Math 109. Summer Session I, 2016. Final. (12 points each question; 108 points total)

Instructions:
(1) On blue book: Name, PID, and Section number.
(2) Write clearly and give a reasonable amount of explanation.
(3) \( \mathbb{Z} \) is the set of integers. \( \mathbb{Z}^+ \) is the set of positive integers. \( \mathbb{R} \) is the set of real numbers. \( \mathcal{P}(X) \) denotes the power set of \( X \).

1. Prove by induction that \( n! > 5^n \) for all integers \( n \geq 12 \). You may use that \( 12! = 479001600 \) and \( 5^{12} = 244140625 \). **Ans:** Base case: We have
   \[
   12! = 479001600 > 5^{12} = 244140625.
   \]

   Inductive step: Suppose \( k \geq 12 \) is such that \( k! > 5^k \). Then
   \[
   (k + 1)! = (k + 1) \cdot k! > (k + 1) \cdot 5^k > 5 \cdot 5^k = 5^{k+1}
   \]
   since \( k + 1 > 5 \) follows from \( k \geq 12 \). By induction, we are done.

2. **Universal and existential quantifiers and inequalities.**
   
   (a) (6 points) Prove: \( \forall x \in \mathbb{R}, \exists y \in \mathbb{R}, \sqrt{y} > |x| \) and \( y < x^2 + 1 \). **Ans:** Let \( y = x^2 + \frac{1}{2} \). Then
   \[
   \sqrt{y} = \sqrt{x^2 + \frac{1}{2}} > \sqrt{x^2} = |x| \quad \text{and} \quad y = x^2 + \frac{1}{2} < x^2 + 1.
   \]
   
   (b) (6 points) Prove: \( \exists x \in \mathbb{R}, x > -\frac{1}{2} \) and \( \forall y \in \mathbb{R}, y^4 - y^2 > x \). **Ans:** Let \( x = -\frac{3}{8} \). Then
   \[
   x = -\frac{3}{8} > -\frac{1}{2}. \quad \text{Let } y \in \mathbb{R}. \quad \text{Then } y^4 - y^2 = (y^2 - \frac{1}{2})^2 - \frac{1}{4} \geq -\frac{1}{4} > -\frac{3}{8} = x.
   \]

3. Let \( X \) and \( Y \) be nonempty disjoint sets. Define \( f : \mathcal{P}(X) \times \mathcal{P}(Y) \rightarrow \mathcal{P}(X \cup Y) \) by \( f(A, B) = A \cup B \) for \( A \in \mathcal{P}(X) \) and \( B \in \mathcal{P}(Y) \).
   
   (a) (6 points) Prove that \( f \) is a surjection. **Ans:** Let \( C \in \mathcal{P}(X \cup Y) \). Then \( C \subseteq X \cup Y \). Define \( A = C \cap X \) and \( B = C \cap Y \). Then
   \[
   f(A, B) = A \cup B = (C \cap X) \cup (C \cap Y) = C \cap (X \cup Y) = C.
   \]
   Hence \( f \) is a surjection.
   
   (b) (6 points) Prove that \( f \) is an injection. **Ans:** Suppose that \( A_1, A_2 \in \mathcal{P}(X) \) and \( B_1, B_2 \in \mathcal{P}(Y) \) are such that \( f(A_1, B_1) = f(A_2, B_2) \). Then \( A_1 \cup B_1 = A_2 \cup B_2 \). Hence
   \[
   A_1 = X \cap (A_1 \cup B_1) = X \cap (A_2 \cup B_2) = A_2.
   \]
   Here we used that \( A_1, A_2 \subseteq X, B_1, B_2 \subseteq Y \), and \( X \cap Y = \emptyset \), which implies
   \[
   X \cap (A_1 \cup B_1) = (X \cap A_1) \cup (X \cap B_1) = A_1 \cup \emptyset = A_1
   \]
   and similarly, \( X \cap (A_2 \cup B_2) = A_2 \). Similarly, we have
   \[
   B_1 = Y \cap (A_1 \cup B_1) = Y \cap (A_2 \cup B_2) = B_2.
   \]

