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 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: ____

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 $x^{p-1} \equiv 1 \pmod{p}$.

Solution: False: for example, take $p = 4$ and $x = 3$.

T F One way to prove a statement of the form $P \implies Q$ is to assume $\neg Q$ and prove $\neg P$.

Solution: True. This is proof by contrapositive.

T F $\forall x \exists y P(x,y) \equiv \exists x \forall y P(y,x)$.

Solution: False. For example, if the domain is $\mathbf{R}$ and $P(x,y)$ is $x < y$, then $\forall x \exists y P(x,y)$ is true but $\exists x \forall y P(y,x)$ is false.

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

Solution: True. This can be seen with a truth table, or by

$$\begin{aligned} P \Rightarrow (Q \Rightarrow R) &\equiv \neg P \vee (\neg Q \vee R) \\ &\equiv (\neg P \vee \neg Q) \vee R \\ &\equiv \neg (P \wedge Q) \vee R \\ &\equiv (P \wedge Q) \Rightarrow R. \end{aligned}$$

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

Solution: False. For example, if P and R are true and Q is false, then $P \Rightarrow (Q \wedge R)$ is false but $(P \Rightarrow Q) \vee R$ is true.

T F To prove $(\forall n \in \mathbf{N})P(n)$, it is enough to prove $P(0)$, $P(2)$ and $(\forall n \geq 2)(P(n) \Rightarrow P(n+2))$.

Solution: False. For example, if $P(n)$ is "n is even", then $(\forall n \in \mathbf{N})P(n)$ is false, but $P(0)$, $P(2)$ and $(\forall n \geq 2)(P(n) \Rightarrow P(n+2))$ is true.

T F In a stable marriage instance, there can be two women with the same optimal man.

Solution: False. If we run the propose and reject algorithm with women proposing, then the resulting pairings will have every woman paired with her optimal man. A single man can not be paired with two women, so any two women must have different optimal men.

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.

Solution: False. For example, consider this instance:

Woman	Ranking			Man	Ranking		
A	1	2	3	1	B	C	A
B	2	3	1	2	A	C	B
C	2	3	1	3	A	C	B

Here, a stable matching is $(1,B),(2,A),(3,C)$.

PRINT your name and student ID: ______________________________

Short Answer

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

Solution: 3.

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

Solution:

$$\begin{aligned}\frac{200+14\cdot 102}{99} \equiv& \frac{0+4\cdot 2}{9} \\ \equiv& \frac{8}{-1} \\ \equiv& -8 \\ \equiv& 2 \pmod{10}\end{aligned}$$

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

Solution: Choose $x = 0$. Then for any $y \in \mathbf{R}$, $x \cdot y = 0 < 2$.

Common mistake:

- You must find a single value of x, since it starts with $\exists$. Providing different values of x for different values of y doesn't prove the proposition. For example, $x = 1/y$ depends on y, so that doesn't work.

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.

Solution: N can be easily factored into 7 and 11. So $(p-1)(q-1) = 60$. The decryption exponent is $43^{-1} \pmod{60}$, which we can find using the extended Euclidean algorithm:

$\gcd(60,43)$	$1 = 2\cdot 43 - 5\cdot(60-43) = -5\cdot 60 + \boxed{7}\cdot 43$
$= \gcd(43,17)$	$1 = -1\cdot 17 + 2\cdot(43 - 2\cdot 17) = 2\cdot 43 - 5\cdot 17$
$= \gcd(17,9)$	$1 = 1\cdot 9 - 1\cdot(17-9) = -1\cdot 17 + 2\cdot 9$
$= \gcd(9,8)$	$1 = 1\cdot 9 - 1\cdot 8$
$= \gcd(8,1)$	$1 = 0\cdot 8 + 1\cdot 1$

So $d \equiv 43^{-1} \equiv 7 \pmod{60}$. $x \equiv E(x)^d \equiv 2^7 \equiv 128 \equiv 51 \pmod{77}$.

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 $n > 2$.)

Solution: Proof by induction.

Base case: $F_1 = 1$ and $F_2 = 1$, so clearly $\gcd(F_1, F_2) = 1$.

Induction hypothesis: Suppose $\gcd(f_{n-1}, f_n) = 1$.

Induction step: We want to show $\gcd(F_n, F_{n+1}) = 1$.

We'll use the fact from Euclid's algorithm that $\gcd(a, a+b) = \gcd(a, b)$. This fact is true because any d that divides both a and b, ($a = kd$, $b = \ell d$) must also divide $a+b$ (because $a+b = (k+\ell)d$), and any d that divides both a and $a+b$ ($a = xd$, $a+b = yd$) must also divide b (because $b = (y-x)d$).

