Proposition 2. *If $a \in \mathbb{Z}$, then $4 \nmid (a^2 - 3)$*

Proof. Because $a \in \mathbb{Z}$, a could be either odd or even, so we need multiple cases.

Case 1: a is odd. By definition, there exists $b \in \mathbb{Z}$ such that $a = 2b+1$. It follows that $a^2 = (2b+1)^2 = 4b^2 + 4b + 1$. Then, $a^2 \equiv 1 \mod 4$ and $3 \equiv 3 \mod 4$. As we can see, a^2 and 3 do not have the same congruence class (mod 4). So, a^2 does not have the same congruence class as 3 (mod 4). Thus, $4 \nmid a^2 - 3$.

Case 2: a is even. By definition, there exists $c \in \mathbb{Z}$ such that $a = 2c$. Consequently, $a^2 = (2c)^2 = 4c^2$. Using modular congruence, we can see that $a^2 \equiv 0 \mod 4$ and $3 \equiv 3 \mod 4$ We can see that a^2 and 3 do not have the same congruence class (mod 4). So, a^2 does not equal 3 (mod 4). Thus, $4 \nmid a^2 - 3$.

As we can see in both cases, $4 \nmid a^2 - 3$. Therefore, we can conclude that no matter the parity of a, $4 \nmid a^2 - 3$.

□

Comments:

Lemma 1. *If $a \in \mathbb{Z}$, then $a^2 \in \mathbb{Z}$*

Proposition 2. *If $a \in \mathbb{Z}$, then $4 \nmid (a^2 - 3)$.*

Proof. Suppose $4|(a^2 - 3)$ by contradiction. This means that there exists $b \in \mathbb{Z}$ such that $a^2 - 3 = 4b$ by definition. This then brings up 2 cases:

Case 1: Suppose $a \in \mathbb{Z}$ and a is even. Since a is even, then there exists $c \in \mathbb{Z}$ such that $a = 2c$ by definition. So then, $(2c)^2 - 3 = 4b$, thus $4c^2 - 3 = 4b$, and then $4(c^2 - b) = 3$. It continues that $c^2 - b = \frac{3}{4}$, and finally $b = c^2 - \frac{3}{4}$. Since $c \in \mathbb{Z}$, then $c^2 \in \mathbb{Z}$ by Lemma 1. Also, $\frac{3}{4} \notin \mathbb{Z}$ by the definition of an integer, then it follows that $b \notin \mathbb{Z}$. This is a contradiction of the assumption that $b \in \mathbb{Z}$, so $4 \nmid (a^2 - 3)$ when a is even.

Case 2: Suppose $a \in \mathbb{Z}$ and a is odd. Since a is odd, then there exists $d \in \mathbb{Z}$ such that $a = 2d + 1$ by definition. So then $(2d+1)^2 - 3 = 4b$, and then $4d^2 + 4d - 2 = 4b$, thus $2d^2 + 2d - 1 = 2b$. It continues that $2(d^2 + d - \frac{1}{2}) = 2b$, and finally $d^2 + d - \frac{1}{2} = b$. Since $d \in \mathbb{Z}$, then $d^2 \in \mathbb{Z}$ by Lemma 1. Therefore, $d^2 + d \in \mathbb{Z}$. Also, $\frac{1}{2} \notin \mathbb{Z}$ by the definition of an integer, then it follows that $b \notin \mathbb{Z}$. This is a contradiction of the assumption that $b \in \mathbb{Z}$, so $4 \nmid (a^2 - 3)$ when a is odd.

Conclusion: Since $4 \nmid (a^2 - 3)$ when a is either even or odd, therefore $4 \nmid (a^2 - 3)$ when $a \in \mathbb{Z}$. □

Comments:

Theorem 2. *If $a \in \mathbb{Z}$, then $4 \nmid (a^2 - 3)$.*

Proof. For the sake of contradiction, assume that $a \in \mathbb{Z}$ and $4 \mid (a^2 - 3)$. By the definition of divides, there exists some integer k such that, $4k = a^2 - 3$. This can be broken into two cases in which a is odd or a is even.

