Asli's Midterm 1 Review

1. For each of the following boolean expressions, decide if it is (i) valid (ii) satisfiable (iii) unsatisfiable. (give all applicable properties, with justification.)

(a) (5) $A \wedge \neg A \wedge \neg B$

(b) (10) $(A \implies B) \wedge (B \implies C) \wedge (C \implies \neg A)$

(c) (5) $(A \implies B) \vee (B \implies A)$

2. Coloring a map:

(a) (10) A *map* is a set of n countries $C_1, \dots C_n$, plus a specification of which countries C_i are adjacent to which countries C_j. A *feasible 2-coloring* assigns one of two colors to each country, such that no adjacent countries are the same color. (For example, the squares of a chessboard have a feasible 2-coloring.)

Given a map, explain how to construct a CNF expression that is satisfiable iff a feasible 2-coloring exists for the map.

(b) (5) Explain how to use a CNF satisfiability-checker to prove that two given countries (call them C_1 and C_2) must be the same color in any feasible 2-coloring of a given map.

3. Induction Proof:

(10) Consider the following:

Theorem 0.1: *For all integers $n \geq 1$, we have $5n - 5 = 0$.*

Plainly this "theorem" is false. What is wrong with the following "proof"?

Proof: We use strong induction on $\mathbf{N}$.

- Base case ($n = 1$): $5 \cdot 1 - 5 = 0$.
- Inductive step:

$$\begin{aligned} 5(n+1) - 5 &= 2(5n - 5) - (5(n-1) - 5) \\ &= 2(0) - 0 \\ &= 0. \end{aligned}$$

□

4. Modular Arithmetic:

If $13x = 5 \pmod{46}$, what is x? (Short answer.)

5. Modular Arithmetic:

What is the maximum number of solutions for x in the range $\{0, \dots, N-1\}$ for any equation of the form $ax = b \pmod N$, when $gcd(a, N) = d$? (Short answer: an expression possibly involving N, a, b, and/or d.)

6. Trees

Given an n-vertex tree, Bob added 10 edges to it, then Alice removed 5 edges and the resulting graph has 3 connected components. How many edges must be removed to remove all cycles in the resulting graph? (An expression that may contain n.)

7. Quantifiers: Does the below statements always hold regardless of P's value.

a. $(\forall n \in N)(P(n))$
b. $(P(0) \wedge P(1)) \rightarrow ((\forall n \in N)(n \geq 1 \rightarrow P(n)))$
c. $((\forall n \in N)(n \text{ is odd} \rightarrow P(n))) \rightarrow ((\forall n \in N)(n \geq 1 \rightarrow P(n)))$
d. $(\forall n \in N)(P(2n))$

8. Short Answer:

(a) What is $3^{240} \pmod{77}$?

(b) What is $3^{16} * 3^{-1}$ mod 7? (Hint: the multiplicative inverse of 3 is 5 modulo 7 and repeated squaring.)

(c) Given an RSA scheme for large primes p and q where $q < p < 2q$ we can set $e = p$ and get a valid construction. (True or False.)

(d) What is d for RSA scheme with $(N = 143, e = 11)$?

9. Polynomials & Error Correction

(a) How many different degree $\leq d$ polynomials modulo p contain d points; $(x_1, y_1), \ldots, (x_d, y_d)$. (Assume that $p > d$.)

(b) What is the maximum number of times that a degree 4 polynomial, $P(x)$, and a degree 2 polynomial, $Q(x)$, can intersect? (That is, what is the maximum number of x-values where $P(x) = Q(x)$.)

(c) What is the minimum modulus that could be used to send the message $3,4,3$ through a channel that drops 3 packets?

(d) What is the polynomial that encodes the message $3,3,0$ modulo 7. (Use the x values $0,1,2$ in your encoding.)

(e) What is the error polynomial for Berlekamp-Welsh for a message $\pmod{11}$ where errors appeared at $x = 2$ and $x = 4$?

(f) We are working modulo seven, $\pmod 7$, in this problem. We have polynomials

$$\begin{array}{lll} p_1(1) = 3 & p_1(2) = 0 & p_1(3) = 0 \\ p_2(1) = 1 & p_2(2) = 1 & p_2(3) = 0 \\ p_3(1) = 0 & p_3(2) = 0 & p_3(3) = 1 \end{array}$$

Describe a polynomial $p(x)$ where $p(1) = 5, p(2) = 3$ and $p(3) = 1$ in terms of polynomials $p_1(x), p_2(x)$, and $p_3(x)$. (Remember this is all $\pmod 7$.)

