Prime Power Fields : $\mathbb{F}_q = \mathbb{Z}_p[x]/m(x) = GF(p^n)$

In [ ]:
```
p:3
```

In [ ]:
```
n:2
```

In [3]:
```
gf_set_data(p,n)
```

Out[3]: $\text{Structure}\,[\text{GF-DATA}]$

In [4]:
```
gf_info()
```

```
characteristic = 3
reduction polynomial = x^2+1
primitive element = x+1
nr of elements = 9
nr of units = 8
nr of primitive elements = 4
```

Out[4]: **false**

In [18]:
```
atable:gf_add_table()
```

Out[18]:
$$\begin{pmatrix}
0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\
1 & 2 & 0 & 4 & 5 & 3 & 7 & 8 & 6 \\
2 & 0 & 1 & 5 & 3 & 4 & 8 & 6 & 7 \\
3 & 4 & 5 & 6 & 7 & 8 & 0 & 1 & 2 \\
4 & 5 & 3 & 7 & 8 & 6 & 1 & 2 & 0 \\
5 & 3 & 4 & 8 & 6 & 7 & 2 & 0 & 1 \\
6 & 7 & 8 & 0 & 1 & 2 & 3 & 4 & 5 \\
7 & 8 & 6 & 1 & 2 & 0 & 4 & 5 & 3 \\
8 & 6 & 7 & 2 & 0 & 1 & 5 & 3 & 4
\end{pmatrix}$$

In [19]:
```
for i:1 thru p^n do for j:1 thru p^n do atable[i,j]:gf_n2p(atable[i,j])
```

Out[19]: **done**

In [20]:
```
print(atable)$
```

```
        [    0    ]         [    1    ]         [    2    ]
        [         ]         [         ]         [         ]
        [    1    ]         [    2    ]         [    0    ]
        [         ]         [         ]         [         ]
        [    2    ]         [    0    ]         [    1    ]
        [         ]         [         ]         [         ]
        [    x    ]         [  x + 1  ]         [  x + 2  ]
        [         ]         [         ]         [         ]
Col 1 = [  x + 1  ] Col 2 = [  x + 2  ] Col 3 = [    x    ]
        [         ]         [         ]         [         ]
        [  x + 2  ]         [    x    ]         [  x + 1  ]
        [         ]         [         ]         [         ]
        [   2 x   ]         [ 2 x + 1 ]         [ 2 x + 2 ]
        [         ]         [         ]         [         ]
        [ 2 x + 1 ]         [ 2 x + 2 ]         [   2 x   ]
        [         ]         [         ]         [         ]
        [ 2 x + 2 ]         [   2 x   ]         [ 2 x + 1 ]
        [    x    ]         [  x + 1  ]         [  x + 2  ]
        [         ]         [         ]         [         ]
        [  x + 1  ]         [  x + 2  ]         [    x    ]
        [         ]         [         ]         [         ]
        [  x + 2  ]         [    x    ]         [  x + 1  ]
        [         ]         [         ]         [         ]
        [   2 x   ]         [ 2 x + 1 ]         [ 2 x + 2 ]
        [         ]         [         ]         [         ]
Col 4 = [ 2 x + 1 ] Col 5 = [ 2 x + 2 ] Col 6 = [   2 x   ]
        [         ]         [         ]         [         ]
        [ 2 x + 2 ]         [   2 x   ]         [ 2 x + 1 ]
        [         ]         [         ]         [         ]
        [    0    ]         [    1    ]         [    2    ]
        [         ]         [         ]         [         ]
        [    1    ]         [    2    ]         [    0    ]
        [         ]         [         ]         [         ]
        [    2    ]         [    0    ]         [    1    ]
        [   2 x   ]         [ 2 x + 1 ]         [ 2 x + 2 ]
        [         ]         [         ]         [         ]
        [ 2 x + 1 ]         [ 2 x + 2 ]         [   2 x   ]
        [         ]         [         ]         [         ]
        [ 2 x + 2 ]         [   2 x   ]         [ 2 x + 1 ]
        [         ]         [         ]         [         ]
        [    0    ]         [    1    ]         [    2    ]
        [         ]         [         ]         [         ]
Col 7 = [    1    ] Col 8 = [    2    ] Col 9 = [    0    ]
        [         ]         [         ]         [         ]
        [    2    ]         [    0    ]         [    1    ]
        [         ]         [         ]         [         ]
        [    x    ]         [  x + 1  ]         [  x + 2  ]
        [         ]         [         ]         [         ]
        [  x + 1  ]         [  x + 2  ]         [    x    ]
        [         ]         [         ]         [         ]
        [  x + 2  ]         [    x    ]         [  x + 1  ]
```

Out[20]:

$$\begin{pmatrix} 0 & 1 & 2 & x & x+1 & x+2 & 2x & 2x+1 & 2x+2 \\ 1 & 2 & 0 & x+1 & x+2 & x & 2x+1 & 2x+2 & 2x \\ 2 & 0 & 1 & x+2 & x & x+1 & 2x+2 & 2x & 2x+1 \\ x & x+1 & x+2 & 2x & 2x+1 & 2x+2 & 0 & 1 & 2 \\ x+1 & x+2 & x & 2x+1 & 2x+2 & 2x & 1 & 2 & 0 \\ x+2 & x & x+1 & 2x+2 & 2x & 2x+1 & 2 & 0 & 1 \\ 2x & 2x+1 & 2x+2 & 0 & 1 & 2 & x & x+1 & x+2 \\ 2x+1 & 2x+2 & 2x & 1 & 2 & 0 & x+1 & x+2 & x \\ 2x+2 & 2x & 2x+1 & 2 & 0 & 1 & x+2 & x & x+1 \end{pmatrix}$$

