Problem 32

Ryan Burmeister

February 15, 2016

1)

$$x_i \leftarrow ax_{i-1} mod m$$
$$x_{-3} = 4, m = 7, a = 3$$
$$x_{-2} = 3(4) mod 7 \quad x_{-2} = 5$$
$$x_{-1} = 3(5) mod 7 \quad x_{-1} = 1$$
$$x_0 = 3(1) mod 7 \quad x_0 = 3$$

2)

$$x_i = (a_1 x_{i-1} + a_2 x_{i-2} + a_3 x_{i-3} + a_4 x_{i-4})\, mod m$$

The first ten integers of the LSR below were produced using a program.

6, 4, 1, 5, 6, 0, 2, 6, 3, 2

$$x_1 = (0 * 3 + 6 * 1 + 4 * 5 + 2 * 4)\, mod 7 = 6$$

3)

Frank's way of generating numbers is not a strong random number generator. As there is only 6 possible slections for the first seed value, the number of sequences generated by the LFSR is only 6 as well. The initial seed value will determine the sequence, and as there are only 6 possible initial seeds, there can only be 6 possible sequences.