

#### 4. NÚMEROS PSEUDOALEATORIOS.

En los experimentos de simulación es necesario generar valores para las variables aleatorias representadas estas por medio de distribuciones de probabilidad.

Para poder generar entradas estocásticas (probabilísticas) para un modelo de simulación, se debe contar con un generador de números pseudoaleatorios. Con estos y métodos de generación de variables aleatorias, se pueden simular las entradas incontrolables para un modelo de simulación.

Inicialmente los números aleatorios se generaban en forma manual o mecánica utilizando técnicas como ruedas giratorias, lanzamientos de dados, barajas. También existen métodos aritméticos que permiten generar un gran conjunto de números aleatorios, pero el advenimiento de la computadora ha permitido crear generadores que permitan generar de manera sucesiva todo los números aleatorios que se requieran.

Un número pseudoaleatorio no es más que el valor de una variable aleatoria  $x$  que tiene una distribución de probabilidad uniforme definida en el intervalo (0, 1).

Se sabe que la función de densidad  $f(x)$  de una variable aleatoria  $x$  con una distribución de probabilidad uniforme en el intervalo  $[a, b]$  es:

$$f(x) = \begin{cases} \frac{1}{b-a} & \text{para } a \leq x \leq b \\ 0 & \text{para otros valores} \end{cases}$$

La función acumulativa  $F(x)$ , que representa la probabilidad de que la variable aleatoria  $x$  sea menor o igual a un valor específico de  $x$  está dada por:

$$F(x) = \begin{cases} 0 & \text{si } x < a \\ \frac{x-a}{b-a} & \text{para } a \leq x \leq b \\ 1 & \text{si } x > b \end{cases}$$

La figura 6, muestra la función de densidad y acumulativa para dicha variable aleatoria

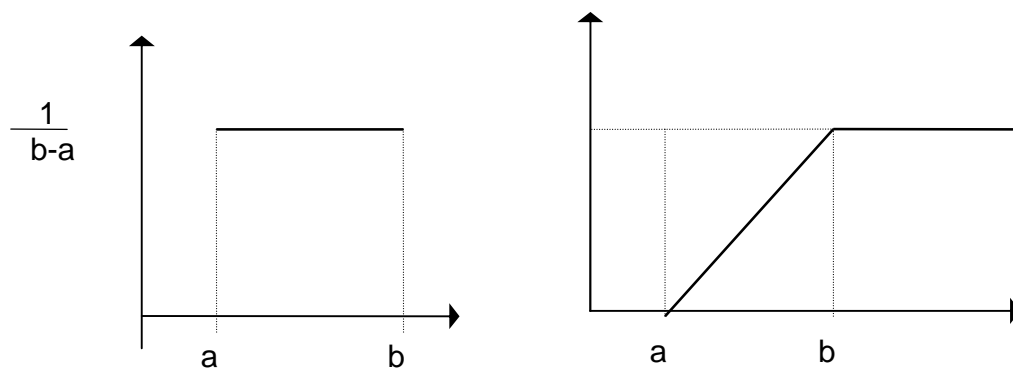


Figura 6. Función de densidad y acumulativa para una variable aleatoria  $x$  con una distribución de probabilidad uniforme en el intervalo  $[a, b]$ .

El valor esperado y la varianza de una distribución de probabilidad uniforme son respectivamente.

$$\mu = \frac{a+b}{2}, \quad \sigma^2 = \frac{(a+b)^2}{12}$$

Al definir la función de densidad de la distribución de probabilidad uniforme en el intervalo  $[0, 1]$ , una variable aleatoria  $R$  tendría una función de densidad  $f(R)$  y una función acumulada  $F(R)$ , dadas por:

$$f(R) = \begin{cases} 1 & \text{para } 0 \leq R \leq 1 \\ 0 & \text{para otros valores} \end{cases}$$

$$F(R) = \begin{cases} 0 & \text{si } R < a \\ \frac{R-a}{b-a} & \text{para } 0 \leq R \leq 1 \\ 1 & \text{si } R > b \end{cases}$$

Los valores de la media y la varianza, están dados por:

$$\mu = \frac{1}{2}, \quad \sigma^2 = \frac{1}{12}$$

La variable aleatoria R es continua y debe ser estadísticamente independiente.

