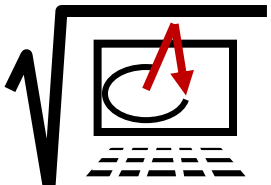
100 OUTILS POUR LES MATHS :

Nombres pseudo-aléatoires



d'après un travail de Rhydwen Volsik

Le hasard a aujourd'hui une importance capitale, aussi bien en cryptographie, en physique, en statistique, en informatique, ou tout simplement dans les jeux…

Un ordinateur permet de générer une suite de nombres qui semblent aléatoires (on parle de suite pseudo-aléatoire). Le problème le plus évident est que l'ordinateur, exécutant des lignes de codes, agit dans une démarche préétablie par son programmeur.

La difficulté est donc d'utiliser des algorithmes les moins prévisibles possible. Toute une série de tests statistiques ont été créés pour tester le « degré d'aléatoire » d'une suite. Nous allons nous contenter de vérifier « à l'œil nu », sur quelques exemples, si la suite obtenue semble aléatoire.

1. Générateur congruentiel linéaire

Un générateur congruentiel linéaire est un générateur de nombres pseudo-aléatoires dont l'algorithme (introduit en 1948 par D.H. Lehmer : http://serge.mehl.free.fr/chrono/Lehmer.html) est basé sur des congruences et une fonction linéaire.

On considère la suite $(\mathbf{X_n})_{\mathbf{n} \geq 0}$ définie par : $\mathbf{X_{n+1}} \equiv \mathbf{a}\,\mathbf{X_n} + \mathbf{b}\ (\mathbf{m})$

$\mathbf{X_0}$ est appelé la « graine » du générateur de nombres aléatoires.

Ce travail est à faire sur tableur (en mode A1).

1. La colonne A a pour titre « **n** » ; y écrire les entiers de 0 à 300.
2. Taper les lettres **a**, **b** et **m** dans les cellules E1, E2 et E3, puis les valeurs 3, 5 et 79 dans les cellules F1, F2 et F3.
3. Remplir la colonne B avec les valeurs de $\mathbf{X_n}$ en prenant $\mathbf{X_0} = 0$. (faire références aux valeurs de **a**, **b** et **m** ; la fonction MOD renvoie le reste d'une division euclidienne)

   Appeler l'examinateur pour une vérification

4.1 À quel intervalle les valeurs de la suite $(\mathbf{X_n})$ appartiennent - elles ?
Quelle est la période de cette suite ?

4.2 Mêmes questions avec $\mathbf{m} = 83$.

4.3 Entre ces deux choix de valeurs de **m**, lequel est le plus intéressant pour générer une suite pseudo-aléatoire ?

5. Dans cette question $\mathbf{a} = 25$, $\mathbf{b} = 16$ et $\mathbf{m} = 256$.

5.1 Que pensez - vous de la suite obtenue si $\mathbf{X_0} = 10$?

5.2 Et si $\mathbf{X_0} = 11$? si $\mathbf{X_0} = 12$?

D. Knuth (http://fr.wikipedia.org/wiki/Donald_Knuth) a déterminé les critères que doivent remplir **a**, **b** et **m** pour obtenir une suite de période **m** :

- **b** et **m** doivent être premiers entre eux ;
- **a** – 1 doit être un multiple de **p** pour tout nombre premier **p** diviseur de **m** ;
- **a** – 1 doit être un multiple de 4 si **m** est un multiple de 4.

6. Vérifier que les nombres $\mathbf{a} = 31\,415\,821$, $\mathbf{b} = 1$ et $\mathbf{m} = 100\,000\,000$ vérifient les critères ci - dessus.
Peut - on dire que la suite obtenue est pseudo-aléatoire ?

7. Dans cette question $\mathbf{a} = 137$, $\mathbf{b} = 187$ et $\mathbf{m} = 2^8$

7.1 Vérifier que ces nombres vérifient les critères ci - dessus (vous pourrez tester la suite avec différentes valeurs pour $\mathbf{X_0}$)

7.2 Comment faire pour obtenir dans la colonne C une suite de nombres pseudo-aléatoires appartenant à l'intervalle [0 ; 1[?
Faire afficher 9 chiffres après la virgule, comme sur la calculatrice.

Appeler l'examinateur pour une vérification

2. Comment « casser » un GCL

Théorie, dans le cas où m *est connu*

On sait que la suite a été obtenue par la formule $\mathbf{X_{n+1}} \equiv \mathbf{a}\,\mathbf{X_n} + \mathbf{b}\ (\mathbf{m})$ et on a trois valeurs $\mathbf{X_0}$ $\mathbf{X_1}$ et $\mathbf{X_2}$ de la suite.

Posons $\mathbf{Y_1} = \mathbf{X_1} - \mathbf{X_0}$ et $\mathbf{Y_2} = \mathbf{X_2} - \mathbf{X_1}$.

1. Montrer que $\mathbf{Y_2} \equiv \mathbf{a}\,\mathbf{Y_1}\ (\mathbf{m})$.
2. On suppose que $\mathbf{Y_1}$ est premier avec **m**.

   a) Montrer qu'il existe un entier relatif **u** tel que $\mathbf{Y_1}\,\mathbf{u} \equiv 1\ (\mathbf{m})$.

   b) Montrer que $\mathbf{Y_2}\,\mathbf{u} \equiv \mathbf{a}\ (\mathbf{m})$.

   c) Exprimer **b** en fonction de **a**, $\mathbf{X_0}$ et $\mathbf{X_1}$.

Exemple

Déterminer **a** et **b** sachant que $\mathbf{m} = 1\,023$ et connaissant le début de la séquence :
97 ; 188 ; 235 ; 293 ; 604 ; 596 ; 412 ; …