

ARTICULO CIENTIFICO

Generación de Números Aleatorios

Merino Vidal Mateo Alejandro

Universidad Mayor de San Simón
Cochabamba, Bolivia
202301308@est.umss.edu

Abstract

El presente trabajo se realizó mediante el análisis sistemático del comportamiento de diversos generadores de números aleatorios, estudiando tanto sus propiedades fundamentales como su naturaleza, con el fin de determinar su longitud de período y evaluar su calidad. Este enfoque permitió establecer criterios claros al momento de seleccionar un generador, asegurando así que este sea el adecuado para cada contexto de aplicación.

Keywords: [generador, aleatoriedad, periodo, semilla]

1. Introducción

En la actualidad, los sistemas informáticos requieren de valores aleatorios para diversos procesos, especialmente en el tema de simulaciones, con el fin de poder tomar diferentes caminos en un proceso y modelar escenarios complejos de la vida real.

La generación de números aleatorios es un tema que hoy en día es aplicado a diversos campos, especialmente en la criptografía y la seguridad informática, permitiendo encriptar datos o crear valores útiles como llaves o keys, garantizando la seguridad en cuanto a la transmisión de la información.

Un ejemplo de su aplicación es la conexión cliente-servidor en el desarrollo web, ya que durante el proceso de sincronización, la información debe viajar de forma segura para evitar que esta misma sea interceptada, por lo que es necesario encriptarla y generar una llave o key para descifrarla, basada en la combinación de los números aleatorios generados tanto por el cliente como el servidor.

Alrededor del mundo, existen múltiples fuentes de números aleatorios, pero cada uno cuenta con un nivel de calidad con respecto a su aleatoriedad. Sin embargo, los generadores más puros se encuentran en la naturaleza, sobre todo en diversos fenómenos como el ruido atmosférico o el decaimiento radiactivo, debido a su comportamiento impredecible, ya que no existe un patrón. Por lo tanto, se considera a la propia naturaleza como un generador de números aleatorios puro.

La informática ha tratado de replicar estos resultados, pero al no poder integrar fuentes naturales de forma práctica en todos los sistemas, se optó por el desarrollo de generadores pseudoaleatorios. Estos parten de una fórmula matemática o algoritmo, a partir de una semilla inicial, para generar

una secuencia de números considerada impredecible, al menos hasta que se logre encontrar un patrón o rasgo simétrico en su comportamiento.

2. Antecedentes

La aleatoriedad es una característica de los fenómenos que ha estado presente en la vida del ser humano desde hace siglos. Inicialmente, al ser un campo desconocido y de interés para su análisis, se plantearon diversos métodos para estudiarlo como el lanzamiento de monedas, dados o la extracción de bolas de un recipiente, siendo efectivos en su época.

Sin embargo, debido a que estos métodos clásicos eran demasiado lentos e ineficientes, se optó por tomar un nuevo rumbo aprovechando los avances de la computación. Esto surgió de la necesidad de que los ordenadores imitaran el azar para realizar cálculos complejos, lo que llevó a los científicos a desarrollar las primeras fórmulas matemáticas capaces de generar secuencias de números que, a simple vista, parecían aleatorias. Este desarrollo marcó el nacimiento de los generadores pseudoaleatorios, que se convirtieron en la base fundamental de la aleatoriedad en la computación.

Cabe recalcar que, a diferencia del azar puro de la naturaleza, los generadores pseudoaleatorios dependen de una "semilla" o valor inicial. Si se usa la misma semilla, se obtendrá exactamente la misma secuencia de números, lo que los hace deterministas, pero si la semilla es desconocida, la secuencia resulta impredecible para la mayoría de las aplicaciones prácticas.

A medida que paso el tiempo, la creciente dependencia de los sistemas informáticos exigió que estos generadores fueran más rápidos, eficientes y, sobre todo, más difíciles de predecir. Esto llevó a crear una serie de pruebas y estándares de calidad para poder determinar que tan "aleatorio" es un generador en realidad. Estas pruebas buscan detectar patrones, repeticiones o sesgos en las secuencias numéricas que podrían revelar su origen artificial.

Fue esta necesidad constante de mejorar y validar la calidad del azar computacional la que dio origen a diversas investigaciones a lo largo de la historia con el objetivo de encontrar un equilibrio entre la velocidad, la eficiencia y la aleatoriedad verdadera.

Gracias a esto, surgieron diferentes familias de algoritmos, cada una con sus propias ventajas y limitaciones. Algunos se optimizaron para ser extremadamente rápidos en simulaciones que requieren millones de valores, mientras que otros se enfocaron en la seguridad, priorizando la imposibilidad de predecir el siguiente número incluso conociendo parte de la secuencia. Esta especialización permitió adaptar los generadores a necesidades específicas, desde videojuegos hasta transacciones bancarias.

Hoy en día, con el auge de la inteligencia artificial y el aprendizaje automático, la demanda de números aleatorios de alta calidad es elevada, ya que los sistemas los utilizan para inicializar parámetros, realizar muestreos y añadir ruido que prevenga el sobre-ajuste.

3. Marco Teórico

3.1 Probabilidad y Estadística

La estadística es una ciencia por naturaleza experimental que se ha desarrollado a lo largo del tiempo, brindando aportes significativos en múltiples áreas como la medicina, la economía y la tecnología. Gracias a ella, es posible aplicar métodos científicos para recopilar, organizar, resumir y analizar datos, lo que permite identificar patrones y extraer conclusiones válidas.

Al trabajar con situaciones al azar, se da la aparición de diversos eventos, que ayudan a reconocer cuándo un resultado influye en otro o cuándo suceden de forma aislada. Estos sucesos pueden ser independientes o dependientes.

- **Eventos dependientes:** Sucesos en los que el resultado de uno influye directamente en el otro. Es decir, lo que ocurra primero afecta la probabilidad de lo que pase después. En este tipo de eventos existe una relación que obliga a considerar ambos sucesos de manera conjunta.
- **Eventos independientes:** Son sucesos en los que el resultado de uno no cambia la probabilidad del otro. Cada acontecimiento ocurre sin que el anterior o posterior lo modifique. Se caracterizan porque pueden analizarse de forma aislada sin alterar el cálculo de probabilidades.

La distribución de probabilidad sirve para mostrar cómo se reparten las posibilidades en una variable. Más allá de los números, ayuda a imaginar distintos escenarios y a darles sentido a los resultados.

- **Distribución de probabilidad:** Forma en que se reparten las probabilidades entre los diferentes resultados de una variable. Permite saber qué tan posible es cada valor en un fenómeno aleatorio.