Finalmente para que para que un conjunto de números sean considerados aleatorios deben cumplir las siguientes características:

- Deben estar uniformemente distribuidos.
- Deben ser estadísticamente independientes.
- Su media debe ser estadísticamente igual a ½.
- Su varianza debe ser estadísticamente igual a 1/12.
- Deben ser reproducibles.

#### **4.1. MÉTODOS PARA GENERAR NÚMEROS PSEUDOALEATORIOS.**

**4.1.1. Métodos Manuales:** son los métodos más simples y lentos, ejemplo de estos métodos son lanzamientos de monedas, dados, cartas y ruletas. Los números producidos por estos métodos cumplen las condiciones estadísticas mencionadas anteriormente, pero es imposible reproducir una secuencia generadas por estos métodos.

**4.1.2. Tablas de números aleatorios:** estos números se pueden generar por medio de una hoja de cálculo o por cualquier generador de cualquier lenguaje de programación razón por la cual su comportamiento es totalmente determinístico.

**4.1.3. Mediante el computador digital:** existen tres métodos para producir números aleatorios mediante un computador:

- Provisión externa.
- Generación interna a través de un proceso físico aleatorio.
- Generación por medio de una regla de recurrencia.

#### **4.2. MÉTODOS ARITMÉTICOS PARA GENERAR NÚMEROS PSEUDOALEATORIOS.**

**4.2.1. Métodos de Cuadrados Medios:** el procedimiento de obtención de números pseudoaleatorios con este tipo de generador es el siguiente:

- Se define una semilla.
- Se eleva la semilla al cuadrado.
- Dependiendo de la cantidad de dígitos que se desea tenga el número pseudoaleatorio, se toman de la parte central del número resultante en el paso anterior el número de dígitos requeridos. Si no es posible determinar la parte central, se completa el número agregando ceros al principio o al final.

- Debe tenerse en cuenta que se desean números pseudoaleatorios entre 0 y 1, en consecuencia el resultado se debe normalizar, es decir, si los números son de dos dígitos se normaliza dividiendo por 100, si es de tres dígitos por mil y así sucesivamente.

*Ejemplo:* generar 3 números aleatorios de 4 dígitos a partir de un generador de cuadrados medios utilizando como semilla el número 445.

Como se quieren números pseudoaleatorios  $R_i$  de 4 dígitos, se tomarán los cuatro dígitos de la parte central del cuadrado de la semilla, de la siguiente manera:

$(445)^2 = 198025 = 9802$	luego $R_1 = 9802 / 10000 = 0.9802$
$(9802)^2 = 96079204 = 0792$	luego $R_2 = 0792 / 10000 = 0.0792$
$(792)^2 = 627264 = 2726$	luego $R_3 = 2726 / 10000 = 0.2726$

Observación: como los números pseudoaleatorios deben estar entre 0 y 1 y son de 4 dígitos, se normaliza dividiendo entre 10000.

**4.2.2. Método de Producto medio:** este método es un poco similar al anterior pero se debe comenzar con dos semillas cada una con  $k$  dígitos, el número resultante se toma como las cifras centrales del producto de los dos números anteriores. Por ejemplo, tomando como semillas a  $X_0 = 13$  y  $X_1 = 15$  el método sería el siguiente:

