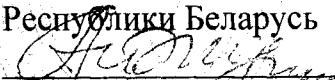


Министерство образования Республики Беларусь

Учебно-методическое объединение по естественнонаучному образованию

УТВЕРЖДАЮ

Первый заместитель Министра образования
Республики Беларусь

 А.И. Жук

30.04.2012

(дата утверждения)

Регистрационный № ТД- Б. 411 /тип.

АЛГЕБРА И ТЕОРИЯ ЧИСЕЛ

Типовая учебная программа

для учреждений высшего образования по направлению специальности

**1-31 03 07-01 Прикладная информатика (программное
обеспечение компьютерных систем)**

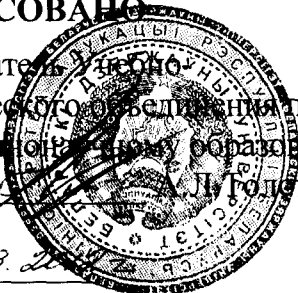
СОГЛАСОВАНО

Председатель Учебно-методического объединения по
естественнонаучному образованию

 Л. Голотик

22.03.2012

(дата)



СОГЛАСОВАНО

Зам. начальника управления высшего и
среднего специального образования
Министерства образования
Республики Беларусь

 Э.Г. Шевцов
(И.О. Фамилия)

30.04.2012

(дата)

Проректор по учебной и воспитатель-
ной работе Государственного учрежде-
ния образования «Республиканский
институт высшей школы»

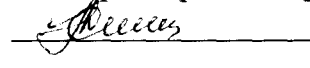
 В.И. Шупляк
(И.О. Фамилия)



02.04.2012

(дата)

Эксперт-нормоконтролер

 Н.В. Сенник
(И.О. Фамилия)

02.04.2012

(дата)

Минск 2012

СОСТАВИТЕЛИ:

Г.П. Размыслович, доцент кафедры высшей математики Белорусского государственного университета, кандидат физико-математических наук, доцент;

В.М. Ширяев, доцент кафедры высшей математики Белорусского государственного университета, кандидат физико-математических наук, доцент;

А.В. Филиппов, доцент кафедры высшей математики Белорусского государственного университета, кандидат физико-математических наук, доцент.

РЕЦЕНЗЕНТЫ:

Кафедра высшей математики Учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»;

С.С.Белявский, доцент кафедры прикладной математики и экономической кибернетики Учреждения образования «Белорусский государственный экономический университет», канд. физ.-мат. наук.

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ В КАЧЕСТВЕ ТИПОВОЙ:

Кафедрой высшей математики Белорусского государственного университета (протокол № 10 от 18.02.2011г.)

Научно-методическим советом Белорусского государственного университета (протокол № 2 от 21.02.2011г.);

Научно-методическим советом по прикладной математике и информатике Учебно-методического объединения по естественному образованию (протокол № 2 от 12.04.2011г.)

Ответственный за выпуск: Г.П. Размыслович

Пояснительная записка

Курс «Алгебра и теория чисел» знакомит студентов с основными понятиями теории чисел, линейной и высшей алгебры, прикладной алгебры.

Базой для изучения данного курса является дисциплина «Алгебра», изучаемая в средней школе.

Предмет «Алгебра и теория чисел» является базовым математическим курсом и непосредственно связан с основными дисциплинами, такими как «Математический анализ» и «Дифференциальные уравнения». Методы, излагаемые в курсе теории чисел и алгебры, используются при изучении дисциплин «Компьютерная графика», «Методы вычислений», «Исследование операций», «Теория вероятностей и математическая статистика», а также при изучении ряда дисциплин специализаций.

Основными целями курса являются:

- во-первых, дать глубокие знания по одному из основных разделов курса высшей математики, имеющего тесную связь с многочисленными прикладными проблемами и приложениями;
- во-вторых, создать фундаментальные основы, необходимые для усвоения материала перечисленных выше дисциплин;
- в-третьих, сформировать одну из основных частей банка знаний специалистов университетского уровня в избранной области деятельности.

При изложении курса важно показать возможности использования аппарата алгебры и теории чисел при решении как чисто теоретических, так и прикладных задач, возникающих в различных областях науки, техники, экономики и др. Целесообразно выделить моменты построения алгоритмов полученных результатов с целью их реализации при помощи средств вычислительной техники.

В результате изучения дисциплины студент должен знать:

- основы теории чисел и ее применение в информатике,
- основные понятия высшей алгебры,
- основы линейной алгебры;

уметь:

- находить решения показательных, степенных сравнений с использованием таблицы индексов и решения систем сравнений,
- применять аппарат алгебры при решении задач специальности;
- решать основные задачи теории векторных, евклидовых пространств.

