Cifrado en flujo

Generadores congruenciales

eman ta zabal zazu
Universidad del País Vasco
Euskal Herriko Unibertsitatea
KISA

Generadores Congruenciales Lineales (LCG)

Sea $m \in \mathbb{Z}$ y $a, b, x_0 \in \mathbb{Z}_m$. Definimos

$$x_n = (ax_{n-1} + b) \mod m, \quad n = 1, 2, \ldots$$

Nota:

- El período de (x_n) es menor o igual que m.
- Bajo ciertas condiciones, (x_n) presenta período máximo m.

Proposición

La secuencia (x_n) es de período máximo si y sólo si

- $\mathrm{mcd}(b, m) = 1$,
- *para todo p primo tal que $p|m$, $a \equiv 1 \mod p$, y*
- *si $4|m$, $a \equiv 1 \mod 4$.*

Parámetros que proporcionan período máximo:

a	b	m
106	1283	6075
211	1663	7875
421	1663	7875
430	2531	11979
936	1399	6655
1366	1283	6075
171	11213	53125
859	2531	11979
419	6173	29282
...	...	...

Ver Schneier, Cryptography, 2000

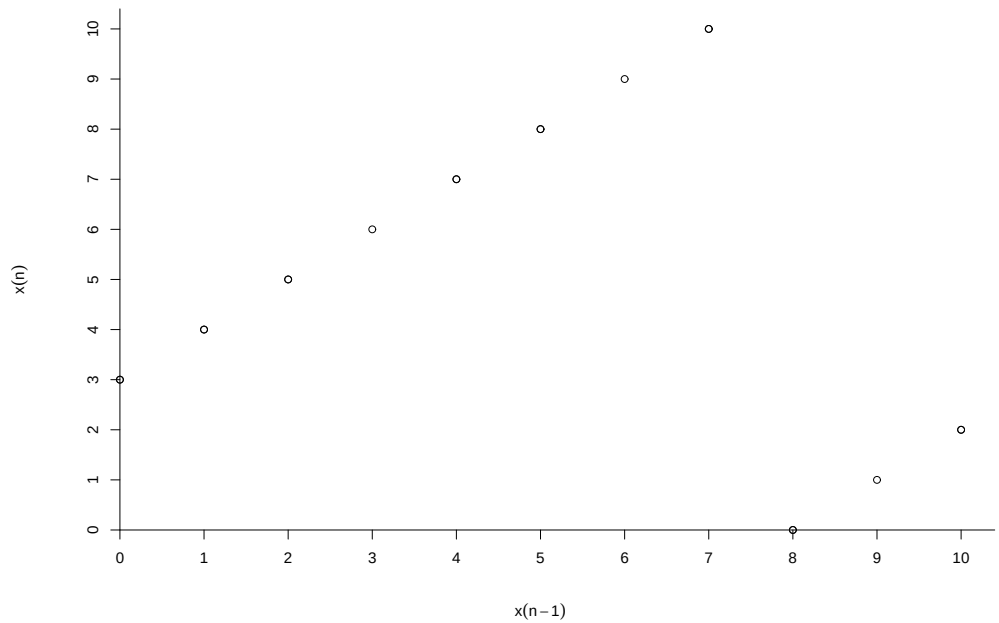
Ejemplo

$a = 1,\ b = 3,\ m = 11,\ x_0 = 1.$

$$x_{n+1} = x_n + 3 \quad \text{mód } 11$$

$$(x_n) = (1, 4, 7, 10, 2, 5, 8, 0, 3, 6, 9, 1, 4, 7, 10, 2, 5, 8, 0, 3, \ldots)$$

presenta período máximo, 11.

