

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ
ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Забайкальский государственный университет»
(ФГБОУ ВО «ЗабГУ»)

Факультет естественных наук, математики и технологий
Кафедра Математики и информатики

УТВЕРЖДАЮ:

Декан факультета

Факультет естественных
наук, математики и
технологий

Токарева Юлия Сергеевна

« ____ » _____ 20 ____
г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.В.05 Элементы абстрактной и компьютерной алгебры
на 108 часа(ов), 3 зачетных(ые) единиц(ы)
для направления подготовки (специальности) 01.03.02 - Прикладная математика и
информатика

составлена в соответствии с ФГОС ВО, утвержденным приказом
Министерства образования и науки Российской Федерации от
« ____ » _____ 20 ____ г. № ____

Профиль – Исследование операций и системный анализ (для набора 2022)
Форма обучения: Очная

1. Организационно-методический раздел

1.1 Цели и задачи дисциплины (модуля)

Цель изучения дисциплины:

овладение основами понятиями абстрактной алгебры; овладение методами программной манипуляции математическими выражениями, заданными символично.

Задачи изучения дисциплины:

овладение основными понятиями и фактами, характеризующими свойства абстрактных алгебраических объектов: группа, кольцо, поле.

формирование умений в области алгоритмически разрешимых алгебраических задач и проблем.

овладение навыками анализа, оценки эффективности и сложности алгоритмов символьных преобразований.

формирование умений реализации алгебраических алгоритмов посредством известных языков программирования.

1.2. Место дисциплины (модуля) в структуре ОП

Курс «Элементы абстрактной и компьютерной алгебры» имеет большое общеобразовательное значение и глубокие межпредметные связи с другими курсами: «Алгебра и геометрия», «Основы информатики». Компьютерная алгебра является одной из областей математики и информатики, особенно активно развивающейся в последние годы. Усилия специалистов в этой области направлены как на разработку новых алгоритмов, так и на создание систем компьютерной алгебры, которые все шире используются и в научных исследованиях, и в практических приложениях. Термин «компьютерная алгебра» (или символьные и алгебраические вычисления) объясняется способностью компьютеров манипулировать математическими выражениями, заданными символично, а не численно, подобно тому, как это делается в алгебре при помощи карандаша и бумаги. Начиная с 1960 г. было разработано много программных систем, предназначенных для различного рода символьных вычислений. Операции над многочленами и рациональными функциями составляют основу любой системы символьных преобразований, поэтому исследования в этой области включают в себя развитие и анализ эффективных алгоритмов для разложения на множители, вычисления наибольших общих делителей и отделения вещественных корней многочленов. Компьютерная алгебра включает в себя большое количество различных тем, а поскольку она до настоящего времени находится в стадии развития, к имеющемуся списку тем постоянно добавляются новые. Дисциплина подразумевает рассмотрение различных вопросов абстрактной и компьютерной алгебры, их взаимосвязей.

1.3. Объем дисциплины (модуля) с указанием трудоемкости всех видов учебной работы

Общая трудоемкость дисциплины (модуля) составляет 3 зачетных(ые) единиц(ы), 108 часов.

Виды занятий	Семестр 6	Всего часов
--------------	-----------	-------------

Общая трудоемкость		108
Аудиторные занятия, в т.ч.	48	48
Лекционные (ЛК)	32	32
Практические (семинарские) (ПЗ, СЗ)	16	16
Лабораторные (ЛР)	0	0
Самостоятельная работа студентов (СРС)	60	60
Форма промежуточной аттестации в семестре	Зачет	0
Курсовая работа (курсовой проект) (КР, КП)		

