Lecture 24

Handout or Document Camera or Class Exercise

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 $ax + by = 6$.

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

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

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

Solution: Answer: If $ax + by = 1$, then $\gcd(6a, 6b) = 6$.

Theorem: (LDET2) Let $d = \gcd(a, b)$ where $a \neq 0$ and $b \neq 0$. If $(x, y) = (x_0, y_0)$ is a solution to the LDE

$$ax + by = c$$

then all solutions are given by

$$x = x_0 + \tfrac{b}{d}n \qquad y = y_0 - \tfrac{a}{d}n$$

for all $n \in \mathbb{Z}$. Alternatively, the solution set is given by

$$\{(x_0 + \tfrac{b}{d}n, y_0 - \tfrac{a}{d}n) : n \in \mathbb{Z}\}$$

Proof: Note that the above are actually solutions to the LDE. It suffices to show that these are all the solutions. Let (x, y) be a different solution to the LDE (other than (x_0, y_0)). Then,

$$\begin{aligned} ax + by &= c \\ ax_0 + by_0 &= c \end{aligned}$$

Subtracting gives

$$\begin{aligned} a(x - x_0) + b(y - y_0) &= 0 \\ a(x - x_0) &= -b(y - y_0) \\ \tfrac{a}{d}(x - x_0) &= \tfrac{-b}{d}(y - y_0) \end{aligned}$$

Now, since $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$ (by DBGCD) and since

$$\tfrac{b}{d} \mid \tfrac{-b}{d}(y - y_0) = \tfrac{a}{d}(x - x_0)$$

we use Coprimeness and Divisibility (CAD) to see that $\frac{b}{d} \mid (x - x_0)$. Thus, there exists an integer n such that $x - x_0 = \frac{b}{d}n$ and thus, $x = x_0 + \frac{b}{d}n$. Plug this into the following:

$$\begin{aligned} \tfrac{a}{d}(x - x_0) &= \tfrac{-b}{d}(y - y_0) \\ \tfrac{a}{d} \cdot \tfrac{b}{d}n &= \tfrac{-b}{d}(y - y_0) \\ \tfrac{-a}{d}n &= y - y_0 \end{aligned}$$

Hence, $y = y_0 - \frac{a}{d}n$ completing the proof. ■

Instructor's Comments: Something to note about the proof. An argument using 'similarly' won't work above since you want to ensure that the n you get from doing the above (and the one you would get by arguing 'similarly') is the same.

Instructor's Comments: This is the 20 minute mark.

Example: Alice has a lot of mail to send. She wishes to spend exactly 100 dollars buying 49 cent and 53 cent stamps. In how many ways can she do this?

Solution: Let x be the number of 49 cent stamps. Let y be the number of 53 cent stamps. Note that $x, y \in \mathbb{Z}$ and that $x, y \geq 0$. We want to solve

$$\begin{aligned} 0.49x + 0.53y &= 100 \\ 49x + 53y &= 10000 \end{aligned}$$

x	y	r	q
0	1	53	0
1	0	49	0
-1	1	4	1
13	-12	1	12
*	*	0	4

We solve this using the Extended Euclidean Algorithm:

Therefore, $49(13) + 53(-12) = 1$. Hence, $49(130000) + 53(-120000) = 10000$. Thus, by LDET2, all solutions are given by

$$\begin{aligned} x &= 130000 - 53n \\ y &= -120000 + 49n \end{aligned}$$

for all $n \in \mathbb{Z}$. Now, to answer the question, we need to determine all the answers that make sense. Since x and y are physical quantities, we know that $x \geq 0$ and $y \geq 0$. The first condition gives

$$\begin{aligned} x &\geq 0 \\ 130000 - 53n &\geq 0 \\ 2452 + \frac{44}{53} = \frac{130000}{53} &\geq n \end{aligned}$$

whereas the second condition gives

$$\begin{aligned} y &\geq 0 \\ -120000 + 49n &\geq 0 \\ n &\geq \frac{120000}{49} = 2448 + \frac{48}{49} \end{aligned}$$

Since $n \in \mathbb{Z}$, we see that $2449 \leq n \leq 2452$. Thus there are 4 possible solutions. ■

Instructor's Comments: Watch for the off by one error! This is the 30-35 minute mark

Handout or Document Camera or Class Exercise

Find all non-negative integer solutions to $15x - 24y = 9$ where $x \leq 20$ and $y \leq 20$.

Solution: Dividing by 3 gives

$$5x - 8y = 3$$

By inspection, $x_0 = -1$ and $y_0 = -1$ is a solution. Since $\gcd(5, -8) = 1$, by LDET2 we have that the complete solution set is given by

$$\begin{aligned} x &= -1 - (-8)n = -1 + 8n \\ y &= -1 + 5n \end{aligned}$$

for all $n \in \mathbb{Z}$. By the statement,

$$\begin{aligned} 0 \leq \quad & x \quad \leq 20 \\ 0 \leq -1 + & 8n \leq 20 \\ 1 \leq \quad & 8n \quad \leq 21 \end{aligned}$$

Giving $n = 1, 2$ and

$$\begin{aligned} 0 \leq \quad & y \quad \leq 20 \\ 0 \leq -1 + & 5n \leq 20 \\ 1 \leq \quad & 5n \quad \leq 21 \end{aligned}$$

giving $n = 1, 2, 3, 4$. Hence the overlap of $n = 1$ or $n = 2$ gives all solutions. These are given by $(7, 4)$ and $(15, 9)$. ■

Instructor's Comments: This is the 40-45 minute mark.

Instructor's Comments: This last page is to motivate the switch to congruences. This is where the number theory really kicks off. If you get the opportunity to, mention the definition of congruences. Seeing this definition once or twice is really useful. Students should be told to commit this to memory quickly otherwise these next two weeks will seem unnecessarily difficult.

Congruences

Idea: Simplify problems in divisibility.

(i) Is 156723 divisible by 11?

(ii) What angle do you get after a 1240 degree rotation?

(iii) What time is it 400 hours from now?

Note: We only care about the above values up to multiples of 11, 360 and 24.

Definition: Let $m \in \mathbb{N}$. We say that two integers a and b are congruent modulo m if and only if $m \mid (a-b)$ and we write $a \equiv b \pmod{m}$. If $m \nmid (a-b)$, we write $a \not\equiv b \pmod{m}$.

Instructor's Comments: It's important enough to mention again - commit the previous definition to memory!!!

Example:

$$7 \equiv 4 \pmod{3}$$
$$4 \equiv 7 \pmod{3}$$
$$4 \equiv 4 \pmod{3}$$
$$7 \not\equiv 4 \pmod{4}$$
$$10 \equiv 15 \pmod{5}$$
$$15 \equiv 30 \pmod{5}$$
$$10 \equiv 30 \pmod{5}$$