1 art;maple_mode(0);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 ----------Initiation syntaxe modulaire et puissance rapide----------

3 On peut modifier l'argument passe a une fonction, a l'interieur de la fonction, en revanche, une fois sorti de la fonction sa valeur initiale avant l'appel est restitu\'ee. Par exemple la fonction suivante remonte P dans Z (ie passer modulo 0)

4 f:=proc(P) P:=P%0;end;

// Success
// End defining f

```
(P)->
{ local NULL;
  P:=P % 0;
}
```

5 Q:=x+1%5;f(Q);Q

$$(x+1\,\%\,5,\ x+1,\ x+1\,\%\,5)$$

6 a:=27%101;

$$27\,\%\,101$$

7 l:=[seq([2^j,time(a^(2^(2^j)))[0]],j=3..18)]:;l:=[op(l),seq([2^(j/7),time(a^(2^(2^j)))[0]],j=7*14..16*7)]:;

Evaluation time: 4.78

(Done , Done)

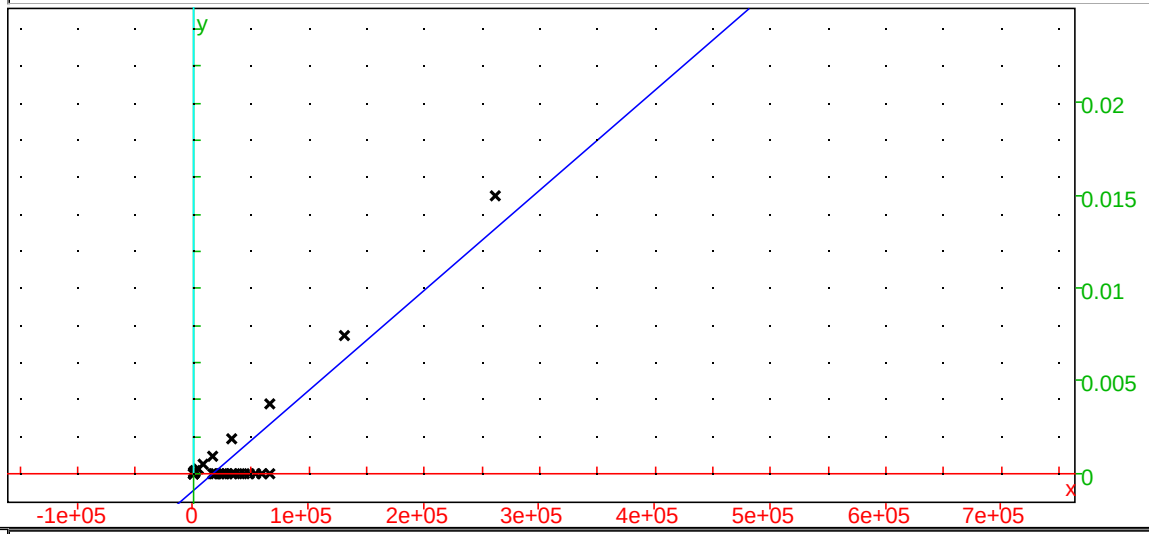
8 d1:=scatterplot(l):; // la croissance lineaire.

Done

9 d2:=line(y-[linear_regression(l)]*[x,1]):;// mal adapte a la repartition irreguliere des abscisses de l

Done

10 affichage(d1,point_width_2),affichage(d2,bleu);



11 P:=2*(x^4+x^3+x^2+x+1);

$$2\cdot(x^4+x^3+x^2+x+1)$$

12 Q:= P % 7;

$$2\,\%\,7\cdot x^4+2\,\%\,7\cdot x^3+2\,\%\,7\cdot x^2+2\,\%\,7\cdot x+2\,\%\,7$$

