Periods of LCGs + LFSRs

LCG from seed x_0 generate

$$x_{n+1} \equiv a x_n + b \pmod{m}$$

$$PRG(x_0) = x_1 x_2 x_3 \ldots$$

The **maximum period** is m.

EG $x_{n+1} \equiv 5x_n + 3 \pmod{8}$

0 3 2 5 4 7 6 1 0 3 2 5 ...

x_0 x_1 ...

LCG has period 8 (for any seed).

EG $x_{n+1} \equiv 5x_n + 2 \pmod{8}$

0 2 4 6 0 2 4 ... period 4

1 7 5 3 1 7 5 ... period 4

LFSR from seed $(x_1, x_2, \ldots, x_\ell)$ generate

$$x_{n+\ell} \equiv c_1 x_{n+\ell-1} + c_2 x_{n+\ell-2} + \ldots + c_\ell x_n \pmod{2}$$

$$PRG((x_1, x_2, \ldots, x_\ell)) = x_{\ell+1} x_{\ell+2} x_{\ell+3} \ldots$$

The **maximum period** is $2^\ell - 1$.

EG $x_{n+3} \equiv x_{n+2} + x_n \pmod{2}$

previously: 1 0 0 1 1 1 0 1 0 0 1 1 ...

seed → repeats

period $7 = 2^3 - 1$

2^3 possible states

special state: 000

$2^3 - 1$ other states