МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Ярославский государственный университет им. П.Г. Демидова
Математический факультет

УТВЕРЖДАЮ

Проректор по развитию образования
_____Е.В.Сапир

"_____"_____2012 г.

Рабочая программа дисциплины послевузовского профессионального образования (аспирантура)

Алгебраические и теоретико-числовые методы в криптографии

по специальности научных работников

01.01.06 Математическая логика, алгебра и теория чисел

Ярославль 2012

1. Цели освоения дисциплины

Целями освоения дисциплины «Алгебраические и теоретико-числовые методы в криптографии» в соответствии с общими целями основной профессиональной образовательной программы послевузовского профессионального образования (аспирантура) (далее - образовательная программа послевузовского профессионального образования) являются:

- усвоение аспирантами знаний об основных алгебраических структурах, об основных понятиях, проблемах и методах алгебры, теории чисел, алгебраической геометрии и комбинаторной теории групп;
- изучение вопросов применения понятий и методов алгебраической геометрии и комбинаторной теории групп в криптографии;
- формирование у аспирантов общей математической культуры.

2. Место дисциплины в структуре ООП послевузовского профессионального образования (аспирантура)

Дисциплина «Алгебраические и теоретико-числовые методы в криптографии» относится к разделу «Обязательные дисциплины» (подраздел «Дисциплины по выбору аспиранта») образовательной составляющей образовательной программы послевузовского профессионального образования по специальности научных работников 01.01.06 Математическая логика, алгебра и теория чисел.

Алгебраические и теоретико-числовые методы широко используются в криптографии. В конце XX в. – начале XXI в. в криптографии стали активно использоваться методы алгебраической геометрии, началась работа по построению криптосистем на базе некоммутативных алгебраических структур. Были построены криптосистемы, базирующиеся на комбинаторной теории групп.

Для изучения данной дисциплины необходимы знания и умения, полученные в процессе обучения по программам специалитета или бакалавриата – магистратуры (дисциплины «Алгебра», «Математическая логика и теория алгоритмов» и «Теория чисел»). Дисциплина «Алгебраические и теоретико-числовые методы в криптографии» развивает и дополняет соответствующий раздел обязательной дисциплины «Специальность».

3. Требования к результатам освоения содержания дисциплины

В результате освоения дисциплины «Алгебраические и теоретико-числовые методы в криптографии» обучающийся должен:

Знать: основные определения, понятия и проблемы алгебраической геометрии и комбинаторной теории групп.

Уметь: применять математический аппарат алгебраической геометрии и комбинаторной теории групп для решения профессиональных задач, в том числе с использованием вычислительной техники.

Владеть: аппаратом алгебраической геометрии и комбинаторной теории групп.

4. Структура и содержание дисциплины «Алгебраические и теоретико-числовые методы в криптографии»

Общая трудоемкость дисциплины составляет 3 зачетные единицы, 108 часов.

№ п/п	Раздел Дисциплины	Курс	Неделя	Виды учебной работы, включая самостоятельную работу обучающихся, и трудоемкость (в часах) Форма обуч.: очная/заочная					Формы текущего контроля успеваемости *(по неделям)* Форма промежуточной аттестации
				Лекций	Лабораторных	Практических	Сам. работа	работыКонтроль сам.	
1	1. Введение. Предмет и задачи курса. Обзор основных результатов.	1	1				14		
2	2. Алгебраические основы		2-4	1			14		контрольная работа № 1
3	3. Алгебраические многообразия		5-6	1			14		реферат
4	4. Кубические кривые		7-8	1/0			15		реферат
5	5. Дополнительные вопросы теории кубических кривых		10	1			15		реферат
6	6. Некоторые приложения эллиптических кривых в криптографии		11	1/0			15		реферат
7	7. Методы комбинаторной теории групп в криптографии		12-15	1			15		контрольная работа №2 реферат
	Всего			6/4			102/ 104		

Содержание разделов дисциплины.

Тема 1. Введение. Принципы построения и изучения курса. Краткое содержание. Роль и место курса в формировании специалистов. Рекомендации по изучению курса, самостоятельной работе и литературе. О формах контроля и отчетности при изучении курса.

Тема 2. Алгебраические основы

Поля, подполя. Простые поля. Характеристика поля.

Расширения полей. Конечно порожденные и простые расширения. Их строение.

