Министерство науки и высшего образования РФ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Национальный исследовательский университет «МЭИ»

Направление подготовки/специальность: 01.03.02 Прикладная математика и информатика

Наименование образовательной программы: Математическое моделирование

Уровень образования: высшее образование - бакалавриат

Форма обучения: Очная

Оценочные материалы
по дисциплине
Современная компьютерная алгебра

Москва
2022

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

Преподаватель	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Фролов А.Б. Идентификатор: Ref8507cb-FrolovAB-a54b01e2	А.Б. Фролов
(должность)	(подпись)	(расшифровка подписи)

СОГЛАСОВАНО:

Руководитель образовательной программы	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Черепова М.Ф. Идентификатор: R9267877e-CherepovaMF-dbb9bf1	М.Ф. Черепова
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)
Заведующий выпускающей кафедры	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Зубков П.В. Идентификатор: R4920bc6f-ZubkovPV-8172426c	П.В. Зубков
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)

ОБЩАЯ ЧАСТЬ

Оценочные материалы по дисциплине предназначены для оценки: достижения обучающимися запланированных результатов обучения по дисциплине, этапа формирования запланированных компетенций и уровня освоения дисциплины.

Оценочные материалы по дисциплине включают оценочные средства для проведения мероприятий текущего контроля успеваемости и промежуточной аттестации.

Формируемые у обучающегося компетенции:

1. ПК-2 Способен участвовать в компьютерной реализации математических моделей
   ИД-1 Демонстрирует знание терминологии, базовых результатов и методов фундаментальной математики
   ИД-3 Использует базовые знания и методы фундаментальной математики для анализа простейших свойств математических моделей
   ИД-5 Выбирает, модифицирует и реализует алгоритмы численной и алгебраической реализации математических моделей
   ИД-6 Демонстрирует понимание основ теории сложности реализации математических моделей

и включает:

для текущего контроля успеваемости:

Форма реализации: Билеты (письменный опрос)

1. Алгоритмы факторизации и дискретного логарифмирования (Тестирование)
2. Методы анализа и генерации простых чисел, неприводимых многочленов и псевдослучайных последовательностей (Тестирование)
3. Методы ускорения алгебраических вычислений, квадратичные вычеты и квадратные корни (Тестирование)
4. Элементы эллиптической криптографии (Тестирование)

Форма реализации: Проверка задания

1. Полугруппы (Проверочная работа)
2. Помехоустойчивое кодирование (Проверочная работа)
3. Проблемы полноты в алгебрах (Проверочная работа)
4. Решётки (Проверочная работа)

БРС дисциплины

6 семестр

Раздел дисциплины	Веса контрольных мероприятий, %				
	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
	Срок КМ:	4	7	10	13
Алгебры и подалгебры					
Алгебры и подалгебры		+			
Проблема полноты в алгебрах					

Проблема полноты в алгебрах	+			
Решетки понятий и шкалы				
Решетки понятий и шкалы		+		
Полугруппы				
Полугруппы			+	
Кольца				
Кольца				+
Модулярная арифметика				
Модулярная арифметика				+
Поля и их применение в кодировании				
Поля и их применение в кодировании				+
Вес КМ:	25	25	25	25

7 семестр

Раздел дисциплины	Веса контрольных мероприятий, %				
	Индекс КМ:	КМ-5	КМ-6	КМ-7	КМ-8
	Срок КМ:	4	8	12	15
Методы ускорения алгебраических вычислений					
Методы ускорения алгебраических вычислений		+			
Квадратичное вычеты и квадратные корни					
Квадратичное вычеты и квадратные корни		+			
Генерация и тестирование простых чисел и неприводимых многочленов					
Генерация и тестирование простых чисел и неприводимых многочленов			+		
Генерация и анализ псевдослучайных последовательностей					
Генерация и анализ псевдослучайных последовательностей			+		
Алгоритмы факторизации и дискретного логарифмирования					
Алгоритмы факторизации и дискретного логарифмирования				+	
Эллиптические кривые. Группа точек эллиптической кривой					
Эллиптические кривые. Группа точек эллиптической кривой					+

Генерация точек и представление данных в группе точек эллиптической кривой				
Генерация точек и представление данных в группе точек эллиптической кривой				+
Применение эллиптических кривых в криптографии				
Применение эллиптических кривых в криптографии				+
Вес КМ:	25	25	25	25

