

1.-The linear congruential method produces a sequence of integers between zero and $m-1$ using the relationship:

$$X_{i+1} = (aX_i + c) \bmod m, \quad i = 0, 1, 2, \dots$$

- The initial value X_0 is called the seed;
- a is called the constant multiplier;
- c is the increment
- m is the modulus

When $c \neq 0$ the form is called the mixed congruential method; When $c = 0$, the form is known as the multiplicative congruential method.

2.-

Handwritten notes on grid paper:

$$X_{i+1} = (aX_i + c) \bmod m \quad i = 0, 1, 2, \dots, [0, m-1]$$

Example with $m=2$, $a=3$, $c=1$:

$$X_0 = 1$$

$$X_1 = (3(1) + 1) \bmod 2 = 0$$

$$X_2 = (3(0) + 1) \bmod 2 = 1$$

$$X_3 = (3(1) + 1) \bmod 2 = 0$$

Conditions for $m > 0$:

$$a > m, \quad c < m, \quad X_0 < m$$

Interval: $[0, 1]$

Parameters: $m=2, a=3, c=1, X_0 < m$

3.- What is the best way to choose the parameters for the generator? (The seed, the multiplier, the increment and the modulus)

The interval will be $[0, m-1]$

$m > 0$ and $a < m, c < m, X < m$

It has full period if and only if the following three conditions hold (Hull and Dobell, 1962):

1. The only positive integer that (exactly) divides both m and c is 1
2. If q is a prime number that divides m , then q divides $a-1$
3. If 4 divides m , then 4 divides $a-1$

- For m a power 2, $m=2^b$, and $c \neq 0$

Longest possible period $P=m=2^b$ is achieved if c is relative prime to m and $a=1+4k$, where k is an integer

- For m a power 2, $m=2^b$, and $c=0$

Longest possible period $P=m/4=2^{b-2}$ is achieved if the seed X_0 is odd and $a=3+8k$ or $a=5+8k$, for $k=0, 1, \dots$

- For m a prime and $c=0$

Longest possible period $P=m-1$ is achieved if the multiplier a has property that smallest integer k such that $ak-1$ is divisible by m is $k = m-1$

4.-

④ $m=7$ $a=15$ $c=5$ $x_0=3$

1: Only int that divides m and C is 1
 2: 7 divides m and $a=1$
 3: Period should be 7

$x_0 = 3$
 $x_1 = [15(3) + 5] \bmod 7 = (50) \bmod 7 = 2$
 $x_2 = 6$
 $x_3 = 4$
 $x_4 = 2$
 $x_5 = 0$
 $x_6 = 5$
 $x_7 = 3$
 $x_8 = 1$
 $x_9 = 6$

period = 7

$M=7$ period = 7 (with the conditions established before meet)

$x_{i+1} = (a x_i + c) \bmod m \quad i = 0, 1, 2, \dots, [0, m-1]$

$x_0 = 1$
 $x_1 = (3(1) + 1) \bmod 2 = 0$
 $x_2 = (3(0) + 1) \bmod 2 = 1$
 $x_3 = (3(1) + 1) \bmod 2 = 0$

$m > 0$
 $a > m$
 $c < m$
 $x_0 < m$

$m = 2$
 $a = 3$
 $c = 1$
 $x_0 < m$
 $\frac{1}{2}$

$M=2$ period = 2

https://www.mi.fu-berlin.de/inf/groups/ag-tech/teaching/2012_SS/L_19540_Modeling_and_Performance_Analysis_with_Simulation/06.pdf