CS 70 Discrete Mathematics and Probability Theory
Fall 2013 Midterm #1 Solutions

1. **(30 points) Multiple choice/Numerical Answer. No justification necessary**

   (a) Suppose you proved the inductive step for a statement $P(n)$ but then discovered that $P(29)$ is false. What can you say about $P(1)$?

   Necessarily true [✓ **Necessarily false**] **Cannot say**

   Explanation: Suppose $P(1)$ is true. That provides the base case of the induction, and together with the inductive step this implies that $P(n)$ is true for all n, including for $n = 29$. But this is a contradiction, as $P(29)$ is false, so $P(1)$ must be false.

   (b) Suppose you proved the inductive step for a statement $P(n)$ but then discovered that $P(29)$ is false. What can you say about $P(50)$?

   Necessarily true **Necessarily false** [✓ **Cannot say**]

   Explanation: Since $P(29)$ is false, and there is no base case to start the induction. So $P(50)$ is not necessarily true. But there is nothing preventing $P(50)$ from being true, so it could either be true or false.

   (c) The polynomial $x^2 - 1 \bmod 15$ has at most 2 zeros.

   True [✓ **False**]

   Explanation: The zeros are $\pm 1, \pm 4$.

   (d) The polynomial $x^2 - 1 \bmod 31$ has at most 2 zeros.

   [✓ **True**] **False**

   Explanation: 31 is prime and a polynomial of degree d modulo a prime has at most d zeros.

   (e) $\gcd(a,b) = \gcd(a, b+25a)$.

   [✓ **True**] **False**

   Explanation: A key idea in the proof of Euclid's algorithm was to show that $gcd(a,b) = gcd(a, b+ka)$ for arbitrary integer k.

   (f) $\gcd(a,b) = \gcd(2a, b+2a)$.

   True [✓ **False**]

   Explanation: For example, $a = 1$ and $b = 2$.

   (g) What is the multiplicative inverse of 7 mod 13?

   2

   Explanation: By inspection, since $2 \times 7 = 13 + 1$.

   (h) 15 has a multiplicative inverse $\bmod 78$.

   True [✓ **False**]

   Explanation: $\gcd(15, 78) = 3 \neq 1$, so 15 has no multiplicative inverse $\bmod 78$.

   (i) What is $5^{547} \bmod 15$?

   5

   Explanation: Use RSA property for $N = 15 = 3 \times 5$. We know that $x^{k(3-1)(5-1)+1} = x \bmod 15$ for arbitrary integer k. So can reduce the exponent modulo $(3-1)(5-1) = 8$ to get $547 \bmod 8 = 3$. So $5^{547} = 5^3 = 5$.

(j) Circle all that apply. The function $f(x) = x^3 \bmod 21$ is:

One-to-one **Onto** **Bijection** [✓ **None of the previous**]

Explanation: $f(1) \equiv f(4) \equiv 1 \bmod 21$, so the function is not one-to-one, and hence also not a bijection. Since the size of the domain and range are finite and equal, it is thus not onto either. Note that the RSA property does not apply since $gcd(3,(3-1)(7-1)) \neq 1$.

(k) The inverse of the function $f(x) = 5x \bmod 21$ is $g(x) = 17x \bmod 21$.

[✓ **True**] **False**

Explanation: $f(g(x)) \equiv 5(17x) \equiv x \bmod 21$. $(5 \cdot 17 \equiv 1 \bmod 21)$

2. **(15 points) Stable Marriage.** Suppose that after running a stable marriage algorithm with n men and n women, the pairing that results includes the couple (1, A). Suppose that after a few days 1 changes his mind, and decides that he does not like woman A as much as he thought he did (i.e. he moves her down on his preference list). What is the maximum number of rogue couples that result in the existing pairing from such a change to 1's preference list? Give a one or two sentence justification for why the number of rogue couples can be as large as you claim. Also give a one or two sentence justification for why the remaining couples cannot be rogue couples.

Answer: There can be $n-1$ rogue couples; this happens when all of the women prefer 1 to all the other men, and 1 at first preferred A to all other women but now puts her as his least preferred. This situation makes $(1,X)$ a rogue couple for all $X \neq A$. (i.e. one rogue couple for every woman who is not A).

Moreover, there cannot be more than $n-1$ rogue couples. To see this, notice that whether or not (i, X) is a rogue couple can be determined just by looking at the preference lists of i and X (and the names of their partners). Since 1 is the only person whose preference list changes, he must be part of any rogue couple, and so there can be at most $n-1$ rogue couples (since (1, A) clearly is not a rogue couple).

So $n-1$ is the maximum number of rogue couples.

3. **(15 points) Well-Ordering Principle.** Suppose I start with a necklace with three beads: one red, one green, and one blue. Each day I cut the necklace at an arbitrary point and then lay it out in a line. I look at the beads on the two ends of the necklace. If the end beads are the same color, I throw away my necklace. If the end beads are different colors, then I add a new bead of the third color to one end (for example, if one bead was red and one bead was green, I add a blue bead) and retie the necklace.

   Use the well-ordering principle to prove that I never have to throw away my necklace (i.e. prove that regardless of my choices, there is no day where I end up throwing my necklace).

   Answer: We argue that the necklace never has two beads of the same color adjacent to each other. This proves the claim because if I had to throw away the necklace, it was because I cut it between two adjacent beads of the same color.

   Applying the WOP, suppose the claim is false, and let n be the first day on which the necklace could end up with two adjacent same-colored beads. Since we start with 3 distinct beads, $n > 0$, and on day $n-1$ the necklace did not have adjacent same-colored beads. So when we cut it the two endpoints had distinct colors, and according to the rules we added a new bead of a third color. Since none of the previously adjacent pairs of beads had the same color, and since the newly added bead has a different color than its two neighbors, it follows that on day n the necklace did not have two adjacent same-colored beads. Contradiction. Therefore I never had to throw away the necklace.

4. **(15 points) Polynomials.** You are doing Lagrange Interpolation to find a polynomial $P(x)$ of degree 10, using the data $(1,P(1)),(2,P(2)),\ldots,(11,P(11))$. You discover that $P(x)=\sum_{i=1}^{11}\Delta_i(x)$. What is $P(20)$? Justify your answer. Ideally your justification of your answer will be at most 3-4 sentences.

   Hint: Recall that $\Delta_i(x)$ is a polynomial of degree 10 such that $\Delta_i(i)=1$ and $\Delta_i(j)=0$ for all other j in $\{1,\ldots,11\}$. If you are having trouble getting started, you might try plotting one of the polynomials $\Delta_i(x)$, say $\Delta_4(x)$, at these values of x.

   Answer: Since we know $P(x)=\sum_{i=1}^{11}\Delta_i(x)$, for every integer $j : 1 \leq j \leq 11$, $P(j)=\sum_{i=1}^{11}\Delta_i(j)=\Delta_j(j)+0=1$. We know there is a unique degree 10 polynomial that goes through these 11 points. But the polynomial $Q(x)=1$ (or $0x^{10}+\cdots+0x+1$) has the property that it goes through all these points. By uniqueness $P(x)=Q(x)$ and therefore $P(20)=1$.

5. **(1 point) Bonus Problem.** Prove that $\sqrt{2\sqrt{3\sqrt{4\cdots\sqrt{n}}}} < 3$.

   (*Hint:* what can you say about the quantity $\sqrt{k\sqrt{(k+1)\cdots\sqrt{n}}}$?).

   Bigger Hint: Strengthen the induction hypothesis to show that $\sqrt{k\sqrt{(k+1)\cdots\sqrt{n}}} < k+1$.