$Общая часть/Для промежуточной аттестации$

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ТЕКУЩЕГО КОНТРОЛЯ

I. Оценочные средства для оценки запланированных результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Индекс компетенции	Индикатор	Запланированные результаты обучения по дисциплине	Контрольная точка
ПК-2	ИД-1$_{ПК-2}$ Демонстрирует знание терминологии, базовых результатов и методов фундаментальной математики	Знать: основные алгебраические структуры принципы преобразования информации алгебраическими методами, в частности, с применением структуры полугруппы Уметь: применять основные определения и свойства полугрупп применять современную компьютерную алгебру в теории кодирования и криптографии применять основные алгебраические структуры	Проблемы полноты в алгебрах (Проверочная работа) Полугруппы (Проверочная работа) Помехоустойчивое кодирование (Проверочная работа)
ПК-2	ИД-3$_{ПК-2}$ Использует базовые знания и методы фундаментальной математики для анализа простейших свойств математических моделей	Уметь: использовать алгоритмы тестирования алгебраических примитивов при построении основанных на	Методы анализа и генерации простых чисел, неприводимых многочленов и псевдослучайных последовательностей (Тестирование)

		них алгебраических систем	
ПК-2	ИД-5$_{ПК-2}$ Выбирает, модифицирует и реализует алгоритмы численной и алгебраической реализации математических моделей	Уметь: применять алгоритмы операций в различных алгебраических структурах разрабатывать алгоритмы алгебраических преобразований и алгоритмы численной и алгебраической реализации математических моделей	Решётки (Проверочная работа) Элементы эллиптической криптографии (Тестирование)
ПК-2	ИД-6$_{ПК-2}$ Демонстрирует понимание основ теории сложности реализации математических моделей	Знать: подходы к решению задач целочисленной факторизации и дискретного логарифмирования Уметь: ускорять алгебраические вычисления	Методы ускорения алгебраических вычислений, квадратичные вычеты и квадратные корни (Тестирование) Алгоритмы факторизации и дискретного логарифмирования (Тестирование)

II. Содержание оценочных средств. Шкала и критерии оценивания

6 семестр

КМ-1. Проблемы полноты в алгебрах

Формы реализации: Проверка задания
Тип контрольного мероприятия: Проверочная работа
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Проверка выполненных студентами решений индивидуальных задач

Краткое содержание задания:
В работе проверяется знание основных алгебраических структур и умение применять основные алгебраические структуры

Контрольные вопросы/задания:

Знать: основные алгебраические структуры	1.Замкнутый класс, полная система, базис в универсальной алгебре 2.Свойства конечно порожденной алгебры 3.Критериальная система. Критерий полноты в конечно порожденной алгебре
Уметь: применять основные алгебраические структуры	1.Пусть A --- некоторое линейно упорядоченное множество. Найдите все подалгебры алгебры (A; $\min(x, y)$, $\max(x, y)$) 2.Пусть A --- некоторое линейно упорядоченное множество. В алгебре (A; $\min(x, y)$, $\max(x, y)$) найдите все предполные классы и критерий полноты. Для каких множеств A существуют предполные классы в такой алгебре? 3.Найдите гомоморфизмы алгебры (**N**; +) в алгебру (**Z**; +) 4.Найдите гомоморфизмы алгебры (**N**; *) в алгебру (**Z**; *) 5.Пусть конечно-порожденная алгебра имеет ровно n предполных классов. Какова может быть мощность базиса в такой алгебре?

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

Оценка: 3
Нижний порог выполнения задания в процентах: 50

Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

КМ-2. Решётки

Формы реализации: Проверка задания
Тип контрольного мероприятия: Проверочная работа
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Проверка выполненных студентами решений индивидуальных задач

Краткое содержание задания:
В работе проверяется умение применять алгоритмы операций в различных алгебраических структурах

Контрольные вопросы/задания:

Уметь: применять алгоритмы операций в различных алгебраических структурах	1.Пусть решетка понятий имеет ровно n атомов. Какова мощность решетки? 2.Пусть решетка понятий имеет ровно n атомов. Какой может быть мощность базиса в ней? 3.Атомами решетки понятий являются 7 дней недели. Постройте минимальную шкалу для ее понятий 4.Атомами решетки понятий являются 12 месяцев года. Постройте минимальную шкалу 5.Атомы решетки понятий --- 31 день календарного месяца. Постройте минимальную шкалу

