```
> restart:with(NumberTheory);
```

[*AreCoprime*, *CalkinWilfSequence*, *CarmichaelLambda*, *ChineseRemainder*, *ContinuedFraction*, *ContinuedFractionPolynomial*, *CyclotomicPolynomial*, *Divisors*, *FactorNormEuclidean*, *HomogeneousDiophantine*, *ImaginaryUnit*, *InhomogeneousDiophantine*, *IntegralBasis*, *InverseTotient*, *IsCyclotomicPolynomial*, *IsMersenne*, *IsSquareFree*, *IthFermat*, *IthMersenne*, *JacobiSymbol*, *KroneckerSymbol*, *Landau*, *LargestNthPower*, *LegendreSymbol*, *Möbius*, *ModExtendedGCD*, *ModularLog*, *ModularRoot*, *ModularSquareRoot*, *Moebius*, *MultiplicativeOrder*, *Möbius*, *NearestLatticePoint*, *NextSafePrime*, *NumberOfIrreduciblePolynomials*, *NumberOfPrimeFactors*, Ω, Φ, *PrimeCounting*, *PrimeFactors*, *PrimitiveRoot*, *PseudoPrimitiveRoot*, *QuadraticResidue*, *Radical*, *RepeatingDecimal*, *RootsOfUnity*, *SimplestRational*, *SumOfDivisors*, *SumOfSquares*, *ThueSolve*, *Totient*, λ, μ, ϕ, π, σ, τ, φ] **(1)**

```
> p := 3; n:= 4; Q := p^n;
```

$$p := 3$$
$$n := 4$$
$$Q := 81 \quad \textbf{(2)}$$

Construct splitting field of x^p^n - x

```
> factor(x^(Q-1) - 1);
```

$$(x-1)\left(x^4+x^3+x^2+x+1\right)(1+x)\left(x^4-x^3+x^2-x+1\right)\left(x^2+1\right)\left(x^8-x^6+x^4-x^2+1\right)\left(x^4+1\right)\left(x^{16}-x^{12}+x^8-x^4+1\right)\left(x^8+1\right)\left(x^{32}-x^{24}+x^{16}-x^8+1\right) \quad \textbf{(3)}$$

Factors are the cyclotomic polynomials of order a divisor of Q - 1. E.g.,

```
> (Q-1)/2;CyclotomicPolynomial((Q-1)/2,x);
```

$$40$$
$$x^{16}-x^{12}+x^8-x^4+1 \quad \textbf{(4)}$$

For prime order, the cyclotomic polynomials are (x^p - 1) / (x - 1), which are irreducible over the integers by Eisenstein's criterion

```
> f23:=CyclotomicPolynomial(23,x); expand(subs(x=u+1,f23)); % mod 23;
```

$$f23 := x^{22}+x^{21}+x^{20}+x^{19}+x^{18}+x^{17}+x^{16}+x^{15}+x^{14}+x^{13}+x^{12}+x^{11}+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1$$
$$u^{22}+23\,u^{21}+253\,u^{20}+1771\,u^{19}+8855\,u^{18}+33649\,u^{17}+100947\,u^{16}+245157\,u^{15}+490314\,u^{14}+817190\,u^{13}+1144066\,u^{12}+1352078\,u^{11}+1352078\,u^{10}+1144066\,u^9+817190\,u^8+490314\,u^7+245157\,u^6+100947\,u^5+33649\,u^4+8855\,u^3+1771\,u^2+253\,u+23$$
$$u^{22} \quad \textbf{(5)}$$

The primitive root of unity has minimum polynomial the cyclotomic polynomial (one of the factors of x^(Q-1) - 1).

```
> f_root_of_unity := CyclotomicPolynomial(Q-1,z);
```

$$f_root_of_unity := z^{32}-z^{24}+z^{16}-z^8+1 \quad \textbf{(6)}$$

It is not irreducible modulo 3, but all factors have the same degree, which is the order of p modulo Q-1:

3, 9, 27, 81 mod 80 = 1.

```
> Factor(x^(Q-1)- 1) mod 3;
```

$$(x^4+x^3+2)\,(x^4+x^3+x^2+2x+2)\,(x^4+2x+2)\,(x^2+2x+2)\,(x^4+2x^3+x+1)\,(x^4+x^3+2x^2+2x+2)\,(x^4+x^3+x^2+1)\,(x^4+2x^2+2)\,(x^4+x^3+x^2+x+1)\,(x^4+x^3+2x+1)\,(x^4+2x^3+x^2+x+2)\,(x^4+x^2+2x+1)\,(x^4+2x^3+2)\,(1+x)\,(x^2+x+2)\,(x^4+x^2+x+1)\,(x^4+x+2)\,(x^4+2x^3+x^2+1)\,(x+2)\,(x^4+x^2+2)\,(x^4+2x^3+x^2+2x+1)\,(x^4+2x^3+2x^2+x+2)\,(x^2+1) \quad (7)$$

Write a symbol for the root of unity

```
> gen_z:=product(x - z^'i', 'i' = 1..Q-1);
```

$$gen_z := (x-z)\,(-z^{49}+x)\,(-z^{50}+x)\,(-z^{51}+x)\,(-z^{52}+x)\,(-z^{53}+x)\,(-z^{54}+x)\,(-z^{55}+x)\,(-z^{56}+x)\,(-z^{57}+x)\,(-z^{58}+x)\,(-z^{59}+x)\,(-z^{60}+x)\,(-z^{61}+x)\,(-z^{62}+x)\,(-z^{63}+x)\,(-z^{64}+x)\,(-z^{65}+x)\,(-z^{66}+x)\,(-z^{67}+x)\,(-z^{68}+x)\,(-z^{69}+x)\,(-z^{70}+x)\,(-z^{71}+x)\,(-z^{72}+x)\,(-z^{73}+x)\,(-z^{74}+x)\,(-z^{75}+x)\,(-z^{76}+x)\,(-z^{77}+x)\,(-z^{78}+x)\,(-z^{79}+x)\,(-z^{80}+x)\,(-z^2+x)\,(-z^3+x)\,(-z^4+x)\,(-z^5+x)\,(-z^6+x)\,(-z^7+x)\,(-z^8+x)\,(-z^9+x)\,(-z^{10}+x)\,(-z^{11}+x)\,(-z^{12}+x)\,(-z^{13}+x)\,(-z^{14}+x)\,(-z^{15}+x)\,(-z^{16}+x)\,(-z^{17}+x)\,(-z^{18}+x)\,(-z^{19}+x)\,(-z^{20}+x)\,(-z^{21}+x)\,(-z^{22}+x)\,(-z^{23}+x)\,(-z^{24}+x)\,(-z^{25}+x)\,(-z^{26}+x)\,(-z^{27}+x)\,(-z^{28}+x)\,(-z^{29}+x)\,(-z^{30}+x)\,(-z^{31}+x)\,(-z^{32}+x)\,(-z^{33}+x)\,(-z^{34}+x)\,(-z^{35}+x)\,(-z^{36}+x)\,(-z^{37}+x)\,(-z^{38}+x)\,(-z^{39}+x)\,(-z^{40}+x)\,(-z^{41}+x)\,(-z^{42}+x)\,(-z^{43}+x)\,(-z^{44}+x)\,(-z^{45}+x)\,(-z^{46}+x)\,(-z^{47}+x)\,(-z^{48}+x) \quad (8)$$

