

Polynominimal

```
v:=seq(ii,ii=1..8);
```

```
[1, 2, 3, 4, 5, 6, 7, 8]
```

```
poly2symb(v,x);
```

```
x*(x*(x*(x*(x*(x*(x+2)+3)+4)+5)+6)+7)+8
```

```
revlist(v);
```

```
[8, 7, 6, 5, 4, 3, 2, 1]
```

```
P:=x^2+1;LP:=[1,0,1];
```

```
(x2+1, [1, 0, 1])
```

```
subst(P,x=sqrt(2));
```

```
3
```

```
unapply(P,x)(sqrt(2)); //c'est preferable et plus Ex pour creer une fonction
```

```
3
```

```
peval(LP,sqrt(2));
```

```
3
```

```
n:=8;v:=seq(ii,ii=1..n); A:=matrix(n,n,(i0,j0)-> rand(20)-10);
```

```
// Succès
```

```
( Done, [1, 2, 3, 4, 5, 6, 7, 8 ],
```

```
4, 4, 8, 4, 5, -7, -3, 7  
-9, -2, 7, -5, -3, -3, 2, -3  
-5, -9, 8, 0, -2, 1, 6, 7  
-8, -8, 8, -3, -9, 8, -9, 5  
-1, 6, 4, -5, -6, -7, 8, 3  
4, -3, 9, 8, 5, -7, 9, -4  
-7, 3, 4, 9, -4, -3, 3, -1  
-5, -5, 1, -6, 3, 7, 8, -3
```

```
B:=v; AA:=v;
```

```
([1, 2, 3, 4, 5, 6, 7, 8 ], [1, 2, 3, 4, 5, 6, 7, 8 ] )
```

```
for(ii:=1;ii<=n;ii++){ AA:=A*AA;B:=B,AA; }
```

```
[1, 2, 3, 4, 5, 6, 7, 8 ], [70, -55, 95, -32, 11, 71, 22, 53 ], [555, -56, 1457, 1272, -88, 588,
```

```
N:=ker(transpose([B]))[0];
```

```
[411308636, 66716599, 4955921, -69820, -11701, 2593, -177, -6, -1]
```

Attention, les polynômes commencent a la puissance maximale, il faut inverser l'ordre

```
undef
```

```
P:=poly2symb(revlist(N),x); // forme de Horner
```

16 `normal (subst (P,x=A)); // on substitue x par A et on developpe avec normal`

0, 0, 0, 0, 0, 0, 0, 0, 0
0, 0, 0, 0, 0, 0, 0, 0, 0
0, 0, 0, 0, 0, 0, 0, 0, 0
0, 0, 0, 0, 0, 0, 0, 0, 0
0, 0, 0, 0, 0, 0, 0, 0, 0
0, 0, 0, 0, 0, 0, 0, 0, 0
0, 0, 0, 0, 0, 0, 0, 0, 0
0, 0, 0, 0, 0, 0, 0, 0, 0

17 `P:=sum(N[j]*x^j,j,0,length(N)-1); // ou bien on cree P simplement.`

$-x^8 - 6x^7 - 177x^6 + 2593x^5 - 11701x^4 - 69820x^3 + 4955921x^2 + 66716599x + 411308636$

18 `unapply (P,x) (A); // on cree la fonction de x a partir de symbole P via unapply`

0, 0, 0, 0, 0, 0, 0, 0, 0
0, 0, 0, 0, 0, 0, 0, 0, 0
0, 0, 0, 0, 0, 0, 0, 0, 0
0, 0, 0, 0, 0, 0, 0, 0, 0
0, 0, 0, 0, 0, 0, 0, 0, 0
0, 0, 0, 0, 0, 0, 0, 0, 0
0, 0, 0, 0, 0, 0, 0, 0, 0
0, 0, 0, 0, 0, 0, 0, 0, 0

19 `A:=diag (companion (x^4-1,x), companion ((x^2-1)^2,x)); // un exemple non cyclique`

0, 0, 0, 1, 0, 0, 0, 0
1, 0, 0, 0, 0, 0, 0, 0
0, 1, 0, 0, 0, 0, 0, 0
0, 0, 1, 0, 0, 0, 0, 0
0, 0, 0, 0, 0, 0, 0, -1
0, 0, 0, 0, 1, 0, 0, 0
0, 0, 0, 0, 0, 1, 0, 2
0, 0, 0, 0, 0, 0, 1, 0

20 `B:=v; AA:=v;`

`([1, 2, 3, 4, 5, 6, 7, 8], [1, 2, 3, 4, 5, 6, 7, 8])`

21 `for (ii:=1;ii<=n;ii++){ AA:=A*AA;B:=B,AA; }`

`[1, 2, 3, 4, 5, 6, 7, 8], [4, 1, 2, 3, -8, 5, 22, 7], [3, 4, 1, 2, -7, -8, 19, 22], [2, 3, 4, 1,`

