Le corps fini à 16 éléments

On va prendre comme polynôme minimal

$$P(X) = X^4 + X^3 + 1.$$

Ce polynôme est **primitif**. On note α la clase de X, qui est donc racine de $P(X)$ dans $\mathbb{F}_{16}$ et qui est un élément primitif.

	1	X	X^2	X^3
α^0	1	0	0	0
α^1	0	1	0	0
α^2	0	0	1	0
α^3	0	0	0	1
α^4	1	0	0	1
α^5	1	1	0	1
α^6	1	1	1	1
α^7	1	1	1	0
α^8	0	1	1	1
α^9	1	0	1	0
α^{10}	0	1	0	1
α^{11}	1	0	1	1
α^{12}	1	1	0	0
α^{13}	0	1	1	0
α^{14}	0	0	1	1

Figure 1 : table des puissances

Dans le corps $\mathbb{F}_{16}$ on sait qu'il y a

$$\phi(15) = \phi(3)\phi(5) = 2 \times 4 = 8$$

éléments primitifs, qui sont racines de polynômes de ddegré 4. Il y a donc 2 polynômes primitifs.

D'après la formule connue il y a 3 polynômes irréductibles de degré 4 sur $\mathbb{F}_2$.

Les ordres des éléments sont 1 (1 élément), 3 (2 éléments), 5 (4 éléments), 15 (8 éléments).

Ordre	éléments
1	1
3	α^5, α^{10}
5	$\alpha^3, \alpha^6,$ α^9, α^{12}
15	$\alpha, \alpha^2,$ $\alpha^4, \alpha^7,$ α^8, α^{11} α^{13}, α^{14}

Polynôme minimal de 1 : $X + 1$
Polynôme minimal de α^5, α^{10} : $X^2 + X + 1$
Polynôme minimal de $\alpha^3, \alpha^6, \alpha^{12}, \alpha^9$: $X^4 + X^3 + X^2 + X + 1$
Polynôme minimal de $\alpha, \alpha^2, \alpha^4, \alpha^8$: $X^4 + X^3 + 1$
Polynôme minimal de $\alpha^7, \alpha^{14}, \alpha^{13}, \alpha^{11}$: $X^4 + X + 1$

Ainsi

$$X^{16} - X =$$

$$X(X+1)(X^2+X+1)(X^4+X^3+X^2+X+1)(X^4+X^3+1)(X^4+X+1).$$