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

**TD no 5**
**Générateur à un pas**

Pour toute question pendant le TD, commencez par lire le résumé de cours à la fin de la feuille.

**Exercice 1 [ Générateur à un pas ]**

Supposons que nous voulions générer une suite d'entiers $X_0$, $X_1$, ..., tels que $0 \leq X_n < m$. Soit $f(x)$ un fonction telle que $0 \leq x < m$ implique $0 \leq f(x) < m$. Considérons un suite formée selon la règle $X_{n+1} = f(X_n)$. (Un exemple est MSN).

1) Pourquoi cette suite est ultimement périodique, c'est-à-dire qu'il existe des nombres $\lambda$ et $\mu$ pour lesquels $X_0, X_1, ..., X_\mu, ..., X_{\mu+\lambda-1}$ sont distinctes, mais $X_{n+\lambda} = X_n$ quand $n \geq \mu$.

2) Que signifie le cas où $\mu = 0$ et $\lambda = m$ ?

3) Donner un exemple où $\mu = m - 1$ et $\lambda = 1$.

**Exercice 2 [ Orbite et paramètre d'un générateur congruentiel linéaire ]**

Donner les orbites et les paramètres des générateurs suivants :

$$x_0 = 1; x_{n+1} = 2x_n + 5 \bmod 17$$

$$x_0 = 0; x_{n+1} = x_n + 6 \bmod 18$$

**Exercice 3 [ Période maximale et Pieuvre ]** Les générateurs suivants sont-ils de période maximale (utilisez le théorème 1) ? Vérifiez votre réponse en donnant leur pieuvre.

$$f(x) = x + 7 \bmod 11$$
$$f(x) = 7x + 5 \bmod 12$$

Une pieuvre est-elle toujours connexe ?

**Exercice 4 [ Algorithmes de Brent et Floyd]**

1 Combien de valeurs est-il nécessaire de stocker en mémoire quand on utilise ces deux algorithmes ?

2 Ecrire en pseudo-code l'un des deux algorithmes.

**Exercice 5 [ GCL particulier ($a = 1$) ]**

Donnez un critère de maximalité plus simple que celui du théorème1 dans le cas où $a = 1$.

**Exercice 6 [ Générateur à un pas ]**

On se place dans le cadre de l'exercice 1. Montrer qu'il existe un $n > 0$ tel que $X_n = X_{2n}$ ; et que le plus petit n qui convient est tel que $\mu \leq n \leq \mu + \lambda$. Montrer de plus que cette valeur est unique, c'est-à-dire que si $X_n = X_{2n}$ et $X_r = X_{2r}$, alors $X_r = X_n$.

**Résumé de cours**

**Définition 0.1** *Soit $F$ un ensemble fini, $x_0 \in F$ et $f : F \to F$ une application. On appelle générateur (à un pas) le triplet $(F, f, x_0)$.*

Les caractéristiques d'un générateur sont données par la proposition démontrée en exercice 1. Les *paramètres du générateur sont $\mu$ et $\lambda$. L'*orbite est l'ensemble des valeurs de la suite $\{x_j\}_{0 \leq j \leq \mu+\lambda-1}$. La *pieuvre* du générateur est l'ensemble des *orbites*. On la représente sous la forme d'un graphe.

On peut déterminer les paramètres de la suite sans stocker en mémoire toutes les valeurs en utilisant les algorithmes de Brent et Floyd.

**Définition 0.2** *On appelle générateurs congruentiels linéaires (GCL) les générateurs à un pas définis par $x_0; x_{n+1} = ax_n + b \bmod m$.*

**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 $a = 1\ [4]$.*