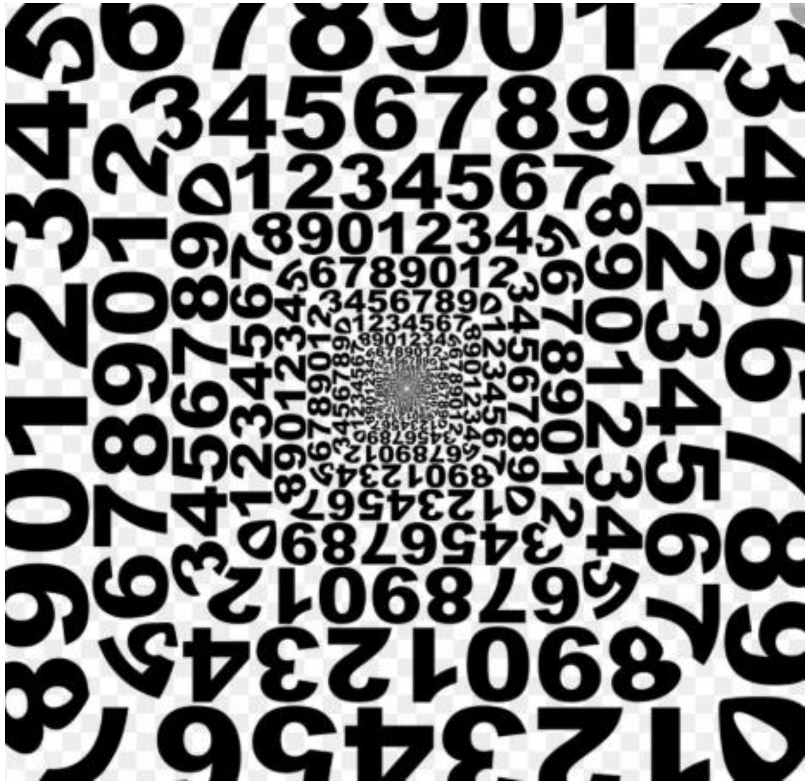


Random Number Generation

Guilherme Souza Rodrigues
guilhermerodrigues@unb.br

Contents

- ✓ Properties of Random Numbers
- ✓ Pseudo-Random Numbers
- ✓ Generating Random Numbers
  - Linear Congruential Method

