

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

Кафедра алгебры и математической логики

УТВЕРЖДАЮ

Декан математического факультета



Нестеров П.Н.

21 мая 2024 г.

**Рабочая программа дисциплины**

**Алгебраическая алгоритмика**

Направление подготовки (специальности)  
10.05.01 Компьютерная безопасность

Направленность (профиль)  
«Математические методы защиты информации»

Форма обучения очная

Программа рассмотрена  
на заседании кафедры  
от 12 апреля 2024 г., протокол № 8

Программа одобрена НМК  
математического факультета  
протокол № 9 от 3 мая 2024 г.

## 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 обязательной части образовательной программы. 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.

## 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
<b>Общепрофессиональные компетенции</b>		
<b>ОПК-3</b> Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности	<b>И-ОПК-3.2</b> Осуществляет постановку задачи, выбирает способ ее решения <b>И-ОПК-3.3</b> Применяет математический аппарат для решения прикладных и теоретических задач	<b>Знать:</b> -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. <b>Уметь:</b> - строить алгоритмы для решения алгебраических задач; - исследовать сложность используемых алгоритмов; - доказывать утверждения, - описывать строение некоторых мультипликативных групп колец вычетов. <b>Владеть навыками:</b> -основными понятиями и методами алгебры в кольце целых чисел; - основными понятиями и методами алгебры в кольце многочленов от одной переменной.

		<p>- методами доказательства утверждений.</p> <p><b>Знать:</b></p> <p>-основные методы решения алгоритмических проблем, возникающих в алгебре и в ее приложениях к решению практических задач;</p> <p><b>Уметь:</b></p> <p>- решать задачи теоретического и прикладного характера из различных разделов курса;</p> <p><b>Владеть навыками:</b></p> <p>-применять методы алгебраической алгоритмики в смежных дисциплинах.</p>
<p><b>ОПК-10</b></p> <p>Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности.</p>	<p><b>И-ОПК-10.1</b></p> <p>Способен использовать методы алгебраической алгоритмики, основные факты и понятия для решения прикладных задач.</p>	<p><b>Знать:</b></p> <p>- возможности применения методов алгебраической алгоритмики в криптографии;</p> <p>-основные виды понятий и алгоритмов, используемых для защиты информации;</p> <p>-- возможные сферы приложений алгоритмов и методов алгебраической алгоритмики для криптографических алгоритмов.</p> <p><b>Уметь:</b></p> <p>- решать задачи теоретического и прикладного характера и разрабатывать машинные алгоритмы решения этих задач.</p> <p><b>Владеть навыками:</b></p> <p>- применения математического аппарата алгебраической алгоритмики в программировании;</p> <p>-применения методов алгебраической алгоритмики в смежных дисциплинах.</p>
<p><b>ОПК-2.1</b></p> <p>Способен разрабатывать алгоритмы, реализующие современные математические методы защиты информации.</p>	<p><b>И-ОПК-2.1.2</b></p> <p>Способен разрабатывать алгоритмы, используемые в современных математических методах защиты информации</p>	<p><b>Знать:</b></p> <p>- возможности применения методов алгебраической алгоритмики в криптографии;</p> <p>-основные виды понятий и алгоритмов курса, используемых в криптографии;</p> <p>-- возможные сферы приложений алгоритмов и методов алгебраической алгоритмики для криптографических алгоритмов.</p> <p><b>Уметь:</b></p> <p>- разрабатывать машинные алгоритмы решения задач.</p> <p><b>Владеть навыками:</b></p> <p>- применения математического аппарата алгебраической алгоритмики в программировании;</p> <p>-применения методов алгебраической алгоритмики для решения задач криптографии.</p>

#### 4. Объем, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет **6** зачетных единиц, **216** 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		
1.	Вводная лекция	4	0,5						
2.	Алгоритм Евклида	4	5,5	2				6	Задания для самостоятельной работы.
3.	Непрерывные дроби	4	3	2		1		6	Задания для самостоятельной работы. Контр. раб. № 1
4.	Евклидовы кольца	4	5	2		1		6	Задания для самостоятельной работы. Контр. раб. № 2
5.	Сравнения. Классы вычетов	4	6	5		1		4	Задания для самостоятельной работы. Контр. раб. № 3
6.	Основные функции и теоремы теории чисел	4	3	1				6	Задания для самостоятельной работы
7.	Группы. Мультипликативные группы колец вычетов	4	3					6	Задания для самостоятельной работы
8.	Тесты простоты	4	2	2		1		4	Задания для самостоятельной работы. Контр. раб. № 4
9.	Модульная арифметика	4	2	2		1		4	Задания для самостоятельной работы.
10.	Линейные рекуррентные последовательности	4	2					4	Задания для самостоятельной работы
							0,3	8,7	Зачет
	Всего за 4 семестр 108 акад. часов		32	16		5	0,3	54,7	
11.	Алгоритм Евклида для многочленов	5	4	2		1		3	Задания для самостоятельной работы.
12.	Интерполяция	5	2	2				3	Задания для самостоятельной работы.

									Контр. раб. № 5
13.	Факторкольцо <div></div>	5	3	2		1		3	Задания для самостоятельной работы.
14.	Разложение многочлена на множители	5	4	1				3	Задания для самостоятельной работы.
15.	Неприводимость многочленов над конечным полем	5	5	1		1		2	Задания для самостоятельной работы. Контр. раб. № 6
16.	Поля Галуа	5	4	2		1		2	Задания для самостоятельной работы.
17.	Быстрые алгоритмы вычисления сверток	5	5	4				2	Задания для самостоятельной работы.
18.	Дискретное преобразование Фурье	5	5	2		1		1	Задания для самостоятельной работы.
						2	0,5	33,5	Экзамен
	Всего за 5 семестр 108 часов		32	16		7	0,5	52,5	
	Всего		64	32		12	0,8	107,2	

### 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. Приложение к решению линейных диофантовых уравнений

#### 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: Евклидовы кольца

Кольцо. 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. Кольцо

#### Тема №5: Сравнения. Классы вычетов

Сравнения и их свойства. Классы вычетов по данному 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: Основные функции и теоремы теории чисел

Теоремы о простых числах. Решето Эратосфена. Функция Эйлера и ее основные свойства. Малая теорема Ферма. Теорема Эйлера. Дихотомический алгоритм. Теорема Вильсона. Теорема Вильсона.