13 rem(x^7,Q);// la division est bien faite dans Z/7Z

$$1\,\%\,7\cdot x^2$$

14 rem(x^(2^10),Q);//Attention, ca a l'air long, signe que la puissance n'est pasrapide

$$-1\,\%\,7\cdot x^3+-1\,\%\,7\cdot x^2+-1\,\%\,7\cdot x+-1\,\%\,7$$

15 rem(x^(2^33),Q);//n'est plus evalue. trop gros

8589934592

16 Pour faire des puissances rapides de polyn\^omes a coefficients dans Z/pZ modulo un autre polynome on le fait avec l'intruction powmod qui attend des polynomes a coefficients entiers, et le nombre premier. Cf ?powmod

17
```
powmod((1+x),2^33,101,P,x);
```

$$-21 \cdot x^2 + 13 \cdot x - 21$$

18 ----------Methode de Berlekamp----------

19
```
sum(rand(20)*x^j,j=0..n);  //sum,mul,add evaluent le random avant!
```

$$\frac{7 \cdot x^{n+1}}{x-1} - \left(\frac{7}{x-1}\right)$$

20
```
randP:=n->poly2symb([1,seq(rand(20),j=0..n-1)],x);
```

```
// Warning: j,x, declared as global variable(s)
// End defining randP
```

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

21
```
P:=expand(mul([seq(randP(rand(7)),j=1..5)])); //on met un seq pour avoir des rand differents
```

$$x^{16} + x^{14} + 58 \cdot x^{15} + 1386 \cdot x^{14} + 17715 \cdot x^{13} + 131260 \cdot x^{12} + 578697 \cdot x^{11} + 1538013 \cdot x^{10} + 2648041 \cdot 5858116 \cdot x^6 + 5979221 \cdot x^5 + 5239798 \cdot x^4 + 4098561 \cdot x^3 + 3176188 \cdot x^2 + 1660466 \cdot x + 705432$$

22
```
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+36874
```

$$x^{16} + x^{14} + 58 \cdot x^{15} + 1386 \cdot x^{14} + 17715 \cdot x^{13} + 131260 \cdot x^{12} + 578697 \cdot x^{11} + 1538013 \cdot x^{10} + 2648041 \cdot 5858116 \cdot x^6 + 5979221 \cdot x^5 + 5239798 \cdot x^4 + 4098561 \cdot x^3 + 3176188 \cdot x^2 + 1660466 \cdot x + 705432$$

23
```
gcd(P,diff(P,x)); //Pour berlekamp, il ne faut pas de facteurs multiples.
```

$$1$$

24 Attention \`a la bonne instruction pour trouver un noyau mod p. en mode maple 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.

25 Prog Edit Add | 1 | nxt | OK (F9) | Save

```
berl:=proc(p,PP)
local f,L,F,n;
PP:=PP % p; // pour le calcul de pgcd on s'assure/(on force) que P est modulo p
if degree(gcd(PP,diff(PP,x))) =0 then
n:=degree(PP)-1;
f:=(i0,j0)->coeff(powmod(x,i0*p,p,PP % 0,x),x,j0);
L:=matrix(n,n,f)-idn(n);
F:=transpose(L) % p;
ker(F);
else afficher("facteurs multiples",p); [[0]] fi;
end;
```

```
// Warning: x,p,PP, declared as global variable(s)
// End defining f
// Warning: x,i0,j0, declared as global variable(s)
// End defining berl
```

```
(p,PP)->
{ local f,L,F,n;
  PP:=PP % p;
  if (((degree(gcd(PP,diff(PP,x))))==0)) {
```

26
```
p:=1:;L:=[];for i0 from 1 to 10 do
p:=nextprime(p):; L:=[op(L),[rowdim(berl(p,P)),p,factor(P % p) ]] od:;
```

```
"facteurs multiples",3
"facteurs multiples",11
"facteurs multiples",13
"facteurs multiples",19
"facteurs multiples",23
Evaluation time: 0.83
```

(Done , [] , Done)

