```
1  restart;maple_mode(1);cas_setup(0,0,0,1,0,1e-10,10,[1,50,0,25],0,0,0); #radians,pas de cmplx, pas de  Sqrt
```

```
2  rem(x^2+2*x+2,x^2+1);
```

$$2 \cdot x + 1$$

```
3  rem([1,2,2],[1,0,1]);
```

$$[|2 \quad 1 \ |]$$

```
4  rem(X^2+2*X+2,X^2+1); #X ne marche pas, il le fait en x. On pourra utiliser ,X
```

$$0$$

```
5  ----------Methode de Berlkamp----------
```

```
6  sum(rand(20)*x^i,i=0..n);  #sum,mul,add evaluent le random avant!
```

$$\frac{19 \cdot x^{n+1}}{x-1} - \left(\frac{19}{x-1}\right)$$

```
7  randP:=n->poly2symb([1,seq(rand(20),i=0..n-1)],x);
// Warning: i x  declared as global variable(s)
// End defining randP
```

$$n \quad \text{->} \quad \text{poly2symb}([1 \quad \text{seq}(\text{rand}(20), i = (0 \ldots (n - 1))) \ ], x)$$

```
8  P:=expand(mul([seq(randP(rand(7)),i=1..5)])); #on met un seq pour avoir des rand differents
```

```
9  gcd(P,diff(P,x)); #Pour berlekamp, il ne faut pas de facteurs multiples.
```

$$1$$

```
10 Attention {'a} la bonne instruction pour trouver un noyau mod p. Prendre la forme
   inerte: Nullspace. De plus, il faut aussi faire attention pour les
   coefficients des polynomes, on les veut tous jusque degree(P)-1 meme si leur
   degr{'e} est plus petit.
```

```
11 berl:=proc(p,PP)
   local L,tmp,i,j,F;
   L:=[];
   if degree(Gcd(PP,diff(PP,x)) mod p) =0 then
   for i from 0 to degree(PP) - 1 do
   tmp:=powmod(x,i*p,p,PP,x); #On utilise la puissance rapide
   tmp:=Rem(tmp-x^i,PP) mod p;
   l:=[seq(coeff(tmp,x,j),j=0..degree(PP)-1)];
   L:=[op(L),l];
   od:
   F:=transpose(L);Nullspace(F) mod p;
   else print("facteurs multiples"); [[0]] fi;
// Warning: x l  declared as global variable(s)
// End defining berl
```

```
proc(p,PP)
  local L,tmp,i,j,F;
  L:=[];
  if degree(irem(Gcd(PP,diff(PP,x)),p))=0 then
    for i from 0 to degree(PP)-1+1/2 do
    tmp:=powmod(x,i*p,p,PP,x);
    tmp:=irem(Rem(tmp-x^i,PP),p);
    l:=[seq(coeff(tmp,x,j),j=(0 .. (degree(PP)-1)))];
    L:=[op(L),l];
     od;;
    F:=transpose(L);
    irem(Nullspace(F),p) else
    print("facteurs multiples");
    [[0]]
  fi ;
```

12 p:=1:L:=[];for i from 1 to 10 do
p:=nextprime(p):L:=[op(L),[rowdim(berl(p,P)),p,Factor(P) mod p]] od;

"facteurs multiples"
"facteurs multiples"
"facteurs multiples"
"facteurs multiples"
"facteurs multiples"
"facteurs multiples"
"facteurs multiples"
Evaluation time: 0.539062

