

Problem: 7

A linear congruential pseudorandom number generator has four parameters:

modulus: m

multiplier a

increment c

and seed $x[0]$

The recursion for n random numbers varying from 0 to n is given by a loop of n steps:

$$x[i+1] = (a * x[i] + c) \bmod m$$

($x[i]$ is i 'th number in the sequence)

The method will or will not properly according to the choice of the seed, modulus and increment.

Example:

For $a = 2$; $c = 1$; $m = 2$; $x[0] = 1$ if we run the loop then the numbers are:

random = [1,1,1,1,1,1,1,1,1,.....1,1,1]

which is not even a little bit of random. The seed comes in only 2nd step.

Or

For $m = 10$, $a = 7$, $c = 7$, then with $x[0] = 7$,

the random sequence is: [7,6,9,0,7,6,9,0,7,6,9,0,.....]

which is an alternating sequence and not random. The seed comes back after every 4 steps.

But,

By proper choice of those quantities, we get good random numbers when the seed never comes back.

Example:

For

$$a = 21356981$$

$$c = 1234567890$$

$$m = 9753113579$$

$$x[0] = 1.325 * \pi$$

If I run the Linear Congruential random number Generator (100 loops) in python with these values then we get:

[1323468678.3615053, 3004514931.0, 6523942507.0, 4716830518.0, 3677116536.0, 9431256975.0, 3024445216.0, 2106083794.0, 8047757178.0, 3586740959.0, 1127688035.0, 6105869310.0, 3811195182.0, 626476708.0, 9323846131.0, 2996178348.0, 5367591232.0, 3500350178.0, 120603200.0, 2214201822.0, 3818341663.0, 1411012809.0, 9466128479.0, 5319922184.0, 5555756418.0, 142863227.0, 3419605533.0, 5789616596.0, 7316600672.0, 8500639157.0, 3411851330.0, 7292046880.0, 9289219298.0, 8218834855.0, 4628102710.0, 7264093535.0, 8066452011.0, 5569336604.0, 3578742968.0, 4217085473.0, 5004205822.0, 4012179895.0, 4012281632.0, 1863129515.0, 1835562851.0, 7817477802.0, 7122822922.0, 448189175.0, 9682064912.0, 5613994381.0, 1896743790.0, 3836857174.0, 6590698121.0, 2706807221.0, 1384977727.0, 3719659829.0, 5670515767.0, 4702193782.0, 4227783049.0, 6245995811.0, 8200727573.0, 8456987991.0, 7403523768.0, 6018631902.0, 3679932725.0, 7274780690.0, 1315641746.0, 1972412452.0, 6105900606.0, 8987549186.0, 5902166698.0, 4840109554.0, 8942902227.0, 4549260428.0, 439269350.0, 6963441614.0, 1792344060.0, 82137236.0, 9614893466.0, 2041251400.0, 4116384559.0, 6325644067.0, 4198375740.0, 6655341388.0, 5245455962.0, 3826893119.0, 7642560370.0, 4685853755.0, 6738574752.0, 6384947923.0, 6441711957.0, 2819463617.0, 6305074697.0, 4295929090.0, 1328145339.0, 720752168.0, 6011470052.0, 6265817334.0, 2195933142.0, 3522300899.0]

Here the seed has never come again.