**Программа утверждена на заседании кафедры теории чисел**

**Рабочая программа дисциплины (модуля)**

1. Код и наименование дисциплины (модуля): Спаривания на эллиптической кривой.

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, дискретное логарифмирование.
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. **Enge A.** Elliptic curves and their applications to cryptography: an introduction. Kluwer Academic Publishers. 1999.
2. **Milne J. S.** Elliptic curves. 2006.
3. **Silverman J. H.** The Arithmetic Of Elliptic Curves. Springer-Verlag, GTM 106, 1986. Expanded 2nd Edition, 2009.
4. **Enge A.** Bilinear pairings on elliptic curves. 2012.
5. **Miller V. S.** The Weil pairing and its efficient calculation. Journal of Cryptology. 2004. Vol. **17**. 235–261.
6. **Menezes A., Okamoto T., Vanstone S.** Reducing elliptic curve logarithms to logarithms in a finite field. IEEE Transactions on Information Theory. 1993. No 39. P. 1639-1646.
7. **Frey G., Ruck H.** A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. Mathematics of Computation. 1994. No 62. P. 865-874.

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. Спаривания на эллиптической кривой.
2. Преподаватель - доц. Е. А. Уланский.
3. Аннотация курса: Для решения задачи дискретного логарифмирования в группе точек эллиптической кривой очень часто применяются спаривания точек кривой. В курсе мы ознакомимся с самими эллиптическими кривыми и узнаем методы построения спариваний и их роль в решении задачи дискретного логарифмирования на них.
4. Тематическое содержание курса:

|  |  |
| --- | --- |
| Тема 1 | Эллиптические кривые. Закон сложения точек эллиптической кривой. |
| Тема 2 | Эллиптические кривые над конечными полями. |
| Тема 3 | Структура группы точек эллиптической кривой, определённой над конечным полем. |
| Тема 4 | Задача дискретного логарифмирования в группе точек эллиптической кривой, определённой над конечным полем. |
| Тема 5 | Дивизоры эллиптической кривой. |
| Тема 6 | Спаривания на эллиптических кривых. |
| Тема 7 | Спаривание Вейля. |
| Тема 8 | Спаривание Тэйта. |
| Тема 9 | Спаривание эйта. |
| Тема 10 | Алгоритм вычисления спаривания Вейля. |
| Тема 11 | Алгоритм вычисления спаривания Тэйта. |
| Тема 12 | Алгоритм вычисления спаривания эйта. |
| Тема 13 | Определение порядка группы точек эллиптической кривой, определённой над конечным полем. |
| Тема 14 | Определение структуры группы точек эллиптической кривой, определённой над конечным полем. |
| Тема 15 | Алгоритм Менезеса-Окамото-Ванстоуна нахождения дискретного логарифма на эллиптических кривых. |
| Тема 16 | Суперсингулярные кривые. |
| Тема 17\* | Дискретное логарифмирование на суперсингулярных кривых. |

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

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

Вопросы к экзамену:

1. Эллиптические кривые. Закон сложения точек эллиптической кривой.
2. Эллиптические кривые над конечными полями.
3. Структура группы точек эллиптической кривой, определённой над конечным полем.
4. Задача дискретного логарифмирования в группе точек эллиптической кривой, определённой над конечным полем.
5. Дивизоры эллиптической кривой.
6. Спаривания на эллиптических кривых.
7. Спаривание Вейля.
8. Спаривание Тэйта.
9. Спаривание эйта.
10. Алгоритм вычисления спаривания Вейля.
11. Алгоритм вычисления спаривания Тэйта.
12. Алгоритм вычисления спаривания эйта.
13. Определение порядка группы точек эллиптической кривой, определённой над конечным полем.
14. Определение структуры группы точек эллиптической кривой, определённой над конечным полем.
15. Алгоритм Менезеса-Окамото-Ванстоуна нахождения дискретного логарифма на эллиптических кривых.
16. Суперсингулярные кривые.
17. Дискретное логарифмирование на суперсингулярных кривых.
18. Перечень дополнительной учебной литературы, ресурсов информационно-телекоммуникационной сети «Интернет»:

**Приложение утверждено на заседании кафедры теории чисел**