IUP3 : Informatique et modelisation. Examen du 14.01.04.

Seules les notes manuscrites et le support de cours sont autorisés. Le candidat s'efforcera de rédiger lisiblement et avec soin sa copie.
Le sujet est (en principe) trop long pour le temps imparti, il est donc conseillé de traiter en priorité les questions que l'on sait faire en en indiquant clairement la référence.

I) Questions de Cours
1) En quoi consiste le modèle de Cox-Ross-Rubinstein ? l'espérance de prix d'un actif qui suit ce modèle ?
2) a) Qu'est-ce qu'un générateur à un pas (G1P), à deux pas (G2P) ?
b) Un GCL2 (ou GL2P) ? Donner des exemples.
c) Donner la décomposition du GL2P dans le cas où l'équation caractéristique (EC) a des racines (deux cas). On utilisera les notations suivantes

$$(x_0,\, x_1;\ x_{n+2} \equiv \alpha x_n + \beta x_{n+1}\ [p]) \tag{1}$$

d) Comment procède-t-on quand l'EC n'a pas de racine ?
3) a) En quoi consiste la méthode RSA ? Sur quoi repose sa fiabilité ?
b) Comment calculer une clé de codage (i.e. un nombre c premier avec $(p-1)(q-1)$) ?
c) Comment calculer d tel que $cd \equiv 1[(p-1)(q-1)]$? À quoi sert d ?
d) Donner des exemples avec $c \neq d$.

II) Exercice
1) a) Donner les orbites des GL2P (i-iii-iv) suivants (pour vous aider, la période est indiquée dans le tableau qui utilise les notations de (1)).

Question	x_0	x_1	a	b	p	λ	Q	x_0	x_1	a	b	p	λ
i)	1	1	1	4	11	10	ii)	1	1	2	5	11	120
iii)	1	1	2	5	17	8	iv)	1	1	6	12	29	7

b) Décomposer les quatre générateurs donnés par le tableau précédent.

4) a) Vérifier que les GL2P donnés par le tableau suivant ont des équations caractéristiques sans racine.

Question	x_0	x_1	a	b	p	$r^2 =$
i)	1	1	1	3	5	3
ii)	1	1	1	3	7	3
iii)	1	1	1	3	11	m

b) Décomposer les générateurs donnés par le tableau précédent (on adjoindra la racine indiquée dans le tableau, pour le (iii), m dsigne le plus petit non-carré dans [0..10]).

III. (Petit) Problème

On considère la suite $x_n = n^2 \times 2^n \mod 13$, le but du problème est de montrer qu'elle provient d'un GL3P. Un GLkP est défini par

$$(x_0,\, x_1,\, \ldots,\, x_{k-1};\ x_{n+k} = \sum_{j=0}^{k-1} \alpha_j x_{n+j})$$

a) Calculer les différences $y_n = x_{n+1} - 2 * x_n;\ z_n = y_{n+1} - 2y_n;\ t_n = z_{n+1} - 2.z_n$
b) Montrer que z_n provient d'un GL1P en calculant $z_{n+1} - 2.z_n$.
c) Montrer, par une méthode similaire que y_n et x_n proviennent respectivement d'un GL2P et d'un GL3P que l'on précisera.

IUP3 : Contrôle de T.D. du 14.01.04.

A) Stuctures de données en Maple.

1) Donner trois exemples d'objets en Maple.
2) Comment sont représentés les objets composés ? (on décrira la structure arborescente de cette représentation en général et sur quelques exemples).
3) Donner le sens et la syntaxe des fonctions `whattype, nops, op(k,l)`.
4) Décrire les types `list, set, exprseq` et les fonctions qui leurs sont attachés `member, union, intersect, minus`.

B) Programmation.

1) a) Que fait le programme suivant ? On donnera le sens des paramètres et des variables locales.

```
> orb2:=proc(x0,x1,f,B) local i,j,LL,x,y,z: x:=x0: y:=x1: LL:=[x,y]: for i from 2 to B do z:=f(x,y)
: x:=y : y:=z: for j to i-1 do if [x,y]=[LL[j],LL[j+1]] then i:=B else fi od: LL:=[op(LL),y] od:
LL end:
```

b) Analyser ce programme. On expliquera sa structure et son fonctionnement en particulier les conditionnelles, les boucles etc..).

c) En simuler l'exécution sur un exemple simple.

2) Que font les deux fonctions suivantes ?

```
> comp:=proc(L,l) local res,i; if nops(L)>=l then res:=L else res:=[op(L),seq(0,i=1..l-nops(L))]
fi : res end;
```

```
> Nmap:=proc(n,N) map(x->x+1,comp(convert(N-1,base,n),n)) end;
```