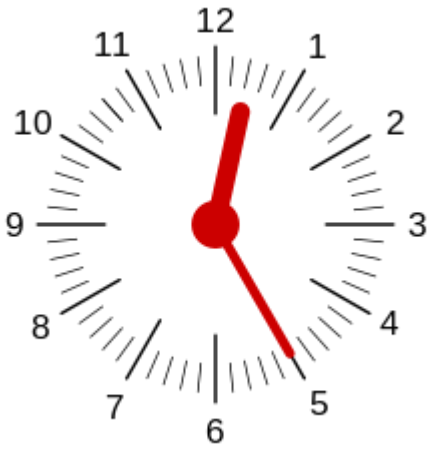
Generadores congruenciales



Conceptos previos

Algoritmo de la división entera

Dado dos enteros a y b, siendo b > 0, existen dos enteros c y r, llamados cociente y residuo, que verifican:

- $a = bc + r$
- $0 \leq r < b$

Donde:

$a,\ es\ el\ dividendo$
$b,\ es\ el\ divisor$
$c,\ es\ el\ cociente$
$r,\ es\ el\ residuo$

Módulo de un número

Dado dos enteros a y b, siendo b > 0, existen dos enteros c y r, llamados cociente y residuo, que verifican:

$$a\ mod\ b = r$$

Congruencia (teoría de números)

Congruencia es un término usado, para designar que dos números enteros x, y tienen el mismo resto al dividirlos por un número natural $m \neq 0$; esto se expresa utilizando la notación:

$$x \equiv y\ (mod\ m)$$

Esto se cumple si y sólo si

$$m \mid (x - y)$$

1. Algoritmo congruencial lineal

Derrick Henry Lehmer (1905 – 1991) fue un matemático estadounidense. En 1940, Lehmer aceptó una posición de regreso en el departamento de matemática de la Universidad de Berkeley. Mientras se encontraba aquí es que desarrolló el generador lineal congruencial (generador de números pseudoaleatorios), conocido como generador de números aleatorios de Lehmer.

El generador congruencial lineal genera una serie de números pseudo-aleatorios de tal forma que se puede generar el siguiente a partir del último número derivado, es decir, que el número X_{n+1} es generado a partir de X_n.

La relación de recurrencia para el método congruencial mixto es:

$$X_{i+1} = (aX_i + c) \bmod m, \qquad i = 0, 1, 2, 3, \ldots n$$

Donde:

X_0, *es la semilla* $(X_0 > 0)$

a, *es el multiplicador* $(a > 0)$

c, *es la constante aditiva* $(c > 0)$

m, *es el módulo* $(m > X_0,\ m > a \ \ y \ \ m > c)$

Para generar números pseudo-aleatorios, se tiene la relación:

$$r_i = \frac{X_i}{m-1}, \qquad i = 0, 1, 2, 3, \ldots n \qquad [0,1]$$

$$r_i = \frac{X_i}{m}, \qquad i = 0, 1, 2, 3, \ldots n \qquad [0,1[$$

Características

- Si se repite un número ya se repite toda la secuencia.
- Utiliza poca memoria y es rápido.
- Se genera la misma secuencia, a partir de la semilla: X_0.

Ejemplos

- X_0=7, a=1, c=7, m=13
- X_0=5, a=7, c=9, m=11
- X_0=7, a=7, c=7, m=10

Selección de: m, a, c, X_0

Para “m” se tiene:

“m” debe ser en el entero más grande que acepte la computadora:

$$m = p^{d-1}$$

Donde:

- p, es la base del sistema que se está usando.
- d, es el número de bits que tiene una palabra de computadora.

Por ejemplo en una computadora XT que trabaja en el sistema binario se tiene que:

- p = 2 y d = 16.

Para mejorar más el generador puede tomarse como “m” al número primo más grande posible y además que sea menor que: p^{d-1}

Para “a” se tiene:

“a” debe ser un número entero impar, que no deberá ser divisible por 3 ni 5. Pero además, para que el generador tenga período completo, el valor que se tome para “a” deberá escogerse según el siguiente criterio:

- (a-1) mod 4 = 0, si 4 es un factor de “m”.
- (a-1) mod b = 0, si b es un factor primo de “m”.

Generalmente se toma “a” igual a 2K+1 cuando se trabaja en el sistema binario. En ambos casos el valor que se asigne a “k” deberá ser mayor o igual que 2.

