РАЗДЕЛЫ ИЗ ПРОГРАММЫ КУРСА, КОТОРЫЕ ВКЛЮЧЕНЫ В ТЕСТ

1. Примеры алгоритмов: проверка простоты, факторизация чисел; Одновременное вычисление максимального и минимального элементов в массиве; быстрое умножение чисел и матриц (алгоритмы Карацубы и Штрассена); аддитивные цепочки.

Модели вычислений. Формальное определение алгоритма. Различные определения трудоемкости алгоритма.

2. Асимптотические оценки. Нотация: $O(\cdot), o(\cdot), \Omega(\cdot), \omega(\cdot), \Theta(\cdot)$. Алгоритмы типа "разделяй-и-властвуй". основная теорема о рекуррентных оценках (нахождение асимптотики рекуррентности вида $T(n) = aT(\frac{n}{b}) + f(n)$). Дерево рекурсии. Линейный алгоритм нахождения медианы массива. Линейные рекуррентные последовательности.

3. Потоки и разрезы в сети. Теорема о максимальном потоке и минимальном разрезе. Понятие остаточного графа и увеличивающего пути. Алгоритм Форда-Фалкерсона для вычисления максимального потока и минимального разреза. Задача о максимальном потоке минимальной стоимости. Обобщения потоковой сети (пропускные способности узлов и пр.). Приложение потоковых алгоритмов: цепное разложение порядков (лемма Дилворта), задача о максимальном паросочетании в двудольном графе, задача о назначениях, расписание с прерываниями на идентичных процессорах.

4. Алгоритмы сортировки: пузырек; быстрая сортировка (quicksort); сортировка с помощью кучи; слияние; цифровая сортировка. Анализ трудоемкости алгоритма quicksort по наихудшему случаю и в среднем. Устойчивость алгоритма сортировки. Нижние оценки сортировки. Разрешающие деревья. Порядковые статистики. Схемы сортировки.

5. Обобщенный алгоритм Евклида. Модульная арифметика. Китайская теорема об остатках. Функция Эйлера. Первообразные корни. Кольца $\mathbb{Z}_n$, в которых существуют первообразные корни. Индексы (дискретные логарифмы). Кодирование с открытым ключом. Квадратичные вычеты. Схема RSA.

Распределение задач теста 23 марта по разделам

1. Оценки, лрп, основная теорема о рекуррентностях.
2. Сортировка и числа.
3. Числовые алгоритмы
4. Потоки в сети
5. Повторительные задачи.

Определения, теоремы, алгоритмы, которые могут использоваться в тесте

Определения и понятия.

Первообразный корень, обратный остаток, порядок элемента в группе вычетов, φ-функция Эйлера, индекс.

Потоковая сеть, остаточный граф, увеличивающий путь, разрез.

Дерево рекурсии.

Разрешающее дерево для алгоритмов сортировки.

Теоремы.

Основная теорема о рекуррентных оценках.
Теорема о максимальном потоке и минимальном разрезе.
Малая теорема Ферма.
Нижние оценки для сортировки.
Китайская теорема об остатках.

Алгоритмы.

Числа

Решето Эратосфена.
Алгоритм Эвклида.
Метод Гаусса решения ситем линейных уравнений.
Быстрое умножение и возведение в степень чисел и матриц.
Построение общего множества решений ЛРП.
Система RSA (кодирование, декодирование, электронная подпись).
Решение линейных диофантовых уравнений.

Потоки

Алгоритм Форда-Фалкерсона нахождения максимального потока и минимального разреза (тут 2 алгоритма, сколь бы ни прост был второй).

Сортировка.

Поиск минимума.
Одновременный поиск максимума и минимума.
Алгоритмы сортировки (пузырек, слияние, куча, quicksort).
Линейные алгоритмы поиска медианы (детерминированный и вероятностный); порядковые статистики (поиск k-о элемента).

ЛИТЕРАТУРА

Основная

1. Ахо А., Хопкрофт Д., Ульман Д.*Построение и Анализ Вычислительных Алгоритмов.* М.: Мир, 1979.
1. Гери М., Джонсон Д. *Вычислительные машины и труднорешаемые задачи.* М.: Мир, 1982.
3. **[Кормен 1]** Кормен Т., Лейзерсон Ч., Ривест Р. *Алгоритмы: Построение и Анализ.* М.: МЦНМО, 2002.
4. **[Кормен 2]** Кормен Т., Лейзерсон Ч., Ривест Р., Штайн К. *Алгоритмы: Построение и Анализ. (2-е изд.)* М.: Вильямс, 2005.
5. Кузюринн Н., Фомин С. *Эффективные алгоритмы и сложность вычислений.* М.: МФТИ, 2007.

