CS 70 Discrete Mathematics for CS
Fall 2003 Wagner

MT2 Soln

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.

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

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

[Counterexample: $x \equiv 0 \pmod{p}$.]

(b) TRUE or $\boxed{\textbf{False}}$: 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.

[Counterexample: $p =$ any Carmichael number.]

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

[Proof: $\varphi(p^2) = p^2 - p$, since there are p multiples of p less than p^2. If $x \not\equiv 0 \pmod{p}$, then $\gcd(x, p^2) = 1$, and the result then follows from Euler's theorem.]

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

[Counterexample: $S = T = \{0\}$.]

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

[Counterexample: any events where $\Pr[A] \neq \Pr[B]$.]

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?

$$\binom{10}{2} \times (2^7 - 2) = \boxed{5670}.$$

$\binom{10}{2}$ counts the number of ways to pick two digits to be part of the phone number (e.g., 8 and 1).
2^7 counts the number of phone numbers you can make from those two digits (e.g., 811-1881, 888-8881, 888-8888), since in each of the 7 positions we can choose either of the two available digits.
Finally, we have to subtract 2 for the one-digit phone numbers (888-8888, 111-1111) which were counted in the 2^7 but which shouldn't be included in the final answer.

(b) What is 70^{2003} mod 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.)

$70^{2003} \equiv 4^{2003} \equiv 4^{2003 \bmod 10} \equiv 4^3 \equiv 64 \equiv 9 \pmod{11}$.
$\boxed{\text{Answer: 9 mod 11.}}$

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

$70^{2003} \equiv 0^{2003} \equiv 0 \pmod 7$.
By part (b), $70^{2003} \equiv 9 \pmod{11}$.
By the Chinese remainder theorem, we see
$70^{2003} \equiv 42 \pmod{77}$.

$\boxed{\text{Answer: 42 mod 77.}}$

Douglas Adams, eat your heart out!

(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?

$\boxed{\text{No.}}$

Counterexample:
Suppose we pick a card from a randomly shuffled deck.
Let $A =$ the card is a spade,
$B =$ the card is a queen,
$C =$ the card is a red card (a heart or diamond).

Then A, B are independent. Also, B, C are independent.
Yet, A, C are not independent, since $\Pr[A \mid C] = 0 \neq \Pr[A]$.

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?

Pick a random prime n.
Choose any e that is relatively prime to $n-1$ and that is in the range $1 < e < n$.
Let $d \equiv e^{-1} \pmod{n-1}$.
(Notice that e is guaranteed to have an inverse, with this choice of e.)
It's easy to check that

$$c^d \equiv (m^e)^d \equiv m^{ed} \equiv m^{ed \bmod n-1} \equiv m^1 \equiv 1 \pmod{n},$$

where we applied Fermat's little theorem and used the fact that n is prime.
Consequently, decryption is the inverse of encryption, and the scheme works.

(b) This scheme is insecure. Explain why.

Given only the public key, we can efficiently learn the private key.
In particular, given (n, e), any eavesdropper can efficiently compute $d \equiv e^{-1} \pmod{n-1}$ (use the extended Euclidean algorithm), and this is all an eavesdropper would need to know to decrypt traffic that was encrypted with this scheme.

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 $a_0, a_1, a_2, \ldots$.

$a_n = a_{n-1} + a_{n-2} + a_{n-3}$. $\quad\quad$ $a_0 = 1, a_1 = 3, a_2 = 5, a_3 = 9$.
Where did this come from?
Any lovely string of length $n \geq 3$ must fall into one of these three cases:

- It starts with 012, and then is followed by any lovely string of length $n-3$. (a_{n-3} ways)
- It starts with 12, and then is followed by any lovely string of length $n-2$. (a_{n-2} ways)
- It starts with 2, and then is followed by any lovely string of length $n-1$. (a_{n-1} ways)

These three cases are disjoint and exhaust all the possibilities, so the total number of lovely strings of length n must be the sum of the number of ways to get each of the three cases.

Alternatively, you could have drawn a tree diagram.

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

Proof by strong induction:
Base cases: $a_0 = 1 \geq (\sqrt[3]{3})^0$, $a_1 = 3 \geq (\sqrt[3]{3})^1 \approx 1.44$, $a_2 = 5 \geq (\sqrt[3]{3})^2 \approx 2.08$.
Inductive step: Assume that $a_k \geq (\sqrt[3]{3})^k$ holds for $k = 0, 1, \ldots, n-1$. Then

$$\begin{aligned}
a_n &= a_{n-1} + a_{n-2} + a_{n-3} && \text{(by the recurrence relation)}\\
&\geq (\sqrt[3]{3})^{n-1} + (\sqrt[3]{3})^{n-2} + (\sqrt[3]{3})^{n-3} && \text{(by the inductive hypothesis)}\\
&\geq [(\sqrt[3]{3})^2 + \sqrt[3]{3} + 1] \times (\sqrt[3]{3})^{n-3} &&\\
&\geq (\sqrt[3]{3})^3 \times (\sqrt[3]{3})^{n-3} && \text{(since } (\sqrt[3]{3})^2 + \sqrt[3]{3} + 1 \geq (\sqrt[3]{3})^3\text{)}\\
&\geq (\sqrt[3]{3})^n. &&
\end{aligned}$$

The result follows by the axiom of strong induction.

Alternate proof:
If "S" is any lovely string of length $n-3$, then "012 S", "122 S", and "222 S" are lovely strings of length n. Hence $a_n \geq 3a_{n-3}$.
The desired result then follows by an easy induction, similar to that above but a little simpler.

The chocolate challenge.

For any interested, here's an optional bonus problem for you to try.
The first to email me a valid solution to this problem will receive a bar of excellent chocolate, not to mention fame and the regard of all your colleagues.

We say that $f(x_1,\ldots,x_n)$ is *a symmetric function* if the parameters may be permuted (re-ordered) without changing the value of the function.

For instance, a symmetric function on two variables is any function f satisfying $f(x_1,x_2) = f(x_2,x_1)$ for all x_1,x_2. For three variables, a symmetric function is one satisfying $f(x_1,x_2,x_3) = f(x_1,x_3,x_2) = f(x_2,x_1,x_3) = f(x_2,x_3,x_1) = f(x_3,x_1,x_2) = f(x_3,x_2,x_1)$ for all x_1,x_2,x_3. And so on.

A symmetric polynomial is a polynomial that is a symmetric function.

The *elementary symmetric functions* are defined as follows. The first elementary symmetric function, $e_1(x_1,\ldots,x_n)$ is just the sum of its inputs:

$$e_1(x_1,\ldots,x_n) = x_1 + x_2 + \cdots + x_n.$$

Obviously this is a symmetric function. The second elementary symmetric function is

$$e_2(x_1,\ldots,x_n) = x_1x_2 + x_1x_3 + \cdots + x_1x_n + x_2x_3 + x_2x_4 + \ldots x_{n-1}x_n = \sum_{1\le i<j\le n} x_i x_j.$$

The third elementary symmetric function is

$$e_3(x_1,\ldots,x_n) = \sum_{1\le i<j<k\le n} x_i x_j x_k.$$

And so on. In general, the k-th elementary symmetric function (for $1 \le k \le n$) is given by

$$e_k(x_1,\ldots,x_n) = \sum_{I\subseteq\{1,\ldots,n\},|I|=k} \prod_{i\in I} x_i.$$

With that background, prove the following result:

Theorem. Let p be a prime, and let $e_k(x_1,\ldots,x_{p-1})$ be the k-th elementary symmetric polynomial for some $k \le p-2$. Then $e_k(1,2,\ldots,p-1) \equiv 0 \pmod{p}$.