CS 70 Discrete Mathematics for CS
Fall 2004 Rao

Midterm 1

PRINT your name: ______________________________, ______________________________
(last) (first)

SIGN your name: ____

PRINT your username on `cory.eecs`: ________________________________

WRITE your section number (101 or 102): ____________________

Three sides of 8.5 by 11 sheet of notes is permitted. No calculators are permitted. Do all your work on the pages of this examination. If you need more space, you may use the reverse side of the page, but try to use the reverse of the same page where the problem is stated.

You have 110 minutes. The questions are of varying difficulty, so avoid spending too long on any one question.

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

Problem 1	
Problem 2	
Problem 3	
Problem 4	
Problem 5	
Problem 6	
Total	

Problem 1. [True or false] (25 points)

Circle TRUE or FALSE. There is no need to justify your answers on this problem.

(a) TRUE or FALSE: If the implication $\not P \implies Q$ is true, then $\not Q \implies P$.

True

(b) TRUE or FALSE: If A **or** B is true and B are true than A must be true.

(c) TRUE or FALSE: $gcd(n+1, 2n+1) = 1$.

True. Apply Euclid's algorithm.

(d) TRUE or FALSE: For all $n > 1$, $2^n - 1$ is prime.

False. $2^4 - 1 = 15$ is not prime.

(e) TRUE or FALSE: For all odd n, $gcd(n, n-2) = 1$.

True. Assume $n = ad$ and $n - 2 = a'd$, then n and $n - 2$ must differ by at least d (or be the same number) but d cannot be 2.

(f) TRUE or FALSE: For all a, m, $a^{m-1} = 1 \mod p$.

False. $a = 0$ for any m.

(g) TRUE or FALSE: For all $a, m = pq$, where p and q are prime, $a^{(p-1)(q-1)} = 1 \mod m$.

False. $a = 0$ for any m.

(h) TRUE or FALSE: For all $a, m = pq$, where $gcd(a, m) = 1$ and p and q are prime, $a^{(p-1)(q-1)} = 1 \mod m$

True. Fermat's little theorem.

(i) TRUE or FALSE: 5 has an inverse mod 12?

True. 5 is the inverse of 5 mod 12.

(j) TRUE or FALSE: The complete graph on n nodes is the graph where every pair of nodes is an edge. The complete graph on n nodes is Eulerian for n odd. **True.** The degree is $n - 1$ which is even which implies that the graph is Eulerian.

Problem 2. [Proof by Induction] (15 points)

Prove by induction that 9 divides $n^3 + (n+1)^3 + (n+2)^3$ for all $n \in \mathbf{N}$.

Proof by induction. Base case: For $n = 0$, the expression evaluates to 27 which is divisible by 9.

Assume that $n^3 + (n+1)^3 + (n+2)^3 = 9a$ for some integer a.

We will prove that

$$(n+1)^3 + (n+2)^3 + (n+3)^3 = 9b$$

for some integer b. Expanding the left hand side and collecting terms, we get

$$n^3 + (n+1)^3 + (n+2)^3 + 27n + 9n^2 + 27.$$

The first three terms is equal to $9a$, the second three is equal to $9c$ where $c = (3n + n^2 + 3)$ which is an integer, thus the expression equals $9(a+c)$ where $(a+c)$ is an integer.

Problem 3. [Graphs] (5 points)

Prove that the complete graph on n nodes is Hamiltonian, for $n \geq 3$.

Proof. A number of proofs work here. Here is one. The sequence of nodes $1, \ldots n$, is a hamiltonion cycle since every edge $(i, i+1)$ and the edge $(n, 1)$ is present.

Here is another. A three node comlete graph is hamiltonian. Given that the $n-1$ node complete graph is hamiltonian, one can construct a Hamiltonian cycle in the n node complete graph by noting that removing a single node yields an $n-1$ node complete graph, forming a Hamiltonian cycle in that graph, and then inserting the new node at any point in the Hamiltonian cycle. The new path is hamiltonian since the new node is connected to its predecesser and successor.

Problem 4. [RSA] (20 points)

1. Say Bob is generating an RSA pair from $p = 5$ and $p = 7$. Say he chooses $e = 3$. What is the problem?
   The RSA scheme requires that $d = e^{-1} \mod (q-1)(p-1)$.
2. Say he chooses $e = 5$, what would the decryption key d be?
3. Encrypt the message 6.
4. Why is encrypting 5 a bad idea?

Problem 5. (Polynomials) (15 points)

1. Given a polynomial of degree at most $n-1$, and n points $(x_1,y_2),(x_2,y_2)..(x_n,y_n)$ that all fall on a degree 1 polynomial, must the polynomial be of at most degree 1? Argue your answer is correct. (Hint: recall that a degree d polynomial can only have d zeros. And adding two polynomials results in a polynomial of degree at most the maximum of the two.)

2. Find the degree 2 polynomial over Z_5, that passes through $(0,1),(1,2),(2,2)$.

Problem 6. [Berlekemp-Welsh] (15 points)

Consider a message $m_1, \ldots, m_n$ where each m_i is a field element. Consider the degree $n-1$ polynomial P where $P(i) = m_i$. Recall that knowing any n correct points on the polynomial allows us to reconstruct the polynomial.

1. Consider a set of $n+2k$ points where at least $n+k$ of them lie on $P(x)$. Argue that the only degree $n-1$ polynomial that hits at least $n+k$ of these points is $P(x)$.
2. Consider a transmission of the polynomial encoding, where errors occur at points 0, 1 and 2. What is the definition of the error polynomial defined in our lecture on the Berlekamp-Welsh lecture?