возможное число баллов определяется отдельно для каждой работы.
3. При оценивании задания учитывается аккуратность оформления и подробное описание хода решения со ссылками на соответствующий теоретический материал.
4. Итоговая оценка за всю работу соответствует проценту полученного суммарного балла по отношению к максимально возможному числу баллов.
5. Положительной считается оценка за работу не менее 60%. При отрицательной оценке студент переписывает работу заново (другой вариант).
6. Студент может повысить рейтинговый балл, выполнив работу над ошибками. Рейтинговый балл за повторную работу и при работе над ошибками не может быть больше 75 %.

Образец домашней контрольной работы (1 раздел)

Вариант 1

1. Пусть R есть множество действительных чисел. Показать, что $\langle R', * \rangle$ является группой, если: $R' = R \setminus \{-1\}$, $a * b = 2ab + 2b + 2a + 1$.
2. Будет ли $A = \{x / x = 8k, k \in \mathbb{Z}\}$ подгруппой, группы $\langle M, + \rangle$, если $M = \{x / x = 2k, k \in \mathbb{Z}\}$? Ответ обоснуйте.
3. Какие из перечисленных ниже алгебр являются: только кольцами, но не полями, и кольцами и полями относительно естественных операций сложения и умножения:
а) $\mathbb{Z}$, б) $\left\{ \begin{pmatrix} a & 1 \\ 0 & v \end{pmatrix} \mid a, v \in \mathbb{Z} \right\}$, в) $\mathbb{Q}^+$, г) $\mathbb{R}$, д) $\left\{ \frac{c}{3^n} \mid c \in \mathbb{Z}, n \in \mathbb{N} \right\}$? Ответ поясните.
4. Составьте таблицы сложения и умножения в кольце $\mathbb{Z}_8$. Какие элементы кольца обратимы? Является ли это кольцо полем? Ответ обосновать.

Примечание. Задание №1 данной работы оценивается в 2 балла, остальные – в 1 балл. Максимально возможное число баллов за работу – 5 баллов (100%).

Образец аудиторной контрольной работы (2 раздел)

1. Сократить дробь $\frac{1073}{3683}$, используя алгоритм Евклида.
2. Какие из чисел: 631, 637, 1027, - являются простыми?
3. С помощью канонического разложения найти НОД и НОК чисел 572 и 1118.
4. Решить в целых числах уравнение $43x + 37y = 21$.

5. Выполнить указанные действия: $40042_5 : 23_5 + 1044_5 - (23_5 \cdot 34_5) =$.
6. Представить число x в указанной системе счисления его краткой и развернутой систематической записью: а) $3A9,24_{16} = x_{10}$; б) $2135,46875 = x_4$.

Примечание. Задание №5 данной работы оценивается в 2 балла, остальные – в 1 балл. Максимально возможное число баллов за работу – 7 баллов (100%).

Образец домашней контрольной работы (3 раздел)

1. Найти остаток от деления 7^{164} на 25.
2. Решить сравнения: а) $14x \equiv 30 \pmod{21}$; б) $4x \equiv 18 \pmod{15}$; в) $14x \equiv 50 \pmod{62}$;
3. Решить систему сравнений используя метод последовательной подстановки и китайскую теорему об остатках:

$$\begin{cases} 3x \equiv 5 \pmod{13}; \\ 2x \equiv 17 \pmod{21}; \\ 5x \equiv 31 \pmod{32}. \end{cases}$$
4. Пусть $n_1=13, n_2=11, n_3=17, x=62, y=24$. Найти сумму, разность, произведение и частное чисел x и y с помощью их модулярного представления. (Все действия описать с подробным объяснением полученных результатов).

Примечание. Задания №1 и №4 данной работы оцениваются в 2 балла, остальные – в 1 балл. Максимально возможное число баллов за работу – 6 баллов (100%).

3. Типовое контрольное задание на этапе формирования УК-1 и ПК-3:

Образец индивидуального домашнего задания (4 раздел)

1. Разделить с остатком многочлен $f(x)$ на $g(x)$ в кольце $Z_5[x]$:
 $f(x) = \bar{2}x^5 - \bar{3}x^4 + \bar{2}x^3 - \bar{3}x + \bar{1}$, $g(x) = \bar{2}x^2 - \bar{3}x + \bar{1}$.
2. Записать равенство, полученное в процессе деления:
 $2x^4 + 4x^3 - x^2 - 3x + 5$ на $x + 2$.
3. Разложить многочлен $f(x)$ по степеням $x - c$, найти значение многочлена и всех его производных при $x = c$: $f(x) = 2x^5 + 3x^4 + x^3 - x^2 + 5 \in R[x]$, $c = -2$.
4. Найти НОД $f(x)$ и $g(x)$ в кольце $Z_7[x]$: $f(x) = x^5 - \bar{2}x^4 + x^3 + \bar{3}x^2 - \bar{5}x + \bar{4}$,
 $g(x) = \bar{3}x^4 - \bar{6}x^3 + \bar{5}x^2 + \bar{2}x - \bar{1}$.
5. Найти НОД многочленов $f(x)$ и $g(x)$ в кольце $R[x]$; выразить НОД $(f(x), g(x))$ через $f(x)$ и $g(x)$, если $f(x) = x^5 - 2x^4 + x^3 + 7x^2 - 12x + 10$,
 $g(x) = 3x^4 - 6x^3 + 5x^2 + 2x - 2$.
6. Являются ли неприводимыми многочлены: а) $2x^3 + 3x^2 + 6x - 4$ над Q ?
 б) $2x^2 - x - 3$ над Z ? в) $3x^2 + x - 1$ над R ? д) $f(x) = \bar{3}x^3 + \bar{2}x^2 - \bar{4}x + \bar{1}$ над Z_5 ?
 Ответ пояснить.
7. Решить уравнения:
 а) $x^3 - 6x^2 + 57x - 196 = 0$;
 б) $x^4 - x^3 - 3x^2 + 5x - 10 = 0$.
8. Используя формулы Виета, построить многочлен в $C[x]$ наименьшей степени по его корням: $x_1 = 1, x_2 = 2, x_3 = 3$.

