Université Paris 7
IUP 2
Analyse de Performance et Simulation
Année 2004-2005

Corrigé de l'interrogation écrite
du mercredi 5 avril 2005
durée 2 heures

Corrigé exercice 1

1. Un générateur à un pas donne une *suite de nombres pseudo-aléatoires* dont chaque élément est une *fonction* de la valeur *du seul élément précédent.*

   Des exemples sont la Middle Square Method ou les générateurs linéaires à un pas (GL1P) ($x_{n+1} = ax_n + b \bmod m$).

2. On mesure la performance d'un générateur à un pas en calculant *la taille de son orbite* (période + prépériode). Elle correspond au nombre d'éléments de la suite avant que celle-ci boucle. Plus elle est grande et plus le générateur est performant.

3. L'algorithme de Floyd 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).

4. 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) $(10110)_2 = 0 \cdot 2^0 + 1 \cdot 2^1 + 1 \cdot 2^2 + 0 \cdot 2^3 + 1 \cdot 2^4 = 2 + 4 + 16 = 22$

   b) $(436)_7 = 6+3 \cdot 7+4 \cdot 49 = 6+21+196 = (223)_{10} = 2*81+2*27+2*3+1 = 2 * 3^4 + 2 * 3^3 + 2 * 3^1 + 3^0 = (22021)_3$

c) $(110)_2 = 2 + 4 = 6$

$(\underbrace{110...110}_{3n \text{ chiffres}})_2 = 6 + 8 \cdot 6 + 8^2 \cdot 6 + \cdots + 6 \cdot 8^{n-1} = 6 \cdot (1 + 8 + 8^2 + \cdots + 8^{n-1}) =$
$6 \cdot \frac{1-8^n}{1-8} = \frac{6}{7}(8^n - 1)$

2. $27/11 = 2.(45)^\infty$.
3. $(3, 43)_6 = 3 + 4 \cdot 6^{-1} + 3 \cdot 6^{-2} = 3 + \frac{4}{6} + \frac{3}{36} = \frac{3 \cdot 36 + 4 \cdot 6 + 3}{36} = \frac{135}{36} = \frac{15}{4}$
4. $(4, (76)^\infty)_{10} = 4 + (\frac{76}{100} + \frac{76}{100} \cdot \frac{1}{100} + \cdots + \frac{76}{100} \cdot \frac{1}{100^n} + \cdots) = 4 + \frac{76}{100} \cdot \frac{1}{1 - \frac{1}{100}} =$
$4 + \frac{76}{100} \cdot \frac{100}{99} = \frac{4 \cdot 99 + 76}{99} = \frac{472}{99} = \frac{343 + 2*49 + 4*7 + 3}{2*49 + 1} = \left(\frac{1243}{201}\right)_7$

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 :

$$\begin{aligned} n \bmod 4 &= (\Sigma_{0 \leq k \leq N} a_k 8^k) \bmod 4 \\ &= (\Sigma_{0 \leq k \leq N} ((a_k 8^k) \bmod 4)) \bmod 4 \\ &= (\Sigma_{0 \leq k \leq N} (a_k \bmod 4) \cdot (8^k \bmod 4)) \bmod 4 \end{aligned}$$

Or $(8^k \bmod 4) = 0$ pour tout $k \geq 1$ et $8^0 = 1 \bmod 4$.

D'où $n \bmod 4 = a_0 \bmod 4$.

Donc n, écrit en base 8, est divisible par 4 quand $a_0 = 0 \bmod 4$, soit quand n finit par un 0 ou un 4.

Corrigé exercice 4

1. Suite géométrique de raison 7 : $u_n = 7^n u_0$.
2. $u_n = u_{n-1} + 12u_{n-2} + 5$ Equation de récurrence linéraire d'ordre 2 avec second membre.