In [21]:
```
mtable:gf_mult_table()$
```

Out[21]:
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 1 & 6 & 8 & 7 & 3 & 5 & 4 \\ 3 & 6 & 2 & 5 & 8 & 1 & 4 & 7 \\ 4 & 8 & 5 & 6 & 1 & 7 & 2 & 3 \\ 5 & 7 & 8 & 1 & 3 & 4 & 6 & 2 \\ 6 & 3 & 1 & 7 & 4 & 2 & 8 & 5 \\ 7 & 5 & 4 & 2 & 6 & 8 & 3 & 1 \\ 8 & 4 & 7 & 3 & 2 & 5 & 1 & 6 \end{pmatrix}$$

In [23]:
```
for i:1 thru p^n-1 do for j:1 thru p^n-1 do mtable[i,j]:gf_n2p(mtable[i,j])
```

Out[23]: **done**

In [24]:
```
print(mtable)
```

```
[    1        2        x      x + 1    x + 2     2 x    2 x + 1  2 x + 2 ]
[                                                                         ]
[    2        1      2 x    2 x + 2  2 x + 1     x      x + 2    x + 1  ]
[                                                                         ]
[    x      2 x        2      x + 2  2 x + 2     1      x + 1    2 x + 1 ]
[                                                                         ]
[  x + 1   2 x + 2   x + 2     2 x       1     2 x + 1     2        x    ]
[                                                                         ]
[  x + 2   2 x + 1  2 x + 2      1        x      x + 1     2 x       2    ]
[                                                                         ]
[   2 x       x        1     2 x + 1   x + 1      2     2 x + 2   x + 2  ]
[                                                                         ]
[ 2 x + 1   x + 2    x + 1      2       2 x    2 x + 2     x        1    ]
[                                                                         ]
[ 2 x + 2   x + 1   2 x + 1     x        2      x + 2      1       2 x   ]
```

Out[24]:
$$\begin{pmatrix} 1 & 2 & x & x+1 & x+2 & 2x & 2x+1 & 2x+2 \\ 2 & 1 & 2x & 2x+2 & 2x+1 & x & x+2 & x+1 \\ x & 2x & 2 & x+2 & 2x+2 & 1 & x+1 & 2x+1 \\ x+1 & 2x+2 & x+2 & 2x & 1 & 2x+1 & 2 & x \\ x+2 & 2x+1 & 2x+2 & 1 & x & x+1 & 2x & 2 \\ 2x & x & 1 & 2x+1 & x+1 & 2 & 2x+2 & x+2 \\ 2x+1 & x+2 & x+1 & 2 & 2x & 2x+2 & x & 1 \\ 2x+2 & x+1 & 2x+1 & x & 2 & x+2 & 1 & 2x \end{pmatrix}$$

In [25]:
```
gf_make_logs()
```

Out[25]: ["{Lisp Array: \#(1 4 6 7 2 8 3 5 1)}" , "{Lisp Array: \#(NIL 0 4 6 1 7 2 3 5)}" , "{Lisp Array: \#
]

In [31]:
```
for i:1 thru p^n-1 do print("(",gf_primitive(),")^",i,"=",gf_n2p(gf_powers[i]))
```

```
( x + 1 )^ 1 = x + 1
( x + 1 )^ 2 = 2 x
( x + 1 )^ 3 = 2 x + 1
( x + 1 )^ 4 = 2
( x + 1 )^ 5 = 2 x + 2
( x + 1 )^ 6 = x
( x + 1 )^ 7 = x + 2
( x + 1 )^ 8 = 1
```

Out[31]: **done**

In [32]:
```
for i:1 thru p^n-1 do print(gf_n2p(i)," has order ",gf_order(gf_n2p(i)))
```

```
1  has order  1
2  has order  2
x  has order  4
x + 1  has order  8
x + 2  has order  8
2 x  has order  4
2 x + 1  has order  8
2 x + 2  has order  8
```

Out[32]: **done**

In [35]:
```
gf_factor(x^(p^n)-x,3)
```

Out[35]: $x\ (x+1)\ (x+2)\ \left(x^2+1\right)\ \left(x^2+x+2\right)\ \left(x^2+2\,x+2\right)$

Universal Polynomial : $x^{p^n} - x$

factors in all irreducible monic polynomials of degree $k \mid n$ In this case $n = 2$ and therefore it factors in all irreducibles of degree 1 or 2

In [64]:
```
gf_factor(x^p^n-x)
```

Out[64]: $x\ (x+1)\ (x+2)\ \left(x^2+1\right)\ \left(x^2+x+2\right)\ \left(x^2+2\,x+2\right)$

In [64]:
```
gf_factor(x^2+1)
```

Out[64]: x^2+1

In [64]:
```
for i:0 thru p^n-1 do ( print(gf_add(x,-gf_n2p(i))))
```

```
x
x + 2
x + 1
0
2
1
2 x
2 x + 2
2 x + 1
```

Out[64]: **done**

In [ ]: