CS 70 Discrete Mathematics and Probability Theory
Summer 2019 James Hulett and Elizabeth Yang Midterm 1

PRINT your name: _____ _____
(First) (Last)

SIGN your name: _____

PRINT your student ID: _____

CIRCLE your exam room: 145 Dwinelle 155 Dwinelle 341A Soda 405 Soda Other

Name of the person sitting to your left: _____

Name of the person sitting to your right: _____

- We will not grade anything outside of the space provided for a problem unless we are clearly told in the space provided for the question to look elsewhere.
- We will not be collecting scratch paper. Write everything you want to be graded on the exam itself.
- For problems with answers modulo m, only answers between 0 and $m-1$ will receive full credit.
- Assume all graphs are undirected and have no self-loops or parallel edges unless otherwise specified.
- You may consult one handwritten double-sided sheet of notes. Apart from that, you may not look at books, notes, etc. Calculators, phones, computers, and other electronics devices are prohibited.
- There are 16 pages (8 sheets) on the exam. Notify a proctor immediately if a page is missing.
- There are 7 questions on this exam, worth a total of 200 points.
- **You may, without proof, use theorems and facts that were proven in the notes, lecture, discussion, or homework.**
- **You have 120 minutes.**

Do not turn this page until your instructor tells you to do so.

1 True/False [3 Points Each, 48 Total]

1 point for True/False marking, 2 points for justification.

For each statement, mark whether it is true or false and give a brief justification (maximum 1 sentence, must fit in box) in the adjacent box.

(a) $\neg(P \vee Q \vee R) \equiv \neg P \wedge \neg Q \wedge \neg R$

◯ **True**

◯ **False**

Answer: True. This is just two applications of De Morgan's Laws.

(b) $[(\forall x \in \mathbb{R}, \exists y \in \mathbb{R}) P(x,y)] \implies [(\exists x \in \mathbb{R}, \exists y \in \mathbb{R}) \neg P(x,y)]$

◯ **True**

◯ **False**

Answer: False. If $P(x,y)$ is always true, the left hand side will be true but the right will be false.

(c) $[\exists x \in (\mathbb{R} \setminus \mathbb{Q})](x \in \mathbb{Z})$

◯ **True**

◯ **False**

Answer: False. This means there is some irrational number that is an integer.

(d) $[(\exists x \in \mathbb{Q}, \forall y \in \mathbb{Z})(P(x,y) \wedge Q(x,y))] \implies [(\forall y \in \mathbb{Z}, \exists x \in \mathbb{Q}) P(x,y)]$

◯ **True**

◯ **False**

Answer: True. For any $y \in \mathbb{Z}$, take the x that is guaranteed by the "if" part.

(e) Every graph **requires** at least Δ colors to be properly vertex-colored, where Δ is the maximum degree on the graph.

◯ **True**

◯ **False**

Answer: False. For example, $K_{3,3}$ has $\Delta = 3$ but can be colored with two colors.

(f) Let G be an acyclic graph on 9 vertices. If G has 3 connected components, G has fewer than 7 edges.

◯ **True**

◯ **False**

Answer: True. Each connected component is a tree, and so has one fewer edge than vertices, meaning the total number of edges is $9-3=6<7$.

(g) Every tree on at least two vertices has two vertices with the same degree.

◯ **True**

◯ **False**

Answer: True. Every tree has at least two leaves, which both have degree 1.

(h) $f(x) = ax \pmod{p}$ is a bijection for all values of a and all primes p.

◯ **True**

◯ **False**

Answer: False. If $a=0$, $f(x)$ is not a bijective function as every input maps to 0.

Alternative Justification: f is only a bijection when $\gcd(a,p)=1$.

(i) Let p and q be distinct primes and $\gcd(a,(p-1)(q-1))=1$. Then $f(x)=x^a \pmod{pq}$ is a bijection.

◯ **True**

◯ **False**

Answer: True. If $d=a^{-1} \pmod{(p-1)(q-1)}$, f has an inverse $f^{-1}(y)=x^d \pmod{pq}$.

(j) In an RSA scheme with decryption key d and primes p and q, $\gcd(d,(p-1)(q-1))$ must equal 1.

◯ **True**

◯ **False**

Answer: True. Since $d=e^{-1} \bmod (p-1)(q-1)$, then $e=d^{-1} \bmod (p-1)(q-1)$. For the inverse to exist, d must be coprime to $(p-1)(q-1)$

(k) $(N,e)=(143,9)$ is a valid RSA public key. *(Note:* $143=11\cdot 13$*)*

◯ **True**

◯ **False**

Answer: False. $e = 9$ is not coprime with $(p-1)(q-1) = 120$.

(l) Every element in $\{0, 1, \ldots, 32\}$ has a multiplicative inverse $\pmod{33}$.

◯ **True**

◯ **False**

Answer: False. For instance, 3 does not have an inverse.

(m) If two degree 5 polynomials overlap on 5 points, then there always exists a 6th point of overlap.

◯ **True**

◯ **False**

Answer: False. You need 6 points to fully determine a degree 5 polynomial.

Alternative justification: $P(x) = x(x-1)(x-2)(x-3)(x-4)(x-5)$ and $-P(x)$ agree on their 5 roots but nowhere else.

(n) A degree d polynomial with real coefficients always has exactly d real roots.

◯ **True**

◯ **False**

Answer: False. Such a polynomial will have at most d roots, but may have fewer.

Alternative Justification: $x^2 + 1$ is degree 2, but has no roots.

(o) There exists a degree *exactly* 2 polynomial through the points $(0,2)$, $(1,3)$, and $(2,4)$.

◯ **True**

◯ **False**

Answer: False. These points uniquely define the degree *at most* 2 polynomial $x + 2$.

(p) Let A, B, C be three finite sets. If there is an injection from A to B, and an injection from B to C, then there is an injection from A to C.

◯ **True**

◯ **False**

Answer: True. We can build an injection from A to C by composing the one from A to B with the one from B to C.

2 Short Answer and Multiple Choice [3 Points Each, 66 Total]

(a) Let S be the set of all streets in Berkeley, and T be the set of days in a week. Define the following statements:

$B(x)$ = "There is a **boba** shop on street x."
$C(x)$ = "Street x borders Berkeley's **campus**.
$D(x,t)$ = "On day t, there is a traffic **delay** on street x.
$E(x,t)$ = "On day t, **employees** who work on street x will run late.
$F(x,y)$ = "Street x and street y are at most **five** blocks apart."

Write each statement below in terms of propositional logic.

(i) There are no boba shops on the border of Berkeley's campus.

Answer: $(\forall x \in S)[C(x) \implies (\neg B(x)]$ or $(\forall x \in S)[(\neg C(x)) \vee (\neg B(x)]$

(ii) On any given day and Berkeley street, if there is a traffic delay, then all employees who work there will run late.

Answer: $(\forall x \in S)(\forall t \in T)(D(x,t) \implies E(x,t)$

(iii) There is at least one day each week where two boba shops at most five blocks apart are on streets that experience employee lateness.

Answer: $(\exists t \in T)(\exists x,y \in S)(B(x) \wedge B(y) \wedge F(x,y) \wedge E(x,t) \wedge E(y,t))$

(iv) All boba shops in Berkeley are more than five blocks away from each other.

Answer: $(\forall x,y \in S)[(B(x) \wedge B(y)) \implies (\neg F(x,y) \vee (x = y))]$. Note: we did not require the $x = y$ condition to receive full credit. There are also several ways to re-write this statement, using De Morgan's Laws; any equivalent statement also received full credit.z

(b) A planar graph has 100 vertices and 42 faces. How many edges does it have?

Answer: 140. From Euler's formula, we know that $v + f = e + 2$. Plugging in our values here, we have $v + f = 142$, so $e = 142 - 2 = 140$.

(c) How many edges does a planar graph have if each face has exactly 4 sides? Write your answer in terms of v, the number of vertices.

Answer: $2v-4$. We know that each face has exactly 4 sides, so the number of sides is four times the number of faces. We also know that each edge contributes two sides, so the number of edges is twice the number of sides. Hence, we have that $4f = 2e$, so $f = \frac{e}{2}$. Plugging this into Euler's formula, we get $v + \frac{e}{2} = e + 2$. Rearranging this, we have $\frac{e}{2} = v - 2$, so $e = 2v - 4$.

(d) We abbreviate the following graph attributes:

(A) The graph has an Eulerian tour.
(B) The graph is 2-colorable.
(C) The graph is planar.

For each graph described below, fill in all attributes that **always** apply. No justification required. Recall that K_n is the complete graph on n vertices, and $K_{m,n}$ is the complete bipartite graph with m vertices on the left and n vertices on the right. *(One point for each circle correctly marked/unmarked.)*

(i) $K_{1,n}$ for $n \geq 1$, n odd.

◯ **(A)** ◯ **(B)** ◯ **(C)**

Answer: (B), (C) hold. (A) n of the vertices will have degree 1, which is odd. (B) This graph is bipartite. (C) This graph always has a planar drawing (a star).

(ii) $K_{n,n}$ for $n \geq 2$, n even.

◯ **(A)** ◯ **(B)** ◯ **(C)**

Answer: (A), (B) hold. (A) Each vertex has degree n, which is even. (B) This graph is bipartite. (C) For $n \geq 4$ this graph is not planar because $K_{3,3}$ is a subgraph.

(iii) K_5 with any single edge removed.

◯ **(A)** ◯ **(B)** ◯ **(C)**

Answer: (C) holds. (A) There are two vertices of degree 3. (B) K_4 is a subgraph, which requires 4 colors already. (C) It cannot contain either K_5 (not enough edges) or $K_{3,3}$ (not enough vertices).

(iv) Two copies of K_{2019}, with a single edge connecting the copies.

◯ **(A)** ◯ **(B)** ◯ **(C)**

Answer: None of the above. (A) The two vertices incident to the connecting edge each have degree 2019. (B) We need ≥ 2019 colors for each copy alone. (C) This graph contains K_5 as a subgraph.

(e) Find $8^{50} \pmod{65}$.

Answer: 64. $65 = 5 \cdot 13$, so similar to the proof of correctness in RSA, we have that $x^{4 \cdot 12+1} \equiv x \pmod{65}$ for any x. Thus, $8^{49} \equiv 8 \pmod{65}$, so $8^{50} \equiv 8^{49} \cdot 8 \equiv 64 \pmod{65}$.

An alternative way to do this problem is to note that $8^2 = 64 \equiv -1 \pmod{65}$. Thus, we have that $8^{50} = 64^{25} \equiv (-1)^{25} \equiv -1 \equiv 64 \pmod{65}$.

(f) Find the smallest positive integer x satisfying $x \equiv 2 \pmod{3}$, $x \equiv 3 \pmod{4}$, and $x \equiv 4 \pmod{5}$.

Answer: 59. One way to shortcut this problem is to notice that $x \equiv -1 \pmod{3}$, $x \equiv -1 \pmod{4}$, and $x \equiv -1 \pmod{5}$. Thus, the solution that the Chinese Remainder Theorem gives must be equivalent to $-1 \bmod 3 \cdot 4 \cdot 5 = 60$. The smallest positive integer satisfying this is 59.

