**Программа утверждена на заседании кафедры теории чисел**

**Рабочая программа дисциплины (модуля)**

1. Код и наименование дисциплины (модуля): Диофантовы уравнения.

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 5зачетных единицы, всего 180 часов, из которых 70 часов составляет контактная работа студента с преподавателем (62 часа занятия лекционного типа, 8 часов мероприятия текущего контроля успеваемости и промежуточной аттестации),110 часов составляет самостоятельная работа студента.*

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, математический анализ, 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 | 4 | 2 |  |  |  |  | 2 | 2 |  | 2 |
| Тема 2 | 4 | 2 |  |  |  |  | 2 | 2 |  | 2 |
| Тема 3 | 4 | 2 |  |  |  |  | 2 | 2 |  | 2 |
| Тема 4 | 4 | 2 |  |  |  |  | 2 | 2 |  | 2 |
| Тема 5 | 4 | 2 |  |  |  |  | 2 | 2 |  | 2 |
| Тема 6 | 4 | 2 |  |  |  |  | 2 | 2 |  | 2 |
| Тема 7 | 4 | 2 |  |  |  |  | 2 | 2 |  | 2 |
| Тема 8 | 4 | 2 |  |  |  |  | 2 | 2 |  | 2 |
| Текущий контроль успеваемости | 10 |  |  |  |  | 2 | 2 | 8 |  | 8 |
| Тема 9 | 4 | 2 |  |  |  |  | 2 | 2 |  | 2 |
| Тема 10 | 4 | 2 |  |  |  |  | 2 | 2 |  | 2 |
| Тема 11 | 4 | 2 |  |  |  |  | 2 | 2 |  | 2 |
| Тема 12 | 4 | 2 |  |  |  |  | 2 | 2 |  | 2 |
| Тема 13 | 4 | 2 |  |  |  |  | 2 | 2 |  | 2 |
| Тема 14 | 4 | 2 |  |  |  |  | 2 | 2 |  | 2 |
| Тема 15 | 4 | 2 |  |  |  |  | 2 | 2 |  | 2 |
| Тема 16 | 4 | 2 |  |  |  |  | 2 | 2 |  | 2 |
| Текущий контроль успеваемости | 10 |  |  |  |  | 2 | 2 | 8 |  | 8 |
| Тема 17 | 4 | 2 |  |  |  |  | 2 | 2 |  | 2 |
| Тема 18 | 4 | 2 |  |  |  |  | 2 | 2 |  | 2 |
| Тема 19 | 4 | 2 |  |  |  |  | 2 | 2 |  | 2 |
| Тема 20 | 4 | 2 |  |  |  |  | 2 | 2 |  | 2 |
| Тема 21 | 4 | 2 |  |  |  |  | 2 | 2 |  | 2 |
| Тема 22 | 4 | 2 |  |  |  |  | 2 | 2 |  | 2 |
| Тема 23 | 4 | 2 |  |  |  |  | 2 | 2 |  | 2 |
| Тема 24 | 4 | 2 |  |  |  |  | 2 | 2 |  | 2 |
| Текущий контроль успеваемости | 10 |  |  |  |  | 2 | 2 | 8 |  | 8 |
| Тема 25 | 4 | 2 |  |  |  |  | 2 | 2 |  | 2 |
| Тема 26 | 4 | 2 |  |  |  |  | 2 | 2 |  | 2 |
| Тема 27 | 4 | 2 |  |  |  |  | 2 | 2 |  | 2 |
| Тема 28 | 4 | 2 |  |  |  |  | 2 | 2 |  | 2 |
| Тема 29 | 4 | 2 |  |  |  |  | 2 | 2 |  | 2 |
| Тема 30 | 4 | 2 |  |  |  |  | 2 | 2 |  | 2 |
| Тема 31 | 4 | 2 |  |  |  |  | 2 | 2 |  | 2 |
| Тема 32 | 2 |  |  |  |  |  | 0 | 2 |  | 2 |
| Промежуточная аттестация  *экзамен*  *зачет* | 24 |  |  |  |  | 2 | 2 | 22 |  | 22 |
| **Итого** | 180 | 62 |  |  |  | 8 | 70 | 110 |  | 110 |

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 «незачтено»)*

* 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. Боревич З.И., Шафаревич И.Р., Теория чисел, М., Наука, 1972.
2. Ленг С., Введение в теорию диофантовых приближений, М., Мир, 1970.
3. Silverman J.Y., Tate J., Rational points on elliptic curves, Springer, 1992.

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. Диофантовы уравнения.
2. Преподаватель - проф. Ю. В. Нестеренко.
3. Аннотация курса: цель курса – изложить теорию, позволяющую решать в целых числах диофантовы уравнения вида f(x;y)=0, где f(x;y) произвольный многочлен второй степени с целыми коэффициентами. Также курс посвящён основам арифметической теории эллиптических кривых – классического и активно развивающегося в настоящее время раздела теории чисел и алгебры.
4. Тематическое содержание курса

