Maths Assignment - 1081

z5417727

October 14, 2022

Contents

1 Question 1

1.1 a)

Prove that in modulo 9, it is not possible for a perfect square to be congruent to $2, 3, 5, 6$ or 8.

Proposition: For any integer $n \in \mathbb{Z}$, we say that $n^2 \equiv 0, 1, 4, 7(\mod 9)$.

Proof: This can be deduced by finding the squares of $0, 1, 2, 3, 4$ respectively.

$$0^2 \equiv 0(\text{mod } 9),$$

$$1^2 \equiv 1(\text{mod } 9),$$
$$2^2 \equiv 4(\text{mod } 9),$$
$$3^2 \equiv 0(\text{mod } 9),$$
$$4^2 \equiv 7(\text{mod } 9).$$

Through finding the modulo of 9, we find the similar rule applied to 5 through 8 (since $9^2 \equiv 0(\mod 9)$).

$$5^2 \equiv (-4)^2 \equiv 7(\text{mod } 9),$$

$$6^2 \equiv (-3)^2 \equiv 0(\text{mod } 9),$$
$$7^2 \equiv (-2)^2 \equiv 4(\text{mod } 9),$$
$$8^2 \equiv (-1)^2 \equiv 1(\text{mod } 9).$$

Here, we see that the modulo of perfect squares always end with the digits $0, 1, 4$ and 7. Thus, it can be proved that in modulo 9, it is not possible for a perfect square to be congruent to $2, 3, 5, 6,$ or 8.

1.2 b)

Hence (and not otherwise) prove that there do not exist three consecutive integer values of n for which $41n + 39$ is a perfect square.

Consider a number $n-1$, n and $n+1$ for $n \in \mathbb{Z}$. Then, we see that the numbers are:

$$41(n-1)+39, 41(n)+39, 41(n+1)+39.$$

Proposition For $41(n-1)+39, 41(n)+39$ and $41(n+1)+39$ to be perfect squares, they should not be congruent to $2, 3, 5, 6$ or 8 in modulo 9 (this is proved in q1 (a)).

Proof Consider $41n + 39$ as a perfect square.

$$41n + 39 \text{ as a perfect square } \Rightarrow 41n + 39 = k^2, \text{ where } k \in \mathbb{Z}.$$

Here, we can use the proof from q1 (a) to deduce that k^2 mod 9 would give $0, 1, 4$ or 7 as the remainder since it is a perfect square.

However, when we check the number $41(n-1)+39$,

$$\Rightarrow 41n - 41 + 39,$$

$$\Rightarrow (41n + 39) - 41,$$

$$\Rightarrow k^2 - 41.$$

Thus, we can consider the modulo of 9 for $k^2 + 41$:

$$\Rightarrow (k^2 - 41)(\text{mod } 9),$$

$$\Rightarrow (k^2(\text{mod } 9) - 41(\text{mod } 9))(\text{mod } 9).(\text{modular subtraction})$$

Here, we know that $41 \equiv 5(\text{mod } 9)$, and k^2 gives a remainder of either $0, 1, 4, 7$. Consider each of the cases individually:
1) $k^2 \equiv 0(\text{mod } 9)$:

$$\Rightarrow (k^2(\text{mod } 9) - 41(\text{mod } 9))(\text{mod } 9).$$

$$\Rightarrow (0 - 5)(\text{mod } 9),$$

$$\Rightarrow -5(\text{mod } 9),$$

$$\Rightarrow -5.$$

Since the $(k^2 - 41) \equiv -5(\text{mod } 9)$, this means that it is not a perfect square (as proven in q1 a)).
2) $k^2 \equiv 1(\text{mod } 9)$:

$$\Rightarrow (k^2(\text{mod } 9) + 41(\text{mod } 9))(\text{mod } 9).$$

$$\Rightarrow (1 - 5)(\text{mod } 9),$$

$$\Rightarrow -4(\text{mod } 9),$$

$$\Rightarrow -4.$$

Since the $(k^2 - 41) \equiv -4(\text{mod } 9)$, this means that it is not a perfect square (as proven in q1 a)).
3) $k^2 \equiv 4(\text{mod } 9)$:

$$\Rightarrow (k^2(\text{mod } 9) - 41(\text{mod } 9))(\text{mod } 9).$$
$$\Rightarrow (4-5)(\text{mod } 9),$$
$$\Rightarrow -1(\text{mod } 9),$$
$$\Rightarrow -1.$$

Since the $(k^2-41) \equiv 0(\text{mod } 9)$, this means that it is not a perfect square (as proven in q1 a)).
4) $k^2 \equiv 7(\text{mod } 9)$:

$$\Rightarrow (k^2(\text{mod } 9) - 41(\text{mod } 9))(\text{mod } 9).$$
$$\Rightarrow (7-5)(\text{mod } 9),$$
$$\Rightarrow 2(\text{mod } 9),$$
$$\Rightarrow 2.$$

Since the $(k^2-41) \equiv 2(\text{mod } 9)$, this means that it is not a perfect square (as proven in q1 a)).
We see that for each case, $41(n-1)+39$ can never be a perfect square if $41n+39$ is a perfect square.

