Учреждение образования
«Гомельский государственный технический университет
имени П. О. Сухого»

УТВЕРЖДАЮ
Первый проректор
ГГТУ им. П.О. Сухого
_____ О. Д. Асенчик
08.12 2021г.
Регистрационный № УД-42-39уч.

ОСНОВЫ ВЫСШЕЙ АЛГЕБРЫ

Учебная программа учреждения высшего образования
по учебной дисциплине для специальностей:
1-40 04 01 «Информатика и технологии программирования»

2021

Библиотека ГГТУ им.П.О.Сухого

Учебная программа составлена на основе:
образовательного стандарта высшего образования первой ступени ОСВО 1-40 04 01-2013;
учебного плана учреждения образования «Гомельский государственный технический университет имени П.О. Сухого» по специальности 1-40 04 01 «Информатика и технологии программирования», регистрационный № I 40-1-23/уч. от 01.06.2021

СОСТАВИТЕЛЬ:
Бабич А.А., заведующий кафедрой «Высшая математика» Учреждения образования «Гомельский государственный технический университет имени П.О. Сухого», кандидат физико-математических наук, доцент.

РЕЦЕНЗЕНТЫ:
Трохова Т.А., заведующая кафедрой «Информатика» Учреждения образования «Гомельский государственный технический университет имени П.О. Сухого», кандидат технических наук, доцент.
Буякевич Л.И., доцент кафедры Организации деятельности органов и подразделений по чрезвычайным ситуациям, Гомельский филиал Университета гражданской защиты МЧС Беларуси, кандидат физико-математических наук, доцент.

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой «Высшая математика» учреждения образования «Гомельский государственный технический университет имени П.О. Сухого»
(протокол № 3 от 22.11.2021);
Научно - методическим советом факультета автоматизированных и информационных систем учреждения образования «Гомельский государственный технический университет имени П.О. Сухого»
(протокол № 4 от 06.12.2021); УДф-02-18/42
Научно - методическим советом учреждения образования «Гомельский государственный технический университет имени П.О. Сухого»
(протокол № 2 от 07.12.2021).

Библиотека ГГТУ им. П.О. Сухого

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Учебная программа «Основы высшей алгебры» разработана в соответствии с образовательным стандартом высшего образования специальности: 1-40 04 01 «Информатика и технологии программирования».

Основные цели учебной дисциплины «Основы высшей алгебры»:

– дать фундаментальные знания по одному из основных разделов высшей математики, имеющему тесную связь с многочисленными приложениями в области информационных технологий;

– создать основы, необходимые для усвоения других естественнонаучных, общепрофессиональных и специальных дисциплин.

Основными задачами дисциплины являются:

– изучение методики построения алгебраических структур;

– усвоение внутренней логики, связывающей основные алгебраические структуры;

– приобретение аналитических навыков, необходимых для исследования и решения практических задач с привлечением современных методов алгебры.

Базой для изучения данной учебной дисциплины является дисциплина «Алгебра», изучаемая в средней школе. Методы, излагаемые в курсе «Основы высшей алгебры», используются при изучении дисциплин «Методы оптимизации и управления», «Системный анализ и исследование операций», «Линейная алгебра в приложениях» при изучении ряда общепрофессиональных и специальных дисциплин, а также дисциплин специализаций (в том числе и магистратуры).

В результате изучения учебной дисциплины «Основы высшей алгебры» у студента должны быть сформированы следующие *компетенции*:

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

– владение системным и сравнительным анализом;

– умение работать самостоятельно;

– обладание навыками, связанными с использованием технических устройств, управлением информацией и работой с компьютером;

– умение учиться, повышать свою квалификацию в течение всей своей жизни;

– использование основных законов естественнонаучных дисциплин и профессиональной деятельности;

– владение основными методами, способами и средствами получения, хранения, переработки информации с использованием компьютерной техники;

– умение работать в команде;

– владение современными технологиями анализа предметной области и разработки требований к создаваемым программным средствам, разработка математических моделей процессов, документации и спецификации для создания программного обеспечения;

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

Библиотека ГГТУ им. П.О.Сухого

– участие в научных исследованиях, связанных с разработкой новых или совершенствованием и развитием имеющихся математических моделей и программных средств.

