

Structural Reliability
Prof. Baidurya Bhattacharya
Department of Civil Engineering
Indian Institute of Technology, Kharagpur

Lecture –72
Monte Carlo Simulations (Part - 04)

(Refer Slide Time: 00:27)

Monte Carlo simulations

Structural Reliability
Lecture 8
Monte Carlo
simulations


Pseudo random number generators: Lehmer algorithm

The linear congruential generator:

$$x_i = a x_{i-1} \text{ mod } m$$

$$u_i = x_i / m$$

Generally,
 $m = 2^b$, $b = \text{bits/word}$
 $a = \sqrt{m}$
 $m_0 = 2^{b-2}$



Derrick Henry Lehmer (1905 – 1991)
developed the linear congruential generator in 1948 while working at UC Berkeley

This generator is a full period generator if and only if:

- m is prime
- a is a primitive root of m

a is a primitive root of m iff
 $a^n \text{ mod } m \neq 1$ for $n = 1, 2, \dots, m-2$.


That is, no integer from the sequence
 $a^{-1}, a^2 - 1, a^3 - 1, \dots, a^{m-2} - 1$
is exactly divisible by m .

Fermat's little theorem,
 $a^m = a \text{ (mod } m) \Leftrightarrow a^{m-1} = 1 \text{ (mod } m)$
that is, $a^{m-1} - 1$ is exactly divisible by m .

"Best" RN Generator:
 $m = 2^{31} - 1$
 $a = 7^5 = 16807$
 $m_0 = m$ (full period)

This value for a was first proposed by Lewis, Goodman and Miller in 1969 while Lehmer himself suggested the Mersenne prime $2^{31} - 1$ for the modulus m in his original work.

Further reading:
Random Number Generators: good ones are hard to find, by Stephen K Park and Keith W Miller, in Computing Practices, Communications of the ACM, vo. 31, October, 1988.



©Baidurya Bhattacharya, IIT Kharagpur www.facweb.iitkgp.ac.in/~baidurya/ 218

We conclude the topic of random number generation with a look at the Lehmer algorithm the linear congruential generator it is what you see on the screen it starts with a seed and then recursively generates the next number in the sequence with modular arithmetic and being the modulus a being the multiplier and the number x_i is normalized by m to obtain the uniform deviate, m_0 is the period of generator and the numbers m and a are typically chosen depending on the word size of the machine.

And it is found that this generator is a full period generator only if the modulus is a prime number and a is a primitive root of m . Now this generator has been studied extensively and the best set of parameters MNA the best RNG it is found to be when m is the Mersenne prime to the power $31 - 1$ and a is 7 to the power of 5 . In this case this generator is a full period generator and m_0 is $m-1$ and these values were first proposed by Lewis et al in 1969.

And the value of m was by Lemur himself in his original work in 1948. I have listed this excellent paper by Park and Miller which discusses this algorithm and others. So, now let us just end this discussion with one or two small examples of the Lemur algorithm.

(Refer Slide Time: 02:27)

Monte Carlo simulations

Structural Reliability
Lecture 8
Monte Carlo simulations

Examples of Lehmer generator

$$x_i = ax_{i-1} \pmod m$$

$$u_i = x_i / m$$

Given $a = 2, m = 2^3 - 1$
What is the period of this generator?

1	3
2	6
4	5

Period=3 Period=3

Given $a = 3, m = 2^3 - 1$
What is the period of this generator?

1	3
2	6
4	5
5	6

Period=6

Given $a = 2, m = 2^5 - 1$
What is the period of this generator?

1	3	5
2	6	10
4	12	20
8	24	9
16	17	18

Period=5 Period=5 Period=5

Given $a = 2, m = 2^5 - 1$
What is the period of this generator?

7	11	15
14	22	30
28	13	29
25	26	27
19	21	23

Period=5 Period=5 Period=5

Given $a = 3, m = 2^5 - 1$
What is the period of this generator?

1	3
2	6
4	5
5	6

Period=6

©Baidurya Bhattacharya | IIT Kharagpur | www.facweb.iitkgp.ac.in/~baidurya/ 220

Let us say that let us have the modulus as 2 to the power 3 - 1 and the multiplier a as 2. So, what would be the period of this generator. If you want to work this through then please pause the video otherwise let me present the solution let us let us choose the seed as 1 and then we find that the period is 1 well the period is 3 that the sequence is 1, 2, 4 and then it starts repeating itself. If you choose a different seed then you hit another sequence and obviously there is no intersection between the two sequences.

If on the other hand we choose the multiplier as 3 then you will find that this becomes indeed becomes a full period generator. So, the choice of the multiplier is actually very important. Let us look at the next Marseille prime to the power 5 - 1 as the modulus and if a is 2 then what would be the period of this generator if you again want to work this out then please pause the video otherwise it turns out that depending on the seed you get different sequences and none of them is a full period generator the period is 5 and there are 6 such sequences.

On the other hand if a is chosen to be 3 then this generated indeed becomes a full period

generator.