Критерии оценки заданий ИДЗ:

1. Каждое задание ИДЗ оценивается в 1 балл (в №7 задания (а) и (б) оцениваются отдельно); при допущенных ошибках оценка за задание снижается. Максимально возможное число баллов за все ИДЗ – 9 баллов (100%).
2. При оценивании задания учитывается аккуратность оформления и подробное описание хода решения со ссылками на соответствующий теоретический материал.
3. Итоговая оценка за всю работу соответствует проценту полученного суммарного балла по отношению к максимально возможному числу баллов за все ИДЗ.
4. Оценка за ИДЗ не менее 60% считается положительной. При отрицательной оценке студент выполняет работу над ошибками; рейтинговый балл за повторную работу не может быть больше 75 %.
5. Оценка аннулируется, если на защите ИДЗ (при собеседовании с преподавателем) студент не подтвердил самостоятельность его выполнения.
6. Оценка за ИДЗ снижается при несоблюдении сроков его сдачи: минус 1% за каждый просроченный день.

4. Типовое контрольное задание на этапе формирования УК-1 и ПК-3:

Итоговый тест по абстрактной и компьютерной алгебре (4 семестр)

Дидактические единицы:

1. Бинарные алгебраические операции. Алгебры
2. Делимость и простые числа.
3. Систематические числа.
4. Отношение сравнения в кольце **Z** и его основные свойства.
5. Сравнения и системы сравнений с неизвестной величиной.
6. Кольцо многочленов над полем

1. БИНАРНЫЕ АЛГЕБРАИЧЕСКИЕ ОПЕРАЦИИ. АЛГЕБРЫ

1. Коммутативными на R являются операции:

1) сложения; 2) вычитания; 3) умножения; 4) деления.

2. Коммутативными на R являются операции:

$$1) a*b=(a+b)^2; 2) a*b=a+3b; 3) a*b=\frac{ab}{3}; 4) a*b=\frac{1}{2}(a-b).$$

3. Ассоциативными на R являются операции:

$$1) a*b=(a+b)^2; 2) a*b=a+3b; 3) a*b=\frac{ab}{3}; 4) a*b=a-3b.$$

4. Укажите пары бинарных алгебраических операций, в которых первая операция дистрибутивна относительно второй:

- 1) сложение и умножение на множестве R;
- 2) умножение и сложение на множестве R;
- 3) объединение и пересечение на множестве $\mathcal{P}(M)$ всех подмножеств некоторого множества M;
- 4) пересечение и объединение на множестве $\mathcal{P}(M)$;
- 5) умножение и деление на множестве $\mathbb{R}^+$.

5. Установите соответствие между алгеброй и элементом этой алгебры, который является нейтральным относительно указанной алгебраической операции:

1) $\langle \mathbf{Z}, + \rangle$; 2) $\langle Q, \cdot \rangle$; 3) $\langle \mathcal{P}(M), \cup \rangle$; 4) $\langle \mathcal{P}(M), \cap \rangle$; 5) $\langle N, + \rangle$.

($\mathcal{P}(M)$ – множество всех подмножеств некоторого множества M)

a) $\emptyset$; б) 0; в) основное множество алгебры не содержит нейтрального элемента; г) 1; д) M .

1) Для алгебры $\langle \{a_1, a_2, a_3\}, * \rangle$, где операция $*$ задана таблицей:

$*$	a_1	a_2	a_3
a_1	a_3	a_1	a_2
a_2	a_1	a_2	a_3
a_3	a_2	a_3	a_1

неверными являются утверждения:

- 1) Операция $*$ коммутативна;
- 2) Нейтральным элементом относительно операции $*$ является элемент a_1 ;
- 3) Нейтральным элементом относительно операции $*$ является элемент a_2 ;
- 4) Симметричным элементом для a_1 является a_2 ;
- 5) Симметричным элементом для a_3 является a_1 .

7. Из следующих алгебр группами являются:

- а) $\langle Z; \cdot \rangle$; б) $\langle Z; + \rangle$; в) $\langle Q^+; \cdot \rangle$; г) $\langle Q; \cdot \rangle$; д) $\langle A; \cdot \rangle$, где $A = \{\alpha \in C \mid \alpha^7 = 1\}$;
 1) только а, г; 2) только б, в, г; 3) а, б, в; 4) б, в, д.

8. Группу относительно умножения образует множество:

- 1) $Z_8 \setminus \{\bar{0}\}$; 2) $Z_{10} \setminus \{\bar{0}\}$; 3) $Z_{11} \setminus \{\bar{0}\}$; 4) $Z_{12} \setminus \{\bar{0}\}$.

9. Подгруппами мультипликативной группы $\langle R \setminus \{0\}; \cdot \rangle$ являются:

- а) $G = \{-1, 1\}$; б) $H = \{1, 2, 3\}$; в) $Q \setminus \{0\}$; г) $Z \setminus \{0\}$.
 1) а, б; 2) а, в; 3) а, г; 4) в, г.

