

## Tema 5. Generación de números aleatorios

# Calendario

	Semana	Tema	Refuerzo	Laboratorio	Actividad
09/11/2020					
16/11/2020	1	S0 + T1			
23/11/2020	2	T2			
30/11/2020	3	T3		L1	
07/12/2020	4	T4			
14/12/2020	5	T5			L1
21/12/2020	--	Semana de repaso	R-L1		
28/12/2020	--	Semana de repaso			
04/01/2021	6	T6			
11/01/2021	7	T6			
18/01/2021	8	T7			
25/01/2021	9	T7			AG
01/02/2021	10	T8			
08/02/2021	11	T9		L2	
15/02/2021	12	T10	R-AG1		
22/02/2021	13	T11			L2
01/03/2021	14	Sesión examen	R-L2		
08/03/2021	15	Repaso (sesión doble)			
15/03/2021	16	Semana			

Próximas sesiones  
T5-> (15/12 18:00CET)

# Contenidos

- Tema 1. Conceptos generales de modelado matemático y simulación
- Tema 2. Modelado matemático de sistemas físicos
- Tema 3. Sistemas físicos y sus modelos
- Tema 4. Simulación
- **Tema 5. Generación de números aleatorios**
- Tema 6. Generación de variables aleatorias
- Tema 7. Medidas estadísticas
- Tema 8. Simulación de Monte Carlo
- Tema 9. Conceptos y elementos de simulación con eventos
- Tema 10. Modelado y simulación de sistemas de eventos discretos
- Tema 11. *Software* para modelado matemático y simulación

# Objetivos

- Conocer métodos para generar números aleatorios de forma eficiente.
- Saber calcular los periodos de generación de los diferentes métodos.

# Introducción

Necesitamos números aleatorios para:

- Describir la aleatoriedad de modelos.
- Reproducir datos que no se conocen con exactitud.

Un número de forma aislada no es aleatorio

# Características básicas

- Eficiencia.
- Generación de números independientes estadísticamente y uniformemente distribuidos (IID).
- Sin ciclos de repetición.
- Ocupar poca memoria.
- Reproducibilidad.
- Rapidez.

# Características básicas

- ¿Propuestas?

# Métodos iterativos de generación

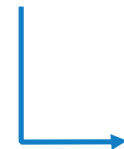
- Base matemática → números pseudoaleatorios
- Objetivo: producir una secuencia de números aleatorios e idénticamente distribuidos entre 0 y 1.
- Idea del método:
  - Tomamos un valor inicial  $x_0$ .
  - Aplicamos una función  $f$  para obtener  $x_{n+1} = f(x_n)$ .
  - Calculamos el valor aleatorio como  $u_n = g(x_n)$Llamamos a  $x_i$  el estado de generación.



# El periodo de generación

- Las sucesiones de números aleatorios serán siempre cíclicas.
  - Un ordenador puede representar un número finito de números.

Número finito de estados  $\longrightarrow$  Existen  $i, j, j > i$  tales que  $x_j = x_i$


$$\begin{aligned}x_{j+k} &= x_{i+k} \\ u_{j+k} &= u_{i+k}\end{aligned}$$

- El **periodo** es el menor número entero de pasos  $T > 0$  para el que el estado del generador se repite, y se verifica que el estado:

$$x_{T+k} = x_k$$

# La operación módulo

Es la operación básica de los métodos de congruencia.  
Consiste en calcular el resto de una división.

Ejemplos:

- $5 \bmod 3 =$
- $17 \bmod 4 =$

# Métodos de congruencia

La recursión empleada es

$$x_{n+1} = (a \cdot x_n + b) \bmod m$$

$a$ ,  $m$  y  $b$  son números enteros positivos denominados multiplicador, módulo e incremento. Se verifica que  $a < m$  y  $b < m$ .

- Si  $b = 0$  se denomina **generador multiplicativo**.
- En caso contrario se denomina **mixto**.

La sucesión de números pseudoaleatorios  $u_i, i \geq 1$  se obtiene:

$$u_i = \frac{x_i}{m}$$

# Métodos de congruencia

Se dice que el generador es de ciclo completo si el periodo es igual a  $m$ .

- El periodo será  $m$  independientemente de la semilla.

