

**Megoldás.** Legyen  $A_{n+1} = np_1^{1!}p_2^{2!}\dots p_n^{n!} + 1$ . Először megmutatjuk, hogy minden prím legfeljebb egyszer szerepelhet a sorozatban. Ha ugyanis lenne két index,  $i < j$ , amelyekre  $p_i = p_j$ , akkor  $(j-1)p_1^{1!}p_2^{2!}\dots p_{j-1}^{(j-1)!}$  osztható  $p_j$ -vel, mert tényezői között szerepel a  $p_i$ , így ha hozzáadunk 1-et, akkor nem lesz osztható vele; ez viszont ellentmond  $p_j$  definíciójának.

Tegyük föl, hogy van olyan  $p$  prím, amely nem szerepel a sorozatban. Belátjuk, hogy ekkor az  $A_n$  sorozat végtelen sok tagja osztható  $p$ -vel. Ez adja majd az ellentmondást, hiszen ha tekintjük a  $p$ -vel osztható  $A_n$  számokat, illetve azok legkisebb prímosztóját, akkor ezek nyilván nem nagyobbak  $p$ -nél, ugyanakkor mind különbözőek a fenti észrevételünk szerint, ami lehetetlen. Tehát elegendő belátnunk, hogy ha a  $p$  prím nem szerepel a sorozatban, akkor az  $A_n$  sorozat végtelen sok tagja osztható  $p$ -vel.

Legyen  $L = p_1^{1!}p_2^{2!}\dots p_{p-2}^{(p-2)!}$ ; ez nyilván nem osztható  $p$ -vel, mert egyik tényezője sem osztható  $p$ -vel (és  $p$  prím).

Legyen  $n > p-1$ , ekkor  $A_{n+1} = n \cdot L \cdot p_{p-1}^{p-1!}p_p^{p!}\dots p_n^{n!} + 1$ . Itt a  $p_k^{k!}$  ( $k > p-2$ ) alakú tényezők  $p$ -vel való maradéka mindig 1 a kis Fermat-tétel szerint, hiszen  $p_k$  nem osztható  $p$ -vel, illetve  $k!$  osztható  $(p-1)$ -gyel, mert az az egyik szorzó tényezője ( $p_k^{k!} \equiv p_k^{(p-1)b} \equiv (p_k^{p-1})^b \equiv 1^b \pmod{p}$ ).

Így  $A_{n+1} \equiv (n \cdot L + 1) \pmod{p}$ , ha  $n > p-1$ . Ezért, ha  $n \cdot L \equiv (-1) \pmod{p}$ -nek létezik  $n$ -re nézve megoldása, akkor készen vagyunk, mert ha  $n_0$  egy ilyen megoldás, akkor az  $A_{tp+n_0+1}$  számok mindegyikére

$$A_{tp+n_0+1} \equiv (tp+n_0) \cdot L + 1 \equiv n_0 \cdot L + 1 \equiv 0 \pmod{p}$$

– legalábbis, ha  $t$  elég nagy ahhoz, hogy  $tp+n_0$  nagyobb legyen  $(p-1)$ -nél; ez biztosítja, hogy az  $A_n$  sorozat végtelen sok tagja osztható  $p$ -vel.

Végül az  $n \cdot L \equiv (-1) \pmod{p}$  kongruenciának azért van megoldása, mert  $p$  prím,  $L$  pedig nem osztható  $p$ -vel, így  $L$  és  $p$  relatív prímek; emiatt a  $0, L, 2L, 3L, \dots, (p-1)L$  számok mind különböző maradékot adnak  $p$ -vel osztva, tehát  $e$   $p$  darab szám valamelyikének a maradéka  $-1$ .