436. Legyen p egy 3-nál nagyobb prímszám, és legyen:

$$S_1 = 1^{p^2-p-2} + 2^{p^2-p-2} + 3^{p^2-p-2} + \ldots + (p-1)^{p^2-p-2},$$
$$S_2 = 1^{p^2-p-1} + 2^{p^2-p-1} + 3^{p^2-p-1} + \ldots + (p-1)^{p^2-p-1}.$$

Igazoljuk, hogy S_1 osztható p-vel, S_2 pedig p^2-tel!

Kelemen József, Miskolc

Megoldás: S_1-ben a kitevők:
$p^2-p-2 = (p-2)(p+1)$. Ez páros szám, és nem osztható $p-1$ - gyel. Általánosan igazolni fogjuk, hogy az

$$S_1 = 1^k + 2^k + 3^k + \ldots + (p-1)^k$$

összeg osztható p-vel, ha p egy 3-nál nagyobb törzsszám, k pedig egy $p-1$-gyel nem osztható pozitív egész szám.

Válasszunk ki ugyanis az $1, 2, 3, ..., (p-1)$ számok közül egy olyan b számot, amelyre

$$b^k \neq 1 \pmod{p}$$

Ilyen mindig van. Ezután nézzük S_1-nek b^k-szorosát:

$$S_1 b^k = b^k + (2b)^k + (3b)^k + \ldots + [(p-1)b]^k,$$

amelynek tagjaiban ugyanazok a maradékok lépnek fel, mint S_1-ben, tehát:

$$S_1 b^k \equiv S_1 \pmod{p},$$

vagy:

$$S_1 \left(b^k - 1\right) \equiv 0 \pmod{p},$$

de a feltevés szerint $b^k - 1$ nem osztható p-vel, így kell, hogy S_1 legyen p-vel osztható, amit állítottunk.

S_2-ben szereplő kitevők páratlan k számok és $k-1$ ugyancsak nem osztható $p-1$-gyel. Minthogy $p-1$ páros szám, S_2 tagjait párosíthatjuk:

$$S_2 = \left[1^k + (p-1)^k\right] + \left[2^k + (p-2)^k\right] + \ldots + \left[\left(\frac{p-1}{2}\right)^k + \left(p - \frac{p-1}{2}\right)^k\right].$$

Mivel k páratlan szám, az $i^k + (p-i)^k$ alakú párosítások mindegyike osztható p-vel, mert ez az alapok összege. Az egyes párokban végezzük el a binomok hatványozását. Abszolút tag nem marad, p-nek második és ennél magasabb hatványát foglaljuk egybe (ez lesz Xp^2), így a következő módon írható az összeg:

$$S_2 = Xp^2 - kp\left[1^{k-1} + 2^{k-1} + 3^{k-1} + \ldots + \left(\frac{p-1}{2}\right)^{k-1}\right]$$

Az itt zárójelben levő összegről kimutatjuk, hogy ez osztható p-vel. Akkor ennek kp-szerese p^2-tel osztható, és ezzel igazolva lesz az, hogy S_2 is osztható p^2-tel.

Vegyük tekintetbe azt, hogy $k-1$ páros szám lévén

$$i^{k-1} \equiv (p-i)^{k-1} \pmod{p}.$$

Ezért az

$$1^{k-1} + 2^{k-1} + 3^{k-1} + \ldots + \left(\frac{p-1}{2}\right)^{k-1}$$

összegnek és a

$$(p-1)^{k-1} + (p-2)^{k-1} + \ldots + \left(p - \frac{p-1}{2}\right)^{k-1}$$

összegnek p-re vonatkozó maradéka ugyanaz. De e kettő összegére érvényes az S_1 sorra bizonyított törvényszerűség, hogy p-vel osztható, aminek az előbbiek alapján, következménye az, hogy S_2 már p^2-tel osztható.

Kőváry Károly, Budapest és Szikszai József, Kazincbarcika