REPUBLIQUE TUNISIENNE
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Concours Nationaux d'Entrée aux Cycles de Formation d'Ingénieurs
Session 2013

الجمهورية التونسية
وزارة التعليم العالي والبحث العلمي

المناظرات الوطنية للدخول إلى مراحل تكوين المهندسين
دورة 2013

Concours Toutes Options
Epreuve d'Informatique

Date : Mardi 04 Juin 2013 **Heure : 14 H** **Durée : 2 H** **Nbre pages : 5**

Barème : EXERCICE : 3 points PROBLEME (MAPLE) : 7 points
PROBLEME (ALGORITHMIQUE) : 10 points

DOCUMENTS NON AUTORISES
L'USAGE DES CALCULATRICES EST INTERDIT

EXERCICE (MAPLE)

On considère la suite réelle $(u_n)_{n\geq 0}$ et les fonctions f, g, et K définies comme suit :

$$\begin{cases} u_0 = -1 \\ u_1 = -1 \\ u_{n+2} = (n+1)u_{n+1} - (n+2)u_n \end{cases}$$

$$f : x \to \sum_{n=0}^{+\infty} u_n x^n$$

$$g : x \to \sum_{n=0}^{+\infty} \frac{u_n}{n!} x^n$$

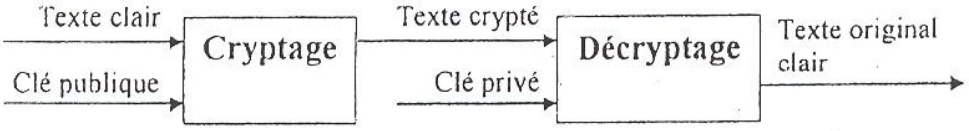
$$K = f \circ g$$

Donner les commandes MAPLE permettant de :

1. Calculer le terme général de u en fonction de n ;
2. Définir la suite u qui à n associe u_n ;
3. Définir f ;
4. Définir g ;
5. Définir K ;
6. Donner une évaluation de $K(-2)$ sur 20 chiffres significatifs ;
7. Calculer $\lim_{x\to-\infty} f(x)$ et $\lim_{x\to+\infty} g(x)$;
8. Résoudre l'équation $f''(x) = 0$
9. Représenter sur le même graphisme f et g pour $x \in [-6,2]$ en limitant les ordonnées dans l'intervalle $[-2,10]$;
10. Donner une approximation numérique des points d'intersection des courbes de f et g.

PROBLEME (MAPLE)

On se propose de développer en MAPLE la méthode de cryptage **RSA**.
Le cryptage/décryptage **RSA** est fondé sur l'utilisation d'une paire de clés composée d'une clé publique pour crypter et d'une clé privée pour décrypter des données confidentielles.



Soient p et q deux grands nombres premiers. La création des clés s'effectue comme suit :

- calculer l'indicatrice $z=(p-1)*(q-1)$;
- calculer $n=p*q$;
- choisir un grand entier c, premier avec z ; (on peut prendre par exemple c égal au premier entier premier supérieur à z)
- calculer l'entier $d=c^{(-1)} \bmod z$.

la clé publique est alors le couple (n,c).

la clé privé est le couple (n,d).

Pour crypter l'entier x, on effectue l'opération : $y=x^c \bmod n$.

Pour décrypter (retrouver x à partir de y), on effectuera : $x=y^d \bmod n$.

Travail demandé :

PARTIE A : cryptage et décryptage d'entier

1. Ecrire une procédure MAPLE nommée *Clef_RSA* qui prend en entrée deux grands nombres premiers **p** et **q** et retourne les deux clés sous forme de séquence de listes.
2. Ecrire une procédure MAPLE nommée ***CryptDecryptE*** qui prend comme argument un entier **a** et une clé **CL** (avec $CL=[u,v]$) et retourne un entier **b** tel que $b=a^u \bmod v$.
3. Ecrire une procédure MAPLE nommée ***CryptDecryptList*** qui prend comme argument une liste d'entiers **L1** et une clé **CL** et retourne la liste **L2** image de **L1** par ***CryptDecryptE***.

PARTIE B : cryptage et décryptage d'une chaîne de caractères

Le cryptage/décryptage d'une chaîne de caractères consiste à crypter/décrypter les codes ASCII correspondants aux caractères de la chaîne.

Sachant qu'une chaîne est une structure indexée de type string et que les fonctions Maple suivantes sont prédéfinies :

- length(Ch) retourne la longueur de la chaîne de caractères Ch.
  Exemple : `length("abc");` retourne 3.
- Ord(C) retourne l'entier correspondant au caractère C (càd son code ASCII).
  Exemple : `Ord("a");` retourne 92.
- Char(n) retourne le caractère correspondant à l'entier n.
  Exemple : `Char(92);` retourne "a".
- cat(Ch1, Ch2) retourne la chaîne de caractères concaténation des chaînes Ch1 et Ch2.
  Exemple : `cat("a", "b");` donne la chaîne "ab".

