Corrigé

Exercice 4

freemaths.fr

BACCALAURÉAT GÉNÉRAL

SESSION 2018

ÉPREUVE DU VENDREDI 4 MAI 2018

MATHÉMATIQUES

– Série S –

Enseignement Spécialité Coefficient : 9

Durée de l'épreuve : 4 heures

Les calculatrices électroniques de poche sont autorisées, conformément à la réglementation en vigueur.

Le sujet est composé de 4 exercices indépendants.
Le candidat doit traiter tous les exercices.
Le candidat est invité à faire figurer sur la copie toute trace de recherche, même incomplète ou non fructueuse, qu'il aura développée.
Il est rappelé que la qualité de la rédaction, la clarté et la précision des raisonnements entreront pour une part importante dans l'appréciation des copies.

Avant de composer, le candidat s'assurera que le sujet comporte bien 9 pages numérotées de 1 à 9.

EXERCICE 4 (5 points)

Candidats ayant suivi l'enseignement de spécialité

À toute lettre de l'alphabet on associe un nombre entier x compris entre 0 et 25 comme indiqué dans le tableau ci-dessous :

Lettre	A	B	C	D	E	F	G	H	I	J	K	L	M
x	0	1	2	3	4	5	6	7	8	9	10	11	12

Lettre	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
x	13	14	15	16	17	18	19	20	21	22	23	24	25

Le « chiffre de RABIN » est un dispositif de cryptage asymétrique inventé en 1979 par l'informaticien Michael RABIN.

Alice veut communiquer de manière sécurisée en utilisant ce cryptosystème. Elle choisit deux nombres premiers distincts p et q. Ce couple de nombres est sa clé privée qu'elle garde secrète.

Elle calcule ensuite $n = p \times q$ et elle choisit un nombre entier naturel B tel que $0 \leqslant B \leqslant n-1$.

Si Bob veut envoyer un message secret à Alice, il le code lettre par lettre.

Le codage d'une lettre représentée par le nombre entier x est le nombre y tel que :

$$y \equiv x(x+B) \ [n] \text{ avec } 0 \leqslant y < n.$$

Dans tout l'exercice on prend $p = 3,\ q = 11$ donc $n = p \times q = 33$ et $B = 13$.

Partie A : Cryptage

Bob veut envoyer le mot « NO » à Alice.

1. Montrer que Bob code la lettre « N » avec le nombre 8.

2. Déterminer le nombre qui code la lettre « O ».

Partie B : Décryptage

Alice a reçu un message crypté qui commence par le nombre 3.
Pour décoder ce premier nombre, elle doit déterminer le nombre entier x tel que :

$$x(x+13) \equiv 3 \ [33] \text{ avec } 0 \leqslant x < 26.$$

1. Montrer que $x(x+13) \equiv 3 \ [33]$ équivaut à $(x+23)^2 \equiv 4 \ [33]$.

2. **a.** Montrer que si $(x+23)^2 \equiv 4 \ [33]$ alors le système d'équations $\begin{cases} (x+23)^2 \equiv 4 \ [3] \\ (x+23)^2 \equiv 4 \ [11] \end{cases}$ est vérifié.

b. Réciproquement, montrer que si $\begin{cases} (x+23)^2 \equiv 4 \ [3] \\ (x+23)^2 \equiv 4 \ [11] \end{cases}$ alors $(x+23)^2 \equiv 4 \ [33]$.

c. En déduire que $x(x+13) \equiv 3 \ [33] \Leftrightarrow \begin{cases} (x+23)^2 \equiv 1 \ [3] \\ (x+23)^2 \equiv 4 \ [11] \end{cases}$.

3. **a.** Déterminer les nombres entiers naturels a tels que $0 \leqslant a < 3$ et $a^2 \equiv 1 \ [3]$.

b. Déterminer les nombres entiers naturels b tels que $0 \leqslant b < 11$ et $b^2 \equiv 4 \ [11]$.

