Белорусский государственный университет

**УТВЕРЖДАЮ**
Декан гуманитарного факультета

_____ В.Е. Гурский
(подпись)

26.06.2013 г.
(дата утверждения)

Регистрационный № УД-1500/р.

# Алгебра и теория чисел

**Учебная программа учреждения высшего образования по учебной дисциплине для специальности:**

**1-31 03 07-03 прикладная информатика**

Факультет Гуманитарный

Кафедра Информационных технологий

Курс (курсы) 1
Семестр (семестры) 1, 2
Лекции 68

Экзамен 2

Практические (семинарские) занятия 68

Зачет 1, 2

Лабораторные занятия

Курсовая работа (проект)

Аудиторных часов по учебной дисциплине 136

Всего часов по учебной дисциплине 252

Форма получения высшего образования очное

Составил(а) О.В. Дубровина

2013 г.

## ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Учебная программа «Алгебра и теория чисел» разработана для студентов 1 курса специальности 1-31 03 07-03 «Прикладная информатика» направления «Веб-программирование и компьютерный дизайн».

Базой для изучения данного курса является предмет «Математика», изучаемый в средней школе.

Дисциплина «Алгебра и теория чисел имеет профессиональную и общенаучную направленность. Целью настоящего курса является обучение студентов фундаментальным основам общей алгебры, линейной алгебры и теории чисел, знакомство с основными алгебраическими структурами. При преподавании данной дисциплины ставятся следующие задачи:

- дать введение в задачи и методы теории чисел;
- изучить комплексные числа;
- дать введение в задачи и методы теории групп, колец, полей;
- изучить многочлены и методы работы с ними;
- изучить теорию линейных пространств и линейных отображений;
- ознакомить студентов с теорией билинейных и квадратичных форм.
- развить у студентов аналитическое и абстрактное мышление.

«Алгебра и теория чисел» является базовым математическим курсом и непосредственно связана с основными дисциплинами аналитического цикла, такими как «Математический анализ» и «Аналитическая геометрия». Методы, излагаемые в курсе, используются при изучении дисциплин «Вычислительные методы», «Теория алгоритмов», «Исследование операций», «Криптографические методы защиты информации», а также при изучении ряда дисциплин специализаций. При изложении курса важно показать возможности использования аппарата алгебры при решении как теоретических, так и прикладных задач.

В результате освоения курса «Алгебра и теория чисел» студент должен:

***знать:***

– основы теории чисел и ее применение в информатике;

– основные определения и теоремы теории основных алгебраических структур: групп, колец, полей;

– основные понятия и теоремы теории многочленов;

– основы векторной алгебры;

***уметь:***

– находить решения сравнений и их систем;

– решать основные задачи теории векторных пространств;

– решать задачи, связанные с делимостью многочленов;

– применять аппарат алгебры при решении задач специальности;

***приобрести навыки:***

– навыками применения алгебраических методов при решении задач моделирования, компьютерной графики, защиты информации и других задач специальности.

Изучение курса «Алгебра и теория чисел» рассчитано на 252 часа, в том числе 136 часов аудиторных занятий.

# СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

## Раздел 1. *Теория чисел*

### Тема 1. *Делимость чисел.*

Множества целых и натуральных чисел. Делимость чисел. Простые числа и составные числа.

Метод математической индукции.

Наибольший общий делитель. Алгоритм Евклида нахождения наибольшего общего делителя. Бинарный алгоритм нахождения наибольшего общего делителя. Наименьшее общее кратное. Механизм непрерывных дробей.

Функции $[x]$ и $\{x\}$. Мультипликативные функции. Примеры. Функция Эйлера.

### Тема 2. *Сравнения*

Равноостаточные числа по модулю $m$. Полная и приведенная системы вычетов по модулю $m$.

Сравнения первой степени. Свойства сравнений первой степени. Решение сравнений первой степени. Приложение теории сравнений к решению линейных уравнений с двумя незвестными.

Системы сравнений первой степени. Решение систем сравнений по простому и составному модулям

Сравнения произвольной степени по простому и составному модулям. Методы решения.

Сравнения второй степени. Квадратичные вычеты и невычеты. Общие теоремы. Символы Лежандра и Якоби.

