**Программа утверждена на заседании кафедры теории чисел**

**Рабочая программа дисциплины (модуля)**

1. Код и наименование дисциплины (модуля): Дискретное логарифмирование.

2. Уровень высшего образования – специалитет.

3. Направление подготовки: 01.05.01 Фундаментальные математика и механика. Специализация:Фундаментальная математика.

4. Место дисциплины (модуля) в структуре ООП: вариативная часть ООП. Является специальной дисциплиной (спецкурсом) для студентов 3-6 годов обучения, специализирующихся в данной научной области или смежной научной области, спецкурсом по выбору студента.

Освоение дисциплины необходимо для последующего изучения дисциплин образовательной программы: курсовая работа, научно-исследовательская практика, преддипломная практика, выпускная квалификационная работа.

5. Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями выпускников)

6. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся:

Объем дисциплины (модуля) составляет 3 зачетных единицы, всего 108 часа, из которых 44 (46\*) часа составляет контактная работа студента с преподавателем (34 (36\*) часа занятия лекционного типа, 12 часов мероприятия текущего контроля успеваемости и промежуточной аттестации), 64 (62\*) часа составляет самостоятельная работа студента.

*\* - если специальный курс читается в нечетном семестре (продолжительность нечетного семестра 18 недель, четного семестра 17 недель).*

7. Входные требования для освоения дисциплины (модуля), предварительные условия.

Для того чтобы изучение дисциплины было возможно, обучающийся должен

1. освоить следующие дисциплины образовательной программы: элементы теории чисел, алгебра, аналитическая геометрия.
2. обладать следующими компетенциями:

Знать: основные методы дисциплин из пункта 1).

Уметь: решать стандартные задачи тех же дисциплин и применять идеи, использованные в их решениях, для решения аналогичных задач.

Владеть: основными понятиями и теоремами тех же дисциплин.

8. Формат обучения.

очная форма обучения, лекционные занятия.

9. Содержание дисциплины (модуля), структурированное по темам (Перечень тем см. Приложения).

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Наименование и краткое содержание разделов и тем дисциплины (модуля),**  **форма промежуточной аттестации по дисциплине (модулю)** | **Всего**  **(часы**) | В том числе | | | | | | | | |
| **Контактная работа (работа во взаимодействии с преподавателем), часы**  из них | | | | | | **Самостоятельная работа обучающегося, часы**  из них | | |
| Занятия лекционного типа | Занятия семинарского типа | Групповые консультации | Индивидуальные консультации | Учебные занятия, направленные на проведение текущего контроля успеваемости, промежуточной аттестации | **Всего** | Выполнение домашних заданий | Подготовка рефератовит.п.. | **Всего** |
| Тема 1 | 6 | 2 |  |  |  |  | 2 | 4 |  | 4 |
| Тема 2 | 6 | 2 |  |  |  |  | 2 | 4 |  | 4 |
| Тема 3 | 6 | 2 |  |  |  |  | 2 | 4 |  | 4 |
| Тема 4 | 6 | 2 |  |  |  |  | 2 | 4 |  | 4 |
| Тема 5 | 6 | 2 |  |  |  |  | 2 | 4 |  | 4 |
| Тема 6 | 6 | 2 |  |  |  |  | 2 | 4 |  | 4 |
| Тема 7 | 6 | 2 |  |  |  |  | 2 | 4 |  | 4 |
| Тема 8 | 6 | 2 |  |  |  |  | 2 | 4 |  | 4 |
| Текущий контроль успеваемости | 6 |  |  |  |  | 2 | 2 | 4 |  | 4 |
| Тема 9 | 6 | 2 |  |  |  |  | 2 | 4 |  | 4 |
| Тема 10 | 6 | 2 |  |  |  |  | 2 | 4 |  | 4 |
| Тема 11 | 6 | 2 |  |  |  |  | 2 | 4 |  | 4 |
| Тема 12 | 6 | 2 |  |  |  |  | 2 | 4 |  | 4 |
| Тема 13 | 6 | 2 |  |  |  |  | 2 | 4 |  | 4 |
| Тема 14 | 6 | 2 |  |  |  |  | 2 | 4 |  | 4 |
| Тема 15 | 6 | 2 |  |  |  |  | 2 | 4 |  | 4 |
| Тема 16 | 4 |  |  |  |  |  | 0 | 4 |  | 4 |
| Тема 17\* | 2\* |  |  |  |  |  |  | 2\* |  | 2\* |
| Промежуточная аттестация  *экзамен*  *зачет* | 8 (6\*) |  |  |  |  | 2 | 2 | 6(4\*) |  | 6 (4\*) |
| **Итого** | 108 | 30 |  |  |  | 4 | 34 | 74 |  | 74 |

10. Перечень учебно-методического обеспечения для самостоятельной работы студентов по дисциплине (модулю):

Конспекты лекций, списки задач к лекциям, основная и дополнительная учебная литература.

11. Фонд оценочных средств для промежуточной аттестации по дисциплине (модулю).

* Перечень компетенций:
* Описание шкал оценивания*:*

*экзамен с оценкой по пятибалльной шкале*

*зачет («зачтено» или «не зачтено»)*

* Критерии и процедуры оценивания результатов обучения по дисциплине (модулю), характеризующих этапы формирования компетенций.
* Типовые контрольные задания или иные материалы, необходимые для оценки результатов обучения, характеризующих этапы формирования компетенций.См. Приложения.