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

КМ-3. Полугруппы

Формы реализации: Проверка задания
Тип контрольного мероприятия: Проверочная работа
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Проверка выполненных студентами решений индивидуальных задач

Краткое содержание задания:

В работе проверяется знание принципов преобразования информации алгебраическими методами, в частности, с применением структуры полугруппы и умение применять основные определения и свойства полугрупп

Контрольные вопросы/задания:

Знать: принципы преобразования информации алгебраическими методами, в частности, с применением структуры полугруппы	1.Полугруппы. Циклические полугруппы. Полугруппы преобразований 2.Цикловой индекс группы подстановок 3.Группа автоморфизмов графа 4.Число геометрически различных окрасок вершин графа 5.Задача об ожерельях
Уметь: применять основные определения и свойства полугрупп	1.Постройте полугруппы порядка 1,2,3 2.Выясните, какие из полугрупп порядка 1,2,3 являются группами, абелевыми группами 3.Найдите все идемпотенты в каждой полугруппе порядка 1,2,3 4.Найдите все подполугруппы в каждой из полугрупп порядка 1,2,3 5.Выясните, какие из полугрупп порядка 1,2,3 являются циклическими. Для каждой циклической полугруппы найдите индекс и порядок

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

КМ-4. Помехоустойчивое кодирование

Формы реализации: Проверка задания
Тип контрольного мероприятия: Проверочная работа
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Проверка выполненных студентами решений индивидуальных задач

Краткое содержание задания:
В работе проверяется умение применять современную компьютерную алгебру в теории кодирования и криптографии

Контрольные вопросы/задания:

Уметь: применять современную	1.Постройте поле GF(16)

компьютерную алгебру в теории кодирования и криптографии	2.Найдите все слова кода $R(3,2)$ 3.Найдите проверочную матрицу кода Хэмминга с 5 проверочными символами 4.Существует ли линейные коды с кодовым расстоянием 0 и 1? 5.Какие значения может принимать кодовое расстояние линейного (n, k)–кода?

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

7 семестр

КМ-5. Методы ускорения алгебраических вычислений, квадратичные вычеты и квадратные корни

Формы реализации: Билеты (письменный опрос)
Тип контрольного мероприятия: Тестирование
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Письменный опрос проводится по вариантам. Работа содержит 4 задания на 20 минут

Краткое содержание задания:
Тест «Методы ускорения алгебраических вычислений, квадратичные вычеты и квадратные корни» имеет целью проверку умения ускорять алгебраические вычисления.

Контрольные вопросы/задания:

Уметь: ускорять алгебраические вычисления	1.Вычислить символ Якоби$\left(\frac{27}{77}\right)$. Выполнить умножение двухразрядных чисел в десятичной системе счисления методом Карацубы. Выполнить умножение пятиразрядных чисел в кольце Z_35 Методом Монтгомери. Выполнить умножение 2×2 матриц над Z_{17} методо Штрассена. Вычислить квадратный корень из квадратичного вычета 17 по модулю 21. Вычислить символ Лежандра $\left(\frac{4}{7}\right)$.

	Вычислить символ Лежандра $\left(\frac{4}{3}\right)$.

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка "отлично" выставляется, если задание выполнено в полном объеме или выполнено преимущественно верно.

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка "хорошо" выставляется, если большинство вопросов раскрыто. выбрано верное направление для решения задач.

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется, если задание преимущественно выполнено

КМ-6. Методы анализа и генерации простых чисел, неприводимых многочленов и псевдослучайных последовательностей

Формы реализации: Билеты (письменный опрос)
Тип контрольного мероприятия: Тестирование
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Письменный опрос проводится по вариантам. Работа содержит 4 задания на 20 минут

Краткое содержание задания:
Тест «Методы анализа и генерации простых чисел, неприводимых многочленов и псевдослучайных последовательностей» имеет целью проверку умения использовать алгоритмы тестирования алгебраических примитивов при построении основанных на них алгебраических систем

Контрольные вопросы/задания:

