Программа курса

Элементы теории чисел

1 курс, 1 поток, 2020–2021 г.

1. Делимость. Элементарные свойства делимости. Деление с остатком.
2. Наибольший общий делитель и наименьшее общее кратное. Важная лемма.
3. Алгоритм Евклида. Теорема Ламе.
4. Конечные цепные дроби. Рекуррентные соотношения для числителей и знаменателей подходящих дробей.
5. Представление н.о.д. двух чисел в виде их линейной комбинации.
6. Линейные диофантовы уравнения. Матричный алгоритм.
7. Основная теорема арифметики.
8. Мультипликативные функции. Формула обращения Мёбиуса. Мультипликативность функции Эйлера.
9. Сравнения по модулю. Элементарные свойства сравнений. Классы вычетов. Сложение и умножение классов вычетов. Полная и приведённая системы вычетов.
10. Теорема Эйлера, Малая теорема Ферма, теорема Вильсона. Показатель вычета по модулю.
11. Алгоритм шифрования RSA.
12. Китайская теорема об остатках.
13. Мультипликативность количества решений полиномиального сравнения.
14. Количество решений полиномиального сравнения по простому модулю.
15. Подъём решения полиномиального сравнения. Лемма Гензеля.
16. Сравнения второй степени. Квадратичные вычеты. Критерий Эйлера.
17. Символ Лежандра. Элементарные свойства символа Лежандра. Лемма Гаусса.
18. Квадратичный закон взаимности.
19. Символ Якоби и его свойства.
20. Первообразные корни. Существование первообразных корней по простому модулю. Построения общего ключа для шифрования.
21. Бесконечные цепные дроби. Теорема Эйлера–Лагранжа.

Лектор: д.ф.-м.н. Герман О.Н.