CS 70 Discrete Mathematics and Probability Theory
Fall 2016 Seshia and Walrand Midterm 2

PRINT Your Name: ______________________________, ______________________________

(last) (first)

SIGN Your Name: _____________________________________

PRINT Your Student ID: _____________________________________

CIRCLE your exam room:
Pimentel 1 GPB 100 Hearst Annex A1 Soda 320 Latimer 120 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 unless we are clearly told in the space provided for the question to look elsewhere.
- The questions vary in difficulty, so if you get stuck on any question, it might help to leave it and try another one.
- On questions 1-2: You need only give the answer in the format requested (e.g., true/false, an expression, a statement.) Note that an expression may simply be a number or an expression with a relevant variable in it. **For short answer questions, correct clearly identified answers will receive full credit with no justification. Incorrect answers may receive partial credit.**
- On question 3-8, do give arguments, proofs or clear descriptions as requested.
- You may consult only *2 sheets of notes*. Apart from that, you may not look at books, notes, etc. Calculators, phones, computers, and other electronic devices are NOT permitted.
- There are **14** single sided pages on the exam. Notify a proctor immediately if a page is missing.
- **You may, without proof, use theorems and lemmas that were proven in the notes and/or in lecture.**
- **You have 120 minutes: there are 8 questions on this exam worth a total of 115 points.**

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

1. TRUE or FALSE?: total 24 points, each part 3 points

For each of the questions below, answer TRUE or FALSE.

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

1. If $x \equiv y \pmod{n}$, $z \equiv w \pmod{n}$, and $GCD(z,n) = GCD(w,n) = 1$, then $x \cdot z^{-1} \equiv y \cdot w^{-1} \pmod{n}$, where z^{-1} and w^{-1} are the inverses of z and $w \pmod{n}$.

2. $f(x) = x^5 \pmod{65}$, $x \in \{0,1,\ldots,64\}$, is not a bijection.

3. $11^{97} \pmod{105} = 11$

4. Polynomial $3x^3 + 5x^2 + 4x + 2$ is perfectly divisible by $x - 3$ (mod 7).

5. Every infinite subset of the set of real numbers $\mathbb{R}$ is uncountable.

6. There exists a program H that determines whether an arbitrary program P on input x outputs the value of $x + 42$ after executing 42 statements.

7. Let p and q be prime numbers, $p \neq q$. Then the number of natural numbers between 1 and pq which are relatively prime to pq is $(p-1)(q-1)$.

8. Professor Random has graded 100 exams and all scores are distinct. In class, she shuffles the exams and begins reading the scores aloud. Let A_k be the event that the kth exam score she reads is the top score so far. Then A_k and A_{k+1} are not independent.

2. **Short Answers: 5x3=15 points Clearly indicate your correctly formatted answer: this is what is to be graded.No need to justify!**

   1. You roll a balanced six-sided die three times. What is the probability that there are exactly two dice whose sum is 11?

   2. How many combinations of even natural numbers (x_1, x_2, x_3, x_4) are there such that $x_1 + x_2 + x_3 + x_4 = 20$?

   3. Astronomers at the University of Infinity have determined that there are countably infinite stars, and they have given each one a unique identifier in $\mathbb{N}$ defined by the function: $id : \text{Stars} \rightarrow \mathbb{N}$. Then, one day, they discover a new star s and add it to Stars. How can they set $id(s)$ to be distinct from all the other identifiers?

4. The standard polynomial secret sharing is being used and we are working mod 5. Three shares are required to determine the secret, encoded as $P(0)$. We have the following shares: $P(1) = 2, P(2) = 0, P(3) = 2$. What is the secret?

5. Suppose $x = 4 \pmod 7$ and $x = 7 \pmod{11}$. What is $x \pmod{77}$?

3. Short Proofs: 4+4+4+4+4=20 points

1. Let $r^2 = 1 \pmod{n}$. Show that, if $GCD(r-1,n) = 1$, then $r = n-1 \pmod{n}$.

2. Let $x_1, x_2, \ldots, x_n$ be n integers, and p be a prime number. Show that:
   $(x_1 + x_2 + \ldots + x_n)^p = x_1^p + x_2^p + \ldots + x_n^p \pmod{p}$.

3. Consider the function `is_mod_2` below which takes as input an arbitrary program `P`:

```
def is_mod_2(P):
 if (P implements the mod 2 function) then
   return TRUE
 else
   return FALSE
```

   Prove that `is_mod_2` cannot exist.