$$X_2 = (13 \cdot 15) = 0195 = 19, \text{ luego } R_2 = 19 / 100 = 0.19.$$

$$X_3 = (15 \cdot 19) = 0285 = 28, \text{ luego } R_3 = 28 / 100 = 0.28.$$

$$X_4 = (19 \cdot 28) = 0532 = 53, \text{ luego } R_4 = 53 / 100 = 0.53.$$

**4.2.3. Método del producto medio modificado:** consiste en usar una constante multiplicativa en lugar de una variable. Es decir  $X_{n+1} = (K \cdot X_n)$ . Debe notarse que los métodos anteriores tienen periodos relativamente cortos, los cuales son afectados grandemente por los valores iniciales que se escojan, además son

estadísticamente insatisfactorios. También debe tenerse en cuenta que un generador con un periodo corto no sirve para hacer un número considerado de ensayos de simulación.

### 4.3. MÉTODOS CONGRUENCIALES.

Se han desarrollado básicamente tres métodos de congruenciales para generar números pseudoaleatorios, los cuales se derivan del empleo de diferentes versiones de la relación fundamental de congruencia. El objetivo de cada uno de los métodos es la generación en un tiempo mínimo, de sucesiones de números aleatorios con periodos máximos. Los métodos congruenciales son: el aditivo, el multiplicativo y el mixto.

**4.3.1. Método Congruencial Aditivo:** calcula una sucesión de números pseudoaleatorios mediante la relación  $X_{n+1} = X_n + X_{n-k} \pmod{M}$ . Para usar este método se necesitan  $k$  valores iniciales, siendo  $k$  entero. Las propiedades estadísticas de la secuencia tienden a mejorarse a medida que  $k$  se incrementa. Este es el único método que produce periodos mayores que  $M$ .

**4.3.2. Método Congruencial Multiplicativo:** calcula una sucesión  $X_n$  de enteros no negativos, cada uno de los cuales es menor que  $M$  mediante la relación  $X_{n+1} = a \cdot X_n \pmod{M}$ . Es un caso especial de la relación de congruencia en que  $c=0$ , este método se comporta de manera satisfactoria estadísticamente, es decir, los números generados por medio de este método están uniformemente distribuidos, y no están correlacionados. Este método tiene un periodo máximo menor que  $M$ , pero se pueden imponer condiciones en  $a$  y  $X_0$  de tal forma que se obtenga el periodo máximo. Desde el punto de vista computacional es el más rápido de todos.

**4.3.3. Método Congruencial Mixto o Lineal:** los generadores congruenciales lineales generan una secuencia de números pseudoaleatorios en la cual el próximo número pseudoaleatorio es determinado a partir del último número generado, es decir, el número pseudoaleatorio  $X_{n+1}$  es derivado a partir del número pseudoaleatorio  $X_n$ . La relación de recurrencia para el generador congruencial mixto es  $X_{n+1} = (a X_n + c) \bmod m$ , en donde

- $X_0$  = es la semilla
- $a$  = el multiplicador
- $c$  = constante aditiva
- $m$  = el modulo ( $m > X_0, a, c$ )
- $X_0, a, c > 0$

Esta relación de recurrencia nos dice que  $X_{n+1}$  es el residuo de dividir a  $X_n + c$  entre el modulo. Lo anterior significa que los valores posibles de  $X_{n+1}$  son  $0, 1, 2, 3, \dots, m-1$ , es decir,  $m$  representa el número posible de valores diferentes que pueden ser generados.

*Ejemplo:* supongamos que se tiene un generador en el cual los valores de sus parámetros son:  $a = 5$ ,  $c = 7$ ,  $X_0 = 4$  y  $m = 8$ . El generador quedará de la siguiente manera:

$$X_{n+1} = (5 X_n + 7) \bmod 8$$

En la tabla 2, se muestran los números aleatorios generados por este método.

n	$X_n$	$(5 X_n + 7)/8$	$X_{n+1}$ (Residuo)	Números aleatorios
1	4	27/8	3	3/8=0.375
2	3	22/8	6	6/8=0.75
3	6	37/8	5	5/8=0.625
4	5	32/8	0	0
5	0	7/8	7	7/8=0.875
6	7	42/8	2	2/8=0.25
7	2	17/8	1	1/8=0.125
8	1	12/8	4	4/8=0.5

Tabla 2. Generación de números aleatorios por el método congruencial mixto.

