Linear Diophantine Equations I

Q: What is a Diophantine Equation?

A: Named after Diophantus...

- polynomial eqn.
- any # of vars.
- integer coefficients
- only solutions are integral

Ex: $x^2 - 2 = 0$ has no solns.

Ex: Pell's Eqn. $x^2 - ny^2 = 1$
sometimes has solns.

↳ Named after John Pell who did not solve the eqn

Linear Diophantine Eqns.

All look like: $a_1 x_1 + a_2 x_2 + \cdots + a_n x_n = k$
for $a_1, \ldots, a_n, k \in \mathbb{Z}$

Ex: Can you make 83 cents out of 6 cent and 15 cent coins?

$\longleftrightarrow$ Are there nonnegative integer solns to

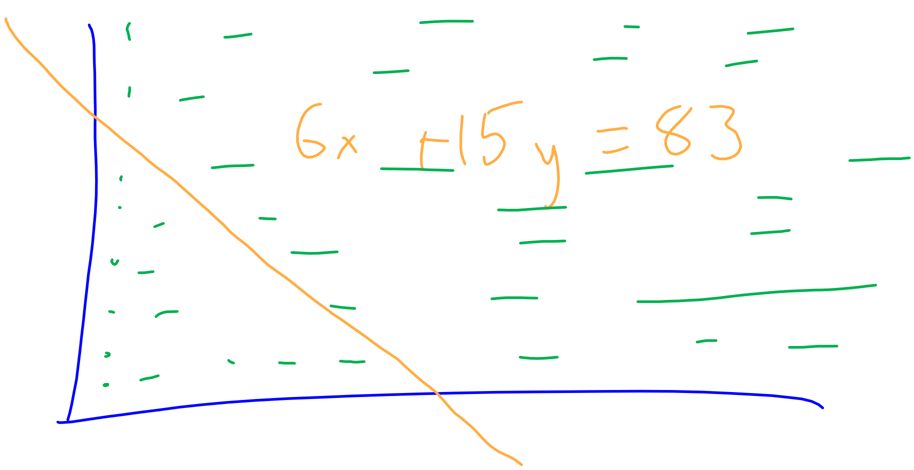
$$6x + 15y = 83 \, ?$$

How to Approach?

① Geometrically

$6x + 15y = 83 \longleftrightarrow$ line in the xy-plane

nonnegative integer solns $\longleftrightarrow$ integer lattice pts. in quadrant 1



No int. lattice pts. on this line

There is no way to make 83 cents out of 6 cent and 15 cent coins.

---

② Algebraically

$$\underbrace{6x + 15y}_{\text{lin. comb. of 6 and 15}} = \underbrace{83}_{\text{not div. by 3}}$$

lin. comb. of 6 and 15

↓

div. by 3

not div. by 3

↓

no integer solns.

$6x + 15y = 21$

Ex: Find a soln. to $6x + 15y = 3$

- Euclidean algorithm $\rightarrow \ldots$
- by inspection: $x = -2$, $y = 1$

Ex: Find a soln. to $6x + 15y = 21$

- inspection: $x = 1$, $y = 1$
- use soln. to $6x + 15y = 3$
  - $\hookrightarrow$ $x = -2$, $y = 1$ solves $6x + 15y = 3$

    So $x = -14$, $y = 7$ solves $6x + 15y = 21$

Ex: Find all solns to $6x + 15y = 3$

Start with a particular soln.

modify

$$6\underset{+5}{(-2)} + 15\underset{-2}{(1)} = 3$$

$$6 \cdot (-2 + 5k) + 15(1-2k) = 3$$

$x = -2 + 5k$
$y = 1 - 2k$
give solns. for all $k \in \mathbb{Z}$

To classify: Suppose $x, y \in \mathbb{Z}$ so that $6x + 15y = 3$

Claim: $x = -2 + 5k$
$y = 1 - 2k$
for some integer k.

We can certainly change vars. to write

$x = -2 + a$ | Let $a = x + 2$
$y = 1 - b$ | $b = 1 - y$

$$3 = 6x + 15y = 6(-2 + a) + 15(1 - b)$$

$= -12 + 6a + 15 - 15b$

$= 3 + 6a - 15b$

$\to 0 = 6a - 15b \to 15b = 6a$

Is a a mult. of 15?

No. $a = 5$, $b = 2$ shows that a need not be a mult. of 15

$$\to 15b = 6a \to \frac{15b}{(15,6)} = \frac{6a}{(15,6)}$$

$$\to 5b = 2a$$

Since 2 is rel. prime to 5, a is a mult. of 5

$a = 5k$ for some k

$5b = 2a \to 5b = 2 \cdot 5k \to b = 2k$

$$x = -2 + a = -2 + 5k$$
$$y = 1 - b = 1 - 2k$$

which is what we wanted to show

Generalizing

Prop: All solns. to $ax + by = c$ have the following form:

① if $(a,b) \nmid c$, there are no solns.

② if $(a,b) \mid c$, then the solns. all have the form

$$x = x_0 + \frac{b}{(a,b)} k$$
$$y = y_0 - \frac{a}{(a,b)} k$$

where $x_0, y_0 \in \mathbb{Z}$ and

$$ax_0 + by_0 = c$$

LCM

Def: For $a, b \in \mathbb{Z}$, the least common multiple of a, b is

$$\operatorname{lcm}(a,b) = \min\{n \in \mathbb{Z}_{>0} : a \mid n \text{ and } b \mid n\}$$

Fact: $\operatorname{lcm}(a,b) = \dfrac{ab}{(a,b)}$

Geometry