

Modeling & Simulation of Discrete Event Systems
Dr. Pradeep K Jha
Department of Mechanical and Industrial Engineering
Indian Institute of Technology, Roorkee

Lecture – 16
Generation of Random Numbers

Welcome to the lecture on generation of random numbers. So, we have studied few things about the course, and we have seen that being the simulation of stochastic in nature, in case of the discrete event simulation, every time you will be required to deal with the random numbers. Now what are the random numbers? As the name indicates they are random. We do not know out of the possible outcomes what will be coming. So, there must be, you know proper way of generating the random numbers which should serve the purpose the way it has been to be used.

So, there are different types of random number generators, and there is requirement for these random numbers; like what it should be or how it should be, like the most requirement for this, is about its uniformity and independence know. Now we will go into little bit into the history of the generation of the random numbers.

(Refer Slide Time: 01:47)

Introduction

- All stochastic simulations need to “generate” IID $U(0,1)$ “random numbers”

Density function: $f(x) = \begin{cases} 1 & \text{if } 0 \leq x \leq 1 \\ 0 & \text{otherwise} \end{cases}$

0 1 x

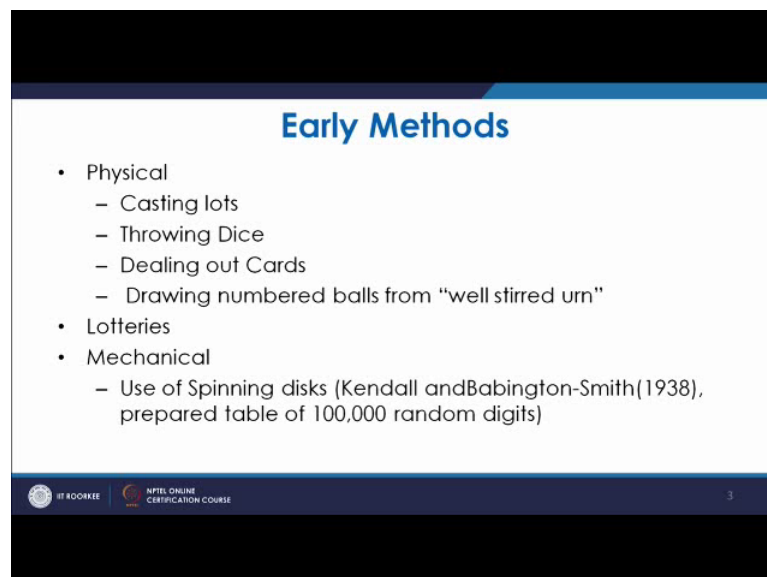
IIT ROORKEE NPTEL ONLINE CERTIFICATION COURSE 2

Now, first of all let us see that, as we discussed that every stochastic simulation requires generation of identical and independent, you know distributed independent and identically distributed random numbers.

So, you normally generate the random numbers or random variants between 0 to 1 that is U, U means it is uniformly distributed. So, as we know for uniform distribution, the density function is shown like this, that if $f(x)$, I mean $f(x)$ will be 1, if the value lie between 0 to 1, and if the value lie between you know either below, you know 0 or more than 1, then the probability is 0. So, that is what the; you know probability distribution function for uniform distribution is. So, whenever we generate the random numbers, we have to be sure that we you know generate the random numbers of uniform distribution. So, normally the generators generate the random numbers of uniform, you know distribution normal, typically you can generate in axially you can have the programs.

So, and even typically when we talk about the random numbers like we toss a dye, you know dice or you take a card from the playing card bunch. All these are the random number sort of. Supposed order 52 cards you take 1 card. So, certainly the probability is 1 by 52. So, for every card, but certainly that probability will be you know 0, if it is outside these 52 cards. So, let us go into the early methods, how earlier the random numbers were generated.

(Refer Slide Time: 03:39)



Early Methods

- Physical
 - Casting lots
 - Throwing Dice
 - Dealing out Cards
 - Drawing numbered balls from “well stirred urn”
- Lotteries
- Mechanical
 - Use of Spinning disks (Kendall and Babington-Smith(1938), prepared table of 100,000 random digits)

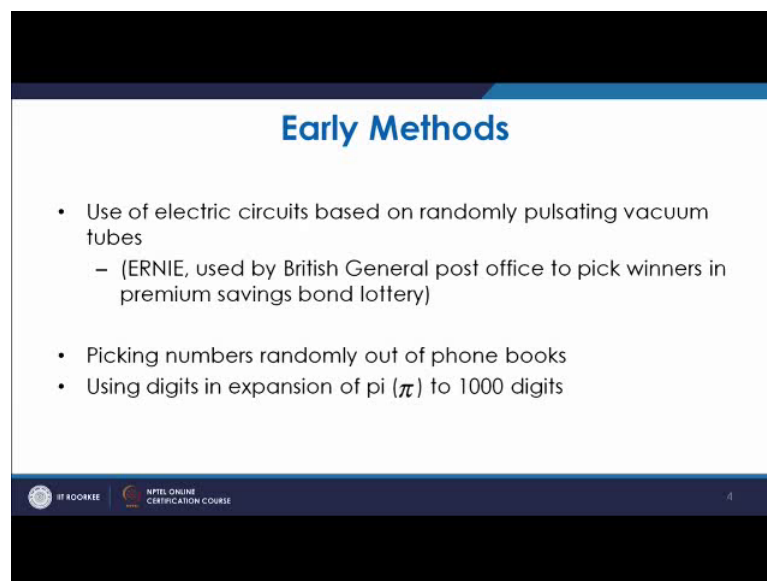
IT ROOKIEE | NPTEL ONLINE CERTIFICATION COURSE | 3

