CS 70 Discrete Mathematics and Probability Theory
Fall 2015 Rao HW 4

Due Wednesday Sept 23 at 10PM

1. **(Trees)** Recall that a **tree** is a connected acyclic graph (graph without cycles). In the note, we presented a few other definitions of a tree, and in this problem, we will prove two fundamental properties of a tree, and derive two definitions of a tree we learn from lecture note based on these properties. Let's start with the properties:

   (a) Prove that any pair of vertices in a tree are connected by exactly one (simple) path.

   Answer: Pick any pair of vertices x, y. We know there is a path between them since the graph is connected. We will prove that this path is unique by contradiction:
   Suppose there are two distinct paths from x to y. At some point (say at vertex a) the paths must diverge, and at some point (say at vertex b) they must reconnect. So by following the first path from a to b and the second path in reverse from b to a we get a cycle. This gives the necessary contradiction.

   (b) Prove that adding any edge to a tree creates a simple cycle.

   Answer: Pick any pair of vertices x, y not connected by an edge. We prove that adding the edge $\{x,y\}$ will create a simple cycle. From part (a), we know that there is a unique path between x and y. Therefore, adding the edge $\{x,y\}$ creates a simple cycle obtained by following the path from x to y, then following the edge $\{x,y\}$ from y back to x.

   Now you will show that if a graph satisfies either of these two properties then it must be a tree:

   (c) Prove that if every pair of vertices in a graph are connected by exactly one simple path, then the graph must be a tree.

   Answer: Assume we have a graph with the property that there is a unique simple path between every pair of vertices. We will show that the graph is a tree, namely, it is connected and acyclic. First, the graph is connected because every pair of vertices is connected by a path. Moreover, the graph is acyclic because there is a unique path between every pair of vertices. More explicitly, if the graph has a cycle, then for any two vertices x, y in the cycle there are at least two simple paths between them (obtained by going from x to y through the right or left half of the cycle), contradicting the uniqueness of the path. Therefore, we conclude the graph is a tree.

   (d) Prove that if the graph has no simple cycles and has the property that the addition of any single edge (not already in the graph) will create a simple cycle, then the graph is a tree.

   Answer: Assume we have a graph with no simple cycles, but adding any edge will create a simple cycle. We will show that the graph is a tree. We know the graph is acyclic because it

has no simple cycles. To show the graph is connected, we prove that any pair of vertices x, y are connected by a path. We consider two cases: If $\{x,y\}$ is an edge, then clearly there is a path from x to y. Otherwise, if $\{x,y\}$ is not an edge, then by assumption, adding the edge $\{x,y\}$ will create a simple cycle. This means there is a simple path from x to y obtained by removing the edge $\{x,y\}$ from this cycle. Therefore, we conclude the graph is a tree.

2. **(Combining moduli)** Suppose we wish to work modulo $n = 40$. Note that $40 = 5 \times 8$, with $\gcd(5,8) = 1$. We will show that in many ways working modulo 40 is the same as working modulo 5 and modulo 8, in the sense that instead of writing down $c \pmod{40}$, we can just write down $c \pmod 5$ and $c \pmod 8$.

   (a) What is $8 \pmod 5$ and $8 \pmod 8$? Find a number $a \pmod{40}$ such that $a \equiv 1 \pmod 5$ and $a \equiv 0 \pmod 8$.

   Answer: $8 \equiv 3 (\text{mod } 5)$ and $8 \equiv 0 (\text{mod } 8)$. We can find such a number by considering multiples of 8, i.e. 0, 8, 16, 24, 32, and find that if $a = 16$, $16 \equiv 1 (\text{mod } 5)$. Therefore 16 satisfies both conditions.

   (b) Now find a number $b \pmod{40}$ such that $b \equiv 0 \pmod 5$ and $b \equiv 1 \pmod 8$.

   Answer: We can find such a number by considering multiples of 5,i.e.0,5,10,15,20,25,30,35, and find that if $b = 25$, $25 \equiv 1 (\text{mod } 8)$, so it satisfies both conditions.

   (c) Now suppose you wish to find a number $c \pmod{40}$ such that $c \equiv 2 \pmod 5$ and $c \equiv 5 \pmod 8$. Find c by expressing it in terms of a and b.

   Answer: We claim $c \equiv 2a + 5b \equiv 37 (\text{mod } 40)$. To see that $c \equiv 2 (\text{mod } 5)$, we note that $b \equiv 0 (\text{mod } 5)$ and $a \equiv 1 (\text{mod } 5)$. So $c \equiv 2a \equiv 2 (\text{mod } 5)$. Similarly $c \equiv 5b \equiv 5 (\text{mod } 8)$.

   (d) Repeat to find a number $d \pmod{40}$ such that $d \equiv 3 \pmod 5$ and $d \equiv 4 \pmod 8$.

   Answer: We can repeat the same procedure as above, and find that $d = 3a + 4b \equiv 28 (\text{mod } 40)$.

   (e) Compute $c \times d \pmod{40}$. Is it true that $c \times d \equiv 2 \times 3 \pmod 5$, and $c \times d \equiv 5 \times 4 \pmod 8$?

   Answer: $c \times d = 37 \times 28 \equiv 36 \pmod{40}$. Note that if $a \equiv b \pmod n$ and $c \equiv d \pmod n$ then $a \times c \equiv b \times d \pmod n$.Therefore we can multiply $c \equiv 2 \pmod 5$ and $d \equiv 3 \pmod 5$ to get $c \times d \equiv 2 \times 3 \pmod 5$. Similarly we can multiply these equations (mod 8) and get $c \times d = 5 \times 4 \pmod 8$.

3. **(The last digit)**
   Let a be a positive integer. Consider the following sequence of numbers x defined by:

$$\begin{aligned} x_0 &= a \\ x_n &= x_{n-1}^2 + x_{n-1} + 1 \text{ if } n > 0 \end{aligned}$$

(a) Show that if the last digit of a is 3 or 7, then for every n, the last digit of x_n is respectively 3 or 7.

Answer: To answer this question, we can study how the last digit of x_n changes from n to $n+1$. We have the following table:

$x_n \bmod 10$	$x_{n+1} \bmod 10$
0	1
1	3
2	7
3	3
4	1
5	1
6	3
7	7
8	3
9	1

(b) Show that there exist $k > 0$ such that the last digit of x_n for $n \geq k$ is constant. Give the smallest possible k,
no matter what a is. **Answer:** 3 and 7 appear as our fixed points. Once we reach one of these, we stay there for all the following iterations by the previous question. But it is not immediate that we always reach one of the fixed points, and this is what we need to prove. Let's unroll each of the 10 cases for a for a few iterations and verify that we always reach 3 or 7.

$a \bmod 10$	$x_1, x_2, \ldots \bmod 10$
0	1, 3, 3, 3, ...
1	3, 3, 3, ...
2	7, 7, 7, ...
3	3, 3, 3, ...
4	1, 3, 3, 3, ...
5	1, 3, 3, 3, ...
6	3, 3, 3, 3, ...
7	7, 7, 7, 7, ...
8	3, 3, 3, 3, ...
9	1, 3, 3, 3, ...

This case-splitting proves the claim. We can see from the table that $k = 2$ is the smallest constant such that the last digit of x_n is constant for $n \geq k$.

4. Here are some questions about Eulerian and hamiltonian cycles.

(a) Recall that an Eulerian cycle uses every edge in a graph exactly once. Some connected graphs have Eulerian cycles and some do not. In contrast, prove that *every* connected undirected graph has a cycle that uses every edge exactly *twice*. (Usually, the definition of a cycle does not allow an edge to be used more than once, but here we obviously must allow it.)
Answer: Recall that an Eulerian cycle uses every edge in a graph exactly once. Some connected graphs have Eulerian cycles and some do not. In contrast, prove that *every* connected undirected graph has a cycle that uses every edge exactly *twice*. (Usually, the definition of a cycle does not allow an edge to be used more than once, but here we obviously must allow it.)

