$$ac \equiv bc \pmod{n}$$

$\to \quad n \mid (ac - bc)$

$\to \quad n \mid (a-b)c$

$\to \quad (a-b)c = nk$ $\qquad\qquad nk = c \cdot \underline{\qquad}$

$\to \quad c \mid (nk)$

$\to \quad c \mid k$ and $\boxed{c \mid n}$ $\qquad n = c \cdot \ell$

$(n, c) = c$

Ex: $c=4$, $n=3$, $k=8$

$4 \mid (3 \cdot 8) \to 4 \mid 8$

Non-Ex: $c = 4$, $n = 6$, $k = 10$

$(c, n) = 2$

$4 \mid (6 \cdot 10)$ but $4 \nmid 6$ and $4 \nmid 10$

Thm 1.41: If $a \mid (bc)$ and $(a, b) = 1$ then $a \mid c$.

$c(a-b) = n \cdot k \to c \mid k$ by 1.41

$k = c \cdot \ell$

$\cancel{c}(a-b) = n(\cancel{c} \cdot \ell) \rightarrow (a-b) = n \cdot \ell$

$\rightarrow n \mid (a-b)$

$\rightarrow a \equiv b \pmod{n}$

<u>Question 1.20</u>: When does

$ac \equiv bc \pmod{n}$ imply $a \equiv b \pmod{n}$?

<u>Answer 1.45</u>: When $(c, n) = 1$.

<u>Ex: $c=4$, $n=3$</u>

$2 \cdot 4 \equiv 5 \cdot 4 \pmod{3} \Rightarrow 2 \equiv 5 \pmod{3}$

$8 \equiv 20 \pmod{3}$ ✓

<u>Non-Ex</u>: <u>$c=4$, $n=6$</u>

$3 \cdot 4 \equiv 12 \cdot 4 \pmod{6} \Rightarrow 3 \not\equiv 12 \pmod{6}$

$12 \equiv 48 \pmod{6}$ ✓

$ax_1 + by_1 = c$

Want: $d = \gcd(a,b)$ divides c

Know: • $d \mid a$ and $d \mid b$

• d is the largest common divisor

$$\left.\begin{array}{l} d \mid a \to a = k \cdot d \\ d \mid b \to b = \ell \cdot d \end{array}\right] \to ax_1 + by_1 = c$$

$$(k\underline{d})x_1 + (\ell \underline{d})y_1 = c$$

$$d(kx_1 + \ell y_1) = c$$

$$\longrightarrow d \mid c.$$

What do we know about linear Diophantine eq's?

Let a, b be integers, not both 0.

1.38/1.39: $ax + by = 1$ has a solution (x and y)

if and only if $(a,b) = 1$

1.48: $ax + by = c$ has a solution (x and y)

if and only if c is a multiple of (a,b)

One question remaining:

How many solutions of

$$ax + by = c$$

are there?

- Zero if (a,b) doesn't divide c.
- At least one if (a,b) divides c.

Can we be more precise?

Yes - there are infinitely many!

Exam 2 next Wed.

- Division alg.
- GCDs
- Euclidean alg.
- Induction
- Linear Diophantine Equations

$ax + by = c \qquad (a,b) = 1, \quad a,b,c > 0$

Will we always have positive solutions $x, y \geq 0$?

No

$3x + 5y = c \qquad (3,5) = 1$

$3(1) + 5(0) = 3$

$3(0) + 5(1) = 5$

$3(1) + 5(1) = 8$

$\vdots$

Positive Solution if

$c = 3, 5$ or ≥ 8

Fix c also: $ax + by = c$

where

- (a,b) divides c
- $a, b, c \geq 0$

$\Rightarrow$ Finitely many solutions (possibly 0) where both $x, y \geq 0$

$$31 \cdot x + 21 \cdot y = 1770$$

Thm 1.48 $\Rightarrow$ there are solutions

Thm 1.51 $\Rightarrow$ there are infinitely many sols

But only a few with $x, y \geq 0$.