Done, [],

1	3	$(x+1)\cdot(x^2+x-1)\cdot(x^2-x-1)\cdot(x^2+1)\cdot x^3\cdot(x-1)^3$
1	5	$x\cdot(x+2)\cdot(x^2-x+2)\cdot(x^3-2\cdot x^2-x-2)\cdot(x^4+2\cdot x^3+2\cdot x^2+1)\cdot(x+1)^2$
1	7	$(x-1)\cdot(x-2)\cdot(x^2-3\cdot x+1)\cdot(x^3+3\cdot x^2-3\cdot x+3)\cdot(x^4+3\cdot x^3-3)\cdot(x+1)^2$
1	11	$(x-5)\cdot(x+1)\cdot(x-1)\cdot(x+4)\cdot(x^2+4\cdot x-3)\cdot(x^2-5\cdot x-4)\cdot(x^3+5\cdot x^2-3)\cdot x^2$
8	13	$(x+2)\cdot(x-6)\cdot(x+6)\cdot(x-2)\cdot(x+1)\cdot(x^2-4\cdot x+6)\cdot(x^2+5\cdot x-3)\cdot(x^4+4\cdot x^3-6\cdot x^2-2)$
1	17	$(x+6)\cdot(x+7)\cdot(x-5)\cdot(x-2)\cdot(x+3)\cdot(x^2-4\cdot x-2)\cdot(x^4+7\cdot x^2-6)\cdot(x+1)^2$
1	19	$(x+3)\cdot(x-4)\cdot(x+6)\cdot(x+1)\cdot(x-3)\cdot(x-9)\cdot(x^2+4\cdot x+1)\cdot(x^3+3\cdot x^2+4\cdot x+3)\cdot x^2$
9	23	$(x+6)\cdot(x-8)\cdot(x+1)\cdot(x-3)\cdot(x+7)\cdot(x^2-10\cdot x+4)\cdot(x^2+4\cdot x-3)\cdot(x^2+9\cdot x+6)\cdot(x^2+6\cdot x-1)$
8	29	$(x+4)\cdot(x-14)\cdot(x+1)\cdot(x+6)\cdot(x^2-x+12)\cdot(x^2-x+8)\cdot(x^2-11\cdot x+13)\cdot(x^3-13\cdot x^2-10)$
		$(1\cdot x-11)\cdot(1\cdot x+15)\cdot(1\cdot x+6)\cdot(1\cdot x-2)\cdot(1\cdot x+1)\cdot(1\cdot x^2+(-4)\cdot x-13)\cdot$

Menu

13 Non, il peut y avoir moins de facteurs dans Z.

14 p:=23; Gcd(P,diff(P,x)) mod p;

(23, 1)

Menu

15 N:=berl(p,P);LX:=[seq(x^(j-1),j=1..degree(P))];

$$\begin{pmatrix} -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 8 & 8 & -3 & -4 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 9 & -5 & -1 & -6 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 5 & 6 & 4 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -7 & -8 & -7 & 10 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 10 & 3 & 8 & -2 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & -1 & -9 & -10 & 1 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & -11 & 10 & -2 & -2 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \end{pmatrix}, [1 \quad x \quad x^2 \quad x^3 \quad x^4 \quad x^5 \quad x^6 \quad x^7 \quad x^8$$

Menu

16 Q:=(LX*N[2]);

2 3 4 5

17 Rem(powmod(Q,p,p,P,x)-Q,P) mod p; # verification:

$$0$$

18 Gcd(Q,P) mod p; #l'un des 3 pgcd est non trivial:

$$1 \cdot x^{2} + (-2) \cdot x - 3$$

19 A:=Rem(powmod(Q,(p-1)/2,p,P,x)-1,P) mod p;

$$3 \cdot x^{12} + 11 \cdot x^{11} + 5 \cdot x^{10} + 3 \cdot x^{9} + (-8) \cdot x^{8} + (-3) \cdot x^{7} + 9 \cdot x^{6} + (-6) \cdot x^{5} + (-11) \cdot x^{4} + 10 \cdot x^{3} + (-7) \cdot x + 9$$

20 Gcd(A,P) mod p;

$$1 \cdot x^{5} + (-3) \cdot x^{4} + (-8) \cdot x^{3} + (-6) \cdot x^{2} + 7 \cdot x - 11$$

21 B:=Rem(powmod(Q,(p-1)/2,p,P,x)+1,P) mod p;

$$3 \cdot x^{12} + 11 \cdot x^{11} + 5 \cdot x^{10} + 3 \cdot x^{9} + (-8) \cdot x^{8} + (-3) \cdot x^{7} + 9 \cdot x^{6} + (-6) \cdot x^{5} + (-11) \cdot x^{4} + 10 \cdot x^{3} + (-7) \cdot x + 11$$

22 Gcd(B,P) mod p;

$$1 \cdot x^{6} + (-6) \cdot x^{5} + (-5) \cdot x^{4} + (-5) \cdot x^{3} + (-4) \cdot x^{2} + 9 \cdot x + 8$$

23
```
unfacteur:=proc(d)
i:=1;
A:=1;B:=1;rep:=1;
r:=[seq(rand(p),i=1..rowdim(N))]*N; #un element du noyau au hasard
Q:=(LX*r);
#On fait 3 essais;
A:=Gcd(Q,d) mod p;
if degree(A)*(degree(A)-degree(d))<>0 then rep:=A ;
else A:=Rem(powmod(Q,(p-1)/2,p,P,x)-1,P) mod p;
A:=Gcd(A,d) mod p;
if degree(A)*(degree(A)-degree(d))<>0 then rep:=A ;
else A:=Rem(Powmod(Q,(p-1)/2,p,P,x)+1,P) mod p;
A:=Gcd(A,d) mod p;
if degree(A)*(degree(A)-degree(d))<>0 then rep:=A fi;
fi;
fi;
if degree(rep)=0 then d else rep  fi;
```

```
// Warning: i A B rep N p r LX Q P x Powmod  declared as global variable(s)
// End defining unfacteur
```

```
proc(d)
  i:=1;
  A:=1;
  B:=1;
  rep:=1;
  r:=[seq(rand(p),i=(1 .. (rowdim(N))))]*N;
  Q:=LX*r;
  A:=irem(Gcd(Q,d),p);
  if (degree(A)*(degree(A)-degree(d)))<>0 then
    rep:=A else
    A:=irem(Rem(powmod(Q,(p-1)/2,p,P,x)-1,P),p);
    A:=irem(Gcd(A,d),p);
    if (degree(A)*(degree(A)-degree(d)))<>0 then
      rep:=A else
      A:=irem(Rem(Powmod(Q,(p-1)/2,p,P,x)+1,P),p);
      A:=irem(Gcd(A,d),p);
      if (degree(A)*(degree(A)-degree(d)))<>0 then
        rep:=A
      fi
    fi
  fi ;
  if degree(rep)=0 then
    d else
    rep
  fi ;

end;
```

24 unfacteur(P);

$$6 \qquad 5 \qquad 4 \qquad 3 \qquad 2$$

```
25 facteurpseudoirred:=proc(d)
   t:=unfacteur(d);
   tt:=d;
   while (degree(t)<degree(tt)) do tt:=t;t:=unfacteur(t); od;
   t;
   end;
// Warning: t unfacteur tt  declared as global variable(s)
// End defining facteurpseudoirred
```

```
proc(d)
  t:=unfacteur(d);
  tt:=d;
  while (degree(t))<(degree(tt)) do
    tt:=t;
    t:=unfacteur(t);
   od;;
  t;

end;
```

Menu

```
26 f:=facteurpseudoirred(P);
```

$$1 \cdot x^2 + 4 \cdot x - 3$$

Menu

```
27 Si le noyau est de dim 1, f est irreductible.
```

```
28 if (rowdim(berl(p,f))==1) then print ("f est irred") fi;
"f est irred"
```

1

Menu

```
29 T:=P;a:=1;L:=[];
while degree(T)>0 do T:=Quo(T,a) mod p;L:=[op(L),a];a:=facteurpseudoirred(T); od:L;
```

$$x^{13} + 58 \cdot x^{12} + 1285 \cdot x^{11} + 13593 \cdot x^{10} + 71850 \cdot x^9 + 202209 \cdot x^8 +$$
$$[\ 376272 \cdot x^7 + 532251 \cdot x^6 + 590684 \cdot x^5 + 545681 \cdot x^4 + 411743 \cdot x^3 + 246450 \cdot x^2 + 144837 \cdot x + 56430,\ 1,\ [\ ]\ ]$$

Don
Menu

```
30 Le nombre de facteurs doit etre la dim de ker F, on teste si l'on a
   trouve tous les facteurs ainsi:
```

```
31 if nops(N)==(nops(L)-1) then print("on a bien trouve tous les facteurs") fi;
```

undef

Menu

```
32 ------------------------------------------------------------
```

```
33 purge(a,b,c,d,e);
```

