CH 7 - Linear Diophantine Equations

Luke Lu • 2025-10-22

Recall the Extended Euclidean Algorithm

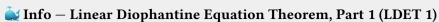
$$253x + 143y = d, d = \gcd(253, 143)$$

i	x	y	r	q
i = 1	1	0	253	0
i = 2	0	1	143	0
i = 3	1	-1	110	1
i=4	-1	2	33	1
i = 5	4	-7	11	3
i = 6	-13	23	0	3

Diophantine Equations

0

 \bigcirc **Tip** — Simplest Linear Diophantine Equation: ax=b



For all integers a, b, and c, with a, b both not zero, the linear Diophantine equation

$$ax + by = c$$

(in variable x and y) has integer solution if and only if $d \mid c$, where $d = \gcd(a, b)$

Proof

Let $a, b, c \in \mathbb{Z}$; $a, b \neq 0$; $d = \gcd(a, b)$

We prove two implications:

1. ⇒

Suppose
$$\exists x_0, y_0 \in \mathbb{Z}, ax_0 + by_0 = c$$

Since $d = \gcd(a, b)$, we have $d \mid a, d \mid b$.

Since $x_0, y_0 \in \mathbb{Z}$, by DIC, $d \mid (ax_0 + by_0)$

2. \Leftarrow Suppose $d \mid c$.

Then by defintion $\exists l \in \mathbb{Z} \text{ s.t } c = l \cdot d$.

By Bézout's Lemma, $\exists s, t \in \mathbb{Z}$ s.t.

as + bt = d. Multiply the equation by $l \Longrightarrow asl + btl = dl = a(ls) + b(lt) = c$.

Since $s, l, t \in \mathbb{Z}$, we have integer solution to the Diophantine equation, namely x = ls, y = lt

Examples:

Are there integer solutions to the following linear Diophantine equation:

1.
$$253x + 143y = 11$$

ANS: YES
$$x = 4, y = -7$$

2.
$$253x + 143y = 155$$

ANS: LDET 1 says there exists a solution if and only if $11\mid 155$.

However, $11 \nmid 155$. Hence there are no integer solutions

3.
$$253x + 143y = 154$$

ANS: LDET 1 says there exists a solution if and only if 11 | 154. 11 | $(11 \cdot 14)$.

By multipling the equation of example 1 by 14:

$$14 \cdot (253x + 143y) = 14 \cdot 11 = 253 \cdot (14x) + 143 \cdot (14y) = 154, x = 56, y = -98$$