Домашнее задание по АМВ

771 группа, Христолюбов Максим

28 апреля 2019 г.

1 Задача 1

$d = e^{-1} (\mod (p-1)(q-1)) = 3^{-1} (\mod 352) = 235 (\mod 352)$
$y = x^e (\mod N) = 41^3 = 352 \cdot 41 (\mod 391) = 105 (\mod 391)$
$x = y^d (\mod N) = 105^{235} (\mod 391) = 41 (\mod 391)$

2 Задача 2

Злоумышленник может умножить d на e и получить число, которое, как известно, равно 1 по модулю $(p-1)(q-1)$. Вычислив число $de - 1$ он может перебирать все делители этого числа, которых полиномиальное от $\log(de-1) O(\log(de))$ количество и которые являются кандидатами на $(p-1)(q-1)$. Для каждого делителя он может перебрать все его разложение на 2 множителя, которые являются кандидатами на $p-1$ и $q-1$, которых тоже полиномиальное от $\log(p-1)(q-1) = O(\log(de))$ количество. Кандидаты на p и q оцениваются по длине, и если их суммарная длина не больше длины N, то их произведение может быть равно N, поэтому они перемножаются, и среди находятся те, что $pq = N$. Перемножение чисел, чья запись не больше N, $O(\log N)$. Таким образом за полиномиальное время $O(\log^2(de) \log N)$ находится разложение N на p и q.

3 Задача 3

То есть $A^{ed} = A (\mod N) = A^{2021d} = A (\mod 25) = A^d = A (\mod 25)$, $d = \phi(25) = 20$.

4 Задача 4

а) Можно сравнить между собой два средних элемента массива. Если $a_k \leq a_{k+1}$, то значит, a_k точно не максимум. Тогда сравним a_{k+3} и a_{k+4} и в дальнейшем будем двигаться вправо от центра (как далее поясняется). В противоположном случае будем сравнивать a_{k-3} и a_{k-2}, и двигаться влево от центра, аналогично тому как двигались бы вправо.

Если оказалось, что $a_{k+3} \geq a_{k+4}$, то следующими 2 шагами можно найти горку. Сравним a_{k+1} и a_{k+2}, если $a_{k+1} \geq a_{K+2}$, то a_{k+1} горка, иначе сравним a_{k+2} и a_{k+3}, и зависимости от результата горкой окажется либо a_{k+2}, либо a_{k+3}.

Если оказалось, что $a_{k+3} < a_{k+4}$? то сравним a_{k+6} и a_{k+7}, и проделаем с ними те же действия, что и в предыдущем абзаце. Либо $a_{k+6} \geq a_{k+7}$, то следующими 2 шагами находим горку, иначе продолжаем со сравнением a_{k+9} и a_{k+10} и т. д.

Так будет продолжаться либо пока горка не найдется, либо не дойдем до правого конца массива. Тогда сравнив a_{n-1} и a_n, и либо a_n окажется горкой, либо a_{n-1} окажется горкой, поскольку на предыдущем шаге горка не нашлась, а значит, либо $a_{n-2} \leq a_{n-1}$, либо, если они не сравнивались, то 2 сравнениями a_{n-2} с a_{n-3}, которое больше a_{n-4}, и с a_{n-1}, горка будет найдена. Всего на движение от центра до края уйдет не более $\frac{n+2}{3}$ сравнений и еще 2 в худшем случае. Значит, асимптотика $\Omega(\frac{n+8}{3})$.

5 Задача 5

Заменим граф G на $\overline{G}$, в котором все ребра из G остутствуют, а отсутсвующие присутствуют. Тогда разбиение графа G на 2 клики будет совпадать с разбиением графа $\overline{G}$ на 2 доли. Проверить можно ли разбить так граф займет полинмиальное время: будем перебирать вершины и рассматривать соседние вершины, относя их в другую долю. Если так разделить получилось, то G тоже можно разбить на 2 клики, а если нет, то значит где то в $\overline{G}$ есть цикл из вершин, соединенные попарно, нечетной длины, поэтому и разбить на 2 доли его нельзя, а значит и G не рахбить на 2 клики. Так как $P \neq NP$, то эта задача не NPC.

6 Задача 6

Условие на граф эквивалентно тому, что существуют пути из s в t длины 10 и 11, так как, все остальные пути можно получить перемещаясь вперед-назад по какому-то ребру. Проверить есть ли такие пути можно за полиномиальное время. Будем строить всевозможные пути длины 10 и 11 из s и смотреть есть ли среди них те, которые оканчиваются в t. Построить один путь можно за константое время переходами по спискам смежности. Всего путей длины 11 не более $n^1 1$, где n — кол-во вершин графа. Значит, их все можно перебрать за полиномиальное время и определить есть ли пути такой длины. Значит задача лежит в P, аследовательно и в $co - NP$.

7 Задача 7

Отсортируем ребра по убыванию веса за $O(m \log m)$. Так как сложность раскраски это максимальный вес ребра, чьи вершины закрашены в один цвет, то единственное о чем нужно заботиться — так это о том, чтоб максимальное количество ребер с максимальным весом были между вершинами разных цветов. Возьмем первое ребро из списка, отсортированного по убыванию, и раскрасим его вершины в 2 разных цвета. Так же поступим со следующим. Так будем продолжать, пока не окажется, что обе вершины ребра уже окрашены в один цвет. Это будет значить, что нельзя раскрасить граф лучше, так как любое изменение в уже проведенной раскраске приведет к тому, что ребро еще большего веса окажется окрашено в один цвет, и сложность раскраски будет больше, чем с ребром, которое оказалось раскрашено в один цвет на данном этапе. Остальные вершины можно раскрасить как угодно, на сложность раскраски это никак не повлияет. Таким образом действий было совершено $O(m \log m) + O(m) = O(m \log m)$ как и требовалось.

$a = \{a_1, \dots, a_n\}, b = \{b_1, \dots, b_n\}$

$DTW(a,b) = ?$

Построим матрицу $\Omega = \Omega(a,b)$: $\Omega_{ij} = |a_i - b_j|$.

Путь из (1,1) в (n,n) в матрице Ω:

$\pi = \{\pi_r\} = \{(i_r,j_r)\}$, причем путь непрерывен и монотонен.

Стоимость пути π: $S(\Omega,\pi) = \sum\limits_{(i,j)\in\pi} \Omega_{ij}$

$DTW(a,b) = \min\limits_{\pi} S(\Omega(a,b),\pi)$

1) Для каждого класса построим матрицу W попарных расстояний между объектами этого класса. и понизим ее размерность методом главных компонент.

Центроидом класса D_e по расстоянию ρ приближенно считаем

$z_e = \underset{z\in D_e}{argmin} \sum\limits_{s_i\in D_e} \rho(W^T s_i, W^T z)$

2) Построим матрицу $X = D \times D_e$, в которой у каждого объекта

признаками выступают расстояния $\rho(x,z_e)$.

3) Будем решать задачу классификации на полученных признаках X методом k ближайших соседей.

По матрице Ω построим матрицу S кратчайших стоимостей путей из (1,1) в (i,j) в Ω, таким образом, что

$S_{11} = \Omega_{11}$

$S_{ij} = \Omega_{ij} + \min(S_{i(j-1)},S_{(i-1)j},S_{(i-1)(j-1)})$

Тогда $DTW(a,b) = S_{nn}$