CS 173, Spring 2012
Midterm 1 Solutions

There were two versions of each exam question. Look for "Bush" or "Obama" in the exam's netID box.

Problem 1: Multiple choice Bush (5 points)

Check the most appropriate box for each statement. Check only one box per statement. If you change your answer, make sure it's easy to tell which box is your final selection.

(a) $\emptyset \in A$

true for any set A □

false for any set A □

true for some sets A ☑

(b) $-2 \equiv 8 \pmod 5$

True ☑ **False** □

(c) cardinality of $\{(p,q) \in \mathbb{N}^2 \mid p+q=2\}$

1 □ 2 □ 3 ☑

6 □ infinite □

(d) $\displaystyle\sum_{i=1}^{k+1} i =$

$\frac{k(k+1)}{2}$ □ $\frac{k(k-1)}{2}$ □

$\frac{(k+2)(k+1)}{2}$ ☑ $k!$ □

(e) $\exists y \in \mathbb{Z}, \forall x \in \mathbb{Z}, y \leq x$

True □ **False** ☑

Problem 1: Multiple choice Obama (5 points)

Check the most appropriate box for each statement. Check only one box per statement. If you change your answer, make sure it's easy to tell which box is your final selection.

(a) $\forall x \in \mathbb{Z}, \exists y \in \mathbb{Z}, y \leq x$

True ☑ **False** □

(b) cardinality of $\{p + q \in \mathbb{N} \mid p \leq 2 \text{ and } q \leq 2\}$

3 □ 4 □ 5 ☑

9 □ infinite □

(c) $\lfloor \lceil x \rceil \rfloor = \lceil \lfloor x \rfloor \rceil$

true for any x in $\mathbb{R}$ □

false for any x in $\mathbb{R}$ □

true for some x in $\mathbb{R}$ ☑

(d) $\sum_{i=1}^{p-1} i =$

$\frac{p(p+1)}{2}$ □ $\frac{p(p-1)}{2}$ ☑

$\frac{(p-1)^2}{2}$ □ $\frac{(p-1)(p+1)}{2}$ □

(e) $\emptyset \subseteq A$

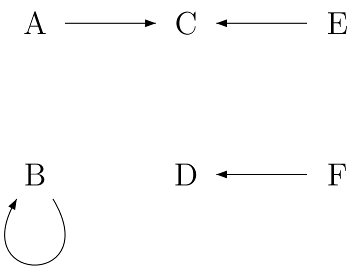
true for any set A ☑

false for any set A □

true for some sets A □

Problem 2: Short answer Bush (10 points)

(a) (5 points) Check all boxes that correctly characterize this relation on the set $\{A, B, C, D, E, F\}$



Reflexive: □ **Irreflexive**: □

Symmetric: □ **Antisymmetric**: ☑

Transitive: ☑

(b) (3 points) Using precise mathematical words and notation, define what it means for a function $f : A \to B$ to be "onto" (also called "surjective").

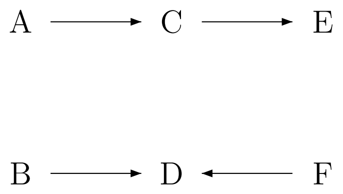
Solution: For any $y \in B$, there is an $x \in A$ such that $f(x) = y$.

(c) (2 points) How does a linear order differ from a partial order?

Solution: In a linear order, every pair of elements is comparable. Or: In a linear order, if x and y are two elements, then either $x = y$ or $x \preceq y$ or $y \preceq x$.

Problem 2: Short answer Obama (10 points)

(a) (5 points) Check all boxes that correctly characterize this relation on the set $\{A, B, C, D, E, F\}$



Reflexive: □ **Irreflexive**: ☑

Symmetric: □ **Antisymmetric**: ☑

Transitive: □

(b) (3 points) Using precise mathematical words and notation, define what it means for a function $f : A \to B$ to be "one-to-one" (also called "injective"). Avoid words such as "unique" which are difficult to use in a fully-precise way.