10. Противоположным классу $\bar{5}$ в группе $\langle Z_7, + \rangle$ является класс вычетов

- 1) $\bar{1}$; 2) $\bar{3}$; 3) $\bar{2}$; 4) $\bar{4}$.

11. Обратным классу $\bar{2}$ в группе $\langle Z_5 \setminus \{\bar{0}\}; \cdot \rangle$ является класс вычетов

- 1) $\bar{1}$; 2) $\bar{2}$; 3) $\bar{3}$; 4) $\bar{4}$.

12. Из следующих алгебр **образуют** кольцо:

- а) $\langle N; +, \cdot \rangle$; б) $\langle Z; +, \cdot \rangle$; в) $\langle Q; +, \cdot \rangle$; г) $\langle R; +, \cdot \rangle$?
 1) а, б; 2) б, в, г; 3) а, б, г; 4) только в, г.

13. Из следующих алгебр **не образуют** кольцо:

- а) $\langle Z; + \rangle$; б) $\langle Z; +, \cdot \rangle$; в) $\langle N; +, \cdot \rangle$; г) $\langle Z_5; +, \cdot \rangle$?
 1) Только а; 2) б, в; 3) в, г; 4) а, в.

14. Подкольцами кольца действительных чисел **являются**:

- а) Z ; б) $2Z$; в) $Q[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in Q\}$; г) $K = \{a + b\sqrt[3]{2} \mid a, b \in Z\}$?
 1) Только а, в; 2) только б, в; 3) только в, г; 4) а, б, в.

15. Нет делителей нуля в кольцах

- 1) $\langle Z; +, \cdot \rangle$; 2) $\langle Z_6; +, \cdot \rangle$; 3) $\langle Z_7; +, \cdot \rangle$; 4) $\langle Z_4; +, \cdot \rangle$.

16. Из следующих алгебр полями **являются**:

- а) $\langle N; +, \cdot \rangle$; б) $\langle Z; +, \cdot \rangle$; в) $\langle Q; +, \cdot \rangle$; г) $\langle R; +, \cdot \rangle$.

17. Из следующих алгебр полями **не являются**:

- а) $\langle Q; +, \cdot \rangle$; б) $\langle Z_6; +, \cdot \rangle$; в) $\langle Z_7; +, \cdot \rangle$; г) $\langle R; +, \cdot \rangle$; д) $\langle Z; +, \cdot \rangle$; е) $\langle N; +, \cdot \rangle$?

1) только б и е; 2) только б, д; 3) б, д, е; 4) б, в, д.

18. Подполями поля действительных чисел **не являются**:

а) $\mathbb{Z}$; б) $\mathbb{Q}$; в) $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} | a, b \in \mathbb{Z}\}$; г) $\mathbb{R}$?

1) только а; 2) только в; 3) а, в; 4) б, г.

19. Элемент, противоположный классу $\bar{3}$ в поле $\langle \mathbb{Z}_{11}; +, \cdot \rangle$ равен:

1) $\bar{4}$; 2) $\bar{7}$; 3) $\bar{9}$; 4) $\bar{8}$.

20. Элемент, обратный классу $\bar{3}$ в поле $\langle \mathbb{Z}_{11}; +, \cdot \rangle$ равен:

1) $\bar{4}$; 2) $\bar{7}$; 3) $\bar{9}$; 4) $\bar{8}$.

2. ДЕЛИМОСТЬ И ПРОСТЫЕ ЧИСЛА

1. При делении целого числа a на некоторое целое положительное число b частное равно q , а остаток r . Какие из утверждений при этом являются верными?

1) $a = bq + r, 0 \leq r < b$; 2) $\text{НОД}(a, b) = \text{НОД}(b, r)$; 3) $\text{НОД}(a, b) = \text{НОД}(q, r)$;

4) При делении $-a$ на b остаток равен $-r$. 5) При делении $-a$ на b остаток равен $b-r$.

2. При делении a на 7 остаток равен 2. Остаток при делении a^5 на 7 равен ____.

3. Наибольший общий делитель для чисел 589 и 713 находится в интервале

1) (0;9); 2) (9;20); 3) (22;30); 4) (30;35).

4. Наименьшее общее кратное чисел 952 и 588 равно ____.

5. Простое число 2 входит в каноническое разложение любого натурального делителя числа $a=5544$ с показателем степени α таким, что

1) $\alpha=3$; 2) $\alpha \leq 3$; 3) $\alpha \geq 3$; 4) $\alpha = 4$.

6. Пусть числа a, b и c представлены в виде $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}$, $b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \dots \cdot p_k^{\beta_k}$, $c = p_1^{\gamma_1} \cdot p_2^{\gamma_2} \cdot \dots \cdot p_k^{\gamma_k}$, где все p_i – попарно различные простые числа, а все $\alpha_i \geq 0, \beta_i \geq 0, \gamma_i \geq 0$. Завершите каждое из предложений соответствующим ему заключением так, чтобы получилось верное утверждение (установите соответствие):

1) Если $c = \text{НОД}(a, b)$, то ...; 2) Если c – общий делитель чисел a и b , то ...;

3) Если $c = \text{НОК}(a, b)$, то ...; 4) Если c – общее кратное чисел a и b , то ...;

5) Если c не является общим делителем чисел a и b , то

а) $\gamma_i = \max\{\alpha_i, \beta_i\}, i=1, 2, \dots, k$. б) $\gamma_i = \min\{\alpha_i, \beta_i\}, i=1, 2, \dots, k$. в) $\gamma_i \leq \min\{\alpha_i, \beta_i\}, i=1, k$.