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

   $$v_n = v_{n-1} + 12v_{n-2}$$

   Son polynôme caractéristique est :

   $$r^2 - r - 12 = 0$$
   $$\Delta = 1 + 48 = 49 = 7^2$$
   $$r_1 = \frac{1 + 7}{2} = 4$$

$$r_2 = \frac{1-7}{2} = -3$$

On a donc

$$v_n = \lambda \cdot 4^n + \mu \cdot (-3)^n$$

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

$$K = K + 12K + 5$$

$$K = -\frac{5}{12}$$

On a alors :

$$u_n = v_n - \frac{5}{12}.$$

Soit

$$u_n = \lambda \cdot 4^n + \mu \cdot (-3)^n - \frac{5}{12}.$$

On exprime λ et μ en fonction de u_0 et u_1.

$$\left\{ \begin{array}{rcl} u_0 & = & \lambda + \mu - \frac{5}{12} \\ u_1 & = & 4\lambda - 3\mu - \frac{5}{12} \end{array} \right.$$

$$\left\{ \begin{array}{rcl} 3u_0 & = & 3\lambda + 3\mu - \frac{15}{12} \\ u_1 & = & 4\lambda - 3\mu - \frac{5}{12} \end{array} \right.$$

$$\left\{ \begin{array}{rcl} u_0 & = & \lambda + \mu - \frac{5}{12} \\ 3u_0 + u_1 + \frac{20}{12} & = & 7\lambda \end{array} \right.$$

$$\left\{ \begin{array}{rcl} \mu & = & u_0 - \frac{1}{7}(3u_0 + u_1) - \frac{5}{21} + \frac{5}{12} \\ \lambda & = & \frac{1}{7}(3u_0 + u_1) + \frac{10}{42} \end{array} \right.$$

$$\left\{ \begin{array}{rcl} \mu & = & \frac{1}{7}(4u_0 - u_1) + \frac{15}{84} \\ \lambda & = & \frac{1}{7}(3u_0 + u_1) + \frac{10}{42} \end{array} \right.$$

$$\left\{ \begin{array}{rcl} \mu & = & \frac{1}{7}(4u_0 - u_1) + \frac{5}{28} \\ \lambda & = & \frac{1}{7}(3u_0 + u_1) + \frac{10}{42} \end{array} \right.$$

On a alors

$$u_n = \left(\frac{1}{7}(3u_0 + u_1) + \frac{10}{42}\right) \cdot 4^n + \left(\frac{1}{7}(4u_0 - u_1) + \frac{5}{28}\right) \cdot (-3)^n - \frac{5}{12}.$$

Corrigé exercice 5

1. $$\Delta = 4^2 - 4 * 3 * (-1) = 16 + 12 = 28$$

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

2.
$$\Delta = 3^2 - 4 * 4 * 2 = 9 - 32 = -23 = 10 \bmod 11$$
On cherche si 10 est un carré dans $\mathbb{Z}/11\mathbb{Z}$: $0^2 = 0, 1^2 = 1, 2^2 = 4, 3^2 = 9, 4^2 = 55^2 = 3$ (on n'a besoin de calculer que la moitié des carrés). 10 n'est pas un carré, donc l'équation n'a pas de solution dans $\mathbb{Z}/11\mathbb{Z}$.

3.
$$\Delta = 1 - 8m$$
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 $(1 - 8m) = 0$ ou $(1 - 8m) = 1$ ou $(1 - 8m) = 4$.

Si $(1 - 8m) = 0$, alors $m = 1/8 = 2$ car $2 * 8 = 16 = 1 \bmod 5$.

Si $(1 - 8m) = 1$, alors $8m = 0$ et $m = 0$.

Si $(1 - 8m) = 4$, alors $m = -3/8 = 2/8 = 4$ car $4 * 8 = 32 = 2 \bmod 5$.

$$x_1 = \frac{-1 - \sqrt{1 - 8m}}{4}$$
$$x_2 = \frac{-1 + \sqrt{1 - 8m}}{4}$$

- $m = 2 : \Delta = 0$. Une racine double $x_1 = x_2 = -1/4 = 4/4 = 1$.
- $m = 0 : \Delta = 1$. $\sqrt{\Delta} = 1$. Deux solutions $x_1 = \frac{-1+1}{4} = 0$ et $x_2 = \frac{-1-1}{4} = -2/4 = 3/4 = 2$ car $2 * 4 = 8 = 3 \bmod 5$.
- $m = 4 : \Delta = 4$. $\sqrt{\Delta} = 2$. Deux solutions $x_1 = \frac{-1+2}{4} = 1/4 = 4$ car $4 * 4 = 16 = 1 \bmod 5$ et $x_2 = \frac{-1-2}{4} = -3/4 = 2/4 = 3$ car $3 * 4 = 12 = 2 \bmod 5$.
- Autres cas : pas de solutions.

