Your Name	Your Signature
Solutions	

Problem	Total Points	Score
1	10	
2	10	
3	10	
4	10	
5	12	
6	10	
7	16	
8	12	
9	10	
Total	100	

- You have 2 hours.
- If you have a cell phone with you, it should be turned off and put away. (Not in your pocket)
- You may not use a calculator, book, notes or aids of any kind.
- In order to earn partial credit, you must show your work.
- **All proofs on this exam are expected to be concise, mathematically rigorous, and formal.** Thus, you must use of complete sentences, correct grammar and punctuation.
- Unless prescribed by the problem, you may use any proof technique you like; however, *you must explicitly state the method you are using.*

1. (10 points) Suppose $x, y, z \in \mathbb{Z}$ and $x \neq 0$. Use proof by contrapositive to prove that if $x \nmid yz$, then $x \nmid y$ and $x \nmid z$.

Proof: (by contrapositive) We will show that if $x \mid y$ or $x \mid z$, then $x \mid yz$.

Suppose $x \mid y$ or $x \mid z$.

Case 1: Suppose $x \mid y$.
Then by the definition of divides, there exists $k \in \mathbb{Z}$ such that $xk = y$. Multiplying both sides of the previous equation by z, we obtain $xkz = yz$. Since $kz \in \mathbb{Z}$, it follows that $x \mid yz$.

Case 2: Suppose $x \mid z$.
Then by the definition of divides, there exists $k \in \mathbb{Z}$ such that $xk = z$. Multiplying both sides of the previous equation by y, we obtain $xky = yz$. Since $ky \in \mathbb{Z}$, it follows that $x \mid yz$.

Since $x \mid yz$ in both cases, it follows that if if $x \mid y$ or $x \mid z$, then $x \mid yz$.

QUESTION for next time: Was the hypothesis $y, z \in \mathbb{Z}$ necessary?

2. (10 points) Let A, B, and C be sets. Prove that if $A \subseteq B$, $B \subseteq C$ and $C \subseteq A$, then $A = B$.

Proof: (direct) Suppose A, B, and C are sets and that $A \subseteq B$, $B \subseteq C$ and $C \subseteq A$.

In order to show $A = B$, we must show that $A \subseteq B$ and $B \subseteq A$.

Observe that $A \subseteq B$ by hypothesis.

To show $B \subseteq A$, let $b \in B$. Since $B \subseteq C$ and $b \in B$, it follows that $b \in C$. Since $C \subseteq A$ and $b \in C$, it follows that $b \in A$. Since $b \in B$ implies $b \in A$, it follows that $B \subseteq A$.

Since we have shown that $A \subseteq B$ and $B \subseteq A$, we can conclude that $A = B$.

NOTE: Asserting the $B \subseteq C$ and $C \subseteq A$ implies $B \subseteq A$ is not sufficient as we have no theorem or homework problem that asserts this. The same applies to an argument that appeals to the “transitivity of subset.” Clearly the properties being asserted are true, but not because the writer proved them.

3. (10 points) Let n be a positive integer. Use the definition of congruence to prove that if $a \equiv 1 \pmod{n}$, then $a^2 \equiv 1 \pmod{n}$.

Proof: (direct) Suppose n is a positive integer and $a \equiv 1 (\mod n)$, where a is an integer. Then by the definition of congruence, $n \mid (a-1)$. By the definition of divides, it follows that there exists an integer k such that $nk = a - 1$, or equivalently, $a = nk + 1$. Squaring both sides, we obtain $a^2 = (nk+1)^2 = n^2k^2 + 2nk + 1 = (nk^2 + 2k)n + 1$. Consequently, $n(nk^2 + 2k) = a^2 - 1$. Since $nk^2 + 2k \in \mathbb{Z}$, the previous equality implies $n \mid (a^2 - 1)$. Thus, $a^2 \equiv 1(\text{mod } n)$.

4. (10 points) Use induction to prove that $3^1 + 3^2 + 3^3 + \cdots + 3^n = \frac{3^{n+1}-3}{2}$ for every $n \in \mathbb{N}$.

