MATH 109 - FINAL EXAM

Name (Last, First): McQueen, Steve

Student ID: 

ANSWERS TO THE TRUE/FALSE QUESTIONS DO NOT NEED TO BE JUSTIFIED. A CORRECT ANSWER IS WORTH 5 POINTS, AN INCORRECT ANSWER IS WORTH 0 POINTS, AND A BLANK ANSWER IS WORTH 2 POINTS.

REMEMBER THIS EXAM IS GRADED BY A HUMAN BEING. WRITE YOUR SOLUTIONS NEATLY AND COHERENTLY, OR THEY RISK NOT RECEIVING FULL CREDIT.

THIS EXAM WILL BE SCANNED. MAKE SURE YOU WRITE ALL SOLUTIONS IN THE SPACES PROVIDED.

THE EXAM CONSISTS OF 9 TRUE/FALSE QUESTIONS, 7 LONGER FORMAT QUESTIONS, AND 1 BONUS QUESTION. YOUR ANSWERS TO THE LONGER FORMAT QUESTIONS SHOULD BE CAREFULLY JUSTIFIED. YOU ARE ALLOWED TO USE RESULTS FROM THE TEXTBOOK, HOMEWORK, AND LECTURE, BUT THEY SHOULD BE CLEARLY REFERENCED. FOR EXAMPLE,

“We prove the statement by induction on ...”
1. (40 points) Label the following statements as true or false. Any ambiguous answer (for example, resembling a hybrid of T and F) will be treated as an incorrect answer.

(a) \[ \text{ } \quad (P \implies Q) \iff (-Q \implies -P). \]
   
   This is the contrapositive.

(b) \[ \text{ } \quad T \quad \text{Let } A, B, C \text{ be sets such that } A \cap B = A \cap C \text{ and } A \cup B = A \cup C. \]
   
   \[ B = (B \cap A) \cup (B \setminus A) \]
   
   \[ C = (C \cap A) \cup (C \setminus A) \]
   
   \[ (A \cup B) \setminus A = B \setminus A \quad \text{so} \quad A \cup B = A \cup C \implies B \setminus A = C \setminus A. \]
   
   \[ (A \cup C) \setminus A = C \setminus A \]
   
   Already know \[ B \cap A = C \cap A. \]

(c) \[ \text{ } \quad F \quad \text{Let } f : X \to Y \text{ and } g : Y \to Z \text{ be functions such that } g \circ f : X \to Z \text{ is a bijection. Then } f \text{ is a surjection and } g \text{ is an injection.} \]
   
   \[ f \text{ is necessarily an injection} \]
   
   \[ g \text{ is necessarily a surjection} \]
   
   As a counterexample, consider \[ f : \{1, 2, 3\} \to \{1, 2, 3\}, \quad 1 \mapsto 1 \]
   
   \[ g : \{1, 2, 3\} \to \{1\}, \quad 1 \mapsto 1 \]
   
   Then \[ g \circ f = \text{id}_{\{1\}} \text{ is bijective, but } f \text{ is not surjective and } g \text{ is not injective}. \]
(d) \( \top \) Suppose that \( A = \bigcup_{i=1}^{\infty} A_i \) is uncountable. Then
\[ \exists i \in \mathbb{N} : A_i \text{ is uncountable.} \]
If not, then \( \forall i \in \mathbb{N}, A_i \text{ is countable.} \)
But then \( \bigcup_{i=1}^{\infty} A_i \) is countable, a contradiction.

(e) \( \top \) If \( a, b, c \) are positive integers such that \( \gcd(a, b) = \gcd(a, c) = 1 \), then
\[ \gcd(a, bc) = 1. \]
Look at the prime factorization of \( a, b, \) and \( c \).

(f) \( \bot \) Let \( X \) be an infinite set. Suppose that \( \Pi \subseteq \mathcal{P}(X) \) is a partition of \( X \).
Then \( \Pi \) is also an infinite set.
\[ \Pi = \mathcal{E} \times \mathcal{B} \text{ is always a partition of } X \text{ if} \]
\[ X \text{ is a non-empty set.} \]
(g) Suppose that $n \in \mathbb{N}$ has the prime factorization $n = p_1^{k_1} \cdots p_r^{k_r}$, where $k_i \geq 1$ for each $i \in [r]$. Then $n$ has exactly $k_1 \cdots k_r$ positive divisors.

Consider $2 = 2^1$, which has two positive divisors.

The actual answer is $(k_1 + 1)(k_2 + 1) \cdots (k_r + 1)$.

