Mivel

$$\binom{p^m}{p} - p^{m-1} = \frac{p^m(p^m-1)\dots(p^m-p+1)}{p(p-1)\dots 2\cdot 1} - p^{m-1} =$$
$$= p^{m-1}\left(\frac{(p^m-1)\dots(p^m-p+1)}{(p-1)\dots 2\cdot 1} - 1\right) = p^{m-1}\left(\binom{p^m-1}{p-1} - 1\right),$$

az állítás azzal ekvivalens, hogy $\binom{p^m-1}{p-1} - 1 = \frac{(p^m-1)\dots(p^m-p+1)}{(p-1)\dots 2\cdot 1} - 1$ osztható $p$-vel, azaz

$$\frac{(p^m-1)\dots(p^m-p+1)}{(p-1)\dots 2\cdot 1} \equiv 1 \pmod p.$$

Ezt a kongruenciát megszorozhatjuk a $p$-hez relatív prím $(p-1)!$-sal:

$$(p^m-1)\dots(p^m-p+1) \equiv (p-1)\dots 2\cdot 1 \pmod p.$$

A bal oldalon minden tényezőt $(p^m-p)$-vel (ami többszöröse $p$-nek) csökkentve, a kongruencia ekvivalens a

$$(p-1)(p-2)\dots 2\cdot 1 \equiv (p-1)(p-2)\dots 2\cdot 1 \pmod p$$

azonossággal, vagyis igaz.

*Megjegyzések.* 1. Ha $p$ páratlan, akkor

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

ezért $\binom{p^m-1}{p-1} - 1 = \frac{(p^m-1)\dots(p^m-p+1)}{(p-1)\dots 2\cdot 1} - 1$ osztható $p^m$-mel. Ebből pedig az is következik, hogy $\binom{p^m}{p} - p^{m-1}$ osztható $p^{2m-1}$-nel.

*Puskás Zsolt* (Budapest, ELTE Apáczai Csere J. Gyak. Gimn., IV. o.t.)

2. Ha $p$ páratlan, akkor az is igaz, hogy $\binom{p^m}{p} - p^{m-1}$ osztható $p^{2m}$-nel.

A zárójelek felbontásával

$$(p^m-1)\dots(p^m-p+1) = (1-p^m)(2-p^m)\dots(p-1-p^m) \equiv$$
$$\equiv 1\cdot 2\cdot\dots\cdot(p-1) - p^m\cdot 2\cdot 3\cdot\dots\cdot(p-1) -$$
$$-1\cdot p^m\cdot 3\cdot\dots\cdot(p-1) - \dots - 1\cdot 2\cdot 3\cdot\dots\cdot(p-2)\cdot p^m =$$
$$= (p-1)! - p^m\left(\frac{(p-1)!}{1} + \frac{(p-1)!}{2} + \dots + \frac{(p-1)!}{p-1}\right) \pmod{p^{2m}}.$$

A zárójelben levő törtek értékei egész számok, nem oszthatók $p$-vel és különböző maradékot adnak $p$-vel osztva, mert ha

$$\frac{(p-1)!}{i} \equiv \frac{(p-1)!}{j} \pmod p,$$

akkor

$$(p-1)!\cdot j \equiv (p-1)!\cdot i \pmod p$$

és $j \equiv i \pmod p$. Ezért

$$\frac{(p-1)!}{1} + \frac{(p-1)!}{2} + \dots + \frac{(p-1)!}{p-1} \equiv 1 + 2 + \dots + (p-1) = p\frac{p-1}{2} \equiv 0 \pmod p,$$

és így

$$(p^m-1)\dots(p^m-p+1) \equiv (p-1)! \pmod{p^{m+1}}.$$

Ebből pedig következik, hogy $\binom{p^m-1}{p-1} - 1$ osztható $p^{m+1}$-nel, $\binom{p^m}{p} - p^{m-1}$ pedig osztható $p^{2m}$-nel.

*Ehreth Imre* (Bonyhád, Petőfi S. Gimn., IV. o.t.)