



Generadores de números pseudoaleatorios

750098M Simulación computacional

Contenido



- 1 Introducción
- 2 Pruebas de bondad
- 3 Secuencia en otras distribuciones
- 4 Práctica

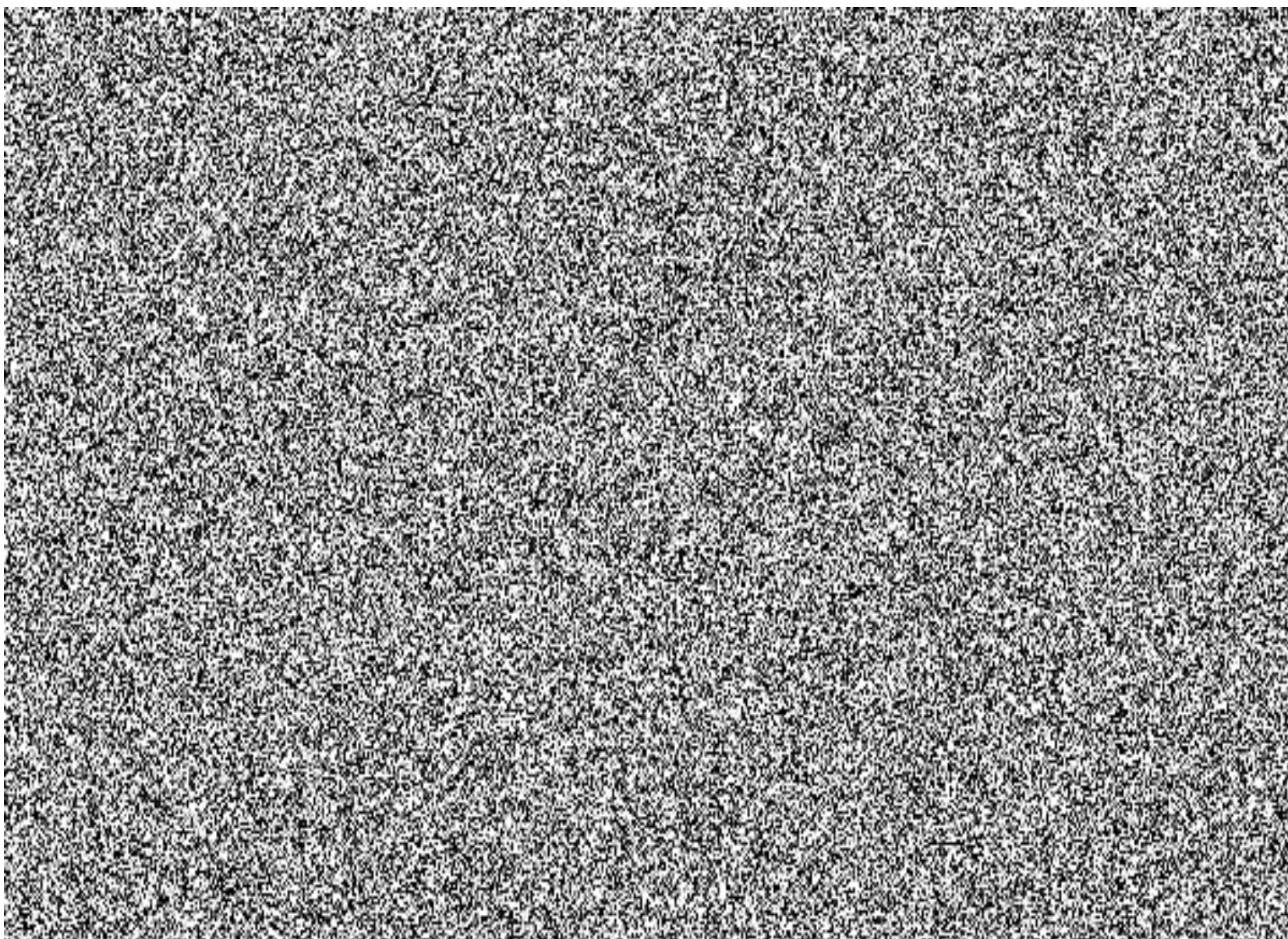
Qué es un número aleatorio?

Es un número generado por un proceso sistemático, cuya salida es impredecible y que no puede ser reproducido

Una secuencia es aleatoria si la cantidad de información que contiene, de acuerdo a la teoría información de Shannon, es también finita.

