DFPF (Divisors from Prime Factorization)

Solving GCD Problems.

- Bézout's Lemma (EEA)
- GCD CT
- GCD WR
- Definition
- GCD PF

L23P2

Q1. I enjoy trying to discover and write MATH 135 proofs.

A) Strongly disagree

B) Disagree

C) Neither agree nor disagree

D) Agree

E) Strongly agree

Q2.When I have difficulties with MATH 135 proofs, I know I can handle them.

A) Strongly disagree

B) Disagree

C) Neither agree nor disagree

D) Agree

E) Strongly agree

Q3. Let $a, b, x, y \in \mathbb{Z}$.

Which one of the following statements is true?

A) If $ax + by = 6$, then $\gcd(a, b) = 6$.

B) If $\gcd(a, b) = 6$, then $ax + by = 6$. X

C) If $a = 12b + 18$, then $\gcd(a, b) = 6$.

D) If $ax + by = 1$, then $\gcd(6a, 6b) = 6$. $\Rightarrow \gcd(a,b)=1$ $\Rightarrow \gcd(6a, 6b) = 6$

E) If $\gcd(a, b) = 3$ and $\gcd(x, y) = 2$, then $\gcd(ax, by) = 6$.

# Linear Diophantine Equations (LDE)

Want to solve

$$ax + by = c$$

where $a, b, c \in \mathbb{Z}$.

Catch! $x, y \in \mathbb{Z}$.

Ex: Solve $143x + 253y = 11$

Solve using EEA!

| x | y | r |
|---|---|---|
| 0 | 1 | 253 |
| 1 | 0 | 143 |
| -1 | 1 | 110 |
| 2 | -1 | 33 |
| -7 | 4 | 11 |
| 23 | -13 | 0 |

$\therefore 143(-7) + 253(4) = 11$

Questions about LDEs.
- Is there a solution?
- ~~Is~~ What is it?
- Is there more than one?

Q: Solve the LDE

$$143x + 253y = 155$$

Assume towards a contradiction that $\exists x_0, y_0 \in \mathbb{Z}$ s.t.

$$143x_0 + 253y_0 = 155$$

By before, $11 \mid 143$ & $11 \mid 253$

Hence by DIC $143x_0 + 253y_0$ is divisible by 11. BUT $11 \nmid 155 = 143x_0 + 253y_0$

#. Hence the original LDE has no integer solutions.

What about

$$143x + 253y = 154$$

$154 = 11 \cdot 14$.

$$143(-7) + 253(4) = 11$$

Multiply by 14

$$143(-7 \cdot 14) + 253(4 \cdot 14) = 154$$

$$143(-98) + 253(56) = 154.$$

<u>LDE T1</u>

Let $d = \gcd(a,b)$. The LDE

$$ax + by = c$$

has a solution iff $d \mid c$.

<u>Pf</u>: $\Rightarrow$ ~~\$~~ Assume $ax+by=c$ has an integer solution, say $x_0, y_0 \in \mathbb{Z}$. Since $d \mid a$ and $d \mid b$, by DIC

$$d \mid ax_0 + by_0 = c.$$

$\Leftarrow$ Assume $d \mid c$. Then $\exists k \in \mathbb{Z}$ s.t. $dk = c$. By Bézout's Lemma $\exists u, v \in \mathbb{Z}$ s.t.

$$au + bv = \gcd(a,b) = d.$$

Mult by $k$ $\quad a(uk) + b(vk) = dk = c$

$\therefore$ a solution is $x = uk$

$\qquad y = vk$ $\Leftarrow$.

Ex: $20x + 35y = 5$ (Solve the LDE)

Simplify: $4x + 7y = 1$

A solution is $x = 2$ $\quad y = -1$

Look at $x_2 = 2 + 7(2)$ $\quad y_2 = -1 - 4(2)$

$$4x_2 + 7y_2 = 4(2 + 7(2)) + 7(-1 - 4(2))$$
$$= 4 \cdot 2 + \cancel{4 \cdot 7(2)} + 7(-1) - \cancel{7 \cdot 4(2)}$$
$$= 4x + 7y$$
$$= 1$$