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

Мультипликативная группа кольца  $\mathbb{Z}/m\mathbb{Z}$ . Циклические группы. Прimitивный корень по модулю  $m$ . Порядок элемента группы. Циклическость группы  $\mathbb{Z}/p\mathbb{Z}$  при простом  $p$ . Лемма Гаусса. Теорема Гаусса (необходимое и достаточное условие циклическости группы  $\mathbb{Z}/m\mathbb{Z}$ ).

### 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: Модульная арифметика

Многомодульная арифметика. Представление со смешанными основаниями. Выбор модулей для двоичного компьютера.

### Тема №10: Линейные рекуррентные последовательности

Линейные рекуррентные последовательности максимального периода. Периодические и почти периодические последовательности. Одношаговые генераторы. Декартово произведение генераторов. Необходимые и достаточные условия того, что линейный генератор сравнений является генератором максимального периода.

### Тема №11: Алгоритм Евклида для многочленов

Отношения делимости в  $\mathbb{Z}[x]$ . Теоремы о евклидовом делении. Алгоритм Евклида в кольце  $\mathbb{Z}[x]$ . Теоремы о представлении НОД в  $\mathbb{Z}[x]$ . Теорема Лазара. Расширенный алгоритм Евклида в  $\mathbb{Z}[x]$ . Вычисление коэффициентов Безу. Оценки коэффициентов Безу. Евклидовы кольца и делимость. Основная теорема арифметики для евклидовых колец. Следствие для кольца  $\mathbb{Z}[x]$ . Факториальное кольцо.

### Тема №12: Интерполяция

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

### Тема №13: Факторкольцо $\mathbb{Z}[x]$

Факторкольцо  $\mathbb{Z}[x]$ . Поле  $\mathbb{Z}[x]$ .

### Тема №14: Разложение многочлена на множители

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

### Тема №15: Неприводимость многочленов над конечным полем

Неприводимые многочлены с коэффициентами из  $\mathbb{F}_p$ . Число неприводимых многочленов степени  $n$  в  $\mathbb{F}_p[x]$ . Критерий неприводимости многочлена над  $\mathbb{F}_p$ . «Решето Эратосфена» для многочленов над  $\mathbb{F}_p$ . Неприводимые многочлены в конечном поле. Разложение многочлена на неприводимые в конечном поле.

### Тема №16: Поля Галуа

Конечное поле. Свойства его элементов. Основные теоремы. Факторкольцо  $\mathbb{F}_p[x]$ . Характеристика поля. Мультипликативная группа конечного поля.

Прimitивный элемент поля. Нахождение прimitивного 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  $\mathbb{F}_{p^n}$ . Существование конечного поля из  $p^n$  элементов. Построение полей Галуа  $\mathbb{F}_{p^n}$ .

### Тема №17: Быстрые алгоритмы вычисления сверток

Линейная и циклическая свертки, их связь. Запись через многочлены. Алгоритм Кука - Тоома. Алгоритм Винограда построения быстрых алгоритмов вычисления коротких сверток.

## **Тема №18: Дискретное преобразование Фурье**

Дискретное преобразование Фурье. Теорема о свертке. БПФ – алгоритм Кули – Тьюки. Алгоритмы Кули – Тьюки по основанию два с прореживанием по времени и по частоте. Алгоритм Рейдера сведения ДПФ к циклической свертке для преобразований простой длины. Алгоритм Рейдера в случае, когда длина преобразования есть степень простого числа. Алгоритм Рейдера в случае, когда длина преобразования есть степень двойки. Малый БПФ-алгоритм Винограда для случаев: 1) длина преобразования есть простое число; 2) длина преобразования есть степень простого числа; 3) длина преобразования есть степень двойки.

## **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.

## **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:

- Автоматизированная библиотечно-информационная система «БУКИ-NEXT»  
[http://www.lib.uniyar.ac.ru/opac/bk\\_cat\\_find.php](http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php)
- Электронная библиотечная система «Лань» <https://e.lanbook.com>
- Электронная библиотечная система «Юрайт» <https://urait.ru>
- Электронная библиотечная система «Консультант студента»  
<https://www.studentlibrary.ru>

## **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.  
<http://www.lib.uniyar.ac.ru/edocs/iuni/20080290.pdf>
2. Яблокова С.И. Основы алгебраической алгоритмики. Часть 2: учебное пособие. – Ярославль: ЯрГУ, 2009.  
<http://www.lib.uniyar.ac.ru/edocs/iuni/20090237.pdf>
3. Яблокова С. И. Введение в быстрые алгоритмы цифровой обработки сигналов: учеб. пособие для вузов - Ярославль, ЯрГУ, 2009  
<http://www.lib.uniyar.ac.ru/edocs/iuni/20090238.pdf>
4. Яблокова С.И. Задачи по алгебраической алгоритмике. Практикум. – Ярославль: ЯрГУ, 2016. <http://www.lib.uniyar.ac.ru/edocs/iuni/20160201.pdf>
5. Яблокова С.И. Задачи по алгебраической алгоритмике. Практикум. Часть 2 – Ярославль: ЯрГУ, 2018. <http://www.lib.uniyar.ac.ru/edocs/iuni/20180230.pdf>

### **б) дополнительная литература**

1. Ноден П., Китте К. Алгебраическая алгоритмика. – Москва, «Мир», 1999.  
<https://matematika76.ru/fm/ноден.djvu>
2. Анеликова Л. А. Алгоритмика в теории и практике - Москва: СОЛОН-ПРЕСС, 2010. <https://www.studentlibrary.ru/ru/doc/ISBN5980033017-SCN0000/000.html>

