CS70: Midterm 1

Instructor: Satish Rao

Fall 2004

Three sides of an 8.5×11 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.

Problem 1. [True or false] (30 points)

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

a TRUE or FALSE: If the implication $\bar{P} \rightarrow Q$ is true, then $\bar{Q} \rightarrow P$.

b TRUE or FALSE: If A or B is true, and B is true, then A must be true.

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

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

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

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

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

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

i TRUE or FALSE: 5 has an inverse 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.

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

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

Problem 3. [Graphs] (5 points)

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

Problem 4. [RSA] (20 points)

1. Say Bob is generating an RSA pair from $p = 5$ and $q = 7$. Say he chooses $e = 3$. What is the problem?
2. Say he chooses $e = 5$, what would the decryption key d be?
3. Encrypt the message 6.
4. Why is encrypting 5 and bad idea?

Problem 5. [Polynomials] (15 points)

1. Given a polynomial of degree at most $n - 1$ and n points (x_1, y_1), (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 zeroes. 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 allow 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?