В результате освоения дисциплины обучающийся должен

знать:

– понятия и принципы общей алгебры;

– основные положения теории групп, колец, полей;

уметь:

– строить математические модели практических задач на основе методов высшей алгебры;

– применять методы высшей алгебры в изучении криптографии и методов защиты информации;

владеть:

– приемами сведения практических задач к изученному математическому аппарату.

Тематический план учебной дисциплины

Согласно учебным планам на изучение дисциплины отведено:
Всего – 108 учебных часа, из них – 50 аудиторных часов. Распределение аудиторных часов по видам занятий: лекций – 26 часов, практических занятий – 24 часа. Трудоемкость учебной дисциплины – 3 зачетных единиц.

Общее количество часов и распределение аудиторного времени по видам занятий и семестрам

Форма получения высшего образования	Курс	Всего аудиторных часов	Лекции (часов)	Практич. занятия (часов)	Зачет, семестр	Экзамен, семестр	Тести-рование
дневная	1	50	26	24		2	

Библиотека ГГТУ им. П.О. Сухого

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Тема 2.1.	Делимость целых чисел.
Тема 2.2.	Простые числа. Взаимно простые числа. Диофантовы линейные уравнения.
Тема 2.3.	Сравнения целых чисел. Множество классов вычетов. Функция Эйлера.
Тема 2.4.	Взаимно однозначные соответствия. Мощность множества.
Тема 2.5.	Классические шифры.
Тема 2.6.	Понятие алгебраической системы. Группы. Подгруппы.
Тема 2.7.	Смежные классы. Нормальные подгруппы. Факторгруппы.
Тема 2.8.	Гомоморфизмы групп. Криптосистема RSA.
Тема 2.9.	Кольца. Подкольца и идеалы колец.
Тема 2.10.	Кольцо полиномов от одной переменной над полем.
Тема 2.11.	Неприводимость над полем и корни полиномов.
Тема 2.12.	Факторкольца. Поля Галуа.
Тема 2.13.	Характеристика кольца. Минимальные поля.

Библиотека ГГТУ им. П.О. Сухого

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА УЧЕБНОЙ ДИСЦИПЛИНЫ
(дневная форма получения образования)

Номер раздела, темы	Название раздела, темы	Количество аудиторных часов					Количество часов УСР	Форма контроля знаний
		Лекции	Практические занятия	Семинарские занятия	Лабораторные занятия	Иное		
1	2	3	4	5	6	7	8	9
Основы высшей алгебры								
2.1	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.	2	2					ПДЗ, Э
2.2	Простые числа и их свойства. Взаимно простые числа. Критерий взаимной простоты чисел. Основная теорема арифметики. Диофантовы линейные уравнения.	2	2					ПДЗ, Э
2.3	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.	2	2					ПДЗ, КР, Э
2.4	Взаимно однозначные соответствия. Мощность множества. Конечные, счетные, несчетные, континуальные множества и их свойства.	2	2					ПДЗ, Э
2.5	Шифры замены и перестановки. Примеры. Шифр Виженера и методы его дешифровки.	2	2					ПДЗ, Э
2.6	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.	2	2					ПДЗ, Э
2.7	Смежные классы и их свойства. Теорема Лагранжа и следствие из нее. Нормальные подгруппы. Критерий нормальности подгруппы. Факторгруппы и их свойства. Подстановки и их свойства. Симметрическая группа и ее основные свойства.	2	2					ПДЗ, КР, Э

Библиотека ГГТУ им. П.О. Сухого

2.8	Гомоморфизмы групп и их основные свойства. Теорема Кэли. Автоморфизмы групп и их свойства. Криптосистема RSA и система электронной цифровой подписи на ее основе.	2	2					ПДЗ, Э
2.9	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.	2	2					ПДЗ, Э
2.10	Кольцо полиномов от одной переменной над полем и его основные свойства. Делимость полиномов. НОД и НОК полиномов. Взаимно простые полиномы.	2	2					ПДЗ, КР, Э
2.11	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 не. Основная теорема алгебры и следствия из нее. Структура неприводимых полиномов над полем.	2	2					ПДЗ, КР, Э
2.12	Факторкольца и их свойства. Примеры факторколец. Структура факторкольца $P[x]/(f(x))$. Построение полей Галуа.	2	2					ПДЗ, Э
2.13	Гомоморфизмы колец и их основные свойства. Теорема существования корня и следствия из нее. Понятие характеристики кольца. Примеры колец и полей различных характеристик. Минимальные поля нулевой и ненулевой характеристики.	2	-					ПДЗ, Э
	ИТОГО по дисциплине	26	24					

Пояснения:
ПДЗ – проверка домашнего задания;
КР – контрольная работа;
Э – экзамен.

