

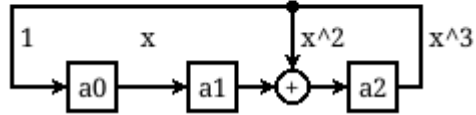
**Пример схемы генератора поля Галуа GF(2<sup>3</sup>)**

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

*Генератор элементов*

*поля Галуа GF(2<sup>3</sup>)*

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



Полиномиальное представление элементов поля:

$$a_0 + a_1x + a_2x^2$$

Векторное представление элементов поля:

$$[a_0 \ a_1 \ a_2]$$

Построение поля Галуа по схеме генератора поля:

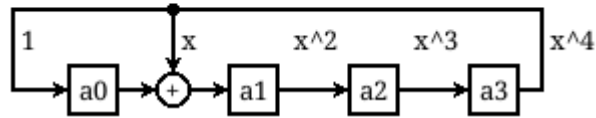
Начальное значение должно соответствовать элементу  $\varepsilon^0 = 1$

Такт	a0	a1	a2	Степенная форма
1	1	0	0	$\varepsilon^0$
2	0	1	0	$\varepsilon^1$
3	0	0	1	$\varepsilon^2$
4	1	0	1	$\varepsilon^3$
5	1	1	1	$\varepsilon^4$
6	1	1	0	$\varepsilon^5$
7	0	1	1	$\varepsilon^6$

**Пример схемы генератора поля Галуа GF(2<sup>4</sup>)**

$$p(x) = x^4 + x + 1$$

*Генератор элементов  
поля Галуа GF(2<sup>4</sup>)  
p(x) = x<sup>4</sup> + x + 1*



Полиномиальное представление элементов поля:

$$a_0 + a_1x + a_2x^2 + a_3x^3$$

Векторное представление элементов поля:

$$[a_0 \ a_1 \ a_2 \ a_3]$$

Построение поля Галуа по схеме генератора поля:

Начальное значение должно соответствовать элементу  $\epsilon^0 = 1$

Такт	a0	a1	a2	a3	Степенная форма
1	1	0	0	0	$\epsilon^0$
2	0	1	0	0	$\epsilon^1$
3	0	0	1	0	$\epsilon^2$
4	0	0	0	1	$\epsilon^3$
5	1	1	0	0	$\epsilon^4$
6	0	1	1	0	$\epsilon^5$
7	0	0	1	1	$\epsilon^6$
8	1	1	0	1	$\epsilon^7$
9	1	0	1	0	$\epsilon^8$
10	0	1	0	1	$\epsilon^9$
11	1	1	1	0	$\epsilon^{10}$
12	0	1	1	1	$\epsilon^{11}$
13	1	1	1	1	$\epsilon^{12}$
14	1	0	1	1	$\epsilon^{13}$
15	1	0	0	1	$\epsilon^{14}$