# PRIMITIVE PYTHAGOREAN TRIPLE

SHANE CHERN

Consider the Diophantine equation

$$x^2 + y^2 = z^2. \tag{1}$$

Apparently, if $x$, $y$ and $z$ have a common divisor $d$, we can divide them by $d$, and (1) still holds. Therefore, we call positive integer solutions $(x, y, z)$ to (1) with $\gcd(x, y, z) = 1$ a *primitive Pythagorean triple.*

**Theorem 1.** *The triple* $(x, y, z) \in \mathbb{Z}^3_{\geq 0}$ *is a primitive Pythagorean if and only if there exist two integers* $r > s > 0$ *of different parities with* $\gcd(r, s) = 1$ *such that*

$$\begin{cases} x = r^2 - s^2, \\ y = 2rs, \\ z = r^2 + s^2, \end{cases} \quad \textit{or} \quad \begin{cases} x = 2rs, \\ y = r^2 - s^2, \\ z = r^2 + s^2. \end{cases}$$

*Proof.* We first claim that given any integer $n$, we always have $n^2 \equiv 0$ or $1 \pmod 4$. This is because when $n$ is even, $n^2 \equiv 0 \pmod 4$ and when $n$ is odd, $n^2 \equiv 1 \pmod 4$.

Since $(x, y, z)$ is a primitive Pythagorean, $x$ and $y$ cannot be simultaneously even, for in this case, $z$ is also even, and the three integers have a common factor 2. Also, $x$ and $y$ cannot be simultaneously odd, for in this case, $x^2 + y^2 \equiv 2 \pmod 4$, which cannot be a square.

Without loss of generality, we assume that $x$ is odd and $y$ is even. Then $z$ is also odd. This assumption corresponds to the first parameterization. For the latter, we assume that $x$ is even and $y$ is odd.

Now, we rewrite (1) as

$$y^2 = z^2 - x^2 = (z - x)(z + x).$$

Since we have assumed that $x$ and $z$ are odd, we know that $z \pm x$ are even, and we write $z + x = 2u$ and $z - x = 2v$. Note also that $\gcd(u, v) = 1$. Otherwise, if $u$ and $v$ have a common prime divisor $p > 1$, then $p$ also divides $u - v = x$ and $u + v = z$, thereby violating the assumption that $(x, y, z)$ is primitive.

Next,

$$y^2 = (z - x)(z + x) = 4uv.$$

Since $y$ is even, we find that $uv$ is a square. Further, since $\gcd(u, v) = 1$, each of them is a square. We write $u = r^2$ and $v = s^2$. Now, $x = u - v = r^2 - s^2$, $y = 2\sqrt{uv} = 2rs$, $z = u + v = r^2 + s^2$. Further, the assumption $r > s > 0$ comes from the fact that $z + x > z - x$ and the assumption that $\gcd(r, s) = 1$ comes from the fact that $\gcd(u, v) = 1$. Finally, we require that $r$ and $s$ have different parities since if they are of the same parity, then all of $x$, $y$ and $z$ have a common factor 2. □

Department of Mathematics and Statistics, Dalhousie University, Halifax, Nova Scotia, B3H 4R2, Canada

*E-mail address*: chenxiaohang92@gmail.com