

# Lecture 4

Mon, Feb 4, 2019

- Review the Euclidean Algorithm. (Transparency)
- Review Thm:  $d > 0, d | a, d | b, \exists x, y \in \mathbb{Z} \text{ such that } ax + by = d \Rightarrow d = \gcd(a, b)$ .

Lemma: Let  $a, b, x_1, x_2, y_1, y_2, r_1, r_2$  be integers. If

$$(1) \quad ax_1 + by_1 = r_1 \quad \text{and}$$

(2)  $ax_2 + by_2 = r_2$ , then for every integer  $g$

$$(1) - g(2) \quad a(x_1 - gx_2) + b(y_1 - gy_2) = r_1 - gr_2.$$

$$\text{Pf: LHS} = (ax_1 + by_1) - g(ax_2 + by_2) \stackrel{\substack{(1) \\ \text{and} \\ (2)}}{=} r_1 - gr_2. \quad \square$$

Note: If we set  $x_3 = x_1 - gx_2, y_3 = y_1 - gy_2, r_3 = r_1 - gr_2$ , then the above Lemma states:

If  $(x_1, y_1, r_1), (x_2, y_2, r_2)$  satisfy  
 $ax_i + by_i = r_i, \quad i = 1, 2$

then so does the triple  $(x_3, y_3, r_3)$ .

(1)

The Extended Euclidean Algorithm (for finding  $\gcd(a, b)$ ) as well as a solution  $(x, y)$  for the Diophantine Equation  $ax + by = \gcd(a, b)$ .

Let  $a > b > 0$  be natural numbers

Construct the following table:

$$ax_i + by_i = r_i$$

Row	$x_i$	$y_i$	$r_i$	$g_i$
1)	1	0	$a$	-
2)	0	1	$b$	-
3)	$x_3$	$y_3$	$r_3$	$g_3$

The first two rows are INITIALISED with the above values.

$m$ )	$x_m$	$y_m$	$r_m$	$g_m$	$\gcd(a, b)$
$m+1$ )	$x_{m+1}$	$y_{m+1}$	0		

General step: Generating row  $i \geq 3$ .

Let  $r_i, g_i$  be the unique pair of integers such that  $r_{i-2} = g_i r_{i-1} + r_i$ ,  $0 \leq r_i < r_{i-1}$ .

$$\text{Let } (x_i, y_i, r_i) = (x_{i-2}, y_{i-2}, r_{i-2}) - g_i(x_{i-1}, y_{i-1}, r_{i-1})$$

$$\text{Ex: } (x_3, y_3, r_3) = (x_1, y_1, r_1) - g_3(x_2, y_2, r_2)$$

as in the previous comment.

STOP when  $r_{n+1} = 0$ .  $\square$

### Conclusion:

(i) The last non-zero  $r_n$  is  $\gcd(a, b)$ .

(ii) Every row  $(x_i, y_i, r_i)$  satisfies  $ax_i + by_i = r_i$ .

(iii) One integer solution to

$$ax + by = \gcd(a, b) \text{ is } x = x_m, y = y_m.$$

Proof (i) The  $r_i$  column is just the sequence of remainders in the Euclidean Algorithm. We already know that the last non-zero remainder is  $\gcd(a, b)$ . Indeed

$$\begin{matrix} \gcd(a, b) &= \gcd(b, r_3) &= \gcd(r_3, r_4) &= \cdots &= \gcd(r_m, r_{m+1}) \\ \downarrow & \downarrow & \downarrow & \ddots & \downarrow \\ r_1 & r_2 & r_2 & & r_m \end{matrix}$$

(ii) True for  $i = 1, 2$ , by the initiation. Follows for all  $i$ , by Strong Induction and the Lemma.

(iii) Follows immediately from (i) and (ii).  $\square$

Example:  $a = 381$ ,  $b = 72$

$$ax_i + by_i = r_i$$

	$x_i$	$y_i$	$r_i$	$g_i$
1)	1	0	381	-
2)	0	1	72	-
3)	1	-5	21	5
4)	-3	16	9	3
5)	7	-37	3	2

$$\text{gcd}(381, 72)$$

$$7 \cdot 381 + (-37) \cdot 72 = 3$$

Ex:  $a = 154$ ,  $b = 105$

	$x_i$	$y_i$	$r_i$	$g_i$
1)	1	0	154	
	0	1	105	
	1	-1	49	1
	-2	3	7	2

$$\text{gcd}(154, 105)$$

$$-2 \cdot 154 + 3 \cdot 105 = 7$$

(4)

Question: Does the equation

$$154x + 105y = 2$$

has an integer solution  $x, y \in \mathbb{Z}$ ?

A. No!  $\gcd(154, 105) = 7 \nmid 2$ .

Theorem 5.1.2: Let  $a, b$  be integers, not both zero. The Diophantine eq  $ax+by=c$  has a solution  $\Leftrightarrow \gcd(a, b) | c$ .