Уметь: использовать алгоритмы тестирования алгебраических примитивов при построении основанных на них алгебраических систем	1.1. Проверить простоту числа по тесту Миллера-Рабина и по тесту Люка (выполнив вычисления "вручную" по известному алгоритму). 1.17419, 2.26561, 3.34129, 4.33329, 5.37649, 6.25411, 7.41411, 8.45631, 9.55631, 10.57731. 2.Построить простое число, содержащее вдвое больше знаков по сравнению с заданным простым числом, применив алгоритм Поклингтона (Проверку

	по тесту Миллера-Рабина выполнять, используя Алгебраический процессор).\\ 1. 127, 2. 911, 3.711 , 4.523 , 5.631 , 6.647 , 7.547 , 8.379 , 9.773 , 10.757. 3. Составить полиномиальный базис и нормальное множество поля $GF(3^2)$, порождаемого неприводимым многочленом $2 + X + X^2$.

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка 5 выставляется при правильном ответе на два вопроса билета и на вопрос на умения.

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка 4 выставляется при ответе на два вопроса билета с возможными несущественными неточностями и на вопрос на умения.

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка 3 выставляется при ответе на два вопроса билета с возможными несущественными неточностями и затруднении с ответом вопрос на умения.

КМ-7. Алгоритмы факторизации и дискретного логарифмирования

Формы реализации: Билеты (письменный опрос)
Тип контрольного мероприятия: Тестирование
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Письменный опрос проводится по вариантам. Работа содержит 4 задания на 20 минут

Краткое содержание задания:
Тест «Алгоритмы факторизации и дискретного логарифмирования» связан с проверкой знания подходов к решению задач целочисленной факторизации и дискретного логарифмирования.

Контрольные вопросы/задания:

Знать: подходы к решению задач целочисленной факторизации и дискретного логарифмирования	1.В чем отличие ро-метода и модифицированного ро-метода? 2.Как в методе Монте Карло Поларда исключаются неудачи?

	3.В каких случаях применение метода Ферма факторизации эффективно? 4. Как обеспечивается ускорение поиска различных квадратных корней в методе факторных баз? 5.Сформулируйте задачу дискретного логарифмирования. 6.При каких условиях задача дискретного логарифмирования легко решается и по какому алгоритму? 7.Назовите два этапа индексного алгоритма дискретного логарифмирования. 8.Какая особенность разложения по степеням элементов факторной базы имеется в индексном алгоритме дискретного логарифмирования в расширении простого поля по сравнению с таким алгоритмом в простом поле? 9. Что общего имеют алгоритмы квадратичного решена целочисленной факторизации и индексный алгоритм дискретного логарифмирования?

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка 5 выставляется при полном ответе на оба вопроса в билете и на два дополнительных вопроса на знание

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка 4 выставляется при ответе на оба вопроса в билете и на два дополнительных вопроса на знание, если допущены две-три несущественные неточности.

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка 4 выставляется при ответе на оба вопроса в билете и на два дополнительных вопроса на знание, если допущены две-три существенные неточности.

КМ-8. Элементы эллиптической криптографии

Формы реализации: Билеты (письменный опрос)
Тип контрольного мероприятия: Тестирование
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Проверка результатов выполнения двух заданий, сформулированных в билетах и ответов на дополнительный вопрос на знания.

Краткое содержание задания:
Тест «Элементы эллиптической криптографии» связан с умением разрабатывать алгоритмы алгебраических преобразований и алгоритмы численной и алгебраической реализации математических моделей

Контрольные вопросы/задания:

