Chapter: Non-linear Diophantine equations

The equation $x^2+y^2=z^2$

"It is impossible to write a cube as a sum of two cubes, a fourth power as a sum of two fourth powers and in general any power beyond the second as a sum of two similar powers. For this I have discovered a truly wonderful proof, but the margin is too small to contain it."

— Fermat (around 1637)

Through this correspondence Fermat was simply asserting that if $n>2$ then the Diophantine equation

$$x^n+y^n=z^n \quad -(1)$$

has no soln in the integers other than the trivial soln in which atleast one of the variable is zero.

Though Fermat may not have given a proof of this statement (which is famously called Fermat's Last theorem) he had proved it for the case $n=4$. To study the proof we first undertake the task of identifying all soln in the positive integers of the equation

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

Def- (Pythagorean triplet) A Pythagorean triplet is a set of three integers x, y, z s.t. $x^2+y^2=z^2$.

The triplet is said to be primitive if $\gcd(x,y,z)=1$

Note Suppose x,y,z is any Pythagorean triple and $d=\gcd(x,y,z)$

Hence we can write $x=dx_1$, $y=dy_1$, $z=dz_1$

$$\therefore \quad x_1^2+y_1^2=\frac{x^2}{d^2}+\frac{y^2}{d^2}=\frac{x^2+y^2}{d^2}=\frac{z^2}{d^2}=z_1^2$$

with $\gcd(x_1,y_1,z_1)=1$

i.e. x, y, z form a primitive Pythagorean triple. Thus it is enough to study the primitive Pythagorean triples. Any other Pythagorean triples can easily be obtained from primitive Pythagorean triple by multiplying a suitable integer.

We will study those primitive Pythagorean triple x, y, z s.t. $x>0, y>0, z>0$

Lemma. If x, y, z is a primitive Pythagorean triple, then one of the integers x or y is even, while the other is odd.

Pf. Suppose x and y are both even. Then

$$2 \mid x^2+y^2 \Rightarrow 2 \mid z^2 \Rightarrow 2 \mid z \Rightarrow z \text{ is even}$$

$\therefore$ $\gcd(x, y, z) \geq 2$ which is impossible

On the other hand suppose x and y are both odd. Then

$$x^2 \equiv 1 \pmod 4 \text{ and } y^2 \equiv 1 \pmod 4$$

$$\therefore \quad z^2 = x^2+y^2 \equiv 1+1 \pmod 4 = 2 \pmod 4$$

This is impossible as square of any integer must be congruent either to 0 or 1 modulo 4

+ Note (a) Note that each pair of integers ~~in~~ x, y, z must be relatively prime.

Pf. Suppose not. Let $\gcd(x, y) = d > 1$

Then $\exists$ a prime p s.t. $p \mid d \Rightarrow p \mid x$ and $p \mid y$

$\Rightarrow p \mid x^2$ and $p \mid y^2$

$\Rightarrow p \mid x^2+y^2$

$\Rightarrow p \mid z^2 \Rightarrow p \mid z$

$\Rightarrow \gcd(x, y, z) \geq p$

(b) $\exists$ no primitive Pythagorean triple x, y, z all of whose values are prime numbers.

<u>Lemma 2.</u> If $ab = c^n$ where $\gcd(a,b) = 1$ then a and b are nth powers i.e. $\exists$ +ve integers a_1, b_1 for which $a = a_1^n$, $b = b_1^n$

Pf. Assume that $a > 1$ and $b > 1$. Then they have prime factorizations

$$a = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}, \quad b = q_1^{j_1} q_2^{j_2} \cdots q_s^{j_s}$$

$\because \gcd(a,b) = 1$ then $p_i \neq q_j \quad \forall\ i, j.$

$\therefore$ The prime factorization of ab is

$$ab = p_1^{k_1} \cdots p_r^{k_r} q_1^{j_1} \cdots q_s^{j_s}$$

Suppose c has prime factorization

$$c = u_1^{t_1} u_2^{t_2} \cdots u_l^{t_l}.$$

Then $\quad ab = c^n.$

$$\Rightarrow p_1^{k_1} \cdots p_r^{k_r} q_1^{j_1} \cdots q_s^{j_s} = u_1^{nt_1} \cdots u_l^{nt_l}$$

It is clear that the primes $u_1, \ldots, u_l$ are $p_1 \cdots p_r\, q_1 \cdots q_s$ (in some order) and $nt_1, \ldots, nt_l$ are $k_1, \ldots k_r, j_1 \cdots j_s$

Hence each of the integers k_i and j_i must be divisible by n

Let
$$a_1 = p_1^{k_1/n} \cdots p_r^{k_r/n}$$
$$b_1 = q_1^{j_1/n} \cdots q_s^{j_s/n}$$

Then $a = a_1^n$ and $b = b_1^n$.

Scanned by CamScanner

Thm (Characterization of all primitive Pythagorean triple)
All the soln of the Pythagorean eqn

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

satisfying the condn

$$\gcd(x,y,z)=1 \quad 2|x \quad x>0,\ y>0,\ z>0.$$

are given by the formulas

$$x=2st,\ y=s^2-t^2,\ z=s^2+t^2$$

for integers $s>t>0$ s.t. $\gcd(s,t)=1$ and $s\not\equiv t \pmod 2$

Pf. Let x, y, z be primitive Pythagorean triple s.t.

$x>0,\ y>0,\ z>0$ and x is even and y and z both odd.

$\therefore$ $z-y$ and $z+y$ are both even say

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

$$\therefore \quad x^2+y^2=z^2$$

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

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

Note that u and v are relatively prime

[If u, v are not relatively prime then $\gcd(u,v)=d>1$

$\because d|u$ and $d|v$ $\therefore$ $d|u-v$ and $d|u+v$

$$\Rightarrow d|y \quad " \quad d|z$$

$$\Rightarrow \gcd(y,z)\geq d \rightarrow \text{contradiction}$$
]

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

$\therefore$ We can find s and t s.t.

$$u = t^2 \text{ and } v = s^2 \quad \text{where } s, t \in \mathbb{N}$$

Substituting these values of u and v we have

$$z = u + v = s^2 + t^2$$

$$y = v - u = s^2 - t^2$$

$$x^2 = 4vu = 4s^2t^2 \Rightarrow x = 2st$$

$\because$ gcd $(y, z) = 1$ therefore gcd $(s, t) = 1$

[Otherwise if gcd $(s,t) = d > 1$, then $d \mid s$ and $d \mid t$

$\Rightarrow d \mid s^2$ " $d \mid t^2$

$\Rightarrow d \mid s^2 + t^2$ and $d \mid s^2 - t^2$

$\Rightarrow d \mid z$ and $d \mid y$

$\Rightarrow$ gcd $(y, z) \geq d$]

Finally it remains to show that $s \not\equiv t \pmod 2$ i.e. s and t are not both even ~~and~~ and not both odd.

Suppose s and t are both even (Then $s \equiv t \pmod 2$).

Then s^2 and t^2 " " even

Hence $s^2 + t^2$ and $s^2 - t^2$ are even i.e. z and y are even

$\therefore$ gcd $(y, z) \geq 2$

This is impossible. Hence both s and t are not even. Similarly both s and t are not odd i.e.

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

Conversely suppose s and t be integers s.t. $s > t > 0$, $\gcd(s,t) = 1$ and $s \not\equiv t \pmod 2$ and

$$x = 2st \qquad y = s^2 - t^2 \qquad z = s^2 + t^2$$

To show: x, y, z forms a primitive Pythagorean triplet

Now $\quad x^2 + y^2 = (2st)^2 + (s^2 - t^2) = (s^2 + t^2)^2 = z^2$

Let us assume that $\gcd(x, y, z) = d > 1$ and let p be any prime divisor of d.

$\because$ $d \mid z^2$. therefore $p \mid z^2 \Rightarrow p \mid z$ ($\because$ p is prime)

Now since $s \not\equiv t \pmod 2$ therefore either s or t is odd. Hence either s^2 or t^2 is odd. Therefore $s^2 + t^2 = z^2$ is odd.

$\because$ $p \mid z$ therefore p cannot be even. Hence $p \neq 2$. (2 is the only eve prime

$\because$ $\quad p \mid y$ and $p \mid z$

$\therefore$ $\quad p \mid z + y$ and $p \mid z - y$

$\Rightarrow p \mid 2s^2$ and $p \mid 2t^2$

$\Rightarrow p \mid s^2$ and $p \mid t^2 \qquad (\because p \nmid 2)$

$\Rightarrow p \mid s$ and $p \mid t$

$\Rightarrow \gcd(s, t) = p > 1$

which is impossible

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