So, among the physical methods you have casting lots, you have throwing dice you dice the. I mean through the dice you get the numbers at random that was one of the method. You have the lot in that you have to take 1; that is among the random number generation.

Then you have dealing out with the cards, you have the pack of cards you take one of the card; that is also a random. So, you know that is an example of taking a random card. So, then again you have drawing numbered balls from well stirred urn. So, many a times this practice is also used, you have the urn which is well stirred, and then you are taking one of the card or a ball with certain number. So, that is again a type of taking 1 random number. So, apart from that the lotteries in earlier days or even today, they use these random numbers.

So, there also you pick any number and the chances you know, I mean you do not know. So, that is the way you know, you generate random numbers there are evens mechanical means; like use of spinning disc. So, that was basically suggested by Kendall and Babington Smith. So, in that basically, they prepared a table of 1 lakh random digits. So, that was a mechanical means to produce the random numbers. Random number has already also been produced using the electrical principles.

(Refer Slide Time: 05:18)



Early Methods

- Use of electric circuits based on randomly pulsating vacuum tubes
 - (ERNIE, used by British General post office to pick winners in premium savings bond lottery)
- Picking numbers randomly out of phone books
- Using digits in expansion of pi (π) to 1000 digits

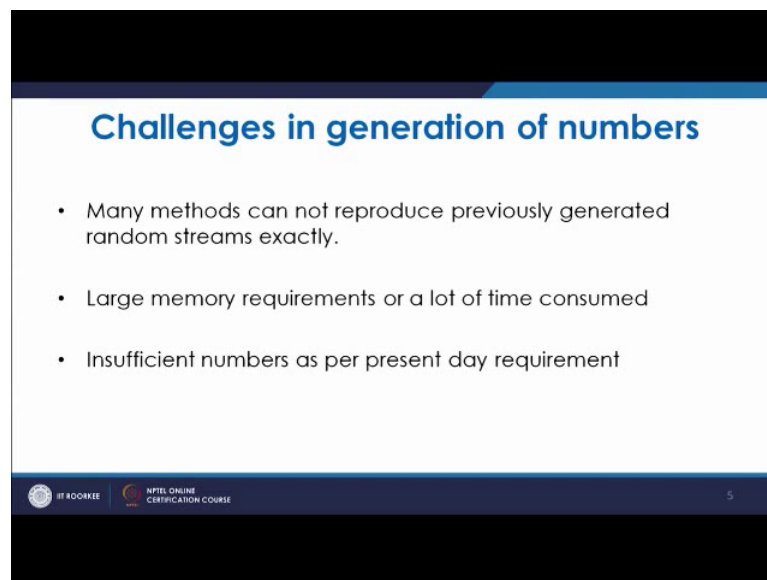
IT ROOKIE NPTEL ONLINE CERTIFICATION COURSE 4

So, using electrical circuits on randomly pulsating vacuum tubes also, these random numbers are generated.

So, that a ERNIE it was used by the British, you know general post office to pick winners in the premium savings bond lottery. So, this way you know random numbers are generated. Now there is another example like picking the random numbers out of the phone books. So, that is also an example of taking random number. Similarly you take

the expansion of pi, and you go to 1000 digits and take any number. So, taking digits in that. So, these are all the examples of random numbers. So, there is randomness you do not know what will be the outcome. So, now, although we generate this random numbers, but there are certainly challenges.

(Refer Slide Time: 06:16)



Challenges in generation of numbers

- Many methods can not reproduce previously generated random streams exactly.
- Large memory requirements or a lot of time consumed
- Insufficient numbers as per present day requirement

IT ROOKIE NPTEL ONLINE CERTIFICATION COURSE 5

In these generation of random numbers that too in this era, in the modern era, where we required largest number of random numbers, and also we need accurate random numbers. We need these random numbers to solve problems of different kinds. So, what are the challenges in generation of these random numbers. Now the thing is, first stage that many of the methods cannot reproduce the previously generated random streams exactly. So, all these methods, which we have discussed in most of them, the reproducibility is not there. If you have to produce these random numbers again; that is not possible. So, that reproducibility is lacking.