4. **a.** En déduire que $x(x+13) \equiv 3 \ [33]$ équivaut aux quatre systèmes suivants :

$$\begin{cases} x \equiv 2 \ [3] \\ x \equiv 8 \ [11] \end{cases} \text{ ou } \begin{cases} x \equiv 0 \ [3] \\ x \equiv 1 \ [11] \end{cases} \text{ ou } \begin{cases} x \equiv 2 \ [3] \\ x \equiv 1 \ [11] \end{cases} \text{ ou } \begin{cases} x \equiv 0 \ [3] \\ x \equiv 8 \ [11] \end{cases}.$$

b. On admet que chacun de ces systèmes admet une unique solution entière x telle que $0 \leqslant x < 33$. Déterminer, sans justification, chacune de ces solutions.

5. Compléter l'algorithme en **Annexe** pour qu'il affiche les quatre solutions trouvées dans la question précédente.

6. Alice peut-elle connaître la première lettre du message envoyé par Bob ? Le « chiffre de RABIN » est-il utilisable pour décoder un message lettre par lettre ?

ANNEXE

À COMPLÉTER ET À REMETTRE AVEC LA COPIE

EXERCICE 4 (spécialité)

```
Pour …… allant de …… à ……
    Si le reste de la division de …… par …… est égal à …… alors
        Afficher ...……
    Fin Si
Fin Pour
```

EXERCICE 4

[Inde, Pondichéry 2018]

Partie A: Cryptage

1. Montrons que Bob code la lettre " N " avec le nombre 8:

La lettre N est associée au nombre entier: $x = 13$.

Le codage de la lettre N est représenté par le nombre y tel que:

$$y \equiv x\,(x + B)\,[n]$$

$$\iff y \equiv 13\,(13 + 13)\,[33], \text{ car: } n = 33 \text{ et } B = 13$$

$$\iff y \equiv 5 \times 33 + 8\,[33]$$

$$\iff y \equiv 8\,[33].$$

Au total: Bob code bien la lettre " N " avec le nombre 8.

2. Déterminons le nombre qui code la lettre " O ":

La lettre O est associée au nombre entier: $x = 14$.

Le codage de la lettre O est représenté par le nombre y tel que:

$$y \equiv x\,(x + 13)\,[n]$$

$$\iff y \equiv 14\,(14 + 13)\,[33]$$

$$\iff y \equiv 11 \times 33 + 15\,[33]$$

$$\iff y \equiv 15\,[33].$$

Au total: Le nombre qui code la lettre " O " est 15.

Partie B: Décryptage

1. Montrons que $x(x+13) \equiv 3\ [33]$ équivaut à $(x+23)^2 \equiv 4\ [33]$:

$$x(x+13) \equiv 3\ [33] \iff x^2 + 13x \equiv 3\ [33]$$

$$\iff x^2 + 13x + 33x \equiv 3\ [33]$$

$$\iff x^2 + 13x + 33x + (23)^2 \equiv 3 + (23)^2\ [33]$$

$$\iff x^2 + 46x + (23)^2 \equiv 3 + (16 \times 33 + 1)\ [33]$$

$$\iff (x+23)^2 \equiv 4\ [33].$$

Au total, nous avons bien: $x(x+13) \equiv 3\ [33] \iff (x+23)^2 \equiv 4\ [33]$.

2. a. Montrons l'implication demandée:

Ici, il s'agit de montrer que: $(x+23)^2 \equiv 4\ [33] \Rightarrow \begin{cases} (x+23)^2 \equiv 4\ [3] \\ (x+23)^2 \equiv 4\ [11] \end{cases}$.

$$(x+23)^2 \equiv 4\ [33] \Rightarrow (x+23)^2 - 4 \equiv 0\ [33]$$

$$\Rightarrow (x+23)^2 - 4 \equiv 0\ [3 \times 11]$$

$$\Rightarrow \begin{cases} (x+23)^2 - 4 \equiv 0\ [3] & (3 \text{ divise } (x+23)^2 - 4) \\ (x+23)^2 - 4 \equiv 0\ [11] & (11 \text{ divise } (x+23)^2 - 4) \end{cases}$$

$$\Rightarrow \begin{cases} (x+23)^2 \equiv 4\ [3] \\ (x+23)^2 \equiv 4\ [11] \end{cases}.$$

Au total, l'implication demandée est bien vérifiée.