Corrigé exercice 6

1. Orbite : $6 \to 3 \to 5 \to 0 \to 7 \to 6$

   Prépériode : 0, période : 5.

2. Pieuvre :

   $0 \to 3 \to 2 \to 11 \to 8 \to 9 \to 0$

   $1 \to 7 \to 5 \to 10 \to 4 \to 6 \to 1$

   $12 \to 12$

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) 5 est inversible dans $\mathbb{Z}/12\mathbb{Z}$ ($5 * 5 = 25 = 1 \bmod 12$).

b) 2 et 3 sont les diviseurs premiers de 12. Il faut $a = 1 \bmod 2$ et $a = 1 \bmod 3$. Donc a ne peut être que 1 ou 7.

c) $4|12$ donc $a = 1$.

Corrigé exercice 8

1. $$5^n = 2 \times 3^n \bmod 7 \quad (1)$$

   On a 5 inverse de 3 ($5 * 3 = 15 = 1 \bmod 7$). On multiplie des deux côtés par 5^n. On a $5 * 5 = 25 = 4 \bmod 7$. D'où $(1) * 5^n$ devient :

   $$5^n * 5^n = 2 \times 3^n \times 5^n \bmod 7$$

   $$(5 * 5)^n = 2 \times (3 * 5)^n \bmod 7$$

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

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

   Analyse de périodicité : 4^n a une période de 3. Donc

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

2. $$7^n = n \times 10^n \bmod 17 \quad (2)$$

   On a 12 inverse de 10 ($12 * 10 = 120 = 1 \bmod 17$).

   On se ramène comme précédemment à l'équation (en utilisant $7 * 12 = 84 = 16 \bmod 17$) :

   $$16^n = n \bmod 7$$

n	$16^n \bmod 17$	$n \bmod 17$	$(16^n - n) \bmod 17$
0	1	0	
1	16	1	
2	1	2	
3	16	3	
4	1	4	
5	16	5	
6	1	6	
7	16	7	
8	1	8	
9	16	9	
10	1	10	
11	16	11	
12	1	12	
13	16	13	
14	1	14	
15	16	15	
16	1	16	
17	16	0	
18	1	1	0
19	16	2	
20	1	3	
21	16	4	
22	1	5	
23	16	6	
24	1	7	
25	16	8	
26	1	9	
27	16	10	
28	1	11	
29	16	12	
30	1	13	
31	16	14	
32	1	15	
33	16	16	0
34	1	0	

Analyse de périodicité : 16^n a une période de 2, n a une période de 17, donc l'équation a une période de 34. On calcule donc les 34 premières valeurs. Et on trouve comme solutions :

$$\begin{cases} n_1 = 18, & n_{2k+1} = 18 + 34k \quad k \geq 0 \\ n_2 = 33, & n_{2k+2} = 33 + 34k \quad k \geq 0 \end{cases}$$

Corrigé exercice 9

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

$$a|b \Leftrightarrow_{\text{par def}} \exists k \in \mathbb{Z}, ka = b \quad (2)$$

$$v \times (2) : kav = bv \quad (3)$$

$$(1) + (3) : au + cv + vb = 1 + kav$$

d'où

$$a(u - kv) + (b + c)v = 1.$$

Donc a premier avec $(b + c)$.

Corrigé exercice 10

$$\begin{array}{rcl} u_{n+2} & = & \sum_{k=0}^{n+2} F_k \\ & = & F_0 + F_1 + \sum_{k=2}^{n+2} (F_{k-1} + F_{k-2}) \\ & = & F_0 + F_1 + \sum_{k=1}^{n+1} F_k + \sum_{k=0}^{n} F_k \\ & = & u_{n+1} + u_n + 1 \end{array}$$