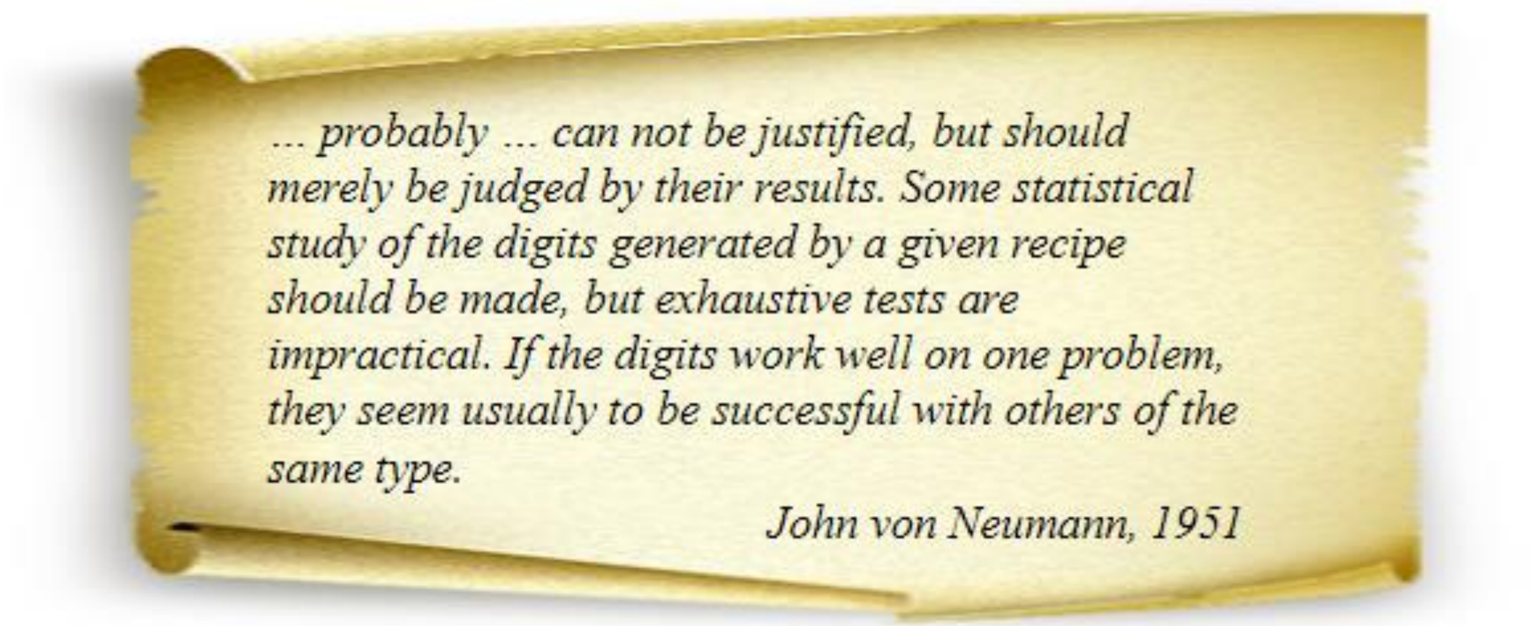
Pseudo-Random Numbers

"Every Cause has its Effect; every Effect has its Cause; everything happens according to Law; Chance is but a name for Law not recognized; there are many planes of causation, but nothing escapes the Law."

The Kybalion

- ✓ Approach: Arithmetically generation (calculation) of random numbers.
- ✓ "Pseudo", because generating numbers using a known method renders it deterministic.

Pseudo-Random Numbers



- ✓ Goal: To produce a sequence of numbers in [0,1] that simulates, or imitates, the ideal properties of random numbers (RN).

Important properties of good random number routines:

✓ Fast

✓ Portable to different computers

✓ Have sufficiently long cycle

✓ Replicable

Verification and debugging

Use identical stream of random numbers for different systems

✓ Closely approximate the ideal statistical properties of

Uniformity and

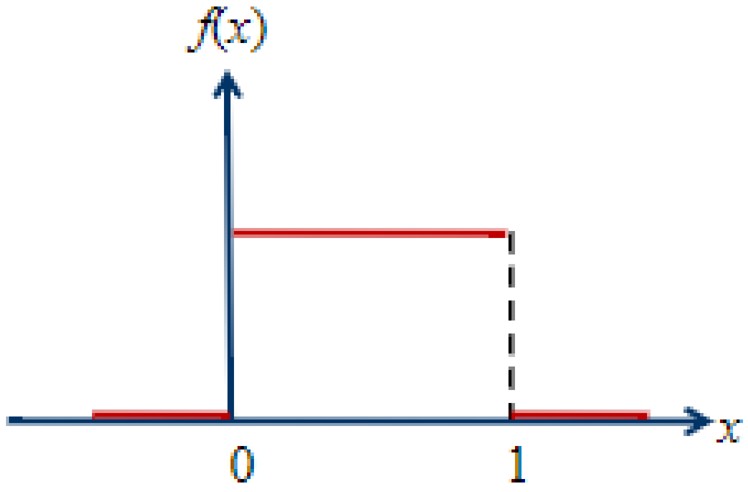
Independence

Pseudo-Random Numbers: Properties

Random number R_i must be independently drawn from a uniform distribution with PDF:

$$f(x) = \begin{cases} 1, & 0 \le x \le 1 \\ 0, & \text{otherwise} \end{cases}$$

$$E(R) = \int_0^1 x\,dx = \left.\frac{x^2}{2}\right|_0^1 = \frac{1}{2}$$



PDF for random numbers

Problems when generating pseudo-random numbers

- ✓ The generated numbers might not be uniformly distributed
- ✓ The generated numbers might be discrete-valued instead of continuous-valued
- ✓ The mean of the generated numbers might be too high or too low
- ✓ The variance of the generated numbers might be too high or too low