(h) Suppose that $p$ and $q$ are distinct prime numbers. Then the equation

\[ [qp]_{p^2} [x]_{p^2} = [p]_{p^2} \]

has a unique solution $[x]_{p^2} \in \mathbb{Z}_{p^2}$.

\[ qpx \equiv p \mod p^2 \iff qx \equiv 1 \mod p \]

$qx \equiv 1 \mod p$ has a unique solution mod $p$ since $\gcd(p, q) = 1$; however, this gives $p$ solutions mod $p^2$.

(i) $(P \lor Q) \iff (\neg P \implies Q)$

This was a common technique we used to prove "or" statements. Can be proven with a truth table.
2. (15 pts) Let \( n \in \mathbb{N} \). Prove that

\[
\sum_{m=1}^{n} m^2 = \frac{n(n+1)(2n+1)}{6}.
\]

We prove this by induction on \( n \).

**Base case:** for \( n = 1 \), \( \sum_{m=1}^{1} m^2 = 1 = \frac{(1+1)(2+1)}{6} \).

**Inductive step:** assume the result is true for some value of \( n \geq 1 \). Then

\[
\sum_{m=1}^{n+1} m^2 = \sum_{m=1}^{n} m^2 + (n+1)^2
\]

\[
= \frac{n(n+1)(2n+1)}{6} + (n+1)^2 \quad \text{by the induction hypothesis.}
\]

Rearranging,

\[
\frac{n(n+1)(2n+1)}{6} + (n+1)^2 = (n+1) \left( \frac{n(2n+1)}{6} + n+1 \right)
\]

\[
= (n+1) \frac{2n^2 + 7n + 6}{6}
\]

\[
= \frac{(n+1)(n+2)(2n+3)}{6},
\]

as was to be shown.
3. (25 pts) Let $S = \{(a_1, a_2, \ldots, a_n, \ldots) \mid a_i \in \mathbb{N} \text{ for each } i \in \mathbb{N}\}$. In other words, $S$ is the set of sequences in $\mathbb{N}$. For example, $(1, 1, 1, \ldots) \in S$.

(a) (10 pts) Give an example of an injective function $f : \mathbb{N} \to S$. Make sure to actually prove that your function is injective.

There are many options to choose from.

One possibility is $f : \mathbb{N} \to S$, $n \mapsto (n, n, n, \ldots)$

If $f(n) = f(m)$, then $(n, n, n, \ldots) = (m, m, m, \ldots)$

In particular, the first coordinate of each sequence is equal, which means $n = m$.

Thus, $f$ is injective.
(b) (15 pts) Prove that no function \( g : \mathbb{N} \to S \) is surjective. Deduce that \( S \) is uncountable.

This is Cantor's diagonal argument.

We define an element \((a_1, a_2, ...) \in S\) as follows.

For \( i \in \mathbb{N} \), we let \( a_i = \begin{cases} \#1 \text{ if } g(i) \neq \#0 \\ \#2 \text{ if } g(i) = \#0 \end{cases} \)

Then \( g(i) \neq (a_1, a_2, ...) \) for any \( i \in \mathbb{N} \),

since the two elements will disagree in the \( i \)th position. So, \((a_1, a_2, ...) \notin \text{Im}(g)\),

which proves that \( g \) is not surjective.

Part (a) proves that \( S \) is an infinite set.

\( S \) is not denumerable by what we just proved.

So, \( S \) is uncountable.
4. (20 pts)
   (a) (5 pts) State the binomial theorem: for all real numbers \( a \) and \( b \) and non-negative integers \( n \),
   
   \[
   (a + b)^n = \sum_{r=0}^{n} \binom{n}{r} a^r b^{n-r}
   \]

   (b) (15 pts) Let \( X \) be a finite set with \( \#(X) = n \geq 1 \). Prove that
   
   \[
   \sum_{A \in \mathcal{P}(X)} (-1)^{\#(A)} = 0.
   \]

   Recall that the notation \( \sum_{A \in \mathcal{P}(X)} \) means to take the sum over all subsets of \( X \). For example, if \( X = \{1, 2\} \), then \( \mathcal{P}(X) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\} \) and
   
   \[
   \sum_{A \in \mathcal{P}(X)} (-1)^{\#(A)} = (-1)^{\#(\emptyset)} + (-1)^{\#(\{1\})} + (-1)^{\#(\{2\})} + (-1)^{\#(\{1, 2\})} = 1 - 1 - 1 + 1 = 0.
   \]

   Hint: Notice that
   
   \[
   \sum_{A \in \mathcal{P}(X)} (-1)^{\#(A)} = \sum_{r=0}^{n} \left( \sum_{A \in \mathcal{P}_r(X)} (-1)^{\#(A)} \right).
   \]

