

Problem 6: Squares mod p

An element $x \in \mathbb{Z}_m$, where m is a positive integer, is called a square if there exists $y \in \mathbb{Z}_m$ such that $x \equiv y^2 \pmod{m}$. Let p be an odd prime. Find the number of non-zero squares mod p . Justify your answer.

As always, show your work, fully explain and justify your answer. A solution mainly obtained by computers or calculators will not be accepted.

Posting Date 10/23/2020. Submit solutions to Noah Aydin, Mathematics Department, RBH 319 by e-mail or hard-copy by 5 pm on Nov 6, 2020. An email submission must be a single pdf file. Hard copy submissions must be dropped in the file holder at my office door (Hayes 319) and must include a time stamp.