г) $\gamma_i \geq \max\{\alpha_i, \beta_i\}, i=1, k$. д) $\gamma_i > \min\{\alpha_i, \beta_i\}$ для некоторых i ($1 \leq i \leq k$).

7. Какие из следующих чисел являются простыми?

1) 473; 2) 273; 3) 149; 4) 281; 5) 119.

8. Какие из утверждений являются верными?

1) Число делится на 45 тогда и только тогда, когда оно делится на 5 и на 9.

2) Число делится на 45 тогда и только тогда, когда оно делится на 5 и на 3.

3) Число делится на 12 тогда и только тогда, когда оно делится на 2 и на 6.

4) Число делится на 12 тогда и только тогда, когда оно делится на 4 и на 3.

9. Простое число 3 входит в каноническое разложение любого натурального кратного числа $a=2520$ с показателем степени α таким, что

1) $\alpha \geq 3$; 2) $\alpha = 2$; 3) $\alpha \leq 2$; 4) $\alpha \geq 2$.

10. Для чисел $a=2^8 \cdot 3^{15} \cdot 7^{21}$ и $b=2^{12} \cdot 5^{14} \cdot 7^{15}$ их наибольший общий делитель равен
 1) $2^{12} \cdot 3^{15} \cdot 5^{14} \cdot 7^{21}$; 2) $2^8 \cdot 3^{15} \cdot 7^{15}$; 3) $2^8 \cdot 5^{14} \cdot 7^{15}$; 4) $2^8 \cdot 7^{15}$.
11. Для чисел $a=2^8 \cdot 3^{15} \cdot 7^{21}$ и $b=2^{12} \cdot 5^{14} \cdot 7^{15}$ их наименьшее общее кратное равно
 1) $2^{12} \cdot 3^{15} \cdot 5^{14} \cdot 7^{21}$; 2) $2^{12} \cdot 5^{14} \cdot 7^{21}$; 3) $2^{12} \cdot 3^{15} \cdot 7^{21}$; 4) $2^{20} \cdot 3^{15} \cdot 5^{14} \cdot 7^{36}$.
12. При делении некоторого целого числа на -142 может получиться остаток
 1) 187; 2) -45 ; 3) 56; 4) -160 .
13. Остаток от деления числа -135 на 14 равен
 1) 9; 2) -9 ; 3) 5; 4) -5 .

3. ОТНОШЕНИЕ СРАВНЕНИЯ В КОЛЬЦЕ Z И ЕГО ОСНОВНЫЕ СВОЙСТВА

1. Для целых чисел a, b, m ($m \neq 0$) утверждение $a \equiv b \pmod{m}$ **не равносильно** утверждению
 1) $a = mq + b$ ($q \in Z$); 2) $(a-b) : m$; 3) a и b имеют одинаковые остатки при делении на m ; 4) $a = bm$.
2. Утверждение «число n имеет вид $10k+3$ » **равносильно** сравнению
 1) $n \equiv 10 \pmod{3}$; 2) $n \equiv 3 \pmod{10}$; 3) $10 \equiv 3 \pmod{n}$; 4) $n \equiv k \pmod{10}$.
3. Установите соответствие между равносильными утверждениями:
 1) a и c имеют одинаковые остатки при делении на b ($b \neq 0$) а) $a \equiv b \pmod{c}$
 2) $(a-b) : c$ б) $a \equiv 0 \pmod{b}$
 3) $a : b$ в) $c \equiv b \pmod{a}$
 4) $c = b + ak, k \in Z$ г) $a \equiv c \pmod{b}$
4. Группу относительно умножения **образует** множество:
 2) $Z_8 \setminus \{ \bar{0} \}$; 2) $Z_6 \setminus \{ \bar{0} \}$; 3) $Z_7 \setminus \{ \bar{0} \}$; 4) $Z_4 \setminus \{ \bar{0} \}$.
5. **Не образует** группу относительно умножения множество:
 3) $Z_3 \setminus \{ \bar{0} \}$; 2) $Z_5 \setminus \{ \bar{0} \}$; 3) $Z_7 \setminus \{ \bar{0} \}$; 4) $Z_8 \setminus \{ \bar{0} \}$.
 4) 6.
6. В кольце $\langle Z_6; +, \cdot \rangle$ нейтральным элементом для сложения является класс
 1) $\bar{0}$; 2) $\bar{1}$; 3) $\bar{5}$; 4) $\bar{4}$.
7. В кольце $\langle Z_6; +, \cdot \rangle$ противоположным классу $\bar{1}$ является класс
 1) $\bar{2}$; 2) $\bar{3}$; 3) $\bar{5}$; 4) $\bar{4}$.
8. Равенства $\bar{7} + \bar{7} = \bar{5}$ и $\bar{7} \cdot \bar{7} = \bar{4}$ имеют место в кольце классов вычетов по модулю m
 1) $m=8$; 2) $m=9$; 3) $m=10$; 4) $m=11$.
9. Полями являются кольца классов вычетов по модулю m
 1) $m=2$; 2) $m=7$; 3) $m=8$; 4) $m=9$.
10. Для класса $\bar{3} \pmod{8}$ обратным является класс: 1) $\bar{1}$; 2) $\bar{6}$; 3) $\bar{5}$; 4) $\bar{3}$.

11. Количество натуральных чисел, не превосходящих $a=125$ и взаимно простых с a , равно ____.
12. Количество натуральных чисел, не превосходящих $a=600$ и взаимно простых с a , равно ____.

