Lecture 3:

Review:

Lemma: Let $a \in \mathbb{Z}$, $b \in \mathbb{N}$ and write $a = qb + r$, $0 \leq r < b$. Then

$$\gcd(a,b) = \gcd(b,r).$$

Thm: (The Euclidean Algorithm)

Let $a, b \in \mathbb{N}$ with $a \geq b$.

(i) If $b \mid a$, then $\gcd(a,b) = b$.

(ii) If $b \nmid a$, then $\gcd(a,b)$ is the last non-zero remainder r_n in the following list of equations provided by the Division Theorem:

$$a = q_1 b + r_1, \quad 0 < r_1 < b$$

$$b = q_2 r_1 + r_2, \quad 0 \leq r_2 < r_1$$

$$\vdots$$

$$r_{n-2} = q_{n-2} r_{n-1} + \boxed{r_n}$$

$$r_{n-1} = q_{n+1} r_n + \underbrace{0}_{r_{n+1}}.$$

The algorithm terminates after finitely many steps.

Example: $\gcd(381, 72) = 3$

$$381 \cdot \overset{x}{\boxed{7}} + 72 \overset{y}{\boxed{-37}} = 3$$

Example: (Redone using the "Extended Euclidean Algorithm"),

$$381 \cdot x + 72y = 3 = \gcd(381, 72)$$

Consider the list of equation

$$381 x_i + 72 y_i = r_i$$

i	x_i	y_i	r_i	q_i
1)	1	0	381	—
2)	0	1	72	—
3)	1	-5	21	$q_3 = 5$, where $381 = 72 q_3 + r_3$ ($0 \le r_3 < 72$) Add $-5 \cdot \text{Row}_2$ to Row_1
4)	-3	16	9	$q_4 = 3$ Add $-3 \cdot \text{Row}_2$ to Row_2
5)	7	-37	$\boxed{3}$	$q_5 = 2$, $\gcd(381, 72)$
			$r_6 = 0$	$q_6 = 3$

Eq_1 $\quad 381 \cdot \boxed{1} + 72 \cdot \boxed{0} = 381$

Eq_2 $\quad 381 \cdot \boxed{0} + 72 \cdot \boxed{1} = 72$

Eq 3 $\quad 381 \cdot \boxed{1} + 72 \boxed{-5} = 21$ Add $-5 \cdot$ Eq 4 to Eq 1.

$\vdots$

$$\text{Eq } 5 \quad 381 \cdot \underbrace{\boxed{7}}_{=x_5} + 72 \underbrace{\boxed{-37}}_{=y_5} = \underbrace{3}_{=r_5}$$

We found a soln $(x, y) = (7, -37)$ to the eq $381 \cdot x + 72 \cdot y = 3 = \gcd(381, 72)$

Theorem: (The Extended Euclidean Alg)

(For finding $\gcd(a,b)$ and a solution for $ax + by = \gcd(a,b)$ with $x, y \in \mathbb{Z}$).

Let $a > b > 0$ be natural numbers. Construct the following table:

$a x_i + b y_i = r_i$

Row	x_i	y_i	r_i	q_i
1)	1	0	a	—
2)	0	1	b	—
3)				

The first two rows are initialized with the above values.

General step: (Generating row $i \geq 3$)

$i-2$	x_{i-2}	y_{i-2}	r_{i-2}	
$i-1$	x_{i-1}	y_{i-1}	r_{i-1}	
i	$x_i = x_{i-2} - q_i x_{i-1}$	$y_i = y_{i-2} - q_i y_{i-1}$	r_i	q_i and r_i are the sol'n $\boxed{r_{i-2} = q_i \cdot r_{i-1} + r_i}$ $0 \leq r_i < r_{i-1}$

$\text{Row}_i = \text{Row}_{i-2} - q_i \text{Row}_{i-1}$

Stop! when $r_{n+1} = 0$.

Conclusion:

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

(ii) Every row (x_i, y_i, r_i) satisfies

$$a x_i + b y_i = r_i$$

(iii) One integral solution to $ax + by = \gcd(a,b)$ is

$x = x_n$ and $y = y_n$ (because $r_n = \gcd(a,b)$)

Ex: $a = 154$, $b = 105$, $ax + by = \gcd(a,b)$

$$154 x_i + 105 y_i = r_i$$

x_i	y_i	r_i	q_i
1	0	154	—
0	1	105	—
1	-1	49	1
-2	3	$\boxed{7}$	2
		0	7

$\gcd(154, 105)$

$$154 \cdot \boxed{-2} + 105 \boxed{3} = 7$$

$$Row_3 = Row_1 - \underset{\overset{\|}{1}}{q_3} Row_2$$

Question: Does the equation

$$154x + 105y = 2$$

have an integer solution (x, y), $x, y \in \mathbb{Z}$?

Answer: No. 7 divides the L.H.S for every choice of integers x, y, but $7 \nmid 2$.

Corollary: (Of the Extended Euclidean Algorithm Theorem).

Let $a, b \in \mathbb{Z}$, not both zero. Then the Diophantine Equation

$$ax + by \overset{(*)}{=} c,$$

$c \in \mathbb{Z}$, has a solution, if and only if $\gcd(a, b) \mid c$.

Proof: If $\gcd(a,b) \nmid c$, then a solution does not exist, since for every $x, y \in \mathbb{Z}$, $\gcd(a,b)$ divides the R.H.S of (*).

Suppose that $\gcd(a,b) \mid c$, so $c = q \cdot \gcd(a,b)$, $q \in \mathbb{Z}$,

Let (x_0, y_0) be the solution to

$$ax + by = \gcd(a,b)$$

provided by the E.E.A.

$$ax_0 + by_0 = \gcd(a,b).$$

Multiplying both sides by q we get

$$a\underbrace{(qx_0)}_{x} + b\underbrace{(qy_0)}_{y} = \underbrace{q \cdot \gcd(a,b)}_{c}$$

So (qx_0, qy_0) is a sol'n to (*). ∎

$$154 \cdot \boxed{-2} + 105 \boxed{3} = 7$$

(*)

Question: Find <u>all</u> solution of the Linear Diophantine Eq

$$154x + 105y \overset{(**)}{=} 14.$$

$$14 = 2 \cdot 7$$

$(x_0, y_0) = 2(-2,3) = (-4,6)$

is a solution of (**).

Note that if (x_h, y_h) is a solution of

$$154x + 105y \underset{\text{Homog.}}{=} 0,$$ then

for every $k \in \mathbb{Z}$, $(x_0, y_0) + k(x_h, y_h) =$

$= (x_0 + kx_h, y_0 + ky_h)$

is a solution to (**). Indeed

$154(x_0 + kx_h) + 105(y_0 + ky_h) =$

$$\underbrace{154x_0 + 105y_0}_{14} + k\underbrace{(154x_h + 105y_h)}_{0} = 14.$$

$$154 \underbrace{\boxed{\left(-\frac{105}{7}\right)}}_{x_h} + 105 \underbrace{\boxed{\frac{154}{7}}}_{y_h}$$

$-\frac{105}{7} = -15$, $\frac{154}{7} = 22$

$(x_n, y_n) = (-15, 22).$

The set

$$\left\{ (x,y) = (\underbrace{-4 + \mathfrak{z}(-15)}^{x_0 + \mathfrak{z} x_n},\ 6 + \mathfrak{z}\, 22) \right\}$$

is a set of solution to (**).

Theorem: I) Let $a, b \in \mathbb{Z}$ be relatively prime and let (x_0, y_0) be a solution to the Diophantine equation

$$ax + by = c, \quad c \in \mathbb{Z}. \tag{+}$$

Then the solution set of the above equation is exactly:

$$S = \{ (x_0 - \mathfrak{z} b,\ y_0 + \mathfrak{z} a) : \mathfrak{z} \in \mathbb{Z} \}.$$

Ex:
$22x + 15y = c$

II) If $a, b \in \mathbb{Z}$ are not relatively prime, but $\gcd(a,b) = d \neq 0$, and (x_0, y_0) is a solution of (+), then the solution set is

$$S = \left\{ \left(x_0 - \mathfrak{z}\frac{b}{d},\ y_0 + \mathfrak{z}\frac{a}{d}\right) : \mathfrak{z} \in \mathbb{Z} \right\}$$

For the proof we need the following;

Euclid's Lemma;