Первообразные корни и индексы. Приложение теории индексов к решению сравнений.

Приложения теории чисел.

## Раздел 2. *Отображения*

Бинарное отношение. Отношения эквивалентности и порядка, классы эквивалентности. Отображения. Инъективное, сюръективное и биективное отображения. Умножение отображений. Обратное отображение.

Подстановки и перестановки. Четность и нечетность перестановки. Разложение перестановок в суперпозицию.

## Раздел 3. *Алгебраические структуры*

Алгебраическая операция. Нейтральный элемент. Симметричный элемент. Свойства. Примеры.

Группа. Примеры групп. Подгруппа. Критерий подгруппы.

Кольцо. Примеры колец. Подкольцо. Критерий подкольца. Поле. Подполе.

**Раздел 4.** *Поле комплексных чисел*

Построение поля комплексных чисел, комплексная плоскость. Арифметические операции над комплексными числами. Геометрическая интерпретация поля комплексных чисел. Формулы Эйлера. Извлечение корней из комплексных чисел. Геометрическая интерпретация.

**Раздел 5.** *Многочлены*

Кольцо многочленов одной переменной над полями действительных и комплексных чисел. Деление с остатком в кольце многочленов. Наибольший общий делитель. Алгоритм Евклида.

Неприводимые многочлены. Корни многочлена. Схема Горнера. Разложение многочленов на неприводимые множители. Алгоритм нахождения целых и рациональных корней многочлена с целыми коэффициентами.

Интерполяционная формула Лагранжа.

Рациональные дроби.

**Раздел 6.** *Линейные пространства. Линейные отображения.*

Векторы. Линейная зависимость (независимость) системы векторов.

Линейное пространство. Определение, примеры. Базис и размерность линейного пространства. Координаты вектора в фиксированном базисе. Преобразования координат вектора при переходе от одного базиса к другому.

Линейное преобразование линейного пространства. Матрица линейного преобразования. Операции над линейными преобразованиями. Изменение матрицы линейного преобразования при замене базиса. Примеры линейных преобразований.

Собственные векторы и собственные значения линейного преобразования. Приведение матрицы линейного преобразования к диагональному виду.

**Раздел 7.** *Билинейные и квадратичные формы.*

Линейные преобразования переменных. Квадратичные формы. Метод Лагранжа приведения квадратичной формы к каноническому виду.

Критерии эквивалентности квадратичных форм над полем $R$ и надо полем $C$. Критерии знакоопределенности действительных квадратичных форм.

Билинейные формы. Определение, примеры, свойства.

## УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА УЧЕБНОЙ ДИСЦИПЛИНЫ
(ПРИМЕРНАЯ ФОРМА)

| Номер раздела, темы | Название раздела, темы | Количество аудиторных часов | | | | | | Форма контроля знаний |
|---|---|---|---|---|---|---|---|---|
| | | Лекции | Практические занятия | Семинарские занятия | Лабораторные занятия | Управляемая самостоятельная работа | Иное | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| | **1 семестр** | **34** | **34** | | | | | |
| **1.** | ***Теория чисел*** | ***18*** | ***18*** | | | | | сам. работа |
| 1.1 | Множества целых и натуральных чисел. Делимость чисел. Простые числа и составные числа. Метод математической индукции. | 2 | 2 | | | | | |
| 1.2 | Наибольший общий делитель. Алгоритм Евклида. Наименьшее общее кратное. Механизм непрерывных дробей. | 2 | 2 | | | | | индив. дом. задание |
| 1.3 | Полная и приведенная системы вычетов по модулю $m$. Функция Эйлера. | 2 | | | | | | устный опрос |
| 1.4 | Сравнения первой степени. Свойства сравнений первой степени. Решение сравнений первой степени. | 2 | 2 | | | | | индив. дом. задание |
| 1.5 | Системы сравнений первой степени. Решение систем сравнений. | 2 | 2 | | | | | сам. работа |
| 1.6 | Сравнения произвольной степени по простому модулю. Сравнения произвольной степени по составному модулю. Методы решения. | 2 | 2 | | | | | опрос |
| 1.7 | Сравнения второй степени. Квадратичные | 2 | 2 | | | | | устный опрос |

