On considère le système (S) : $\begin{cases} t \equiv -4 \pmod{19} \\ t \equiv 4 \pmod{17} \end{cases}$

1. Montrer que les solutions du système (S) sont les entiers t de la forme $t = 323\,k + 72$ (k entier relatif)

2. Soit t une solution système (S)

a. montrer que $t^{36} \equiv 1$ mod. 323.

b. vérifier que $t^{30} \equiv 7$ (mod. 19) et $t^{30} \equiv -1$ (mod. 17).

CORRECTION

1. $t \equiv -4$ (mod. 19) donc 19 divise $t + 4$ donc il existe un entier relatif n tel que $t = 19\,n - 4$

$t \equiv 4$ (mod. 17) $\Leftrightarrow$ $19\,n - 4 \equiv 4$ (mod. 17) $\Leftrightarrow$ $2\,n \equiv 8$ (mod. 17) $\Leftrightarrow$ $16\,n \equiv 8 \times 8$ (mod. 17) $\Leftrightarrow$ $-n \equiv 64$ (mod. 17)

$64 = 17 \times 4 - 4$ donc $-n \equiv 64$ (mod. 17) $\Leftrightarrow$ $n \equiv 4$ (mod. 17) donc il existe un entier relatif k tel que $n = 17\,k + 4$

Alors $t = 19\,(17\,k + 4) - 4$ soit $t = 323\,k + 76 - 4$ soit $t = 323\,k + 72$

Réciproquement : si $t = 323\,k + 72$, $t = 19 \times 17\,k + 72$

or $72 = 17 \times 4 + 4$ donc $t \equiv 4$ (mod. 17) et $72 = 19 \times 4 - 4$ donc $t \equiv -4$ (mod. 19)

Les solutions du système (S) sont les entiers t de la forme $t = 323\,k + 72$ (k entier)

2. *a.* 19 est un nombre premier, 4 n'est pas divisible par 19 donc d'après le petit théorème de Fermat : $4^{18} \equiv 1$ (mod. 19)

donc $t^{18} \equiv 1$ (mod. 19) donc $(t^{18})^2 \equiv 1$ (mod. 19) soit $t^{36} \equiv 1$ (mod. 19)

$4^2 = 16$ donc $4^2 \equiv -1$ (mod. 17) donc $(4^2)^{18} \equiv (-1)^{18}$ (mod. 17) soit $4^{36} \equiv 1$ mod 17 donc soit $t^{36} \equiv 1$ (mod. 17)

19 divise $t^{36} - 1$ donc il existe un entier relatif n tel que $t^{36} - 1 = 19\,n$

17 divise $t^{36} - 1$ donc 17 divise $19\,n$, or 17 et 19 sont premiers entre eux donc d'après le théorème de Gauss, 17 divise n soit $n = 17\,q$

$t^{36} - 1 = 19\,n = 19 \times 17\,q$ donc $t^{36} - 1 = 323\,q$ soit $t^{36} \equiv 1$ mod. 323

2. *b.* $t \equiv -4$ (mod. 19), donc $t^{30} \equiv (-4)^{30}$ (mod. 19) soit $t^{30} \equiv 4^{30}$ (mod. 19)

$4^2 \equiv -3$ (mod. 19) donc $(4^2)^3 \equiv -27$ (mod. 19) or $-27 + 2 \times 19 = 11$ donc $4^6 \equiv 11$ (mod. 19) donc $4^{12} \equiv 11^2$ (mod. 19)

$11^2 = 121 = 19 \times 6 + 7$ donc $4^{12} \equiv 7$ (mod. 19)

$4^{30} = 4^{18} \times 4^{12}$ et $4^{18} \equiv 1$ (mod. 19) et $4^{12} \equiv 7$ (mod. 19) donc $4^{30} \equiv 1 \times 7$ (mod. 19) soit $4^{30} \equiv 7$ (mod. 19) donc $t^{30} \equiv 7$ (mod. 19)

$t \equiv 4$ (mod. 17) donc $t^2 \equiv 16$ (mod. 17) soit $t^2 \equiv -1$ (mod. 17) donc $(t^2)^{15} \equiv (-1)^{15}$ (mod. 17) soit $t^{30} \equiv -1$ (mod. 17)