Alternatively, one can also run the algorithm given by the Chinese Remainder Theorem. For this, we'll have that $4 \cdot 5 \equiv 2 \pmod{3}$, so $b_3 = 20 \cdot (2^{-1} \bmod 3) = 40$. We then have $3 \cdot 5 \equiv 3 \pmod{4}$, so $b_4 = 15 \cdot (3^{-1} \bmod 4) = 45$. Finally, we have $3 \cdot 4 \equiv 2 \pmod{5}$, so $b_5 = 12 \cdot (2^{-1} \bmod 5) = 36$. Thus, we have that we can set $x = (2 \cdot 40) + (3 \cdot 45) + (4 \cdot 36) = 80 + 135 + 144 = 359$. Taking this modulo 60, we again get 59.

(g) Let $\mathbb{Z}_{24}$ be the set of integers modulo 24. We say an element $x \in \mathbb{Z}_{24}$ is *nilpotent* if, for some $n \in \mathbb{N}$, $x^n \equiv 0 \pmod{24}$. List all nilpotent elements in $\mathbb{Z}_{24}$.

Answer: $\{0, 6, 12, 18\}$. In order for x^n to be equivalent to 0 mod 24, it must be divisible by 24. Hence, it must contain all of the prime factors of 24. Raising a number to a power cannot add additional prime factors, so x can only be nilpotent mod 24 if it has both 2 and 3 as factors to begin with. Furthermore, if we have an x with both these factors, raising it to a high enough power will ensure that it has at least 3 factors of 2 and one factor of 3, and hence will be divisible by 24. Thus, the set of nilpotent elements mod 24 is just the set of elements divisible by 6.

(h) Alice sets up an RSA scheme with $p = 5$, $q = 11$. If $e = 3$, compute d.

Answer: We need $d \equiv e^{-1} \pmod{(5-1)(11-1) = 40}$. We note that $3 \cdot 27 = 81 \equiv 1 \pmod{40}$, so we would take $d = 27$.

(i) Suppose we have the following equivalences.

$$4x \equiv 1 \pmod{13}$$
$$3y \equiv 4 \pmod{13}$$

Determine $x+y \pmod{13}$.

Answer: 7. 10 is 4's inverse mod 13, while 9 is 3's inverse. Hence, the first congruence says that $x \equiv 1 \cdot 10 \equiv 10 \pmod{13}$, while the second says that $x \equiv 4 \cdot 9 \equiv 36 \equiv 10 \pmod{13}$. Hence, $x+y \equiv 20 \equiv 7 \pmod{13}$.

Alternatively, one could multiply the first congruence by 3 and the second by 4. Noting that $12 \equiv -1 \pmod{13}$, this will give us that $-x \equiv 3 \pmod{13}$ and $-y \equiv 16 \equiv 3 \pmod{13}$. Hence, $x+y \equiv -3-3 \equiv 7 \pmod{13}$.

(j) James' Day 1 as a CS 70 GSI was a Tuesday. He has been a CS 70 GSI for 1200 continuous days! (What an achievement!) On which day of the week was his Day 1200?

Answer: Thursday. $1200 \equiv 3 \pmod{7}$. If Tuesday corresponds to $1 \pmod{7}$, then $3 \pmod{7}$ day would fall on a Thursday.

(k) Consider two **distinct** polynomials in $GF(p)$: $P(x)$ of degree d and $Q(x)$ of degree k. Assume $d,k < p$. What is the maximum number of times $P(x)$ can intersect $Q(x)$?

Answer: This is asking the number of solutions to the equation $P(x) = Q(x)$ which is the same as asking the number of roots of the polynomial $P(x) - Q(x)$ which is $\max(d,k)$. Because the polynomials are distinct, the difference is never the 0 polynomial so we do not need to consider that case.

(l) Consider two **distinct** polynomials $P(x)$ and $Q(x)$ in $GF(p)$, both degree d, with $10 < d < p$. Suppose $P(i) = Q(i)$ for $i = 0,1,...9$. What is the maximum number of times $P(i) = Q(i)$ for $i = 10,...,p-1$?

Answer: $d-10$. Suppose they intersect at $d-9$ points, then they would agree on $(d-9)+10 = d+1$ points and therefore be the same polynomial.

(m) Alice uses two RSA schemes, with public keys (N,e_1) and (N,e_2), to send the same message m to Bob and Carol. You may assume $0 \leq m < N$. Eve the eavesdropper is able to see both of the encrypted messages that Alice sends.

(i) If $e_1 = 11$ and $e_2 = 37$, find $a, b \in \mathbb{Z}$ such that $ae_1 + be_2 = 1$.

Answer: $a = -10$ and $b = 3$. To compute a and b, we apply the Extended Euclidean algorithm.

(ii) Let M_1 be the **encrypted** message sent to Bob, and M_2 be the **encrypted** message sent to Carol. You may assume M_1, M_2 are coprime to N. Write an expression for m in terms of M_1, M_2, a, b, and N, where a and b are the answers to Part (i).

Answer: $M_1^a \cdot M_2^b \pmod N$. This is equivalent to $m^{e_1 a + e_2 b} \pmod N$. From the previous part, we know $ae_1 + be_2 = 1$, which gives us m.

(n) Suppose we wish to interpolate a degree at most two polynomial through the points $(0,3)$, $(1,2)$, and $(2,5)$ modulo 7, using Lagrange interpolation.

(i) Determine $\Delta_0(x)$ in **simplified form**, i.e. in the form $ax^2 + bx + c$.

Answer: To calculate $\Delta_0(x)$, we take $\frac{(x-1)(x-2)}{(0-1)(0-2)} \equiv 4(x^2 - 3x + 2) \equiv 4x^2 - 12x + 8 \equiv 4x^2 + 2x + 1 \pmod 7$

(ii) Express the final interpolated polynomial $p(x)$ in terms of $\Delta_0(x), \Delta_1(x)$, and $\Delta_2(x)$.

Answer: $p(x) \equiv 3\Delta_0(x) + 2\Delta_1(x) + 5\Delta_2(x) \pmod 7$. Full credit was also given if you solved for the polynomial which is $p(x) = 2x^2 + 4x + 3$

3 Short Proof Potpourri [5 Points Each, 10 Total]

(a) Prove that $\sqrt{10}$ is irrational.

Answer: Assume for contradiction that $\sqrt{10}$ is rational, so we can write an equation $\sqrt{10} = \frac{a}{b}$, where $a, b \in \mathbb{Z}$. We may assume that $\gcd(a,b) = 1$, otherwise we can cancel out common factors until they are coprime. If we square both sides of our equation, we have $\frac{a^2}{b^2} = 10$; rearranged it becomes $a^2 = 10b^2$. We know the right hand side must be divisible by 2, so a must also be divisible by 2. Thus, the left hand side is actually divisible by 4. We only get one factor of 2 from 10, so b must also be divisible by 2. However, this contradicts the assumption that $\gcd(a,b) = 1$.

(b) At Cheeseboard, there are 12 employees who each work 2 hour-long shifts every day. Each shift starts on the hour. Cheeseboard is open 10 hours each day, from 10 AM to 8 PM. Prove that there is an hour during the day when at least 3 employees are on shift.

Answer: Since there are 12 workers each with a 2-hour shift, we have 24 distinct (people, hour) pairs. We now apply the pigeonhole principle, with the hours as the holes and the (people, hour) pairs as the pigeons. Since there are 10 hours to the day, there is at least one hour of the day with $> \frac{24}{10} > 2$ (people, hour) pairs assigned to it, which gives the desired result.

4 Drop the Base (Case) [5/5/3/7 Points, 20 Total]

(a) Consider the sequence defined by

$$a_0 = 2$$

$$a_n = 3a_{n-1} + 2$$

(i) Using induction, prove that $a_n = 3^{n+1} - 1$.

Answer: The given information $a_0 = 2$ confirms the base case $n = 0$. Now, assume for all $n \leq k$ that $a_n = 3^{n+1} - 1$. Now, let $n = k+1$. Using the recursion definition and inductive hypothesis:

$$a_{k+1} = 3a_k + 2 = 3(3^{k+1} - 1) + 2 = 3^{k+2} - 3 + 2 = 3^{k+2} - 1$$

This verifies the statement for $n = k+1$.

(ii) Prove that

$$\sum_{i=0}^{n} a_i < \frac{3}{2} \cdot 3^{n+1}$$

You may use the result from Part (i), even if you did not do Part (i).

Answer: For the base case $n = 0$, we check that $2 < \frac{3}{2} \cdot 3 = \frac{9}{2}$. Now, assume for all $n \leq k$ that the inequality holds. For $n = k+1$, we have:

$$\sum_{i=0}^{k+1} a_i = \left(\sum_{i=0}^{k} a_i \right) + a_{k+1} < \frac{3}{2} \cdot 3^{k+1} + 3^{k+2} = \frac{1}{2} \cdot 3^{k+2} + 3^{k+2} = \frac{3}{2} \cdot 3^{k+2}$$

This verifies the inequality for $n = k+1$.

(b) We wish to prove the following general form of one of De Morgan's Laws:

$$\neg(A_1 \wedge A_2 \wedge \ldots \wedge A_n) = (\neg A_1) \vee (\neg A_2) \vee \ldots \vee (\neg A_n)$$

(i) Fill in the truth table to prove that $\neg(A_1 \wedge A_2) \equiv (\neg A_1) \vee (\neg A_2)$.

A_1	A_2	$A_1 \wedge A_2$	$\neg(A_1 \wedge A_2)$	$\neg A_1$	$\neg A_2$	$\neg A_1 \vee \neg A_2$
T	T					
T	F					
F	T					
F	F					

Answer:

A_1	A_2	$A_1 \wedge A_2$	$\neg(A_1 \wedge A_2)$	$\neg A_1$	$\neg A_2$	$\neg A_1 \vee \neg A_2$
T	T	T	F	F	F	F
T	F	F	T	F	T	T
F	T	F	T	T	F	T
F	F	F	T	T	T	T

(ii) Use induction to prove the desired statement.

Answer: We induct on n. The base case, $n = 2$ was proven in Part (i).
Now, assume the equivalence holds for all $n \leq k$ and any choice of A_i. We want to now verify the equivalence for $n = k+1$, and any choice of A_i:

$$\neg(A_1 \wedge A_2 \wedge \ldots \wedge A_k \wedge A_{k+1}) = (\neg A_1) \vee (\neg A_2) \vee \ldots \vee (\neg A_k) \vee (\neg A_{k+1})$$

Let the clause $A' = A_1 \wedge A_2 \wedge \ldots \wedge A_k$. We can thus write the left side as $\neg(A' \wedge A_{k+1})$. Using Part (i), this is equivalent to $(\neg A') \wedge (\neg A_{k+1})$. We also know:

$$\neg A' \equiv \neg(A_1 \wedge A_2 \wedge \ldots \wedge A_n) \equiv (\neg A_1) \vee (\neg A_2) \vee \ldots \vee (\neg A_n)$$

This is due to the inductive hypothesis. This gives us the right hand side.

5 The Best Things in Life are Three [6/2/4/4/4 Points, 20 Total]

*In this section, you may use **any previous part's result**, even if you did not complete that part. For example, if you skip a(i), you can still use the result from a(i) to prove b(ii) and get full credit.*

(a) Let $G = (V, E)$ be a planar graph. For a fixed planar drawing of G, there exists a vertex v that touches each face.

(i) Prove that $G \setminus v$ (i.e. G without vertex v) is acyclic.

Answer: Fix a planar drawing of G, and let $F(G)$ denote the set of faces of G using this drawing. Assume for contradiction that $G \setminus v$ is not acyclic, so it contains a cycle C that bounds a face $f \in F(G)$. We now have two cases for where v can go:

- Case 1: If v belongs inside face f in the planar drawing, then it does not touch any face in $F(G) \setminus f$, which is a contradiction to v touching every face of G.
- Case 2: If v belongs to some face in $F(G) \setminus f$, then it cannot touch f, which is also a contradiction.