(1, b not assigned , c not assigned , d not assigned , e not assigned)

Menu

```
34 P:=a*b^2*c^3*d^4*e^6;
```

$$a \cdot b^2 \cdot c^3 \cdot d^4 \cdot e^6$$

Menu

```
35 Q:=a*b*d; #Q est P divise par le pgcd de P et P'
```

$$a \cdot b \cdot d$$

Menu

```
36 T1:=P;V1:=Q;
```

$$(\ a \cdot b^2 \cdot c^3 \cdot d^4 \cdot e^6,\ a \cdot b \cdot d\ )$$

Menu

```
37 V2:=gcd(T1,V1);T2:=normal(T1/V2);
```

$$(\ a \cdot b \cdot d,\ b \cdot c^3 \cdot d^3 \cdot e^6\ )$$

Menu

```
38 V3:=gcd(T2,V2);T3:=normal(T2/V3);normal(V2/V3); #on obtient a
```

$$(\ b \cdot d,\ c^3 \cdot d^2 \cdot e^6,\ a\ )$$

Menu

```
39 V4:=gcd(T3,V3);T4:=normal(T3/V4);normal(V3/V4); #on obtient b
```

$$(\ d,\ c^3 \cdot d \cdot e^6,\ b\ )$$

Menu

```
40 V5:=gcd(T4,V4);T5:=normal(T4/V5);normal(V4/V5); #on obtient d
```

$$(\ d,\ c^3 \cdot e^6,\ 1\ )$$

Menu

```
41 On a obtenu le polynome T5=c^3e^6. Ce polynome en n'est autre que
   Q(x^3) ou Q=c.e^2. On recommence alors avec Q. (On obtient  c.e
   en divisant Q par le pgcd de Q et Q').
```

```
42 T6:=c*e^2;V6:=c*e;
```

43 V7:=gcd(T6,V6);T7:=normal(T6/V7);

$(c \cdot e,\ e)$

44 V8:=gcd(T7,V7);T8:=normal(T7/V8);normal(V7/V8); #on obtient c

$(e,\ 1,\ c)$

45 V9:=gcd(T8,V8);normal(V8/V9); #on obtient e

$(1,\ e)$

46

47 Prog Edit Add | nxt | OK | Save

```
facto1:= proc(P,p)
local VV,T,V,k,L;
T:=Gcd(P,diff(P,x)) mod p;
V:=Quo(P,T) mod p; #Attention, il faut    faire  les divisions modp
V:=Gcd(P,V) mod p;T:=Quo(P,V) mod p;
L:=[];
k:=1;
while degree(V) > 0  do
VV:=V;V:=Gcd(T,V) mod p; T:=Quo(T,V) mod p;
if degree(V)<degree(VV)   then L:=[op(L),[Quo(VV,V) mod p,k]];    fi;
k:=k+1;
od;
```

```
// Warning: x  declared as global variable(s)
// End defining facto1
```

```
proc(P,p)
  local VV,T,V,k,L;
  T:=irem(Gcd(P,diff(P,x)),p);
  V:=irem(Quo(P,T),p);
  V:=irem(Gcd(P,V),p);
  T:=irem(Quo(P,V),p);
  L:=[];
  k:=1;
  while (degree(V))>0 do
    VV:=V;
    V:=irem(Gcd(T,V),p);
    T:=irem(Quo(T,V),p);
    if (degree(V))<(degree(VV)) then
      L:=[op(L),[irem(Quo(VV,V),p),k]]
    fi ;
    k:=k+1;
   od;;
  L;

end;
```