Proof: (by induction on n)

Basis Step: Let $n = 1$. Then the statement in this case is $3^1 = 3 = \frac{6}{2} = \frac{3^{1+1}-3}{2}$, which is true. Thus, the statement holds in this case.

Inductive Step: We must show that if $3^1 + 3^2 + 3^3 + \cdots + 3^n = \frac{3^{n+1}-3}{2}$, then $3^1 + 3^2 + 3^3 + \cdots + 3^n + 3^{n+1} = \frac{3^{n+2}-3}{2}$.

Suppose $3^1 + 3^2 + 3^3 + \cdots + 3^n = \frac{3^{n+1}-3}{2}$. Now, observe

$$\begin{aligned}
3^1 + 3^2 + 3^3 + \cdots + 3^n + 3^{n+1} &= (3^1 + 3^2 + 3^3 + \cdots + 3^n) + 3^{n+1} && \text{associativity} \\
&= \frac{3^{n+1} - 3}{2} + 3^{n+1} && \text{by the inductive hypothesis} \\
&= \frac{3^{n+1} - 3 + 2 \cdot 3^{n+1}}{2} && \text{algebra} \\
&= \frac{3 \cdot 3^{n+1} - 3}{2} \\
&= \frac{3^{n+2} - 3}{2}.
\end{aligned}$$

Thus, if $3^1 + 3^2 + 3^3 + \cdots + 3^n = \frac{3^{n+1}-3}{2}$, then $3^1 + 3^2 + 3^3 + \cdots + 3^n + 3^{n+1} = \frac{3^{n+2}-3}{2}$.

Thus, $3^1 + 3^2 + 3^3 + \cdots + 3^n = \frac{3^{n+1}-3}{2}$ for every $n \in \mathbb{N}$.

5. (12 points) Prove the $9 \mid (4^{3n} + 8)$ for every integer $n \geq 0$.

Proof: (by induction on n)

Base Step: Suppose $n = 0$. Then $4^{3n} + 8 = 4^0 + 8 = 9$, which is divisible by 9. Thus, the statement holds in this case.

Inductive Step: We must show that if $9 \mid (4^{3n} + 8)$ then $9 \mid (4^{3(n+1)} + 8)$.

Suppose $9 \mid (4^{3n} + 8)$. Observe

$$\begin{aligned} 4^{3(n+1)} + 8 &= 4^{3n+3} + 8 \\ &= 64 \cdot 4^{3n} + 8 \\ &= (63 + 1) \cdot 4^{3n} + 8 \\ &= 63 \cdot 4^{3n} + 4^{3n} + 8. \qquad\qquad \text{(equ. 1)} \end{aligned}$$

By the inductive hypothesis, we know $4^{3n} + 8$ is divisible by 9. Thus, there exists an integer k such that $4^{3n} + 8 = 9k$.

Returning to the two ends of equation 1 above, we observe:

$$4^{3(n+1)} + 8 = 63 \cdot 4^{3n} + 4^{3n} + 8 = 9 \cdot 7 \cdot 4^{3n} + 9k = 9(7 \cdot 4^{3n} + k).$$

Since $7 \cdot 4^{3n} + k \in \mathbb{Z}$, the previous string of equalities implies that $9 \mid (4^{3(n+1)} + 8)$. Thus, we have shown that if $9 \mid (4^{3n} + 8)$ then $9 \mid (4^{3(n+1)} + 8)$.

Thus, $9 \mid (4^{3n} + 8)$ for every integer $n \geq 0$.

6. (10 points) Suppose $A = \{(m,n) \in \mathbb{N} \times \mathbb{R} : n = \pi m\}$. Prove $|A| = |\mathbb{N}|$, by using the definition. (That is, find an appropriate map and show it is a bijection.)

Proof: Observe that

$$A = \{(m,n) \in \mathbb{N} \times \mathbb{R} : n = \pi m\} = \{(m, \pi m) : m \in \mathbb{Z}\}.$$

Let $f : \mathbb{N} \to A$ be defined as $f(m) = (m, \pi m)$.

