Legendre's Theorem L.

Let p be an odd prime >3 and let $0<x<y<z=(y+1)$ be relatively prime integers such that $x^p+y^p=z^p$ and let p not divide xyz. We obtain a contradiction.

Now $x^p \equiv x \pmod p$; $y^p \equiv y \pmod p$; $z^p \equiv z \pmod p$.

So $0 \equiv x^p+y^p-z^p \equiv (x+y-z) \equiv (x-1) \pmod p$.

So $x \equiv 1 \pmod p$ ---------- (1)

So $x^p \equiv 1 \pmod{p^2}$ ---------- (2).

Let $y^p = y+bp$; $z^p = z+b'p$ ---------- (3)

where b, b' are integers.

Then $0 \equiv x^p+y^p-z^p \pmod{p^2}$

$\equiv 1+y+bp-z-b'p$

$\equiv (b-b')p \pmod{p^2}$.

So $b'p \equiv bp \pmod{p^2}$ ---------- (4)

Now $x^p = z^p-y^p = (z-y)(z^{(p-1)}+z^{(p-2)}y+\cdots+y^{(p-1)})$

$= z^{(p-1)}+z^{(p-2)}y+\cdots+y^{(p-1)}$.

$x^p-z^{(p-1)}-y^{(p-1)} = yz(z^{(p-3)}+z^{(p-4)}y+\cdots+y^{(p-3)})$ ---------- (5)

(5) $\times yz(z-y)$;

$$yz(z-y)(x^{p}-z^{(p-1)}-y^{(p-1)}) \equiv y^2z^2(z-y)(z^{(p-3)}+z^{(p-4)}y+\cdots+y^{(p-3)})$$

$$\equiv y^2z^2(z^{(p-2)}-y^{(p-2)})$$

$$x^p yz(z-y)-(z-y)(yz^p+zy^p) \equiv y^2z^p-z^2y^p \quad \text{---(6)}$$

(6) mod p^2;

$$yz-y(z+b'p)-z(y+bp) \equiv y^2(z+b'p)-z^2(y+bp)$$

By (4), we get;

$$-yz-(y+z)bp \equiv yz(y-z)+bp(y^2-z^2)$$

$$\equiv yz+bp(-2y-1)$$

$$0 \equiv 0 \pmod{p^2} \equiv yz-(y+z)bp$$

Thus; $2y^2z+2yz \equiv 0 \pmod{p^2}$ ---(7).

This is; $2yz(y+z) \equiv 0 \pmod{p^2}$

Which is; $yz(y+z) \equiv 0 \pmod{p^2}$ ---(8).

But, by assumption, $p \nmid yz$. So $p^2 \mid (y+z)$ ---(9)

So $y \equiv \left(\frac{p^2-1}{2}\right) \pmod{p^2}$,

$z \equiv \left(\frac{p^2+1}{2}\right) \pmod{p^2}$

Similarly $p^2 \mid (x+z)$.

So $p^2 \mid (x+y+2z)$ (10)

But $p \mid (x+y-z)$.

So $p \mid 3z$. $p \neq 3$.

So contradiction shows FLT holds, $p \neq 3$. (11).

So $(2y)^p \equiv -1 \pmod{p^3}$

$(2z)^p \equiv +1 \pmod{p^3}$

So $2^p \equiv 2 \pmod{p^3}$. So $2^{p-1} \equiv 1 \pmod{p^2}$. Hence $(b-b')p \equiv 0 \pmod{p^2}$, etc, allowing induction. Hence $(y+1)-z \equiv 1 \pmod{p^2}$

(3).

Legendre's Theorem: L.

Put (10) into $x \equiv (z-y) \pmod{p^2}$ (see below). and get

$x \equiv 1 \pmod{p^2}$ ---------- (12).

So $x^p \equiv 1 \pmod{p^3}$ ---------- (13).

Let $b'_p \equiv b_p \pmod{p^3}$.

Hence $yz(y+z) \equiv 0 \pmod{p^3}$ ---------- (14).

So $y \equiv \left(\frac{p^3-1}{2}\right) \pmod{p^3}$

and $z \equiv \left(\frac{p^3+1}{2}\right) \pmod{p^3}$ } ---------- (15).

Now $x^p \equiv x \pmod{p^2}$; $y^p \equiv y \pmod{p^2}$; $z^p \equiv z \pmod{p^2}$ is known, so we can use it. Indeed, Ribenboim's "13 Lectures on FLT" has a short proof that, if FLT1 fails, $x^p \equiv x \pmod{p^3}$; $y^p \equiv y \pmod{p^3}$; $z^p \equiv z \pmod{p^3}$.

So we get

$y \equiv \left(\frac{p^4-1}{2}\right) \pmod{p^4}$

and $z \equiv \left(\frac{p^4+1}{2}\right) \pmod{p^4}$ } ---------- (16).

Induction cannot go further ??

Get $x \equiv 1 \pmod{p^4}$ ---------- (17).

$2^p x^p \equiv 2^p z^p - 2^p y^p \equiv (p^4+1)^p - (p^4-1)^p \equiv 2 \pmod{p^5}$

$2 \equiv 2^p x^p \pmod{p^5} \equiv 2^p \pmod{p^5}$ ---------- (18).

Surely $2^p \equiv 2 \pmod{p^5}$ is impossible ??

Or, maybe we only have $x \equiv 1 \pmod{p^3}$? Thus, we only get $2^p \equiv 2 \pmod{p^4}$, which is also surely impossible. Thus, Ribenboim, somewhere in "13 lectures on FLT", states that there is no odd prime p for which $2^p \equiv 2 \pmod{p^3}$.