Библиотека ГГТУ им. П.О. Сухого

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

Основная литература

1. Головина, Л. И. Линейная алгебра и некоторые ее приложения / Л. И. Головина. – М. : Наука, 1979.
2. Ефимов, А. В. Сборник задач по математике для втузов. Ч. 1 : Линейная алгебра и основы математического анализа / А. В. Ефимов, Б. П. Демидович. – М. : Наука, 1993.
3. Гельфанд, И. М. Лекции по линейной алгебре / И. М. Гельфанд, - 5-е изд., испр. – М. : Добросвет, 1998.
4. Кострикин, А. И. Введение в алгебру / А. И. Кострикин. – М. : Наука, 1977.
5. Биркгоф, Г. Современная прикладная алгебра / Г. Биркгоф, Т. Барти ; пер. с англ. – М. : Мир, 1976.
6. Виноградов, И. М. Основы теории чисел / И. М. Виноградов. – 9-е изд., перераб. – М. : Наука, 1981.

Дополнительная литература

7. Проскуряков, И. В. Сборник задач по линейной алгебре / И. В. Проскуряков, - 12-е изд., стереотип. – СПб. : Лань, 2008.
8. Ленг, С. Алгебра / С. Ленг ; пер. с англ. – М. : Мир, 1968.
9. Липницкий, В. А. Современная прикладная алгебра. Математические основы защиты информации от помех и несанкционированного доступа : учеб. пособие / В. А. Липницкий. – Минск : БГУИР, 2005.
10. Ноден, П. Алгебраическая алгоритмика / П. Ноден, К. Китте. – М. : Мир, 1999.
11. Стройникова, Е. Д. Основы прикладной алгебры / Е. Д. Стройникова. – Минск : БГУИР, 2010.
12. Харин, Ю. С. Математические и компьютерные основы криптологии / Ю. С. Харин. – Минск : Новое знание, 2003.
13. Балдин, К.В. Высшая математика: учебник / К.В. Балдин, В.Н. Башлыков, А.В. Рукосуев; под общ. ред. К.В. Балдина. – 2-е изд., стер. – Москва: Флинта, 2016. – 361 с.: табл., граф., схем. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=79497.

Учебно-методические материалы

14. Бабич, А.А. Высшая алгебра [Электронный ресурс] : пособие по курсу "Математика. Геометрия и алгебра" для студентов специальности 1-40 04 01 "Информатика и технологии программирования" дневной формы обучения / А.А. Бабич; Учреждение образования "Гомельский государственный технический университет имени П. О. Сухого", Кафедра "Высшая математика". - Гомель : ГГТУ им. П.О. Сухого, 2020. - 64 с. https://elib.gstu.by/handle/220612/23805.
15. Высшая алгебра [Электронный ресурс]: практикум по курсу "Математика. Геометрия и алгебра" для студентов специальности 1-40 04 01 "Информатика и технологии программирования" дневной формы обучения / составители: А.А. Бабич, Н.Н. Бородин, А.В. Емелин; Учреждение образования "Гомельский государственный технический университет имени П. О. Сухого", Кафедра "Высшая математика".- Гомель: ГГТУ им. П.О. Сухого, 2020. - 27с. https://elib.gstu.by/handle/220612/22894

Библиотека ГГТУ им. П.О. Сухого

ВОПРОСЫ К ЭКЗАМЕНУ

по дисциплине «Основы высшей математики»

1-40 04 01 «Информатика и технологии программирования»