22 `nullspace (B);`

9	4	9	4
5,	5,	5,	5,
-1,	0,	-1,	0
4	9	4	9

23 `N:=nullspace(transpose([B])); // ou bien ker`

-1, 0, 1, 0, 1, 0, -1, 0, 0
0, -1, 0, 1, 0, 1, 0, -1, 0
-1, 0, 0, 0, 2, 0, 0, 0, -1

24 Pour donner une base du noyau le logiciel fait du pivot. ici il met le triangle de 0 sur la fin des coordonnées, donc notre polynome minimal est le premier vecteur de la base (dans sage c'est le contraire)

25 `N:=nullspace(transpose([B]))[0];`

-1, 0, 1, 0, 1, 0, -1, 0, 0

26 `P:=poly2symb(revlist(N),x);`

$$x^2 * (x^2 * (-x^2 + 1) + 1) - 1$$

27 `normal(subst(P,x=A));`

0, 0, 0, 0, 0, 0, 0, 0, 0
0, 0, 0, 0, 0, 0, 0, 0, 0
0, 0, 0, 0, 0, 0, 0, 0, 0
0, 0, 0, 0, 0, 0, 0, 0, 0
0, 0, 0, 0, 0, 0, 0, 0, 0
0, 0, 0, 0, 0, 0, 0, 0, 0
0, 0, 0, 0, 0, 0, 0, 0, 0
0, 0, 0, 0, 0, 0, 0, 0, 0

28

29 Prog Edit Ajouter 1 nxt Fonctions Test Boucle OK Save

```
B:=[v]; AA:=v
for(ii:=1;ii<=n;ii++){
  AA:=A*AA; B:=append(B,AA);
  B:=ref(B);
}
```

:2: syntax error, unexpected T_FOR line 2 col 1 at for

:2: syntax error, unexpected T_SEMI, expecting T_END_PAR line 2 col 10 at ;

Warning, input parsed as a constant function undef applied to undef++

:5: syntax error, unexpected T_BLOC_END line 5 col 3 at }

30 On a calculé les $A^k(v)$ par récurrence. AA est un vecteur donc $A*AA$ a un coût de n^2 , et l'on fait n tours, donc c'est en $O(n^3)$

31 Il existe toujours un vecteur v tel que $P_-(u,v)=p_{\min}(u)$, les vecteurs à éviter sont dans $\ker(P(u))$ ou P divise p_{\min} , donc nom fini despace vectoriels à éviter.

32 Méthode de Bakamp

```

33 randP(n):=ratnormal(poly2symb([1,seq(alea(20),j=0..n-1)],x));

// Interprète randP
// Attention: j,x, declared as global variable(s). If symbolic variables are required, declare them as local and
// lors de la compilation randP
^@

n -> ratnormal(poly2symb([1,seq(rand(20),j=(0..(n-1))],x))

```

```

34 randP(n):={
  local P,j;
  P:=x^n; for(j:=0;j<n;j++){P:=P+x^j*alea(20)}
  return P;
}

// Interprète randP
// Attention: x, declared as global variable(s). If symbolic variables are required, declare them as local and
// lors de la compilation randP
^@

(n)->
{ local P,j;
  P:=x^n;
  for (j:=0;j<n;j++) P:=P+x^j*alea(20); ;
  return(P);
}

```

```

35 randP(10);

x10 + x9 + 17*x8 + 18*x7 + 16*x6 + 4*x5 + 9*x4 + 13*x3 + 7*x + 11

```

```

36

x20 + 53*x19 + 1002*x18 + 7977*x17 + 25680*x16 + 54762*x15 + 151007*x14 + 306829*x13 + 492320*x12 + 648041*x11 + 797700*x10 + 891000*x9 + 891000*x8 + 797700*x7 + 648041*x6 + 492320*x5 + 306829*x4 + 151007*x3 + 54762*x2 + 25680*x + 53

```

```

37 P:=x^16+x^14+58*x^15+1386*x^14+17715*x^13+131260*x^12+578697*x^11+1538013*x^10+2648041*x^9+368740*x^8+368740*x^7+1538013*x^6+578697*x^5+131260*x^4+17715*x^3+1386*x^2+58*x+1

x16 + 58*x15 + 1387*x14 + 17715*x13 + 131260*x12 + 578697*x11 + 1538013*x10 + 2648041*x9 + 368740*x8 + 368740*x7 + 1538013*x6 + 578697*x5 + 131260*x4 + 17715*x3 + 1386*x2 + 58*x + 1

```

```

38 god(P,diff(P,x)); //Pour berlekamp, il ne faut pas de facteurs multiples.

1

```

```

39 Attention {\`a} la bonne instruction pour trouver un noyau mod p. Il ne faut PAS
que le noyau soit calcule dans Z puis la reponse reduite modulo p!!!
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.