На лекционных занятиях по дисциплине «Алгебра и теория чисел» возможно использование элементов проблемного обучения: проблемное изложение некоторых аспектов предмета, заданий и упражнений на доказательство или опровержение тех или иных положений. На практических и лабораторных занятиях по дисциплине рекомендуется использовать индивидуальный творческий подход: студенту предлагаются индивидуальные задачи по основным разделам курса, для решения которых он разрабатывает свои методы решения и представляет работу на проверку преподавателю.

Для самостоятельной работы студентов, в частности, для развития навыков самоконтроля, способствующих интенсификации учебного процесса предлагается:

- использовать в учебном процессе разработанные компьютерные тесты;

– обеспечить доступность электронного (твердого экземпляра) курса лекций, учебно-методических пособий и сборников задач по основным разделам дисциплин.

В соответствии с типовым учебным планом по направлению специальности 1-31 03 07-01 «Прикладная информатика (программное обеспечение компьютерных систем)» учебная программа предусматривает для изучения дисциплины 246 учебных часов, в том числе 136 аудиторных часов: лекции – 68 часов, практические занятия – 68 часов.

Примерный тематический план

№	Название раздела, темы	Количество аудиторных часов		
		Всего	В том числе	
			Лекции	Практические занятия
	Введение.	1	1	
	Раздел 1. Теория чисел			
1.	Делимость чисел	6	2	4
2.	Простые числа и составные числа	6	4	4
3.	Числовые сравнения	8	4	4
4.	Сравнения с одним неизвестным	8	4	4
5.	Системы сравнений первой степени	8	4	4
6.	Приложения теории чисел	6	4	4
	Раздел 2. Алгебра.			
7.	Алгебраическая операция. Группа, кольцо, поле	4	2	2
8.	Комплексные числа	8	4	4
9.	Многочлены	8	4	4
10.	Матрицы и определители	8	4	4
11.	Векторные пространства	12	6	6
12.	Системы уравнений	8	4	4
13.	Линейные отображения	8	4	4
14.	Квадратичные формы	10	5	4
15.	Евклидовы и унитарные пространства	8	4	4
16.	Изометрические и симметрические преобразования	10	5	4
17.	Элементы линейного программирования	9	5	4
	Всего	136	68	68

Содержание

Введение

Предмет дисциплины «Алгебра и теория чисел». Исторические сведения о развитии этого раздела математики. Роль и место теории чисел и алгебры в системе математического образования.

Раздел 1. Теория чисел

1. Делимость чисел

Свойства делимости целых чисел. Деление с остатком. Наибольший общий делитель и наименьшее общее кратное. Алгоритм Евклида.

2. Простые числа и составные числа

Простые числа и их свойства. Взаимно простые числа, критерий взаимной простоты. Свойства взаимно простых чисел. Основная теорема арифметики. Элементарные делители.

3. Числовые сравнения

Сравнения целых чисел по данному модулю и их свойства. Кольцо вычетов по данному модулю. Приведенная группа вычетов. Функция Эйлера, свойства. Теорема Эйлера, малая теорема Ферма.

4. Сравнения с одним неизвестным

Решение сравнений первой степени. Существование первообразного элемента по простому модулю, по примарному модулю и по двойному модулю. Свойства индексов. Решение показательных и степенных сравнений. Китайская теорема об остатках.

5. Системы сравнений первой степени

Решение систем сравнений первой степени. Решение систем линейных уравнений над кольцом целых чисел. Метод Серпинского, метод элементарных преобразований.

6. Приложения теории чисел

Разделение секрета и пороговая схема. Протокол Диффи-Хелмана. RSA-криптосистемы и система цифровой подписи на её основе.

Раздел 2. Алгебра

7. Алгебраическая операция. Группа, кольцо, поле

Бинарное отношение. Отношения эквивалентности и порядка, классы эквивалентности. Алгебраическая операция. Группа, кольцо, поле и их простейшие свойства.

8. Комплексные числа

Построение системы комплексных чисел. Алгебраическая, тригонометрическая и экспоненциальная формы комплексных чисел. Возведение в степень и извлечение корня n -ой степени из комплексного числа. Корни из единицы.

9. Многочлены

Кольцо многочленов над полем. Деление с остатком. Алгоритм Евклида. Корни многочлена. Разложение многочленов на неприводимые многочлены. Интерполяция. Схема Горнера.

10. Матрицы и определители

Матричная алгебра. Определители. Теорема Лапласа. Обратная матрица. Системы линейных уравнений. Правило Крамера. Метод Гаусса. Матричные уравнения.

11. Векторные пространства

Векторное (линейное) пространство. Линейная зависимость и независимость векторов. Базис и размерность. Подпространства. Линейные оболочки. Сумма и пересечение подпространств. Ранг системы векторов. Ранг матрицы и теорема о базисном миноре.

12. Системы уравнений

Критерий совместности систем линейных уравнений. Общее решение систем линейных уравнений.

