

Theorem If $x^2 + y^2 = z^2$ with $(x, y) = 1$ & $x, y, z \in \mathbb{N}$

then $\exists p, q \in \mathbb{N}$ with $(p, q) = 1$ and
$$\left. \begin{aligned} x &= 2pq \\ y &= p^2 - q^2 \\ z &= p^2 + q^2 \end{aligned} \right\} \textcircled{1}$$

Proof (Note: $(x, y) = d \neq 1 \Rightarrow \left(\frac{x}{d}\right)^2 + \left(\frac{y}{d}\right)^2 = \left(\frac{z}{d}\right)^2$ & $\left(\frac{x}{d}, \frac{y}{d}\right) = 1$.)

(a) x and y have opposite parity: If both are even $\Rightarrow 2 \mid (x, y)$ (!!!).

If both are odd: $x^2 = (2n+1)^2 = 4m+1 \equiv 1 \pmod{4}$ for some $n, m \in \mathbb{Z}$.

Similarly $y^2 \equiv 1 \pmod{4} \Rightarrow x^2 + y^2 \equiv 2 \pmod{4}$, but $z^2 \equiv 0 \pmod{4}$ is false.

(b) Assume x is even and y odd. Then z is odd: $(2n)^2 + (2m+1)^2 = 4l+1$

so z can't be even, hence it must be odd.

(c) Write $x = 2n$ so $4n^2 = z^2 - y^2 = (z+y)(z-y)$

$$\Rightarrow n^2 = \left(\frac{z+y}{2}\right)\left(\frac{z-y}{2}\right) \textcircled{2}$$

Note that since y and z are odd, $z+y$ is even & so is $z-y$

Also with $(x, y) = 1 \Rightarrow (z, y) = 1 \Rightarrow \left(\frac{z+y}{2}, \frac{z-y}{2}\right) = 1$: to see

this last step let $p \in \mathbb{P}$ have
$$\left. \begin{aligned} p \mid \frac{z+y}{2} \\ p \mid \frac{z-y}{2} \end{aligned} \right\} \begin{aligned} p \mid \frac{z+y}{2} + \frac{z-y}{2} = z \\ p \mid -\frac{z-y}{2} + \frac{z+y}{2} = y \end{aligned} \Rightarrow p \mid (z, y) \textcircled{!!!}$$

(d) Hence $\frac{z+y}{2} = p^2$ for $p, q \in \mathbb{N}$ and $(p, q) = 1$.

by $\textcircled{2}$
$$\frac{z-y}{2} = q^2$$

But then
$$z = p^2 + q^2$$

$$y = p^2 - q^2$$

Finally
$$x^2 = -y^2 + z^2 \Rightarrow x^2 = (p^2 + q^2)^2 - (p^2 - q^2)^2 = 4p^2q^2$$

$$\Rightarrow x = 2pq$$

and so $\textcircled{1}$ has been proved. //