## Sum of Two Square

Broofen Das

### Pythagorean Triple:

**Def:** A Pythagorean triple is a set of three integers $x, y, z$ such that $x^2+y^2=z^2$. A Pythagorean triple is called primitive if $\gcd(x,y,z)=1$

e.g. $(3,4,5)$ is a primitive Pythagorean triple.

But $(6,8,10)$ is a non-primitive Pythagorean triple.

If $(x,y,z)$ is a Pythagorean triple st. $\gcd(x,y,z)=d$ then $\exists\ x_1, y_1, z_1$ st $x=dx_1$, $y=dy_1$ and $z=dz_1$ with $\gcd(x_1,y_1,z_1)=1$

Then $x_1^2+y_1^2=\left(\frac{x}{d}\right)^2+\left(\frac{y}{d}\right)^2=\frac{x^2+y^2}{d^2}=\frac{z^2}{d^2}=z_1^2$

ie $(x_1,y_1,z_1)$ is a primitive Pythagorean triple.

**Lemma:-**

If $x,y,z$ is a primitive Pythagorean triple. Then one of $x$ & $y$ is even, while $z$ is odd.

**Proof:-** If both $x$ & $y$ even then $2|x$, $2|y$.

it implies $2|x^2+y^2 \Rightarrow 2|z^2 \Rightarrow 2|z$

Thus $\gcd(x,y,z)\geq 2$. is a contradiction to $x,y,z$ is a primitive triple. So one of $x$ or $y$ is ~~even~~ odd.

If both $x,y$ are odd then $x^2\equiv 1 \pmod 4$

$y^2\equiv 1 \pmod 4 \Rightarrow x^2+y^2\equiv 2 \pmod 4$

$\Rightarrow z^2\equiv 2 \pmod 4$ is a contradiction as square of an integer either $\equiv 0$ or $1 \pmod 4$

Since one of $x$ or $y$ is even and other is odd so ~~___~~ one of $x^2$, $y^2$ is even and other is odd. Thus $x^2+y^2$ is odd ie $z^2$ is odd. So $z$ is odd.

<u>Lemma:</u> If $ab = c^n$, where $\gcd(a,b)=1$, then $a$ and $b$ are $n$th powers; that is, there exist positive integers $a_1, b_1$ for which $a = a_1^n$, $b = b_1^n$.

<u>proof:</u> Assume that $a>1$ and $b>1$

and let $a = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$

$b = q_1^{j_1} q_2^{j_2} \cdots q_s^{j_s}$

Since $\gcd(a,b)=1$ therefore the primes $p_i$ and $q_i$ are distinct.

So $ab = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} q_1^{j_1} q_2^{j_2} \cdots q_s^{j_s} = c^n$

Therefor each $k_i$ and $j_i$ are divisible by $n$

Hence $a = \left(p_1^{k_1/n} p_2^{k_2/n} \cdots p_r^{k_r/n}\right)^n = a_1^n$

and $b = \left(q_1^{j_1/n} q_2^{j_2/n} \cdots q_s^{j_s/n}\right)^n = b_1^n$

<u>Theorem:-</u> All the solutions of the Pythagorean equation $x^2+y^2=z^2$ satisfying the conditions $\gcd(x,y,z)=1$, $2|x$, $x>0$, $y>0$, $z>0$ are given by the formulas $x=2st$, $y=s^2-t^2$, $z=s^2+t^2$ for integers $s>t>0$ such that $\gcd(s,t)=1$ and $s \not\equiv t \pmod{\ldots}$

Proof.- Let $x, y, z$ be a primitive Pythagorean triple.

Since one of $x$ & $y$ is even so let $x$ be even and $y$ and $z$ be odd.

Thus $z+y$ and $z-y$ both are even

Let $z+y = 2v$ and $z-y = 2u$

Now from $x^2+y^2=z^2$

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

$$\Rightarrow \left(\frac{x}{2}\right)^2 = uv$$

Note that $\gcd(u,v)=1$, if $\gcd(u,v)=d>1$ then $d \mid u+v$ and $d \mid u-v$

$\Rightarrow d \mid y$, $d \mid z$

$\Rightarrow d \mid x$ also

Then $\gcd(x,y,z) > d > 1$ is a contradiction.

Since $\gcd(u,v)=1$ and $uv = \left(\frac{x}{2}\right)^2$ ~~by the~~ so we have $u = t^2$ and $v = s^2$ (Second lemma)

where $s$ and $t$ are positive integers. Then

$$z = u+v = s^2+t^2$$
$$y = v-u = s^2-t^2$$
$$x^2 = 4uv = 4s^2t^2 \Rightarrow x = 2st$$

We claim $\gcd(s,t)=1$. If $\gcd(s,t)=d>1$. Then $d \mid s, d \mid t$ implies $d \mid s^2, d \mid t^2 \Rightarrow d \mid z+y, d \mid z-y$

$$\Rightarrow d \mid z, d \mid y \Rightarrow \gcd(z,y) \geq d > 1$$

which is impossible as $\gcd(y,z)=1$

So. both of $s, t$ can't be even or ~~or~~ odd at same time. If so it will make $\gcd(y,z)>1$

Hence $s \not\equiv t \pmod 2$

Conversely let $s$ & $t$ be +ve integers such that $s \not\equiv t \pmod 2$ and

$$x = 2st, \quad y = s^2 - t^2, \quad z = s^2+t^2, \text{ with } s>t.$$

Then $x^2+y^2 = 4s^2t^2 + s^4+t^4 - 2s^2t^2 = s^4+t^4+2s^2t^2 = (s^2+t^2)^2$
$= z^2$

If $\gcd(x,y,z) = d > 1$ then ~~god~~ if $p$ be a prime divisor of $d$ then $d \mid y \Rightarrow d \mid s^2-t^2$

$\Rightarrow d \mid \cancel{(s+t)(s-t)}$

$\Rightarrow p \mid s^2 - t^2$.

Similarly $p \mid s^2+t^2$

$$\left.\begin{array}{l} \Rightarrow p \mid s^2 \Rightarrow p \mid s \\ p \mid t^2 \Rightarrow p \mid t \end{array}\right\} \Rightarrow \gcd(s,t) > p$$

is a contradiction.

Thus $\gcd(x,y,z)=1$