Lecture 38 15th Nov 2022

Note Title 11/15/2022

<u>Theorem 1:</u> If p is an odd prime and g is a primitive root modulo p^2, then g is a primitive root modulo p^α for $\alpha = 3, 4, 5, \ldots$

<u>Theorem 2:</u> If p is an odd prime and g is a primitive root modulo p^α, then g is a primitive root modulo $2p^\alpha$.

<u>Proof:</u> Suppose that g is odd.

The numbers $g, g^2, \ldots, g^{\phi(p^\alpha)}$ form a reduced residue system mod p^α. Note that $\phi(2p^\alpha) = \phi(p^\alpha)$ since p is odd. Also, since g is odd, so $g, g^2, \ldots, g^{\phi(p^\alpha)}$ are all odd, and hence they also form a reduced residue system mod $2p^\alpha$

This proves that g is a primitive root modulo $2p^\alpha$.

—— x ——

<u>Theorem 3 (Gauss):</u> There exists a primitive root modulo m $\Leftrightarrow$ $m = 1, 2, 4, p^\alpha$ or $2p^\alpha$, where p is an odd prime and $\alpha \geq 1$.

<u>Proof</u>: We have already seen that, if $m = 1, 2, 4, p^\alpha$ or $2p^\alpha$, then there exists a primitive root modulo m.

To complete the proof, we prove that if there exists a primitive root modulo m, then $m = 1, 2, 4, p^\alpha$ or $2p^\alpha$, where p is odd. We have already proved that there is no primitive root modulo 2^α for $\alpha \geq 3$.

Suppose now that m is not a prime power or twice a prime power. Then, m can be expressed as a product

$$m = m_1 \cdot m_2 \quad \text{with } \gcd(m_1, m_2) = 1, \; m_1 > 2, \; m_2 > 2.$$

Let $l = \text{l.c.m.}(\phi(m_1), \phi(m_2))$.

Let 'a' be such that $\gcd(a, m) = 1$. (that is, $a \in U(\mathbb{Z}_m)$)

Then, $\gcd(a, m_1) = \gcd(a, m_2) = 1$.

$\Rightarrow a^{\varphi(m_1)} \equiv 1 \pmod{m_1}$ & $a^{\varphi(m_2)} \equiv 1 \pmod{m_2}$

$\Rightarrow a^{l} \equiv 1 \pmod{m_1}$ and $a^{l} \equiv 1 \pmod{m_2}$

$\Rightarrow a^{l} \equiv 1 \pmod{\text{lcm}(m_1, m_2)} \Rightarrow a^{l} \equiv 1 \pmod{m}$.

$\Rightarrow \; o(a) \leq \ell \quad \forall \; a \in U(\mathbb{Z}_m).$

Now, $\ell = \mathrm{lcm}(\phi(m_1), \phi(m_2))$

$$= \frac{\phi(m_1)\,\phi(m_2)}{\gcd(\phi(m_1), \phi(m_2))} = \frac{\phi(m)}{\gcd(\phi(m_1), \phi(m_2))} \longrightarrow (1)$$

Since $m_1 > 2$, so $2 \mid \phi(m_1)$. Also, $m_2 > 2 \Rightarrow 2 \mid \phi(m_2)$.

$\therefore \; 2 \mid \gcd(\phi(m_1), \phi(m_2))$.

$$\Rightarrow \frac{\phi(m)}{\gcd(\phi(m_1), \phi(m_2))} < \phi(m) \longrightarrow (2)$$

(1) & (2) $\Rightarrow \ell < \phi(m)$. Hence, every $a \in U(\mathbb{Z}_m)$ has order less than $\phi(m) = |U(\mathbb{Z}_m)|$.

This proves that $U(\mathbb{Z}_m)$ is not cyclic

$\Rightarrow$ there does not exist primitive root modulo m.

This completes the proof.

---

§ Quadratic residues / nonresidues:

<u>Definition:</u> Let $m \geq 1$ and 'a' be such that $\gcd(a, m) = 1$. Then, 'a' is called a quadratic residue modulo m if the congruence $x^2 \equiv a \pmod{m}$ has a solution.

If it has no solution, then 'a' is called a quadratic nonresidue modulo m.

