CS 173, Spring 2008
Midterm 1 Solutions

Problem 1: Short Answer (8 points)

(a) Suppose p, q, and r are propositional variables (i.e. they can be true or false). Using propositional logic, write a proposition that is true when p and q are true and r is false, but is false otherwise. You may use any or all of the logical operators $\vee, \wedge, \neg, \rightarrow$. Show that your proposition gives the desired results by writing out a truth table for it.

Solution:

$(p \wedge q) \wedge \neg r$

p	q	r	$p \wedge q$	$\neg r$	$(p \wedge q) \wedge \neg r$
T	T	T	T	F	F
T	F	T	F	F	F
F	T	T	F	F	F
F	F	T	F	F	F
T	T	F	T	T	T
T	F	F	F	T	F
F	T	F	F	T	F
F	F	F	F	T	F

(b) Use the Euclidean Algorithm to compute the GCD(111,201). Show every step the algorithm takes to compute the answer.

Solution:

a	b	r
111	201	
201	111	90
111	90	21
90	21	6
21	6	3

So the GCD is 3. (The first line swaps the two input values so the first one is larger, but we weren't picky about whether you showed this explicitly.)

Problem 2: Set theory (9 points)

List all the elements of the following sets. Recall that $\Re$ is the set of real numbers and that $\mathbb{P}(S)$ denotes the power set of a set S. Show your work.

(a) $\{x : x \epsilon \Re \wedge (3.5 \leq x < 10) \wedge (\lfloor x \rfloor = \lceil x \rceil)\}$

Solution: The condition that $\lfloor x \rfloor = \lceil x \rceil$ means that x must be an integer. So the set is $\{4, 5, 6, 7, 8, 9\}$. Notice that it does not contain 10 because x must be strictly less than 10.

(b) $\mathbb{P}(\{8\}) \times \{4, 5\}$

Solution: $\mathbb{P}(\{8\}) = \{\emptyset, \{8\}\}$. So $\mathbb{P}(\{8\}) \times \{4, 5\}$ is $\{(\emptyset, 4), (\emptyset, 5), (\{8\}, 4), (\{8\}, 5)\}$

(c) $\mathbb{P}(\{27\}) - \{27, 38\}$

Solution: $\mathbb{P}(\{27\}) = \{\emptyset, \{27\}\}$. Notice that neither 27 nor 38 is an element of this set, so the set subtraction does nothing. and our answer is $\{\emptyset, \{27\}\}$.

Problem 3: Set theory (9 points)

Suppose A is a non-empty set containing n elements and B is a non-empty set containing m elements. Remember that $\mathbb{P}(S)$ denotes the power set of a set S. Show your work.

(a) What is $|\mathbb{P}(A \times B)|$? **Solution:** $A \times B$ contains mn elements. So its powerset contains 2^{mn} elements.

(b) What is $|\mathbb{P}(A)||\mathbb{P}(B)|$? **Solution:** $|\mathbb{P}(A)|$ is 2^m and $|\mathbb{P}(B)|$ is 2^n. So the product is $2^m \times 2^n = 2^{m+n}$.

(c) Under what conditions is $|\mathbb{P}(A \times B)| = |\mathbb{P}(A)||\mathbb{P}(B)|$?

Solution: That is, when is $2^{mn} = 2^{m+n}$? This will be exactly when $mn = m + n$. This can only happen when $m = \frac{n}{n-1}$. Since m and n are supposed to be positive integers, this happens only when $n = m = 2$.

The problem specified that the two sets were non-empty, so m and n can't be zero. Otherwise, this would be another situation where $mn = m + n$.

Problem 4: Remembering definitions (8 points)

(a) Suppose that A and B are sets and f is a function from A to B. State precisely what it means for f to be one-to-one.

Solution: f is one-to-one if and only if for every $x, y \in A$, $x \neq y$ implies that $f(x) \neq f(y)$.

Or, equivalently, f is one-to-one if and only if for every $x, y \in A$, $f(x) = f(y)$ implies that $x = y$.

(b) Suppose that p and q are positive integers. State precisely what it means for p and q to be relatively prime.

Solution: The GCD of p and q is 1. That is, they have no common factors other than 1 (and -1).

Problem 5: Logic and proof mechanics (8 points)

(a) Give the negation of the following statement. Write your answer out in words and move the negatives (e.g. "not") so they are on individual predicates (e.g. "has two wheels").

> For any vehicle V, if V has two wheels and V's wheel diameter is more than 16 inches, then V is a bicycle.

Solution:

> There is a vehicle V such that V has two wheels and V's wheel diameter is more than 16 inches and V is not a bicycle.

(b) What's wrong with the following proof that $\overline{A \cup B} = \overline{A} \cap \overline{B}$? (Hint: you are looking for a major flaw, not a small issue with wording or justifications.)

> Let A and B be sets. Let x be an element of $\overline{A \cup B}$. By the definition of set complement, it is not the case that x is in $A \cup B$. By the definition of set union, this means that the following is not the case: x is in A or x is in B. By de Morgan's law for logic, this is equivalent to saying that x is not in A and x is not in B. So (by the definition of set complement), x is in $\overline{A}$ and x is in $\overline{B}$. So x is in in $\overline{A} \cap \overline{B}$ by the definition of set intersection.

Solution: This proves that $\overline{A \cup B} \subseteq \overline{A} \cap \overline{B}$. To prove the two sets are equal, we still need to show that $\overline{A} \cap \overline{B} \subseteq \overline{A \cup B}$. [This question was very hard.]

Problem 6: Writing a proof (8 points)

Recall the following definition: Given any positive integer m, the integers a and b are *congruent modulo* m if and only if there is an integer k such that $a = b + km$. a is congruent to b modulo m is written as $a \equiv b \pmod{m}$.

Prove that, for any integers a, b, c, and d and any positive integer m,

$$\text{if } a \equiv c \pmod{m} \text{ and } b \equiv d \pmod{m}, \text{ then } a + b \equiv c + d \pmod{m}.$$

Prove this directly using the above definition, together with basic logic and algebra. Do not use other facts about modular arithmetic proved in class or in the book.

Solution: Let a, b, c, and d be integers and let m be a positive integer. Suppose that $a \equiv c \pmod{m}$ and $b \equiv d \pmod{m}$.

By the definition of congruence modulo m, $a \equiv c \pmod{m}$ means that there is an integer k such that $a = c + km$. Similarly, since $b \equiv d \pmod{m}$, there is an integer j such that $b = d + jm$.

Adding these two equations together, we get that $a + b = (c + km) + (d + jm)$ So $a + b = (c + d) + (k + j)m$. Since k and j are integers, so is $k + j$. Therefore, by the definition of congruence modulo m, $a + b \equiv c + d \pmod{m}$, whis is what we needed to show.