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**

(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**

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

○ **True**

○ **False**

(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**

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

○ **True**

○ **False**

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

○ **True**

○ **False**

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

○ **True**

○ **False**

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

○ **True**

○ **False**

(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**

(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**

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

○ **True**

○ **False**

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

○ **True**

○ **False**

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

○ **True**

○ **False**

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

○ **True**

○ **False**

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

○ **True**

○ **False**

(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**

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.

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

(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.

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

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

(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.

(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)**

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

○ **(A)** ○ **(B)** ○ **(C)**

(iii) K_5 with any single edge removed.

○ **(A)** ○ **(B)** ○ **(C)**

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

○ **(A)** ○ **(B)** ○ **(C)**

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

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

(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 $\mathbb{Z}_{24}$.

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

(i) Suppose we have the following equivalences.

$$\begin{aligned} 4x &\equiv 1 \pmod{13} \\ 3y &\equiv 4 \pmod{13} \end{aligned}$$

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

(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?

(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 $Q(x)$?

(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 $i = 0, 1, \ldots 9$. What is the maximum number of times $P(i) = Q(i)$ for $i = 10, \ldots, p-1$?

(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 $ae_1 + be_2 = 1$.

(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).

(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 $ax^2 + bx + c$.

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

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

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

(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.

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 $a_n = 3^{n+1} - 1$.

(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).

(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					

(ii) Use induction to prove the desired statement.

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.

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

(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.

(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.

(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.

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.

$$\boxed{} \equiv \boxed{} \pmod{p_1} \qquad \boxed{} \equiv \boxed{} \pmod{p_2}$$

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

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

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

$$\boxed{} \equiv \boxed{} \pmod{p_2} \qquad \boxed{} \equiv \boxed{} \pmod{p_3}$$

(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).)*

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

(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.)*

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 $1 \leq i \leq (D+1)$ ○ for $i =$ ____

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

○ for all $1 \leq i \leq (D+1)$ ○ for $i =$ ____

(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 $0 \leq i \leq D$ ○ for $i =$ ____

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

○ for all $0 \leq i \leq D$ ○ for $i =$ ____