GFSR - Lewis , Payne 1973

Uses the same LFSR across all bits of the words : if the degree of the LFSR is n then the period is $2^n - 1$.

The initialization is problematic and slow especially in the original rng.

If we see the state as made by n vertical words then fill each row of bits one after the other with the LFSR skipping some outcomes after any row :

$$[\mathbf{w_0}, \mathbf{w_1}, \ldots] = \begin{bmatrix} w_{0,0} & \ldots & w_{0,n-1} \\ w_{1,0} & \ldots & w_{1,n-1} \\ w_{2,0} & \ldots & w_{2,n-1} \end{bmatrix}$$

In [2]:
```
p:2
```
Out[2]: 2

In [3]:
```
n:3
```
Out[3]: 3

In [4]:
```
gf_primitive_poly(p,3)
```
Out[4]: $x^3 + x + 1$

Therefore a $LFSR(3, 1 + x + x^3)$ will have maximal period $p^n - 1 = 2^3 - 1 = 8 - 1 = 7$

In [5]:
```
seed:[1,0,1]
```
Out[5]: $[1, 0, 1]$

In [6]:
```
lfsr:matrix([1,1,0],
            [0,0,1],
            [1,0,0])
```
Out[6]: $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$

In [7]:
```
for i:1 thru p^n  do ( seed:mod(seed . lfsr,p), print(i,seed))
```
```
1 [ 0  1  0 ]
2 [ 0  0  1 ]
3 [ 1  0  0 ]
4 [ 1  1  0 ]
5 [ 1  1  1 ]
6 [ 0  1  1 ]
7 [ 1  0  1 ]
8 [ 0  1  0 ]
```
Out[7]: **done**

Let's now build a GFSR with the same polynomial using numbers $0 \le x \le m : 2^3$

In [17]:
```
m:2^3
```
Out[17]: 8

In [20]:
```
mseed:matrix([7,3,2])
```
Out[20]: $\begin{pmatrix} 7 & 3 & 2 \end{pmatrix}$

In [21]:
```
for i:1 thru p^m-1 do ( mseed:mod(mseed . lfsr,m), print(i,mseed))
```

```
1 [ 1  7  3 ]
2 [ 4  1  7 ]
3 [ 3  4  1 ]
4 [ 4  3  4 ]
5 [ 0  4  3 ]
6 [ 3  0  4 ]
7 [ 7  3  0 ]
8 [ 7  7  3 ]
9 [ 2  7  7 ]
10 [ 1  2  7 ]
11 [ 0  1  2 ]
12 [ 2  0  1 ]
13 [ 3  2  0 ]
14 [ 3  3  2 ]
15 [ 5  3  3 ]
16 [ 0  5  3 ]
17 [ 3  0  5 ]
18 [ 0  3  0 ]
19 [ 0  0  3 ]
20 [ 3  0  0 ]
21 [ 3  3  0 ]
22 [ 3  3  3 ]
23 [ 6  3  3 ]
24 [ 1  6  3 ]
25 [ 4  1  6 ]
26 [ 2  4  1 ]
27 [ 3  2  4 ]
28 [ 7  3  2 ]
29 [ 1  7  3 ]
30 [ 4  1  7 ]
31 [ 3  4  1 ]
32 [ 4  3  4 ]
33 [ 0  4  3 ]
34 [ 3  0  4 ]
35 [ 7  3  0 ]
36 [ 7  7  3 ]
37 [ 2  7  7 ]
38 [ 1  2  7 ]
39 [ 0  1  2 ]
40 [ 2  0  1 ]
41 [ 3  2  0 ]
42 [ 3  3  2 ]
43 [ 5  3  3 ]
44 [ 0  5  3 ]
45 [ 3  0  5 ]
46 [ 0  3  0 ]
47 [ 0  0  3 ]
48 [ 3  0  0 ]
49 [ 3  3  0 ]
50 [ 3  3  3 ]
51 [ 6  3  3 ]
52 [ 1  6  3 ]
53 [ 4  1  6 ]
54 [ 2  4  1 ]
55 [ 3  2  4 ]
56 [ 7  3  2 ]
57 [ 1  7  3 ]
58 [ 4  1  7 ]
59 [ 3  4  1 ]
60 [ 4  3  4 ]
61 [ 0  4  3 ]
62 [ 3  0  4 ]
63 [ 7  3  0 ]
64 [ 7  7  3 ]
65 [ 2  7  7 ]
66 [ 1  2  7 ]
67 [ 0  1  2 ]
68 [ 2  0  1 ]
69 [ 3  2  0 ]
70 [ 3  3  2 ]
71 [ 5  3  3 ]
72 [ 0  5  3 ]
73 [ 3  0  5 ]
74 [ 0  3  0 ]
75 [ 0  0  3 ]
76 [ 3  0  0 ]
77 [ 3  3  0 ]
78 [ 3  3  3 ]
79 [ 6  3  3 ]
```

Out[21]: **done**

In [ ]:

```

```