<http://www.randomnumbers.info/content/Random.htm>

Aparición en la naturaleza



1

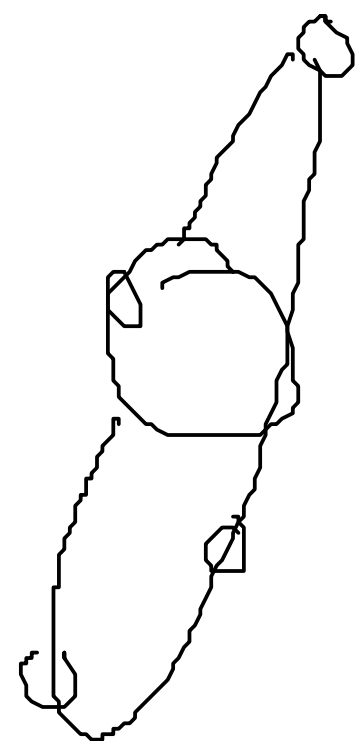
Ruido blanco

2

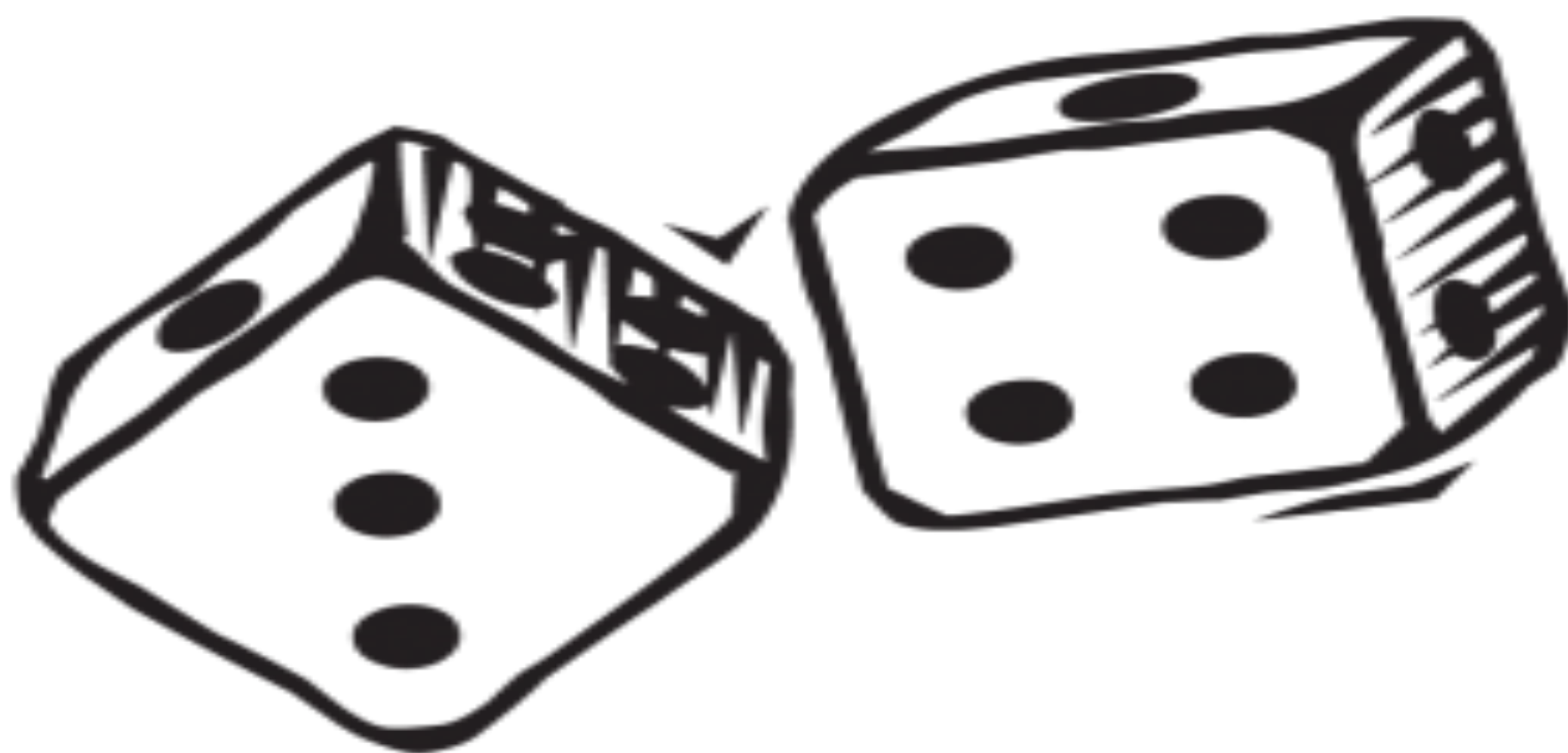
Movimiento de esporas de
helecho

3

Lanzar dados



Existe el azar?



Lanzar dados es aleatorio?

<https://www.youtube.com/watch?>

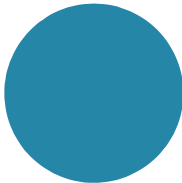
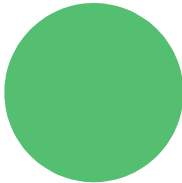

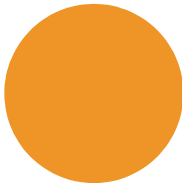
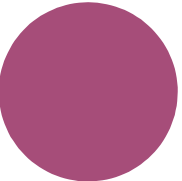
Una definición

Algo es aleatorio si es algorítmicamente incompresible o irreducible.

Exploring RANDOMNESS G J Chaitin, IBM Research
Published by Springer-Verlag London, 2001, ISBN
1-85233-417-7



Aplicaciones

-  Simulación
-  Muestreo
-  Análisis numérico
-  Programación computacional
-  Toma de decisiones

Diferencias

Números aleatorios	Números pseudoaleatorios
Son datos continuos	Puede resultar en datos discretos (si son generados en el computador, siempre son discretos)
<p>Siguen distribución uniforme $U(0,1)$</p> <p>media $1/2$ varianza $1/12$</p>	<p>Si se divide el intervalo $[0,1]$ en subintervalos iguales pueden resultar intervalos donde caen significativamente más o menos datos que el número esperado</p> <p>media por encima o por debajo de $1/2$ varianza por encima o por debajo de $1/12$</p>
Los datos son independientes: una observación no depende de las observaciones anteriores; no hay ninguna clase de patrón	<p>Se pueden presentar regularidades como:</p> <ul style="list-style-type: none"> periodicidad autocorrelación patrones de crecimiento-decrecimiento patrones de valores encima o por de bajo de la mediay muchos más

Qué es un número pseudoaleatorio?

- Es un número generado por una distribución uniforme.
- Un verdadero número aleatorio necesita una fuente impredecible y no reproducible.
- Una estrategia es usar algoritmos matemáticos para generar cadenas de números aleatorios.
- Estos algoritmos reproducen números de una forma determinística, dependiendo de la semilla

