Math 4460
4/12/23

Def: Let $n \in \mathbb{Z}$ with $n \geq 2$. Define the Euler phi function (or the Euler totient function) by the formula

$$\varphi(n) = |\mathbb{Z}_n^\times|$$

size of the set $\mathbb{Z}_n^\times$

Ex:

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

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

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

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

$\vdots \qquad \vdots$

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

$\vdots \qquad \vdots \qquad \gcd(0,4)=4 \qquad \gcd(2,4)=2$

$\gcd(1,4)=1 \qquad \gcd(3,4)=1$

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

$g(x,10)=1$
$1 \le x \le 9$

Theorem:

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

② If p is prime and k is a positive integer, then

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

③ If a and b are integers with $a, b \geq 2$ and $\gcd(a,b)=1$ then $\varphi(ab) = \varphi(a)\varphi(b)$

(4) If $n = p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}$ is the prime factorization of n, then

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

Proof:

We won't prove this theorem.

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

We have

$$360 = 36 \cdot 10 = 6^2 \cdot 2 \cdot 5 = 2^2 \cdot 3^2 \cdot 2 \cdot 5$$

$$360 = 2^3 \cdot 3^2 \cdot 5^1$$

So,

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

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

$$\boxed{1 - \frac{1}{p} = \frac{p-1}{p}}$$

$$= 2^2 \cdot 3 \cdot 2 \cdot 4$$

$$= 96$$

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

<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

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

<u>Ex:</u> Let $n=10$

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

Let $\overline{a}=\overline{9}$.

Then,

$$\begin{aligned}
\overline{9}\cdot\mathbb{Z}_{10}^\times &= \{\overline{9}\cdot\overline{1},\overline{9}\cdot\overline{3},\overline{9}\cdot\overline{7},\overline{9}\cdot\overline{9}\}\\
&= \{\overline{9},\overline{27},\overline{63},\overline{81}\}\\
&= \{\overline{9},\overline{7},\overline{3},\overline{1}\}\\
&= \{\overline{1},\overline{3},\overline{7},\overline{9}\}
\end{aligned}$$

$$= \mathbb{Z}_{10}^{\times}$$

Theorem: Let $n \in \mathbb{Z}$ with $n \geq 2$. Let $\overline{a} \in \mathbb{Z}_n^{\times}$. Then, $\overline{a} \cdot \mathbb{Z}_n^{\times} = \mathbb{Z}_n^{\times}$

proof:

We will show ① $\mathbb{Z}_n^{\times} \subseteq \overline{a} \cdot \mathbb{Z}_n^{\times}$ and ② $\overline{a} \cdot \mathbb{Z}_n^{\times} \subseteq \mathbb{Z}_n^{\times}$.

① $\left(\mathbb{Z}_n^{\times} \subseteq \overline{a} \cdot \mathbb{Z}_n^{\times} \right)$

Idea

$$\overline{x} = \overline{a} \cdot (?)$$

$$\overline{x} = \overline{a} \cdot \left(\overline{a}^{-1} \cdot \overline{x} \right)$$

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

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

Since $\overline{x}, \overline{a}^{-1} \in \mathbb{Z}_n^\times$ and $\mathbb{Z}_n^\times$ is closed under multiplication by a previous theorem we know $\overline{a}^{-1} \cdot \overline{x} \in \mathbb{Z}_n^\times$.

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

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

② $(\overline{a} \cdot \mathbb{Z}_n^\times \subseteq \mathbb{Z}_n^\times)$

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

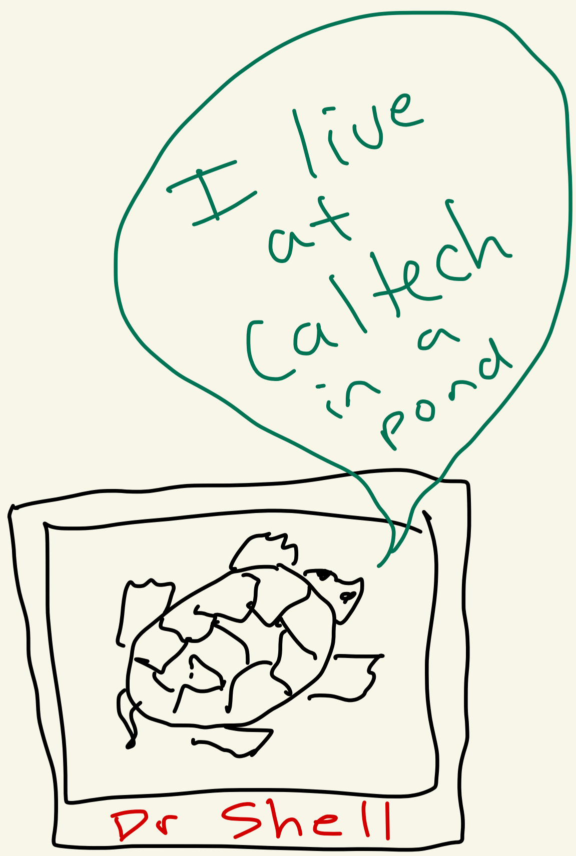
Then, $\overline{y} = \overline{a} \cdot \overline{z}$ where $\overline{z} \in \mathbb{Z}_n^{\times}$.