This looks like a problem for induction! Let

$P =$ any connected, undirected graph G has a cycle that visits each edge exactly twice

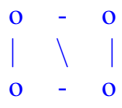
We will prove P by induction on the number of nodes in G.

Base Case: $n = 1$.
Trivially, we have created a cycle that starts and ends at our only node, using each edge exactly twice. ✓
Inductive Hypothesis: Assume for some $n \in \mathbb{N}$, $P(n)$.
Inductive Step: Consider a graph with $n+1$ nodes. Arbitrarily pick one node v (and all its edges) to "hold out." From our inductive hypothesis, we know there exists a cycle that uses each edge (not including the edges involving v) exactly twice. Arbitrarily pick one edge, $\{u,v\}$. For every other edge $\{v,u'\}$ where $u \neq u'$, traverse the edge $\{v,u'\}$, followed by $\{u',v\}$. Next, traverse the edge $\{v,u\}$, follow the cycle found from before, and finally traverse $\{u,v\}$. We have now found a cycle that uses each edge in G exactly twice.
Therefore, $\forall n \in \mathbb{N}\ P(n).\square$

Note: Alternatively, we could simply double each edge in the graph, at which point every vertex would have even degree, which means we can find an Eulerian cycle that uses each edge exactly twice.

(b) Give an example of an undirected graph G with no isolated vertices, such that G has a hamiltonian cycle but does not have an Eulerian cycle.

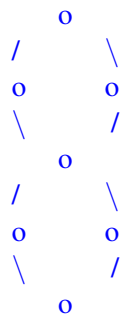
Answer: Consider the following graph:



It is easy to see how we can create a hamiltonian cycle, but it is impossible to create an Eulerian cycle.

(c) Give an example of an undirected graph G with no isolated vertices, such that G has an Eulerian cycle but does not have a hamiltonian cycle.

Answer: Consider the following graph:



We can easily create an Eulerian cycle, but it is impossible to create a Hamiltonian cycle.

5. (a) Compute the inverse of 37 modulo 64 using Euclid's extended GCD algorithm.
Answer:

We can use the following form to find the inverse using Euclid's extended GCD algorithm, and the x,y for this case would be 64 and 37 since we need to have $x \geq y \geq 0$;

x, y	d	a, b
64, 37	1	11, -19
37, 27	1	-8, 11
27, 10	1	3, -8
10, 7	1	-2, 3
7, 3	1	1, -2
3, 1	1	0, 1
1, 0	1	1, 0

Here's how to read the chart:
The LHS top down is just the standard GCD algorithm, the last row indicates where we find the GCD for 64 and 37, which is 1. Then the RHS (including the middle column) bottom up is the recursive return value for extended GCD algorithm. Finally, the a,b value (11,-19) in the top row will be the return value for extended-gcd(64,37). We can check that this pair is indeed the value we are looking for by calculating $11 * 64 - 19 * 37 = 1$ i.e. $a * x + b * y = 1$
Therefore, the inverse of 37 modulo 64 is -19.

(b) Prove that $gcd(F_n, F_{n-1}) = 1$, where $F_0 = 0$ and $F_1 = 1$ and $F_n = F_{n-1} + F_{n-2}$.
Answer: We prove this by induction.

In the base case, we have $gcd(F_1, F_0) = gcd(1, 0) = 1$, which is trivially true.
Inductive hypothesis: Assume we have $gcd(F_k, F_{k-1}) = 1$ for some $k \geq 1$
Inductive steps: Now we need to show that $gcd(F_{k+1}, F_k) = 1$ as well.
We can show that:
$gcd(F_{k+1}, F_k) = gcd(F_k + F_{k-1}, F_k) = gcd(F_k, (F_k + F_{k-1}) - F_k) = gcd(F_k, F_{k-1}) = 1$
Therefore the statement is also true for $n = k + 1$.
By the rule of induction, we can conclude that $gcd(F_n, F_{n-1}) = 1$ for all $n \geq 1$ where $F_0 = 0$ and $F_1 = 1$ and $F_n = F_{n-1} + F_{n-2}$.