Example 1. Show that the positive integers of the form $4n+3$, that is, the integers

$$3, 7, 11, 15, 19, \ldots$$

cannot be written as the sum of two perfect squares.

Summary — Show that the squares leave a remainder of 0 or 1 upon division by 4. Conclude that a sum of two squares leaves a remainder of $0, 1, 2$ upon division by 4.

Walkthrough.

(a) Consider the integers

$$\begin{gathered}
0^2+1^2, 0^2+2^2, 0^2+3^2, 0^2+4^2, \ldots, \\
1^2+1^2, 1^2+2^2, 1^2+3^2, 1^2+4^2, \ldots, \\
2^2+1^2, 2^2+2^2, 2^2+3^2, 2^2+4^2, \ldots, \\
3^2+1^2, 3^2+2^2, 3^2+3^2, 3^2+4^2, \ldots, \\
4^2+1^2, 4^2+2^2, 4^2+3^2, 4^2+4^2, \ldots.
\end{gathered}$$

(b) Observe that upon division by 4, they leave the integers $0, 1, 2$ as remainders.

$$\begin{gathered}
0^2+1^2 \rightsquigarrow \mathbf{1}, 0^2+2^2 \rightsquigarrow \mathbf{0}, 0^2+3^2 \rightsquigarrow \mathbf{1}, 0^2+4^2 \rightsquigarrow \mathbf{0}, \ldots, \\
1^2+1^2 \rightsquigarrow \mathbf{2}, 1^2+2^2 \rightsquigarrow \mathbf{1}, 1^2+3^2 \rightsquigarrow \mathbf{2}, 1^2+4^2 \rightsquigarrow \mathbf{1}, \ldots, \\
2^2+1^2 \rightsquigarrow \mathbf{1}, 2^2+2^2 \rightsquigarrow \mathbf{0}, 2^2+3^2 \rightsquigarrow \mathbf{1}, 2^2+4^2 \rightsquigarrow \mathbf{0}, \ldots, \\
3^2+1^2 \rightsquigarrow \mathbf{2}, 3^2+2^2 \rightsquigarrow \mathbf{1}, 3^2+3^2 \rightsquigarrow \mathbf{2}, 3^2+4^2 \rightsquigarrow \mathbf{1}, \ldots, \\
4^2+1^2 \rightsquigarrow \mathbf{1}, 4^2+2^2 \rightsquigarrow \mathbf{0}, 4^2+3^2 \rightsquigarrow \mathbf{1}, 4^2+4^2 \rightsquigarrow \mathbf{0}, \ldots.
\end{gathered}$$

(c) Show that it is **always** the case, namely, upon division by 4, the sum of two perfect squares leaves one of $0, 1, 2$ as the remainder.

(d) Conclude that no integer, which leaves the remainder of 3 **upon division by** 4, can be written as the sum of two squares.

Solution 1. The solution relies on the following claim.

> **Claim** — For any integer x, the integer x^2 leaves a remainder of 0 or 1 upon division by 4.

Proof of the claim. Let x be an integer. Let us consider the following cases.

1. Upon division by 4, x leaves a remainder of 0.
2. Upon division by 4, x leaves a remainder of 1.
3. Upon division by 4, x leaves a remainder of 2.
4. Upon division by 4, x leaves a remainder of 3.

In the first case, x is a multiple of 4, and hence x^2 leaves a remainder of 0 upon division by 4. Similarly, in the third case, x is a multiple[1] of 2, i.e. x is equal to $2k$, and hence x^2 is a multiple of 4.

In the second case, x is equal to $4k+1$ for some integer k. Note that

$$\begin{aligned} x^2 &= (4k+1)^2 \\ &= (4k)^2 + 2 \cdot 4k + 1 \\ &= 4(4k^2+2k)+1, \end{aligned}$$

and hence x^2 leaves a remainder of 1 upon division by 4.

In the fourth case, x is equal to $4k+3$ for some integer k. Note that

$$\begin{aligned} x^2 &= (4k+3)^2 \\ &= (4k)^2 + 2 \cdot 4k \cdot 3 + 9 \\ &= 4(4k^{+}6k+2)+1, \end{aligned}$$

and hence x^2 leaves a remainder of 1 upon division by 4.

This proves the claim. □

Using the claim, it follows that a sum of two squares leaves one of $0, 1, 2$ as a remainder upon division by 4. Hence, no integer of the form $4n+3$ can be expressed as a sum of two perfect squares. ■

[1] Is it clear?