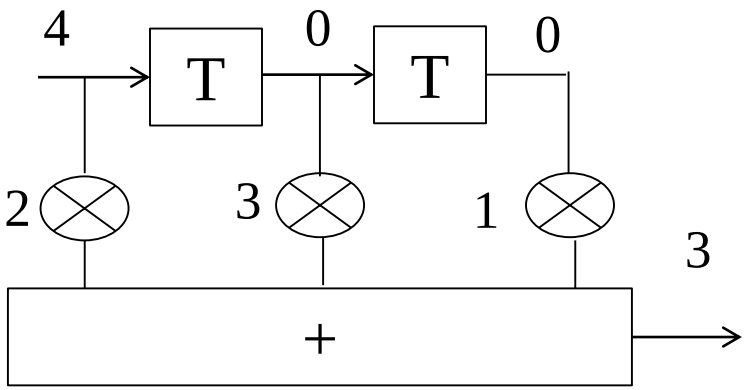
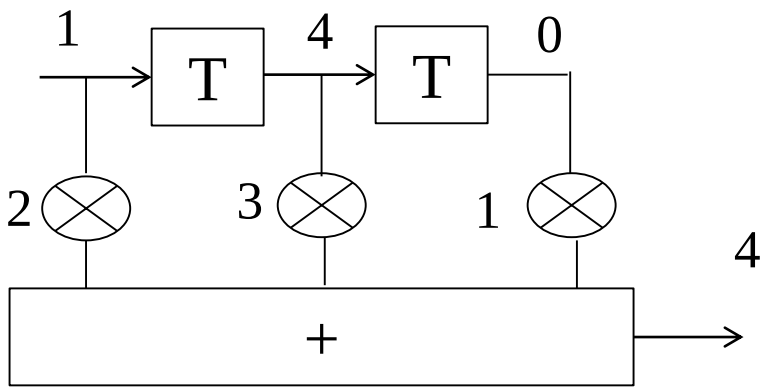
Multiplication by Linear FeedForward Shift Registers