13. Линейные преобразования

Матрица линейного преобразования. Ядро и образ линейного преобразования (оператора). Невырожденное линейное преобразование. Собственные векторы и собственные значения. Характеристическая матрица и характеристический многочлен. Операторы простой структуры.

14. Квадратичные формы

Метод Лагранжа приведения квадратичной формы к каноническому виду. Критерии эквивалентности квадратичных форм над полем R и над полем C . Приведение квадратичной формы к каноническому виду при помощи ортогональных преобразований. Критерии знакоопределённости действительных квадратичных форм.

15. Евклидово пространство

Длина вектора. Неравенства Коши-Шварца-Буняковского и неравенство треугольника. Процесс ортогонализации Грама-Шмидта. Матрица Грама и матрица скалярного произведения.

16. Изометрические и симметрические преобразования

Изометрический оператор. Самосопряжённый оператор. Разложение произвольного линейного оператора в произведение изометрического и самосопряжённого операторов.

17. Элементы линейного программирования

Системы линейных неравенств. Прямая и двойственная задачи. Симплекс метод. Графический метод решения задач линейного программирования.

Информационно-методическая часть

Литература

Основная

1. Айерленд К., Роузен М. Классическое введение в теорию чисел. М., "Мир", 1987, 415 с.
2. Арнольд И.В. Теория чисел. М., 1939, 288 с.
3. Беляш-Кривец В.В., Мельников О.В. Лекции по алгебре. Группы, кольца, поля. Мн.: БГУ, 2009, 115 с.
4. Биркгоф Г., Барти Т. Современная прикладная алгебра. М., 2005, 400 с.
5. Бурдун А.А., Мурашко Е.А., Толкачев М.М., Феденко А.С. Сборник задач по алгебре и аналитической геометрии. – Мн., "Университетское", 1989, 222 с.
6. Виноградов И.М. Основы теории чисел. М., Наука, 1981, с.176.
7. Ильин В.А., Позняк Э.Г. Линейная алгебра. – М: "Наука", 1981, 294 с.
8. Милованов М.В., Тышкевич Р.И., Феденко А.С. Линейная алгебра и аналитическая геометрия. I. – Мн., "Выш. школа", 1976, 544 с.

9. Милованов М.В., Тышкевич Р.И., Феденко А.С. Линейная алгебра и аналитическая геометрия. II. – Мн., “Выш. школа”, 1984, 302 с.
10. Нестеренко Ю.В. Теория чисел. М., “Академия”, 2008, 272 с.
11. Размыслович Г.П., Феденя М.М., Ширяев В.М. Геометрия и алгебра. – Мн., “Университетское”, 1987, 350 с.
12. Размыслович Г.П., Феденя М.М., Ширяев В.М. Сборник задач по геометрии и алгебре. – Мн., “Университетское”, 1999, 384 с.
13. Тышкевич Р.И., Феденко А.С. Линейная алгебра и аналитическая геометрия. Мн., “Выш. школа”, 1976, 544 с.
14. Харин Ю.С. Математические и компьютерные основы криптологии. Мн., 2003, 391 с.
15. Ширяев В.М. Прикладная алгебра. Теория чисел. Сборник задач. Мн.: БГУ, 2009, 152 с.
16. Шнеперман Л.Б. Курс алгебры и теории чисел в задачах и упражнениях. Т. 1, Мн: “Выш. школа”, 1986, 272 с.
17. Шнеперман Л.Б. Курс алгебры и теории чисел в задачах и упражнениях. Т. 2, Мн: “Выш. школа”, 1987, 256 с.

Дополнительная

1. Воеводин В.В. Линейная алгебра. – М., “Наука”, 1990, 400 с.
2. Гантмахер Ф.Р. Теория матриц. М.: “Наука”, 1967, 575 с.
3. Курош А.Г. Курс высшей алгебры. – М., “Наука”, 1975, 431 с.
4. Кострикин А.И., Манин Ю.И. Линейная алгебра и геометрия. М.: “Наука”, 1986, 304 с.
5. Проскуряков И.В. Сборник задач по линейной алгебре. М.: “Наука”, 1978, 384 с.
6. Фаддеев Д.К., Соминский И.С. Сборник задач по высшей алгебре. – М.: “Наука”, 1977, 188 с.

Типовым учебным планом специальности в качестве формы итогового контроля по дисциплине «Алгебра и теория чисел» предусмотрены два зачета и экзамен. Оценка учебных достижений студента на экзамене осуществляется по десятибалльной шкале.

С целью текущего контроля знаний и умений студентов по данной дисциплине рекомендуется использовать следующий диагностический инструментарий:

- проведение в каждом семестре одного – двух коллоквиумов;
- проведение в каждом семестре одной – двух контрольных работ;
- персональное собеседование и устный опрос по отдельным разделам дисциплины;
- критериально-ориентированные тесты по отдельным темам дисциплины;
- решение проблемных задач, предполагающих неформальный ответ.