UNIVERSIDAD
TECNOLÓGICA NACIONAL
FACULTAD REGIONAL
RESISTENCIA

CÁTEDRA: “SIMULACIÓN”

Docentes:
Ing. Carlos Vecchi
Ing. Dominga Concepción Aquino
Auxiliar Gabriela Dos Santos
Auxiliar Simón Leonardo Figueroa

NÚMEROS PSEUDOALEATORIOS

- Generación de números pseudoaleatorios
- Pruebas estadísticas para los números pseudoaleatorios

GENERACIÓN DE NÚMEROS PSEUDOALEATORIOS

- **Algoritmo de cuadrados medios**
- **Algoritmo de productos medios**
- **Algoritmo de multiplicador constante**
- **Algoritmo lineal**
- **Algoritmo congruencial multiplicativo**

UNIVERSIDAD
TECNOLÓGICA NACIONAL
FACULTAD REGIONAL
RESISTENCIA

GENERACIÓN DE NÚMEROS PSEUDOALEATORIOS

- **Algoritmo de cuadrados medios**

1) Seleccionar una semilla (X_0) con *D* dígitos (*D*>3).

2) Sea $Y_0 = (X_0)^2$; sea X_1 = *D* dígitos del centro; y sea r_1 = 0.*D* dígitos del centro.

3) Sea $Y_i = (X_i)^2$; sea X_{i+1} = *D* dígitos del centro; y sea r_{i+1} = 0.*D* dígitos del centro para toda i = 1, 2,...,n

4) Repetir el paso 3 hasta obtener los **n** números r_i deseados.

Nota: Si no es posible obtener los *D* dígitos del centro del número Y_i, agregue ceros a la izquierda del número Y_i.

- El algoritmo de cuadrados medios generalmente es incapaz de generar una secuencia de r_i con período de vida *n* grande. Además, en ocasiones sólo es capaz de generar un número.

  Por ejemplo:

  Si $X_0 = 1000$, entonces $X_1 = 0000$; $r_i = 0{,}0000$

  Se dice que el algoritmo se degenera con la semilla de

  $X_0 = 1000$.

Ejercicio: Generar los primeros **5** números r_i a partir de una semilla $\mathbf{X_0 = 5015}$, de donde se puede observar que D = 4 dígitos.

Tomo los 4 dígitos del centro

Se agrega un 0 (cero) a la izquierda de Y_i para obtener los 4 dígitos del centro

$Y_0 = (X_0)^2 = (5015)^2 = 25\underbrace{1502}25$	$X_1 = 1502$	$r_1 = 0{,}1502$
$Y_1 = (X_1)^2 = (1502)^2 = 2256004 = 02\underbrace{2560}04$	$X_2 = 2560$	$r_2 = 0{,}2560$
$Y_2 = (X_2)^2 = (2560)^2 = 6553600 = 06\underbrace{5536}00$	$X_3 = 5536$	$r_3 = 0{,}5536$
$Y_3 = (X_3)^2 = (5536)^2 = 30\underbrace{6472}96$	$X_4 = 6472$	$r_4 = 0{,}6472$
$Y_4 = (X_4)^2 = (6472)^2 = 41\underbrace{8867}84$	$X_5 = 8867$	$r_5 = 0{,}8867$

GENERACIÓN DE NÚMEROS PSEUDOALEATORIOS

- **Algoritmo de productos medios**

1) Seleccionar una semilla (X_0) con *D* dígitos (*D*>3).

2) Seleccionar una semilla (X_1) con *D* dígitos (*D*>3).

3) Sea $Y_0 = X_0 * X_1$; sea $X_2 = D$ dígitos del centro; y sea $r_1 = 0.D$ dígitos del centro.

4) Sea $Y_i = X_i * X_{i+1}$; sea $X_{i+2} = D$ dígitos del centro; y sea $r_{i+1} = 0.D$ dígitos del centro para toda i = 1, 2,...,n.

5) Repetir el paso 4 hasta obtener los **n** números r_i deseados.

Nota: Si no es posible obtener los *D* dígitos del centro del número Y_i, agregue ceros a la izquierda del número Y_i.

<u>Ejercicio</u>: Generar los primeros **5** números r_i a partir de las semillas $\mathbf{X_0 = 5115}$ y $\mathbf{X_1 = 5736}$; observe que ambas semillas tienen D = 4 dígitos.

Tomo los 4 dígitos del centro

$Y_0 = (X_0)*(X_1) = (5115)*(5736) = 29\underbrace{3396}40$	$X_2 = 3396$	$r_1 = 0{,}3396$
$Y_1 = (X_1)*(X_2) = (5736)*(3396) = 19\underbrace{4794}56$	$X_3 = 4794$	$r_2 = 0{,}4794$
$Y_2 = (X_2)*(X_3) = (3396)*(4794) = 16\underbrace{2804}24$	$X_4 = 2804$	$r_3 = 0{,}2804$
$Y_3 = (X_3)*(X_4) = (4794)*(2804) = 13\underbrace{4423}76$	$X_5 = 4423$	$r_4 = 0{,}4423$
$Y_4 = (X_4)*(X_5) = (2804)*(4423) = 12\mathbf{4020}92$	$X_6 = 4020$	$r_5 = 0{,}4020$

GENERACIÓN DE NÚMEROS PSEUDOALEATORIOS

- **Algoritmo de multiplicador constante**

1) Seleccionar una semilla (X_0) con *D* dígitos (*D*>3).

2) Seleccionar una constante (**a**) con *D* dígitos (*D*>3).

3) Sea $Y_0 = a*X_0$; sea $X_1 = D$ dígitos del centro; y sea $r_1 = 0.D$ dígitos del centro.