| Номер раздела, темы | Название раздела, темы | Количество аудиторных часов | | | | | | Форма контроля знаний |
|---|---|---|---|---|---|---|---|---|
| | | Лекции | Практические занятия | Семинарские занятия | Лабораторные занятия | Управляемая самостоятельная работа | Иное | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| | вычеты и невычеты. Общие теоремы. Символы Лежандра и Якоби | | | | | | | |
| 1.8 | Первообразные корни и индексы. Решение сравнений с использованием индексов. | 2 | 2 | | | | | устный опрос |
| 1.9 | Приложения теории чисел | 2 | 2 | | | | | индив. дом. задание |
| ***2.*** | ***Множества и отображения*** | ***4*** | ***4*** | | | | | |
| 2.1 | Бинарное отношение. Отношения эквивалентности и порядка, классы эквивалентности. Отображения. Свойства отображений. | 2 | 2 | | | | | письменный опрос |
| 2.2 | Подстановки и перестановки. Четность и нечетность перестановки. Разложение перестановок в суперпозицию. | 2 | 2 | | | | | индив. дом. задание |
| ***3*** | ***Алгебраические структуры*** | ***6*** | ***6*** | | | | | самост. работа |
| 3.1 | Алгебраическая операция. Нейтральный элемент. Симметричный элемент | 2 | 2 | | | | | индив. дом. задание |
| 3.2 | Группа. Примеры групп. Подгруппа. Критерий подгруппы | 2 | 2 | | | | | индив. дом. задание |
| 3.3 | Кольцо. Примеры колец. Подкольцо. Критерий подкольца. Поле. Подполе. | 2 | 2 | | | | | индив. дом. задание |
| ***4*** | ***Поле комплексных чисел*** | ***6*** | ***6*** | | | | | самост. работа |
| 4.1 | Построение поля комплексных чисел, комплексная плоскость. Арифметические | 2 | 2 | | | | | индив. дом. задание |

| Номер раздела, темы | Название раздела, темы | Количество аудиторных часов | | | | | | Форма контроля знаний |
|---|---|---|---|---|---|---|---|---|
| | | Лекции | Практические занятия | Семинарские занятия | Лабораторные занятия | Управляемая самостоятельная работа | Иное | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| | операции над комплексными числами | | | | | | | |
| 4.2 | Геометрическая интерпретация поля комплексных чисел. Формулы Эйлера. | 2 | 2 | | | | | индив. дом. задание |
| 4.3 | Извлечение корней из комплексных чисел. Геометрическая интерпретация. | 2 | 2 | | | | | индив. дом. задание |
| | **2 семестр** | **34** | **34** | | | | | |
| ***6.*** | ***Многочлены*** | ***14*** | ***14*** | | | | | |
| 6.1 | Кольцо многочленов одной переменной над полем действительных чисел. Деление с остатком в кольце многочленов. Наибольший общий делитель. Алгоритм Евклида. | 2 | 2 | | | | | устный опрос, индив. дом. задание |
| 6.2 | Корни многочлена. Нахождение целых и рациональных корней многочлена Неприводимые многочлены. Разложение многочленов на неприводимые многочлены. Схема Горнера. | 6 | 6 | | | | | индив. дом. задание |
| 6.3 | Рациональные дроби. Представление рациональной дроби в виде многочлена и суммы простейших дробей. | 4 | 4 | | | | | индив. дом. задание |
| 6.4 | Интерполяционные многочлены Ньютона и Лагранжа. | 2 | 2 | | | | | устный опрос |
| ***7.*** | ***Линейные пространства. Линейные отображения*** | ***14*** | ***14*** | | | | | |
| 7.1 | Векторы. Линейная зависимость векторов. | 2 | 2 | | | | | индив. дом. |

