TD N#01 : Génération des Nombres Pseudo-aléatoires

Exercice 01

1. Proposez une procédure expérimentale qui permet de générer des nombres aléatoires dans l'intervalle [0,1) avec une précision de deux décimales, à partir d'un **phénomène physique**.

2. Décrivez étape par étape la méthode de conversion de l'observation physique en un nombre numérique compris entre 0 et 1.

3. Indiquez dans quel type de contexte il est pertinent d'utiliser un TRNG plutôt qu'un PRNG classique.

Exercice 02

- Déterminez **la période maximale théorique** d'un générateur de type carré médian, en fonction de la longueur en chiffres de la graine initiale.

- Soient les graines: $X_0 = 3792$, $X_0 = 6759$

1. En utilisant la méthode du carré médian, générez les suites de nombres pseudo-aléatoires associées à chacune des graines fournies.
2. Pour chaque graine, identifiez la période du générateur.

- Soient les graines: $X_0 = 0100$, $X_0 = 7600$, $X_0 = 2500$, $X_0 = 3333$, $X_0 = 1325$, $X_0 = 1275$, $X_0 = 50$

1. Déterminez la période obtenue pour chacune de ces graines.
2. Expliquez pourquoi un générateur utilisant la méthode du carré médian peut rapidement entrer dans des cycles courts, ou dégénérer vers zéro, conduisant à une séquence constante.
3. Proposez et justifiez des stratégies permettant d'augmenter la période ou d'améliorer la qualité statistique de ce type de générateur.

Exercice 03

1. Soient $X_0 = 27$, $a = 8$, $c = 47$, et $m = 100$. Utilisez la méthode congruentielle linéaire pour générer une séquence des entiers aléatoires à deux chiffres ainsi que les nombres aléatoires correspondants.
2. Rencontre-t-on un problème dans l'exercice précédent si $X_0 = 0$?
3. Soient $X_0 = 117$, $a = 43$, et $m = 1000$. Utilisez la méthode congruentielle multiplicative pour générer une séquence des entiers aléatoires à trois chiffres.
4. Utilisez la méthode congruentielle mixte pour générer une séquence de nombres aléatoires à deux chiffres, avec : $X_0 = 37$, $a = 7$, $c = 29$, et $m = 100$.
5. Utilisez la méthode congruentielle mixte pour générer une séquence de nombres aléatoires à deux chiffres compris entre 0 et 24, avec : $X_0 = 13$, $a = 9$, et $c = 35$.
6. Déterminez si ces générateurs congruentiels linéaires peuvent atteindre une période maximale ; indiquez également les restrictions sur X_0 nécessaires pour obtenir cette période.

$a = 2814749767109; c = 59482661568307\ ;\ m = 248$	$a = 69\,069;\ c = 0;\ m = 232$
$a = 4951;\ c = 247;\ m = 256$	$a = 6507;\ c = 0;\ m = 1024$

Exercice 04

L'Ecuyer [1988] propose un générateur combinant trois générateurs multiplicatifs, définis par les paramètres suivants :

$$a_1 = 157, m_1 = 32363, a_2 = 146, m_2 = 31727, a_3 = 142, et\ m_3 = 31657.$$

La période de ce générateur combiné est d'environ $8 * 10^{12}$.

- Générez cinq nombres aléatoires à l'aide de ce générateur combiné, en utilisant comme graines initiales : $X_{1,0} = 100, X_{2,0} = 300\ et\ X_{3,0} = 500$

Exercice 05

Considérons un LFSR de Fibonacci de 5 bits avec le polynôme de rétroaction : $P(x) = x^5 + x^3 + 1$, avec:

1. Soit l'état initial [1, 0, 0, 0, 0]. Générez tous les états successifs jusqu'au retour à l'état initial.
2. Est-ce la période maximale $(2^5 - 1)$?
3. Que se passe-t-il avec l'état initial [0, 0, 0, 0, 0] ?
4. Quelle transformation applique-t-on à la sortie binaire d'un LFSR pour obtenir une variable uniforme [0,1) ?

Rappel:

- ✧ Le nouveau bit est calculé par XOR des bits indiqués dans les prises (taps).
- ✧ Le **bit de gauche** (MSB) correspond à la position 1.
- ✧ Le décalage se fait vers la droite, et le nouveau bit est ajouté à gauche.

Exercice 06

- Considérez un XORShift 8-bit avec les paramètres suivants : décalage à gauche de 3 bits, décalage à droite de 5 bits, décalage à gauche de 7 bits

1. En partant de la graine $X_0 = 202$ (en décimal), calculez les premiers termes de la suite.

- Pour un XORShift 32-bit quelconque :

1. Démontrez que la période ne peut pas dépasser $(2^{32} - 1)$
2. Donnez une condition nécessaire sur les paramètres de décalage pour obtenir une période maximale

Exercice 07

Vérifiez, au seuil de confiance de 99 %, l'uniformité et l'indépendance de la suite de nombres suivante à l'aide du test de Kolmogorov–Smirnov (K–S) et du test d'auto-corrélation.

0.594, 0.928, 0.515, 0.055, 0.507, 0.351, 0.262, 0.797, 0.788, 0.442, 0.097, 0.798, 0.227, 0.127, 0.474, 0.825, 0.007, 0.182, 0.929, 0.852.

Exercice 08

Considérons la suite des nombres pseudo-aléatoires suivante:

0.2379	0.7551	0.2989	0.247	0.3237	0.2972	0.8469	0.4566	0.6146	0.6723
0.9496	0.2268	0.8699	0.9084	0.5649	0.3045	0.6964	0.1709	0.3387	0.9804
0.1246	0.842	0.6557	0.9672	0.3356	0.3525	0.8075	0.9462	0.9583	0.3807
0.1489	0.5480	0.9537	0.9376	0.8364	0.5095	0.4047	0.9058	0.3795	0.6242
0.5195	0.6545	0.1117	0.3258	0.8589	0.6536	0.3427	0.6653	0.7864	0.5824

1. Vérifiez, au seuil de confiance de 95%, l'hypothèse selon laquelle les nombres générés suivent une loi uniforme U(0,1) à l'aide du test du khi-deux χ^2 avec 10 intervalles.
2. Vérifiez, au seuil de confiance de 95%, l'hypothèse d'indépendance des nombres générés à l'aide du test des séquences fondé sur la comparaison des valeurs successives.