13. Количество натуральных чисел, не превосходящих $a=180$ и взаимно простых с a , равно ____.
14. Приведённой системой вычетов по модулю $m=12$ является совокупность чисел
 1) $\{0,1,17,23\}$; 2) $\{1,3,5,7,11\}$; 3) $\{-47,17,31,-1\}$; 4) $\{-13,17,19,23,25\}$.
15. Делятся на 7 числа:
 1) $1^{18}+2^{18}+3^{18}+4^{18}+5^{18}+6^{18}+1$; 2) 454111; 3) $5^{25}+2$; 4) $5^{61}-3$; 5) $5^{121}+1$.
16. Остаток от деления 3^{126} на 5 равен: 1) 4; 2) 3; 3) 1; 4) 9.
17. Последняя цифра в десятичном представлении числа 3^{126} равна: 1) 4; 2) 3; 3) 1; 4) 9.
18. Последние две цифры в десятичном представлении числа 3^{243} равны:
 1) 81; 2) 27; 3) 43; 4) 29.
19. Решением уравнения $\bar{3}-\bar{x}=\bar{7}$, где $\bar{3}$ и $\bar{7}$ – классы вычетов по модулю 11, является класс:
 1) $\bar{7}$; 2) $\bar{8}$; 3) $\bar{9}$; 4) $\bar{10}$.
20. Мультипликативную группу обратимых элементов образует следующая совокупность классов вычетов по модулю 8.
 1) $\{\bar{0},\bar{1},\bar{3},\bar{5}\}$; 2) $\{\bar{1},\bar{3},\bar{5},\bar{7}\}$; 3) $\{\bar{1},\bar{3},\bar{7}\}$; 4) $\{\bar{1},\bar{2},\bar{3},\bar{5},\bar{7}\}$.

4. СРАВНЕНИЯ И СИСТЕМЫ СРАВНЕНИЙ С НЕИЗВЕСТНОЙ ВЕЛИЧИНОЙ

1. Степень сравнения $36x^6+18x^5-6x^4-4x^3+x^2+5x+1 \equiv 0 \pmod{6}$ равна: 1) 6; 2) 5; 3) 4; 4) 3.
2. Сравнение $20x^3-19x^2+15x+6 \equiv 0 \pmod{5}$ равносильно сравнению:
 1) $4x^2+1 \equiv 0 \pmod{5}$; 2) $x^2+1 \equiv 0 \pmod{5}$; 3) $x^2-1 \equiv 0 \pmod{5}$; 4) $3x+1 \equiv 0 \pmod{5}$.
3. Число решений сравнения $ax \equiv b \pmod{11}$ **может** быть равно: 1) 0; 2) 1; 3) 2; 4) 11.
4. Число решений сравнения $ax \equiv b \pmod{10}$ в случае его разрешимости **не может** быть равным: 1) 2; 2) 3; 3) 4; 4) 5.
5. Сравнение $ax \equiv 18 \pmod{30}$ в зависимости от принимаемого значения a может иметь различное количество решений. Установите соответствие между значением a и числом решений сравнения $ax \equiv 18 \pmod{30}$:
 1) $a=7$; а) 0;
 2) $a=6$; б) 1;
 3) $a=5$; в) 3;
 4) $a=3$. г) 6.
6. Решением сравнения $13x \equiv 4 \pmod{5}$ **является** класс вычетов: 1) $\bar{1}$; 2) $\bar{2}$; 3) $\bar{3}$; 4) $\bar{4}$.
7. Решением сравнения $15x \equiv 9 \pmod{6}$ **не является** класс вычетов: 1) $\bar{1}$; 2) $\bar{2}$; 3) $\bar{3}$; 4) $\bar{5}$.
8. Неразрешимыми являются системы сравнений:
 1) $\begin{cases} 2x \equiv 1 \pmod{4}; \\ 3x \equiv 2 \pmod{5}; \end{cases}$ 2) $\begin{cases} 2x \equiv 1 \pmod{3}; \\ 3x \equiv 2 \pmod{4}; \end{cases}$ 3) $\begin{cases} x \equiv 3 \pmod{5}; \\ x \equiv 2 \pmod{3}; \end{cases}$ 4) $\begin{cases} x \equiv 2 \pmod{3}; \\ 3x \equiv 2 \pmod{6}. \end{cases}$
9. Решением системы сравнений $\begin{cases} a_1x \equiv b_1 \pmod{m_1} \\ a_2x \equiv b_2 \pmod{m_2} \end{cases}$
 в случае её разрешимости является класс вычетов по модулю
 1) $m=m_1+m_2$; 2) $m=\text{НОД}(m_1,m_2)$; 3) $m=\text{НОК}(m_1,m_2)$; 4) $m=m_1 \cdot m_2$.
10. Чтобы найти числа, которые при делении на 4 и 5 дают, соответственно, остатки 2 и 3, надо решить систему сравнений

$$1) \begin{cases} x \equiv 2 \pmod{4}; \\ x \equiv 3 \pmod{5}; \end{cases} \quad 2) \begin{cases} 2x \equiv 1 \pmod{4}; \\ 3x \equiv 1 \pmod{5}; \end{cases} \quad 3) \begin{cases} 4x \equiv 1 \pmod{5}; \\ 5x \equiv 1 \pmod{4}; \end{cases} \quad 4) \begin{cases} x \equiv 4 \pmod{2}; \\ x \equiv 5 \pmod{3}. \end{cases}$$

