# CM5 Nombres aléatoires

Les systèmes informatique sont intrinséquement déterministes, le hasard est éliminé. Pourtant, dans certaines applications on a besoin des valeurs aléatoires. Quelles sont ces applicatins, qu'est-ce que c'est le hasard en informatique, comment on le génère sont le questions auquelles on se propose de répondre dans ce chapitre.

## 1 Nécessité du hasard

1. *Les simulations*: pour reproduire des phénomènes aléatoires;
2. en *cryptographie*, où, pour pour cacher l'information on la « mélange » avec des valeurs aléatoires;
3. en *théorie de l'information* (au sense de Kolmogorov), ou les suites au plus fort contenu en information sont celles dificilement prédictibles.

## 2 Qu'est-ce que c'est un nombre aléatoire

Les suites suivantes sont-elles aléatoires?

- 01234567890123
- 31415926535897
- 82845904523536
- **Hasard faible**: *uniformité* (bon mélange). Peut être généré par des algorithmes rapides. Utile en simulation.
- **Hasard moyen**: Imprévisible pour un observateur ayant des moyens de calcul raisonnables. Peut être produit par des algorithmes efficaces. Utile en cryptographie.
- **Hasard fort**: Imprévisibilité totale. Peut être produit par des moyens physiques. Utile en cryptographie et théorie de l'information. Voir: `http://lavarand.sgi.com/`

## 3 Génération

### 3.1 Générateur naïf

### 3.2 Générateur congruentiel

On se donne les entiers $M$, $a$ et $b$, ainsi qu'une « graine » $x_0$. On calcule itérativement $x_n$ par

$$x_{n+1} = (a \times x_n + b) \bmod M$$

avec $x_n \in \{0, 1, \ldots, M-1\}$ et on calcule $u_n \in [0, 1[$ par

$$u_n = \frac{x_n}{M}$$

L'expression formelle d'une intégrale peut ne pas être (facilement) calculable. Un moyen d'en trouver une valeur approcheée (autres que des méthodes numeriques *traditionelles*) est la méthode de Monte-Carlo.

## 5