M

27
```
L;
```

$$
\begin{array}{lll}
6, & 5, & (1\,\%\,5 \cdot x^4 + 1\,\%\,5 \cdot x^2 + -2\,\%\,5 \cdot x + -2\,\%\,5) \\
 & & 1\,\%\,7 \cdot x \cdot (1\,\%\,7 \cdot x + -1\,\%\,7) \cdot \\
 & & (1\,\%\,7 \cdot x + -2\,\%\,7) \cdot (1\,\%\,7 \cdot x^2 + 2\,\%\,7 \cdot x + 3\,\%\,7) \cdot \\
 & & (1\,\%\,7 \cdot x^5 + 1\,\%\,7 \cdot x^3 + 3\,\%\,7 \cdot x^2 + -2\,\%\,7 \cdot x + -2\,\%\,7) \cdot \\
 & & 1\,\%\,7 \cdot x^6 + 3\,\%\,7 \cdot x^5 + -3\,\%\,7 \cdot x^4 + \\
5, & 7, & (-2\,\%\,7 \cdot x^3 + 3\,\%\,7 \cdot x^2 + 2\,\%\,7 \cdot x + -2\,\%\,7) \\
 & & (1\,\%\,11 \cdot x + 2\,\%\,11) \cdot (1\,\%\,11 \cdot x + -3\,\%\,11) \cdot \\
 & & (1\,\%\,11 \cdot x + -4\,\%\,11) \cdot (1\,\%\,11 \cdot x + -5\,\%\,11)^2 \cdot \\
 & & (1\,\%\,11 \cdot x^2 + 1\,\%\,11 \cdot x + 4\,\%\,11) \cdot \\
 & & (1\,\%\,11 \cdot x^2 + -2\,\%\,11 \cdot x + -5\,\%\,11) \cdot \\
 & & (1\,\%\,11 \cdot x^2 + 5\,\%\,11 \cdot x + -1\,\%\,11) \cdot \\
1, & 11, & (1\,\%\,11 \cdot x^5 + 3\,\%\,11 \cdot x^4 + -3\,\%\,11 \cdot x^3 + 4\,\%\,11 \cdot x^2 + -2\,\%\,11) \\
 & & 1\,\%\,13 \cdot x \cdot (1\,\%\,13 \cdot x + -2\,\%\,13)^2 \cdot \\
 & & (1\,\%\,13 \cdot x + 3\,\%\,13)^2 \cdot (1\,\%\,13 \cdot x + -4\,\%\,13)^2 \cdot \\
 & & (1\,\%\,13 \cdot x^4 + -2\,\%\,13 \cdot x^3 + -6\,\%\,13 \cdot x^2 + -4\,\%\,13 \cdot x + 4\,\%\,13) \cdot \\
 & & 1\,\%\,13 \cdot x^5 + 1\,\%\,13 \cdot x^4 + -4\,\%\,13 \cdot x^3 + \\
1, & 13, & (2\,\%\,13 \cdot x^2 + -1\,\%\,13 \cdot x + 5\,\%\,13) \\
 & & 1\,\%\,17 \cdot x \cdot (1\,\%\,17 \cdot x + -4\,\%\,17) \cdot \\
 & & (1\,\%\,17 \cdot x + 6\,\%\,17) \cdot (1\,\%\,17 \cdot x + -8\,\%\,17) \cdot \\
 & & (1\,\%\,17 \cdot x^2 + -5\,\%\,17 \cdot x + -3\,\%\,17) \cdot \\
 & & (1\,\%\,17 \cdot x^2 + 7\,\%\,17 \cdot x + -3\,\%\,17) \cdot \\
 & & (1\,\%\,17 \cdot x^3 + 7\,\%\,17 \cdot x^2 + 6\,\%\,17 \cdot x + -4\,\%\,17) \cdot \\
 & & 1\,\%\,17 \cdot x^5 + 4\,\%\,17 \cdot x^4 + -6\,\%\,17 \cdot x^3 + \\
7, & 17, & (7\,\%\,17 \cdot x^2 + -8\,\%\,17 \cdot x + 6\,\%\,17) \\
 & & 1\,\%\,19 \cdot x \cdot (1\,\%\,19 \cdot x + -2\,\%\,19) \cdot \\
 & & (1\,\%\,19 \cdot x + -6\,\%\,19)^2 \cdot \\
 & & (1\,\%\,19 \cdot x^2 + -5\,\%\,19 \cdot x + -2\,\%\,19) \cdot \\
 & & (1\,\%\,19 \cdot x^2 + 6\,\%\,19 \cdot x + 1\,\%\,19) \cdot \\
 & & (1\,\%\,19 \cdot x^2 + -7\,\%\,19 \cdot x + -5\,\%\,19) \cdot \\
 & & (1\,\%\,19 \cdot x^2 + 9\,\%\,19 \cdot x + -2\,\%\,19) \cdot \\
1, & 19, & (1\,\%\,19 \cdot x^4 + -7\,\%\,19 \cdot x^3 + 4\,\%\,19 \cdot x^2 + -6\,\%\,19 \cdot x + 5\,\%\,19) \\
 & & (1\,\%\,23 \cdot x + 4\,\%\,23) \cdot (1\,\%\,23 \cdot x + -4\,\%\,23) \cdot
\end{array}
$$

