Note Title 09-08-2021

MA -222

Lec-5

Diophantine equations

Diophantus ~ 3^{rd} AD

Given $a, b, c \in \mathbb{Z}$ $ax + by = c$ find $x, y \in \mathbb{Z}$

finding a rational soln.

$ax + by + cz = d$

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

$\not\exists\, x, y, z \in \mathbb{Z}$ $x^n + y^n = z^n$ $n > 2$

has integer soln.

Fermat's Last Thm. 1655

Andrew Wiles. 1993 800 pgs.

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

$ax + by = c$ iff $\exists\, x, y \in \mathbb{Q}$. $\exists\, x, y \in \mathbb{Z}$

Amartya Dutta
Resonance
2002/3

Aryabhatta – 4
Bhaskaracharya – 5

Finding all integer sol^ns.

Sulabhsutra

B. . .

$ax + by = c$

$2x - 3y = 4$

B. Dutta & AN Singh

B. . . Bhushan Dutta

$ax - by = \pm c$

$ax - by = c$

$x = \dfrac{by + c}{a} \in \mathbb{Z}$ iff $a \mid by + c$

iff $\gcd(|a|, |b|) \mid c$

$f(x,y) = c$ $\quad$ $f(x,y) \in \mathbb{Z}[x,y]$

If $(x_0, y_0) \in \mathbb{Q}^2$ s.t. $f(x_0, y_0) = c$

$\Rightarrow$? $\exists\, (m_0, n_0) \in \mathbb{Z}^2$ s.t. $f(m_0, n_0) = c$

Yes if f is homogeneous.

Thm: $a, b, c \in \mathbb{Z}$. $ax + by = c$ has a sol^n (intg) iff $\gcd(a, b) \mid c$.

Further if (x_0, y_0) is a sol^n then all other sol^{n}s are of the form

$$x = x_0 + \left(\frac{b}{d}\right)t \quad \& \quad y = y_0 - \left(\frac{a}{d}\right)t$$

$t \in \mathbb{Z}$

where $d = \gcd(a, b)$.

Pf:

x_0, y_0 $\qquad\qquad$ x_1, y_1

$a x_0 + b y_0 = c$ $\qquad\qquad$ $a x_1 + b y_1 = c$.

$a(x_0 - x_1) = -b(y_0 - y_1)$ $\qquad\qquad$ $d \mid a$, $d \mid b$.

$d = \gcd(a, b)$ $\qquad\qquad$ $a = dr$ $\quad$ $b = ds$

$r(x_0 - x_1) = -s(y_0 - y_1)$ $\qquad$ & $(r, s) = 1$.

$r \mid s(y_0 - y_1) \Rightarrow r \mid y_0 - y_1$.

$\Rightarrow y_0 - y_1 = rt$ for some $t \in \mathbb{Z}$.

$$\cancel{r}(x_0 - x_1) = -s\cancel{r}t$$

$$x_0 - x_1 = -st$$

$$x_1 = x_0 + st$$

$$x_1 = x_0 + \left(\frac{b}{d}\right)t$$

$$y_0 - y_1 = rt$$

$$y_1 = y_0 - rt$$

$$y_1 = y_0 + \left(\frac{-a}{d}\right)t$$

If $\gcd(a,b) \mid c$ $\qquad d \mid c$ $\qquad a = dr$

$c = dt$ $\qquad b = ds$

$$ax + by = c$$

$$\cancel{d}rx + \cancel{d}sy = \cancel{d}t$$

$\gcd(a,b) \mid c$ $\quad d \mid c$ $\quad a = dr$

d " $\quad b = ds$

$c = dt$

To show $ax + by = c$ has a solⁿ.

$drx + dsy = dt$.

iff

$rx + sy = t$ has a solⁿ.

$(r, s) = 1$.

$rx + sy = t$

$x = \dfrac{t - sy}{r}$

$y = \dfrac{t - rx}{s}$

iff $r \mid t - sy$

$s \mid t - rx$

$ax + by = c$

$x = \dfrac{c - by}{a}$ $\quad a \mid c - by$