Linear Congruential Generators

- $X_{i+1} = (a * X_i + c) \bmod m$
- $R_i = X_i / m$
- X_0 = Starting Seed value
- a is the multiplier
- C is the increment
- m is the modulus

Example

Given values

- $X_{0=27,a=17,c=43,m=100}$
- $X_{i+1=(aXi+c)mod\ m}$
- **X1=(17*27+43)mod 100**

  =502 mod 100

X1=2

X2=(17*2+43)mod 100

=77 mod 100

X2=77

- X3=(17*77+43)mod 100

  =1352 mod 100

  =52

X4=(17*52+43)mod 100

=927mod 100

=27

X5=(17*27+43)mod 100

=502 mod 100

=2

Ri=Xi/m

R1=2/100=0.02

R2=77/100=0.77

R3=52/100=0.52

R4=27/100=0.27

R5=2/100=0.02

Blum Blum Shub Generator

- It was created by Lenore Blum, Manuel Blum and Michael Shub in 1968.
- Cryptographically secure pseudorandom generator
- Choose two prime numbers p,q such that both have a remainder of 3 when divided by 4
- Next compute n=p*q(**eg:p=7,q=11**)
- Choose a random number s , such that s is relatively prime to n(**any integer that is not divisible by 7 or 11 will be relatively prime to 77.**)

Algorithm

$X_0=s^2 \bmod n$

For i=1 to infinity

$X_i=(X_i-1)^2 \bmod n$

$B_i= X_i \bmod 2$

Division Algorithm

The notation ***b* | *a*** is commonly used to mean ***b*** divides ***a***. Also, if ***b* | *a***, we say that *b* is a **divisor** of *a*.

Given any positive integer ***b*** and ***a***,

if we divide ***a*** by ***b*,** we get an integer quotient ***q*** and an integer remainder ***r*** that obey the following relationship:

$a=qb+r$ where $0<r<b$;$q=a/b$

Example

$a=21$, $b=2$

$a=10*2+1$($r=1$ and r is between 0 and 2)