

Multiplication tables

$GF(2^2)=GF(2)[y] / y^2+y+1$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{pmatrix}$$

$$\begin{pmatrix} 01 & 10 & 11 \\ 10 & 11 & 01 \\ 11 & 01 & 10 \end{pmatrix}$$

0	00	0000
1	01	0001
2	02	0010
3	03	0011
4	10	0100
5	11	0101
6	12	0110
7	13	0111
8	20	1000
9	21	1001
a	22	1010
b	23	1011
c	30	1100
d	31	1101
e	32	1110
f	33	1111

$GF(2)[z] / z^4+z+1$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & a & b & c & d & e & f \\ 2 & 4 & 6 & 8 & a & c & e & 3 & 1 & 7 & 5 & b & 9 & f & d \\ 3 & 6 & 5 & c & f & a & 9 & b & 8 & d & e & 7 & 4 & 1 & 2 \\ 4 & 8 & c & 3 & 7 & b & f & 6 & 2 & e & a & 5 & 1 & d & 9 \\ 5 & a & f & 7 & 2 & d & 8 & e & b & 4 & 1 & 9 & c & 3 & 6 \\ 6 & c & a & b & d & 7 & 1 & 5 & 3 & 9 & f & e & 8 & 2 & 4 \\ 7 & e & 9 & f & 8 & 1 & 6 & d & a & 3 & 4 & 2 & 5 & c & b \\ 8 & 3 & b & 6 & e & 5 & d & c & 4 & f & 7 & a & 2 & 9 & 1 \\ 9 & 1 & 8 & 2 & b & 3 & a & 4 & d & 5 & c & 6 & f & 7 & e \\ a & 7 & d & e & 4 & 9 & 3 & f & 5 & 8 & 2 & 1 & b & 6 & c \\ b & 5 & e & a & 1 & f & 4 & 7 & c & 2 & 9 & d & 6 & 8 & 3 \\ c & b & 7 & 5 & 9 & e & 2 & a & 6 & 1 & d & f & 3 & 4 & 8 \\ d & 9 & 4 & 1 & c & 8 & 5 & 2 & f & b & 6 & 3 & e & a & 7 \\ e & f & 1 & d & 3 & 2 & c & 9 & 7 & 6 & 8 & 4 & a & b & 5 \\ f & d & 2 & 9 & 6 & 4 & b & 1 & e & c & 3 & 8 & 7 & 5 & a \end{pmatrix}$$

$$\begin{pmatrix} 0001 & 0010 & 0011 & 0100 & 0101 & 0110 & 0111 & 1000 & 1001 & 1010 & 1011 & 1100 & 1101 & 1110 & 1111 \\ 0010 & 0100 & 0110 & 1000 & 1010 & 1100 & 1110 & 0011 & 0001 & 0111 & 0101 & 1011 & 1001 & 1111 & 1101 \\ 0011 & 0110 & 0101 & 1100 & 1111 & 1010 & 1001 & 1011 & 1000 & 1101 & 1110 & 0111 & 0100 & 0001 & 0010 \\ 0100 & 1000 & 1100 & 0011 & 0111 & 1011 & 1111 & 0110 & 0010 & 1110 & 1010 & 0101 & 0001 & 1101 & 1001 \\ 0101 & 1010 & 1111 & 0111 & 0010 & 1101 & 1000 & 1110 & 1011 & 0100 & 0001 & 1001 & 1100 & 0011 & 0110 \\ 0110 & 1100 & 1010 & 1011 & 1101 & 0111 & 0001 & 0101 & 0011 & 1001 & 1111 & 1110 & 1000 & 0010 & 0100 \\ 0111 & 1110 & 1001 & 1111 & 1000 & 0001 & 0110 & 1101 & 1010 & 0011 & 0100 & 0010 & 0101 & 1100 & 1011 \\ 1000 & 0011 & 1011 & 0110 & 1110 & 0101 & 1101 & 1100 & 0100 & 1111 & 0111 & 1010 & 0010 & 1001 & 0001 \\ 1001 & 0001 & 1000 & 0010 & 1011 & 0011 & 1010 & 0100 & 1101 & 0101 & 1100 & 0110 & 1111 & 0111 & 1110 \\ 1010 & 0111 & 1101 & 1110 & 0100 & 1001 & 0011 & 1111 & 0101 & 1000 & 0010 & 0001 & 1011 & 0110 & 1100 \\ 1011 & 0101 & 1110 & 1010 & 0001 & 1111 & 0100 & 0111 & 1100 & 0010 & 1001 & 1101 & 0110 & 1000 & 0011 \\ 1100 & 1011 & 0111 & 0101 & 1001 & 1110 & 0010 & 1010 & 0110 & 0001 & 1101 & 1111 & 0011 & 0100 & 1000 \\ 1101 & 1001 & 0100 & 0001 & 1100 & 1000 & 0101 & 0010 & 1111 & 1011 & 0110 & 0011 & 1110 & 1010 & 0111 \\ 1110 & 1111 & 0001 & 1101 & 0011 & 0010 & 1100 & 1001 & 0111 & 0110 & 1000 & 0100 & 1010 & 1011 & 0101 \\ 1111 & 1101 & 0010 & 1001 & 0110 & 0100 & 1011 & 0001 & 1110 & 1100 & 0011 & 1000 & 0111 & 0101 & 1010 \end{pmatrix}$$

