Générateur de nombres pseudo-aléatoires
Générateur congruentiel linéaire

$$\mathbf{X_{n+1} = a\,X_n + c \bmod m}$$

a : multiplicateur
c : incrément
m : module
X_0 : seed (graine)

À chaque nouvelle graine correspond une nouvelle suite.
Trouver a,c et m pour faire un « bon » générateur aléatoire n'est pas simple …
Ex : a = 25, *c* = 16, *m* = 256 et X0 = 10 donne la suite 10 10 10 ...

Générateur de nombres pseudo-aléatoires
Générateur congruentiel linéaire

En C, il existe un générateur de nombres aléatoires donné par la fonction **rand();**
rand() génère un nombre aléatoire compris en 0 et la constante RAND_MAX, définie dans stdlib.h (la valeur de RAND_MAX est 32767)

L'instruction : srand(time(0)) ; permet d'initialiser le générateur. time(0) renvoie le nombre de secondes entre l'instant où elle est appelée et le 01/01/1970.

$$\bar{x} = \frac{1}{n}\sum_i x_i \qquad \sqrt{\frac{1}{n}\sum_i (x_i - \bar{x})^2}$$

(population entière)