

## Solution de Franck Gautier (Pérignat lès Sarliève).

Pour  $1 \leq p \leq l \leq k$ , on note

$$A_p^l = \prod_{i=p}^l (a_i - 1).$$

Si  $1 \leq p < l \leq k$ , alors

$$A_p^l = (a_p - 1) A_{p+1}^l = a_p A_{p+1}^l - A_{p+1}^l.$$

Puisque  $n$  divise  $a_p (a_{p+1} - 1)$ , il divise aussi  $a_p A_{p+1}^l$ , d'où la congruence

$$A_p^l \equiv -A_{p+1}^l \pmod{n}.$$

On en déduit

$$A_p^l \equiv (-1)^{l-p} A_l^l \pmod{n}.$$

En prenant successivement  $(p, l) = (1, k)$  et  $(p, l) = (2, k)$ , on obtient

$$A_1^k \equiv (-1)^{k-1} (a_k - 1) \pmod{n}$$

puis

$$A_2^k \equiv (-1)^k (a_k - 1) \pmod{n}.$$

Comme  $A_1^k = (a_1 - 1) A_2^k$ , on trouve

$$a_1 (a_k - 1) \equiv 0 \pmod{n}.$$

Donc  $n$  divise  $a_1 (a_k - 1)$ . Pour finir, si  $n$  divisait aussi  $a_k (a_1 - 1)$ , il diviserait

$$a_1 (a_k - 1) - a_k (a_1 - 1) = a_k - a_1,$$

ce qui est impossible puisque  $1 \leq a_k - a_1 \leq n - 1$ .