МИНОБРНАУКИ РОССИИ
Ярославский государственный университет им. П.Г. Демидова

Кафедра алгебры и математической логики

УТВЕРЖДАЮ

Декан математического факультета

Нестеров П.Н.

20 июня 2023 г.

Рабочая программа дисциплины

Алгебраическая алгоритмика

Направление подготовки (специальности)
02.04.01 Математика и компьютерные науки

Направленность (профиль)
«Компьютерная математика»

Форма обучения очная

Программа рассмотрена
на заседании кафедры
от 18 апреля 2023 г., протокол № 8

Программа одобрена НМК
математического факультета
протокол № 9 от 3 мая 2023 г.

Ярославль

1. Цели освоения дисциплины

Целями освоения дисциплины "Алгебраическая алгоритмика" являются: обеспечение подготовки в одной из важных областей, находящихся на границе алгебры и информатики; овладение основными алгоритмическими вопросами классической и современной алгебры; освоение основных методов разработки эффективных алгоритмов для решения задач, возникающих как в самой алгебре, так и в ее приложениях.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Алгебраическая алгоритмика» относится к вариативной части Блока 1. Для ее успешного изучения необходимы знания, умения и навыки, приобретенные в ходе изучения таких базовых курсов, как «Алгебра» и «Теория чисел», а также курсы, связанные с изучением основ программирования. Эта дисциплина закладывает основы алгебраического и алгоритмического образования будущего специалиста. «Геометрия» относится к базовой части Блока 1. Для ее успешного изучения необходимы знания и умения, приобретенные в результате освоения некоторых разделов из курсов алгебры и математического анализа.

3. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины направлен на формирование следующих элементов компетенций в соответствии с ФГОС ВО, ОП ВО и приобретения следующих знаний, умений, навыков и (или) опыта деятельности:

Формируемая компетенция (код и формулировка)	**Индикатор достижения компетенции (код и формулировка)**	**Перечень планируемых результатов обучения**
Общепрофессиональные компетенции		
ОПК-2 Способен использовать современные методы разработки и реализации конкретных алгоритмов математических моделей на базе языков программирования и пакетов прикладных программ моделирования.	**ИД-ОК-2_1** Осуществляет постановку задачи, выбирает способ ее решения, применяет математический аппарат и теорию для решения прикладных и теоретических задач.	**Знать:** -основные методы решения алгоритмических проблем, возникающих в алгебре и в ее приложениях к решению практических задач; -формировать алгоритмическое мировоззрение, творческое мышление и навыки в проведении самостоятельных научных исследований. -основные задачи алгоритмики и методы их решения; - определения и свойства математических объектов, используемых в курсе; -формулировки утверждений, методы их доказательства, возможные сферы их приложений. **Уметь:**

		- строить алгоритмы для решения алгебраических задач; - исследовать сложность используемых алгоритмов;. - решать задачи теоретического и прикладного характера из различных разделов курса; - доказывать утверждения; - описывать строение некоторых мультипликативных групп колец вычетов. **Владеть навыками:** -основными понятиями и методами алгебры в кольце целых чисел; - основными понятиями и методами алгебры в кольце многочленов от одной переменной. - методами доказательства утверждений; -применять методы алгебраической алгоритмики в смежных дисциплинах.

4. Объем, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет __3__ зачетных единиц, 108_ акад. часов.

№ п/п	Темы (разделы) дисциплины, их содержание	Семестр	Виды учебных занятий, включая самостоятельную работу студентов, и их трудоемкость (в академических часах)						Формы текущего контроля успеваемости Форма промежуточной аттестации *(по семестрам)*
			Контактная работа						
			лекции	практические	лабораторные	консультации	аттестационные испытания	самостоятельная работа	
1.	**Вводная лекция**	1	0,5						
2.	**Алгоритм Евклида** для кольца целых чисел и кольца многочленов. Оценка сложности алгоритма.	1	1,5	1				4	Задания для самостоятельной работы.
3.	**Непрерывные дроби** и алгоритм Евклида	1	2	1				4	Задания для самостоятельной работы.
4.	**Факториальные и и евклидовы кольца**.	1	1	1				2	Задания для самостоятельной работы.
5.	**Кольцо и поле вычетов по модулю m.**	1	2					4	Задания для самостоятельной работы. Контр. раб. № 1
6.	**Факторкольцо** $K[x]/(m(x))$. **Поле** $K[x]/(m(x))$.	1	2	1				4	Задания для самостоятельной работы
7.	**Группы. Мультипликативные группы колец вычетов**	1	2	1		1		4	Задания для самостоятельной работы
8.	**Тесты простоты**	1	1					2	Задания для самостоятельной работы.
9.	**Китайская теорема об остатках**.	1	1	1		1		2	Задания для самостоятельной работы.
10.	**Интерполяция над полем.**	1	1	1				2	Задания для самостоятельной работы

11.	**Факторкольцо** $Z_p[x]/(p(x))$.	1	2					2	Задания для самостоятельной работы.
12.	**Разложение многочлена на множители**.	1	2	1		1		4	Задания для самостоятельной работы.
13.	**Поля Галуа**	1	4	2		1		4	Задания для самостоятельной работы. Контр. раб. № 2.
			22	10			**0,3**	**33,7**	**Зачет**
	Всего за 1 семестр 108 часов		32			4	0,3	71,7	

Содержание разделов дисциплины:

Тема №1: **Вводная лекция**

История появления и развития алгебраической алгоритмики, ее место среди других математических наук. История появления быстрых алгоритмов, их применение.

