CS 70 Discrete Mathematics for CS Fall 2003 Wagner Midterm 2

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

SIGN your name: _____

PRINT your username on `cory.eecs`: _____

WRITE your section number (101 or 102): _____

This exam is open-book, open-notes. *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 80 minutes. There are 4 questions, worth from 20 to 30 points each (100 points total). 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	
Total	

Problem 1. [True or false] (20 points)

Circle TRUE or FALSE. You do not need to justify your answers on this problem.

N denotes the set of natural numbers, $\{0, 1, 2, \ldots\}$.

(a) TRUE or FALSE: Let p be prime; then we're guaranteed that $x^{p-1} \equiv 1 \pmod{p}$ for all $x \in \mathbf{N}$.

(b) TRUE or FALSE: Let $p \in \mathbf{N}$ be such that $x^{p-1} \equiv 1 \pmod{p}$ holds for every $x \in \mathbf{N}$ with $\gcd(x, p) = 1$; then p is guaranteed to be prime.

(c) TRUE or FALSE: Let p be prime and suppose $x \in \mathbf{N}$ satisfies $x \not\equiv 0 \pmod{p}$; then we're guaranteed that $x^{p^2-p} \equiv 1 \pmod{p^2}$.

(d) TRUE or FALSE: Let S, T be arbitrary sets; then we're guaranteed that $|S \cup T| = |S| + |T|$.

(e) TRUE or FALSE: Let A, B be events; then we're guaranteed that $\Pr[B \mid A] = \Pr[A \text{ and } B] / \Pr[B]$.

Problem 2. [Short answer] (30 points)

Show your work on these problems. Circle your final answer.

(a) You've been hired by the local phone company. They're concerned, because all the local taxi companies have started demanding phone numbers made up of exactly 2 different digits. (For instance, "555-5556" and "811-1881" are acceptable, but "111-1111" and "123-4567" are not.) Your job is to help the phone company figure out how long they've got before they run out of acceptable phone numbers.

How many 7-digit numbers are there that contain exactly 2 different digits?

(b) What is $70^{2003} \bmod 11$? Simplify your answer to an integer between 0 and 10.

(Reminder: *no calculators allowed!* You should be able to do this in your head, in any case.)

(c) What is 70^{2003} mod 77? Simplify your answer to an integer between 0 and 76.

(d) Suppose events A, B are independent, and moreover events B, C are independent. Are we guaranteed that events A, C are independent? Why or why not?

Problem 3. [An Insecure RSA Variant] (20 points)

After briefly toying with the idea of outlawing magic markers and the SHIFT key, Hapless Copy Protection, Inc. has decided that they are instead going to pursue a technical solution to the problem of MP3 sharing: they're going invent a new encryption algorithm. For maximum speed, their Cryptographer-In-Chief proposes a variant on RSA, where the modulus n is chosen to be a product of just *one* prime (i.e., $n = p$).

In other words, Bob's public key is (n, e), where n is prime and e is an encryption exponent satisfying $1 < e < n$. Bob's private key is d, the decryption exponent, satisfying $1 < d < n$. To encrypt a message m, Alice computes $c = m^e \bmod n$. To decrypt, Bob computes $c^d \bmod n$.

(a) To make this work, this variant needs a key generation procedure. How can Bob choose e and d so that the decryption algorithm will correctly recover the message that Alice encrypted?

(b) This scheme is insecure. Explain why.

Problem 4. [Counting] (30 points)

Call a ternary string *lovely* if every 0 is immediately followed by a 1 and every 1 is immediately followed by a 2. For instance, the strings "0120120120," "01212," and "222201" are all lovely, but "0120112" is not lovely. Let a_n denote the number of ternary strings of length n that are lovely.

(a) Find a recurrence relation that defines the sequence $a_0, a_1, a_2, \ldots$.

(b) Prove that $a_n \geq (\sqrt[3]{3})^n$ holds for all $n \in \mathbf{N}$.
Hint: $(\sqrt[3]{3})^2 + \sqrt[3]{3} + 1 \geq (\sqrt[3]{3})^3$.