Homework 10

- Please submit your answers to all questions.
- We will mark your answers to 3 questions.
- We will provide you with full solutions to all questions.

1. Prove that there is no integer a so that $a \equiv 2 \pmod 6$ and $a \equiv 7 \pmod 9$.

   Proof. Suppose such an integer a exists. Then the first congruence implies that $a = 6k + 2$ for some integer k. Similarly, the second congruence implies that $a = 9l + 7$ for some integer l. Thus we have

   $$6k + 2 = 9l + 7$$

   or, equivalently

   $$6k - 9l = 5.$$

   This gives a contradiction since $3|6k + 9l = 3(2k + 3l)$ but $3 \nmid 5$. □

2. Prove that the equation $5y^2 - 4x^2 = 7$ has no integer solutions.
   Hint: Consider the equation modulo 4.

   Proof. Suppose there are integers x and y satisfying $5y^2 - 4x^2 = 7$. Then

   $$\begin{aligned} 5y^2 - 4x^2 &\equiv 7 \mod 4 \\ 1y^2 - 0x^2 &\equiv 3 \mod 4 \\ y^2 &\equiv 3 \mod 4 \end{aligned}$$

   However, we can see the square of any integer is equivalent to either 0 or 1 modulo 4.
   Case 1 If $y \equiv 0 \mod 4$, then $y^2 \equiv 0^2 \equiv 0 \mod 4$.
   Case 2 If $y \equiv 1 \mod 4$, then $y^2 \equiv 1^2 \equiv 1 \mod 4$.
   Case 3 If $y \equiv 2 \mod 4$, then $y^2 \equiv 2^2 \equiv 0 \mod 4$.
   Case 4 If $y \equiv 3 \mod 4$, then $y^2 \equiv 3^2 \equiv 1 \mod 4$.
   This is a contradiction. Hence, the equation has no integer solutions.

   □

3. Let $f : X \to Y$ be a function. Suppose that f admits an inverse function.

   (a) Prove the inverse function is unique.

   (b) Let $g : Y \to Z$ be another function with an inverse. Show that the inverse function of $g \circ f$ is given by $f^{-1} \circ g^{-1}$

   Proof. To show a), we suppose g and h are both inverse functions of f. Then

   $$\begin{aligned} g \circ f = h \circ f &= i_X \\ f \circ g = f \circ h &= i_Y, \end{aligned}$$

where i_A is the identity function on the set A.

By above equalities and associativity, we have

$$g = g \circ i_Y = g \circ (f \circ h) = (g \circ f) \circ h = i_X \circ h = h.$$

By a), both f and g admit a unique inverse function, say f^{-1} and g^{-1}. Then

$$(f^{-1} \circ g^{-1}) \circ (g \circ f) = f^{-1} \circ (g^{-1} \circ g) \circ f = f^{-1} \circ i_Y \circ f = f^{-1} \circ f = i_X$$
$$(g \circ f) \circ (f^{-1} \circ g^{-1}) = g \circ (f \circ f^{-1}) \circ g^{-1} = g \circ i_Y \circ g^{-1} = g \circ g^{-1} = i_Z.$$

Thus $f^{-1} \circ g^{-1}$ is the inverse function of $g \circ f$. □

4. Prove that $\sqrt[3]{25}$ is irrational.

   Proof. Assume that $\sqrt[3]{25} \in \mathbb{Q}$. Then we can write $\sqrt[3]{25} = a/b$ for some $a, b \in \mathbb{Z}$, $\gcd(a, b) = 1$. Then $25 = a^3/b^3$, so $25b^3 = a^3$. Therefore $25 \mid a^3$, so $5 \mid a^3$ and since 5 is prime, we have $5 \mid a$.

   We write $a = 5a'$. Then we substitute into the above equation to get $25b^3 = 125a'^3$. This implies $b^3 = 5a'^3$, so $5 \mid b^3$. Therefore $5 \mid b$. This is a contradiction on $\gcd(a, b) = 1$. So $\sqrt[3]{25} \notin \mathbb{Q}$. □

5. Let $n \in \mathbb{N}$. Suppose that n is a perfect square; that is $n = m^2$ for some $m \in \mathbb{Z}$. Show that $2n$ is not a perfect square.

   Proof. Since n is a perfect square we have $n = k^2$ for some integer k. Assume that $2n$ is a perfect square as well so that $2n = \ell^2$. Then $2n = \ell^2 = 2k^2$ so that $2 = \frac{\ell^2}{k^2}$. Taking the square root we get $\sqrt{2} = \frac{\ell}{k}$ which entails that $\sqrt{2}$ is rational. This is a contradiction. Hence $2n$ is not a perfect square. □