Exercice 4 Candidats ayant suivi l'endeignement de spécialité 5 points

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

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

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
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 Michaël 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 $n=p\times q$ 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 :

$$y\equiv x(x+B) \quad (n) \quad \text{avec} \quad 0 \leqslant y \leqslant n-1$$

Dans tout l'exercice on prend $p=3$ et $q=11$ 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 :

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

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

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

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

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

3.a. Déterminer les nombres entiers naturels a tels que $0 \leqslant a < 1$ et $a^2\equiv 1 \quad (11)$

3.b. Déterminer les nombres entiers naturels b tels que $0 \leqslant b < 11$ et $b^2\equiv 4 \quad (11)$

Copyright ® meilleurenmaths.com. Tous droits réservés

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

$\begin{cases} x\equiv 2\ (3) \\ x\equiv 8\ (11) \end{cases}$ ou $\begin{cases} x\equiv 0\ (3) \\ x\equiv 1\ (11) \end{cases}$ ou $\begin{cases} x\equiv 2\ (3) \\ x\equiv 1\ (11) \end{cases}$ ou $\begin{cases} x\equiv 0\ (3) \\ x\equiv 8\ (11) \end{cases}$

4.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 envoyer 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

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

Copyright ® meilleurenmaths.com. Tous droits réservés

CORRECTION

Partie A : cryptage

1. Pour la lettre N le nombre associé est 13 donc x = 13.
$x(x+B)=x(x+13)=13\times(13+13)=13\times26=338$
$338=33\times10+8$
$338\equiv8\ \ (33)$ y = 8.
La lettre N est codée avec le nombre **8.**

2. Pour la lettre O le nombre associé est 14 donc x = 14.
$x(x+13)=14\times(14+13)=14\times27=378$
$378=33\times11+15$
$378\equiv15\ \ (33)$ y = 15
La lettre O est codée avec le nombre **15.**

Partie B : décryptage

1. $(x+23)^2=x^2+46x+529$
$529=33\times16+1$ $46=33\times1+13$
donc
$(x+23)^2\equiv x^2+13x+1\ \ (33)$
$(x+23)^2\equiv x(x+13)+1\ \ (33)$
$(x+23)^2\equiv4\ \ (33)\ \Leftrightarrow\ x(x+13)+1\equiv4\ \ (33)\ \Leftrightarrow\ x(x+13)\equiv3\ \ (33)$

2.a. si $(x+23)^2\equiv4\ \ (33)$ alors il existe un entier relatif k tel que $(x+23)^2=33k+4$.
$33k+4=3\times(11k)+4=11\times(3k)+4$ donc il existe un entier relatif $k'=11k$ tel que $(x+23)^2=3k'+4$
et $(x+23)^2\equiv4\ \ (3)$; il existe aussi un entier relatif $k''=3k$ tel que $(x+23)^2=11k''+4$
et $(x+23)^2\equiv4\ \ (11)$
Conclusion
Si $(x+23)^2\equiv4\ \ (33)$ alors le système $\begin{cases}(x+23)^2\equiv4\ \ (3)\\(x+23)^2\equiv4\ \ (11)\end{cases}$ est vérifié.

2.b. Si $(x+23)^2\equiv4\ \ (3)$ **et** $(x+23)^2\equiv4\ \ (11)$ alors il existe deux entiers relatifs K et K' tels que $(x+23)^2=4+3K=4+11K'$ donc $3K=11K'$.
3 et 11 sont premiers entre eux, le théorème de Gauss nous permet d'affirmer qu'il existe des entiers h et h' tels que $K=11h$ et $K'=3h'$ et $3K=33h=11K'=33h'$ on obtient $h=h'$.
$(x+23)^2=4+33h$ et $(x+23)^2\equiv4\ \ (33)$
Conclusion
Si $\begin{cases}(x+23)^2\equiv4\ \ (3)\\(x+23)^2\equiv4\ \ (11)\end{cases}$ alors $(x+23)^2\equiv4\ \ (33)$

2.c. En utilisant les résultats précédents et en remarquant $4\equiv1\ \ (3)$ on obtient :
$x(x+13)\equiv3\ \ (33)\ \Leftrightarrow\ \begin{cases}(x+23)^2\equiv1\ \ (3)\\(x+23)^2\equiv4\ \ (11)\end{cases}$

3.a. On donne les résultats sous forme de tableau.

a	0	1	2
a^2	0	1	4
Congruences modulo 3	0	1	1

Copyright ® meilleurenmaths.com. Tous droits réservés

Conclusion

Les entiers naturels a = 1 et a = 2 sont les solutions.

3.b. On donne les résultats sous forme de tableau.

b	0	1	2	3	4	5	6	7	8	9	10
b^2	0	1	4	9	16	25	36	49	64	81	100
Congruences modulo 11	0	1	4	9	5	3	3	5	9	4	1

Conclusion

Les entiers naturels b = 2 et b = 9 sont les solutions.

4.a. Pour $(x+23)^2 \equiv 1 \ (3)$

$a^2 \equiv 1 \ (3) \Leftrightarrow (a=1 \text{ ou } a=2)$

donc

$x+23 \equiv 1 \ (3)$ ou $x+23 \equiv 2 \ (3)$

$23 = 3\times 7+2 \quad 23 \equiv 2 \ (3)$

$x+23 \equiv 1 \ (3) \Leftrightarrow x+2 \equiv 1 \ (3) \Leftrightarrow x \equiv -1 \ (3) \Leftrightarrow x \equiv 2 \ (3)$ (car $-1 = 3\times(-1)+2$)

$x+23 \equiv 2 \ (3) \Leftrightarrow x+2 \equiv 2 \ (3) \Leftrightarrow x \equiv 0 \ (3)$

. Pour $(x+23)^2 \equiv 4 \ (11)$

$b^2 \equiv 4 \ (11) \Leftrightarrow (b=2 \text{ ou } b=9)$

donc

$x+23 \equiv 2 \ (11)$ ou $x+23 \equiv 9 \ (11)$

$23 = 11\times 2+1 \quad 23 \equiv 1 \ (11)$

$x+23 \equiv 2 \ (11) \Leftrightarrow x+1 \equiv 2 \ (11) \Leftrightarrow x \equiv 1 \ (11)$

$x+23 \equiv 9 \ (11) \Leftrightarrow x+1 \equiv 9 \ (11) \Leftrightarrow x \equiv 8 \ (11)$

. Le système proposé équivaut aux quatre systèmes suivants :

$\begin{cases} x \equiv 2 \ (3) \\ x \equiv 8 \ (11) \end{cases}$ ou $\begin{cases} x \equiv 0 \ (3) \\ x \equiv 1 \ (11) \end{cases}$ ou $\begin{cases} x \equiv 2 \ (3) \\ x \equiv 1 \ (11) \end{cases}$ ou $\begin{cases} x \equiv 0 \ (3) \\ x \equiv 8 \ (11) \end{cases}$

4.b. Pour le premier système on obtient : **8**

Pour le deuxième système on obtient : **12**

Pour le troisième système on obtient: **23**

Pour le quatrième système on obtient : **30**

5. Algorithme

Pour **x** allant de **0** à **32**

  Si le reste de la division de **x(x+13)** est égal à **3** alors

    Afficher **x**

  Fin Si

Fin Pour

Complément (non demandé)

En utilisant le logiciel Python, on obtient :

Programme

```
print('Début de programme')
for x in range(33):
    y=x*(x+13)
    z=y%33              # z est le reste de la division de y par 33
    if z==3:            # si ce reste est égal à 3 alors x est une solution
        print(x)
print('Fin de programme')
```

Copyright ® meilleurenmaths.com. Tous droits réservés

Exécution du programme

```
Début de programme
8
12
23
30
Fin de programme
```

6. Il y a 3 solutions strictement inférieures à 26 donc il y a 3 lettres possibles : I ; M et X.
Alice ne peut pas connaître de manière précise la première lettre du message envoyé par Bob.
Pour le choix des nombres premiers (pour la méthode du « chiffre de RABIN » il faut des nombres premiers grands), il n'est pas utilisable pour décoder un message lettre par lettre.
Lorsque n est très grand, la probabilité d'obtenir plusieurs solutions inférieures à 26 est faible.

Remarque
Dans le cours de seconde, partie ALGORITHMIQUE, les TP permettent de définir les premières instructions du logiciel Python.

Copyright ® meilleurenmaths.com. Tous droits réservés