Similarly, in earlier days you required the random number in a small quantities. Now in present day, because of complex systems, because of the study of those systems you require very large number of, you know computer are in random numbers for that, if you are generating even through arithmetic means or computer means, you require a very powerful you know computer; otherwise it will take a lot of time. This is large amount of memory requirement. So, earlier you had the restriction, now that is why you have different type of algorithms to generate these random numbers. So, as we discussed that

you have the insufficient numbers at present, you know as per the present day requirement, you have the insufficient numbers of random numbers being generated.

So, there has been even in the past, you know in 1945 this arithmetic methods were used, and it was one of the method which was used by Von Neumann and Metropolis.

(Refer Slide Time: 08:07).

The slide is titled "Arithmetic methods" in blue text. It contains two bullet points. The first bullet point describes the sequential method. The second bullet point describes the midsquare method, attributed to Von Neumann and Metropolis (1945). It includes a sub-bullet point detailing the process: starting with a 4-digit positive integer Z_0 , squaring it to get 8 digits, taking the middle 4 digits to form Z_1 , and repeating the process to form U_1 , Z_2 , and U_2 . The slide footer includes the IIT Kharagpur logo, the text "IIT KHARAGPUR", and "NPTEL ONLINE CERTIFICATION COURSE". A small number "6" is visible in the bottom right corner of the slide content area.

Arithmetic methods

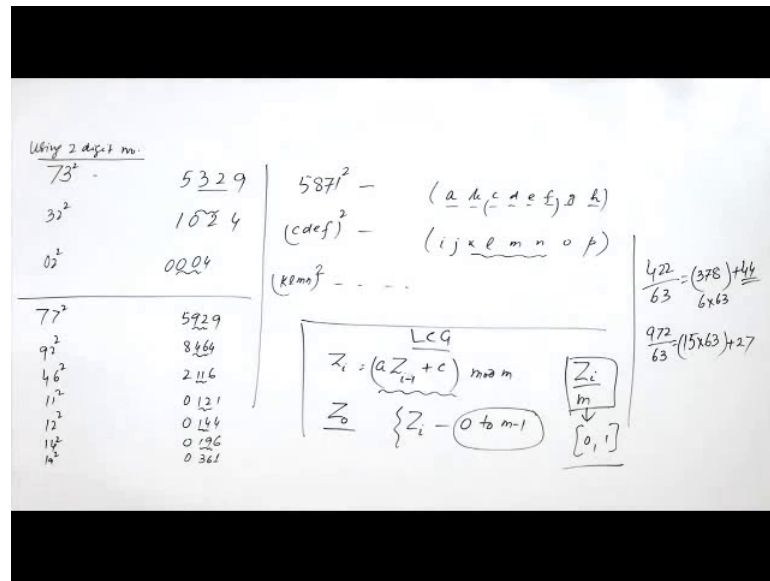
- Sequential: the next "random" number is determined by one or several of its predecessors according to a fixed mathematical formula
- The midsquare method: by Von Neumann and Metropolis (1945)
 - Start with Z_0 = 4-digit positive integer, Z_1 = middle 4 digits of Z_0^2 (append 0 if necessary to left to get exactly 8 digits); $U_1 = Z_1$, with decimal point at left, Z_2 = middle 4 digits of Z_1^2 ; $U_2 = Z_2$, with decimal point at left and so

IIT KHARAGPUR NPTEL ONLINE CERTIFICATION COURSE 6

So, that they have categorized as mid square method. So, it is the sequential, in the sequential way it generates the random number you know by using a fixed mathematical formula. So, in the mid square method what they do is, they take a 4 digit numbers, the seed value; that is Z naught or Z_0 , and this 4 digit number is squared, you know and then the squared number we will have 8 digits. So, this out of this 8 digits, you take the 4 digits. So, this 4 digit will be Z_1 for the next, and then in that case you know from Z_1 you go again to Z_1 square, and then the next 4, I mean middle 4 digit is taken and then that is further squared.

So, this way you are getting the different random numbers . So, as it is shown that you have Z naught or Z_0 ; that is 4 digit integer, you have Z_1 as middle of the 4 digits of Z naught square, and then U , because Z naught square will be of 8 digits. So, U_1 will be Z_1 ; that is with decimal point at the left. So, you get the random number in between these, you know I mean the middle 4 digits. So, this way you get $U_1 U_2 U_3$ and. So, random variates, you can get for example, if we try to see for. I mean for 2 digit, suppose you do for 4 digit.

