

МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учебно-методическое объединение по образованию
в области информатики и радиоэлектроники

УТВЕРЖДАЮ

Первый заместитель Министра образования
Республики Беларусь

_____ И.А. Старовойтова

_____ /тип.
Регистрационный № ТД-_____/тип.

ОСНОВЫ ВЫСШЕЙ АЛГЕБРЫ

Типовая учебная программа по учебной дисциплине
для специальности

1-40 04 01 «Информатика и технологии программирования»

СОГЛАСОВАНО

Начальник Управления
электроники и приборостроения,
электротехнической и оптико-
механической промышленности
Министерства промышленности
Республики Беларусь
_____ А.С. Турцевич

СОГЛАСОВАНО

Председатель Учебно-методического
объединения по образованию
в области информатики
и радиоэлектроники
_____ В.А. Богуш

СОГЛАСОВАНО

Начальник Главного управления
профессионального образования
Министерства образования
Республики Беларусь
_____ С.А. Касперович

СОГЛАСОВАНО

Проректор по научно-методической
работе Государственного учреждения
образования «Республиканский
институт высшей школы»
_____ И.В. Титович

Эксперт-нормоконтролер

СОСТАВИТЕЛИ:

М.А. Калугина, доцент кафедры информатики учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», кандидат физико-математических наук, доцент;

Е.Д. Стройникова, старший преподаватель кафедры информатики учреждения образования «Белорусский государственный университет информатики и радиоэлектроники».

РЕЦЕНЗЕНТЫ:

Кафедра высшей математики Белорусского государственного университета (протокол № 3 от 04.11.2021 г.);

Д.В. Васильев, заведующий отделом теории чисел Государственного научного учреждения «Институт математики Национальной академии наук Беларуси», кандидат физико-математических наук.

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ В КАЧЕСТВЕ ТИПОВОЙ:

Кафедрой информатики учреждения образования «Белорусский государственный университет информатики и радиоэлектроники» (протокол № 3 от 19.10.2021 г.);

Научно-методическим советом учреждения образования «Белорусский государственный университет информатики и радиоэлектроники» (протокол № 2 от 19.11.2021 г.);

Научно-методическим советом по разработке программного обеспечения и информационно-коммуникационным технологиям Учебно-методического объединения по образованию в области информатики и радиоэлектроники (протокол № 3 от 08.11.2021 г.).

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

ХАРАКТЕРИСТИКА УЧЕБНОЙ ДИСЦИПЛИНЫ

Типовая учебная программа по учебной дисциплине «Основы высшей алгебры» разработана для студентов учреждений высшего образования, обучающихся по специальности 1-40 04 01 «Информатика и технологии программирования», в соответствии с требованиями образовательного стандарта высшего образования первой ступени и типового учебного плана вышеуказанной специальности.

Учебная дисциплина «Основы высшей алгебры» является одной из дисциплин, закладывающих основу математической подготовки специалистов в области информатики и информационных технологий. Данная учебная дисциплина знакомит студентов с основными понятиями и методами высшей алгебры и математическими основами криптографии, имеет общенаучную и профессиональную направленность.

Актуальность изучения учебной дисциплины «Основы высшей алгебры» определяется той ролью, которую играет математика в жизни современного общества, ее влиянием на темпы развития научно-технического прогресса, а для студентов – будущих инженеров-системных программистов – профессиональной направленностью.

В последнее время значительно возросла роль математики, чему во многом способствовало и расширение ее возможностей, связанное с созданием быстродействующих электронно-вычислительных машин. Благодаря стремительному развитию вычислительной техники существенно расширяются возможности применения математики при решении конкретных задач. Математические методы широко применяются в науках, еще недавно весьма далеких от математики: в экономике, биологии, медицине. С уверенностью можно сказать, что ни один научно-технический замысел современности не обходится без участия математики. Аппарат алгебры является неотъемлемой частью языков различных областей современной математики и естествознания и имеет универсальное значение.

Проникновение информационных технологий во все отрасли человеческой деятельности становится определяющим в тенденциях развития современной фундаментальной науки. В частности, прогресс в вычислительной технике не только привел к возникновению новых направлений математики, но и стимулировал фундаментальные исследования в тех классических разделах алгебры, теории чисел и алгебраической геометрии (группы, кольца и поля, модульная арифметика, эллиптические кривые над конечными полями, булева алгебра и др.), которые еще недавно считались абстрактными и оторванными от практики.

При изложении учебной дисциплины «Основы высшей алгебры» важно показать возможности использования алгебраического аппарата при решении как чисто теоретических, так и прикладных задач, возникающих в различных областях науки и техники. Целесообразно выделить моменты построения алго-

ритмов получения результатов с целью их реализации при помощи средств вычислительной техники.

