Министерство науки и высшего образования РФ
Федеральное государственное автономное образовательное учреждение высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.В.ДВ.05.02 Конечные поля и многочлены над ними

наименование дисциплины (модуля) в соответствии с учебным планом

Направление подготовки / специальность

01.03.04 Прикладная математика

Направленность (профиль)

01.03.04 Прикладная математика

Форма обучения очная

Год набора 2019

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Программу составили _____

Н.Н.Осипов

должность, инициалы, фамилия

1 Цели и задачи изучения дисциплины

1.1 Цель преподавания дисциплины

Целью дисциплины «Конечные поля и многочлены над ними» является формирование у студентов знаний и представлений по основам теории конечных полей. Указанная дисциплина имеет существенное значение в системе подготовки специалистов в области прикладной математики и компьютерных наук. В частности, она может быть использована при чтении таких специальных дисциплин, как «Обработка сигналов» и «Основы компьютерной алгебры». Предлагаемые в дисциплине разделы теории конечных полей давно вошли в разряд общеизучаемых и составляют неотъемлемую часть языка современной прикладной математики и компьютерных наук.

1.2 Задачи изучения дисциплины

Основной задачей дисциплины «Конечные поля и многочлены над ними» является дальнейшее развитие у студентов математической культуры в области таких дискретных алгебраических структур как конечные поля.

1.3 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Код и наименование индикатора достижения компетенции	Запланированные результаты обучения по дисциплине
ПК-3: Способен применять математический аппарат для решения поставленных задач.	
ПК-3.1: Знать основы применения математического аппарата для решения поставленных задач.	основные понятия теории конечных полей конструировать неприводимые многочлены над конечными полями основными навыками в употреблении модулярной арифметики, основными приемами факторизации многочленов над конечными полями
ПК-3.2: Уметь самостоятельно разрабатывать математические модели, на основе содержательного и физического описания процессов и объектов.	строение конечных полей вычислять минимальные многочлены элементов конечного поля практическими навыками в употреблении критерия неприводимости Батлера и алгоритма факторизации Берлекэмпа (включая его вероятностную версию) многочленов над конечными полями
ПК-3.3: Владеть основными понятиями и результатами основополагающих математических дисциплин;	основные теоремы о неприводимых многочленах и методах факторизации многочленов над конечными полями применять алгоритмы построения неприводимых и примитивных многочленов над конечными полями практическими навыками в употреблении критериев неприводимости и алгоритмов факторизации (в том числе и вероятностных) многочленов над конечными полями

1.4 Особенности реализации дисциплины

Язык реализации дисциплины: Русский.

Дисциплина (модуль) реализуется с применением ЭО и ДОТ

URL-адрес и название электронного обучающего курса: https://e.sfu-kras.ru/course/view.php?id=193.

2. Объем дисциплины (модуля)

Вид учебной работы	Всего, зачетных единиц (акад.час)	е 1
Контактная работа с преподавателем:	**1,5 (54)**	
занятия лекционного типа	0,5 (18)	
практические занятия	1 (36)	
Самостоятельная работа обучающихся:	**1,5 (54)**	
курсовое проектирование (КП)	Нет	
курсовая работа (КР)	Нет	

3 Содержание дисциплины (модуля)

3.1 Разделы дисциплины и виды занятий (тематический план занятий)

№ п/п	Модули, темы (разделы) дисциплины	Контактная работа, ак. час.							
		Занятия лекционного типа		Занятия семинарского типа				Самостоятельная работа, ак. час.	
				Семинары и/или Практические занятия		Лабораторные работы и/или Практикумы			
		Всего	В том числе в ЭИОС	Всего	В том числе в ЭИОС	Всего	В том числе в ЭИОС	Всего	В том числе в ЭИОС
1. Основы теории конечных полей									
	1. Построение конечных полей с помощью неприводимых многочленов.	1							
	2. Конечное поле как векторное пространство. Число элементов конечного поля и число подпространств данной размерности.	1							
	3. Мультипликативная группа конечного поля. Примитивные элементы конечного поля.	1							
	4. Функция Мебиуса. Число неприводимых многочленов данной степени над конечным полем	1							
	5. Подполя и автоморфизмы конечного поля.	1							
	6. Порядок многочлена над конечным полем и примитивные многочлены.	1							