M

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

29
```
p:=7; P:=P % p ;gcd(P ,diff(P ,x)) ;
```

$$
1\,\%\,7 \cdot x^{16} + 2\,\%\,7 \cdot x^{15} + 1\,\%\,7 \cdot x^{14} + -2\,\%\,7 \cdot x^{13} + 3\,\%\,7 \cdot x^{12} +
$$

$$
1\,\%\,7 \cdot x^{10} + -3\,\%\,7 \cdot x^{9} + 1\,\%\,7 \cdot x^{8} + 3\,\%\,7 \cdot x^{7} + -2\,\%\,7 \cdot x^{6} +
$$

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

$$\begin{bmatrix} -1\%7, & 0\%7, & 0\%7, & 0\%7, & 0\%7, & 0\%7, & 0\%7, & 0\%7, & 0\%7, & 0\%7, & 0\%7, & 0, \\ 0, & 0\%7, & -1\%7, & 3\%7, & 3\%7, & 2\%7, & -2\%7, & 1\%7, & -3\%7, & 2\%7, & 2\%7, & -1\%7, \\ 0, & 3\%7, & 2\%7, & -3\%7, & -3\%7, & 0\%7, & 0\%7, & -2\%7, & 0\%7, & -3\%7, & 0\%7, & 0, \\ 0, & -2\%7, & -1\%7, & -1\%7, & -1\%7, & -1\%7, & -2\%7, & 0\%7, & -2\%7, & -1\%7, & -2\%7, & 0, \\ 0, & -2\%7, & -1\%7, & 1\%7, & -3\%7, & -1\%7, & -1\%7, & 3\%7, & -1\%7, & -1\%7, & -3\%7, & 0, \end{bmatrix}$$

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

$$x \cdot 3\%7 + x^2 \cdot 2\%7 + x^3 \cdot -3\%7 + x^4 \cdot -3\%7 + x^5 \cdot 0\%7 + x^6 \cdot 0\%7 + x^7 \cdot -2\%7 + x^8 \cdot 0\%7 + x^9 \cdot -3\%7$$

```
32 rem(powmod(Q % 0 ,p,p,P % 0,x)-Q,P ); //  verification:
```

$$0$$

```
33 gcd(Q ,P);  //l'un des 3 pgcd est non trivial:
```

$$1\%7 \cdot x^2 + -1\%7 \cdot x$$

```
34 A:=rem(powmod(Q % 0,(p-1)/2,p,P % 0,x)-1,P ) ;
```

$$-x^{14} + 3 \cdot x^{13} - x^{12} + 3 \cdot x^{11} - 3 \cdot x^{10} - 2 \cdot x^7 - 3 \cdot x^6 + 3 \cdot x^5 + 2 \cdot x^4 - x^3 - 1$$

```
35 gcd(A,P);
```

$$1\%7 \cdot x^{12} + 1\%7 \cdot x^{11} + -1\%7 \cdot x^{10} + 1\%7 \cdot x^9 + -1\%7 \cdot x^8 + -3\%7 \cdot x^7 + 1\%7 \cdot x^6 + 3\%7 \cdot x^5 + 2\%7$$

```
36 B:=rem(powmod(Q % 0,(p-1)/2,p,P % 0,x)+1,P);
```

$$-x^{14} + 3 \cdot x^{13} - x^{12} + 3 \cdot x^{11} - 3 \cdot x^{10} - 2 \cdot x^7 - 3 \cdot x^6 + 3 \cdot x^5 + 2 \cdot x^4 - x^3 + 1$$

