Deriving a Solution to Quadratic Residues

by : Aly Shmahell

Jan 3^{rd} 2016

if

$x^2 \equiv a \bmod p \Rightarrow a \equiv x^2 \bmod p \quad ....(1)$

then :

$a^{\frac{(p-1)}{2}} \equiv x^{2^{\frac{(p-1)}{2}}} \equiv x^{p-1} \equiv 1 \bmod p$

assuming

$\frac{(p-1)}{2} = 2k + 1 \quad ....(2)$

therefor :

$a^{2k+1} \equiv 1 \bmod p \quad ....(3)$

And :

$a^{2k+1} * a \equiv a^{2k+2} \bmod p$

$a \equiv a^{2k+2} \bmod p \quad ....$ according to (3)

$x^2 \equiv a^{2(k+1)} \bmod p \; ....$ according to (1)

$x \equiv a^{k+1} \bmod p \quad ....$ where k can be calculated from (2)