## **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.



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)*

Практикум "Задачи по алгебраической алгоритмике" снабжен указаниями и примерами с подробным разбором методов решения. Он также содержит задачи по темам первой части курса, как для решения на практических занятиях так и для самостоятельной работы:

задачи на тему 2 содержат задания 1-6 (1-4, 11, 17, 32 задания для самостоятельного решения);

задачи на тему 3 содержат задания 7 - 14 (5-10 задания для самостоятельного решения);

задачи на тему 4 содержат задания 15 - 18 (12-14 задания для самостоятельного решения);

задачи на тему 5 содержат задания 20 - 24 (15, 22-23 задания для самостоятельного решения);

задачи на тему 6 содержат задания 19, 25 - 30 (18-21, 24, 25 задания для самостоятельного решения);

задачи на тему 7 содержат задания 31 - 34 (26-28 задания для самостоятельного решения);

задачи на тему 8 содержит задание 35 (29-31 задания для самостоятельного решения);

задачи на тему 9 содержит задание 36 (33-35 задания для самостоятельного решения);

задачи на тему 10 содержит задание 36 для самостоятельного решения.

Практикум "Задачи по второй части курса Алгебраическая алгоритмика" содержит задачи по темам второй части курса, как для решения на практических занятиях так и для самостоятельной работы. Он также снабжен указаниями и примерами с подробным разбором методов решения:

задачи на тему 11 содержат задания 1-3,9 (1-2, 5, 10 задания для самостоятельного решения);

задачи на тему 12 содержат задания 4 - 7 (3,4,7,8 задания для самостоятельного решения);

задачи на тему 13 содержит задание 8 (9,16 задания для самостоятельного решения);

задачи на тему 14 содержат задания 10,11,17(11, 17 задания для самостоятельного решения);

задачи на тему 15 содержат задания 12 - 15 (6, 12-15 задания для самостоятельного решения);

задачи на тему 16 содержат задания 16, 18 - 20 (18-20 задания для самостоятельного решения).

### Контрольная работа № 1

(проверка сформированности ОПК-3, индикатор И-ОПК-3.2)

(проверка сформированности ОПК-10, индикатор И-ОПК-10.1)

1. Найти все целочисленные решения уравнения:

$$21x - 15y = 39.$$

2. Используя расширенный алгоритм Евклида, найти коэффициенты Безу и представить НОД чисел  $a$  и  $b$  в виде  $au + bv$ :  $a = 127$ ,  $b = 35$ .

3. Найти наибольший общий делитель двух чисел, представленных в двоичной системе счисления, используя бинарный алгоритм:

$$1111111100, \quad 101101100.$$

4. Разложить число в цепную дробь:

5. Свернуть периодическую цепную дробь:  $[(1,2,3)]$ .

6. Разложить в непрерывную дробь (найти период, если число представляется бесконечной периодической дробью)  $\sqrt{21}$ .

7. Найти иррациональное число  $\alpha = [a_1, a_2, \dots, a_k, \alpha_{k+1}]$ , если  $\frac{p_k}{q_k} = \frac{17}{5}$  и

$$\alpha_{k+1} = \frac{1+\sqrt{5}}{2}.$$

#### Ответы к задачам:

1.  $x = 4 + 5t, \quad y = 3 + 7t, \quad t \in \mathbb{Z};$

2.  $\text{НОД}(127, 35) = 1 = 8 \cdot 127 - 29 \cdot 35;$

3. 100;

4.  $[0, 1, 8, 1, 3, 2, 2];$

5.  $\frac{4 + \sqrt{37}}{7};$

6.  $[4, (1, 1, 2, 1, 1, 8)];$

7.  $\frac{73 + \sqrt{5}}{22}.$

#### 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 26-28 соответствует оценке «отлично», 23-28 баллов – оценке «хорошо», 16-22 баллов – оценке «удовлетворительно», менее 22 баллов –

оценке «неудовлетворительно» (умения и навыки на данном этапе освоения дисциплины не сформированы).

### Контрольная работа № 2

(проверка сформированности ОПК-3, индикатор И-ОПК-3.2)

(проверка сформированности ОПК-10, индикатор И-ОПК-10.1)

1. Найти НОД в  $\mathbb{Z}[i]$  чисел  $16 + 28i$ ,  $-8 + 38i$ .
2. Является ли число  $13 + 7i$  приводимым в кольце  $\mathbb{Z}[i]$ ? Если да, то разложить его в произведение неприводимых элементов этого кольца.
3. Является ли данное простое число 113 приводимым элементом кольца  $\mathbb{Z}[i]$ ? Если да, то представить его в виде произведения неприводимых элементов этого кольца.

#### Ответы к задачам:

1.  $4-6i$ ;
2.  $13 + 7i = (1 + i)(10 - 3i)$ ;
3.  $113 = (8 + 7i)(8 - 7i)$ .

#### 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 10-12 соответствует оценке «отлично», 8-9 баллов – оценке «хорошо», 6-7 баллов – оценке «удовлетворительно», менее 7 баллов – оценке «неудовлетворительно» (умения и навыки на данном этапе освоения дисциплины не сформированы).

### Контрольная работа № 3

(проверка сформированности ОПК-3, индикатор И-ОПК-3.2)

(проверка сформированности ОПК-10, индикатор И-ОПК-10.1)

1. Решить сравнение  $72x \equiv 2 \pmod{10}$ .
2. Решить систему сравнений
$$\begin{cases} 17x \equiv 7 \pmod{2} \\ 2x \equiv 1 \pmod{3} \\ 2x \equiv 2 \pmod{5} \end{cases}$$
3. Является ли элемент  $a$  кольца  $\mathbb{Z}_n$  обратимым? Если да, то найти  $a^{-1}$ :  $a = 7$ ,  $n = 15$ .
4. Найти примитивный корень по модулю  $n = 27$ .
5. Является ли мультипликативная группа кольца  $\mathbb{Z}_{98}$  циклической? Ответ обосновать. Найти порядок мультипликативной группы.