Расширения конечной степени. Теорема о башне полей для расширений конечной степени.

Алгебраические и трансцендентные элементы поля относительно его подполя. Минимальный полином алгебраического элемента, некоторые его свойства. Строение расширения поля, полученное присоединением алгебраического элемента. Алгебраические расширения полей. Теорема о башне полей для алгебраических расширений.

Конечные поля. Теорема о числе элементов конечного поля. Цикличность мультипликативной группы конечного поля. Дискретное логарифмирование в циклической группе.

Автоморфизм Фробениуса. Группа автоморфизмов конечного поля. Сепарабельные

и несепарабельные расширения поля.

Неприводимые полиномы над конечными полями, некоторые их свойства. Функция Мебиуса. Формула обращения Мебиуса. Число неприводимых полиномов данной степени над конечным полем с данным числом элементов. Мультипликативные теоретико-числовые функции.

Реализация основных операций конечного поля: сложение, умножение, возведение в степень, обращение.

Алгебраическое замыкание поля. Теорема о существовании алгебраического замыкания счетного поля.

Трансцендентные расширения полей. Базисы трансцендентности расширений полей.

Евклидовы кольца и кольца главных идеалов.

Тема 3. Алгебраические многообразия

Нетеровы кольца. Теорема Гильберта о базисе. Алгебраические множества и топология Зариского. Аффинные многообразия. Теорема Гильберта о нулях.

Регулярные и рациональные функции. Размерность аффинного многообразия.

Касательное пространство Зарисского к аффинному многообразию в точке. Особые и неособые точки.

Дифференцирования колец. Связь между касательным пространством Зарисского в точке и дифференцированиями в этой точке.

Проективные пространства. Проективные алгебраические множества. Проективные многообразия. Поле рациональных функций проективного многообразия Аффинные карты проективного пространства.

Дискретные нормирования поля. Эквивалентность нормирований.

Дискретные нормирования полей степени трансцендентности. Дивизоры на кривых.

Рациональная параметризация кривой. Рациональные многообразия.

Тема 4. Кубические кривые

Гессиан и точки перегиба плоских кривых.

Нормальная форма Вейерштрасса уравнения кубической кривой. Дискриминант и j-инвариант. Точки перегиба кубических кривых.

Групповая операция на эллиптической (неособой кубической) кривой.

Нерациональность неособых кубических кривых.

Тема 5. Дополнительные вопросы теории кубических кривых

Теорема Римана - Роха для эллиптической кривой. Эллиптические кривые над полем комплексных чисел. Римановы поверхности. Эллиптические функции. Функция Вейерштрасса. Морфизмы кривых. Точки конечного порядка и многочлены деления.

Эндоморфизмы и автоморфизмы эллиптических кривых. Неравенство Хассе.

Тема 6. Некоторые приложения эллиптических кривых в криптографии

Проверка чисел на простоту при помощи эллиптических кривых.

Разложение чисел на простые множители при помощи эллиптических кривых.

Некоторые протоколы эллиптической криптографии. Распределение ключей по протоколу Диффи – Хеллмана. Распределение ключей по протоколу Massey – Omura. Использование группы точек эллиптической кривой. Протокол распределения ключей Менезеса – Кью – Ватсона (MQV-протокол).

Электронная подпись Эль Гамаля и ее обобщения.

Схема электронной подписи Эль Гамаля с возвратом сообщения (Nyberg – Rueppel алгоритм) с использованием группы точек эллиптической кривой.

Тема 7. Методы комбинаторной теории групп в криптографии

Задание групп образующими элементами и определяющими соотношениями.

Фундаментальные проблемы М. Дэна. Преобразования Тице. Свободные группы.

Факторгруппы и подгруппы. Метод Рейдемейстера – Шрейера. Подгруппы свободных групп. Теорема Нильсена. Вербальные подгруппы и приведенные свободные группы. Теорема о строении конечно порожденной абелевой группы. Тождества в группах. Многообразия групп. Нильпотентные и разрешимые группы.

Автоморфизмы и эндоморфизмы групп. Проблемы автоморфной и эндоморфной сводимости для элементов и наборов элементов групп. Фундаментальные группы топологических пространств. Группы узлов и кос. Свободные произведения и свободные произведения с объединением. HNN-расширения. Теорема П.С. Новикова.

Распознавание групповых свойств, теорема С.И. Адяна.