4. Let \( A, B, \) and \( C \) be sets. Define \( A \Delta B = \{ x \mid x \in A \cup B \text{ and } x \notin A \cap B \} \).
(a) (6 points) Prove that if \( x \in A \cap (B \Delta C) \), then \( x \in (A \cap B) \Delta (A \cap C) \).  
**Ans:** Let \( x \in A \cap (B \Delta C) \). Then 
\[
x \in A \text{ and } x \in B \cup C \text{ and } x \notin B \cap C.
\]
So 
\[
x \in A \cap (B \cup C) = (A \cap B) \cup (A \cap C)
\]
and 
\[
x \notin A \cap (B \cap C) = (A \cap B) \cap (A \cap C).
\]
That is, 
\[
x \in (A \cap B) \Delta (A \cap C).
\]
(b) (6 points) Prove that if \( x \in (A \cap B) \Delta (A \cap C) \), then \( x \in A \cap (B \Delta C) \).  
**Ans:** Let \( x \in (A \cap B) \Delta (A \cap C) \). Then 
\[
x \in (A \cap B) \cup (A \cap C) = A \cap (B \cup C)
\]
and 
\[
x \notin (A \cap B) \cap (A \cap C) = A \cap (B \cap C).
\]
Thus 
\[
x \in A \text{ and } x \in B \cup C \text{ and } x \notin A \cap (B \cap C).
\]
Since \( x \in A \), the last part of the statement is equivalent to \( x \notin B \cap C \). We conclude that \( x \in A \cap (B \Delta C) \).

5. Recall the following fact (do not prove): If \( x, y, z \) are positive integers such that \( x \) divides \( yz \) and \( \gcd(x, y) = 1 \), then \( x \) divides \( z \).

(a) (6 points) Suppose that \( a \) is a positive integer such that \( 9 \) divides \( 6a \). Prove that \( 3 \) divides \( a \).  
**Ans:** Since \( 9 \) divides \( 6a \), we have \( 3 \) divides \( 2a \). Since \( \gcd(3, 2) = 1 \), by the result above, this implies \( 3 \) divides \( a \).

(b) (6 points) Prove that if \( a \) is a positive integer such that \( 2 \) divides \( a \) and \( 3 \) divides \( a \), then \( 6 \) divides \( a \).  
**Ans:**

6. **Using the fact stated at the beginning of Problem 5.**

(a) (6 points) Prove that if a prime \( p \) divides \( a^2 \), where \( a \) is a positive integer, then \( p \) divides \( a \).  
**Ans:** Since \( p \) is a prime, \( \gcd(p, a) = 1 \) or \( \gcd(p, a) = p \). If \( \gcd(p, a) = p \), then \( p \) divides \( a \) and we are done. If \( \gcd(p, a) = 1 \), then by the result of \#5 and \( p \) divides \( a \cdot a \), we conclude that \( p \) divides \( a \).

(b) (6 points) Suppose that \( a \) is a positive integer such that \( \gcd(a, 3) = 1 \). Prove that \( \sqrt{3a} \) is irrational.  
**Ans:** Suppose that \( \sqrt{3a} \) is rational. Then there exists integers \( m \) and \( n \) with \( 3a = \frac{m^2}{n^2} \), where \( \gcd(m, n) = 1 \). So \( 3an^2 = m^2 \), which implies \( 3 \) divides \( m^2 \). Since \( 3 \) is prime, this implies \( 3 \) divides \( m \). Hence there exists an integer \( k \) such that \( m = 3k \). Thus \( 3(3k^2) = 3an^2 \), that is, \( 3k^2 = an^2 \). Since \( \gcd(a, 3) = 1 \) and \( 3 \) divides \( an^2 \), we conclude that \( 3 \) divides \( n^2 \). Thus \( \gcd(m, n) \geq 3 \), a contradiction.