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Планируемые результаты освоения образовательной программы		Планируемые результаты обучения по дисциплине
Код и наименование компетенции	Индикаторы достижения компетенции, формируемые в рамках дисциплины	Дескрипторы: знания, умения, навыки и (или) опыт деятельности
ОПК-1	ОПК-1.1. Знает: основные понятия, факты, концепции, принципы математики, информатики и естественных наук для решения практических задач, связанных с прикладной математикой и информатикой	Знать: основные понятия абстрактной алгебры; основные понятия теории кодирования; основные понятия теории криптографии; первые криптографические шифры, известные в истории
ОПК-1	ОПК-1.2. Умеет применять на практике математические модели и компьютерные технологии для решения практических задач, возникающих в профессиональной деятельности	Уметь: решать алгебраические задачи на группы и кольца; решать алгебраические задачи в кольце целых чисел и кольце многочленов от одной переменной
ОПК-1	ОПК-1.3. Владеет умением выполнять стандартные действия, решения типовых задач с учетом основных понятий и общих закономерностей, формируемых в рамках базовых математических и	Владеть: понятийным аппаратом абстрактной алгебры; понятийным аппаратом компьютерной алгебры; простейшими криптографическими шифрами

	естественнонаучных дисциплин	
ПК-2	ПК-2.1. Обладает: базовыми знаниями, полученными в области математических и (или) естественных наук, программирования и информационных технологий.	Знать: основные свойства объектов абстрактной алгебры; основные свойства объектов теории кодирования и теории криптографии
ПК-2	ПК-2.2. Умеет разрабатывать и реализовывать алгоритмы математических моделей, в том числе на базе языков и пакетов прикладных программ моделирования	Уметь: решать задачи компьютерной алгебры, используя алгоритмы абстрактной алгебры; программно реализовывать алгебраические алгоритмы; решать задачи из криптографии
ПК-2	ПК-2.3. Владеет практическим опытом применения указанных выше методов и технологий	Владеть: математическими алгоритмами для их дальнейшего использования в информатике; навыками использования пакетов компьютерной алгебры для решения математических задач

3. Содержание дисциплины

3.1. Разделы дисциплины и виды занятий

3.1 Структура дисциплины для очной формы обучения

Модуль	Номер раздела	Наименование раздела	Темы раздела	Всего часов	Аудиторные занятия			С Р С
					Л К	П З (С З)	Л Р	
1	1.1	Группы, кольца, идеалы, факторкольца	Бинарные алгебраические операции. Алгебры с 1-ой б.а.о. Группы, их свойства. Подгруппы. Нормальные подгруппы и факторгруппы. Морфизм групп. Изоморфизм групп	27	4	8	0	15
2	2.1	Кольцо целых чисел. Теория сравнений	Кольцо Z . Отношение делимости и его свойства. Теорема о	27	4	8	0	15

			деления с остатком. НОД и НОК. Алгоритм Евклида. Простые числа. Сравнения в кольце целых чисел					
3	3.1	Кольцо многочленов от одной переменной	Построение кольца $F[x]$. Отношение делимости в $F[x]$. Теорема о делении с остатком. Схема Горнера, формула Тейлора. Корни многочленов, теорема Безу. НОД и НОК многочленов. Алгоритм Евклида	27	4	8	0	15
4	4.1	Теория кодирования. Симметричные и ассиметричные криптосистемы	Теория кодирования. Симметричные и ассиметричные криптосистемы.	27	4	8	0	15
Итого				108	16	32	0	60

3.2. Содержание разделов дисциплины

3.2.1. Лекционные занятия, содержание и объем в часах

Модуль	Номер раздела	Тема	Содержание	Трудоемкость (в часах)
1	1.1	Бинарные алгебраические операции. Алгебры с 1-ой б.а.о. Группы, их свойства	Бинарные алгебраические операции. Алгебры с 1-ой б.а.о.: группоид, полугруппа, моноид, группа. Группы, их свойства. Абелевы группы	2
	1.1	Подгруппы. Нормальные подгруппы и факторгруппы. Морфизм групп.	Подгруппы. Смежные классы. Свойства смежных классов. Нормальные подгруппы и факторгруппы. Морфизм групп. Изоморфизм групп	2