Знание высшей алгебры является необходимым для фундаментальной подготовки специалистов инженерного профиля. Ускорение развития технических наук предъявляет повышенные требования к математическому образованию современных инженеров. Главное из них – это ориентация обучения студентов на применение математических методов к решению прикладных задач и широкое использование компьютерных технологий. Математический стиль мышления, умение рассуждать строго, умение аналитически разлагать задачу на основные базисные составляющие – все эти качества крайне необходимы будущему специалисту. Учебная дисциплина «Основы высшей алгебры» играет важную роль в математическом образовании, так как ее конструкции, идеи и методы исследований широко используются в других математических дисциплинах.

Воспитательное значение учебной дисциплины «Основы высшей алгебры» заключается в формировании у обучающихся математической культуры и научного мировоззрения; развитии исследовательских умений, аналитических способностей, креативности, необходимых для решения научных и практических задач; развитии познавательных способностей и активности: творческой инициативы, самостоятельности, ответственности и организованности; формировании способностей к саморазвитию, самосовершенствованию и самореализации.

Изучение данной учебной дисциплины способствует созданию условий для формирования интеллектуально развитой личности обучающегося, которой присущи стремление к профессиональному совершенствованию, активному участию в экономической и социально-культурной жизни страны, гражданская ответственность и патриотизм.

ЦЕЛИ, ЗАДАЧИ, РОЛЬ УЧЕБНОЙ ДИСЦИПЛИНЫ

Цели учебной дисциплины: развитие интеллектуального потенциала, способностей к логическому и алгоритмическому мышлению; освоение студентами фундаментальных методов высшей алгебры, техники математических рассуждений и доказательств, необходимых для дальнейшего использования в других математических дисциплинах, а также в областях знаний естественно-научного содержания.

Задачи изучения учебной дисциплины:

приобретение систематизированных знаний по основным разделам высшей алгебры;

изучение принципов внутренней логики, связывающей теорию чисел, теорию групп, колец и полей;

приобретение аналитических навыков, необходимых для исследования и решения практических задач;

овладение современными методами высшей алгебры, в том числе с применением средств вычислительной техники.

Базовыми учебными дисциплинами для учебной дисциплины «Основы высшей алгебры» являются «Аналитическая геометрия и линейная алгебра» и «Математическая логика». Учебная дисциплина «Основы высшей алгебры» непосредственно связана с математическими дисциплинами «Математический анализ» и «Дискретная математика», а также с учебной дисциплиной «Основы алгоритмизации и программирования». В свою очередь учебная дисциплина «Основы высшей алгебры» является базой для таких учебных дисциплин, как «Теория вероятностей», «Прикладные задачи математического анализа», «Методы численного анализа» (учебная дисциплина компонента учреждения высшего образования), «Системный анализ и исследование операций» (учебная дисциплина компонента учреждения высшего образования), «Методы защиты информации» (учебная дисциплина компонента учреждения высшего образования).

ТРЕБОВАНИЯ К УРОВНЮ ОСВОЕНИЯ СОДЕРЖАНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

В результате изучения учебной дисциплины «Основы высшей алгебры» формируются следующие компетенции:

универсальные:

обладать навыками творческого аналитического мышления;

базовые профессиональные:

применять методы высшей и линейной алгебры, приемы сведения практических задач к изученному математическому аппарату.

В результате изучения учебной дисциплины обучающийся должен:

знать:

основные понятия и принципы высшей алгебры;

основные принципы внутренней логики, связывающей теорию чисел, теорию групп, колец и полей;

уметь:

применять базовые научно-теоретические знания для решения теоретических и практических задач;

строить математические модели практических задач на основе методов высшей алгебры;

применять основные математические модели и методы в научных исследованиях в области профессиональной деятельности;

владеть:

системным и сравнительным анализом;

приемами сведения практических задач к изученному математическому аппарату.

В рамках образовательного процесса по учебной дисциплине «Основы высшей алгебры» студент должен приобрести не только теоретические и практические знания, умения и навыки по специальности, но и развить свой ценностно-личностный, духовный потенциал, сформировать качества патриота и

гражданина, готового к активному участию в экономической, производственной, социально-культурной и общественной жизни страны.

Программа рассчитана на 104 учебных часа, из них – 50 аудиторных.

Примерное распределение аудиторных часов по видам занятий: лекций – 26 часов, практических занятий – 24 часа.

Программа разработана без учета часов, отводимых на проведение текущей аттестации, определенной типовым учебным планом.