Case 1. a is odd. By the definition of odd, there exists some integer i such that, $a = 2i + 1$. Using this value in $4k = a^2 - 3$ we find, $4 = (2i + 1)^2 - 3$. This can then be written as, $4k = 4i^2 + 4i - 2$. Then factoring out a 4 shows, $k = i^2 + i - \frac{1}{2}$. However, $i^2 + i$ is an integer but, $\frac{1}{2}$ is rational. So, $i^2 + i - \frac{1}{2}$ is not an integer. This contradicts that k is an integer.

Case 2. a is even. By the definition of even, there exists some integer n such that, $a = 2n$. Using this value in $4k = a^2 - 3$ we find, $4 = (2n)^2 - 3$. This can then be written as, $4k = 4n^2 - 3$. Then factoring out a 4 shows, $k = n^2 - \frac{3}{4}$. However, n^2 is an integer but, $\frac{3}{4}$ is rational. So, $n^2 - \frac{3}{4}$ is not an integer. This contradicts that k is an integer.

Therefore by contradiction, $4 \nmid (a^2 - 3)$ for all $a \in \mathbb{Z}$. □

Comments:

Proposition. If $a \in \mathbf{Z}$, then $4 \not| (a^2 - 3)$.

Proof by contradiction. Assume that $4|(a^2 - 3)$ for some $a \in \mathbf{Z}$. Then by definition, $4n = (a^2 + 3)$ for some integer n. We then have to consider two cases.

Case 1: Consider than a is even. Then by definition, there exists an integer k such that $a = 2k$. So $4n = (2k)^2 + 3$ which can also be written as $4n = 4k^2 - 3$. Thus $n = k^2 - \frac{3}{4}$. Since, $\frac{3}{4}$ is not an integer, n is not an integer. This is a contradiction.

Case 2. Consider that a is odd. Then by definition, there exists an integer m such that $a = 2m + 1$. So $4n = (2m + 1)^2 + 3 = (4m^2 + 4m + 1) - 3 = 4m^2 + 4m - 2$. Dividing by 4, we get $n = m^2 + m - \frac{1}{2}$. Since $\frac{1}{2}$ is not an integer, n is not an integer. This is a contradiction.

Therefore, if $a \in \mathbf{Z}$, then $4 \not| (a^2 - 3)$.

■

Comments:

Proposition 2. *Let $a \in \mathbb{Z}$, if $a \in \mathbb{Z}$, then $4 \nmid a^2 - 3$*

$$\forall a \in \mathbb{Z},\ \nexists c\colon 4c = a^2 - 3$$

Definition 1 (Divides)**.** Let $a, b \in \mathbb{Z}$
a divides b, written $a|b$, if there is $c \in \mathbb{Z}$ such that ac = b.

Definition 2 (Even)**.** Let $a \in \mathbb{Z}$
a is even if $a = 2(k)$ for some $k \in \mathbb{Z}$

Definition 3 (Odd)**.** Let $a \in \mathbb{Z}$
a is odd if $a = 2(k) + 1$ for some $k \in \mathbb{Z}$