| Номер раздела, темы | Название раздела, темы | Количество аудиторных часов | | | | | | Форма контроля знаний |
|---|---|---|---|---|---|---|---|---|
| | | Лекции | Практические занятия | Семинарские занятия | Лабораторные занятия | Управляемая самостоятельная работа | Иное | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| | | | | | | | | задание |
| 7.2 | Линейное пространство. Определение, примеры. Базис и размерность линейного пространства. Координаты вектора в фиксированном базисе. | 2 | 2 | | | | | устный опрос |
| 7.3 | Формулы перехода от одного базиса к другому Преобразование координат. | 2 | 2 | | | | | устный опрос |
| 7.4 | Линейное преобразование линейного пространства и его матрица. Операции над линейными преобразованиями. Изменение матрицы линейного преобразования при замене базиса. Примеры линейных преобразований. Собственные векторы и собственные значения линейного преобразования. | 8 | 8 | | | | | письменный опрос, индив. дом. задание |
| ***8.*** | ***Билинейные и квадратичные формы*** | ***6*** | ***6*** | | | | | |
| 8.1 | Линейные преобразования переменных. Квадратичные формы. Метод Лагранжа приведения квадратичной формы к каноническому виду. | 2 | 2 | | | | | устный опрос |
| 8.2 | Критерии эквивалентности квадратичных форм над полем *R* и надо полем *C*. Критерии знакоопределенности действительных | 2 | 2 | | | | | устный опрос |

| Номер раздела, темы | Название раздела, темы | Количество аудиторных часов | | | | | | Форма контроля знаний |
|---|---|---|---|---|---|---|---|---|
| | | Лекции | Практические занятия | Семинарские занятия | Лабораторные занятия | Управляемая самостоятельная работа | Иное | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| | квадратичных форм. | | | | | | | |
| 8.3 | Билинейные формы | 2 | 2 | | | | | устный опрос |

# ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

## ОСНОВНАЯ ЛИТЕРАТУРА


1. Милованов, М.В. Алгебра и аналитическая геометрия. Часть 1. / Милованов М.В., М.М. Толкачев, Р.И. Тышкевич, А.С. Феденко –2-е изд.– Мн.: Амалфея, 2001. – 400 с.
2. Милованов, М.В. Алгебра и аналитическая геометрия. Часть 2 / Милованов М.В., Р.И. Тышкевич, А.С. Феденко –2-е изд.– Мн.: Амалфея, 2001. – 352 с.
3. Виноградов, И.М. Основы теории чисел / И.М. Виноградов. – М.: Наука, 1981. – 176 с.
4. Бурдун, А.А., Сборник задач по алгебре геометрии и аналитической геометрии / А.А. Бурдун, Е.А. Мурашко, М.М. Толкачев, А.С. Феденко – Мн.: Універсітэцкае, 1999. – 302 с.
5. Монахов, В.С., Алгебра и теория чисел. Практикум. Ч. 1. / В.С. Монахов, А.В. Бузланов. – Мн.: изд. Центр БГУ, 2007. – 264 с.
6. Практические занятия по алгебре и теории чисел / М.П. Лельчук, И.И. Полевченко, А.М Радьков, Б.М. Чеботаревский. – Мн.: Вышэйшая школа, 1986. – 302 с.


## ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА


1. Курош, А.Г. Курс высшей алгебры / А.Г. Курош – М.: Наука, 1975. – 431 с.
2. Фаддеев, Д.К. Сборник задач по высшей алгебре / Д.К. Фаддеев, И.С. Соминский. – М.: Наука,1977. – 188 с.
3. Размыслович, Г.П. Геометрия и алгебра / Г.П. Размыслович, М.М. Феденя, В.М. Ширяев. – Мн.: Універсітэцкае, 1987. – 350 с.
4. Размыслович, Г.П., Сборник задач по геометрии и алгебре / / Г.П. Размыслович, М.М. Феденя, В.М. Ширяев. – Мн.: Універсітэцкае, 1999. – 384 с.
5. Грибанов, В.У. Сборник задач по теории чисел / В.У. Грибанов, П.И. Титов. – М.: Просвещение, 1964. – 145 с.
6. Степанов, С.А. Сравнения / С.А. Степанов. – М.: Знание, 1975. – 62 с.
7. Александров, В.А., Задачник-практикум по теории чисел / В.А. Александров, С.М. Горшенин. – М.: Просвещение, 1972. – 81 с.
8. Ширяев, В.М. Прикладная алгебра. Теория чисел. / В.М. Ширяев. – Мн.: БГУ, 2009. – 152 с.