Dentro de estas representaciones se encuentran las distribuciones uniformes y no uniformes, que se diferencian por la forma en que se comportan. En las primeras, todo tiene la misma oportunidad de suceder, mientras que en las segundas hay resultados que aparecen más seguido que otros.

- **Distribución uniforme:** Es aquella en la que todos los resultados posibles tienen la misma probabilidad de ocurrir, permitiendo representar una situación justa y equilibrada.
- **Distribución no uniforme:** Es aquella en donde algunos resultados son más probables que otros, permitiendo reflejar mejor fenómenos de la vida real, donde no todo ocurre con la misma frecuencia.

Cuando los resultados empiezan a seguir un orden más marcado, aparece la famosa campana de Gauss o distribución normal, cuya característica es que la mayoría de los valores se concentran alrededor del punto central o esperanza matemática.

- **Distribución normal:** Se caracteriza por su forma simétrica con la mayoría de los valores concentrados en el centro.

Cabe mencionar que también existen diversos teoremas matemáticos que ayudan a calcular probabilidades, siendo uno de ellos el teorema de Bayes, el cual permite ajustar nuestras ideas conforme surge nueva información.

- **Teorema de Bayes:** Es una regla matemática de la probabilidad condicional que parte de una probabilidad inicial o previa y la ajusta conforme se dispone de nueva evidencia, permitiendo así obtener una probabilidad actualizada o posterior.

3.2 Fuentes Generadoras De Números Aleatorios

Una forma de comunicarse es a través de los números, ya que estos componen un lenguaje con mayor formalidad y precisión. A diferencia de las palabras, que pueden tener múltiples interpretaciones, los números ofrecen un sistema estructurado y universal que permite transmitir información de manera clara y sin ambigüedades.

Al momento de modelar un sistema se requiere de números asociados a la incertidumbre, ya que se busca representar dicho sistema a través de un modelo, manteniendo su esencia, considerando siempre el factor de aleatoriedad.

- **Aleatoriedad:** Propiedad de un proceso cuyos resultados individuales son impredecibles y no siguen un patrón específico. Sin embargo, al repetirse numerosas veces, estos muestran regularidades estadísticas. Por ejemplo, al lanzar una moneda no podemos saber si caerá cara o cruz en un intento particular, pero tras cientos de lanzamientos observaremos que ambas caras aparecen en proporciones muy similares.
- **Sistema:** Conjunto de elementos interrelacionados que trabajan conjuntamente para lograr un objetivo común.

Debido a esto, se buscan fuentes generadoras de números aleatorios que sean formales, es decir, que estén definidas matemáticamente y algorítmicamente, representando expresiones puras de aleatoriedad. Sin embargo, al modelar un sistema, se buscan estas expresiones, lo cual es complejo, ya que si se detecta algún patrón de comportamiento en la supuesta aleatoriedad, entonces dejan de considerarse verdaderamente números aleatorios y pierden sus propiedades fundamentales.

- **Patron:** Regularidad o repetición observable en una secuencia de números que hace que los resultados sean predecibles y no independientes.

Dentro de las definiciones matemáticas, se requieren relaciones recursivas mediante fórmulas definidas en sus propios términos, lo que permite que sean programables. Estas relaciones de recurrencia se utilizan con la expectativa de generar números aleatorios que funcionen como verdaderos generadores de números aleatorios.

Estas fórmulas deben cumplir con ciertas características para ser consideradas fuentes válidas de generación de números aleatorios:

- **Complejidad:** Una característica clave es cuán complejas son las funciones construidas como fuentes generadoras; se espera que sean lo más sencillas posibles.
- **Programables:** Deben poder implementarse en código en un lenguaje de programación. Esto es importante, ya que no todos los problemas son modelables de manera directa.
- **Consumo equilibrado de recursos de cómputo:** Al definir estas funciones de manera recursiva, es fundamental considerar los recursos que consumen durante su ejecución. Lo ideal es que el consumo sea equilibrado.

- **Análisis de resultados:** Los valores obtenidos deben ser no solo correctos, sino también reproducibles, lo que permite tener control sobre el sistema.
- **Larga periodicidad:** Mientras más largo sea el período, mejor; este concepto está directamente relacionado con las relaciones de recurrencia.
- **Independencia y uniformidad:** Se refieren al ámbito estadístico, propio de las probabilidades condicionales, como en el teorema de Bayes.

3.3 Tipos de Generadores de Números Aleatorios

3.3.1 Generador Congruencial Mixto

El generador congruencial mixto (GCM) es uno de los métodos más empleados para la generación de números pseudoaleatorios debido a su facilidad de implementación. Se define formalmente mediante la siguiente expresión:

$$X_{n+1} = (aX_n + c) \mod m; X_0$$

donde:

- X_0 : valor inicial o semilla.
- a : multiplicador.
- c : incremento.
- m : módulo.

El valor inicial X_0 da inicio a la secuencia, mientras que los parámetros a , c y m determinan la calidad y longitud del período del generador. Estos parámetros deben ser escogidos cuidadosamente, ya que de ellos depende la capacidad del generador para producir secuencias con propiedades cercanas a la verdadera aleatoriedad.

Propiedades fundamentales: Para asegurar que el generador tenga una buena calidad, debe cumplir con un conjunto de propiedades, que son las siguientes:

1. El valor c y el módulo m deben ser primos relativos (coprimos).
2. Todo número primo que divida a m también debe dividir a $a - 1$.
3. Si m es múltiplo de 4, entonces $a - 1$ también debe ser múltiplo de 4.

Cabe mencionar que la tercera condición es de carácter **condicional**. Esto significa que si la premisa es falsa pero la consecuencia es cierta, la propiedad se sigue considerando válida. En lógica, esto se refleja mediante la tabla de verdad de la implicación ($P \Rightarrow Q$):

P	Q	$P \Rightarrow Q$
V	V	V
V	F	F
F	V	V
F	F	V

Ejemplo práctico: Si se toman los valores $a = 5$, $c = 7$, $m = 10$ y $X_0 = 2$, el generador está definido como:

$$X_{n+1} = (5X_n + 7) \mod 10; X_0 = 2$$

Construyendo la tabla de valores se obtiene:

n	X_n	$aX_n + c$	X_{n+1}	$(aX_n + c)/m$
0	2	17	7	$17/10 = 1.7$
1	7	42	2	$42/10 = 4.2$
2	2	17	7	$17/10 = 1.7$
3	7	42	2	$42/10 = 4.2$

Se puede ver que la secuencia empieza a repetirse con un período de 2. Esto muestra que el generador no crea números totalmente aleatorios, sino una serie determinada que solo da la impresión de ser aleatoria por intervalos.