Cuando se quiere construir un generador de números aleatorios para simular los valores de una variable aleatoria, se deben elegir los parámetros de tal manera que se garantice un periodo largo para que se puedan hacer todos los ensayos de simulación, por lo tanto se deben tener en cuenta las siguientes condiciones:

- $a$  debe ser un número impar, no divisible ni por 3 ni por 5.
- $c$  usualmente puede ser cualquier constante, sin embargo, para asegurar buenos resultados, se debe seleccionar  $a$  de tal forma que,  $a \bmod 8 = 5$  para una computadora binaria, o  $a \bmod 200 = 21$  para computadora decimal.
- $m$  debe ser el número entero más grande que la computadora acepte.

De acuerdo con Hull y Dobell, los mejores resultados para un generador congruencial mixto en una computadora binaria son:

- $c = 8 \cdot a \pm 3$
- $a =$  cualquier entero
- $X_0 =$  Cualquier entero impar.
- $M = 2^b$  donde  $b > 2$  y que  $m$  sea aceptado por la computadora.

#### **4.4. PROBLEMAS PROPUESTOS.**

Determine el período de los siguientes generadores congruenciales mixtos:

- $X_{n+1} = (8 X_n + 16) \bmod 100$  y  $X_0 = 15$ .
- $X_{n+1} = (50 X_n + 17) \bmod 64$  y  $X_0 = 13$ .
- $X_{n+1} = (5 X_n + 24) \bmod 32$  y  $X_0 = 7$ .
- $X_{n+1} = (5 X_n + 21) \bmod 100$  y  $X_0 = 3$ .
- $X_{n+1} = (9 X_n + 13) \bmod 32$  y  $X_0 = 8$ .



Determine el período de los siguientes generadores congruenciales multiplicativos:

- $X_{n+1} = 203 X_n \bmod 10^5$  y  $X_0 = 17$ .
- $X_{n+1} = 211 X_n \bmod 10^8$  y  $X_0 = 19$ .
- $X_{n+1} = 221 X_n \bmod 10^3$  y  $X_0 = 3$ .
- $X_{n+1} = 5X_n \bmod 64$  y  $X_0 = 7$ .
- $X_{n+1} = 11 X_n \bmod 128$  y  $X_0 = 9$ .

Genere números aleatorios entre 0 y 1 con los siguientes generadores congruenciales y determine el ciclo de vida de cada uno.

- $X_{n+1} = (40 X_n + 13) \bmod 33$  y  $X_0 = 302$ .
- $X_{n+1} = (71 X_n + 57) \bmod 341$  y  $X_0 = 71$ .
- $X_{n+1} = (71 X_n + 517) \bmod 111$  y  $X_0 = 171$ .
- $X_{n+1} = (71561 X_n + 56822117) \bmod 341157$  y  $X_0 = 31767$ .
- $X_{n+1} = (723 X_n + 531) \bmod 314$  y  $X_0 = 927$ .
- $X_{n+1} = (452 X_n + 37452) \bmod 1231$  y  $X_0 = 4571$ .
- $X_{n+1} = (17 X_n) \bmod 37$  y  $X_0 = 51$ .
- $X_{n+1} = (16X_n + 4) \bmod 14$  y  $X_0 = 22$ .

Genere 50 números aleatorios entre 0 y 1 de 4 dígitos, mediante un generador de cuadrados medios cuya semilla sea:

- 4567234902.
- 3567345.
- 1234500012.

En cada caso calcule el valor esperado, la varianza y el histograma. Demuestre que los números generados provienen de una distribución uniforme con un nivel de aceptación del 90%.