2. b. Montrons la réciproque:

Ici, il s'agit de montrer que: $\begin{cases} (x+23)^2 \equiv 4\ [3] \\ (x+23)^2 \equiv 4\ [11] \end{cases} \Rightarrow (x+23)^2 \equiv 4\ [33]$.

$$\begin{cases} (x+23)^2 \equiv 4\ [3] \\ (x+23)^2 \equiv 4\ [11] \end{cases} \Rightarrow \begin{cases} (x+23)^2 - 4 \equiv 0\ [3] \\ (x+23)^2 - 4 \equiv 0\ [11] \end{cases}$$

$$\Rightarrow \begin{cases} 3 \text{ divise } (x+23)^2 - 4 \\ 11 \text{ divise } (x+23)^2 - 4 \end{cases}$$

$$\Rightarrow \begin{cases} \text{il existe un entier relatif " } \mathbf{a} \text{ " avec: } \mathbf{(x+23)^2 - 4 = 3 \times a} \\ \text{il existe un entier relatif " } \mathbf{b} \text{ " avec: } \mathbf{(x+23)^2 - 4 = 11 \times b} \end{cases}.$$

Dans ces conditions, nous pouvons écrire: $3 \times a = 11 \times b$.

Donc 3 divise $11 \times b$.

Or, 3 et 11 sont premiers entre eux et par conséquent, d'après le **théorème de GAUSS**: 3 divise b.

D'où, il existe un entier relatif " **c** " tel que: $b = 3 \times c$.

Ainsi: $(x+23)^2 - 4 = 11 \times b$

$= 11 \times (3 \times c)$

$= 33 \times c$.

Et donc: $(x+23)^2 - 4 \equiv 0\ [33] \Rightarrow (x+23)^2 \equiv 4\ [33]$.

Au total, la réciproque est bien vérifiée.

2. c. Déduisons-en l'équivalence demandée:

D'après les réponses aux questions **Partie B, 2. a.** et **2. b.**, nous pouvons affirmer que:

$$(x+23)^2 \equiv 4\ [33] \iff \begin{cases} (x+23)^2 \equiv 4\ [3] \\ (x+23)^2 \equiv 4\ [11] \end{cases}.$$

De plus, d'après la réponse à la question **Partie B, 1.**:

$$(x+23)^2 \equiv 4\ [33] \iff x(x+13) \equiv 3\ [33].$$

D'où, au total, nous pouvons écrire:

$$x(x+13) \equiv 3\ [33] \iff \begin{cases} (x+23)^2 \equiv 4\ [3] \\ (x+23)^2 \equiv 4\ [11] \end{cases}$$

$$\iff \begin{cases} (x+23)^2 \equiv 1\ [3] \\ (x+23)^2 \equiv 4\ [11] \end{cases}.$$

3. a. Déterminons les nombres entiers naturels a tels que $0 \leqslant a < 3$ et $a^2 \equiv 1\ [3]$:

Distinguons 3 cas:

- Si $a = 0$, $a^2 = 0$ et par conséquent: $a^2 \equiv 0\ [3]$.
- Si $a = 1$, $a^2 = 1$ et par conséquent: $a^2 \equiv 1\ [3]$.
- Si $a = 2$, $a^2 = 4 = 3 + 1$ et par conséquent: $a^2 \equiv 1\ [3]$.

Au total, les nombres entiers naturels " a " demandés sont: $a = 1$ et $a = 2$.

3. b. Déterminons les nombres entiers naturels b tels que $0 \leqslant b < 11$ et $b^2 \equiv 4\ [11]$:

Distinguons 11 cas:

- Si $b = 0$, $b^2 = 0$ et par conséquent: $b^2 \equiv 0\ [11]$.
- Si $b = 1$, $b^2 = 1$ et par conséquent: $b^2 \equiv 1\ [11]$.
- Si $b = 2$, $b^2 = 4$ et par conséquent: $b^2 \equiv 4\ [11]$.
- Si $b = 3$, $b^2 = 9$ et par conséquent: $b^2 \equiv 9\ [11]$.
- Si $b = 4$, $b^2 = 16$ et par conséquent: $b^2 \equiv 5\ [11]$.
- Si $b = 5$, $b^2 = 25$ et par conséquent: $b^2 \equiv 3\ [11]$.
- Si $b = 6$, $b^2 = 36$ et par conséquent: $b^2 \equiv 3\ [11]$.
- Si $b = 7$, $b^2 = 49$ et par conséquent: $b^2 \equiv 5\ [11]$.
- Si $b = 8$, $b^2 = 64$ et par conséquent: $b^2 \equiv 9\ [11]$.
- Si $b = 9$, $b^2 = 81$ et par conséquent: $b^2 \equiv 4\ [11]$.
- Si $b = 10$, $b^2 = 100$ et par conséquent: $b^2 \equiv 1\ [11]$.

Au total, les nombres entiers naturels " b " demandés sont: $b = 2$ et $b = 9$.

4. a. Déduisons-en les 4 équivalences demandées:

Nous savons que: $x\,(x + 13) \equiv 3\ [33] \iff \begin{cases} (x + 23)^2 \equiv 1\ [3] \\ (x + 23)^2 \equiv 4\ [11] \end{cases}$.

Soit $(x + 23)^2 \equiv 1\ [3]$, d'après Partie B, 3. a., nous avons:

• $(x+23)^2 \equiv 1\,[3] \iff a^2 \equiv 1\,[3]$

$$\iff \begin{cases} a \equiv 1\,[3] \\ a \equiv 4\,[3] \end{cases}$$

$$\iff \begin{cases} x+23 \equiv 1\,[3] \\ x+23 \equiv 2\,[3] \end{cases}$$

$$\iff \begin{cases} x \equiv -22\,[3] \\ x \equiv -21\,[3] \end{cases}$$

$$\iff \begin{cases} x \equiv 2\,[3] \\ x \equiv 0\,[3] \end{cases}.$$

Soit $(x+23)^2 \equiv 4\,[11]$, d'après Partie B, 3. b., nous avons:

• $(x+23)^2 \equiv 4\,[11] \iff b^2 \equiv 4\,[11]$

$$\iff \begin{cases} b \equiv 2\,[11] \\ b \equiv 9\,[11] \end{cases}$$

$$\iff \begin{cases} x+23 \equiv 2\,[11] \\ x+23 \equiv 9\,[11] \end{cases}$$

$$\iff \begin{cases} x \equiv -21\,[11] \\ x \equiv -14\,[11] \end{cases}$$

$$\iff \begin{cases} x \equiv 1\,[11] \\ x \equiv 8\,[11] \end{cases}.$$

Au total, nous avons bien:

$$\begin{cases} x \equiv 2\,[3] \\ x \equiv 8\,[11] \end{cases} \text{ ou } \begin{cases} x \equiv 0\,[3] \\ x \equiv 1\,[11] \end{cases} \text{ ou } \begin{cases} x \equiv 2\,[3] \\ x \equiv 1\,[11] \end{cases} \text{ ou } \begin{cases} x \equiv 0\,[3] \\ x \equiv 8\,[11] \end{cases}.$$

(1) (2) (3) (4)

4. b. Déterminons chacune de ces solutions:

4. b. b1. La solution du système (1):

La solution du système (1) est: $x = 8$. $\begin{pmatrix} 8 = 2 \times 3 + 2 \\ 8 = 0 \times 11 + 8 \end{pmatrix}$

4. b. b2. La solution du système (2):

La solution du système (2) est: $x = 12$. $\begin{pmatrix} 12 = 4 \times 3 + 0 \\ 12 = 1 \times 11 + 1 \end{pmatrix}$

4. b. b3. La solution du système (3):

La solution du système (3) est: $x = 23$. $\begin{pmatrix} 23 = 7 \times 3 + 2 \\ 23 = 2 \times 11 + 1 \end{pmatrix}$

4. b. b4. La solution du système (4):

La solution du système (4) est: $x = 30$. $\begin{pmatrix} 30 = 10 \times 3 + 0 \\ 30 = 2 \times 11 + 8 \end{pmatrix}$

5. Recopions et complétons l'algorithme:

L'algorithme recopié et complété est le suivant:

```
Pour x allant de 0 à 32
    Si le reste de la division de x(x + 13) par 33 est égal à 3 alors
        Afficher x
    Fin Si
Fin Pour
```

6. a. Alice peut-elle connaître la première lettre du message envoyé par Bob ?

Non ! car l'équation $x(x+13) \equiv 3\ [33]$ admet plusieurs solutions, d'après **Partie B, 4.**

Donc, il n'y a pas unicité de la première lettre.

6. b. Le " chiffre de RABIN " est-il utilisable pour décoder un message lettre par lettre ?

Dans ces conditions: **non**, le " chiffre de RABIN " n'est pas utilisable pour décoder un message lettre par lettre.