Verificación de propiedades:

- 1. Primalidad entre c y m : (CUMPLE)**
 $c = 7$, $m = 10 = 2 \cdot 5$. No hay factores comunes, por lo tanto, son primos relativos.
- 2. Primos de m dividen a $a - 1$: (NO CUMPLE)**
 Los primos que dividen a $m = 10$ son $\{2, 5\}$.
 $a - 1 = 5 - 1 = 4$. Es divisible entre 2, pero no entre 5.
- 3. Condición condicional (si m es múltiplo de 4, entonces $a - 1$ también debe serlo): (CUMPLE)**
 $m = 10$ no es múltiplo de 4 (premisa falsa).
 $a - 1 = 4$ sí es múltiplo de 4 (consecuencia verdadera).
 Como esta propiedad es condicional, se cumple según la tabla de verdad del implicador ($P \Rightarrow Q$).

Limitaciones: El generador congruencial mixto presenta algunas limitaciones generadas por su propia definición:

- Los valores generados están restringidos al rango $[0, m]$, ya que dependen de la operación módulo.
- Siempre existe la presencia de un período, lo que implica que, tarde o temprano, la secuencia se repetirá.
- En períodos cortos, la calidad del generador disminuye significativamente, ya que aparecen patrones evidentes en la secuencia.

3.3.2 Generador Congruencial Multiplicativo

El generador congruencial multiplicativo (GCMu) es una variación del generador congruencial mixto, con la diferencia de que elimina el término de incremento c , quedando definido únicamente por la multiplicación. Se expresa formalmente como:

$$X_{n+1} = (aX_n) \mod m; X_0$$

donde:

- X_0 : valor inicial o semilla.
- a : multiplicador.
- m : módulo.

El valor inicial X_0 determina el inicio de la secuencia y, al igual que en el generador mixto, la calidad y longitud del período dependen directamente de los parámetros elegidos. En este caso, la ausencia del término c hace que la semilla y el multiplicador adquieran mayor importancia.

Propiedades fundamentales: Para que el generador congruencial multiplicativo produzca secuencias de buena calidad, debe cumplir con un conjunto de propiedades:

1. La semilla X_0 debe ser un número impar, no divisible entre 2 ni entre 5, y además debe ser relativamente primo con respecto a m .
2. El valor del multiplicador a se obtiene de la relación:

$$a = 200t \pm p$$

donde $t \in \mathbb{Z}^+$ y p pertenece al conjunto de primos específicos

$$P = \{3, 11, 13, 19, 21, 27, 29, 37, 51, 57, 61, 67, 69, 77, 83, 93\}.$$

3. El valor del período con $m = 10^d$ se determina de la siguiente forma:
 - Si $d \geq 5$: el período es $5 \cdot 10^{d-2}$.
 - Si $d < 5$: el período se calcula como el mínimo común múltiplo de los valores $\lambda(p_i^{d_i})$, según la factorización de m .

Ejemplo práctico: Sea $a = 3$, $m = 100$ y $X_0 = 17$. El generador queda definido como:

$$X_{n+1} = (3X_n) \mod 100; X_0 = 17$$

Verificación de propiedades:

1. **Condición sobre la semilla X_0 :** (CUMPLE)
La semilla $X_0 = 17$ es un número impar, no divisible entre 2 ni entre 5, y además es relativamente primo con respecto a $m = 100$.
2. **Forma del multiplicador a :** (CUMPLE)
El valor de $a = 3$ proviene de la relación $a = 200t \pm p$, donde $t = 0$ y $p = 3$. De este modo, se cumple con la regla establecida.

3. Determinación del período: (CUMPLE)

Para $m = 10^2 = 100$, se tiene $d = 2$, y como $d < 5$, el período se calcula como el mínimo común múltiplo de los valores $\lambda(p_i^{d_i})$:

$$\text{Período} = \text{mcm}\{\lambda(2^2), \lambda(5^2)\}$$

$$\lambda(2^2) = (2 - 1) \cdot 2^{2-1} = 2$$

$$\lambda(5^2) = (5 - 1) \cdot 5^{2-1} = 20$$

$$\Rightarrow \text{Período} = \text{mcm}\{2, 20\} = 20$$

Por lo tanto, la secuencia generada tendrá un período de 20 antes de repetirse.

Limitaciones: El generador congruencial multiplicativo también presenta limitaciones importantes:

- La elección de la semilla es más estricta: debe cumplir condiciones de imparidad y coprimidad con m .
- Si los parámetros no se eligen adecuadamente, el período puede ser muy corto, reduciendo la calidad de la secuencia.
- Al no contar con el incremento c , la estructura del generador puede ser menos flexible que en el caso mixto.

4. Descripción del Problema

La generación de números aleatorios en la informática no proviene de fenómenos naturales, sino de algoritmos diseñados para imitar el azar. Estos algoritmos, conocidos como generadores pseudoaleatorios, producen secuencias numéricas que aparentan ser impredecibles, pero que en realidad están determinadas por parámetros iniciales.

El problema surge porque no todos los generadores ofrecen la misma calidad: algunos logran secuencias con períodos largos y buena distribución, mientras que otros generan ciclos cortos o patrones evidentes que limitan su utilidad. Esto significa que la elección de los parámetros (semilla, multiplicador, incremento y módulo) puede marcar la diferencia entre un generador confiable y uno deficiente.

En el caso de los generadores congruenciales, ampliamente usados por su sencillez, resulta fundamental verificar si cumplen con ciertas propiedades matemáticas que garantizan períodos máximos y una distribución adecuada. Sin este análisis, los resultados producidos pueden perder aleatoriedad y afectar negativamente a cualquier aplicación que dependa de ellos.

De este modo, se trata de comprender las condiciones bajo las cuales estos generadores funcionan correctamente, así como las limitaciones que presentan cuando dichas condiciones no se cumplen.

5. Objetivos

- Analizar el comportamiento de diferentes generadores de números aleatorios, observando cómo varían sus resultados en función de los parámetros iniciales y del tipo de generador empleado.

- Verificar el cumplimiento de las propiedades matemáticas de los generadores congruenciales mixto y multiplicativo, determinando en qué medida estas garantizan la calidad de las secuencias producidas.
- Construir ejemplos prácticos de cada generador, desarrollando tablas de valores que permitan visualizar la secuencia generada y la aparición de patrones o repeticiones.
- Evaluar la longitud del período en cada caso, identificando cuándo la secuencia alcanza un ciclo repetitivo y cómo este factor afecta en la aleatoriedad.
- Analizar e interpretar los resultados obtenidos a partir de las secuencias generadas, utilizando gráficas y aplicando conceptos de probabilidad y estadística para estudiar el comportamiento de la distribución producida por el generador.

