```
> p := 11;
```

$$p := 11 \tag{1}$$

```
> d := 5; # d := 10;
```

$$d := 5 \tag{2}$$

```
> f1 := Randprime(d,x) mod p;
```

$$f1 := x^5 + 3x^4 + 2x^3 + 3x^2 + 9x + 1 \tag{3}$$

```
> f2 := Randprime(d,x) mod p;
```

$$f2 := x^5 + 3x^4 + 2x^3 + 6x^2 + 10x + 2 \tag{4}$$

```
> a := Expand(f1*f2) mod p;
```

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

```
> Gcd( x^p-x, a ) mod p;
```

$$1 \tag{6}$$

```
> st := time();
  for k to 5 do
      x^(p^k)-x, GCD = Gcd( a, x^(p^k)-x ) mod p;
  od;
  time()-st;
```

$$st := 60.626$$

$$x^{11} - x,\ GCD = 1$$

$$x^{121} - x,\ GCD = 1$$

$$x^{1331} - x,\ GCD = 1$$

$$x^{14641} - x,\ GCD = 1$$

$$x^{161051} - x,\ GCD = x^{10} + 6x^9 + 2x^8 + 10x^7 + 6x^6 + x^5 + 10x^4 + 2x^3 + 3x^2 + 6x + 2$$

$$0.028 \tag{7}$$

Use $gcd\left(x^{(p^k)} - x, a\right) = gcd\left(\left(x^{(p^k)} \bmod a\right) - x, a\right)$

```
> st := time():
  w := x;
  for k to d do
      w := Rem( w^p, a, x ) mod p;
      print( GCD = Gcd(a,w-x) mod p );
  od:
  time()-st;
```

$$w := x$$

$$GCD = 1$$

$$GCD = 1$$

$$GCD = 1$$

$$GCD = 1$$

$$GCD = x^{10} + 6x^9 + 2x^8 + 10x^7 + 6x^6 + x^5 + 10x^4 + 2x^3 + 3x^2 + 6x + 2$$

$$0.014 \tag{8}$$

To split use $gcd\left(v^{\frac{(p^k-1)}{2}} - 1, a\right)$

```
> k := 5;
```

$$k := 5 \tag{9}$$

```
> v := Randpoly(k,x) mod p;
```

$$v := 4x^5 + 10x^4 + 4x^3 + 4x^2 + 10x + 10 \quad (10)$$

```
> v^((p^k-1)/2)-1;
```

$$\left(4x^5 + 10x^4 + 4x^3 + 4x^2 + 10x + 10\right)^{80525} - 1 \quad (11)$$

```
> w := Powmod( v, (p^k-1)/2, a, x ) mod p;
```

$$w := 6x^9 + 8x^8 + 9x^7 + 6x^6 + 2x^5 + 5x^4 + 3x^3 + 8x^2 + 4x + 1 \quad (12)$$

```
> g := Gcd( a, w-1 ) mod p;
```

$$g := x^5 + 3x^4 + 2x^3 + 3x^2 + 9x + 1 \quad (13)$$

```
> Divide(a,g,'f') mod p;
```

$$true \quad (14)$$

```
> f;
```

$$x^5 + 3x^4 + 2x^3 + 6x^2 + 10x + 2 \quad (15)$$

```
> good := 0:
  n := 100:
  to n do
     v := Randpoly(k,x) mod p;
     w := Powmod( v, (p^k-1)/2, a, x ) mod p;
     g := Gcd(a,w-1) mod p;
     if degree(g)=k then good += 1; fi;
  od:
  good;
```

$$55 \quad (16)$$