Modulo the minimum polynomial, we get back x^(Q-1) - 1

```
> rem(expand(gen_z), f_root_of_unity, z);
```

$$x^{80}-1 \quad (9)$$

For the cyclotomic polynomial, the other roots are the remaining primitive roots

```
> Phi_f := 1: for i from 1 to Q-1 do
                  if igcd(i,Q-1)=1
                     then Phi_f := Phi_f * (x - z^i):
               fi: od: Phi_f;
```

$$(x-z)\,(-z^3+x)\,(-z^7+x)\,(-z^9+x)\,(-z^{11}+x)\,(-z^{13}+x)\,(-z^{17}+x)\,(-z^{19}+x)\,(-z^{21}+x)\,(-z^{23}+x)\,(-z^{27}+x)\,(-z^{29}+x)\,(-z^{31}+x)\,(-z^{33}+x)\,(-z^{37}+x)\,(-z^{39}+x)\,(-z^{41}+x)\,(-z^{43}+x)\,(-z^{47}+x)\,(-z^{49}+x)\,(-z^{51}+x)\,(-z^{53}+x)\,(-z^{57}+x)\,(-z^{59}+x)\,(-z^{61}+x)\,(-z^{63}+x)\,(-z^{67}+x)\,(-z^{69}+x)\,(-z^{71}+x)\,(-z^{73}+x)\,(-z^{77}+x)\,(-z^{79}+x) \quad (10)$$

```
> cyc_80:=rem(expand(Phi_f), f_root_of_unity, z);
```

$$cyc_80 := x^{32}-x^{24}+x^{16}-x^8+1 \quad (11)$$

Get the minimum polynomial modulo 3

```
> Factor(cyc_80) mod 3; irred := op(1,%);
```

$$(x^4+x^3+2)\,(x^4+x^3+x^2+2x+2)\,(x^4+2x+2)\,(x^4+x^3+2x^2+2x+2)\,(x^4+2x^3+x^2+x+2)\,(x^4+2x^3+2)\,(x^4+x+2)\,(x^4+2x^3+2x^2+x+2)$$

$$irred := x^4+x^3+2 \quad (12)$$

```
> g := subs(x=z,irred);
```

$$g := z^4 + z^3 + 2 \tag{13}$$

```
> Factor(irred,RootOf(g,z)) mod 3;
```

$$\left(2\,RootOf\left(_Z^4+_Z^3+2\right)^3+2\,RootOf\left(_Z^4+_Z^3+2\right)^2+x+1\right)\left(2\,RootOf\left(_Z^4+_Z^3+2\right)^3+x\right)\left(2\,RootOf\left(_Z^4+_Z^3+2\right)^3+RootOf\left(_Z^4+_Z^3+2\right)^2+RootOf\left(_Z^4+_Z^3+2\right)+x\right)\left(x+2\,RootOf\left(_Z^4+_Z^3+2\right)\right) \tag{14}$$

All powers of the modulo 3 root still have generate x^(Q-1) - 1. Therefore F_{p^n} has a multiplicative primitive root

```
> Rem(expand(gen_z),g,z) mod 3;
```

$$x^{80} + 2 \tag{15}$$

Some cyclotomic polynomials factor by formula modulo 2: 2^(3 7^i) equiv 1 mod 7^i

```
> for i from 1 to 4 do f:=CyclotomicPolynomial(7^i,x); print(i, f,
  Factor(f) mod 2); od:
```

$$1,\ x^6+x^5+x^4+x^3+x^2+x+1,\ \left(x^3+x+1\right)\left(x^3+x^2+1\right)$$
$$2,\ x^{42}+x^{35}+x^{28}+x^{21}+x^{14}+x^7+1,\ \left(x^{21}+x^{14}+1\right)\left(x^{21}+x^7+1\right)$$
$$3,\ x^{294}+x^{245}+x^{196}+x^{147}+x^{98}+x^{49}+1,\ \left(x^{147}+x^{49}+1\right)\left(x^{147}+x^{98}+1\right)$$
$$4,\ x^{2058}+x^{1715}+x^{1372}+x^{1029}+x^{686}+x^{343}+1,\ \left(x^{1029}+x^{686}+1\right)\left(x^{1029}+x^{343}+1\right) \tag{16}$$

```
> for i from 1 to 4 do 8^(7^(i-1)) - 1 mod 7^i; od;
```

$$0$$
$$0$$
$$0$$
$$0 \tag{17}$$

```
>
```