6. Desarrollo de la Solución

6.1 Metodología e implementación

Para este trabajo se desarrolló un *modelo de simulación* en **R**, ejecutado en **RStudio** y documentado en **L^AT_EX**. El objetivo fue observar el comportamiento de distintos generadores de números pseudoaleatorios bajo un mismo marco experimental y con salidas reproducibles.

La implementación se organizó en dos clases independientes (usando `setRefClass`):

- **GeneradorCongruencialMixto** ($X_{n+1} = (aX_n + c) \bmod m$)
- **GeneradorCongruencialMultiplicativo** ($X_{n+1} = (aX_n) \bmod m$)

Cada clase expone un conjunto común de métodos, más algunos específicos:

- **generarNumeros(N)**: Produce la secuencia X_0, \dots, X_N y su versión normalizada $u_n = X_n/m$. Además, genera de forma automática un *plot* de líneas con marcadores para visualizar la trayectoria de u_n a lo largo del tiempo.
- **propiedad_I()**, **propiedad_II()**, **propiedad_III()**: Verifican, una por una, las condiciones teóricas de validez de cada generador (coprimalidad, forma del multiplicador, condición condicional, etc.).
- **evaluarCalidad()**: Resume el estado de las tres propiedades (*CUMPLE/NO CUMPLE*) e informa si, en conjunto, el generador es apto para alcanzar período máximo bajo los parámetros provistos.

Además, se añadieron rutinas específicas por tipo de generador:

- **Mixto**: Detección del **período** y del **preperíodo** dentro de los N valores generados, mediante un registro de ocurrencias (*hash*) que identifica el primer reingreso a un estado; así se mide la longitud del ciclo (λ) y del tramo transitorio (μ), incluso cuando el ciclo no empieza en X_0 .
- **Multiplicativo**: Cálculo teórico del período cuando $m = 10^d$ (vía función λ de Carmichael y mcm), y, en general, la misma detección empírica del ciclo en la muestra generada.

El programa principal (**main**) solicita al usuario: tipo de generador, parámetros (a, c, m, X_0) y el vector de corridas N (por ejemplo, 1, 3, 5, 10, 30, 50, 100, 300, 500, 1000, 3000, 5000, 10000). Para cada N , el sistema:

1. Genera y muestra la secuencia (con el mismo formato de tablas usado en el informe).
2. Gráfica u_n para apreciar patrones y densidad en $[0, 1)$.
3. Intenta detectar (si aparece dentro de la muestra) el período y el preperíodo.
4. Registra en consola la evaluación de las propiedades.

Este esquema permitió comparar, bajo idénticas condiciones, la **uniformidad visual** de u_n , la **presencia de bandas** o patrones, y la **longitud de los ciclos** observables en cada generador. Más adelante se incluyen las figuras y capturas de las corridas seleccionadas para ambos casos.

6.2 Generador Congruencial Mixto

1. Definición del modelo

Se implementó el generador congruencial mixto (GCM),

$$X_{n+1} = (aX_n + c) \bmod m, \quad u_n = \frac{X_n}{m},$$

con métodos para: (i) verificar sus tres propiedades teóricas, (ii) generar N valores, (iii) graficar la serie u_n y (iv) detectar, dentro de los N valores generados, el *período* (si aparece) y el *preperíodo*.

2. Parámetros y verificación previa

Para las corridas principales se usó $a = 21$, $c = 37$, $m = 1000$ y $X_0 = 5$. Con estos valores:

- c y m son coprimos.
- Los primos de m (2 y 5) dividen a $a - 1 = 20$.
- Como m es múltiplo de 4, también lo es $a - 1$.

Por lo tanto, el generador **cumple las tres propiedades** y es de **período completo** ($m = 1000$).

3. Corridas y colección de datos

Se ejecutaron corridas con $N \in \{1, 3, 5, 10, 30, 50, 100, 300, 500, 1000, 3000, 5000, 10000\}$. En cada N se registró la secuencia X_n , la normalizada u_n y, si ocurría dentro de los N valores, el período detectado y el preperíodo.

```

> main()
Elige una opción:
1. Generador Congruencial Mixto
2. Generador Congruencial Multiplicativo
Opción: 1
Ingrese el multiplicador a: 21
Ingrese el incremento c: 37
Ingrese el módulo m: 1000
Ingrese la semilla: 5
Ingrese el número de corridas a los que se someterá el generador, separados por una coma (ej: 10,20,30):
1,3,5,10,30,50,100,300,500,1000,3000,5000,10000
=== Evaluación de propiedades (Mixto) ===
I) El valor c y el módulo m deben ser primos relativos (coprimos): CUMPLE
II) Todo número primo que divida a m también debe dividir a (a-1): CUMPLE
III) Si m es múltiplo de 4, entonces (a-1) también debe ser múltiplo de 4: CUMPLE
Resultado: El generador es de periodo completo.

Para 1 numeros aleatorios
No se detectó el ciclo dentro de los 2 valores generados.
Secuencia generada: 5 142

=====
Para 3 numeros aleatorios
No se detectó el ciclo dentro de los 4 valores generados.
Secuencia generada: 5 142 19 436

=====
Para 5 numeros aleatorios
No se detectó el ciclo dentro de los 6 valores generados.
Secuencia generada: 5 142 19 436 193 90

=====
Para 10 numeros aleatorios
No se detectó el ciclo dentro de los 11 valores generados.
Secuencia generada: 5 142 19 436 193 90 927 504 621 78 675

=====
Para 30 numeros aleatorios
No se detectó el ciclo dentro de los 31 valores generados.
Secuencia generada: 5 142 19 436 193 90 927 504 621 78 675 212 489 306 463 760 997 974 491 348 345 282 959 176 733 430 67 444 361 618 15 352 429 46 3 100 137 914 231 888 685 422 899 916

=====
Para 500 numeros aleatorios
No se detectó el ciclo dentro de los 501 valores generados.
Secuencia generada: 5 142 19 436 193 90 927 504 621 78 675 212 489 306 463 760 997 974 491 348 345 282 959 176 733 430 67 444 361 618 15 352 429 46 3 100 137 914 231 888 685 422 899 916
273 770 207 384 101 158 355
=====
Para 1000 numeros aleatorios
No se detectó el ciclo dentro de los 1001 valores generados.
Secuencia generada: 5 142 19 436 193 90 927 504 621 78 675 212 489 306 463 760 997 974 491 348 345 282 959 176 733 430 67 444 361 618 15 352 429 46 3 100 137 914 231 888 685 422 899 916
273 770 207 384 101 158 355 492 309 786 543 440 277 854 971 428 25 562 839 656 813 110 347 324 841 698 695 632 309 526 83 780 417 794 731 968 365 702 739 396 353 450 487 264 581 238 35
772 249 266 623 120 557 734 451 508 705 842 719 136 893 790 627 204 321 778 375 912 189 6 163 460 697 674 191 48 45 982 659 876 43 130 767 144 61 318 715 52 129 746 703 800 817 614 931
588 385 122 599 616 973 470 807 84 801 838 55 192 69 486 243 140 977 554 671 128 725 262 539 356 913 810 47 24 541 398 395 332 9 226 783 480 117 494 411 668 65 402 479 96 51 150 187 964
281 938 735 472 949 966 323 820 257 434 151 208 405 542 419 836 593 490 327 904 21 478 75 612 889 760 863 160 397 374 891 748 745 682 359 576 133 830 467 844 761 18 415 752 829 446 403
500 537 314 613 288 85 822 299 316 673 170 607 784 501 558 755 892 769 186 943 840 677 254 371 828 425 962 239 56 213 510 747 724 241 98 95 32 709 926 483 180 817 194 111 368 765 102 17
9 796 733 850 887 664 981 638 435 172 649 666 23 520 957 134 651 908 105 242 119 336 293 190 27 604 721 178 775 312 589 406 563 860 97 74 591 448 445 382 59 276 833 530 167 544 461 718
115 452 529 146 103 200 237 14 331 988 785 522 999 16 373 870 307 484 201 258 455 592 469 886 643 540 377 954 71 528 125 692 359 716 913 214 427 424 941 798 795 732 409 626 183 880 517
894 811 68 465 802 879 465 812 336 687 364 681 338 155 872 349 366 723 202 657 834 553 608 805 942 819 236 993 809 727 304 421 878 475 12 289 106 263 560 797 774 291 148 145 82 759 976
535 200 867 244 161 419 815 152 229 846 803 900 937 714 31 688 465 222 699 716 73 570 7 184 901 958 155 292 169 586 343 240 77 654 773 228 625 362 639 456 613 910 147 124 641 498 495 43
2 109 326 883 580 217 594 511 768 165 502 579 196 153 250 287 64 381 38 835 572 49 66 423 920 357 534 251 308 505

=====
Para 500 numeros aleatorios
No se detectó el ciclo dentro de los 501 valores generados.
Secuencia generada: 5 142 19 436 193 90 927 504 621 78 675 212 489 306 463 760 997 974 491 348 345 282 959 176 733 430 67 444 361 618 15 352 429 46 3 100 137 914 231 888 685 422 899 916
273 770 207 384 101 158 355 492 309 786 543 440 277 854 971 428 25 562 839 656 813 110 347 324 841 698 695 632 309 526 83 780 417 794 731 968 365 702 739 396 353 450 487 264 581 238 35
772 249 266 623 120 557 734 451 508 705 842 719 136 893 790 627 204 321 778 375 912 189 6 163 460 697 674 191 48 45 982 659 876 43 130 767 144 61 318 715 52 129 746 703 800 817 614 931
588 385 122 599 616 973 470 807 84 801 838 55 192 69 486 243 140 977 554 671 128 725 262 539 356 913 810 47 24 541 398 395 332 9 226 783 480 117 494 411 668 65 402 479 96 51 150 187 964
281 938 735 472 949 966 323 820 257 434 151 208 405 542 419 836 593 490 327 904 21 478 75 612 889 760 863 160 397 374 891 748 745 682 359 576 133 830 467 844 761 18 415 752 829 446 403
500 537 314 613 288 85 822 299 316 673 170 607 784 501 558 755 892 769 186 943 840 677 254 371 828 425 962 239 56 213 510 747 724 241 98 95 32 709 926 483 180 817 194 111 368 765 102 17
9 796 733 850 887 664 981 638 435 172 649 666 23 520 957 134 651 908 105 242 119 336 293 190 27 604 721 178 775 312 589 406 563 860 97 74 591 448 445 382 59 276 833 530 167 544 461 718
115 452 529 146 103 200 237 14 331 988 785 522 999 16 373 870 307 484 201 258 455 592 469 886 643 540 377 954 71 528 125 692 359 716 913 214 427 424 941 798 795 732 409 626 183 880 517
894 811 68 465 802 879 465 812 336 687 364 681 338 155 872 349 366 723 202 657 834 553 608 805 942 819 236 993 809 727 304 421 878 475 12 289 106 263 560 797 774 291 148 145 82 759 976
535 200 867 244 161 419 815 152 229 846 803 900 937 714 31 688 465 222 699 716 73 570 7 184 901 958 155 292 169 586 343 240 77 654 773 228 625 362 639 456 613 910 147 124 641 498 495 43
2 109 326 883 580 217 594 511 768 165 502 579 196 153 250 287 64 381 38 835 572 49 66 423 920 357 534 251 308 505

=====
Para 1000 numeros aleatorios
Periodo detectado (lambda): 1000
Longitud del preperiodo (mu): 0
Secuencia generada: 5 142 19 436 193 90 927 504 621 78 675 212 489 306 463 760 997 974 491 348 345 282 959 176 733 430 67 444 361 618 15 352 429 46 3 100 137 914 231 888 685 422 899 916
273 770 207 384 101 158 355 492 309 786 543 440 277 854 971 428 25 562 839 656 813 110 347 324 841 698 695 632 309 526 83 780 417 794 731 968 365 702 739 396 353 450 487 264 581 238 35
772 249 266 623 120 557 734 451 508 705 842 719 136 893 790 627 204 321 778 375 912 189 6 163 460 697 674 191 48 45 982 659 876 43 130 767 144 61 318 715 52 129 746 703 800 817 614 931
588 385 122 599 616 973 470 807 84 801 838 55 192 69 486 243 140 977 554 671 128 725 262 539 356 913 810 47 24 541 398 395 332 9 226 783 480 117 494 411 668 65 402 479 96 51 150 187 964
281 938 735 472 949 966 323 820 257 434 151 208 405 542 419 836 593 490 327 904 21 478 75 612 889 760 863 160 397 374 891 748 745 682 359 576 133 830 467 844 761 18 415 752 829 446 403
500 537 314 613 288 85 822 299 316 673 170 607 784 501 558 755 892 769 186 943 840 677 254 371 828 425 962 239 56 213 510 747 724 241 98 95 32 709 926 483 180 817 194 111 368 765 102 17
9 796 733 850 887 664 981 638 435 172 649 666 23 520 957 134 651 908 105 242 119 336 293 190 27 604 721 178 775 312 589 406 563 860 97 74 591 448 445 382 59 276 833 530 167 544 461 718
115 452 529 146 103 200 237 14 331 988 785 522 999 16 373 870 307 484 201 258 455 592 469 886 643 540 377 954 71 528 125 692 359 716 913 214 427 424 941 798 795 732 409 626 183 880 517
894 811 68 465 802 879 465 812 336 687 364 681 338 155 872 349 366 723 202 657 834 553 608 805 942 819 236 993 809 727 304 421 878 475 12 289 106 263 560 797 774 291 148 145 82 759 976
533 290 867 244 161 419 815 152 229 846 803 900 937 714 31 688 465 222 699 716 73 570 7 184 901 958 155 292 169 586 343 240 77 654 773 228 625 362 639 456 613 910 147 124 641 498 495 43
2 109 326 883 580 217 594 511 768 165 502 579 196 153 250 287 64 381 38 835 572 49 66 423 920 357 534 251 308 505 429 474 917
48 845 782 459 676 233 930 967 944 861 118 513 852 909 546 503 600 637 414 731 389 185 922 399 416 773 270 707 884 603 658 855 902 869 286 41 940 777 354 473 908 525 62 339 156 313 610
4 842 834 198 195 132 809 26 583 280 917 294 211 468 865 207 279 896 853 950 987 764 81 738 135 252 749 766 123 620 57 234 951 8 205 342 219 636 393 290 127 704 821 778 959 402 412 689 50
6 663 960 197 174 601 548 545 482 119 976 833 630 267 444 961 188 215 552 629 246 205 300 357 114 432 88 885 622 916 116 473 970 407 584 301 558 553 692 569 749 640 477 54 171 628 22
7 872 39 856 13 310 547 18 898 895 832 509 726 283 980 617 994 911 688 955 902 979 596 553 650 687 464 781 438 25 972 449 606 603 700 737 514 813 488 285 22 479 516 873 870 984 701 758 953 9
52 969 188 443 40 875 454 571 28 625 162 439 256 413 710 947 924 141 298 295 252 909 126 683 380 17 394 311 588 965 903 31 396 965 57 7 894 881 838 635 572 848 866 225 720 157 334 51 1
08 300 442 319 76 493 390 227 804 821 378 973 512 789 606 763 60 297 274 781 648 645 582 259 476 33 730 367 744 661 918 313 657 729 346 305 400 437 214 531 188 985 722 199 216 573 70
07 084 401 458 655 792 669 86 843 740 577 154 271 728 325 862 578 713 728 632 141 998 995 932 609 826 383 80 717 94 1 108 665 2 7 894 881 838 535 722 549 566 92
3 420 857 34 251 808 5

=====

