Université Paris 7
IUP 2
Analyse de Performance et Simulation
Année 2003-2004

Corrigé de l'interrogation écrite
du mercredi 31 mars 2004
durée 2 heures

Corrigé exercice 1

1. La 'Middle Square Method' est une des première *méthodes de génération de suites de nombres pseudo-aléatoires*. Elle a été inventée dans les années 50 par Von Neuman. Son principe est de créer une suite de *nombres de n chiffres* $(x_i)_{i\in\mathbb{N}}$ à partir d'un nombre x_0 de départ à n chiffres selon *l'algorithme suivant* :
   (a) mettre x_i au carré (on obtient un nombre d'au maximum $2n$ chiffres.)
   (b) garder les n chiffres du milieu.
   (c) recommencer.
2. L'algorithme de Brent calcule les *paramètres de générateurs de suites de nombres pseudo-aléatoires à un pas*, c'est-à-dire leur *prépériode* et leur *période*.
   Il est efficace parce qu'il *ne garde en mémoire à chaque instant que deux valeurs de la suite* tout en étant rapide (temps linéaire).
3. Une suite de nombres pseudo-aléatoires est une suite qui *imite une suite de nombres aléatoires*, cette dernière ne pouvant être générée par un ordinateur qui suit son programme sans improviser.
   Le mathématicien D. H. Lehmer définit : " Une suite pseudo-aléatoire est une vague notion couvrant l'idée d'une suite dans laquelle *chaque terme est imprévisible pour un non-initié*, et dont les éléments satisfont un certain nombre de *tests statistiques* traditionnels, dépendant éventuellement de l'usage auquel est destinée la suite."
   Dans le cas uniforme : indépendance, même probabilité pour chaque élément d'être à un indice quelconque.

Corrigé Exercice 2

1. Convertir les nombres suivants :
   a) $(11011)_2 = 1\cdot 2^0 + 1\cdot 2^1 + 0\cdot 2^2 + 1\cdot 2^3 + 1\cdot 2^4 = 1+2+8+16 = 27$
   b) $(368)_9 = 8 + 6\cdot 9 + 3\cdot 81 = 8+54+243 = 305 = 256+32+16+1 = (100110001)_2$

c) $(1101)_2 = 1 + 4 + 8 = 13$

$(\underbrace{1101...1101}_{4n \text{ chiffres}})_2 = 13 + 16 \cdot 13 + 16^2 \cdot 13 + \cdots + 13 \cdot 16^{n-1} = 13 \cdot (1 + 16 + 16^2 + \cdots + 16^{n-1}) = 13 \cdot \frac{1-16^n}{1-16} = \frac{13}{15}(16^n - 1)$

2. $23/11 = 2.(09)^\infty$.
3. $(2, 45)_7 = 2 + 4 \cdot 7^{-1} + 5 \cdot 7^{-2} = 2 + \frac{4}{7} + \frac{5}{49} = \frac{2 \cdot 49 + 4 \cdot 7 + 5}{49} = \frac{131}{49}$
4. $(5, (61)^\infty)_{10} = 5 + (\frac{61}{100} + \frac{61}{100} \cdot \frac{1}{100} + \cdots + \frac{61}{100} \cdot \frac{1}{100^n} + \cdots) = 5 + \frac{61}{100} \cdot \frac{1}{1-\frac{1}{100}} = 5 + \frac{61}{100} \cdot \frac{100}{99} = \frac{5 \cdot 99 + 61}{99} = \frac{556}{99} = \frac{512 + 5 * 8 + 4}{64 + 4 * 8 + 3} = \left(\frac{1054}{143}\right)_8$

Corrigé exercice 3

Comme on a vu que :

$$((x \bmod n) + (y \bmod n)) \bmod n = (x + y) \bmod n$$

$$((x \bmod n) * (y \bmod n)) \bmod n = (x * y) \bmod n$$

On a :

$$\begin{aligned} n \bmod 5 &= (\Sigma_{0 \le k \le N} a_k 10^k) \bmod 5 \\ &= (\Sigma_{0 \le k \le N} ((a_k 10^k) \bmod 5)) \bmod 5 \\ &= (\Sigma_{0 \le k \le N} (a_k \bmod 5) \cdot (10^k \bmod 5)) \bmod 5 \end{aligned}$$

Or $(10^k \bmod 5) = 0$ pour tout $k \ge 1$ et $10^0 = 1 \bmod 5$.

D'où $n \bmod 5 = a_0 \bmod 5$.

Donc n est divisible par 5 quand $a_0 = 0 \bmod 5$, soit quand n finit par un 0 ou un 5.

Corrigé exercice 4

1. Suite géométrique de raison 6 : $u_n = 6^n u_0$.
2. $u_n = u_{n-1} + 6u_{n-2} + 7$ Equation de récurrence linéraire d'ordre 2 avec second membre.

   On résoud d'abord l'équation sans second membre :

   $$v_n = v_{n-1} + 6v_{n-2}$$

   Son polynôme caractéristique est :

   $$r^2 - r - 6 = 0$$
   $$\Delta = 1 + 24 = 25 = 5^2$$
   $$r_1 = \frac{1 + 5}{2} = 3$$

$$r_2 = \frac{1-5}{2} = -2$$

On a donc

$$v_n = \lambda \cdot 3^n + \mu \cdot (-2)^n$$

On exprime λ et μ en fonction de v_0 et v_1.

$$\left\{ \begin{array}{rcl} v_0 & = & \lambda + \mu \\ v_1 & = & 3\lambda - 2\mu \end{array} \right.$$

$$\left\{ \begin{array}{rcl} \lambda & = & v_0 - \mu \\ v_1 & = & 3v_0 - 3\mu - 2\mu \end{array} \right.$$

$$\left\{ \begin{array}{rcl} \lambda & = & v_0 - \frac{1}{5}(3v_0 - v_1) \\ 5\mu & = & 3v_0 - v_1 \end{array} \right.$$

$$\left\{ \begin{array}{rcl} \mu & = & \frac{1}{5}(3v_0 - v_1) \\ \lambda & = & \frac{1}{5}(v_1 + 2v_0) \end{array} \right.$$

$$v_n = \frac{1}{5}(v_1 + 2v_0) \cdot 3^n + \frac{1}{5}(3v_0 - v_1) \cdot (-2)^n$$

On cherche une solution particulière sous la forme d'une constante :

$$K = K + 6K + 7$$

$$K = -\frac{7}{6}$$

On a alors :

$$u_n = v_n - \frac{7}{6}.$$

Corrigé exercice 5

1. $$\Delta = 9 + 24 = 33$$

   33 n'a pas de racine dans $\mathbb{Z}$, donc l'équation n'a pas de solution dans $\mathbb{Z}$.

2. $$\Delta = 4 - 4 * 3 * 6 = 4 - 72 = -68 = 2 \bmod 7$$

   Or $3 * 3 = 9 = 2 \bmod 7$. Donc 3 est racine de 2. On a donc comme solution :

   $$x_1 = \frac{-2+3}{6} = \frac{1}{6} = 6$$

   $$x_2 = \frac{-2-3}{6} = \frac{-5}{6} = \frac{2}{6} = 5$$

   car $6 * 6 = 36 = 1 \bmod 7$ et $5 * 6 = 30 = 2 \bmod 7$.

3.

$$\Delta = 4 - 4m = 4(1-m)$$

Δ est un carré si et seulement si $(1-m)$ est un carré (en effet $\sqrt{ab} = \sqrt{a} \cdot \sqrt{b}$). On calcule les carrés dans $\mathbb{Z}/5\mathbb{Z}$. $0^2 = 0, 1^2 = 1, 2^2 = 4, 3^2 = 4, 4^2 = 1$.

Donc Δ est un carré si $(1-m) = 0$ ou $(1-m) = 1$ ou $(1-m) = 4$. Soit $m = 1$, $m = 0$ ou $m = 2$.

$$x_1 = \frac{-2 - 2\sqrt{1-m}}{2} = -1 - \sqrt{1-m}$$

$$x_2 = -1 + \sqrt{1-m}$$

- $m = 1$: une racine double $x_1 = x_2 = -1$.
- $m = 2$: deux solutions $x_1 = -1 - 2 = -3 = 2$ et $x_2 = -1 + 2 = 1$.
- $m = 0$: deux solutions $x_1 = -1 - 1 = -2 = 3$ et $x_2 = -1 + 1 = 0$.
- Autres cas : pas de solutions.