There might 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

Linear Congruential Method

- ✓ To produce a sequence of integers $X_1, X_2, \ldots$ between 0 and $m - 1$ by following a recursive relationship:

$$X_{i+1} = (\underbrace{a}_{\text{The multiplier}} X_i + \underbrace{c}_{\text{The increment}}) \bmod \underbrace{m}_{\text{The modulus}}, \quad i = 0,1,2,\ldots$$

- ✓ Assumption: $m > 0$ and $\mathrm{a} < m$, $\mathrm{c} < m$, $\quad X_0 < m$

- ✓ The selection of the values for $\mathrm{a}, \mathrm{c}, \mathrm{m}$ and X_0 drastically affects the statistical properties and the cycle length

- ✓ The random integers X_i are being generated in $[0, \mathrm{m} - 1]$

Linear Congruential Method

- ✓ Convert the integers X_i to random numbers $R_i = \dfrac{X_i}{m}, \quad i = 1,2,\ldots$
- ✓ Note $X_i \in \{0, 1, ..., m\text{-}1\}$

  $R_i \in [0, (m\text{-}1)/m]$

Example 1:

Use: X_0=27, a=17, c=43, m=100

$$X_1 = (17\times27+43) \bmod 100 = 502 \bmod 100 = 2 \quad ➡ \quad R_1 = 0.02$$

$$X_2 = (17\times2 \ +43) \bmod 100 = 77 \quad ➡ \quad R_2 = 0.77$$

$$X_3 = (17\times77+43) \bmod 100 = 52 \quad ➡ \quad R_3 = 0.52$$

$$X_4 = (17\times52+43) \bmod 100 = 27 \quad ➡ \quad R_3 = 0.27$$

$$\ldots$$

Example 2:

Use: X_0=27, a=13, c=0, m=64

✓ The period of the generator is very low

✓ Seed X_0 influences the sequence

The LCG has full period if and only if the following three conditions hold (Hull and Dobell, 1962):

1. The only positive integer that (exactly) divides both m and c is 1

2. If q is a prime number that divides m, then q divides a-1

3. If 4 divides m, then 4 divides a-1

i	X_i $X_0=1$	X_i $X_0=2$	X_i $X_0=3$	X_i $X_0=4$
0	1	2	3	4
1	13	26	39	52
2	41	18	59	36
3	21	42	63	20
4	17	34	51	4
5	29	58	23	
6	57	50	43	
7	37	10	47	
8	33	2	35	
9	45		7	
10	9		27	
11	53		31	
12	49		19	
13	61		55	
14	25		11	
15	5		15	
16	1		3	

Proper choice of parameters

- ✓ For m a power 2, $m=2^b$, and $c \neq 0$

  Longest possible period $P=m=2^b$ is achieved
  if c is relative prime to m and $a=1+4k$, where k is an integer

- ✓ For m a power 2, $m=2^b$, and $c=0$

  Longest possible period $P=m/4=2^{b-2}$ is achieved
  if the seed X_0 is odd and $a=3+8k$ or $a=5+8k$, for $k=0,1,\ldots$

- ✓ For m a prime and $c=0$

  Longest possible period $P=m-1$ is achieved
  if the multiplier a has property that smallest integer k such that a^k-1 is divisible by m is $k = m-1$

Linear Congruential Method

- Linear Congruential Generators are a special case of generators defined by:

$$X_{i+1} = g(X_i, X_{i-1}, \ldots) \bmod m$$

- where $g()$ is a function of previous X_i's

  $X_i \in [0, m\text{-}1]$, $R_i = X_i / m$

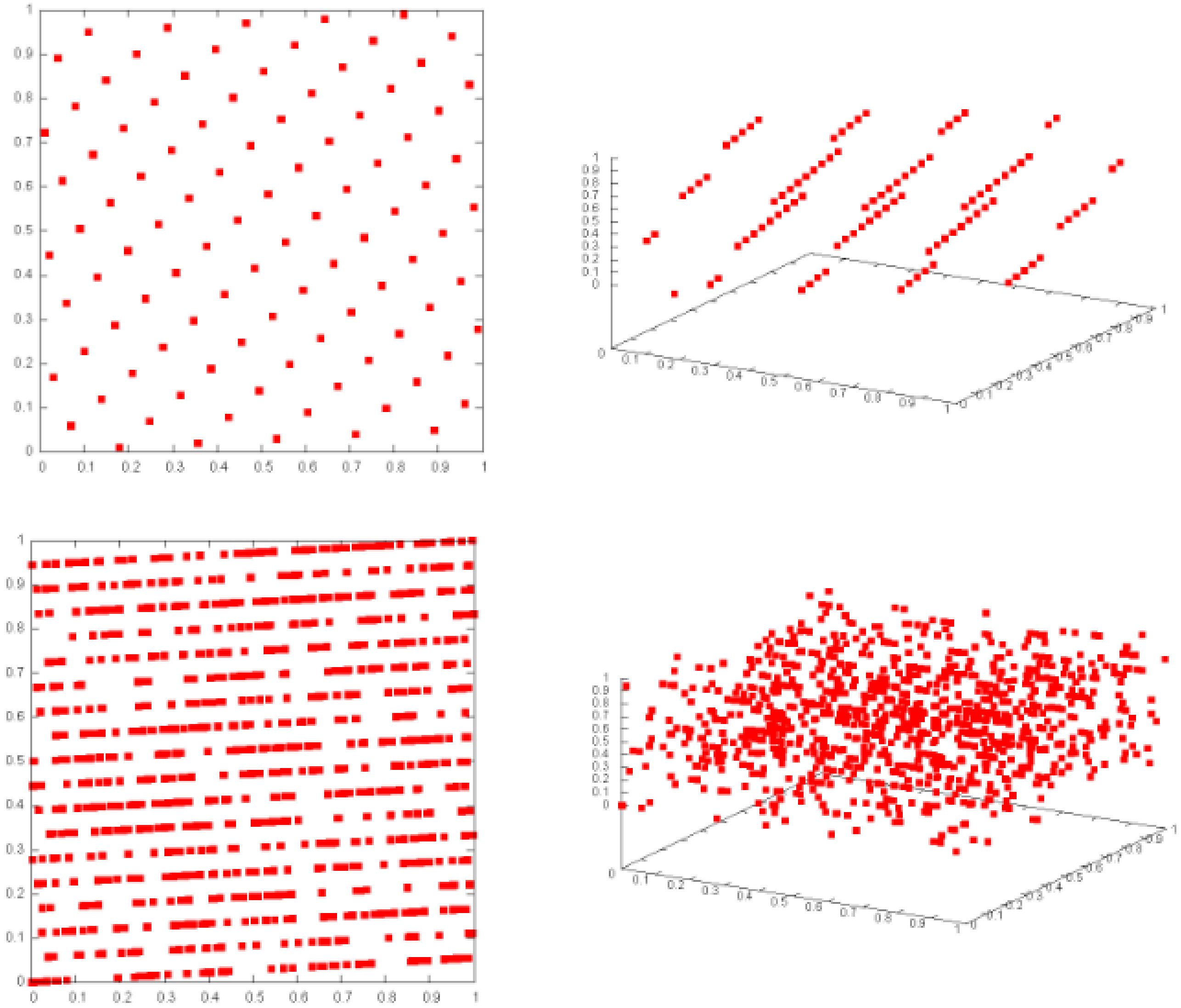
- Quadratic congruential generator

  Defined by: $g(X_i, X_{i-1}) = aX_i^2 + bX_{i-1} + c$
- Multiple recursive generators

  Defined by: $g(X_i, X_{i-1}, \ldots) = a_1 X_i + a_2 X_{i-1} + \cdots + a_k X_{i-k}$
- Fibonacci generator

  Defined by: $g(X_i, X_{i-1}) = X_i + X_{i-1}$

Characteristics of a Good Generator



Exemplo 1 -Gerador Congruencial Linear

```
m <- 100;a <- 17;c <- 43;seed <- 27;n<-10

xn=seed
x=numeric(n)
for (i in 1:n){
  xn=(a*xn+c)%%m #resto da divisão
  x[i]=xn
}
x
```

OBRIGADO!