

# Polynésie 2012. Enseignement de spécialité

## EXERCICE 4

### Partie A

- 1)  $25 \times 13 - 108 \times 3 = 325 - 324 = 1$ . Donc le couple  $(x_0, y_0) = (13, 3)$  est un couple d'entiers relatifs solution de l'équation (E). Notons alors que les entiers relatifs 25 et 108 sont premiers entre eux d'après le théorème de BÉZOUT.
- 2) Soit  $(x, y)$  un couple d'entiers relatifs.

$$25x - 108y = 1 \Leftrightarrow 25x - 108y = 25x_0 - 108y_0 \Leftrightarrow 25(x - x_0) = 108(y - y_0).$$

Ainsi, si  $(x, y)$  est un couple d'entiers relatifs solution de l'équation (E), alors l'entier 108 divise l'entier  $108(y - y_0) = 25(x - x_0)$  et puisque 108 et 25 sont des entiers premiers entre eux, le théorème de GAUSS permet d'affirmer que 108 divise  $x - x_0$ . Par suite, il existe un entier relatif  $k$  tel que  $x - x_0 = 108k$  ou encore  $x = x_0 + 108k$ . De même, l'entier 25 divise  $y - y_0$  et donc il existe un entier relatif  $k'$  tel que  $y - y_0 = 25k'$  ou encore  $y = y_0 + 25k'$ . Réciproquement, soient  $k$  et  $k'$  deux entiers relatifs puis  $x = x_0 + 108k$  et  $y = y_0 + 25k'$ .

$$\begin{aligned} 25x - 108y = 1 &\Leftrightarrow 25(x_0 + 108k) - 108(y_0 + 25k') = 1 \Leftrightarrow 25x_0 - 108y_0 + 25 \times 108 \times (k - k') = 1 \\ &\Leftrightarrow 25 \times 108 \times (k - k') = 0 \Leftrightarrow k = k'. \end{aligned}$$

Finalement,

les couples d'entiers relatifs solutions de l'équation (E) sont les couples de la forme  $(13 + 108k, 3 + 25k)$ ,  $k \in \mathbb{Z}$ .

### Partie B

- 1) Si  $x \equiv a \pmod{7}$  et  $x \equiv a \pmod{19}$ , alors  $x - a$  est divisible par les nombres premiers 7 et 19. On sait alors que  $x - a$  divisible par  $7 \times 19$  c'est-à-dire 133. Finalement,  $x - a$  est un multiple de 133 ou encore  $x \equiv a \pmod{133}$ .

2) a)

- $1^6 = 1$  et donc  $1^6 \equiv 1 \pmod{7}$ .
- $2^6 = 8^2$ . Or,  $8 \equiv 1 \pmod{7}$  et donc  $8^2 \equiv 1^2 \pmod{7}$  ou encore  $2^6 \equiv 1 \pmod{7}$ .
- $3^6 = 9^3$ . Or,  $9 \equiv 2 \pmod{7}$  et donc  $9^3 \equiv 8 \pmod{7}$  ou encore  $3^6 \equiv 1 \pmod{7}$ .
- $4 \equiv -3 \pmod{7}$ . Or,  $(-3)^6 = 3^6$  et donc  $4^6 \equiv 3^6 \pmod{7}$  ou encore  $4^6 \equiv 1 \pmod{7}$ .
- De même,  $5 \equiv -2 \pmod{7}$  et  $6 \equiv -1 \pmod{7}$ . Par suite,  $5^6 \equiv (-2)^6 \pmod{7}$  et  $6^6 \equiv (-1)^6 \pmod{7}$  ou encore  $5^6 \equiv 1 \pmod{7}$  et  $6^6 \equiv 1 \pmod{7}$ .

On a montré que pour tout entier  $x$  tel que  $1 \leq x \leq 6$ ,  $x^6 \equiv 1 \pmod{7}$ .

- b) On sait qu'un entier naturel est congru modulo au reste de la division euclidienne de cet entier par 7. Soit  $a$  un entier naturel non multiple de 7. Le reste de la division euclidienne de  $a$  par 7 n'est pas nul et donc il existe un entier  $x$  tel que  $1 \leq x \leq 6$  et  $a \equiv x \pmod{7}$ .