10. True or False

1. $(\neg P \implies R) \wedge (\neg P \implies \neg R) \equiv P$

   ○ True

   ○ False

2. $\forall x \in \mathbb{N}, (P(x) \wedge (\exists y \in \mathbb{N}, Q(x,y)) \equiv \forall y \in \mathbb{N}, \exists x \in \mathbb{N}, P(x) \wedge Q(x,y).$

   ○ True

   ○ False

3. $(\neg P(0) \wedge \forall n \in \mathbb{N}, (P(n) \implies P(n-1))) \equiv \forall n \in \mathbb{N}, \neg P(n)$

   ○ True

   ○ False

4. $\forall x, ((P(x) \implies Q(x)) \wedge Q(x)) \equiv \forall x, P(x)$

   ○ True

   ○ False

5. $P \vee Q \equiv \neg P \implies Q$

   ○ True

   ○ False

11. Strong Induction vs Strengthening Hypothesis

Use induction to prove that $1 + \frac{1}{2} + \cdots (\frac{1}{2})^n \leq 2$? (Hint: strengthen the statement.)

12. Graphs!

Consider a directed graph where every pair of vertices u and v are connected by a single directed arc either from u to v or from v to u. Show that every vertex has a directed path of length at most two to **the vertex with maximum in-degree.** Note that this is quite similar to a homework problem but asks for a more specific answer. (Hint: Our solution doesn't require induction.)

13. Short Graph Questions

For all $n \geq 3$, the complete graph on n vertices, K_n has more edges than the d-dimensional hypercube for $d = n$. (True or False)

The complete graph with n vertices where p is an odd prime can have all its edges covered with x Rudrata cycles: a cycle where each vertex appears exactly once. What is the number, x, of such cycles in a cover? (Answer should be an expression that depends on n.)

14. Quick Proofs

Prove or disprove that for integers a, b, if $a + b \geq 1016$ that either a is at least 508 or b is at least 508.

15. RSA and CRT

Given an RSA public key pair $(N, e = 3)$, somehow you obtain d. Give an efficient algorithm to find p and q? (Hint: e is 3.)

16. Modular Arithmetic Short Answers

1. What is $2^{24} \pmod{35}$?

2. What is the $x \pmod{105}$ where $x = 1 \pmod{3}$, $x = 0 \pmod{5}$ and $x = 0 \pmod{7}$?

3. How many numbers in $\{0, \ldots, 104\}$ are relatively prime to 105?

4. What is $2^{49} \pmod{105}$?

5. What is the multiplicative inverse of 3 modulo 37?

17. Modular Short Answers

1. (Short Answer.) Give a number y modulo 35, where $y = 0 \pmod 5$ and $y = 1 \pmod 7$.

2. (Short Answer.) Give a number y modulo 35, where $y = 1 \pmod 5$ and $y = 0 \pmod 7$.

3. (Short Answer)Give a number y modulo 35, where $y = 4 \pmod 5$ and $y = 3 \pmod 7$.

4. (True/False) The public key d is relatively prime to $(p-1)(q-1)$.

   ○ True

   ○ False

5. Consider an RSA scheme where $p = 23, q = 5$ and $e = 3$. What is d?

18. True False Exercises

(a) A proposition and its contrapositive cannot both be true.
Circle one: **True** **False**

(b) The proposition $(A \wedge B) \vee (\neg A \wedge B) \vee \neg B$ can never be false.
Circle one: **True** **False**

(c) The hypercube graph always has an Eulerian tour.
Circle one: **True** **False**

(d) If $f\colon A \to B$ is an injective (1-1) function, then there exists a surjective (onto) function $g\colon B \to A$.
Circle one: **True** **False**

(e) If $\gcd(a,b) = d$, then a has no factor larger than d.
Circle one: **True** **False**

(f) In RSA with modulus $n = 91$ and encryption power $e = 5$, the decryption power is $d = 73$ because $de = 365 \equiv 1 \bmod 91$.
Circle one: **True** **False**

(g) If the multiplicative inverse $a^{-1} \bmod p$ exists for all $a \in \{1, \ldots, p-1\}$, then p is a prime.
Circle one: **True** **False**

(h) For any $d \in \mathbb{N}$, the set of polynomials of degree d with integer coefficients is countable.
Circle one: **True** **False**