#### Ответы к задачам:

1.  $x \equiv 1, 6 \pmod{10}$ ;
2.  $x \equiv 11 \pmod{30}$ ;
3.  $7^{-1} \equiv 13 \pmod{15}$ ;
4. 2;
5.  $98 = 2 \cdot 7^2$ ; по теореме Гаусса группа циклическая, порядок равен 42.

#### 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 не существенные 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 № 4**

*(проверка сформированности ОПК-3, индикатор И-ОПК-3.2)*  
*(проверка сформированности ОПК-10, индикатор И-ОПК-10.1)*  
*(проверка сформированности ОПК-2.1, индикатор И-ОПК-2.1.2)*

1. Является ли число 105 псевдопростым по основанию 8? Сильно псевдопростым?
2. Найти оптимальное число умножений для вычисления  $a^{65}$ .
3. Не находя числа  $x$ , определить его знак, если относительно вектора оснований  $\vec{a} = \{5, 7, 11, 13, 2\}$  ему соответствует стандартный набор остатков  $\vec{x} = (3, 0, 4, 6, 1)$ .

#### **Ответы к задачам:**

1.  $8^{12} \equiv 1 \pmod{105}$ ,  $8^{104} \equiv (8^{12})^{26} \equiv 1 \pmod{105}$ , псевдопростое;  
 $104 = 2^3 \cdot 13$ ,  $8^{13} \equiv 8 \pmod{105}$ ,  $(8^{13})^2 \equiv 64 \pmod{105}$ ,  $(8^{13})^{2^2} \equiv 1 \pmod{105}$ , не сильно псевдопростое;
2. 7 умножений;
3.  $x < 0$ .

#### 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 не существенные 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 10-12 соответствует оценке «отлично», 8-9 баллов – оценке «хорошо», 6-7 баллов – оценке «удовлетворительно», менее 7 баллов – оценке «неудовлетворительно» (умения и навыки на данном этапе освоения дисциплины не сформированы).

### Контрольная работа № 5

(проверка сформированности ОПК-3, индикатор И-ОПК-3.3)  
 (проверка сформированности ОПК-10, индикатор И-ОПК-10.1)  
 проверка сформированности ОПК-2.1, индикатор И-ОПК-2.1.2)

1. С помощью расширенного алгоритма Евклида найти НОД и «коэффициенты Безу» в кольце
2. С помощью алгоритма, основанного на китайской теореме об остатках, решить задачу интерполяции в кольце
3. Является ли многочлен приводимым? Если да, то разложить на неприводимые сомножители в кольце  $\mathbb{Z}_5[x]$ :
4. Разложить многочлен на свободные от квадратов множители:  

$$x^7 + 4x^6 + 3x^5 - 5x^4 - 8x^3 - 3x^2 + 4x + 4.$$

#### Ответы к задачам:

1.  $\text{НОД}(f_1, f_2) = x^2 + x + 1 = (x + 1)f_1 + x^2f_2$ ;
2.  $x^4 - x^3 + x^2 + 3x + 2$ ;
3.  $(x - 1)(x - 2)^2(x^2 + 2)$ ;
4.  $(x + 1)(x^2 + x + 1)((x - 1)(x + 2))^2 = (x^3 + 2x^2 + 2x + 1)(x^2 + x - 2)^2$ .

#### 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 15-16 соответствует оценке «отлично», 13-14 баллов – оценке «хорошо», 8-12 баллов – оценке «удовлетворительно», менее 8 баллов – оценке

«неудовлетворительно» (умения и навыки на данном этапе освоения дисциплины не сформированы).

### Контрольная работа № 6

(проверка сформированности ОПК-3, индикатор И-ОПК-3.2)

(проверка сформированности ОПК-10, индикатор И-ОПК-10.1)

1. Найти все неприводимые многочлены третьей степени из  $\mathbb{Z}_3[x]$  вида  $ax^3 + bx^2 + 1$ .
2. Найти минимальный многочлен элемента  $\beta = \alpha + 1$ , в  $\mathbb{Z}_2[x]$ , если  $\alpha$  -- корень неприводимого многочлена  $m(x) = x^5 + x^4 + x^2 + x + 1 \in \mathbb{Z}_2[x]$ .
3. 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.  $x^3 + 2x^2 + 1$ ,  $2x^3 + 2x^2 + 1$ ; 2.  $x^5 + x^2 + 1$ ;
- 3.

Степенное представление	Представление в виде многочлена	Векторное представление
0	0	(0,0,0,0,0)
1	1	(1,0,0,0,0)
$\alpha$	$\alpha$	(0,1,0,0,0)
$\alpha^2$	$\alpha^2$	(0,0,1,0,0)
$\alpha^3$	$\alpha^3$	(0,0,0,1,0)
$\alpha^4$	$\alpha^4$	(0,0,0,0,1)
$\alpha^5$	$\alpha^4 + \alpha^3 + \alpha + 1$	(1,1,0,1,1)
$\alpha^6$	$\alpha^3 + \alpha^2 + 1$	(1,0,1,1,0)
$\alpha^7$	$\alpha^4 + \alpha^3 + \alpha$	(0,1,0,1,1)
$\alpha^8$	$\alpha^3 + \alpha^2 + \alpha + 1$	(1,1,1,1,0)
$\alpha^9$	$\alpha^4 + \alpha^3 + \alpha^2 + \alpha$	(0,1,1,1,1)
$\alpha^{10}$	$\alpha^2 + \alpha + 1$	(1,1,1,0,0)
$\alpha^{11}$	$\alpha^3 + \alpha^2 + \alpha$	(0,1,1,1,0)
$\alpha^{12}$	$\alpha^4 + \alpha^3 + \alpha^2$	(0,0,1,1,1)
$\alpha^{13}$	$\alpha + 1$	(1,1,0,0,0)
$\alpha^{14}$	$\alpha^2 + \alpha$	(0,1,1,0,0)
$\alpha^{15}$	$\alpha^3 + \alpha^2$	(0,0,1,1,0)
$\alpha^{16}$	$\alpha^4 + \alpha^3$	(0,0,0,1,1)
$\alpha^{17}$	$\alpha^3 + \alpha + 1$	(1,1,0,1,0)
$\alpha^{18}$	$\alpha^4 + \alpha^2 + \alpha$	(0,1,1,0,1)
$\alpha^{19}$	$\alpha^4 + \alpha^2 + \alpha + 1$	(1,1,1,0,1)
$\alpha^{20}$	$\alpha^4 + \alpha^2 + 1$	(1,0,1,0,1)
$\alpha^{21}$	$\alpha^4 + 1$	(1,0,0,0,1)
$\alpha^{22}$	$\alpha^4 + \alpha^3 + 1$	(1,0,0,1,1)
$\alpha^{23}$	$\alpha^3 + 1$	(1,0,0,1,0)
$\alpha^{24}$	$\alpha^4 + \alpha$	(0,1,0,0,1)
$\alpha^{25}$	$\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1$	(1,1,1,1,1)
$\alpha^{26}$	$\alpha^2 + 1$	(1,0,1,0,0)
$\alpha^{27}$	$\alpha^3 + \alpha$	(0,1,0,1,0)
$\alpha^{28}$	$\alpha^4 + \alpha^2$	(0,0,1,0,1)
$\alpha^{29}$	$\alpha^4 + \alpha + 1$	(1,1,0,0,1)
$\alpha^{30}$	$\alpha^4 + \alpha^3 + \alpha^2 + 1$	(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 не существенные 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 10-12 соответствует оценке «отлично», 8-9 баллов – оценке «хорошо», 6-7 баллов – оценке «удовлетворительно», менее 7 баллов – оценке «неудовлетворительно» (умения и навыки на данном этапе освоения дисциплины не сформированы).

