1°. $\binom{p-1}{k}^2 - 1 = \left[\binom{p-1}{k} + 1\right]\left[\binom{p-1}{k} - 1\right].$

Kimutatjuk, hogy a jobboldali tényezők egyike és így a szorzat is osztható p-vel, ha p törzsszám; még pedig ha k páros, akkor $\binom{p-1}{k} - 1$, ha k páratlan, akkor $\binom{p-1}{k} + 1$ osztható p-vel.

$$\text{Nyilván } \binom{p-1}{k} - 1 = 1 - 1 = 0,$$
$$\binom{p-1}{k} + 1 = p - 1 + 1 = p.$$
$$\binom{p-1}{k} 1 = \frac{p(p-1)(p-2)}{2} - 1 = \frac{p^2 - 3p + 2 - 2}{2} = \frac{p(p-3)}{2}.^{1}$$

Ezen esetekben tehát állításunk igaz. Tetszőleges l szám esetében

$$\binom{p-1}{l} + \binom{p-1}{l+1} = \binom{p}{l+1} = p\frac{(p-1)(p-2)\dots(p-l)}{1\cdot 2\cdot 3\dots(l+1)} = E,$$

ahol E egész szám és kell, hogy osztható legyen p-vel, mert p az $1,\ 2,\ 3\dots\ (l+1)$ tényezők mindegyikéhez relatív prím.

Eszerint $\binom{p-1}{l} + \binom{p-1}{l+1}$ összeg osztható p-vel ... I.

Láttuk, hogy ha $l = 2$, $\binom{p-1}{2} - 1 = mp$; tehát, ha $l = 3$, akkor I. miatt $\binom{p-1}{3} + 1 = m'p$ Ebből ismét következik, hogy $\binom{p-1}{4} - 1 = m''p$, s í. t.

2°. Az előbbiek szerint

$$\binom{p-1}{k} = mp + 1,\ \text{ha } k \text{ páros; tehát}$$
$$\binom{p-1}{k}^s = (mp+1)^s = Mp + 1.$$

Mint hogy ekkor $k+1$ páratlan,

$$\binom{p-1}{k+1} - m'p - 1 \text{ és így } \binom{p-1}{k+1}^s = (m'p-1)^s = \begin{cases} Np+1, & \text{ha } s \text{ páros} \\ Np-1, & \text{ha } s \text{ páratlan} \end{cases}$$

Legyen s páros. Ekkor

$$\begin{aligned}&\binom{p-1}{0}^s + \binom{p-1}{1}^s + \binom{p-1}{2}^s + \dots + \binom{p-1}{p-1}^s = \\ =&M_0p + 1 + M_1p + 1 + M_2p + 1 + \dots + M_{p-1}p + 1 = \\ =&(M_0 + M_1 + M_2 + \dots + M_{p-1})p + p\cdot 1 = M'p.\end{aligned}$$

Ha pedig s páratlan, akkor a szóbanforgó hatványösszeg

$$\begin{aligned}(M_0p+1) + (M_1p-1) + (M_2p+1) + (M_3p-1) + \dots + (M_{p-1}p+1)^{2} =\\ (M_0 + M_1 + M_2 + \dots + M_{p-1})p + 1 - 1 + 1 - 1 + \dots + 1 - 1 + 1 =\\ = M'p + 1.\end{aligned}$$

Q. e. d.

Schreiber Béla (Izr. g. VIII. o., Bp.)

[1] p a 2-nél nagyobb törzsszám páratlan és így $p-3$ páros.
[2] A zárójeles tagok száma p_1 páratlan.