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 вероятностного алгоритма Шенкса.

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. Алгоритм Соловея-Штрассена отсеивания составных чисел. Оценка сложности алгоритма и вероятности его успеха.

10. Отсеивание составных чисел с помощью малой теоремы Ферма. Числа Кармайкла. Тест Миллера-Рабина. Его обоснование (без оценки вероятности успеха).

11. Построение больших простых чисел.

12. Факторизация многочленов над полем Z/pZ с помощью разлагающих многочленов в алгоритме Берлекемпа. Размерность пространства разлагающих многочленов.

13. Алгоритм Берлекемпа. Построение разлагающих многочленов. Обоснование успешности завершения алгоритма Берлекемпа.

14. Сведение задачи разложения на неприводимые множители к нахождению корней многочленов.

15. Алгоритм пробных делений для разложения целых чисел на множители. $(p-1)$-метод Полларда.

16. ρ-метод Полларда. Эвристическая оценка сложности алгоритма.

17. Алгоритм Диксона разложения чисел на множители.

18. Приближения чисел подходящими дробями. Алгоритм Бриллхарта-Моррисона разложения чисел на множители.

19. Дискретное логарифмирование с помощью метода Гельфонда.

20. Дискретное логарифмирование с помощью метода Полига-Хеллмана.

21. Алгоритм Карацубы умножения целых чисел. Оценка его сложности.

22. Алгоритм RSA. Алгоритм Диффи-Хелмана обмена ключами.

23. Алгоритм RSA. Электронная числовая подпись.

24. Оценка числа решений сравнения $x^m \equiv a \mod n$. Уязвимость схемы RSA при использовании одного и того же модуля.

25. 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. 142 – 115. ГН стр. 62 – 67.

4. Решение квадратичных сравнений с помощью вероятностного алгоритма Шенкса. 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. Алгоритм Соловея-Штрассена отсеивания составных чисел. Оценка сложности алгоритма и вероятности его успеха. В стр. 37, 38.

10. Отсеивание составных чисел с помощью малой теоремы Ферма. Числа Кармайкла. Тест Миллера-Рабина. Его обоснование (без оценки вероятности успеха). ГН стр. 78 – 81.

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

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

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

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

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

16. ρ-метод Полларда. Эвристическая оценка сложности алгоритма. ГН стр. 194 – 197.

17. Алгоритм Диксона разложения чисел на множители. В стр. 78 – 82.

18. Приближения чисел подходящими дробями. Алгоритм Бриллхарта-Моррисона разложения чисел на множители. В стр. 84 – 88.

19. Дискретное логарифмирование с помощью метода Гельфонда. ГН стр. 219 – 221.

20. Дискретное логарифмирование с помощью метода Полига-Хеллмана. ГН стр. 221 – 224.

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

22. Алгоритм RSA. Алгоритм Диффи-Хелмана обмена ключами. ГН стр. 275 – 278.

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

24. Оценка числа решений сравнения $x^m \equiv a \mod n$. Уязвимость схемы RSA при использовании одного и того же модуля. Н стр. 181 – 183; ГН стр. 281, 282.

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

МАТЕРИАЛ ЛЕКЦИЙ ОХВАТЫВАЕТ ВСЕ ВОПРОСЫ ЭКЗАМЕНА.