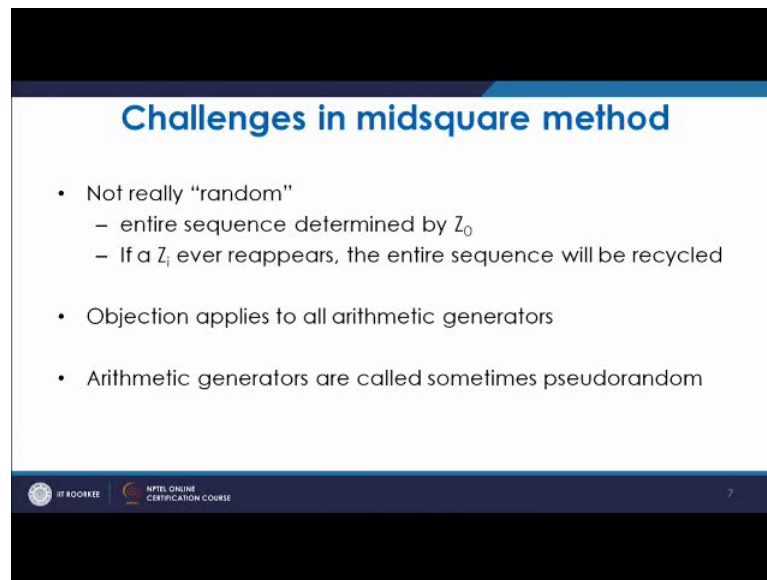
(Refer Slide Time: 10:05)



So, suppose you are starting with 73. So, 73 will be 5329. So, 5329 will be suppose 4 digit number it is coming. So, you take. So, using 4 2 digit number. So, it will be 32. So, 32 will be square. So, 32 square 73 square. So, 32 square will be 10 to 4. So, it will be 2. So, 2 square will be again 04; so that way, it is basically vanishing, but if you take another number or if we take the 4 digit number. In that case suppose 5871. So, 5871 be squared, and you will get a number here of 8 digits.

So, your this 4 digit will be taken, and suppose you get this digit as a b c d e f g h. So, this number c d e f will come here. So, this c d f again it will be squared. So, you will get something like i j k l m n o p. these are the digits from 0 to 9. all these are from 0 to 9. So, again you will take this. So, this will come as k l m n. So, this way, your these numbers will be, and this you put. So, you put a decimal you know at the beginning. So, that will be a random number between 0 and 1. So, this way these arithmetic methods; like mid square method is, you know working and you get the random numbers.

(Refer Slide Time: 12:17)



The slide is titled "Challenges in midsquare method" in blue text. It contains three bullet points: "Not really 'random'" with sub-points "entire sequence determined by Z_0 " and "If a Z_i ever reappears, the entire sequence will be recycled"; "Objection applies to all arithmetic generators"; and "Arithmetic generators are called sometimes pseudorandom". The slide footer includes the IIT ROORKEE logo, the text "NPTEL ONLINE CERTIFICATION COURSE", and the number "7".

- Not really "random"
 - entire sequence determined by Z_0
 - If a Z_i ever reappears, the entire sequence will be recycled
- Objection applies to all arithmetic generators
- Arithmetic generators are called sometimes pseudorandom

So, this is based on the arithmetic generator. Now the thing is that, you have certain challenges in case of this mid square method. So, basically it is not really random, because you know that what will come, and the entire sequence will be depending upon Z_0 ; that is seed value. So, Z_0 ; that is whatever you take that, according to that you will have the values coming. So, and further if a Z_i reappears then sequence will be recycled. So, the thing is that one thing is that you know it. So, it is not totally random, and also that there will be recycling. Once the similar Z_i comes in that case it will further be recycling. Now this objection is applied to most of the arithmetic generators.

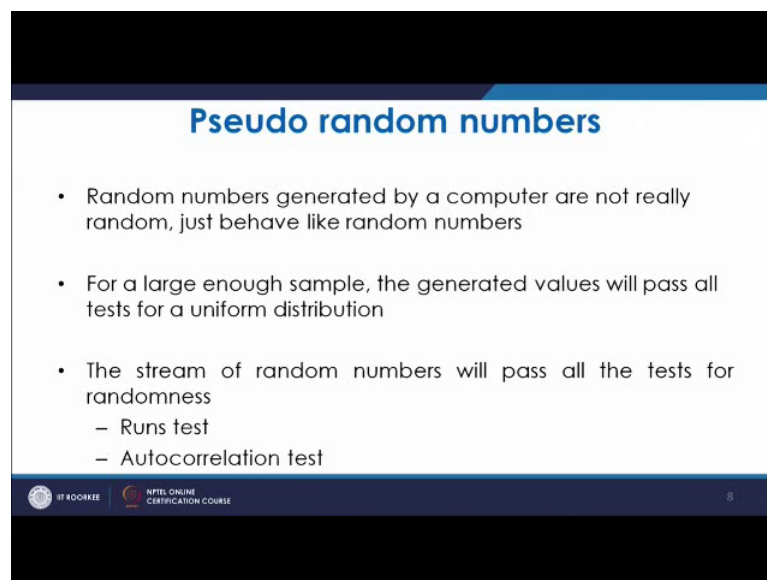
So, that is why, and we have to use these generators, we have the arithmetic, means to generate the random numbers. So, that is why whenever we generate the random numbers, we basically you know call, it has pseudo random numbers, because it's not truly random numbers, that is why it is known as pseudo random numbers. We also see that, as we have seen that in this case, if the number is chosen like this. In that case, we see that very early stage it is vanishing. So, you are not getting further random numbers. Suppose you start with 77. So, you get 5929, and if you do that, then you have 92 square that is 8464. So, you are getting this 46 square will be 2116 and. So, 11 square will be 0121.

