For a large and important class of algorithms, we sample a problem domain and then use statistical analysis over those samples to generate an answer. These are often called Monte Carlo algorithms.

For Monte Carlo algorithms to work, the random samples must be distributed according to the statistics required by the problem and each sample must be unpredictable given knowledge of other samples.

The best we can do on a computer is to produce numbers that appar to be random, that is, numbers that lack correlations between them, or other features that would make the numbers predictable. We call these Pseudo-Random numbers.

Pseudo-random number generators are usually based on iterative algorithms, such as $x_{i+1} = f(x_i)$ or $x_{i+k} = f(x_i, ..., x_{i+k-1})$, where x_0 or $x_0, ..., x_{k-1}$ is the seed of the generator. It should be clear that the numbers x_i obtained using such an iterative algorithm are neither random nor independent from each other, but for many practical applications everything works "as if" thesenumbers were truly indipendent and identically distributed (iid) random quantities.

Whether a given random number generator is "good enough" for this cheat to be trustworthy is a non trivial problem.

Simple and very well studied pseudo-random number generators are linear congruential generators, by use of which natural numbers in $[0, m)$ are generated by iterating

$$x_{n+1} = (ax_n + c) \; mod \; m \tag{1}$$

where $0 \leq x_0 < m$ is the random seed, $0 < m$ is the modulus, $0 < a < m$ is the multiplier and $0 \leq c < m$ is the increment. There are at most m values that can be obtained by iterating Eq. ....

Let's now explore Monte Carlo methods and pseudo random number generators with a classic problem. The value of π can be estimated by uniformly sampling the area of a square with side $L = 2 * r$ with a circle enclosed inside the square of radius r. The area of the square is $A_s = 4 * r^2$, the area of the circle is $A_c = \pi * r^2$ and their ratio is $P = \frac{A_c}{A_s} = \frac{\pi}{4}$. You can think of this as randomly and uniformly throwing darts on a digital dart board. The chance of a dart falling in the circle is P, and thus proportional to π.