Math 4460

4/16/25

We will now find a formula for all the primitive, positive, Pythagorean triples.

Consider $(x, y, z)$
where $x, y, z \in \mathbb{Z}$,
$x > 0, y > 0, z > 0$, ← positive
$\gcd(x, y, z) = 1$, ← primitive
and $x^2 + y^2 = z^2$ ← Pythagorean triple

- Let's show $x$ and $y$ can't both be even.

Suppose $x, y$ are both even.

Then in $\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$ we get

$$\bar{x} = \bar{0}, \quad \bar{y} = \bar{0}.$$

So,

$$\bar{z}^2 = \bar{x}^2 + \bar{y}^2 = \bar{0}^2 + \bar{0}^2 = \bar{0}$$

in $\mathbb{Z}_2$.

Then $\bar{z} = \bar{0}$.

So, $z$ is even.

But then $2 | x$, $2 | y$, $2 | z$

making $\gcd(x, y, z) \geq 2$

contradicting $\gcd(x, y, z) = 1$.

Thus, $x$ and $y$ cannot both be even.

- $x$ and $y$ cannot both be odd.

Why?

Suppose $x$ and $y$ are both odd.

Let's use $\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$.

Recall if $\bar{a} \in \mathbb{Z}_4$ with $a$ odd

then $\bar{a} = \bar{1}$ or $\bar{a} = \bar{3}$.

This gives $\bar{a}^2 = \bar{1}^2 = \bar{1}$

or $\bar{a}^2 = \bar{3}^2 = \bar{9} = \bar{1}$.

Thus, in $\mathbb{Z}_4$ we get

$$\bar{x}^2 = \bar{1} \quad \text{and} \quad \bar{y}^2 = \bar{1}$$

Then in $\mathbb{Z}_4$ we get

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

By the following table

there is no $\overline{z}$ with $\overline{z}^2 = \overline{2}$

giving a contradiction.

| $\overline{z}$ | $\overline{z}^2$ |
| --- | --- |
| $\overline{0}$ | $\overline{0}$ |
| $\overline{1}$ | $\overline{1}$ |
| $\overline{2}$ | $\overline{4} = \overline{0}$ |
| $\overline{3}$ | $\overline{9} = \overline{1}$ |

never get $\overline{2}$

Thus $x$ and $y$ are not both odd.

Therefore either

$x$ is odd and $y$ is even

or

$x$ is even and $y$ is odd.

Since $x^2+y^2=z^2$ is symmetric in $x$ and $y$ we can just do one of the above cases.

Let's assume $x$ is odd and $y$ is even.

Then, in $\mathbb{Z}_2=\{\bar{0},\bar{1}\}$ we get $\bar{x}=\bar{1}$ and $\bar{y}=\bar{0}$.

So, $\bar{z}^2=\bar{x}^2+\bar{y}^2=\bar{1}^2+\bar{0}^2=\bar{1}$

Thus, in $\mathbb{Z}_2$ we get $\bar{z}=\bar{1}$.

Then, z is odd.

Since $x$ is odd and $z$ is odd we know $z-x$ is even and $z+x$ is even.

Note that

$$y^2 = z^2 - x^2$$

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

So, dividing by 4 gives

$$\boxed{\left(\frac{y}{2}\right)^2 = \left(\frac{z+x}{2}\right)\left(\frac{z-x}{2}\right)} \quad (*)$$

Note $\frac{y}{2}, \frac{z+x}{2}, \frac{z-x}{2} \in \mathbb{Z}$

because $y, z+x, z-x$ are even.

Let's show that

$$\gcd\left(\frac{z+x}{2}, \frac{z-x}{2}\right) = 1.$$

Any common divisor of

$\frac{z+x}{2}$ and $\frac{z-x}{2}$ must divide their sum

$$\left(\frac{z+x}{2}\right)+\left(\frac{z-x}{2}\right)=z$$

and their difference

$$\left(\frac{z+x}{2}\right)-\left(\frac{z-x}{2}\right)=x$$

So we just need to show $\gcd(x,z)=1$.

**HW 3-5(a)**

$\gcd(x,z)>1$ iff there exists a prime $p$ where $p \mid x$ and $p \mid z$

Suppose $\gcd(x,z)>1$. Then there exists a prime $p$ where $p \mid x$ and $p \mid z$.

Then, $p \mid x^2$ and $p \mid z^2$.

So, $p \mid (z^2 - x^2)$.

So, $p \mid y^2$.

$p$ prime
$p \mid ab \rightarrow p \mid a$ or $p \mid b$

Then $p \mid y$.

Since $p \mid x$, $p \mid y$, $p \mid z$ we get $\gcd(x,y,z) \geq p$ contradicting $\gcd(x,y,z) = 1$.

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

From above this implies $\gcd\left(\frac{z+x}{2}, \frac{z-x}{2}\right) = 1$.

Recall this theorem: (topic 3)

If $A, B, C$ are positive integers and $\gcd(A,B)=1$ and $C^n = AB$, then there exists positive integers $R, S$ where $A = R^n$ and $B = S^n$

Our situation from $(*)$ is

$$\left(\frac{y}{2}\right)^2 = \left(\frac{z+x}{2}\right)\left(\frac{z-x}{2}\right) \leftarrow C^2 = AB$$

with

$$\gcd\left(\frac{z+x}{2}, \frac{z-x}{2}\right) = 1 \leftarrow \gcd(A,B) = 1$$

Hence

$$\frac{z+x}{2} = r^2 \quad \text{and} \quad \frac{z-x}{2} = s^2$$

where $r, s > 0$ are integers

and $\gcd(r,s)=1$

because
$\gcd(r^2,s^2)=\gcd\left(\frac{z+x}{2},\frac{z-x}{2}\right)=1$

So,
$$\left(\frac{y}{2}\right)^2=\left(\frac{z+x}{2}\right)\left(\frac{z-x}{2}\right)=r^2s^2$$

Thus, $y/2=rs$ and so
$$\boxed{y=2rs}$$

Note that $r^2=\frac{z+x}{2}>\frac{z-x}{2}=s^2$

So, $\boxed{r>s>0}$

And
$$x=\left(\frac{z+x}{2}\right)-\left(\frac{z-x}{2}\right)=r^2-s^2$$
$$z=\left(\frac{z+x}{2}\right)+\left(\frac{z-x}{2}\right)=r^2+s^2$$

Since z is odd and

$$z = r^2 + s^2$$

by this table $\rightarrow$

In $\mathbb{Z}_2$

| $\overline{r}$ | $\overline{s}$ | $\overline{z} = \overline{r}^2 + \overline{s}^2$ |
|---|---|---|
| $\cancel{\overline{0}}$ | $\cancel{\overline{0}}$ | $\cancel{\overline{0}}$ |
| $\overline{0}$ | $\overline{1}$ | $\overline{1}$ |
| $\overline{1}$ | $\overline{0}$ | $\overline{1}$ |
| $\cancel{\overline{1}}$ | $\cancel{\overline{1}}$ | $\cancel{\overline{0}}$ |

r and s have <u>opposite parity</u>

that is, one is even and one is odd.

---

<u>Theorem</u>: If $(x, y, z)$ is a primitive, positive Pythagorean triple, with $y$ even (and $x$ odd), then

$$x = r^2 - s^2$$

$$y = 2rs$$

$$z = r^2 + s^2$$

Where $r > s > 0$ are integers of opposite parity with $\gcd(r,s) = 1$

---

A similar formula would hold for $x$ even / $y$ odd

---

| $s$ | $r$ | $x = r^2 - s^2$ | $y = 2rs$ | $z = r^2 + s^2$ |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |
| 1 | 4 | 15 | 8 | 17 |
| 1 | 6 | 35 | 12 | 37 |
| 2 | 3 | 5 | 12 | 13 |
| 2 | 5 | 21 | 20 | 29 |

| | | | | |
|---|---|---|---|---|
| 3 | 4 | 7 | 24 | 25 |
| 3 | 8 | 55 | 48 | 73 |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |