Recall: last time, we introduced Eulidean algorithm

Theorem 5.1 (Euclidean Alogorithm) Let $a, b$ be two integers. We compute the successive quotients and remainders:

$$a = q_1 b + r_1$$
$$b = q_2 r_1 + r_2$$
$$r_1 = q_3 r_2 + r_3$$
$$\vdots$$
$$r_{n-2} = q_n r_{n-1} + r_n$$
$$r_{n-1} = q_{n+1} r_n + 0$$

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

Here we prove the theorem.

The proof of the theorem is based on an important observation:

Observation: Let $a, b$ be two integers. and $d$ be another integer satisfying $d \mid a$ and $d \mid b$.

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

This is true sime $\gcd(a,b)$ is the largest common divisor.

Proof of theorem: Let $d = \gcd(a,b)$. Goal: $d = r_n$.

We show the following 2 things:

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

(2) $d \mid r_n$.

Then by the observation, $d = r_n$.

(1): $r_{n-1} = q_{n+1} \cdot r_n \Rightarrow r_n \mid r_{n-1}$

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

$\cdots$

$r_1 = q_3 r_2 + r_2 \Rightarrow r_n \mid r_1$

$b = q_2 r_1 + r_2 \Rightarrow r_n \mid b$ ✓

$a = q_1 b + r_1 \Rightarrow r_n \mid a$

(2) Let $d = \gcd(a,b)$

$d \mid a,\ d \mid b \qquad a = q_1 b + r_1 \Rightarrow d \mid r_1$

$d \mid b,\ d \mid r_1 \qquad b = q_2 r_1 + r_2 \Rightarrow d \mid r_2$

$d \mid r_1,\ d \mid r_2 \qquad r_1 = q_3 r_2 + r_3 \Rightarrow d \mid r_3$

$\vdots$

$d \mid r_{n-2},\ d \mid r_{n-1} \qquad r_{n-2} = q_n r_{n-1} + r_n \Rightarrow d \mid r_n$

Therefore $d \mid r_n$. ✓

By (1), (2) and the observation,

we showed: $\gcd(a,b) = r_n$. $\square$.

See next page!

In this lecture, we want to prove the following theorem.

**Theorem:** Let $m, n$ be two integers. Then we can find (necessarily negative) integers $r, s$ such that

$\boxed{\text{Bezout's identity}}$

$$rm + sn = \gcd(m,n).$$

Before the proof, we look at one example:

$$m = 100 \qquad n = 46$$

Euclidean algorithm:

$$100 = 2 \cdot 46 + 8 \qquad\qquad 8 = 100 - 2\cdot 46$$

$$46 = 5 \cdot 8 + 6 \qquad\qquad 46 = 5(100 - 2\cdot 46) + 6$$

$$46 = 5 \cdot 100 - 10 \cdot 46 + 6$$

$$-5 \cdot 100 + 11 \cdot 46 = 6$$

$$8 = 1 \cdot 6 + 2 \qquad\qquad 100 - 2 \cdot 46 = 1 \cdot (-5 \cdot 100 + 11 \cdot 46) + 2$$

$$100 - 2 \cdot 46 = -5 \cdot 100 + 11 \cdot 46 + 2$$

$$6 \cdot 100 - 13 \cdot 46 = 2.$$

$$6 = 3 \cdot 2 + 0 \qquad\qquad = \gcd(100, 46)$$

$$\Rightarrow \quad \underset{r}{6} \cdot \underset{m}{100} - \underset{s}{13} \cdot \underset{n}{46} = \underset{\gcd(m,n)}{2} \qquad r = 6 \qquad s = -13.$$

This gives us the idea to prove: for general $m, n$.

$$
\begin{aligned}
m &= q_1 n + r_1 & &\Rightarrow \quad r_1 = m - q_1 n \\
n &= q_2 r_1 + r_2 & & n = q_2(m - q_1 n) + r_2 \\
r_1 &= q_3 r_2 + r_3 & & \vdots \\
&\vdots & & \\
r_{n-2} &= q_n r_{n-1} + r_n & & \\
r_{n-1} &= q_{n+1} r_n + 0 & &
\end{aligned}
$$

We can always do the substitution such that

$r_1, r_2, \ldots r_{n-1}$ is the combination of $m$ and $n$.

Then so will $r_n$ since $r_{n-2} = q_n r_{n-1} + r_n$.

$$r_n = r_{n-2} - q_n r_{n-1} \qquad \square$$

<u>Definition:</u> Let $m, n$ be two integers. $m$ and $n$ are <u>coprime</u> (relatively prime) if $\gcd(m, n) = 1$.

Corollary of Theorem: Let $m$ and $n$ be coprime. Then we can find integers $r, s$ such that

$$rm + sn = 1.$$

Proposition: Let $m, n$ be two integers. Suppose that we can find $r, s$ such that $rm + sn = 1$.

Then $m, n$ are coprime.

Proof: Let $d = \gcd(m, n)$. $d \mid m$ and $d \mid n$

Since we can find $r, s$ such that $rm + sn = 1$

$$d \mid rm + sn \Rightarrow d \mid 1.$$

However, 1 only has one divisor: $d = 1$.

Therefore $\gcd(m, n) = 1$. $\square$.

Corollary: For any integer $n$, $\gcd(n, n+1) = 1$.

Proof: We can write:

$$1 \cdot (n+1) + (-1) \cdot n = 1.$$

Therefore, $\gcd(n, n+1) = 1$ $\square$