Q05 Let x be an integer and let p be an odd prime, we can thus start with an if and only if statement which can be expressed as:

$$x^2 + 1 \equiv 0 \pmod{p^2} \iff x^2 + 1 \equiv 0 \pmod{\text{p}}$$

We will split this into two cases such that the first case is:

$$x^2 + 1 \equiv 0 \pmod{p^2} \implies x^2 + 1 \equiv 0 \pmod{\text{p}}$$

To start we will assume the hypothesis such that $x_0^2 + 1 \equiv 0 \pmod{p^2}$ has a solution x_0, CTR tells us that therefore:

$$p^2 | (x_0^2 + 1)$$

We know from TD that since $p^2|(x_0^2 + 1)$ and $p|p^2$ that:

$$p|(x_0^2 + 1)$$

Thus from CTR we find that:

$$x_0^2 + 1 = 0 \pmod{\text{p}}$$

This thus proves the first iimplication as if a solution exists in the hypothesis that same solution (and others) will also exist in the conclusion.

The second case is of the form:

$$x^2 + 1 \equiv 0 \pmod{p} \implies x^2 + 1 \equiv 0 \pmod{p^2}$$

To start we will assume the hypothesis such that $x_0^2 + 1 \equiv 0 \pmod{p}$ has a solution, we also know that x can be re-written as:

$$x^2 + 1 \equiv 0 \pmod{p} = (qp + r)^2 + 1 \equiv \pmod{p}$$

Expanding we find that it equals:

$$q^2p^2 + 2qpr + r^2 + 1 \equiv 0 \pmod{p}$$

Lets get rid of the left most term by using CAM (as we know $p^2 \pmod{\text{p}} = 0$):

$$q^2(0)^2 + 2qpr + r^2 + 1 \equiv 0 \pmod{p}$$

$$2qpr + r^2 + 1 \equiv 0 \pmod{p}$$

We will let a value s such that s is a solution of $s^2 + 1 = 0 \pmod{\text{p}}$, from CTR this becomes $p|(s^2 + 1)$ and for some integer o, $po = s^2 + 1$. Setting r = s we find that:

$$2qps + s^2 + 1 \equiv 0 \pmod{p}$$

$$2qps + (s^2 + 1) \equiv 0 \pmod{p}$$

$$2qps + po \equiv 0 \pmod{p}$$

If we apply CTR again we find that:

$$p|2qps + po$$

In order for there to be a solution for

$$2qps + po \equiv 0 \pmod{p}$$

, the CTR will become:

$$p^2|p(2qs + o)$$

$$p|2qs + o$$

The definition of derivatives tells us that for some integer m:

$$2qs + o = mp$$

The solution set to $p^2|p(2qs + o)$, is thus equal to $2qs + o = mp$ which now has the congurence form:

$$(2s)q = -o \pmod{\text{p}}$$

Notice that $2s$ is even while p is false this implies that from LCT, gcd(2s,p) = 1 and $1|-o$ (as m is defined as an integer). This means a solution exists to $(2s)q = -o$ (mod p) if we have a solution to $x_0^2 + 1 \equiv 0 \pmod{p}$.
More over we know the solution set of $(2s)q = -o$ (mod p) is equal to the solution set of

$$p^2|p(2qs + o)$$

and since by CTR thats equal to:

$$2pqs + po = 0 \pmod{p^2}$$

We have thus proved this has a solution if $x_0^2 + 1 \equiv 0$ (mod p) has a the solution x, thus proving the implication. Now that we have proved both implications true for any p and the solution x is an integer (as q,b,r are all integers) we have proved the if and only if statement.