

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Локтионова Оксана Геннадьевна
Должность: проректор по учебной работе
Дата подписания: 16.06.2023 12:27:40
Уникальный программный ключ:
0b817ca911e6668abb13a5d426d39e5f1c11eabbf73e943df4a4851fda56d089

МИНОБРАЗОВАНИЯ И НАУКИ РОССИИ

Федеральное государственное бюджетное образовательное
учреждения высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ

Проректор по учебной работе

 О.Г. Локтионова
« 5 » 03 (ЮЗГУ) 2019 г.



АЛГЕБРА И ТЕОРИЯ ЧИСЕЛ

Методические указания по выполнению самостоятельной
работы для студентов направления подготовки бакалавриата
02.03.03 «Математическое обеспечение и администрирование
информационных систем»

Курск 2019

УДК 511, 512

Составитель: В.П. Добрица

Рецензент

Кандидат технических наук, доцент кафедры
«Информационные системы и технологии» Ю.А. Халин

Алгебра и теория чисел: методические указания по выполнению самостоятельной работы / Юго-Зап. гос. ун-т; сост.: В.П. Добрица. – Курск, 2019. – 21 с.: табл. 5. – Библиогр.: с. 20.

Содержатся сведения о темах для самостоятельного изучения по дисциплине «Алгебра и теория чисел», необходимые для успешного освоения дисциплины. Указывается порядок выполнения самостоятельной работы всех предусмотренных учебным планом видов, приводятся рекомендации по оформлению результатов работы.

Методические указания соответствуют требованиям программы, утвержденной учебно-методическим объединением по специальности.

Предназначены для студентов направления подготовки бакалавриата 02.03.03 «Математическое обеспечение и администрирование информационных систем».

Текст печатается в авторской редакции

Подписано в печать 5.03.19. Формат 60x84 1/16.
Усл.печ. л. 1,34. Уч.-изд. л. 1,21. Тираж 100 экз.

Заказ. 182 Бесплатно.

Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

Содержание

1 Введение.....	4
2 Учебно-методическое обеспечение для самостоятельной работы.....	6
3 Запланированные виды самостоятельной работы по дисциплине.....	7
4 Оценивание знаний, умений, навыков.....	13
5 Рекомендации по выполнению самостоятельной работы.....	15
6 Контрольные вопросы для самоконтроля.....	16
7 Библиографический список.....	20

1 Введение

Самостоятельная работа - это индивидуальная или коллективная учебная деятельность, осуществляемая без непосредственного руководства преподавателя, но по его заданиям и под его контролем.

Самостоятельная работа студентов включает:

- изучение лекционного материала по конспекту с использованием рекомендованной литературы;
- отработку изучаемого материала по печатным и электронным источникам, конспектам лекций;
- подготовку к выполнению практических работ;
- выполнение отчетов по практическим работам и подготовку к их защите;
- индивидуальные задания (решение задач, подготовка сообщений, докладов, исследовательские работы и т.п.);
- работу над творческими заданиями;
- подготовку кратких сообщений, докладов, рефератов, самостоятельное составление задач по изучаемой теме (по указанию преподавателя).

Назначение самостоятельной работы студентов.

- **Овладение знаниями**, что достигается:

чтением текста (учебника, первоисточника, дополнительной литературы), составлением плана текста, графическим структурированием текста, конспектированием текста, выписками из текста, работой со словарями и справочниками, поиском информации в сети Интернет и т.п.;

- **закрепление знаний**, что достигается:

работой с конспектом лекций, обработкой текста, повторной работой над учебным материалом (учебником, первоисточником, дополнительной литературой), составлением плана, составлением таблиц для систематизации учебного материала, ответами на контрольные вопросы, заполнением рабочей тетради, аналитической обработкой текста (аннотирование, рецензирование,

реферирование, конспект-анализ и др), составлением библиографии и т.п.;

- *формирование навыков и умений*, что достигается:

решением задач и упражнений по образцу, решением вариативных задач, выполнением схем, выполнением расчетов, решением ситуационных задач, подготовкой к дискуссиям, проектированием и моделированием разных видов и компонентов профессиональной деятельности, математическим описанием опытно экспериментальной работой и т.п.

