Erweiterungskörper $GF(2^3)/M(x) = x^3 + x^2 + 1$

Elemente des $GF(2^3)$	Polynomreste $\alpha^i \bmod M(x = \alpha)$	Koeffizienten der Polynomreste	Minimalpolynome $m_i(x)$
Nullelement	0	$0\,0\,0$	
α^0	1	$0\,0\,1$	$m_0(x) = x + 1$
α^1	α	$0\,1\,0$	$m_1(x) = x^3 + x^2 + 1$
α^2	α^2	$1\,0\,0$	$m_2(x) = x^3 + x^2 + 1$
α^3	$\alpha^2 + 1$	$1\,0\,1$	$m_3(x) = x^3 + x + 1$
α^4	$\alpha^2 + \alpha + 1$	$1\,1\,1$	$m_4(x) = x^3 + x^2 + 1$
α^5	$\alpha + 1$	$0\,1\,1$	$m_5(x) = x^3 + x + 1$
α^6	$\alpha^2 + \alpha$	$1\,1\,0$	$m_6(x) = x^3 + x + 1$
α^7	1	$0\,0\,1$	

Zyklen der Elemente eines Erweiterungskörpers:

$\alpha^{2^{j-1} i \bmod p} \qquad (j = 1, 2, \ldots, k_1 (= \operatorname{grad} M(x)))$

$= \alpha^i,\ \alpha^{2i},\ \alpha^{4i \bmod p},\ \ldots$

$GF(2^3)$:

α^0

$\alpha^1, \alpha^2, \alpha^4$

$\alpha^3, \alpha^6, \alpha^{12 \bmod 7} = \alpha^5$

Entsprechend gilt:

$m_0(x)$

$m_1(x) = m_2(x) = m_4(x) = M_1(x)$

$m_3(x) = m_6(x) = m_5(x)$

Erweiterungskörper $GF(2^4)/M(x) = x^4 + x + 1$

Elemente des $GF(2^4)$			
α^i	Polynomreste	Koeffizienten	Minimalpolynome $m_i(x)$
0	0	0 0 0 0	
1	1	0 0 0 1	$m_0(x) = x + 1$
α^1	α	0 0 1 0	$m_1(x) = x^4 + x + 1$
α^2	α^2	0 1 0 0	$m_2(x) = x^4 + x + 1$
α^3	α^3	1 0 0 0	$m_3(x) = x^4 + x^3 + x^2 + x + 1$
α^4	$\alpha + 1$	0 0 1 1	$m_4(x) = x^4 + x + 1$
α^5	$\alpha^2 + \alpha$	0 1 1 0	$m_5(x) = x^2 + x + 1$
α^6	$\alpha^3 + \alpha^2$	1 1 0 0	$m_6(x) = x^4 + x^3 + x^2 + x + 1$
α^7	$\alpha^3 + \alpha + 1$	1 0 1 1	$m_7(x) = x^4 + x^3 + 1$
α^8	$\alpha^2 + 1$	0 1 0 1	$m_8(x) = x^4 + x + 1$
α^9	$\alpha^3 + \alpha$	1 0 1 0	$m_9(x) = x^4 + x^3 + x^2 + x + 1$
α^{10}	$\alpha^2 + \alpha + 1$	0 1 1 1	$m_{10}(x) = x^2 + x + 1$
α^{11}	$\alpha^3 + \alpha^2 + \alpha$	1 1 1 0	$m_{11}(x) = x^4 + x^3 + 1$
α^{12}	$\alpha^3 + \alpha^2 + \alpha + 1$	1 1 1 1	$m_{12}(x) = x^4 + x^3 + x^2 + x + 1$
α^{13}	$\alpha^3 + \alpha^2 + 1$	1 1 0 1	$m_{13}(x) = x^4 + x^3 + 1$
α^{14}	$\alpha^3 + 1$	1 0 0 1	$m_{14}(x) = x^4 + x^3 + 1$

α^0	$m_0(x)$
$\alpha^1, \alpha^2, \alpha^4, \alpha^8$	$m_1(x) = m_2(x) = m_4(x) = m_8(x)$
$\alpha^3, \alpha^6, \alpha^{12}, \alpha^{24 \bmod 15} = \alpha^9$	$m_3(x) = m_6(x) = m_{12}(x) = m_9(x)$
α^5, α^{10}	$m_5(x) = m_{10}(x)$
$\alpha^7, \alpha^{14}, \alpha^{13}, \alpha^{11}$	$m_7(x) = m_{14}(x) = m_{13}(x) = m_{11}(x)$

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

Multiplikationsverfahren

i	a_i^*	a_i
0	0000	0000000
1	0001	0001101
2	0010	0011010
3	0011	0010111
4	0100	0110100
5	0101	0111001
6	0110	0101110
7	0111	0100011

i	a_i^*	a_i
8	1000	1101000
9	1001	1100101
10	1010	1110010
11	1011	1111111
12	1100	1011100
13	1101	1010001
14	1110	1000110
15	1111	1001011

Divisionsverfahren

i	a_i^*	a_i
0	0000	0000000
1	0001	0001101
2	0010	0010111
3	0011	0011010
4	0100	0100011
5	0101	0101110
6	0110	0110100
7	0111	0111001

i	a_i^*	a_i
8	1000	1000110
9	1001	1001011
10	1010	1010001
11	1011	1011100
12	1100	1100101
13	1101	1101000
14	1110	1110010
15	1111	1111111

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

Multiplikationsverfahren

i	a_i^*	a_i
0	0000	0000000
1	0001	0001011
2	0010	0010110
3	0011	0011101
4	0100	0101100
5	0101	0100111
6	0110	0111010
7	0111	0110001

i	a_i^*	a_i
8	1000	1011000
9	1001	1010011
10	1010	1001110
11	1011	1000101
12	1100	1110100
13	1101	1111111
14	1110	1100010
15	1111	1101001

Divisionsverfahren

i	a_i^*	a_i
0	0000	0000000
1	0001	0001011
2	0010	0010110
3	0011	0011101
4	0100	0100111
5	0101	0101100
6	0110	0110001
7	0111	0111010

i	a_i^*	a_i
8	1000	1000101
9	1001	1001110
10	1010	1010011
11	1011	1011000
12	1100	1100010
13	1101	1101001
14	1110	1110100
15	1111	1111111

Zyklen $k_1 = 3$: α^0

$\alpha^1, \alpha^2, \alpha^4$

$\alpha^3, \alpha^6, \alpha^5$

Zyklen $k_1 = 4$: α^0

$\alpha^1, \alpha^2, \alpha^4, \alpha^8$

$\alpha^3, \alpha^6, \alpha^{12}, \alpha^9$

α^5, α^{10}

$\alpha^7, \alpha^{14}, \alpha^{13}, \alpha^{11}$

Zyklen $k_1 = 5$: α^0

$\alpha^1, \alpha^2, \alpha^4, \alpha^8, \alpha^{16}$

$\alpha^3, \alpha^6, \alpha^{12}, \alpha^{24}, \alpha^{17}$

$\alpha^5, \alpha^{10}, \alpha^{20}, \alpha^9, \alpha^{18}$

$\alpha^7, \alpha^{14}, \alpha^{28}, \alpha^{25}, \alpha^{19}$

$\alpha^{11}, \alpha^{22}, \alpha^{13}, \alpha^{26}, \alpha^{21}$

$\alpha^{15}, \alpha^{30}, \alpha^{29}, \alpha^{27}, \alpha^{23}$

Zyklen $k_1 = 6$: α^0

$\alpha^1, \alpha^2, \alpha^4, \alpha^8, \alpha^{16}, \alpha^{32}$

$\alpha^3, \alpha^6, \alpha^{12}, \alpha^{24}, \alpha^{48}, \alpha^{33}$

$\alpha^5, \alpha^{10}, \alpha^{20}, \alpha^{40}, \alpha^{17}, \alpha^{34}$

$\alpha^7, \alpha^{14}, \alpha^{28}, \alpha^{56}, \alpha^{49}, \alpha^{35}$

$\alpha^9, \alpha^{18}, \alpha^{36}$

$\vdots$

Zyklen $k_1 = 9$: α^0

$\alpha^1, \alpha^2, \alpha^4, \alpha^8, \alpha^{16}, \alpha^{32}, \alpha^{64}, \alpha^{128}, \alpha^{256}$

$\alpha^3, \alpha^6, \alpha^{12}, \alpha^{24}, \alpha^{48}, \alpha^{96}, \alpha^{192}, \alpha^{384}, \alpha^{257}$

$\alpha^5, \alpha^{10}, \alpha^{20}, \alpha^{40}, \alpha^{80}, \alpha^{160}, \alpha^{320}, \alpha^{129}, \alpha^{258}$

$\alpha^7, \alpha^{14}, \alpha^{28}, \alpha^{56}, \alpha^{112}, \alpha^{224}, \alpha^{448}, \alpha^{385}, \alpha^{259}$

$\vdots$