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

Solution: False. This is not a valid proof method. For example, it would allow us to prove $0 = 1$, as follows:
Proof. Assume $0 = 1$. Clearly it is true that $\neg(0 = 1)$. ■
We should not be able to prove $0 = 1$, so this is not a valid proof method.

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

Solution: True. Proof: Let $Q(n)$ be the proposition "$P(-n)$ is true". Then we are given that $Q(1)$ and that $(\forall m \in \mathbf{Z})(Q(m-1) \Rightarrow Q(m))$ (substituting $-m$ for n in $P(n+1) \Rightarrow P(n)$). So by induction, $Q(n)$ is true for every positive integer n, which is what we wanted to prove. ■

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

Solution: False. For example, if P and Q are false but R is true, then the left-hand side is true but the right-hand side is false.

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

Solution: True. This can be verified with a truth table, or the following reasoning using the simpler logical equivalences $A \Rightarrow B \equiv \neg A \vee B$, $A \Rightarrow B \equiv \neg B \Rightarrow \neg A$, $\neg(A \vee B \equiv) \equiv \neg A \wedge \neg B$ and $\neg\neg A \equiv A$:

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

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

Solution: False. Indeed, we can prove $\neg((\exists x \in \mathbf{R})(\forall y \in \mathbf{R})(x > 0 \wedge x^2 \leq y))$, which is logically equivalent (using De Morgan's laws) to $(\forall x \in \mathbf{R})(\exists y \in \mathbf{R})(\neg(x > 0 \wedge x^2 \leq y))$.
Proof. Let $x \in \mathbf{R}$ be any number. Case 1: $x \leq 0$. In this case, take $y = 0$ (or any real number, for that matter), and it will be the case that $\neg(x > 0 \wedge x^2 \leq y)$. Case 2: $x > 0$. Then take $y = x^2/2$, and again, it will be the case that $\neg(x > 0 \wedge x^2 \leq y)$. ■

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

Solution: True. Every number coprime to q has an inverse mod q, and distinct prime numbers are always coprime.

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 $P(y) = 0$.

Solution: False. For example, consider $P(x) = x^5$. There is only one root, $x = 0$.

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.

Solution: False. For example, consider two men and two women with the following preferences:

Woman	Prefs		Man	Prefs	
A	1	2	1	A	B
B	2	1	2	B	A

Then 1 is optimal for A and A is optimal for 1.

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

Solution: Let's run the propose and reject algorithm.

- Day 1: 1 proposes to A, 2 proposes to B, 3 and 4 propose to C.
- Night 1: C rejects 3.
- Day 2: 3 proposes to A.
- Night 2: A rejects 3.
- Day 3: 3 proposes to B.
- Night 3: B rejects 2.
- Day 4: 2 proposes to D

Now each woman has a proposal from a different man, so we have a stable matching: (A, 1), (B, 3), (C, 4), (D, 2).

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

Solution: Using Fermat's Little Theorem, $2^6 \equiv 3^6 \equiv 1 \pmod 7$, so $2^{63} \equiv 2^3 \equiv 1 \pmod 7$ and $3^{14} \equiv 3^2 \equiv 2 \pmod 7$.

So $2^{63} + 3^{14} \equiv 3 \pmod 7$.

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 $0, 1, \ldots, 18$. 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?

Solution: The error correcting code for general errors requires sending $n+2k$ pieces, where $n = 5$ is the length of the original message and $k = 3$ is the maximum number of errors. So Alice must send 11 pieces.

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

Solution: Recall that $x^{(p-1)(q-1)} \equiv 1 \pmod{pq}$ if p and q are prime and x is coprime to pq. Since $pq = 55$, we deduce that $p = 5$ and $q = 11$, so $(p-1)(q-1) = 40$. So for any k, $6^{40k} \equiv 1 \pmod{55}$. So $6^{122} \equiv 6^{120} \cdot 6^2 \equiv 1 \cdot 36 \equiv 36 \pmod{55}$.

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

Solution: Given any $x \in \mathbf{N}$, take $y = x+1$. Then x and y cannot have any common divisors greater than 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 $a = 3, b = 4, c = 5$.