|  |  |
| --- | --- |
| Тема 1 | Рациональные параметризации кривых второго порядка. |
| Тема 2 | Теорема Лежандра о целых решениях уравнения ax2 + by2 + cz2 = 0. |
| Тема 3 | Квадратичные иррациональности, сопряженные числа, след и норма. Квадратичные поля. Линейность следа и мультипликативность нормы. |
| Тема 4 | Уравнение Пелля. Бесконечность множества решений. |
| Тема 5 | Кольцо целых чисел, фундаментальный базис и дискриминант поля, группа единиц квадратичного поля. |
| Тема 6 | Цепные дроби. Свойство наилучшего приближения. Эквивалентные числа и цепные дроби. |
| Тема 7 | Вычисление группы единиц квадратичного поля. |
| Тема 8 | Приведённые квадратичные иррациональности, свойство их цепных дробей. |
| Тема 9 | Конечность множества приведённых квадратичных иррациональностей с заданным дискриминантом. |
| Тема 10 | Порядки в квадратичных полях. Группы единиц в порядках. |
| Тема 11 | Цепные дроби целых квадратичных иррациональностей. |
| Тема 12 | Модули, умножение модулей, норма модуля, мультипликативность нормы в квадратичных полях. |
| Тема 13 | Соответствие между модулями и формами. Представление чисел бинарными формами и подобие модулей. |
| Тема 14 | Подобие модулей в действительных и мнимых квадратичных полях. |
| Тема 15 | Целые точки на кривых второго порядка. |
| Тема 16 | Уравнения и |
| Тема 17 | Рациональные точки на кривых второго порядка. |
| Тема 18 | Геометрия кубических кривых. |
| Тема 19 | Вейерштрассова нормальная форма. |
| Тема 20 | Точные формулы для группового закона. |
| Тема 21 | Точки второго и третьего порядков. |
| Тема 22 | Действительные и комплексные точки на кубических кривых. |
| Тема 23 | Точки конечного порядка имеют целые координаты. |
| Тема 24 | Теорема Нагеля-Лютц. |
| Тема 25 | Группа рациональных точек на эллиптической кривой. Высоты и спуск. |
| Тема 26 | Высота суммы двух точек. Высота удвоенной точки. |
| Тема 27 | Теорема Морделла о конечности ранга группы рациональных точек на эллиптической кривой. |
| Тема 28 | Кубические кривые над конечными полями. Теорема Гаусса о числе решений уравнения x3 + y3 + z3=0 над конечными полями Fp для простых p. |
| Тема 29 | Теорема Хассе об оценках числа точек эллиптической кривой над конечным полем. |
| Тема 30 | Целые точки на кубических кривых. О числе целых решений уравнения x3 + y3=m. |
| Тема 31 | Теорема Туэ о рациональных приближениях алгебраических чисел. |
| Тема 32 | Конечность множества решений диофантова уравнения Туэ. |

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

Вопросы к экзамену:

1. Рациональные параметризации и рациональные точки на кривых второго порядка.
2. Теорема Лежандра о целых решениях уравнения ax2 + by2 + cz2 = 0.
3. Квадратичные иррациональности, сопряженные числа, след и норма. Квадратичные поля. Линейность следа и мультипликативность нормы.
4. Уравнение Пелля. Бесконечность множества целых решений.
5. Кольцо целых чисел. Фундаментальный базис и дискриминант поля.
6. Группа единиц квадратичного поля.
7. Цепные дроби. Свойство наилучшего приближения.
8. Эквивалентные числа и цепные дроби.
9. Вычисление группы единиц квадратичного поля.
10. Приведённые квадратичные иррациональности, свойство их цепных дробей.
11. Конечность множества приведённых квадратичных иррациональностей с заданным дискриминантом.
12. Порядки в квадратичных полях. Группы единиц в порядках.
13. Цепные дроби целых квадратичных иррациональностей.
14. Модули, умножение модулей, норма модуля, мультипликативность нормы.
15. Соответствие между модулями и формами. Представление чисел бинарными формами и подобие модулей.
16. Подобие модулей в действительных полях.
17. Подобие модулей в мнимых квадратичных полях.
18. Целые точки на общих кривых второго порядка.
19. Целые решения уравнения .
20. Целые решения уравнения
21. Геометрия кубических кривых.
22. Вейерштрассова нормальная форма.
23. Точные формулы для группового закона.
24. Точки второго и третьего порядков.
25. Действительные и комплексные точки на кубических кривых.
26. Точки конечного порядка имеют целые координаты.
27. Теорема Нагеля-Лютц.
28. Группа рациональных точек на эллиптической кривой. Высоты и спуск.
29. Высота суммы двух точек. Высота удвоенной точки.
30. Теорема Морделла о конечности ранга группы рациональных точек на эллиптической кривой.
31. Кубические кривые над конечными полями.
32. Теорема Гаусса о числе решений уравнения x3 + y3 + z3=0 над конечными полями Fp для простых p.
33. Теорема Хассе об оценках числа точек эллиптической кривой над конечным полем.
34. Целые точки на кубических кривых. О числе целых решений уравнения x3 + y3=m.
35. Теорема Туэ о рациональных приближениях алгебраических чисел.
36. Конечность множества решений диофантова уравнения Туэ.
37. Перечень дополнительной учебной литературы, ресурсов информационно-телекоммуникационной сети «Интернет»:
38. Айерленд К.А., Роузен М., Классическое введение в современную теорию чисел, М., Мир, 1987.
39. Венков Б.А., Элементарная теория чисел, М., ОНТИ, 1937.
40. Шидловский А.Б., Диофантовы приближения и трансцендентные числа, Издательство МГУ, 1982.

**Приложение утверждено на заседании кафедры теории чисел**