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

$$1\%7 \cdot x^2 + 2\%7 \cdot x + 3\%7$$

```
38 unfacteur:=proc(d)
i0:=1;
A:=1;B:=1;rep:=1;
r:=[seq(alea(p),i0=1..rowdim(N))]*N; //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 then rep:=A ;
else A:=rem(powmod(Q % 0 ,(p-1)/2,p,P % 0,x)-1,P);
A:=gcd(A,d);
if degree(A)*(degree(A)-degree(d))<>0 then rep:=A ;
else A:=rem(powmod(Q % 0,(p-1)/2,p,P % 0,x)+1,P);
A:=gcd(A,d);
if degree(A)*(degree(A)-degree(d))<>0 then rep:=A fi;
fi;
fi;
if degree(rep)=0 then d else rep  fi;
end proc;
```

```
// End defining unfacteur
(d)->
{ local NULL;
 i0:=1;
 A:=1;
 B:=1;
 rep:=1;
 r:=[seq(alea(p),i0=(1 .. (rowdim(N))))]*N;
 Q:=LX*r;
 A:=gcd(Q,d);
```

```
if ((degree(A)*(degree(A)-degree(d)))!=0) {
  rep:=A;
 }
 else {
  A:=rem(powmod(Q % 0,(p-1)/2,p,P % 0,x)-1,P);
  A:=gcd(A,d);
  if ((degree(A)*(degree(A)-degree(d)))!=0) {
    rep:=A;
   }
   else {
    A:=rem(powmod(Q % 0,(p-1)/2,p,P % 0,x)+1,P);
    A:=gcd(A,d);
    if ((degree(A)*(degree(A)-degree(d)))!=0) {
      rep:=A;
     };
   }; ;
 }; ;
if (((degree(rep))==0)) {
```

39 unfacteur(P);

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

40
```
facteurpseudoirred:=proc(d)
t:=unfacteur(d);
tt:=d;
while (degree(t)<degree(tt)){tt:=t;t:=unfacteur(t);};
t;
end:
```

```
// Warning: t,tt, declared as global variable(s)
// End defining facteurpseudoirred
```

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

41 f:=facteurpseudoirred(P);

$$1 \% 7 \cdot x^{16} + 2 \% 7 \cdot x^{15} + 1 \% 7 \cdot x^{14} + -2 \% 7 \cdot x^{13} + 3 \% 7 \cdot x^{12} + 1 \% 7 \cdot x^{10} + -3 \% 7 \cdot x^{9} + 1 \% 7 \cdot x^{8} + 3 \%$$

42 Si le noyau est de dim 1, f est irreductible.

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

undef

44 La construction dans la boucle suivante cree une liste L qui commence systematiquement par 1, les facteurs de P trouves sont ranges dans L apres.

45
```
T:=P;a:=1;L:=[];
while(degree(T)>0){T:=quo(T,a);L:=[op(L),a];a:=facteurpseudoirred(T)}:;L;
```

$$1 \% 7 \cdot x^{16} + 2 \% 7 \cdot x^{15} + 1 \% 7 \cdot x^{14} + -2 \% 7 \cdot x^{13} + 3 \% 7 \cdot x^{12} +$$
$$1 \% 7 \cdot x^{10} + -3 \% 7 \cdot x^{9} + 1 \% 7 \cdot x^{8} + 3 \% 7 \cdot x^{7} + -2 \% 7 \cdot x^{6} +$$
$$[3 \% 7 \cdot x^{5} + -3 \% 7 \cdot x^{4} + -2 \% 7 \cdot x^{3} + 1 \% 7 \cdot x^{2} + 3 \% 7 \cdot x, 1, [], \text{Done}, [1, 1 \% 7 \cdot x^{5} + 1 \% 7$$

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

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

on a bien trouve tous les facteurs

1