CS 70 Discrete Mathematics and Probability Theory
Fall 2012 Vazirani Midterm 1

PRINT your name: _____, _____
(last) (first)

PRINT your GSI name and discussion section: _____

Name of the person sitting to your left: _____

Name of the person sitting to your right: _____

You may consult one single-sided sheet of notes. Calculators are not permitted, and cellphones must be turned off and put away. Do all your work on the pages of this examination. Give reasons for all your answers. Good Luck!

Do not turn this page until your instructor tells you to do so.

Problem 1	
Problem 2	
Problem 3	
Total	

Problem 1. [True or false] (20 points)

Circle TRUE or FALSE. Do not justify your answers on this problem.

(a) **True** or FALSE: $(P \Rightarrow Q) \Rightarrow (\neg Q \Rightarrow \neg P)$

–Observation–

Definition of contraposition.

(b) **True** or FALSE: $(P \wedge Q) \Rightarrow (P \Rightarrow Q)$

–Observation–

P and Q both True, $P \Rightarrow Q$ must be True.

(c) **True** or FALSE: $(P \Rightarrow (P \wedge Q)) \Rightarrow (P \Rightarrow Q)$

–Observation–

Proof by contraposition. If RHS False, $P \wedge \neg Q$. This implies LHS, $P \Rightarrow (P \wedge Q)$ is False. Therefore, True.

(d) **True** or FALSE: $\neg(\forall x \in \mathbf{N} \ \ \exists y \in \mathbf{N} \ \ P(x,y)) \ \Rightarrow \ (\exists x \in \mathbf{N} \ \ \forall y \in \mathbf{N} \ \ \neg P(x,y))$

–Observation–

Proper negation of quantifiers.

(e) **True** or FALSE: $\forall x \in \mathbf{N} \ \ \exists y \in \mathbf{N} \ \ \forall z \in \mathbf{N} \ \ x - y \leq z$

–Observation–

Set $y = x$. Then, $\forall z \in \mathbf{N}$, $0 \leq z$. True because $\mathbf{N}$ has minimal element, and that is 0.

(f) TRUE or **False**: $\forall x \in \mathbf{Z} \ \ \exists y \in \mathbf{Z} \ \ \forall z \in \mathbf{Z} \ \ x - y \leq z$

–Observation–

There is no minimal element in the integers, this expression cannot be satisfied.

(g) **True** or FALSE: $\forall x, y \in \mathbf{N} \ \ gcd(2x, 2y) = 2gcd(x, y)$

–Observation–

d divides x, y. $2d$ divides $2x, 2y$.

(h) TRUE or **False**: $\forall x, y \in \mathbf{N}$ $gcd(2x, 4y) = 2gcd(x, y)$

–Observation–

Let $x = 2$, $y = 1$. $2gcd(x, y) = 2$. $gcd(2x, 4y) = gcd(4, 4) = 4$.

(i) TRUE or **False**: For all $x, y \in \mathbf{N}$, if $6x \equiv y \pmod{11}$, then $x \equiv 6y \pmod{11}$.

–Observation–

$6^{-1} \not\equiv 6 \pmod{11}$. Let $x = 1$, $y = 6$. $6x \equiv y \pmod{11}$, but $6y \equiv 3 \pmod{11}$ so $x \not\equiv 6y \pmod{11}$.

(j) TRUE or **False**: In every stable pairing that is pessimal for a woman, that woman is matched to her least favorite man.

–Observation–

Many women may list the same man as their least favorite.

2. Modular Arithmetic (40 points)

(a) Let p be prime. Simplify $1^p + 2^p + \cdots + p^p \pmod{p}$.

–Solution–

Let $f(p) = 1^p + 2^p + \cdots + p^p \mod p$. Consider $p = 2$. $1^2 \mod 2 = 1$.
Consider $p > 2$; p must be odd. Note that $p^p \equiv 0 \mod p$.
$f(p) = \sum_{i=1}^{p-1} i^p = \sum_{i=1}^{(p-1)/2} i^p + \sum_{i=(p-1)/2+1}^{p-1} i^p$. On the second sum, we perform a change of variable, and let $k = p - i$. The bounds of the summation are therefore from $p - (p-1) = 1$ to $p - ((p-1)/2 + 1) = (p-1)/2$. Note that $p - k \equiv -k \mod p$. Therefore,

$$f(p) = \sum_{i=1}^{(p-1)/2} i^p + \sum_{k=1}^{(p-1)/2} (p-k)^p \equiv \sum_{i=1}^{(p-1)/2} i^p + \sum_{k=1}^{(p-1)/2} (-k)^p \mod p$$

Combining the summations, we have

$$f(p) = \sum_{i=1}^{(p-1)/2} (i-i)^p \equiv 0 \mod p$$

Therefore, if $p = 2$, $f(p) \equiv 1 \mod p$, and otherwise, $f(p) \equiv 0 \mod p$.

(b) Compute $8^{-1} (\mathrm{mod} 21)$ using Euclid's extended GCD algorithm. Show your steps.