Самостоятельная работа может осуществляться индивидуально или группами студентов в зависимости от поставленной цели, объема, конкретной тематики самостоятельной работы, уровня сложности, уровня умений студентов.

Контроль результатов внеаудиторной самостоятельной работы студентов может осуществляться в пределах времени, отведенного на обязательные учебные занятия по дисциплине и внеаудиторную самостоятельную работу студентов по дисциплине, может проходить в письменной, устной или смешанной форме.

Текущий контроль качества выполнения самостоятельной работы может осуществляться с помощью:

- контрольного опроса;
- собеседования;
- автоматизированного программированного контроля (машинного контроля, тестирования с применением ЭВМ).

Контроль выполнения индивидуальных заданий осуществляется поэтапно в соответствии с разработанным преподавателем графиком.

2 Учебно-методическое обеспечение для самостоятельной работы

Студенты могут при самостоятельном изучении отдельных тем и вопросов дисциплины пользоваться учебно-методическими пособиями и методическими разработками кафедры в рабочее время, установленное Правилами внутреннего распорядка работников.

Учебно-методическое обеспечение для самостоятельной работы обучающихся по данной дисциплине организуется:

библиотекой университета:

- библиотечный фонд укомплектован учебной, методической, периодической, справочной литературой в соответствии с Учебным планом (УП) и Рабочей программой данной дисциплины (РПД);

- имеется доступ к основным информационным образовательным ресурсам, информационной базе данных, в том числе библиографической, возможность выхода в Интернет;

кафедрой:

- путем обеспечения доступности всего необходимого учебно-методического и справочного материала;

- путем предоставления сведений о наличии учебно-методической литературы, современных программных средств;

- путем разработки:

- заданий для самостоятельной работы;

- вопросов к экзамену;

- тестов;

- методических указаний к выполнению практических работ и

т.д.;

типографией университета:

- помощь авторам в подготовке и издании научной, учебной и методической литературы;

- удовлетворение потребности в тиражировании научной, учебной и методической литературы.

3 Запланированные виды самостоятельной работы по дисциплине

В соответствии с учебным планом, на самостоятельную работу студентов в рамках дисциплины «Алгебра и теория чисел» отводится 105,7 часов. Распределение часов самостоятельной работы по темам (видам деятельности) приведено в рабочей программе дисциплины (Таблица 4.3).

В таблице 1 ниже приведены соответствующие сведения, взятые из Рабочей программы дисциплины.

Таблица 1 – Самостоятельная работа студентов в соответствии с рабочей программой дисциплины

№ раздела (темы)	Наименование раздела учебной дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час.
1	2	3	4
1	Вводная по дисциплине Алгебра и теория чисел	1-3 неделя	16
2	Алгоритм Евклида	5-8 недели	36
3	Простые числа и "основная" теорема арифметики	9-10 недели	17,7
4	Важнейшие функции в теории чисел	11-12 недели	18
5	Конечные цепные дроби.	13-18 недели	18
Итого			105,7

Текущий контроль знаний, основанный на выяснении качества самостоятельной работы студентов при работе с конспектом лекций и учебной основной и дополнительной литературой, производится в соответствии с Рабочей программой дисциплины (Таблица 7.3) и предусматривает контрольный опрос (КО) и собеседование (С).

В таблице ниже приведены соответствующие сведения, взятые из Рабочей программы дисциплины.