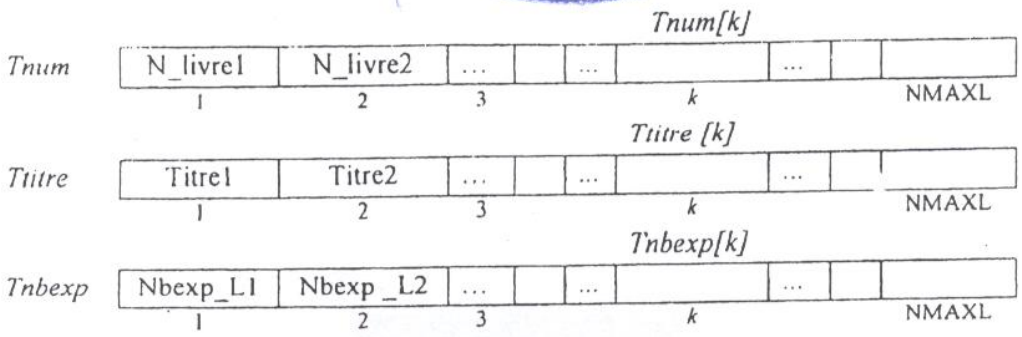
4. Ecrire une procédure MAPLE nommée ***Codage*** qui prend comme argument une chaîne **CH** de type ***string*** et retourne la liste des codes ASCII correspondants.
5. Ecrire une procédure MAPLE nommée ***Decodage*** qui prend comme argument une liste d'entiers L (codes ASCII des caractères) et retourne la chaîne de caractères correspondante.
6. Ecrire une procédure MAPLE nommée ***CryptageC*** qui prend une chaîne **CH** et une clé **CL** et retourne la liste des entiers cryptés de la liste des codes de **CH**.
7. Ecrire une procédure MAPLE nommée ***DecryptageC*** qui prend une liste d'entiers cryptés **L1** et une clé **CL** et retourne la chaîne claire.

PROBLEME (ALGORITHMIQUE)

L'objectif du problème est d'implémenter quelques algorithmes de gestion de livres d'une bibliothèque (saisie, emprunt, affichage, ...).

Chaque livre est caractérisé par un numéro, un titre et un nombre d'exemplaires. Les caractéristiques relatives à tous les livres présents dans la bibliothèque sont représentées par les 3 tableaux à une dimension suivants:

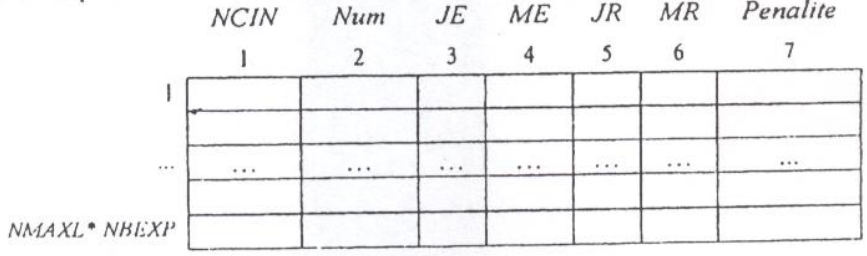
- *Tnum* pour tous les numéros des livres.
- *Ttitre* pour tous les titres des livres.
- *Tnbexp* pour le nombre d'exemplaires des différents livres.



Le livre dont le numéro est *Tnum[k]* a pour titre *Ttitre[k]* et un nombre d'exemplaires disponibles dans la bibliothèque *Tnbexp[k]*.

- Chaque numéro de livre (*Tnum[k]*) est un entier strictement positif.
- Chaque titre de livre (*Ttitre [k]*) est une chaîne.
- Le nombre d'exemplaires de chaque livre (*Tnbexp[k]*) est un entier compris entre 1 et *NBEXP* (*NBEXP* est le nombre d'exemplaires maximum par livre dans la bibliothèque).

Pour la gestion des emprunts des livres on utilise le tableau d'entiers *M* à deux dimensions suivant :



Un emprunt est caractérisé par un numéro de *CIN (NCIN)* de l'emprunteur, le numéro du livre emprunté (*Num*), la date de l'emprunt (*JE/ME*), la date de retour prévue (*JR/MR*) ainsi que la pénalité (*Penalite*) indiquant si l'emprunteur est pénalisé ou non.

- *NCIN* est un entier strictement positif composé de 8 chiffres.
- *Num* doit correspondre à un numéro de livre existant dans la bibliothèque (présent dans le tableau *Tnum*).
- La date de l'emprunt est représentée par le jour (*JE*) et le mois (*ME*) de l'emprunt qui sont des entiers.
- La date de retour prévue est représentée par le jour (*JR*) et le mois (*MR*) du retour du livre qui sont deux entiers. La date de retour prévue est 10 jours après la date de l'emprunt.
- *Penalite* indique qu'un emprunteur est pénalisé (valeur 1) ou non (valeur 0). Un emprunteur est pénalisé s'il a dépassé la date de retour prévue (*JR/MR*).

