

## Lecture 23

**Instructor's Comments: If you ran out of time last lecture, you should give students the following tips.**

When solving GCD problems, the following gives a rough order of how and when you should try a technique

- (i) Bézout's Theorem (EEA) [Good when gcd is in hypothesis]
- (ii) GCDWR [Good when terms in gcd depend on each other; good for computations]
- (iii) GCDCT [Good when gcd is in conclusion]
- (iv) Definition [Good when nothing else seems to work]
- (v) GCDPF [Good when you're desperate]

Handout or Document Camera or Class Exercise

Find  $x, y \in \mathbb{Z}$  such that  $143x + 253y = \gcd(143, 253)$ .

Determine which of the following equations are solvable for integers  $x$  and  $y$ :

(i)  $143x + 253y = 11$

(ii)  $143x + 253y = 155$

(iii)  $143x + 253y = 154$

**Instructor's Comments:** The answers to these questions will be part of the lecture today.

## Linear Diophantine Equations (LDE)

We want to solve  $ax + by = c$  where  $a, b, c \in \mathbb{Z}$  under the condition that  $x, y \in \mathbb{Z}$

**Instructor's Comments:** Relate this to solving for the equation of a line over the real case and invite students to think critically about the difference in the integer case.

**Example:** Solve the LDE  $143x + 253y = 11$ .

**Solution:** We can solve this using the Extended Euclidean Algorithm!

x	y	r	q
0	1	253	
1	0	143	
-1	1	110	1
2	-1	33	1
-7	4	11	3
23	-13	0	3

Therefore,  $143(-7) + 253(4) = 11$ . Are there other solutions?

**Instructor's Comments:** This is the 10-15 minute mark depending on the introduction. Students should do the EEA on their own and you should do it simultaneously.

Questions to ask about LDE's

- (i) Is there a solution?
- (ii) What is it?
- (iii) Are there more than one?

**Example:** Solve the LDE

$$143x + 253y = 155$$

**Solution:** Assume towards a contradiction that there exist  $x_0$  and  $y_0$  integers such that

$$143x_0 + 253y_0 = 155$$

By before,  $11 \mid 143$  and  $11 \mid 253$ . Hence by Divisibility of Integer Combinations,  $143x_0 + 253y_0$  is divisible by 11. HOWEVER,

$$11 \nmid 155 = 143x_0 + 253y_0$$

which is a contradiction. Hence the original LDE has no integer solutions. ■

**Instructor's Comments:** This is the 25 minute mark.

What about

$$143x + 253y = 154$$

as an LDE? Now, notice that  $154 = 11 \cdot 14$ . Hence, since

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

multiplying by 14 gives

$$\begin{aligned}143(-7 \cdot 14) + 253(4 \cdot 14) &= 11 \cdot 14 \\143(-98) + 253(56) &= 154\end{aligned}$$

**Instructor's Comments: This is the 35 minute mark.**

These insights lead to the following theorem

**Theorem:** (LDET1) Let  $d = \gcd(a, b)$ . The LDE

$$ax + by = c$$

has a solution if and only if  $d \mid c$ .

**Proof:** ( $\Rightarrow$ ) Assume that  $ax + by = c$  has an integer solution, say  $x_0, y_0 \in \mathbb{Z}$ . Since  $d \mid a$  and  $d \mid b$ , by Divisibility of Integer Combinations, we have that  $d \mid (ax_0 + by_0) = c$ .

( $\Leftarrow$ ) Assume that  $d \mid c$ . Then, there exists an integer  $k$  such that  $dk = c$ . By Bézout's Lemma, there exist integers  $u$  and  $v$  such that  $au + bv = \gcd(a, b) = d$ . Multiplying by  $k$  gives

$$a(uk) + b(vk) = dk = c$$

Therefore, a solution is given by  $x = uk$  and  $y = vk$ . ■

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

**Example:** Solve  $20x + 35y = 5$  as an LDE.

**Solution:** Notice here that we can simplify the LDE by dividing by 5 first to give

$$4x + 7y = 1$$

An easy solution is given by  $x = 2$  and  $y = -1$ .

Now, look at  $x_2 = 2 + 7$  and  $y_2 = -1 - 4$ . Notice that

$$\begin{aligned}4x_2 + 7y_2 &= 4(2 + 7) + 7(-1 - 4) \\&= 4(2) + 4(7) + 7(-1) + 7(-4) \\&= 4(2) + 7(-1) \\&= 4x + 7y \\&= 1\end{aligned}$$

In fact, if I take  $x_2 = 2 + 7(11)$  and  $y_2 = -1 - 4(11)$ . Notice that

$$\begin{aligned}4x_2 + 7y_2 &= 4(2 + 7(11)) + 7(-1 - 4(11)) \\&= 4(2) + 4(7)(11) + 7(-1) + 7(-4)(11) \\&= 4(2) + 7(-1) \\&= 4x + 7y \\&= 1\end{aligned}$$

and 11 above is very arbitrary. In fact, this gives us an insight into the complete characterization of solutions for an LDE.