```

40

```

local F;
supposons(x,symbol); //facultatif mais au cas ou x serait affectee
Pp:=PP % p; //la classe de P
n:=degree(Pp);
if( degree(gcd(Pp, diff(Pp,x)))==0){
    // on definit une fonction
    F(u,v):={
        local tmp;
        tmp:=powmod(x,v*p, Pp);
        return coeff(tmp-x^v,x,u)
    }
    return matrix(n,n,F);
}
};

```

// Interprète F

// Attention: x,p,Pp, declared as global variable(s). If symbolic variables are required, declare them as local
// lors de la compilation F

// Interprète berl

// Attention: x,Pp,n,p, declared as global variable(s). If symbolic variables are required, declare them as local
// lors de la compilation berl

^@^@

```

(p,PP)->
{ local F;
  supposons(x,symbol);
  Pp:=PP % p;
  n:=degree(Pp);
  if (((degree(gcd(Pp,diff(Pp,x))))==0)) {
    F:= (u,v)->
    { local tmp;
      tmp:=powmod(x,v*p,Pp);
      return(coeff(tmp-x^v,x,u));
    };
    return(matrix(n,n,F));
  }; ;
}

```

41

```

p:=1;L:=[];
for(j:=0;j<10;j++){
  p:=nextprime(p);
  // Attention si gcd(P,P') rend une constante autre que 1
  // il vaut mieux tester le degre
  if ( degree(gcd(P % p, diff(P % p,x)))==0){
    L:=[op(L),[rowdim(ker(berl(p,P))),p,factor(P % p) ]];
  }
};L;

```

```

((-1)%5+x*(1%5))*((-2%5+x*(1%5))*
(1%5+x*(2%5)+x^3*(1%5))*
((-1)%5+x*(1%5)+x^3*(1%5))*
((-1)%5+x*(2%5)+x^2*(1%5))*
(2%5+x*((-1)%5)+x^2*(1%5))*
7, 5, ((-2%5+x*((-2%5)+x^2*(1%5)+x^4*(1%5))
x*((-1)%7+x*(1%7))*((-2%7+x*(1%7))*
(3%7+x*(2%7)+x^2*(1%7))*
((-2%7+x*((-2%7)+x^2*(3%7)+x^3*(1%7)+x^5*(1%7))*
(-2%7+x*(2%7)+x^2*(3%7)+

```

1, [], Done,

$$\begin{aligned}
 & x * ((-4 \% 17 + x * (1 \% 17)) * \\
 & (6 \% 17 + x * (1 \% 17)) * ((-8 \% 17 + x * (1 \% 17)) * \\
 & ((-3 \% 17 + x * ((-5 \% 17) + x^2 * (1 \% 17)) * \\
 & ((-3 \% 17 + x * (7 \% 17) + x^2 * (1 \% 17)) * \\
 & ((-4 \% 17 + x * (6 \% 17) + x^2 * (7 \% 17) + x^3 * (1 \% 17)) * \\
 & 6 \% 17 + x * ((-8 \% 17) + x^2 * (7 \% 17) + \\
 & 8, 17, (x^3 * ((-6 \% 17) + x^4 * (4 \% 17) + x^5 * (1 \% 17)) * (1 \% 17) \\
 & ((-5 \% 29 + x * (1 \% 29)) * \\
 & ((-8 \% 29 + x * (1 \% 29)) * \\
 & ((-6 \% 29 + x * (1 \% 29)) * (12 \% 29 + x * (1 \% 29)) *
 \end{aligned}$$

42 F27:=GF(3,3,'a');

Assigne les variables a et K
Par exemple a^200+1 construira un élément de K
^@^@

$$GF(3k^3 + 2k^2 + 1[k, K, a]_{undef})$$

43 a^4;

$$a^2 - a - 1$$

44 F27(5);

$$(-1) \% 3$$

45 factor(randPoly(6,x) % 3);

$$((1 \% 3) * x + 1 \% 3) * ((1 \% 3) * x^5 + ((-1) \% 3) * x + (-1) \% 3)$$

46 Q:=((1 % 3)*x^6+(-1 % 3)*x^5+(-1 % 3)*x^4+(1 % 3)*x^2-1 % 3) % 0;

$$x^6 - x^5 - x^4 + x^2 - 1$$

47 factor(F27(Q));

$$(x^2 + (-a + 1) * x + a) * (x^2 + (-a^2 - 1) * x + a^2 - 1) * ((1 \% 3) * x^2 + (a^2 + a - 1) * x + -a^2 - a - 1)$$

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

49 p:=7; gcd(P % p,diff(P % p,x));

$$(7, 1) \% 7$$

50 Pour calculer Q^n [P] vu comme polynomes en x
powmod a plusieurs syntaxes possibles: il peut recevoir:

- 1) des polynomes a coefficients ds ZZ, dans ce cas:
powmod(Q,n,p,P,x)
- 2) des polynomes dont les coeff sont deja modulaires (% p), dans ce cas
powmod(Q,n,P,x)