(ii) Deduce that G is 3-vertex-colorable.

Answer: Since $G \setminus v$ is acyclic, it is either a tree or a collection of trees (known as a *forest*). In either case, it is bipartite, and thus can be 2-vertex-colored. Then, we can assign a third color to v to get a valid 3-vertex-coloring for G.

(b) Let G be a graph with exactly two cycles, C_1 and C_2, that intersect in at most one vertex. Any such G will always be planar; *you may use this fact without proof.*

(i) First, prove that if C_1 and C_2 intersect at some vertex v, the resulting graph is 3-vertex-colorable.

Answer: Fix a planar drawing of G. Since there are exactly two cycles, there are only 3 regions: the one bounded by C_1, the one bounded by C_2, and the infinite region. v is incident to all three regions, so we can apply Part a(ii).

Alternate Solution: Deleting v would render the graph acyclic, so we can color $G \setminus v$ with two colors. Then, we can add v back with a third.

(ii) *For the remaining parts, we now assume C_1 and C_2 do not intersect.* Prove that there can be at most one edge between the vertices in C_1 and the vertices in C_2.

Answer: If we can find 2 edges between vertices in C_1 and vertices in C_2, we can then form another cycle C_3, a contradiction.

(iii) Deduce that we can find $v_1 \in C_1$ and $v_2 \in C_2$ that are not connected by an edge. Use this fact to prove that G is 3-vertex-colorable.

Answer: Since C_1 and C_2 each have at least 3 vertices, and there is at most one edge between C_1 and C_2, at least 2 vertices in each cycle do not have edges to the other cycle. This completes the "deduction." Now, if we delete v_1 and v_2 from G, the remaining graph is acyclic, and thus 2-colorable. We can now give both v_1 and v_2 with the same 3rd color.

6 Almost, But Not Quite, Entirely Unlike (CR)Tea [2/3/3/2/2/4/4 Points, 20 Total]

Let p_1, p_2, and p_3 be distinct primes. Consider the following system of congruences:

$$x \equiv a \pmod{p_1 p_2} \tag{1}$$
$$x \equiv b \pmod{p_2 p_3} \tag{2}$$

where a is some number modulo $p_1 p_2$ and b is some number modulo $p_2 p_3$.

(a) Fill in the following two congruences such that (1) holds if and only if the following congruences do.

$\square \equiv \square \pmod{p_1}$ $\square \equiv \square \pmod{p_2}$

Answer: $x \equiv a \pmod{p_1}$ and $x \equiv a \pmod{p_2}$

(b) Prove that if (1) holds, the equivalences in part (a) hold.

Answer: If $x \equiv a \pmod{p_1 p_2}$, we have $x = a + k p_1 p_2$ for some integer k. Taking this equation mod p_1 gives us $x \equiv a \pmod{p_1}$; taking it mod p_2 gives us $x \equiv a \pmod{p_2}$.

(c) Prove that if the equivalences in part (a) hold, (1) holds. *(Hint: Use the Chinese Remainder Theorem.)*

Answer: The Chinese Remainder Theorem tells us that there is a unique x modulo $p_1 p_2$ such that $x \equiv a \pmod{p_1}$ and $x \equiv a \pmod{p_2}$. We know that a satisfies these congruences, and hence is the only possible value x could take on modulo $p_1 p_2$.

(d) Fill in the following two congruences such that (2) holds if and only if the following congruences do.

$\square \equiv \square \pmod{p_2}$ $\square \equiv \square \pmod{p_3}$

Answer: $x \equiv b \pmod{p_2}$ and $x \equiv b \pmod{p_3}$

(e) Give a condition (using any or all of a, b, p_1, p_2, or p_3) under which there exists an integer x satisfying both (1) and (2). *(Hint: Consider the equivalences from Parts (a) and (d).)*

Answer: $a \equiv b \pmod{p_2}$

(f) Prove that if your condition from Part (e) does not hold, no integer x can satisfy both (1) and (2).