Тема №2: **Алгоритм Евклида**

Теория делимости в целостных кольцах. Наибольший общий делитель (НОД) элементов кольца. Свойства НОД. Отношения делимости в $\mathbb{Z}$. Алгоритм Евклида в кольце $\mathbb{Z}$. Теоремы о представлении НОД в $\mathbb{Z}$. Сложность алгоритма Евклида. Теорема Ламе. Расширенный алгоритм Евклида в $\mathbb{Z}$. Вычисление коэффициентов Безу. Оценки коэффициентов Безу.

Тема №3: **Непрерывные дроби**

Алгоритм Евклида и цепные дроби. Свойства цепных дробей. Теорема единственности, Теорема о представлении рациональных чисел цепными дробями. Периодические цепные дроби.

Тема №4: **Факториальные и евклидовы кольца**

Кольцо $\mathbb{Z}$. Целостное кольцо. Теория делимости в целостных кольцах. Обратимый элемент кольца, ассоциированные элементы кольца. Группа обратимых элементов кольца. Наибольший общий делитель (НОД) элементов кольца. Евклидовы кольца. Основная теорема арифметики для евклидовых колец. Следствия для кольца $\mathbb{Z}$. Факториальное кольцо. Неприводимые и простые элементы кольца. Разложение на множители в евклидовом кольце. Теорема Гаусса. Рациональные корни многочленов из $Z[x]$. Критерий неприводимости многочлена над Z.

Тема №5 **Кольцо и поле вычетов по модулю m.**

Сравнения и их свойства. Классы вычетов по данн

ому модулю. Кольцо вычетов по модулю m . Поле $\mathbb{Z}/(n)$. Решения линейного сравнения с одним неизвестным. Китайская теорема об остатках для чисел. Китайские теоремы об остатках для систем сравнений.

Тема №6: **Факторкольцо $K[x]/(m(x))$. Поле $K[x]/(m(x))$.**

Простые и неприводимые многочлены. Классы эквивалентности по модулю m(x). Факторкольцо $K[x]/(m(x))$. Поле $K[x]/(m(x))$.

Тема №7: **Группы. Мультипликативные группы колец вычетов**

Мультипликативная группа кольца Z_n. Циклические группы. Примитивный корень по модулю m . Порядок элемента группы. Цикличность группы Z_p при простом p. Лемма Гаусса. Теорема Гаусса (необходимое и достаточное условие цикличности группы Z_n^*).

Тема №8: **Тесты простоты**

Псевдопростые числа по данному основанию. Числа Кармайкла. Теорема Вильсона. Тесты простоты. Детерминистические тесты и тесты псевдопростоты. Сильно псевдопростые числа по данному основанию.

Тема 9: **Китайская теорема об остатках**

Китайская теорема об остатках для чисел. Китайские теоремы об остатках для систем сравнений. Китайская теорема об остатках для многочленов.

Тема №10: **Интерполяция над полем.**

Формула Лагранжа. Интерполяция с помощью китайской теоремы об остатках.

Тема №11: **Факторкольцо $Z_p[x]/(p(x))$.**

Неприводимые многочлены с коэффициентами из Z_p. Число неприводимых многочленов степени n в $Z_p[x]$. Критерий неприводимости многочлена над Z_p.

Тема №12: **Разложение многочлена на множители**

Неприводимые многочлены. Разложение на множители над $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ и $\mathbb{Z}$. Теорема Гаусса. Примитивные многочлены. Рациональные корни многочленов с целыми коэффициентами. Критерий Эйзенштейна.

Тема №13: **Поля Галуа**

Конечное поле. Свойства его элементов. Основные теоремы. Факторкольцо $Z_p[x]/(p(x))$. Характеристика поля. Мультипликативная группа конечного поля.
Примитивный элемент поля. Нахождение примитивного элемента в конечном поле. Поле разложения многочлена. Минимальный многочлен алгебраического над полем элемента. Правило возведения в степень p в поле с характеристикой p. Корни неприводимого

многочлена в $Z_p[x]$.Существование конечного поля из p^r элементов. Построение полей Галуа $GF(2^n)$.

5. Образовательные технологии, в том числе технологии электронного обучения и дистанционные образовательные технологии, используемые при осуществлении образовательного процесса по дисциплине

В процессе обучения используются следующие образовательные технологии:

Вводная лекция – дает первое целостное представление о дисциплине и ориентирует студента в системе изучения данной дисциплины. Студенты знакомятся с назначением и задачами курса, его ролью и местом в системе учебных дисциплин и в системе подготовки в целом. Дается краткий обзор курса, история развития науки и практики, достижения в этой сфере, имена известных ученых, излагаются перспективные направления исследований. На этой лекции высказываются методические и организационные особенности работы в рамках данной дисциплины, а также дается анализ рекомендуемой учебно-методической литературы.

Академическая лекция с элементами лекции-беседы – последовательное изложение материала, осуществляемое преимущественно в виде монолога преподавателя. Элементы лекции-беседы обеспечивают контакт преподавателя с аудиторией, что позволяет привлекать внимание студентов к наиболее важным темам дисциплины, активно вовлекать их в учебный процесс, контролировать темп изложения учебного материала в зависимости от уровня его восприятия.