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

В тесте 13 вопросов, за правильный ответ на каждый вопрос дается 1 балл. На прохождение теста дается время 30 минут.

Количество набранных баллов от 11 до 13 соответствует оценке «отлично».

Количество набранных баллов от 9 до 10 соответствует оценке «хорошо».

Количество набранных баллов от 7 до 8 соответствует оценке «удовлетворительно».

Количество баллов меньше 7 соответствует оценке «неудовлетворительно».

### Примерные вопросы теста:

1. НОД( $a, b$ )=5, а НОК( $a, b$ )=75. Чему равны числа  $a$  и  $b$ ?

Варианты ответов:

- 1) 35 и 25;
  - 2) 15 и 25;
  - 3) 10 и 25;
  - 4) 15 и 35.
2. Не проводя вычислений оценить сверху модули коэффициентов Безу для представления НОД(143,91).  
Выбрать верный ответ:
- 1)  $|u| \leq 7$ .  $|v| \leq 11$ ;
  - 2)  $|u| \leq 4$ .  $|v| \leq 5$ ;
  - 3)  $|u| \leq 11$ .  $|v| \leq 7$ ;
  - 4)  $|u| \leq 7/2$ .  $|v| \leq 11/2$ ;
  - 5)  $|u| \leq 11/2$ .  $|v| \leq 7/2$ .
3. Разрешимо ли диофантово уравнение  $5x - 15y = 11$ ?  
Выбрать верный ответ:
- 1) да;    2) нет.
4. Какое вещественное число представляется бесконечной непрерывной дробью?  
(выбрать верный ответ):
- 1) рациональное;



- 2) иррациональное;  
3) квадратичная иррациональность.
5. Является ли число  $13 + 11i$  неразложимым в  $\mathbb{Z}[i]$ ? (выбрать верный ответ):  
1) да; 2) нет.
6. Является ли группа  $\mathbb{Z}_{242}^*$  циклической? (выбрать верный ответ):  
1) да; 2) нет.
7. Чему равно значение функции Мёбиуса от числа 325?  
Выбрать верный ответ:  
1) 240;  
2) -1;  
3) 1;  
4) 0.
8. Можно ли найти  $a^{25}$ , выполнив 6 умножений? (выбрать верный ответ):  
1) да; 2) нет.
9. Сколько чисел не взаимно простых с 20 содержится в интервале от 1 до 40?  
Выбрать верный ответ:  
1) 24;  
2) 12;  
3) 32;  
4) 16.
10. Сколько решений имеет сравнение  $x^{\varphi(22)} \equiv 1 \pmod{22}$ ?  
Выбрать верный ответ:  
1) 10;  
2) 21;  
3) 11;  
4) 20.
11. Решением сравнения  $2^n \equiv 6 \pmod{13}$  является (выбрать правильный ответ):  
1)  $n \equiv 5 \pmod{12}$ ;  
2)  $n \equiv 5 \pmod{13}$ ;  
3)  $n \equiv 5 \pmod{6}$ .
12. Можно ли утверждать, что полной системой представителей классов вычетов, являющихся элементами группы  $\mathbb{Z}_9^*$ , является следующая система вычетов  $\{10, -7, 13, 5, -2, -1\}$ ? (выбрать верный ответ):  
1) да; 2) нет.
13. Генератор сравнений  $x_{n+1} \equiv x_n + 8 \pmod{15}$  имеет период, равный (выбрать верный ответ):  
1) 9;  
2) 6;  
3) 15;  
4) 5.

**Правильные ответы:**

Вопрос №	Вариант ответа	Вопрос №	Вариант ответа
1	2	8	1
2	4	9	1
3	2	10	1
4	2 и 3	11	1
5	2	12	1

6	1		13	3
7	4			

**Тест для самопроверки по результатам освоения дисциплины  
перед экзаменом  
(тест проводится в ЭУК «Алгебраическая алгоритмика (КБ-3)» 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:

- 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.
- 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)  $n \leq 3$ .
- Является ли факторкольцо  $\mathbb{Z}_2[x]/(x^5 + x^3 + 1)$  полем? Выбрать правильный ответ:  
1) да;      2) нет.
- 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.
- Является ли многочлен  $f(x) = x^4 + 19$  приводимым в  $\mathbb{Z}_{23}[x]$  ? Выбрать правильный ответ:  
1) да;      2) нет
- Сколько существует унитарных неприводимых многочленов 6-й степени в  $\mathbb{Z}_3[x]$  ?(выбрать верный ответ):  
1) 128;  
2) 116;  
3) 122;  
4) 121.
- Какие условия должны выполняться, чтобы элемент  $a$  являлся примитивным корнем в  $GF(64)$ ?  
Выбрать правильный ответ:  
1)  $\begin{cases} a^9 \not\equiv 1 \pmod{64} \\ a^7 \not\equiv 1 \pmod{64} \end{cases}$ ;

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

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

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

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

8. Чему равно оптимальное число вещественных умножений для вычисления  $4 \times 5$  – свертки над полем  $\mathbb{R}$ ?

