Friday, December 4, 2015 11:01 AM

In the previous lecture we defined $\underline{\gcd(a,b)}$, and proved

- $\forall\, a,b \in \mathbb{Z}^+,\ \exists\, x,y \in \mathbb{Z},\ \gcd(a,b) = ax + by$.

We used this to show that the linear Diophantine equation

$$ax + by = c$$

has integer solutions, if and only if, $\gcd(a,b) \mid c$.

Two questions:

1. How can we compute $\gcd(a,b)$ (specially when a,b are huge)?

2. How can we give a solution of $ax+by=c$?

__Lemma__. $a \overset{n}{\equiv} b \implies \gcd(a,n) = \gcd(b,n)$

__Proof__. Let $d_1 = \gcd(a,n)$ and $d_2 = \gcd(b,n)$.

We will prove $d_1 \le d_2$ and $d_2 \le d_1$, which implies $d_1 = d_2$.

$$a \overset{n}{\equiv} b \implies \exists\, k \in \mathbb{Z},\ a - b = nk \implies b = a - nk$$

$$\left.\begin{array}{l} d_1 \mid a \\ d_1 \mid n \end{array}\right\} \implies \left.\begin{array}{l} d_1 \mid a - nk = b \\ d_1 \mid n \end{array}\right\} \implies d_1 \le \gcd(b,n) = d_2.$$

By a similar argument, we have $d_2 \le d_1$. ■

__Corollary__. If r is the remainder of a divided by b, then

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

__Proof__. Since $a \overset{b}{\equiv} r$, by the above lemma we are done. ■

__Euclid algorithm__

Let $a,b \in \mathbb{Z}^+$. Suppose $a \ge b$ and define the sequence x_n of non-negative integers as follows:

$$\begin{cases} x_1 = a,\ x_2 = b, \end{cases}$$

Let x_n be the remainder of x_{n-2} divided by x_{n-1}.

Stop when $x_{n_0} = 0$.

Output x_{n_0-1}.

Claim. $x_{n_0-1} = \gcd(a,b)$.

Why does Euclid algorithm work?

We know by the previous corollary that

$$\gcd(x_n, x_{n-1}) = \gcd(x_{n-2}, x_{n-1})$$

And $x_{n-2} < x_{n-1}$.

So $\gcd(x_1, x_2) = \gcd(x_2, x_3) = \cdots = \gcd(x_{n_0-1}, x_{n_0}) = x_{n_0-1}$.

$$x_1 \geq x_2 > x_3 > \cdots > x_{n_0-1} > x_{n_0} = 0$$

(Since at each step we are getting a strictly smaller non-negative integer, at most in $x_2 = \min\{a,b\}$ steps we get to zero.)

Ex. Find $\gcd(2015, 109)$

$2015 = 109 \times 18 + 53$, $109 = 53 \times 2 + 3$, $53 = 3 \times 17 + 2$
$3 = 2 \times 1 + 1$, $2 = 1 \times 2 + 0$.

A solution of linear Diophantine equation.

Ex. Find $x, y \in \mathbb{Z}$, $2015x + 109y = 1$.

Solution. $1 = 3 - 2 \times 1$

$$= 3 - (53 - 3 \times 17) \times 1$$

$$= -53 \times 1 + 3 \times (1 + 17 \times 1)$$

$$= -53 \times 1 + 3 \times 18$$

$$= -53 \times 1 + (109 - 53 \times 2) \times 18$$

$$= 109 \times 18 - 53 \times (1 + 2 \times 18)$$

$$= 109 \times 18 - 53 \times 37$$

$$= 109 \times 18 - (2015 - 109 \times 18) \times 37$$

$$= -2015 \times 37 + 109 \times (18 + 18 \times 37)$$

$$= -2015 \times 37 + 109 \times 684.$$

So $x = -37$, $y = 684$ is a solution of

$$2015x + 109y = 1. \qquad \blacksquare$$