Since $\overline{a}, \overline{z} \in \mathbb{Z}_n^{\times}$ and $\mathbb{Z}_n^{\times}$ is closed under multiplication we know $\overline{y} = \overline{a} \cdot \overline{z} \in \mathbb{Z}_n^{\times}$.

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

So, by 1 and 2

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



Euler's Theorem: Let $n \in \mathbb{Z}$ with $n \geq 2$.
Let $\bar{a} \in \mathbb{Z}_n^{\times}$.
Then, $\bar{a}^{\varphi(n)} = \bar{1}$.

Equivalently: $a^{\varphi(n)} \equiv 1 \pmod{n}$
when $\gcd(a,n) = 1$

Ex: $n = 360$
Recall $\varphi(360) = |\mathbb{Z}_{360}^{\times}| = 96$

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

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

<u>Euler says:</u> $\overline{7}^{96} = \overline{1}$

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

<u>Ex:</u> $n = 10$

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

$\varphi(10) = |\mathbb{Z}_{10}^{\times}| = 4$

<u>Euler says:</u>

$$\left.\begin{aligned} \overline{1}^4 &= \overline{1} \\ \overline{3}^4 &= \overline{1} \\ \overline{7}^4 &= \overline{1} \end{aligned}\right\} \text{happening in } \mathbb{Z}_{10}^{\times}$$

$$\overline{9}^4 = \overline{1}$$

<u>Or:</u>

$$1^4 \equiv 1 \pmod{10}$$

$$3^4 \equiv 1 \pmod{10}$$

$$7^4 \equiv 1 \pmod{10}$$

$$9^4 \equiv 1 \pmod{10}$$

<u>Proof of Euler's Theorem:</u>

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

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

We want to show that $\overline{a}^{\varphi(n)} = \overline{1}$.

Recall that $\bar{a} \cdot \mathbb{Z}_n^\times = \mathbb{Z}_n^\times$.

Thus,

$$\underbrace{(\bar{a}\,\bar{a}_1)(\bar{a}\,\bar{a}_2)\cdots(\bar{a}\,\bar{a}_{\varphi(n)})}_{\text{all the elements of } \bar{a}\cdot\mathbb{Z}_n^\times \text{ multiplied together}} = \underbrace{\bar{a}_1\,\bar{a}_2 \cdots \overline{a_{\varphi(n)}}}_{\text{all the elements of } \mathbb{Z}_n^\times \text{ multiplied together}}$$

Factoring we get

$$\bar{a}^{\varphi(n)}\left[\bar{a}_1\,\bar{a}_2 \cdots \overline{a_{\varphi(n)}}\right] = \bar{a}_1\,\bar{a}_2 \cdots \overline{a_{\varphi(n)}}$$

Since each $\bar{a}_i \in \mathbb{Z}_n^\times$ we know $\bar{a}_i^{-1}$ exists for each i.

multiply both sides by $\bar{a}_1^{-1}\,\bar{a}_2^{-1} \cdots \overline{a_{\varphi(n)}}^{-1}$

to get

$$\overline{a}^{\varphi(n)}\overbrace{\left[\overline{a_1}\,\overline{a_2}\cdots\overline{a_{\varphi(n)}}\right]\overline{a_1}^{-1}\,\overline{a_2}^{-1}\cdots\overline{a_{\varphi(n)}}^{-1}}^{\overline{1}}$$

$$= \underbrace{\overline{a_1}\,\overline{a_2}\cdots\overline{a_{\varphi(n)}}\,\overline{a_1}^{-1}\,\overline{a_2}^{-1}\cdots\overline{a_{\varphi(n)}}^{-1}}_{\overline{1}}$$

Cancelling gives

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

$\blacksquare$