

ВОПРОСЫ К ЭКЗАМЕНУ

по обязательному курсу "Теоретико-числовые методы и алгоритмы".

1. Алгоритм Евклида нахождения наибольшего общего делителя. Оценка количества операций деления с остатком. Решение линейных сравнений с помощью алгоритма Евклида. Китайская теорема об остатках.
2. Быстрый алгоритм возведения в степень. Оценка сложности алгоритма.
3. Символы Лежандра и Якоби. Их вычисление. Оценка сложности алгоритма.
4. Решение квадратичных сравнений с помощью алгоритма Шенкса. Оценка сложности алгоритма.
5. Вероятностный алгоритм решения полиномиальных сравнений по простому модулю. Оценка сложности алгоритма и вероятности его успеха.
6. Группа $(Z/mZ)^*$. Теорема Эйлера. Малая теорема Ферма. Вывод явной формулы для функции Эйлера.
7. Существование первообразных корней по простому модулю.
8. Существование первообразных корней по модулю p^n , их количество и способ нахождения.
9. Отсевание составных чисел с помощью малой теоремы Ферма. Числа Кармайкла. Алгоритм Соловья-Штрассена отсеивания составных чисел. Оценка вероятности его успеха.
10. Оценка числа решений сравнения $x^m \equiv a \pmod n$. Оценка числа решений совокупности сравнений вида $x^t \equiv 1 \pmod n$, $x^{2^k t} \equiv -1 \pmod n$.
11. Тест Миллера-Рабина. Его обоснование. Оценка вероятности его успеха.
12. Построение больших простых чисел.
13. Факторизация многочленов над полем Z/pZ с помощью разлагающих многочленов в алгоритме Берлекемпа. Размерность пространства разлагающих многочленов.
14. Алгоритм Берлекемпа. Построение разлагающих многочленов. Обоснование успешности завершения алгоритма Берлекемпа.
15. Сведение задачи разложения на неприводимые множители к нахождению корней многочленов.
16. Алгоритм пробных делений для разложения целых чисел на множители. $(p-1)$ -метод Полларда.
17. ρ -метод Полларда. Эвристическая оценка сложности алгоритма.
18. Алгоритм Диксона разложения чисел на множители. Оценка сложности и вероятности успеха.
19. Цепные дроби. Свойства неполных частных. Подходящие дроби как наилучшие приближения.
20. Алгоритм Бриллхарта-Моррисона разложения чисел на множители с помощью цепных дробей. Эвристическая оценка сложности.
21. Алгоритм Диффи-Хелмана обмена ключами. Дискретное логарифмирование с помощью алгоритма Гельфонда. Оценка сложности.
22. Дискретное логарифмирование с помощью метода Полига-Хеллмана. Оценка сложности.
23. Алгоритм Карацубы умножения целых чисел. Оценка его сложности.
24. Алгоритм RSA. Электронная числовая подпись.
25. Уязвимость схемы RSA при использовании одного и того же модуля.
26. Недостатки использования малого секретного ключа в алгоритме RSA.

Лектор

А.И.Галочкин

Л И Т Е Р А Т У Р А

по обязательному курсу "Теоретико-числовые методы и алгоритмы".

ГН. О.Н.Герман, Ю.В.Нестеренко. Теоретико-числовые методы в криптографии. Есть на сайте кафедры теории чисел.

В. О.Н.Василенко. Теоретико-числовые алгоритмы в криптографии. М. МЦНМО, 2006.

Н. Ю.В.Нестеренко. Теория чисел. М. Академия, 2008.

ЛИТЕРАТУРА ПО ВОПРОСАМ ЭКЗАМЕНА

1. Алгоритм Евклида нахождения наибольшего общего делителя. Оценка количества операций деления с остатком. Решение линейных сравнений с помощью алгоритма Евклида. Китайская теорема об остатках. ГН стр. 60, 61; Н стр. 112 – 116.

