Az állítás $k = p-1$-re nem igaz, mivel $(p-1)!$ nem osztható p-vel, hiszen p prím. Megmutatjuk, hogy $1 \leq k < p-1$ esetén teljesül az állítás.

Először a következőt igazoljuk. Ha $f(x)$ egy n-edfokú egész együtthatós polinom és x^n együtthatója nem osztható p-vel, akkor $f(x)$ legfeljebb n db 0 és $p-1$ közötti egész számra osztható p-vel.

A bizonyítást az n fokszámra vonatkozó teljes indukcióval végezzük. $n = 0$-ra az állítás nyilvánvaló. Tegyük fel, hogy az állítás $(n-1)$-re igaz. Legyen most $f(x)$ n-edfokú egész együtthatós polinom. Ha az $f(x) \equiv 0 \bmod p$ kongruenciának nincs megoldása, akkor nincs mit bizonyítanunk. Ellenkező esetben legyen α egy olyan 0 és $p-1$ közötti egész szám, amelyre

$$f(\alpha) \equiv 0 \bmod p \tag{1}$$

Ismeretes, hogy $(f(x) - f(\alpha))$-ból $(x - \alpha)$ kiemelhető, azaz

$$f(x) - f(\alpha) = (x - \alpha)\, g(x),$$

ahol $g(x)$ az x-nek $(n-1)$-edfokú egész együtthatós polinomja. α-ra fennáll (1), így a megoldandó kongruencia ilyen alakba írható:

$$f(x) - f(\alpha) \equiv 0 \bmod p,$$

azaz

$$(x - \alpha)\, g(x) \equiv 0 \bmod p. \tag{2}$$

Megjegyezzük, hogy $g(x)$ együtthatói függhetnek α-tól, de $g(x)$-ben x^{n-1} együtthatója megegyezik x^n-nek az $f(x)$-beli együtthatójával, tehát nem osztható p-vel.

Egy szorzat akkor és csak akkor osztható egy p prímmel, ha valamelyik tényezője osztható vele, azaz (2)-nek 0 és $p-1$ közötti megoldásai az $x = \alpha$ és a $g(x) \equiv 0 \bmod p$ megoldásai lesznek. Utóbbiból az indukciós feltétel szerint legföljebb $n-1$ van, mert $g(x)$ $(n-1)$-edfokú, következésképp (2)-nek és így (1)-nek legfeljebb n darab 0 és $p-1$ közötti megoldása van. Ezzel segédtételünket bebizonyítottuk.

Most rátérünk a feladat állításának igazolására. Legyen

$$f(x) = (x-1)(x-2)\ldots(x-p+1) - (x^{p-1} - 1).$$

A „kis-Fermat”-tétel értelmében $f(1), f(2), \ldots, f(p-1)$ mindegyike osztható p-vel, tehát az

$$f(x) \equiv 0 \bmod p$$

kongruenciának $p-1$ db 0 és $p-1$ közötti megoldása van. Másrészt f$f(x)$ legföljebb $(p-2)$-edfokú. Tehát a segédtétel értelmében $f(x)$ minden együtthatója osztható p-vel. $f(x)$-ben $1 \leq k < p-1$-re x^{p-1-k} együtthatója úgy kapható meg, hogy az $1, 2, \ldots, (p-1)$ számok közül minden lehetséges módon kiveszünk k különbözőt, ezeket összeszorozzuk, képezzük az így kapott $\binom{n-1}{k}$ szorzat összegét, és ezt az összeget megszorozzuk $(-1)^k$-na1. Ez a szám tehát osztható p-vel, ami a feladat állítását adja $1 \leq k < p-1$-re.

Megjegyzés. A bizonyított állításból teljes indukcióval az is kiadódik, hogy az $1^k + \ldots + (p-1)^k$ összeg minden $1 \leq k < (p-1)$-re osztható p-vel.