

# Deriving a Solution to Quadratic Residues

by : Aly Shmahell

Jan 3<sup>rd</sup> 2016

if

$$x^2 \equiv a \pmod{p} \Rightarrow a \equiv x^2 \pmod{p} \quad \dots(1)$$

then :

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

assuming

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

therefor :

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

And :

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

$$a \equiv a^{2k+2} \pmod{p} \quad \dots \text{ according to (3)}$$

$$x^2 \equiv a^{2(k+1)} \pmod{p} \quad \dots \text{ according to (1)}$$

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