TS spé Sujets de baccalauréat mai 2018

eee

Il est demandé de ne rien écrire sur l'énoncé.

I. La suite de Fibonacci (Liban 29 mai 2018)

On considère la suite (a_n) définie sur $\mathbb{N}$ par ses deux premiers termes $a_0 = 0$ et $a_1 = 1$ ainsi que par la relation de récurrence $a_{n+2} = a_{n+1} + a_n$ pour tout entier naturel *n*.

On admet que a_n est un entier naturel. pour tout entier naturel *n*,

On admet que la suite (a_n) est une suite croissante d'entiers naturels.

1°) Recopier et compléter l'algorithme ci-dessous pour qu'à la fin de son exécution la variable A contienne le terme a_n. On précise que *n* est un entier naturel supérieur ou égal à 1.

Entrée :
Saisir *n*

Initialisations :
A prend la valeur 0
B prend la valeur 1

Traitement :
Pour *i* allant de 1 à *n* **Faire**
  C prend la valeur $A + B$
  A prend la valeur ….
  B prend la valeur ….
FinPour

Sortie :
Afficher A

2°) Recopier et compléter le tableau :

n	0	1	2	3	4	5	6	7	8	9	10
a_n											

3°) On considère la matrice $A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$.

Calculer A^2, A^3, A^4, A^5.

4°) On peut démontrer, et nous admettrons, que pour tout entier naturel $n \geqslant 1$, $A^n = \begin{pmatrix} a_{n+1} & a_n \\ a_n & a_{n-1} \end{pmatrix}$.

a) Soit *p* et *q* deux entiers naturels supérieurs ou égaux à 1. Calculer le produit $A^p \times A^q$ et en déduire que $a_{p+q} = a_p \times a_{q+1} + a_{p-1} \times a_q$.

b) En déduire que si un entier *r* divise les entiers a_p et a_q, alors *r* divise également a_{p+q}.

c) Soit *p* un entier naturel supérieur ou égal à 1.
Démontrer, en utilisant un raisonnement par récurrence sur *n*, que pour tout entier naturel *n*, a_p divise a_{np}.

5°) a) Soit n un entier naturel supérieur ou égal à 5.
Démontrer que si n est un entier naturel qui n'est pas premier, alors a_n n'est pas un nombre premier.
b) Calculer a_{19}. Que penser de la réciproque de la propriété obtenue dans la question précédente ?

On peut aussi utiliser le sujet de la Nouvelle_Caledonie_27_nov_2018

$u_{2n+2} = u_{n+2} \times u_{n+1} + u_{n+1} \times u_n$
En déduire que $u_{2n+2} = (u_{n+2})^2 - (u_n)^2$

II. Chiffre de Rabin (Pondichéry mai 2018)

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 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 $0 \leqslant \mathrm{B} \leqslant n-1$.

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

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

1°) Coder le mot « NO ».

2°) « Décoder » la lettre D. Le « chiffre de Rabin » est-il utilisable pour décoder un message lettre par lettre ?

Corrigé des exercices

I. La suite de Fibonacci

On considère la suite (a_n) définie sur $\mathbb{N}$ par ses deux premiers termes $a_0 = 0$ et $a_1 = 1$ ainsi que par la relation de récurrence $a_{n+2} = a_{n+1} + a_n$ pour tout entier naturel *n*.
On admet que pour tout entier naturel *n*, a_n est un entier naturel.

1°) Recopier et compléter l'algorithme ci-dessous pour qu'à la fin de son exécution la variable A contienne le terme a_n. On précise que *n* est un entier naturel supérieur ou égal à 1.

Entrée :
Saisir *n*

Initialisations :
A prend la valeur 0
B prend la valeur 1

Traitement :
Pour *i* allant de 1 à *n* **Faire**
    C prend la valeur $A + B$
    A prend la valeur B
    B prend la valeur C
FinPour

Sortie :
Afficher A

2°) Recopier et compléter le tableau :

n	0	1	2	3	4	5	6	7	8	9	10
a_n	0	1	1	2	3	5	8	13	21	34	55

3°) On considère la matrice $A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$.

Calculer A^2, A^3, A^4, A^5.

