Math 300 Summer 2009 Final Exam Solutions

1. (a) (12 pts) Let $f : A \to B$ be a function. For this function, answer the following questions:

   i. Give the precise definition of one-to-one and give the negation of the definition.
   DEFINITION: $\forall x_1, x_2 \in A$**, if** $f(x_1) = f(x_2)$**, then** $x_1 = x_2$**.**

   NEGATION: $\exists x_1, x_2 \in A$ **such that** $f(x_1) = f(x_2)$ **and** $x_1 \neq x_2$

   ii. Give the precise definition, using proper quantifiers, of onto and give the negation of the definition.
   DEFINITION: $\forall b \in B, \exists a \in A$ **such that** $f(a) = b$.

   NEGATION: $\exists b \in B, \forall a \in A, f(a) \neq b$**.**

   (b) (5 pts) Find the truth values of the statement $P \Rightarrow (Q \vee \neg Q)$ for all possible truth values of the statements P and Q (That is, fill in the table below).

P	Q	$\neg Q$	$Q \vee \neg Q$	$P \Rightarrow (Q \vee \neg Q)$
T	T	**F**	**T**	**T**
T	F	**T**	**T**	**T**
F	T	**F**	**T**	**T**
F	F	**T**	**T**	**T**

   (c) (6 pts) TWO of the steps in the 'proof' below are wrong. Circle the two steps that are wrong and briefly explain why they are wrong.
   (don't tell me why the theorem is wrong, tell me why the proof is wrong):

   False Statement: If $n \not| \, y - 1$, then $n \not| \, xy - x$ and $n|x$.

   False Proof: We prove the contrapositive.
   (1) That is, we must show $n|xy - x$ and $n \not| \, x$ implies $n|y - 1$.
   (2) By definition, $n|xy - x$ is the same as $xy - x \equiv 0 \pmod{n}$.
   (3) Adding x to both sides of the congruence gives $xy \equiv x \pmod{n}$.
   (4) Since $n \not| \, x$, canceling the x gives $y \equiv 1 \pmod{n}$.
   (5) Thus, $n|y - 1$. $\square$

   EXPLANATION: **STEP (1) IS WRONG: The contrapositive is incorrectly stated. DeMorgan's Law should have been used to give** $n|xy - x$ **OR** $n \not| \, x$ **implies** $n|y - 1$**. STEP (4) IS WRONG: In order to cancel** x**, we need the condition** $\gcd(x, n) = 1$**.**

2. (a) (12 pts) Consider the statement: If $6b \equiv 0 \pmod{a}$, then $b \equiv 0 \pmod{a}$.

   i. Give a counterexample to this statement (with specific numbers a and b) and add a hypothesis about a that would make the statement true.

   COUNTEREXAMPLE: **Any example where** $\gcd(a, 6) > 1$ **and** b **is a multiple of** $a/\gcd(a, 6)$**.** **(**$a = 12$**,** $b = 2$ **is one and** $a = 6$**,** $b = 1, 2, 3, 4$**, or** 5 **is another)**.

   ADDED HYPOTHESIS: **We need** $\gcd(6, a) = 1$ **in order to cancel the 6.**

   ii. Prove that the converse of the original statement is always true.

   The converse states: If $b \equiv 0 \pmod{a}$**, then** $6b \equiv 0 \pmod{a}$**.**
   By definition of $b \equiv 0 \pmod{a}$**,** $a|b$**. Thus,** $b = ak$ **for some integer** k**. Multiplying by 6 gives** $6b = a(6k)$**. Thus,** $a|6b$**, so** $6b \equiv 0 \pmod{a}$**.** $\square$

(b) (14 pts) Prove that $\displaystyle\sum_{k=1}^{n} k \cdot k! = (n+1)! - 1$ for all $n \in \mathbb{N}$.

PROOF: We use induction on n**.**

Base Step: For $n = 1$**,** $\sum_{k=1}^{n} k \cdot k! = 1 \cdot 1! = 1$ **and** $(n+1)! - 1 = (1+1)! - 1 = 2 - 1 = 1$**.**
Thus, the equality holds for $n = 1$**.**

Inductive Step: Assume $\sum_{k=1}^{m} k \cdot k! = (m+1)! - 1$ **for some** $m \in \mathbb{N}$**.**
Then

$$\begin{aligned}
\textstyle\sum_{k=1}^{m+1} k \cdot k! &= (m+1)(m+1)! + \textstyle\sum_{k=1}^{m} k \cdot k! && \textbf{(pulling out the last term)} \\
&= (m+1)(m+1)! + (m+1)! - 1 && \textbf{(by the inductive hypothesis)} \\
&= (m+1+1)(m+1)! - 1 && \textbf{(factoring out } (m+1)!\textbf{)} \\
&= (m+2)! - 1
\end{aligned}$$

Thus, equality holds for all $n \in \mathbb{N}$**.** $\square$

3. (a) (8 pts) Find an integer a such that $0 \leq a < 5$ and $3^{800} + 4^{801} + 5 \cdot 6^{100} + 7 \equiv a \pmod 5$. (You must show your work to get credit)

