Random Numbers

Random numbers are ubiquitous in physics – thermodynamics, radioactivity, particle collision and everything in between

Two basic methods to generate random number with varying degree of randomness

- *True* RNG
- *Pseudo* RNG

True RNG : uses natural phenomenon like coin flipping, dice rolling, radioactive decay, thermal noise, atmospheric radio-noise etc.

`Requires post-processing, slow` $\Rightarrow$ `not useful for regular usage`

Pseudo RNG : based on algorithms, generated iteratively

`Deterministic, finite sequence length, correlated but extremely fast and portable`

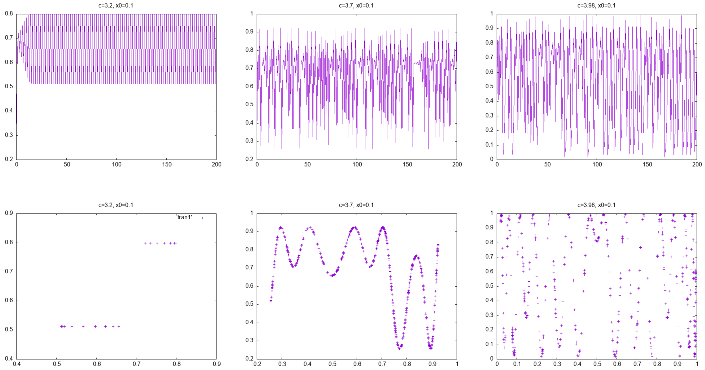
Sequence length can be made veryyy long by proper choice of parameters

Example : a quick and dirty pRNG

$$x_{i+1} = c\, x_i\, (1 - x_i)$$

x_0 is the seed which defines the random sequence.

An exercise with $x_0 = 0.1$ and $c = 3.2, 3.7, 3.98$



Linear Congruential Generator

One of the oldest and most common choice of pRNG having a uniform distribution,

$$x_{i+1} = \left(ax_i + c\right) \mathrm{mod}\, m \quad \equiv \quad x_{i+1} = \mathrm{remainder}\left(\frac{ax_i + c}{m}\right)$$

The m determines the period of the generator *i.e.* produces random numbers between 0 and $m-1$, whereas x_i/m yields randoms in the interval [0,1].

- m is typically chosen to be 2^{32}
- a is *multiplier* and usually $0 < a < m$. Numerical Recipes uses $a = 1664525$ and gcc uses $a = 1103515245$
- c is *increment* and usually $0 < c < m$. Numerical Recipes uses $c = 1013904223$ and gcc uses $c = 12345$

LCG : Hull-Dobell theorem

LCG is extremely sensitive to a, c, x_0, m. Particularly, a has to be chosen with great care else short / very short periodicity will set in.

Hull-Dobell theorem : LCG has a period m *iff* $c \neq 0$ and

1. c is coprime to m,
2. $a - 1$ is a multiple of p for every prime p dividing m
3. $a - 1$ is a multiple of 4, if m is a multiple of 4.

LCG works well for m having many repeated prime factors p, such as power of 2. But if m are square-free integer (having no n^2 factor for any n), then only $a = 1$ is allowed and it is a very bad pRNG.

$c = 0$ corresponds to Lehmer, Park-Miller pRNG

$$x_{i+1} = ax_i \cdot \bmod m$$

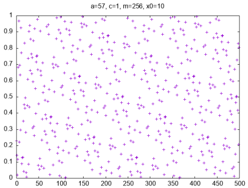
m can be a prime or a prime just less than a power of 2 (Mersenne primes $2^{31} - 1$, $2^{61} - 1$ etc.) or can be a simple power of 2.

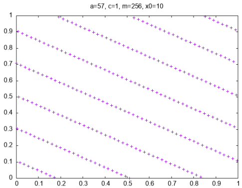
A few exercise in **LCG**

$a = 27,\ c = 11,\ m = 54,\ x_0 = 10$ (Ugly choice) :

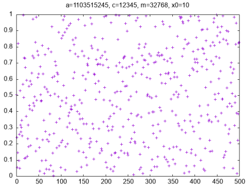
$0.204,\ 0.704,\ 0.204,\ 0.704,\ \ldots$

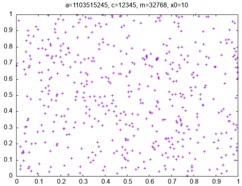
$a = 57,\ c = 1,\ m = 256,\ x_0 = 10$ (Bad choice)





$a = 1103515245,\ c = 12345,\ m = 32768,\ x0 = 10$ (Good choice)

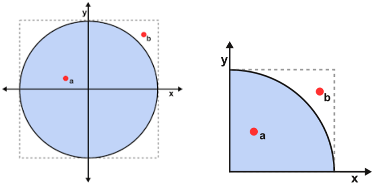




Application : Determination of π

Consider a unit circle $r = 1$ centered at origin $\Rightarrow$ area $= \pi$.

Put unit circle in a square of side $2r = 2$.
Confine to first quadrant $\Rightarrow$ area $= \pi/4$.



Randomly generate points (x, y) and check for inside points $x^2 + y^2 \leq 1$. Then over LARGE number of trials

$$\frac{\text{circle area}}{\text{square area}} \approx \frac{\text{total inside}}{\text{total trials}} \Rightarrow \pi \approx 4\times\frac{\text{total inside}}{\text{total trials}}$$