```
alea := proc(n, p)
 local a, b, i:
 a := 0:
 b := rand(0..p - 1):
 for i from 0 to n - 1 do a := a + b( )·x^i :od:
 a;
 end:

 alea(4, 3);
```

$$2 + 2\,x^3 \tag{1}$$

```
dist := proc(f, p)
 local a, b, g, A, i:
 a := x: b := f: A := NULL: i := 1:
 while b ≠ 1 do a := powmod(a, p, f, x) mod p: g := Gcd(a - x, b) mod p: b := quo(b, g, x)
     mod p :if degree(g, x) ≥ 1 then A := A, g, i :fi: i := i + 1 :od:
 A;
 end:

P := expand(x(x + 1)·(x^2 + 4)(x^2 + x + 2));
```

$$x^6 + 2\,x^5 + 7\,x^4 + 10\,x^3 + 12\,x^2 + 8\,x \tag{2}$$

```
dist(P, 3);
```

$$x^2 + x,\ 1,\ x^4 + x^3 + x + 2,\ 2 \tag{3}$$

```
Cantor := proc(f, p, d)
 local a, g, b:
 a := alea(degree(f, x), p) :if degree(a, x) ≤ 0 then return 0 :fi:
 g := Gcd(a, f) mod p:
if degree(g, x) ≥ 1 then return(g);
 else b := powmod(a, (p^d - 1)/2, f, x) mod p: b := rem(b - 1, f, x):
 g := Gcd(b, f) mod p :if g ≠ f and g ≠ 1 then return(g);else return(0) :fi:
 fi:
 end:

Cantor(x^4 + x^3 + x + 2, 3, 2);
```

$$x^2 + x + 2 \tag{4}$$

```
Cantor(x + 1, 3, 1);
```

$$0 \tag{5}$$

```
irr := proc( f, p, k, d )
 local j, b;
 j := 0 : b := 0 :
 while j < k and b = 0 do j := j + 1 : b := Cantor( f, p, d ) : od:
 if j = k then return 1 :
 else return b :
 fi:
 end:
```

```
irr( x^3 + 1, 3, 5, 1 );
```

$$x + 1 \tag{6}$$

```
decomp := proc( f, p, k, d )
 local A, g, a, b :
 A := NULL :
g := f:
 while g ≠ 1 do
 a := irr( g, p, k, d ) : b := g :
 while a ≠ 1 do b := a mod p : a := irr( b, p, k, d ) :od:
 g := quo( g, b, x ); A := A, b :od:
 return( A );
 end:
```

```
decomp( x^4 + x^3 + x + 2, 3, 5, 2 );
```

$$x^2 + 1,\ x^2 + x - 1 \tag{7}$$

```
fac := proc( f, p, k )
 local A, z, B, i, n :
 B := NULL : g := f:
z := Gcd( g, g' ) mod p :
if z ≠ 1 then B := B, z : return B, fac( quo( f, z, x ), p, k );
else A := dist( f, p ) :
 n := nops( [ A ] ) :
 for i from 1 to n - 1 by 2 do B := B, decomp( A[ i ], p, k, A[ i + 1 ] ) :od:
 fi:
 return( B );
 end:
```

```
fac( x^6 + 2 x^5 + 7 x^4 + 10 x^3 + 12 x^2 + 8 x, 3, 5 );
```

$$x, x+1, x^2+x+2, x^2+1 \tag{8}$$

$alea(9, 5);$

$$4 + x + 2x^2 + 4x^3 + 4x^4 + 2x^5 + 3x^6 + 4x^8 \tag{9}$$

$fac(1 + 2x + 3x^2 + 4x^3 + 3x^5 + x^7, 5, 5);$

$$x^2 + 2x + 3, x^2 - x + 2, x^3 + 4x^2 + x + 1 \tag{10}$$

$expand((x-1)^2 \cdot (x+1)) \bmod 3;$

$$2x + 1 + 2x^2 + x^3 \tag{11}$$

$fac(x^3 + 2x^2 + 2x + 1, 3, 5);$

$$2 + x, x + 1, -1 + x \tag{12}$$

$fac(x^3 - 1, 3, 5);$

$$2 + x^3 \tag{13}$$

$alea(13, 7, 5);$

$$6 + 6x + x^2 + x^3 + 6x^4 + 2x^5 + 4x^6 + 5x^7 + 3x^{10} + 5x^{11} + x^{12} \tag{14}$$

$fac(x + 4x^3 + 2x^4 + x^5 + x^6 + x^7, 7, 5);$

$$x, 2 + x, x^2 + 4x + 5, x^3 + 2x^2 + 4x + 5 \tag{15}$$

```
rac := proc(f, p)
 local n, i, z, g, u :
 n := degree(f, x) :
  z := unapply(f, x) : g := z(0) : u := z(0) :

 for i from p to n by p do z := unapply(quo(f - u, x^i, x), x) : g := g + z(0)·x^(i/p) : u := u + z(0)x^i :
     od:
 g;
 end:
```

$rac(x^3 - 1, 3);$ $rac(x^6 + 2x^3 + 1, 3);$

$$-1 + x$$

$$1 + 2x + x^2 \tag{16}$$