МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
"Казанский (Приволжский) федеральный университет"
Факультет математики и естественных наук

УТВЕРЖДАЮ
Проректор по образовательной деятельности КФУ
Проф. Д.А. Таюрский
ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ (ДО КФУ)
«___»_____20__г.

*подписано электронно-цифровой подписью*

# Программа дисциплины

Компьютерная алгебра Б1.Б.12

Направление подготовки: 02.03.01 - Математика и компьютерные науки
Профиль подготовки: Математическое и компьютерное моделирование
Квалификация выпускника: бакалавр
Форма обучения: очное
Язык обучения: русский

**Автор(ы):**

Гильмуллин М.Ф.

**Рецензент(ы):**

Костин А.В.

**СОГЛАСОВАНО:**

Заведующий(ая) кафедрой: Анисимова Т. И.
Протокол заседания кафедры No ___ от "____" _____ 201__г

Учебно-методическая комиссия Елабужского института КФУ (Факультет математики и естественных наук):
Протокол заседания УМК No ____ от "____" _____ 201__г

Регистрационный No 1016718318

Казань
2018

## Содержание

Программу дисциплины разработал(а)(и) доцент, к.н. (доцент) Гильмуллин М.Ф. Кафедра математики и прикладной информатики Факультет математики и естественных наук , MFGilmullin@kpfu.ru

## 1. Цели освоения дисциплины

Курс направлен на формирование представлений о понятиях, методах и системах компьютерной алгебры, алгоритмически разрешимых задачах алгебры и математики в целом, ознакомление с основными задачами компьютерной алгебры, с методами создания эффективных алгоритмов, с современными компьютерными системами с возможностями символьных преобразований, с алгебраическими методами теории кодирования.

При этом необходимо:

- изложить основные понятия анализа алгоритмов;

- формировать знания, умения, навыки работы с алгоритмами абстрактной алгебры, особенно теории чисел и теории многочленов, подчеркнув при этом особенности и специфику их применения в области информационных технологий;

- выработать у студентов умение проводить анализ и оценку сложности алгоритмов;

- развить у студентов навыки самостоятельной работы с литературой по математике и ее приложениям.

## 2. Место дисциплины в структуре основной образовательной программы высшего профессионального образования

Данная учебная дисциплина включена в раздел " Б1.Б.12 Дисциплины (модули)" основной образовательной программы 02.03.01 Математика и компьютерные науки и относится к базовой (общепрофессиональной) части. Осваивается на 2 курсе, 4 семестр.

Дисциплина 'Компьютерная алгебра' включена в блок 1.

Для ее успешного освоения необходимы знания и умения, приобретенные в результате освоения предшествующих дисциплин: алгебры, математического анализа, теории вероятностей, численных методов, языков и методов программирования, дискретной математики, информатики, компьютерного моделирования.

Освоение дисциплины 'Компьютерная алгебра' необходимо при изучении всех дисциплин последнего года обучения по программам бакалавриата: математического моделирования, базы данных, методов оптимизации и др.

## 3. Компетенции обучающегося, формируемые в результате освоения дисциплины /модуля

В результате освоения дисциплины формируются следующие компетенции:

| Шифр компетенции | Расшифровка приобретаемой компетенции |
|---|---|
| ОПК-1 (профессиональные компетенции) | готовностью использовать фундаментальные знания в области математического анализа, комплексного и функционального анализа, алгебры, аналитической геометрии, дифференциальной геометрии и топологии, дифференциальных уравнений, дискретной математики и математической логики, теории вероятностей, математической статистики и случайных процессов, численных методов, теоретической механики в будущей профессиональной деятельности |
| ПК-1 (профессиональные компетенции) | способностью к определению общих форм и закономерностей отдельной предметной области |

| Шифр компетенции | Расшифровка приобретаемой компетенции |
|---|---|
| ПК-5 (профессиональные компетенции) | способностью использовать методы математического и алгоритмического моделирования при решении теоретических и прикладных задач |
| ПК-9 (профессиональные компетенции) | способностью к организации учебной деятельности в конкретной предметной области (математика, физика, информатика) |

В результате освоения дисциплины студент:

1. должен знать:

определения основных понятий компьютерной алгебры;
основные алгоритмы теории чисел и полиномов;
современные методы и наиболее распространенные системы компьютерной алгебры

2. должен уметь:

проводить анализ алгоритмов, оценить их сложность и эффективность;
доказывать свойства основных алгоритмов теории целых чисел и полиномов;
пользоваться возможностями основных систем компьютерной алгебры.