Corrigé exercice 6

1. Orbite : $1 \to 8 \to 7 \to 4 \to 6 \to 1$

   Prépériode : 0, période : 5.

2. Pieuvre :

   $0 \to 11 \to 7 \to 12 \to 9 \to 3 \to 4 \to 6 \to 10 \to 5 \to 8 \to 1 \to 0$

   $2 \to 2$

Corrigé exercice 7

On rappelle le théorème :

Théorème 1 *Pour qu'un GCL $x_{n+1} = ax_n + b \bmod m$ soit de période maximale il faut et il suffit que les conditions suivantes soient vérifiées :*

a) b est inversible $\bmod m$

b) $a = 1\ [p]$ pour tout p permier divisant m.

c) Si $4|m$ alors $a = 1\ [4]$.

On applique le théorème :

a) 3 est inversible dans $\mathbb{Z}/8\mathbb{Z}$ ($3 * 3 = 9 = 1 \bmod 8$).

b) 2 est le seul premier qui divise 8. Il faut $a = 1 \bmod 2$. Donc a doit être impair.

c) $4|m$ donc $a = 1$ ou $a = 5$.

Corrigé exercice 8

1.

$$5^n = 4 \times 6^n \bmod 7 \quad (1)$$

On a 6 inverse de 6 ($6 * 6 = 36 = 1 \bmod 7$). On multiplie des deux côtés par 6^n. On a $5 * 6 = 30 = 2 \bmod 7$. D'où $(1) * 6^n$ devient :

$$5^n * 6^n = 4 \times 6^n \times 6^n \bmod 7$$

$$(5 * 6)^n = 4 \times (6 * 6)^n \bmod 7$$

$$2^n = 4 \bmod 7$$

n	$2^n \bmod 7$
0	1
1	2
2	4
3	1

Analyse de périodicité : 2^n a une période de 3. Donc

$$\begin{cases} n_1 &= 2 \\ n_k &= 2 + 3(k-1), k \geq 1. \end{cases}$$

2. On se ramène comme précédemment à l'équation :

$$2^n = 4n \bmod 7$$

n	$2^n \bmod 7$	$4n \bmod 7$	$(2^n - 4n) \bmod 7$
0	1	0	
1	2	4	
2	4	1	
3	1	5	
4	2	2	0
5	4	6	
6	1	3	
7	2	0	
8	4	4	0
9	1	1	0
10	2	5	
11	4	2	
12	1	6	
13	2	3	
14	4	0	
15	1	4	
16	2	1	
17	4	5	
18	1	2	
19	2	6	
20	4	3	
21	1	0	

Analyse de périodicité : 2^n a une période de 3, $4n$ a une période de 7, donc l'équation a une période de 21. On calcule donc les 21 premières valeurs. Et on trouve comme solutions :

$$\left\{\begin{array}{llcll} n_1 = 4, & n_{3k+1} & = & 4+21k & k \geq 0 \\ n_2 = 8, & n_{3k+2} & = & 8+21k & k \geq 0 \\ n_3 = 9, & n_{3k} & = & 9+21(k-1) & k \geq 1 \end{array}\right.$$

Corrigé exercice 9

$$ab|cd \Leftrightarrow_{\text{par def}} \exists k \in mathbbZ, kab = cd \quad (1)$$

$$a \text{ premier avec } c \Leftrightarrow_{\text{Bezout}} \exists u, v \in \mathbb{Z}, au + cv = 1 \quad (2)$$

$$c \times (1) : akbv = cvd, (2) \Rightarrow akbv = (1-au)d$$

d'où

$$a(\underbrace{kbv + ud}\, k') = d.$$

Donc a divise d.

Par un raisonnement symétrique, b divise c.

Corrigé exercice 10

$a_{n+2} = F_{2(n+2)+1} = F_{2n+5} = F_{2n+4} + F_{2n+3} = (F_{2n+3} + F_{2n+2}) + F_{2n+3}$.
Or $F_{2n+3} = F_{2n+2} + F_{2n+1}$. D'où $F_{2n+2} = F_{2n+3} - F_{2n+1}$.
On a alors $a_{n+2} = 2F_{2n+3} + (F_{2n+3} - F_{2n+1}) = 3F_{2n+3} - F_{2n+1} = 3a_{n+1} - a_n$.