5. КОЛЬЦО МНОГОЧЛЕНОВ НАД ПОЛЕМ

1. Остаток от деления многочлена $x^4 + x^3 - 3x^2 - 4x - 1$ на многочлен $x^3 + x^2 - x - 1$ равен:
1) $2x^2 + 3x + 1$; 2) $-2x^2 - 3x - 1$; 3) $2x^2 - 3x - 1$; 4) $-2x^3 - 3x + 1$.
2. Неполное частное от деления многочлена $3x^3 - 2x^2 + x + 2$ на многочлен $x^2 - x + 1$ равно:
1) $-x + 1$; 2) $3x + 1$; 3) $3x + 2$; 4) $x - 1$.
3. Степень остатка от деления многочлена $f(x) = x^6 + 5$ на $x^2 + x - 1$ может быть равной:
1) 5; 2) 4; 3) 2; 4) 1.
4. Степень остатка от деления некоторого многочлена $f(x)$ на многочлен $x^2 + x - 1$ **не может** быть равной:
1) 3; 2) 2; 3) 1; 4) 0.
5. Остаток от деления $f(x) = x^3 - 5x^2 + 8x - 4$ на $x - 2$ равен:
1) 1; 2) 0; 3) 2; 4) 4.
6. Остаток от деления многочлена $x^4 + 4x^3 - 2x^2 - 12x + 9$ на $x + 2$ равен:
1) 7; 2) -1 ; 3) 6; 4) 9.
7. Неполное частное от деления многочлена $x^4 - 3x^2 + x + 5$ на $x - 2$ равно:
1) $x^2 - x + 1$; 2) $x^3 + 2x^2 + x + 3$; 3) $x^3 + 2x^2 - 7x + 15$; 4) $x^3 + 2x^2 + x - 3$.
8. Корнем многочлена $f(x) = x^3 - 5x^2 + 8x - 4$ является число:
1) 1; 2) -1 ; 3) -2 ; 4) 4.
9. Известно, что многочлен $f(x) = x^4 + 4x^3 - 2x^2 - 12x + 9$ при делении на $(x + 3)^2$ даёт в остатке 0. Его корнем является число: 1) 3; 2) 9; 3) -3 ; 4) 6.
10. Многочлен наименьшей степени с числовыми коэффициентами, имеющий двукратный корень -1 и простой корень 1, равен:
1) $x^2 - x + 2$; 2) $x^4 + x^2 - x - 1$; 3) $x^3 + x^2 - x - 1$; 4) $x^3 - x^2 + x - 1$.
11. Кратность корня $x = 1$ многочлена $f(x) = x^5 - 5x^4 - 2x^3 + 26x^2 - 31x + 11$ равна:
1) 3; 2) 2; 3) 1; 4) 4.
12. Показатель кратности корня 2 многочлена $f(x) = x^5 - 5x^4 + 7x^3 - 2x^2 + 4x - 8$ равен:
1) 1; 2) 2; 3) 3; 4) 4.
13. Наибольший общий делитель многочленов $f(x) = (x - 1)(x + 2)^2(x - 3)$ и $q(x) = (x + 2)(x - 3)^2(x + 1)$ равен:
1) $x^2 - x - 6$; 2) $x^2 - 1$; 3) $(x^2 - x - 6)^2$; 4) $x^2 + 3x + 2$.
14. Наибольший общий делитель многочленов $f(x) = x^4 - 3x^2 + x + 2$ и $q(x) = 0$ равен:
1) $x^4 - 3x^2 + x + 2$; 2) 0; 3) $-2x^4 + 6x^2 - 2x - 4$; 4) 1.
15. Наименьшее общее кратное многочленов $f(x) = (x - 1)(x + 2)$ и $q(x) = (x + 1)(x + 2)^2$ равно:
1) $(x - 1)(x + 2)^2$; 2) $(x^2 - 1)(x + 2)$; 3) $(x^2 - 1)(x + 2)^2$; 4) $(x + 1)(x - 1)$.
16. Произведение всех комплексных корней многочлена $x^4 + 4x^3 - 2x^2 - 12x + 9$ равно:
1) 6; 2) 9; 3) -9 ; 4) -3 .
17. Сумма всех комплексных корней многочлена $x^4 + 4x^3 - 2x^2 - 12x + 9$ равна:
1) -9 ; 2) 9; 3) 4; 4) -4 .
18. Сумма всех комплексных корней многочлена $4x^5 + 12x^4 + x^3 + 6x^2 + 10x + 3$ равна:
1) -12 ; 2) 12; 3) 3; 4) -3 .

19. Произведение всех комплексных корней многочлена $4x^5 + 12x^4 + x^3 + 6x^2 + 10x + 4$ равно:
1) 1; 2) -1; 3) 4; 4) -4.
20. Числа x_1, x_2 являются корнями уравнения $5x^2 + x + 3 = 0$. Значение выражения $\frac{1}{x_1} + \frac{1}{x_2}$ равно:
1) $\frac{3}{5}$; 2) $-\frac{3}{25}$; 3) $-\frac{1}{3}$; 4) $\frac{25}{3}$.
21. Число корней уравнения $x^5 - 6x^4 - 20x^2 + 14x - 4 = 0$ в поле комплексных чисел равно:
1) 0; 2) 5; 3) 1; 4) 6.
22. Имеет хотя бы один действительный корень многочлен:
1) $x^2 - 3x + 5$; 2) $x^{17} + 5x^6 - x + 9$; 3) $x^2 + x + 1$; 4) $x^2 - 6x + 9$.
23. Неприводимыми над полем действительных чисел являются многочлены:
1) $x^2 + 3x + 5$; 2) $2x^3 - 3x^2 + 1$; 3) $5x - 4$; 4) 7.
24. Приводимыми над $\mathbb{R}$ многочленами являются:
1) $x^2 - x - 3$; 2) $x + 9$; 3) $x^{10} + x + 1$; 4) $2x^3 + x^2 - x - 2$; 5) $x^2 + x + 1$.
25. Не имеет целых корней многочлен:
1) $3x^2 - 2x - 1$; 2) $4x^3 - 4x^2 - x + 1$; 3) $9x^2 - 6x + 1$; 4) $3x + 9$
26. Сумма целых корней уравнения $x^4 + 4x^3 - 2x^2 - 12x + 9 = 0$ равна:
1) 4; 2) -4; 3) -2; 4) 2.
27. Неприводимыми над $\mathbb{Q}$ являются многочлены:
а) $7x^{13} + 2x^4 - 16x^3 + 4x - 10$;
б) $4x^3 + x + 5$;
в) $x^2 - 7x + 30$;
г) $x^2 + 7x - 30$.
28. Приводимыми над $\mathbb{Q}$ являются многочлены:
а) $12x^7 + 5x^6 - 15x^3 + 5x - 20$; б) $x^2 + 3x + 5$; в) $x^2 - 6x - 2$; г) $4x^3 + x + 5$; д) $x^3 + 1$.