Therefore, we can say that there do not exist three consecutive integer values of n for which $41n+39$ is a perfect square.

2 Question 2

A certain relation $\star$ is defined on the set $\mathbb{Z}^+$ by:

$$x \star y \textbf{ if and only if every factor of } x \textbf{ is a factor of } y.$$

For each of the questions below, be sure to provide a proof supporting your answer.

2.1 a)

Is $\star$ reflexive?

Theorem: If $\star$ is to be reflexive, then $x \sim x$.

[not done yet]

2.2 b)

Is $\star$ symmetric?

Theorem: If $\star$ is symmetric, then $x \sim y \leftrightarrow y \sim x$.

[not done yet]

2.3 c)

Is $\star$ anti-symmetric?

Theorem: If a set $A \leq B, B \leq A \rightarrow A = B$.

[not done yet]

2.4 d)

Is $\star$ transitive?

If a set $A \leq B, B \leq C \rightarrow A \leq C$.

[not done yet]

2.5 e)

Is $\star$ an equivalence relation, a partial order, both or neither?

[not done yet]

3 Question 3

Consider the two functions $f : X \to Y$ and $g : Y \to Z$ for non-empty sets X, Y, Z. Decide whether each of the following statements is true or false, and prove each claim.

3.1 a)

If $g \circ f$ is injective, then g is injective.

Counterexample

Consider sets $X = \{1\}, Y = \{2, 3\}, Z = \{4\}$.

Function $g \circ f$ implies that $g \circ f : X \to Z$ (since $f : X \to Y$ and $g : Y \to Z$). Therefore, $g(f(1)) = 4$. This makes it an injective function as it is one to one.

However, for the function g, $g(2) = g(3) = 4$, making the function non-injective.

Therefore, by a counterexample, we can conclude that the statement is false.

3.2 b)

If $g \circ f$ is injective, then f is injective.

Proof: Suppose f is not injective. Since $f : X \to Y$, we take two numbers $x_1, x_2 \in \mathbb{Z}$, where x_1, x_2 are in the set X and $f(x_1)$ and $f(x_2)$ are in set Y, giving:

$$f(x_1) = f(x_2) \text{ when } x_1 \neq x_2,$$

Similarily, since $g : Y \to Z$, this would imply that:

$$(g \circ f)(x_1) = (g \circ f)(x_2) \text{ when } f(x_1) \neq f(x_2) \text{ ie,}$$

$$g(f(x_1)) = g(f(x_2)) \text{ when } f(x_1) \neq f(x_2).$$

Since $f(x_1), f(x_2) \in Y$ and $g(f(x_1)) = g(f(x_2)) \in Z$, we can consider that this proves the statement " if f is not injective, then $g \circ f$ is not injective".

Therefore, by contrapositive, we can conclude that if $g \circ f$ is injective then f is injective.

3.3 c)

If $g \circ f$ is injective and f is surjective, then g is injective

Proof Consider two variables $y_1, y_2 \in Y$. such that $g(y_1) = g(y_2).[y_1, y_2 \in \mathbb{R}]$

Since f is known to be surjective, we can consider two other variables $x_1, x_2 \in X[x_1, x_2 \in \mathbb{R}]$.

Then, if we map f to g, using this surjective nature of f, we can presume $f(x_1) = y_1, f(x_2) = y_2$. With this, the proof follows:

$$\Rightarrow g(f(x_1)) = g(f(x_2)),$$

$$\Rightarrow g \circ f(x_1) = g \circ f(x_2),$$

where $x_1 = x_2$ because $g \circ f$ is injective (given in question).
Then,

$$\Rightarrow f(x_1) = f(x_2),$$

$$\Rightarrow y_1 = y_2.$$

Thus, $g(y_1) = g(y_2) \Rightarrow y_1 = y_2$, which means g is injective.

Therefore, we can conclude that if $g \circ f$ is injective and f is surjective, then g is injective.