Lecture 37 14th Nov 2022

Note Title 11/15/2022

§ <u>Primitive roots</u>: Let m denote a positive integer and 'a' any integer such that $\gcd(a, m) = 1$. Let h be the smallest positive integer such that $a^h \equiv 1 \pmod{m}$. We say that the order of 'a' modulo m is h, denoted by $o(a)$.

Since $\gcd(a, m) = 1$, so $a \in U(\mathbb{Z}_m)$, and h is nothing but the order of 'a' as an element of the group $U(\mathbb{Z}_m)$. If $o(a) = \varphi(m)$, then 'a' is called a primitive root modulo m.

- $\gcd(a,m) = 1$. Then, 'a' is a primitive root modulo m if 'a' is a generator of $U(\mathbb{Z}_m)$.

Thus, $\exists$ a primitive root modulo $m \iff U(\mathbb{Z}_m)$ is cyclic.

<u>Ex:</u> $m = 4$. Then, $U(\mathbb{Z}_4) = \{1, 3\}$ and 3 is a primitive root modulo 4.

$m = 8$. Then, $U(\mathbb{Z}_8) = \{1, 3, 5, 7\}$.

Since $U(\mathbb{Z}_8)$ is not cyclic, so there does not exist primitive roots modulo 8

Theorem 1: If p is a prime, then there exist $\varphi(p-1)$ primitive roots modulo p.

Proof: Since p is a prime, so $\mathbb{Z}_p$ is a field, and hence

$$U(\mathbb{Z}_p) = \mathbb{Z}_p - \{0\} \text{ is a cyclic group.}$$

$\therefore$ There exist primitive roots modulo p.

Since a primitive root modulo p is a generator of $U(\mathbb{Z}_p)$ and $U(\mathbb{Z}_p)$ has order $p-1$, so there are $\varphi(p-1)$ primitive roots modulo p.

—x—

Theorem 2: If p is a prime then there are $\varphi(\varphi(p^2)) = (p-1)\varphi(p-1)$ primitive roots modulo p^2.

Proof: Let g be a primitive root mod p.

Claim: $g+tp$ is a primitive root (mod p^2) for exactly $p-1$ values of t (mod p).

Proof of the claim: Let $h = o(g+tp)$ in $U(\mathbb{Z}_{p^2})$.

Then, $(g+tp)^h \equiv 1 \pmod{p^2}$

$\boxed{\text{Easy to see that } g+tp \in U(\mathbb{Z}_{p^2}).}$

$\Rightarrow (g+tp)^h \equiv 1 \pmod{p} \Rightarrow g^h \equiv 1 \pmod{p}$

$\Rightarrow p-1 \mid h. \rightarrow$ 1

Again, $|U(\mathbb{Z}_{p^2})| = \varphi(p^2) = p^2 - p = p(p-1)$

and hence, $h = o(g+tp) \mid p(p-1)$. $\longrightarrow$ (2)

From (1) and (2), we have

$$h = p-1 \quad \text{or} \quad h = p(p-1)$$

If $h = p(p-1)$, then $g+tp$ is a primitive root mod p^2.

We now prove that $h = p-1$ only for one value of $t \pmod{p}$, say, $t = t_0$.

Let $f(x) = x^{p-1} - 1$.

Then, $(g+t_0p)^{p-1} \equiv 1 \pmod{p^2} \Rightarrow g+t_0p$ is a root of $f(x) \equiv 0 \pmod{p^2}$.

Also, $f(g) = g^{p-1} - 1 \equiv 0 \pmod{p}$.

and $f'(g) = (p-1)\, g^{p-2} \not\equiv 0 \pmod{p}$

By Hensel's lemma, $g \pmod{p}$ lifts to a unique solution $g + tp \pmod{p^2}$ of $f(x) \equiv 0 \pmod{p^2}$

Due to uniqueness, we must have $t = t_0$.

Thus, for exactly one value $t \equiv t_0 \pmod{p}$, $o(g + t_0 p) = p-1$,

and for the other $(p-1)$ values of $t \pmod{p}$, $o(g + tp) = (p-1)p$
$= \phi(p^2)$.

$\therefore$ There exist primitive roots modulo p^2.

Thus, $U(\mathbb{Z}_{p^2})$ is a cyclic group.

We know that $|U(\mathbb{Z}_{p^2})| = \varphi(p^2)$.

$\therefore$ Number of primitive roots modulo p^2

$=$ Number of generators in the cyclic group $U(\mathbb{Z}_{p^2})$

$= \varphi(\varphi(p^2)) = \varphi(p(p-1)) = \phi(p-1)\,\phi(p)$

$= (p-1)\,\phi(p-1)$.

This completes the proof.

#

Theorem 3: $U(\mathbb{Z}_{2^n})$ is not cyclic if $n \geq 3$.

That is, there is no primitive root modulo 2^n if $n \geq 3$.

Proof: We have $|U(\mathbb{Z}_{2^n})| = \varphi(2^n) = 2^n - 2^{n-1} = 2^{n-1}$.

$\therefore U(\mathbb{Z}_{2^n}) = \{k \mid 1 \leq k \leq 2^n, \ k \text{ is odd}\}$.

Let $a = 2^n - 1 \in U(\mathbb{Z}_{2^n})$. Then, $a^2 = (2^n - 1)^2$

$$= 2^{2n} - 2^{n+1} + 1$$

$$\equiv 1 \pmod{2^n}.$$

$\therefore o(a) = 2$.

Let $b = 2^{n-1} + 1$. Then, $b \in U(\mathbb{Z}_{2^n})$.

Now, $b^2 = 2^{2n-2} + 2^n + 1$.

$$\equiv 1 \pmod{2^n} \text{ if } n \geq 2$$

$\left[\, 2n-2 = n + (n-2) \geq n \text{ if } n \geq 2 \,\right]$

Hence $o(b) = 2$.

<u>Claim:</u> $a \not\equiv b \pmod{2^n}$ if $n \geq 3$.

We have
$$a - b = 2^n - 1 - 2^{n-1} - 1$$
$$= 2^{n-1} - 2 \neq 0 \text{ if } n \geq 3.$$

Thus, if $n \geq 3$, then a and b are two elements each of order 2 in $U(\mathbb{Z}_{2^n})$.

But in a cyclic group, there is exactly one element of order 2.

Hence, $U(\mathbb{Z}_{2^n})$ is not cyclic if $n \geq 3$. That is, there is no primitive roots modulo 2^n if $n \geq 3$.

#