ПРИМЕРНЫЙ ТЕМАТИЧЕСКИЙ ПЛАН

Наименование раздела, темы	Всего ауди-торных, часы	Лекции, часы	Практи-ческие занятия, часы
Раздел 1. Основы теории чисел	16	8	8
Тема 1. Делимость целых чисел	4	2	2
Тема 2. Простые числа. Взаимно простые числа. Диофантовы линейные уравнения	4	2	2
Тема 3. Сравнения целых чисел. Множество классов вычетов. Функция Эйлера	4	2	2
Тема 4. Классические шифры	4	2	2
Раздел 2. Элементы теории групп	16	8	8
Тема 5. Понятие алгебраической системы. Группы. Подгруппы	4	2	2
Тема 6. Смежные классы. Нормальные подгруппы. Факторгруппы	4	2	2
Тема 7. Симметрические группы	4	2	2
Тема 8. Гомоморфизмы групп. Криптосистема RSA	4	2	2
Раздел 3. Введение в теорию колец и полей	18	10	8
Тема 9. Кольца. Подкольца и идеалы колец	4	2	2
Тема 10. Кольцо полиномов от одной переменной над полем	4	2	2
Тема 11. Неприводимость над полем и корни полиномов	4	2	2
Тема 12. Факторкольца. Гомоморфизмы колец	4	2	2
Тема 13. Характеристика кольца. Минимальные поля	2	2	–
Итого:	50	26	24

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Раздел 1. ОСНОВЫ ТЕОРИИ ЧИСЕЛ

Тема 1. ДЕЛИМОСТЬ ЦЕЛЫХ ЧИСЕЛ

Целые числа. Свойства операций сложения и умножения целых чисел. Свойства делимости. Наибольший общий делитель (НОД) и его нахождение по алгоритму Евклида. Наименьшее общее кратное (НОК) и его вычисление.

Тема 2. ПРОСТЫЕ ЧИСЛА. ВЗАИМНО ПРОСТЫЕ ЧИСЛА. ДИОФАНТОВЫ ЛИНЕЙНЫЕ УРАВНЕНИЯ

Простые числа и их свойства. Взаимно простые числа. Критерий взаимной простоты чисел. Основная теорема арифметики. Диофантовы линейные уравнения.

Тема 3. СРАВНЕНИЯ ЦЕЛЫХ ЧИСЕЛ. МНОЖЕСТВО КЛАССОВ ВЫЧЕТОВ. ФУНКЦИЯ ЭЙЛЕРА

Сравнения целых чисел, свойства сравнений. Множество классов вычетов по натуральному модулю. Функция Эйлера и ее вычисление. Теорема Эйлера. Малая теорема Ферма и следствия из нее. Решение линейных сравнений в целых числах.

Тема 4. КЛАССИЧЕСКИЕ ШИФРЫ

Шифры замены и перестановки. Примеры. Шифр Виженера и методы его дешифрования.

Раздел 2. ЭЛЕМЕНТЫ ТЕОРИИ ГРУПП

Тема 5. ПОНЯТИЕ АЛГЕБРАИЧЕСКОЙ СИСТЕМЫ. ГРУППЫ. ПОДГРУППЫ

Бинарная алгебраическая операция на множестве. Виды алгебраических систем. Группы, их основные типы и свойства. Подгруппы. Порядок элементов в группе и циклическая подгруппа. Основные свойства циклических групп.

Тема 6. СМЕЖНЫЕ КЛАССЫ. НОРМАЛЬНЫЕ ПОДГРУППЫ. ФАКТОРГРУППЫ

Смежные классы и их свойства. Теорема Лагранжа и следствия из нее. Нормальные подгруппы. Критерий нормальности подгруппы. Факторгруппы и их свойства. Примеры факторгрупп.

Тема 7. СИММЕТРИЧЕСКИЕ ГРУППЫ

Подстановки и их свойства. Симметрическая группа и ее основные свойства. Знакопеременная группа и ее свойства.

Тема 8. ГОМОМОРФИЗМЫ ГРУПП. КРИПТОСИСТЕМА RSA

Гомоморфизмы групп и их основные свойства. Теорема Кэли. Автоморфизмы групп и их свойства. Криптосистема RSA и система электронной цифровой подписи на ее основе.

Раздел 3. ВВЕДЕНИЕ В ТЕОРИЮ КОЛЕЦ И ПОЛЕЙ

Тема 9. КОЛЬЦА. ПОДКОЛЬЦА И ИДЕАЛЫ КОЛЕЦ

Кольца, их основные типы и свойства. Примеры колец. Мультипликативная группа кольца. Делители нуля в кольце. Тело и поле. Основные свойства полей. Подкольца, подполя. Идеалы колец и их виды.