## ПЕРЕЧЕНЬ ИСПОЛЬЗУЕМЫХ СРЕДСТВ ДИАГНОСТИКИ РЕЗУЛЬТАТОВ УЧЕБНОЙ ДЕЯТЕЛЬНОСТИ

Оценка уровня знаний студента при защите курсовой работы производится по десятибалльной шкале в соответствии с критериями, утвержденными Министерством образования Республики Беларусь.

Оценка промежуточных учебных достижений студента также осуществляется по десятибалльной шкале.

Для оценки достижений студента используется следующий диагностический инструментарий:

– защита выполненных на практических занятиях индивидуальных заданий;

– выполнение индивидуальных домашних заданий;

– проведение текущих контрольных опросов по отдельным темам;

– проведение контрольных работ по отдельным темам

– сдача зачета по дисциплине в первом и втором семестрах;

– сдача экзамена.

## ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ТЕМ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

1. Метод математической индукции. Делимость чисел. Признаки делимости. Теорема о делении с остатком.
2. Простые и составные числа. Наибольший общий делитель. Наименьшее общее кратное.
3. Функция Эйлера. Полная и приведенная системы вычетов по модулю $m$.
4. Сравнения. Свойства сравнений.
5. Решение сравнений первой степени.
6. Решение систем сравнений первой степени.
7. Решение сравнений произвольной степени.
8. Квадратичные сравнение. Символ Лежандра.
9. Первообразные корни и индексы.
10. Приложения теории чисел.
11. Бинарное отношение. Отображения.
12. Перестановки и подстановки.
13. Алгебраическая операция. Нейтральный элемент. Симметричный элемент.
14. Группа. Подгруппа.
15. Кольцо. Подкольцо. Поле. Подполе.
16. Арифметические операции над комплексными числами.
17. Извлечение корней из комплексных чисел.
18. Деление с остатком в кольце многочленов одной переменной. Алгоритм Евклида.
19. Неприводимые многочлены. Корни многочлена.
20. Схема Горнера. Разложение многочленов на неприводимые множители.
21. Алгоритм нахождения целых и рациональных корней многочлена с целыми коэффициентами.
22. Интерполяционные многочлены Ньютона и Лагранжа.
23. Рациональные дроби.
24. Векторы. Линейная зависимость (независимость) системы векторов.
25. Линейное пространство. Определение, примеры.
26. Базис и размерность линейного пространства.

27. Координаты вектора в фиксированном базисе. Преобразования координат вектора при переходе от одного базиса к другому.
28. Линейное преобразование линейного пространства. Матрица линейного преобразования.
29. Операции над линейными преобразованиями.
30. Изменение матрицы линейного преобразования при замене базиса.
31. Собственные векторы и собственные значения линейного преобразования. Приведение матрицы линейного преобразования к диагональному виду.
32. Линейные преобразования переменных. Квадратичные формы. Метод Лагранжа приведения квадратичной формы к каноническому виду.
33. Эквивалентные квадратичные формы над полями $R$ и $C$. Знакоопределенная действительная квадратичная форма.
34. Билинейные формы.

ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ

| Название учебной дисциплины, с которой требуется согласование | Название кафедры | Предложения об изменениях в содержании учебной программы учреждения высшего образования по учебной дисциплине | Решение, принятое кафедрой, разработавшей учебную программу (с указанием даты и номера протокола)[1] |
|---|---|---|---|
| 1. | | | |
| | | | |

[1] При наличии предложений об изменениях в содержании учебной программы учреждения высшего образования по учебной дисциплине.

ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ К УЧЕБНОЙ ПРОГРАММЕ
на _____/_____ учебный год

| №№ пп | Дополнения и изменения | Основание |
|---|---|---|
| | | |

Учебная программа пересмотрена и одобрена на заседании кафедры
_____ (протокол № ____ от _____ 201_ г.)
(название кафедры)

Заведующий кафедрой

_____ _____ _____
(ученая степень, ученое звание) (подпись) (И.О.Фамилия)

УТВЕРЖДАЮ
Декан факультета

_____ _____ _____
(ученая степень, ученое звание) (подпись) (И.О.Фамилия)