1.37 Given, $X = \alpha$ is a solution, $X^2 \equiv b \pmod{p^1}$. Prove, by induction. every $e \geq 1$, there exist a unique solution, $X = \beta$ satisfying both,

$$\beta^2 \equiv b \pmod{p^e} \quad \text{and} \quad \beta \equiv \alpha \pmod{p}$$

The case $e = 1$, given to us, we must take $\beta = \alpha$, Now, suppose that we have a value of β work for e, we need sol. that work for $e+1$. Now, if Ψ is a sol for $e+1$, then $\Psi \pmod{p^e}$ is a sol. for e. $\Psi \equiv \beta \pmod{p^e}$, the sol of Ψ for $e+1$, will have from

$$\Psi = \beta + yp^e \quad \text{for some integer } y. \quad y \,\%\, p = \Phi.$$

And, Φ will make Ψ into, a sol of $X^2 \equiv b \pmod{p^{e+1}}$.

β is a sol to $X^2 = b \pmod{p^e}$, mean. $\beta^2 = b + p^e B$ for $\mathbb{Z} \ni B$

Sub $\Psi = \beta + yp^e$ into congruency $X^2 \equiv b \pmod{p^{e+1}}$ solve for y.

$$(\beta + yp^e)^2 \equiv b \pmod{p^{e+1}}$$

$$\beta^2 + 2yp^e + y^2p^{2e} \equiv b \quad ''$$

$$\beta^2 + 2yp^e \equiv b \quad '' \quad \text{since } 2e \geq e+1$$

$$b + p^eB + 2yp^e \equiv b \quad '' \quad \text{since } \beta^2 = b + p^eB$$

$$\cancel{p^e}(B + 2y) \equiv 0 \pmod{p^{e+1}} \text{ or } \pmod{\cancel{p^e}p}$$

$$B + 2y \equiv 0 \pmod{p}, \quad y \equiv \frac{p-1}{2} \cdot B \pmod{p} \quad p > 2$$

$\therefore$ y is unique for any value of B.

This proves the for every $e \geq 1$, there exist a unique value of $\beta \pmod{p^e}$ satisfying $\beta^2 \equiv b \pmod{p^e}$ and $\beta \equiv \alpha \pmod{p}$