Générateur de carrés médians

John von Neumann (1903 - 1957)

Les savants utilisent les générateurs de nombres aléatoires pour s'atteler à une grande variété de problèmes, tels que la création de codes secrets, la modélisation du mouvement des atomes et la conduite d'enquêtes rigoureuses. Un générateur de nombres pseudo-aléatoires est un algorithme produisant une séquence de nombres qui simulent les propriétés statistiques des nombres aléatoires.

La méthode des carrés médians, développée par le mathématicien John von Neumann en 1946, est l'un des plus célèbres et des premiers générateurs de nombres aléatoires fondés sur un ordinateur. Le mathématicien commença par un nombre tel que 1946 et l'éleva au carré pour produire 3786916, qui peut s'écrire sous la forme 03786916. Il supprima les quatre chiffres du milieu, 7869, et poursuivit le processus d'élévation au carré et de suppression. Dans la pratique, von Neumann utilisa des nombres à 10 chiffres et appliqua les mêmes règles.

Von Neumann, célèbre pour sa participation à la recherche sur les réactions thermonucléaires qui conduisirent à la bombe à hydrogène, comprit que son approche comportait des failles et que les séquences finiraient par se répéter, mais il fut satisfait de la méthode pour de nombreuses applications. En 1951, von Neumann avertit les utilisateurs de ces procédés : « Quiconque envisage l'emploi de méthodes arithmétiques pour produire des nombres aléatoires est, bien sûr, en état de péché. » Néanmoins, il préféra cette approche aux générateurs matériels de nombres aléatoires, car ceux-ci n'enregistraient pas leurs valeurs et rendaient difficile la répétition de procédures permettant d'identifier les problèmes. Quoi qu'il en soit, von Neumann ne disposait pas d'une mémoire informatique suffisante pour stocker de nombreuses valeurs « aléatoires ». De fait, sa solution, merveilleusement simple, générait les nombres aléatoires sur l'ENIAC à une vitesse cent fois plus rapide que la lecture des nombres sur les cartes perforées.

Les générateurs de nombres aléatoires les plus récents et les plus utiles utilisent la méthode de congruence linéaire de la forme $X_{n+1} = aX_n + c$ (mod. m). Ici, $n \geqslant 0$, a est le multiplicateur, m le module, c l'incrément et X_0 la valeur de départ. Le générateur de nombres aléatoires appelé *Mersenne Twister*, développé en 1997 par Makoto Matsumoto et Takuji Nishimura, est aussi adapté à nombre d'applications actuelles.

VOIR AUSSI Dés (3000 av. J.-C), Aiguille de Buffon (1777), L'émergence des machines aléatoires (1938) et ENIAC (1946).

John von Neumann dans les années 1940. Von Neumann développa la méthode des carrés médians, célèbre générateur de nombres aléatoires fondé sur un ordinateur.

Source :
1946 Générateurs de carrés médians
Le Beau Livre des Maths De Pythagore à la 57e dimension, Clifford A. Pickover, Dunod.