Minden $p > 5$ prímszámra érvényes a

$$2 < \frac{p-1}{2} < p-1$$

becslés, ami azt jelenti, hogy a $2,\ (p-1)/2,\ p-1$ egész számok egymástól különböznek, és mindegyikük előfordul az $1,\ 2,\ \ldots,\ p-1$ számok között. Így

$$(p-1)^2 = \left(2 \cdot \frac{p-1}{2} \cdot (p-1)\right) \Big| (p-1)!.$$

Ha valamely $p > 5$ prímszám és m természetes szám esetén

$$(p-1)! + 1 = p^m$$

teljesülne, akkor abból $(p-1)^2 | (p^m - 1)$ következne. Mindkét oldalt $(p-1)$-gyel osztva azt kapnánk, hogy

$$p - 1 | p^{m-1} + \ldots + p + 1, \tag{1}$$

a jól ismert

$$p^k - 1 = (p-1)(p^{k-1} + \ldots + p + 1)$$

azonosság alapján.
Ugyanebből az azonosságból az is következik, hogy$(p-1)|(p^k - 1)$, vagyis

$$p^k \equiv 1 \pmod{p-1}, \qquad \text{ha } k = 0,\ 1,\ 2, \ldots;$$

ezért

$$p^{m-1} + p^{m-2} + \ldots + p - 1 \equiv m \pmod{(p-1)},$$

(1) szerint ekkor $(p-1)|m$.

Tehát szükségképpen $m \geq p-1$, ezért

$$p^m \geq p^{p-1} > (p-1)^{p-1} > (p-1)! = p^m - 1, \quad \text{ellentmondás.}$$