

If $x^2 \equiv b \pmod{p}$ has no sol. $x^2 \equiv b \pmod{p^e}$ for $e \geq 2$, since any such sol $x^2 \equiv b \pmod{p^e}$ could always be reduced modulo p . And if it has two sol, then it implies that it will have two sol, $x^2 \equiv b \pmod{p^e}$ for each $e \geq 1$, the sol, are matched one-to-one.

$$2^{(p-1)/2} \pmod{p}$$

$$p=3$$

$$2^1 = 2 \equiv 2$$

$$p=5$$

$$2^2 = 4 \equiv 4$$

$$p=7$$

$$2^3 = 8 \equiv 1$$

$$p=11$$

$$2^5 = 32 \equiv 10$$

$$p=13$$

$$2^6 = 64 \equiv 12$$

$$p=17$$

$$2^8 = 256 \equiv 1$$

$$p=19$$

$$2^9 = 512 \equiv 18$$

$2^{(p-1)/2}$ is congruent to 1 or $(p-1) \pmod{p}$

Let $a = 2^{(p-1)/2}$. Then $a^2 \equiv 2^{p-1} \equiv 1 \pmod{p}$

$\therefore a \equiv \pm 1 \pmod{p}$, note that $p \mid (a^2 - 1)$, so $p \mid (a+1)(a-1)$. So, since p is a prime, it divides one of $a-1$ or $a+1$, which means $a \equiv \pm 1 \pmod{p}$