Factor A(x) over Z mod 5

```
> A:=x^16+x^15+3*x^14+x^13+4*x^12+2*x^10+4*x^8+3*x^6+3*x^5+3*x^3+3*
  x^2+2;
```

$$A := x^{16} + x^{15} + 3\,x^{14} + x^{13} + 4\,x^{12} + 2\,x^{10} + 4\,x^{8} + 3\,x^{6} + 3\,x^{5} + 3\,x^{3} + 3\,x^{2} + 2$$

Check that A(x) is square-free in Z_5[x].

```
> Gcd(A,diff(A,x)) mod 5;
```

$$1$$

```
> w := x^5;
```

$$w := x^5$$

```
> f1 := Gcd(A,w-x) mod 5;
```

$$f1 := x^3 + 4\,x^2 + x + 4$$

There are three linear factors. We are left with

```
> a := Quo(A,f1,x) mod 5;
```

$$a := x^{13} + 2\,x^{12} + 4\,x^{11} + 4\,x^{10} + x^{9} + x^{8} + x^{7} + x^{6} + 4\,x^{3} + 2\,x^{2} + 3\,x + 3$$

Now compute $w = Rem\left(x^{5^2}, a, x\right)$ **mod** $5 = Rem\left(w^5, a, x\right)$ **mod** 5 using Powmod

```
> w := Powmod(w,5,a,x) mod 5;
```

$$w := x^{11} + x^{10} + 3\,x^{9} + 4\,x^{8} + 3\,x^{5} + 4\,x^{4} + 3\,x^{3} + x^{2} + x + 3$$

```
> f2 := Gcd(a,w-x) mod 5;
```

$$f2 := x^2 + x + 2$$

There is one quadratic factor. We are left with

```
> a := Quo(a,f2,x) mod 5;
```

$$a := x^{11} + x^{10} + x^{9} + x^{8} + 3\,x^{7} + x^{6} + 4\,x^{5} + 2\,x^{3} + 3\,x^{2} + 2\,x + 4$$

Now compute $w = Rem\left(x^{5^3}, a, x\right)$ **mod** $5 = Rem\left(w^5, a, x\right)$ **mod** 5 using Powmod

```
> w := Powmod(w,5,a,x) mod 5;
```

$$w := 4\,x^{10} + 4\,x^{9} + 4\,x^{8} + 3\,x^{7} + 3\,x^{5} + x^{3} + 4\,x^{2} + 2\,x$$

```
> f3 := Gcd(a,w-x) mod 5;
```

$$f3 := x^6 + x^5 + x^4 + x^3 + 4\,x^2 + x + 4$$

There are two cubic factors. We are left with

```
> a := Quo(a,f3,x) mod 5;
```

$$a := x^5 + 4x + 1$$

which has no linear, quadratic or cubic factors so must be irreducible. Thus the distinct degree factorizaton of A is given by

```
> A = f1*f2*f3*a;
```

$$x^{16} + x^{15} + 3x^{14} + x^{13} + 4x^{12} + 2x^{10} + 4x^8 + 3x^6 + 3x^5 + 3x^3 + 3x^2 + 2 = (x^3 + 4x^2 + x + 4)(x^2 + x + 2)(x^6 + x^5 + x^4 + x^3 + 4x^2 + x + 4)(x^5 + 4x + 1)$$

The three linear factors split as follows: first we try $\alpha = 1$.

```
> w := Powmod( (x+1), 2, f1, x ) mod 5;
```

$$w := x^2 + 2x + 1$$

```
> h := Gcd(f1,w+1) mod 5;
```

$$h := x^2 + 2x + 2$$

```
> f1 := Quo(f1,h,x) mod 5;
```

$$f1 := x + 2$$

```
> w := Powmod( (x+2), 2, h, x ) mod 5;
```

$$w := 2x + 2$$

```
> Gcd( h, w+1) mod 5;
```

$$x + 4$$

```
> f1 := f1 * (x+4) * Quo(h,x+4,x) mod 5;
```

$$f1 := (x + 2)(x + 4)(x + 3)$$

It remains to split f3 into two cubic factors.

```
> f3;
```

$$x^6 + x^5 + x^4 + x^3 + 4x^2 + x + 4$$

```
> v := (x^3+x+1);
  w := Powmod(v,(5^3-1)/2,f3,x) mod 5;
  g := Gcd(w+1,f3) mod 5;
```

$$v := x^3 + x + 1$$

$$w := 4$$

$$g := x^6 + x^5 + x^4 + x^3 + 4x^2 + x + 4$$

This choice $v(x) = x^3 + x + 1$ did not work as we did not split f3. Thus we try another value for v of the form $v(x) = x^3 + \alpha x^2 + \beta x + \gamma$ where α, β, γ are chosen from Z_5.

```
> v := (x^3+x+2);
  w := Powmod(v,(5^3-1)/2,f3,x) mod 5;
```

```
g := Gcd(w+1,f3) mod 5;
```

$$v := x^3 + x + 2$$

$$w := x^4 + 2x^3 + x^2 + x + 2$$

$$g := x^3 + x + 4$$

```
> f3 := g*Quo(f3,g,x) mod 5;
```

$$f3 := (x^3 + x + 4)(x^3 + x^2 + 1)$$

Thus the complete factorization is given by 3 lines, 1 quadratic, 2 cubics, one quintic.

```
> f1*f2*f3*a;
```

$$(x + 2)(x + 4)(x + 3)(x^2 + x + 2)(x^3 + x + 4)(x^3 + x^2 + 1)(x^5 + 4x + 1)$$

```
> Factor(A) mod 5;
```

$$(x + 2)(x + 4)(x + 3)(x^2 + x + 2)(x^3 + x + 4)(x^3 + x^2 + 1)(x^5 + 4x + 1)$$