So, if you again 12 square will be 0144 like that. So, it will move, it will move like that, they can 14 square will be 0196. Again 19 square will be 0361. So, anyway it is moving,

but as we took this number for a 2 digit x naught, we saw that very you know early stage we started getting, you know 00, and we cannot proceed further, but if we took the seed value somewhat different. In that case what we see is that, you get these random numbers at least this cycling, the period is increased. So, it all depends upon the seed value, and this is one of the drawback of such generators of, suppose mid square method.

Where depending upon the initial seed, you know this period is calculated. So, period is very important, because you need the different types of random numbers, and for that the seed is important. So, it depends upon the. See this is also one of the drawback. So, you have to very particularly select what is the seed value, based on that you can get the different random numbers.

(Refer Slide Time: 15:39)



Pseudo random numbers

- Random numbers generated by a computer are not really random, just behave like random numbers
- For a large enough sample, the generated values will pass all tests for a uniform distribution
- The stream of random numbers will pass all the tests for randomness
 - Runs test
 - Autocorrelation test

IT ROOKIE NPTEL ONLINE CERTIFICATION COURSE 8

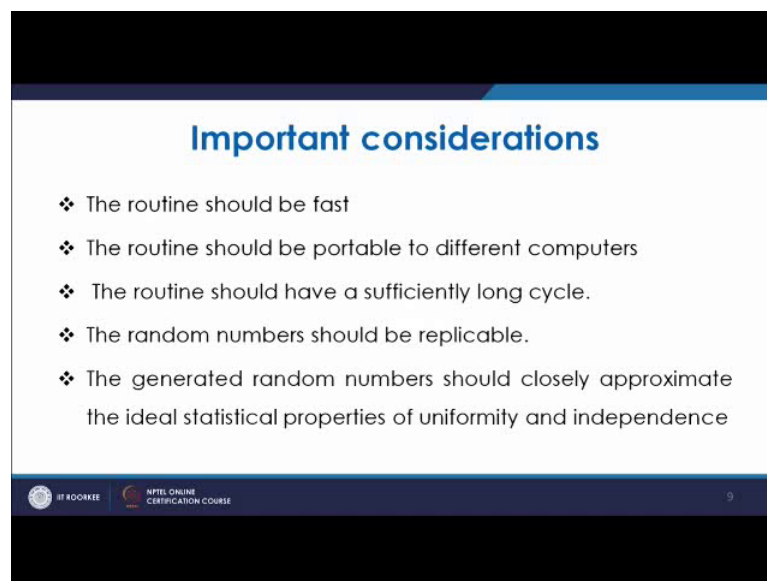
So, let us now discuss something about pseudo random numbers. So, as we discussed that, because we cannot think of having complete random numbers we do not know. We will not be replicated the same thing, we will not be able to reproduce the same thing. So, for keeping all these requirements in mind, you need the random numbers, which you can further replicate, which you can further produce with certain algorithm with certain principles

So, that is why they are known as pseudo random numbers. Now random numbers generated by a computer are not really random. They are just like, just behave like random number; that is why they are known as pseudo random numbers so, but then we

have to see that, it serves the purpose for which it is generated. Now for the large sample, the generator values will pass through a test for its distribution. So, as we discussed, we have to see that the random numbers should be uniformly distributed, uniformly distributed it. So, it should follow the uniform distribution; that is you know $f(x)$ equal to x , you know I mean effects is 1 for. I mean when $g(0)$ axis varying between 0 to 1 and then it is 0, when it is outside that range.

So, it should be uniformly distributed. So, in the range the equal probability should be there for all the; you know random numbers generated, and there is another test first. So, for this test you have the uniformity test, as well as you have the independence test. So, you have the uniformity test; that is also known as frequency test, and for that we take either the Kolmogorov Smirnov test or the chi square test, and there is autocorrelation test.

(Refer Slide Time: 17:47)



Important considerations

- ❖ The routine should be fast
- ❖ The routine should be portable to different computers
- ❖ The routine should have a sufficiently long cycle.
- ❖ The random numbers should be replicable.
- ❖ The generated random numbers should closely approximate the ideal statistical properties of uniformity and independence