$A^2 = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$ $\quad A^3 = \begin{pmatrix} 3 & 2 \\ 2 & 1 \end{pmatrix}$ $\quad A^4 = \begin{pmatrix} 5 & 3 \\ 3 & 2 \end{pmatrix}$ $\quad A^5 = \begin{pmatrix} 8 & 5 \\ 5 & 3 \end{pmatrix}$

4°) On peut démontrer, et nous admettrons, que pour tout entier naturel $n \geqslant 1$, $\mathrm{A}^n = \begin{pmatrix} a_{n+1} & a_n \\ a_n & a_{n-1} \end{pmatrix}$.

On peut démontrer ce résultat grâce à une récurrence d'ordre 2.

a) Soit *p* et *q* deux entiers naturels supérieurs ou égaux à 1. Calculer le produit $\mathrm{A}^p \times \mathrm{A}^q$ et en déduire que $a_{p+q} = a_p \times a_{q+1} + a_{p-1} \times a_q$.

$\mathrm{A}^p = \begin{pmatrix} a_{p+1} & a_p \\ a_p & a_{p-1} \end{pmatrix}$ $\qquad$ $\mathrm{A}^q = \begin{pmatrix} a_{q+1} & a_q \\ a_q & a_{q-1} \end{pmatrix}$

$$\mathrm{A}^p \times \mathrm{A}^q = \begin{pmatrix} a_{p+1} \times a_{q+1} + a_p \times a_q & a_{p+1} \times a_q + a_p \times a_{q-1} \\ a_p \times a_{q+1} + a_{p-1} \times a_q & a_p \times a_q + a_{p-1} \times a_{q-1} \end{pmatrix}$$

On a : $\mathrm{A}^p \times \mathrm{A}^q = \mathrm{A}^{p+q}$ (propriété des puissances de matrices).

$$\mathrm{A}^p \times \mathrm{A}^q = \begin{pmatrix} a_{p+q+1} & a_{p+q} \\ a_{p+q} & a_{p+q-1} \end{pmatrix}$$

On procède par identification des coefficients.

On identifie le coefficient situé sur la 2e ligne et la 1ère colonne.

b) En déduire que si un entier *r* divise les entiers a_p et a_q, alors *r* divise également a_{p+q}.

On a : $a_{p+q} = a_p \times a_{q+1} + a_{p-1} \times a_q$.

Si un entier *r* divise a_p et a_q, alors *r* divise toute combinaison linéaire de a_p et a_q à coefficients entiers relatifs.

Or $a_p \times a_{q+1} + a_{p-1} \times a_q$ est une combinaison linéaire de a_p et a_q à coefficients entiers relatifs.

c) Soit *p* un entier naturel supérieur ou égal à 1.
Démontrer, en utilisant un raisonnement par récurrence sur *n*, que pour tout entier naturel $n \geqslant 1$, a_p divise a_{np}.

On va utiliser le résultat de la question précédente.

Pour tout $n \in \mathbb{N}$, on définit la phrase $\mathscr{P}(n)$: « a_p divise a_{np} ».

Vérifions que $\mathscr{P}(0)$ est vraie.

$a_{0p} = a_0 = 0$

0 est divisible par n'importe quel entier donc $\mathscr{P}(0)$ est vraie.

Considérons un entier naturel k tel que la phrase $\mathscr{P}(k)$ soit vraie c'est-à-dire a_p divise a_{kp}.
Démontrons qu'alors la phrase $\mathscr{P}(k+1)$ est vraie c'est-à-dire a_p divise $a_{(k+1)p}$.

On observe tout d'abord que $a_{(k+1)p} = a_{kp+p}$.

a_p divise a_{kp} et a_p divise a_p donc d'après la formule établie à la question précédente a_p divise $a_{(k+1)p}$.

Donc la phrase $\mathscr{P}(k+1)$ est vraie.

On en déduit que la phrase $\mathscr{P}(n)$ est vraie pour tout entier naturel n.

5°) a) Soit n un entier naturel supérieur ou égal à 5.
Démontrer que si n est un entier naturel qui n'est pas premier, alors a_n n'est pas un nombre premier.

Démontrer que si an est premier, alors n est premier. Indication : contraposée

b) Calculer a_{19}. Que penser de la réciproque de la propriété obtenue dans la question précédente ?

Pour déterminer la valeur de a_{19}, on peut par exemple calculer A^{19}.

$a_{19} = 4181$

a_{19} est divisible par 37.

On constate que a_{19} n'est pas premier donc la réciproque est fausse.

On peut rajouter la question suivante :

$\det\left(\mathrm{A}^n\right) = (-1)^n$
Démontrer que $a_{n+1} \times a_{n-1} - a_n{}^2 = (-1)^n$.

II. Chiffre de Rabin (Pondichéry mai 2018)

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 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 $0 \leqslant \mathrm{B} \leqslant n-1$.

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

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

ee

$p = 3$
$q = 11$
$n = 33$
$\mathrm{B} = 13$
$y \equiv x(x+13)$ [33] avec $0 \leqslant y \leqslant n$.

1°) Coder le mot « NO ».

« IP »

2°) « Décoder » la lettre D. Le « chiffre de Rabin » est-il utilisable pour décoder un message lettre par lettre ?

La lettre D correspond au nombre 3.

On cherche donc le(s) entiers naturel(s) x tels que $0 \leqslant x \leqslant 25$ et $x(x+13) \equiv 3$ (mod. 33).

Je conseille : on tape Y1=reste(X(X+13),33)
On obtient la table.

On cherche dans la table les valeurs qui donnent 3.

On obtient : 8, 12, 23.

1 A ← 0
2 B ← 1
3 Pour i allant de 2 à n :
4 C ← A + B
5 A ← ...

6 B ← ...
7 Fin Pour

EXERCICE 4 : (5 points) ***Candidats AYANT SUIVI l'enseignement de spécialité mathématiques***

On considère la suite (u_n) définie par $u_0 = 3$, $u_1 = 8$ et, pour tout n supérieur ou égal à 0 :

$$u_{n+2} = 5u_{n+1} - 6u_n .$$

1. Calculer u_2 et u_3.
2. Pour tout entier naturel $n \geq 2$, on souhaite calculer u_n à l'aide de l'algorithme suivant :

Variables : a, b et c sont des nombres réels
i et n sont des nombres entiers naturels supérieurs ou égaux à 2
Initialisation : a prend la valeur 3
b prend la valeur 8
Traitement : Saisir n
Pour i variant de 2 à n faire
  c prend la valeur a
  a prend la valeur b
  b prend la valeur .....
Fin Pour
Sortie : Afficher b

a. Recopier la ligne de cet algorithme comportant des pointillés et les compléter.

On obtient avec cet algorithme le tableau de valeurs suivant :

n	7	8	9	10	11	12	13	14	15
u_n	4502	13378	39878	119122	356342	1066978	3196838	9582322	28730582

Exercice :

Cet exercice met en œuvre sur de petits nombres le premier système de cryptage asymétrique. Dans ce système, une personne destinataire qui veut recevoir des informations confidentielles publie une clé permettant à quiconque de lui envoyer des messages sous forme cryptée. Cependant, seule la personne destinataire peut décrypter les messages à l'aide d'une autre clé connue d'elle seule.

Partie A - Détermination de la clé publique servant au cryptage

1°) Dans tout l'exercice, on choisit deux nombres premiers entre eux : $p = 78$ et $q = 95$.
Justifier que les entiers p et q sont premiers entre eux.

2°) La personne destinataire choisit 5 entiers $b_1 = 45$, $b_2 = 22$, $b_3 = 13$, $b_4 = 4$, $b_5 = 2$.
La clé de cryptage est formée des 5 nombres entiers $(a_1,\ a_2,\ a_3,\ a_4,\ a_5)$ ainsi calculés :
pour tout $i \in \{1,\ 2,\ 3,\ 4,\ 5\}$, $0 \leqslant a_i \leqslant 77$ et $b_i \times q \equiv a_i$ (mod. p).
Exemple : Pour le calcul de a_1, on calcule $b_1 \times q = 45 \times 95 = 4275$.
Or $4275 \equiv 63$ (mod. p), et 63 est bien compris entre 0 et 77. Donc $a_1 = 63$.
Calculer les 4 autres entiers de la clef.

Partie B - Cryptage d'un message

Cette clé, publiée par la personne destinataire, permet à quiconque de lui envoyer un message crypté.
Cette partie va expliquer comment on crypte le message.
On associe d'abord à chaque lettre son rang dans l'alphabet, selon la correspondance suivante :

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Pour crypter une lettre :
- on détermine son rang à l'aide du tableau de correspondance précédent ;
- on écrit ce nombre en base 2 sur 5 bits ; on ainsi obtient 5 chiffres $(m_1,\ m_2,\ m_3,\ m_4,\ m_5)$, chaque chiffre étant égal à 0 ou à 1 ;
- on détermine alors la valeur cryptée, égale à la somme $\sigma = a_1m_1 + a_2m_2 + a_3m_3 + a_4m_4 + a_5m_5$.

On remarque qu'une lettre est ainsi cryptée par un nombre entier.

