University of Lethbridge
Department of Mathematics and Computer Science
29th October, 2015
Math 2000A/B - Midterm

Last Name: **SOLUTIONS**

First Name: **THE**

Student Number: _____

Record your answers below each question in the space provided. **Left-hand pages may be used as scrap paper for rough work.** If you want any work on the left-hand pages to be graded, please indicate so on the right-hand page.

Partial credit will be awarded for partially correct work, so be sure to show your work, and include all necessary justifications needed to support your arguments.

The value of each problem is indicated in the left-hand margins. The value of a problem does not always indicate the amount of work required to do the problem.

Outside aids, including, but not limited to, cheat sheets, smart phones, laptops, spy cameras, drones, and telepathic communication, are not permitted. You can keep a calculator with you if it makes you feel better.

For grader's use only:

Page	Grade
2	/10
3	/10
4	/8
5	/12
6	/10
7	/10
Total	/60

1. For each conditional statement below, identify (i) the hypothesis, (ii) the conclusion, and (iii) whether it is true or false.

[2] (a) If $3 + 4 = 8$, then $42 > 15$.

The hypothesis $3+4 = 8$ is false, and the conclusion $42 > 15$ is true, so the conditional statement is true.

[2] (b) If $1 + 1 = 2$, then $5 - 3 = 7$.

The hypothesis $1 + 1 = 2$ is true, but the conclusion $5 - 3 = 7$ is false. Therefore, the conditional statement is false.

[2] (c) If $5 \geq 5$, then $3 - 7 > 0$.

The hypothesis $5 \geq 5$ is true, but the conclusion $3 - 7 > 0$ is false. Therefore, the conditional statement is false.

2. For each predicate below, add (i) a universal set, and (ii) appropriate quantifier(s) such that the resulting quantified statement is true.
(For example, given the predicate $2x - 4 = 6$, you could form the true statement $(\exists x \in \mathbb{Z})(2x - 4 = 6)$.)

[2] (a) $x^2 + 1 > 0$.

One possible answer is $\forall x \in \mathbb{R}, x^2 + 1 > 0$. (Really any choice of quantifier and universal set will work, except for $\forall x \in \mathbb{C}, x^2 + 1 > 0$.)

[2] (b) $2m - 3n = 4$.

One possibility is $(\exists m \in \mathbb{Z})(\exists n \in \mathbb{Z})(2m - 3n = 4)$. (This is true: take $m = 2$ and $n = 0$.) Other possibilities could involve using $\mathbb{Q}$ or $\mathbb{R}$ for your universal set.

3. For each of the problems below, provide a definition or example, as requested.

[2] (a) Define the **truth set** of a predicate $P(x)$.

The **truth set** of $P(x)$ is the set T of all values for the variable x that make $P(x)$ true. Symbolically,

$$T = \{x \in U : P(x) \text{ is true}\}.$$

[2] (b) Give an example of a tautology.

Here are three examples: Either $2 = 0$ or $2 \neq 0$. $P \vee \neg P$. $[P \wedge (P \to Q] \to Q]$.

[2] (c) Define what it means for an integer a to be **congruent** to an integer b, modulo n.

Given integers $a, b, n \in \mathbb{Z}$ with $n \geq 1$, we say that a is **congruent** to b modulo n, and write $a \equiv b \pmod{n}$, if $n|(a - b)$.

[2] (d) Give four examples of integers a such that $a \equiv 3 \pmod{7}$.

We need to choose a such that $7|(a - 3)$, which is equivalent to $a = 3 + 7k$ for some $k \in \mathbb{Z}$. For $k = 1, 2, 3, 4$, we get $a = 10, 17, 24, 31$. There are infinitely many other examples.

[2] (e) What is the **contrapositive** of a conditional statement $P \to Q$?

$$\neg Q \to \neg P.$$

4. A set of real numbers A is defined to be *pronghornian*[1] if for each $a \in A$ there exists some element $b \in A$ such that $a^2 + b$ is even and $a^2 \equiv b^3 \pmod{2015}$. Complete the following [3] sentence:

   A set of real numbers A is **not** pronghornian if...

   The negation of $(\forall a \in A)(\exists b \in A)(a^2 + b$ is even and $a^2 \equiv b^3 \pmod{2015})$ is:

   $$(\exists a \in A)(\forall b \in A)(a^2 + b \text{ is } \textbf{not} \text{ even } \textbf{or } a^2 \not\equiv b^3 \pmod{2015}),$$

   so A is not pronghornian if there exists some $a \in A$ such that for all $b \in B$, either $a^2 + b$ is odd, or $a^2 \not\equiv b^3 \pmod{2015}$.

5. Prove the following logical equivalence using previously established logical equivalences: [5] $(P \wedge Q) \to R \equiv (P \to R) \vee (Q \to R)$.

   Starting from the left-hand side, we have:

   $$\begin{aligned}
   (P \wedge Q) \to R &\equiv \neg(P \wedge Q) \vee R && \text{(using 1(a))} \\
   &\equiv (\neg P \vee \neg Q) \vee R && \text{(de Morgan's law)} \\
   &\equiv (\neg P \vee \neg Q) \vee (R \vee R) && \text{(Idempotent Law)} \\
   &\equiv (\neg P \vee R) \vee (\neg Q \vee R) && \text{(Associative and Commutative Laws)} \\
   &\equiv (P \to R) \vee (Q \to R) && \text{(using 1(a)),}
   \end{aligned}$$

   which is the right-hand side.

[1] Yes, I just made that up.

6. Determine whether the following statements are true or false. If a statement is true, give a **direct** proof of the statement. If it is false, provide a counterexample to support your claim.

[4] (a) For any integers a and b, if $a \equiv 3 \pmod 5$ and $b \equiv 2 \pmod 5$, then $ab \equiv 1 \pmod 5$.

This statement is **true** (as long as you corrected the typo).
Suppose that $a \equiv 3 \pmod 5$ and $b \equiv 2 \pmod 5$. It follows from a result in class that $ab \equiv 3(2) \pmod 5$, and since $3(2) = 6$ and $6 \equiv 1 \pmod 5$, it follows that $ab \equiv 1 \pmod 5$.

Alternative (slightly less short) proof: Suppose that $a \equiv 3 \pmod 5$ and $b \equiv 2 \pmod 5$. It follows that there exist integers k and l such that $a = 5k+3$ and $b = 5l+2$. Thus

$$ab = (5k + 3)(5l + 2) = 25kl + 10k + 15l + 6 = 5(5kl + 2k + 3l + 1) + 1,$$

and therefore $ab \equiv 1 \pmod 5$.

(b) For any integers a and b, if $ab \equiv 0 \pmod{12}$, then $a \equiv 0 \pmod{12}$ or $b \equiv 0 \pmod{12}$.

[4]

This statement is false. For example, consider $a = 3$ and $b = 4$. Then $ab = 12$ and $12 \equiv 0 \pmod{12}$, but $3 \not\equiv 0 \pmod{12}$ and $4 \not\equiv 0 \pmod{12}$.

[4] (c) For any integers a, b, and c, if $a|b$ and $a|c$, then $a|(2b - 3c)$.

This statement is true. Suppose that $a|b$ and $a|c$. Then there exist integers k and l such that $b = ak$ and $c = al$, and thus

$$2b - 3c = 2(ak) - 3(al) = a(2k) - a(3l) = a(2k - 3l).$$

Since $2b - 3c$ can be written as a multiple of a, it follows that $a|(2b - 3c)$.

[5] 7. Given that $x \in \mathbb{R}$ is **irrational**, prove the following:

For every real number y, either $x + y$ is irrational, or $x - y$ is irrational.

Hint: Use proof by contradition, and take care to correctly form the negation of the given statement.

Let $x \in \mathbb{R}$ be irrational, and suppose for the sake of contradiction that there exists $y \in \mathbb{R}$ such that $x+y$ is rational and $x-y$ is rational. Since the set of rational numbers is closed under addition and multiplication, it follows that $(x + y) + (x - y) = 2x$ is rational, and therefore $\frac{1}{2}(2x) = x$ is rational, which contradicts the assumption that x is irrational.

[5] 8. Use proof by cases to prove that for each integer n, $n^3 \equiv n \pmod 3$.

For any integer n, the division algorithm guarantees that we can write $n = 3q + r$ for some $q \in \mathbb{Z}$, where $r = 0, 1$, or 2.

If $r = 0$, then $n \equiv 0 \pmod 3$, and thus $n^3 \equiv 0^3 \pmod 3$. Since $0^3 = 0$, we see that both n and n^3 are congruent to 0 modulo 3, and thus $n^3 \equiv n \pmod 3$.

If $r = 1$, then $n \equiv 1 \pmod 3$, and thus $n^3 \equiv 1^3 \pmod 3$. Since $1^3 = 1$, we see that both n and n^3 are congruent to 1 modulo 3, and thus $n^3 \equiv n \pmod 3$.

If $r = 2$, then $n \equiv 2 \pmod 3$, and thus $n^3 \equiv 2^3 \pmod 3$. Since $2^3 = 8$ and $8 \equiv 2 \pmod 3$, it follows that $n^3 \equiv 2 \pmod 3$ as well, and thus $n^3 \equiv n \pmod 3$.

In all three cases, we see that $n^3 \equiv n \pmod 3$, so the result holds for all integers n.

Alternative proof: Instead of using the fact that if $a \equiv b \pmod n$, then $a^k \equiv b^k \pmod n$, you can handle each case explicitly.

For $r = 0$, $n = 3q$, and thus $n^3 = (3q)^3 = 27q^3 = 3(9q^3)$, and therefore $n^3 - n = 3(9q^3 - q)$ is divisible by 3.