NPTEL ONLINE CERTIFICATION COURSE 9

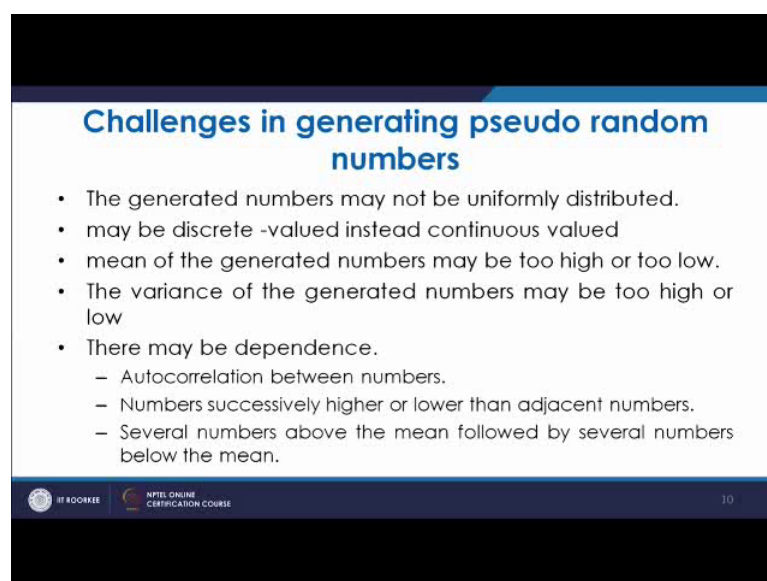
So, that is done for checking the independence of the random numbers generated. Now the concentrations which are to be kept in mind are basically, you know you have the routine should be fast. So, in the last lecture, it was basically not the run test. Run test are different tests a part, I mean that is coming later before that you have uniformity test as well as the autocorrelation test. Now let us see that what are the important requirements for the important considerations for such, you know routines. The routine must be fast, your requirement is that the random number generation should be at fast rate. You

require the random numbers quickly, because you require it during the simulation. So, you must have the generation at a fast rate.

So, otherwise the next simulation will be hampered. So, the routine by which you are making these random numbers. It should be fast, the routine should be portable to different computers one or the other requirement, other concentration is that it should be portable to different computers, then, because it can be used in other computers or. So, it should have a sufficiently long cycle, as we saw that in this case, you know you will see cycle, means you know it changes it further repeats. So, you must have a long cycle; otherwise same random number will be used. So, your routine must be; such that you have a larger cycle of the random numbers.

So, for that anyway seed number, seed values and other things are required random number should be re applicable, whenever you are thinking of further, findings the random numbers you must be in a position to run the program again, and get the random numbers. The generated random numbers should closely approximate the ideal statistical properties of uniformity and independence; that is also one of the criteria. Means that random number which you are generating, they should be uniform, as well as they should be independent. So, they must be approximately you know uniform as well as independent. What are the challenges in generating the pseudo random numbers?

(Refer Slide Time: 20:21)



Challenges in generating pseudo random numbers

- The generated numbers may not be uniformly distributed.
- may be discrete -valued instead continuous valued
- mean of the generated numbers may be too high or too low.
- The variance of the generated numbers may be too high or low
- There may be dependence.
 - Autocorrelation between numbers.
 - Numbers successively higher or lower than adjacent numbers.
 - Several numbers above the mean followed by several numbers below the mean.

IT ROOKIE NPTEL ONLINE CERTIFICATION COURSE 10

Now, the thing is that, once we generate the random numbers by different techniques. These generated random numbers may not be uniformly distributed. So, this is one of the challenge, while generating the pseudo random numbers, then you may get discrete value instead of continuous value, many a times your requirement, you should get some in continuous range. You must get proper, but you are getting the discrete value. So, that is what, this point means, and that is one of the, you know point which should be kept in mind.

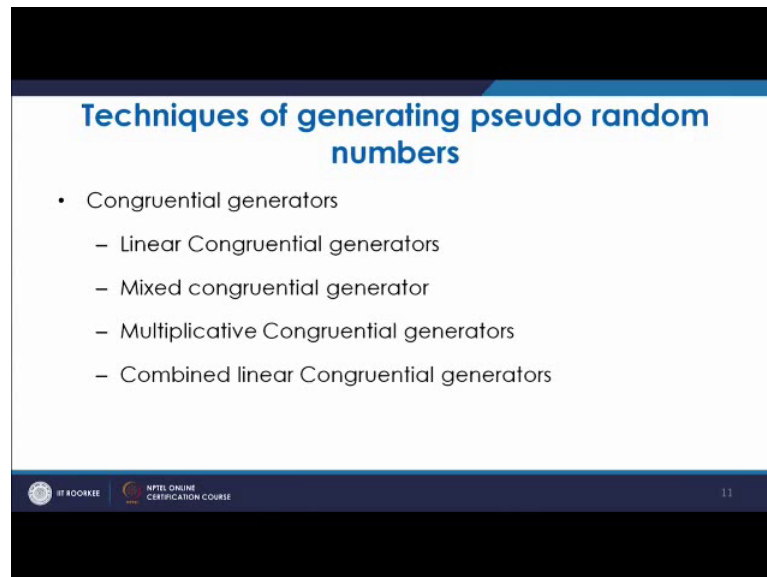
Many a times when we generate the random numbers we see that mean of the generated numbers; either it is too high or too low. So, it means you know feel from the ideal, mean neither it is higher or lower side too high too low. So, that is also not a desirable property. So, this is one of the challenge, while generating the random numbers, the variance of the generated numbers that may also be quite high or quite low. So, that should also be in the limit. And if these are the cases, then we will have to look into that, whether we should rely upon these random numbers or not.