Si un generador no es de ciclo completo, la longitud de ciclo puede depender de la semilla utilizada.

Criterios para un buen generador:

- el módulo  $m$  es una potencia de 2.
- $m$  debe ser grande.

# Métodos mixtos – Condiciones $T$ máximo

Criterio de periodo completo ( $T = m$ ):

- Caso  $m$  general:
  - $m$  y  $b$  son primos entre sí.
  - Si  $q$  es un número primo que divide a  $m \Rightarrow q$  divide a  $a - 1$ .
  - Si  $m$  es un múltiplo de 4,  $a - 1$  debe ser un múltiplo de 4.
- Caso  $m = 2^k$ :
  - $b$  es impar
  - $a \bmod 4 = 1$ .

# Mts. multiplicativos – Condiciones $T$ máximo

No puede tener periodo completo

$b = 0$  y entonces  $m$  y  $b$  no son primos entre sí

Hablaremos de periodo máximo. Deberemos escoger  $a$  y  $m$  de la forma adecuada.

- Caso general ( $b = 0, m$  cualquiera)
  - Si  $T = m - 1 \Rightarrow m$  es primo.
  - Si  $m$  primo  $\Rightarrow T$  divide a  $m - 1$ .
  - Si  $m$  es primo, entonces  $T=m-1$  si y sólo si  $a$  es una raíz primitiva de módulo  $m$

$a$  es raíz primitiva de modulo  $m$  si todo  $b < m$  es resultado de  $a^k \bmod m = b$  para algún  $k$ .

# Mts. multiplicativos – Condiciones $T$ máximo

No puede tener periodo completo

$b = 0$  y entonces  $m$  y  $b$  no son primos entre sí

Hablaremos de periodo máximo. Deberemos escoger  $a$  y  $m$  de la forma adecuada.

- Caso general ( $b = 0, m$  cualquiera)
  - Si  $T = m - 1 \Rightarrow m$  es primo.
  - Si  $m$  primo  $\Rightarrow T$  divide a  $m - 1$ .
  - Si  $m$  es primo, entonces  $T=m-1$  si y sólo si  $a$  es una raíz primitiva de módulo  $m$
- Caso  $m = 2^k$  ( $b = 0$ )
  - $x_0$  es impar.
  - $a \bmod 8$  es 3 ó 5.Entonces  $T = 2^{k-2}$

Tiene malas propiedades estadísticas

# Ejemplo 1

Sea el generador  $x_n = (3x_{n-1}) \bmod 2^5$  y la semilla  $x_0 = 1$ .

- ¿Podemos calcular su periodo sin realizar ninguna iteración?
- Realizar las primeras iteraciones
- Encontrar los primeros valores aleatorios generados.



# Ejemplo 1

Sea el generador  $x_n = (3x_{n-1}) \bmod 2^5$  y la semilla  $x_0 = 1$ .

- ¿Podemos calcular su periodo sin realizar ninguna iteración?
  - Se trata de un método multiplicativo ( $b = 0$ ).
  - Debemos verificar:
    - Semilla impar
    - $a \bmod 8 = 3$  o  $5$
- Realizar las primeras iteraciones.

$$x_1 = 3x_0 \bmod 2^5 = 3 \cdot 1 \bmod 32 = 3$$

$$x_2 = 3x_1 \bmod 2^5 = 3 \cdot 3 \bmod 32 = 9 \bmod 32 = 9$$

$$x_3 = 3x_2 \bmod 2^5 = 3 \cdot 9 \bmod 32 = 27 \bmod 32 = 27$$

$$x_4 = 3x_3 \bmod 2^5 = 3 \cdot 27 \bmod 32 = 81 \bmod 32 = 17$$

La secuencia sigue: 3, 9, 27, 17, 19, 25, 11, 1, 3,...

El periodo coincide con el calculado.

# Ejemplo 1

Sea el generador  $x_n = (3x_{n-1}) \bmod 2^5$  y la semilla  $x_0 = 1$ .

- Encontrar los primeros valores aleatorios generados.