Уравнения в свободных группах, теоремы Г.С. Маканина, А.А. Разборова, В.Г.Дурнева и И.Г. Лысенка.

Криптосистемы, базирующиеся на проблеме сопряженности и проблеме эндоморфной сводимости для наборов элементов групп. Некоторые подходы к обоснованию их стойкости.

5. Образовательные технологии

В преподавании используются методические пособия, программные комплексы.

В преподавании курса используются активные и интерактивные технологии проведения занятий в сочетании с внеаудиторной работой.

Часть практических занятий проводится в дисплейном классе с целью разработки, тестирования и модифицирования приложений, реализующих алгоритмы на графах.

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы обучающихся

В качестве средств текущего контроля используется 2 контрольных работы, а также написание в течение семестра 1 реферата на выбранную тему. Итоговая форма контроля (зачет) дает возможность выявить уровень профессиональной подготовки аспиранта по данной дисциплине.

Задачи для контрольной работы № 1.

1. Доказать, что для любого поля его аддитивная группа не изоморфна его мультипликативной группе.
2. Пусть $P<F$ – расширение простой степени p ($[F:P]=p$). Показать, что нет промежуточных полей, т.е. таких полей H, что $P<H<F$.
3. Найти минимальный многочлен элемента $1 + i$ из поля C комплексных чисел над подполем Q рациональных чисел.
4. Пусть $P < F$ – расширение полей и a – элемент из F. Доказать, что $P(a) = P[a]$ тогда и только тогда, когда a – алгебраический элемент над P.
5. Построить поле из 8 элементов.
6. Доказать, что мультипликативная группа бесконечного поля не может быть циклической.

Задания для контрольной работы № 2.

1. Построить алгоритм, позволяющий по двум произвольным элементам свободной группы определить, сопряжены ли они.

2. Построить алгоритм, позволяющий по двум произвольным элементам свободной группы определить, является ли один из них степенью другого.

3. Показать, что симметрическая группа степени 3 имеет задание
$(a, b \mid a^3 = 1, b^2 = 1, ab = ba^2)$.

4. Показать, что группы с заданиями (a, b || a^3 = 1, b^2 = 1, ab = ba) и (c || c^6 = 1) изоморфны.

5. Показать, что группы с заданиями (c, d || cdc = dcd) и (a, b || a^3 = b^2) изоморфны.

Темы рефератов

1. Расширения конечной степени.
2. Алгебраические и трансцендентные расширения поля.
3. Конечные поля. Цикличность мультипликативной группы конечного поля.
4. Группа автоморфизмов конечного поля. Сепарабельные и несепарабельные расширения поля.
5. Неприводимые полиномы над конечными полями.
6. Алгебраическое замыкание поля.
7. Трансцендентные расширения полей.
8. Евклидовы кольца и кольца главных идеалов.
9. Нетеровы кольца. Теорема Гильберта о базисе.
10. Алгебраические множества и аффинные многообразия.
11. Теорема Гильберта о нулях.
12. Касательное пространство Зарисского к аффинному многообразию в точке.
13. Дифференцирования колец. Связь между касательным пространством Зарисского в точке и дифференцированиями в этой точке.
14. Проективные пространства и проективные алгебраические множества. Проективные многообразия.
15. Дискретные нормирования поля. Эквивалентность нормирований.
16. Нормальная форма Вейерштрасса уравнения кубической кривой. Дискриминант и j-инвариант.
18. Групповая операция на эллиптической (неособой кубической) кривой.
19. Теорема Римана - Роха для эллиптической кривой.
13. Эллиптические кривые над полем комплексных чисел. Римановы поверхности.
14. Эллиптические функции. Функция Вейерштрасса.
15. Проверка чисел на простоту при помощи эллиптических кривых.
16. Разложение чисел на простые множители при помощи эллиптических кривых.
17. Некоторые протоколы эллиптической криптографии.
18. Схема электронной подписи Эль Гамаля с возвратом сообщения (Nyberg – Rueppel алгоритм) с использованием группы точек эллиптической кривой.
19. Задание групп образующими элементами и определяющими соотношениями.
20. Преобразования Тице.
21. Факторгруппы и подгруппы. Метод Рейдемейстера – Шрейера.
22. Подгруппы свободных групп. Теорема Нильсена.
23. Вербальные подгруппы и приведенные свободные группы.
24. Теорема о строении конечно порожденной абелевой группы.
25. Тождества в группах. Многообразия групп.
26. Нильпотентные и разрешимые группы.
27. Автоморфизмы и эндоморфизмы групп. Проблемы автоморфной и эндоморфной сводимости для элементов и наборов элементов групп.
28. Фундаментальные группы топологических пространств. Группы узлов и кос.
29. Свободные произведения и свободные произведения с объединением.
30. HNN-расширения. Теорема П.С. Новикова.
31. Распознавание групповых свойств, теорема С.И. Адяна.
32. Уравнения в свободных группах, теоремы Г.С. Маканина, А.А. Разборова, В.Г.Дурнева и И.Г. Лысенка.
34. Криптосистемы, базирующиеся на проблеме сопряженности и проблеме эндоморфной сводимости для наборов элементов групп.

