

Partie A

On considère l'équation (E) : $25x - 108y = 1$ où x et y sont des entiers relatifs.

1. Vérifier que le couple $(13; 3)$ est solution de cette équation.
2. Déterminer l'ensemble des couples d'entiers relatifs solutions de l'équation (E).

Partie B

Dans cette partie, a désigne un entier naturel et les nombres c et g sont des entiers naturels vérifiant la relation $25g - 108c = 1$.

On rappelle le petit théorème de Fermat :

Si p est un nombre premier et a un entier naturel non divisible par p , alors a^{p-1} est congru à 1 modulo p que l'on note $a^{p-1} \equiv 1 [p]$.

1. Soit x un entier naturel.

Démontrer que si $x \equiv a [7]$ et $x \equiv a [19]$ alors $x \equiv a [133]$.

2. (a) On suppose que a n'est pas un multiple de 7.

Démontrer que $a^6 \equiv 1 [7]$ puis que $a^{108} \equiv 1 [7]$.

En déduire que $(a^{25})^g \equiv a [7]$.

- (b) On suppose que a est un multiple de 7.

Démontrer que $(a^{25})^g \equiv a [7]$.

- (c) On admet que pour tout entier naturel a , $(a^{25})^g \equiv a [19]$.

Démontrer que $(a^{25})^g \equiv a [133]$.

Partie C

On note A l'ensemble des entiers naturels a tels que : $1 \leq a \leq 26$.

Un message, constitué d'entiers appartenant à A , est codé puis décodé.

La phase de codage consiste à associer, à chaque entier a de A , l'entier r tel que $a^{25} \equiv r \pmod{133}$ avec $0 \leq r < 133$.

La phase de décodage consiste à associer à r , l'entier r_1 tel que $r^{13} \equiv r_1 \pmod{133}$ avec $0 \leq r_1 < 133$.

1. Justifier que $r_1 \equiv a \pmod{133}$.
2. Un message codé conduit à la suite de deux entiers suivants :
128 59.
Décoder ce message.

Analyse

Théorème de Gauss, petit théorème de Fermat, propriétés de la relation de congruence sont « au programme » de cet exercice d'arithmétique qui propose, classiquement désormais, comme application des résultats intermédiaires un travail de décodage où la calculatrice peut être assez utile ...

Résolution

Partie A

Question 1.

On a immédiatement : $25 \times 13 - 108 \times 3 = 325 - 324 = 1$.

Le couple $(13; 3)$ est solution de l'équation $25x - 108y = 1$.

Question 2.

En utilisant le résultat de la question précédente, l'équation se réécrit classiquement :

$$25x - 108y = 25 \times 13 - 108 \times 3$$

Soit : $25(x - 13) = 108(y - 3)$.

25 divise donc le produit $108(y - 3)$.

Les entiers $25 = 5^2$ et 108 étant premiers entre eux (5 ne divise pas 108), on en déduit que 25 divise $y - 3$ (théorème de Gauss), soit : $y - 3 = 25k$ où k est un entier relatif.

Il vient alors : $25(x - 13) = 108 \times 25k$, soit : $x - 13 = 108k$.

En définitive : $(x; y) = (13 + 108k; 3 + 25k)$ où k est un entier relatif.

L'ensemble des couples d'entiers relatifs solutions de l'équation (E) est l'ensemble :

$$\{(13 + 108k; 3 + 25k) / k \in \mathbb{Z}\}$$

Partie B

Question 1.

Comme $x \equiv a [7]$, il existe un entier k tel que : $x = a + 7k$.

De même, comme $x \equiv a [19]$, il existe un entier k' tel que : $x = a + 19k'$.

On a donc : $x = a + 7k = a + 19k'$, soit : $7k = 19k'$.

Les entiers 7 et 19 étant premiers entre eux, On en déduit (théorème de Gauss) que 7 divise k' , soit $k' = 7k''$, où k'' est un entier.

On a alors : $x = a + 19k' = a + 19 \times 7k'' = a + 133k''$.

L'entier x est bien congru à a modulo 133.

$$\text{Si } x \equiv a [7] \text{ et } x \equiv a [19] \text{ alors } x \equiv a [133]$$

Question 2.a.

Ici, a n'est pas un multiple de 7 qui est premier. Le petit théorème de Fermat nous permet alors d'affirmer que a^{7-1} est congru à 1 modulo p , soit $a^6 \equiv 1 [7]$.

Remarquons que l'on a : $108 = 6 \times 18$.

D'après le résultat précédent, il vient alors : $(a^6)^{18} \equiv 1^{18} [7]$, soit : $a^{108} \equiv 1 [7]$.

On a : $25g - 108c = 1$, soit : $25g = 108c + 1$.

Il vient alors : $(a^{25})^g = a^{25g} = a^{108c+1}$.

Comme $a^{108} \equiv 1 [7]$, on a : $(a^{108})^c \equiv 1^c [7]$, soit : $a^{108c} \equiv 1 [7]$.

D'où : $a^{108c} \times a \equiv 1 \times a [7]$, soit : $a^{108c+1} \equiv a [7]$, c'est-à-dire : $(a^{25})^g \equiv a [7]$.

Si a n'est pas un multiple de 7, on a :

$$a^6 \equiv 1 [7], a^{108} \equiv 1 [7] \text{ et } (a^{25})^g \equiv a [7].$$

Question 2.b.

Puisque a est un multiple de 7, il en va de même pour toute puissance de a d'exposant entier naturel non nul. Ainsi, $(a^{25})^g$ est un multiple de 7.

La différence $(a^{25})^g - a$ est elle-même un multiple de 7, soit : $(a^{25})^g - a \equiv 0 [7]$.

D'où : $(a^{25})^g \equiv a [7]$.

$$\text{Si } a \text{ est un multiple de 7 alors } (a^{25})^g \equiv a [7].$$

Question 2.c.

D'après les deux questions précédentes, on a, pour tout entier a : $(a^{25})^8 \equiv a \pmod{7}$.

On admet, par ailleurs, que l'on a : $(a^{25})^8 \equiv a \pmod{19}$.

D'après la question 1 de cette partie (on prend $x = (a^{25})^8$), on en déduit immédiatement :

$$(a^{25})^8 \equiv a \pmod{133}.$$

$$\text{Pour tout entier naturel } a, \text{ on a : } (a^{25})^8 \equiv a \pmod{133}.$$

Partie C

Question 1.

On a $a^{25} \equiv r \pmod{133}$. Donc : $(a^{25})^{13} \equiv r^{13} \pmod{133}$. Soit : $a^{25 \times 13} \equiv r_1 \pmod{133}$.

Mais d'après la question 2.c de la partie B, comme le couple $(g; c) = (13; 3)$ est solution de l'équation (E), on a : $a^{25 \times 13} \equiv a \pmod{133}$.

De $a^{25 \times 13} \equiv r_1 \pmod{133}$ et $a^{25 \times 13} \equiv a \pmod{133}$, on tire immédiatement $r_1 \equiv a \pmod{133}$.

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

Remarque : l'entier r_1 vérifie $0 \leq r_1 < 133$ et l'entier a vérifie $1 \leq a \leq 26$. La relation $r_1 \equiv a \pmod{133}$ nous permet alors de conclure $a = r_1$.

Question 2.

→ 1^{er} cas : $r = 128$.

On s'intéresse ici 128^{13} dont on cherche le reste dans la division euclidienne par 133.

128 étant proche de 133, on a intérêt à partir de $128 \equiv -5 \pmod{133}$.

Il vient alors : $128^{13} \equiv (-5)^{13} \pmod{133} \equiv -5^{13} \pmod{133}$.

On a : $5^3 = 125 \equiv -8 \pmod{133}$. D'où : $5^{12} = (5^3)^4 \equiv (-8)^4 \pmod{133} \equiv 4096 \pmod{133}$.

Comme $3 \times 133 = 399$, on a facilement : $4096 = 3990 + 133 - 27 = 31 \times 133 - 27$.

D'où : $5^{12} \equiv -27 \pmod{133}$. Alors : $-5^{13} = -5 \times 5^{12} \equiv -5 \times (-27) \pmod{133} \equiv 135 \pmod{133} \equiv 2 \pmod{133}$.

Pour $r = 128$ on obtient donc $r_1 = a = 2$.

→ 2^{ème} cas : $r = 59$

On s'intéresse ici 59^{13} dont on cherche le reste dans la division euclidienne par 133.

59 étant « éloigné » de 133, on ne peut, à priori, reproduire la démarche précédente.

On a facilement : $59^2 \equiv 23 [133]$, $59^3 \equiv 27 [133]$ et $59^4 \equiv 130 [133] \equiv -3 [133]$.

Nous exploitons ce dernier résultat : $59^{12} = (59^4)^3 \equiv (-3)^3 [133] \equiv -27 [133]$.

D'où : $59^{13} = 59^{12} \times 59 \equiv -27 \times 59 [133] \equiv -1593 [133]$.

Comme $1593 = 133 \times 12 - 3$, on a finalement : $59^{13} \equiv 3 [133]$.

Le message décodé est donc :

2 3