CS 70 Discrete Mathematics and Probability Theory
Spring 2015 Vazirani Midterm #2

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

SIGN your name: ______________________________

PRINT your student ID: ________________________

CIRCLE your exam room: 3106 Etcheverry 3108 Etcheverry 180 Tan

241 Cory 247 Cory 1 Pimentel

Name of the person sitting to your left: ____________________

Name of the person sitting to your right: ____________________

Please write your name and student ID on every page.

Please write your answers in the spaces provided in the test. We will not grade anything on the back of an exam page or outside the space provided for a question unless we are clearly told on the front of the page in the space provided for the question to look there.

You may consult one double-sided sheet of handwritten notes. Apart from that, you may not look at books, notes, etc. Calculators and computers are not permitted.

You have 110 minutes. There are 5 questions worth a total of 100 points. Use the number of points as a rough guide for the amount of time to allocate to that question. Note that many of the points are for proofs and justifications for your answers. Please make sure you spend the time to write clear, correct and concise justifications. Good luck!

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

Q.1 / 40	Q.2 / 10	Q.3 / 10	Q.4 / 20	Q.5 / 20	Total / 100

Name: ______________________ SID: ______________

1. **Short Answers (40 points)**

   Provide brief justifications of your answers. In parts (d)–(f) you can leave your answers as factorials, n choose k, etc., but do explain your calculations clearly.

   (a) Are there integers x, y such that $21x + 55y = 3$?

   (b) Is the set of all C programs countable?

   (c) Consider a function f that takes as input a program P, and outputs:

   $$f(P) = \begin{cases} 1 & \text{if program } P \text{ on input } P \text{ does not halt within the first 1000 steps,} \\ 0 & \text{otherwise.} \end{cases}$$

   Is f computable?

   (d) How many seven-card hands are there with three pairs? That is, there are two cards each of three different ranks, and one card of a different rank. For example, $(2\clubsuit, 2\heartsuit, 5\diamondsuit, 5\spadesuit, 6\clubsuit, 10\diamondsuit, 10\spadesuit)$ is one such hand with three pairs, but $(2\clubsuit, 2\heartsuit, 5\diamondsuit, 5\spadesuit, 5\clubsuit, 10\diamondsuit, 10\spadesuit)$ is not. Here the ordering does not matter.

(e) How many different ways are there to rearrange the letters of DIAGONALIZATION without the two N's being adjacent?

(f) How many non-decreasing sequences of k numbers from $\{1,\dots,n\}$ are there? For example, for $n = 12$ and $k = 7$, $(2,3,3,6,9,9,12)$ is a non-decreasing sequence, but $(2,3,3,9,9,6,12)$ is not.

For the remaining two parts: Three people each independently choose a random number between 1 and 50. Let $A_{i,j}$ be the event that persons i and j choose the same number. Let $A_{1,2,3}$ be the event that all three people choose the same number.

(g) Are $A_{1,2}$ and $A_{2,3}$ independent?

(h) Are $A_{1,2}$ and $A_{1,2,3}$ independent?

Name: ______________________________ SID: ______________

2. **Las Vegas (10 points)**

   A certain dice game in Las Vegas involves the dealer rolling either two or three standard (six-sided) dice with 50-50 probability and then reporting the total of all rolls. Suppose that after such a roll the reported total is 3. What is the probability that the dealer rolled two dice? Express your answer as a rational number in its lowest terms. Make sure you explain your calculation clearly.

3. **Infinity (10 points)**

Find the precise error in the following proof:

Theorem: The set of rationals between 0 and 1 is uncountable.

Proof: Suppose towards a contradiction that there is a bijection $f : \mathbb{N} \to \mathbb{Q}[0,1]$, where $\mathbb{Q}[0,1]$ denotes the rationals between 0 and 1. This allows us to list all the rationals between 0 and 1, with the j-th element of the list being $f(j)$. Now consider the number d along the diagonal, whose j-th digit d_j is the j-th digit of $f(j)$. We define a new number e, whose j-th digit e_j is equal to $(d_j + 5) \bmod 10$. We claim that e does not occur in our list of rationals between 0 and 1. This is because e cannot be the j-th number on the list for any j, since it differs from the j-th number on the j-th digit. Contradiction. Therefore the set of rationals between 0 and 1 is uncountable.

$$\begin{array}{ccccccccc}
j & \leftrightarrow & & & f(j) & & & & \\ \hline
0 & \leftrightarrow & 0. & \boxed{5} & 2 & 1 & 4 & 9 & \dots \\
1 & \leftrightarrow & 0. & 1 & \boxed{4} & 1 & 6 & 2 & \dots \\
2 & \leftrightarrow & 0. & 9 & 4 & \boxed{7} & 8 & 2 & \dots \\
3 & \leftrightarrow & 0. & 5 & 3 & 0 & \boxed{9} & 8 & \dots \\
4 & \leftrightarrow & 0. & 6 & 2 & 5 & 7 & \boxed{2} & \dots \\
\vdots & & & & & \vdots & & &
\end{array}
\qquad \Longrightarrow \qquad
\begin{array}{c}
d = 0.54792\dots \\
\downarrow \\
e = 0.09247\dots
\end{array}$$