Уметь: разрабатывать алгоритмы	1.1. Используя программы с операциями в группе

алгебраических преобразований и алгоритмы численной и алгебраической реализации математических моделей	точек ЭС над большим полем ElCurveFp , а также над расширением поля GF(3) ElCurveF3lPointOperations a) Взять по три точки P,Q и T на эллиптических кривых сначала над большим полем, а затем над расширением поля GF(3) и практически подтвердить ассоциативность: (P+Q)+T=P+(Q+T). b) Для точек P и Q этих двух кривых практически подтвердить тождество: 2P+T=P+(P+T). 2. Определить порядок эллиптической кривой над полем GF(3^n) N.Эллиптическая кривая.n. 1).y^2=X^3+2X+1;11, 2).y^2=X^3+2X+1;7, 3).y^2=X^3+2X+1;13, 4).y^2=X^3+2X+2;11, 5).y^2=X^3+2X+2;7, 6).y^2=X^3+2X+2;9, 7).y^2=X^3+2X+1;9, 8).y^2=X^3+2X+2;13, 9).y^2=X^3+2X+2;5, 10).y^2=X^3+2X+1;9. 3. Применить алгоритм согласования для вычистлния дискретного логарифма x точки Q=xP эллиптической кривой над полем GF(3^n). N.F.Эллиптическая кривая.P.n.Q; 1).F_{11}.Y^2=X^3+7X.(4,9).6.(3,9); 2).F_{11}.Y^2=X^3+7X.4,2).6.(4,9); 3).F_{11}.Y^2=X^3+2X.(5,5).6.(1,5); 4).F_{11}.Y^2=X^3+2X.(5,6).6.(3,0); 5).F_{11}.Y^2=X^3+6X(2,3).6.(7,0); 6).F_{11}.Y^2=X^3+6X.(2,8).6.(5,10); 7).F_{11}.Y^2=X^3+8X.(7,5).6.(9,3); 8).F_{11}.Y^2=X^3+8X.(7,6).6.(0,0); 9).F_{11}.Y^2=X^3+6X.(2,8).6.(5,1); 10).F_{11}.Y^2=X^3+2X.(5,5).6.(1,6). \end{tabular} 4.Передать сообщение m по протоколу Месси-Омуры с использованием функций размещения сообщения (в программе ElCurveF3lPointGen) в точке кривой Y^2=X^3+2X^2+1 над полем GF(3^{l}), умножения точки на константу (программа ElCurveF3l), а также функции обращения в конечном поле из библиотеки (программа Uni.py). 1. m=(2,2,1,1,2,2,1)\ l=13; 2.m=(2,2,1,1,2,2,2)\ l=11; 3.m=(2,2,1,1,2,1,0)\ l=13; 4.m=(2,2,1,1,2,1,1)\ l=11; 5.m=(2,2,1,1,2,1,2)\ l=13; 6.m=(2,2,1,1,2,2,0)\ l=11; 7.m=(2,2,1,1,2,2,1)\ l=13; 8.m=(2,2,1,1,2,2,2)\ l=11;

	9.m=(2,2,1,1,1,0,0)\ l=13; 10.m=(2,2,1,1,1,0,1)\ l=11.

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка 5 выставляется при полном ответе на оба вопроса билета и ответе на два дополнительных вопроса на умения при возможных несущественных неточностях.

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка 5 выставляется при ответе на оба вопроса билета и ответе на два дополнительных вопроса на умения при возможных даже существенных неточностях.

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка 3 выставляется при ответе на один вопрос билета и ответе на два дополнительных вопроса на умения при возможных несущественных неточностях.

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

6 семестр

Форма промежуточной аттестации: Экзамен

Пример билета

1. Сортировка методом Шелла.
2. Постройте поле GF(4) как расширение поля GF(2) и решите в поле GF(4) уравнение x^2+x+1=0.

Процедура проведения

Экзамен проводится в письменно-устной форме. На подготовку ответа дается 60 минут. Кроме ответа на вопросы билета, студент должен ответить на дополнительные вопросы.

I. Перечень компетенций/индикаторов и контрольных вопросов проверки результатов освоения дисциплины

1. Компетенция/Индикатор: ИД-1$_{ПК-2}$ Демонстрирует знание терминологии, базовых результатов и методов фундаментальной математики

Вопросы, задания

1.Замкнутый класс, полная система, базис в универсальной алгебре
2.Свойства конечно порожденной алгебры
3.Предполный класс. Расширение замкнутого класса до предполного в конечно порожденной алгебре
4.Критериальная система. Критерий полноты в конечно порожденной алгебре
5.Задача о размене денег. Число Фробениуса
6.Разбиения матриц
7.Сортировка Шелла
8.Сети Петри. Структура и функционирование. Проблема живучести
9.Число Фробениуса и живучесть консервативной сети Петри
10.Функциональные системы и их замкнутые классы
11.Алгебра функций k-значной логики
12.Канонические формулы для функций k-значной логики
13.Примеры полных систем в k-значной логике
14.Многомодульная арифметика
15.Полугруппы. Циклические полугруппы. Полугруппы преобразований
16.Цикловой индекс группы подстановок
17.Группа автоморфизмов графа
18.Число геометрически различных окрасок вершин графа
19.Задача об ожерельях
20.Конечное поле, его характеристика, алгебраическое расширение поля
21.Построение полей порядка 4,8,9
22.Различные способы представления конечного поля
23.Линейный код над конечным полем, его матрицы
24.Кодовое расстояние и корректирующие способности линейного кода
25.Декодирование по синдрому
26.Код m-кратного повторения, бинарный код проверки на четность
27.Коды Хэмминга
28.Коды Рида-Малера