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

  We have $3^2 = 9 \equiv 1 \pmod 8$, $5^2 \equiv 1 \pmod 8$, $7^2 \equiv 1 \pmod 8$.

$\therefore$ 3, 5, and 7 are all quadratic nonresidues modulo 8.

1 is the only quadratic residue mod 8.

Remark: Since $a + m$ is a quadratic residue or nonresidue mod m according as a is or is not, we consider as distinct residues or nonresidues only which are distinct modulo m.

So, we consider elements of $U(\mathbb{Z}_m)$ while studying quadratic residues/nonresidues.

Theorem 4: Let p be an odd prime. Let $\gcd(a, p) = 1$.

Then, a is a quadratic residue modulo p

$$\Leftrightarrow a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

Equivalently, 'a' is a quadratic nonresidue modulo p

$$\Leftrightarrow a^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

$$\left(a^{\frac{p-1}{2}}\right)^2 = a^{p-1} \equiv 1 \pmod{p}$$

$\therefore a^{\frac{p-1}{2}}$ is a solution of $x^2 \equiv 1 \pmod{p}$

$\therefore a^{\frac{p-1}{2}} \equiv 1$ or $-1 \pmod{p}$

Proof: Let 'a' be a quadratic residue mod p.

Then, $a \equiv b^2 \pmod{p}$ for some $b \in U(\mathbb{Z}_p)$

Now, $a^{\frac{p-1}{2}} \equiv (b^2)^{\frac{p-1}{2}} \equiv b^{p-1} \equiv 1 \pmod{p}$.

Conversely, suppose that $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

Let g be a primitive root mod p.

Then, $a \equiv g^k \pmod{p}$.

Now, $a^{\frac{p-1}{2}} \equiv 1 \pmod{p} \Rightarrow g^{k \cdot \frac{p-1}{2}} \equiv 1 \pmod{p}$

$\Rightarrow o(g) \mid k \cdot \frac{p-1}{2} \Rightarrow p-1 \mid k \cdot \frac{p-1}{2} \Rightarrow k$ is even.

$\therefore a \equiv g^k \pmod{p} \Rightarrow a \equiv \left(g^{k/2}\right)^2 \pmod{p}$

$\Rightarrow$ 'a' is a quadratic residue mod p.

$\#$

__Definition:__ If p denotes an odd prime, then the Legendre symbol $\left(\frac{a}{p}\right)$ is defined as follows:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a \\ 1 & \text{if } p \nmid a, \text{ and `}a\text{' is a quadratic residue mod } p \\ -1 & \text{if } p \nmid a, \text{ and `}a\text{' is a quadratic nonresidue mod } p. \end{cases}$$

__Theorem 5:__ Let p be an odd prime. Then,

(1) $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.

(2) $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$

(3) $a \equiv b \pmod{p} \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(4) If $\gcd(a, p) = 1$, then $\left(\frac{a^2}{p}\right) = 1$, $\left(\frac{a^2 b}{p}\right) = \left(\frac{b}{p}\right)$

(5) $\left(\frac{1}{p}\right) = 1$, $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

<u>Theorem 6</u>: Let p be an odd prime. Then, there are $\frac{p-1}{2}$ quadratic residues mod p and there are $\frac{p-1}{2}$ quadratic nonresidues mod p.

<u>Proof</u>: Let g be a primitive root mod p.

Then, $U(\mathbb{Z}_p) = \{1, 2, \dots, p-1\} = \{g, g^2, \dots, g^{p-1}\}$.

We first show that g is a quadratic nonresidue mod p.

Since, g is a generator of $U(\mathbb{Z}_p)$, so $o(g) = p-1$.

$$\therefore \quad g^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

$\Rightarrow$ g is a quadratic nonresidue mod p.

$\Rightarrow$ $g, g^3, g^5, \ldots, g^{p-2}$ are all quadratic nonresidue mod p

$$\left(\because \left(\frac{g^{2k+1}}{p}\right) = \left(\frac{g^{2k}}{p}\right)\left(\frac{g}{p}\right) = \left(\frac{g}{p}\right) = -1 \right) \leftarrow \text{Thm 5 (4)}$$

Again, $g^2, g^4, \ldots, g^{p-1}$ are all quadratic residues mod p.

This completes the proof. #