Таблица 2 – Формы текущего контроля в соответствии с рабочей программой дисциплины

№ п/п	Раздел (тема) дисциплины	Код контролируемой компетенции (или её части)	Технология формирования	Оценочные средства		Описание шкал оценивания
				наименование	№№ заданий	
1	2	3	4	5	6	7
1	Вводная по дисциплине Алгебра и теория чисел	ОПК – 1	Лекция, СРС, ЛР	С Защита ЛР №1	1-10 1-2	Согласно табл. 7.2
2	Алгоритм Евклида	ОПК – 1	Лекция, СРС, ЛР, ПР	С, Защита ЛР №2 Защита ПР №1	11-18 1-2 1-3	Согласно табл. 7.2
3	Простые числа и "основная" теорема арифметики	ОПК – 1	Лекция, СРС, ЛР, ПР	С, Защита ЛР №3 Защита ПР №2	19-31 1-3 1-2	Согласно табл. 7.2
4	Важнейшие функции в теории чисел	ОПК – 1	Лекция, СРС, ПР	С, Защита ПР №3	32-49 1-3	Согласно табл. 7.2
5	Конечные цепные дроби.	ОПК – 1	Лекция, СРС, ПР	С, Защита ПР №4	50-86 1-4	Согласно табл. 7.2

Лекционные занятия проводятся в соответствии с Рабочей программой дисциплины (Таблица 4.1.1) и включают следующие темы.

Таблица 3 – Краткое содержание лекционного курса

№ п/п	Раздел (тема) дисциплины	Содержание
1.	Вводная по дисциплине Алгебра и теория чисел	Предмет, цели и содержание читаемого курса. Числовые системы. Основная теорема о делимости целых чисел. Наибольший общий делитель. Алгоритм Евклида нахождения НОД чисел a, b
2.	Алгоритм Евклида	Алгоритм Евклида нахождения НОД чисел a, b . Линейное представление НОД. Расширенный алгоритм Евклида. Наименьшее общее кратное (НОК) и его свойства. Основная теорема арифметики
3.	Простые числа и "основная" теорема арифметики	Простые числа. Основные теоремы. Решето Эратосфена. Основная теорема арифметики.
4.	Важнейшие функции в теории чисел	Целая и дробная часть. Функция Эйлера.
5.	Конечные цепные дроби.	Разложение в правильную цепную дробь. Подходящие дроби, их свойства. Свойства подходящих дробей.

Основная литература для освоения дисциплины включает источники [1-3], дополнительная литература включает источники [4-10].

Практические и лабораторны занятия, предусмотренные Рабочей программой дисциплины, описаны в таблице 4.2.1 и 4.2.2.

Таблица 4.2.1 – Практические занятия

Номер занятия	Наименование практического (семинарского) занятия	Объем в часах
1	2	3
1	1) Делимость в кольце целых чисел. Теорема о делении с остатком. Алгоритм Евклида и наибольший общий делитель	6
2	Делимость в кольце целых чисел. Простые числа. Решето Эратосфена	4
3	2) Числовые функции и их свойства.	4
4	3) Непрерывные (цепные) дроби	4
	Всего	18 часов

Таблица 4.2.2 – Лабораторные работы

Номер занятия	Наименование практического (семинарского) занятия	Объем в часах
1	2	3
1	4) Сравнение по модулю	4
2	5) Системы вычетов	8

3	6) Сравнение первой степени	6
	Всего	18 часов

Рекомендации по выполнению практических заданий приведены в соответствующих методических [1]. Методические указания содержат полные требования к видам и объему самостоятельной работы при подготовке, выполнении, оформлении отчетов и защите работ.

4 Оценивание знаний, умений, навыков

Процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций, регулируются следующими нормативными актами университета:

- положение П 02.016–2018 Обально-рейтинговой системе оценивания результатов обучения по дисциплинам (модулям) и практикам при освоении обучающимися образовательных программ;
- методические указания, используемые в образовательном процессе, указанные в списке литературы.

