Quadratic residue

- For a prime p & $a \in \mathbb{Z}$, coprime to a,
  a is a quadratic ~~resi~~ residue modulo p if
  $x^2 \equiv a \mod p$ has a soln.

Euler criterion: Let p be an odd prime. Then $a \in \mathbb{Z}$ is a quadratic module p if & only if

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

Proof: Suppose a is a quadratic modulo p.

Then $y^2 \equiv a \mod p$ for some $y \in \mathbb{Z}$.

By assumption $p \nmid a$ & $p \mid y^2 - a$.

So $p \nmid y^2$

$\Rightarrow p \nmid y$

Think $[y] \in U(\mathbb{Z}_p)$ $\qquad [y]^{p-1} = 1$

$$\therefore y^{p-1} \equiv 1 \pmod p$$

$$\left(y^2\right)^{\frac{p-1}{2}} \qquad p-1 \text{ is an even integer}$$

$$\Rightarrow a^{\frac{p-1}{2}} \equiv 1 \pmod p \quad \left(\text{since } a \equiv y^2 \pmod p\right)$$

Conversely assume that $\boxed{a^{\frac{p-1}{2}} \equiv 1 \mod p}$

Recall $U(\mathbb{Z}_p)$ is a cyclic group of order $p-1$.

Suppose $\langle g \rangle = U(\mathbb{Z}_p)$ so that $g^{p-1} \equiv 1 \bmod p$

& $g^k \not\equiv 1 \bmod p$ if $1 \leq k \leq p-2$

[Have to show $p \nmid a$ & $x^2 \equiv a \bmod p$ has a sol'n]

Since $a^{\frac{p-1}{2}} \equiv 1 \bmod p$, $p \nmid a$.

Let $a = g^s$

So $\left(g^s\right)^{\frac{p-1}{2}} \equiv 1 \bmod p$

$\Rightarrow g^{\frac{s(p-1)}{2}} \equiv 1 \bmod p$

Since $p-1$ is the order of g, $p-1 \mid \frac{s(p-1)}{2}$

So $\frac{s}{2} \in \mathbb{Z}$

Set $\frac{s}{2} = r$

Let $b = g^r = g^{s/2}$

Now $b^2 \equiv g^s \equiv a \pmod p$

Recall fundamental thm of algebra:

There are at most n roots of of $f_n(x) = a_n x^n + \cdots + a_1 x + a_0$ where $a_n \neq 0$ in $\mathbb{Z}_p$, $a_0, \ldots, a_n \in \mathbb{Z}_p$

Show that for $n=0$ & $n=1$ this statement is true.

Induction hypothesis: $f_k(x)$ has at most k roots in $\mathbb{Z}_p$.

Let $w_1, w_2, \ldots, w_k, w_{k+1}, w_{k+2}$ are distinct roots of $f_{k+1}(x)$ in $\mathbb{Z}_p$.

Let $h(x) = f_{k+1}(x) - a_{k+1}(x-\omega_1)\cdots(x-\omega_{k+1})$

Then $\underline{\deg h(x) \le k}$

So $h(x)$ has at most k roots.

Observe $h(\omega_i) = 0$ for $i = 1, \dots, k+1$

But $h(\omega_{k+2}) = 0 - a_{k+1}(\omega_{k+2} - \omega_1)\cdots(\omega_{k+2} - \omega_{k+1})$
$\ne 0$

Thus our assumption that $f_{k+1}(x)$ has $k+2$ distinct roots is false.

Aside

Remark: If $\mathbb{F}$ is a field, & $f(x) \in \mathbb{F}[x]$ of degree ≥ 2 & irreducible, then the quotient ring

$\underline{\mathbb{K} = \frac{\mathbb{F}[x]}{\langle f(x) \rangle}}$ is a field & $\mathbb{K}$ is an extension of $\mathbb{F}$
$\left(\begin{matrix} \mathbb{F} \hookrightarrow \mathbb{K} \\ a \longmapsto \langle f(x) \rangle + a \end{matrix}\right)$

& $f(x)$ has a root in $\mathbb{K}$

(If $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{F}[x]$
its image in $\mathbb{K}[x]$, $\tilde{f}(x) = (I + a_n)X^n + (I + a_{n-1})X^{n-1} + \cdots + (I + a_1)X + I + a_0$
where $I = \langle f(x) \rangle$)

If $\alpha = I + t$, then $\tilde{f}(\alpha) = I$ ($= 0$ in $\mathbb{K}$)

Thm: Let p be a prime of the form $\underline{4k+3}$ for $k \in \mathbb{N} \cup \{0\}$

If $a \in \mathbb{Z}$ s.t. $p \nmid a$ & if $x^2 \equiv a \bmod p$ has a soln, in $\mathbb{Z}$, then $x \equiv \underline{\pm a}^{\left(\frac{p+1}{4}\right)}$ are the $\underline{\text{the soln.}}$

If $x = \pm a^{\left(\frac{p+1}{4}\right)}$, then

$$
\begin{aligned}
x^2 &= a^{\left(\frac{p+1}{2}\right)} \cdot 1 \\
&\equiv a^{\frac{p+1}{2}} \cdot a^{\frac{p-1}{2}} \pmod{p}. \\
&= a^{p-1} \cdot a \\
&\equiv 1 \cdot a \\
&\equiv a \mod p
\end{aligned}
$$

$a^{p-1} \equiv 1 \mod p$

(a is a quadratic residue modulo p

$\Rightarrow a^{\frac{p-1}{2}} = 1$