TS1 spé

Contrôle du jeudi 21 février 2019 (1 heure)

Prénom et nom : ……

Note : ….. / 20

I. (15 points : 1°) 2 points ; 2°) 2 points + 2 points ; 3°) 3 points ; 4°) 2 points ; 5°) 2 points ; 6°) 2 points)

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 ne cherchera pas à l'exprimer en fonction de *n*.

Compléter le tableau suivant :

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

1°) On considère la matrice $\mathrm{A} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$.
Calculer A^2, A^3, A^4, A^5. On écrira quatre égalités sur une même ligne sans détailler les calculs.

2°) Le but de la question est de démontrer par récurrence que pour tout entier naturel $n \geqslant 1$, $\mathrm{A}^n = \begin{pmatrix} a_{n+1} & a_n \\ a_n & a_{n-1} \end{pmatrix}$.
Les étapes de la récurrence sont données. Il est demandé de compléter les passages manquants.

Pour $n \in \mathbb{N}^*$, on définit la phrase $\boldsymbol{P}\ (n)$: « $\mathrm{A}^n = \begin{pmatrix} a_{n+1} & a_n \\ a_n & a_{n-1} \end{pmatrix}$ ».

Vérifions que la phrase $\boldsymbol{P}\ (1)$ est vraie.

Considérons un entier naturel $k \geqslant 1$ tel que la phrase $\boldsymbol{P}\ (k)$ soit vraie, c'est-à-dire $\mathrm{A}^k = \begin{pmatrix} a_{k+1} & a_k \\ a_k & a_{k-1} \end{pmatrix}$.

Démontrons qu'alors la phrase $\boldsymbol{P}\ (k+1)$ est vraie, c'est-à-dire $\mathrm{A}^{k+1} = \begin{pmatrix} a_{k+2} & a_{k+1} \\ a_{k+1} & a_k \end{pmatrix}$.

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

On en déduit que la phrase $\boldsymbol{P}\ (n)$ est vraie pour tout entier naturel $n \geqslant 1$.

3°) Soit *p* et *q* deux entiers naturels supérieurs ou égaux à 1.
En considérant le produit $\mathrm{A}^p \times \mathrm{A}^q$, démontrer que $a_{p+q} = a_p \times a_{q+1} + a_{p-1} \times a_q$.

4°) On reprend les notations de la question 3°).
Étant donné un entier naturel r, on considère la phrase U : « r divise a_{p+q} » et la phrase V : « r divise a_p et a_q ».
Quel lien y a-t-il entre les phrases U et V ? Justifier avec précision.

……

……

……

……

……

……

……

……

5°) Soit n un entier naturel supérieur ou égal à 1.
Démontrer en utilisant la relation établie à la question 3°) que $a_{2n+2} = a_{n+2} \times a_{n+1} + a_{n+1} \times a_n$ et en déduire que $a_{2n+2} = (a_{n+2})^2 - (a_n)^2$.

……

……

……

……

……

……

……

……

6°) Cette question est indépendante des précédentes.
Compléter l'algorithme ci-contre 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

II. (5 points : 2 points + 3 points)

À toute lettre de l'alphabet on associe un entier naturel 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. Le couple $(p\,;q)$ 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 l'entier naturel x est l'entier y tel que $y \equiv x(x+B)\ [n]$ avec $0 \leqslant y < n$.

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

Coder le mot « NO » puis décoder la lettre D.

…….. (une seule réponse) ……..

Le « chiffre de Rabin » est-il utilisable pour décoder un message lettre par lettre ?

……

Corrigé du contrôle du 21-2-2019

I.

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 ne cherchera pas à l'exprimer en fonction de *n*.

Compléter le tableau suivant :

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

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

1°) On considère la matrice $\mathrm{A} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$.
Calculer A^2, A^3, A^4, A^5. On écrira quatre égalités sur une même ligne sans détailler les calculs.

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

2°) Le but de la question est de démontrer par récurrence que pour tout entier naturel $n \geqslant 1$, $\mathrm{A}^n = \begin{pmatrix} a_{n+1} & a_n \\ a_n & a_{n-1} \end{pmatrix}$.
Les étapes de la récurrence sont données. Il est demandé de compléter les passages manquants.

Pour $n \in \mathbb{N}^*$, on définit la phrase $\boldsymbol{P}\ (n)$: « $\mathrm{A}^n = \begin{pmatrix} a_{n+1} & a_n \\ a_n & a_{n-1} \end{pmatrix}$ ».

Vérifions que la phrase $\boldsymbol{P}\ (1)$ est vraie.

On a $\mathrm{A}^1 = \mathrm{A} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$. Or $a_0 = 0$, $a_1 = 1$ et $a_2 = 1$. Donc on peut écrire $\mathrm{A}^1 = \begin{pmatrix} a_2 & a_1 \\ a_1 & a_0 \end{pmatrix}$.
Ainsi, la phrase $\boldsymbol{P}\ (1)$ est vraie.

Considérons un entier naturel $k \geqslant 1$ tel que la phrase $\boldsymbol{P}\ (k)$ soit vraie, c'est-à-dire $\mathrm{A}^k = \begin{pmatrix} a_{k+1} & a_k \\ a_k & a_{k-1} \end{pmatrix}$.