4. Assume $a > b \geq 1$ where $a, b \in \mathbb{N}$. Prove $\sum_{k=b}^{a} \binom{k}{b} = \binom{a+1}{b+1}$.

5. Suppose $P(B|A) = P(B|\bar{A})$ where $\bar{A}$ is the complement of A. Prove that it must be the case that B is independent of A.

4. Checking Work:3+3= 6 points

Each of the parts below has some work (proof, reasoning, computation, etc.) that you must check. State the *first error* you find, and explain your answer briefly.

1. Suppose Alice wishes to send Bob a confidential message using RSA. For this, Bob must first set up his public-private key pair. Below, we show the choices Bob made in picking his keys, where he makes at least one mistake.

   Suppose that Bob chooses primes $p = 7$, $q = 13$. (Assume these are large enough.)

   He computes $N = pq = 91$.

   Then Bob chooses $e = 3$ so his public key is $(3, 91)$.

   Finally Bob chooses $d = 61$ which is his private key.

   □

2. Proposition: Consider a set of n identical aliens who each want to pick a single color for their T-shirt from a set of k colors. Then the number of ways of assigning colors to the aliens is $\frac{k^n}{k!}$.

   Proof: The first alien picks a T-shirt color in k ways.

   Same for the second, third, etc. So total k^n ways.

   But these aliens are all identical, so we divide by the number of orderings of the k colors, which is $k!$.

   This yields the desired answer. □

5. Sharing RSA Keys: 5+5+5=15 points

Consider a set of n people connected on a broadcast network: that is, any message sent by one person intended for another can be received by all. Further, assume that there is exactly one malicious person on this network, named Eve.

Recall that RSA provides Alice a secure way of sending a message to Bob provided that she knows Bob's public key. But how does Alice get to know Bob's public key in the first place? She could send a message to Bob asking him for it, but what if Eve pretends to be Bob and sends her the wrong key?

To deal with this problem, Alice decides to design a new protocol based on the secret sharing scheme studied in class. The general idea is that Bob will send a piece of his public key to everyone, including Eve. If at least k of those people get together, they can reconstruct Bob's key. Otherwise, they cannot.

Answer the following questions:

(a) Recall that the public key is of the form (N,e), where $N = pq$. Design a polynomial $P(x)$ that Bob can use to share his public key using the protocol Alice designed.

(b) Now suppose Alice broadcasts a request for Bob's public key and gets back exactly k numbers. Can Alice always recover Bob's public key? Why or why not?

(c) At least how many numbers must Alice get back to be able to completely reconstruct the secret? Justify.

6. Correcting Errors that Grow: 5+5=10 points

Consider a communication channel that *slowly degrades* over time. Specifically, it behaves as follows: Of the first n packets, it drops none; of the second n packets, it drops 1 (but you don't know which one); of the third set of n, it drops some 2; and so on, until for the $n+1$th set of n packets (and thereafter), it drops all of them.

In the questions below, a message is the cumulative sequence of packets transmitted over the channel over all time. Justify all answers, supplying a proof where needed.

(a) Suppose the channel does not corrupt any packets. What is the maximum size, if any, of a message that you can transmit through this channel using the Erasure code you studied in class?

(b) Now suppose that the channel does not drop packets, but corrupts packets as above — i.e., corrupts none of the first n, an arbitrary one of the next n, etc. What is the maximum size message you can transmit successfully using Reed-Solomon codes and Berlekamp-Welch decoding?

7. **Countability: 5+5=10 points**

Let S be the power set of $\mathbb{E}$, the set of all *even* natural numbers. Let T be the set of functions that map $\mathbb{E}$ to $\{0,1\}$.

(a) Prove that there exists a bijection between S and T.

(b) Is S countable? Justify your answer.

8. Line up for Class, Randomly: 3+3+3+6=15 points

There is a class with $2n$ children where n are boys and n are girls. They have to stand in a line to go to class. Assume that all possible ways in which they might line up are equally likely.

Answer the following questions. *Justify/prove your answer in all cases.*

(a) What is the probability that they alternate by gender?

(b) What is the probability that all of the girls are before all of the boys?

(c) What is the probability that between any two girls there are no boys (i.e. that all of the girls stand together in an uninterrupted block)?

(d) What is the probability that neither the boys nor the girls stand together in an uninterrupted block?

(Scratch space)