Программа учебной дисциплины: Алгебра

Утверждена

Кафедрой компьютерной

безопасности МИЭМ НИУ ВШЭ

Протокол № 5 от «24» июня 2019 г.

Академическим советом ОП 25.06.2019 г.

Автор	Рожков М.И. (rozhkov.m.i@yandex.ru)
Число кредитов	3
Контактная работа (час.)	56
Самостоятельная работа (час.)	58
Курс	2 курс 1,2 модуль
Формат изучения дисциплины	Без использования онлайн курса

I. ЦЕЛЬ, РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ И ПРЕРЕКВИЗИТЫ

Целью освоения дисциплины является формирование у студентов следующих навыков, необходимых для решения предусмотренных программой специальности 10.05.01 "Компьютерная безопасность" профессиональных задач:

- Применение соответствующего математического аппарата для формализации, анализа и решения проблем, возникающих в ходе профессиональной деятельности
- Решение систем линейных уравнений над полем и кольцом вычетов
- Проведение эффективных вычислений в кольцах вычетов и кольцах многочленов

В результате освоения дисциплины студент должен:

Знать:

- Основные определения, понятия и свойства конечных групп, колец и полей
- Условия и методы разложения конечных групп и колец вычетов в прямую сумму
- Методы решения линейных и квадратных уравнений над кольцами вычетов
- Формулировки китайской теоремы об остатках для чисел и многочленов
- Свойства конечных полей и их подполей
- Методы построения примитивных элементов конечного поля
- Строение поля разложения для неприводимого многочлена над конечным полем
- Методы оценки периодов многочленов над конечным полем

Уметь:

- Проводить вычисления в числовых и конечных группах, кольцах вычетов и полях
- Находить число решений (и сами решения) линейных и квадратных уравнений над кольцами вычетов

– Вычислять периоды многочленов над конечным полем

– Устанавливать изоморфизм заданного кольца вычетов с прямой суммой колец вычетов

Иметь навыки (приобрести опыт):

– Проведения вычислений в числовых и конечных группах, кольцах вычетов и полях

– Нахождения корней многочленов в конечном поле

– Вычисления периода многочленов над конечным полем

Настоящая дисциплина относится к циклу математических и естественно-научных дисциплин и блоку дисциплин, обеспечивающих базовую подготовку.

Для освоения учебной дисциплины, студенты должны владеть следующими знаниями и компетенциями:

- Школьными знаниями и компетенциями.
- Основными понятиями линейной алгебры и теории множеств.

Основные положения дисциплины должны быть использованы в дальнейшем при изучении следующих дисциплин:

- Криптографические методы защиты информации
- Криптографические протоколы
- Теоретико-числовые методы в криптографии

II. СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Тема 1. Группа, подгруппа, нормальный делитель, факторгруппа. Примеры на основе групп (Z,+), (Zn,+), (Zn*,·), Sn.

Тема 2. Отношение эквивалентности, смежные классы по подгруппе как классы эквивалентности. Примеры на основе групп (Z,+), (Zn,+), (Zn*,·), Sn.

Тема 3. Порядок элемента группы, циклическая группа, описание множества образующих элементов циклической группы (Zn,+).

Тема 4. Гомоморфизм групп, ядро гомоморфизма. Примеры на основе групп (Z,+), (Zn,+), (Zn*,·), Sn.

Тема 5. Характеры групп.

Тема 6. Внешнее и внутреннее прямое произведение (сумма) групп. Примеры на основе групп (Z,+), (Zn,+), (Zn*,·), Sn.

Тема 7. Кольцо, подкольцо, идеал, фактор-кольцо. Примеры на основе колец Z, Zn, F[x], F[x]/f(x).

Тема 8. Характеристика кольца, делители нуля, обратимые элементы. Примеры на основе колец Z, Zn, F[x], F[x]/f(x).

Тема 9. Гомоморфизм и изоморфизм колец. Примеры на основе колец Z, Zn, F[x], F[x]/f(x).

Тема 10. Кольцо многочленов F[x] над полем F, деление с остатком, формула для остатка от деления многочлена f(x) на одночлен (x-a), критерий отсутствия кратных корней у многочлена над полем, оценка числа различных корней.

Тема 11. Кольцо многочленов F[x]/f(x) над полем F по модулю заданного многочлена f(x), критерий отсутствия в данном кольце делителей нуля.

Тема 12. Критерий мультипликативной обратимости и методы нахождения обратного элемента для колец Zn и F[x]/f(x).

Тема 13. Неприводимые многочлены, критерий неприводимости для многочленов степени ≤ 3, описание всех неприводимых многочленов степени ≤ 3 над полем из двух элементов.

Тема 14. Идеалы колец $K \in \{Z, Zn, F[x], F[x]/f(x)\}$. Доказательство того, что каждый идеал этих колец является главным идеалом. Критерий совпадения идеала $J=a \cdot K$ с кольцом K.

Тема 15. Критерий максимальности идеалов $J=a \cdot K$.

Тема 16. Китайская теорема об остатках для чисел и многочленов.

Тема 17. Условия разложимости кольца $K \in \{Zn, F[x]/f(x)\}$ в прямую сумму колец.

Тема 18. Методы решения уравнений (оценки числа решений) и нахождения мультипликативных порядков элементов в кольце $K \in \{Zn, F[x]/f(x)\}$ (критерий наличия решений уравнения $ax=b$, оценка числа решений данного уравнения, связь с решениями уравнения $ax=0$).

Тема 19. Основные понятия и свойства теории конечных полей.

Тема 20. Описание конечного поля GF(q) как поля разложения многочлена $x^q-x=0$.

Тема 21. Описание подполей конечного поля GF(q).

Тема 22. Алгебраические элементы поля над заданным подполем. Минимальный многочлен алгебраического элемента и его свойства.

Тема 23. Поле разложения неприводимого многочлена над конечным полем.

Тема 24. Примитивные элементы конечного поля (теорема существования, число примитивных элементов, описание всех примитивных элементов через степени одного из них, алгоритмы проверки примитивности элементов поля, примеры на основе полей Zp и F[x]/f(x)).

Тема 25. Функция след и ее свойства.

Тема 26. Квадратичные вычеты и невычеты в поле Zp (описание через степени примитивного элемента, доказательство равномощности множеств вычетов и невычетов).

Тема 27. Символы Лежандра и Якоби, формула Эйлера (использование для проверки неприводимости квадратного многочлена над полем Zp).

Тема 28. Период многочлена над конечным полем. Методы нахождения периода многочлена, многочлены максимального периода.

Тема 29. Методы нахождения корней многочленов над полем Zp.

III. ОЦЕНИВАНИЕ

Формы контроля:

Тип контроля	Форма контроля	2 курс		Примечания
		1 модуль	2 модуль	
Промежуточный	Контрольная работа	*		
Итоговый	Экзамен в устной форме		*	

На втором курсе письменная контрольная работа проводится на 7 неделе модуля. На контрольной работе студент должен продемонстрировать освоение тематических разделов дисциплины, относящихся к навыкам проведения вычислений в конечных группах, кольцах вычетов и конечных полях.

В 1 модуле контрольная состоит из 10 задач. Каждая верно решенная задача (имеется верный ответ и все необходимые корректные обоснования, приведшие к нему) оценивается в 1 балл. При наличии грубых ошибок в решении (отсутствует, непонятна либо некорректна часть необходимых обоснований или расчетов, в том числе при верном итоговом ответе, отсутствие итогового ответа) задача считается нерешенной и оценивается в 0 баллов (равно как и задача, решение которой полностью отсутствует). В остальных случаях (по усмотрению преподавателя) задача может быть оценена в 0.5 балла. Например, итоговый ответ: «многочлен $f(x)=x^3+1$ неприводим» - неверен, однако в приведенном обосновании студент сформулировал правильное понимание понятия неприводимости многочлена, верно установил, что данный многочлен есть произведение многочленов $g(x)=x+1$ и $h(x)=x^2-x+1$, степени которых меньше, чем степень многочлена $f(x)$, и на основании этого явно и верно указал на приводимость многочлена $f(x)$. Т.е. ошибка появилась исключительно на этапе переписывания коректно полученного верного результата в графу «Ответ».

