Let $f: \mathbb{Z}_4 \times \mathbb{Z}_5 \to \mathbb{Z}_{20}$ be the isomorphism of CRT. Then

a) $f(x,y) = 16x + 5y$

b) $f(x,y) = 13x + 8y$

c) $f(x,y) = 5x + 16y$ ✓

d) $f(x,y) = 8x + 13y$

Solution:

$f(a,b) = af(1,0) + bf(0,1)$ linear combination

$\begin{cases} x \equiv 1 \bmod 4 \\ x \equiv 0 \bmod 5 \end{cases} \Rightarrow x = 5y$

$5y \equiv 1 \bmod 4 \Rightarrow y = 1$

$6 = 2 \bmod 4$
$ 1 \bmod 5$

Es 2

A m-bit Fibonacci LFSR has m flip flops and produces an output stream $...s_2 s_1 s_0$

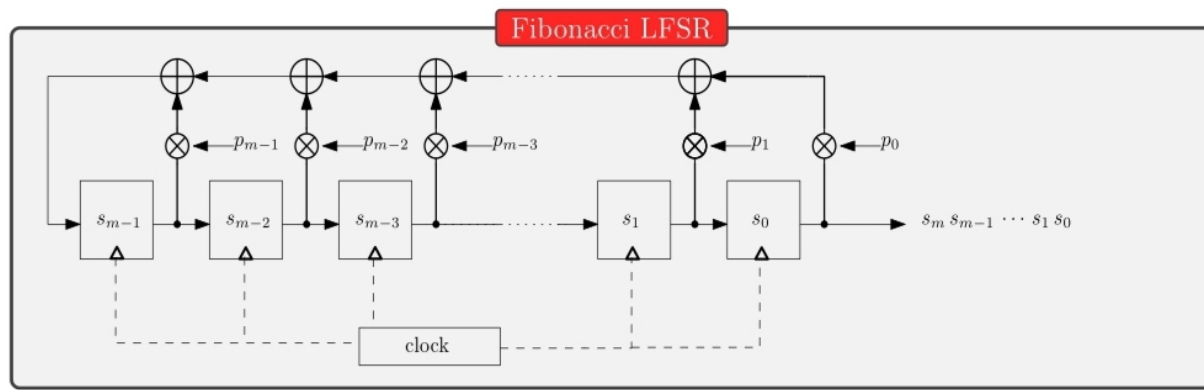If a sequence like $...0110000100 1...$ is observed in the output stream, then

a) $m = 4$

b) $m = 2$

c) $m = 5$ ✓

d) $m = 3$

Solution:

2.4.1 Fibonacci LFSRs

Fibonacci LFSR

We see that at some point there are 4 consecutives zeros in the string maximum. Then $m = 5$ because if $m=4$ there would be a moment in which all the flip flops contain ϕ, so the whole stream would be composed by zeros. Hence $m > 4$ and the first number is 5