6.37

$p \geq 3 \qquad x^2 \equiv b(\mathrm{mod}\ p)$

a) $x^2 \equiv b(\mathrm{mod}\ p^e) \qquad e \geq 1$

b) $x = a$, $\underset{z \equiv b(\mathrm{mod}\ p^e)}{x^2} \equiv (\mathrm{mod}\ p)$, $\beta = a(\mathrm{mod}\ p)$

c) prove $\beta \equiv \beta'(\mathrm{mod}\ p^e)$

We can solve a, b, and c at the same time using induction on the variables above. It doesn really make since why they split up this question.

$w \equiv \beta(\mathrm{mod}\ p^e)$

There are many solutions for $e+1$ so $w = \beta + yp^e$ we need to show $y \mathrm{mod}\ p$ is unique the solution would be $x^2 \equiv b(\mathrm{mod}\ p^{e+1})$. Since $x^2 \equiv b(\mathrm{mod}\ p^e)$ then $\beta^2 = b + p^e B$. Substitute $w = \beta + yp^e$ into the congurence & solve for y.

$$(\beta_2 + yp^e)^2 \equiv b\ (\mathrm{mod}\ p^{e+1})$$

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

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

$$b + p^e B + 2yp^e \equiv b\ (\mathrm{mod}\ p^{e+1})$$

$$\underline{p^e(B+2y) \equiv 0\ (\mathrm{mod}\ p^{e+1})}$$ Finally...

So solve $B + 2y \equiv 0 \ \mathrm{mod}\ p$

as a result ~~from using above~~ variables $\boxed{y \equiv \frac{p-1}{2} B\ (\mathrm{mod}\ p)}$ which satisfies $e \geq 1$

which gives us $\boxed{\beta^2 \equiv b(\mathrm{mod}\ p^e)}$ and $\boxed{\beta \equiv a\ (\mathrm{mod}\ p)}$

d) It depends on the e that we are given.

When $e \geq 1$ ...

par