Características

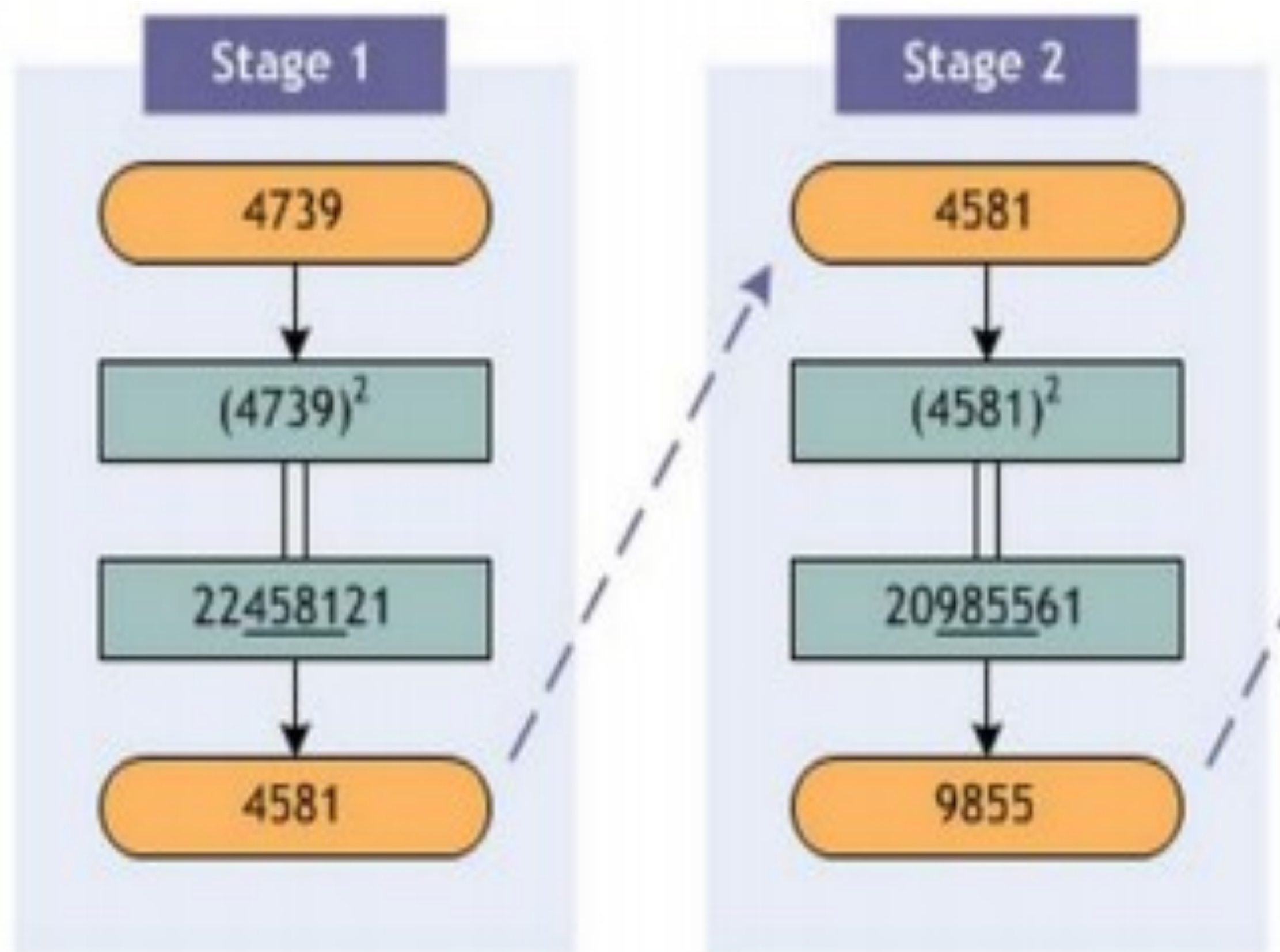
- Uniformemente distribuido
- Dependencia estadística
- Reproducible
- No se repite ningún número en una longitud dada
- Usan una semilla

Consideraciones

- Uniformidad: en cualquier punto del tiempo, la ocurrencia de 0 o no 0 es igual de probable
- Escalabilidad: Si una secuencia es aleatoria, cualquier subsecuencia debe ser aleatoria
- Consistencia: El comportamiento del generador debe ser bueno con varias semillas

Método Von Neumann

1. 4739
2. $(4739)^2 = 22458121$
3. $22458121 \rightarrow 4581$
4. $(4581)^2 = 20985561$
5. $20985561 \rightarrow 9855$
6. $(9855)^2 = 97121025$



Es conocido como método de los números cuadrados medios

Preocupaciones



- Velocidad de algoritmo
- Fácil implementación
- Técnicas de paralelización
- Implementación portable

Generadores de números pseudoaleatorios

- Produce números enteros X_i uniformemente en $(0, X_{MAX})$
- Se normalizan $(0-1)$ mediante: $u_i = x_i / x_{MAX}$
- Su periodo es hasta que se repite un número (por qué?)
- Un periodo completo es igual a x_{MAX} (por qué?)

Método Congruencia Lineal

Dada una semilla dada X_0 y unos enteros a, c y m :

- 1 $X_{n+1} = (a * x_n + c) \text{ MOD } m$
- 2 Repite $X_n = X_{n+1}$ las veces que sean necesarias

Método Congruencia Lineal

Por ejemplo para $X_0=7$, $a=1$, $c=7$ y $m=10$:

1 $X_1 = (1 \cdot 7 + 7) \bmod 10 = 4$

2 $X_2 = (1 \cdot 4 + 7) \bmod 10 = 1$

3 $X_3 = (1 \cdot 1 + 7) \bmod 10 = 8$

4 $X_4 = (1 \cdot 8 + 7) \bmod 10 = 5$

$$X_5 = (5 + 7) \bmod 10$$

$$X_5 = 2$$

$$X_6 = 9$$

$$X_7 = 3$$

$$X_7 = 6$$

$$X_8 = 7$$

Ahora para $x_0=4$, $a=1$, $c=3$ y $m=5$ haga los 6 primeros pasos

$$X_9 = 0$$

$$(aX_n + c) \bmod m$$

$$X_0 = 4$$

$$X_1 = 2$$

$$X_2 = 0$$

$$X_3 = 3$$

$$X_4 = 1$$

$$X_5 = 4$$

$$1) \ a = 3 \ c = 2 \ m = 10, X_0 = 3$$

$$x_0 = 3, \ x_1 = 1, \ x_2 = 5, \ x_3 = 7, \\ x_4 = 3$$

$$\text{Teorico} = 10 \ (0 \text{ ---- } 9)$$

$$p_e = 4$$

$$2) \ a = 5 \ c = 6 \ m = 8, x_0 = 4$$

$$\text{Teorico} \ (0 \text{ } 7) \ 8$$

$$x_0 = 4, \ x_1 = 2, \ x_2 = 0, \ x_3 = 6, \ x_4 = 4$$

$$4$$

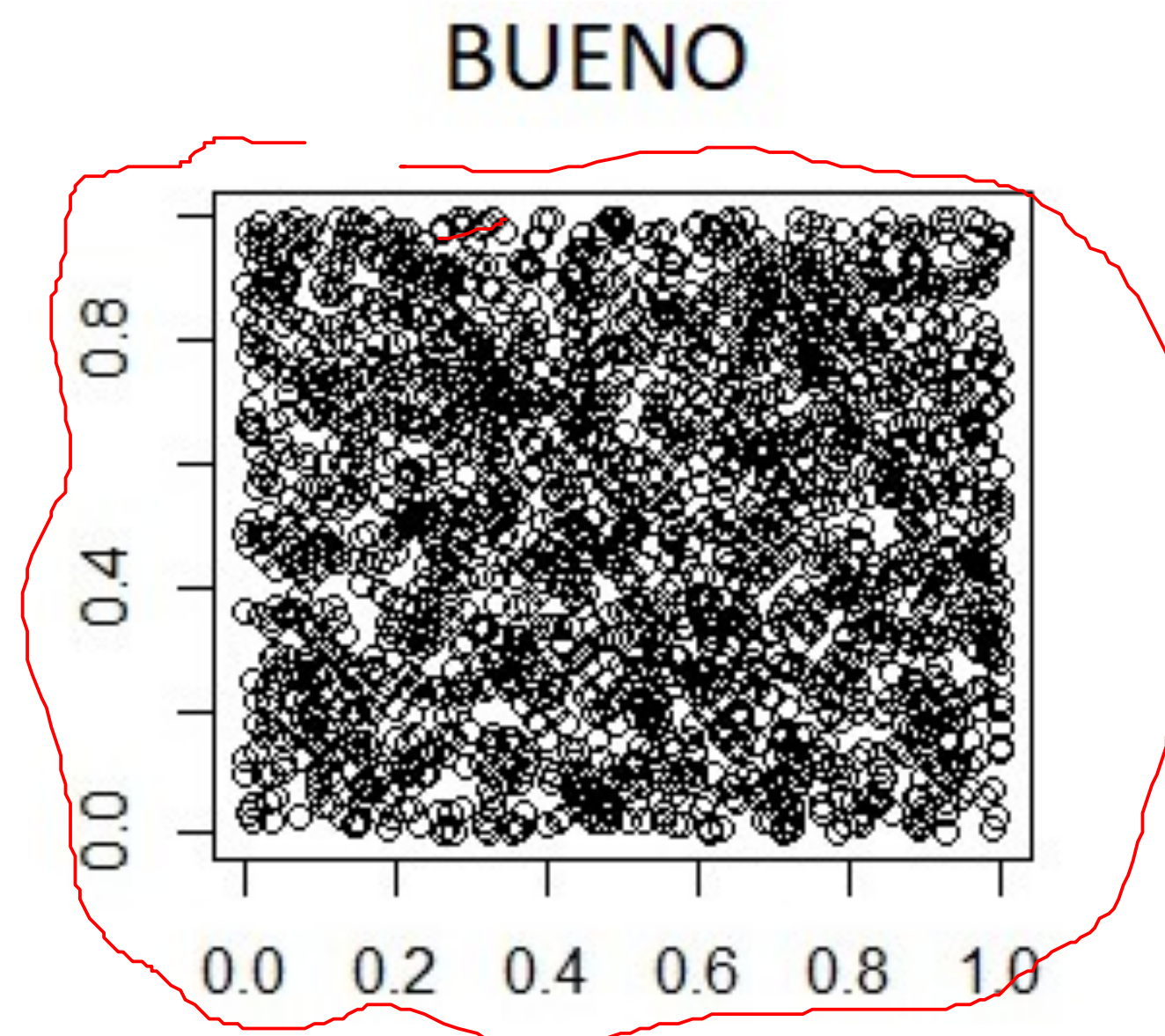
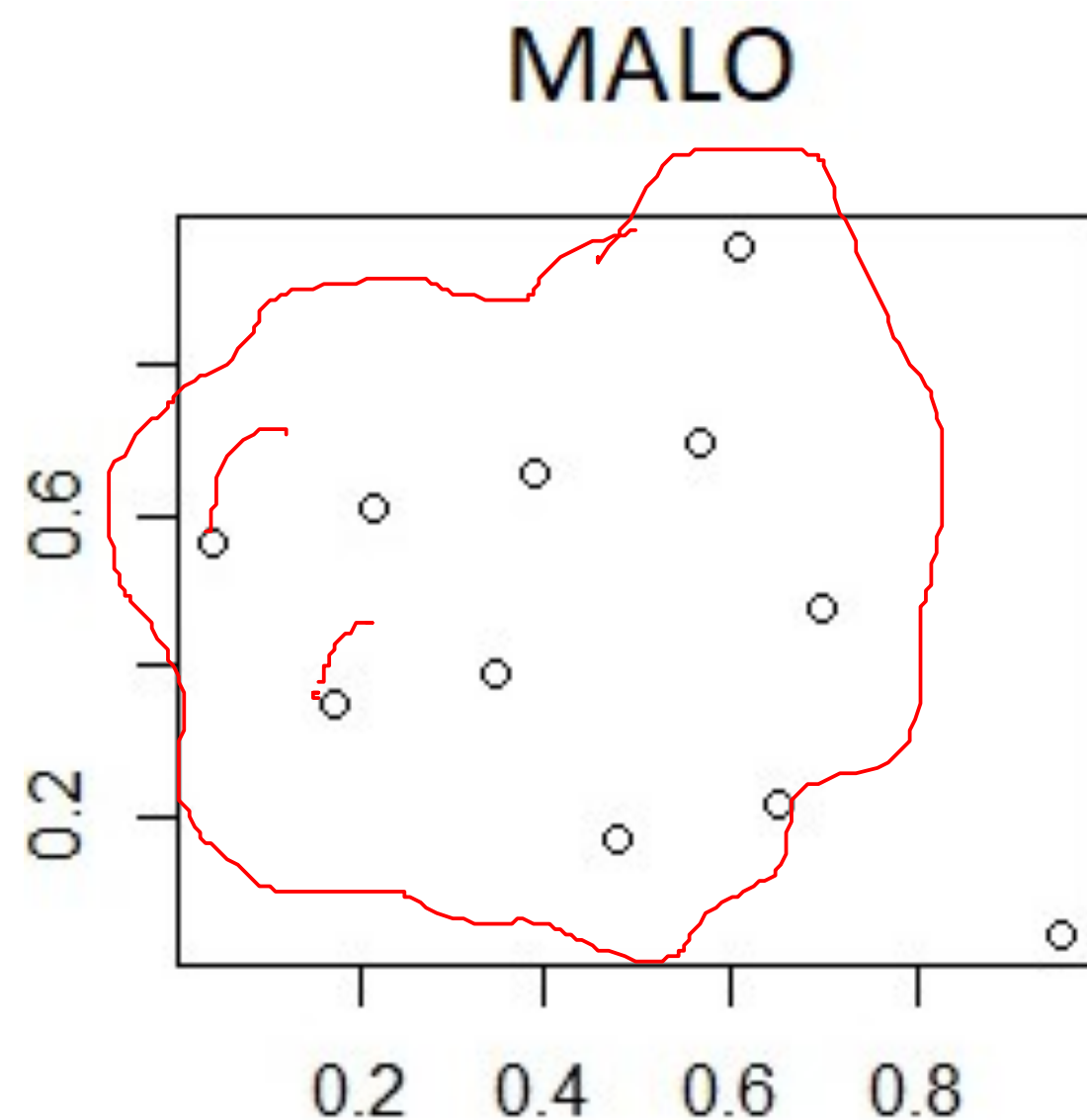
$$X_n = X_{n-1} + 2$$

$$X_n = X_{n-1} + 3X_{n-2}$$

Método general de congruencia

La expresión general es: $x_{i+1} = f(x_i, x_{i-1})(\text{mod } m)$

Donde $f()$ es una función de los números previamente generados



Seleccionar el m

$$O \bmod m$$

$$\begin{array}{r} 16 \dots 3 \ 2 \ 1 \\ \hline 17 \end{array}$$

- La secuencia de números es finita
- La secuencia es máximo $m \rightarrow m$ debe ser grande
- Se recomienda que ~~m~~ debe ser un número primo
- Se recomienda que m sea una potencia de 2

$$\begin{array}{r} 11010 \\ \hline 100 \end{array} \rightarrow 110/10 \quad \begin{array}{r} 1110 \\ \hline 10 \end{array} = 111$$

