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

Warning: some commands like subs might change arguments order   0   0   0   1   0   1e-10   10   [1   50   0   25]   0   0

2 F729:=GF(3,6,'a');

$$GF(3,a^6-a^5-a^4+a^2-1,a,undef)$$

3 F729((1+a)^17);

$$GF(3,a^6-a^5-a^4+a^2-1,a,a^5-a^3)$$

4 a:=F729(a); #On note a cette classe.

$$GF(3,a^6-a^5-a^4+a^2-1,a,a)$$

5 (1+a)^17

$$GF(3,a^6-a^5-a^4+a^2-1,a,a^5-a^3)$$

6 Factor(x^3-x+1) mod 3;

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

7 factor(x^3-x+1,a);

6 5 4 2 4 3 2 6 5 4 2 4 3 2 6 5

8 factor(x^3-x+a,a);

$$x^3-x+GF(3,a^6-a^5-a^4+a^2-1,a,a)$$

9 Factor(x^{3^5}-x) mod 3;

$(1\cdot x^5+1\cdot x^3+1\cdot x^2+(-1)\cdot x-1)\cdot(1\cdot x^5+(-1)\cdot x^3+1\cdot x^2+1\cdot x-1)\cdot(1\cdot x^5+1\cdot x^3+(-1)\cdot x^2+1)\cdot(1\cdot x^5+1\cdot x^3+(-1)\cdot x^2+(-1)\cdot x+1)\cdot(1\cdot$

$(1\cdot x^5+(-1)\cdot x^4+1\cdot x+1)\cdot(1\cdot x^5+(-1)\cdot x^4+(-1)\cdot x^2-1)\cdot(1\cdot x^5+(-1)\cdot x-1)\cdot(1\cdot x^5+(-1)\cdot x^3+(-1)\cdot x^2-1)\cdot(1\cdot x^5+1\cdot x^4+1\cdot x^2+1)\cdot(1$

$(1\cdot x^5+1\cdot x^4+1\cdot x^3+1\cdot x^2+(-1)\cdot x+1)\cdot(1\cdot x^5+1\cdot x^4+(-1)\cdot x^3+1)\cdot(1\cdot x^5+1\cdot x^4+(-1)\cdot x^3+1\cdot x^2+1\cdot x+1)\cdot(1\cdot x^5+1\cdot x^4+1\cdot x-1)\cdot$

$(1\cdot x-1)\cdot 1\cdot x\cdot(1\cdot x^5+(-1)\cdot x^3+1\cdot x^2+(-1)\cdot x-1)\cdot(1\cdot x^5+1\cdot x^4+1\cdot x^3+1\cdot x+1)\cdot(1\cdot x+1)\cdot(1\cdot x^5+(-1)\cdot x^4+1\cdot x^3+(-1)\cdot x^2+(-1)\cdot x$

$(1\cdot x^5+1\cdot x^4+(-1)\cdot x^3+(-1)\cdot x-1)\cdot(1\cdot x^5+1\cdot x^4+1\cdot x^3+(-1)\cdot x^2+1\cdot x+1)\cdot(1\cdot x^5+(-1)\cdot x+1)\cdot(1\cdot x^5+(-1)\cdot x^4+1\cdot x^3+1\cdot x^2+1\cdot x-1$

$(1\cdot x^5+(-1)\cdot x^2+1\cdot x+1)\cdot(1\cdot x^5+(-1)\cdot x^3+(-1)\cdot x^2+(-1)\cdot x+1)\cdot(1\cdot x^5+1\cdot x^4-1)\cdot(1\cdot x^5+1\cdot x^4+1\cdot x^2+1\cdot x+1)\cdot(1\cdot x^5+1\cdot x^2+1\cdot x$

$(1\cdot x^5+(-1)\cdot x^4+(-1)\cdot x^3+(-1)\cdot x^2+1)\cdot(1\cdot x^5+1\cdot x^4+1\cdot x^3+(-1)\cdot x^2+1\cdot x-1)\cdot(1\cdot x^5+(-1)\cdot x^4+(-1)\cdot x^2+1\cdot x-1)\cdot(1\cdot x^5+(-1)\cdot x^4+$

$(1\cdot x^5+(-1)\cdot x^4+(-1)\cdot x^3+1\cdot x^2-1)\cdot(1\cdot x^5+(-1)\cdot x^3+1\cdot x^2+1)\cdot(1\cdot x^5+1\cdot x^4+(-1)\cdot x^3+(-1)\cdot x^2-1)\cdot(1\cdot x^5+(-1)\cdot x^4+1\cdot x^3+1\cdot x^2+$

$(1\cdot x^5+(-1)\cdot x^4+(-1)\cdot x^3+(-1)\cdot x^2+1\cdot x-1)\cdot(1\cdot x^5+(-1)\cdot x^4+(-1)\cdot x^3+(-1)\cdot x+1)\cdot(1\cdot x^5+1\cdot x^3+1\cdot x-1)\cdot(1\cdot x^5+1\cdot x^4+(-1)\cdot x^3+1$