Hypothèses et nomenclatures:

Dans la suite, on suppose avoir effectué les déclarations suivantes :

Constante *NMAXL* = 1000 *NBEXP* = 10

Type
TAB1 = *tableau*[1.. *NMAXL*] *de entier*
TAB2 = *tableau*[1.. *NMAXL*] *de chaîne*
TAB3 = *tableau*[1.. *NMAXL* * *NBEXP*] *de entier*
MAT = *tableau*[1.. *NMAXL* * *NBEXP*, 1..7] *de entier*

- Un emprunteur n'a pas le droit d'emprunter plus d'un livre à la fois.
- Un emprunteur pénalisé n'a plus droit à un nouvel emprunt.
- On suppose que l'année est non bissextile (mois février contient 28 jours).

Nom de variables	Type	Rôle
NBT	*entier*	Nombre de titres dans la bibliothèque compris entre 1 et *NMAXL*.
Tnum	*TAB1*	Tableau des numéros des titres de livres.
Ttitre	*TAB2*	Tableau des titres des livres.
Tnbexp	*TAB1*	Tableau des nombres des exemplaires par titre supposé initialisé à 0.
NBEMP	*entier*	Nombre d'emprunts compris entre 1 et *NMAXL*NBEXP*.
M	*MAT*	Matrice de gestion des emprunts.
NCIN	*entier*	Identifiant de l'emprunteur
NP	*entier*	Nombre d'étudiants pénalisés, dans le tableau *P*, compris entre 1 et *NMAXL*NBEXP*
P	*TAB3*	Tableau de pénalité contenant les identifiants des emprunteurs pénalisés ayant rendu leurs livres.
JE et ME	*entier*	Respectivement jour et mois d'emprunt.
JR et MR	*entier*	Respectivement jour et mois de retour.

Travail demandé :

1. Ecrire une fonction algorithmique, nommée ***Nombre***, qui saisit et retourne un entier compris entre les paramètres en entrée **min** et **max**.
2. Ecrire une fonction algorithmique, nommée ***Index***, qui à partir d'un numéro de livre **Num** retourne l'indice **k** du livre s'il existe et -1 sinon. Les paramètres sont **NBT**, **Tnum** et **Num**.
3. Ecrire une procédure algorithmique, nommée ***Ajout_Tit***, qui permet de saisir un nouveau numéro de livre à ajouter à la bibliothèque, son titre ainsi que le nombre d'exemplaires en faisant les contrôles nécessaires. Les paramètres de la procédure sont **NBT**, **Tnum**, **Ttitre** et **Tnbexp**.

   NB :

   - Le nombre d'exemplaires à saisir est contrôlé par appel à la fonction *Nombre*.
   - L'ajout des caractéristiques d'un livre se fait à la fin des tableaux.
4. Ecrire une procédure algorithmique, nommée ***Ajout_NbEx***, qui ajoute **Nb** exemplaires d'un titre ayant le numéro **Num**. Les paramètres de la procédure sont **NBT**, **Tnum**, **Num**, **Nb** et **Tnbexp**.
5. Ecrire une procédure algorithmique, nommée ***Etat_Bib***, qui affiche pour chaque livre son titre ainsi que le nombre d'exemplaires encore disponibles.
   Les paramètres de la procédure sont **NBT**, **Tnum**, **Ttitre** et **Tnbexp**.
6. Ecrire une fonction algorithmique, nommée ***Aut_Emp***, qui retourne *vrai* si un emprunteur identifié par **NCIN** est autorisé à emprunter et *faux* sinon. Un emprunteur est autorisé s'il n'a pas un livre en sa possession et son identifiant ne figure pas dans le tableau **P**. Les paramètres sont **NCIN**, **NBEMP**, **M** , **NP** et **P**.
7. Ecrire une procédure algorithmique, nommée ***Calcul_Date***, qui calcule la date de retour prévue. Les paramètres de la procédure sont **JE**, **ME**, **JR** et **MR**.
8. Ecrire une procédure algorithmique, nommée ***Emprunt***, qui saisit le numéro de l'emprunteur et vérifie s'il est autorisé à emprunter ou non. Dans le cas de non pénalité, saisir le numéro du livre à emprunter. Si le livre est disponible en stock, saisir la date d'emprunt (supposée valide). Un livre emprunté est déduit du stock et la matrice d'emprunt **M** est mise à jour. Les paramètres de la procédure sont **NBEMP**, **M**, **NCIN**, **NP**, **P**, **Num**, **JE**, **ME** et **Tnbexp**.
9. Ecrire une procédure algorithmique, nommée ***Maj_Pen***, qui à partir d'une date donnée (**Jo/Mo**), met à jour la matrice **M** pour les emprunteurs ayant dépassé la date limite de retour. Les paramètres de la procédure sont **NBEMP**, **M**, **Jo** et **Mo**.
10. Ecrire une procédure algorithmique, nommée ***Etat_Pen***, qui affiche pour une date donnée (**Jo/Mo**), les numéros des emprunteurs ayant dépassé la date limite de retour ainsi que les titres des livres en leurs possessions.
11. Ecrire une procédure algorithmique, nommée ***Retour***, qui gère le retour d'un livre. La ligne correspondante à l'emprunteur dans la matrice **M** sera écrasée par la dernière ligne de **M**.