3. должен владеть:

методами анализа алгоритмов; теории чисел, теории полиномов.

4. должен демонстрировать способность и готовность:

применять результаты освоения дисциплины в профессиональной деятельности.

## 4. Структура и содержание дисциплины/ модуля

Общая трудоемкость дисциплины составляет 2 зачетных(ые) единиц(ы) 72 часа(ов).

Форма промежуточного контроля дисциплины зачет в 4 семестре.

Суммарно по дисциплине можно получить 100 баллов, из них текущая работа оценивается в 50 баллов, итоговая форма контроля - в 50 баллов. Минимальное количество для допуска к зачету 28 баллов.

86 баллов и более - "отлично" (отл.);

71-85 баллов - "хорошо" (хор.);

55-70 баллов - "удовлетворительно" (удов.);

54 балла и менее - "неудовлетворительно" (неуд.).

### 4.1 Структура и содержание аудиторной работы по дисциплине/ модулю

**Тематический план дисциплины/модуля**

| N | Раздел Дисциплины/ Модуля | Семестр | Неделя семестра | Виды и часы аудиторной работы, их трудоемкость (в часах) | | | Текущие формы контроля |
|---|---|---|---|---|---|---|---|
| | | | | Лекции | Практические занятия | Лабораторные работы | |
| 1. | Тема 1. Введение в компьютерную алгебру. | 4 | | 4 | 4 | 0 | Устный опрос |

| N | Раздел Дисциплины/ Модуля | Семестр | Неделя семестра | Виды и часы аудиторной работы, их трудоемкость (в часах) | | | Текущие формы контроля |
|---|---|---|---|---|---|---|---|
| | | | | Лекции | Практические занятия | Лабораторные работы | |
| 2. | Тема 2. Алгоритмы теории чисел. | 4 | | 6 | 6 | 0 | Отчет |
| 3. | Тема 3. Алгоритмы теории полиномов. | 4 | | 4 | 4 | 0 | Устный опрос |
| 4. | Тема 4. Теория кодирования и криптография. | 4 | | 4 | 4 | 0 | Устный опрос |
| . | Тема . Итоговая форма контроля | 4 | | 0 | 0 | 0 | Зачет |
| | Итого | | | 18 | 18 | 0 | |

**4.2 Содержание дисциплины**

**Тема 1. Введение в компьютерную алгебру.**

***лекционное занятие (4 часа(ов)):***

Введение в компьютерную алгебру. Предмет, задачи и методы компьютерной алгебры. Представление символьных данных в компьютере. Символьные преобразования, оценка их сложности и эффективности. Размерность задачи, временная сложность алгоритма, функция сложности, асимптотическая сложность алгоритма, порядок роста, классы роста, детерминированные и вероятностные алгоритмы. Полиномиальные и экспоненциальные по времени алгоритмы. Правило суммы и произведения. Правила асимптотического анализа алгоритмов. Методы разработки эффективных алгоритмов. Системы компьютерной алгебры.

***практическое занятие (4 часа(ов)):***

Анализ алгоритмов. Основные понятия анализа алгоритмов. Подсчёт временной и асимптотической сложности алгоритмов.

**Тема 2. Алгоритмы теории чисел.**

***лекционное занятие (6 часа(ов)):***

Алгоритмически разрешимые задачи теории целых чисел. Дроби. Наибольший общий делитель. Алгоритмы вычисления НОД и оценка их сложности. Анализ алгоритма Евклида. Теорема Ламе. Расширенный алгоритм Евклида. Вычисление коэффициентов Безу. Алгоритмы отделения простых чисел. Критерии простоты целого числа. Алгоритмы разложения целых чисел на множители. Позиционная нумерация. Модулярная арифметика. Взаимно обратные по модулю числа и их вычисление. Китайская теорема об остатках. Операции над большими числами.

***практическое занятие (6 часа(ов)):***

Наибольший общий делитель. Различные алгоритмы вычисления НОД целых чисел, оценка их сложности. Теорема Ламе. Расширенный алгоритм Евклида и рекуррентные формулы вычисления коэффициентов Безу. Алгоритмы отделения простых и составных чисел. Различные критерии простоты целого числа. Вычисление минимального простого делителя целого числа. Метод Ферма определения наибольшего множителя. Применение малой теоремы Ферма для отделения составных чисел. Числа Кармайкла. Взаимно обратные по модулю числа и их вычисление. Китайская теорема об остатках. Модулярная арифметика.

**Тема 3. Алгоритмы теории полиномов.**

***лекционное занятие (4 часа(ов)):***

Алгоритмы символьных преобразований в алгебре полиномов. Представление полиномов. Вычисление полиномов. Схема Горнера. Операции над полиномами. Полиномиальное деление с остатком. Нахождение НОД полиномов. Разложение на неприводимые множители.

***практическое занятие (4 часа(ов)):***

Операции над полиномами. Схема Горнера. Обобщение схемы Горнера. Вычисление НОД многочленов. Модулярный алгоритм. Модулярные операции над полиномами.

**Тема 4. Теория кодирования и криптография.**

***лекционное занятие (4 часа(ов)):***

Основные понятия и задачи теории кодирования. Алгебраические методы в теории кодирования и защиты информации. Алфавитное кодирование. Криптография. Системы с закрытым и открытым ключом. Коды, исправляющие ошибки.

***практическое занятие (4 часа(ов)):***

Алгебраические методы в теории кодирования и защиты информации. Алфавитное кодирование. Криптография. Системы с закрытым и открытым ключом. Коды, исправляющие ошибки.

### 4.3 Структура и содержание самостоятельной работы дисциплины (модуля)

| N | Раздел Дисциплины | Семестр | Неделя семестра | Виды самостоятельной работы студентов | Трудоемкость (в часах) | Формы контроля самостоятельной работы |
|---|---|---|---|---|---|---|
| 1. | Тема 1. Введение в компьютерную алгебру. | 4 | | подготовка к устному опросу | 8 | Устный опрос |
| 2. | Тема 2. Алгоритмы теории чисел. | 4 | | Выполнение индивидуального задания для самостоятельной оценки алгоритмов. | 12 | Отчет |
| 3. | Тема 3. Алгоритмы теории полиномов. | 4 | | подготовка к устному опросу | 8 | Устный опрос |
| 4. | Тема 4. Теория кодирования и криптография. | 4 | | подготовка к устному опросу | 8 | Устный опрос |
| | Итого | | | | 36 | |

## 5. Образовательные технологии, включая интерактивные формы обучения

В преподавании дисциплины используются следующие образовательные технологии:

Информационные технологии - обучение в электронной образовательной среде с целью расширения доступа к образовательным ресурсам (теоретически к неограниченному объему и скорости доступа), увеличения контактного взаимодействия с преподавателем, построения индивидуальных траекторий подготовки и объективного контроля и мониторинга знаний студентов.

Проблемное обучение - стимулирование студентов к самостоятельному приобретению знаний, необходимых для решения конкретной проблемы.

Контекстное обучение - мотивация студентов к усвоению знаний путем выявления связей между конкретным знанием и его применением.

Междисциплинарное обучение - использование знаний из разных областей, их группировка и концентрация в контексте решаемой задачи.

Опережающая самостоятельная работа - изучение студентами нового материала до его изучения в ходе аудиторных занятий.

## 6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов

**Тема 1. Введение в компьютерную алгебру.**

Устный опрос , примерные вопросы:

Анализ алгоритмов. Основные понятия анализа алгоритмов. Подсчёт временной и асимптотической сложности алгоритмов.

**Тема 2. Алгоритмы теории чисел.**

Отчет , примерные вопросы:

Каждый студент выполняет полную обработку одного из следующих алгоритмов (описание алгоритма, вычисление асимптотической сложности, контрольные примеры, блок-схема, программа на выбранном языке). 1. Алгоритм Евклида. 2. Расширенный алгоритм Евклида. 3. Минимальный множитель. 4. Метод Ферма. 5. Вероятностный алгоритм. 6. Бинарный метод. 7. Метод множителей. 8. Схема Горнера. 9. Обобщенная схема Горнера. 10. Вычисление обратного по модулю числа. 11. Китайская теорема об остатках для трёх чисел. 12. Сортировка массива. 13. Перевод в двоичную систему счисления. 14. Экономное умножение. 15. Нерекурсивный алгоритм.