Практическое занятие – занятие, посвященное освоению конкретных умений и навыков по закреплению полученных на лекции знаний.

Консультации – вид учебных занятий, являющийся одной из форм контроля самостоятельной работы студентов. На консультациях по просьбе студентов рассматриваются наиболее сложные моменты при освоении материала дисциплины, преподаватель отвечает на вопросы студентов, которые возникают у них в процессе самостоятельной работы.

В процессе обучения используются следующие технологии электронного обучения и дистанционные образовательные технологии:

Электронный учебный курс «Алгебраическая алгоритмика » в LMS Электронный университет Moodle ЯрГУ, в котором:

- представлены задания для самостоятельной работы обучающихся по темам дисциплины;
- осуществляется проведение отдельных мероприятий текущего контроля успеваемости студентов;
- представлены тексты лекций по всем темам дисциплины;
- представлены правила прохождения промежуточной аттестации по дисциплине;
- представлен список учебной литературы, рекомендуемой для освоения дисциплины;
- представлена информация о форме и времени проведения консультаций по дисциплине в режиме онлайн;
- посредством форума осуществляется синхронное и (или) асинхронное взаимодействие между обучающимися и преподавателем в рамках изучения дисциплины.

6. Перечень лицензионного и (или) свободно распространяемого программного обеспечения, используемого при осуществлении образовательного процесса по дисциплине

В процессе осуществления образовательного процесса по дисциплине используются:

для формирования материалов для текущего контроля успеваемости и проведения промежуточной аттестации, для формирования методических материалов по дисциплине:

- программы Microsoft Office;
- издательская система LaTex;
- Adobe Acrobat Reader.

7. Перечень современных профессиональных баз данных и информационных справочных систем, используемых при осуществлении образовательного процесса по дисциплине (при необходимости)

В процессе осуществления образовательного процесса по дисциплине используются:

томатизированная библиотечно-информационная система «БУКИ-NEXT» http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php
Электронная библиотека учебных материалов ЯрГУ
http://www.lib.uniyar.ac.ru/opac/bk_one_find.php
Электронная картотека "Книгообеспеченность"
http://www.lib.uniyar.ac.ru/opac/bk_one_find.php

8. Перечень основной и дополнительной учебной литературы, ресурсов информационно-телекоммуникационной сети «Интернет» (при необходимости), рекомендуемых для освоения дисциплины

а) основная литература

1. Яблокова С.И. Основы алгебраической алгоритмики. Часть 1: учебное пособие. – Ярославль: ЯрГУ, 2008. – 127с.
http://www.lib.uniyar.ac.ru/edocs/iuni/20080290.pdf
2. Яблокова С.И. Основы алгебраической алгоритмики. Часть 2: учебное пособие. – Ярославль: ЯрГУ, 2009. – 120с. [Электронный ресурс]
http://www.lib.uniyar.ac.ru/edocs/iuni/20090237.pdf
3. Яблокова С.И. Задачи по алгебраической алгоритмике. Практикум. Часть 2 – Ярославль, 2018. – 56 с. http://www.lib.uniyar.ac.ru/edocs/iuni/20180230.pdf
4. Ноден П., Китте К. Алгебраическая алгоритмика. – М.: Мир, 1999. – 720с

б) дополнительная литература

4. Ван дер Варден Б.Л. Алгебра. – М.: Наука, 1976.
5. Берлекэмп Э. Алгебраическая теория кодирования. – М.: Мир, 1971. -- 239 с.
6. Акритас А. Основы компьютерной алгебры с приложениями. – М.: Мир, 1994. – 554с

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине включает в свой состав специальные помещения:

- учебные аудитории для проведения занятий лекционного типа;
- учебные аудитории для проведения практических занятий (семинаров);
- учебные аудитории для проведения групповых и индивидуальных консультаций;
- учебные аудитории для проведения текущего контроля и промежуточной аттестации;
- помещения для самостоятельной работы;

- помещения для хранения и профилактического обслуживания технических средств обучения.

Специальные помещения укомплектованы средствами обучения, служащими для представления учебной информации большой аудитории.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде ЯрГУ.

Автор:
Доцент кафедры алгебры и математической логики, к.ф.-м.н. С. И. Яблокова

Приложение № 1 к рабочей программе дисциплины
«Алгебраическая алгоритмика»

Фонд оценочных средств
для проведения текущего контроля успеваемости
и промежуточной аттестации студентов
по дисциплине

1. Типовые контрольные задания и иные материалы, используемые в процессе текущего контроля успеваемости

Задания для самостоятельной работы

(данные задания выполняются студентом самостоятельно и преподавателем в обязательном порядке не проверяются)

Задания по самостоятельному решению задач студенты получают на лекции после прохождения темы курса. Задачи берутся из практикума:
Яблокова С.И. Задачи по алгебраической алгоритмике. Практикум. Часть 2 – Ярославль, 2018. – 56 с. http://www.lib.uniyar.ac.ru/edocs/iuni/20180230.pdf

Контрольная работа № 1

(проверка сформированности ПК-2, индикатор ИД-ПК-2_1)

1. Используя расширенный алгоритм Евклида, найти коэффициенты Безу и представить НОД чисел a и b в виде au+bv: a=127, b=35.
2. С помощью расширенного алгоритма Евклида найти НОД и «коэффициенты Безу» в кольце $Z_2[x]$:

$$f_1(x) = x^5 + x^4 + 1, \qquad f_2(x) = x^4 + x^2 + 1.$$

3. Свернуть периодическую цепную дробь: [(1,2,3)].
4. С помощью алгоритма, основанного на китайской теореме об остатках, решить задачу интерполяции в кольце $Z_5[x]$:

x_i	0	1	2	3	4
$f_i(x)$	2	1	0	4	2

5. Является ли многочлен приводимым? Если да, то разложить на неприводимые сомножители в кольце Z_5: $x^5 + x^2 + x + 2$.