For $r = 1$, $n = 3q + 1$, so

$$n^3 = (3q + 1)^3 = 27q^3 + 27q^2 + 9q + 1 = 3(9q^3 + 9q^2 + 3q) + 1,$$

and thus $n^3 - n = 3(9q^3 + 9q^2 + 2q)$ is divisible by 3.

Similarly, for $r = 2$, $n = 3q+2$ and $n^3 = 27q^3+54q^2+36q+8 = 3(9q^3+14q^2+12q+2)+2$, so $n^3 - n = 3(9q^3 + 14q^2 + 11q + 2)$ is divisible by 3.

In all three cases, we see that $n^3 - n$ is divisible by 3, so $n^3 \equiv n \pmod 3$ for all integers n.

[5] 9. Use mathematical induction to prove that $4 \mid (5^n - 1)$ for each natural number n.

When $n = 1$, we have $5^n - 1 = 5 - 1 = 4$, and since $4|4$, the base case holds.

Suppose that we know that $4|(5^k - 1)$ for some integer $k \geq 1$. Then we can write $5^k - 1 = 4p$ for some $p \in \mathbb{Z}$, which gives us $5^k = 4p + 1$. Multiplying both sides of this last equation by 5, we obtain:

$$5^{k+1} = 5(5^k) = 5(4p + 1) = 20p + 5 = 20p + 4 + 1 = 4(5p + 1) + 1,$$

so $5^{k+1} - 1 = 4(5p + 1)$, which shows that $4|(5^{k+1} - 1)$. Thus, whenever the result is true for $n = k$, it holds for $n = k + 1$ as well, and thus $4|(5^n - 1)$ for all natural numbers n by the Principle of Mathematical Induction.

10. For which natural numbers n is it true that $2^n > (n + 1)^2$? Support your claim with a
[5] proof by induction.

We have $2^1 = 2 < 4 = (1 + 1)^2$, $2^2 = 4 < 9 = (2 + 1)^2 4$, $2^3 = 8 < 16 = (3 + 1)^2$, $2^4 = 16 < 25 = (4 + 1)^2$, and $2^5 = 32 < 36 = (5 + 1)^2$, but $2^6 = 64 > 49 = (6 + 1)^2$. Thus, the result is false for $1 \leq n \leq 5$ but true for $n = 6$. Suspecting that the result will continue to hold for $n > 6$, we take $n = 6$ as our base case and proceed by induction.

Since the result holds for $n = 6$, we suppose that $2^k > (k + 1)^2$ for some $k \geq 6$, and need to show that it follows from this that $2^{k+1} > (k + 1 + 1)^2 = (k + 2)^2$.

Since $2^k > (k + 1)^2$, we can multiply both sides of this inequality by 2 (noting that $2 > 0$), giving us

$$2^{k+1} = 2(2^k) > 2(k + 1)^2 = 2(k^2 + 2k + 1) = 2k^2 + 4k + 2.$$

Since we want to show that $2^{k+1} > (k + 2)^2$, the result will follow if we can show that $2k^2 + 4k + 2 > (k + 2)^2 = k^2 + 4k + 4$. But since $k \geq 6$, it follows that $k^2 \geq 36$, and in particular, $k^2 > 2$. Thus,

$$2k^2 + 4k + 2 = k^2 + k^2 + 4k + 2 > 2 + k^2 + 4k + 2 = k^2 + 4k + 4 = (k + 2)^2,$$

which is what we needed to show.

List of basic equivalences

1. Equivalences involving conditional statements
   (a) $P \to Q \equiv \neg P \vee Q$
   (b) $\neg(P \to Q) \equiv P \wedge \neg Q$
   (c) $P \to Q \equiv \neg Q \to \neg P$
2. Commutative properties
   (a) $P \vee Q \equiv Q \vee P$
   (b) $P \wedge Q \equiv Q \wedge P$
3. Associative properties
   (a) $(P \vee Q) \vee R \equiv P \vee (Q \vee R)$
   (b) $(P \wedge Q) \wedge R \equiv P \wedge (Q \wedge R)$
4. Distributive properties
   (a) $P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$
   (b) $P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$
5. Idempotent laws
   (a) $P \vee P \equiv P$
   (b) $P \wedge P \equiv P$
6. De Morgan's Laws
   (a) $\neg(P \vee Q) \equiv \neg P \wedge \neg Q$
   (b) $\neg(P \wedge Q) \equiv \neg P \vee \neg Q$
7. Law of the Excluded Middle
   (a) $P \vee \neg P \equiv T$
   (b) $P \wedge \neg P \equiv F$
8. Effect of Tautologies and Contradictions
   (a) $P \vee T \equiv T$
   (b) $P \wedge T \equiv P$
   (c) $P \vee F \equiv P$
   (d) $P \wedge F \equiv F$