QUADRATIC RESIDUES

* U_n denotes the set of residues modulo n of integers coprime to n. [where $n \in \mathbb{Z}^+$].

* Definition: An integer, a coprime to n is called quadratic residue modulo n if it is coprime to n and is the square of an integer modulo n.

If a is not a quadratic residue of n, we call it a quadratic non-residue.

Example: Quadratic residues of ~~[illegible]~~ 5.

0
1
2
3
4

These are the unique ~~values~~ terms, which will be repeated when we do mod 5 operation.

we are squaring;

$$\Rightarrow \quad \left.\begin{aligned} 0^2 &= 0 \\ 1^2 &= 1 \\ 2^2 &= 4 \\ 3^2 &= 9 \equiv 4 \pmod 5. \\ 4^2 &= 16 \equiv 1 \pmod 5. \end{aligned}\right\}$$

doing mod 5 operation for the square of unique ~~values~~ terms.

$\therefore$ quadratic residues of ~~[illegible]~~ 5 are 1, 4.
[0 is not considered because it is a quadratic residue for all numbers]

* PROPOSITION 5·2: Let p be a prime. The no: of quadratic residues modulo p is $\frac{p-1}{2}$.

Proof: As $c^2 = (-c)^2$, the no: of quadratic residues is at most $\frac{p-1}{2}$.
On the other hand, if 'a' is a quadratic residue of p, it follows easily that $x^2 \equiv a \bmod p$ has only two solutions modulo p as follows.

Let $b \in U_p$ such that $b^2 \equiv a \bmod p$.

$x^2 \equiv a \bmod p$.
$\Rightarrow x^2 \equiv b^2 \bmod p$.
$\Rightarrow p \mid (x^2 - b^2)$
$\Rightarrow p \mid (x-b)(x+b)$.

$\Rightarrow p \mid (x-b)$ or $p \mid (x+b)$

$\Rightarrow x \equiv b$ or $x \equiv -b \bmod p$.

Example: quadratic residue of 7.
$\Rightarrow 1^2 = 1$
$2^2 = 4$
$3^2 = 9 \equiv 2 \pmod 7$
$4^2 = 16 \equiv 2 \pmod 7$
$5^2 = 25 \equiv 4 \pmod 7$
$6^2 = 36 \equiv 1 \pmod 7$

Here for $a = 4$ there are two x's $2 \& 5$.

As p is odd and b is coprime to p, $b \not\equiv -b \bmod p$.
Hence $x^2 \equiv a \bmod p$ has precisely two solutions modulo p, namely b and $-b$

$\therefore$ There are exactly $\frac{p-1}{2}$ quadratic residues modulo p, and there are $\frac{p-1}{2}$ quadratic non-residues.