Критерии оценки теста:

1. Каждое задание теста оценивается в 1 балл.
2. Итоговая оценка за весь тест соответствует проценту правильных ответов по отношению к общему числу всех вопросов в тесте.
3. Оценка за тест считается положительной, если студент ответил правильно не менее, чем на 60% вопросов теста.

5. Типовое контрольное задание на этапе формирования УК-1 и ПК-3:

Программа экзамена по абстрактной и компьютерной алгебре (4 семестр)

1. Алгебры и алгебраические системы. Алгебры с одной бинарной алгебраической операцией: полугруппа, моноид, группа. Примеры таких алгебр.
2. Определение группы. Примеры групп. Простейшие свойства группы. Подгруппы
3. Определение кольца. Примеры колец. Z_m как пример конечного нечислового кольца. Простейшие свойства кольца.
4. Определение поля. Примеры полей. Z_p как пример конечного нечислового поля.
5. Простейшие свойства поля. Отсутствие в поле делителей нуля.
6. Подполе. Расширение поля.
7. Отношение делимости и его простейшие свойства.
8. Деление с остатком.
9. НОД и его свойства.

10. Алгоритм Евклида и его сложность; теорема Ламе. Расширенный алгоритм Евклида.
11. Взаимно простые числа; необходимое и достаточное условие взаимной простоты двух чисел; необходимое и достаточное условие делимости целого числа на произведение взаимно простых чисел.
12. НОК и его свойства; теорема о взаимосвязи н.о.д. и н.о.к. двух целых чисел
13. Простые числа. Свойства простых чисел; свойство наименьшего простого делителя числа; основная теорема арифметики.
14. Систематические числа; единственность представления числа в виде систематической записи по любому основанию; переход из одной системы счисления в другую; арифметические операции над систематическими числами. Представление больших целых чисел в памяти компьютера.
15. Отношение сравнения в кольце целых чисел и его свойства.
16. Функция Эйлера и ее свойства. Теоремы Эйлера и Ферма.
17. Сравнения с неизвестной величиной: степень сравнения, решение сравнения, равносильные сравнения. Сравнения первой степени и их решение.
18. Системы сравнений. Системы сравнений первой степени.
19. Модулярное представление числа. Преобразование модулярного представления целого числа в его позиционное представление. Точные вычисления, использующие модулярную арифметику.
20. Кольцо многочленов от одной переменной над полем.
21. Отношение делимости в кольце многочленов над полем. НОД и НОК двух многочленов в кольце многочленов над полем. Свойства НОД и НОК.
22. Теорема о делении с остатком в кольце многочленов над полем. Алгоритм Евклида в кольце многочленов над полем.
23. Неприводимые над данным полем многочлены. Свойства неприводимых над полем многочленов. Теорема о разложении многочлена над полем в произведение неприводимых над данным полем многочленов.
24. Деление многочлена на двучлен $x-a$. Теорема Безу. Схема Горнера. Формула Тейлора.
25. Многочлены над полем комплексных чисел. Основная теорема алгебры и ее следствия. Формулы Виета.
26. Многочлены над полем действительных чисел и их свойства.
27. Целые и рациональные корни многочлена с рациональными коэффициентами. Критерий неприводимости Эйзенштейна.
28. Компьютерное представление полиномов. Алгоритмы операций над полиномами.
29. Понятие о кодировании. Выбор алфавита для хранения информации. Алфавитное кодирование. Неравенство Макмиллана как необходимое и достаточное условие существования однозначного декодирования.
30. Помехоустойчивое кодирование. Свойства кодов по обнаружению и исправлению ошибок. Простейшие методы обнаружения одиночных ошибок (проверка на четность, двоичный код с защитой удвоенными элементами, и т.д.).
31. Понятие о криптографии. Криптосистемы с закрытым ключом (без передачи ключей).
32. Криптосистема с открытым ключом. Надежность системы.
33. Электронная подпись.

Критерии оценки ответа на экзамене:

1. Зачет с оценкой проводится по билетам, в которые включены по два вопроса из программы.
2. При оценивании ответа учитывается: правильность формулировок; установление взаимосвязи теории и практики; содержательность и аргументированность, полнота и структурная логичность ответа; глубина знаний вопроса.
3. При допущенных ошибках и неточностях в формулировках определений и доказательствах теорем оценка за ответ снижается.
4. Допуск к экзамену осуществляется только при выполнении всех видов практических работ: контрольные работы по теории делимости, по теории сравнений, ИДЗ по многочленам, итоговый тест.
5. Студент, успешно отчитавшийся (не менее 60 %) по всем формам контроля (2 теоретических опроса, контрольные работы по теории делимости, по теории сравнений, ИДЗ по многочленам, итоговый тест), по его желанию может быть освобожден от экзамена с выставлением оценки по рейтингу.
6. Рейтинговая оценка на экзамене может быть улучшена не более, чем на 30%.

