Notion de suites
Problème de recherche : le générateur de nombres aléatoires

Pour simuler le hasard (jeux vidéo, simulations, cryptographie), les ordinateurs utilisent des **générateurs pseudo-aléatoires**. L'un des plus simples est défini par

$$u_0 = 1 \qquad \text{et} \qquad u_{n+1} = (5u_n + 3) \ \% \ 16,$$

où a % 16 désigne le reste de la division euclidienne de a par 16 (c'est l'opérateur % de Python). Les termes sont donc des entiers entre 0 et 15.

La mission

1. Calculer à la main u_1, u_2 et u_3.
2. Écrire un programme Python qui affiche les 40 premiers termes. Que constate-t-on ? Au bout de combien de termes la suite se répète-t-elle ?
3. Chaque entier de 0 à 15 apparaît-il ? Peut-on dire pour autant que ce générateur imite bien le hasard ? (On pourra observer la parité des termes.)
4. Un élève propose le générateur $v_0 = 1$ et $v_{n+1} = (4v_n + 3)$ % 16. Qu'en penser ?

Pour aller plus loin

Tester d'autres multiplicateurs à la place de 5 (en gardant +3 et % 16). Lesquels donnent une suite qui prend les 16 valeurs ?

Coups de pouce

Bloqué ? Des indices progressifs sont disponibles en ligne. N'en ouvrir qu'un à la fois, et seulement après avoir cherché !