Proof. let $a \in \mathbb{Z}$ Suppose that $4|a^2 - 3$, so $\exists c \in \mathbb{Z} : 4c = a^2 - 3$ by the definition of divides (Definition 1).
Case 1: Let a be odd, then by the definition of odd (Definition 3), $a = 2k + 1, k \in \mathbb{Z}$ It follows that $a^2 - 3 = (2k+1)(2k+1) - 3 = 4k^2 + 4k - 2$. If $4|a^2 - 3$, $4c = 4k^2 + 4k - 2$, and $4c = 2(2(k^2 - k) - 1)$, so $2c = 2(k^2 - k) - 1$ so $c = k^2 - k - 1/2$. Furthermore, because the integers are closed under multiplication and subtraction, $(k^2 - k) \in \mathbb{Z}$. Because $1/2$ is a rational number and not an integer, $4 \notin \mathbb{Z}$ and therefore $c \nmid a^2 - 3$ when a is odd by the definition of divides (Definition 1).
Case 2: Let a be odd, then by the definition of even (Definition 2), $a = 2k, k \in \mathbb{Z}$ It follows that $a^2 - 3 = (2k)^2 - 3 = 4k^2 - 3$. If $4|a^2 - 3$, $4c = 4k^2 - 3$, and $c = k^2 - 3/4$. Since integers are closed under multiplication, $k^2 \in \mathbb{Z}$. Because $3/2$ is a rational number and not an integer, $c \notin \mathbb{Z}$ and therefore $4 \nmid a^2 - 3$ when a is even by the definition of divides (Definition 1).
By Case 1 and Case 2, $4 \nmid a^2 - 3$ when a is odd or when a is even, but this contradicts our assumption that $\exists a \in \mathbb{Z} : 4|a^2 - 3$ so if $a \in \mathbb{Z}$, then $4 \nmid a^2 - 3$ ∎

Comments:

Proposition 2. *If $x \in \mathbb{Z}$ then $4 \nmid (a^2 - 3)$.*

Proof. Suppose, by way of contradiction, that $4 \mid (a^2 - 3)$.
By definition $\exists m \in \mathbb{Z}$ such that $4m = a^2 - 3$.

Case 3. a is even.
By definition, $\exists k \in \mathbb{Z}$ such that $a = 2k$.
Then

$$(2k)^2 - 3 = 4m$$
$$4k^2 - 3 = 4m$$
$$k^2 - \frac{3}{4} = m$$

Since $\frac{3}{4} \notin \mathbb{Z}$, $k^2 - \frac{3}{4} \notin \mathbb{Z}$, which is a contradiction since $m \in \mathbb{Z}$.

Case 4. a is odd.
By definition, $\exists k \in \mathbb{Z}$ such that $a = 2k + 1$.
Then

$$(2k+1)^2 - 3 = 4m$$
$$4k^2 + 4k + 1 - 3 = 4m$$
$$4k^2 + 4k - 2 = 4m$$
$$k^2 + k - \frac{1}{2} = m$$

Hence $k^2 + k \in \mathbb{Z}$ due to integers being closed under addition, but $\frac{1}{2} \notin \mathbb{Z}$, so $k^2 + k - \frac{1}{2} \notin \mathbb{Z}$, which is a contradiction since $m \in \mathbb{Z}$.

Therefore, in both cases contradiction shows if $x \in \mathbb{Z}$ then $4 \nmid (a^2 - 3)$. □

Comments:

Proposition 2. *If $a \in \mathbb{Z}$, then $4 \nmid (a^2 - 3)$.*

Proof. We will prove this by contradiction. Let $a \in \mathbb{Z}$ and suppose $4 \mid (a^2 - 3)$. Then, for some integer x, $(a^2 - 3) = 4x$. We can break this into two cases.

Case 1: a is even.

By definition, there is an integer m where $a = 2m$. Then $(2m)^2 - 3 = 4x$. Thus $4m^2 - 3 = 4x$. $4m^2 - 3$ is odd because $4m^2$ must be even and subtracting 3 results in an odd number. $4x$ is even because $2(2x)$ and by the definition of even. This is a contradiction because $4m^2 - 3$ is odd and $4x$ is even.

Case 2: a is odd.

By definition, there is an integer n where $a = 2n+1$. Then $(2n+1)^2 - 3 = 4x$. Thus $4n^2 + 4n + 1 - 3 = 4x$. Hence $4n^2 + 4n - 2 = 4x$. Dividing both sides by 4 leads to $n^2 + n - \frac{1}{2} = x$. This is a contradiction because $n^2 + n - \frac{1}{2}$ cannot be an integer while x is an integer.

