Random Number Generators

Examples

Steven Gordon

1 Linear Congruential Generator

$$X_{n+1} = (aX_n + c) \bmod m$$

1.1 Example 1

a = c = 1; m =100
X_0 = 23

X_1 = (23 + 1) mod 100
= 24

X_2 = (24 + 1) mod 100
= 25

Sequence will be: { 24, 25, 26, 27, … 99, 0, 1, 2 }

1.2 Example 2

a= 7, c = 0 m = 32
X_0=1

X_1 = (7 + 0) mod 32
= 7

X_2 = (7 x 7 + 0) mod 32
= 17

X_3 = (7 x 17 + 0) mod 32
= 23

X_4 = (23 x 7 + 0) mod 32
= 1

X_5 = 7

Sequence will be: {7, 17, 23, 1, 7, 17, 23, 1, …} only uses 4 out of 32 values

1.3 Example 3

A = 5, c = 0 m=32
X_0 =1

X_1 = 5
X_2 = 5 x 5 mod 32
= 25
X_3 =25 x 5 mod 32
= 29
X_4 = 29 x 5 mod 32
= 17

Sequence will be: {5, 25, 29, 17, 21, 9, 13, 1, 5, …}