Для *текущего контроля успеваемости* по дисциплине в рамках действующей в университете балльно-рейтинговой системы применяется следующий порядок начисления баллов:

Таблица 7.4 – Порядок начисления баллов в рамках БРС

Форма контроля	Минимальный балл		Максимальный балл	
	балл	примечание	балл	примечание
Выполнение лабораторной работы №1	2	Выполнил, но «не защитил»	4	Выполнил и «защитил»
Выполнение лабораторной работы №2	2	Выполнил, но «не защитил»	4	Выполнил и «защитил»
Собеседование	2	Доля правильных ответов 50%	4	Доля правильных ответов 90%

Выполнение лабораторной работы №3	2	Выполнил, но «не защитил»	4	Выполнил и «защитил»
Собеседование	2	Доля правильных ответов 50%	4	Доля правильных ответов 90%
Выполнение практической работы №1	2	Выполнил, но «не защитил»	4	Выполнил и «защитил»
Собеседование	2	Доля правильных ответов 50%	4	Доля правильных ответов 90%
Выполнение практической работы №2	2	Выполнил, но «не защитил»	4	Выполнил и «защитил»
Выполнение практической работы №3	2	Выполнил, но «не защитил»	4	Выполнил и «защитил»
Собеседование	2	Доля правильных ответов 50%	4	Доля правильных ответов 90%
Выполнение практической работы №4	2	Выполнил, но «не защитил»	4	Выполнил и «защитил»
Собеседование	2	Доля правильных ответов 50%	4	Доля правильных ответов 90%
Всего	24		48	
Посещаемость	0		16	
Сдача экзамена			36	
ИТОГО	18		100	

Для промежуточной аттестации обучающихся, проводимой в виде тестирования, используется следующая методика оценивания знаний, умений, навыков и (или) опыта деятельности. В каждом варианте КИМ –16 заданий (15 вопросов и одна задача).

Каждый верный ответ оценивается следующим образом:

- задание в закрытой форме – 2 балла,
- задание в открытой форме – 2 балла,
- задание на установление правильной последовательности – 2 балла,
- задание на установление соответствия – 2 балла,
- решение компетентностно-ориентированной задачи – 6 баллов.

Максимальное количество баллов за тестирование – 36 баллов.

5 Рекомендации по выполнению самостоятельной работы

Изучение теоретических основ дисциплин

Изучение теоретической части дисциплин способствует углублению и закреплению знаний, полученных на аудиторных занятиях, а также развивает у студентов творческие навыки, инициативу и умение рационально организовать свое время.

Самостоятельная работа при изучении дисциплины включает:

- работу над конспектом лекций;
- изучение рекомендованной литературы;
- поиск и ознакомление с информацией в сети Интернет;
- подготовку к различным формам контроля (контрольный опрос, собеседование, тесты);
- подготовку ответов на вопросы по различным темам дисциплины, в том числе заданным преподавателем по результатам контроля знаний.

Материал, законспектированный в течение лекций, необходимо регулярно прорабатывать и дополнять сведениями из других источников и литературы.

При освоении дисциплины сначала необходимо по каждой теме изучить рекомендованную литературу и составить краткий конспект основных положений, терминов, сведений, требующих запоминания и являющихся основополагающими в этой теме для освоения последующих тем курса. После этого следует разобраться с обоснованием утверждений. Для расширения знаний по дисциплине рекомендуется использовать Интернет-ресурсы; проводить поиски в различных системах и использовать материалы сайтов, рекомендованных преподавателем.

По требованию преподавателя конспект лекций предоставляется ему для проверки. Замеченные недостатки и внесенные замечания и предложения следует отработать в приемлемые сроки.

Выполнение практических заданий

При подготовке и защите практических заданий необходимо обращать особое внимание на полноту и грамотность выполнения отчета по работе, наличие в них кратких обоснований принимаемых решений и выводов по результатам работы. При несоответствии отчета этим требованиям преподаватель может возвращать его на доработку. При опросе студентов основное внимание обращается на усвоение ими основных теоретических положений, на которых базируется данная работа, и понимание того, как эти положения применяются на практике. Для освоения дисциплины в полном объеме студенту необходимо посещать все аудиторные занятия и самостоятельно прорабатывать полученный материал.

Контроль результатов самостоятельной работы студентов осуществляется перед выполнением практических заданий, в процессе защиты отчета по работе, а так же на зачете.

При самостоятельном изучении дисциплины, подготовке к аудиторным занятиям и выполнении домашних заданий студенты должны использовать рекомендованную учебную литературу и учебно-методические указания. Источники информации доступны на сайте кафедры.