Вопросы к зачету

1. Поля, подполя. Простые поля. Характеристика поля.
2. Расширения полей. Конечно порожденные и простые расширения. Их строение.
3. Расширения конечной степени. Теорема о башне полей для расширений конечной степени.
4. Алгебраические и трансцендентные элементы поля относительно его подполя.
5. Минимальный полином алгебраического элемента, некоторые его свойства.
6. Строение расширения поля, полученное присоединением алгебраического элемента.
7. Алгебраические расширения полей. Теорема о башне полей для алгебраических расширений.
8. Конечные поля. Теорема о числе элементов конечного поля. Цикличность мультипликативной группы конечного поля. Дискретное логарифмирование в циклической группе.
9. Автоморфизм Фробениуса. Группа автоморфизмов конечного поля. Сепарабельные и несепарабельные расширения поля.
10. Неприводимые полиномы над конечными полями, некоторые их свойства. Функция Мебиуса. Формула обращения Мебиуса. Число неприводимых полиномов данной степени над конечным полем с данным числом элементов. Мультипликативные теоретико-числовые функции.
11.Реализация основных операций конечного поля: сложение, умножение, возведение в степень, обращение.
12. Алгебраическое замыкание поля. Теорема о существовании алгебраического замыкания счетного поля.
13. Трансцендентные расширения полей. Базисы трансцендентности расширений полей.
14. Евклидовы кольца и кольца главных идеалов.
15. Нетеровы кольца. Теорема Гильберта о базисе.
16. Алгебраические множества и топология Зариского. Аффинные многообразия. Теорема Гильберта о нулях.
17. Регулярные и рациональные функции. Размерность аффинного многообразия.
18. Касательное пространство Зарисского к аффинному многообразию в точке. Особые и неособые точки.
19. Дифференцирования колец. Связь между касательным пространством Зарисского в точке и дифференцированиями в этой точке.
20. Проективные пространства. Проективные алгебраические множества. Проективные многообразия. Поле рациональных функций проективного многообразия Аффинные карты проективного пространства.
21. Дискретные нормирования поля. Эквивалентность нормирований.
22. Дискретные нормирования полей степени трансцендентности Дивизоры на кривых.
23. Рациональная параметризация кривой. Рациональные многообразия.
24. Гессиан и точки перегиба плоских кривых.
25. Нормальная форма Вейерштрасса уравнения кубической кривой. Дискриминант и j-инвариант.
26. Точки перегиба кубических кривых.
27. Групповая операция на эллиптической (неособой кубической) кривой.
28. Нерациональность неособых кубических кривых.
29. Теорема Римана - Роха для эллиптической кривой.
30. Эллиптические кривые над полем комплексных чисел. Римановы поверхности.