Округление итоговой оценки за контрольную работу – арифметическое.

Во 2 модуле контрольная состоит из 15 задач. Приводятся только ответы к задачам. Задача считается решенной, если приведен верный ответ. Все необходимые обоснования, которые использовались при получении ответа, хранятся у студента и могут быть им использованы при защите полученных ответов на экзамене. Оценка за контрольную работу зависит от числа решенных задач следующим образом:

Число решенных задач	≥ 14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Баллы	10	9	8	7	6	5	4	3	3	3	2	2	1	1	0

Экзамен по итогам 2 модуля проводится в форме собеседования по теоретическим вопросам, которые использовались студентом при решении задач контрольной работы, и заключается в защите студентом своих результатов по каждой решенной задаче контрольной работы. Каждая такая защита добавляет 1 балл к результату зкзамена. Студент должен продемонстрировать знание и умение пользоваться на практике соответствующими теоретическими результатами, знание определений и терминов. Для проверки указанных знаний студенту может быть предложено решить одну или несколько дополнительных практических задач, решение которых не связано с проведением сложных вычислений. Если студент на экзамене не демонстрирует необходимых знаний и навыков, которые должны были им использоваться при решении положительно оцененной задачи контрольной работы, данная задача оценивается в 0 баллов (и ничего не добавляет к результату зкзамена). Студент имеет право на дополнительный вопрос или задачу (в рамках полной программы дисциплины), правильный ответ на который оценивается в 1 дополнительный балл, а неверный ответ к уменьшению оценки на 1 балл.

Результирующая оценка 2 модуля есть среднее арифметическое накопленной оценки (оценки за контрольную работу в 1 модуле) и оценки за экзамен. При необходимости Округления студенту может быть предложен дополнительный вопрос в рамках учебной программы.

На экзамене студент, по уважительной причине не выполнявший контрольную работу, по согласованию с преподавателем может выполнить ее во время экзамена. При этом студент обязан предупредить преподавателя об этом заранее (не позднее суток до начала экзамена) и к началу экзамена подойти к преподавателю за вариантом контрольной работы с тем, чтобы после отведенного времени на ее выполнение (80 мин.) оставалось время для ее проверки и принятия (на основе ее результатов) экзамена до завершения отведенного на экзамен времени.

В противном случае на экзамене у такого студента проверяются как теоретические знания, так и практические навыки решения задач по всей программе дисциплины на усмотрение преподавателя.

1. Основная литература

– Рожков М.И. Алгебра. Основы теории конечных групп, колец, полей. Учебное пособие. М., МГИЭМ, 2009. – 82 с.

2. Дополнительная литература

- Глухов М.М., Елизаров В.П., Нечаев А.А. Алгебра: Учебник. В 2-х т. М.:Гелиос АРВ, 2003. – 336 с.
- Лидл Р., Нидеррайтер Г. Конечные поля: в 2-х т. М.: Мир, 1988. – 430 с.

3. Программное обеспечение

Не требуется

4. Профессиональные базы данных, информационные справочные системы, интернет-ресурсы (электронные образовательные ресурсы)

Не требуется

5. Материально-техническое обеспечение дисциплины

Учебные аудитории для лекционных занятий по дисциплине обеспечивают использование и демонстрацию тематических иллюстраций, соответствующих программе дисциплины в составе:

- ПЭВМ с доступом в Интернет (операционная система, офисные программы, антивирусные программы);
- мультимедийный проектор с дистанционным управлением.

Учебные аудитории для лабораторных и самостоятельных занятий по дисциплине оснащены компьютерами, с возможностью подключения к сети Интернет и доступом к электронной информационно-образовательной среде НИУ ВШЭ.