$\text{GF}(2)[z] / z^4 + z^3 + 1$

1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
2	4	6	8	a	c	e	9	b	d	f	1	3	5	7
3	6	5	c	f	a	9	1	2	7	4	d	e	b	8
4	8	c	9	d	1	5	b	f	3	7	2	6	a	e
5	a	f	d	8	7	2	3	6	9	c	e	b	4	1
6	c	a	1	7	d	b	2	4	e	8	3	5	f	9
7	e	9	5	2	b	c	a	d	4	3	f	8	1	6
8	9	1	b	3	2	a	f	7	6	e	4	c	d	5
9	b	2	f	6	4	d	7	e	c	5	8	1	3	a
a	d	7	3	9	e	4	6	c	b	1	5	f	8	2
b	f	4	7	c	8	3	e	5	1	a	9	2	6	d
c	1	d	2	e	3	f	4	8	5	9	6	a	7	b
d	3	e	6	b	5	8	c	1	f	2	a	7	9	4
e	5	b	a	4	f	1	d	3	8	6	7	9	2	c
f	7	8	e	1	9	6	5	a	2	d	b	4	c	3

0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
0010	0100	0110	1000	1010	1100	1110	1001	1011	1101	1111	0001	0011	0101	0111
0011	0110	0101	1100	1111	1010	1001	0001	0010	0111	0100	1101	1110	1011	1000
0100	1000	1100	1001	1101	0001	0101	1011	1111	0011	0111	0010	0110	1010	1110
0101	1010	1111	1101	1000	0111	0010	0011	0110	1001	1100	1110	1011	0100	0001
0110	1100	1010	0001	0111	1101	1011	0010	0100	1110	1000	0011	0101	1111	1001
0111	1110	1001	0101	0010	1011	1100	1010	1101	0100	0011	1111	1000	0001	0110
1000	1001	0001	1011	0011	0010	1010	1111	0111	0110	1110	0100	1100	1101	0101
1001	1011	0010	1111	0110	0100	1101	0111	1110	1100	0101	1000	0001	0011	1010
1010	1101	0111	0011	1001	1110	0100	0110	1100	1011	0001	0101	1111	1000	0010
1011	1111	0100	0111	1100	1000	0011	1110	0101	0001	1010	1001	0010	0110	1101
1100	0001	1101	0010	1110	0011	1111	0100	1000	0101	1001	0110	1010	0111	1011
1101	0011	1110	0110	1011	0101	1000	1100	0001	1111	0010	1010	0111	1001	0100
1110	0101	1011	1010	0100	1111	0001	1101	0011	1000	0110	0111	1001	0010	1100
1111	0111	1000	1110	0001	1001	0110	0101	1010	0010	1101	1011	0100	1100	0011

$$\text{GF}((2^2)^2) = \text{GF}(2^2)[x] / x^2 + x + 2$$

$$P(x) = x^2 + x + 2 = 1x^2 + 1x + 2 = 1x^2 + 1x + y$$

01	02	03	10	11	12	13	20	21	22	23	30	31	32	33
02	03	01	20	22	23	21	30	32	33	31	10	12	13	11
03	01	02	30	33	31	32	10	13	11	12	20	23	21	22
10	20	30	12	02	32	22	23	33	03	13	31	21	11	01
11	22	33	02	13	20	31	03	12	21	30	01	10	23	32
12	23	31	32	20	11	03	13	01	30	22	21	33	02	10
13	21	32	22	31	03	10	33	20	12	01	11	02	30	23
20	30	10	23	03	13	33	31	11	01	21	12	32	22	02
21	32	13	33	12	01	20	11	30	23	02	22	03	10	31
22	33	11	03	21	30	12	01	23	32	10	02	20	31	13
23	31	12	13	30	22	01	21	02	10	33	32	11	03	20
30	10	20	31	01	21	11	12	22	02	32	23	13	33	03
31	12	23	21	10	33	02	32	03	20	11	13	22	01	30
32	13	21	11	23	02	30	22	10	31	03	33	01	20	12
33	11	22	01	32	10	23	02	31	13	20	03	30	12	21

1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
2	3	1	8	a	b	9	c	e	f	d	4	6	7	5
3	1	2	c	f	d	e	4	7	5	6	8	b	9	a
4	8	c	6	2	e	a	b	f	3	7	d	9	5	1
5	a	f	2	7	8	d	3	6	9	c	1	4	b	e
6	b	d	e	8	5	3	7	1	c	a	9	f	2	4
7	9	e	a	d	3	4	f	8	6	1	5	2	c	b
8	c	4	b	3	7	f	d	5	1	9	6	e	a	2
9	e	7	f	6	1	8	5	c	b	2	a	3	4	d
a	f	5	3	9	c	6	1	b	e	4	2	8	d	7
b	d	6	7	c	a	1	9	2	4	f	e	5	3	8
c	4	8	d	1	9	5	6	a	2	e	b	7	f	3
d	6	b	9	4	f	2	e	3	8	5	7	a	1	c
e	7	9	5	b	2	c	a	4	d	3	f	1	8	6
f	5	a	1	e	4	b	2	d	7	8	3	c	6	9

0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
0010	0011	0001	1000	1010	1011	1001	1100	1110	1111	1101	0100	0110	0111	0101
0011	0001	0010	1100	1111	1101	1110	0100	0111	0101	0110	1000	1011	1001	1010
0100	1000	1100	0110	0010	1110	1010	1011	1111	0011	0111	1101	1001	0101	0001
0101	1010	1111	0010	0111	1000	1101	0011	0110	1001	1100	0001	0100	1011	1110
0110	1011	1101	1110	1000	0101	0011	0111	0001	1100	1010	1001	1111	0010	0100
0111	1001	1110	1010	1101	0011	0100	1111	1000	0110	0001	0101	0010	1100	1011
1000	1100	0100	1011	0011	0111	1111	1101	0101	0001	1001	0110	1110	1010	0010
1001	1110	0111	1111	0110	0001	1000	0101	1100	1011	0010	1010	0011	0100	1101
1010	1111	0101	0011	1001	1100	0110	0001	1011	1110	0100	0010	1000	1101	0111
1011	1101	0110	0111	1100	1010	0001	1001	0010	0100	1111	1110	0101	0011	1000
1100	0100	1000	1101	0001	1001	0101	0110	1010	0010	1110	1011	0111	1111	0011
1101	0110	1011	1001	0100	1111	0010	1110	0011	1000	0101	0111	1010	0001	1100
1110	0111	1001	0101	1011	0010	1100	1010	0100	1101	0011	1111	0001	1000	0110
1111	0101	1010	0001	1110	0100	1011	0010	1101	0111	1000	0011	1100	0110	1001

another $\text{GF}((2^2)^2) = \text{GF}(2^2)[x] / x^2 + x + 3$

$$P(x) = x^2 + x + 3 = 1x^2 + 1x + 3 = 1x^2 + 1x + y + 1$$

01	02	03	10	11	12	13	20	21	22	23	30	31	32	33
02	03	01	20	22	23	21	30	32	33	31	10	12	13	11
03	01	02	30	33	31	32	10	13	11	12	20	23	21	22
10	20	30	13	03	33	23	21	31	01	11	32	22	12	02
11	22	33	03	12	21	30	01	10	23	32	02	13	20	31
12	23	31	33	21	10	02	11	03	32	20	22	30	01	13
13	21	32	23	30	02	11	31	22	10	03	12	01	33	20
20	30	10	21	01	11	31	32	12	02	22	13	33	23	03
21	32	13	31	10	03	22	12	33	20	01	23	02	11	30
22	33	11	01	23	32	10	02	20	31	13	03	21	30	12
23	31	12	11	32	20	03	22	01	13	30	33	10	02	21
30	10	20	32	02	22	12	13	23	03	33	21	11	31	01
31	12	23	22	13	30	01	33	02	21	10	11	20	03	32
32	13	21	12	20	01	33	23	11	30	02	31	03	22	10
33	11	22	02	31	13	20	03	30	12	21	01	32	10	23

1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
2	3	1	8	a	b	9	c	e	f	d	4	6	7	5
3	1	2	c	f	d	e	4	7	5	6	8	b	9	a
4	8	c	7	3	f	b	9	d	1	5	e	a	6	2
5	a	f	3	6	9	c	1	4	b	e	2	7	8	d
6	b	d	f	9	4	2	5	3	e	8	a	c	1	7
7	9	e	b	c	2	5	d	a	4	3	6	1	f	8
8	c	4	9	1	5	d	e	6	2	a	7	f	b	3
9	e	7	d	4	3	a	6	f	8	1	b	2	5	c
a	f	5	1	b	e	4	2	8	d	7	3	9	c	6
b	d	6	5	e	8	3	a	1	7	c	f	4	2	9
c	4	8	e	2	a	6	7	b	3	f	9	5	d	1
d	6	b	a	7	c	1	f	2	9	4	5	8	3	e
e	7	9	6	8	1	f	b	5	c	2	d	3	a	4
f	5	a	2	d	7	8	3	c	6	9	1	e	4	b

0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
0010	0011	0001	1000	1010	1011	1001	1100	1110	1111	1101	0100	0110	0111	0101
0011	0001	0010	1100	1111	1101	1110	0100	0111	0101	0110	1000	1011	1001	1010
0100	1000	1100	0111	0011	1111	1011	1001	1101	0001	0101	1110	1010	0110	0010
0101	1010	1111	0011	0110	1001	1100	0001	0100	1011	1110	0010	0111	1000	1101
0110	1011	1101	1111	1001	0100	0010	0101	0011	1110	1000	1010	1100	0001	0111
0111	1001	1110	1011	1100	0010	0101	1101	1010	0100	0011	0110	0001	1111	1000
1000	1100	0100	1001	0001	0101	1101	1110	0110	0010	1010	0111	1111	1011	0011
1001	1110	0111	1101	0100	0011	1010	0110	1111	1000	0001	1011	0010	0101	1100
1010	1111	0101	0001	1011	1110	0100	0010	1000	1101	0111	0011	1001	1100	0110
1011	1101	0110	0101	1110	1000	0011	1010	0001	0111	1100	1111	0100	0010	1001
1100	0100	1000	1110	0010	1010	0110	0111	1011	0011	1111	1001	0101	1101	0001
1101	0110	1011	1010	0111	1100	0001	1111	0010	1001	0100	0101	1000	0011	1110
1110	0111	1001	0110	1000	0001	1111	1011	0101	1100	0010	1101	0011	1010	0100
1111	0101	1010	0010	1101	0111	1000	0011	1100	0110	1001	0001	1110	0100	1011

??? = GF(2²)[x] / x²+x+1

01	02	03	10	11	12	13	20	21	22	23	30	31	32	33
02	03	01	20	22	23	21	30	32	33	31	10	12	13	11
03	01	02	30	33	31	32	10	13	11	12	20	23	21	22
10	20	30	11	01	31	21	22	32	02	12	33	23	13	03
11	22	33	01	10	23	32	02	13	20	31	03	12	21	30
12	23	31	31	23	12	00	12	00	31	23	23	31	00	12
13	21	32	21	32	00	13	32	21	13	00	13	00	32	21
20	30	10	22	02	12	32	33	13	03	23	11	31	21	01
21	32	13	32	13	00	21	13	32	21	00	21	00	13	32
22	33	11	02	20	31	13	03	21	30	12	01	23	32	10
23	31	12	12	31	23	00	23	00	12	31	31	12	00	23
30	10	20	33	03	23	13	11	21	01	31	22	12	32	02
31	12	23	23	12	31	00	31	00	23	12	12	23	00	31
32	13	21	13	21	00	32	21	13	32	00	32	00	21	13
33	11	22	03	30	12	21	01	32	10	23	02	31	13	20

1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
2	3	1	8	a	b	9	c	e	f	d	4	6	7	5
3	1	2	c	f	d	e	4	7	5	6	8	b	9	a
4	8	c	5	1	d	9	a	e	2	6	f	b	7	3
5	a	f	1	4	b	e	2	7	8	d	3	6	9	c
6	b	d	d	b	6	0	6	0	d	b	b	d	0	6
7	9	e	9	e	0	7	e	9	7	0	7	0	e	9
8	c	4	a	2	6	e	f	7	3	b	5	d	9	1
9	e	7	e	7	0	9	7	e	9	0	9	0	7	e
a	f	5	2	8	d	7	3	9	c	6	1	b	e	4
b	d	6	6	d	b	0	b	0	6	d	d	6	0	b
c	4	8	f	3	b	7	5	9	1	d	a	6	e	2
d	6	b	b	6	d	0	d	0	b	6	6	b	0	d
e	7	9	7	9	0	e	9	7	e	0	e	0	9	7
f	5	a	3	c	6	9	1	e	4	b	2	d	7	8

0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
0010	0011	0001	1000	1010	1011	1001	1100	1110	1111	1101	0100	0110	0111	0101
0011	0001	0010	1100	1111	1101	1110	0100	0111	0101	0110	1000	1011	1001	1010
0100	1000	1100	0101	0001	1101	1001	1010	1110	0010	0110	1111	1011	0111	0011
0101	1010	1111	0001	0100	1011	1110	0010	0111	1000	1101	0011	0110	1001	1100
0110	1011	1101	1101	1011	0110	0000	0110	0000	1101	1011	1011	1101	0000	0110
0111	1001	1110	1001	1110	0000	0111	1110	1001	0111	0000	0111	0000	1110	1001
1000	1100	0100	1010	0010	0110	1110	1111	0111	0011	1011	0101	1101	1001	0001
1001	1110	0111	1110	0111	0000	1001	0111	1110	1001	0000	1001	0000	0111	1110
1010	1111	0101	0010	1000	1101	0111	0011	1001	1100	0110	0001	1011	1110	0100
1011	1101	0110	0110	1101	1011	0000	1011	0000	0110	1101	1101	0110	0000	1011
1100	0100	1000	1111	0011	1011	0111	0101	1001	0001	1101	1010	0110	1110	0010
1101	0110	1011	1011	0110	1101	0000	1101	0000	1011	0110	0110	1011	0000	1101
1110	0111	1001	0111	1001	0000	1110	1001	0111	1110	0000	1110	0000	1001	0111
1111	0101	1010	0011	1100	0110	1001	0001	1110	0100	1011	0010	1101	0111	1000