CS 70 Discrete Mathematics and Probability Theory
Fall 2015 Rao/Walrand Midterm 2

PRINT Your Name: _____, _____
(last) (first)

SIGN Your Name: _____

PRINT Your Student ID: _____

CIRCLE your exam room: 2040 VLSB 2060 VLSB 145 Dwinelle 155 Dwinelle 10 Evans OTHER

Name of the person sitting to your left: _____

Name of the person sitting to your right: _____

- After the exam starts, please write your student ID (or name) on every odd page (we will remove the staple when scanning your exam).
- We will not grade anything outside of the space provided for a problem. Please use scratch paper as necessary and clearly indicate your answer.
- On the short answer questions 1-5. You need only give the answer in the format requested (e.g., true/false, an expression, a statement.) We note that an expression may simply be a number or an expression with a relevant variable in it. **We will only grade the answers, and are unlikely to even look at any justifications or explanations.**
- On questions 6 and 7, do give arguments, proofs or clear descriptions as requested.
- You may consult two sides of notes. Apart from that, you may not look at books, notes, etc. Calculators, phones, and computers are not permitted.
- There are 10 pages on the exam. Notify a proctor immediately if a page is missing.
- **You may, without proof, use theorems and facts that were proven in the notes and/or in lecture.**
- **You have 105 minutes: there are roughly 30 parts on this exam.**
  - **Problems 1-5: roughly 20 short answers total. No justification required!**
  - **Problem 6a. A proof. Problem 6b: A multipart problem with a proof.**
  - **Problem 7: 6 part problem, first part is possibly not hard.**

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

1. Short Answer: Modular Arithmetic/RSA. 16 points: 3/3/3/3/4

Clearly indicate your correctly formatted answer: this is what is to be graded. No need to justify!

For each question, please answer in the correct format. When an expression is asked for, it may simply be a number, or an expression involving variables in the problem statement, you have to figure out which is appropriate.

(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 $(N = 143, e = 11)$?

(e) Background: Alice wants a signature of x from Bob but doesn't want Bob to know x.
Let (N, e) be Bob's public key, and d be his decryption key. Alice chooses a random r that is relatively prime to N, and sends Bob $r^e x \pmod{N}$ to sign, and Bob returns $m = (r^e x)^d \pmod{N}$ to Alice .
Give an expression that yields Bob's signature of x: $x^d \pmod{N}$. Your expression may use the variables m, x, r, N and e.

2. Polynomials. 19 points. 3/3/3/3/3/4

Clearly indicate your correctly formatted answer: this is what is to be graded. No need to justify!

(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 $\pmod{7}$.)

3. Short Answer: Counting. 18 points: 3/3/3/3/3/3

Clearly indicate your correctly formatted answer: this is what is to be graded. No need to justify!

(a) How many distinguishable orderings of CALIFORNIA are there?

(b) How many ways are there to split up 10 dollars among Bob, Alice and Eve? (Notice that it is valid to give 0 to one or two of the people.)

(c) How many ways are there to split up 10 dollars among Bob, Alice and Eve so that Eve gets at least 5 dollars?

(d) How many ways are there to place k indistinguishable balls into n distinguishable bins?

(e) How many five card heart flushes are there in a fifty two card poker deck? (A heart flush has all the cards being a heart. Recall also that each suit has thirteen cards.)

(f) How many five card poker hands have exactly one Ace or is completely composed of clubs (a club flush)?

4. Short Answer: Countable and UnCountable. 6 points. 3/3

Clearly indicate your correctly formatted answer: this is what is to be graded. No need to justify!

(a) Give a bijection from the real number interval $(1,\infty)$ to the real number interval $(0,1)$. (Notice the intervals are open.)

(b) Given an $n \times n$ matrix A where the diagonal consist of alternating 1's and 0's starting from 1, $A[0,0] = 1$, describe a n length vector from $\{0,1\}^n$ that is not equal to a row in the matrix. (Hint: the all ones vector or the all zeros vector of length n could each be rows in the matrix.)

5. Short Answer: Computability. 6 points. 3/3.

Clearly indicate your correctly formatted answer: this is what is to be graded. No need to justify!

(a) The problem of determining whether a program halts in time 2^{n^2} on an input of size n is undecidable. (True or False.)

(b) There is no computer program DEAD which takes a program P, an input, x, and a line number, n, and determines whether the nth line of code is executed when the program P is run on the input x. (True or False.)

6. A couple of proofs. 20 points: 8/12.

(a) Give a combinatorial proof that $3^n = \sum_{i=0}^{i=n} \sum_{j=0}^{j=n-i} \binom{n}{i} \times \binom{n-i}{j}$

(b) Let S_n be the numbers in $\{0,\ldots,n-1\}$ that are relatively prime to n.

(i) For a set $T_a = \{ax \pmod{n} : \ x \in S_n\}$ where $a \in S_n$ show that $T_a = S_n$.

(ii) For any $a \in S_n$, $a^x = 1 \pmod{n}$. What is x? (State your answer as an expression using S_n and other standard math expression symbols, e.g, $|\cdot|$. Briefly justify.)

(iii) For $n = pq$ where p, and q are distinct primes, what is $|S_n|$?

7. Hamming: Another optimal code. 16 points. 3/3/3/3/2/2

(a) Consider communicating 7 bits in an 8 bit message where the final bit will be the parity of the number of ones in the first seven. That is, if the number of ones is odd in the first 7 bits, the 8th bit will be 1, if the number of ones is even, the 8th bit is 0. Given that at most 1 bit gets corrupted, how can you tell if the message was corrupted or not. (Notice the parity bit itself could be the bit that was corrupted.)

(b) Consider communicating 4 bits in an 7 bit message. We will make sure the following equations holds.

$$m_1 + m_3 + m_5 + m_7 = 0 \pmod 2$$
$$m_2 + m_3 + m_6 + m_7 = 0 \pmod 2$$
$$m_4 + m_5 + m_6 + m_7 = 0 \pmod 2$$

We will send a message 1011 by setting bits $m_1 = 1, m_2 = 0, m_3 = 1, m_4 = 1$. How should the bits m_5, m_6 and m_7 be set to satisfy the equations above.

(c) Say the previous encoding was used and the message received was 1101100, where there is at most one bit that was flipped. What was the original message? (Note the message you should reconstruct is not necessarily the one from part (b).)

(d) Argue that you can recover from any 1-bit error using the scheme above.

(e) A codeword is any 7-bit string that satisfies the equations above. As the codewords are 7-bit strings, we can consider them to be vertices in a 7 dimensional hypercube. What is the minimum distance (length of a path) in the hypercube between codewords?

(f) Notice that there are 7 places where an error can occur plus a case where no error occurs or a total of 8 possible outcomes of the transmission. Argue that at least 3 extra bits are required to recover from one error; i.e., that one can only transmit 4 message bits in any scheme that send at least 7 bits and tolerates a single bit flip error.