1 Mods! Ban Them! (16 Points)

a. Shreyas claims that for all positive integers $m > 2$, the number $m - 1$ always has an inverse modulo m. Do you agree? Either prove your answer or give a counterexample. [3 pts]

Solution: Shreyas is right! Recall that for a number x to have an inverse modulo m it suffices to show that $\gcd(x, m) = 1$. In this case, by the Euclidean Algorithm,

$$\gcd(m, m-1) = \gcd(m-1, 1) = \gcd(1, 0) = 1$$

so an inverse in fact always exists.

Alternatively, one could have shown $(m-1)(m-1) = m^2 - 2m + 1 \equiv 1 \pmod{m}$, so $(m-1)^{-1} \equiv m - 1 \pmod{m}$. However, explicitly finding the inverse was not necessary.

b. Show that there is no integer $n \geq 0$ that satisfies the equation $13^n \equiv (7n)^{22} - 5n^2 \pmod{11}$. [4 pts]

Solution: Using FLT, we know $(7n)^{11} \equiv 7n \pmod{11}$, so we have

$$(7n)^{22} - 5n^2 \equiv (7n)^2 - 5n^2 \equiv 44n^2 \equiv 0 \pmod{11}$$

We also have $13^n \equiv 2^n \pmod{11}$, so we can rewrite the equation as $2^n \equiv 0 \pmod{11}$. If n is a solution, we must have $11 | 2^n$, but this is impossible.

c. Prove that if n is a positive integer and the sum of its digits is divisible by 3, then it is also divisible by 3.
(Hint: A number like 735 can be expressed as $735 = 7 \cdot 10^2 + 3 \cdot 10^1 + 5 \cdot 10^0$). [4 pts]

Solution: The hint motivates us to consider an arbitrary number $n = A_k A_{k-1} \cdots A_0$ where each A_i is a digit. In expanded form, we can express the number as $n = A_k \cdot 10^k + A_{k-1} \cdot 10^{k-1} + \ldots + A_0 \cdot 10^0$. We see that

$$n = \sum_{i=0}^{k} 10^i \cdot A_i \equiv \sum_{i=0}^{k} A_i \pmod{3}.$$

The expression allows us to conclude that the remainder of a number and the sum of its digits when divided by 3 is the same. Hence, if the sum of the digits of n is divisible by 3, then so is n.

d. Alice is trying to send a message x to Bob where x is a positive integer less than 15. Suppose Alice and Bob are using a variant of RSA where only N is publicly shared, not (N, e) like usual (you can imagine Bob secretly shares e with just Alice beforehand so she is able to encrypt her message). Suppose Eve knows that $N = 15$ from looking at the public key and Eve is able to factor 15, but Eve does not know e. If Eve spies on their communication and sees that Alice's encrypted message is $E(x) \equiv 10 \pmod{15}$, can she recover Alice's original message? (Hint: CRT). [5 pts]

Solution: Yes. Denote the original message as x, and we see that

$$x \equiv 10^d \pmod{15}.$$

By applying the Chinese Remainder Theorem in reverse, if we can compute $x \pmod{3}$ and $x \pmod{5}$, we can uniquely construct $x \pmod{15}$ since $\gcd(3, 5) = 1$. We know that

$$x \equiv 10^d \equiv 1 \pmod{3}$$

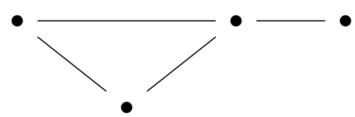
for all $d \geq 0$ and

$$x \equiv 10^d = 0 \pmod 5$$

since $10 \equiv 0 \pmod 5$. Using the method from discussion, we can use the system of congruences to compute $x \equiv 10 \pmod{15}$. Hence, Eve can always retrieve the original message $x = 10$ without ever knowing the private key d, or even knowing e.

2 Graphic Content (16 Points)

a. Given a graph $G = (V, E)$ with $|V| = n$, its degree sequence is the sequence $d_1, d_2, d_3, \ldots, d_n$ where each d_i is the degree of some vertex in G, and the degrees are sorted from largest to smallest. For instance, the below graph has degree sequence 3, 2, 2, 1.