7. **Linear congruences.**
(a) (6 points) Find a complete set of solutions to \(12x \equiv 18 \mod 27\) that are distinct modulo 27. If the set of solutions is empty, explain why. **Ans:** Since \(\gcd(6, 27) = 1\), the congruence equation is equivalent to \(2x \equiv 3 \mod 9\). This is equivalent to \(2x \equiv 12 \mod 9\), which is equivalent to \(x \equiv 6 \mod 9\). A complete set of solutions that are distinct modulo 27 is 6, 15, 24.

(b) (6 points) Find a complete set of solutions to \(21x \equiv 17 \mod 35\) that are distinct modulo 35. If the set of solutions is empty, explain why. **Ans:** There are no solutions because \(\gcd(21, 35) = 3\) does not divide 17.


(a) (10 points) Prove that for any integer \(n\), we have that \(n^3\) is not congruent to 2 modulo 4, i.e., \(n^3 \not\equiv 2 \mod 4\). **Hint:** Use the division theorem for dividing by 4 and use basic properties of congruence. **Ans:** Let \(n \in \mathbb{Z}\). By the division theorem, there exists \(k, \ell \in \mathbb{Z}\) such that one of the following is true:

\[
\begin{align*}
\text{(i)} & \quad n^3 = (4k)^3 \equiv 0 \mod 4, \\
\text{(ii)} & \quad n^3 = (4k + 1)^3 \equiv 1 \mod 4, \\
\text{(iii)} & \quad n^3 = (4k + 2)^3 \equiv 2^3 \equiv 0 \mod 4, \\
\text{(iv)} & \quad n^3 = (4k + 3)^3 \equiv 27 \equiv 3 \mod 4.
\end{align*}
\]

Hence \(n^3\) is congruent to 0, 1, or 3 mod 4. In particular, \(n^3 \not\equiv 2 \mod 4\).

(b) (2 points) Use part (a) to show that 8888890 is not the cube of an integer. **Ans:**

\[
8888890 = 1111110 \cdot 8 + 2,
\]

so 8888890 \(\equiv 2 \mod 4\), which implies that 8888890 is not the cube of an integer by part (a).

9. Let \(m\) be a positive integer. Let the universal set be the set of integers \(\mathbb{Z}\).

(a) (6 points) Prove (directly) that if \(a_1 \equiv a_2 \mod m\) and \(b_1 \equiv b_2 \mod m\), then \(a_1 - b_1 \equiv a_2 - b_2 \mod m\). **Ans:** Suppose \(a_1 \equiv a_2 \mod m\) and \(b_1 \equiv b_2 \mod m\). Then there exist integers \(k, \ell \in \mathbb{Z}\) such that

\[
\begin{align*}
a_1 - a_2 &= km, \\
b_1 - b_2 &= \ell m.
\end{align*}
\]

Thus

\[
(a_1 - b_1) - (a_2 - b_2) = (a_1 - a_2) - (b_1 - b_2) = (k - \ell) m.
\]

This proves \(a_1 - b_1 \equiv a_2 - b_2 \mod m\).

(b) (6 points) Given \(a \in \mathbb{Z}\), let \([a]_m = \{x \in \mathbb{Z} | x \equiv a \mod m\}\) denote the congruence class of \(a\) modulo \(m\). Prove that if \(a, b \in \mathbb{Z}\) are such that \([a]_m \cap [b]_m \neq \emptyset\), then \(a \equiv b \mod m\). **Ans:** Suppose that \(a, b \in \mathbb{Z}\) are such that \([a]_m \cap [b]_m \neq \emptyset\). Then there exists \(c \in [a]_m \cap [b]_m\), so that there exist integers \(k, \ell \in \mathbb{Z}\) such that

\[
c - a = km, \quad c - b = \ell m.
\]

Thus

\[
a - b = c - km - c + \ell m = (\ell - k) m.
\]

This proves \(a \equiv b \mod m\).