CS 70 Discrete Mathematics and Probability Theory

Summer 2014 James Cook

Midterm 1 (Version B)

Instructions:

- Do not turn over this page until the proctor tells you to.
- Don't write any answers on the backs of pages (we won't be scanning those). There is an extra page at the end in case you run out of space.
- The exam has 10 pages (the last two are mostly blank).

PRINT your student ID: ____

PRINT AND SIGN your name: ____________________, ____________________ ________________________

(last) (first) (signature)

PRINT your discussion section and GSI (the one you attend): ____

Name of the person to your left: ____

Name of the person to your right: ____

Name of someone in front of you: ____

Name of someone behind you: ____

PRINT your name and student ID: ______________________________

True/False

1. (16 pts.) For each of the following statements, circle T if it is true and F otherwise. You do not need to justify or explain your answers.

T F One way to prove a statement P is to assume P and conclude $\neg P$.

T F To prove $P(n)$ is true for all negative integers n, it's enough to prove $P(-1)$ and $(\forall n \in \mathbf{Z})(P(n+1) \Rightarrow P(n))$.

T F $P \vee (Q \vee R) \equiv \neg(\neg P \wedge \neg(Q \wedge R))$

T F $(P \Rightarrow Q) \Rightarrow R \equiv \neg R \Rightarrow (P \wedge \neg Q)$

T F $(\exists x \in \mathbf{R})(\forall y \in \mathbf{R})(x > 0 \wedge x^2 \leq y)$

T F If p and q are prime numbers and $p \neq q$, then there exists a number x such that $x \cdot p \equiv 1 \pmod{q}$.

T F For every degree-5 polynomial $P(x)$, there are at least two real numbers $x, y \in \mathbf{R}$ such that $x \neq y$ and $P(x) = 0$ and $P(y) = 0$.

T F In every instance of the stable marriage problem, if a man M is optimal for a woman W, then W is not optimal for M.

PRINT your name and student ID: ______________________________

Short Answer

2. (4 pts.) Find a stable matching for the following instance of the stable marriage problem:

Woman	Prefs				Man	Prefs			
A	1	2	3	4	1	A	B	C	D
B	1	3	2	4	2	B	D	A	C
C	1	4	2	3	3	C	A	B	D
D	4	2	3	1	4	C	A	B	D

3. (4 pts.) Compute $2^{63} + 3^{14} \pmod 7$.

PRINT your name and student ID: ______________________________

4. (3 pts.) Suppose Alice wants to send Bob a message over an unreliable channel. Her message consists of 5 pieces, and each piece is a number in the range $0, 1, \dots, 18$. The channel might change up to 3 of the pieces of her message. Bob will not know which pieces were changed.

If Alice decides to use the error correcting code we learned in class, how many pieces (numbers) must she send?

5. (4 pts.) Compute $6^{122} \pmod{55}$.

6. (4 pts.) Prove that $(\forall x \in \mathbf{N})(\exists y \in \mathbf{N})(y > 1 \land \gcd(x, y) = 1)$.

Induction

7. (12 pts.) Prove using induction that for every integer $n > 0$, there exist integers a, b and c such that $a > 0$, $b > 0$, $c > 0$ and $a^2 + b^2 = c^n$.

Hint: You will probably want to use strong induction, and prove the statement for $n = 1$ and $n = 2$ first. For $n = 2$, one possible solution is $a = 3, b = 4, c = 5$.

Modular Arithmetic

8. (12 pts.) Find integers x and y in the range $0, 1, \ldots, 42$ satisfying the following two equastions:

$$12x \equiv y + 3 \pmod{43}$$

and

$$x + y \equiv 1 \pmod{43}.$$

PRINT your name and student ID: ______________________________

Secret Sharing

9. (12 pts.) Alice decides to share a secret with 12 people so that any 3 of them can get together to find out the secret.

Her secret is an integer s which is between 0 and 12. Following the secret-sharing protocol from class, she finds a polynomial $P(x)$ with the appropriate degree, such that $P(0) \equiv s \pmod{13}$.

Three of her friends decide to get together to learn the secret. Their combined knowledge is: $P(1) \equiv 2 \pmod{13}$, $P(2) \equiv 1 \pmod{13}$, and $P(8) \equiv 1 \pmod{13}$.

What is the secret $P(0)$? Express your answer as a number between 0 and 12.

Polynomials

10. (6 pts.) Suppose p is a prime number, $P(x)$ is a polynomial with degree d, and $0 < d < p/2$.
Prove that there are less than $2d+1$ distinct values of x such that $P(x)^2 - P(x) + 1 \equiv 0 \pmod{p}$.

PRINT your name and student ID: ______________________________

[Extra page. If you want the work on this page to be graded, make sure you tell us on the problem's main page.]

PRINT your name and student ID: ____

[Doodle page! Draw us something if you want or give us suggestions or complaints.]