Exercise 2:

1. Calculate the value of the autocorrelation function.

   Example 1:
   A sequence of length 15, not produced by a LFSR of length 4 with a primitive feedback polynomial.
   S=100011011010011, T=15.
   Find $AC(0)$, $AC(2)$, $AC(5)$, $AC(14)$.

   Example 2:
   A sequence of length 15, produced by a LFSR of length 4 with a primitive feedback polynomial $f(x)=1+x+x^4$, with the initial state 0101.
   S=110010001111010, T=15.
   Find $AC(0)$, $AC(2)$, $AC(5)$, $AC(14)$.

2. Check the Golomb's postulates for S=110010001111010.
3. Check the singularity of the DeBruijn's diagram for the feedback function $f(x_1,x_2,x_3)=x_1 \oplus x_2x_3$.
4. Find the characteristic polynomial of the linear recurring sequence $a(t)=a(t-1) \oplus a(t-3) \oplus a(t-4)$.
5. Find (157,91).
6. Find $(x^8+x^6+x^3+x^2+1, x^5+x^3+1)$. Coefficients are from GF(2).
7. Find $(x^9+x^8+x^7+x^6+x+1, x^8+x^7+x^6+x^5+x^4+x^3+x+1)$. Coefficients are from GF(2).
8. Check $f(x)=x^6+x^3+x+1$ for irreducibility in GF(2).
9. Check $f(x)=x^6+x^5+1$ for irreducibility in GF(2).
10. Check whether $f(x)=x^4+x^3+1$ is primitive in GF(2).
11. Check whether $f(x)=x^4+x^3+x^2+x+1$ is primitive in GF(2).
12. Find the reciprocal polynomial of $f(x)=x^6+x^5+1$. Is it irreducible?
13. Find the reciprocal polynomial of $f(x)=x^4+x^3+1$. Is it primitive?
14. Determine all the cycles of the LFSR with the feedback polynomial $f(x)= x^4+x^3+x^2+x+1$.
15. Determine all the cycles of the LFSR with the feedback polynomial $f(x)=x^5+x^4+1$.
16. Generate the whole state period of the LFSR with the feedback polynomial $f(x)=x^5+x^4+x^3+x^2+1$. The initial state is 01101.
17. How many primitive polynomials of degree 4 are there?
18. The output sequence of the LFSR with the characteristic polynomial $f(x)=x^5+x^4+x^3+x^2+1$ is 11110... Find the initial state of the LFSR.
19. Find the linear complexity and the characteristic polynomial of the minimum LFSR that generates the sequence S=001101110 in GF(2).

Solutions :

1. Exemple 1 : $S = 1000110110100 11$ $T = 15$

$k = 0$

1000110110100 11
1000110110100 11

$A = 15$, $D = 0$

$\Rightarrow AC(0) = \frac{A - D}{T} = \frac{15 - 0}{15} = 1$

$k = 2$

1 0 0 0 1 1 0 1 1 0 1 0 0 1 1
0 0 1 1 0 1 1 0 1 0 0 1 1 1 0
• • •• •

$A = 5, \; D = 10$

$\Rightarrow AC(2) = \frac{A - D}{T} = \frac{5 - 10}{15} = -\frac{1}{3}$

$k = 5$

1 0 0 0 1 1 0 1 1 0 1 0 0 1 1
1 0 1 1 0 1 0 0 1 1 1 0 0 0 1
•• •• • ••• •

$A = 9, \; D = 6$

$\Rightarrow AC(5) = \frac{A - D}{T} = \frac{9 - 6}{15} = \frac{1}{5}$

$k = 14$

1 0 0 0 1 1 0 1 1 0 1 0 0 1 1
1 1 0 0 0 1 1 0 1 1 0 1 0 0 1
• •• • • • •

$A = 7, \; D = 8$

$\Rightarrow AC(14) = \frac{A - D}{T} = \frac{7 - 8}{15} = -\frac{1}{15}$

Example 2.: $S = 1100100011111010$

$k = 0$

1 1 0 0 1 0 0 0 1 1 1 1 0 1 0
1 1 0 0 1 0 0 0 1 1 1 1 0 1 0

$A = 15, \; D = 0$

$\Rightarrow AC(0) = \frac{A - D}{T} = \frac{15 - 0}{15} = 1$

$k = 2$

1 1 0 0 1 0 0 0 1 1 1 1 0 1 0
0 0 1 0 0 0 1 1 1 1 0 1 0 1 1
• • •• ••• •

$A = 7, \; D = 8$

$\Rightarrow AC(2) = \frac{A - D}{T} = \frac{7 - 8}{15} = -\frac{1}{15}$

$k = 5$

1100100011111010
0001111010111001
 • • •• •••

$A = 7, D = 8$

$\Rightarrow AC(5) = \frac{A - D}{T} = \frac{7-8}{15} = -\frac{1}{15}$

$k = 14$

1100100011111010
0111001000111101
 • • •• •••

$A = 7, D = 8$

$\Rightarrow AC(14) = \frac{A - D}{T} = \frac{7-8}{15} = -\frac{1}{15}$

2. G_1 $\quad S = 1100100011111010$

The number of 1s = 8

The number of 0s = 7

$\Rightarrow G_1$ is satisfied.