Dans les 2 cas la variable par default est x (minuscule!) et peut etre omise.
c'est pourtant une bonne habitude de la preciser.


```
57 A:=ratnormal(powmod(Q,(p-1)/2,P,x)-(1 % p));
```

```
58 gcd(A,P % p);
```

```

$$(-2\%7 + x * ((-2\%7) + x^2 * (3\%7) + x^3 * (1\%7) + x^5 * (1\%7))$$

```

```
59 B:=powmod(Q,(p-1)/2,P,x)+(1 % p);
```

```
60 gcd(B,P);
```

```

$$(-1\%7 + x * (2\%7) + x^2 * ((-1\%7) + x^3 * ((-1\%7) + x^4 * (1\%7))$$

```

```
61 unfacteur(d):={
  //en entree, d est n pol en x a coeff modulaires (% p)
  j:=1;
  A:=1;B:=1;rep:=1;
  r:=seq(alea(p)*j,j=1..rowdim(kN))*kN; //un element du noyau au hasard
  Q:=(LX*r);
  //On fait 3 essais;
  A:=gcd(Q,d);
  if(degree(A)*(degree(A)-degree(d))<>0){
    rep:=A;
  }
  else{
    A:=powmod(Q,(p-1)/2,P,x)-(1 % p);
    A:=gcd(A,d);
    if(degree(A)*(degree(A)-degree(d))<>0){
      rep:=A;
    }
    else{
      A:= powmod(Q,(p-1)/2,P,x)+(1 % p);
      A:=gcd(A,d);
      if( degree(A)*(degree(A)-degree(d))<>0){
        rep:=A;
      }
    }
  }
  if(degree(rep)==0){ return d;}
  else{return rep};
};
unfacteur(P % p);
```

// Interprete unfacteur

// Attention: j,A,B,rep,p,kN,r,LX,Q,P,x, declared as global variable(s). If symbolic variables are required, dec

// lors de la compilation unfacteur

^@

```
(d)->{
  j:=1;
  A:=1;
  B:=1;
  rep:=1;
  r:=seq(alea(p)*j,j=(1 .. (rowdim(kN))))*kN;
  Q:=LX*r;
  A:=gcd(Q,d);
  if ((degree(A)*(degree(A)-degree(d)))<>0) rep:=A; else {
    A:=powmod(Q,(p-1)/2,P,x)-(1 % p);
    A:=gcd(A,d);
    if ((degree(A)*(degree(A)-degree(d)))<>0) rep:=A; else {
      A:= powmod(Q,(p-1)/2,P,x)+(1 % p);
      A:=gcd(A,d);
      if( degree(A)*(degree(A)-degree(d))<>0) rep:=A;
    }
  }
}
```



```

        if ((degree(A)*(degree(A)-degree(d)))<>0) rep:=A; ;
    };
};
if (((degree(rep))==0)) return(d); else return(rep); ;

