Lecture 3

Euclidean Algorithm

$a, b \in \mathbb{Z}, b > 0$

$a = b \cdot q + r, \ 0 \le r < b$

$\gcd(a, b)$

$\gcd(225, 120)$

$225 = 120 \times 1 + 105$

$120 = 105 \times 1 + 15$

$105 = 15 \times 7 + 0$

so $\gcd(225, 120) = 15$

Chapter 6 Linear Equations & GCD

$ax \equiv b \mod n$

a, b positive integer

Consider $S = \{ax + by : x, y \in \mathbb{Z}\} = d\mathbb{Z}$ = integer multiples of d

claim: The smallest positive integer in the set is $\gcd(a, b) = d$

[This is equivalent to saying that $\mathbb{Z}$ is a principal ideal domain]

1st step: d is the smallest positive integer in S

$S \subseteq d\mathbb{Z}$

If $\alpha \in S$, suppose $d \nmid \alpha$

Then $\alpha = dq + r, \ 0 < r < d$

$r = \alpha - dq \in S$ contradiction $\Rightarrow d \mid \alpha \Rightarrow S \subseteq d\mathbb{Z}$

$= ax + by - (ax' + by')q = a(x - x'q) + b(y - y'q) \in S$

The other direction $d\mathbb{Z} \subseteq S$ is obvious

So $S = d\mathbb{Z}$

2nd step: $d = \gcd(a, b)$

① $d \mid a, d \mid b$

② if $d' \mid a, d' \mid b$, then $d' \mid d$ (d is the longest)

②: If $d' \mid a$, $d' \mid b$, then $d' \mid ax + by$, So $d' \mid d$

①: $a = dq + r, \ 0 \le r < d$

$r = a - dq \in S$

since d is the smallest positive integer in S, $r = 0$, So $d \mid a$

i.e. there exist $x, y \in \mathbb{Z}$ s.t. $\gcd(a, b) = ax + by$

$15 = 225x + 120y$

$15 = 120 - 105$

$= 120 - (225 - 120) \Rightarrow x = -1, y = 2$

$= (-1) \times 225 + 2 \times 120$

$$\boxed{\begin{aligned} 12453 &= 2347 \times 5 + 781 \\ 2347 &= 718 \times 3 + 193 \\ &\vdots \\ 23 &= 8 \times 2 + 7 \\ 8 &= 7 + 1 \end{aligned}}$$

$a = bq_1 + r_1$

$b = r_1 q_2 + r_2$

$\vdots$

$r_{n-2} = r_{n-1} q_n + r_n$

$r_{n-1} = r_n q_n$

$\gcd(a, b) = r_n = r_{n-2} - r_{n-1} q_n$

$= \cdots$

$= a \cdot x + b \cdot y$

$\gcd(12453, 2347) = 1$

$1 = 8 - 7$

$= 8 - (23 - 8 \times 2)$

$= -23 + 8 \times 3$

$= -23 + 3 \times (31 - 23)$

$= \cdots$

$= 12453 \times 304 + 2347 \times (-1613)$

We know $\gcd(a,b)=ax+by$ has a solution

Find all solutions

Consider the case $\gcd(a,b)=1$

Suppose (x_1, y_1) is a set of $ax+by=1$

We have other solutions (x_1+kb, y_1-ka), $k\in\mathbb{Z}$

$$a(x_1+kb)+b(y_1-ka)=ax_1+by_1=1$$ so ∞ many solutions for $ax+by=1$

Claim: These are all integer solutions.

Suppose (x_2,y_2) is a set of solution. (want to show it is in the form of above)

$$\left.\begin{array}{l} ax_1+by_1=1 \\ ax_2+by_2=1 \end{array} \Rightarrow \begin{array}{l} y_2ax_1+y_2by_1=y_2 \\ y_1ax_2+y_1by_2=y_1 \end{array} \Rightarrow (y_2x_1-y_1x_2)a=(y_2-y_1) \\ \begin{array}{l} x_2ax_1+x_2by_1=x_2 \\ x_1ax_2+x_1by_2=x_1 \end{array} \Rightarrow (x_2y_1-x_1y_2)b=(x_2-x_1) \right\} \Rightarrow \begin{array}{l} x_2=x_1+bk \\ y_2=y_1-ak \end{array}$$

done. ∎

Let $k=x_2y_1-x_1y_2$

e.g.

$5x+3y=1$

-1 2

All solutions are $(-1+3k, 2-5k)$, $k\in\mathbb{Z}$

if $k=1$, $(2,-3)$ ✓

$k=-1$, $(-4,7)$ ✓

...

So:

Sps $d=\gcd(a,b)>1$

$d=ax+by$

$1=\frac{a}{d}x+\frac{b}{d}y$

All solutions are $(x_1+k\cdot\frac{b}{d}, y_1-k\cdot\frac{a}{d})$, $k\in\mathbb{Z}$, (x_1,y_1) is one set of solution.