G_2

...10 | 1100100011111010 | 11... repeated sequence S

The runs:

0 11 0
1 00 1
0 1 0
1 000 1
0 1111 0
1 0 1
0 1 0
1 0 1

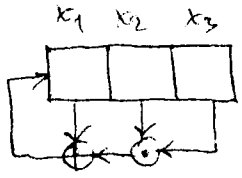
8 runs in total, of which
4 runs of length 1
2 runs of length 2
1 run of length 3
1 run of length 4

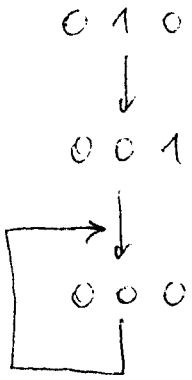
$\Rightarrow G_2$ is satisfied.

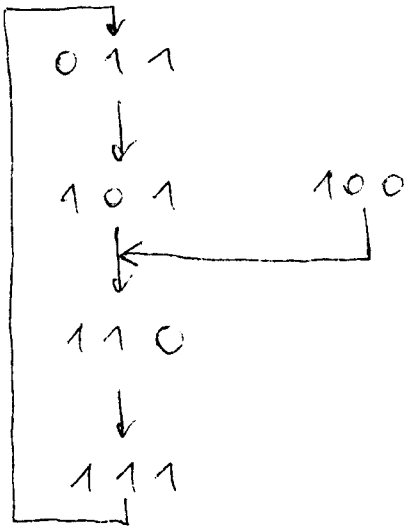
G_3

See task 4, Example 2. G_3 is satisfied.

3. $f(x_1, x_2, x_3) = x_1 \oplus x_2 x_3$







The register is singular!

4. $a(t) = a(t-1) \oplus a(t-3) \oplus a(t-4)$

$f(x) = 1 + x + x^3 + x^4$

$(157, 91) = 1$

5.