```

$$x^9(2\%7) + x^{12}((-3\%7) + x^{13}(3\%7) + x^{16}(2\%7) + x^{19}(-3\%7) + x^{22}(3\%7) + x^{25}(-2\%7) + x^{28}(1\%7) + x^{31}(-3\%7) + x^{34}(2\%7) + x^{37}(-3\%7) + x^{40}(3\%7) + x^{43}(-2\%7) + x^{46}(1\%7) + x^{49}(-3\%7) + x^{52}(3\%7) + x^{55}(-2\%7) + x^{58}(1\%7) + x^{61}(-3\%7) + x^{64}(2\%7) + x^{67}(-3\%7) + x^{70}(3\%7) + x^{73}(-2\%7) + x^{76}(1\%7) + x^{79}(-3\%7) + x^{82}(3\%7) + x^{85}(-2\%7) + x^{88}(1\%7) + x^{91}(-3\%7) + x^{94}(2\%7) + x^{97}(-3\%7) + x^{100}(3\%7) + x^{103}(-2\%7) + x^{106}(1\%7) + x^{109}(-3\%7) + x^{112}(3\%7) + x^{115}(-2\%7) + x^{118}(1\%7) + x^{121}(-3\%7) + x^{124}(2\%7) + x^{127}(-3\%7) + x^{130}(3\%7) + x^{133}(-2\%7) + x^{136}(1\%7) + x^{139}(-3\%7) + x^{142}(3\%7) + x^{145}(-2\%7) + x^{148}(1\%7) + x^{151}(-3\%7) + x^{154}(2\%7) + x^{157}(-3\%7) + x^{160}(3\%7) + x^{163}(-2\%7) + x^{166}(1\%7) + x^{169}(-3\%7) + x^{172}(3\%7) + x^{175}(-2\%7) + x^{178}(1\%7) + x^{181}(-3\%7) + x^{184}(2\%7) + x^{187}(-3\%7) + x^{190}(3\%7) + x^{193}(-2\%7) + x^{196}(1\%7) + x^{199}(-3\%7) + x^{202}(3\%7) + x^{205}(-2\%7) + x^{208}(1\%7) + x^{211}(-3\%7) + x^{214}(2\%7) + x^{217}(-3\%7) + x^{220}(3\%7) + x^{223}(-2\%7) + x^{226}(1\%7) + x^{229}(-3\%7) + x^{232}(3\%7) + x^{235}(-2\%7) + x^{238}(1\%7) + x^{241}(-3\%7) + x^{244}(2\%7) + x^{247}(-3\%7) + x^{250}(3\%7) + x^{253}(-2\%7) + x^{256}(1\%7) + x^{259}(-3\%7) + x^{262}(3\%7) + x^{265}(-2\%7) + x^{268}(1\%7) + x^{271}(-3\%7) + x^{274}(2\%7) + x^{277}(-3\%7) + x^{280}(3\%7) + x^{283}(-2\%7) + x^{286}(1\%7) + x^{289}(-3\%7) + x^{292}(2\%7) + x^{295}(-3\%7) + x^{298}(3\%7) + x^{301}(-2\%7) + x^{304}(1\%7) + x^{307}(-3\%7) + x^{310}(3\%7) + x^{313}(-2\%7) + x^{316}(1\%7) + x^{319}(-3\%7) + x^{322}(2\%7) + x^{325}(-3\%7) + x^{328}(3\%7) + x^{331}(-2\%7) + x^{334}(1\%7) + x^{337}(-3\%7) + x^{340}(3\%7) + x^{343}(-2\%7) + x^{346}(1\%7) + x^{349}(-3\%7) + x^{352}(2\%7) + x^{355}(-3\%7) + x^{358}(3\%7) + x^{361}(-2\%7) + x^{364}(1\%7) + x^{367}(-3\%7) + x^{370}(3\%7) + x^{373}(-2\%7) + x^{376}(1\%7) + x^{379}(-3\%7) + x^{382}(2\%7) + x^{385}(-3\%7) + x^{388}(3\%7) + x^{391}(-2\%7) + x^{394}(1\%7) + x^{397}(-3\%7) + x^{400}(3\%7) + x^{403}(-2\%7) + x^{406}(1\%7) + x^{409}(-3\%7) + x^{412}(2\%7) + x^{415}(-3\%7) + x^{418}(3\%7) + x^{421}(-2\%7) + x^{424}(1\%7) + x^{427}(-3\%7) + x^{430}(3\%7) + x^{433}(-2\%7) + x^{436}(1\%7) + x^{439}(-3\%7) + x^{442}(2\%7) + x^{445}(-3\%7) + x^{448}(3\%7) + x^{451}(-2\%7) + x^{454}(1\%7) + x^{457}(-3\%7) + x^{460}(3\%7) + x^{463}(-2\%7) + x^{466}(1\%7) + x^{469}(-3\%7) + x^{472}(2\%7) + x^{475}(-3\%7) + x^{478}(3\%7) + x^{481}(-2\%7) + x^{484}(1\%7) + x^{487}(-3\%7) + x^{490}(3\%7) + x^{493}(-2\%7) + x^{496}(1\%7) + x^{499}(-3\%7) + x^{502}(2\%7) + x^{505}(-3\%7) + x^{508}(3\%7) + x^{511}(-2\%7) + x^{514}(1\%7) + x^{517}(-3\%7) + x^{520}(3\%7) + x^{523}(-2\%7) + x^{526}(1\%7) + x^{529}(-3\%7) + x^{532}(2\%7) + x^{535}(-3\%7) + x^{538}(3\%7) + x^{541}(-2\%7) + x^{544}(1\%7) + x^{547}(-3\%7) + x^{550}(3\%7) + x^{553}(-2\%7) + x^{556}(1\%7) + x^{559}(-3\%7) + x^{562}(2\%7) + x^{565}(-3\%7) + x^{568}(3\%7) + x^{571}(-2\%7) + x^{574}(1\%7) + x^{577}(-3\%7) + x^{580}(3\%7) + x^{583}(-2\%7) + x^{586}(1\%7) + x^{589}(-3\%7) + x^{592}(2\%7) + x^{595}(-3\%7) + x^{598}(3\%7) + x^{601}(-2\%7) + x^{604}(1\%7) + x^{607}(-3\%7) + x^{610}(3\%7) + x^{613}(-2\%7) + x^{616}(1\%7) + x^{619}(-3\%7) + x^{622}(2\%7) + x^{625}(-3\%7) + x^{628}(3\%7) + x^{631}(-2\%7) + x^{634}(1\%7) + x^{637}(-3\%7) + x^{640}(3\%7) + x^{643}(-2\%7) + x^{646}(1\%7) + x^{649}(-3\%7) + x^{652}(2\%7) + x^{655}(-3\%7) + x^{658}(3\%7) + x^{661}(-2\%7) + x^{664}(1\%7) + x^{667}(-3\%7) + x^{670}(3\%7) + x^{673}(-2\%7) + x^{676}(1\%7) + x^{679}(-3\%7) + x^{682}(2\%7) + x^{685}(-3\%7) + x^{688}(3\%7) + x^{691}(-2\%7) + x^{694}(1\%7) + x^{697}(-3\%7) + x^{700}(3\%7) + x^{703}(-2\%7) + x^{706}(1\%7) + x^{709}(-3\%7) + x^{712}(2\%7) + x^{715}(-3\%7) + x^{718}(3\%7) + x^{721}(-2\%7) + x^{724}(1\%7) + x^{727}(-3\%7) + x^{730}(3\%7) + x^{733}(-2\%7) + x^{736}(1\%7) + x^{739}(-3\%7) + x^{742}(2\%7) + x^{745}(-3\%7) + x^{748}(3\%7) + x^{751}(-2\%7) + x^{754}(1\%7) + x^{757}(-3\%7) + x^{760}(3\%7) + x^{763}(-2\%7) + x^{766}(1\%7) + x^{769}(-3\%7) + x^{772}(2\%7) + x^{775}(-3\%7) + x^{778}(3\%7) + x^{781}(-2\%7) + x^{784}(1\%7) + x^{787}(-3\%7) + x^{790}(3\%7) + x^{793}(-2\%7) + x^{796}(1\%7) + x^{799}(-3\%7) + x^{802}(2\%7) + x^{805}(-3\%7) + x^{808}(3\%7) + x^{811}(-2\%7) + x^{814}(1\%7) + x^{817}(-3\%7) + x^{820}(3\%7) + x^{823}(-2\%7) + x^{826}(1\%7) + x^{829}(-3\%7) + x^{832}(2\%7) + x^{835}(-3\%7) + x^{838}(3\%7) + x^{841}(-2\%7) + x^{844}(1\%7) + x^{847}(-3\%7) + x^{850}(3\%7) + x^{853}(-2\%7) + x^{856}(1\%7) + x^{859}(-3\%7) + x^{862}(2\%7) + x^{865}(-3\%7) + x^{868}(3\%7) + x^{871}(-2\%7) + x^{874}(1\%7) + x^{877}(-3\%7) + x^{880}(3\%7) + x^{883}(-2\%7) + x^{886}(1\%7) + x^{889}(-3\%7) + x^{892}(2\%7) + x^{895}(-3\%7) + x^{898}(3\%7) + x^{901}(-2\%7) + x^{904}(1\%7) + x^{907}(-3\%7) + x^{910}(3\%7) + x^{913}(-2\%7) + x^{916}(1\%7) + x^{919}(-3\%7) + x^{922}(2\%7) + x^{925}(-3\%7) + x^{928}(3\%7) + x^{931}(-2\%7) + x^{934}(1\%7) + x^{937}(-3\%7) + x^{940}(3\%7) + x^{943}(-2\%7) + x^{946}(1\%7) + x^{949}(-3\%7) + x^{952}(2\%7) + x^{955}(-3\%7) + x^{958}(3\%7) + x^{961}(-2\%7) + x^{964}(1\%7) + x^{967}(-3\%7) + x^{970}(3\%7) + x^{973}(-2\%7) + x^{976}(1\%7) + x^{979}(-3\%7) + x^{982}(2\%7) + x^{985}(-3\%7) + x^{988}(3\%7) + x^{991}(-2\%7) + x^{994}(1\%7) + x^{997}(-3\%7) + x^{1000}(3\%7)$$

```

62 facteurpseudoirred(d):={
    t:=unfacteur(d);
    tt:=d;
    while (degree(t)<degree(tt)){
        tt:=t;
        t:=unfacteur(t);
    }
    return t;
};