Since we proved that $4 \nmid (a^2 - 3)$ for a is even and a is odd, we know that $4 \nmid (a^2 - 3)$ for a beings all integers. Therefore, $4 \nmid (a^2 - 3)$. $\square$

Comments:

Theorem 2. *If $a \in \mathbb{Z}$, then $4 \not| (a^2 - 3)$.*

Lemma 2. *Let $a \in \mathbb{Z}$ a^2 is odd if and only if a is odd (this was proved in class).*

Proof. Let $a \in \mathbb{Z}$ and suppose, by way of contradiction, that $4|(a^2 - 3)$.

By definition, there exists $b \in \mathbb{Z}$ such that $4b = a^2 - 3$

This is equivalent to $a^2 = 4b+3 = 4b+2+1 = 2(2b+1)+1$. Because $b \in \mathbb{Z}$, we can see that $2(2b+1)+1$ is odd, and thus a^2 is odd. By Lemma 1, we can see that a is odd.

By definition, there exists $c \in \mathbb{Z}$ such that $a = 2c + 1$. Substituting $a = 2c + 1$ in the above equation, we can see that $0 = a^2 - 4b - 3 = (2c+1)^2 - 4b - 3 = 4c^2 + 4c + 1 - 4b - 3 = 4c^2 + 4c - 4b - 2$.

From this, we can see that $2 = 4c^2 + 4c - 4b$ and $1 = 2c^2 + 2c - 2b = 2(c^2 + c - b)$. Because $b, c \in \mathbb{Z}$ we can see that $2(c^2 + c - b)$ is even. This is a contradiction because 1 is odd.

Therefore, we can see $4 \not| (a^2 - 3)$. □

Comments:

Proposition 2. *If $a \in \mathbb{Z}$, then $4 \nmid (a^2 - 3)$.*

Proof. Let $a \in \mathbb{Z}$, and let's consider the following cases:

Case 5. a is even. Then there is $k \in \mathbb{Z}$ such that $a = 2k$.
Then $a^2 - 3 = (2k)^2 - 3 = 4k^2 - 3 \equiv -3(mod 4) \equiv 1(mod 4)$.

Case 6. a is odd: Then there is $k \in \mathbb{Z}$ such that $a = 2k + 1$.
Then $a^2 - 3 = (2k+1)^2 - 3 = 4k^2 + 4k - 2 \equiv -2(mod 4) \equiv 2(mod 4)$.

In either case, $a^2 - 3 \not\equiv 0(mod 4)$. Therefore $4 \nmid (a^2 - 3)$.

□

Comments:

Proposition 2. *If $a \in \mathbb{Z}$, then $4 \nmid (a^2 - 3)$.*

Proof. Let $a \in \mathbb{Z}$. Assume, by contradiction, that $4|(a^2 - 3)$. Then there exists an integer b such that $4b = a^2 - 3$.

First, let a be even. Since a is even, there exists an integer k such that $a = 2k$. So

$$(2k)^2 - 3 = 4b$$
$$4k^2 - 3 = 4b$$
$$k^2 - \frac{3}{4} = b$$

So k^2 is an integer but since $\frac{3}{4}$ is rational, $k^2 - \frac{3}{4}$ is not an integer and thus a contradiction.

Next, let a be odd. Since a is odd, there exists an integer k such that $a = 2k + 1$. So

$$a^2 - 3 = 4b$$
$$(2k + 1)^2 - 3 = 4b$$
$$4k^2 + 4k + 1 - 3 = 4b$$
$$2k^2 + 2k - 1 = 2b$$
$$k^2 + k - \frac{1}{2} = b$$

So $k^2 + k$ is an integer. And since $\frac{1}{2}$ is rational, $k^2 + k - \frac{1}{2}$ which is a contradiction. Therefore, $4 \not| (a^2 - 3)$ for any integer. □

Comments:

Proposition 5. *If a is an integer, then 4 does not divide $2(2c^2 + 2c - 1)$.*

Proof. Suppose a is an integer. As such, a can be odd or even.