$157 : 91 = 1$ / 66

$91 : 66 = 1$ / 25

$66 : 25 = 2$ / 16

$25 : 16 = 1$ / 9

$16 : 9 = 1$ / 7

$9 : 7 = 1$ / 2

$7 : 2 = 3$ / 1

$2 : 1 = 2$ / 0

6. $(x^8 + x^6 + x^3 + x^2 + 1,\ x^5 + x^3 + 1) = 1$

$(x^8 + x^6 + x^3 + x^2 + 1) : (x^5 + x^3 + 1) = x^3$

$x^8 + x^6 + x^3$

$x^2 + 1$

$(x^5 + x^3 + 1) : (x^2 + 1) = x^3$

$x^5 + x^3$

1 //

$(x^2 + 1) : 1 = x^2 + 1$

0

7. $\left(x^9+x^8+x^7+x^6+x+1,\ x^8+x^7+x^6+x^5+x^4+x^2+x+1\right) = x+1$

$(x^9+x^8+x^7+x^6+x+1) : (x^8+x^7+x^6+x^5+x^4+x^3+x+1) = x$

$x^9+x^8+x^7+x^6+x^5+x^4+x^2+x$

$x^5+x^4+x^2+1$

$(x^8+x^7+x^6+x^5+x^4+x^3+x+1) : (x^5+x^4+x^2+1) = x^3+x+1$

$x^8+x^7+x^5+x^3$

x^6+x^4+x+1

$x^6+x^5+x^3+x$

$x^5+x^4+x^3+1$

$x^5+x^4+x^2+1$

x^3+x^2

$(x^5+x^4+x^2+1) : (x^3+x^2) = x^2$

x^5+x^4

x^2+1

$(x^3+x^2) : (x^2+1) = x+1$

x^3+x

x^2+x

x^2+1

$x+1$

$(x^2+1) : (x+1) = x+1$

x^2+x

$x+1$

$x+1$

0

8. $f(x) = x^6 + x^3 + x + 1$, $GF(2)$

$n = 6 \Rightarrow k = 1, 2, 3$

$k = 1$

$(x^{2^k} + x) \bmod f(x) = (x^2 + x) \bmod (x^6 + x^3 + x + 1) = x^2 + x$

$(x^2 + x, x^6 + x^3 + x + 1) = x + 1 \neq 1 \Rightarrow$ not irreducible

$(x^6 + x^3 + x + 1) : (x^2 + x) = x^4 + x^3 + x^2$

$x^6 + x^5$

$x^5 + x^3 + x + 1$

$x^5 + x^4$

$x^4 + x^3 + x + 1$

$x^4 + x^3$

$x + 1$

$(x^2 + x) : (x + 1) = x$

$x^2 + x$

0

9. $f(x) = x^6 + x^5 + 1$, $GF(2)$

$n = 6 \Rightarrow k = 1, 2, 3$

$k = 1$

$(x^{2^k} + x) \bmod f(x) = (x^2 + x) \bmod (x^6 + x^5 + 1) = x^2 + x$

$(x^2 + x, x^6 + x^5 + 1) = 1$

$(x^6 + x^5 + 1) : (x^2 + x) = x^4$

$x^6 + x^5$

1

$(x^2 + x) : 1 = x^2 + x$

0

$k = 2$

$$(x^{2^k} + x) \bmod f(x) = (x^4 + x) \bmod (x^6 + x^5 + 1) = x^4 + x$$

$$(x^4 + x,\ x^6 + x^5 + 1) = 1$$

$$(x^6 + x^5 + 1) : (x^4 + x) = x^2 + x$$

$x^6 + x^3$

$x^5 + x^3 + 1$

$x^5 + x^2$

$x^3 + x^2 + 1$

$$(x^4 + x) : (x^3 + x^2 + 1) = x + 1$$

$x^4 + x^3 + x$

x^3

$x^3 + x^2 + 1$

$x^2 + 1$

$$(x^3 + x^2 + 1) : (x^2 + 1) = x + 1$$

$x^3 + x$

$x^2 + x + 1$

$x^2 + 1$

x

$$(x^2 + 1) : x = x$$

x^2 etc.

1

$x : 1 = x$

0

$k = 3$

$(x^{2^3} + x) \bmod f(x) = (x^8 + x) \bmod (x^6 + x^5 + 1) = x^5 + x^2 + 1$

$(x^8 + x) : (x^6 + x^5 + 1) = x^2 + x + 1$

$x^8 + x^7 + x^2$

$x^7 + x^2 + x$

$x^7 + x^6 + x$

$x^6 + x^2$

$x^6 + x^5 + 1$

$x^5 + x^2 + 1$

$(x^5 + x^2 + 1, x^6 + x^5 + 1) = 1 \Rightarrow$ irreducible

$(x^6 + x^5 + 1) : (x^5 + x^2 + 1) = x + 1$

$x^6 + x^3 + x$

$x^6 + x^3 + x + 1$

$x^5 + x^2 + 1$

$x^3 + x^2 + x$

$(x^5 + x^2 + 1) : (x^3 + x^2 + x) = x^2 + x$

$x^5 + x^4 + x^3$

$x^4 + x^3 + x^2 + 1$

$x^4 + x^3 + x^2$

1

$(x^3 + x^2 + x) : 1 = x^3 + x^2 + x$

0

10. $f(x) = x^4 + x^3 + 1$

first, we check whether $f(x)$ is irreducible

$n = 4 \Rightarrow k = 1, 2$

$k = 1$

$$\left(x^{2^1} + x\right) \bmod \left(x^4 + x^3 + 1\right) = x^2 + x$$

$$\left(x^2 + x,\ x^4 + x^3 + 1\right) = 1$$

$$\left(x^4 + x^3 + 1\right) : \left(x^2 + x\right) = x^2$$

$$\underline{x^4 + x^3}$$

$$1$$

$$\left(x^2 + x\right) : 1 = x^2 + x$$

$$\underline{\quad}$$

$$0$$

$k = 2$

$$\left(x^{2^2} + x\right) \bmod \left(x^4 + x^3 + 1\right) = \left(x^4 + x\right) \bmod \left(x^4 + x^3 + 1\right) = x^3 + x + 1$$

$$\left(x^4 + x\right) : \left(x^4 + x^3 + 1\right) = 1$$

$$\underline{x^4 + x^3 + 1}$$

$$x^3 + x + 1$$

$$\left(x^3 + x + 1,\ x^4 + x^3 + 1\right) = 1 \Rightarrow \text{irreducible!}$$

$$\left(x^4 + x^3 + 1\right) \cdot \left(x^3 + x + 1\right) = x + 1$$

$$\underline{x^4 + x^2 + x}$$

$$x^3 + x^2 + x + 1$$

$$\underline{x^3 + x + 1}$$

$$x^2$$

$$\left(x^3 + x + 1\right) : x^2 = x$$

$$\underline{x^3}$$

$$x + 1$$

$$x^2 \cdot (x + 1) = x + 1$$

$$\underline{x^2 + x}$$

$$x$$

$$\underline{x + 1}$$

$$1$$

$$\left(x + 1\right) : 1 = x + 1$$

$$\underline{\quad}$$

$$0$$

now we check whether it is primitive

$x^k + 1, \quad k = 1, \dots, 2^4 - 1 - 1$

$k = 1, \dots, 14$

$k = 1 \quad \underbrace{(x+1)}_{x+1} : (x^4 + x^3 + 1) = 0$

$k = 2 \quad \underbrace{(x^2+1)}_{x^2+1} : (x^4 + x^3 + 1) = 0$

$k = 3 \quad \underbrace{(x^3+1)}_{x^3+1} \cdot (x^4 + x^3 + 1) = 0$

$k = 4$

$(x^4 + 1) : (x^4 + x^3 + 1) = 1$

$x^4 + x^3 + 1$

x^3

$k = 5 \quad (x^5 + 1) : (x^4 + x^3 + 1) = x + 1$

$x^5 + x^4 + x$

$x^4 + x + 1$

$x^4 + x^3 + 1$

$x^3 + x$

$k = 6 \quad (x^6 + 1) : (x^4 + x^3 + 1) = x^2 + x + 1$

$x^6 + x^5 + x^2$

$x^5 + x^2 + 1$

$x^5 + x^4 + x$

$x^4 + x^2 + x + 1$

$x^4 + x^3 + 1$

$x^3 + x^2 + x$

$k = 7 \quad (x^7 + 1) : (x^4 + x^3 + 1) = x^3 + x^2 + x + 1$

$x^7 + x^6 + x^3$

$x^6 + x^3 + 1$

$x^6 + x^5 + x^2$

$x^5 + x^3 + x^2 + 1$

$x^5 + x^4 + x$

$x^4 + x^3 + x^2 + x + 1$

$x^4 + x^3 + 1$

$x^2 + x$

$k = 8$

$$(x^8+1) : (x^4+x^3+1) = x^4+x^3+x^2+x$$

$x^8+x^7+x^4$

x^7+x^4+1

$x^7+x^6+x^3$

$x^6+x^4+x^3+1$

$x^6+x^5+x^2$

$x^5+x^4+x^3+x^2+1$

x^5+x^4+x

x^3+x^2+x+1

$k = 9$

$$(x^9+1) : (x^4+x^3+1) = x^5+x^4+x^3+x^2+1$$

$x^9+x^8+x^5$

x^8+x^5+1

$x^8+x^7+x^4$

$x^7+x^5+x^4+1$

$x^7+x^6+x^3$

$x^6+x^5+x^4+x^3+1$

$x^6+x^5+x^2$

$x^4+x^3+x^2+1$

x^4+x^3+1

x^2

$k = 10$

$$(x^{10}+1) : (x^4+x^3+1) = x^6+x^5+x^4+x^3+x$$

$x^{10}+x^9+x^6$

x^9+x^6+1

$x^9+x^8+x^5$

$x^8+x^6+x^5+1$

$x^8+x^7+x^4$

$x^7+x^6+x^5+x^4+1$

$x^7+x^6+x^3$

$x^5+x^4+x^3+1$

x^5+x^4+x

x^3+x+1

$k = 11$

$(x^{11} + 1) : (x^4 + x^3 + 1) = x^7 + x^6 + x^5 + x^4 + x^2 + 1$

$x^{11} + x^{10} + x^7$

$x^{10} + x^7 + 1$

$x^{10} + x^9 + x^6$

$x^9 + x^7 + x^6 + 1$

$x^9 + x^8 + x^5$

$x^8 + x^7 + x^6 + x^5 + 1$

$x^8 + x^7 + x^4$

$x^6 + x^5 + x^4 + 1$

$x^6 + x^5 + x^2$

$x^4 + x^2 + 1$

$x^4 + x^3 + 1$

$x^3 + x^2$