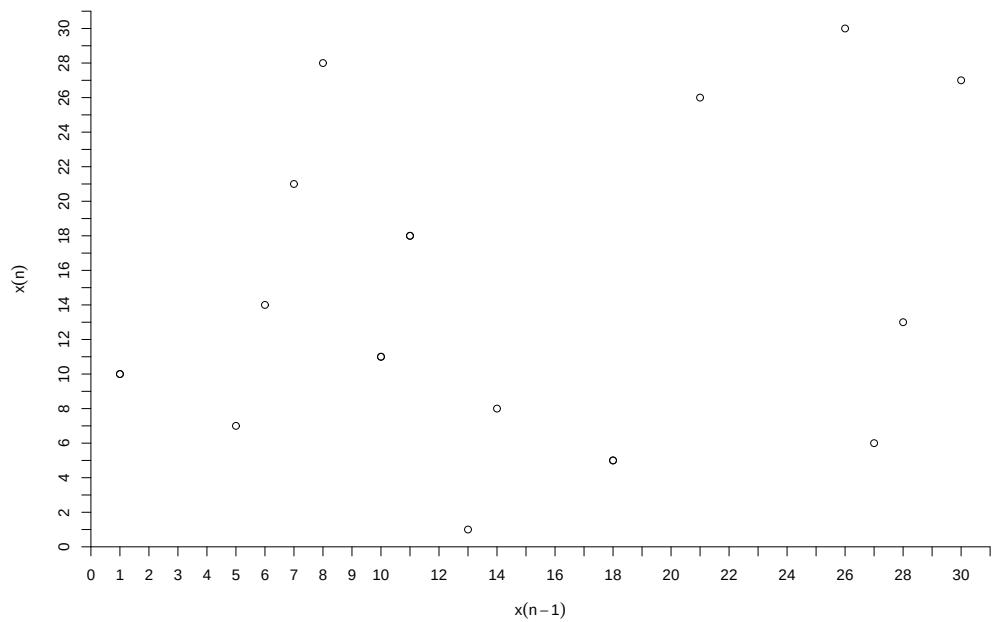


Ejemplo

$a = 7,\ b = 3,\ m = 31,\ x_0 = 1.$

$$x_{n+1} = 7x_n + 3 \quad \text{mód } 31$$

$$(x_n) = (1, 10, 11, 18, 5, 7, 21, 26, 30, 27, 6, 14, 8, 28, 13, 1, 10, 11, 18, 5 \ldots)$$



Características de los LCGs

Ventajas:

- Buenas propiedades aleatorias: pasan tests de aleatoriedad.
- Son rápidos, involucran pocas operaciones.
- Son eficientes para simulaciones.

Inconvenientes:

- No son de uso criptográfico: es fácil reconstruir la secuencia a partir de parte de ella.
- Sucede lo mismo con los cuadráticos:

$$x_n = (ax_{n-1}^2 + bx_{n-1} + c) \mod m$$

- Y con los cúbicos, ...

Reconstrucción de una secuencia

Ejemplo

Consideremos la secuencia

$$(x_n) = (1, 10, 11, 18, 5, 7, 21, 26, 30, 27, 6, 14, 8, 28, 13, 1, 10, 11, 18, 5 \ldots)$$

Supongamos que ha sido producida por un generador congruencial lineal de módulo 31:

$$x_{n+1} = ax_n + b \quad \text{mód } 31$$

Queremos encontrar a y b.

Los términos de la sucesión deben satisfacer

$$\begin{array}{lcll} x_1 & = & a \cdot x_0 + b & \text{mód } 31 \\ x_2 & = & a \cdot x_1 + b & \text{mód } 31 \\ x_3 & = & a \cdot x_2 + b & \text{mód } 31 \\ \vdots & & \vdots & \end{array}$$

Veamos cómo a partir de 3 términos consecutivos de la secuencia podemos reconstruirla entera. Las dos primeras ecuaciones son

$$\begin{aligned} 10 &= a \cdot 1 + b \mod 31 \\ 11 &= a \cdot 10 + b \mod 31 \end{aligned}$$

Hemos de resolver el sistema. Restando las dos ecuaciones

$$1 = a \cdot 9 \mod 31$$

es decir

$$a = (9^{-1} \mod 31) = 7$$

Sustiuyendo en la primera ecuación

$$b = ((10 - 7 \cdot 1) \mod 31) = 3$$

Por tanto

$$x_{n+1} = 7x_n + 3 \mod 31,\ n = 0, 1, 2, \ldots$$

con lo cual podemos obtener toda la secuencia.

Obtención de una secuencia de bits a partir de un LCG

Sea (x_n) producida por un LCG de período máximo m.
La secuencia de bits de paridad posee buenas propiedades aleatorias:

$$(s_n) = (x_n \mod 2)$$

Ejemplo

Sea la secuencia generada por el LCG de la transparencia 4, de período 11:

$$(x_n) = (1, 4, 7, 10, 2, 5, 8, 0, 3, 6, 9, 1, 4, 7, 10, 2, 5, 8, 0, 3, 6, 9, 1, \ldots)$$

La secuencia de bits de paridad $(x_n \mod 2)$ es

$$(s_n) = (x_n \mod 2) = (1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, \ldots)$$

y posee buenas propiedades aleatorias.

Nota: En cambio no tienen buenas propiedades aleatorias:

- (x_n) representada en base 2:

$$(1\ 100\ 111\ 1010\ 10\ 101\ 1000\ 0\ 11\ 110\ 1001\ldots)$$

- (x_n) representada en código ASCII:

$$(00000001\ 00000100\ 00000111\ 00001010\ 00000010\ 00000101$$
$$00001000\ 00000000\ 00000011\ 00000110\ 00001001\ldots)$$

Fin de la sección