Primitive polynomials

$primitive\ polynomials \subset irreducible\ polynomials \subset polynomials$

Is $f(x) = x^3 + x + 1$ a *primitive polynomial* over $\mathbb{Z}_2$?

In [1]:
```
f:x^3+x+1;
```
Out[1]: $x^3 + x + 1$

In [2]:
```
n:hipow(f,x);
```
Out[2]: 3

In [3]:
```
p:modulus:2;
```
Out[3]: 2

To be primitive $f(x)$ should divide $x^{p^n-1} - 1$ and no other $x^e - 1$ for $e < p^n - 1$

In [4]:
```
divide(x^(p^n-1)-1,f);
```
Out[4]: $[x^4 + x^2 + x + 1, 0]$

In [5]:
```
for e:1 thru p^n-1 do print("e=",e,",",divide(x^e-1,f));
```
```
e= 1 , [0, x + 1]
                2
e= 2 , [0, x  + 1]
e= 3 , [1, x]
                2
e= 4 , [x, x  + x + 1]
             2       2
e= 5 , [x  + 1, x  + x]
             3           2
e= 6 , [x  + x + 1, x ]
             4    2
e= 7 , [x  + x  + x + 1, 0]
```
Out[5]: **done**

In [6]:
```
gf_primitive_poly_p(f,p);
```
Out[6]: **true**

In [7]:
```
factor(x^(p^n-1)-1);
```
Out[7]: $(x+1)\left(x^3+x+1\right)\left(x^3+x^2+1\right)$

Universal polynomial : $U(x) = x^{p^n} - x$

The universal polynomial is the product of all irreducible polynomials of degree d for $\forall d : d \mid n$

In [8]:
```
factor(x^p^n -x);
```
Out[8]: $x\,(x+1)\,\left(x^3+x+1\right)\,\left(x^3+x^2+1\right)$

If $f(x)$ is a primitive polynomial of degree n over $\mathbb{Z}_p$ then x is a generator of $\mathbb{F}_{p^n} = \mathbb{Z}_p[x]/f(x)$

In [9]:
```
gf_set_data(p,n);
```
Out[9]: $\mathrm{Structure}\;[\mathrm{GF\text{-}DATA}]$

In [10]:
```
for i:1 thru p^n-1 do print("x^",i,"=",gf_exp(x,i));
```
```
x^ 1 = x
        2
x^ 2 = x
x^ 3 = x + 1
        2
x^ 4 = x  + x
        2
x^ 5 = x  + x + 1
        2
x^ 6 = x  + 1
x^ 7 = 1
```
Out[10]: **done**

The above should give you a hint of why the LFSR works. Multiplying by x is shifting left.

If x is a generator then the order of x should be $p^n - 1$

In [11]:
```
for i:1 thru p^n-2 do print(gf_exp(x,i)," has order ",gf_order(gf_exp(x,i)))
;
```
```
x  has order  7
 2
x   has order  7
x + 1  has order  7
 2
x  + x  has order  7
 2
x  + x + 1  has order  7
 2
x  + 1  has order  7
```
Out[11]: **done**

If we know the factorization of $p^n - 1$ then we can check that
$\forall\ primes\ q | (p^n - 1), f \nmid x^{\frac{p^n-1}{q}} - 1$

In [12]:
```
modulus:3;
```
Out[12]: 3

In [13]:
```
p:3;
```
Out[13]: 3

In [14]:
```
n:4;
```
Out[14]: 4

In [15]:
```
f:gf_primitive_poly(p,n);
```
Out[15]: $x^4 + x + 2$

In [16]:
```
ifactors(p^n-1);
```
Out[16]: $[[2, 4], [5, 1]]$

Prime factors of 80 are $2, 5$

In [17]:
```
q:2;
```
Out[17]: 2

In [18]:
```
divide(x^((p^n-1)/q)-1,f);
```
Out[18]: $\left[x^{36} - x^{33} + x^{32} + x^{30} + x^{29} + x^{28} - x^{27} - x^{24} - x^{23} + x^{21} - x^{19} - x^{18} + x^{17} + x^{16} - x^6 + x^4 - x^3 - x^2 - x - 1, 1\right]$

In [19]:
```
q:5;
```
Out[19]: 5

In [20]:
```
divide(x^((p^n-1)/q)-1,f);
```
Out[20]: $\left[x^{12} - x^9 + x^8 + x^6 + x^5 + x^4 - x^3 - 1, -x^3 + x + 1\right]$

In [ ]:

In [ ]: