

## CH 7 - Linear Diophantine Equations

Luke Lu • 2025-12-17


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

 **Tip** — Simplest Linear Diophantine Equation:  $ax = b$

 **Info** — **Linear Diophantine Equation Theorem, Part 1 (LDET 1)**

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.  $\implies$

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 definition  $\exists l \in \mathbb{Z}$  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  $l \implies asl + btl = dl = a(ls) + b(lt) = c$ .

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

□

**Info – Linear Diophantine Equation Theorem, Part 2 (LDET 2)**

Let  $a, b, c$  be integers with  $a, b$  both not zero, and define  $d = \gcd(a, b)$ . If  $x = x_0$  and  $y = y_0$  is one particular integer solution to the linear Diophantine equation  $ax + by = c$ , then the set of all solutions is given by

$$\left\{ (x, y) : x = x_0 + \frac{b}{d}n, y = y_0 + \frac{a}{d}n, n \in \mathbb{Z} \right\}$$

**Proof**

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

Suppose  $x = x_0, y = y_0$  is one particular solution to LDE  $ax + by = c$

Let  $A = \left\{ (x, y) : x = x_0 + \frac{b}{d}n, y = y_0 + \frac{a}{d}n, n \in \mathbb{Z} \right\}$

Let  $B = \left\{ (x, y) : ax + by = c, x, y \in \mathbb{Z} \right\}$

We want to show

1.  $A \subseteq B$ , suppose  $(x, y) \in A$ , then  $x = x_0 + \frac{b}{d}n, y = y_0 + \frac{a}{d}n, n \in \mathbb{Z}$

Note, since  $d \mid a, d \mid b \implies \frac{b}{d}, \frac{a}{d} \in \mathbb{Z}$

So  $x = x_0 + \frac{b}{d}n \in \mathbb{Z}$  and  $y = y_0 + \frac{a}{d}n \in \mathbb{Z}$

Now substitute in  $x, y$  to then LHS of the linear Diophantine equation.

Then  $ax + by = a\left(x_0 + \frac{b}{d}n\right) + b\left(y_0 + \frac{a}{d}n\right) = ax_0 + \frac{ab}{d}n + by_0 + \frac{ab}{d}n$

$\implies ax_0 + by_0 = c$ .

$\therefore (x, y) \in B \implies A \subseteq B$

2.  $B \subseteq A$  consider  $(x, y) \in B$ , then  $x, y \in \mathbb{Z}$  and  $ax + by = c$ .

We also have  $(x_0, y_0)$  is a solution to the LDE, so  $ax_0 + by_0 = c$

Subtract those equations:  $ax + by - ax_0 - by_0 = 0 \implies a(x - x_0) + b(y - y_0) = 0$

Then  $a(x - x_0) = -b(y - y_0)$

Note, since  $a, b \neq 0, d = \gcd(a, b) > 0, \frac{a}{d}$  and  $-\frac{b}{d} \in \mathbb{Z}$

So  $\frac{a}{d}(x - x_0) = -\frac{b}{d}(y - y_0) \implies \frac{b}{d} \mid \left(\frac{a}{d}(x - x_0)\right)$

By Division by GCD,  $\gcd\left(\frac{a}{d}, -\frac{b}{d}\right) = 1$

By Coprimeness and Divisibility,  $\frac{b}{d} \mid (x - x_0)$ .

By definition of divisibility,  $\exists n \in \mathbb{Z}, x - x_0 = \frac{b}{d}n$  in other words,  $x = x_0 + \frac{b}{d}n$ .

Substitute  $y - y_0 = \frac{b}{d}n$  and isolate:  $-\frac{a}{d}\left(\frac{b}{d}n\right) = -\frac{b}{d}y - by_0 \implies y = y_0 - \frac{a}{d}n$

$\therefore (x, y) \in A$ , so  $B \subseteq A$

□

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  $11 \mid 154$ .  $11 \mid (11 \cdot 14)$ .

By multiplying the equation of example 1 by 14:

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

4.  $343x + 259y = 658$

ANS: Has a solution,  $x = -282, y = 376$

To find all solutions, we apply LEDT 2, the solution set is

$$\{(x, y) : -282 + 37n, y = 376 - 49n, n \in \mathbb{Z}\}$$

5. A customer has a large quantity of dimes and quarters. In how many ways can she pay exactly for an item that costs \$ 2.65?

ANS: Let  $x$  be number of quarters and  $y$  be number of dimes.

Consider LDE:  $25x + 10y = 265$ . We look for non-negative integer solutions.

By inspection,  $x = 9, y = 4$  is one particular solution

By LDET 2, we have  $\{x, y\} : 9 + 2n, 4 - 5n, n \geq 0$ . We get  $n = \{-4, -3, -2, -1, 0\}$  that satisfy the inequalities.