Show f is injective.
Assume $m, n \in \mathbb{N}$, such that $f(m) = f(n)$. Then, by the definition of f, we know $(m, \pi m) = (n, \pi n)$. By equating first coordinates, we obtain $m = n$. Thus, f is injective.

Show f is surjective.
Let $(a,b) \in A$. Then, by the definition of A, $b = \pi a$ and $(a,b) = (a, \pi a)$. Pick $a \in \mathbb{N}$. Now $f(a) = (a, \pi a)$. Thus, f is surjective.

Since $f : \mathbb{N} \to A$ is surjective and injective, f is bijective. Since f is bijective, $|\mathbb{N}| = |A|$.

7. (16 points) Let S be a relation on $\mathbb{R}$ defined as xSy if $x - y \in \mathbb{Z}$.

(a) Explain why $\left(\frac{3}{2}, \frac{7}{2}\right) \in S$ and $\left(\frac{3}{2}, 1\right) \notin S$.

Since $\frac{3}{2} - \frac{7}{2} = -2 \in \mathbb{Z}$, we know $\left(\frac{3}{2}, \frac{7}{2}\right) \in S$.

Since $\frac{3}{2} - 1 = \frac{-1}{2} \notin \mathbb{Z}$, we know $\left(\frac{3}{2}, 1\right) \notin S$.

(b) Show that S is reflexive.

Let $r \in \mathbb{R}$. Then $r - r = 0 \in \mathbb{Z}$. Thus for every $r \in \mathbb{R}$, $(r,r) \in S$. Thus, S is reflexive.

(c) Show that S is transitive.

Suppose $a, b, c \in \mathbb{R}$ such that $(a,b), (b,c) \in S$. By the definition of S, it follows that $a - b, b - c \in \mathbb{Z}$. Since the integers are closed under addition, we know $a - c = (a - b) + (b - c) \in \mathbb{Z}$. Since $a - c \in \mathbb{Z}$, $(a,c) \in S$. Since $(a,b), (b,c) \in S$ implies $(a,c) \in S$, it follows that S is transitive.

(d) The relation S is an equivalence relation. Describe [1], the equivalence class containing 1. You do not need to formally prove your answer is correct.

$[1] = \mathbb{Z}$.

8. (12 points) Let $f : A \to B$ and $g : B \to C$ be functions.

(a) Prove that if $g \circ f : A \to C$ is surjective, then g is surjective.

Proof: Let $f : A \to B$ and $g : B \to C$ be functions such that $g \circ f : A \to C$ is surjective. In order to show that g is surjective, we must show that for every $c \in C$, there exists some $b \in B$, such that $g(b) = c$.

Let c be an arbitrary element of C. Since $g \circ f$ is surjective, from the definition of surjective, there exists an $a \in A$, such that $g(f(a)) = c$. Since $f : A \to B$, $f(a) \in B$. Let $b = f(a)$. Thus $g(b) = g(f(a)) = c$. Since c was arbitrary, we have shown that for every $c \in C$, there exists a $b \in B$ such that $g(b) = c$. Hence, g is surjective.

(b) Give a counterexample to show that if $g \circ f : A \to C$ is surjective, it does *not* necessarily follow that f is surjective.

Let $A = B = \mathbb{R}$ and $C = \{0\}$. Define $f : A \to B$ as $f(x) = x^2$. Define $g : B \to C$ as $g(x) = 0$. We know f is not onto even though $g \circ f$ trivially is.

9. (10 points) Prove or disprove

(a) For all integers m and n, if $m + 2n$ is even, then m and n are both even.

This is false. Pick $m = 2$ and $n = 1$. Then $m + 2n = 2 + 2 \cdot 1 = 4$, which is even. But n is not even. So m and n are not both even.

(b) Let a be any rational number and b by any irrational number, then $a+b$ is irrational.

This is true. We proceed by contradiction. Suppose a is rational, b is irrational, and $a + b = c$ is rational. Then $b = c - a$, the difference of two rational numbers. Since $\mathbb{Q}$ is closed under addition, $b = c - a$ is rational. Now we have the contradiction that b is rational and irrational, which is impossible. Thus, the supposition that c is rational must be incorrect. Thus, c must be irrational.