4) Sea $Y_i = a*X_i$; sea $X_{i+1} = D$ dígitos del centro; y sea $r_{i+1} = 0.D$ dígitos del centro para toda i = 1, 2,...,n.

5) Repetir el paso 4 hasta obtener los **n** números r_i deseados.

Nota: Si no es posible obtener los *D* dígitos del centro del número Y_i, agregue ceros a la izquierda del número Y_i.

Ejercicio: Generar los primeros **5** números r_i a partir de la semilla **X_0=5115** y con la constante **a=3624**. Observe que tanto la semilla como la constante tienen D = 4 dígitos.

$Y_0 = (X_0)^*a = (5115)^*(3624) = 18\mathbf{5367}60$	$X_1 = 5367$	$r_1 = 0{,}5367$
$Y_1 = (X_1)^*a = (5367)^*(3624) = 19\mathbf{4500}08$	$X_2 = 4500$	$r_2 = 0{,}4500$
$Y_2 = (X_2)^*a = (4500)^*(3624) = 16\mathbf{3080}00$	$X_3 = 3080$	$r_3 = 0{,}3080$
$Y_3 = (X_3)^*a = (3080)^*(3624) = 11\mathbf{1619}20$	$X_4 = 1619$	$r_4 = 0{,}1619$
$Y_4 = (X_4)^*a = (1619)^*(3624) = 05\mathbf{8672}56$	$X_5 = 8672$	$r_5 = 0{,}8672$

GENERACIÓN DE NÚMEROS PSEUDOALEATORIOS

- **Algoritmo lineal**

Genera una secuencia de números enteros $S=\{0,1,2,\ldots,m-1\}$ por medio de la siguiente ecuación recursiva:

$$X_{i+1} = (\mathbf{a} * X_i + \mathbf{c}) \bmod (\mathbf{m}) \qquad i = 0, 1, 2, \ldots, n$$

donde:

X_0 es la semilla; $X_0 > 0$
a es la constante multiplicativa; **a** > 0
c es una constante aditiva; **c** > 0
m es el módulo; **m** > 0

deben ser números enteros

Para obtener números pseudoaleatorios en el intervalo (0,1) se requiere la siguiente ecuación:

$$r_i = \frac{X_i}{m-1} \qquad i = 1, 2, \ldots, n$$

Condiciones que los parámetros deben cumplir para alcanzar el máximo período de vida **n**:

$m = 2^g$
$a = 1+4*k$
k debe ser entero
c relativamente primo a **m**
g debe ser entero

Bajo estas condiciones se obtiene un período de vida máximo:

$N = m = 2^g$

Conclusión: si no se cumple alguna de las condiciones, el período de vida máximo **N = m** no se garantiza, por lo que el período de vida será menor que **m**.

Ejercicio N° 1: Generar **4** números entre 0 y 1 con los siguientes parámetros:

$X_0 = 37$
a = 19
c = 33
m = 100

Nota: Se dice que dos números son relativamente primos si su factor común más grande es 1.
Los factores de **33** son: 1; 3; 11; 33
Los factores de **100** son: 1; 2; 4; 5; 10; 20; 25; 50
El único factor común es **1**.
Por lo tanto 33 y 100 son relativamente primos.

Ejercicio N° 2: Generar suficientes números entre 0 y 1 con los parámetros $X_0 = 6$, $k = 3$, $g = 3$ y $c = 7$, hasta encontrar el período de vida máximo (N).

Ejercicio N° 3: Consideremos nuevamente el ejercicio anterior, pero tratemos de violar arbitrariamente alguna de las condiciones.

Supongamos que **a** = 12; se sabe que **a** no es el resultado de 1 + 4*k, donde **k** es un entero. Veamos el comportamiento del algoritmo congruencial lineal ante tal cambio.

GENERACIÓN DE NÚMEROS PSEUDOALEATORIOS

- **Algoritmo congruencial multiplicativo**

Surge del algoritmo congruencial lineal cuando **c = 0**. Entonces la ecuación recursiva es:

$$X_{i+1} = (\mathbf{a} * X_i) \bmod (\mathbf{m}) \qquad i = 0,1, 2,\ldots,n$$

donde:

X_0 es la semilla; $X_0 > 0$ e impar
a es la constante multiplicativa; **a** > 0
m es el módulo; **m** > 0

deben ser números enteros

Para obtener números pseudoaleatorios en el intervalo (0,1) se requiere la siguiente ecuación:

$$r_i = \frac{X_i}{m-1} \qquad i = 1, 2,\ldots,n$$

Condiciones que los parámetros deben cumplir para alcanzar el máximo período de vida **N**:

$m = 2^g$

$a = 3+8*k$ ó $a = 5+8*k$

k = 0,1,2,3,… debe ser entero

X_0 debe ser un número impar

g debe ser entero

A partir de estas condiciones se logra un período de vida máximo:

$$\mathbf{N = m/4 = 2^{g-2}}$$

<u>Nota</u>: Toda vez que la semilla X_0 se repite, volverán a generarse los mismos números.

Ejercicio N° 1: Generar suficientes números entre 0 y 1 con los siguientes parámetros:

$X_0 = 17$, $k = 2$ y $g = 5$, hasta encontrar el período o ciclo de vida.

Nota: Para calcular **a** utilice la siguiente ecuación: $a = 5+8*k$

Ejercicio N° 2: Consideremos nuevamente el ejercicio anterior, pero tratemos de violar arbitrariamente la condición de que la semilla sea un número impar. Supongamos que $X_0 = 12$.

Veamos el comportamiento del algoritmo congruencial multiplicativo ante tal cambio.