• On veut crypter la lettre « I ».

- Le rang de I est 9 (en base dix) ;
- on écrit ce nombre en base deux sur 5 bits : $\overline{9}^{(10)} = 8 + 1 = \overline{01001}^{(2)}$;
- on calcule la somme $\sigma = 0 \times a_1 + 1 \times a_2 + 0 \times a_3 + 0 \times a_4 + 1 \times a_5 = \ldots$ (écrire le calcul correspondant).

Par quel entier la lettre « I » est-elle cryptée ?

• Crypter la lettre « W ».

Réponses :

Partie A

1°)

2°)

$a_1 = 63$
$b_2 \times q \equiv 62$ (mod. 78) donc $a_2 = 62$
$b_3 \times q \equiv 65$ (mod. 78) donc $a_3 = 65$
$b_4 \times q \equiv 68$ (mod. 78) donc $a_4 = 68$
$b_5 \times q \equiv 34$ (mod. 78) donc $a_5 = 34$

$a_2 = 62$, $a_3 = 65$, $a_4 = 68$ et $a_5 = 34$.
La clé de cryptage est donc $(a_1, a_2, a_3, a_4, a_5) = (63, 62, 65, 68, 34)$.

Partie B

La décomposition en base 2 sur 5 bits fait intervenir les puissances de 2 d'exposant entier naturel : 16 8 4 2 1.

$\sigma = 0 \times 63 + 1 \times 62 + 0 \times 65 + 0 \times 68 + 1 \times 34 = 96$

La lettre « I » est donc cryptée par l'entier 96.

Le rang de W est 23 et $23 = 16 + 4 + 2 + 1$.
23 s'écrit donc en base 2 sur 5 bits : 10111.
On calcule $\sigma = 1 \times 63 + 0 \times 62 + 1 \times 65 + 1 \times 68 + 1 \times 34 = 230$.
W est crypté par l'entier 230.

Source : Services informatiques aux organisations / épreuve obligatoire / 13 mai 2019Brevet de technicien supérieur Métropole A. P. M. E. P.

Méthode RSA ou Système RSA

Centres étrangers 11 juin 2018 Baccalauréat S

Le but de cet exercice est d'envisager une méthode de cryptage à clé publique d'une information numérique, appelée système RSA, en l'honneur des mathématiciens Ronald Rivest, Adi Shamir et Leonard Adleman, qui ont inventé cette méthode de cryptage en 1977 et l'ont publiée en 1978.
Les questions 1°) et 2°) sont des questions préparatoires, la question 3°) aborde le cryptage, la question 4°) le décryptage.

1°) Déterminer le reste de la division euclidienne de 8^{23} par 55.
Il est conseillé de travailler en congruences en utilisant de petites puissances de 8.

2°) Déterminer le plus petit entier naturel *d* tel que le reste de la division euclidienne de 23*d* par 40 soit égal à 1.

3°) **Cryptage dans le système RSA**
Une personne A choisit deux nombres premiers *p* et *q* distincts, puis calcule les produits $\mathrm{N} = pq$ et $n = (p-1)(q-1)$ (*n* est *l'indicateur d'Euler* de *n*).
Elle choisit également un entier naturel *c* premier avec *n*.
La personne A publie le couple $(\mathrm{N}\,;c)$, qui est une clé publique permettant à quiconque de lui envoyer un nombre crypté.
Les messages sont numérisés et transformés en une suite d'entiers naturels compris entre 0 et $\mathrm{N}-1$.
Pour crypter un entier *a* de cette suite, on procède ainsi : on calcule le reste *b* dans la division euclidienne par N du nombre a^c et le nombre crypté est l'entier *b*.
Dans la pratique, cette méthode est sûre si la personne A choisit des nombres premiers *p* et *q* très grands, s'écrivant avec plusieurs dizaines de chiffres.

On peut noter que les nombres *p* et *q* sont ensuite détruits.

On va l'envisager ici avec des nombres plus simples : $p = 5$ et $q = 11$.
La personne A choisit également $c = 23$.
a) Calculer les nombres N et *n*, puis justifier que la valeur de *c* vérifie la condition voulue.
b) Un émetteur souhaite envoyer à la personne A le nombre $a = 1$.
Déterminer la valeur du nombre crypté *b*.
c) Un émetteur souhaite envoyer à la personne A le nombre $a = 8$.
Déterminer la valeur du nombre crypté *b*.

