Le générateur pseudo-aléatoire **RANDU** est considéré comme un mauvais générateur pseudo-aléatoire en raison de plusieurs défauts mathématiques qui entraînent des corrélations non désirées dans les séquences de nombres qu'il produit. Ces défauts rendent les résultats moins aléatoires et peu fiables pour de nombreuses applications. Voici quelques raisons spécifiques qui expliquent pourquoi RANDU est problématique :

1. Corrélations linéaires dans les séquences tridimensionnelles

L'un des défauts les plus notoires de RANDU est la forte corrélation entre les triplets successifs générés. Lorsqu'on représente les nombres générés par RANDU dans un espace tridimensionnel, les points tendent à se regrouper sur des plans distincts au lieu d'être uniformément répartis dans l'espace. Cela signifie que les nombres générés ne sont pas vraiment "aléatoires", mais suivent des motifs réguliers.

Cette propriété a été analysée et démontrée par des chercheurs dans les années 1960, montrant que RANDU ne parvient pas à produire une distribution uniforme en trois dimensions, ce qui est crucial dans de nombreuses applications scientifiques et de simulation.

2. Faible qualité statistique

RANDU repose sur un générateur congruentiel linéaire de la forme :

$$X_{n+1} = (65539 \times X_n) \bmod 231$$

Ce type de générateur est simple à mettre en œuvre, mais le choix des paramètres (65539 et 231) est problématique. En particulier, le multiplicateur 65539 est mal choisi, ce qui contribue aux mauvaises propriétés statistiques du générateur. Cela conduit à une faible période (la longueur avant que la séquence de nombres ne commence à se répéter) et des problèmes de distribution non uniforme.

3. Longue période, mais dépendance cyclique

Bien que RANDU puisse générer une longue séquence avant de répéter des valeurs (ce qu'on appelle la "période"), les corrélations internes dans cette séquence rendent cette propriété inutile. Même si la période théorique peut sembler acceptable, la dépendance cyclique et les corrélations dans les sous-séquences affectent la qualité du générateur.

4. Inadéquat pour les simulations numériques

RANDU a été utilisé dans les premiers jours de l'informatique pour des simulations Monte Carlo, mais en raison de ses corrélations et de sa distribution non uniforme, il a conduit à des résultats incorrects dans certains cas. Les simulations nécessitent des nombres aléatoires de haute qualité, et l'utilisation de RANDU pour ces tâches peut entraîner des biais ou des résultats faussés.

5. Obsolète

Depuis la création de RANDU, de nombreux autres générateurs pseudo-aléatoires de bien meilleure qualité ont été développés, comme le Mersenne Twister ou le générateur congruentiel linéaire amélioré (comme le **Lehmer RNG**). Ces générateurs produisent des séquences avec des propriétés statistiques bien plus solides, une meilleure distribution et des périodes bien plus longues, sans les corrélations problématiques de RANDU.

Conclusion

En résumé, **RANDU** est un mauvais générateur pseudo-aléatoire principalement en raison de ses corrélations non désirées, de ses mauvaises propriétés statistiques, et de la mauvaise qualité de la "randomisation" des nombres générés. Ces faiblesses rendent ce générateur inadapté à de nombreuses applications nécessitant des nombres aléatoires de qualité, comme les simulations numériques et les études statistiques. Aujourd'hui, il est considéré comme un exemple classique de ce qu'il ne faut pas faire dans la conception de générateurs pseudo-aléatoires.