So, we have to see that the variance of generated numbers. I mean it should not be too high or too low, and there may be dependence. The thing is that the random numbers, when, which we produce, we may see that there they, there is dependence autocorrelation between numbers; like we may see that there is some relationship found between the numbers. We can very much predict that this is number after that, this will come after that that will come maybe after 5 numbers this is coming. So, some is repetition pattern is observed, or we see that after 1 large, there is 1 small after 1 larger is 1 small, and this is how much of difference that kind of pattern you may observe.

So, these are basically the you know challenges while generating the random numbers. number successively higher or lower than adjacent numbers. The numbers which you are making successively higher or lower than the adjacent numbers as we discussed. Do you have a finite pattern from there you can you know correlate. So, that is how this correlation should not be there. So, that is one of the disadvantage, several numbers above the mean followed by several numbers below the mean. This is also one of the trend which is observed many a times, you will see that the numbers which you have seen sometimes they are about the mean, and sometimes then. So, many of them come in a group. So, that is above the mean, and then further many a times they are coming, which are below the mean.

So, this way you are seeing that you have you know this is predictable, this is correlated. So, all these things should not be there, they are basically not fulfilling the condition of independence. So, these are the challenges, and these challenges are to be addressed.

(Refer Slide Time: 24:05).



The slide is titled "Techniques of generating pseudo random numbers" in blue text. Below the title, there is a bulleted list of congruential generators. The list includes "Congruential generators" as a main category, followed by four sub-points: "Linear Congruential generators", "Mixed congruential generator", "Multiplicative Congruential generators", and "Combined linear Congruential generators". At the bottom of the slide, there is a footer with logos for "IIT ROORKEE" and "NPTEL ONLINE CERTIFICATION COURSE", and the number "11" on the right.

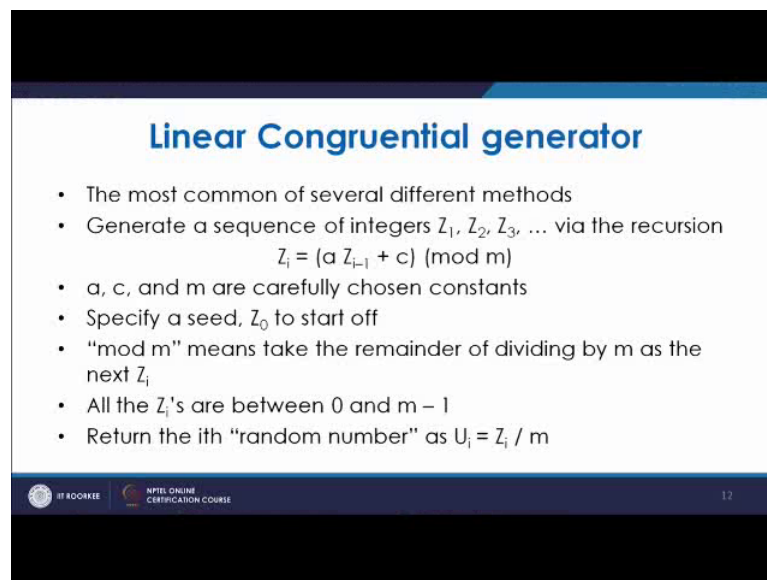
- Congruential generators
 - Linear Congruential generators
 - Mixed congruential generator
 - Multiplicative Congruential generators
 - Combined linear Congruential generators

Now, let us. So, we have to keep all that in mind, and then accordingly you know before that. So, this is at the point which must be thought before that. Once we generate the random numbers, we have to test them, we have to test them and then we have to see that whether they are uniformly distributed and whether they are independent. So, this is to, I mean to be checked techniques of generating pseudo random numbers. So, there are different techniques of generating pseudo random numbers, you have a very famous you know method; that is generator known as linear congruential generator.

So, you have a linear formula. So, you have some constant a is there, x is there, a is there c and m . So, there is a linear equation based on that, since this generator forms the random numbers. So, that is why it is known as linear congruential generators. Now in the linear congruential generator. So, as we see that in the linear equation you have some constants. So, by changing this constants, you may get the different kind of mixed congruential generator or multiplicative congruential generator, and then you have combined linear congruential generator, because many a times you will required to have large number of periods.

So, you need to have a composite generator or a combined linear congruential generator, where 2 generators are combined or mixed. So, that you get large number of generators 2 raise to the power 30 31 or. So, nowadays even that is less. So, you need very large number of generators. So, that is why we go for such generators.

(Refer Slide Time: 26:16)



Linear Congruential generator

- The most common of several different methods
- Generate a sequence of integers Z_1, Z_2, Z_3, \dots via the recursion

$$Z_i = (a Z_{i-1} + c) \pmod{m}$$
- a , c , and m are carefully chosen constants
- Specify a seed, Z_0 to start off
- "mod m " means take the remainder of dividing by m as the next Z_i
- All the Z_i 's are between 0 and $m - 1$
- Return the i th "random number" as $U_i = Z_i / m$

IT ROOKIE NPTEL ONLINE CERTIFICATION COURSE 12

Now, let us see; what is a linear congruential generator. So, the most common of the methods which is formed is linear congruential generator. It generates a sequence of integers Z_1, Z_2, Z_3 in. I mean where the recursion formula; that is Z_i equal to $a Z_{i-1} + c \pmod{m}$. So, what you see in the linear congruential generator.

So, a equal to I mean Z_i will be $a Z_{i-1} + c \pmod{m}$. So, as you see in this case a and m are constant. So, you require the first number this. So, initially you require is a Z_0 . So, that is known as a seed. So, you require that seed, and you know this constants a and m . So, and then mod m , mod m means, once you know a and c and Z_0 . So, this product, this using this expression you find $a Z_{i-1} + c$ and then you divide it using m , m is an integer.

So, you divide it using m , and you get the remainder, that remainder is basically the Z_i value. So, that Z_i is you are getting. So, once you get the Z_i , this Z_i will vary from 0 to $m - 1$, because it is the remainder by dividing with m . So, it will vary between 0 to $m - 1$. So, basically you get these random numbers, or you can get this random number between 0 to 1, uniformly distributed by dividing it with m modulo it is known

as. So, this number you divide. So, you get. So, this if you get, you will get this value in between 0 to 1. So, this way you get this you know number, random number between 0 to 1. So, you just see the example.

(Refer Slide Time: 29:02)

Example of a LCG

i	$22 Z_{i-1} + 4$	Z_i	U_i
0		19	
1	422	44	0.6984
2	972	27	0.4286
3	598	31	0.4921
4	686	56	0.8889
⋮	⋮	⋮	⋮
61	158	32	0.5079
62	708	15	0.2381
63	334	19	0.3016
64	422	44	0.6984
65	972	27	0.4286
66	598	31	0.4921
⋮	⋮	⋮	⋮

Parameters $m = 63$, $a = 22$, $c = 4$, $Z_0 = 19$:
 $Z_i = (22 Z_{i-1} + 4) \pmod{63}$, seed with $Z_0 = 19$

- **Cycling** — will repeat forever
- **Cycle length** ($\leq m$)
(could be $< m$ depending on parameters)

IIT ROORKEE
 NPTEL ONLINE CERTIFICATION COURSE

Simulation with Arena — Further Statistical Issues

C11/13

Now in fact, coming to back to this slide, if we have c equal to c is not equal to 0, then it is a mixed type of congruential generator. If c is equal to 0, then it is known as multiplicative type of LCG linear congruential generator, then the just example of this l c g. If you look at the example of linear congruential generator what we see here is, just see an example, where it is shown that you are taking a as 22 m as 63 c as 4 and Z naught as 19 19 is the seed value.

So, you have 19 as the seed value, it is multiplied with a that is 22. So, 19 multiplied by 22 that becomes 418 plus you add in 4 into it. So, 418 plus 4. So, that is 422 and 422 will be the Z_1 , Z_1 once you get 422, 422 will be divided by m, m is 63. So, 422 divided by 63. So, that will be basically 63 into 63 78. So, if you divide 422 by 63. So, this 422 by 63, this is m.

So, it will be 378; that is 6 into 63 plus 44. So, this 44 is coming here, this 44 is the Z_i the first random number which you have computed from this linear congruential generator. So, then you have the second generator second number. For second number this 44 will come as the Z_1 . So, 44 multiplied by you know 44 multiplied by a, a is 22.

So, 44 multiplied by 22 it will be 968, and 968 plus 4. So, it will be 972. So, 972 multiplied by 63.

So, if you divide 972 divided by 63. So, this is 1, and this is 30 42. So, again 5 15 into 63 plus 27 I hope. So, it is 27, this 27 has come here, this 27 has come here, and this 972 and this 27 divided by 63. So, this here in this case 44 is divided by 63, and in this case 27 is divided by 63. So, you are getting the random number between 0 and 1. So, that is how it is going, and by looking at this random number what we see is that, you see that when we are coming to this number 62 numbers, after 62 or 63 you are seeing that it is getting repeated.

It is getting repeated. So, it will come. So, it means that your maximum period is m , if you are taking m as 63 your, that is your maximum period after 63 you are bound to get repeated. So, once you get, because your value is in between that numbers at any point. once this previous number comes you are bound to get repeated. So, once you are getting repeated, then same sequence of numbers will be coming. So, what you see that, your this, this is shown as the period. So, this period fortunately is coming here to be quite equal to its m value; that is its modulo value, but in many cases they may not be the same, they maybe lesser than that; that is the maximum value. So, cycle length many a times will depend upon, basically it may be equal to a m or will be normally less than or equal to m . So, that depends on different parameters. So, we will discuss how this parameters are effecting that in our next lecture.

Thank you very much.