   Now find a way to apply the binomial theorem.

   \[
   \sum_{A \in \mathcal{P}(X)} (-1)^{\#(A)} = \sum_{r=0}^{n} \left( \sum_{A \in \mathcal{P}_r(X)} (-1)^{\#(A)} \right) = \sum_{r=0}^{n} \left( \sum_{A \in \mathcal{P}_r(X)} (-1)^r \right)
   \]

   \[
   = \sum_{r=0}^{n} \binom{n}{r} (-1)^r = \sum_{r=0}^{n} \binom{n}{r} (-1)^r = (-1 + 1)^n = 0.
   \]
5. (20 pts) Let $\Pi_1$ and $\Pi_2$ be partitions of a set $X$. We say that $\Pi_1$ is finer than $\Pi_2$ if
\[ \forall A \in \Pi_1, \exists B \in \Pi_2 : A \subseteq B. \]
Assume throughout this problem that $\Pi_1$ is finer than $\Pi_2$.
(a) (5 pts) Prove that
\[ \forall A \in \Pi_1, \exists! B \in \Pi_2 : A \subseteq B. \]
Suppose $B, C \in \Pi_2$ satisfy $A \subseteq B, C$.
Then $B \cap C \neq \emptyset$. Since $\Pi_2$ is a partition, this implies that $B = C$.

(b) (5 pts) Let $\sim_1$ be the equivalence relation defined by $\Pi_1$ and let $\sim_2$ be the equivalence relation defined by $\Pi_2$. For an element $a \in X$, we write
\[ [a]_1 = \{x \in X : a \sim_1 x\} \]
\[ [a]_2 = \{x \in X : a \sim_2 x\}. \]
Prove that
\[ \forall a \in X, [a]_1 \subseteq [a]_2. \]
Suppose $b \in [a]_1$. Then $a \sim_1 b$, meaning $A \in \Pi_1$ is the unique set such that $a \in A$,
then $b \in A$. Since $\Pi_1$ is finer than $\Pi_2$, 
\[ \exists B \in \Pi_2 : A \subseteq B. \]
But then $a, b \in A \subseteq B$, so $a \sim_2 b$. This means $b \in [a]_2$. We conclude that $[a]_1 \subseteq [a]_2$. 
(c) (10 pts) Prove that
\[ |X/\sim_1| \geq |X/\sim_2|. \]

We define a map \( f : X/\sim_1 \to X/\sim_2 \)
by \([a]_1 \mapsto [a]_2\). First, we verify that
\( f \) is well-defined. Assume that
\([a]_1 = [b]_1\).

Then \( b \in [a]_1 \subseteq [a]_2 \), so \([a]_2 = [b]_2\).

Now let \([c]_2 \in X/\sim_2\). Then \([c]_1 \in X/\sim_1\)
and \( f([c]_1) = [c]_2 \), which shows that \( f \)
is surjective. Thus,

\[ |X/\sim_1| \geq |X/\sim_2|. \]
6. (15 pts) Suppose that \( a, b \in \mathbb{N} \) with \( \gcd(a, b) = d \). Prove that \( \frac{a}{d} \) and \( \frac{b}{d} \) are coprime.

One can use prime factorization for this problem, but we use an earlier technique. Namely, we use the fact that \( \gcd(a, b) = \min \left( \left\{ am + bn : m, n \in \mathbb{Z} \cap \mathbb{N} \right\} \right) \).

Since \( \gcd(a, b) = d \), \( \exists m_0, n_0 \in \mathbb{Z} : am_0 + bn_0 = d \).

Then \( \frac{a}{d}m_0 + \frac{b}{d}n_0 = 1 \), so

\[
\min \left( \left\{ \frac{a}{d}m + \frac{b}{d}n : m, n \in \mathbb{Z} \cap \mathbb{N} \right\} \right) = 1.
\]

Thus \( \gcd \left( \frac{a}{d}, \frac{b}{d} \right) = 1 \).
7. (15 pts) Suppose that $q > 1$ is a positive integer such that
\[ \forall a, b \in \mathbb{N}, q \mid ab \implies q \mid a \text{ or } q \mid b. \]

Prove that $q$ is prime.

Assume, for a contradiction, that $q$ is composite.

Then $q = ab$ for some $1 < a, b < q$.

But then $q \mid ab$; however $q \nmid a$ since $1 < a < q$

$q \nmid b$ since $1 < b < q$.

This contradicts the stated property of $q$. 
8. (20 pts) Let \( p \) and \( q \) be distinct primes.
(a) (10 pts) Let \( n \in \mathbb{N} \). Prove that
\[
pq \mid n \iff p \mid n \text{ and } q \mid n.
\]

\((\Rightarrow)\) If \( pq \mid n \), then \( pqm = n \) for some \( m \in \mathbb{Z} \).

But then \( p(qm) = n \), so \( p \mid n \)
and \( q(pm) = n \), so \( q \mid n \).

\((\Leftarrow)\) One can use prime factorization, or
\[
p \mid n \Rightarrow dp = n \text{ for some } d \in \mathbb{Z}
\]

since \( q \mid n \) and \( n = dp \), this means \( q \mid dp \).

Since \( q \) is prime, this means \( q \mid d \) or \( q \mid p \).
Since \( p \neq q \) are primes, \( q \nmid p \). Thus, \( q \mid d \)
meaning \( qm = d \) for some \( m \in \mathbb{Z} \).

Then \( n = dp = qmp = pqm \), so \( pq \mid n \).
(b) (10 pts) Prove that
\[ p^{q-1} + q^{p-1} \equiv 1 \mod pq. \]

Hint: You may use the conclusion of part (a) even if you are not able to prove it.

By the first part, we will be done if we can show that
\[ p^{q-1} + q^{p-1} \equiv 1 \mod p \quad \text{and} \quad p^{q-1} + q^{p-1} \equiv 1 \mod q. \]

By Fermat’s little theorem, we know
\[ q^{p-1} \equiv 1 \mod p \quad \text{and} \quad p^{q-1} \equiv 1 \mod q. \]

Clearly
\[ p^{q-1} \equiv 0 \mod p \quad \text{and} \quad q^{p-1} \equiv 0 \mod q. \]

The result now follows.
9. (Bonus, 15 pts) Let \( X \) be a set. Suppose that \( \Pi_1 \) and \( \Pi_2 \) are partitions of \( X \). Let
\[
\Pi = \{ A \cap B : A \in \Pi_1 \text{ and } B \in \Pi_2 \} \subseteq \mathcal{P}(X).
\]
Note that \( \Pi \) is not necessarily a partition since it could be that \( \emptyset \in \Pi \). Prove that \( \Pi \setminus \{ \emptyset \} \) is a partition of \( X \). Note that we are NOT assuming that \( \Pi_1 \) is finer than \( \Pi_2 \) in this problem. However, you should also prove that \( \Pi \) is finer than both \( \Pi_1 \) and \( \Pi_2 \).

We need to verify the three conditions of a partition.

The first one is a freebie: if \( C \in \Pi \setminus \{ \emptyset \} \), then \( C \neq \emptyset \).

Now suppose that \( C_1, C_2 \in \Pi \setminus \{ \emptyset \} \) are distinct \( C_1 \neq C_2 \).

By definition, \( C_1 = A_1 \cap B_1 \) for some \( A_1, A_2 \in \Pi_1 \),
\[ C_2 = A_2 \cap B_2 \]
\( B_1, B_2 \in \Pi_2 \).

Since \( C_1 \neq C_2 \), it must be that \( A_1 \neq A_2 \) or \( B_1 \neq B_2 \).

If \( A_1 \neq A_2 \), then \( A_1 \cap A_2 = \emptyset \) and so \( C_1 \cap C_2 = \emptyset \).

If \( B_1 \neq B_2 \), then \( B_1 \cap B_2 = \emptyset \) and so \( C_1 \cap C_2 = \emptyset \).

Finally, let \( x \in X \). Since \( \Pi_1 \) and \( \Pi_2 \) are partitions,
\[ \exists A \in \Pi_1 : x \in A \]
\[ \exists B \in \Pi_2 : x \in B \]
Then \( x \in A \cap B \in \Pi \setminus \{ \emptyset \} \).

Now suppose that \( C \in \Pi \setminus \{ \emptyset \} \). Then by definition,
\[ C = A \cap B \]
for some \( A \in \Pi_1 \) and \( B \in \Pi_2 \).

Then \( C \subseteq A \) and \( C \subseteq B \), so \( \Pi \) is finer than \( \Pi_1 \) and \( \Pi_2 \).
(ADDITIONAL SPACE FOR WORK, CLEARLY INDICATE THE PROBLEM YOU ARE WORKING ON)
(ADDITIONAL SPACE FOR WORK, CLEARLY INDICATE THE PROBLEM YOU ARE WORKING ON)
(ADDITIONAL SPACE FOR WORK, CLEARLY INDICATE THE PROBLEM YOU ARE WORKING ON)