Para “c” se tiene:

- Para una computadora binaria
  - c mod 8 = 5
- Para una decimal
  - c mod 200 = 21

En consecuencia “c” deberá tomar un valor entero, impar y relativamente primo a “m”.

Para "X_0" se tiene:

El valor que tome "X_0" es irrelevante y tiene poca o ninguna influencia sobre las propiedades estadísticas de las series de números pseudo-aleatorios que se generen. Aunque otros consideran un número impar.

Caso: computadora binaria:

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

- c = 8*a±3
- a = cualquier entero
- X_0 = cualquier entero impar
- m = 2^b ,tal que b>2 y "m" debe ser aceptado por la computadora

Otras recomendaciones:

Bank, Carson, Nelson y Nicol sugieren:

- m = 2^b , b es cualquier entero
- a = 1+4k, k es cualquier entero
- c es un primo relativo a "m"

Ejemplos

- X_0=6, k=3, c=7, b=3 → X_0=6, a=13, c=7, m=8

Actividades

Determinar el periodo de los siguientes generadores congruenciales lineales:

- X_{n+1} = (8X_n+16) mod 100 y X_0 = 15.
- X_{n+1} = (50X_n+17) mod 64 y X_0 = 13.

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

- X_{n+1} = (40X_n+13) mod 33 y X_0 = 30.
- X_{n+1} = (71X_n+57) mod 341 y X_0 = 71.

2. Algoritmo congruencial multiplicativo

Partiendo de la relación:

$$X_{i+1} = (aX_i + c) \, mod \, m, \qquad i = 0, 1, 2, 3, \ldots n$$

con c=0 se tiene:

$$X_{i+1} = (aX_i) \, mod \, m, \qquad i = 0, 1, 2, 3, \ldots n$$

esta última expresión corresponde al algoritmo congruencial multiplicativo

Criterios para los parámetros :

Bank, Carson, Nelson y Nicol sugieren:

- m = 2^b , b es cualquier entero
- a = 3+8k o también a = 5+8k, k = 0, 1, 2, 3, ...
- X_0= debe ser un número impar

Con estas condiciones se logra un periodo de vida máximo de N = m/4 = 2^{b-2}

Ejemplo

- X_0=17, k=2, b=5 → X_0=17, a=19, m=32

Actividades

Determinar los periodos

- X_0=5, a=5, m=32
- X_0=1, a=6, m=13
- X_0=10, a=7, m=13
- X_0=5, a=5, m=13
- X_0=5, a=7, m=11
- X_0=3, a=6, m=11

3. Algoritmo congruencial aditivo

Partiendo de la secuencia de números enteros: $X_1, X_2, X_3, \ldots, X_n$, para generar una nueva secuencia de números enteros que empiezan en: $X_{n+1}, X_{n+2}, X_{n+3}, \ldots$ su ecuación recursiva es:

$$X_i = (X_{i-1} + X_{i-n}) \, mod \, m, \qquad i = n + 1, n + 2, n + 3, \ldots$$

Ejemplo

Genere 7 números pseudo-aleatorios a partir de la secuencia: 65, 89, 98, 03, 69 y m=100

4. Algoritmos congruenciales no lineales

a. Algoritmo congruencial cuadrático

La relacion recursiva corresponde a:

$$X_{i+1} = (aX^2_i + bX_i + c) \, mod \, m, \qquad i = 0, 1, 2, 3, \ldots$$

De acuerdo con L'Ecuyer, las condiciones que deben cumplir los parámetros. a, b, c y m para alcanzar un periodo máximo N=m son:

- $m = 2^b$, b es cualquier entero
- "a" debe un número par
- (b-1) mod 4 = 1
- "c" debe un número impar

Ejemplo

Generar números pseudo-aleatorios hasta alcanzar el periodo de vida, con los parámetros: X_0=13, m=8, a=26, b=27, c=27.

b. Algoritmo de Blum, Blum y Shub

Partiendo de la relación:

$$X_{i+1} = (aX^2_i + bX_i + c) \, mod \, m, \qquad i = 0, 1, 2, 3, \ldots$$

para el caso: a=1, b=0 y c=0 se tiene:

$$X_{i+1} = (X^2_i) \, mod \, m, \qquad i = 0, 1, 2, 3, \ldots$$

esta última relación corresponde al algoritmo de Blum, Blum y Shub

Ejemplo

Generar números pseudo-aleatorios hasta alcanzar el periodo de vida, con los parámetros: X_0=13, m=8

Referencia

E. Garcia, Simulacion y analisis de sistemas con Promodel, 2da edición,