Уровни сформированности компетенций УК-1, ПК-3 в рамках дисциплины:

Уровни сформированности компетенций УК-1, ПК-3	Основные признаки уровня
Пороговый	При выполнении заданий всех форм контроля студент демонстрирует знание: - определений основных алгебраических структур компьютерной математики (полугрупп, групп, колец, полей); - определения и свойств отношения делимости целых чисел; - определения отношения сравнения целых чисел и его простейшие свойства; проявляет умение: - применять имеющиеся знания по теории делимости к решению типовых задач на делимость; - представлять числа систематической записью по любому основанию, переходить от одной системы счисления к другой, выполнять операции над числами в любой позиционной системе счисления; - сравнивать целые числа по любому модулю, выполнять операции сложения и умножения в кольцах классов вычетов по любому модулю; - решать сравнения первой степени и их системы; - выполнять по образцу основные операции модулярной арифметики; - решать типовые задачи теории многочленов над полем. По итогам балльно-рейтинговой системы сумма рейтинговых баллов студента составляет от 60 до 75 баллов.
Базовый	При выполнении заданий всех форм контроля студент демонстрирует знание:

	- определений основных алгебраических структур компьютерной математики (полугрупп, групп, колец, полей); - определений основных понятий и фактов теории делимости в кольце целых чисел; - определений основных понятий и фактов теории сравнений в кольце целых чисел; - определений основных понятий теории многочленов от одной переменной над полем; проявляет умение: - распознавать основные алгебраические структуры компьютерной математики среди различных алгебр; - применять имеющиеся знания по теории делимости к решению типовых задач на делимость; - представлять числа систематической записью по любому основанию, переходить от одной системы счисления к другой и выполнять операции над числами в любой позиционной системе счисления; - использовать основные факты теории сравнений в кольце целых чисел при решении задач модулярной арифметики, возможно допуская при этом некоторые неточности; - решать типовые задачи теории многочленов над полем; показывает владение: - навыками решения основных типовых задач данной предметной области. По итогам балльно-рейтинговой системы сумма рейтинговых баллов студента составляет от 75 до 87 баллов
Повышенный	При выполнении заданий всех форм контроля студент демонстрирует знание: - определений основных понятий абстрактной алгебры, необходимых для глубокого понимания теоретических основ компьютерной алгебры; - основополагающих фактов теории делимости и теории сравнений в кольце целых чисел, положенных в основу построения модулярной арифметики, составляющей фундамент компьютерной алгебры и теории защиты информации; - способов представления в компьютере математических объектов (целых и рациональных чисел, многочленов от одной и нескольких переменных, рациональных и алгебраических выражений); - начальных сведений о сущности теории и способов кодирования; - основ теории делимости в кольце целых чисел; - основ теории сравнений в кольце целых чисел; - основ теории многочленов от одной переменной

	над полем; проявляет умение: - узнавать основные алгебры (полугруппы, группы, кольца, поля); определять их свойства и приводить примеры конечных и бесконечных групп, колец, полей; - использовать основные факты теории делимости (свойства отношения делимости, свойства простых и взаимно простых чисел) при решении задач на делимость; - использовать основные факты теории сравнений в кольце целых чисел при решении задач модулярной арифметики и объяснении сущности современных методов шифрования (открытый ключ. электронная подпись); - использовать основные факты теории многочленов при рассмотрении основных алгоритмов полиномиальной арифметики; показывает владение: - навыками применения полученных знаний и умений в различных ситуациях (в пределах изученной тематики курса); - представлениями о взаимосвязи абстрактной и компьютерной алгебр. По итогам балльно-рейтинговой системы сумма рейтинговых баллов студента составляет от 87 до 100 баллов.
--	---

Методические материалы, определяющие процедуры оценивания

Целью промежуточной аттестации по данной дисциплине является оценка уровня сформированности компетенций в результате усвоения знаний, приобретения умений, навыков и опыта деятельности в рамках освоения дисциплины (модуля).

Процедура оценивания охватывает обучающихся, освоивших дисциплину (модуль). Процедура оценивания проводится по окончании освоения дисциплины (модуля). Оценка уровня сформированности компетенций на этапах их формирования определяется на основании собеседования, включающих теоретические вопросы или задания, в которых обучающемуся предлагают осмыслить реальную профессионально-ориентированную ситуацию, необходимую для решения данной проблемы; при этом актуализируется определенный комплекс знаний, необходимый для разрешения данной проблемы. Оценивание ответов обучающихся проводится в соответствии с приведенными критериями.

На основании ответов (ответов на тест, выполнение практико-ориентированного задания) оценивается уровень сформированности компетенций на этапах их формирования в рамках дисциплины (модуля), а также уровень знаний, умений, навыков и опыта деятельности, по результатам выставляется оценка. Результаты проведения процедуры в установленном порядке проставляются преподавателем в зачетные книжки

обучающихся и электронные ведомости. По результатам проведения процедуры оценивания преподавателем делается вывод о результатах промежуточной аттестации по дисциплине.

Процедура оценивания (экзамен) соответствует действующим в вузе текущим положениям, включая Положение о рейтинговой системе текущего контроля успеваемости и промежуточной аттестации студентов.