Using this fact, $\gcd(F_n, F_{n+1}) = \gcd(F_n, F_n + F_{n-1}) = \gcd(F_n, F_{n-1}) = 1$; the last equality is the induction hypothesis. ■

Common mistakes:

- Giving a base case that is not $\gcd(1, 1)$. If you do this, you haven't proved for $n \geq 1$.
- Giving an induction hypothesis like "for all $n > 1$, $P(n)$". Notice this is what you're trying to show!

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.)

Solution:

(a) We solve using the method of Lagrange Interpolation:

$$\Delta_1(x) = \frac{(x-3)(x-4)}{(1-3)(1-4)} = \frac{(x-3)(x-4)}{6} = 2*(x-3)(x-4) = 2x^2 - 3x + 2$$

$$\Delta_3(x) = \frac{(x-1)(x-4)}{(3-1)(3-4)} = \frac{(x-1)(x-4)}{-2} = 5*(x-1)(x-4) = 5x^2 - 3x - 2$$

$$\Delta_4(x) = \frac{(x-1)(x-3)}{(4-1)(4-3)} = \frac{(x-1)(x-3)}{3} = 4*(x-1)(x-3) = 4x^2 + 6x + 1$$

$P(x) = 4*\Delta_1(x) + 1*\Delta_3(x) + 5*\Delta_4(x) = 4*(2x^2 - 3x + 2) + (5x^2 - 3x - 2) + 5*(4x^2 + 6x + 1) = 8x^2 + 5x^2 + 20x^2 - 12x - 3x + 30x + 8 - 2 + 5 = 33x^2 + 15x + 11 = 4x$

Thus, the original encoding polynomial is $P(x) = 4x$, and the missing point is $P(2) = 4*2 = 8$.

Common mistakes:

- Remember to check your work! Most points were lost just due to calculation mistakes. For error-correcting problems, checking your answer is easy, because you can just plug in the points that you received into the polynomial that you calculated.
- Also remember that you can simplify numbers based on the modulus in the middle of a calculation. Simplifying the delta polynomials modulo 11, for example, would probably help make calculating the original polynomial easier, and decrease the chance of calculation errors.

(b) The integers modulo 10 do not form a field, so there is no guarantee that Alice would be able to find a polynomial $P(x)$ that passes through her three points.

Alternate answer: Since the integers module 10 do not form a field, we have to guarantee that only one polynomial goes through the points Bob receives. So Bob may find more than one possible message.

Common mistakes for (b):

- Some people thought all computations were done modulo 11, but while sending or decoding the message a modulo of 10 was used instead.
- Some people said using 10 instead of 11 would cause the message to be "insecure". Note that error correcting codes don't try to address security.

PRINT your name and student ID: ________________________________

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.

Solution:

(a) Proof by induction on n. Base case: $n = 1$: $P(1) = 1 \cdot P(1)$. Induction step: If $P(n) = n \cdot P(1)$, then $P(n+1) = P(n) + P(1) = nP(1) + P(1) = (n+1)P(1)$.

Common mistakes:

- Giving an induction hypothesis like "for all $n > 1$, $P(n)$". Notice this is what you're trying to show!

(b) Define the polynomial $Q(x)$ by $Q(x) = P(1)x$. We will show that $P(x)$ and $Q(x)$ are the same polynomial. Let d be the degree of $P(x)$. By part (a), there are at least d+1 points where $P(x) = Q(x)$. So $P(x)$ and $Q(x)$ are the same polynomial.

Note: this was the most difficult question on the midterm. Only seven people got full credit, and six others got partial credit.

Common mistakes:

- Many people said that because $xP(1)$ is a linear polynomial, $P(x)$ must be linear, but did not explain why the polynomial $P(x)$ is equal to the polynomial $xP(1)$. (Part (a) only shows that it's equal when x is a positive integer.)
- Many people argued that if $P(x)$ had degree $d > 1$, say $P(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$, then since

$$P(x+y) = a_d(x+y)^d + a_{d-1}(x+y)^{d-1} + \cdots + a_1(x+y) + a_0$$

and

$$P(x+y) = P(x) + P(y) = a_d(x^d + y^d) + a_{d-1}(x^{d-1} + y^{d-1}) + \cdots + a_1(x+y) + 2a_0$$

it must follow that $(x+y)^d = x^d + y^d$, $(x+y)^{d-1} = x^{d-1} + y^{d-1}$, etc. However, it's not clear why that would have to be true: in general, it's possible to have $a + b + c = a' + b' + c'$ without it being true that $a = a'$, $b = b'$ and $c = c'$.

- Some people argued that if $P(x)$ had degree at least two, then it would have at least two roots, and reached a contradiction based on that. However, it is possible for a polynomial of any degree to have zero roots: consider $x^d + 1$. The property from class only says that a degree-d polynomial must have *at most* degree roots. (If we allow complex numbers, then it is true that every degree-d polynomial has d roots, if we count "repeated roots" multiple times; however, since we were only given that $P(x+y) = P(x) + p(y)$ when x, y are real numbers, that line of reasoning doesn't seem fruitful either.)

[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.]