Suppose a is even. By definition, $a = 2c$, where c is an integer. It follows that $a^2 - 3 = 4c^2 - 3$. Here, 4 does not divide $4c^2 - 3$.

Suppose a is odd. By definition, $a = 2c + 1$, where c is an integer. Then, $a^2 - 3 = 4c^2 - 4c - 2 = 2(2c^2 + 2c - 1)$. Here, 4 also cannot divide $2(2c^2 + 2c - 1)$.

Therefore, 4 does not divide $2(2c^2 + 2c - 1)$. □

Comments:

Proposition 3. *For any natural numbers a and b, $a = lcm(a, b)$ if and only if $b|a$.*

Proof. First we prove that if $a = lcm(a, b)$, then $b|a$. Suppose $a = lcm(a, b)$. Since a is the lcm, a is a multiple of both a and b. By definition if a is a multiple of b, $b|a$.

Now we will show that if $b|a$, then $a = lcm(a, b)$. Since $b|a$, $a = bn$ for $n \in \mathbb{Z}$. Thus $lcm(a, b) = lcm(bn, b)$. By definition, the $lcm(bn, b) = bn$. We have already shown that $a = bn$. Therefore $a = lcm(a, b)$. □

Comments:

Claim 1. *3 For any natural numbers a and b, $a = lcm(a, b)$ if and only $b|a$*

Proof. Since we are proving a biconditional, we need to establish that if b divides a, then a is the least common multiple of a and b, along with proving that if a is the least common multiple of a and b, then b divides a. First, we'll prove the former. Let a and b be natural numbers, and suppose that b divides a. By definition of division, we know that there exists a natural number, z such that $bz = a$. It follows that $lcm(a, b) = lcm(bz, b)$. Since we know that $b|bz$, and since z is a natural number, therefore $bz >= b$, $lcm(bz, b) = bz$. Therefore, $lcm(a, b) = a$. Next, we will try to prove that if $a = lcm(a, b)$, then $b|a$. Again, let a and b be natural numbers, and suppose $a = lcm(a, b)$. By definition of being a multiple, there exists natural numbers, j and k, such that $lcm(a, b) = aj = bk$, both of which are equal to a. Taking the expression, $bk = a$, we see that $b|a$. Therefore $a = lcm(a, b)$ if and only if $b|a$.

□

Comments:

Proposition 3. *a = lcm(a,b) if and only if $b \mid a$.*

Proof. Let $a, b \in \mathbb{N}$.

First suppose a = lcm(a,b). By definition, the least common multiple is the smallest positive integer that is divisible by both a and b. In other words, a divides the least common multiple and b divides the least common multiple. Since a = lcm(a,b) it follows that $a \mid a$ and $b \mid a$. This proves the statement if a = lcm(a,b), then $b \mid a$.

Conversely suppose, by way of contradiction, that $b \mid a$ and $a \neq lcm(a, b)$. By definition, there is $c \in \mathbb{Z}$ such that bc = a. Since $a, b \in \mathbb{N}$, it follows that $c \in \mathbb{N}$. Also, since bc = a, we know that b $\leq$ a. It follows that lcm(a,b) $\geq$ a since the least common multiple of two natural numbers must be no less than the greater of the two numbers. And, since $a \mid a$ and $b \mid a$, it follows that a = lcm(a,b) which is a contradiction. This proves the statement if $b \mid a$, then a = lcm(a,b). □

Comments:

Proposition 3. *For any natural numbers a and b, $a = lcm(a, b)$ if and only if $b \mid a$*

Proof. First we show that for natural numbers a, b, if $a = \text{lcm}(a, b)$ then $b \mid a$. Suppose $a = \text{lcm}(a, b)$. By definition of least common multiple, there exists some natural number k such that $a = bk$. Observe that $a = bk$ follows the same form as if $b \mid a$. By definition of divides, there exists some natural number k such that $a = bk$. Therefore if if $a = \text{lcm}(a, b)$ then $b \mid a$.

