Legyen

$$f(x) = (x+1)(x+2)\dots(x+p-1) = x^{p-1} + a_{p-2}x^{p-2} + \dots + a_1 x + a_0.$$

Ezzel a jelöléssel

$$\binom{2p-1}{p-1} - 1 = \frac{(p+1)\dots(2p-1) - 1\cdot 2\cdot\dots\cdot(p-1)}{(p-1)!} = \frac{f(p)-f(-p)}{(p-1)!}.$$

Mivel p prím, $(p-1)!$ és p^3 relatív prímek, ezért azt kell igazolnunk, hogy

$$f(p) - f(-p) = 2\left(a_1 p + a_3 p^3 + \dots + a_{p-2}p^{p-2}\right)$$

osztható p^3-nel, vagyis a_1 osztható p^2-tel.

Az f polinom definíciója alapján

$$a_1 = \sum_{k=1}^{p-1} \frac{(p-1)!}{k} = \sum_{k=1}^{\frac{p-1}{2}} \left(\frac{(p-1)!}{k} + \frac{(p-1)!}{p-k}\right) = p\sum_{k=1}^{\frac{p-1}{2}} \frac{(p-1)!}{k(p-k)}.$$

Mivel p prím, minden $1 \le k \le p-1$ egészhez egyértelműen létezik egy olyan $1 \le k\prime \le p-1$ egész, amelyre $k\prime k \equiv 1 \pmod p$. (A $k\prime$ számot k modulo p multiplikatív inverzének is nevezik.) A $k\prime$ lehetséges értékei között az $1, 2, \dots, p-1$ számok mindegyike pontosan egyszer fordul elő. Ezért

$$\frac{(p-1)!}{k(p-k)} + (p-1)!\cdot k\prime^2 = \frac{(p-1)!\cdot(1-(kk\prime)^2 + kpk\prime^2)}{k(p-k)} \equiv 0 \pmod p$$

és

$$2\sum_{k=1}^{\frac{p-1}{2}} \frac{(p-1)!}{k(p-k)} = \sum_{k=1}^{p-1} \frac{(p-1)!}{k(p-k)} \equiv -(p-1)!\sum_{k\prime=1}^{p-1} k\prime^2 =$$
$$= -(p-1)!\frac{p(p-1)(2p-1)}{6} \equiv 0 \pmod p.$$

Megjegyzések. 1. Wilson tétele szerint $(p-1)! \equiv -1 \pmod p$. Erre a tényre a megoldáshoz nincs szükség, de néhány kifejezés egyszerűbb alakba írható a segítségével.

2. Hasonló megoldás nyerhető a

$$2\left(\binom{2p-1}{p-1} - 1\right) = \binom{2p}{p} - 2 = \sum_{k=1}^{p-1}\binom{p}{k}^2 = p^2\sum_{k=1}^{p-1}\binom{p-1}{k-1}^2\frac{1}{k^2}$$

azonosságból is, felhasználva hogy $\binom{p-1}{k-1} \equiv (-1)^{k-1} \pmod p$.