```

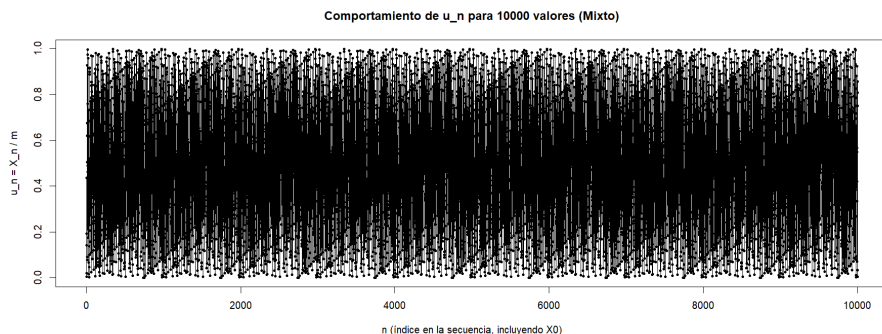



Figure 1. Comportamiento de $u_n = X_n/m$ para $N = 10000$ (GCM).

5. Validación

- **Propiedades:** las tres condiciones se cumplen.
- **Ciclo:** con $N \geq 1000$ se observa claramente la repetición con período 1000 y preperíodo 0.
- **Inspección visual:** la dispersión de u_n es homogénea; no se aprecian “bandas” horizontales marcadas.

6. Experimentación e interpretación

Con pocos N el ciclo no se alcanza y la serie luce “saltada”. Al crecer N , la trayectoria va llenando $[0, 1)$ y alrededor de $N \approx 1000$ se hace evidente la repetición.

6.3 Generador Congruencial Multiplicativo

1. Definición del modelo

Se implementó el generador congruencial multiplicativo (GCMu),

$$X_{n+1} = (aX_n) \bmod m, \quad u_n = \frac{X_n}{m},$$

con los mismos módulos del software que en el caso mixto: verificación de propiedades, generación de N valores, graficación de u_n y detección de período/preperíodo dentro de los N valores generados.

2. Parámetros y verificación previa

Para las corridas principales se usó $a = 203$, $m = 2000$ y $X_0 = 17$.

- La semilla es impar y coprime con m .
- El multiplicador verifica la forma $a = 200t \pm p$ (con $t = 1$, $p = 3$).
- La regla especial del período para $m = 10^d$ **no aplica** (aquí $m \neq 10^d$); por tanto, el ciclo se estudia empíricamente en las corridas.

3. Corridas y colección de datos

Se ejecutaron corridas con $N \in \{1, 3, 5, 10, 30, 50, 100, 300, 500, 1000, 3000, 5000, 10000\}$. En cada N se guardó X_n , u_n y—si aparecía dentro de los N valores—período y preperíodo.

14 Merino Vidal Mateo Alejandro *et al.*

Elige una opción:

1. Generador Congruencial Mixto
2. Generador Congruencial Multiplicativo

Opción: 2

Ingrese el multiplicador a: 203

Ingrese el módulo m: 2000

Ingrese la semilla: 17

Ingrese el número de corridas a los que se someterá el generador, separados por una coma (ej: 10,20,30):

1,3,5,10,30,50,100,300,500,1000,3000,5000,10000

El módulo no es una potencia de 10. No aplica la regla.

== Evaluación de propiedades (Multiplicativo) ==

1) La semilla X_0 debe ser un número impar, no divisible entre 2 ni entre 5, y además debe ser relativamente primo con respecto a m: CUMPLE

2) El multiplicador a debe ser diferente a la relación ($a = 200 * t \pm p$): CUMPLE

3) Período estimado: No calculado

Resultado: Generador válido con período determinado.

Para 1 números aleatorios

No se detectó el ciclo dentro de los 2 valores generados.

Secuencia generada: 17 1451

=====

Para 3 números aleatorios

No se detectó el ciclo dentro de los 4 valores generados.

Secuencia generada: 17 1451 553 259

=====

Para 5 números aleatorios

No se detectó el ciclo dentro de los 6 valores generados.

Secuencia generada: 17 1451 553 259 577 1131

=====

Para 10 números aleatorios

No se detectó el ciclo dentro de los 11 valores generados.

Secuencia generada: 17 1451 553 259 577 1131 1593 1379 1937 1211 1833

=====

Para 30 números aleatorios

No se detectó el ciclo dentro de los 31 valores generados.

Secuencia generada: 17 1451 553 259 577 1131 1593 1379 1937 1211 1833 99 97 1691 1273 419 1057 571 1913 339 817 1851 1753 1859 1377 1531 793 979 737 1611 1033 1699 897 91 473 19 1857 97

=====

Para 50 números aleatorios

No se detectó el ciclo dentro de los 51 valores generados.

Secuencia generada: 17 1451 553 259 577 1131 1593 1379 1937 1211 1833 99 97 1691 1273 419 1057 571 1913 339 817 1851 1753 1859 1377 1531 793 979 737 1611 1033 1699 897 91 473 19 1857 97

1 1113 1939 1617 251 953 1459 177 1931 1993 579 1537 11 233

Para 100 números aleatorios

Período detectado (lambda): 100

Longitud del preperíodo (mu): 0

Secuencia generada: 17 1451 553 259 577 1131 1593 1379 1937 1211 1833 99 97 1691 1273 419 1057 571 1913 339 817 1851 1753 1859 1377 1531 793 979 737 1611 1033 1699 897 91 473 19 1857 97

1113 1217 1051 1353 659 1777 731 393 1779 1137 811 633 499 1297 1291 73 819 257 171 713 739 17

=====

Para 300 números aleatorios

Período detectado (lambda): 100

Longitud del preperíodo (mu): 0

Secuencia generada: 17 1451 553 259 577 1131 1593 1379 1937 1211 1833 99 97 1691 1273 419 1057 571 1913 339 817 1851 1753 1859 1377 1531 793 979 737 1611 1033 1699 897 91 473 19 1857 97

1113 1217 1051 1353 659 1777 731 393 1779 1137 811 633 499 1297 1291 73 819 257 171 713 739 17

1113 1217 1051 1353 659 1777 731 393 1779 1137 811 633 499 1297 1291 73 819 257 171 713 739 17

1113 1217 1051 1353 659 1777 731 393 1779 1137 811 633 499 1297 1291 73 819 257 171 713 739 17

1113 1217 1051 1353 659 1777 731 393 1779 1137 811 633 499 1297 1291 73 819 257 171 713 739 17

1113 1217 1051 1353 659 1777 731 393 1779 1137 811 633 499 1297 1291 73 819 257 171 713 739 17

1113 1217 1051 1353 659 1777 731 393 1779 1137 811 633 499 1297 1291 73 819 257 171 713 739 17

1113 1217 1051 1353 659 1777 731 393 1779 1137 811 633 499 1297 1291 73 819 257 171 713 739 17

1113 1217 1051 1353 659 1777 731 393 1779 1137 811 633 499 1297 1291 73 819 257 171 713 739 17

1113 1217 1051 1353 659 1777 731 393 1779 1137 811 633 499 1297 1291 73 819 257 171 713 739 17

1113 1217 1051 1353 659 1777 731 393 1779 1137 811 633 499 1297 1291 73 819 257 171 713 739 17

1113 1217 1051 1353 659 1777 731 393 1779 1137 811 633 499 1297 1291 73 819 257 171 713 739 17

1113 1217 1051 1353 659 1777 731 393 1779 1137 811 633 499 1297 1291 73 819 257 171 713 739 17

1113 1217 1051 1353 659 1777 731 393 1779 1137 811 633 499 1297 1291 73 819 257 171 713 739 17

1113 1217 1051 1353 659 1777 731 393 1779 1137 811 633 499 1297 1291 73 819 257 171 713 739 17

1113 1217 1051 1353 659 1777 731 393 1779 1137 811 633 499 1297 1291 73 819 257 171 713 739 17

1113 1217 1051 1353 659 1777 731 393 1779 1137 811 633 499 1297 1291 73 819 257 171 713 739 17

1113 1217 1051 1353 659 1777 731 393 1779 1137 811 633 499 1297 1291 73 819 257 171 713 739 17

1113 1217 1051 1353 659 1777 731 393 1779 1137 811 633 499 1297 1291 73 819 257 171 713 739 17

1113 1217 1051 1353 659 1777 731 393 1779 1137 811 633 499 1297 1291 73 819 257 171 713 739 17

1113 1217 1051 1353 659 1777 731 393 1779 1137 811 633 499 1297 1291 73 819 257 171 713 739 17

1113 1217 1051 1353 659 1777 731 393 1779 1137 811 633 499 1297 1291 73 819 257 171 713 739 17

1113 1217 1051 1353 659 1777 731 393 1779 1137 811 633 499 1297 1291 73 819 257 171 713 739 17

1113 1217 1051 1353 659 1777 731 393 1779 1137 811 633 499 1297 1291 73 819 257 171 713 739 17

1113 1217 1051 1353 659 1777 731 393 1779 1137 811 633 499 1297 1291 73 819 257 171 713 739 17

1113 1217 1051 1353 659 1777 731 393 1779 1137 811 633 499 1297 1291 73 819 257 171 713 739 17

1113 1217 1051 1353 659 1777 731 393 1779 1137 811 633 499 1297 1291 73 819 257 171 713 739 17

1113 1217 1051 1353 659 1777 731 393 1779 1137 811 633 499 1297 1291 73 819 257 171 713 739 17

1113 1217 1051 1353 659 1777 731 393 1779 1137 811 633 499 1297 1291 73 819 257 171 713 739 17

1113 1217 1051 1353 659 1777 731 393 1779 1137 811 633 499 1297 1291 73 819 257 171 713 739 17

1113 1217 1051 1353 659 1777 731 393 1779 1137 811 633 499 1297 1291 73 819 257 171 713 739 17

1113 1217 1051 1353 659 1777 731 393 1779 1137 811 633 499 1297 1291 73 819 257 171 713 739 17

1113 1217 1051 1353 659 1777 731 393 1779 1137 811 633 499 1297 1291 73 819 257 171 713 739 17

1113 1217 1051 1353 659 1777 731 393 1779 1137 811 633 499 1297 1291 73 819 257 171 713 739 17

1113 1217 1051 1353 659 1777 731 393 1779 1137 811 633 499 1297 1291 73 819 257 171 713 739 17

1113 1217 1051 1353 659 1777 731 393 1779 1137 811 633 499 1297 1291 73 819 257 171 713 739 17

1113 1217 1051 1353 659 1777 731 393 1779 1137 811 633 499 1297 1291 73 819 257 171 713 739 17

1113 1217 1051 1353 659 1777 731 393 1779 1137 811 633 499 1297 1291 73 819 257 171 713 739 17

1113 1217 1051 1353 659 1777 731 393 1779 1137 811 633 499 1297 1291 73 819 257 171 713 739 17

1113 1217 1051 1353 659 1777 731 393 1779 1137 811 633 499 1297 1291 73 819 257 171 713 739 17

1113 1217 1051 1353 659 1777 731 393 1779 1137 811 633 499 1297 1291 73 819 257 171 713 739 17

1113 1217 1051 1353 659 1777 731 393 1779 1137 811 633 499 1297 1291 73 819 257 171 713 739 17

1113 1217 1051 1353 659 1777 731 393 1779 1137 811 633 499 1297 1291 73 819 257 171 713 739 17

1113 1217 1051 1353 659 1777 731 393 1779 1137 811 633 499 1297 1291 73 819 257 171 713 739 17

1113 1217 1051 1353 659 1777 731 393 1779 1137 811 633 499 1297 1291 73 819 257 171 713 739 17

1113 1217 1051 1353 659 1777 731 393 1779 1137 811 633 499 1297 1291 73 819 257 171 713 739 17

1113 1217 1051 1353 659 1777 731 393 1779 1137 811 633 499 1297 1291 73 819 257 171 713 739 17

1113 1217 1051 1353 659 1777 731 393 1779 1137 811 633 499 1297 1291 73 819 257 171 713 739 17

1113 1217 1051 1353 659 1777 731 393 1779 1137 811 633 499 1297 1291 73 819 257 171 713 739 17

1113 1217 1051 1353 659 1777 731 393 1779 1137 811 633 499 1297 1291 73 819 257 171 713 739 17

1113 1217 1051 1353 659 1777 731 393 1779 1137 811 633 499 1297 1291 73 819 257 171 713 739 17

1113 1217 1051 1353 659 1777 731 393 1779 1137 811 633 499 1297 1291 73 819 257 171 713 739 17

1113 1217 1051 1353 659 1777 731 393 1779 1137 811 633 499 1297 1291 73 819 257 171 713 739 17

1113 1217 1051 1353 659 1777 731 393 1779 1137 811 633 499 1297 1291 73 819 257 171 713 739 17

1113 1217 1051 1353 659 1777 731 393 1779 1137 811 633 499 1297 1291 73 819 257 171 713 739 17

1113 1217 1051 1353 659 1777 731 393 1779 1137 811 633 499 1297 1291 73 819 257 171 713 739 17

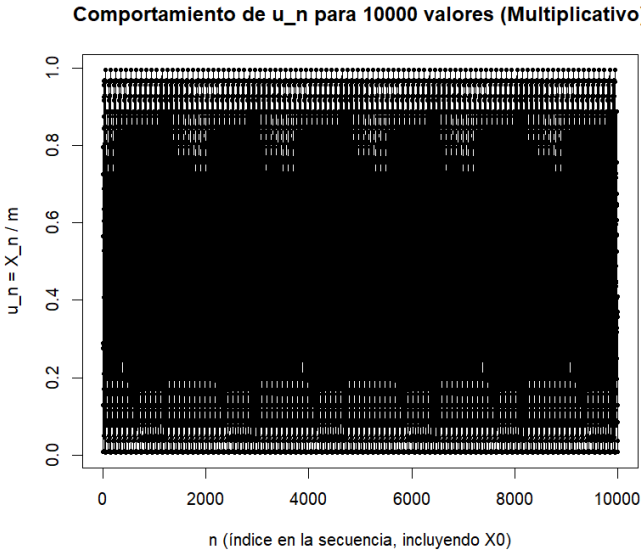


Figure 2. Comportamiento de $u_n = X_n/m$ para $N = 10000$ (GCMu).

5. Validación

- **Propiedades:** la semilla y el multiplicador cumplen las condiciones exigidas.
- **Ciclo:** la detección del período depende de m y del tamaño N ; no siempre se cierra el ciclo dentro de las corridas consideradas.
- **Inspección visual:** las bandas indican que la secuencia visita niveles discretos con mayor regularidad; conviene tenerlo presente cuando se requiera mayor uniformidad.

6. Experimentación e interpretación

Con pocos N no se observa el cierre de ciclo. Al aumentar N , se mantiene el patrón en bandas, lo que sugiere una estructura interna más fuerte que en el caso mixto. Más adelante se incluirán las capturas de todas las corridas para este generador.

7. Conclusiones

- El estudio de los generadores congruenciales permitió comprender cómo es posible imitar la aleatoriedad mediante fórmulas matemáticas, mostrando que aunque las secuencias aparentan ser impredecibles, en realidad están determinadas por parámetros iniciales.
- Se verificó que la calidad del generador depende directamente del cumplimiento de ciertas propiedades matemáticas. En el caso del generador congruencial mixto, el no cumplimiento de alguna condición reduce el período y evidencia patrones repetitivos.
- En el generador congruencial multiplicativo se demostró que la elección adecuada de la semilla y del multiplicador es fundamental, ya que de ello depende que la secuencia alcance un período más largo y una distribución más equilibrada.

- Los ejemplos prácticos realizados confirmaron que, si bien estos generadores no producen números verdaderamente aleatorios, permiten obtener secuencias útiles en simulaciones y aplicaciones computacionales, siempre y cuando se escojan correctamente los parámetros.
- El análisis apoyado en tablas y gráficas facilitó la identificación de patrones, ciclos y distribuciones, lo que hizo más clara la relación entre la teoría matemática de los generadores y los resultados experimentales obtenidos.

8. Bibliografía

References

- [1] García Gómez, José Alfredo; Martínez De La Cruz, Miguel Ángel; Jauregui Wade, Lucila; Valles Rivera, Diana; Sánchez Vasconcelos, Ángel Gabriel. (2024). *Importancia del uso de los generadores de números pseudoaleatorios en los contenidos de la asignatura de simulación*. Innovación y Desarrollo Tecnológico, Vol. 16, Núm. 3. Instituto Tecnológico de Villahermosa.
- [2] ScienceDirect. (s.f.). *Random Number Generation*. Recuperado de: <https://www.sciencedirect.com/topics/computer-science/random-number-generation>
- [3] The Dojo. (2021). *Generadores de números aleatorios y su importancia para el desarrollo*. Blog The Dojo. Recuperado de: <https://blog.thedojo.mx/2021/12/07/generadores-de-numeros-aleatorios-y-su-importancia-para-el-desarrollo.html>
- [4] Batanero, C.; Estepa, A.; Godino, J. D. (1992). Análisis exploratorio de datos: sus posibilidades en la enseñanza secundaria. *Suma*, 9, 25-31.
- [5] Bennett, D. (1993). *The development of the mathematical concept of randomness; educational implications*. Doctoral Thesis, New York University. (DAI n. 931 7657).