Conversely, suppose that $b \mid a$. By definition of divides, there exists some natural number n such that $a = bn$. Observe that $a = bn$ takes the form of $a = \text{lcm}(a, b)$. By definition of least common multiple, there exists some natural number b such that $a = bn$. Therefore, if $b \mid a$, then $a = \text{lcm}(a, b)$. □

Comments:

Proposition 4. *Let C be a circle in $\mathbb{R}^2$ centered at $(1,1)$. Then either $(2,3) \notin C$ or $(0,2) \notin C$. (Note that C is just the circle itself, not the interior).*

Proof. Let C be a circle in $\mathbb{R}^2$ centered at $(1,1)$. Note that the two key pieces of information of a circle in $\mathbb{R}^2$ are its center point and its radius. With those two pieces of information, all points of the circle can be determined. Since we are saying that C is centered at $(1,1)$, the radius of C is the only thing that can vary. Also note that we are trying to prove that $(2,3)$ and $(0,2)$ can not both be in C at the same time.

If $(2,3)$ is not a point in C, then clearly it is true that either $(2,3) \notin C$ or $(0,2) \notin C$. So, suppose that $(2,3)$ is a point in C. The distance between $(2,3)$ and the center, $(1,1)$, is the radius of C. Let r represent the length of the radius of the circle. This variable can be calculated by finding the Euclidean distance between the points $(1,1)$ and $(2,3)$.

$$\begin{aligned} r &= \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2} \\ &= \sqrt{(2-1)^2 + (3-1)^2} \\ &= \sqrt{1^2 + 2^2} \\ &= \sqrt{5} \end{aligned}$$

So all points in C must be a distance of $\sqrt{5}$ units away from $(1,1)$ if $(2,3)$ is a point in C. Let d be the distance from $(1,1)$ and $(0,2)$, and let us calculate d in the same manner.

$$\begin{aligned} d &= \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2} \\ &= \sqrt{(0-1)^2 + (2-1)^2} \\ &= \sqrt{(-1)^2 + 1^2} \\ &= \sqrt{2} \end{aligned}$$

Since the distance from $(0,2)$ to $(1,1)$ is not $\sqrt{5}$, $(0,2)$ can not be a point in C while $(2,3)$ is a point in C.

Therefore, if C is a circle in $\mathbb{R}_2$ centered at $(1,1)$, then either $(2,3) \notin C$ or $(0,2) \notin C$. □

Comments:

Proposition 1. *Let* $n \in \mathbb{N}$ *and* $n \geq 2$*, then* $\sqrt[n]{2}$ *is irrational.*

Proof. Let $n \in \mathbb{N}$ and $n \geq 2$. Suppose, by way of contradiction, that $\sqrt[n]{2}$ is rational. Then by definition of a rational number, there exists $a, b \in \mathbb{Z}$, such that $\sqrt[n]{2} = a/b$. We may also assume that $gcd(a, b) = 1$. Then, $\sqrt[n]{2} = a/b \to 2 = a^n/b^n \to 2b^n = a^n$. Since $b^n \in \mathbb{Z}$, we can see by definition of evens that a^n is even. Since a^n is even, it follows that a is even. Then there exists an integer c, such that $a = 2c$. Then $2b^n = 2^n c^n \to b^n = 2^{n-1}c^n$. Since $n \geq 2$, b is even. This means that a and b are both multiples of 2, meaning $gcd(a, b) \geq 2$. This is a contradiction. □

Definition 4. Let $a \in \mathbb{Z}$. a is even if there exists an integer c such that $a = 2c$.

Definition 5. A real number x is rational if $x = a/b$ for some $a, b \in \mathbb{Z}$.

Comments: