Lecture 3

The Bézout's Identity

Theorem: Let $a, b \in \mathbb{Z} \setminus \{0\}$. Then there exist (not necessarily unique) integers u and v such that $\gcd(a,b) = au + bv$.

Moreover, $\gcd(a,b)$ is the smallest positive integer of the form $au + bv$.

Proof: Let $S := \{ am + bn \mid m, n \in \mathbb{Z} \text{ and } am + bn > 0 \} \subseteq \mathbb{N}$.

STEP 1: $\boxed{\text{Find the smallest element of } S.}$

Observe that $a^2 + b^2 > 0$ and $a^2 + b^2 \in S$, i.e. $S \neq \emptyset$.

By the Well-Ordering Axiom, S contains a smallest element, call it d.

By definition of S, $d = au + bv$ for some $u, v \in \mathbb{Z}$.

STEP 2: Prove that $d = \gcd(a,b)$. This is, prove that

(1) $d \mid a$ and $d \mid b$.

(2) If $c \mid a$ and $c \mid b$, then $c \leq d$.

(1) By the Division Algorithm, applied to a and d (observe that $d>0$)

$$\exists!\, q, r \in \mathbb{Z} \text{ st } 0 \leq r < d \text{ and } a = dq + r.$$

If $r > 0$, then

$$0 < r = a - dq = a - (au + bv)q = a(1 - uq) + b(vq),$$

this means $r \in S$ and $r < d$. Contradiction!!!

because d is the smallest element of S.

Then $r = 0$, i.e. $a = dq$. Thus $d \mid a$.

A similar argument shows that $d \mid b$.

(2) Let c be another common divisor of a and b, i.e. $c \mid a$ and $c \mid b$.

Then $\exists\, k, l \in \mathbb{Z}$ st $a = ck$ and $b = cl$.

$$\Rightarrow \quad d = au + bv = (ck)u + (cl)v = c(ku + lv)$$

$$\Rightarrow \quad c \mid d$$

$$\Rightarrow \quad c \leq |d| \qquad \text{from Proposition 2}$$

$$\Rightarrow \quad c \leq d \qquad \text{because } d > 0$$

Thus, $\gcd(a,b) = au + bv$.

$\blacksquare$

Corollary 4: Let $a, b \in \mathbb{Z} \setminus \{0\}$. If $c = ax + by$ for some $x, y \in \mathbb{Z}$, then $\gcd(a,b) \mid c$.

Other elements of S are multiples of $\gcd(a,b) = au + bv$

Proof: Exercise.

!!! **Corollary 5:** Let $a, b \in \mathbb{Z} \setminus \{0\}$, and let d be a positive integer.

Another def of gcd

$d = \gcd(a,b)$ iff d satisfies the following

(1) $d \mid a$ and $d \mid b$

(2) If $c \mid a$ and $c \mid b$, then $c \mid d$.

Proof: Read Corollary 1.3 in Hungerford's book.

!!! **Corollary 6:** Integers a and b are relatively prime if and only if there exist integers x and y so that $ax + by = 1$.

Proof:

($\Rightarrow$) We have that $1 = \gcd(a,b) = ax + by$ for some $x, y \in \mathbb{Z}$.

($\Leftarrow$) Suppose $ax + by = 1$ for some $x, y \in \mathbb{Z}$. By Corollary 5 we have $\gcd(a,b) \mid 1$, then $\gcd(a,b) = 1$.

Proposition 7: If $a \mid bc$ and $\gcd(a,b) = 1$, then $a \mid c$.

Proof: There are $x, y \in \mathbb{Z}$ s.t. $ax + by = 1$, then $acx + bcy = c$.

Since $a \mid bc$, then $bc = al$ for some $l \in \mathbb{Z}$.

Thus, $c = acx + aly = a(cx + ly)$, i.e. $a \mid c$.

Proposition 7 is false if we omit the hypothesis $\gcd(a,b)=1$:

$a=12$, $b=6$ and $c=2$. $12 \mid 12$, $\gcd(12,6)=6$ and $12 \nmid 2$

Question: How do we find the gcd of $a,b \in \mathbb{Z}\setminus\{0\}$?

How do we find $u,v \in \mathbb{Z}$ s.t. $\gcd(a,b) = au+bv$?

Answer: The Euclidean Algorithm!

The Euclidean Algorithm

Let $a, b \in \mathbb{Z} \setminus \{0\}$.

Step 1: Apply the Division Algorithm several times until you obtain remainder zero.

Step 2: The last nonzero remainder is the gcd.

$$\gcd(a,b) = r_N$$

$$
\begin{array}{lll}
a = b q_0 + r_0 & 0 \leq r_0 \leq |b| & (0) \\
b = r_0 q_1 + r_1 & 0 \leq r_1 < r_0 & (1) \\
r_0 = r_1 q_2 + r_2 & 0 \leq r_2 < r_1 & (2) \\
r_1 = r_2 q_3 + r_3 & 0 \leq r_3 < r_2 & (3) \\
\vdots & \vdots & \\
r_{N-2} = r_{N-1} q_N + r_N & 0 \leq r_N < r_{N-1} & (N) \\
r_{N-1} = r_N q_{N+1} & r_{N+1} = 0 & (N+1)
\end{array}
$$

Why does the algorithm stop?

Because $|b| > r_0 > r_1 > r_2 > r_3 > \cdots \geqslant 0$ is a decreasing sequence of strictly positive integers if the remainders are not zero and such sequence cannot continue indefinitely.

Why is $r_N = \gcd(a,b)$?

Proposition 8: Let a, b, q and r in $\mathbb{Z}$ so that $b > 0$ and $a = bq + r$.

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

Proof: Exercise.

From Proposition 8, $\gcd(a,b) = \gcd(b, r_0) = \gcd(r_0, r_1) = \cdots = \gcd(r_N, 0) = r_N$.

How do we find the linear combination $au + bv = \gcd(a,b)$?

By recursively writing r_i in terms of r_{i-1} and r_{i-2}:

$$
\begin{aligned}
r_N &= r_{N-2} - q_N r_{N-1} && \text{from eq } (N) \\
&= r_{N-2} - q_N \left(r_{N-3} - q_{N-1} r_{N-2} \right) && \text{from eq } (N-1) \\
&\ \vdots \\
&= ua + vb
\end{aligned}
$$

Ex: Use the Euclidean Algorithm to find the $\gcd(56, 72)$ and write it as a linear combination of 56 and 72.

$$72 = 56 \cdot 1 + 16$$
$$56 = 16 \cdot 3 + 8$$
$$16 = 8 \cdot 2 + 0$$

Then $\gcd(56, 72) = 8$.

$$\gcd(72, 56) = \gcd(56, 16) = \gcd(16, 8) = \gcd(8, 0) = 8.$$

Moreover,
$$\begin{aligned} 8 &= 56 - 16 \cdot 3 \\ &= 56 - (72 - 56)3 \\ &= 56(4) + 72(-3) \end{aligned}$$

Is 8 the smallest positive integer of the form $56x + 72y$? Yes, by def of gcd.

We just proved that $56x + 72y = 8$ has one solution $(x, y) = (4, -3)$. This solution is not unique. Indeed, you will see what the general solution is in Problem Set 2.