Math 4460

4/17/23

Corollary (Fermat's theorem)

If p is prime and $\overline{a} \in \mathbb{Z}_p^\times$, then $\overline{a}^{p-1} = \overline{1}$ in $\mathbb{Z}_p^\times$.

proof: Since p is prime,

$$\varphi(p) = |\mathbb{Z}_p^\times| = |\{\overline{1}, \overline{2}, \ldots, \overline{p-1}\}| = p-1$$

So, Euler says that

$$\overline{a}^{p-1} = \overline{a}^{\varphi(p)} = \overline{1} \text{ in } \mathbb{Z}_p^\times$$

$\blacksquare$

Ex: (HW 5 #9)

Reduce $\overline{5}^{127}$ in $\mathbb{Z}_{12}$.

We have

$$\mathbb{Z}_{12}^{\times} = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}$$

So, $\overline{5} \in \mathbb{Z}_{12}^{\times}$

And, $\varphi(12) = |\mathbb{Z}_{12}^{\times}| = 4$

Thus, Euler says that

$$\boxed{\overline{5}^{4} = \overline{1}} \text{ in } \mathbb{Z}_{12}^{\times}.$$

Note,

$$127 = 4(31) + 3$$

$$\begin{array}{r} 31 \\ 4\,\overline{)\,127} \\ -12 \\ \hline 07 \\ -4 \\ \hline 3 \end{array}$$

So,

$$\bar{5}^{127} = \bar{5}^{4(31)+3}$$

$$= (\bar{5}^{4})^{31} \cdot \bar{5}^{3}$$

$\bar{5}^4 = \bar{1}$

$$= \bar{1}^{31} \cdot \bar{5}^{3}$$

$$= \bar{5}^{3}$$

$$= \overline{25} \cdot \bar{5}$$

$\overline{25} = \bar{1}$ in $\mathbb{Z}_{12}$

$$= \bar{1} \cdot \bar{5}$$

$$= \bar{5}$$

So, $\bar{5}^{127} = \bar{5}$ in $\mathbb{Z}_{12}$.

__Def:__ Let $n \in \mathbb{Z}$, $n \geq 2$.

We say that $\bar{g} \in \mathbb{Z}_n^\times$ is a __primitive root__ for $\mathbb{Z}_n^\times$ if every element $\bar{y}$ in $\mathbb{Z}_n^\times$ can be written in the form

$$\bar{y} = \bar{g}^k$$

where k is a positive integer.

__4550 language:__

$\bar{g}$ is a primitive root means $\mathbb{Z}_n^\times$ is cyclic with $\bar{g}$ as a generator

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

Is $\overline{1}$ a primitive root in $\mathbb{Z}_{10}^{\times}$?

$$\left.\begin{aligned} \overline{1}^1 &= \overline{1} \\ \overline{1}^2 &= \overline{1} \\ \overline{1}^3 &= \overline{1} \\ &\vdots \end{aligned}\right\}$$

you don't get all of $\mathbb{Z}_{10}^{\times}$ from the positive powers of $\overline{1}$. So, $\overline{1}$ is not a primitive root of $\mathbb{Z}_{10}^{\times}$.

Is $\overline{3}$ a primitive root of $\mathbb{Z}_{10}^{\times}$?

$$\overline{3}^1 = \overline{3}$$

$$\overline{3}^2 = \overline{9}$$

$$\overline{3}^3 = \overline{27} = \overline{7}$$

$\bar{3}^4 = \bar{3}^3 \cdot \bar{3} = \bar{7} \cdot \bar{3} = \overline{21} = \bar{1}$

$\bar{3}^5 = \bar{3}^4 \cdot \bar{3} = \bar{1} \cdot \bar{3} = \bar{3}$

$\bar{3}^6 = \bar{9}$

$\bar{3}^7 = \bar{7}$

$\bar{3}^8 = \bar{1}$

$\vdots \qquad \vdots$

repeats

$\boxed{\text{So, } \bar{3} \text{ is a primitive root,}}$

because $\bar{3}^1 = \bar{3}$

$\bar{3}^2 = \bar{9}$

$\bar{3}^3 = \bar{7}$

$\bar{3}^4 = \bar{1}$

all the elements of $\mathbb{Z}_{10}^{\times}$ are a positive power of $\bar{3}$

Is $\overline{7}$ a primitive root of $\mathbb{Z}_{10}^{\times}$?