$k = 12$

$(x^{12} + 1) : (x^4 + x^3 + 1) = x^8 + x^7 + x^6 + x^5 + x^3 + x + 1$

$x^{12} + x^{11} + x^8$

$x^{11} + x^8 + 1$

$x^{11} + x^{10} + x^7$

$x^{10} + x^8 + x^7 + 1$

$x^{10} + x^9 + x^6$

$x^9 + x^8 + x^7 + x^6 + 1$

$x^9 + x^8 + x^5$

$x^7 + x^6 + x^5 + 1$

$x^7 + x^6 + x^3$

$x^5 + x^3 + 1$

$x^5 + x^4 + x$

$x^4 + x^3 + x + 1$

$x^4 + x^3 + 1$

x

$k = 13$

$(x^{13}+1) : (x^4+x^3+1) = x^9+x^8+x^7+x^6+x^4+x^2+x$

$x^{13}+x^{12}+x^9$

$x^{12}+x^9+1$

$x^{12}+x^{11}+x^8$

$x^{11}+x^9+x^8+1$

$x^{11}+x^{10}+x^7$

$x^{10}+x^9+x^8+x^7+1$

$x^{10}+x^9+x^6$

$x^8+x^7+x^6+1$

$x^8+x^7+x^4$

x^6+x^4+1

$x^6+x^5+x^2$

$x^5+x^4+x^2+1$

x^5+x^4+x

x^2+x+1

$k = 14$

$(x^{14}+1) : (x^4+x^3+1) = x^{10}+x^9+x^8+x^7+x^5+x^3+x^2$

$x^{14}+x^{13}+x^{10}$

$x^{13}+x^{10}+1$

$x^{13}+x^{12}+x^9$

$x^{12}+x^{10}+x^9+1$

$x^{12}+x^{11}+x^8$

$x^{11}+x^{10}+x^9+x^8+1$

$x^{11}+x^{10}+x^7$

$x^9+x^8+x^7+1$

$x^9+x^8+x^5$

x^7+x^5+1

$x^7+x^6+x^3$

$x^6+x^5+x^3+1$

$x^6+x^5+x^2$

x^3+x^2+1

$\Rightarrow$ primitive!

11. $f(x) = x^4 + x^3 + x^2 + x + 1$

$n = 4 \Rightarrow k = 1, 2$

$k = 1$

$(x^{2^1} + x) \bmod (x^4 + x^3 + x^2 + x + 1) = x^2 + x$

$(x^2 + x,\ x^4 + x^3 + x^2 + x + 1) = 1$

$(x^4 + x^3 + x^2 + x + 1) : (x^2 + x) = x^2 + 1$

$\underline{x^4 + x^3}$

$x^2 + x + 1$

$\underline{x^2 + x}$

$1 =$

$(x^2 + x) : 1 = x^2 + x$

$\underline{\ \ 0}$

$k = 2$

$(x^{2^2} + x) \bmod (x^4 + x^3 + x^2 + x + 1) = (x^4 + x) \bmod (x^4 + x^3 + x^2 + x + 1) =$

$= x^3 + x^2 + 1$

$(x^4 + x) : (x^4 + x^3 + x^2 + x + 1) = 1$

$\underline{x^4 + x^3 + x^2 + x + 1}$

$x^3 + x^2 + 1$

$(x^3 + x^2 + 1,\ x^4 + x^3 + x^2 + x + 1) = 1 \Rightarrow$ ireducibile

$(x^4 + x^3 + x^2 + x + 1) : (x^3 + x^2 + 1) = x$

$\underline{x^4 + x^3 + x}$

$x^2 + 1$

$(x^3 + x^2 + 1) : (x^2 + 1) = x + 1$

$\underline{x^3 + x}$

$x^2 + x + 1$

$\underline{x^2 + 1}$

x

$(x^2 + 1) : x = x$

$\underline{x^2}$

$1 =$

$x : 1 = x$

$\underline{\ \ 0}$

$k = 1, \dots, 14$

$k=1 \quad (x+1) : (x^4+x^3+x^2+x+1) = 0$

$x+1$

$k=2 \quad (x^2+1) : (x^4+x^3+x^2+x+1) = 0$

x^2+1

$k=3 \quad (x^3+1) : (x^4+x^3+x^2+x+1) = 0$

x^3+1

$k=4 \quad (x^4+1) : (x^4+x^3+x^2+x+1) = 1$

$x^4+x^3+x^2+x+1$

x^3+x^2+x

$k=5 \quad (x^5+1) : (x^4+x^3+x^2+x+1) = x+1$

$x^5+x^4+x^3+x^2+x$

$x^4+x^3+x^2+x+1$

$x^4+x^3+x^2+x+1$

$0 \quad \Rightarrow$ not primitive!