1. Множество целых чисел (основные аксиомы и свойства).
2. Принцип математической индукции. Принцип Дирихле.
3. Делимость целых чисел. Свойства операции деления.
4. Теорема Евклида о делимости целых чисел.
5. Наибольший общий делитель (НОД). Нахождение НОД по алгоритму Евклида.
6. Наименьшее общее кратное (НОК), его свойства и вычисление.
7. Взаимно простые числа. Критерий взаимной простоты.
8. Линейные диофантовые уравнения. Понятие частного и общего решения.
9. Матричный метод решения линейных диофантовых уравнений.
10. Простые числа и их свойства.
11. Основная теорема арифметики и ее следствия.
12. Сравнение целых чисел по натуральному модулю. Основные свойства сравнений.
13. Классы вычетов по модулю. Полная система вычетов. Приведенная система вычетов.
14. Функция Эйлера и ее свойства.
15. Формула для вычисления функции Эйлера. Примеры.
16. Теорема Эйлера. Малая теорема Ферма.
17. Сравнения первой степени. Теорема о разрешимости сравнений первой степени и ее следствия.
18. Системы сравнений первой степени. «Китайская» теорема об остатках.
19. Основные понятия криптографии. Шифры перестановки.
20. Шифры замены. Шифр Виженера.
21. Криптосистема RSA.
22. Общее определение алгебры. Сигнатура и тип алгебр. Полугруппа.
23. Определение группы. Общие свойства групп. Группы классов вычетов.
24. Определение подгруппы. Смежные классы и их свойства.
25. Теорема Лагранжа и ее следствия.
26. Циклические группы. Основные свойства циклических групп.
27. Симметрические группы. Основные свойства симметрических групп.
28. Циклы и транспозиции. Теорема о разложимости подстановок по циклам.
29. Знакопеременная подгруппа группы подстановок и ее свойства.
30. Классы сопряженных элементов группы и их свойства.
31. Нормальная подгруппа и ее свойства. Фактор-группа.
32. Гомоморфизмы групп и их свойства.
33. Ядро гомоморфизма групп. Теорема о гомоморфизме.
34. Изоморфизмы групп. Теорема Кэли.
35. Кольца, их основные типы и свойства. Примеры колец.
36. Мультипликативная группа кольца. Делители нуля.
37. Область целостности, тело и поле. Основные свойства полей. Примеры полей.
38. Подкольца, подполя. Идеалы колец, их виды.

Библиотека ГГТУ им. П.О. Сухого

39. Фактор-кольца и их свойства. Примеры фактор-колец.
40. Центр кольца и его свойства.
41. Гомоморфизмы колец и их основные свойства. Примеры гомоморфизмов колец.
42. Характеристика кольца. Примеры колец различных характеристик.
43. Минимальные поля нулевой и ненулевой характеристик.
44. Линейные системы над полем.
45. Кольцо полиномов от одной переменной над полем, его свойства.
46. Делимость полиномов. НОД и НОК полиномов. Взаимно простые полиномы.
47. Неприводимость над полем и теорема о разложении на множители в кольце полиномов.
48. Каноническое разложение полинома. Корни полинома и их кратность.
49. Теорема Безу и ее следствия.
50. Основная теорема алгебры, ее следствия. Структура неприводимых полиномов над полем.

Библиотека ГГТУ им.П.О.Сухого

ПЕРЕЧЕНЬ ТЕМ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

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

Методы (технологии) обучения

Основными методами (технологиями) обучения, отвечающими целям изучения дисциплины, являются:

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

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

Организация самостоятельной работы студента

При изучении дисциплины рекомендуется использовать следующие формы самостоятельной работы:

– выполнение домашних заданий в подготовке к практическим занятиям;
– изучение теоретического материала в процессе подготовки к лекциям;
– подготовка к контрольным работам;
– получение консультаций преподавателя по изучаемым вопросам;
– самостоятельная работа на базе электронного учебно-методического комплекса над определенными разделами учебной дисциплины;
– подготовка к экзаменам.

Диагностика компетенций студента

Типовым учебным планом по специальности в качестве формы текущей аттестации по учебной дисциплине «Основы высшей алгебры» предусмотрен экзамен. Оценка уровня знаний студента производится по десятибалльной шкале.

Для промежуточного контроля и самоконтроля знаний и умений студентов по данной учебной дисциплине допускается использование следующего диагностического инструментария:

– типовые задания;
– контрольные работы;
– устный опрос во время занятий;
– расчетно-графические работы;
–коллоквиумы.

Библиотека ГГУ им.Ф.Скорины

Протокол согласования программы с другими дисциплинами специальности на 20___/___ учебный год

Наименование дисциплины, с которой требуется согласование	Название кафедры	Предложения об изменениях в содержании учебной программы по изучаемой дисциплине	Принятое решение (протокол № , дата) кафедрой, разработавшей программу
1	2	3	4
Методы защиты информации	информатика	нет	№5 от 22.11.2021

Зав. кафедрой
«Высшая математика» _____ А.А.Бабич

Библиотека ГГТУ им.П.О.Сухого