29.Матрицы и преобразования Адамара
30.Декодирование кодов R(1,m)
31.Оптимальные коды. Метод Хаффмана
32.Коды, исправляющие замены 0 на 1
33.Коды, исправляющие вставки и выпадения символов
34.Циклический код и его порождающий многочлен
35.Уравнения в конечных полях
36.Проверочная матрица циклического кода. Кодирование и декодирование
37.Пусть A --- некоторое линейно упорядоченное множество. Найдите все подалгебры алгебры (A; min(x, y), max(x, y))
38.Пусть A --- некоторое линейно упорядоченное множество. В алгебре (A; min(x, y), max(x, y)) найдите все предполные классы и критерий полноты. Для каких множеств A существуют предполные классы в такой алгебре?
39.Найдите гомоморфизмы алгебры (**N**; +) в алгебру (**Z**; +)
40.Найдите все слова кода R(3,2)
41.Найдите проверочную матрицу кода Хэмминга с 5 проверочными символами
42.Существует ли линейные коды с кодовым расстоянием 0 и 1?
43.Постройте полугруппы порядка 1,2,3
44.Выясните, какие из полугрупп порядка 1,2,3 являются группами, абелевыми группами
45.Найдите все идемпотенты в каждой полугруппе порядка 1,2,3

Материалы для проверки остаточных знаний

1.Алгебра из n (n=2,3,4,…) элементов может быть

Ответы:

a) конечно порожденной,
b) бесконечно порожденной,
c) алгеброй без базиса,
d) алгеброй без предполных классов,
e) алгеброй с бесконечным базисом.

Верный ответ: a) конечно порожденной

2.В любой конечно порожденной алгебре есть

Ответы:

a) предполные классы,
b) критериальная система,
c) подалгебры,
d) полная система,
e) базис.

Верный ответ: a) предполные классы, b) критериальная система, c) подалгебры, d) полная система, e) базис.

3.Если алгебра имеет базис, то в ней есть

Ответы:

a) предполные классы,
b) критериальная система,
c) полная система,
d) собственные подалгебры,
e) замкнутые классы.

Верный ответ: c) полная система, e) замкнутые классы.

4.Операция полугруппы обязательно

Ответы:

a) коммутативна,
b) ассоциативна,
c) обратима,

d) имеет нейтральный элемент,
e) имеет идемпотент.
Верный ответ: b) ассоциативна
5.Циклическая полугруппа обязательно
Ответы:
a) коммутативна,
b) конечно порождаема,
c) конечна,
d) имеет единицу,
e) имеет идемпотент.
Верный ответ: a) коммутативна
6.Поле может иметь следующий порядок
Ответы:
a) 1,
b) 2,
c) 3,
d) 4,
e) 5.
Верный ответ: b) 2, c) 3, d) 4, e) 5.
7.Код Хэмминга с m проверочными символами имеет кодовое расстояние
Ответы:
a) 2,
b) 3,
c) m-1,
d) m,
e) 2^m-m-1.
Верный ответ: b) 3
8.Бинарный код с проверкой на четность является
Ответы:
a) циклическим,
b) линейным,
c) исправляющим ошибки,
d) кодом с повторением символов,
e) кодом с расстоянием 3.
Верный ответ: b) линейным

2. Компетенция/Индикатор: ИД-5$_{ПК-2}$ Выбирает, модифицирует и реализует алгоритмы численной и алгебраической реализации математических моделей

Вопросы, задания

1.Максимальная и минимальная шкалы в булевой алгебре понятий
2.Пусть решетка понятий имеет ровно n атомов. Какова мощность решетки?
3.Пусть решетка понятий имеет ровно n атомов. Какой может быть мощность базиса в ней?
4.Атомами решетки понятий являются 7 дней недели. Постройте минимальную шкалу для ее понятий

Материалы для проверки остаточных знаний

1.Решетка содержит ровно 16 понятий. Укажите мощность максимальной шкалы.
Ответы:
a) 2,
b) 3,
c) 4,

d) 5,
e) 8.