Démontrons qu'alors la phrase $\boldsymbol{P}\ (k+1)$ est vraie, c'est-à-dire $\mathrm{A}^{k+1} = \begin{pmatrix} a_{k+2} & a_{k+1} \\ a_{k+1} & a_k \end{pmatrix}$.

$$\mathrm{A}^{k+1} = \mathrm{A}^k \times \mathrm{A}$$

$$= \begin{pmatrix} a_{k+1} & a_k \\ a_k & a_{k-1} \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} a_{k+1} + a_k & a_{k+1} \\ a_k + a_{k-1} & a_k \end{pmatrix}$$

$$= \begin{pmatrix} a_{k+2} & a_{k+1} \\ a_{k+1} & a_k \end{pmatrix}$$

Ainsi la phrase $\boldsymbol{P}\ (k+1)$ est vraie.

On en déduit que la phrase $\boldsymbol{P}\ (n)$ est vraie pour tout entier naturel $n \geqslant 1$.

3°) Soit *p* et *q* deux entiers naturels supérieurs ou égaux à 1.
En considérant le produit $\mathrm{A}^p \times \mathrm{A}^q$, démontrer que $a_{p+q} = a_p \times a_{q+1} + a_{p-1} \times a_q$.

On sait que $\mathrm{A}^p = \begin{pmatrix} a_{p+1} & a_p \\ a_p & a_{p-1} \end{pmatrix}$ et que $\mathrm{A}^q = \begin{pmatrix} a_{q+1} & a_q \\ a_q & a_{q-1} \end{pmatrix}$.

Par produit de ces deux matrices, on obtient $\mathrm{A}^p \times \mathrm{A}^q = \begin{pmatrix} a_{p+1} \times a_{q+1} + a_p \times a_q & a_{p+1} \times a_q + a_p \times a_{q-1} \\ a_p \times a_{q+1} + a_{p-1} \times a_q & a_p \times a_q + a_{p-1} \times a_{q-1} \end{pmatrix}$.

Par ailleurs, on peut écrire que $\mathrm{A}^p \times \mathrm{A}^q = \mathrm{A}^{p+q}$ (propriété des puissances de matrices).

Or $\mathrm{A}^{p+q} = \begin{pmatrix} a_{p+q+1} & a_{p+q} \\ a_{p+q} & a_{p+q-1} \end{pmatrix}$ puisque $p+q$ est un entier naturel supérieur ou égal à 1.

On procède alors par identification des coefficients.

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

On peut donc écrire $a_{p+q} = a_p \times a_{q+1} + a_{p-1} \times a_q$.

4°) On reprend les notations de la question 3°).
Étant donné un entier naturel *r*, on considère la phrase *U* : « *r* divise a_{p+q} » et la phrase *V* : « *r* divise a_p et a_q ».
Quel lien y a-t-il entre les phrases *U* et *V* ? Justifier avec précision.

La phrase *V* implique la phrase *U*.

En effet, l'égalité $a_{p+q} = a_p \times a_{q+1} + a_{p-1} \times a_q$ fait apparaître a_{p+q} comme combinaison linéaire de a_p et a_q à coefficients entiers.

Or si un entier *r* divise a_p et a_q, il divise toute combinaison linéaire de a_p et a_q à coefficients entiers.
Donc il divise a_{p+q}.

Il n'y a pas équivalence.

5°) Soit n un entier naturel supérieur ou égal à 1.
Démontrer en utilisant la relation établie à la question 3°) que $a_{2n+2} = a_{n+2} \times a_{n+1} + a_{n+1} \times a_n$ et en déduire que $a_{2n+2} = (a_{n+2})^2 - (a_n)^2$.

On applique la relation établie à la question 3°) avec les entiers $p = n$ et $q = n+1$.

On obtient $a_{2n+2} = a_{n+2} \times a_{n+1} + a_{n+1} \times a_n$.

$a_{2n+2} = a_{n+1}(a_{n+2} + a_n)$ (factorisation dans l'égalité précédente)

$= (a_{n+2} - a_n)(a_{n+2} + a_n)$ (utilisation de la relation $a_{n+2} = a_{n+1} + a_n$ écrite sous la forme $a_{n+1} = a_{n+2} - a_n$)

$= (a_{n+2})^2 - (a_n)^2$ (identité remarquable)

6°) Cette question est indépendante des précédentes.
Compléter l'algorithme ci-contre 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

II.

À toute lettre de l'alphabet on associe un entier naturel 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. Le couple $(p\,;q)$ 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 l'entier naturel x est l'entier y tel que $y \equiv x(x+B)$ [n] avec $0 \leqslant y < n$.

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

Coder le mot « NO » puis décoder la lettre D.

$p = 3$
$q = 11$
$n = 33$
$B = 13$
$y \equiv x(x+13)$ [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 ou les entier(s) naturel(s) x tel(s) que $0 \leqslant x \leqslant 25$ et $x(x+13) \equiv 3$ (mod. 33).

Le mieux est d'utiliser la calculatrice. On tape $Y1 = \text{reste}(X(X+13), 33)$.

On obtient la table.

On cherche dans la table les valeurs qui donnent 3.

On obtient : 8, 12, 23.

Les lettres correspondantes sont donc les lettres I, N, X.

Le « chiffre de Rabin » n'est donc pas utilisable pour décoder un message lettre par lettre.