**Тема 3. Алгоритмы теории полиномов.**

Устный опрос , примерные вопросы:

Операции над полиномами. Схема Горнера. Обобщение схемы Горнера. Вычисление НОД многочленов. Модулярный алгоритм. Модулярные операции над полиномами.

**Тема 4. Теория кодирования и криптография.**

Устный опрос , примерные вопросы:

Алгебраические методы в теории кодирования и защиты информации. Алфавитное кодирование. Криптография. Системы с закрытым и открытым ключом. Коды, исправляющие ошибки.

**Итоговая форма контроля**

зачет

Примерные вопросы к зачету:

Вопросы к зачету

1. Предмет и задачи компьютерной алгебры.
2. Сложность и эффективность алгоритмов.
3. Правила анализа алгоритмов.
4. Методы разработки эффективных алгоритмов.
5. Представление данных в компьютере.
6. Алгоритмы вычисления НОД целых чисел.
7. Алгоритм Евклида, анализ времени его работы.
8. Теорема Ламе.
9. Расширенный алгоритм Евклида.
10. Алгоритмы нахождения простых чисел.
11. Алгоритмы разложения целых чисел на множители.
12. Взаимно обратные по модулю числа и их вычисление.
13. Китайская теорема об остатках.
14. Вычисление полиномов.
15. Схема Горнера.
16. Полиномиальное деление с остатком.
17. Нахождение НОД полиномов.

18. Разложение полинома на неприводимые множители.
19. Основные понятия и задачи теории кодирования.
20. Основные задачи криптографии.

### 7.1. Основная литература:

1. Абрамов, С.А. Элементы компьютерной алгебры линейных обыкновенных дифференциальных, разностных и q-разностных операторов [Электронный ресурс] : учебное пособие / С.А. Абрамов. - Электрон. дан. - Москва : МЦНМО, 2012. - 127 с. - URL:https://e.lanbook.com/reader/book/56384/#1

2. Шевцов, Г.С. Численные методы линейной алгебры [Электронный ресурс] : учебное пособие / Г.С. Шевцов, О.Г. Крюкова, Б.И. Мызникова. - Электрон. дан. - Санкт-Петербург : Лань, 2011. - 496 с. - URL:https://e.lanbook.com/reader/book/1800/#2

3. Теория алгоритмов: Учебное пособие / В.И. Игошин. - М.: ИНФРА-М, 2012. - 318 с. - URL:http://znanium.com/bookread2.php?book=241722

### 7.2. Дополнительная литература:

1. Штарьков, Ю.М. Универсальное кодирование. Теория и алгоритмы [Электронный ресурс] : учебное пособие / Ю.М. Штарьков. - Электрон. дан. - Москва : Физматлит, 2013. - 288 с. - URL:https://e.lanbook.com/reader/book/59667/#2

2. Василенко, О.Н. Теоретико-числовые алгоритмы в криптографии [Электронный ресурс] : монография / О.Н. Василенко. - Электрон. дан. - Москва : МЦНМО, 2006. - 336 с. - URL:https://e.lanbook.com/reader/book/9303/#1

3. Бабенко, Л.К. Параллельные алгоритмы для решения задач защиты информации [Электронный ресурс] : учебное пособие / Л.К. Бабенко, Е.А. Ищукова, И.Д. Сидоров. - Электрон. дан. - Москва : Горячая линия-Телеком, 2014. - 304 с. - URL:https://e.lanbook.com/reader/book/63228/#1

4. Численные методы и программирование: Учебное пособие / В.Д. Колдаев; Под ред. Л.Г. Гагариной. - М.: ИД ФОРУМ: НИЦ Инфра-М, 2013. - 336 с. - URL:http://znanium.com/bookread2.php?book=370603

5. Черняк, А.А. Математическое программирование. Алгоритмический подход [Электронный ресурс] : учеб. пос. / А.А. Черняк, Ж.А. Черняк, Ю.М. Метельский. - Минск: Выш. шк., 2006. - URL:http://znanium.com/bookread2.php?book=505174