Верный ответ: c) 4

2.Решетка содержит ровно 16 понятий. Укажите мощность минимальной шкалы.

Ответы:

a) 2,
b) 3,
c) 4,
d) 5,
e) 8.

Верный ответ: b) 3

II. Описание шкалы оценивания

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Работа выполнена в рамках "продвинутого" уровня. Ответы даны верно, четко сформулированные особенности практических решений

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Работа выполнена в рамках "базового" уровня. Большинство ответов даны верно. В части материала есть незначительные недостатки

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Работа выполнена в рамках "порогового" уровня. Основная часть задания выполнена верно. На вопросы углубленного уровня даны неверные ответы

III. Правила выставления итоговой оценки по курсу

Оценка определяется в соответствии с Положением о балльно-рейтинговой системе для студентов НИУ «МЭИ» на основании семестровой и экзаменационной составляющих

7 семестр

Форма промежуточной аттестации: Экзамен

Пример билета

1. 1. Метод Карацубы умножения целых чисел.
2. 2. Алгоритм согласования для дискретного логарифмирования в мультипликативной группе.
3. 3. Алгоритм тестирования многочлена на неприводимость.

Процедура проведения

Экзамен проводится в письменно-устной форме. На подготовку ответа дается 60 минут. Кроме ответа на вопросы билета, студент должен ответить на дополнительные вопросы.

I. Перечень компетенций/индикаторов и контрольных вопросов проверки результатов освоения дисциплины

1. Компетенция/Индикатор: ИД-З$_{ПК-2}$ Использует базовые знания и методы фундаментальной математики для анализа простейших свойств математических моделей

Вопросы, задания

1.Какой вероятностный тест простоты является предпочтительным и почему?
2. Как получить простое число, существенно большее заданного простого числа?
3.Какова достоверность заключения о простоте числа по вероятностному тесту простоты?
4. Какие числа называются свидетелями разложимости составного нечетного числа, а какие - лжесвидетелями его простоты?
5.Какое заключение теста разложимости является абсолютно достоверным?
6.Проверить простоту числа по тесту Миллера-Рабина и по тесту Люка (выполнив вычисления "вручную" по известному алгоритму)
7.Составить полиномиальный базис и нормальное множество поля $GF(3^2)$, порождаемого неприводимым многочленом $2 + X + X^2$.
8.Как построить линейную рекуррентную последовательность максимального периода?

Материалы для проверки остаточных знаний

1.Какова вероятность, что число простое, если при однократном применении теста Миллера Рабина не был получен результат. что оно составное?

Ответы:

а. ¼,
б. ½,
в. ⅔.

Верный ответ: а. ¼,

2.Построить линейную рекуррентную последовательность с периодом 31

Ответы:

1.Степени корня х примитивного многочлена $1 + x + x$,
2.Степени корня х примитивного многочлена $1 + x + x$.

Верный ответ: 2.

2. Компетенция/Индикатор: ИД-5$_{ПК-2}$ Выбирает, модифицирует и реализует алгоритмы численной и алгебраической реализации математических моделей

Вопросы, задания

1.Дайте определение эллиптической кривой над конечным полем.
2.Приведите уравнение эллиптической кривой над полем характеристика которого больше трех.
3.Приведите алгоритм сложения точек эллиптической кривой.
4.Как взять (построить) точку эллиптической кривой.
5.Что называется порядком точки эллиптической кривой?
6.В чем сходство и в чем различие алгоритмов возведения в степень в конечном поле и скалярного умножения на эллиптической кривой?
7.Сформулируйте проблему Диффи---Хэлмана на эллиптической кривой.
8.В чем состоит уязвимость протокола Диффи---Хэллмэна согласования ключей на эллиптической кривой?
9.Каким образом передать секретное сообщение по открытым каналам?
10.Перечислите алгебраические операции, используемые в протоколе цифровой подписи российского стандарта 2012 года.

11.Каким образом блокируется уязвимость протокола Диффи---Хеллмана в MQV-протоколе?
12.Определить порядок эллиптической кривой над полем GF(3^n)
13.Применить алгоритм согласования для вычисления дискретного логарифма x точки Q=xP эллиптической кривой над полем GF(3^n)

Материалы для проверки остаточных знаний

1.Приведите уравнение эллиптической кривой над полем, характеристика которого больше трех.