31. Эллиптические функции. Функция Вейерштрасса.
32. Точки конечного порядка и многочлены деления.
33. Морфизмы кривых. Эндоморфизмы и автоморфизмы эллиптических кривых.
34. Неравенство Хассе.
35. Проверка чисел на простоту при помощи эллиптических кривых.
36. Разложение чисел на простые множители при помощи эллиптических кривых.
37. Некоторые протоколы эллиптической криптографии. Распределение ключей по протоколу Диффи – Хеллмана. Распределение ключей по протоколу Massey – Omura. Использование группы точек эллиптической кривой. Протокол распределения ключей Менезеса – Кью – Ватсона (MQV-протокол).
38. Электронная подпись Эль Гамаля и ее обобщения.
39. Схема электронной подписи Эль Гамаля с возвратом сообщения (Nyberg – Rueppel алгоритм) с использованием группы точек эллиптической кривой.
40. Задание групп образующими элементами и определяющими соотношениями.
41. Фундаментальные проблемы М. Дэна.
42.Преобразования Тице.
43. Свободные группы.
44. Факторгруппы и подгруппы. Метод Рейдемейстера – Шрейера.
45.Подгруппы свободных групп. Теорема Нильсена.
46. Вербальные подгруппы и приведенные свободные группы.
47. Теорема о строении конечно порожденной абелевой группы.
48. Тождества в группах. Многообразия групп.
49. Нильпотентные и разрешимые группы.
50. Автоморфизмы и эндоморфизмы групп. Проблемы автоморфной и эндоморфной сводимости для элементов и наборов элементов групп.
51. Фундаментальные группы топологических пространств. Группы узлов и кос.
52. Свободные произведения и свободные произведения с объединением.
53. HNN-расширения. Теорема П.С. Новикова.
54. Распознавание групповых свойств, теорема С.И. Адяна.
55. Уравнения в свободных группах, теоремы Г.С. Маканина, А.А. Разборова, В.Г.Дурнева и И.Г. Лисенка.
56 Криптосистемы, базирующиеся на проблеме сопряженности и проблеме эндоморфной сводимости для наборов элементов групп. Некоторые подходы к обоснованию их стойкости.

7. Учебно-методическое и информационное обеспечение дисциплины

а) основная литература:

1. Болотов А.А., Гашков С.Б., Фролов А.Б., Часовских А.А. Алгоритмические основы эллиптической криптографии. -- М.: Московский энергетический институт, 2000. – 112.

2. Виноградов И.М. Основы теории чисел. - М.: Наука, 1972. – 168 с.

2. Глухов М.М., Елизаров В.П., Нечаев А.А. Алгебра. Том П. - М.: «Гелиос АРВ», 2003. – 416 с.

3. Кострикин А.И. Введение в алгебру. Часть III. Основные структуры алгебры. -- М.:Физико-математическая литература, 2000. – 272 с.

4. Коблиц Н. Курс теории чисел и криптографии. - М.: Научное издательство «ТВП», 2001. – 254 с.

5. Лидл Р., Нидеррайтер Г. Конечные поля. Том I, II. - М.: Мир, 1988.

6. Магнус В., Каррас А., Солитэр Д. Комбинаторная теория групп. – М.: Физико-математическая литература, 1974. – 456 с.

7. Прохоров Ю.Г. Лекции по алгебраической геометрии. Эллиптические кривые в криптографии. - М.: МГУ, 2004. – 126 с.

8. Ростовцев А. Алгебраические основы криптографии. - СПб.: НПО «Мир и семья». ООО «Интерлайн», 2000. 354 с.

9. Шафаревич И.Р. Основы алгебраической геометрии. - М.: Наука, 1988.

б) дополнительная литература:

1. Ленг С. Алгеба. - М.: Мир, 1968. 564 с.
2. Линдон Р., Шупп П. Комбинаторная теория групп. – М.: Мир, 1980. – 448 с.
3. Ноден П., Китте К. Алгебраическая алгоритмика. – М.: Мир, 1999. – 720 с.
4. Черемушкин А.В. Лекции по арифметическим алгоритмам в криптографии. – М.:МЦНМО, 2002. 104 с.

б) программное обеспечение и Интернет-ресурсы:

1. Электронная библиотека ЯрГУ: http://www.lib.uniyar.ac.ru
2. http://mech.math.msu.su/department/

8. Материально-техническое обеспечение дисциплины

Аудитории для лекций и практических занятий (с необходимым материальным оснащением). Наличие рекомендованной литературы. Наличие электронных версий методических материалов.

Программа составлена в соответствии с федеральными государственными требованиями к структуре основной профессиональной образовательной программы послевузовского профессионального образования (аспирантура) (приказ Минобрнауки от 16.03.2011 г. № 1365) с учетом рекомендаций, изложенных в письме Минобрнауки от 22.06.2011 г. № ИБ – 733/12.

Программа одобрена на заседании кафедры компьютерной безопасности и математических методов обработки информации 02.10.2012 (протокол № 2).

Заведующий кафедрой В.Г.Дурнев, доктор физ-мат.наук, профессор

Автор В.Г.Дурнев, доктор физ-мат.наук, профессор