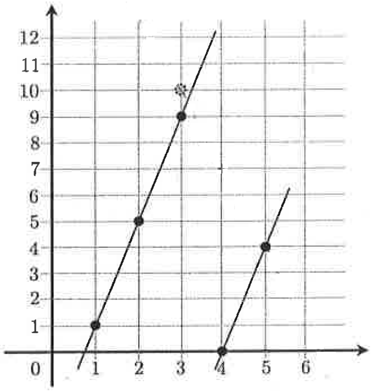
4. **Error Correction (20 points)**

Recall that a polynomial error correcting code sends a message $m_1, \ldots, m_{d+1}$ consisting of $d+1$ characters, each modulo a prime q, by constructing a polynomial $P(x)$ of degree (at most) d such that $P(i) = m_i$ for $i = 1, \ldots, d+1$. We transmit the message along with several additional points on $P(x)$ to guard against errors.

The main idea behind error correction is to try to recover the degree d polynomial that was used to create the encoded message. The way this is done is by finding a polynomial of degree d that goes through the maximum number of received points.

(a) Consider the following example where we are working modulo 13 and the message is $m_1 = 1$ and $m_2 = 5$. We encode the message using a polynomial $P(x) = 4x - 3$ of degree 1 over $GF(13)$. The transmitted points $P(1) = 1$, $P(2) = 5$, $P(3) = 9$, $P(4) = 0$, $P(5) = 4$ lie on a line (shown as black points below; the line "wraps around" because we are working mod 13).

Suppose that the received values are $r_1 = 1$, $r_2 = 5$, $r_3 = 10$, $r_4 = *$, and $r_5 = 4$, with errors in positions 3 (shown as grey dotted point below) and 4. Specify a value for r_4 such that the recipient cannot uniquely decode the message. Justify your answer.



Name: ______________________________ SID: ________________

(b) In part (a) we showed that transmitting 3 extra points does not protect against two errors. In this problem you will prove that transmitting 4 extra points is sufficient to correct two errors.

Specifically, consider the same setting as in part (a), but suppose we transmit 6 points instead of 5: $P(1)$, $P(2)$, $P(3)$, $P(4)$, $P(5)$, and $P(6)$. The received values are r_1, r_2, r_3, r_4, r_5, r_6, with two errors, say in positions 1 and 2: i.e. $r_1 \neq P(1)$ and $r_2 \neq P(2)$. Clearly the original polynomial $P(x)$ agrees with four of the received values. Prove that no other degree 1 polynomial can agree with more than 3 of the received values. This means the recipient can uniquely reconstruct $P(x)$, and therefore the original message.

(Note: You must prove this from first principles relying on simple properties of polynomials. You are not allowed to rely on any results about the Berlekamp-Welch algorithm.)

Name: ______________________________ SID: ______________

5. **Random RSA (20 points for parts (a)–(c), extra credit for part (d))**

   Let $n = pq$ be the product of two distinct primes, and let $E(a) = a^e \bmod n$ be the RSA encryption function, where as usual, the exponent e is relatively prime to $(p-1)(q-1)$. In this problem we will explore the probabilistic aspect of RSA.

   (a) Show that if r is chosen uniformly at random mod n, then $E(r)$ is also a uniformly random number mod n. That is, prove that $\Pr[E(r) = i] = 1/n$ for every $i \in \{0, 1, \ldots, n-1\}$.

   (b) Show that $E(ab \bmod n) = E(a)E(b) \bmod n$ for any messages a and b.

(c) Let a be relatively prime to n. Show that if r is chosen uniformly at random mod n, then $E(a)E(r) \bmod n$ is also a uniformly random number mod n. Make sure you explain where you use the assumption that $\gcd(a,n) = 1$.

(d) **(Extra credit)** Alice suspects that Bob might have misplaced his RSA private key. So she asks him to decrypt a cypher text to prove to her that he still has it. She assures him this is completely safe because the cypher text that she has chosen is uniformly random and nonzero (mod n). After all, as she explains to Bob, she has the ability to decrypt a random nonzero cypher text herself by just picking a uniformly random r from $\{1,\dots,n-1\}$ and encrypting it using Bob's public key to get $c = E(r)$. Then c is a uniformly random nonzero cypher text and Alice knows its decryption.

Bob suspects there is something fishy about Alice's claim, but he believes her anyway, and is willing to decrypt a random nonzero cypher text for Alice. It turns out Alice has an ulterior motive: She has intercepted a cypher text $E(a)$ that Eve sent Bob and is dying to decrypt it to recover the message a.

Show how Alice can give Bob a uniformly random nonzero cypher text to decrypt and use his answer to recover the message a.