$$\left(x^2+3x+2\right)\left(x+4\right) \quad \text{over} \quad GF(5)$$

$$\left(x^2+3x+2\right)\left(x+4\right)=x^3+3x^2+2x+4x^2+2x+3=x^3+2x^2+4x+3$$

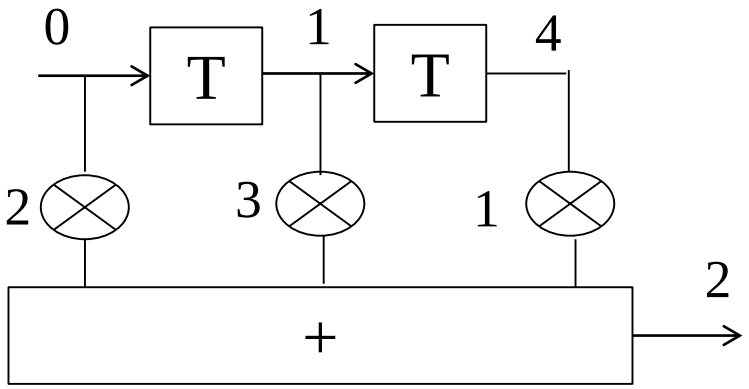


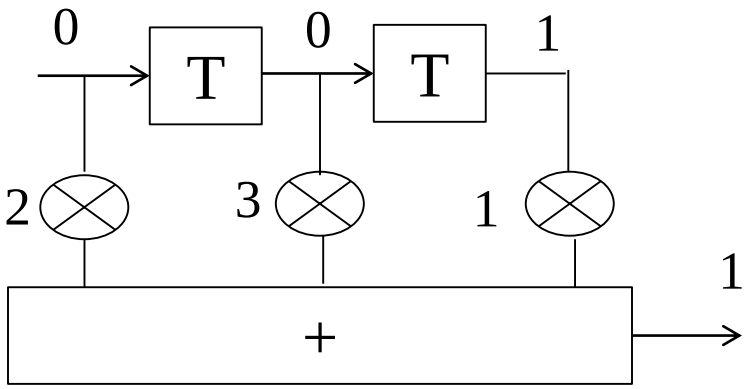


Operation LFFSR

$$\left(x^2+3x+2\right)\left(x+4\right) \text{ over } GF(5)$$

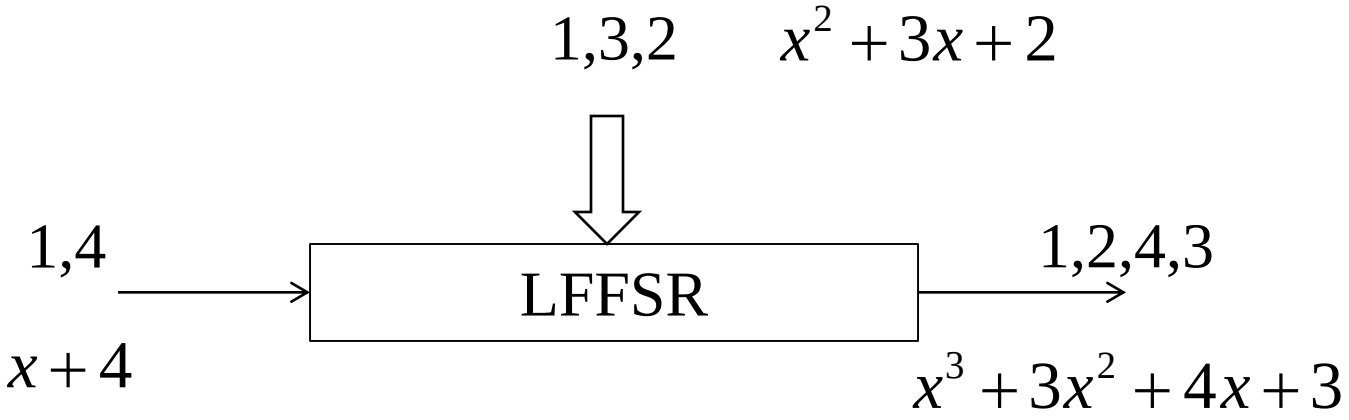
$$\left(x^2+3x+2\right)\left(x+4\right)=x^3+3x^2+2x+4x^2+2x+3=x^3+2x^2+4x+3$$





Final result of multiplication

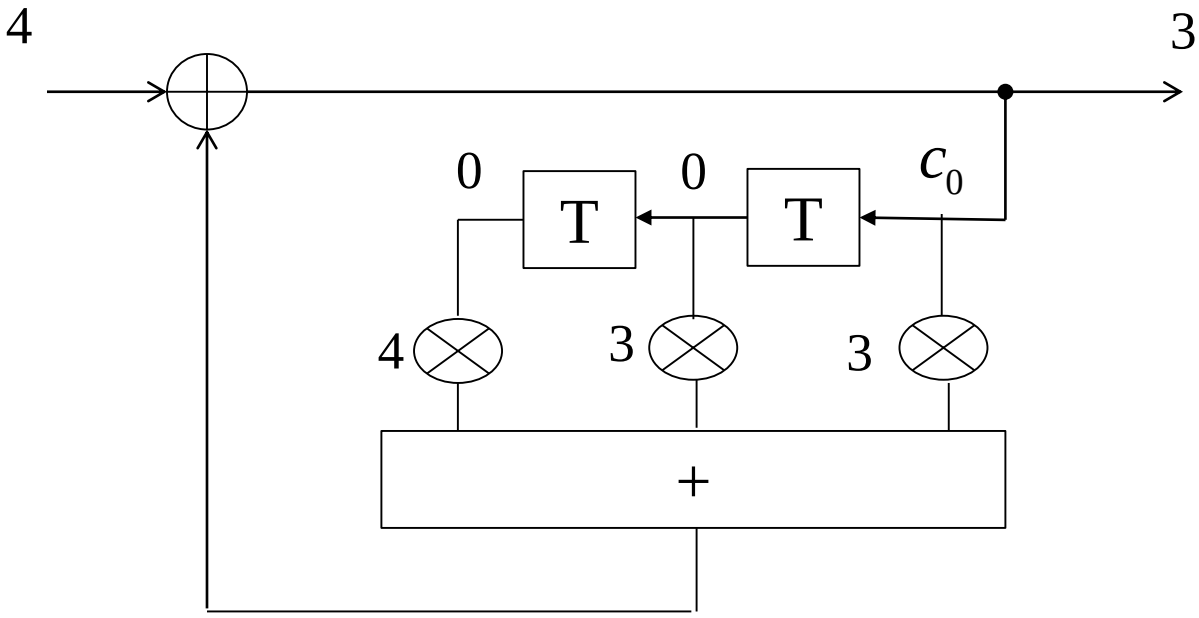
$$\left(x^2+3x+2\right)\left(x+4\right)=x^3+3x^2+2x+4x^2+2x+3=x^3+2x^2+4x+3$$



Division by Linear Feedback Shift Registers

$$\left(x^3+4x+4\right):\left(x^2+2x+3\right) = x+3 \text{ over } GF(5)$$

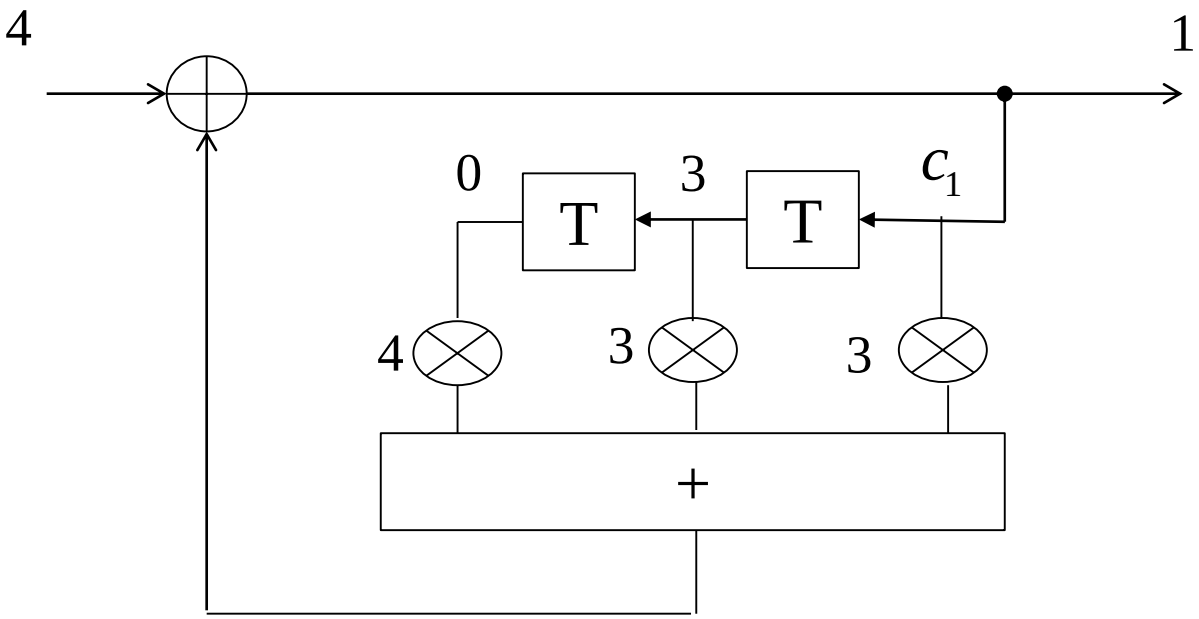
$$1-a_0 = 1-3 = -2 = 3;\ a_1 = -2 = 3;\ a_2 = -1 = 4$$



$$4+3c_0 = c_0 \rightarrow 2c_0 = -4 \rightarrow c_0 = \left(2\right)_m^{-1} 1 = 3*1 = 3$$

$$\left(x^3+4x+4\right):\left(x^2+2x+3\right) = x+3 \text{ over } GF(5)$$

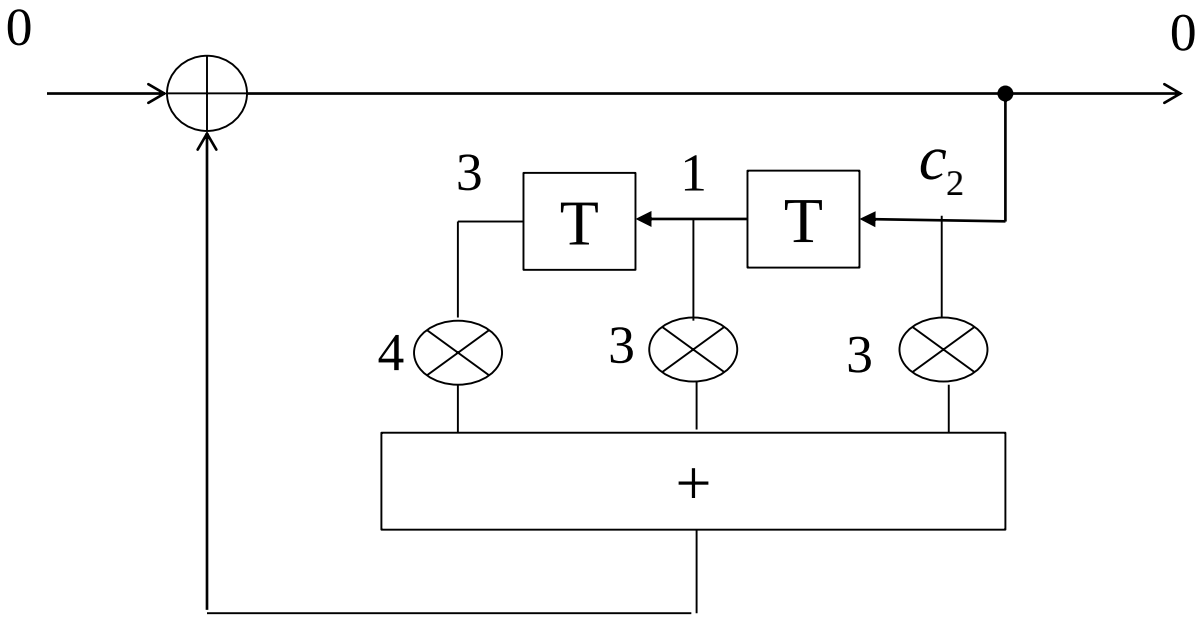
$$1-a_0 = 1-3 = -2 = 3;\ a_1 = -2 = 3;\ a_2 = -1 = 4$$



$$4+4+3c_1 = c_1 \rightarrow 2c_1 = -3 \rightarrow c_1 = \left(2\right)_m^{-1} 2 = 3*2 = 1$$

$$\left(x^3+4x+4\right):\left(x^2+2x+3\right) = x+3 \text{ over } GF(5)$$

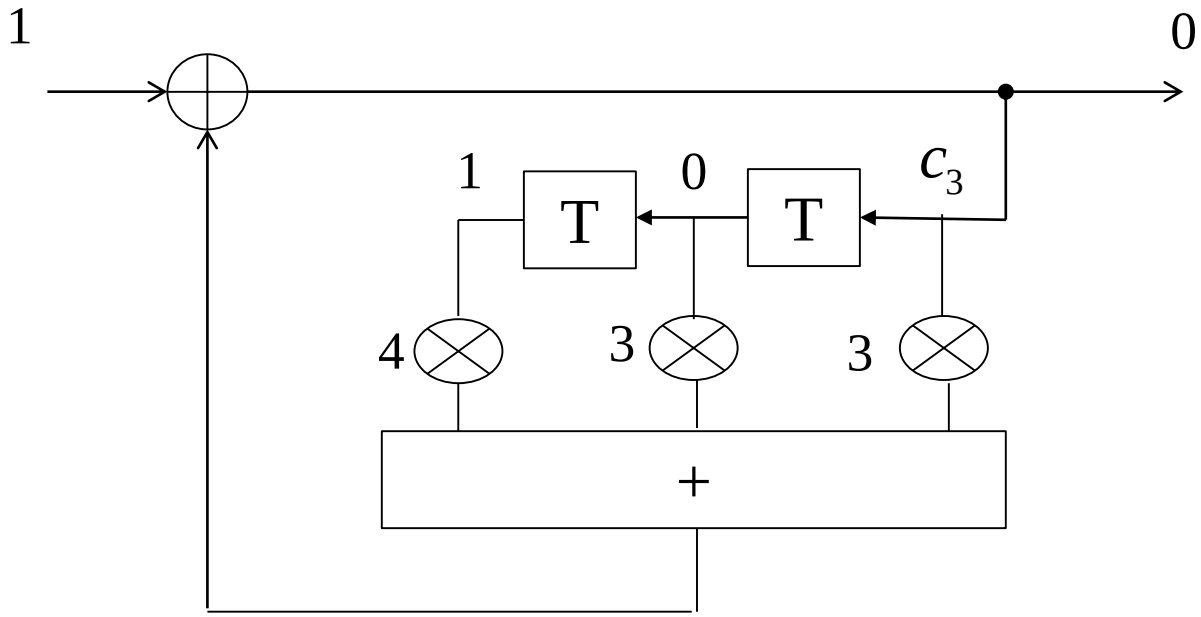
$$1-a_0 = 1-3 = -2 = 3;\ a_1 = -2 = 3;\ a_2 = -1 = 4$$



$$2+3+3c_2 = c_2 \rightarrow 2c_2 = 0 \rightarrow c_2 = \left(2\right)_m^{-1} 0 = 3*0 = 0$$

$$\left(x^3+4x+4\right):\left(x^2+2x+3\right) = x+3 \text{ over } GF(5)$$

$$1-a_0 = 1-3 = -2 = 3;\ a_1 = -2 = 3;\ a_2 = -1 = 4$$



$$4+1+3c_3 = c_3 \rightarrow 2c_3 = 0 \rightarrow c_3 = \left(2\right)_m^{-1} 0 = 3*0 = 0$$

Final result of division

$$\left(x^3+4x+4\right):\left(x^2+2x+3\right) = x+3 \text{ over } GF(5)$$

$$1-a_0 = 1-3 = -2 = 3;\ a_1 = -2 = 3;\ a_2 = -1 = 4$$