12. Ресурсное обеспечение:

Перечень основной учебной литературы:

1. **Kraitchik M.** Theorie des Nombres. 1922. Vol. 1. Gauthier-Villars.
2. **Kraitchik M.** Recherches sur la theorie des nombres. 1924. Gauthier-Villars.
3. **Enge A.** Elliptic curves and their applications to cryptography: an introduction. Kluwer Academic Publishers. 1999.
4. **Pohlig S. and Hellman M.** An improved algorithm for computing logarithms over GF(p)GF(p) and its cryptographic significance. IEEE Transactions on Information Theory. 1978. No 24. P. 106-110.
5. **Pollard J.** Monte Carlo methods for index computation mod pp. Mathematics of Computation. 1978. No 32. P. 918-924.
6. **Milne J. S.** Elliptic curves. 2006.
7. **Silverman J. H.** The Arithmetic Of Elliptic Curves. Springer-Verlag, GTM 106, 1986. Expanded 2nd Edition, 2009.
8. **Smart N. P.** The discrete logarithm problem on elliptic curves of trace one. Hewlett-Packard Company. 1997.
9. **Semaev I.** Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic pp. Mathematics of Computation. 1998. No 67. P. 353-356.
10. **Schoof R. J.** Elliptic curves over finite fields and the computation of square roots mod pp. Math. Comp. 1985. **44**. 483–494.
11. **Lenstra H. W. Jr.** Complex multiplication structure of elliptic curves. Journal of Number Theory. 1996. **56**. 227-241.
12. **Айерленд К., Роузен М.** Классическое введение в современную теорию чисел. М.: Мир, 1987, 416 с.

Перечень дополнительной учебной литературы: см. Приложения

Перечень ресурсов информационно-телекоммуникационной сети «Интернет»: см. Приложения.

Описание материально-технической базы: аудитории для проведения лекционных занятий.

13. Язык преподавания: русский (при необходимости – английский).

ПРИЛОЖЕНИЕ

1. Дискретное логарифмирование.
2. Преподаватель - доц. Е. А. Уланский.
3. Аннотация курса: Для решения задачи дискретного логарифмирования в мультипликативной группе конечного поля известны субэкспоненциальные алгоритмы. Если же ставить подобную задачу в группе точек эллиптической кривой, то её решение настолько трудно, что на основе этой задачи строится защита информации в банковской и многих других сферах. В курсе мы ознакомимся с самими эллиптическими кривыми и узнаем о подходах к решению задачи дискретного логарифмирования на них.
4. Тематическое содержание курса:

|  |  |
| --- | --- |
| Тема 1 | Задача дискретного логарифмирования на примере мультипликативной группы конечного поля. Метод индексного исчисления. |
| Тема 2 | Эллиптические кривые. Закон сложения точек эллиптической кривой. |
| Тема 3 | Эллиптические кривые над конечными полями. |
| Тема 4 | Структура группы точек эллиптической кривой, определённой над конечным полем. |
| Тема 5 | Задача дискретного логарифмирования в группе точек эллиптической кривой, определённой над конечным полем. |
| Тема 6 | Метод Полига-Хелмана вычисления дискретного логарифма. |
| Тема 7 | Метод Полларда вычисления дискретного логарифма. |
| Тема 8 | Эллиптические кривые над p-адическими полями. |
| Тема 9 | Эллиптический логарифм. |
| Тема 10 | Решение задачи дискретного логарифмирования для эллиптических кривых порядка p над полем F\_p. |
| Тема 11 | Кольцо эндоморфизмов эллиптической кривой. |
| Тема 12 | Дивизоры эллиптической кривой. |
| Тема 13 | Многочлены деления. |
| Тема 14 | Суперсингулярные кривые. |
| Тема 15 | Дискретное логарифмирование на суперсингулярных кривых. |
| Тема 16 | Связь структуры группы эллиптической кривой, определенной над конечным полем с кольцом эндоморфизмов этой кривой. |
| Тема 17 | Теорема Ленстры. |
| Тема 18 | Быстрое вычисление структуры группы и дискретного логарифма на некоторых эллиптических кривых специального вида. |

1. Типовые контрольные задания или иные материалы, необходимые для оценки результатов обучения, характеризующих этапы формирования компетенций.

Вопросы к экзамену:

1. Задача дискретного логарифмирования на примере мультипликативной группы конечного поля. Метод индексного исчисления.
2. Эллиптические кривые. Закон сложения точек эллиптической кривой.
3. Эллиптические кривые над конечными полями.
4. Структура группы точек эллиптической кривой, определённой над конечным полем.
5. Задача дискретного логарифмирования в группе точек эллиптической кривой, определённой над конечным полем.
6. Метод Полига-Хелмана вычисления дискретного логарифма.
7. Метод Полларда вычисления дискретного логарифма.
8. Эллиптические кривые над p-адическими полями.
9. Эллиптический логарифм.
10. Решение задачи дискретного логарифмирования для эллиптических кривых порядка p над полем F\_p.
11. Кольцо эндоморфизмов эллиптической кривой.
12. Дивизоры эллиптической кривой.
13. Многочлены деления.
14. Суперсингулярные кривые.
15. Дискретное логарифмирование на суперсингулярных кривых.
16. Связь структуры группы эллиптической кривой, определенной над конечным полем с кольцом эндоморфизмов этой кривой.
17. Теорема Ленстры.
18. Быстрое вычисление структуры группы и дискретного логарифма на некоторых эллиптических кривых специального вида.
19. Перечень дополнительной учебной литературы, ресурсов информационно-телекоммуникационной сети «Интернет»:

**Приложение утверждено на заседании кафедры теории чисел**