

Introduction to quadratic residues

Definition 1 (quadratic residue). *Let $a, m \in \mathbb{Z}$ with $m > 0$ and $(a, m) = 1$. The a is said to be a quadratic residue modulo m if the quadratic congruence $x^2 \equiv a \pmod{m}$ is solvable in \mathbb{Z} . Otherwise, a is said to be a quadratic nonresidue modulo m .*

Remark 1. *When finding squares modulo m , we only need to check up to $\frac{m}{2}$, since $(-a)^2 = a^2$ and $m - a \equiv -a \pmod{m}$.*