

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

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

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

$$(2) \quad ax_2 + by_2 = r_2, \quad \text{then for every integer } g$$

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

$$\text{Pf: LHS} = (ax_1 + by_1) - g(ax_2 + by_2) \stackrel{(1)}{=} r_1 - g r_2 \stackrel{(2)}{=} r_1 - g r_2. \quad \square$$

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) .

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	δ_i
1)	1	0	a	—
2)	0	1	b	—
3)	x_3	y_3	r_3	δ_3

The first two rows are INITIALISED with the above values.

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

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

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

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

Ex: $(x_3, y_3, r_3) = (x_1, y_1, r_1) - q_3 (x_2, y_2, r_2)$
as in the previous comment.

STOP: When $r_{m+1} = 0$. (2)

Conclusion:

(i) The last non-zero r_m 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

$$\gcd(a, b) = \gcd(r_1, r_2) = \gcd(r_2, r_3) = \dots = \gcd(r_m, r_{m+1})$$

$r_1 \quad r_2 \quad r_2 \quad r_3 \quad r_3 \quad r_4 \quad r_4 \quad r_5 \quad r_5 \quad r_6 \quad r_6 \quad r_7 \quad r_7 \quad r_8 \quad r_8 \quad r_9 \quad r_9 \quad r_{10} \quad r_{10} \quad r_{11} \quad r_{11} \quad r_{12} \quad r_{12} \quad r_{13} \quad r_{13} \quad r_{14} \quad r_{14} \quad r_{15} \quad r_{15} \quad r_{16} \quad r_{16} \quad r_{17} \quad r_{17} \quad r_{18} \quad r_{18} \quad r_{19} \quad r_{19} \quad r_{20} \quad r_{20} \quad r_{21} \quad r_{21} \quad r_{22} \quad r_{22} \quad r_{23} \quad r_{23} \quad r_{24} \quad r_{24} \quad r_{25} \quad r_{25} \quad r_{26} \quad r_{26} \quad r_{27} \quad r_{27} \quad r_{28} \quad r_{28} \quad r_{29} \quad r_{29} \quad r_{30} \quad r_{30} \quad r_{31} \quad r_{31} \quad r_{32} \quad r_{32} \quad r_{33} \quad r_{33} \quad r_{34} \quad r_{34} \quad r_{35} \quad r_{35} \quad r_{36} \quad r_{36} \quad r_{37} \quad r_{37} \quad r_{38} \quad r_{38} \quad r_{39} \quad r_{39} \quad r_{40} \quad r_{40} \quad r_{41} \quad r_{41} \quad r_{42} \quad r_{42} \quad r_{43} \quad r_{43} \quad r_{44} \quad r_{44} \quad r_{45} \quad r_{45} \quad r_{46} \quad r_{46} \quad r_{47} \quad r_{47} \quad r_{48} \quad r_{48} \quad r_{49} \quad r_{49} \quad r_{50} \quad r_{50} \quad r_{51} \quad r_{51} \quad r_{52} \quad r_{52} \quad r_{53} \quad r_{53} \quad r_{54} \quad r_{54} \quad r_{55} \quad r_{55} \quad r_{56} \quad r_{56} \quad r_{57} \quad r_{57} \quad r_{58} \quad r_{58} \quad r_{59} \quad r_{59} \quad r_{60} \quad r_{60} \quad r_{61} \quad r_{61} \quad r_{62} \quad r_{62} \quad r_{63} \quad r_{63} \quad r_{64} \quad r_{64} \quad r_{65} \quad r_{65} \quad r_{66} \quad r_{66} \quad r_{67} \quad r_{67} \quad r_{68} \quad r_{68} \quad r_{69} \quad r_{69} \quad r_{70} \quad r_{70} \quad r_{71} \quad r_{71} \quad r_{72} \quad r_{72} \quad r_{73} \quad r_{73} \quad r_{74} \quad r_{74} \quad r_{75} \quad r_{75} \quad r_{76} \quad r_{76} \quad r_{77} \quad r_{77} \quad r_{78} \quad r_{78} \quad r_{79} \quad r_{79} \quad r_{80} \quad r_{80} \quad r_{81} \quad r_{81} \quad r_{82} \quad r_{82} \quad r_{83} \quad r_{83} \quad r_{84} \quad r_{84} \quad r_{85} \quad r_{85} \quad r_{86} \quad r_{86} \quad r_{87} \quad r_{87} \quad r_{88} \quad r_{88} \quad r_{89} \quad r_{89} \quad r_{90} \quad r_{90} \quad r_{91} \quad r_{91} \quad r_{92} \quad r_{92} \quad r_{93} \quad r_{93} \quad r_{94} \quad r_{94} \quad r_{95} \quad r_{95} \quad r_{96} \quad r_{96} \quad r_{97} \quad r_{97} \quad r_{98} \quad r_{98} \quad r_{99} \quad r_{99} \quad r_{100} \quad r_{100}$

(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	q_i
1)	1	0	381	-
2)	0	1	72	-
3)	1	-5	21	5
4)	-3	16	9	3
5)	7	-37	3	2
			0	

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

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

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

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

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

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

(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 $\Leftrightarrow \gcd(a, b) \mid c$.