

Linear Congruence method for generating Pseudo Random Numbers

Linear Congruential Method is a class of Pseudo Random Number Generator (PRNG) algorithms used for generating sequences of random-like numbers in a specific range. This method can be defined as:

$$X_{i+1} = aX_i + c \text{ mod } m$$

where,

X_i is the sequence of pseudo-random numbers

m , (> 0) the modulus

a , ($0, m$) the multiplier

c , ($0, m$) the increment

x_0 , $[0, m)$ – Initial value of sequence known as seed

m , a , c , and x_0 should be chosen appropriately to get a period almost equal to m .