Math 4460
4/9/25

(Topic 5 continued...)

Fermat's Theorem

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

Reformulation: $a \in \mathbb{Z}$

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

proof: Let $\bar{a} \in \mathbb{Z}_p^{\times}$

Since p is prime, then

$$\mathbb{Z}_p^{\times} = \{\bar{1}, \bar{2}, \bar{3}, \ldots, \overline{p-1}\}$$

only $\bar{0}$ doesn't have an inverse

So,

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

Euler's theorem says

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

Thus,

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

FERMAT

<u>Ex:</u> (HW 5 #9)

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

gcd(5,12) = 1

$$\mathbb{Z}_{12} = \{\cancel{\overline{0}}, \overline{1}, \cancel{\overline{2}}, \cancel{\overline{3}}, \cancel{\overline{4}}, \overline{5}, \cancel{\overline{6}}, \overline{7}, \cancel{\overline{8}}, \cancel{\overline{9}}, \cancel{\overline{10}}, \overline{11}\}$$

gcd(1,12) = 1 gcd(2,12) = 2 ≠ 1 gcd(3,12) = 3 ≠ 1

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

Thus, $\overline{5} \in \mathbb{Z}_{12}^{\times}$ and $\varphi(12) = |\mathbb{Z}_{12}^{\times}| = 4$

Euler says: $\boxed{\overline{5}^{4} = \overline{1}}$ $\leftarrow$ $\overline{5}^{\varphi(12)} = \overline{1}$

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

$\boxed{127 = 31(4) + 3}$

So,

$$\overline{5}^{127} = \overline{5}^{31\cdot 4+3} = \overline{5}^{31\cdot 4} \cdot \overline{5}^{3}$$

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

$$\overset{\overline{5}^{4} = \overline{1}}{=} \overline{1}^{31} \cdot \overline{5}^{3}$$

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

$$= \overline{125}$$

$$\begin{array}{r} 10 \\ 12\overline{)125} \\ -120 \\ \hline 5 \end{array}$$

$$= \overline{5}$$

Thus, $\overline{5}^{127} = \overline{5}$ in $\mathbb{Z}_{12}$

or $5^{127} \equiv 5 \pmod{12}$

<u>Def</u>: Let $n \in \mathbb{Z}$, $n \geq 2$.
We say that $\bar{g} \in \mathbb{Z}_n^\times$ is
a <u>primitive root</u> if every
element $\bar{x} \in \mathbb{Z}_n^\times$ is
of the form $\bar{x} = \bar{g}^k$
where k is a positive integer.

<u>4550</u>
$\bar{g}$ is a primitive root means
$\bar{g}$ is a generator for
$\mathbb{Z}_n^\times$ under multiplication
so $\mathbb{Z}_n^\times$ is cyclic

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

Is $\bar{1}$ a primitive root?

$$\left.\begin{aligned} \bar{1}^1 &= \bar{1} \\ \bar{1}^2 &= \bar{1} \\ \bar{1}^3 &= \bar{1} \\ &\vdots \end{aligned}\right\} \text{positive powers only give } \bar{1}$$

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

Is $\bar{3}$ a primitive root?

$$\left.\begin{aligned} \bar{3}^1 &= \bar{3} \\ \bar{3}^2 &= \bar{9} \\ \bar{3}^3 &= \overline{27} = \bar{7} \\ \bar{3}^4 &= \overline{81} = \bar{1} \end{aligned}\right\} \text{every element of } \mathbb{Z}_{10}^{\times} \text{ is a positive power of } \bar{3}$$

Thus, $\bar{3}$ is a primitive root

Is $\overline{7}$ a primitive root?

$$\overline{7}^1 = \overline{7}$$
$$\overline{7}^2 = \overline{49} = \overline{9}$$
$$\overline{7}^3 = \overline{7}^2 \cdot \overline{7} = \overline{9} \cdot \overline{7} = \overline{63} = \overline{3}$$
$$\overline{7}^4 = \overline{7}^3 \cdot \overline{7} = \overline{3} \cdot \overline{7} = \overline{21} = \overline{1}$$

we get all of $\mathbb{Z}_{10}^{\times}$ 😊

Thus, $\overline{7}$ is a primitive root.

Is $\overline{9}$ a primitive root?

$$\overline{9}^1 = \overline{9}$$
$$\overline{9}^2 = \overline{81} = \overline{1}$$
$$\overline{9}^3 = \overline{9}^2 \cdot \overline{9} = \overline{1} \cdot \overline{9} = \overline{9}$$
$$\overline{9}^4 = \overline{9}^3 \cdot \overline{9} = \overline{9} \cdot \overline{9} = \overline{1}$$
$$\vdots \qquad \vdots$$

the powers of $\overline{9}$ don't generate all the elements of $\mathbb{Z}_{10}^{\times} = \{\overline{1}, \overline{3}, \overline{7}, \overline{9}\}$

$\overline{9}$ is not a primitive root

The primitive roots of

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

are $\overline{3}$ and $\overline{7}$.

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

What are the primitive roots?

powers of $\overline{1}$	powers of $\overline{3}$	powers of $\overline{5}$
$\overline{1}^1 = \overline{1}$	$\overline{3}^1 = \overline{3}$	$\overline{5}^1 = \overline{5}$
$\overline{1}^2 = \overline{1}$	$\overline{3}^2 = \overline{9} = \overline{1}$	$\overline{5}^2 = \overline{25} = \overline{1}$
$\overline{1}^3 = \overline{1}$	$\overline{3}^3 = \overline{3} \cdot \overline{3}^2 = \overline{3} \cdot \overline{1} = \overline{3}$	$\overline{5}^3 = \overline{5} \cdot \overline{5}^2 = \overline{5} \cdot \overline{1} = \overline{5}$
$\vdots$	$\overline{3}^4 = \overline{3} \cdot \overline{3} = \overline{9} = \overline{1}$	$\overline{5}^4 = \overline{5} \cdot \overline{5} = \overline{1}$
	$\vdots$	$\vdots \quad \vdots$

powers of $\overline{7}$

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

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

$\overline{7}^3 = \overline{7}^2 \cdot \overline{7} = \overline{1} \cdot \overline{7} = \overline{7}$

$\overline{7}^4 = \overline{7} \cdot \overline{7} = \overline{49} = \overline{1}$

$\vdots \qquad \vdots$

There is <u>no</u> primitive root in $\mathbb{Z}_8^\times$

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

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

$p = 5$ is prime

primitive roots: $\bar{2}, \bar{3}$

not primitive root: $\bar{1}, \bar{4}$

$$\varphi(p-1) = \varphi(5-1) = \varphi(4)$$
$$= |\mathbb{Z}_4^\times|$$
$$= |\{\bar{1}, \bar{3}\}|$$
$$= 2$$

2 primitive roots

<u>Theorem:</u> There exists a primitive root in $\mathbb{Z}_n^{\times}$ if and only if n is one of the following forms:

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

where p is an odd prime

<u>Ex:</u> Does $\mathbb{Z}_{27}^{\times}$ have a primitive root?

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

So, $\mathbb{Z}_{27}^{\times}$ has at least one primitive root

Ex: $n = 12 = 2^2 \cdot 3$

Not in the list

$\mathbb{Z}_{12}^{\times}$ has no primitive root