2. Быстрый алгоритм возведения в степень. Оценка сложности алгоритма. ГН стр. 67, 68.

3. Символы Лежандра и Якоби. Их вычисление. Оценка сложности алгоритма. Н стр. 134 – 139, 142 – 145. ГН стр. 62 – 67.

4. Решение квадратичных сравнений с помощью вероятностного алгоритма Шенкса. Оценка сложности алгоритма. ГН стр. 75 – 77.

5. Вероятностный алгоритм решения полиномиальных сравнений по простому модулю. Оценка сложности алгоритма и вероятности его успеха. В стр. 167, 168.

6. Группа $(Z/mZ)^*$. Теорема Эйлера. Малая теорема Ферма. Вывод явной формулы для функции Эйлера. Н стр. 70 – 72, 90 – 91.

7. Существование первообразных корней по простому модулю. Н стр. 158 – 161.

8. Существование первообразных корней по модулю p^n , их количество и способ нахождения. Н стр. 164 – 166.

9. Отсевание составных чисел с помощью малой теоремы Ферма. Числа Кармайкла. Алгоритм Соловья-Штрассена отсеивания составных чисел. Оценка вероятности его успеха. В стр. 37, 38.

10. Оценка числа решений сравнения $x^m \equiv a \pmod{n}$. Оценка числа решений совокупности сравнений вида $x^t \equiv 1 \pmod{n}$, $x^{2^k t} \equiv -1 \pmod{n}$. Н стр. 181 – 183; ГН стр. 281, 282, лекция на сайте кафедры теории чисел.

11. Тест Миллера-Рабина. Его обоснование. Оценка вероятности его успеха. Лекция на сайте кафедры теории чисел.

12. Построение больших простых чисел. В стр. 25, 26.

13. Факторизация многочленов над полем Z/pZ с помощью разлагающих многочленов в алгоритме Берлекемпа. Размерность пространства разлагающих многочленов. ГН стр. 106 – 109.

14. Алгоритм Берлекемпа. Построение разлагающих многочленов. Обоснование успешности завершения алгоритма Берлекемпа. ГН стр. 109 – 112.

15. Сведение задачи разложения на неприводимые множители к нахождению корней многочленов. ГН стр. 112 – 115.

16. Алгоритм пробных делений для разложения целых чисел на множители. $(p-1)$ -метод Полларда. ГН стр. 186 – 188, 197 – 198.

17. ρ -метод Полларда. Эвристическая оценка сложности алгоритма. ГН стр. 194 – 197. В стр. 63 – 65.

18. Алгоритм Диксона разложения чисел на множители. Оценка сложности и вероятности успеха. В стр. 78 – 82.

19. Цепные дроби. Свойства неполных частных. Подходящие дроби как наилучшие приближения. Н стр. 189 – 203.

20. Алгоритм Бриллахарта-Моррисона разложения чисел на множители с помощью цепных дробей. Эвристическая оценка сложности. В стр. 84 – 88.

21. Алгоритм Диффи-Хелмана обмена ключами. Дискретное логарифмирование с помощью алгоритма Гельфонда. Оценка сложности. ГН стр. 275 – 276, 219 – 221, В стр. 135.

22. Дискретное логарифмирование с помощью метода Полига-Хеллмана. Оценка сложности. В стр 135, 136.

23. Алгоритм Карацубы умножения целых чисел. Оценка его сложности. В стр. 266, 267 или ГН стр. 92, 93.

24. Алгоритм RSA. Электронная числовая подпись. ГН стр. 277 – 279.

25. Уязвимость схемы RSA при использовании одного и того же модуля. ГН стр. 281, 282.

26. Недостатки использования малого секретного ключа в алгоритме RSA. ГН стр. 283, 284.

МАТЕРИАЛ ЛЕКЦИЙ ОХВАТЫВАЕТ ВСЕ ВОПРОСЫ ЭКЗАМЕНА.