Тема 10. КОЛЬЦО ПОЛИНОМОВ ОТ ОДНОЙ ПЕРЕМЕННОЙ НАД ПОЛЕМ

Кольцо полиномов от одной переменной над полем и его основные свойства. Делимость полиномов. НОД и НОК полиномов. Взаимно простые полиномы.

Тема 11. НЕПРИВОДИМОСТЬ НАД ПОЛЕМ И КОРНИ ПОЛИНОМОВ

Неприводимость над полем и теорема о разложении на множители в кольце полиномов. Каноническое разложение полинома. Корни полинома и их кратность. Теорема Безу и следствия из нее. Основная теорема алгебры и следствия из нее. Структура неприводимых полиномов над полем.

Тема 12. ФАКТОРКОЛЬЦА. ГОМОМОРФИЗМЫ КОЛЕЦ

Факторкольца и их свойства. Примеры факторколец. Структура факторкольца $R[x]/(f(x))$. Построение полей Галуа. Гомоморфизмы колец и их основные свойства. Теорема существования корня и следствия из нее. Виды и примеры гомоморфизмов колец.

Тема 13. ХАРАКТЕРИСТИКА КОЛЬЦА. МИНИМАЛЬНЫЕ ПОЛЯ

Понятие характеристики кольца. Примеры колец и полей различных характеристик. Минимальные поля нулевой и ненулевой характеристики.

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

ЛИТЕРАТУРА

ОСНОВНАЯ

1. Бухштаб, А. А. Теория чисел / А. А. Бухштаб. – 3-е изд., стереотип. – М. : URSS, 2008. – 384 с.
2. Винберг, Э. Б. Алгебра многочленов : учеб. пособие / Э. Б. Винберг. – М. : Просвещение, 1980. – 176 с.
3. Виноградов, И. М. Основы теории чисел / И. М. Виноградов. – 9-е изд., перераб. – М. : Наука, 1981. – 176 с.
4. Каргополов, М. И. Основы теории групп / М. И. Каргополов, Ю. И. Мерзляков. – М. : Наука, 1972. – 240 с.
5. Кострикин, А. И. Введение в алгебру. В 3 ч. Ч. 1 : Основы алгебры / А. И. Кострикин. – 3-е изд. – М. : Физматлит, 2004. – 272 с.
6. Кострикин, А. И. Сборник задач по алгебре / А. И. Кострикин. – М. : Физматлит, 2001. – 464 с.
7. Криптология : учебник / Ю. С. Харин [и др.]. – Минск : БГУ, 2013. – 511 с.
8. Курош, А. Г. Курс высшей алгебры : учебник для вузов / А. Г. Курош. – 17-е изд., стереотип. – СПб. : Лань, 2008. – 432 с.
9. Липницкий, В. А. Современная прикладная алгебра. Математические основы защиты информации от помех и несанкционированного доступа : учеб.-метод. пособие / В. А. Липницкий. – 2-е изд., испр. – Минск : БГУИР, 2006. – 88 с.
10. Милованов, М. В. Алгебра и аналитическая геометрия : учебник для вузов. В 2 ч. Ч. 1 / М. В. Милованов, Р. И. Тышкевич, А. С. Феденко. – Минск : Амалфея, 2001. – 400 с.
11. Проскуряков, И. В. Сборник задач по линейной алгебре / И. В. Проскуряков. – 12-е изд., стер. – СПб. : Лань, 2008. – 480 с.
12. Стройникова, Е. Д. Алгебра в примерах и задачах : учеб.-метод. пособие / Е. Д. Стройникова. – Минск : БГУИР, 2018. – 100 с.
13. Стройникова, Е. Д. Основы прикладной алгебры : учеб.-метод. пособие / Е. Д. Стройникова. – Минск : БГУИР, 2010. – 120 с.
14. Шнеперман, Л. Б. Сборник задач по алгебре и теории чисел / Л. Б. Шнеперман. – 3-е изд., стереотип. – СПб. : Лань, 2008. – 224 с.

ДОПОЛНИТЕЛЬНАЯ

1. Айерлэнд, К. Классическое введение в современную теорию чисел / К. Айерлэнд, М. Роузен ; пер. с англ. – М. : Мир, 1987. – 416 с.
2. Аршинов, Н. Н. Коды и математика / Н. Н. Аршинов, Л. Е. Садовский. – М. : Наука, 1983. – 124 с.
3. Баричев, С. Г. Основы современной криптографии : учеб. пособие для вузов / С. Г. Баричев, В. В. Гончаров, Р. Е. Серов. – 2-е изд., испр. и доп. – М. : Горячая линия-Телеком, 2002. – 175 с.