3 → 00000001 } and Short

5 → 000010

1 000001 ALU

↘

Otras selecciones



- $0.01m < a < 0.99m$
- Que pasa cuando $c=0$? (más rápido, periodo corto)
- ¿Cómo escoger el x_0 ? reloj, ultimo valor, etc
- ¿Que pasa si selecciono un mismo valor de x_0 ?

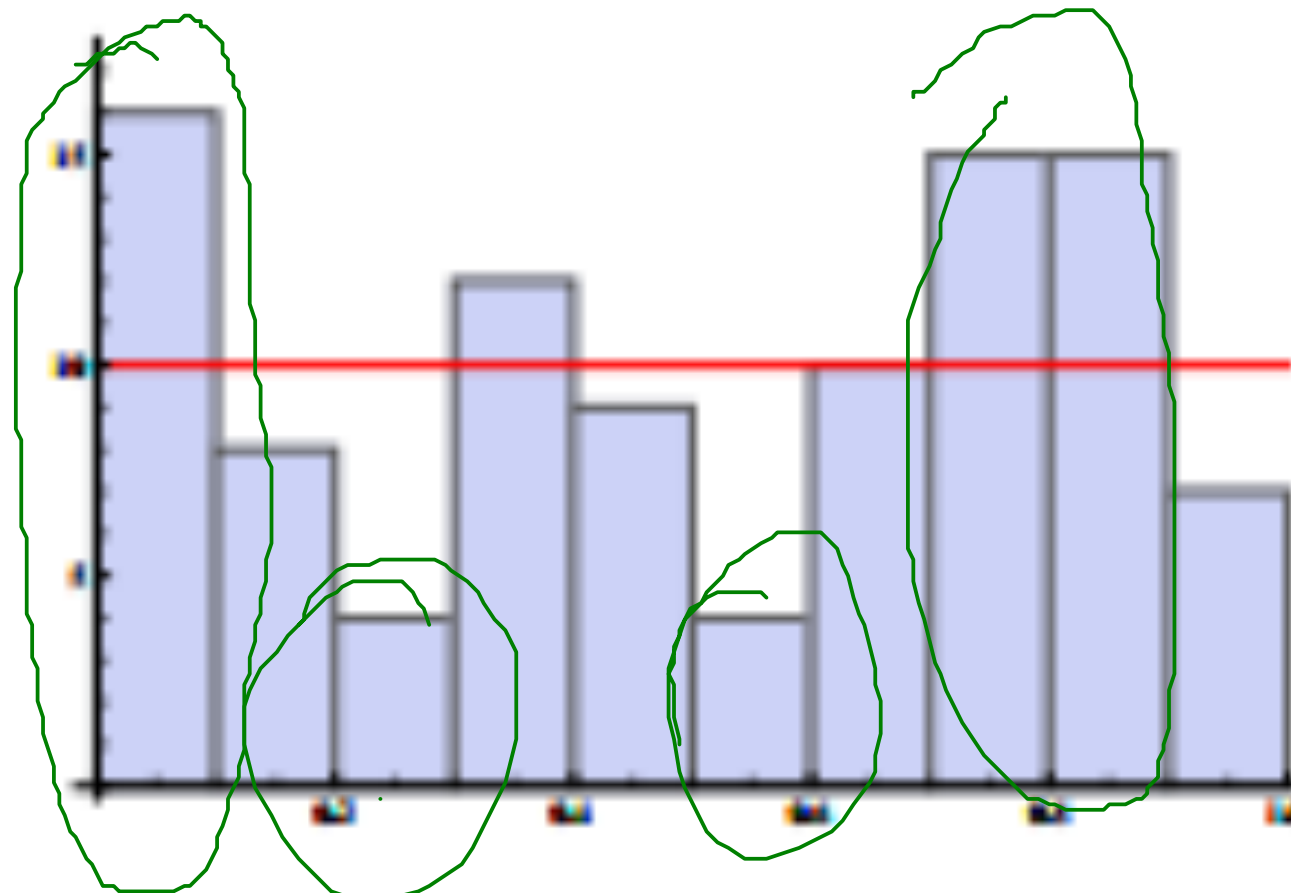
Ejemplos,Cuál es mejor?

$$X_0 = 5$$

$$a = 255$$

$$c = 100$$

$$m = 1032$$

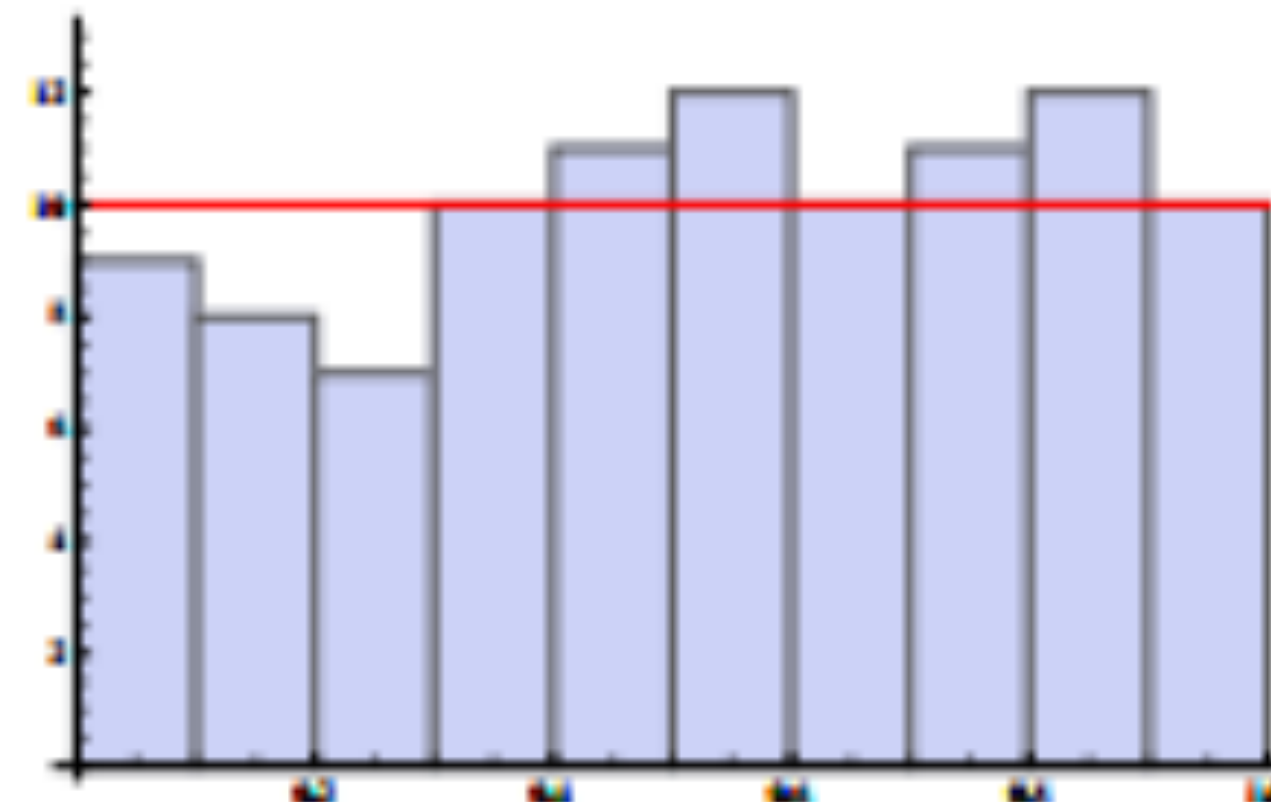


$$X_0 = 5$$

$$a = 255$$

$$c = 100$$

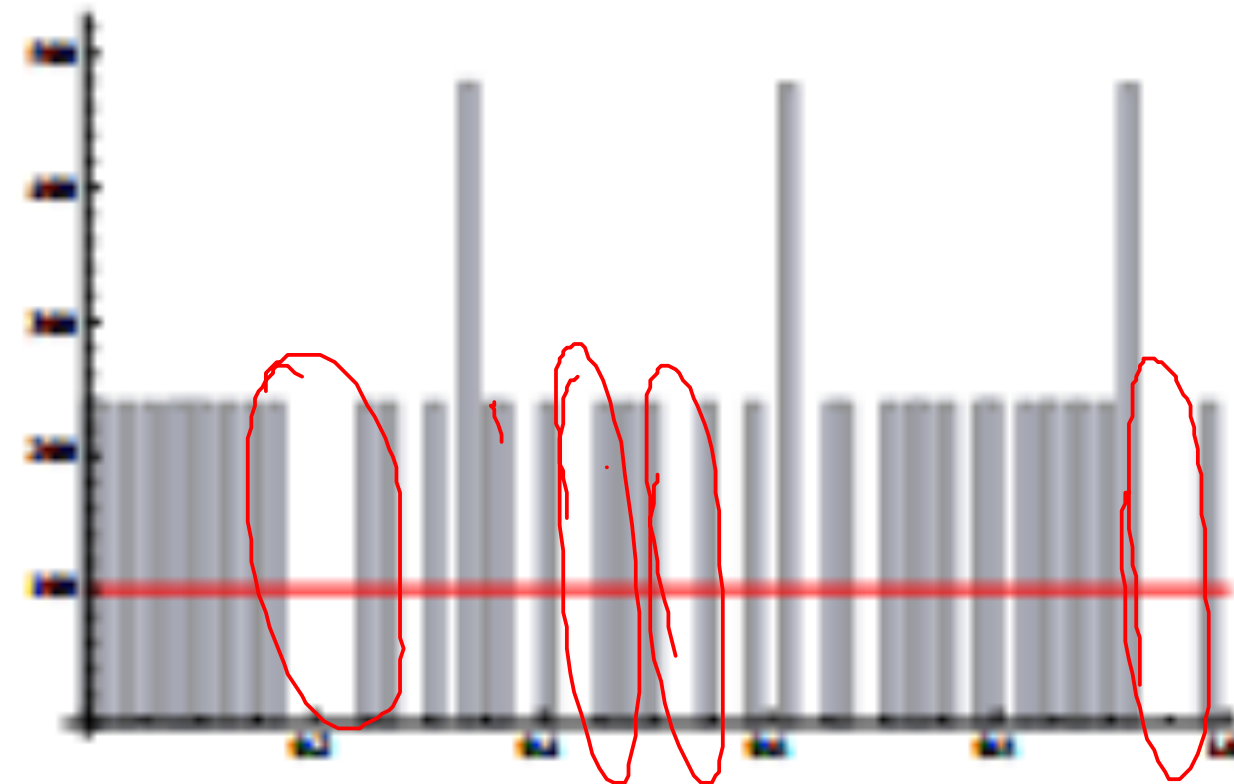
$$m = 1031$$



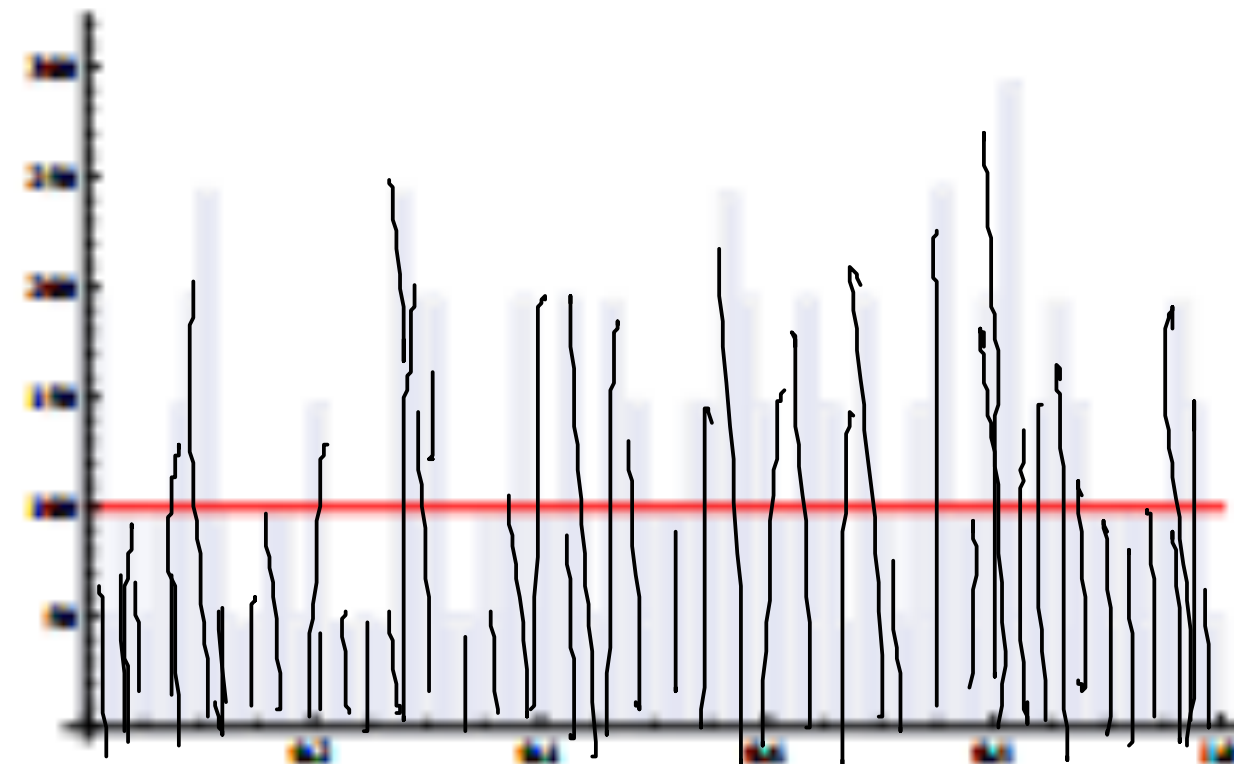
100 Datos

Ejemplos,Cuál es mejor?

$X_0 = 5$
 $a = 255$
 $c = 100$
 $m = 1032$



$X_0 = 5$
 $a = 255$
 $c = 100$
 $m = 1031$



10000 Datos

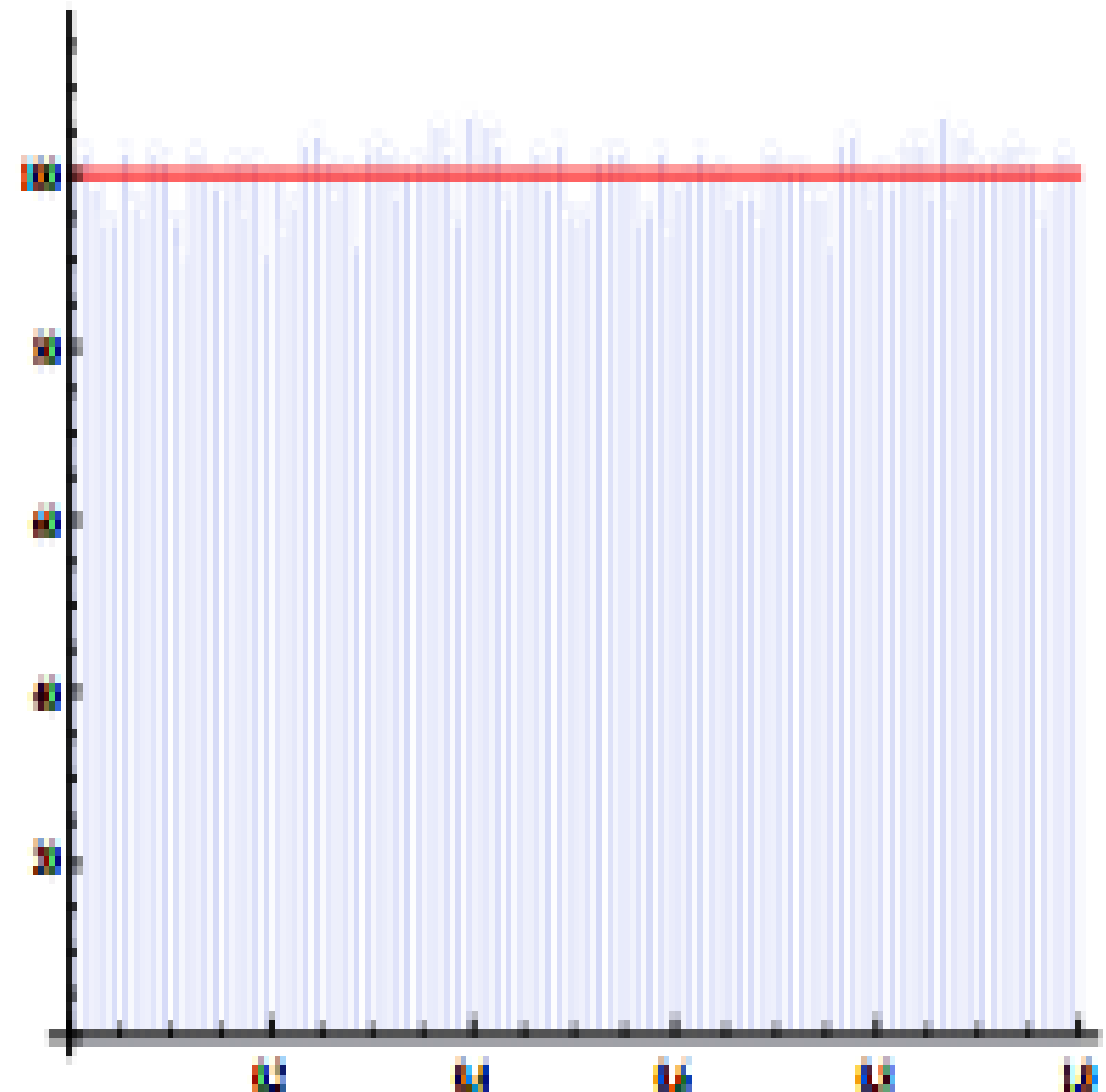
Un excelente generador

$$a = 106$$

$$c = 1283$$

$$m = 6075$$

$$X_0 = 5$$



Generador estándar mínimo (GEM)