4°) **Décryptage dans le système RSA**

La personne A calcule dans un premier temps l'unique entier naturel *d* vérifiant les conditions $0 \leqslant d < n$ et $cd \equiv 1$ (mod. *n*).
Elle garde secret ce nombre *d* qui lui permet, et à elle seule, de décrypter les nombres qui lui ont été envoyés cryptés avec sa clé publique.
Pour décrypter un nombre crypté *b*, la personne A calcule le reste *a* dans la division euclidienne par N du nombre b^d, et le nombre en clair – c'est-à-dire le nombre avant cryptage – est le nombre *a*.
On admet l'existence et l'unicité de l'entier *d*, et le fait que le décryptage fonctionne.
Les nombres choisis par A sont encore $p = 5$, $q = 11$ et $c = 23$.
a) Quelle est la valeur de *d* ?
b) En appliquant la règle de décryptage, retrouver le nombre en clair lorsque le nombre crypté est $b = 17$.
Ce résultat était-il prévisible ?
c) Déterminer le nombre en clair lorsque le nombre crypté est $b = 9$.

RSA est robuste, car il est très difficile de trouver *p* et *q* à partir de *n* (qui est public) : en effet les algorithmes de factorisation sont très lents (de l'ordre de milliers d'années pour des entiers aussi grands), jusqu'au jour où on en trouvera de plus rapides… qui feront s'effondrer RSA tel un château de cartes.
Conclusion : RSA sera un jour abandonné, vraisemblablement remplacé par un outil très prometteur en terme de robustesse : les courbes elliptiques (équations du type $y^2 = x^2 + ax + b$) : il semble que leur résistance soit vraiment démentielle (mais là, on entre dans le domaine terriblement complexe de la géométrie algébrique…).

Corrigé :

1°) Il y a plusieurs manières de faire.
La plus grande puissance de 8 calculable sur la calculatrice est 8^{11}.
Le reste de la division euclidienne de 8^{11} par 55 est 52.
On peut donc écrire $8^{11} \equiv -3$ (mod. 55) donc $8^{22} \equiv 9$ (mod. 55). On a alors $8^{22} \times 8 \equiv 9 \times 8$ (mod. 55) soit $8^{23} \equiv 72$ (mod. 55) soit $8^{23} \equiv 17$ (mod. 55).

2°) Il y a plusieurs méthodes de résolution.

1ère manière :
On utilise la calculatrice.
On rentre la fonction Y1 = reste(23X,40.
On trouve $d = 7$.

2e méthode :
On utilise une équation diophantienne.

3°)
p et *q* nombres premiers distincts
$\mathrm{N} = pq$
$n = (p-1)(q-1)$
c premier avec *n*.
clé=$(\mathrm{N}\,;c)$
$p = 5$
$q = 11$
$c = 23$

a) $\mathrm{N} = 55$
$n = 40$

a) 23 est un nombre premier. Comme 23 ne divise pas 40, 23 est premier avec 40.
Autrement dit, *c* et *n* sont premiers entre eux.

b) $a^c = 1$
b est le reste de la division euclidienne de 1 par 55.
Donc $b = 1$.

c) *b* est le reste de la division euclidienne de 8^{23} par 55.
On en déduit que $b = 17$.

4°)
a) $cd \equiv 1$ (mod. *n*) soit $23d \equiv 1$ (mod. 40).

D'après le résultat de la question 2°), on a $d = 7$.

b) En appliquant la règle de décryptage, retrouver le nombre en clair lorsque le nombre crypté est $b = 17$.
Ce résultat était-il prévisible ?

$b^d = 17^7$
On cherche le reste de la division euclidienne de 17^7 par 55.
Grâce à la commande de la calculatrice, on trouve 8.
Ainsi, $a = 8$.
Le résultat était prévisible.

c) On cherche le reste de la division euclidienne de 9^7 par 55.
Grâce à la commande de la calculatrice, on trouve 4.
Ainsi, $a = 4$.

Version originale :

1°) Déterminer le reste de la division euclidienne de 8^5 par 55.
En utilisant les congruences puis en déduire le reste de la division euclidienne. En déduire
À l'aide des congruences, déterminer le reste de la division euclidienne de 8^23 par 55.

Déterminer le reste de la division euclidienne de 8^20 par 55.
On pourra commencer par le reste de 8^5 par 55.

Déterminer les restes de la division euclidienne de 8^2 et de 8^7 par 55.
En déduire à l'aide des congruences le reste de la division euclidienne de 8^23 par 55.