Самостоятельная работа осуществляется при подготовке к работе в соответствии с заданными темами, подготовке ответов к вопросам для самоконтроля и контрольным вопросам.

Отчет по практическим заданиям выполняется индивидуально или один на бригаду по решению преподавателя.

Отчет должен содержать все предусмотренные методическими указаниями разделы, включая задания и краткое изложение необходимого теоретического материала.

6 Контрольные вопросы для самоконтроля

1. Последовательность расширения понятия числа.
2. Различные подходы к изучению свойств чисел.
3. Теорема деления целых чисел с остатком.
4. Делимость чисел и её свойства.
5. Простые и составные числа. Свойства.
6. Решето Эратосфена.
7. Теорема Евклида о бесконечности множества простых чисел.
8. Каноническое представление целого числа.
9. Условие делимости чисел при их каноническом представлении.
10. Число натуральных делителей натурального числа.
11. Сумма натуральных делителей целого числа.
12. Наибольший общий делитель его единственность и существование.
13. Свойства НОД.
14. Алгоритм Евклида нахождения НОД двух чисел.
15. Линейное представление НОД нескольких целых чисел.
16. Взаимно простые числа и их свойства.
17. Наименьшее общее кратное целых чисел.
18. Свойства НОК.
19. Распределение простых чисел. Асимптотические оценки.
20. Простые числа в арифметических прогрессиях.
21. Сравнения и их свойства.
22. Классы вычетов и их свойства.
23. Функция Эйлера и её свойства.
24. Теорема Ферма.
25. Теорема Эйлера.
26. Мультипликативно обратные по модулю элементы.
27. Сравнения первой степени и способы их решения.
28. Системы сравнений первой степени.
29. Китайская теорема об остатках.
30. Первообразные корни и их свойства.
31. Дискретные логарифмы.
32. Решение показательных и степенных сравнений.
33. Сравнения второй степени.

34. Символы Лежандра и Якоби и их свойства.
35. Квадратичные вычеты и невычеты и их свойства.
36. Непрерывные дроби. Свойства.
37. Разложение рациональных чисел в цепные дроби.
38. Подходящие дроби и их свойства.
39. Подходящие дроби как наилучшие приближения действительных чисел.
40. Свойства наилучших приближений действительных чисел.
41. Группа и её свойства.
42. Подгруппы и их свойства.
43. Циклические группы и подгруппы.
44. Таблицы Кэли.
45. Классы смежности и их свойства.
46. Теорема Лагранжа.
47. Гомоморфизм групп и его свойства.
48. Фактор-группа.
49. Группа перестановок.
50. Теорема Кэли.
51. Действие группы на множестве.
52. Лемма Беренсайда.
53. Транзитивные группы.
54. Кольца и их свойства.
55. Область целостности и её свойства.
56. Поля и их свойства.
57. Подкольца и их свойства.
58. Идеалы кольца и их свойства.
59. Фактор-кольца.
60. Гомоморфизм колец и их свойства.
61. Характеристика кольца.
62. Центр кольца.
63. Евклидовы кольца и их свойства.
64. Конечные расширения полей и их свойства.
65. Алгебраические элементы. Свойства.
66. Схема Горнера. Нахождение целых корней многочленов.
67. Порядки неприводимых многочленов.
68. Поле разложения многочлена.
69. Конечные поля (поля Галуа).

70. Эллиптические кривые над полем.
71. Уравнение Вейерштрасса.
72. Алгебраически замкнутое поле.
73. Алгебраическое расширение поля.
74. Алгебраическое замыкание поля.
75. Теорема Штейница.
76. Аффинные, F -рациональные и точки эллиптической кривой.
77. Невырожденная эллиптическая кривая.
78. Дискриминант и j -инвариант эллиптической кривой.
79. Изоморфизм эллиптических кривых.
80. Проективная плоскость. Проективная точка. Бесконечно удаленная точка.
81. Теорема Виета для кубического уравнения.
82. Сложение точек на эллиптической кривой. Его геометрический смысл.
83. Эллиптические кривые над конечными полями.
84. ζ -функция эллиптической кривой над полем Галуа.
85. Теорема Хассе.
86. Теорема Ленстры.