Ответы:

а. Y^2=X^3+aX+b,
б. Y^2=X^3+aX^2+bX+c,
в. Y^3=X^2+aX+b,

Верный ответ: а. Y^2=X^3+aX+b,

2.Как взять точку эллиптической кривой над полем, характеристика которого больше трех?

Ответы:

Подобрать x так, чтобы правая часть была квадратичным вычетом и взять квадратный корень y от нее.

Верный ответ: Подобрать x так, чтобы правая часть была квадратичным вычетом и взять квадратный корень y от нее.

3.Найти сумму точек (9, 5) и (9, 18) эллиптической кривой.Y^2=X^3+X над полем GF(23).

Ответы:

О-точка в бесконечности.

Верный ответ: О-точка в бесконечности, т.к. 5+18=23 в поле GF(23).

3. Компетенция/Индикатор: ИД-6$_{ПК-2}$ Демонстрирует понимание основ теории сложности реализации математических моделей

Вопросы, задания

1.Как зависит сложность рекурсивного алгоритма от того, на сколько частей разбиваются операнды на каждом шаге рекурсии.
2.В каких случаях применение метода Ферма факторизации эффективно?
3. Как обеспечивается ускорение поиска различных квадратных корней в методе факторных баз?
4. Сформулируйте задачу дискретного логарифмирования.
5.При каких условиях задача дискретного логарифмирования легко решается и по какому алгоритму?
6.Как в методе Монте Карло Поларда исключаются неудачи?
7.За счет чего достигается ускорение умножения и возведения в степень по методам Монтгомери?
8.В чем различие двух способов реализации вычислений по китайской теореме об остатках?
9.Дайте определения квадратичного вычета и квадратичного невычета по заданному модулю.
10. Дайте определения символов Лежандра и символа Якоби.
11.Каковы свойства символа Якоби, позволяющие вычислить его, не прибегая к разложению модуля? Сформулируйте критерий Эйлера для символа Лежандра.
12.Как вычислить символ Якоби, не используя разложение числа n?
13.Для каких мультипликативных групп известны детерминированные алгоритмы извлечения квадратного корня?

14.Какова особенность алгоритма извлечения квадратного корня по простому модулю для общего случая?
15. Сформулируйте проблему квадратного корня.
16.Представьте формулы квадратных корней по модулю составного числа через корни по модулю одного и другого простого числа.
17.Что такое число Блюма и каковы его свойства?
18.Выполнить умножение двухразрядных чисел в десятичной системе счисления методом Карацубы.
19.Выполнить умножение пятиразрядных чисел в кольце Z_35 Методом Монтгомери.
20.Выполнить умножение 2×2 матриц над Z_{17} методом Штрассена.

Материалы для проверки остаточных знаний

1.Сколько операций умножения нужно выполнить по методу Карацубы при перемножении двухразрядных десятичных чисел.

Ответы:

а. 3,
б. 2,
в. 4.

Верный ответ: а. 3.

2.Вычислить символ Лежандра вычета 3 по модулю 7 (по критерию Эйлера).

Ответы:

3^{(7-1)/2}mod 7=3^ 3 mod 7=-1.

Верный ответ: 3^{(7-1)/2}mod 7=3^ 3 mod 7=-1.

II. Описание шкалы оценивания

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка «ОТЛИЧНО» выставляется студенту, правильно выполнившему практическое задание, который показал при ответе на вопросы экзаменационного билета, и на дополнительные вопросы, что владеет материалом изученной дисциплины, свободно применяет свои знания для объяснения различных явлений и решения задач.

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка «ХОРОШО» выставляется студенту, правильно выполнившему практическое задание и в основном правильно ответившему на вопросы экзаменационного билета (билета коллоквиума) и на дополнительные вопросы, но допустившему при этом непринципиальные ошибки.

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка «УДОВЛЕТВОРИТЕЛЬНО» выставляется студенту, который в ответах на вопросы экзаменационного билета допустил существенные и даже грубые ошибки, но затем исправил их сам, а также не выполнил практическое задание из экзаменационного билета, но либо наметил правильный путь его выполнения, либо по указанию экзаменатора решил другую задачу из того же раздела дисциплины.

III. Правила выставления итоговой оценки по курсу

Оценка определяется в соответствии с Положением о балльно-рейтинговой системе для студентов НИУ «МЭИ» на основании семестровой и экзаменационной составляющих