Recall:

Theorem 20.2. (Quadratic Residue Multiplication Rule, Version I)

Let p be an odd prime.

(1) The product of two quadratic residues (mod p) is a quadratic residue. $QR \times QR = QR$.

(2) The product of a quadratic residue and a nonresidue is a non residue $QR \times NR = NR$.

(3) The product of two nonresidues (mod p) is a quadratic residue. $NR \times NR = QR$.

Proof of (1) Let a, b be QR. (mod p)

Then
$$x_1^2 \equiv a \pmod{p}$$
$$x_2^2 \equiv b \pmod{p}$$

This shows: $x_1^2 x_2^2 \equiv ab \pmod{p}$

i.e. $(x_1 x_2)^2 \equiv ab \pmod{p}$

Therefore, $x^2 \equiv ab \pmod p$ has a solution

and ab is a QR $\pmod p$.

Proof of (2). Let a be a QR

Then $x_1^2 \equiv a \pmod p$

Let b be a NR, then $x^2 \equiv b \pmod p$ has no solution.

(Proof by contradiction). Suppose that ab is a QR. Then we can find z_0 such that

$$z_0^2 \equiv ab \pmod p.$$

Mutiply $\overline{x_1}^2$ on each side,

$$z_0^2 \cdot \overline{x_1}^2 \equiv ab \cdot \overline{x_1}^2 \pmod p$$

$$\equiv a\overline{x_1}^2 \cdot b \pmod p$$

$$(z_0 \overline{x})^2 \equiv 1 \cdot b \pmod p$$

This shows that b is a QR mod p.

A contradiction! $\square$

Proof of (3) Let a be a NR. We look at

$$\{1, 2, 3, \cdots, p-1\} \quad (*)$$

By the previous lecture, there are exactly $\frac{p-1}{2}$ QR and $\frac{p-1}{2}$ NR.

Mutiply $(*)$ by a and $(\text{mod } p)$

$$\{a (\text{mod } p), 2 (\text{mod } p), \cdots (p-1) \text{ mod } p\}$$

This gives another complete list of numbers modulo p (and coprime to p).

Therefore, there are exactly $\frac{p-1}{2}$ QR and $\frac{p-1}{2}$ NR.

Let $b \in \{1, 2, \cdots p-1\}$ be a QR.

Then ab is NR by (2)

However, thee are only $\frac{p-1}{2}$ NR after the multiplication of a.

Therefore, the numbers left are QR.

and this means; every time we have b as a NR, ab is a QR.

$$\begin{tikzcd} \{1,2,\cdots p\} & \boxed{QR} \arrow[d, "\times a"] & \sqcup & \boxed{NR.} \arrow[d, dashed, "a."] \\ \{a(\mathrm{mod}\,p), 2a(\mathrm{mod}\,p), \cdots (p-1)a(\mathrm{mod}\,p)\} & \boxed{NR} & \sqcup & \boxed{QR} \end{tikzcd}$$

$\square$

Theorem: (Polynomial Roots Mod p Theorem)

Let p be a prime number and let

$$f(x) = a_0 x^d + a_1 x^{d-1} + \cdots a_d$$

be a polynomial of degree $d \geq 1$ with integer coefficients and with $p \nmid a_0$

Then the congruence

$$f(x) \equiv 0 \pmod{p}$$

has at most d incongruent solutions.

Proof: (Proof by contradiction.)

Let

$$f(x) = A_0 x^d + A_1 x^{d-1} + \cdots A_d \quad p \nmid A_0$$

be a polynomial with d+1 incongruent solutions mod p.

We can further assume that $f(x)$ has the smallest degree.

Let $r_1, r_2, \cdots r_{d+1}$ be the solutions.

Then $f(x) \equiv f(r_i) \pmod{p}$ $1 \le i \le d$.

$$f(x) - f(r_1) = A_0 x^d + A_1 x^{d-1} + \cdots A_d$$
$$- (A_0 r_1^d + A_1 r_1^{d-1} + \cdots A_d)$$

$$= A_0(x^d - r_1^d) + A_1(x^{d-1} - r_1^{d-1}) + \cdots$$

Note: $x^n - r^n = (x-r)(x^{n-1} + x^{n-2} r + \cdots r^{n-1})$

$f(x) - f(r_1) = (x - r_1) \cdot g(x)$ such that

① The degree of $g(x)$ is $d-1$

② $g(x) = B_0 x^{d-1} + B_1 x^{d-2} + \cdots B_{d-1}$

with $p \nmid B_0$

③ $g(x)$ has $r_2, r_3 \cdots r_{d+1}$ as solutions

This contradicts that $f(x)$ has the smallest degree.

Proof of ①, ②: $x^d - r_1^d = (x - r_1)(x^{d-1} + \cdots)$

This implies:

$$g(x) = A_0 x^{d-1} + \cdots$$

This is degree $d-1$ and $p \nmid A_0$

Proof of ③: Let $i \in [2, 3, \cdots d]$

$$f(r_i) - f(r_1) \equiv 0 - 0 \pmod p$$

$$\Rightarrow (r_i - r_1)\, g(r_i) \equiv 0 \pmod p$$

$$\Rightarrow p \mid r_i - r_1 \quad \text{or} \quad p \mid g(r_i)$$

r_i is incongruent to $r_1 \pmod{p}$

$\Rightarrow p \nmid r_i - r_1$

Therefore $p \mid g(r_i)$ and r_i is a solution

for $g(x) \equiv 0 \pmod{p}$. $\square$.