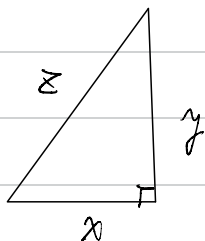


10/12/2026

Pythagorean triples



$$x^2 + y^2 = z^2, \quad x, y, z \in \mathbb{Z}.$$

Eg. $(x, y, z) = (3, 4, 5), (5, 12, 13).$

Goal: Find all $x, y, z \in \mathbb{Z}$ satisfying

$$x^2 + y^2 = z^2.$$

Observation: If (x_0, y_0, z_0) is a solution, then

$(x_0 d, y_0 d, z_0 d)$ is also a solution, where $d \in \mathbb{Z}$.

Idea: Suppose $z \neq 0$ and $(x, y) = 1$.

Factor: $\overbrace{(x+y)}^d \overbrace{(x-y)}^{\bar{d}} = z^2$

If we can show

$$(x + yi, x - yi) = 1,$$

then $x + yi = \epsilon \cdot \beta^2$, $\beta \in \mathbb{Z}[i]$

$\uparrow$
unit $= \pm 1, \pm i$

say $\beta = u + vi$, $u, v \in \mathbb{Z}$.

Then $\beta^2 = (u + vi)^2 = (u^2 - v^2) + 2uv \cdot i$

$$\epsilon \beta^2 = \begin{cases} (u^2 - v^2) + 2uv \cdot i & \epsilon = 1 \\ -(u^2 - v^2) - 2uv \cdot i & \epsilon = -1 \\ -2uv + (u^2 - v^2) i & \epsilon = i \\ 2uv - (u^2 - v^2) i & \epsilon = -i \end{cases}$$

$$\text{so } x + iy = \pm(u^2 - v^2) \pm 2uv \cdot i$$

$$\text{or } = \pm 2uv \pm i(u^2 - v^2).$$

$$\Rightarrow (x, y) = (\pm(u^2 - v^2), \pm 2uv)$$

$$\text{or } = (\pm 2uv, \pm(u^2 - v^2))$$

$$\Rightarrow z^2 = x^2 + y^2 = (u^2 - v^2)^2 + (2uv)^2$$

$$= (u^2 + v^2)^2$$

$$\Rightarrow z = \pm(u^2 + v^2).$$

Now we solve $x^2 + y^2 = z^2$ completely.

1. $z = 0$: $x = y = 0$.

2. $z \neq 0$: Then x, y are not both 0.

Let $d = (x, y)$. Then $d \mid x$, $d \mid y$ and so

$d^2 \mid x^2$ and $d^2 \mid y^2$. Thus, $d^2 \mid z^2$. Hence, $d \mid z$.

Write $x = x_1 d$, $y = y_1 d$, $z = z_1 d$. Then

$$x_1^2 + y_1^2 = z_1^2,$$

where $(x_1, y_1) = 1$.

If z_1 is even, $x_1^2 + y_1^2 \equiv 0 \pmod{4}$. Since x_1^2, y_1^2

$\equiv 0, 1 \pmod{4}$, we know $x_1^2, y_1^2 \equiv 0 \pmod{4}$.

So $2|x_1$, $2|y_1$, contradicting $(x_1, y_1) = 1$.

Hence $2 \nmid z_1$. As a result, exactly one of x_1, y_1

is even.

Now factor

$$\underbrace{(x_1 + y_1 i)}_{\alpha} \underbrace{(x_1 - y_1 i)}_{\bar{\alpha}} = z_1^2.$$

Let $\pi | \gcd(\alpha, \bar{\alpha})$. Then $\pi | \alpha$, $\pi | \bar{\alpha}$. So

$$\pi | \alpha + \bar{\alpha} = 2x_1$$

$$\pi | \alpha - \bar{\alpha} = 2y_1 \cdot i \Rightarrow \pi | 2y_1.$$

$\uparrow$
unit

$$\Rightarrow \pi | (2x_1, 2y_1) = 2 \underbrace{(x_1, y_1)}_2 \rightarrow \gcd \text{ of } x_1, y_1 \text{ in } \mathbb{Z}[i], \text{ but}$$

we showed that this is 1 when $(x_1, y_1) = 1$ in $\mathbb{Z}$.

So $\pi | 2$. Thus $N(\pi) = \pi \bar{\pi} = 2$. But

$$\pi | 2, \bar{\pi} | 2 \Rightarrow \underbrace{\pi \bar{\pi}}_2 | 2 = z_1^2,$$

So z_1 is even, impossible. Hence, $(\alpha, \bar{\alpha}) = 1$.

Since $\alpha \bar{\alpha} = z_1^2$, $\exists$ unit ϵ and $\beta = u + iv \in \mathbb{Z}[i]$

s.t.

$$\alpha = \epsilon \cdot \beta^2$$

As sketched earlier,

$$x_1 = \pm(u^2 - v^2), \quad y_1 = \pm 2uv, \quad z_1 = \pm(u^2 + v^2)$$

or

$$x_1 = \pm 2uv, \quad y_1 = \pm(u^2 - v^2), \quad z_1 = \pm(u^2 + v^2)$$

Primitive solutions: $(u, v) = 1$, exactly one of which is even.

Thus

$$x = \pm(u^2 - v^2)d, \quad y = \pm 2uvd, \quad z = \pm(u^2 + v^2)d.$$

or

$$x = \pm 2uvd, \quad y = \pm(u^2 - v^2)d, \quad z = \pm(u^2 + v^2)d.$$

These are all solutions if we allow d to be 0.

Fermat's Last Theorem:

$$x^n + y^n = z^n \quad (n > 2)$$

has no solutions (x, y, z) with $x, y, z \neq 0$.

This was proved by Wiles and Wiles-Taylor (1995).