Math 4460

4/7/25

Topic 5 continued...

Def: Let $n \in \mathbb{Z}$ with $n \geq 2$. Define the Euler phi function to be

$$\varphi(n) = \underbrace{|\mathbb{Z}_n^\times|}_{\text{size of } \mathbb{Z}_n^\times}$$

Ex:

$$\varphi(2) = |\mathbb{Z}_2^\times| = |\{\overline{1}\}| = 1$$

$\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$

$\gcd(0,2) = 2 \neq 1$

$\gcd(1,2) = 1$

$$\varphi(3) = |\mathbb{Z}_3^\times| = |\{\bar{1}, \bar{2}\}| = 2$$

$$\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$$

$\gcd(0,3) = 3 \neq 1$

$\gcd(1,3) = 1$

$\gcd(2,3) = 1$

$$\varphi(4) = |\mathbb{Z}_4^\times| = |\{\bar{1}, \bar{3}\}| = 2$$

$$\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$$

$\gcd(0,4) = 4 \neq 1$

$\gcd(1,4) = 1$

$\gcd(2,4) = 2 \neq 1$

$\gcd(3,4) = 1$

$$\varphi(10) = |\mathbb{Z}_{10}^\times| = |\{\bar{1}, \bar{3}, \bar{7}, \bar{9}\}| = 4$$

3/24

Theorem:

① If p is prime, then $\varphi(p) = p-1$.

② If p is prime, then

$$\varphi(p^k) = p^k - p^{k-1}$$

③ If a and b are positive integers and $\gcd(a,b)=1$, then $\varphi(ab) = \varphi(a)\varphi(b)$

[φ is a multiplicative function]

④ If $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ is the prime factorization of n, then

$$\varphi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)$$

proof: We won't prove. $\square$

Ex: Let's calculate $|\mathbb{Z}_{360}^{\times}|$

Here $n = 360$.

Then, $n = 36 \cdot 10 = 6 \cdot 6 \cdot 5 \cdot 2$

$$= 2^3 \cdot 3^2 \cdot 5^1$$

Hence,

$$\varphi(360) \overset{4}{=} 360\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right)$$

$$= 360\left(\frac{1}{2}\right)\left(\frac{2}{3}\right)\left(\frac{4}{5}\right)$$

$$= \frac{2^3 \cdot 3^{\cancel{2}\,1} \cdot \cancel{5^1} \cdot \cancel{2} \cdot 4}{\cancel{2} \cdot \cancel{3} \cdot \cancel{5}} = 96$$

So, $|\mathbb{Z}_{360}^{\times}| = \varphi(360) = 96$

<u>Notation:</u> Let $n \in \mathbb{Z}$, $n \geq 2$.

Let $\overline{a} \in \mathbb{Z}_n^\times$.

Suppose $\mathbb{Z}_n^\times = \{\overline{a}_1, \overline{a}_2, \ldots, \overline{a}_{\varphi(n)}\}$

Define

$$\overline{a} \cdot \mathbb{Z}_n^\times = \{\overline{a} \cdot \overline{a}_1, \overline{a} \cdot \overline{a}_2, \ldots, \overline{a} \cdot \overline{a}_{\varphi(n)}\}$$

<u>Ex:</u> $\mathbb{Z}_{10}^\times = \{\overline{1}, \overline{3}, \overline{7}, \overline{9}\}$

$\overline{a} = \overline{7}$

Then,

$$\begin{aligned}\overline{a} \cdot \mathbb{Z}_{10}^\times &= \overline{7} \cdot \mathbb{Z}_{10}^\times \\ &= \{\overline{7} \cdot \overline{1}, \overline{7} \cdot \overline{3}, \overline{7} \cdot \overline{7}, \overline{7} \cdot \overline{9}\} \\ &= \{\overline{7}, \overline{21}, \overline{49}, \overline{63}\}\end{aligned}$$

$= \{\bar{7}, \bar{1}, \bar{9}, \bar{3}\}$

$= \{\bar{1}, \bar{3}, \bar{7}, \bar{9}\} = \mathbb{Z}_{10}^{\times}$

<u>Theorem:</u> Let $n \in \mathbb{Z}$, $n \geq 2$.

Let $\bar{a} \in \mathbb{Z}_n^{\times}$.

Then, $\bar{a} \cdot \mathbb{Z}_n^{\times} = \mathbb{Z}_n^{\times}$

<u>proof:</u>

We will prove that

$\bar{a} \cdot \mathbb{Z}_n^{\times} \subseteq \mathbb{Z}_n^{\times}$ and $\mathbb{Z}_n^{\times} \subseteq \bar{a} \cdot \mathbb{Z}_n^{\times}$

(1) Let's show $\mathbb{Z}_n^{\times} \subseteq \bar{a} \cdot \mathbb{Z}_n^{\times}$

Pick some $\bar{x} \in \mathbb{Z}_n^{\times}$.