6. Сагитов Р. В., Шершнев В.Г. Линейная алгебра. Часть II. Линейное программирование, динамическое программирование и теория игр: Учебно-методическое пособие. - М.: Издательство 'Менеджер', 2007. - 192 с. - URL:http://znanium.com/bookread2.php?book=347844

### 7.3. Интернет-ресурсы:

1. Бурланков Д.Е., Кузнецов М.И., Чирков А.Ю., Яковлев В.А. Компьютерная алгебра. Электронный учебник. - http://www.itlab.unn.ru/?dir=201
2. Малышев И.А. Компьютерная алгебра (курс лекций) - http://aivt.ftk.spbstu.ru/course/comp-algebra
3. Бесплатный ресурс для студентов - http://math24.ru/calculus-list.html
4. Образовательный математический сайт - http://www.exponenta.ru/
5. Учебные материалы - http://math.fizteh.ru/study/

### 8. Материально-техническое обеспечение дисциплины(модуля)

Освоение дисциплины "Компьютерная алгебра" предполагает использование следующего материально-технического обеспечения:

Мультимедийная аудитория, вместимостью более 60 человек. Мультимедийная аудитория состоит из интегрированных инженерных систем с единой системой управления, оснащенная современными средствами воспроизведения и визуализации любой видео и аудио информации, получения и передачи электронных документов. Типовая комплектация мультимедийной аудитории состоит из: мультимедийного проектора, автоматизированного проекционного экрана, акустической системы, а также интерактивной трибуны преподавателя, включающей тач-скрин монитор с диагональю не менее 22 дюймов, персональный компьютер (с техническими характеристиками не ниже Intel Core i3-2100, DDR3 4096Mb, 500Gb), конференц-микрофон, беспроводной микрофон, блок управления оборудованием, интерфейсы подключения: USB,audio, HDMI. Интерактивная трибуна преподавателя является ключевым элементом управления, объединяющим все устройства в единую систему, и служит полноценным рабочим местом преподавателя. Преподаватель имеет возможность легко управлять всей системой, не отходя от трибуны, что позволяет проводить лекции, практические занятия, презентации, вебинары, конференции и другие виды аудиторной нагрузки обучающихся в удобной и доступной для них форме с применением современных интерактивных средств обучения, в том числе с использованием в процессе обучения всех корпоративных ресурсов. Мультимедийная аудитория также оснащена широкополосным доступом в сеть интернет. Компьютерное оборудованием имеет соответствующее лицензионное программное обеспечение.

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе "ZNANIUM.COM", доступ к которой предоставлен студентам. ЭБС "ZNANIUM.COM" содержит произведения крупнейших российских учёных, руководителей государственных органов, преподавателей ведущих вузов страны, высококвалифицированных специалистов в различных сферах бизнеса. Фонд библиотеки сформирован с учетом всех изменений образовательных стандартов и включает учебники, учебные пособия, УМК, монографии, авторефераты, диссертации, энциклопедии, словари и справочники, законодательно-нормативные документы, специальные периодические издания и издания, выпускаемые издательствами вузов. В настоящее время ЭБС ZNANIUM.COM соответствует всем требованиям федеральных государственных образовательных стандартов высшего профессионального образования (ФГОС ВПО) нового поколения.

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе Издательства "Лань" , доступ к которой предоставлен студентам. ЭБС Издательства "Лань" включает в себя электронные версии книг издательства "Лань" и других ведущих издательств учебной литературы, а также электронные версии периодических изданий по естественным, техническим и гуманитарным наукам. ЭБС Издательства "Лань" обеспечивает доступ к научной, учебной литературе и научным периодическим изданиям по максимальному количеству профильных направлений с соблюдением всех авторских и смежных прав.

Освоение данной дисциплины предполагает использование следующего материально-технического обеспечения: проектор, экран и интерактивная трибуна.

Программа составлена в соответствии с требованиями ФГОС ВПО и учебным планом по направлению 02.03.01 "Математика и компьютерные науки" и профилю подготовки Математическое и компьютерное моделирование .

Автор(ы):
Гильмуллин М.Ф. _____
"__" _____ 201 __ г.

Рецензент(ы):
Костин А.В. _____
"__" _____ 201 __ г.