D'après la question précédente, on a  $x^6 \equiv 1 \pmod{7}$  et on en déduit que  $a^6 \equiv 1 \pmod{7}$ .

On en déduit que  $(a^6)^{18} \equiv 1^{18} \pmod{7}$  ou encore  $a^{108} \equiv 1 \pmod{7}$ .

Ensuite,  $(a^{25})^9 = a^{25 \cdot 9} = a^{1+108c} = a \times (a^{108})^c$ . Mais alors  $(a^{25})^9 \equiv a \times 1^c \pmod{7}$  ou encore  $(a^{25})^9 \equiv a \pmod{7}$ .

- c) Si  $a$  est un multiple de 7, alors  $a \equiv 0 \pmod{7}$  puis  $(a^{25})^9 \equiv (0^{25})^9 \pmod{7}$  ou encore  $(a^{25})^9 \equiv 0 \pmod{7}$ .

En résumé, si  $a \equiv 0 \pmod{7}$  et  $(a^{25})^9 \equiv 0 \pmod{7}$ . En particulier,  $(a^{25})^9 \equiv a \pmod{7}$ .

- d)  $(a^{25})^9 \equiv a \pmod{7}$  et  $(a^{25})^9 \equiv a \pmod{19}$ . D'après la question 1) de la partie B,

pour tout entier naturel  $a$ ,  $(a^{25})^9 \equiv a \pmod{133}$ .

### Partie C

- 1)  $r_1 \equiv r^{13} \pmod{133}$  et  $r^{13} \equiv (a^{25})^{13} \pmod{133}$ . Donc,  $r_1 \equiv (a^{25})^{13} \pmod{133}$ .

D'autre part, le couple  $(g, c) = (13, 3)$  est un couple d'entiers relatifs solution de l'équation (E) d'après la question 1) de la partie A.

Mais alors  $(a^{25})^{13} \equiv a \pmod{133}$  d'après la question 2)c) de la partie B.

En résumé,  $r_1 \equiv (a^{25})^{13} \pmod{133}$  et  $(a^{25})^{13} \equiv a \pmod{133}$ . On en déduit que

$$r_1 \equiv a \pmod{133}.$$

2) •  $128^2 \equiv (-5)^2 \pmod{133}$  ou encore  $128^2 \equiv 25 \pmod{133}$  puis  $128^{12} \equiv 25^6 \pmod{133}$ .  
 $25^6 = 5^{12} = (5^3)^4 = 125^4$ . Comme  $125 \equiv -8 \pmod{133}$ ,  $128^{12} \equiv (-8)^4 \pmod{133}$  ou encore  $128^{12} \equiv 8^4 \pmod{133}$ .  
 $8^4 = 2^{12} = 2^7 \times 2^5 = 128 \times 32$  et donc  $128^{12} \equiv -5 \times 32 \pmod{133}$  ou encore  $128^{12} \equiv -160 \pmod{133}$  ou encore  $128^{12} \equiv -160 + 133 \pmod{133}$  ou enfin

$$128^{12} \equiv -27 \pmod{133}.$$

$128^{13} = 128^{12} \times 128$  et donc  $128^{13} \equiv -27 \times -5 \pmod{133}$  ou encore  $128^{13} \equiv 135 \pmod{133}$  ou enfin

$$128^{13} \equiv 2 \pmod{133},$$

(avec  $0 \leq 2 < 133$ ).

•  $59^2 = 3481 = 23 + 26 \times 133$  et donc  $59^2 \equiv 23 \pmod{133}$  puis  $59^{12} \equiv 23^6 \pmod{133}$ .  
 $23^2 = 529 = -3 + 4 \times 133$  et donc  $23^2 \equiv -3 \pmod{133}$  puis  $59^{12} \equiv (-3)^3 \pmod{133}$  ou encore  $59^{12} \equiv -27 \pmod{133}$ .  
Mais alors,  $59^{13} \equiv -27 \times 59 \pmod{133}$  ou encore  $59^{13} \equiv -1593 \pmod{133}$  ou encore  $59^{13} \equiv -1593 + 12 \times 133 \pmod{133}$   
ou enfin  $59^{13} \equiv 3 \pmod{133}$  (avec  $0 \leq 3 < 133$ ).

Le message qui a été codé est le message : 2 3.