Ha az a szám p-vel osztva 1 maradékot adna, akkor a minden hatványa is 1 maradékot adna p-vel osztva, hiszen a^i-1 osztható $(a-1)$-gyel, $a-1$ pedig p-vel. Ekkor az $S=a^k+a^{k-1}+\ldots+a+1$ összeg p-vel osztva $k+1$ maradékot ad. De a feltétel szerint $0<k+1<p$, ezért az S összeg nem lehetne osztható p-vel. Látható tehát, hogy $a-1$ nem osztható p-vel.

A feltétel szerint S osztható p-vel, így $(a-1)$-szerese, $(a-1)(a^k+a^{k-1}+\ldots+a+1)=a^{k+1}-1$ is. Így $a^{k+1}=mp+1$ alakú, valamilyen m egész számmal. Ekkor $(a^{k+1})^p=(mp+1)^p=(mp)^p+\binom{p}{1}(mp)^{p-1}+\ldots+\binom{p}{p-2}(mp)^2+\binom{p}{p-1}mp+1$.

Itt az utolsó tag kivételével mindegyik osztható p^2-tel. Az utolsó előtti tag azért, mert $\binom{P}{p-1}mp=mp^2$. A többiben pedig mp legalább másodfokon szerepel. Ezzel azt kaptuk, hogy $a^{(k+1)p}-1=(a^p-1)(a^{kp}+a^{(k-1)p}+\ldots+a^p+1)$ osztható p^2-tel.

Azt állítjuk, hogy a^p-1 nem osztható p-vel. Ugyanis a^p-a osztható p-vel; Fermat tétele szerint; s ha a^p-1 is osztható volna p-vel, akkor különbségük, $a-1$ is osztható volna p-vel, ami ellentmond a megoldás elején tett észrevételnek.

Tehát a^p-1 nem osztható p-vel, így relatív prím p^2-hez. Ekkor p^2 csak úgy lehet osztója $a^{(k+1)p}-1=(a^p-1)(a^{kp}+a^{(k-1)p}+\ldots+a^p+1)$-nek, ha osztója az $a^{kp}+a^{(k-1)p}+\ldots+a^p+1$ összegnek, és éppen ezt kellett bizonyítani.