Master en Ingeniería Matemática
Modelización y Simulación numérica
Resumen Generación números aleatorios

1. Generación números aleatorios

Hemos visto los métodos de congruencia:
Dada una semilla x_0 calculamos el siguiente valor del estado cómo:

$$x_n = (ax_{n-1} + b) \bmod m$$

Sabemos que esta sucesión será periódica. En general nos interesará que el periodo de la sucesión sea lo más largo posible. Si el periodo es completo mejor.

1.1. Periodo Completo:

1.1.1. Caso general

En el caso general el periodo es completo si:

- m y b coprimos (no tienen factores comunes).
- $a - 1$ es divisible por todos los factores primos de m.
- si m es múltiplo de 4, entonces $a - 1$ es múltiplo de 4.

En la práctica:
para verificar que el periodo es completo debemos:

1. Realizar la descomposición en factores primos de m y b.
2. Comprobar las dos descomposiciones no tienen factores comunes.
3. Comprobar que $a - 1$ es divisible por todos los factores primos de m.
4. Si m es múltiplo de 4, verificar que $a - 1$ también lo es.

Si alguna de las comprobaciones 2, 3 o 4 no se cumple entonces el periodo no es completo.

1.1.2. Caso m potencia de 2

Si m es una potencia de 2 ($m = 2^k$), entonces el periodo es completo si:

- b impar.
- $a \bmod 4 = 1$

1.2. Métodos multipicativos ($b = 0$)

El periodo máximo es $m - 1$.

1.2.1. Caso $m = 2^k > 16$

En este caso el periodo máximo es $\frac{m}{4} = 2^{k-2}$. Se consigue si:

- x_0 es impar.
- a mod $8 = 3$ o 5.

1.2.2. Caso $m \neq 2^k$

Se alcanza el periodo máximo $T = m - 1$ si:

- m es primo.
- a es raíz primitiva de m.

Comproción de raíz primitiva:
a es raíz primitiva de m si $a \neq 0$ y no existe ningún factor primo p de m?1 tal que $a^{\frac{m-1}{p}}$ mod $m = 1$.
Para comprobarlo, debemos:

1. buscar los factores primos p de $m - 1$.
2. Verificar que $a^{\frac{m-1}{p}}$ mod $m \neq 1$. Para realizar el cálculo es aconsejable multiplicar y hacer módulo las veces necesarias, si no, podemos encontrarnos con casos en los que no tengamos suficiente precisión en la calculadora.
   Ejemplo: a=3, m=31. Los factores primos de 30 son 2,3,5. Debemos comprobar pues:
   $$3^{30/5} \bmod 31 = 3^6 \bmod 31 = 16 \neq 1$$
   $$3^{30/3} \bmod 31 = 3^{10} \bmod 31 = 25 \neq 1$$
   $$3^{30/2} \bmod 31 = 3^{15} \bmod 31 = 30 \neq 1$$
   Observemos que $3^{15} = 14348907$. Algunas calculadoras pueden tener dificultad para almacenar números grandes. Si se da el caso se puede hacer la operación descomponiendo el exponente y realizando la descomposición a cada paso cómo sigue:
   $$3^{15} = 3^5 \cdot 3^5 \cdot 3^5 = 243 \cdot 3^5 \cdot 3^5 = 26 \cdot 3^5 \cdot 3^5 = 5318 \cdot 3^5 = 25 \cdot 3^5 = 6075 = 30 \bmod 31$$
   En la tercera, quinta y séptima igualdad hemos realizado la operación módulo sobre el primer número del producto.

2. Indicaciones sobre los ejercicios

Pasos para seguir en los ejercicios de generación de números aleatorios

1. Identificar si se trata de un generador multiplicativo o mixto y si es del tipo potencia de dos o no.
2. Según el caso mirar cuál es el periodo máximo posible.
3. Verificar las condiciones de periodo máximo.
4. Si no se cumplen las condiciones, buscar el periodo .ª mano". Es decir, aplicando el método las veces que sea necesario.