CS 70 Discrete Mathematics and Probability Theory

Summer 2014 James Cook

Midterm 1

Thursday July 17, 2014, 12:40pm-2:00pm.

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 9 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	For all positive integers x and p, if $\gcd(x,p)=1$, then $x^{p-1} \equiv 1 \pmod{p}$.
T	F	One way to prove a statement of the form $P \implies Q$ is to assume $\neg Q$ and prove $\neg P$.
T	F	$\forall x \exists y P(x,y) \equiv \exists x \forall y P(y,x)$.
T	F	$P \Rightarrow (Q \Rightarrow R) \equiv (P \wedge Q) \Rightarrow R$
T	F	$P \Rightarrow (Q \wedge R) \equiv (P \Rightarrow Q) \vee R$
T	F	To prove $(\forall n \in \mathbf{N})P(n)$, it is enough to prove $P(0)$, $P(2)$ and $(\forall n \geq 2)(P(n) \Rightarrow P(n+2))$.
T	F	In a stable marriage instance, there can be two women with the same optimal man.
T	F	In stable marriage, if Man 1 is at the top of Woman A's ranking but the bottom of every other woman's ranking, then every stable matching must pair 1 with A.

Short Answer

2. (4 pts.) Compute $(2^3 \cdot 5^{71}) + (3^3 + 4^2) \bmod 8$.

3. (4 pts.) Compute $\frac{200 + 14 \cdot 102}{99} \bmod 10$.

4. (4 pts.) Prove that $(\exists x \in \mathbf{R})(\forall y \in \mathbf{R})\ x \cdot y < 2$.

RSA

5. (12 pts.) Someone sends Pandu an RSA-encrypted message x. The encrypted value is $E(x) = 2$. However, Pandu was silly and picked numbers far too small to make RSA secure. Given his public key $(N = 77, e = 43)$, find x.

Induction

6. (12 pts.) Prove that every two consecutive numbers in the Fibonacci sequence are coprime. (In other words, for all $n \geq 1$, $\gcd(F_n, F_{n+1}) = 1$. Recall that the Fibonacci sequence is defined by $F_1 = 1$, $F_2 = 1$ and $F_n = F_{n-2} + F_{n-1}$ for $n > 2$.)

Error-Correcting Codes

7. (15 pts.) Alice wants to send to Bob a message of length 3, and protect against up to 2 erasure errors. Using the error-correcting code we learned in class, she obtains a polynomial $P(x)$ modulo 11 and sends 5 points to Bob. Bob only receives 3 of the points: $P(1) = 4, P(3) = 1, P(4) = 5$.

(a) (12 pts.) Decode Alice's original message $P(1), P(2), P(3)$.

(b) (3 pts.) If Alice tried to send a message with a modulus of 10 instead of 11, what exactly could go wrong? (You don't need to do any computations in your answer.)

Polynomials

8. (16 pts.) Suppose P is a polynomial over $\mathbf{R}$, and for every $x, y \in \mathbf{R}$, $P(x+y) = P(x) + P(y)$.

(a) Prove that for every positive integer n, $P(n) = n \cdot P(1)$.

(b) Prove that P has degree at most 1.

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.]