Quadratic Residue

> 💡 When we say "modulo p=29", it means we're working within a system where numbers "wrap around" every 29 steps. For example, 30 in this system is equivalent to 1, 31 is equivalent to 2, and so on.

Squaring in Modular Arithmetic:

If we have a number aa and we square it modulo p, denoted as $a2$ mod p, we're finding the remainder when $a2$ is divided by p.

Finding Square Roots Modulo p:

Now, if we're given a number x and we want to find a number a such that $a^2 \equiv x \mod p$, it's like trying to solve for a where a^2 wraps around to give us x when divided by p.

Quadratic Residues and Non-Residues:

- **Quadratic Residue**: If there exists an *a* such that $a^2 \equiv x \mod p$, then *x* is a quadratic residue.
- **Quadratic Non-Residue**: If no such *a* exists, then *x* is a quadratic non-residue.

Two Solutions for Quadratic Residues:

If x is a quadratic residue, there are always two solutions for a, because if $a^2 \equiv x \mod p$, then $(-a)^2 \equiv x \mod p$ as well.

So, when working with modular arithmetic, some numbers have square roots modulo p (quadratic residues), and some don't (quadratic non-residues). And for those that do, there are always two solutions.