		Изоморфизм групп		
2	2.1	Кольцо Z . Отношение делимости и его свойства. Теорема о делении с остатком. НОД и НОК. Алгоритм Евклида. Простые числа	Кольцо Z . Отношение делимости и его свойства. Теорема о делении с остатком. НОД и НОК. Алгоритм Евклида. Простые числа. Свойства простых чисел	2
	2.1	Сравнения в кольце целых чисел	Отношение сравнения в кольце целых чисел, его свойства. Сравнения первой степени, сравнения высших степеней, системы сравнений	2
3	3.1	Построение кольца $F[x]$. Отношение делимости в $F[x]$. Теорема о делении с остатком. Схема Горнера, формула Тейлора	Построение кольца $F[x]$. Отношение делимости в $F[x]$. Теорема о делении с остатком. Схема Горнера, формула Тейлора	2
	3.1	Корни многочленов, теорема Безу. НОД и НОК многочленов. Алгоритм Евклида	Корни многочленов, теорема Безу. НОД и НОК многочленов. Свойства НОД и НОК. Алгоритм Евклида	2
4	4.1	Симметричные и ассимметричные криптосистемы	Основные понятия. История криптографии. Криптосистемы	4

3.2.2. Практические занятия, содержание и объем в часах

--	--	--	--	--

Модуль	Номер раздела	Тема	Содержание	Трудоемкость (в часах)
1	1.1	Бинарные алгебраические операции. Алгебры с 1-ой б.а.о. Группы, их свойства	Бинарные алгебраические операции. Алгебры с 1-ой б.а.о. Группы,	4
	1.1	Подгруппы. Нормальные подгруппы и факторгруппы. Морфизм групп. Изоморфизм групп	Подгруппы. Смежные классы. Нормальные подгруппы и факторгруппы. Морфизм групп. Изоморфизм групп	4
2	2.1	Кольцо Z . Отношение делимости и его свойства. Теорема о делении с остатком. НОД и НОК. Алгоритм Евклида. Простые числа	Кольцо Z . Отношение делимости и его свойства. Теорема о делении с остатком. НОД и НОК. Алгоритм Евклида. Простые числа. Решето Эратосфена	4
	2.1	Сравнения в кольце целых чисел	Сравнения. Свойства сравнений. Решение сравнений 1-й степени. Системы сравнений. Приложение сравнений	4
3	3.1	Построение кольца $F[x]$. Отношение делимости в $F[x]$. Теорема о делении с остатком. Схема Горнера, формула Тейлора	Отношение делимости в $F[x]$. Теорема о делении с остатком. Схема Горнера, формула Тейлора	4
	3.1	Корни	Корни многочленов, теорема Безу.	4

		многочленов, теорема Безу. НОД и НОК многочленов. Алгоритм Евклида	НОД и НОК многочленов. Алгоритм Евклида	
4	4.1	Симметричны е и ассимметричны е криптосистем ы	Задачи на использование шифров	8

3.2.3. Лабораторные занятия, содержание и объем в часах

Модуль	Номер раздела	Тема	Содержание	Трудоемкость (в часах)

3.3. Содержание материалов, выносимых на самостоятельное изучение

Модуль	Номер раздела	Содержание материалов, выносимого на самостоятельное изучение	Виды самостоятельной деятельности	Трудоемкость (в часах)
1	1.1	Алгебры с 2-мя бинарными алгебраическими операциями. Кольца, их свойства. Примеры колец. Подкольца и идеалы. Фактор кольца. Морфизмы колец	Составление конспекта Решение практических задач	15
2	2.1	Факториальность кольца Z . Простейшие свойства сравнений. Системы вычетов. Сравнения первой степени	Составление конспекта Решение практических задач	15
3	3.1	Взаимно простые, приводимые и неприводимые многочлены. Разложение на неприводимые множители. Понятие о	Составление конспекта Решение практических задач	15

		многочленах от нескольких переменных		
4	4.1	Информация слов и теоремы кодирования. Неравномерное кодирование слов. Коды, исправляющие ошибки	Составление конспекта Решение практических задач	15

4. Фонд оценочных средств для проведения текущей и промежуточной аттестации обучающихся по дисциплине

Фонд оценочных средств текущего контроля и промежуточной аттестации по итогам освоения дисциплины представлен в приложении.