Дополнительная

1. Верещагин Н., Шень А. *Вычислимые Функции.* М.: МЦНМО, 1999. (Электронный вариант: www.mccme.ru/free-books)
2. Виноградов И. *Основы теории чисел.* М.-Л.: Гостехиздат, 1952
3. Вялый М., Журавлев Ю., Флеров Ю. *Дискретный анализ. Основы высшей алгебры.* М.: МЗ Пресс, 2007.
4. **К-Ш-В** Китаев А., Шень А., Вялый М. *Классические и квантовые вычисления.* М.: МНЦМО-ЧеРо, 1999.
4. **Хинчин** Хинчин А. Цепные дроби. М.: Наука, 1979.
6. Шень А. *Программирование. Теоремы и задачи.* М.: МЦНМО, 2007. (Электронный вариант: www.mccme.ru/free-books)
7. Lovasz L. *Computational complexity.* www.cs.elte.hu/ lovasz/complexity.pdf

Вариант для подготовки с подсказками Он может сильно отличаться от теста.

Числа

1. (i) Для последовательности Фибоначчи $F_0 = 1, F_1 = 1, F_{n+1} = F_n + F_{n-1}$ найдите НОД(F_{n+1}, F_n).

Подсказка. Из определения $F_{n+1} = F_{n-1} \pmod{F_n}$. Следовательно, НОД$(F_{n+1}, F_n)$= НОД$(F_n, F_{n-1})$.

(*ii*) Сколько элементов кольца целых $\pmod{13^3}$ обратимы?

Подсказка. Эту величину можно вычислить непосредственно или вспомнить о функции Эйлера.

(*iii*) Найдите подходящие ключи для системы RSA с модулем $N = 7 \cdot 11$.

Ответ. Подойдут, например, 7 и 43.

(*iv*) Вычислите $2^{2^{2013}} \pmod 3$.

Подсказка. $2^2 = 1 \pmod 3$, поэтому $(2^2)^{2012} = 1 \pmod 3$.

Сортировка

2. (*i*) Все целые числа из отрезка перемешали, а потом одно число выкинули. Предложите, как можно более быстрый алгоритм иденфикации удаленного числа.

Подсказка. Можно воспользоваться принципом "разделяй-и-властвуй" или работать с битовыми записями чисел.

(*ii*) Верно ли, что для любого n можно подобрать вход, на котором алгоритм быстрой сортировки с рандомизацией проведет $const \cdot n^2$ сравнений ($const$ от n не зависит)?

Подсказка. Нужно вспомнить, для чего и как используется рандомизация в алгоритме быстрой сортировки

(*iii*) Ниже сформулирована известная (в некоторых кругах) задача, т.н. majority problem. Дан массив $A[1..n]$ с повторяющимися элементами. Назовем некоторый элемент **частым**, если он встречается больше, чем $\lceil \frac{n}{2} \rceil$ раз. Нужно разработать как можно более быструю процедуру идентификации такого элемента, если он существует.

Простой вариант: на элементах A определено отношение полного порядка (скажем, элементы — числа).

Подсказка. Тут хорошо бы вспомнить порядковые статистики.

Сложный вариант: элементы A — записи, скажем, картинки.

Подсказка. Задача имеет в этом случае простое, красивое и нетривиальное решение!

Оценки

3. Найдите Θ-асимптотики следующих рекуррентностей:

(*i*) $T(n) = 2013T(\frac{n}{2012}) + n^{2.011}$;

(*ii*) $T(n) = T(n-1) + n\sqrt{n}$ю

(*iii*) Найдите трудоемкость детерминированного алгоритма вычисления медианы массива (процедура "Выбор" в Кормене), если исходный массив бьется на тройки, а не на пятерки.

Подсказка. Стандартные аргументы приводят в этом случае к оценке $O(n \log n)$.

Потоки

4. (*i*) Верно ли, что величина минимального разреза не увеличивается при удалении произвольного ребра потоковой сети? (Вы должны привести формальные аргументы.)