Answer: Suppose for contradiction that there was an integer x satisfying both (1) and (2). By Part (a), we must have that $x \equiv a \pmod{p_2}$; by part (d), we must have that $x \equiv b \pmod{p_2}$. If $a \not\equiv b \pmod{p_2}$, these two statements contradict each other.

(g) Prove that if your condition from Part (e) holds, there exists an integer x satisfying both (1) and (2). *(Hint: Use the Chinese Remainder Theorem again.)*

Answer: By the Chinese Remainder Theorem, there exists an integer x such that $x \equiv a \pmod{p_1}$, $x \equiv a \equiv b \pmod{p_2}$, and $x \equiv b \pmod{p_3}$. Hence, our conditions from parts (a) and (d) hold, meaning that this x satisfies both (1) and (2).

7 Malcolm in the Middle [4 Points Each, 16 Total]

1 point for the bubble, 3 for the box. No justification is necessary.
For each part, either mark "for all ..." to indicate that Malcolm changes all of the messages, or mark "for $i =$ __" and fill in the blank if Malcolm only changes one message. Write what the messages get changed to in the box.

Alice wants to securely send Bob a polynomial $p(x)$ of degree D with coefficients in $\mathbb{Z}$. They use a standard RSA scheme with public key $(N = pq, e)$. However, a malicious party, Malcolm, intercepts Alice's messages and alters them before Bob can receive them.

(a) Alice's first idea is to choose a set of $(D+1)$ points on the polynomial with x-coordinates in $\mathbb{Z}$, and encrypts both coordinates, so Bob can decrypt them and perform Lagrange interpolation.
She sends $\{(x_i^e \pmod N, p(x_i)^e \pmod N)\}$ to Bob, where x_i corresponds to the i-th point.

(i) If Malcolm wants Bob to receive $p(-x)$, which changed message(s) should he send?

◯ for all $1 \le i \le (D+1)$ ◯ for $i =$ ____

Answer: For all i, Malcolm can send $((-1)^e \cdot x_i^e \pmod N, p(x_i)^e \pmod N)$. The polynomial $p(-x)$ is $p(x)$ when reflected across the x-axis.

(ii) Now, if Malcolm wants Bob to receive $5 \cdot p(x)$, which changed message(s) should he send?

◯ for all $1 \le i \le (D+1)$ ◯ for $i =$ ____

Answer: For all i, Malcolm can send $(x_i^e \pmod N, 5^e \cdot p(x_i)^e \pmod N)$. Each y-coordinate should be multipled by 5 before being encrypted.

(b) Alice's next idea is to encrypt each coefficient.
She sends Bob the set $\{c_i^e \pmod N\}$, where c_i is the coefficient of x^i.

(i) If Malcolm wants Bob to receive $p(2x)$, which changed message(s) should he send?

◯ for all $0 \le i \le D$ ◯ for $i =$ ____

Answer: For all i, Malcolm should send $2^{ie} \cdot c_i^e \pmod N$. If we compute $p(2x)$, the x^i term will be replaced with $(2x)^i = 2^i x^i$, so we need to absorb the additional 2^i into the coefficient before encoding it.

(ii) If Malcolm wants Bob to receive $p(x) + 2 \cdot p(0)$, which changed message(s) should he send?

◯ for all $0 \le i \le D$ ◯ for $i =$ ____

Answer: For $i = 0$, Malcolm should send $3^e \cdot c_0^e \pmod N$. If we shift the polynomial by $2 \cdot p(0)$, it is equivalent to adding $2 \cdot p(0)$ to the constant term. However, the constant term itself is $p(0)$, so we are effectively multiplying it by 3.