Az állítást k szerinti teljes indukcióval bizonyítjuk.

Ha $k = 1$, akkor kétféle összeg van: 0 és a_1, ezért az állítás igaz, sőt a kívánt 1 helyett kétféle maradékot adtunk p-vel osztva.

Tegyük fel, hogy at állítás igaz $k = k_0$-ra, ahol $2 \leq k_0 < p$. Jelölje az $e_1a_1+\ldots+e_{k_0}a_{k_0}$-tagú összegeket $s_1, s_2, \ldots, s_n$. Az indukciós feltevés szerint ezek legalább k_0-féle maradékot adnak p-vel osztva. Tekintsük most a $(k_0 + 1)$ tagú összegeket, és csoportosítsuk őket e_{k_0+1} értéke szerint. Ha $e_{k_0} = 0$, akkor éppen az $s_1, s_2, \ldots, s_n$ összegeket kapjuk; amikor $e_{k_0+1} = 1$, akkor pedig az $s_1 + a_{k_0+1}, s_2 + a_{k_0+1}, \ldots, s_n + a_{k_0+1}$ számokat.

Ha $s_1, s_2, \ldots, s_n$ *teljes maradékrendszer* modulo p (azaz p-vel osztva minden maradékot kiadnak), akkor készen vagyunk, hiszen a különböző maradékok száma $p \geq k$.

Feltehetjük tehát, hogy $s_1, s_2, \ldots, s_n$ nem adnak ki minden maradékot p-vel osztva.

Azt állítjuk, hogy ekkor $s_1 + a_{k_0+1}, s_2 + a_{k_0+1}, \ldots, s_n + a_{k_0+1}$ valamelyike olyan maradékot ad p-vel osztva, amely $s_1, \ldots, s_n$ maradékai között nem szerepel. Ebből az állítás már következik, mivel így a $(k_0 + 1)$-tagú összegek legalább 1-gyel több féle maradékot adnak p-vel osztva, mint a k_0-tagúak.

Tekintsük a $0, a_{k_0+1}, 2a_{k_0+1}, \ldots, (p-1)a_{k_0+1}$ számokat. Mivel a_{k_0+1} nem osztható p-vel, azért ezek p-vel osztva mind különböző maradékot adnak (ha ia_{k_0+1} és ja_{k_0+1} ugyanazt a maradékot adja, akkor különbségük, $(i-j)a_{k_0+1}$ osztható p-vel, ami csak $i = j$ esetén lehetséges); így ez egy teljes maradékrendszer modulo p.

Ezen számok között biztosan szerepel olyan, amelynek p-vel való osztási maradéka az s_i-k maradékai között nem szerepel, hiszen feltételezésünk szerint az s_i-k nem adnak ki minden lehetséges maradékot. Legyen az első ilyen szám az $l \cdot a_{k_0+1}$. Mivel a 0 szerepel az s_i-k között, l nem lehet 0, azaz $l \geq 1$.

A feltevés szerint $(l-1)a_{k_0+1}$ maradéka előfordul az s_i-k maradékai között, mondjuk

$$s_m \equiv (l-1)a_{k_0+1} \pmod{p},$$

ahol $1 \leq m \leq n$. Ekkor viszont $s_m + a_{k_0+1} \equiv la_{k_0+1} \pmod{p}$, tehát $s_m + a_{k_0+1}$ maradéka nem szerepel az s_i-k maradékai között.

Ezzel az állítást igazoltuk.

Megjegyzések. 1. Ezzel a módszerrel valójában azt bizonyítottuk be, hogy $k \leq p-1$ esetén a maradékok száma legalább $k+1$.

2. Ha $a_1 = a_2 = \ldots = a_k$ és $k \leq p-1$, akkor a különböző maradékok száma $k+1$.