```

// Interprète facteurpseudoirred
 // Attention: t,tt, declared as global variable(s). If symbolic variables are required, declare them as local and
 // lors de la compilation facteurpseudoirred
 ^@

```

(d)->{
    t:=unfacteur(d);
    tt:=d;
    while((degree(t)<(degree(tt))){
        tt:=t;
        t:=unfacteur(t);
    };
    return(t);
}

```

```

63 f:=facteurpseudoirred(P % p);

```

$$(-1\%7 + x(1\%7))$$

64 Si le noyau est de dim 1, f est irréductible.

```

65 if (rowdim(ker(berl((p,f))))==1){print ("f est irred")};

```

f est irred

1

```

66 T:=P % p;a:=1;L:=[];
while(degree(T)>0){T:=quo(T,a);L:=[op(L),a];a:=facteurpseudoirred(T);};
L;

```

$$x^8(3\%7) + x^{11}(1\%7) + x^{14}((-2\%7) + x^{17}((-3\%7) + x^{20}(3\%7) + x^{23}((-2\%7) + x^{26}(3\%7) + x^{29}(1\%7) + x^{32}((-3\%7) + x^{35}(1\%7) + x^{38}(3\%7) + x^{41}((-2\%7) + x^{44}(1\%7) + x^{47}(2\%7) + x^{50}(-3\%7) + x^{53}(3\%7) + x^{56}(-2\%7) + x^{59}(1\%7) + x^{62}(-3\%7) + x^{65}(3\%7) + x^{68}(-2\%7) + x^{71}(1\%7) + x^{74}(-3\%7) + x^{77}(3\%7) + x^{80}(-2\%7) + x^{83}(1\%7) + x^{86}(-3\%7) + x^{89}(3\%7) + x^{92}(-2\%7) + x^{95}(1\%7) + x^{98}(-3\%7) + x^{101}(3\%7) + x^{104}(-2\%7) + x^{107}(1\%7) + x^{110}(-3\%7) + x^{113}(3\%7) + x^{116}(-2\%7) + x^{119}(1\%7) + x^{122}(-3\%7) + x^{125}(3\%7) + x^{128}(-2\%7) + x^{131}(1\%7) + x^{134}(-3\%7) + x^{137}(3\%7) + x^{140}(-2\%7) + x^{143}(1\%7) + x^{146}(-3\%7) + x^{149}(3\%7) + x^{152}(-2\%7) + x^{155}(1\%7) + x^{158}(-3\%7) + x^{161}(3\%7) + x^{164}(-2\%7) + x^{167}(1\%7) + x^{170}(-3\%7) + x^{173}(3\%7) + x^{176}(-2\%7) + x^{179}(1\%7) + x^{182}(-3\%7) + x^{185}(3\%7) + x^{188}(-2\%7) + x^{191}(1\%7) + x^{194}(-3\%7) + x^{197}(3\%7) + x^{200}(-2\%7) + x^{203}(1\%7) + x^{206}(-3\%7) + x^{209}(3\%7) + x^{212}(-2\%7) + x^{215}(1\%7) + x^{218}(-3\%7) + x^{221}(3\%7) + x^{224}(-2\%7) + x^{227}(1\%7) + x^{230}(-3\%7) + x^{233}(3\%7) + x^{236}(-2\%7) + x^{239}(1\%7) + x^{242}(-3\%7) + x^{245}(3\%7) + x^{248}(-2\%7) + x^{251}(1\%7) + x^{254}(-3\%7) + x^{257}(3\%7) + x^{260}(-2\%7) + x^{263}(1\%7) + x^{266}(-3\%7) + x^{269}(3\%7) + x^{272}(-2\%7) + x^{275}(1\%7) + x^{278}(-3\%7) + x^{281}(3\%7) + x^{284}(-2\%7) + x^{287}(1\%7) + x^{290}(-3\%7) + x^{293}(3\%7) + x^{296}(-2\%7) + x^{299}(1\%7) + x^{302}(-3\%7) + x^{305}(3\%7) + x^{308}(-2\%7) + x^{311}(1\%7) + x^{314}(-3\%7) + x^{317}(3\%7) + x^{320}(-2\%7) + x^{323}(1\%7) + x^{326}(-3\%7) + x^{329}(3\%7) + x^{332}(-2\%7) + x^{335}(1\%7) + x^{338}(-3\%7) + x^{341}(3\%7) + x^{344}(-2\%7) + x^{347}(1\%7) + x^{350}(-3\%7) + x^{353}(3\%7) + x^{356}(-2\%7) + x^{359}(1\%7) + x^{362}(-3\%7) + x^{365}(3\%7) + x^{368}(-2\%7) + x^{371}(1\%7) + x^{374}(-3\%7) + x^{377}(3\%7) + x^{380}(-2\%7) + x^{383}(1\%7) + x^{386}(-3\%7) + x^{389}(3\%7) + x^{392}(-2\%7) + x^{395}(1\%7) + x^{398}(-3\%7) + x^{401}(3\%7) + x^{404}(-2\%7) + x^{407}(1\%7) + x^{410}(-3\%7) + x^{413}(3\%7) + x^{416}(-2\%7) + x^{419}(1\%7) + x^{422}(-3\%7) + x^{425}(3\%7) + x^{428}(-2\%7) + x^{431}(1\%7) + x^{434}(-3\%7) + x^{437}(3\%7) + x^{440}(-2\%7) + x^{443}(1\%7) + x^{446}(-3\%7) + x^{449}(3\%7) + x^{452}(-2\%7) + x^{455}(1\%7) + x^{458}(-3\%7) + x^{461}(3\%7) + x^{464}(-2\