CS 70 Discrete Mathematics and Probability Theory
Spring 2020

Quiz 3

1. [True or False?] The following questions refer to stable matching instances with n jobs and n candidates.

(a) □ In any stable matching instance, in the pairing the Propose-and-Reject produces there is some job who gets their favorite candidate (the first candidate on their preference list).

(b) □ It is possible for a stable matching to have a job A and a candidate 1 be paired if A is 1's least preferred choice and 1 is A's least preferred choice.

Solution:

(a) **False.** Let job A have preference list $(1,3,2)$, B have $(1,2,3)$, and C have $(2,1,3)$. We develop a "cyclic" chain of preferences, causing A to displace B to displace C who then displaces A.

   (a) If candidate 1 prefers A over B, she puts A on a string and rejects B.

   (b) B does not get their favorite and proposes to 2, who prefers B over C and thus rejects C.

   (c) C does not get their favorite and proposes to 1, who prefers C over A and thus rejects A.

   Thus, A also does not get their favorite, and no job gets their favorite.

(b) **True.**
A and 1 are respectively all the candidate's and job's least favorite. Job A proposes to everyone in their list and gets rejected by all of them until they gets to their last option who is candidate 1. On the other hand no one proposes to candidate 1 until the day that job A proposes to her.

2. [True or False?]

(a) □ A graph with k edges and n vertices has a vertex of degree at least $2k/n$.

(b) □ If $e \leq 3v - 6$ holds for a graph G, then G is planar.

(c) □ If all vertices of an undirected graph have degree 4, the graph must be the complete graph on five vertices, K_5.

Solution:

(a) **True.**
The sum of degrees is $2k$. Since there are n vertices, the average vertex degree is $2k/n$ and hence there is at least one vertex with degree at least $2k/n$.

(b) **False.**
The graph $K_{3,3}$ is not planar. It has $e = 9$ and $v = 6$ which satisfy the condition $e \leq 3v - 6$.

(c) **False.**
Consider the 4-dimensional hypercube. Each vertex has exactly 4 neighbors, but it is not K_5.

3. [Coloring Trees]

Prove that all trees with at least 2 vertices are *bipartite*: the vertices can be partitioned into two groups so that every edge goes between the two groups.

[*Hint:* Use induction on the number of vertices.]

Solution:

Proof using induction on the number of vertices n.

Base case $n = 2$. A tree with two vertices has only one edge and is a bipartite graph by partitioning the two vertices into two separate parts.

Inductive hypothesis. Assume that all trees with k vertices for an arbitrary $k \geq 2$ is bipartite.

Inductive step. Consider a tree $T = (V,E)$ with $k+1$ vertices. We know that every tree must have at least two leaves, so remove one leaf u and the edge connected to u, say edge e. The resulting graph $T - u$ is a tree with k vertices and is bipartite by the inductive hypothesis. Thus there exists a partitioning of the vertices $V = R \cup L$ such that there does not exist an edge that connects two vertices in L or two vertices in R. Now when we add u back to the graph. If edge e connects u with a vertex in L then let $L' = L$ and $R' = R \cup \{u\}$. On the other hand if edge e connects u with a vertex in R then let $L' = L \cup \{u\}$ and $R' = R$. L' and R' gives us the required partition to show that T is bipartite. This completes the inductive step and hence by induction we get that all trees with at least 2 vertices are bipartite.

CS 70 Discrete Mathematics and Probability Theory
Spring 2020 DIS 3B

1 Baby Fermat

Assume that a does have a multiplicative inverse mod m. Let us prove that its multiplicative inverse can be written as $a^k \pmod{m}$ for some $k \geq 0$.

(a) Consider the sequence $a, a^2, a^3, \ldots \pmod{m}$. Prove that this sequence has repetitions. (**Hint:** Consider the Pigeonhole Principle.)

(b) Assuming that $a^i \equiv a^j \pmod{m}$, where $i > j$, what can you say about $a^{i-j} \pmod{m}$?

(c) Prove that the multiplicative inverse can be written as $a^k \pmod{m}$. What is k in terms of i and j?

Solution:

(a) There are only m possible values mod m, and so after the m-th term we should see repetitions.