ANSWER: First, by basic replacement, note:

$$3^{800} + 4^{801} + 5 \cdot 6^{100} + 7 \equiv 3^{800} + (-1)^{801} + 0 \cdot 1^{100} + 2 \equiv 3^{800} - 1 + 2 \equiv 3^{800} + 1 \pmod 5.$$

Now we compute $3^{800} \pmod 5$**.**
METHOD 1:
By Fermat's Little Theorem, $3^4 \equiv 1 \pmod 5$**. Thus,** $3^{800} = (3^4)^{200} \equiv 1^{200} \equiv 1 \pmod 5$**.**
METHOD 2:
By Successive Squaring, $3^{800} = (3^2)^{400} \equiv 9^{400} \equiv 4^{400} \equiv (-1)^{400} \equiv 1 \pmod 5$**.**
No matter what method you use, $3^{800} \equiv 1 \pmod 5$**, so**

$$3^{800} + 4^{801} + 5 \cdot 6^{100} + 7 \equiv 3^{800} + 1 \equiv 1 + 1 \equiv 2 \pmod 5.$$

(b) (5 pts) A certain fast food restaurant sells chicken nuggets in packs of either 6 or 9. If these are the only size packs you can buy, is it possible to purchase exactly 94 nuggets? (Specifically, tell me which theorem from class gives us the answer to this question and explain the relationship between these three numbers that allows you to make your conclusion).

ANSWER: This problem is asking if $6x+9y = 94$ **has a nonnegative integer solution for** x **and** y**. By the Bezout's Lemma (the LDE theorem), the equation** $6x+9y = 94$ **has NO integer solutions (nonnegative or otherwise), because** $\gcd(6, 9) = 3$ **does not divide 94.**

(c) (12 pts) Prove that 3 divides $n^3 + 8n$ for all $n \in \mathbb{N}$.

PROOF: (This could be done by induction, but using congruences is a bit easier.)
Let $n \in \mathbb{N}$**. From class, every integer (including** n**) must fit in one of three congruence classes modulo 3.**
CASE 1: If $n \equiv 0 \pmod 3$**, then** $n^3 + 8n \equiv 0^3 + 2 \cdot 0 \equiv 0 \pmod 3$**.**
CASE 2: If $n \equiv 1 \pmod 3$**, then** $n^3 + 8n \equiv 1^3 + 2 \cdot 1 \equiv 3 \equiv 0 \pmod 3$**.**
CASE 2: If $n \equiv 2 \pmod 3$**, then** $n^3 + 8n \equiv 2^3 + 2 \cdot 2 \equiv 6 \equiv 0 \pmod 3$**.**
Thus, in all cases, $n^3 + 8n \equiv 0 \pmod 3$**. Hence,** $3 | n^3 + 8n$**.** $\square$

4. (a) (16 pts)

   i. Let p be an odd prime.
   Prove that if $p = a^2 + 1$ for some integer a, then $p \equiv 1 \pmod 4$.
   (Hint: Break your proof into cases, based on a).

   PROOF: Let p be an odd prime and $p = a^2 + 1$ for some integer a.
   CASE 1: If a is even, then $a = 2m$ for some integer m. By substitution, $p = (2m)^2 + 1 = 4m^2 + 1$. **Thus, in this case,** $p \equiv 0m^2 + 1 \equiv 1 \pmod 4$.
   CASE 2: If a is odd, then $a = 2n+1$ for some integer n. Thus, $p = (2n+1)^2+1 = 4n^2 + 4n + 1 + 1 = 4(n^2 + n) + 2$. **In particular, p is even. By assumption, p is an odd prime so it can't be even. Hence, this case can't occur.**
   Therefore, if the hypotheses are satisfied, then $p \equiv 1 \pmod 4$.

   ii. Briefly explain why we can use the theorem above to conclude that all primes of the form $p \equiv 3 \pmod 4$ cannot be written as one more than a square.
   (for example, $11 \equiv 3 \pmod 4$ and 11 is not one more than a square).

   ANSWER: The contrapositive of the theorem above would say for an odd prime, if $p \not\equiv 1 \pmod 4$, then $p \neq a^2 + 1$ for any integer a. In particular, if $p \equiv 3 \pmod 4$, then p is an odd prime and it is not congruent to 1 modulo 4, so it cannot be written as one more than a square.

(b) (10 pts) Let $f : A \to B$ and $g : B \to C$ be functions and define $h : A \to C$ by $h(x) = g(f(x))$ for all $x \in A$. Prove if h is one-to-one and f is onto, then g is one-to-one.
(Hint: You will use the fact that f is a function, so it is well-defined.)

PROOF: Assume $g(b_1) = g(b_2)$ for some b_1 and b_2 in B.
Since f is onto, $f(a_1) = b_1$ and $f(a_2) = b_2$ for some a_1 and a_2 in A.
By substitution, $g(f(a_1)) = g(f(a_2))$ and so $h(a_1) = h(a_2)$.
Since h is one-to-one, $a_1 = a_2$.
Since f is a function (and thus, f is well-defined), $b_1 = f(a_1) = f(a_2) = b_2$.
Thus, g is one-to-one. $\square$