7. Построение примитивных многочленов над конечным полем. Число примитивных многочленов данной степени.	1							
8. Техника вычислений в конечных полях.	1							
9. Построение конечных полей с помощью неприводимых многочленов.			2					
10. Конечное поле как векторное пространство. Число элементов конечного поля и число подпространств данной размерности.			2					
11. Мультипликативная группа конечного поля. Примитивные элементы конечного поля.			2					
12. Функция Мебиуса. Число неприводимых многочленов данной степени над конечным полем.			2					
13. Подполя и автоморфизмы конечного поля.			2					
14. Порядок многочлена над конечным полем и примитивные многочлены.			2					
15. Построение примитивных многочленов над конечным полем. Число примитивных многочленов данной степени.			2					
16. Техника вычислений в конечных полях.			2					
17. Основы теории конечных полей							6	
2. Факторизация многочленов над конечными полями								
1. Критерий Батлера неприводимости многочленов над конечным полем.	1							
2. Вероятностный алгоритм тестирования на неприводимость многочленов над конечным полем.	1							
3. Факторизация многочленов над конечным полем.	1							

4. Алгоритм Берлекэмпа.	1							
5. Модификация алгоритма Берлекэмпа для случая больших конечных полей.	1							
6. Метод Цассенхауза.	1							
7. Вероятностная версия алгоритма Берлекэмпа	1							
8. Вероятностный алгоритм Кантора-Цассенхауза факторизации многочленов над конечным полем.	1							
9. Вероятностный алгоритм нахождение корней многочленов над конечным полем.	1							
10. Алгоритмы решения квадратных уравнений над конечным полем.	1							
11. Критерий Батлера неприводимости многочленов над конечным полем.			2					
12. Вероятностный алгоритм тестирования на неприводимость многочленов над конечным полем.			2					
13. Факторизация многочленов над конечным полем.			2					
14. Алгоритм Берлекэмпа.			2					
15. Модификация алгоритма Берлекэмпа для случая больших конечных полей.			2					
16. Метод Цассенхауза.			2					
17. Вероятностная версия алгоритма Берлекэмпа			2					
18. Вероятностный алгоритм Кантора-Цассенхауза факторизации многочленов над конечным полем.			2					
19. Вероятностный алгоритм нахождение корней многочленов над конечным полем			2					
20. Алгоритмы решения квадратных уравнений над конечным полем.			2					

21. Факторизация многочленов над конечными полями							12	
22.								
Всего	18		36				18	

4 Учебно-методическое обеспечение дисциплины

4.1 Печатные и электронные издания:

1. Кострикин А. И. Введение в алгебру: Т. 3. Основные структуры алгебры: учебник для студентов по специальностям "Математика" и "Прикладная математика"(Москва: Физико-математическая литература).
2. Глухов М.М., Елизаров В.П., Нечаев А.А. Алгебра: Т. 1: Учебник для вузов: В 2-х т.(Москва: Гелиос АРВ).
3. Глухов М.М., Елизаров В.П., Нечаев А.А. Алгебра: Т. 2: Учебник для вузов: В 2-х т.(Москва: Гелиос АРВ).
4. Лидл Р., Нидеррайтер Г., Нечаев В. И. Конечные поля: Том 1: [в 2-х томах] : перевод с английского(Москва: Мир).
5. Лидл Р., Нидеррайтер Г., Нечаев В. И. Конечные поля: Том 2: [в 2-х томах] : перевод с английского(Москва: Мир).
6. Власов Е. Г. Конечные поля в телекоммуникационных приложениях. Теория и применение FEC, CRC, M-последовательностей: практическое пособие(Москва: ООО "Научно-издательский центр ИНФРА-М").
7. Осипов Н. Н., Медведева М. И. Многочлены над конечными полями: учебное пособие [для студентов специальности 01.03.04 «Прикладная математика»](Красноярск: СФУ).

4.2 Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства (программное обеспечение, на которое университет имеет лицензию, а также свободно распространяемое программное обеспечение):

1. Не требуется.

4.3 Интернет-ресурсы, включая профессиональные базы данных и информационные справочные системы:

1. Методика проведения занятий допускает использование технических средств (проекторы, интерактивные доски), обеспеченных соответствующим программным обеспечением, предлагается применение вычислительной техники и стандартных пакетов прикладных программ.

5 Фонд оценочных средств

Оценочные средства находятся в приложении к рабочим программам дисциплин.

6 Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине (модулю)

Методика проведения занятий допускает как использование технических средств (проекторы, интерактивные доски), так и классические аудиторные занятия, обеспечиваемые стандартными материально-техническими средствами.