Exercices
Semaine 12

Cours Turing

1 Générateur de nombres aléatoires de Lehmer

Dans cet exercice, nous nous intéressons à simuler des séquences de nombres (pseudo-)aléatoires générées comme suit. Soit $N \geq 1$ un nombre entier positif et A, X_0 deux nombres entiers compris entre 2 et $N-1$. On pose

$$X_{n+1} = (A \cdot X_n) \pmod N \quad \text{pour } n \geq 0$$

Première partie

a) Ecrivez un programme en Python qui pour des valeurs de N, A et X_0 données, génère une suite de N nombres $X_0, X_1, X_2, \ldots, X_{N-1}$ selon l'algorithme ci-dessus. Dans un premier temps, commencez par de petites valeurs de N.

Affichez la liste des nombres ainsi produits ; pour mieux visualiser le résultat, vous pouvez aussi tracer un graphique grâce aux commandes suivantes :

```
import matplotlib.pyplot as plt
plt.plot(L)
plt.show()
```

où L est la liste des nombres en sortie de votre programme.

b) Jouez un peu avec les paramètres N, A et X_0. Pouvez-vous identifier quelle relation entre A et N garantit que la suite de nombres générée ne devient pas une longue suite de zéros à partir d'un moment donné ?

c) Ecrivez maintenant un programme qui teste si la suite de nombres générée passe par toutes les valeurs possibles comprises entre 1 et $N-1$ avant de revenir à X_0.

Indication : Que devez-vous tester pour vérifier que c'est bien le cas ?

Note : Il n'y a malheureusement pas de relation facile entre A et N permettant de prédire si la séquence générée va effectivement passer par toutes les valeurs possibles ou pas !

Deuxième partie

a) Toujours à l'aide de matplotlib, tracez le graphique en deux dimensions, constitué des points (x, y) tels que

$$x = X_n \quad \text{et} \quad y = X_{n+1} = (A \cdot X_n) \,(\mathrm{mod}\ N)$$

pour n allant de 0 à $N - 1$.

Indication : Ici, il vous faudra constituer deux listes de nombres :

`L1=L[0:N-1]`   et   `L2=L[1:N]`

puis utiliser la commande

```
plt.plot(L1,L2)
```

b) A nouveau, jouez un peu avec les paramètres N, A et X_0, et observez quels graphiques vous obtenez, et lesquels vous semblent correspondre à des séquences les plus aléatoires possible.