MA 3110: Logic and Proof (Spring 2009)
Exam 2 (take-home portion)

NAME: Solutions

Instructions: Prove any *three* of the following theorems. If you turn in more than three proofs, I will only grade the first three that I see. I expect your proofs to be *well-written, neat, and organized.* You should write in *complete sentences.* Do not turn in rough drafts. What you turn in should be the "polished" version of potentially several drafts.

This portion of Exam 2 is worth 30 points, where each proof is worth 10 points.

The simple rules for this portion of the exam are:

1. You may freely use any theorems that we have discussed in class, but you should make it clear where you are using a previous result and which result you are using.
2. You are NOT allowed to copy someone else's work.
3. You are NOT allowed to let someone else copy your work.
4. You are allowed to discuss the problems with each other and critique each other's work.

This half of Exam 2 is due at the beginning of class on **Monday, April 6** (no exceptions). You should turn in this cover page and the three proofs that you have decided to submit.

Good luck and have fun!

Theorem 1: For every prime number p and for every natural number n, $\mathrm{GCD}(p,n) = 1$ iff p does not divide n.*

Pf: Let p be a prime number and let $n \in \mathbb{N}$.

($\Rightarrow$) Assume $GCD(p,n)=1$. For sake of a contradiction, assume that $p \mid n$. Since $p \mid p$ and $p \mid n$, $GCD(p,n) \geq p$. But $p > 1$, which contradicts $GCD(p,n) = 1$. Thus, $p \nmid n$.

($\Leftarrow$) Assume $p \nmid n$. Since p is prime, the only divisors of p are p and 1. But since $p \nmid n$, the only possibility remaining is that $GCD(p,n) = 1$. $\boxed{}$

*If a and b are natural numbers, then $\mathrm{GCD}(a,b)$ is the greatest common divisor of a and b. That is, $\mathrm{GCD}(a,b) = d$ iff d divides a and d divides b and d is greater than or equal to all other divisors common to a and b.

Theorem 2: Let x and y be real numbers. If x is rational and y is irrational, then $x+y$ is irrational.

Pf: Let x and y be real numbers. Assume that x is rational and y is irrational. Since x is rational, $\exists\ p, q \in \mathbb{Z}$ s.t. $x = \frac{p}{q}$, where $q \neq 0$. For sake of a contradiction, assume $x+y$ is rational. Then $\exists$ $r, s \in \mathbb{Z}$ s.t. $x+y = \frac{r}{s}$, where $s \neq 0$.

We see that

$$\frac{r}{s} = x+y = \frac{p}{q} + y,$$

which implies that

$$y = \frac{r}{s} - \frac{p}{q} = \frac{rq-ps}{sq}.$$

Since $p, q, r, s \in \mathbb{Z}$, $rq-ps$ and sq are both integers. Furthermore, since ~~[illegible]~~ $s \neq 0$ and $q \neq 0$, $sq \neq 0$. This implies that $y = \frac{rq-ps}{sq}$ is a rational number, which is a contradiction. Therefore, $x+y$ is irrational. $\boxtimes$

Theorem 3: Let A, B, C be sets. If $(A \cap C)^c \subseteq B$, then $A \subseteq (A - B^c) \cup C$.[†]

Pf: Let A, B, C be sets. Assume that $(A \cap C)^c \subseteq B$. We need to show that $A \subseteq (\cancel{B} A - B^c) \cup C$. Let $x \in A$. There are two possibilities:

(1) Suppose $x \in C$. Then $x \in (A - B^c) \cup C$, which implies that $A \subseteq (A - B^c) \cup C$.

(2) On the other hand, suppose $x \notin C$. Then $x \in C^c$. This implies that $x \in A^c \cup C^c$. But $A^c \cup C^c = (A \cap C)^c$, and so $x \in (A \cap C)^c$. Then $x \in B$ since we assumed that $(A \cap C)^c \subseteq B$. So, $x \notin B^c$. Since $x \in A$, but $x \notin B^c$, we have $x \in A - B^c$. Thus, $x \in (A - B^c) \cup C$, which implies that $A \subseteq (A - B^c) \cup C$. ■

[†]Hint: I'm sure there are many ways to do this one, but *probably* at some point in your proof, you should consider 2 cases: (1) $x \in C$; (2) $x \notin C$.

Definition: If $x \in \mathbb{R}$ and $A \subseteq \mathbb{R}$ with $A \neq \emptyset$, then we define the *translation* of A by x to be the set

$$A + x = \{a + x : a \in A\}.$$

Theorem 4: Let A and B be subsets of $\mathbb{R}$. If $A \neq \emptyset$ and if for all $x \in \mathbb{R}$, $(A + x) \cap B = \emptyset$, then $B = \emptyset$.

Pf: Let A and B be subsets of $\mathbb{R}$. Assume that $A \neq \phi$ and that for all $x \in \mathbb{R}$, $(A+x) \cap B = \phi$. For sake of a contradiction, assume $B \neq \phi$. Then $\exists$ at least one $b \in B$. Since $A \neq 0$, $\exists$ at least one $a \in A$. Now, let $x = b - a$. Then $a + x \in A + x$. But $a + x = a + b - a = b$. So, $b \in B$ and $b \in A + x$, which implies that $(A+x) \cap B \neq \phi$. This is a contradiction. Therefore, $B = \phi$. ▨

Theorem 5: Let A, B, C, D be sets. If $A \cup B \subseteq C \cup D$ and $A \cap D = \emptyset$, then $A \subseteq C$.

Pf: Let A, B, C, D be sets. Assume $A \cup B \subseteq C \cup D$ and $A \cap D = \phi$. We need to show that $A \subseteq C$. Let $x \in A$. Since $A \subseteq A \cup B$, $x \in A \cup B$. Since $A \cup B \subseteq C \cup D$, $x \in C \cup D$. This implies that $x \in C$ or $x \in D$. But since $x \in A$ and $A \cap D = \phi$, $x \notin D$. This implies that $x \in C$. Therefore, $A \subseteq C$. ▨