The Pigeonhole principle applies here - we have m boxes that represent the different unique values that a^k can take on $\pmod{m}$. Then, we can view $a, a^2, a^3, \cdots$ as the objects to put in the m boxes. As soon as we have more than m objects (in other words, we reach a^{m+1} in our sequence), the Pigeonhole Principle implies that there will be a collision, or that at least two numbers in our sequence take on the same value $\pmod{m}$.

(b) We will temporarily use the notation a^* for the multiplicative inverse of a to avoid confusion. If we multiply both sides by $(a^*)^j$ in the third line below, we get

$$\begin{aligned}
a^i &\equiv a^j && \pmod{m}, \\
a^{i-j}\underbrace{a\cdots a}_{j \text{ times}} &\equiv \underbrace{a\cdots a}_{j \text{ times}} && \pmod{m}, \\
a^{i-j}\underbrace{a\cdots a}_{j \text{ times}}\cdot\underbrace{a^*\cdots a^*}_{j \text{ times}} &\equiv \underbrace{a\cdots a}_{j \text{ times}}\cdot\underbrace{a^*\cdots a^*}_{j \text{ times}} && \pmod{m}, \\
a^{i-j} &\equiv 1 && \pmod{m}.
\end{aligned}$$

(c) We can rewrite $a^{i-j} \equiv 1 \pmod{m}$ as $a^{i-j-1}a \equiv 1 \pmod{m}$. Therefore a^{i-j-1} is the multiplicative inverse of $a \pmod{m}$.

2 Bijections

Let n be an odd number. Let $f(x)$ be a function from $\{0,1,\dots,n-1\}$ to $\{0,1,\dots,n-1\}$. In each of these cases say whether or not $f(x)$ is necessarily a bijection. Justify your answer (either prove $f(x)$ is a bijection or give a counterexample).

(a) $f(x) = 2x \pmod n$.

(b) $f(x) = 5x \pmod n$.

(c) n is prime and

$$f(x) = \begin{cases} 0 & \text{if } x = 0, \\ x^{-1} \pmod n & \text{if } x \neq 0. \end{cases}$$

(d) n is prime and $f(x) = x^2 \pmod n$.

Solution:

(a) Bijection, because there exists the inverse function $g(y) = 2^{-1}y \pmod n$. Since n is odd, $\gcd(2,n) = 1$, so the multiplicative inverse of 2 exists.

(b) Not necessarily a bijection. For example, $n = 5, f(0) = f(1) = 0$.

(c) Bijection, because the multiplicative inverse is unique.

(d) Definitely not a bijection. For example, if $n = 3$, $f(1) = f(2) = 1$.

3 Introduction to Chinese Remainder Theorem

Solve for $x \in \mathbb{Z}$ where

$$\begin{aligned} x &\equiv 3 \pmod{11}, \\ x &\equiv 7 \pmod{13}. \end{aligned}$$

(a) Find the multiplicative inverse of 13 modulo 11.

(b) What is the smallest $b \in \mathbb{Z}^+$ such that $13 \mid b$ and $b \equiv 3 \pmod{11}$?

(c) Find the multiplicative inverse of 11 modulo 13.

(d) What is the smallest $a \in \mathbb{Z}^+$ such that $11 \mid a$ and $a \equiv 7 \pmod{13}$?

(e) Now, write down the set of possible solutions for x.

Solution:

(a) 6.

(b) We want to make sure that $b \equiv 0 \bmod 13$, we can see that 13×3 satisfies this requirement. To make sure b is still equivalent to 3 mod 11, we can multiply by the multiplicative inverse of 13 mod 11, which is 6 (from the last part). Although $13 \times 6 \times 3$ yields a correct answer, it is not the smallest number that meets both requirements. To do so, we can apply the modulus before multiplying by 13, giving us

$13 \times ((6 \times 3) \bmod 11) = 91$

(c) 6.

(d) Following a similar process to part (b), we get $11 \times ((6 \times 7) \bmod 13) = 33$

(e) $x \equiv 91 + 33 \pmod{\operatorname{lcm}(11,13)} \equiv 124 \pmod{143}$.