%7) + x^{467}(1\%7) + x^{470}(-3\%7) + x^{473}(3\%7) + x^{476}(-2\%7) + x^{479}(1\%7) + x^{482}(-3\%7) + x^{485}(3\%7) + x^{488}(-2\%7) + x^{491}(1\%7) + x^{494}(-3\%7) + x^{497}(3\%7) + x^{500}(-2\%7) + x^{503}(1\%7) + x^{506}(-3\%7) + x^{509}(3\%7) + x^{512}(-2\%7) + x^{515}(1\%7) + x^{518}(-3\%7) + x^{521}(3\%7) + x^{524}(-2\%7) + x^{527}(1\%7) + x^{530}(-3\%7) + x^{533}(3\%7) + x^{536}(-2\%7) + x^{539}(1\%7) + x^{542}(-3\%7) + x^{545}(3\%7) + x^{548}(-2\%7) + x^{551}(1\%7) + x^{554}(-3\%7) + x^{557}(3\%7) + x^{560}(-2\%7) + x^{563}(1\%7) + x^{566}(-3\%7) + x^{569}(3\%7) + x^{572}(-2\%7) + x^{575}(1\%7) + x^{578}(-3\%7) + x^{581}(3\%7) + x^{584}(-2\%7) + x^{587}(1\%7) + x^{590}(-3\%7) + x^{593}(3\%7) + x^{596}(-2\%7) + x^{599}(1\%7) + x^{602}(-3\%7) + x^{605}(3\%7) + x^{608}(-2\%7) + x^{611}(1\%7) + x^{614}(-3\%7) + x^{617}(3\%7) + x^{620}(-2\%7) + x^{623}(1\%7) + x^{626}(-3\%7) + x^{629}(3\%7) + x^{632}(-2\%7) + x^{635}(1\%7) + x^{638}(-3\%7) + x^{641}(3\%7) + x^{644}(-2\%7) + x^{647}(1\%7) + x^{650}(-3\%7) + x^{653}(3\%7) + x^{656}(-2\%7) + x^{659}(1\%7) + x^{662}(-3\%7) + x^{665}(3\%7) + x^{668}(-2\%7) + x^{671}(1\%7) + x^{674}(-3\%7) + x^{677}(3\%7) + x^{680}(-2\%7) + x^{683}(1\%7) + x^{686}(-3\%7) + x^{689}(3\%7) + x^{692}(-2\%7) + x^{695}(1\%7) + x^{698}(-3\%7) + x^{701}(3\%7) + x^{704}(-2\%7) + x^{707}(1\%7) + x^{710}(-3\%7) + x^{713}(3\%7) + x^{716}(-2\%7) + x^{719}(1\%7) + x^{722}(-3\%7) + x^{725}(3\%7) + x^{728}(-2\%7) + x^{731}(1\%7) + x^{734}(-3\%7) + x^{737}(3\%7) + x^{740}(-2\%7) + x^{743}(1\%7) + x^{746}(-3\%7) + x^{749}(3\%7) + x^{752}(-2\%7) + x^{755}(1\%7) + x^{758}(-3\%7) + x^{761}(3\%7) + x^{764}(-2\%7) + x^{767}(1\%7) + x^{770}(-3\%7) + x^{773}(3\%7) + x^{776}(-2\%7) + x^{779}(1\%7) + x^{782}(-3\%7) + x^{785}(3\%7) + x^{788}(-2\%7) + x^{791}(1\%7) + x^{794}(-3\%7) + x^{797}(3\%7) + x^{800}(-2\%7) + x^{803}(1\%7) + x^{806}(-3\%7) + x^{809}(3\%7) + x^{812}(-2\%7) + x^{815}(1\%7) + x^{818}(-3\%7) + x^{821}(3\%7) + x^{824}(-2\%7) + x^{827}(1\%7) + x^{830}(-3\%7) + x^{833}(3\%7) + x^{836}(-2\%7) + x^{839}(1\%7) + x^{842}(-3\%7) + x^{845}(3\%7) + x^{848}(-2\%7) + x^{851}(1\%7) + x^{854}(-3\%7) + x^{857}(3\%7) + x^{860}(-2\%7) + x^{863}(1\%7) + x^{866}(-3\%7) + x^{869}(3\%7) + x^{872}(-2\%7) + x^{875}(1\%7) + x^{878}(-3\%7) + x^{881}(3\%7) + x^{884}(-2\%7) + x^{887}(1\%7) + x^{890}(-3\%7) + x^{893}(3\%7) + x^{896}(-2\%7) + x^{899}(1\%7) + x^{902}(-3\%7) + x^{905}(3\%7) + x^{908}(-2\%7) + x^{911}(1\%7) + x^{914}(-3\%7) + x^{917}(3\%7) + x^{920}(-2\%7) + x^{923}(1\%7) + x^{926}(-3\%7) + x^{929}(3\%7) + x^{932}(-2\%7) + x^{935}(1\%7) + x^{938}(-3\%7) + x^{941}(3\%7) + x^{944}(-2\%7) + x^{947}(1\%7) + x^{950}(-3\%7) + x^{953}(3\%7) + x^{956}(-2\%7) + x^{959}(1\%7) + x^{962}(-3\%7) + x^{965}(3\%7) + x^{968}(-2\%7) + x^{971}(1\%7) + x^{974}(-3\%7) + x^{977}(3\%7) + x^{980}(-2\%7) + x^{983}(1\%7) + x^{986}(-3\%7) + x^{989}(3\%7) + x^{992}(-2\%7) + x^{995}(1\%7) + x^{998}(-3\%7) + x^{1001}(3\%7)$$

67 Le nombre de facteurs doit être la dim de ker F, on teste si l'on a trouvé tous les facteurs ainsi:

```

68 if (nops(kN)==(nops(L)-1)){print ("on a bien trouvé tous les facteurs")};

```

0

69