4. Беняш-Кривец, В. В. Лекции и семинары по алгебре: группы, кольца, поля : пособие / В. В. Беняш-Кривец, Г. Е. Пунинский. – Минск : БГУ, 2015. – 152 с.
5. Беняш-Кривец, В. В. Лекции и семинары по алгебре: основные понятия алгебры и теории чисел : пособие / В. В. Беняш-Кривец, Г. Е. Пунинский. – Минск : БГУ, 2015. – 114 с.
6. Биркгоф, Г. Современная прикладная алгебра / Г. Биркгоф, Т. К. Барти ; пер. с англ. – 2-е изд., стереотип. – СПб. : Лань, 2005. – 400 с.
7. Василенко, О. Н. Теоретико-числовые алгоритмы в криптографии / О. Н. Василенко. – М. : МЦНМО, 2003. – 326 с.
8. Введение в криптографию / В. В. Ященко [и др.] ; под общ. ред. В. В. Ященко. – 4-е изд., доп. – М. : МЦНМО, 2012. – 348 с.
9. Коутинхо, С. Введение в теорию чисел. Алгоритм RSA / С. Коутинхо ; пер. с англ. – М. : Постмаркет, 2001. – 328 с.
10. Ленг, С. Алгебра / С. Ленг ; пер. с англ. – М. : Мир, 1968. – 564 с.
11. Лидл, Р. Конечные поля : в 2 т. / Р. Лидл, Г. Нидеррайтер ; пер. с англ. – М. : Мир, 1988. – 820 с.
12. Ноден, П. Алгебраическая алгоритмика / П. Ноден, К. Китте ; пер. с англ. – М. : Мир, 1999. – 720 с.
13. Прасолов, В. В. Многочлены / В. В. Прасолов. – 3-е изд., испр. – М. : МЦНМО, 2003. – 336 с.
14. Фаддеев, Д. К. Сборник задач по высшей алгебре / Д. К. Фаддеев, И. С. Соминский. – 11-е изд., перераб. и доп. – М. : Наука, 1977. – 288 с.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ И ВЫПОЛНЕНИЮ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

При изучении учебной дисциплины рекомендуется использовать следующие формы самостоятельной работы:

- выполнение домашних заданий и подготовка к практическим занятиям;
- изучение теоретического материала в процессе подготовки к лекциям;
- подготовка к проверочным работам;
- выполнение контрольных работ;
- получение консультаций преподавателя по изучаемым вопросам;
- самостоятельная работа на базе электронного образовательного ресурса по учебной дисциплине над определенными преподавателем разделами учебной дисциплины;
- подготовка к экзамену.

ПЕРЕЧЕНЬ РЕКОМЕНДУЕМЫХ СРЕДСТВ ДИАГНОСТИКИ КОМПЕТЕНЦИЙ СТУДЕНТА

Типовым учебным планом по специальности 1-40 04 01 «Информатика и технологии программирования» в качестве формы текущей аттестации по учебной дисциплине «Основы высшей алгебры» рекомендуется экзамен.

Оценка учебных достижений студента производится по десятибалльной шкале.

Для промежуточного контроля по учебной дисциплине и диагностики компетенций студентов могут использоваться следующие формы:

типовые задания;
 проверочные работы;
 контрольные работы;
 устный опрос во время занятий;
 коллоквиумы.

РЕКОМЕНДУЕМЫЕ МЕТОДЫ (ТЕХНОЛОГИИ) ОБУЧЕНИЯ

Основные рекомендуемые методы (технологии) обучения, отвечающие целям и задачам дисциплины:

элементы проблемного обучения (проблемное изложение, вариативное изложение, частично-поисковый метод), реализуемые на лекционных занятиях;

элементы учебно-исследовательской деятельности, творческий подход, реализуемые на практических занятиях.

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ТЕМ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

1. Делимость целых чисел. НОД и НОК целых чисел.
2. Простые числа. Взаимно простые числа и их свойства. Диофантовы линейные уравнения.
3. Сравнения целых чисел. Множество классов вычетов. Функция Эйлера.
4. Классические шифры.
5. Понятие алгебраической системы. Группы. Подгруппы.
6. Смежные классы. Нормальные подгруппы. Факторгруппы.
7. Симметрические группы.
8. Гомоморфизмы групп. Алгоритм RSA.
9. Кольца. Подкольца и идеалы колец.
10. Кольцо полиномов от одной переменной над полем.
11. Неприводимость над полем и корни полиномов.
12. Факторкольца. Гомоморфизмы колец. Характеристика кольца.