Linear Congruential Generator (LCG)

$$R_{i+1} = (aR_i + c) \bmod m \quad \text{for } i = 0, 1, 2, \ldots \tag{2.1}$$

where R_0 is called the seed of the sequence, a *is called the constant multiplier,* c *is called the increment, and* m *is called the modulus.* (m, a, c, R_0) *are integers with* $a > 0$, $c \geq 0, m > a, m > c, m > R_0$, *and* $0 \leq R_i \leq m - 1$.

To compute the corresponding pseudorandom uniform number, we use

$$U_i = \frac{R_i}{m} \tag{2.2}$$

The mod operator is defined as:

$$\begin{aligned} z &= y \bmod m \\ &= y - m\left\lfloor \frac{y}{m} \right\rfloor \end{aligned}$$

where $\lfloor \cdot \rfloor$ is the floor operator,

How it is computed when y=17 **and** m=3 **?**

$$\begin{aligned} z &= 17 \bmod 3 \\ &= 17 - 3\left\lfloor \frac{17}{3} \right\rfloor \\ &= 17 - \lfloor 5.\overline{66} \rfloor \\ &= 17 - 3 \times 5 = 2 \end{aligned}$$

EXAMPLE:

Consider an LCG with parameters (m = 8, a = 5, c = 1, R0 = 5). Compute the first nine values for Ri and Ui from the defined sequence. how to compute using the mod operator.

In our example
m = 8
a = 5
c = 1
R_0 = 5

$$R_1 = (5R_0 + 1) \bmod 8 = 26 \bmod 8 = 2 \Rightarrow U_1 = 0.25$$
$$R_2 = (5R_1 + 1) \bmod 8 = 11 \bmod 8 = 3 \Rightarrow U_2 = 0.375$$
$$R_3 = (5R_2 + 1) \bmod 8 = 16 \bmod 8 = 0 \Rightarrow U_3 = 0.0$$
$$R_4 = (5R_3 + 1) \bmod 8 = 1 \bmod 8 = 1 \Rightarrow U_4 = 0.125$$
$$R_5 = 6 \Rightarrow U_5 = 0.75$$
$$R_6 = 7 \Rightarrow U_6 = 0.875$$
$$R_7 = 4 \Rightarrow U_7 = 0.5$$
$$R_8 = 5 \Rightarrow U_8 = 0.625$$
$$R_9 = 2 \Rightarrow U_9 = 0.25$$

Theorem: (LCG Full Period Conditions)

An LCG has full period if and only if the following three conditions hold:

1. The only positive integer that (exactly) divides both m and c is 1 (i.e., c and m have no common factors other than 1).
2. If q is a prime number that divides m then q should divide (a − 1) (i.e., (a − 1) is a multiple of every prime number that divides m).
3. If 4 divides m, then 4 should divide (a − 1) (i.e., (a − 1) is a multiple of 4 if m is a multiple of 4).

EXAMPLE:

To apply the theorem, you must check if each of the three conditions holds for the generator.

m = 8 , a = 5 , c = 1

Cond-1. c and m have no common factors other than 1:

factors of m = 8 are (1, 2, 4, 8), since c = 1 (with factor 1) condition 1 is true.

Cond-2. (a − 1) is a multiple of every prime number that divides m:

The first few prime numbers are (1, 2, 3, 5, 7). The prime numbers, q, that divide m = 8 are (q = 1, 2). Since a = 5 and (a − 1) = 4, clearly q = 1 divides 4 and q = 2 divides 4. Thus, condition 2 is true.

Cond. 3: If 4 divides m, then 4 should divide (a − 1):

Since m = 8, clearly 4 divides m. Also, 4 divides (a − 1) = 4. Thus, condition 3 holds.

Exercise:

Analyze the following LCG:

$$x_i = (11\, x_{i-1} + 5)\ mod\ 16$$

What is the maximum possible period length for this generator? Does this generator achieve the maximum possible period length? Justify your answer.