[Фонд оценочных средств](#)

5. Учебно-методическое и информационное обеспечение дисциплины

5.1. Основная литература

5.1.1. Печатные издания

1. 1. Виноградов И.М. Основы теории чисел: учеб. пособие 12-е изд., стереотип. СПб.; М.; Краснодар: Лань, 2009. 176 с.
2. 2. Казачек Н.А. Элементы абстрактной и компьютерной алгебры. Ч. I. Элементы абстрактной алгебры: учеб.-метод. пособие. Чита: ООО «Экспресс-издательство». 2013. 56 с.
3. 3. Сизый С.В. Лекции по теории чисел : учеб. пособие. М. : ФИЗМАТЛИТ, 2007. 192 с.

5.1.2. Издания из ЭБС

- 1.

5.2. Дополнительная литература

5.2.1. Печатные издания

1. 1. Кормен Т., Лейзерсон Ч., Ривест Р. Алгоритмы: построение и анализ. М.: МЦНМО, 2000. - 263 с.
2. 2. Левин М. Криптография: руководство пользователя / М. Левин. - М.: Познавательная книга плюс. 2001. 320 с.
3. 3. Матрос Д. Ш., Поднебесова Г.Б. Элементы абстрактной и компьютерной алгебры: учеб. пособие для студентов пед. вузов. М.: Академия. 2004. 240 с.

5.2.2. Издания из ЭБС

1. 4. Черпаков И.В. Теоретические основы информатики: учебник и практикум для академического бакалавриата [Электронный ресурс]: М.: Издательство Юрайт, 2017. 353 с.

5.3. Базы данных, информационно-справочные и поисковые системы

Название	Ссылка
http://www.math.ru/lib/formats Math.ru - библиотека	http://www.math.ru

6. Перечень программного обеспечения

Программное обеспечение общего назначения: ОС Microsoft Windows, Microsoft Office, ABBYY FineReader, ESET NOD32 Smart Security Business Edition, Foxit Reader, АИБС "МегаПро".

Программное обеспечение специального назначения:

- 1) Mathematica Standart Version Education

7. Материально-техническое обеспечение дисциплины

Наименование помещений для проведения учебных занятий и для самостоятельной работы обучающихся	Оснащенность специальных помещений и помещений для самостоятельной работы
Учебные аудитории для проведения занятий лекционного типа	Состав оборудования и технических средств обучения указан в паспорте аудитории, закрепленной расписанием по факультету
Учебные аудитории для проведения практических занятий	
Учебные аудитории для промежуточной аттестации	
Учебные аудитории для проведения групповых и индивидуальных консультаций	Состав оборудования и технических средств обучения указан в паспорте аудитории, закрепленной расписанием по кафедре
Учебные аудитории для текущей аттестации	

8. Методические рекомендации по организации изучения дисциплины

Некоторые разделы (делимость в кольце целых чисел, теория многочленов и др.) имеют прямую связь со школьным курсом математики, поэтому необходимо обращаться к школьному опыту студентов (обучению и преподаванию).

Преподавание алгебраических разделов курса должно сопровождаться примерами их приложений в информатике.

Математические алгоритмы (Алгоритм Евклида, Решето Эратосфена и др.) необходимо предлагать студентам реализовывать на известном им языке программирования и демонстрировать программы всей группе на практических занятиях.

Разработчик/группа разработчиков:
Маргарита Геннадьевна Никифорова

Типовая программа утверждена

Согласована с выпускающей кафедрой
Заведующий кафедрой

_____ «___» _____ 20__ г.