Find the degree sequence for the following graphs. [4 pts total]

i. G is a tree with 3 vertices.

ii. G is a connected graph with 7 vertices and 8 edges that also has an Eulerian tour.

iii. G is a connected planar graph with 4 vertices and 3 faces.

Solution:

i. 2, 1, 1. There is only one way to draw a tree with 3 vertices.

ii. 4, 2, 2, 2, 2, 2, 2. The sum of the degrees must be 16 by the Handshake lemma, there must be 7 terms in the sequence, and all terms must be ≥ 2 and even. The given sequence is the only one that meets all these conditions.

iii. 3, 3, 2, 2. By Euler's formula, G has 5 edges and thus the sum of the must be 10. There must be 4 terms in the series. Since there are only 4 vertices, all degrees must be 3 or less. Also, the graph is connected, so all degrees must be greater than 0. So, the sequence must be 3, 3, 2, 2 or 3, 3, 3, 1. If we try to draw a graph corresponding to the second sequence, we will quickly realize it is impossible. So, it must be the first.

b. A sequence $d_1, d_2, \ldots, d_n$ is called graphic if there is a graph with n vertices that has the sequence as its degree sequence. For each of the following sequences, either demonstrate that it is graphic or prove that it is not. [6 pts total]

i. 4, 4, 4, 4, 4.

ii. 3, 3, 3, 3, 3, 3, 3, 3 (eight 3's).

iii. 3, 3, 3, 3, 3.

iv. 3, 3, 2, 2, 2.

Solution:

i. This is graphic, since it is the degree sequence for K_5.

ii. This is graphic, since it is the degree sequence for the 3-dimensional hypercube.

iii. This is not graphic. By the Handshake lemma $2|E| = \sum_{v \in V} \deg v$, but if the sequence was a degree sequence we would have $\sum_{v \in V} \deg v = 15$, which is odd and hence cannot be $2|E|$ for any $|E|$.

iv. This is graphic, since it is the degree sequence for $K_{2,3}$.

c. Prove that if a graph with $n \geq 2$ vertices has strictly more than $\frac{(n-1)(n-2)}{2}$ edges, then it is connected.
(Hint: This is unrelated to parts (a) and (b). Use induction on n). [6 pts]

Solution: As per the hint, we use induction on n.
Base Case ($n = 2$): If a graph with 2 vertices has $> \frac{(n-1)(n-2)}{2} = 0$ edges, there must be exactly one edge which connects the two vertices.
Induction Hypothesis: Suppose we know that for some $k \geq 2$, when a graph has k vertices and more than $\frac{(k-1)(k-2)}{2}$ edges, it is connected.
Inductive Step: Consider a graph with $k+1$ vertices and more than $\frac{k(k-1)}{2}$ edges. If there was a vertex of degree k in the graph, we would be done since we could use it to get between any two vertices and thus the graph would be connected. Clearly, not all vertices have degree 0 since we have more than $\frac{k(k-1)}{2}$ edges. So, pick a vertex v with $0 < \deg v < k$. Remove it and its associated edges. The resulting graph has k vertices and has more than

$$\frac{k(k-1)}{2} - (k-1) = \frac{k(k-1) - 2(k-1)}{2} = \frac{(k-2)(k-1)}{2} \text{ edges}$$

So, by the induction hypothesis, the graph with v removed is connected. Adding v and its edges back, the graph is still connected because $\deg v > 0$. So, we are done.

3 Let the Fun(ctions) Begin... (18 Points)

a. Let X be a set with subsets $A, B \subseteq X$. Recall that the complement of B is $B^C = X \setminus B$. Prove that $A \setminus B = A \cap B^C$. [3 pts]

Solution: First, say $x \in A \setminus B$. Then, $x \in A$ and $x \notin B$. So, $x \in B^C$. So, $x \in A \cap B^C$. Thus, $A \setminus B \subseteq A \cap B^C$. The same argument in reverse shows $A \cap B^C \subseteq A \setminus B$, so $A \cap B^C = A \setminus B$.

b. We will call a subset $A \subseteq \mathbb{N}$ decidable if there is a computer program $P(n)$ that takes in any natural number $n \in \mathbb{N}$ and returns True if $n \in A$, and False otherwise. Is every subset $A \subseteq \mathbb{N}$ decidable? Prove your answer.
(Hint: You may use the fact that the power set $\mathcal{P}(\mathbb{N})$ is uncountable). [4 pts]

Solution: Not all subsets $A \subseteq \mathbb{N}$ are decidable. For the sake of contradiction, suppose they all are. Then, we could build an injection from $\mathcal{P}(\mathbb{N})$ to the set of computer programs by mapping each subset $A \subseteq \mathbb{N}$ to a computer program that decides it. However, we know $\mathcal{P}(\mathbb{N})$ is uncountable, while the set of computer programs is countable. Contradiction!

c. Suppose we have a function $f : A \to A$ for some set A. Prove that if $f \circ f$ is a bijection, then f is a bijection. (Hint: Recall that $(f \circ f)(x) = f(f(x))$ for all $x \in A$). [4 pts]

Solution: We must show the two properties for a bijection.

One-to-one/Injection: We wish to show for arbitrary $x, y \in A$ that $f(x) = f(y) \implies x = y$. The bijection of the composition function gives us

$$f(x) = f(y) \implies f(f(x)) = f(f(y)) \implies x = y.$$

Onto/Surjection: We wish to show that for arbitrary $y \in A$, there exists an $x \in A$ such that $f(x) = y$. The bijection of the composition guarantees us that for all $y \in A$, there exists a $x' \in A$ such that $f(f(x')) = y$. Recognizing that $f(x') \in A$, we define $x = f(x') \in A$. Hence, we've shown that for an arbitrary $y \in A$, there exists a $x \in A$ such that $f(x) = y$.

d. We can consider graphs $G = (V, E)$ with a countably infinite number of vertices. Namely, put $V = \mathbb{N}$ so there is one vertex for each natural number. Consider the set of graphs $G = (V, E)$ with $V = \mathbb{N}$ such that each connected component contains finitely many vertices.

For instance, $G = (\mathbb{N}, \emptyset)$ is in our set since all connected components have a single vertex, while $G = (\mathbb{N}, E)$ with $E = \{(n, n+1) \mid n \in \mathbb{N}\}$ is not since all vertices are in a single infinite connected component.

Prove that this set is uncountable. [7 pts]

Solution: For the sake of contradiction, suppose it is countable. Then, we can list the graphs $G = (\mathbb{N}, E)$ such that each connected component contains finitely many vertices. In particular, we can list the graphs amongst these which only have edges between adjacent vertices (of the form $(n, n+1)$ for some $n \in \mathbb{N}$). There is a bijection between these graphs and infinite lists of positive integers, describing the size of the next connected component. For instance $(3, 2, 1, 2, 1, 1, 1, \ldots)$ would correspond to the graph with $E = \{(0, 1), (1, 2), (3, 4), (6, 7)\}$. Now, consider any list of these graphs.

$$\begin{array}{ll} G_1: & (3, 2, 1, 2, 1, 1, 1, \ldots) \\ G_2: & (5, 1, 8, 3, 1, 3, 2, \ldots) \\ G_3: & (7, 7, 1, 1, 9, 4, 6, \ldots) \\ & \vdots \end{array}$$

Using a typical diagonalization argument, we can construct a graph missing from the list by making the first connected component 1 bigger than G_1, the second one bigger than G_2, and so on. In the above example, the missing element we would construct is $(4, 2, 2, \ldots)$, i.e. the graph with $E = \{(0, 1), (1, 2), (2, 3), (4, 5), (6, 7), \ldots\}$. Contradiction! Since we cannot even list this subset of the graphs, the set must be uncountable.