

www.freemaths.fr

Maths Expertes Terminale

Arithmétique



ÉNONCÉ DE L'EXERCICE

ARITHMÉTIQUE

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 $0 \leq B \leq n-1$.

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 :

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

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 :

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

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 $0 \leq a < 3$ et $a^2 \equiv 1 [3]$.

b. Déterminer les nombres entiers naturels b tels que $0 \leq b < 11$ 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 $0 \leq x < 33$. 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

Pour allant de à

Si le reste de la division de par est égal à alors

Afficher

Fin Si

Fin Pour