Since $\overline{a} \in \mathbb{Z}_n^\times$ we know $\overline{a}^{-1}$ exists and $\overline{a}^{-1} \in \mathbb{Z}_n^\times$.

Since $\overline{a}^{-1} \in \mathbb{Z}_n^\times$ and $\overline{x} \in \mathbb{Z}_n^\times$ we know from a previous theorem $\overline{a}^{-1} \cdot \overline{x} \in \mathbb{Z}_n^\times$.

Ergo,

$$\overline{x} = \overline{a} \cdot \underbrace{(\overline{a}^{-1} \cdot \overline{x})}_{\text{in } \mathbb{Z}_n^\times} \in \overline{a} \cdot \mathbb{Z}_n^\times$$

Thus, $\mathbb{Z}_n^\times \subseteq \overline{a} \cdot \mathbb{Z}_n^\times$.

2 Let's show $\overline{a} \cdot \mathbb{Z}_n^\times \subseteq \mathbb{Z}_n^\times$

Let $\overline{y} \in \overline{a} \cdot \mathbb{Z}_n^\times$

Then, $\overline{y} = \overline{a} \cdot \overline{z}$ where $\overline{z} \in \mathbb{Z}_n^\times$.

Since $\overline{a}, \overline{z} \in \mathbb{Z}_n^\times$ by a previous theorem $\overline{a} \cdot \overline{z} \in \mathbb{Z}_n^\times$

So, $\overline{y} \in \mathbb{Z}_n^\times$.

Thus, $\overline{a} \cdot \mathbb{Z}_n^\times \subseteq \mathbb{Z}_n^\times$.

By ① and ② we have

$$\overline{a} \cdot \mathbb{Z}_n^\times = \mathbb{Z}_n^\times$$

■

Euler's Theorem

Let $n \in \mathbb{Z}$ with $n \geq 2$.

Let $\overline{a} \in \mathbb{Z}_n^\times$

Then, $\overline{a}^{\varphi(n)} = \overline{1}$ in $\mathbb{Z}_n^\times$

Equivalently:

If $\gcd(a,n)=1$, then $a^{\varphi(n)} \equiv 1 \pmod{n}$

Ex: Recall $\varphi(360)=96$

Also, $\gcd(7,360)=1$

Thus, $\overline{7} \in \mathbb{Z}_{360}^{\times}$

Euler says:

$$\overline{7}^{96} = \overline{1}$$

in $\mathbb{Z}_{360}^{\times}$

$7^{96} \equiv 1 \pmod{360}$

So,

$360 \mid (7^{96}-1)$

Proof of Euler's theorem:

Let $\mathbb{Z}_n^\times = \{\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_{\varphi(n)}\}$

Let $\bar{a} \in \mathbb{Z}_n^\times$

We know $\mathbb{Z}_n^\times = \bar{a} \cdot \mathbb{Z}_n^\times$

Then

$$\underbrace{\bar{a}_1 \cdot \bar{a}_2 \cdots \bar{a}_{\varphi(n)}}_{\text{product of elements of } \mathbb{Z}_n^\times} = \underbrace{(\bar{a}\bar{a}_1)(\bar{a}\bar{a}_2)\cdots(\bar{a}\bar{a}_{\varphi(n)})}_{\text{product of elements of } \bar{a}\cdot\mathbb{Z}_n^\times}$$

So,

$$\bar{a}_1 \bar{a}_2 \cdots \bar{a}_{\varphi(n)} = \bar{a}^{\varphi(n)}\, \bar{a}_1 \bar{a}_2 \cdots \bar{a}_{\varphi(n)}$$

Since each $\overline{a_i} \in \mathbb{Z}_n^{\times}$ we know each $\overline{a_i}^{-1}$ exists.

Thus,

multiply both sides by

$$(\overline{a}_1\overline{a}_2\cdots\overline{a}_{\varphi(n)})(\overline{a}_1^{-1}\overline{a}_2^{-1}\cdots\overline{a}_{\varphi(n)}^{-1})$$

$$= \overline{a}^{\varphi(n)}(\overline{a}_1\overline{a}_2\cdots\overline{a}_{\varphi(n)})(\overline{a}_1^{-1}\overline{a}_2^{-1}\cdots\overline{a}_{\varphi(n)}^{-1})$$

So,

$$1 = \overline{a}^{\varphi(n)} \cdot \overline{1}$$

Thus,

$$\overline{a}^{\varphi(n)} = \overline{1}$$

$\blacksquare$