**Программа утверждена на заседании кафедры теории чисел**

**Рабочая программа дисциплины (модуля)**

1. Код и наименование дисциплины (модуля): Теоретико-числовые алгоритмы.

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, алгебраические числа.
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] Василенко О.Н., Теоретико-числовые алгоритмы в криптографии, М., МЦНМО, 2003.

[2] Герман О.Н., Нестеренко Ю.В., Теоретико-числовые методы в криптографии, М., Академия, 2012.

[3] H. Cohen, A Course in Computational Algebraic Number Theory, Springer, 1996.

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. Теоретико-числовые алгоритмы.
2. Преподаватель - асс. И. П. Рочев.
3. Аннотация курса: специальный курс знакомит с большим количеством важных математических алгоритмов, касающихся быстрого вычисления, проверки чисел на простоту, факторизации и многого другого.
4. Тематическое содержание курса

|  |  |
| --- | --- |
| Тема 1 | Арифметическая сложность алгоритмов. Алгоритм Евклида, оценка его сложности (теорема Ламе). |
| Тема 2 | Квадратичные сравнения. Малая теорема Ферма. |
| Тема 3 | Символ Лежандра и его свойства. Вычисление символа Лежандра. |
| Тема 4 | Символ Якоби. Быстрый алгоритм для вычисления символа Якоби. |
| Тема 5 | Быстрый алгоритм возведения в степень. Вычисление членов линейных рекуррентных последовательностей. |
| Тема 6 | Вероятностные алгоритмы. |
| Тема 7 | Первообразные корни и их вычисление. |
| Тема 8 | Алгоритм Шенкса решения квадратичных сравнений и оценка его сложности при известном квадратичном невычете. |
| Тема 9 | Вероятностный алгоритм нахождения квадратичных невычетов. |
| Тема 10 | Числа Кармайкла, псевдопростые числа. |
| Тема 11 | Вероятностные методы отсеивания составных чисел (тесты Миллера-Рабина, Соловея-Штрассена). |
| Тема 12 | Алгоритм Берлекэмпа для разложения многочленов на неприводимые множители над конечным полем. |
| Тема 13 | Сведение задачи разложения многочлена на множители к нахождению корней. |
| Тема 14 | Нахождение корней многочленов в полях малой характеристики. |
| Тема 15 | Вероятностные алгоритмы для нахождения корней многочленов в полях большой характеристики. |
| Тема 16 | Условный алгоритм Миллера для доказательства простоты чисел. |
| Тема 17 | Детерминированные n±1-методы проверки простоты чисел. Простота чисел Ферма и Мерсенна. |
| Тема 18 | Построение больших простых чисел. |
| Тема 19 | Полиномиальный детерминированный алгоритм проверки чисел на простоту. |
| Тема 20 | Алгоритм Адлемана-Ленстры-Коэна доказательства простоты чисел. |
| Тема 21 | Факторизация чисел с экспоненциальной сложностью: метод Ферма, алгоритмы Ленстры и Шермана-Лемана. |
| Тема 22 | ρ метод Полларда, p-1 метод Полларда, алгоритм Полларда-Штрассена. |
| Тема 23 | Дополнительные стратегии. Алгоритм Бриллхарта - Моррисона. |
| Тема 24 | Квадратичное решето. |
| Тема 25 | Решето числового поля на примере факторизации числа Ферма F9. |
| Тема 26 | Алгоритмы дискретного логарифмирования по простому модулю: метод Гельфонда, алгоритм Поллига-Хеллмана. |
| Тема 27 | Алгоритм Адлемана, алгоритм Копперсмитта-Одлыжко-Шреппеля. |
| Тема 28 | Дискретное логарифмирование и решето числового поля. |
| Тема 29 | Решетки и их свойства. |
| Тема 30 | LLL-алгоритм построения приведенного базиса решетки. |
| Тема 31 | Факторизация многочленов в Z[x1,...,xm] с полиномиальной сложностью. |
| Тема 32 | Построение совместных рациональных приближений и нахождение минимумов квадратичных форм с помощью LLL-алгоритма. |

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

Вопросы к экзамену:

1. Арифметическая сложность алгоритмов. Алгоритм Евклида, оценка его сложности (теорема Ламе).
2. Квадратичные сравнения. Малая теорема Ферма.
3. Символ Лежандра и его свойства. Вычисление символа Лежандра.
4. Символ Якоби. Быстрый алгоритм для вычисления символа Якоби.
5. Быстрый алгоритм возведения в степень. Вычисление членов линейных рекуррентных последовательностей.
6. Вероятностные алгоритмы.
7. Первообразные корни и их вычисление.
8. Алгоритм Шенкса решения квадратичных сравнений и оценка его сложности при известном квадратичном невычете.
9. Вероятностный алгоритм нахождения квадратичных невычетов.
10. Числа Кармайкла, псевдопростые числа.
11. Вероятностные методы отсеивания составных чисел (тесты Миллера-Рабина, Соловея-Штрассена).
12. Алгоритм Берлекэмпа для разложения многочленов на неприводимые множители над конечным полем.
13. Сведение задачи разложения многочлена на множители к нахождению корней.
14. Нахождение корней многочленов в полях малой характеристики.
15. Вероятностные алгоритмы для нахождения корней многочленов в полях большой характеристики.
16. Условный алгоритм Миллера для доказательства простоты чисел.
17. Детерминированные n±1-методы проверки простоты чисел. Простота чисел Ферма и Мерсенна.
18. Построение больших простых чисел.
19. Полиномиальный детерминированный алгоритм проверки чисел на простоту.
20. Алгоритм Адлемана-Ленстры-Коэна доказательства простоты чисел.
21. Факторизация чисел с экспоненциальной сложностью: метод Ферма, алгоритмы Ленстры и Шермана-Лемана.
22. ρ метод Полларда, p-1 метод Полларда, алгоритм Полларда-Штрассена.
23. Дополнительные стратегии. Алгоритм Бриллхарта - Моррисона.
24. Квадратичное решето.
25. Решето числового поля на примере факторизации числа Ферма F9.
26. Алгоритмы дискретного логарифмирования по простому модулю: метод Гельфонда, алгоритм Поллига-Хеллмана.
27. Алгоритм Адлемана, алгоритм Копперсмитта-Одлыжко-Шреппеля.
28. Дискретное логарифмирование и решето числового поля.
29. Решетки и их свойства.
30. LLL-алгоритм построения приведенного базиса решетки.
31. Факторизация многочленов в Z[x1,...,xm] с полиномиальной сложностью.
32. Построение совместных рациональных приближений и нахождение минимумов квадратичных форм с помощью LLL-алгоритма.
33. Перечень дополнительной учебной литературы, ресурсов информационно-телекоммуникационной сети «Интернет»:

**Приложение утверждено на заседании кафедры теории чисел**