Solution: For any $x, y \in A$, if $f(x) = f(y)$ then $x = y$. Or: for any $x, y \in A$, if $x \neq y$ then $f(x) \neq f(y)$.

(c) (2 points) What are the three properties that define an equivalence relation?

Solution: Reflexive, symmetric, and transitive.

Problem 3: Sets and functions Bush (8 points)

$$\begin{aligned} A &= \{\text{Fred}, \text{George}, \text{Arthur}, \text{Molly}, \text{Ginny}\} \\ B &= \{\text{rat}, \text{owl}, \text{toad}\} \\ C &= \{\text{George}, (\text{Molly}, \text{Ron}), \text{Fred}\} \end{aligned}$$

(a) (3 points) List the elements of $B \times (A \cap C)$.

Solution: (rat,George), (owl,George), (toad,George), (rat,Fred), (owl,Fred), (toad,Fred)

(b) (2 points) How many one-to-one functions $B \to (A \times C)$ are there?

Solution: $15 \cdot 14 \cdot 13$

(c) (3 points) Give a set D which is a subset of A and give a function $h : D \to B$ which is onto, but is not one-to one.

Solution: Let $D = A$. And define h by

$$h(Fred) = h(George) = h(Arthur) = rat$$

$$h(Molly) = toad$$

$$h(Ginny) = owl$$

Problem 3: Sets and functions Obama (8 points)

$$\begin{aligned} A &= \{\text{Ford}, \text{Tesla}, \text{Mazda}\} \\ B &= \{\text{sedan}, \text{wagon}, \text{pickup}, \text{hatchback}, \text{minivan}\} \\ C &= \{\text{GM}, (\text{Mazda}, \text{Volvo}), \text{Ford}\} \end{aligned}$$

(a) (3 points) List the elements of $B \times (A \cap C)$.

Solution: (sedan,Ford), (wagon,Ford), (pickup,Ford), (hatchback,Ford), (minivan,Ford)

(b) (2 points) How many one-to-one functions $B \to (A \times C)$ are there?

Solution: $9 \cdot 8 \cdot 7 \cdot 6 \cdot 5$

(c) (3 points) Give a set D which is a subset of B and give a function $h : D \to A$ which is onto, but is not one-to one.

Solution: Let $D = B$. And define h by

$$h(sedan) = Ford$$

$$h(wagon) = Tesla$$

$$h(pickup) = h(hatchback) = h(minivan) = Mazda$$

Problem 4: Number Theory Bush (9 points)

(a) (3 points) In $\mathbb{Z}_{11}$, find the value of $([7])^{18}$. You must show your work, keeping all numbers in your calculations small. **You may not use a calculator.** You must express your final answer as $[n]$, where $0 \leq n \leq 10$.

Solution:

$[7]^4 = ([7]^2)^2 = [5]^2 = [25] = [3]$

$$\begin{aligned}
[7]^2 &= [49] = [5] \\
[7]^4 &= ([7]^2)^2 = [5]^2 = [25] = [3] \\
[7]^8 &= ([7]^4)^2 = [3]^2 = [9] \\
[7]^{16} &= ([7]^8)^2 = [9]^2 = [81] = [4] \\
[7]^{18} &= [7]^{16} \cdot [7]^2 = [4] \cdot [5] = [20] = [9]
\end{aligned}$$

Final answer is [9].

(b) (3 points) State the negation of the following claim, moving all negations (e.g. "not") so that they are on individual predicates.

Claim: For all positive integers a, b, and c, if $\gcd(a, b) > 1$ and $\gcd(b, c) > 1$, then $\gcd(a, c) > 1$.

Solution: There are positive integers a, b, and c such that $\gcd(a, b) > 1$ and $\gcd(b, c) > 1$, but $\gcd(a, c) = 1$.

