Math 2200-002/Discrete Mathematics

First Midterm. Answer Key

1. (4 points each) Restate each of the following as a logical proposition.

(a) Every integer has an additive inverse.

$$(\forall a \in \mathbb{Z})(\exists b \in \mathbb{Z})(a + b = 0)$$

(b) There is no largest natural number.

$$\neg(\exists n \in \mathbb{N})(\forall m \in \mathbb{N})(n \geq m)$$

(c) Each nonempty subset of $\mathbb{N}$ has a smallest element.

$$(\forall S \subseteq \mathbb{N})((S = \emptyset) \vee (\exists s \in S)(\forall t \in S)(s \leq t))$$

(d) There is a natural number that divides all other natural numbers.

$$(\exists n \in \mathbb{N})(\forall m \in \mathbb{N})(n|m)$$

(e) $f(x) = x^2$ (with domain $\mathbb{R}$) is not an increasing function.

$$\neg(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})((x < y) \rightarrow (x^2 \leq y^2))$$

2. Demonstrate that the following are logically equivalent.

(a) (10 points) $(p \rightarrow q)$ and $(\neg q \rightarrow \neg p)$

$$(p \rightarrow q) \equiv (\neg p \vee q) \text{ and} (\neg q \rightarrow \neg p) \equiv \neg(\neg q) \vee \neg p \equiv q \vee \neg p$$

so they are equivalent. (Or else use truth tables).

(b) (10 points) $((p \rightarrow \neg q) \wedge q)$ and $(\neg p \wedge q)$

$$(p \rightarrow \neg q) \wedge q \equiv (\neg p \vee q) \wedge q \equiv (\neg p \wedge q) \vee (q \wedge \neg q) \equiv (\neg p \wedge q) \vee \mathbf{F} \equiv (\neg p \wedge q)$$

(Or else use truth tables.)

3. (a) (10 points) Prove that there are infinitely many prime numbers.

Proof by Contradiction. If there are finitely many primes, then there is an $n \in \mathbb{N}$ and a set:

$$S = \{p_1, ..., p_n\}$$

consisting of all the primes. Then the number:

$$N = p_1 \cdot p_2 \cdots p_n + 1$$

is **not** divisible by any of the primes in the set S. But N has a prime factorization:

$$N = q_1 \cdots q_m$$

so q_1 is a prime that divides N and is not in the set S. Contradiction.

(b) (10 points) Prove there are infinitely many composite numbers.

Direct Proof. The set of even numbers bigger than 2:

$$\{4, 6, 8, ...\}$$

is an infinite set of composite numbers. Also, the set of powers of 2:

$$\{4, 8, 16, ...\}$$

is an infinite set of composite numbers. (There are lots of examples).

4. (a) (10 pts) Prove that if $3|n^2$ then $3|n$.

Proof by Contrapositive. Suppose 3 does not divide n.

Then there are two cases. Either:

(a) $n = 3k + 1$ for some k or (b) $n = 3k + 2$ for some k.

In case (a), we have

$$n^2 = (3k + 1)^2 = 9k^2 + 6k + 1 = 3(3k^2 + 2k) + 1$$

so 3 does not divide n^2, and in case (b) we have

$$n^2 = (3k + 2)^2 = 9k^2 + 12k + 4 = 3(3k^2 + 4k + 1) + 1$$

so in that case, also, 3 does not divide n^2.

We conclude that if 3 does not divide n, then 3 does not divide n^2. This gives us the contrapositive: if 3 divides n^2, then 3 divides n.

(b) (10 points) Use (a) to prove that $\sqrt{3}$ is irrational.

Proof by Contradiction. Suppose $\sqrt{3}$ is rational, and write:

$$\sqrt{3} = \frac{m}{n}$$

in lowest terms, i.e. with $\gcd(m, n) = 1$. Then:

$$3 = \frac{m^2}{n^2}$$

and:

(1) $m^2 = 3n^2$, so 3 divides m^2, so 3 divides m (using (a)).

(2) Let $m = 3k$ Then $9k^2 = (3k)^2 = 3n^2$ so:

(3) $n^2 = 3k^2$, so 3 divides n (again using (a)).

We conclude that 3 divides m and n, contradicting $\gcd(m, n) = 1$ and since **every** rational number can be put in lowest terms, we conclude that $\sqrt{3}$ is not a rational number.

5. (5 points each) Give examples of each of the following:

(a) An infinite subset of $\mathbb{R}$ that is disjoint from $\mathbb{Q}$.

$$\mathbb{R} - \mathbb{Q}$$

or $\{\sqrt{2}, \sqrt{2}+1, \sqrt{2}+2, ...\}$ or $\{\sqrt{2}, 2\sqrt{2}, 3\sqrt{2}, ...\}$.

(b) A function $f : \mathbb{R} \to \mathbb{R}$ that is nondecreasing but not one-to-one.

$$f(x) = 0 \text{ the constant function}$$

(c) The first 12 terms of a nonzero sequence satisfying:

$$a_n = a_{n-1} - a_{n-2}$$

Choose any first two terms and then run the recursion. For example:

$$1, 2, 1, -1, -2, -1, 1, 2, 1, -1, -2, -1$$

(Fun fact: The sequence will always repeat after 6 terms)

(d) A triple of sets $S, \mathcal{P}(S), \mathcal{P}(\mathcal{P}(S))$.

$$S = \emptyset,\ \mathcal{P}(S) = \{\emptyset\},\ \mathcal{P}(\mathcal{P}(S)) = \{\emptyset, \{\emptyset\}\}$$

or else

$$S = \{1\},\ \mathcal{P}(S) = \{\emptyset, \{1\}\}, \mathcal{P}(\mathcal{P}(S)) = \{\emptyset, \{\emptyset\}, \{\{1\}\}, \{\emptyset, \{1\}\}\}$$