Hemos obtenido la secuencia: 3, 9, 27, 17, 19, 25, 11, 1, 3,...

$$u_0 = \frac{x_0}{m} = \frac{1}{32} = 0.03125$$

$$u_1 = \frac{x_1}{m} = \frac{3}{32} = 0.09375$$

$$u_2 = \frac{x_2}{m} = \frac{9}{32} = 0.28125$$

$$u_3 = \frac{x_3}{m} = \frac{27}{32} = 0.85375$$

# Ejemplo 1b

Sea el generador  $x_n = (7x_{n-1}) \bmod 2^5$  y la semilla  $x_0 = 1$ .

- ¿Podemos calcular su periodo sin realizar ninguna iteración?
  - trata de un método multiplicativo ( $b = 0$ ).
  - Debemos verificar:
    - Semilla impar
    - $a \bmod 8 = 3$  o  $5$
- Realizar las primeras iteraciones.

La secuencia obtenida es 7, 17, 23, 1, 7, ...

Periodo es 4!

# Ejemplo 2

Sea el generador  $x_n = (3x_{n-1}) \bmod 31$  y la semilla  $x_0 = 1$ .

- ¿Podemos calcular su periodo sin realizar ninguna iteración?
- Realizar las primeras iteraciones
- Encontrar los primeros valores aleatorios generados.

# Ejemplo 2

Sea el generador  $x_n = (3x_{n-1}) \bmod 31$  y la semilla  $x_0 = 1$ .

- ¿Podemos calcular su periodo sin realizar ninguna iteración?
  - Se trata de un método multiplicativo ( $b = 0$ ).
  - El módulo no es potencia de 2.
  - Debemos verificar:
    - $m$  primo
    - $a$  raíz primitiva de módulo 31:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
3	9	27	19	26	16	17	20	29	25	13	8	24	10	30	28	22	4	12	5	15	14	11	2	6	18	23	7	21	1

- Realizar las primeras iteraciones.
  - $x_1 = 3x_0 \bmod 31 = 3 \cdot 1 \bmod 31 = 3$
  - $x_2 = 3x_1 \bmod 31 = 3 \cdot 3 \bmod 31 = 9 \bmod 32 = 9$
  - $x_3 = 3x_2 \bmod 31 = 3 \cdot 9 \bmod 31 = 27 \bmod 32 = 27$
  - $x_4 = 3x_3 \bmod 31 = 3 \cdot 27 \bmod 31 = 81 \bmod 32 = 19$

# Ejemplo 2

Sea el generador  $x_n = (3x_{n-1}) \bmod 31$  y la semilla  $x_0 = 1$ .

- Encontrar los primeros valores aleatorios generados.

Hemos obtenido la secuencia: 3, 9, 27, 19, 26, 16, 17, 20, 29, 25, 13, 8, 24, 10, 30, 28, 22, 0, 12, 5, 15, 14, 11, 2, 6, 18, 23, 7, 21, 1, 3,...

$$u_0 = \frac{x_0}{m} = \frac{1}{31} = 0.03226$$

$$u_1 = \frac{x_1}{m} = \frac{3}{31} = 0.09677$$

$$u_2 = \frac{x_2}{m} = \frac{9}{31} = 0.29032$$

$$u_3 = \frac{x_3}{m} = \frac{27}{31} = 0.87097$$

# Ejemplo 3

Sea el generador  $x_n = (8x_{n-1} + 15) \bmod 31$  y la semilla  $x_0 = 13$ .

- ¿Podemos calcular su periodo sin realizar ninguna iteración?
- Realizar las primeras iteraciones
- Encontrar los primeros valores aleatorios generados.

# Ejemplo 3

Sea el generador  $x_n = (8x_{n-1} + 15) \bmod 31$  y la semilla  $x_0 = 13$ .

- ¿Podemos calcular su periodo sin realizar ninguna iteración?
  - Se trata de un método mixto ( $b \neq 0$ ).
  - El módulo no es potencia de 2.
  - Debemos verificar:
    - $m$  y  $b$  coprimos
    - Los factores de  $m$  dividen a  $a - 1$
    - Si 4 es factor de  $m$  entonces 4 es factor de  $a - 1$
- Realizar las primeras iteraciones.
  - $x_1 = 8x_0 + 15 \bmod 31 = 8 \cdot 13 + 15 \bmod 31 = 119 \bmod 31 = 26$
  - $x_2 = 8x_1 + 15 \bmod 31 = 8 \cdot 26 + 15 \bmod 31 = 223 \bmod 31 = 6$
  - $x_3 = 8x_2 + 15 \bmod 31 = 8 \cdot 6 + 15 \bmod 31 = 63 \bmod 31 = 1$
  - $x_4 = 8x_3 + 15 \bmod 31 = 8 \cdot 1 + 15 \bmod 31 = 23 \bmod 31 = 23$



# Ejemplo 3

Sea el generador  $x_n = (8x_{n-1} + 15) \bmod 31$  y la semilla  $x_0 = 13$ .

- Encontrar los primeros valores aleatorios generados.

La secuencia sigue como: 13, 26, 6, 1, 23, 13,...

El periodo es  $T = 5$

$$u_0 = \frac{x_0}{m} = \frac{13}{31} = 0.4194$$

$$u_1 = \frac{x_1}{m} = \frac{26}{31} = 0.8387$$

$$u_2 = \frac{x_2}{m} = \frac{6}{31} = 0.1935$$

$$u_3 = \frac{x_3}{m} = \frac{1}{31} = 0.0322$$

# Ejemplo 4

Sea el generador  $x_n = (5x_{n-1} + 3) \bmod 8$  y la semilla  $x_0 = 7$ .

- ¿Podemos calcular su periodo sin realizar ninguna iteración?
- Realizar las primeras iteraciones
- Encontrar los primeros valores aleatorios generados.

# Ejemplo 3

Sea el generador  $x_n = (5x_{n-1} + 3) \bmod 8$  y la semilla  $x_0 = 7$ .

- ¿Podemos calcular su periodo sin realizar ninguna iteración?
  - Se trata de un método mixto ( $b \neq 0$ ).
  - El módulo es potencia de 2.
  - Debemos verificar:
    - $b$  impar
    - $a \bmod 4 = 1$
  - Periodo máximo  $T = 8$ .
- Realizar las primeras iteraciones.
  - La secuencia de estados es: 7, 6, 1, 0, 3, 2, 5, 4, 7,...
- Encontrar los primeros valores aleatorios generados.
  - $u_0 = 0.875, u_1 = 0.75, u_2 = 0.125, u_3 = 0, \dots$

# Combinación de métodos congruenciales

- Los generadores de congruencia se pueden generalizar y definir recursiones de orden mayor. Estos métodos se definen de forma general como se muestra a continuación,

$$x_n = (a_1x_{n-1} + a_2x_{n-2} + \dots + a_kx_{n-k}) \bmod m$$

- Donde  $m$  y  $k$ , son números enteros positivos y los coeficientes  $a_i$  toman sus valores entre  $-(m-1)$  y  $(m-1)$ .

# Combinación de métodos congruenciales

- Para obtener periodos más largos combinamos generadores multiplicativos. Sumamos los números obtenidos de dos o más generadores. La fórmula para obtener los números de la secuencia es

$$x_n = \left( \sum_{j=1}^k (-1)^{j-1} X_{i,j} \right) \bmod M$$

- Donde las  $X_{i,j}, j = 1, \dots, k$  son las salidas obtenidas de diferentes generadores de congruencia multiplicativa y  $M = \max(m_1, \dots, m_k)$ .

# Combinación de métodos congruenciales

- A su vez se deberán obtener los números pseudo-aleatorios buscados según la siguiente definición:

$$u_n = \begin{cases} \frac{X_n}{M}, & \text{si } X_n > 0 \\ \frac{M-1}{M}, & \text{si } X_n = 0 \end{cases}$$

- El periodo se obtiene como el mínimo común múltiplo de los periodos de los generadores.

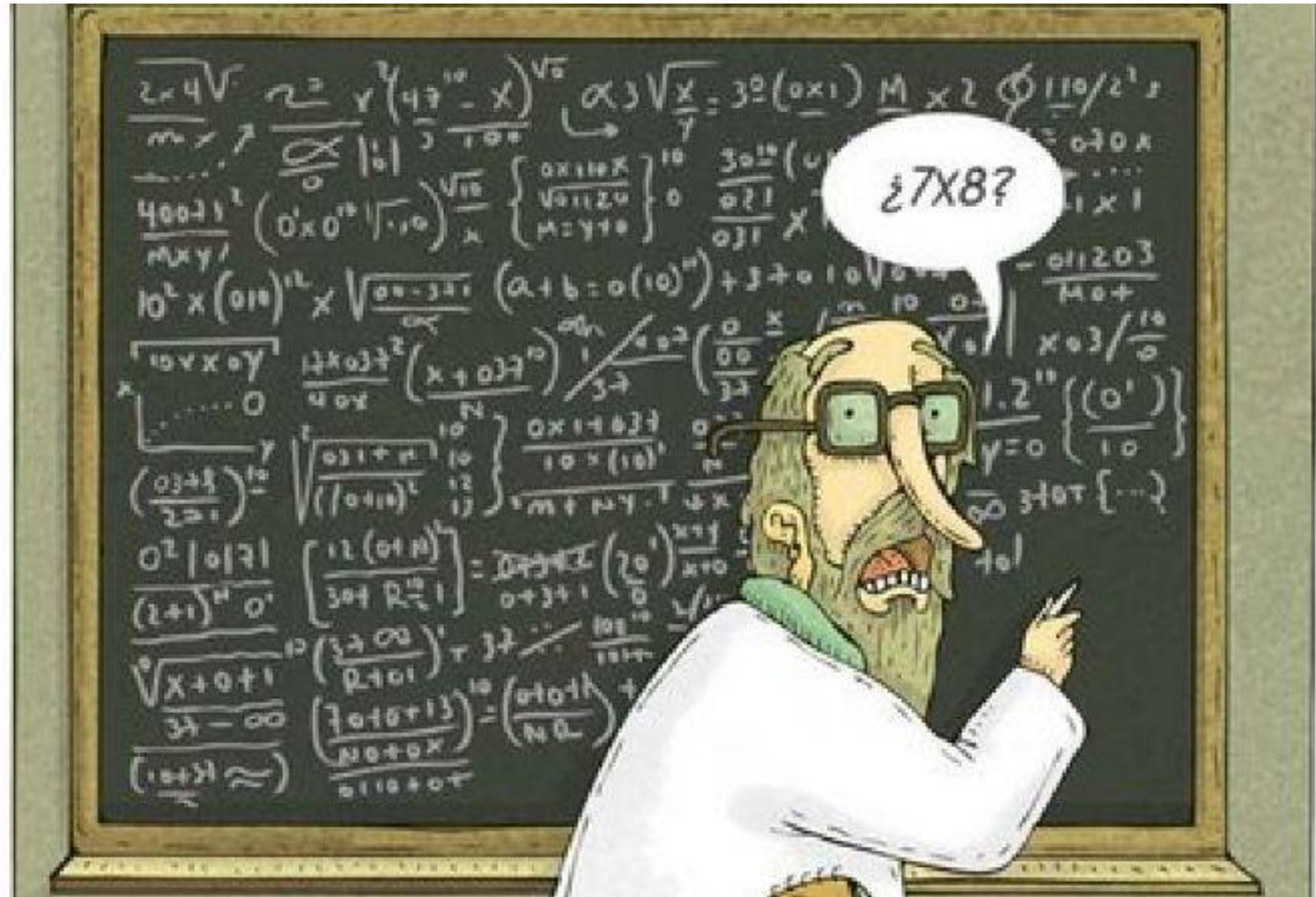
# Ejemplo de combinación

Dados los siguientes generadores de congruencia multiplicativos.

- $v_n = 157 \cdot v_{n-1} \bmod 32363$
- $t_n = 146 \cdot t_{n-1} \bmod 31727$
- $w_n = 142 \cdot w_{n-1} \bmod 31657$
- El generador combinado se define a partir de los anteriores como:
  - $X_n = (v_n - t_n + w_n) \bmod 32363$
- Y el periodo es:
$$\begin{aligned} T &= m.c.m.(32363 - 1, 31727 - 1, 31657 - 1) \\ &= 2^3 \cdot 3 \cdot 11 \cdot 29 \cdot 547 \cdot 1319 \cdot 1471 \\ &= 8\,125\,436\,850\,168 \end{aligned}$$

$$\begin{aligned} 32362 &= 2 \cdot 11 \cdot 1471 \\ 31726 &= 2 \cdot 29 \cdot 547 \\ 31656 &= 2^3 \cdot 3 \cdot 1319 \end{aligned}$$

# ¿Dudas?







[www.unir.net](http://www.unir.net)