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

TD no 2
MSN, Arithmétique modulaire, Récurrence linéaire et Méthode congruentielle linéaire

Exercice 1 [La méthode MSN.]
Quel nombre suit 1010101010 (nombre décimal) en utilisant la méthode MSN ?

Exercice 2 [Les problèmes de la méthode MSN.]

- *Etude de la MSN dans le cas des nombres décimaux de 2 chiffres :*

  Calculer la suite si on commence par : 09, 43, 10, 29, 24.

  Que peut-on deviner sur cette méthode dans ce cas ?

- *Désavantage de la MSN sur un nombre à 2n chiffres* :

  Montrer que si la suite a un élément dont les n chiffres les plus significatifs sont nuls, alors les éléments suivants seront de plus en plus petits jusqu'à arriver à 0.

Exercice 3 [Arithmétique modulaire.]

- 1) Prouvez que :

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

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

- 2) Soit n un entier et $S(n)$ la somme des chiffres $a_0, ...a_N$ de l'écriture décimale de $n = a_N...a_0 = \Sigma_{0 \leq k \leq N} a_k 10^k$.

  a) Comparer $n \bmod 3$ et $S(n) \bmod 3$; en déduire un critère de divisibilité par 3.

  b) Comparer $nmod9$ et $S(n) \bmod 9$; en déduire un critère de divisibilité par 9.

  c) Donner un critère de divisibilité par 11 en étudiant les puissances de 10 modulo 11.

Exercice 4 [Résoudre une récurrence linéaire.]
Déterminer l'ensemble des solutions des relations de récurrence suivantes :

- 1) $u_n = 4u_{n-1}$

- 2) $u_n = 2u_{n-1} + 3u_{n-2}$

- 3) $u_n = u_{n-1} + 2u_{n-2} + 3$
- 4) $u_n = au_{n-1} + b$ avec a et b réels.

Exercice 5 [La Méthode congruentielle linéaire.]

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).

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

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

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

b) 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 $X_r = X_n$.