48 Factor(x^49-x) mod 7; #On cherche des facteurs irred de degre 2 distincts pour connaitre la reponse.

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

49 P:=normal((x+1)*(x^2-2*x+1)^2*(x+2)^3*(x^2+3*x-2)^3*x^7*(x^2-x-3)^7*(x^2-x-1)^9*(x^2-2*x-2)^14) mod 7;

$$x^{81}+3 \cdot x^{80}+5 \cdot x^{79}+4 \cdot x^{78}+4 \cdot x^{77}+4 \cdot x^{75}+3 \cdot x^{74}+4 \cdot x^{73}+3 \cdot x^{71}+5 \cdot x^{70}+6 \cdot x^{69}+6 \cdot x^{68}+x^{67}+5 \cdot x^{66}+2 \cdot x$$
$$x^{54}+6 \cdot x^{52}+5 \cdot x^{51}+x^{50}+3 \cdot x^{49}+4 \cdot x^{48}+4 \cdot x^{47}+6 \cdot x^{45}+6 \cdot x^{44}+x^{43}+6 \cdot x^{42}+4 \cdot x^{41}+5 \cdot x^{40}+5 \cdot x^{39}+4 \cdot x^{38}$$
$$4 \cdot x^{26}+3 \cdot x^{24}+6 \cdot x^{23}+4 \cdot x^{22}+5 \cdot x^{21}+2 \cdot x^{20}+2 \cdot x^{19}+x^{18}+6 \cdot x^{17}+x^{16}+x^{15}+2 \cdot x^{13}+3 \cdot x^{12}+5 \cdot x^{11}+x^{10}+5 \cdot$$

50 Factor(P) mod 7; #On verifie que nos facteurs sont bien premiers entre eux.

51 facto1(P,7);

$$\begin{bmatrix} 1 \cdot x+1 & 1 \\ 1 \cdot x^3+(-2) \cdot x^2+(-3) \cdot x+3 & 3 \\ 1 \cdot x-1 & 4 \\ 1 \cdot x^2+(-1) \cdot x-1 & 9 \end{bmatrix}$$

52

53 Prog Edit Add | nxt | OK | Save

```
facto2:= proc(P,p)
local VV,T,V,k,L,j;
T:=Gcd(P,diff(P,x)) mod p;
V:=Quo(P,T) mod p; #Attention, il faut    faire  les divisions modp
T:=Quo(P,V) mod p;
L:=[];
k:=1;j:=1
while degree(T)>0  do
while degree(V) > 0  do
VV:=V;V:=Gcd(T,V) mod p; T:=Quo(T,V) mod p;
if degree(V)<degree(VV)   then L:=[op(L),[Quo(VV,V) mod p,k]];    fi;
k:=k+j;
od;
//Attention pour poly2symb les coeffs sont dans l'ordre des degres decroissant
j:=j*p;k:=j;T:=poly2symb([seq(coeff(T,i*p),i=degree(T)/p..1)],x);
V:=Quo(T,Gcd(T,diff(T,x)) mod p) mod p;
T:=Quo(T,V) mod p;
od;
L;
```

```
// Warning: x i  declared as global variable(s)
// End defining facto2
```

```
proc(P,p)
  local VV,T,V,k,L,j;
  T:=irem(Gcd(P,diff(P,x)),p);
  V:=irem(Quo(P,T),p);
  T:=irem(Quo(P,V),p);
  L:=[];
  k:=1;
  j:=1;
  while (degree(T))>0 do
    while (degree(V))>0 do
      VV:=V;
      V:=irem(Gcd(T,V),p);
      T:=irem(Quo(T,V),p);
      if (degree(V))<(degree(VV)) then
        L:=[op(L),[irem(Quo(VV,V),p),k]]
      fi ;
      k:=k+j;
     od;;
    j:=j*p;
    k:=j;
    T:=poly2symb([seq(coeff(T,i*p),i=(((degree(T))/p) .. 1))],x);
    V:=irem(Quo(T,irem(Gcd(T,diff(T,x)),p)),p);
    T:=irem(Quo(T,V),p);
   od;;
  L;

end;
```

Menu

54 facto2(P,7);

$$\begin{bmatrix} 1\cdot x+1 & 1 \\ 1\cdot x^3+(-2)\cdot x^2+(-3)\cdot x+3 & 3 \\ 1\cdot x-1 & 4 \\ 1\cdot x^2+(-1)\cdot x-1 & 9 \\ 1\cdot x^2+(-1)\cdot x-3 & 7 \\ 1\cdot x^2+(-2)\cdot x-2 & 14 \end{bmatrix}$$

Menu

55