EECS 212

Northwestern 2019

Homework 8

Due at 3:59pm, June 4th (Tuesday), 2019

Congratulations! Finally you are here!

Scoring: There are total 20 points in this homework. Problem 1 and Problem 4 carries 3 points each. Problem 2 carries 8 points. Problem 3 carries 6 points.

Please write down sufficient steps how you get the result. Simply writing down a final answer will not give your full credit. You are responsible for any mistake resulted from illegible submissions.

Problem 1

For any two positive integers a, b, define $k(a, b)$ to be the largest k such that $a^k \mid b$ but $a^{k+1} \nmid b$. Given two positive integers x, y, show that

(a) $k(a, gcd(x, y)) = \min\{k(a, x), k(a, y)\}$ for any positive integer a.

(b) $k(a, lcm(x, y)) = \max\{k(a, x), k(a, y)\}$ for any positive integer a.

Hint: Think of the prime factorization of the numbers.

Problem 2

Consider any regular simple graph G on n vertices of degree d and let A be its adjacency matrix. Consider the matrix $L = dI - A$ where I is the identity matrix of size $n \times n$ (it has 1s on the diagonal and 0 elsewhere). For any set $S \subseteq \{1, 2, \ldots, n\}$, let $1_S \in \mathbb{R}^n$ be a vector such that the jth co-ordinate is $1_S(j) = 1$ if $j \in S$ and $1_S(j) = 0$ if $j \notin S$.

(a) Show that for any vector $x \in \mathbb{R}^n$ show that

$$x^T L x = \sum_{(i,j) \in E} (x_i - x_j)^2.$$

Note that in the right hand side of the above formula, there are $nd/2$ terms; one term for each edge in E. Hence both (i, j) and (j, i) are both captured by one term that corresponds to the edge between i, j.

(b) Show that $(1_S^T L 1_S)$ is the number of edges between the set of vertices S and the rest of graph (i.e. number of edges (u, v) such that $u \in S$ and $v \in \{1, 2, \ldots, n\} \setminus S$).

(c) Show that the matrix A has an eigenvalue of d.

(d) Show that if the graph is disconnected, there are at least two eigenvalues equal to d (note that you need to exhibit two eigenvectors of this graph, whose eigenvalue is d).

Problem 3

A general would like to count his soldiers before a battle, but they are too numerous for him to do so by counting them one by one. Instead, he asks his soliders to get into a number of different formations consisting of rows of particular lengths. He can then determine the total number of solider by counting the number of soldiers remaining who do not form a complete row in each of these formations. In this problem, we will find out how he can do so.

Let $m_1, m_2, \ldots, m_k$ be k prime numbers. For some unknown positive integer x, suppose following relations holds:

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\cdots \\ x &\equiv a_k \pmod{m_k} \end{aligned} \tag{1}$$

We want to find the smallest x that satisfies the above congruence relations. Let $M = m_1 m_2 \ldots m_k$ and $M_i = M/m_i$.

(a) Show that there exists some integer M_i^{-1} such that

$$\begin{aligned} a_i M_i M_i^{-1} &\equiv a_i \pmod{m_i} \\ a_i M_i M_i^{-1} &\equiv 0 \pmod{m_j} \text{ for } (i \neq j). \end{aligned}$$

(b) Show that

$$x_0 \equiv (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + \cdots + a_k M_k M_k^{-1}) \mod M$$

satisfies the above relations.

(c) Show that if x_1, x_2 both satisfy the above relations given by (1), then $x_1 - x_2$ is a multiple of $M = m_1 m_2 \ldots m_k$. Use this to conclude that x_0 is indeed the smallest positive integer satisfying the above relations.

Hint: Use the fact that if $gcd(m,p) = 1$ then there is some m' (which we will denote by m^{-1}) such that $mm' \equiv m'm \pmod{p} \equiv 1 \pmod{p}$.

Problem 4

In class we know that, for two positive integers a, b, there exists two positive integers s, t such that

$$sa + tb = \gcd(a, b).$$

In this problem, we will modify the Euclids Algorithm to find the s and t.

$\mathbf{gcd}'(a, b)$

1. If $a < b$, swap a, b
2. $r \leftarrow \text{remainder}(a, b)$
3. If $r = 0$, return $(0, 1)$;
4. $(s', t') \leftarrow \mathbf{gcd}'(b, r)$
5. return $(t', s' - (a - r)t'/b)$

We will figure out why the above algorithm works in part (a) and (b).

Let $r = \text{remainder}(a, b)$ and assume

$$s'b + t'r = \gcd(b, r)$$

when $r > 0$.

(a) Show that if $r = 0$, then $s = 0$ and $t = 1$.

(b) Show that if $r > 0$,

$$t'a + (s' - \frac{(a-r)t'}{b})b = \gcd(a, b)$$

Hint: Represent r using $r = a - (a - r)/b \cdot b$.

Problem 5 (Optional: not for grade)

Suppose we have some data points $(m_1, a_1), \ldots, (m_k, a_k) \in \mathbb{R}^2$, we want to find a polynomial $p(x)$ of degree $k - 1$ such that $p(m_i) = a_i$ for $i = 1, \ldots, k$.

It turns out that we can actually use the idea of Problem 3 to find this $p(x)$. In fact, we can view this problem in the same format as that of Problem 4:

Find $p(x)$ with degree less than $k-1$, satisfying

$$\begin{aligned} p(x) &\equiv a_1 \mod (x - m_1) \\ p(x) &\equiv a_2 \mod (x - m_2) \\ &\dots \\ p(x) &\equiv a_k \mod (x - m_k) \end{aligned}$$

(a) Find an analogy for the M_i and M_i^{-1} respectively in this problem.

(b) Construct a $p(x)$ using the same manner as part (b) of Problem 3. Verify that your $p(x)$ indeed satisfy $p(m_i) = a_i$ for $i = 1, \dots, k$.