Note: since the gcd is always positive, the negation of $\gcd(a, c) > 1$ can be either $\gcd(a, c) \leq 1$ or $\gcd(a, c) = 1$.

(c) (3 points) Disprove the claim from part (b) using a concrete counter-example. Briefly explain why your counter-example works.

Solution: Suppose that $a = 3$, $b = 6$, and $c = 2$. Then $\gcd(a, b) = 3 > 1$ and $\gcd(b, c) = 2 > 1$. But $\gcd(a, c) = 1$.

Problem 4: Number Theory Obama (9 points)

(a) (3 points) In $\mathbb{Z}_{13}$, find the value of $([7])^{18}$. You must show your work, keeping all numbers in your calculations small. **You may not use a calculator.** You must express your final answer as $[n]$, where $0 \leq n \leq 12$.

Solution:

$$\begin{aligned}
[7]^2 &= [49] = [10] \\
[7]^4 &= ([7]^2)^2 = [10]^2 = [100] = [9] \\
[7]^8 &= ([7]^4)^2 = [9]^2 = [81] = [3] \\
[7]^{16} &= ([7]^8)^2 = [3]^2 = [9] \\
[7]^{18} &= [7]^{16} \cdot [7]^2 = [9] \cdot [10] = [90] = [12]
\end{aligned}$$

Final answer is [12].

(b) (3 points) State the negation of the following claim, moving all negations (e.g. "not") so that they are on individual predicates.

Claim: For all positive integers a, b, and c, if $\gcd(a, bc) > 1$, then $\gcd(a, b) > 1$ and $\gcd(a, c) > 1$.

Solution: There exist positive integers a, b, and c such that $\gcd(a, bc) > 1$, but $\gcd(a, b) = 1$ or $\gcd(a, c) = 1$.

Note: since the gcd is always positive, the negation of $\gcd(a, c) > 1$ can be either $\gcd(a, c) \leq 1$ or $\gcd(a, c) = 1$.

(c) (3 points) Disprove the claim from part (b) using a concrete counter-example. Briefly explain why your counter-example works.

Solution: Suppose that $a = 3$, $b = 3$, and $c = 1$. Then $\gcd(a, bc) = 3 > 1$. But $\gcd(a, c) = 1$.

Problem 5: Relation proof Bush (9 points)

Let $P = \{(x, 2x+1) \mid x \in \mathbb{R}^+\}$. That is, P is the collection of all all 2D points of the form $(x, 2x+1)$ in the first quadrant.

Let T be a relation on P defined by $(a, b)T(p, q)$ if and only if $aq \geq pb$.

Prove that T is antisymmetric. You must work directly from the definitions of P and T, using basic rules of algebra. Use your best mathematical style: proof in logical order, variables introduced, and key steps justified.

Solution: Let $(x, 2x + 1)$ and $(s, 2s + 1)$ be elements of P. Suppose that $(x, 2x + 1)T(s, 2s + 1)$ and $(s, 2s + 1)T(x, 2x + 1)$

Since $(x, 2x+1)T(s, 2s+1)$, $x(2s+1) \geq s(2x+1)$ by the definition of T. Similarly, since $(s, 2s+1)T(x, 2x+1)$ $s(2x+1) \geq x(2s+1)$.

Since $x(2s+1) \geq s(2x+1)$ and $s(2x+1) \geq x(2s+1)$, $s(2x+1) = x(2s+1)$. That is, $2sx+s = 2sx+x$. So $s = x$.

Since $s = x$, $2s+1 = 2x+1$. So $(x, 2x+1) = (s, 2s+1)$ which is what we needed to show.

Problem 5: Relation proof Obama (9 points)

Let $M = \{(3y+1, y) \mid y \in \mathbb{R}^+\}$. That is, M is the collection of all all 2D points of the form $(3y+1, y)$ in the first quadrant.

Let P be a relation on M defined by $(a, b)P(p, q)$ if and only if $aq \geq pb$.