Solution: Proof by strong induction.

Induction hypothesis: let n be a positive integer and assume that for every $0 < k < n$, there is a solution to $a^2 + b^2 = c^k$.

If $n = 1$, set $a = 1$, $b = 1$, $c = 2$. If $n = 2$, set $a = 3$, $b = 4$, $c = 5$ as suggested. In both cases, you can verify that $a^2 + b^2 = c^n$.

The last case is that $n > 2$. Then find any solution a', b', c to the equation $(a')^2 + (b')^2 = c^{n-2}$. Then set $a = ca'$ and $b = ca'$. Then $a^2 + b^2 = c^2((a')^2 + (b')^2) = c^2(c^{n-2}) = c^n$. ■

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

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

Solution: The second equation implies

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

Substituting into the first equation, we have

$$12x \equiv -x + 4 \pmod{43}$$

so

$$13x \equiv 4 \pmod{43}$$

so

$$x \equiv 13^{-1} \cdot 4 \pmod{43}.$$

We'll use the extended Euclidean algorithm to find $13^{-1} \pmod{43}$:

$$\begin{array}{ll} \gcd(43,13) & 1 = 1 \cdot 13 - 3 \cdot (43 - 3 * 13) = -3 \cdot 43 + \boxed{10} \cdot 13 \\ = \gcd(13,4) & 1 = 0 \cdot 4 + 1 \cdot (13 - 3 \cdot 4) = 1 \cdot 13 - 3 \cdot 4 \\ = \gcd(4,1) & 1 = 0 \cdot 4 + 1 \cdot 1 \\ = 1 & \end{array}$$

So $13^{-1} \equiv 10 \pmod{43}$. Continuing,

$$x \equiv 10 \cdot 4 \equiv 40 \pmod{43}$$

and substituting back for y, we have

$$y \equiv -x + 1 \equiv -39 \equiv 4 \pmod{43}.$$

Indeed, we can check that $x = 40, y = 4$ satisfies the two equations.

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.

Solution: According to the secret-sharing protocol from class, $P(x)$ should have degree 2 in order for any three people to be able to discover the secret. We'll use Lagrange interpolation to find $P(x)$.

$$\Delta_1(x) \equiv \frac{(x-2)(x-8)}{(1-2)(1-8)} \equiv \frac{x^2-10x+3}{7} \equiv 2(x^2-10x+3) \equiv 2x^2+6x+6$$

$$\Delta_2(x) \equiv \frac{(x-1)(x-8)}{(2-1)(2-8)} \equiv \frac{x^2-9x+8}{-6} \equiv 2(x^2-9x+8) \equiv 2x^2+8x+3$$

$$\Delta_3(x) \equiv \frac{(x-1)(x-2)}{(8-1)(8-2)} \equiv \frac{x^2-3x+2}{42} \equiv 9(x^2-3x+2) \equiv 9x^2+12x+5$$

Noting that $7^{-1} \equiv 2 \pmod{13}$, $(-6)^{-1} \equiv 7^{-1} \equiv 2 \pmod{13}$ and $42^{-1} \equiv 3^{-1} \equiv 9 \pmod{13}$.

We construct our polynomial: $P(x) = 2\Delta_1(x) + \Delta_2(x) + \Delta_3(x) \equiv 2x^2+6x+7 \pmod{13}$. The secret then is $P(0) \equiv 7 \pmod{13}$. (Note that we could have saved some work by only computing the constant terms.)

PRINT your name and student ID: ______________________________

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 $P(x)^2 - P(x) + 1 \equiv 0 \pmod{p}$.

Solution: Suppose for a contradiction that there are at least $2d+1$ distinct values of x such that $P(x)^2 - P(x) + 1 \equiv 0 \pmod{p}$.

Then for each of those x-values, we have $P(x)^2 + 1 \equiv P(x) \pmod{p}$. So $P(x)$ and $P(x)^2 + 1$ are two polynomials of degree at most $2d$ that match at $2d+1$ points: so they are the same polynomial. But this is impossible, since they have different degrees. ■

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.]