Выбрать правильный ответ:

- 1) 10;
- 2) 9;
- 3) 8;
- 4) 15;
- 5) 20.

9. Чему равно оптимальное число комплексных умножений для вычисления 8-точечной циклической свертки над полем  $\mathbb{C}$ ?

Выбрать правильный ответ:

- 1) 6;
- 2) 10;
- 3) 11;
- 4) 12.

**Правильные ответы:**

Вопрос №	Вариант ответа		Вопрос №	Вариант ответа
<b>1</b>	2		<b>6</b>	2
<b>2</b>	2		<b>7</b>	2
<b>3</b>	1		<b>8</b>	3
<b>4</b>	2		<b>9</b>	2
<b>5</b>	1			

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

Промежуточная 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 -- 4, 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"**

Принцип полной упорядоченности. Наибольший общий делитель (НОД) целых чисел. Теорема о представлении НОД. Теорема о решении линейных диофантовых уравнений. Свойства НОД. Наименьшее общее кратное (НОК) целых чисел.

Алгоритм Евклида и теорема Ламе. Последовательность Фибоначчи. 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. Теорема о простых числах. Функция Эйлера и ее основные свойства. Решето Эратосфена

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. Кольцо целых гауссовых чисел  $\mathbb{Z}[i]$  проверка его евклидовости. Разложение на множители в евклидовом кольце. Теорема единственности разложения на множители. Факториальность кольца  $\mathbb{Z}[\frac{1}{2}]$  Теорема о простоте нормы неприводимого элемента из  $\mathbb{Z}[\frac{1}{2}]$  Теорема о точной сумме двух квадратов и следствие из нее. Необходимое и достаточное условие неприводимости целого числа в  $\mathbb{Z}[\frac{1}{2}]$  Неприводимость элемента из  $\mathbb{Z}[\frac{1}{2}]$

Функция Мёбиуса и ее свойство. Формула обращения Мёбиуса (аддитивная форма).

Малая теорема Ферма. Теорема Эйлера. Дихотомический алгоритм для возведения в степень. Аддитивная форма дихотомического алгоритма.

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

Мультипликативная группа кольца  $\mathbb{Z}/m\mathbb{Z}$ . 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. Циклическость группы  $\mathbb{Z}/p\mathbb{Z}$  при простом  $p$ . Лемма Гаусса. Теорема Гаусса (необходимое и достаточное условие циклическости группы  $\mathbb{Z}/m\mathbb{Z}$ ). Количество примитивных корней по модулю  $m$ .

Теорема о решениях линейного сравнения с одним неизвестным и следствие из нее. Китайская теорема об остатках для абелевой группы  $\mathbb{Z}/m\mathbb{Z}$  Следствие из нее. Обобщение на случай  $\mathbb{Z}/m_1\mathbb{Z} \times \dots \times \mathbb{Z}/m_k\mathbb{Z}$  Китайские теоремы об остатках для систем сравнений.

Многомодульная арифметика. Представление со смешанными основаниями.

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.

Линейные рекуррентные последовательности максимального периода. Периодические и почти периодические последовательности. Одношаговые генераторы. Теорема о длине периода и индексе вхождения в период. Декартово произведение генераторов. Теорема о периоде и индексе вхождения в период для декартова произведения генераторов. Формулировки лемм о степени линейного генератора, о

функции  $\square$  в случаях, когда  $\square$  -- простое нечетное и  $\square$  Лемма о генераторе максимального периода. Необходимые и достаточные условия того, что линейный генератор имеет максимальный период.

### Вопросы для самопроверки при подготовке к зачету на примере тем 2 - 5.

**Вопрос 1.** Каковы условия разрешимости линейного диофантова уравнения с двумя неизвестными?

Варианты ответов:

- 1). Диофантово уравнение разрешимо всегда.
- 2). Диофантово уравнение разрешимо тогда и только тогда, когда НОД коэффициентов при неизвестных делит свободный член.
- 3). Диофантово уравнение разрешимо, если все его коэффициенты делятся на одно и то же число.

**Вопрос 2.** 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

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

где  $M$  -- максимальное из двух чисел.

**Вопрос 3.** 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 4.** Какой непрерывной дробью представляется рациональное число?

Варианты ответов:

- 1). Бесконечной периодической.
- 2). Конечной.
- 3). Бесконечной непериодической.

**Вопрос 5.** 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 6.** 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 7.** Является ли евклидовым кольцо целых гауссовых чисел? Как проверить евклидовость кольца?

- 1). Не является, так как в нем нельзя ввести норму.
- 2). Является. Это целостное кольцо, в котором введена евклидова "норма", т. е. каждому ненулевому элементу кольца  $z$  поставлено в соответствие целое неотрицательное число  $g(z)$ , удовлетворяющее следующим свойствам:

а) для  $z \neq 0$  и  $u \neq 0$  справедливо  $g(zu) \geq g(z)$ ;

б). для любых двух элементов  $a, b$  кольца, где  $b \neq 0$ , существует представление  $a = bq + r$ , в котором  $r = 0$  или  $g(r) < g(b)$ .

Норма вводится следующим образом:  $g(a + bi) = a^2 + b^2$ .

- 3). Является. Это целостное кольцо, в котором введена евклидова "норма", т. е. каждому ненулевому элементу кольца  $z$  поставлено в соответствие целое неотрицательное число  $g(z)$ , удовлетворяющее следующим свойствам:

а) для  $z \neq 0$  и  $u \neq 0$  справедливо  $g(zu) \geq g(z)$ ;

б). для любых двух элементов  $a, b$  кольца, где  $b \neq 0$ , существует представление  $a = bq + r$ , в котором  $r = 0$  или  $g(r) < g(b)$ .

Норма вводится следующим образом:  $g(a + bi) = a^2 - b^2$ .

**Вопрос 8.** 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 9.** 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 их представителей, т.е.

$$Z_n = \{[0], [1], \dots, [n-1]\}$$

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

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 10.** 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 11.** Имеет ли решения сравнение

$$15x \equiv 7 \pmod{25}?$$

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 12.** Сколько решений имеет сравнение

$$24x \equiv 16 \pmod{40}?$$

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
1	2		5	3		9	1
2	1,3		6	3		10	3
3	3		7	2		11	3
4	2		8	2		12	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".

### Список вопросов и (или) заданий для проведения итоговой аттестации

Итоговая аттестация по дисциплине проводится в форме экзамена. Экзамен состоит из письменной и устной частей. Письменная часть проводится в виде контрольной работы по задачам, решавшимся во втором семестре (темы 11 -18). Задачи аналогичны приведенным в контрольных работах 5 - 6. Возможно добавление задач по теме "Быстрые алгоритмы цифровой обработки сигналов". Устная часть проводится в виде собеседования. Студент отвечает на вопросы билета и вопросы преподавателя, возникающие в процессе изложения теоретического материала.

### Примерные задания по теме "Быстрые алгоритмы цифровой обработки сигналов"

1. Используя алгоритм Винограда, построить оптимальный по умножению алгоритм вычисления произведения двух многочленов по модулю многочлена

$$(x - 2)(x^2 + 1)$$

над полем  $\mathbb{R}$ . Найти число умножений и сложений.

2. Используя алгоритм Рейдера, свести 9-точечное преобразование Фурье к свертке.

## Вопросы к экзамену по курсу "алгебраическая алгоритмика"

### Кольцо целых чисел

Принцип полной упорядоченности. Наибольший общий делитель (НОД) целых чисел. Теорема о представлении НОД. Теорема о решении линейных диофантовых уравнений. Свойства НОД. Наименьшее общее кратное (НОК) целых чисел.

Алгоритм Евклида и теорема Ламе. Последовательность Фибоначчи. 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. Теорема о простых числах. Функция Эйлера и ее основные свойства. Решето Эратосфена

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. Кольцо целых гауссовых чисел  $\mathbb{Z}[i]$  проверка его евклидовости. Разложение на множители в евклидовом кольце. Теорема единственности разложения на множители. Факториальность кольца  $\mathbb{Z}[\sqrt{d}]$  Теорема о простоте нормы неприводимого элемента из  $\mathbb{Z}[\sqrt{d}]$  Теорема о точной сумме двух квадратов и следствие из нее. Необходимое и достаточное условие неприводимости целого числа в  $\mathbb{Z}[\sqrt{d}]$  Неприводимость элемента из  $\mathbb{Z}[\sqrt{d}]$

Функция Мёбиуса и ее свойство. Формула обращения Мёбиуса (аддитивная форма).

Малая теорема Ферма. Теорема Эйлера. Дихотомический алгоритм для возведения в степень. Аддитивная форма дихотомического алгоритма.

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

Мультипликативная группа кольца  $\mathbb{Z}/m\mathbb{Z}$ . 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. Циклическость группы  $\mathbb{Z}/m\mathbb{Z}$  при простом  $p$ . Лемма Гаусса. Теорема Гаусса (необходимое и достаточное условие циклическости группы  $\mathbb{Z}/m\mathbb{Z}$ ). Количество примитивных корней по модулю  $m$ .

Теорема о решениях линейного сравнения с одним неизвестным и следствие из нее. Китайская теорема об остатках для абелевой группы  $\mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z}$  Следствие из нее. Обобщение на случай  $\mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \mathbb{Z}/m_3\mathbb{Z}$  Китайские теоремы об остатках для систем сравнений.

Многомодульная арифметика. Представление со смешанными основаниями.

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.



Линейные рекуррентные последовательности максимального периода. Периодические и почти периодические последовательности. Одношаговые генераторы. Теорема о длине периода и индексе вхождения в период. Декартово произведение генераторов. Теорема о периоде и индексе вхождения в период для декартова произведения генераторов. Формулировки лемм о степени линейного генератора, о функции  $\phi$  в случаях, когда  $n$  -- простое нечетное и  $n$ . Лемма о генераторе максимального периода. Необходимые и достаточные условия того, что линейный генератор имеет максимальный период.

### **Кольцо многочленов**

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  $R[x]/(f(x))$  Поле  $R[x]/(f(x))$  Простые расширения поля  $F$

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  $\mathbb{Z}[x]$  Критерий Эйзенштейна неприводимости многочлена над  $\mathbb{Z}$  (в факториальном кольце).

Разложение многочлена на свободные от квадратов множители в кольце характеристики 0.

Неприводимые многочлены с коэффициентами из  $\mathbb{F}_p$ . Теоремы. Число неприводимых многочленов степени  $n$  в  $\mathbb{F}_p[x]$  Критерий неприводимости многочлена над  $\mathbb{F}_p$ . «Решето Эратосфена» для многочленов над  $\mathbb{F}_p$ .

### **Поля Гауа**

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  $\mathbb{F}_p[x]/(f(x))$  Простое расширение поля  $F$ . 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  $\mathbb{F}_{p^n}$  Теорема о корнях. Существование конечного поля из  $p^n$  элементов ( $p$  – простое). Неприводимые многочлены в конечном поле. Теорема существования неприводимого многочлена степени  $n$  в конечном поле. Теорема о произведении всех неприводимых многочленов из  $\mathbb{F}_p[x]$  степени которых делят  $n$ . Разложение многочлена на неприводимые в конечном поле. Построение полей Гауа  $\mathbb{F}_{p^n}$

### **Быстрые алгоритмы цифровой обработки сигналов**

Понятие быстрого алгоритма. Матричная запись алгоритма. Матрицы предсложений и постсложений. Цифровой фильтр. Задача фильтрации, Фильтр с

конечным импульсным откликом (КИО-фильтры). Определение линейной свертки. Запись через многочлены.

Циклическая свертка и ее связь с линейной. Запись через многочлены.

Алгоритм Кука – Тоома вычисления линейной свертки. Иллюстрация на примере  $2 \times 2$  – свертки. Матричная форма записи алгоритма. Модификация алгоритма.

Алгоритмы Винограда вычисления коротких сверток. Иллюстрация на примере  $3 \times 2$  – свертки. Матричная запись алгоритма. Построение алгоритмов коротких линейных сверток:  $3 \times 3$  – свертка.

Модификация алгоритма Винограда, соответствующая выбору многочлена меньшей степени.

Построение алгоритмов коротких циклических сверток. Два способа решения. Иллюстрация на примере 4 – точечной циклической свертки. Матричная запись.

Сложность алгоритмов свертки. Оценка снизу количества умножений для вычисления линейной свертки. Теорема об оценке снизу числа умножений при вычислении произведения двух многочленов по модулю неприводимого многочлена  $\square$  степени  $\square$ . Обобщение на случай, когда  $\square$  раскладывается в произведение  $\square$  различных неприводимых многочленов (формулировка).

Определение дискретного преобразования Фурье (ДПФ). Теорема о свертке.

Вычисление циклической свертки с использованием теоремы о свертке и дискретного преобразования Фурье. Вещественное преобразование Фурье. Одновременное вычисление двух вещественных сверток.

Алгоритм Кули – Тьюки быстрого преобразования Фурье. Оценка сложности алгоритма.

Алгоритмы Кули – Тьюки по малому основанию: БПФ – алгоритм Кули – Тьюки по основанию два с прореживанием по времени, БПФ – алгоритм Кули – Тьюки по основанию два с прореживанием по частоте. Иллюстрация на примере 8 – точечного преобразования. Оценка сложности этих алгоритмов.

БПФ – алгоритмы Кули – Тьюки по основанию четыре с прореживанием по времени и по частоте. Матричная запись и оценка сложности.

Алгоритм Гуда – Томаса быстрого преобразования Фурье. Сложность алгоритма.

Вычисление преобразования Фурье с помощью свертки. Алгоритм Рейдера для простых чисел. Иллюстрация алгоритма Рейдера в поле  $\square$ . Построение 5 – точечного преобразования Фурье с помощью алгоритма Рейдера.

Алгоритм Рейдера в случае, когда длина преобразования равна степени нечетного простого числа. Случай, когда длина преобразования равна степени двойки. Иллюстрация на примере 16 – точечного преобразования Фурье.

Алгоритм Винограда для быстрого преобразования Фурье малой длины. Случай, когда длина преобразования равна:

- а) простому числу;
- б) степени простого числа;
- в) степени двойки.

### 3. Правила выставления оценки на экзамене.

Экзамен состоит из письменной и устной частей. Письменная часть проводится в виде контрольной работы по задачам, решавшимся в течение семестра. Задачи аналогичны приведенным в контрольных работах 1 - 5. Устная часть проводится в виде ответа на вопросы экзаменационного билета. В экзаменационный билет включается два теоретических вопроса. На подготовку к ответу дается не менее 1 часа.

Студент отвечает на вопросы билета и вопросы преподавателя, возникающие в процессе изложения теоретического материала.

По итогам экзамена выставляется одна из оценок: «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

**Оценка «Отлично»** выставляется студенту, который демонстрирует глубокое и полное владение содержанием материала и понятийным аппаратом курса «Геометрия»; решает не менее 3 задач из практической части экзамена; осуществляет межпредметные связи; умеет связывать теорию с практикой. Студент дает развернутые, полные и четкие ответы на вопросы экзаменационного билета и дополнительные вопросы, соблюдает логическую последовательность при изложении материала. Грамотно использует терминологию геометрии.

**Оценка «Хорошо»** выставляется студенту, ответ которого на экзамене в целом соответствуют указанным выше критериям, но отличается меньшей обстоятельностью, глубиной, обоснованностью и полнотой. В ответе имеют место отдельные неточности (несущественные ошибки), которые исправляются самим студентом после дополнительных и (или) уточняющих вопросов экзаменатора.

**Оценка «Удовлетворительно»** выставляется студенту, который дает недостаточно полные и последовательные ответы на вопросы экзаменационного билета и дополнительные вопросы, но при этом демонстрирует умение выделить существенные и несущественные признаки и установить причинно-следственные связи; в практической части решает не более 2 задач. Ответы излагаются в математических терминах, но при этом допускаются ошибки в определении и раскрытии некоторых основных понятий, формулировке положений, которые студент затрудняется исправить самостоятельно. При аргументации ответа студент не обосновывает свои суждения. На часть дополнительных вопросов студент затрудняется дать ответ или дает неверные ответы.

**Оценка «Неудовлетворительно»** выставляется студенту, который демонстрирует разрозненные, бессистемные знания; беспорядочно и неуверенно излагает материал; не умеет выделять главное и второстепенное, не умеет соединять теоретические положения с практикой, не устанавливает межпредметные связи; решает менее 2 задач в практической части; допускает грубые ошибки при определении сущности раскрываемых понятий, явлений, вследствие непонимания их существенных и несущественных признаков и связей; дает неполные ответы, логика и последовательность изложения которых имеют существенные и принципиальные нарушения, в ответах отсутствуют выводы. Дополнительные и уточняющие вопросы экзаменатора не приводят к коррекции ответов студента. На основную часть дополнительных вопросов студент затрудняется дать ответ или дает неверные ответы.

Оценка «Неудовлетворительно» выставляется также студенту, который взял экзаменационный билет, но отвечать отказался.

## 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  $\mathbb{Z}/(p)[x]$ ;
- теорема о произведении всех неприводимых многочленов из  $\mathbb{Z}/(p)[x]$ , степени которых делят  $n$ .