8 Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

8.1 Основная учебная литература

1. Хаггарти, Р. Дискретная математика для программистов [Электронный ресурс] : учебное пособие / Р. Хаггарти ; пер. англ. под ред. С. А. Кулешов ; пер. с англ. А. А. Ковалев, В. А. Головешкин, М. В. Ульянов. - Изд. 2-е, испр. - М. : Техносфера, 2012. - 400 с. - Режим доступа : biblioclub.ru

2. Судоплатов, С. В. Дискретная математика [Электронный ресурс]: учебник / С. В. Судоплатов, Е. В. Овчинникова. - 4-е изд. - Новосибирск : НГТУ, 2012. - 278 с. – Режим доступа : biblioclub.ru

3. Кнауб, Л. В. Теоретико-численные методы в криптографии [Электронный ресурс] : учебное пособие / Л. В. Кнауб, Е. А. Новиков, Ю. А. Шитов; Министерство образования и науки Российской Федерации, Сибирский Федеральный университет. - Красноярск: Сибирский федеральный университет, 2011. - 160 с. - Режим доступа: biblioclub.ru

8.2 Дополнительная учебная литература

1 Кострикин, А. И. Введение в алгебру. Основы алгебры [Текст] : учебник для студ. ун-тов / А. И. Кострикин. - М. : Физматлит, 1994. - 320 с.

2 Милых, В. А. Дискретная математика [Электронный ресурс] : учебное пособие / Курск. гос. техн. ун-т; Министерство образования и науки Российской Федерации, Курский государственный технический университет. - Курск: КурскГТУ, 2006. - 139 с.

3 Милых, В. А. Дискретная математика [Текст] : учебное пособие / В. А. Милых, И. Г. Уразбахтин; Курский государственный технический университет, Гуманитарно-технический институт (г. Курск). - Курск: КурскГТУ, 2006. - 139 с.

4 Роджерс, Х. Теория рекурсивных функций и эффективная вычислимость [Текст] / пер. с англ. В. А. Душского; под ред. В. А. Успенского. - Москва: Мир, 1972. - 624 с.

5 Панкратова, В. Г. Теория чисел [Текст]: конспект лекций / Калининский гос. ун-т. - Вып. 3. - Калинин: [б. и.], 1972. - 58 с.

6 Зуланке, Р. Алгебра и геометрия [Текст] : учебник / Р. Зуланке; А. Л. Онищик. - М. : МЦНМО, 2008. - Т. 2: Модули и алгебры. - 336 с.

7 Биркгоф, Гаррет. Современная прикладная алгебра [Текст] / пер. с англ. Ю. И. Манина. - М. : Мир, 1976. - 400 с.

8.3 Перечень методических указаний

9 Алгебра и теория чисел [Электронный ресурс] : методические указания к практическим занятиям для бакалавров направления 02.03.03 Математическое обеспечение и администрирование информационных систем / Юго-Зап. гос. ун-т ; сост.: В. П. Добрица, Ю. А. Халин. - Курск : ЮЗГУ, 2019. – 26 с.

10 Алгебра и теория чисел [Электронный ресурс] : методические указания к лабораторным занятиям для бакалавров направления 02.03.03 Математическое обеспечение и администрирование информационных систем / Юго-Зап. гос. ун-т ; сост.: В. П. Добрица, Ю. А. Халин. - Курск : ЮЗГУ, 2019. - 28 с.

11 Добрица, В. П. Алгебра и теория чисел [Электронный ресурс] : методические указания по выполнению самостоятельной работы для студентов направления подготовки бакалавриата 02.03.03 «Математическое обеспечение и администрирование информационных систем» / Юго-Зап. гос. ун-т ; сост. В. П. Добрица. - Курск : ЮЗГУ, 2019. - 21 с.