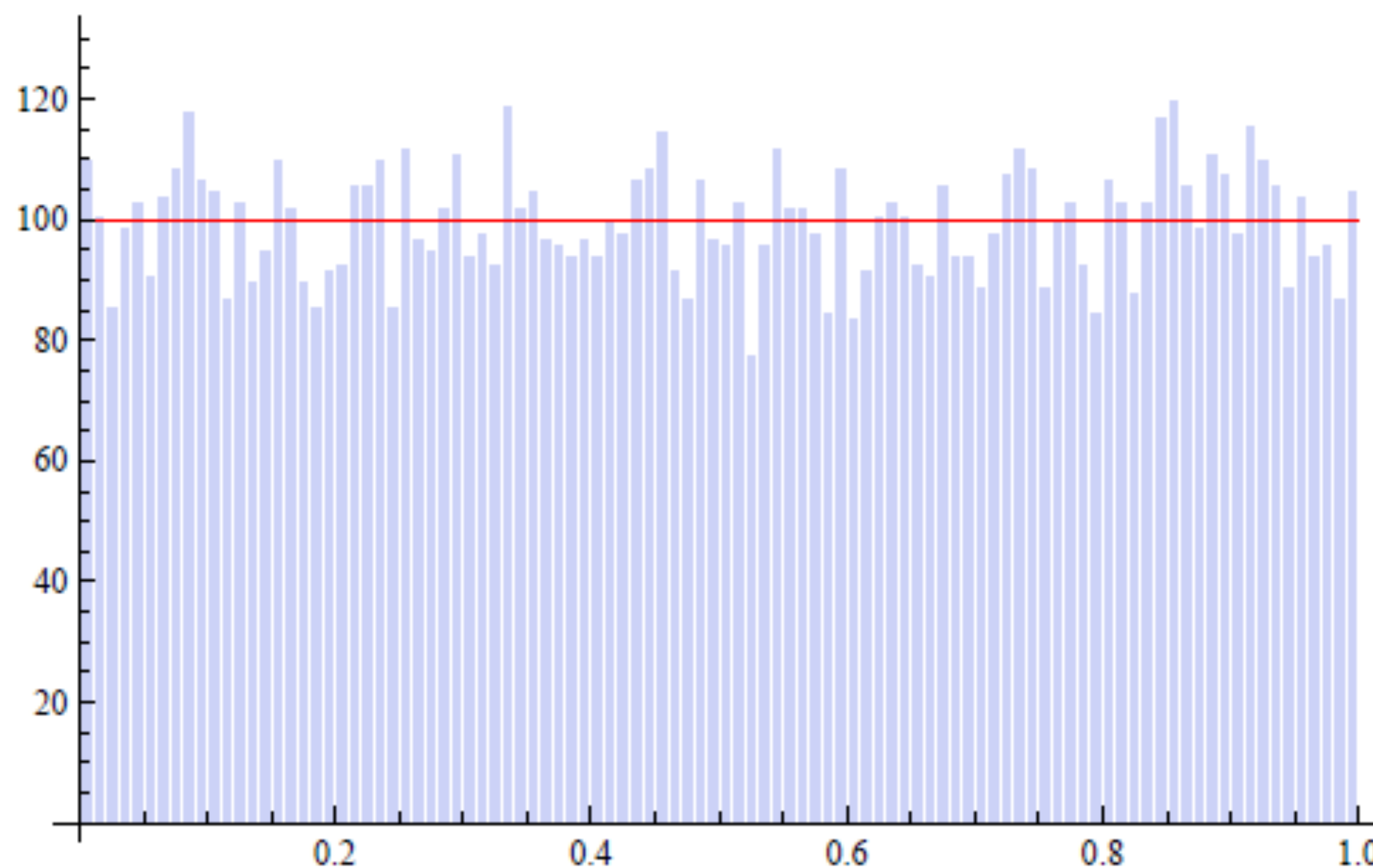
$$a = 7^5 = 16807 \quad c = 0 \quad m = 2^{31} - 1$$

- Cumple con las exigencias para ser un buen generador
- Se debe garantizar que no se use 0 como semilla
- Su periodo es $m - 1$

$$2^{31} - 1 \quad 31$$

Generador estándar mínimo (GEM)

Histograma con 10000 puntos del generador de estándar mínimo



Generador Fibonacci (LFG)

La secuencia Fibonacci es 0,1,1,2,3,5,8,13,21,...

$$X_n = X_{n-1} + X_{n-2}$$

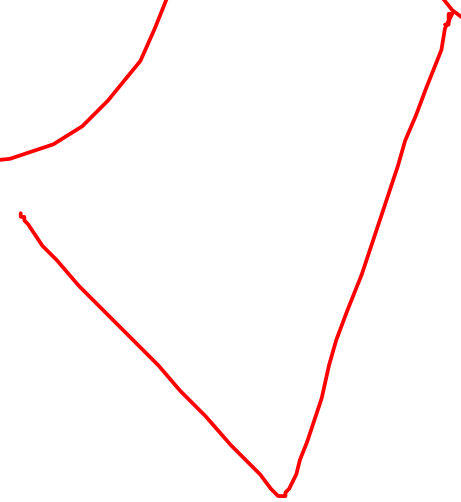
El generador se puede expresar entonces en:

$$X_n = (X_{n-j} \text{ Op } X_{n-k}) \bmod m$$

Donde $0 < j < k$ y OP es sumar o multiplicar

$$(X_{n-1} \text{ Op } X_{n-2}) \bmod m$$

$$F(n) = F_{n-1} + F_{n-2}$$



2 Anteriores

LFG Aditivo vs Multiplicativo

Aditivo

$$X_n = X_{n-j} + X_{n-k} \bmod m$$

Multiplicativo

$$X_n = X_{n-j} * X_{n-k} \bmod m$$

Un periodo $m^k - 1$ si m es primo

m es por lo general 2^{32} o 2^{64}

$$X_n = X_{n-10} * X_{n-7} \bmod m$$

/dev/random

random

$$X_n \equiv 9X_{n-1} \pmod{m}$$

$$q=3$$

$$m=10$$

$$X_0 = 0$$

$$X_0 = 0$$

$$X_1 \equiv 0 \pmod{10} = 0$$

$$X_2 \equiv 0$$

$$X_3 = 0$$

$$X_{100} = 0$$

1) $m = 10$, $X_0 = 3$, $X_1 = 6$

$x_n = x_{n-1}OP\ x_{n-2} \bmod 10$

Aditivo

$$x_2 = 9$$

$$x_3 = 5$$

$$x_4 = 4$$

$$x_5 = 9$$

$$x_6 = 3$$

$$x_{12} = 1$$

$$x_{14} = 1$$

$$x_{16} = 2$$

$$x_{18} = 5$$

$$x_7 = 2$$

$$x_8 = 5$$

$$x_9 = 7$$

$$x_{10} = 2$$

$$x_{11} = 9$$

$$x_{13} = 0$$

$$x_{15} = 1$$

$$x_{17} = 3$$

$$x_{19} = 8$$

$$x_{20} = 3$$

$$x_{21} = 1$$

$$x_{22} = 4$$

$$x_{23} = 5$$

$$x_{24} = 9$$