12. $f(x) = x^6+x^5+1$

$f^*(x) = x^6\left(\frac{1}{x^6}+\frac{1}{x^5}+1\right) = 1+x+x^6$

$n=6 \Rightarrow k = 1,2,3$

$k=1$

$(x^{2^1}+x) \bmod (x^6+x+1) = x^2+x$

$(x^2+x, x^6+x+1) = 1$

$(x^6+x+1) : (x^2+x) = x^4+x^3+x^2+x+1 \qquad (x^2+x) : 1 = x^2+x$

x^6+x^5

x^5+x+1

x^5+x^4

x^4+x+1

x^4+x^3

x^3+x+1

x^3+x^2

x^2+x+1

x^2+x

1 //

0

$k = 2$

$(x^{2^2} + x) \bmod (x^6 + x + 1) = x^4 + x$

$(x^4 + x,\ x^6 + x + 1) = 1$

$(x^6 + x + 1) : (x^4 + x) = x^2$

$x^6 + x^3$

$x^3 + x + 1$

$(x^4 + x) : (x^3 + x + 1) = x$

$x^4 + x^2 + x$

x^2

$(x^3 + x + 1) : x^2 = x$

x^3

$x + 1$

$x^2 : (x + 1) = x + 1$

$x^2 + x$

x

$x + 1$

1

$=$

$(x+1) : 1 = x + 1$

0

$k = 3$

$(x^{2^3} + x) \bmod (x^6 + x + 1) = (x^8 + x) \bmod (x^6 + x + 1) = x^3 + x^2 + x$

$(x^8 + x) : (x^6 + x + 1) = x^2$

$x^8 + x^3 + x^2$

$x^3 + x^2 + x$

$(x^3 + x^2 + x,\ x^6 + x + 1) = 1 \Rightarrow$ irreducible

$(x^6 + x + 1) : (x^3 + x^2 + x) = x^3 + x^2 + 1$

$x^6 + x^5 + x^4$

$x^5 + x^4 + x + 1$

$x^5 + x^4 + x^3$

$x^3 + x + 1$

$x^3 + x^2 + x$

$x^2 + 1$

16a

$(x^3 + x^2 + x) : (x^2 + 1) = x + 1$

$x^3 + x$

x^2

$x^2 + 1$

1

$(x^2 + 1) : 1 = x^2 + 1$

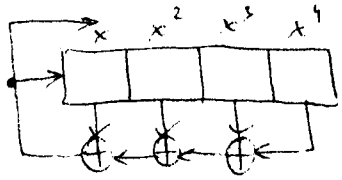
0

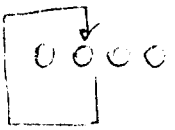
13. $f(x) = x^4 + x^3 + 1$ primitive, see the task number 13.

$$f^*(x) = x^4\left(\frac{1}{x^4} + \frac{1}{x^3} + 1\right) = 1 + x + x^4$$

$f^*(x)$ is primitive (recall the theorem from the lecture).

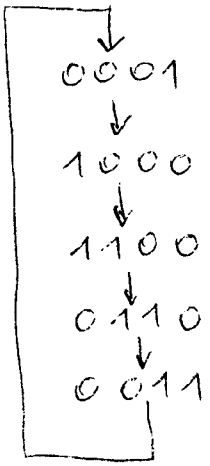
14. $f(x) = x^4 + x^3 + x^2 + x + 1$





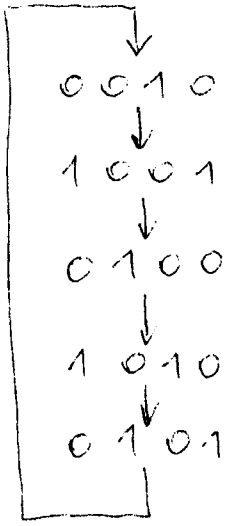
↓	↓	↓	↓
0	0	0	1
1	0	0	0
1	1	0	0
0	1	1	0
0	0	1	1
0	0	0	1

=>



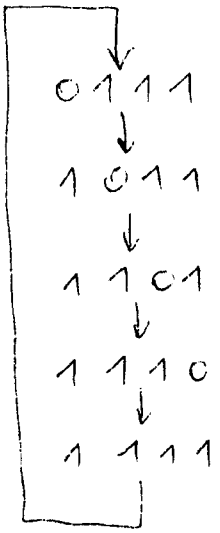
↓	↓	↓	↓
0	0	1	0
1	0	0	1
0	1	0	0
1	0	1	0
0	1	0	1
0	0	1	0

=>



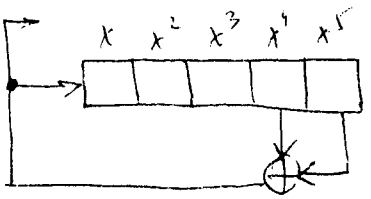
↓	↓	↓	↓
0	1	1	1
1	0	1	1
1	1	0	1
1	1	1	0
1	1	1	1
0	1	1	1

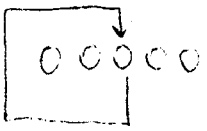
=>



Since $f(x)$ is irreducible, we have cycles (except the 0000) of length 5 that divides $2^4 - 1$.

15. $f(x) = x^5 + x^4 + 1$ → not irreducible (check!)