–Solution–

$$\begin{aligned}
21 &= 2(8) + 5 && (1)\\
8 &= 5 + 3 && (2)\\
5 &= 3 + 2 && (3)\\
3 &= 2 + 1 && (4)\\
3 - 1 &= 2 && (5)\\
5 &= 3 + (3-1) = 2(3) - 1 && (6)\\
5 + 1 &= 2(3) && (7)\\
2(8) &= 2(5) + 2(3) && (8)\\
2(8) &= 2(5) + 5 + 1 = 3(5) + 1 && (9)\\
2(8) - 1 &= 3(5) && (10)\\
3(21) &= 6(8) + 3(5) && (11)\\
3(21) &= 6(8) + 2(8) - 1 && (12)\\
1 &= 8(8) - 3(21) && (13)
\end{aligned}$$

Therefore, $8^{-1} \mod 21 = 8$.

(c) Bijections & RSA: For each of the following functions f on the numbers modulo 35 (i.e. $f : S \to S$, where $S = \{0, 1, \ldots, 34\}$) indicate whether f is a bijection or not by circling the appropriate choice.

- **Bijection**, Not a Bijection: $f(x) = 3x \pmod{35}$

  –Observation–

  3 has an inverse mod 35 (coprime).

- Bijection, **Not a Bijection**: $f(x) = 5x \pmod{35}$

  –Observation–

  5 and 35 not coprime. $f(7) = 0$, $f(0) = 0$, not injective.

- **Bijection**, Not a Bijection: $f(x) = x - 6 \pmod{35}$

  –Observation–

  Add 6 to invert $f(x)$.

- **Bijection**, Not a Bijection: $f(x) = x/8 \pmod{35}$

  –Observation–

  8 inverse exists, multiply by 8 to invert $f(x)$.

- **Bijection**, Not a Bijection: $f(x) = x^{25} \pmod{35}$

  –Observation–

  $35 = 7 \times 5$. $p = 7$, $q = 5$. $(p-1)(q-1) = 24$. $x^{24} \mod 35 = 1$ by extension to FLT. $x(x^{24}) \mod 35 = x$.

- **Bijection**, Not a Bijection: $f(x) = x^5 \pmod{35}$

  –Observation–

  $x^{25} = (x^5)^5 \mod 35$ is a bijection. If $x^5 \mod 35$ were not a bijection, x^{25} couldn't possibly be a bijection.

- Bijection, **Not a Bijection**: $f(x) = x^2 \pmod{35}$

  –Observation–

  Consider $x = 34 \equiv -1 \mod 35$. $x^2 \equiv 1 \mod 35$, not injective.

- Bijection, **Not a Bijection**: $f(x) = x^{10} \pmod{35}$

  –Observation–

  x^2 not a bijection, so $(x^2)^5$ is not a bijection.

3. Proofs (30 points)

(a) Grade these attempts at executing the stated proof strategies Pass or Fail, with one or two lines of justification:

- You wish to prove by contradiction that $x < y$ implies $x^2 < y^2$.
  So you start by assuming for contradiction that $x \geq y$ and $x^2 \geq y^2$.

–Solution–

Fail: A proof by contradiction should begin by assuming $x < y$ and $x^2 \geq y^2$. When trying to prove a proposition P, we assume $\neg P$ and look for a contradiction. $\neg(P \Rightarrow Q) = \neg Q \wedge P$.

- You wish to prove by contradiction that $x < y$ implies $x^2 < y^2$.
  So you start by assuming for contradiction that $x \geq y$ and $x^2 < y^2$.

–Solution–

Fail: A proof by contradiction should begin by assuming $x < y$ and $x^2 \geq y^2$.

- You wish to prove by contraposition that $\exists x\ P(x) \Rightarrow \forall x\ Q(x)$.
  So you start by assuming $\exists x\ \neg Q(x)$.

–Solution–

Pass: A proof by contraposition of $P \Rightarrow Q$ assumes $\neg Q$ and attempts a direct proof of $\neg P$.

- You wish to prove by contraposition that $\exists x\ P(x) \Rightarrow \forall x\ Q(x)$.
  So you start by assuming $\forall x\ Q(x)$.

–Solution–

Fail: We should assume $\neg\ (\forall x\ Q(x)) \equiv \exists x\ \neg Q(x)$, as in previous part.

(b) You wish to break a standard $m \times n$ Hershey chocolate bar into mn little squares to distribute to mn kids. In each step you can pick up exactly one piece of chocolate and break it along one of the horizontal or vertical lines etched into the bar. No stacking! Prove by induction that the minimum number of steps required to completely break the bar into mn little squares is $mn - 1$.

Proof by induction on:

–Solution–

$r = mn$. Induction on the number of pieces in the bar.

Base Case:

–Solution–

The minimum number of breaks required is $g(r)$. $r = 1$. $m = 1$, $n = 1$. No breaks are necessary, and we observe that $g(r) = r - 1 = 0$.

Induction Hypothesis:

–Solution–

Assume that $\forall s \leq k \; g(s) = s - 1$. We will apply strong induction.

Induction Step:

–Solution–

Consider $r = k + 1$. Since we have one big piece and $k + 1$ pieces to distribute, we need to begin by making 1 break. This results in two bars, one with $u < k + 1$ and another with $v < k+1$ pieces, where $u+v = k+1$. Applying the inductive hypothesis, it takes a minimum of $g(v) = v-1$ breaks on the bar of size v, and it takes $g(u) = u-1$ breaks on the bar of size u. The total minimum number of breaks is then $g(k+1) = 1+(v-1)+(u-1) = (u+v)-1 = (k+1)-1$. Therefore, for any bar of size mn, it takes a minimum of $mn - 1$ breaks.