Thm 1.38: If $(a,b)=1$, then there exist integers x and y such that

$$ax+by=1$$

Thm 1.40: There exist integers x and y such that

$$ax+by=(a,b)$$

An equation of the form

$$ax+by=c$$

where a, b, c are integers is called a linear Diophantine equation

x', y'

integer coefficients
+ want integer solutions

Ex: $(36,22)=2=(22,36)$

$\Rightarrow$ there exist integers x and y such that

$$36x+22y=2$$

$x=-3, \quad y=5$

$$36 = 1\cdot 22 + 14 \to 14 = 36 - 22$$
$$22 = 1\cdot 14 + 8 \to 8 = 22 - 14$$
$$14 = 1\cdot 8 + 6 \to 6 = 14 - 8$$
$$8 = 1\cdot 6 + 2 \to 2 = 8 - 1\cdot 6$$
$$6 = 3\cdot 2 + 0$$

$$\begin{aligned}
2 &= 8 - 6 \\
&= 8 - (14 - 8) = 2\cdot 8 - 14 \\
&= 2(22 - 14) - 14 = 2\cdot 22 - 3\cdot 14 \\
&= 2\cdot 22 - 3(36 - 22) \\
&= \boxed{5}\,22 \boxed{-3}\cdot 36
\end{aligned}$$

$110 - 108 = 2$ ✓

Questions:

- $ax + by = c$ has a solution if $c = (a,b)$.

  Does it have more than one solution?

- What if $c \neq (a,b)$? Can $ax + by = c$ still have solutions?

Ex: $36x + 22y = 3$ has <u>no</u> solutions

$36x + 22y = 4$ does have solution(s)

$$\left(36\cdot(-3) + 22\cdot(5) = 2\right) \times 2$$

$$36\cdot(-6) + 22(10) = 4 \quad \checkmark$$

Thms 1.41 - 1.43 are "applications" of Thm 1.38.

<u>Thm 1.42</u>: Let a, b, and n be integers. If $a \mid n$ and $b \mid n$, <u>and $(a,b) = 1$</u>, then $ab \mid n$.

this is important!

<u>Proof</u>: By Thm 1.38, since $(a,b) = 1$, there exist integers x and y such that

$$ax + by = 1. \quad (*)$$

the integers

Since $a \mid n$, we have <u>$n = a\cdot k$</u> for some $k \in \mathbb{Z}$.

"is in"

Similarly, $b \mid n$, so <u>$n = b \cdot \ell$</u> for some $\ell \in \mathbb{Z}$.

Multiply both sides of (*) by n:

$$(ax + by)\,n = n$$

$$axn + byn = n$$

$$ax(bl) + by(ak) = n$$

$$ab(xl + yk) = n.$$

So $(ab) \mid n$. ∎

Thm 1.43: Let a, b, and n be integers.

If $(a, n) = 1$ and $(b, n) = 1$, then $(ab, n) = 1$.

Proof: By Thm 1.38, there exist integers x, y with

$$ax + ny = 1 \quad \rightarrow \quad ax = 1 - ny$$

and integers z and w with

$$bz + nw = 1. \quad \rightarrow \quad bz = 1 - nw$$

So $(ax)\cdot(bz) = (1-ny)(1-nw)$

$$(ab)(xz) = 1 - ny - nw + n^2yw$$
$$= 1 - n(y + w - nyw).$$

Rearrange:

$$ab\underbrace{(xz)}_{\in \mathbb{Z}} + n\underbrace{(y+w-nyw)}_{\in \mathbb{Z}} = 1$$

By Thm 1.39, $(ab, n) = 1.$ ∎

Thm 1.38/1.39:

$$(a,b) = 1 \quad \overset{1.38}{\underset{1.39}{\Longleftrightarrow}} \quad \text{there exist } x, y \in \mathbb{Z} \text{ with } ax + by = 1$$