Ответы к задачам:

1. $\text{НОД}(127, 35) = 1 = 8 \cdot 127 - 29 \cdot 35;$
2. $\text{НОД}\big(f_1(x), f_2(x)\big) = x^2 + x + 1 = (x+1)f_1(x) + x^2 f_2(x);$
3. $\frac{4+\sqrt{37}}{7}$;
4. $x^4 - x^3 + x^2 + 3x + 2;$
5. $(x-1)(x-2)^2(x^2+2).$

Правила выставления оценки по результатам контрольной работы:

Оценка по результатам контрольной работы считается в баллах по каждому заданию по следующему принципу:

- правильно выполненное задание – 4 балла;
- при выполнении задания правильно найден оптимальный алгоритм решения, но имеются незначительные ошибки в численных расчетах – 3 балла;
- при выполнении задания не найден оптимальный алгоритм и допущены несущественные ошибки в вычислениях – 2 балла;
- при выполнении задания не найден оптимальный алгоритм и допущены существенные ошибки в вычислениях – 1 балл;
- при выполнении задания неправильно – 0 баллов.

Набранное количество баллов 19-20 соответствует оценке «отлично», 16-18 баллов – оценке «хорошо», 12-15 баллов – оценке «удовлетворительно», менее 12 баллов – оценке «неудовлетворительно» (умения и навыки на данном этапе освоения дисциплины не сформированы).

Контрольная работа № 2

(проверка сформированности ПК-2, индикатор ИД-ПК-2_1)

1. Решить систему сравнений
$$\begin{cases} 17x \equiv 7 \ (mod\ 2) \\ 2x \equiv 1 \ (mod\ 3) \\ 2x \equiv 2 \ (mod\ 5). \end{cases}$$
2. Является ли элемент a кольца $\mathbb{Z}_n$ обратимым? Если да, то найти a^{-1}: $a = 7,\ n = 15.$
3. Найти примитивный корень по модулю $n = 27.$
4. Является ли мультипликативная группа кольца $\mathbb{Z}_{98}$ циклической? Ответ обосновать. Найти порядок мультипликативной группы.
5. В $Z_2[x]$ найти минимальный многочлен элемента $\beta = \alpha + 1$, если α -- корень многочлена $x^4 + x^3 + 1$.
6. Построить поле Галуа $GF(2^5) \cong \mathbb{Z}_2[x]/(m(x))$, где $m(x) = x^5 + x^4 + x^3 + x + 1$
c – примитивен в $\mathbb{Z}_2[x]$. Дать три возможных представления элементов поля.

Ответы к задачам:

1. $x \equiv 11\ (mod\ 30)$;
2. $7^{-1} \equiv 13\ (mod\ 15)$;
3. 2;
4. Да: порядок равен 42;
5. $x^4 + x^3 + x^2 + x + 1$;
6.

Степенное представление	Представление в виде многочлена	Векторное представление
0	0	(0,0,0,0,0)
1	1	(1,0,0,0,0)
α	α	(0,1,0,0,0)

α^2	α^2	(0,0,1,0,0)
α^3	α^3	(0,0,0,1,0)
α^4	α^4	(0,0,0,0,1)
α^5	$\alpha^4+\alpha^3+\alpha+1$	(1,1,0,1,1)
α^6	$\alpha^3+\alpha^2+1$	(1,0,1,1,0)
α^7	$\alpha^4+\alpha^3+\alpha$	(0,1,0,1,1)
α^8	$\alpha^3+\alpha^2+\alpha+1$	(1,1,1,1,0)
α^9	$\alpha^4+\alpha^3+\alpha^2+\alpha$	(0,1,1,1,1)
α^{10}	$\alpha^2+\alpha+1$	(1,1,1,0,0)
α^{11}	$\alpha^3+\alpha^2+\alpha$	(0,1,1,1,0)
α^{12}	$\alpha^4+\alpha^3+\alpha^2$	(0,0,1,1,1)
α^{13}	$\alpha+1$	(1,1,0,0,0)
α^{14}	$\alpha^2+\alpha$	(0,1,1,0,0)
α^{15}	$\alpha^3+\alpha^2$	(0,0,1,1,0)
α^{16}	$\alpha^4+\alpha^3$	(0,0,0,1,1)
α^{17}	$\alpha^3+\alpha+1$	(1,1,0,1,0)
α^{18}	$\alpha^4+\alpha^2+\alpha$	(0,1,1,0,1)
α^{19}	$\alpha^4+\alpha^2+\alpha+1$	(1,1,1,0,1)
α^{20}	$\alpha^4+\alpha^2+1$	(1,0,1,0,1)
α^{21}	α^4+1	(1,0,0,0,1)
α^{22}	$\alpha^4+\alpha^3+1$	(1,0,0,1,1)
α^{23}	α^3+1	(1,0,0,1,0)
α^{24}	$\alpha^4+\alpha$	(0,1,0,0,1)
α^{25}	$\alpha^4+\alpha^3+\alpha^2+\alpha+1$	(1,1,1,1,1)
α^{26}	α^2+1	(1,0,1,0,0)
α^{27}	$\alpha^3+\alpha$	(0,1,0,1,0)
α^{28}	$\alpha^4+\alpha^2$	(0,0,1,0,1)
α^{29}	$\alpha^4+\alpha+1$	(1,1,0,0,1)
α^{30}	$\alpha^4+\alpha^3+\alpha^2+1$	(1,0,1,1,1)

Правила выставления оценки по результатам контрольной работы:

Оценка по результатам контрольной работы считается в баллах по каждому заданию по следующему принципу:

- правильно выполненное задание – 4 балла;
- при выполнении задания правильно найден оптимальный алгоритм решения, но имеются незначительные ошибки в численных расчетах – 3 балла;
- при выполнении задания не найден оптимальный алгоритм и допущены несущественные ошибки в вычислениях – 2 балла;
- при выполнении задания не найден оптимальный алгоритм и допущены существенные ошибки в вычислениях – 1 балл;
- при выполнении задания неправильно – 0 баллов.

Набранное количество баллов 23-24 соответствует оценке «отлично», 20-22 баллов – оценке «хорошо», 17-21 баллов – оценке «удовлетворительно», менее 17 баллов – оценке «неудовлетворительно» (умения и навыки на данном этапе освоения дисциплины не сформированы).

Тест для самопроверки по результатам освоения дисциплины перед зачетом

В тесте 7 вопросов, за правильный ответ на каждый вопрос дается 1 балл. На прохождение теста дается время 20 минут.

Количество набранных баллов от 6 до 7 соответствует оценке «отлично».

Количество набранных баллов от 4 до 5 соответствует оценке «хорошо».

Количество набранных баллов 3 соответствует оценке «удовлетворительно».

Количество баллов меньше 3 соответствует оценке «неудовлетворительно».

Примерные вопросы теста:

1. Можно ли утверждать, что многочлен $f(x) = x^2 - 1 \in \mathbb{Z}_{12}[x]$ имеет в $\mathbb{Z}_{12}$ два различных корня?(выбрать верный ответ):

1) да; 2) нет.

2. Оценить сверху число делений для нахождения НОД многочленов $f(x) = x^5 - 2x^3 + 3x^2 - 2x + 4$ и $g(x) = x^3 - 2x + 5$ в $\mathbb{R}[x]$, не проводя вычислений.

Выбрать правильный ответ:

1) $n \leq 6$;
2) $n \leq 4$;
3) $n \leq 3$.

3. Является ли факторкольцо $\mathbb{Z}_2[x]/(x^5 + x^3 + 1)$ полем? Выбрать правильный ответ:

1) да; 2) нет.

4. Является ли многочлен $f(x) = x^5 + 4x^4 - 7x^3 + 2x + 3$ приводимым в $\mathbb{Z}[x]$? Выбрать правильный ответ:

1) да; 2) нет.

5. Является ли многочлен $f(x) = x^4 + 19$ приводимым в $\mathbb{Z}_{23}[x]$? Выбрать правильный ответ:

1) да; 2) нет

6. Сколько существует унитарных неприводимых многочленов 6-й степени в $\mathbb{Z}_3[x]$?(выбрать верный ответ):

1) 128;
2) 116;
3) 122;
4) 121.

7. Какие условия должны выполняться, чтобы элемент a являлся примитивным корнем в $GF(64)$?

Выбрать правильный ответ:

1) $\begin{cases} a^9 \not\equiv 1 \ (mod\ 64) \\ a^7 \not\equiv 1 \ (mod\ 64) \end{cases}$;

2) $\begin{cases} a^9 \not\equiv 1 \ (mod\ 64) \\ a^{21} \not\equiv 1 \ (mod\ 64) \end{cases}$;

3) $\begin{cases} a^3 \not\equiv 1\ (mod\ 64) \\ a^7 \not\equiv 1\ (mod\ 64) \end{cases}$;

4) $\begin{cases} a^9 \not\equiv 1\ (mod\ 64) \\ a^{63} \equiv 1\ (mod\ 64) \end{cases}$;

5) $\begin{cases} a^7 \not\equiv 1\ (mod\ 64) \\ a^{63} \equiv 1\ (mod\ 64) \end{cases}$.

Правильные ответы:

Вопрос №	Вариант ответа		**Вопрос №**	Вариант ответа
1	2		**5**	1
2	2		**6**	2
3	1		**7**	2
4	2			

Тест для самопроверки по результатам освоения дисциплины
перед зачетом
(тест проводится в ЭУК «Алгебраическая алгоритмика (магистры)» в LMS Moodle)

В тесте 9 вопросов, за правильный ответ на каждый вопрос дается 1 балл. На прохождение теста дается время 30 минут.

Количество набранных баллов от 8 до 9 соответствует оценке «отлично».

Количество набранных баллов от 6 до 7 соответствует оценке «хорошо».

Количество набранных баллов от 4 до 5 соответствует оценке «удовлетворительно».

Количество баллов меньше 4 соответствует оценке «неудовлетворительно».

Примерные вопросы теста:

1. Можно ли утверждать, что многочлен $f(x) = x^2 - 1 \in \mathbb{Z}_{12}[x]$ имеет в $\mathbb{Z}_{12}$ два различных корня?(выбрать верный ответ):
1) да; 2) нет.
2. Оценить сверху число делений для нахождения НОД многочленов $f(x) = x^5 - 2x^3 + 3x^2 - 2x + 4$ и $g(x) = x^3 - 2x + 5$ в $\mathbb{R}[x]$, не проводя вычислений. Выбрать правильный ответ:
1).$n \leq 6$;
2).$n \leq 4$;
3).$n \leq 3$.
3. Является ли факторкольцо $\mathbb{Z}_2[x]/(x^5 + x^3 + 1)$ полем? Выбрать правильный ответ:
1) да; 2) нет.

4.Является ли многочлен $f(x) = x^5 + 4x^4 - 7x^3 + 2x + 3$ приводимым в $\mathbb{Z}[x]$? Выбрать правильный ответ:
1) да; 2) нет.

5.Является ли многочлен $f(x) = x^4 + 19$ приводимым в $\mathbb{Z}_{23}[x]$? Выбрать правильный ответ:
1) да; 2) нет
6.Сколько существует унитарных неприводимых многочленов 6-й степени в $\mathbb{Z}_3[x]$?(выбрать верный ответ):
1). 128;
2). 116;
3). 122;
4)121.
7.Какие условия должны выполняться, чтобы элемент a являлся примитивным корнем в $GF(64)$?
Выбрать правильный ответ:

1). $\begin{cases} a^9 \not\equiv 1 \ (mod\ 64) \\ a^7 \not\equiv 1 \ (mod\ 64) \end{cases}$;

2). $\begin{cases} a^9 \not\equiv 1 \ (mod\ 64) \\ a^{21} \not\equiv 1 \ (mod\ 64) \end{cases}$;

3). $\begin{cases} a^3 \not\equiv 1 \ (mod\ 64) \\ a^7 \not\equiv 1 \ (mod\ 64) \end{cases}$;

4). $\begin{cases} a^9 \not\equiv 1 \ (mod\ 64) \\ a^{63} \equiv 1 \ (mod\ 64) \end{cases}$;

5).

$$\begin{cases} a^7 \not\equiv 1 \ (mod\ 64) \\ a^{63} \equiv 1 \ (mod\ 64) \end{cases}.$$

Правильные ответы:

Вопрос №	Вариант ответа		**Вопрос №**	Вариант ответа
1	2		**6**	2
2	2		**7**	2
3	1			
4	2			
5	1			

2. Список вопросов и (или) заданий для проведения промежуточной аттестации

Аттестация по дисциплине проводится в форме зачета. Зачет проводится в форме собеседования. Для допуска к собеседованию студент в течение семестра должен удовлетворительно написать контрольные №№ 1 -- 2, т. е. в каждой контрольной работе

правильно решить 75-80% предложенных задач. Если это условие не выполнено, студенту сначала предлагается решить задачи по тем темам, которые вызывали у него трудности в течение семестра. Задачи подбираются аналогичные тем, которые предлагались в контрольных работах.

ВОПРОСЫ К ЗАЧЕТУ ПО КУРСУ "АЛГЕБРАИЧЕСКАЯ АЛГОРИТМИКА"

Наибольший общий делитель (НОД) целых чисел. Теорема о представлении НОД. Свойства НОД. Наименьшее общее кратное (НОК) целых чисел.

Алгоритм Евклида и теорема Ламе. Леммы о числе итераций алгоритма Евклида. Двоичная оценка сложности алгоритма.

Расширенный алгоритм Евклида для чисел. Вычисление коэффициентов Безу. Оценки коэффициентов Безу.

Алгоритм Евклида и цепные дроби. Свойства цепных дробей. Теорема единственности. Теорема о представлении рациональных чисел цепными дробями. Периодические цепные дроби. Свойства подходящих дробей. Теорема о приближении иррациональных чисел подходящими дробями.

Неразложимые и простые числа. Связь между ними. Основная теорема арифметики. Факториальные кольца.

Сравнения и их свойства. Классы вычетов по модулю m. Целостное кольцо. Необходимые и достаточные условия целостности кольца. Условие существования мультипликативного обратного по модулю m. Кольцо и поле вычетов по модулю m .

Евклидовы кольца. Целостное кольцо. Разложение на множители в евклидовом кольце. Теорема единственности разложения на множители.

Псевдопростые числа по данному основанию. Примеры. Числа Кармайкла. Теорема Вильсона.

Мультипликативная группа кольца Z_n. Теорема о порядке группы. Циклические группы. Примитивный корень по модулю m . Порядок элемента группы. Теоремы о порядке элемента группы. Лемма о порядке произведения двух элементов абелевой группы. Лемма о группе, порядок которой равен НОК порядков всех её элементов. Цикличность группы Z_p при простом p. Лемма Гаусса. Теорема Гаусса (необходимое и достаточное условие цикличности группы Z_n^*). Количество примитивных корней по модулю m .

Китайские теоремы об остатках для систем сравнений.

Тесты простоты. Детерминистические тесты, основанные на решете Эратосфена, критерии Вильсона. Тест Люка и его обоснование. Недостатки детерминистических тестов. Тесты псевдопростоты. Сильно псевдопростые числа по данному основанию. Теорема о существовании бесконечного числа псевдопростых чисел по основанию 2. свойство чисел Кармайкла. Обоснование теста сильной псевдопростоты.

Многочлены. Евклидово деление. Корни многочлена. Метод Горнера (два алгоритма).

Интерполяция над полем. Формула Лагранжа. Интерполяция с помощью китайской теоремы об остатках.

Простые и неприводимые многочлены. Классы эквивалентности по модулю m(x). Факторкольцо $K[x]/(m(x))$. Поле $K[x]/(m(x))$. Простые расширения поля K.

Евклидовы кольца и делимость многочленов. Норма элемента. НОД многочленов. Алгоритм Евклида для многочленов.

Алгоритм Евклида для многочленов над полем. Расширенный алгоритм Евклида для многочленов над полем. «Коэффициенты» Безу.

Китайская теорема об остатках для многочленов.

Неприводимые многочлены. Факториальные и евклидовы кольца. Разложение на множители. Теорема Гаусса. Примитивные многочлены. Рациональные корни многочленов из $Z[x]$. Критерий Эйзенштейна неприводимости многочлена над Z (в факториальном кольце).

Неприводимые многочлены с коэффициентами из Z_p. Теоремы. Число неприводимых многочленов степени n в $Z_p[x]$. Критерий неприводимости многочлена над Z_p.

Конечное поле. Теорема об условиях, которым должно удовлетворять кольцо, чтобы оно являлось полем. Теорема об уравнении, которому удовлетворяют все элементы конечного поля и следствие из нее. Теорема о порядке элемента конечного поля. Теорема о факторкольце $Z_p[x]/(p(x))$. Простое расширение поля Z_p. Обратное утверждение. Характеристика поля. Мультипликативная группа конечного поля. Примитивный элемент поля. Нахождение примитивного элемента в конечном поле. Лемма. Поле разложения многочлена. Теорема о существовании минимального многочлена для алгебраического над полем элемента. Теорема об алгебраичности любого элемента простого расширения. Правило возведения в степень p в поле с характеристики p и следствия из нее. Обобщение теоремы о возведении в степень.

Корни неприводимого многочлена в $Z_p[x]$. Теорема о корнях. Существование конечного поля из p^r элементов (p – простое). Неприводимые многочлены в конечном поле. Теорема существования неприводимого многочлена степени r в конечном поле. Теорема о произведении всех неприводимых многочленов из $Z_p[x]$, степени которых делят r. Разложение многочлена на неприводимые в конечном поле. Построение полей Галуа $GF(2^n)$.

Вопросы для самопроверки при подготовке к зачету.

Вопрос 1. Какова оценка числа делений алгоритма Евклида нахождения НОД двух целых положительных чисел?
Варианты ответов:
1). Число делений мажорируется 5-кратным числом десятичных цифр в представлении наименьшего из двух чисел.
2). Число делений мажорируется 5-кратным числом десятичных цифр в представлении наибольшего из двух чисел.
3). Количество делений мажорируется числом

$$\lfloor 2log_2 M \rfloor + 1$$

где M -- максимальное из двух чисел.

Вопрос 2. Есть ли отличие между алгоритмом Евклида и расширенным алгоритмом Евклида?
Варианты ответов:
1). Эти алгоритмы ничем не отличаются друг от друга.
2). Расширенный алгоритм Евклида ищет коэффициенты Безу, а алгоритм Евклида ищет НОД двух чисел.

3). Расширенный алгоритм Евклида ищет НОД двух чисел и коэффициенты Безу, в то время как с помощью алгоритма Евклида можно найти лишь НОД чисел.

Вопрос 3. Какой непрерывной дробью представляется рациональное число?
Варианты ответов:
1). Бесконечной периодической.
2). Конечной.
3). Бесконечной непериодической.

Вопрос 4. Что можно сказать о НОД числителя и знаменателя подходящей дроби?
Варианты ответов:
1). Он больше 1.
2). Он равен числителю подходящей дроби.
3). Он равен 1.

Вопрос 5. Отличается ли метод разложения в непрерывную дробь для рациональных и иррациональных чисел?
Варианты ответов:
1). И рациональные и иррациональные числа можно раскладывать в непрерывную дробь с помощью выделения целой и дробной части числа.
2). Метод одинаков для всех чисел.
3). Иррациональные числа нужно раскладывать в непрерывную дробь с помощью выделения целой и дробной части числа. Рациональные можно раскладывать в непрерывную дробь тем же методом, а можно использовать алгоритм Евклида, применяя его к числителю и знаменателю данного рационального числа.

Вопрос 6. Совпадают ли понятия простого и неразложимого элемента в кольце? Когда эти понятия совпадают? Есть ли между этими понятиями какая-то связь?
Варианты ответов:
1). Эти два понятия совпадают в любом кольце.
2). Для любого кольца эти понятия, вообще говоря, не совпадают. В кольце без делителей нуля простой элемент является неразложимым. Обратное утверждение для произвольного кольца неверно. Эти два понятия совпадают в факториальном кольце.
3). Для любого кольца эти понятия, вообще говоря, не совпадают. В кольце без делителей нуля неразложимый элемент является простым. Обратное утверждение для произвольного кольца неверно. Эти два понятия совпадают в факториальном кольце.

Вопрос 7. Дайте определение кольца вычетов по модулю данного натурального числа.
Варианты ответов:
1). Кольцо вычетов по модулю n -- это множество из n классов вычетов с введенными на нем операциями сложения и умножения, определенными через из представителей, т.е. $Z_n = \{[0], [1], \dots, [n-1]\}$

$$[a] + [b] = [a + b], \qquad [a][b] = [ab]$$

где класс $[a]$ содержит все целые числа, сравнимые с a по модулю n.
2). Кольцо вычетов по модулю n -- это множество из n чисел
$Z_n = \{0,1,2, \dots, n-1\}$
сложение и умножение которых проводится по модулю n.
3). Кольцо вычетов по модулю n -- это множество из n чисел
$Z_n = \{0,1,2, \dots, n-1\}$.

Вопрос 8. Сформулируйте условия обратимости элемента в кольце вычетов по модулю n.
Варианты ответов:
1). Любой ненулевой элемент кольца вычетов обратим по модулю n.
2). Элемент кольца вычетов обратим, если он не делится на n.
3). Элемент кольца вычетов обратим тогда и только тогда, когда он взаимно прост с n.

Вопрос 9. Имеет ли решения сравнение
$$15x \equiv 7 \ (mod\ 25)?$$ Ответ обосновать.
Варианты ответов:
1). Это сравнение имеет 5 решений, поскольку НОД 15 и 25 равен 5.
2). Это сравнение имеет одно решение.
3). Сравнение не имеет решений, поскольку НОД 15 и 25 не делит 7.

Вопрос 10. Сколько решений имеет сравнение
$$24x \equiv 16 \ (mod\ 40)?$$
Варианты ответов:
1). Оно имеет 8 решений по модулю 40, так как НОД 24 и 40 равен 8, и 8 делит правую часть сравнения.
2). Оно имеет одно решение.
3). Оно не имеет решений.

Правильные ответы

Вопрос №	Вариант ответа		Вопрос №	Вариант ответа		Вопрос №	Вариант ответа
			4	3		**8**	3
1	1,3		**5**	3		**9**	3
2	3		**6**	2		**10**	1
3	2		**7**	1			

Количество правильных ответов не менее 8 вместе с правильно решенными задачами по изученным темам соответствует уровню формирования в рамках данной дисциплины компетенций ОПК-2 не ниже порогового уровня. В этом случае студенту выставляется оценка "зачтено".

1.3. Список вопросов и (или) заданий для проведения итоговой аттестации

Итоговая аттестация по дисциплине проводится в форме зачета. Зачет проводится в форме собеседования. Для допуска к собеседованию студент в течение семестра должен удовлетворительно написать контрольные №№ 1 -- 2, т. е. в каждой контрольной работе правильно решить 75-80% предложенных задач. Если это условие не выполнено, студенту сначала предлагается решить задачи по тем темам, которые вызывали у него трудности в течение семестра. Задачи подбираются аналогичные тем, которые предлагались в контрольных работах.

Приложение № 2 к рабочей программе дисциплины
« Алгебраическая алгоритмика»

Методические указания для студентов по освоению дисциплины

Для успешного усвоения данного курса необходимо знание следующих вопросов:
- сравнения по модулю целого числа, свойства сравнений;
- функция Эйлера и ее основные свойства;
- теорема Эйлера и малая теорема Ферма;
- кольцо и поле вычетов по модулю натурального числа;
- мультипликативная группа кольца вычетов;
- строение мультипликативных групп колец вычетов по модулю простого числа, по модулю степени простого числа и по модулю степени двойки;
- алгоритм Евклида для чисел и многочленов над полем;
- строение полей Галуа;
- понятие примитивного элемента поля Галуа;
- понятие минимального многочлена алгебраического над полем элемента;
- свойство корней неприводимого многочлена из кольца Z/(p)[x];
- теорема о произведении всех неприводимых многочленов из Z/(p)[x], степени которых делят n.

Все эти вопросы изложены в пособиях:

1. Яблокова С.И. Основы алгебраической алгоритмики. Часть 1. -- Ярославль, ЯрГУ, 2008.-- 127с.
2. Яблокова С.И. Основы алгебраической алгоритмики. Часть 2. -- Ярославль, ЯрГУ, 2009. -- 120с.
3. Яблокова С.И. Задачи по алгебраической алгоритмике. Практикум. -- Ярославль, 2016. -- 76 с.
4. Задачи по второй части курса "Алгебраическая алгоритмика". В локальной сети 7 корпуса на диске I (I/Inform/ M_КБ/ Яблокова/КБ_2/algor_z22.pdf.

Кроме того, можно найти изложение этих вопросов в следующих книгах:

1. Ноден П., Китте К. Алгебраическая алгоритмика. -- М.: Мир, 1999. -- 720с.
2. Акритас А. Основы компьютерной алгебры с приложениями. -- М.: Мир, 1994. -- 544с.
3. Берлекэмп Э. Алгебраическая теория кодирования. – М.: Мир, 1971. -- 239 с.

Практикум " Задачи по алгебраической алгоритмике" снабжен указаниями и примерами с подробным разбором методов решения. Он также содержит задачи по темам, связанным с кольцом целых чисел, как для решения на практических занятиях так и для самостоятельной работы.

Практикум "Задачи по второй части курса Алгебраическая алгоритмика" (локальная сеть 7 корпуса ЯрГУ на диске I (I/Inform/ M_КБ/ Яблокова/КБ_2/algor_z22.pdf) содержит задачи по темам, связанным с кольцом многочленов, как для решения на практических занятиях так и для самостоятельной работы. Он также снабжен указаниями и примерами с подробным разбором методов решения: