Primitive Elements in GF(q)

$GF(q) = \{0, 1, 2, \ldots, q-1\}$

$GF(3) = \{0, 1, 2\}$

$2^0 = 1$

$2^1 = 2$

$2^2 = 4 \bmod 3 = 1$

$GF(5) = \{0, 1, 2, 3, 4\}$

$2^0 = 1$

$2^1 = 2$

$2^2 = 4$

$2^3 = 8 \bmod 5 = 3$

$2^4 = 16 \bmod 5 = 1$

$3^0 = 1$

$3^1 = 3$

$3^2 = 9 \bmod 5 = 4$

$GF(7) = \{0, 1, 2, 3, 4, 5, 6\}$

$2^0 = 1$

$2^1 = 2$

$2^2 = 4$

$2^3 = 8 \bmod 7 = 1$

$2^4 = 16 \bmod 7 = 2$

$3^0 = 1$

$3^1 = 3$

$3^2 = 9 \bmod 7 = 2$

$3^3 = 27 \bmod 7 = 6$

$3^4 = 81 \bmod 7 = 4$

$3^5 = 243 \bmod 7 =$

GF(2)

+	0	1
0	0	1
1	1	0

×	0	1
0	0	0
1	0	1

GF(3)

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

×	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

GF(5)

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Irreducible polynomials

- $GF(2) = \{0, 1\}$

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

$f(0) = (0)^2+1 = 0+1 = 1$

$f(1) = (1)^2+1 = 1+1 = 0$

$x=1$ is satisfy x^2+1

$x+1$ is factor of x^2+1

$$\begin{array}{r|l} & x+1 \\ \hline x+1 & x^2+1 \\ & x^2 \quad +x \\ \hline & \quad x+1 \\ & \quad x+1 \\ \hline & \quad 0 \end{array}$$

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

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

$= x^2+0+1$

$= x^2+1$

polynomial of degree 1

	x^1	x^0
x	1	0
$x+1$	1	1

polynomial of degree 2

	x^2	x^1	x^0
x^2	1	0	0
x^2+1	1	0	1
x^2+x	1	1	0
x^2+x+1	1	1	1

$f(x) = x^2 = x \cdot x$

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

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

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

check $f(0) = 0+0+1 = 1$

$f(1) = 1+1+1 = 1$

polynomial of degree 3

	x^3	x^2	x^1	x^0
x^3	1	0	0	0
x^3+1	1	0	0	1
x^3+x	1	0	1	0
x^3+x+1	1	0	1	1
x^3+x^2	1	1	0	0
x^3+x^2+1	1	1	0	1
x^3+x^2+x	1	1	1	0
x^3+x^2+x+1	1	1	ϕ	1

Extension of $GF(2)$ to $GF(4)$

$GF(4) = \{0, 1, 2, 3\}$

$GF(2) = \{0, 1\}$

$P(x) = x^2$

$P(0) = 0$

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

$P(0) = 0 + 1 = 1$

$P(1) = 1 + 1 = 0$

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

$P(0) = 0 + 0 + 1 = 1$

$P(1) = 1 + 1 + 1 = 1$

$x^2 + x + 1 = 0$

$x^2 = x + 1$

$x^2 + x = 1$

$x^2 + 1 = x$

Remainder $0, 1, x, x+1$

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$1+x$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$*$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

$x = 2$

$+$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

$\times$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2