Prove that P is antisymmetric. You must work directly from the definitions of M and P, using basic rules of algebra. Use your best mathematical style: proof in logical order, variables introduced, and key steps justified.

Solution: Let $(3y+1, y)$ and $(3m+1, m)$ be elements of M. Suppose that $(3y+1, y)P(3m+1, m)$ and $(3m+1, m)P(3y+1, y)$.

Since $(3y+1, y)P(3m+1, m)$, $(3y+1)m \geq (3m+1)y$ by the definition of P. Similarly, since $(3m+1, m)P(3y+1, y)$, $(3m+1)y \geq (3y+1)m$.

Since $(3y+1)m \geq (3m+1)y$ and $(3m+1)y \geq (3y+1)m$, $(3m+1)y = (3y+1)m$. That is $3my+y = 3my+m$. So $y = m$.

Since $y = m$, $3y+1 = 3m+1$. So $(3y+1, y) = (3m+1, m)$, which is what we needed to show.

Problem 6: Number Theory Proof Bush (9 points)

For any integers s and t define $L(s, t) = \{sx + ty \mid x, y \in \mathbb{Z}\}$.
Thus, $L(s, t)$ consists of all integers that can be expressed as the sum of multiples of s and t.

Prove the following claim. Your proof must use the definition of divisibility; you may not use lemmas about manipulating divides relationships. You must prove the set inclusion by choosing an element from the smaller set and showing that it is also a member of the larger set.

Claim: For any integers a, r, m, where m is positive, if $a \equiv r \pmod{m}$, then $L(a, m) \subseteq L(r, m)$.

Solution: We show that if $a \equiv r \pmod{m}$ then $L(a,m) \subseteq L(r,m)$.

Let $a \equiv r \pmod{m}$, and suppose that $p \in L(a,m)$. We will show that $p \in L(r,m)$.

Since $a \equiv r \pmod{m}$, by definition of equivalence, we know that $m|a-r$, and by definition of divides, there must be an integer k such that $mk = a - r$, or equivalently, $a = r + mk$.

Since $p \in L(a,m)$, by definition of $L(a,m)$ there are integers x and y such that

$$p = ax + my.$$

Substituting $r + mk$ for a, we now know that

$$\begin{aligned} p &= (r+mk)x + my \\ &= rx + mkx + my \\ &= r(x) + m(kx+y) \end{aligned}$$

and since x and $kx+y$ are integers (the latter because k, x, and y are), we've shown that $p \in L(r,m)$.

Problem 6: Number Theory Proof Obama (9 points)

For any integers s and t define $L(s,t) = \{sx + ty \mid x, y \in \mathbb{Z}\}$.
Thus, $L(s,t)$ consists of all integers that can be expressed as the sum of multiples of s and t.

Prove the following claim. Your proof must use the definition of divisibility; you may not use lemmas about manipulating divides relationships. You must prove the set inclusion by choosing an element from the smaller set and showing that it is also a member of the larger set.

Claim: For any integers a, r, m, where r is positive, if $a \equiv m \pmod{r}$, then $L(a,m) \subseteq L(r,m)$.

Solution:

We show that if $a \equiv m \pmod{r}$ then $L(a,m) \subseteq L(r,m)$.

Let $a \equiv m \pmod{r}$, and suppose that $p \in L(a,m)$. We will show that $p \in L(r,m)$.

Since $a \equiv m \pmod{r}$, by definition of equivalence, we know that $r|a-m$, and by definition of divides, there must be an integer k such that $rk = a - m$, or equivalently, $a = m + rk$.

Since $p \in L(a,m)$, by definition of $L(a,m)$ there are integers x and y such that

$$p = ax + my.$$

Substituting $m + rk$ for a, we now know that

$$\begin{aligned} p &= (m + rk)x + my \\ &= rkx + mx + my \\ &= r(kx) + m(x + y) \end{aligned}$$

and since kx and $x + y$ are integers (because k, x, and y are), we've shown that $p \in L(r, m)$.