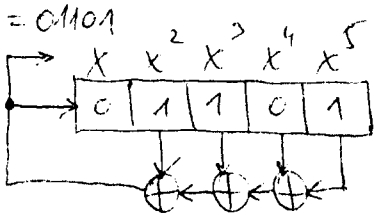
↓ ↓
0 0 0 0 1
1 0 0 0 0
0 1 0 0 0
0 0 1 0 0
0 0 0 1 0
1 0 0 0 1
1 1 0 0 0
0 1 1 0 0
0 0 1 1 0
1 0 0 1 1
0 1 0 0 1
1 0 1 0 0
0 1 0 1 0
1 0 1 0 1
1 1 0 1 0
1 1 1 0 1
1 1 1 1 0
1 1 1 1 1
0 1 1 1 1
0 0 1 1 1
0 0 0 1 1
0 0 0 0 1

↓ ↓
0 0 1 0 1
1 0 0 1 0
1 1 0 0 1
1 1 1 0 0
0 1 1 1 0
1 0 1 1 1
0 1 0 1 1
0 0 1 0 1

↓ ↓
0 1 1 0 1
1 0 1 1 0
1 1 0 1 1
0 1 1 0 1

16. $f(x) = x^5 + x^4 + x^3 + x^2 + 1$ → primitive! (check!)

$S = 01101$




```
  ↓ ↓ ↓
  0 1 1 0 1
  ---------
  1 0 1 1 0
  0 1 0 1 1
  1 0 1 0 1
  0 1 0 1 0
  0 0 1 0 1
  0 0 0 1 0
  1 0 0 0 1
  1 1 0 0 0
  1 1 1 0 0
  0 1 1 1 0
  1 0 1 1 1
  1 1 0 1 1
  1 1 1 0 1
  1 1 1 1 0
  1 1 1 1 1
  0 1 1 1 1
  0 0 1 1 1
  1 0 0 1 1
  0 1 0 0 1
  0 0 1 0 0
  1 0 0 1 0
  1 1 0 0 1
  0 1 1 0 0
  0 0 1 1 0
  0 0 0 1 1
  0 0 0 0 1
  1 0 0 0 0
  0 1 0 0 0
  1 0 1 0 0
  1 1 0 1 0
  0 1 1 0 1
```

17. $n = 4$

$$N = \phi(2^n - 1)/n = \phi(2^4 - 1)/4$$

$\phi(15) = 8$

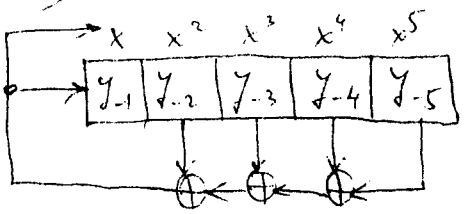
1, 2, 4, 7, 8, 11, 13, 14 → the numbers less than 15, mutually prime with 15.

$\Rightarrow N = 8/4 = 2$

There are only 2 primitive polynomials of degree 4.

18. $f(x) = x^5 + x^4 + x^3 + x^2 + 1$

$S = 1111c\ldots$



S

$1 = y_0$

$1 = y_1$

$1 = y_2$

$1 = y_3$

$0 = y_4$

The equations:

$$y_0 = y_{-2} + y_{-3} + y_{-4} + y_{-5}$$

$$y_1 = y_{-1} + y_{-2} + y_{-3} + y_{-4}$$

$$y_2 = y_0 + y_{-1} + y_{-2} + y_{-3}$$

$$y_3 = y_1 + y_0 + y_{-1} + y_{-2}$$

$$y_4 = y_2 + y_1 + y_0 + y_{-1}$$

$$1 = y_{-2} + y_{-3} + y_{-4} + y_{-5}$$

$$1 = y_{-1} + y_{-2} + y_{-3} + y_{-4}$$

$$1 = 1 + y_{-1} + y_{-2} + y_{-3}$$

$$1 = 1 + 1 + y_{-1} + y_{-2}$$

$$0 = 1 + 1 + 1 + y_{-1}$$

$\Rightarrow y_{-1} = 1;\ y_{-2} = 0;\ y_{-3} = 1;\ y_{-4} = 1;\ y_{-5} = 1.$

19. $S = \overset{s_0\, s_1\, s_2\, s_3\, s_4\, s_5\, s_6\, s_7\, s_8}{0\,0\,1\,1\,0\,1\,1\,1\,0}$, $GF(2)$

$C(D) = 1$, $C^*(D) = 1$

$L = 0$, $\delta^* = 1$

$x = 1$, $m = 0$

$s_0 = 0$

$\delta = s_0 = 0$

$\Rightarrow x \leftarrow x+1 = 2$

$m \leftarrow m+1 = 1$

$s_1 = 0$

$\delta = s_1 = 0$

$\Rightarrow x \leftarrow x+1 = 3$

$m \leftarrow m+1 = 2$

$s_2 = 1$

$\delta = s_2 = 1$

$\Rightarrow T(D) = C(D) = 1$

$C(D) \leftarrow C(D) + D^3 C^*(D) = 1 + D^3$ ($c_0 = 1$, $c_3 = 1$)

$2L \overset{?}{\leq} m$ yes $\Rightarrow L \leftarrow m+1-L = 3$

$x = 1$

$C^*(D) = T(D) = 1$

$\delta^* = \delta = 1$

$m \leftarrow m+1 = 3$

$s_3 = 1$

$\delta = s_3 + c_1 s_2 + c_2 s_1 + c_3 s_0 = 1 + 0 \cdot 1 + 0 \cdot 0 + 1 \cdot 0 = 1$

$\Rightarrow T(D) = C(D) = 1 + D^3$

$C(D) \leftarrow C(D) + D^1 C^*(D) = 1 + D + D^3$ ($c_0 = 1$, $c_1 = 1$, $c_3 = 1$)

$2L \overset{?}{\leq} m$ no $\Rightarrow x \leftarrow x+1 = 2$

$m \leftarrow m+1 = 4$

$s_4 = 0$

$\delta = s_4 + c_1 s_3 + c_2 s_2 + c_3 s_1 = 0 + 1\cdot 1 + 0\cdot 1 + 1\cdot 0 = 1$

$\Rightarrow \quad T(D) = C(D) = 1 + D + D^3$

$C(D) \leftarrow C(D) + D^2 C^*(D) = 1 + D + D^2 + D^3$
$\quad c_0=1\ c_1=1\ c_2=1\ c_3=1$

$2L \overset{?}{\leq} n \quad$ no $\Rightarrow X \leftarrow X+1 = 3$

$n \leftarrow n+1 = 5$

$s_5 = 1$

$\delta = s_5 + c_1 s_4 + c_2 s_3 + c_3 s_2 = 1 + 1\cdot 0 + 1\cdot 1 + 1\cdot 1 = 1$

$\delta = 1 \Rightarrow T(D) = C(D) = 1 + D + D^2 + D^3$

$C(D) \leftarrow C(D) + D^3 C^*(D) = 1 + D + D^2$
$\quad c_0=1\ c_1=1\ c_2=1\ c_3=0$

$2L \overset{?}{\leq} n \quad$ no $\Rightarrow X \leftarrow X+1 = 4$

$n \leftarrow n+1 = 6$

$s_6 = 1$

$\delta = s_6 + c_1 s_5 + c_2 s_4 + c_3 s_3 = 1 + 1\cdot 1 + 1\cdot 0 + 0\cdot 1 = 0$

$\Rightarrow \quad X \leftarrow X+1 = 5$

$n \leftarrow n+1 = 7$

$s_7 = 1$

$\delta = s_7 + c_1 s_6 + c_2 s_5 + c_3 s_4 = 1 + 1\cdot 1 + 1\cdot 1 + 0\cdot 0 = 1$

$\Rightarrow \quad T(D) = C(D) = 1 + D + D^2$

$C(D) \leftarrow C(D) + D^5 C^*(D) = 1 + D + D^2 + D^5$
$\quad c_0=1\ c_1=1\ c_2=1\ c_5=1$

$2L \overset{?}{\leq} n \quad$ yes $\Rightarrow L \leftarrow n+1-L = 5$

$X \leftarrow 1$

$C^*(D) = T(D) = 1 + D + D^2$

$\delta^* = \delta - 1$

$n \leftarrow n+1 = 8$

$s_8 = 0$

$\delta = s_8 + c_1 s_7 + c_2 s_6 + c_3 s_5 + c_4 s_4 + c_5 s_3 = 0 + 1\cdot 1 + 1\cdot 1 + 0\cdot 1 + 0\cdot 0 + 1\cdot 1 = 1$

$\Rightarrow T(D) = C(D) = 1 + D + D^2 + D^5$

$C(D) \leftarrow C(D) + D^1 C^*(D) = 1 + D + D^2 + D^5 + D(1 + D + D^2) = 1 + \cancel{D} + \cancel{D^2} + D^5 + \cancel{D} + \cancel{D^2} + D^3 =$

$= 1 + D^3 + D^5$

$2L \leq n$ no $\Rightarrow$ $X \leftarrow X+1 = 2$

end.

$\Rightarrow \langle L, f(x) \rangle = \langle 5, 1+D^3+D^5 \rangle$