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

$\overline{7}^2 = \overline{49} = \overline{9}$

$\overline{7}^3 = \overline{7}^2 \cdot \overline{7} = \overline{9} \cdot \overline{7} = \overline{63} = \overline{3}$

$\overline{7}^4 = \overline{7}^3 \cdot \overline{7} = \overline{3} \cdot \overline{7} = \overline{21} = \overline{1}$

Yes, $\overline{7}$ is a primitive root

$$\left.\begin{aligned}
\overline{7}^5 &= \overline{7} \\
\overline{7}^6 &= \overline{9} \\
\overline{7}^7 &= \overline{3} \\
\overline{7}^8 &= \overline{1} \\
&\vdots
\end{aligned}\right\} \text{repeats forever}$$

Since

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

$\overline{7}^2 = \overline{9}$

$\overline{7}^3 = \overline{3}$

$\overline{7}^4 = \overline{1}$

we see $\overline{7}$ is a primitive root.

What about $\overline{9}$?

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

$\overline{9}^2 = \overline{81} = \overline{1}$

the positive powers only give you $\overline{1}$ and $\overline{9}$

$\overline{9}^3 = \overline{9}$

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

$\vdots \qquad \vdots$

repeats forever

So, $\overline{9}$ is not a primitive root.

<u>Summary:</u> The primitive roots of $\mathbb{Z}_{10}^{\times} = \{\overline{1}, \overline{3}, \overline{7}, \overline{9}\}$ are $\overline{3}$ and $\overline{7}$.

Ex: $\mathbb{Z}_8^\times = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$

$\bar{1}$ is not a primitive root.

$\bar{3}^1 = \bar{3}$

$\bar{3}^2 = \bar{9} = \bar{1}$

$\bar{3}^3 = \bar{3}$

$\bar{3}^4 = \bar{1}$

$\vdots \quad \vdots$

repeats

$\bar{3}$ is not a primitive root

$\bar{5}^1 = \bar{5}$

$\bar{5}^2 = \overline{25} = \bar{1}$

$\bar{5}^3 = \bar{5}$

repeats

$\bar{5}$ is not a primitive root

$\overline{5}^4 = \overline{1}$

$\vdots \qquad \vdots$

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

$\overline{7}^2 = \overline{49} = \overline{1}$

$\overline{7}^3 = \overline{7}$

$\overline{7}^4 = \overline{1}$

$\vdots \qquad \vdots$

repeats

$\overline{7}$ is <u>not</u> a primitive root.

<u>Summary:</u> $\mathbb{Z}_8^\times$ has no primitive roots.

Theorem: Let p be a prime. Then, there exists a primitive root for $\mathbb{Z}_p^\times$. Moreover, there are $\varphi(p-1)$ primitive roots.

Ex: $\mathbb{Z}_5^\times = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$

$\boxed{\text{powers of elements}}$

$\overline{1}^1 = \overline{1}$	$\overline{2}^1 = \overline{2}$	$\overline{3}^1 = \overline{3}$	$\overline{4}^1 = \overline{4}$
$\overline{1}^2 = \overline{1}$	$\overline{2}^2 = \overline{4}$	$\overline{3}^2 = \overline{9} = \overline{4}$	$\overline{4}^2 = \overline{16} = \overline{1}$
$\overline{1}^3 = \overline{1}$	$\overline{2}^3 = \overline{8} = \overline{3}$	$\overline{3}^3 = \overline{12} = \overline{2}$	$\overline{4}^3 = \overline{4}$
$\overline{1}^4 = \overline{1}$	$\overline{2}^4 = \overline{6} = \overline{1}$	$\overline{3}^4 = \overline{6} = \overline{1}$	$\overline{4}^4 = \overline{1}$
$\vdots \quad \vdots$	$\vdots \quad \vdots$	$\vdots \quad \vdots$	$\vdots \quad \vdots$

The primitive roots of $\mathbb{Z}_5^\times$ are $\overline{2}$ and $\overline{3}$

Note $\varphi(p-1) = \varphi(5-1)$

$$= \varphi(4)$$

$$= |\mathbb{Z}_4^\times|$$

$$= |\{\overline{1}, \overline{3}\}|$$

$$= 2$$

The theorem says there are 2 primitive roots

Theorem: There exists a primitive root of $\mathbb{Z}_n^\times$ if and only if

$n = 2,\ 2^2 = 4,\ p^k,$ or $2p^l$

where p is an odd prime.
and k, l are positive integers

Ex: Consider $\mathbb{Z}_8^\times$.

$n = 8 = 2^3$

no primitive roots

Ex: Consider $\mathbb{Z}_{27}^\times$

$n = 27 = 3^3 = p^3$ where $p = 3$ is an odd prime

there are primitive roots

Ex: Consider $\mathbb{Z}_{50}^{\times}$

$n = 50 = 2 \cdot 5^2 = 2 \cdot p^{\ell}$, $p = 5$ odd prime, $\ell = 2$

Ex: Consider $\mathbb{Z}_{120}^{\times}$

$n = 120 = 2 \cdot 60 = 2^2 \cdot 30 = 2^3 \cdot 3 \cdot 5$

not in above list

So, $\mathbb{Z}_{120}^{\times}$ has no primitive roots