10 GF(3,20,a); #trop gros

No irreducible primitive polynomial found Error: Bad Argument Value

11 Factor(X^8+1) mod 3;

$$(1\cdot X^4+1\cdot X^2-1)\cdot(1\cdot X^4+(-1)\cdot X^2-1)$$

12 l:={1,2,3,4,3,4};

$$[1\quad 2\quad 3\quad 4]$$

13 l minus {1,3};

$$[2\quad 4]$$

14 l minus l;

$$\{\ \}$$

16 Prog Edit Ajouter nxt OK Save

```
orbites:=proc(n)
local a,i,j,k,l,o,liste;
liste:=[];
if n mod 3 =0 then print("Erreur: 3 divise",n)
else
l:={seq(i,i=0..n-1)};
j:=1;
while l<>{} do
i:=l[1];
o:={i};a:=(3*i) mod n;
while a<>i do o:=o union {a};a:= (3*a) mod n; od;
l:= (l minus o); liste:=[op(liste),o];
od;
fi;
liste;
end proc;
```

// Success
// End defining orbites

```
proc(n)
 local a,i,j,k,l,o,liste;
 liste:=[];
 if irem(n,3)=0 then
   print("Erreur: 3 divise",n) else
   l:={seq(i,i=(0 .. (n-1)))};
   j:=1;
   while l<>{ } do
     i:=l[1];
     o:={i};
     a:=irem(3*i,n);
     while a<>i do
       o:=o union {a};
       a:=irem(3*a,n);
      od;;
     l:=l minus o;
     liste:=[op(liste),o];
    od;
 fi ;
 liste;

end;
```

17 Factor(X^32-1) mod 3;

2 2 2 4 2 4 2 8 4

18 orbites(32);

[[0] [1 3 9 27 17 19 25 11] [2 6 18 22] [4 12] [5 15 13 7 21 31 29 23] [8 24] [10

19 Factor(X^14-1) mod 3;

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

20 orbites(14);

[[0] [1 3 9 13 11 5] [2 6 4 12 8 10] [7]]

21 On remarque que pour tout i il y a autant d'orbites 'a i elements que de facteurs irreductibles de degre i

22 for i from 1 to 8 do print(nops(orbites(2^i)[2]),2^i) od;

```
1,2
2,4
2,8
4,16
8,32
16,64
32,128
64,256
```

1

23 (Cf cours)On peut montrer que le noyau de la surjection donn'ee par la reduction mod 4 est cyclique d'ordre 2^(n-2)
-3=1+4.m ou m est impair, donc -3 est d'ordre maximal donc 3 aussi.
En fait les elements d'ordre max sont ceux congrus a 5 ou -5 mod 8

24 for i from 1 to 8 do print(factor(X^(2^i)-1),2^i) od;

```
(X-1)*(X+1),2
(X-1)*(X+1)*(X^2+1),4
(X-1)*(X+1)*(X^2+1)*(X^4+1),8
(X-1)*(X+1)*(X^2+1)*(X^4+1)*(X^8+1),16
(X-1)*(X+1)*(X^2+1)*(X^4+1)*(X^8+1)*(X^16+1),32
(X-1)*(X+1)*(X^2+1)*(X^4+1)*(X^8+1)*(X^16+1)*(X^32+1),64
(X-1)*(X+1)*(X^2+1)*(X^4+1)*(X^8+1)*(X^16+1)*(X^32+1)*(X^64+1),128
(X-1)*(X+1)*(X^2+1)*(X^4+1)*(X^8+1)*(X^16+1)*(X^32+1)*(X^64+1)*(X^128+1),256
Evaluation time: 0.63
```

25 le poly cyclo Phi_2^n est phi(n)

26 phi:=n->X^(2^(n-1))+1;

// Warning: X declared as global variable(s)
// End defining phi

$n \to X^{2^{n-1}}+1$

27 for i from 1 to 8 do print(Factor(phi(i)) mod 3) od;

```
1*X^2+1
(1*X^2+1*X-1)*(1*X^2-1*X-1)
(1*X^4+1*X^2-1)*(1*X^4-1*X^2-1)
(1*X^8+1*X^4-1)*(1*X^8-1*X^4-1)
(1*X^16+1*X^8-1)*(1*X^16-1*X^8-1)
(1*X^32+1*X^16-1)*(1*X^32-1*X^16-1)
(1*X^64+1*X^32-1)*(1*X^64-1*X^32-1)
```

1

28 for i from 1 to 100 do if ((3^i-1) mod 2^8) == 0 then print(i) fi; od;

i:64

undef

29 on prend i=64

30 Factor(X^128+1) mod 3;

$(1\cdot X^{64}+1\cdot X^{32}-1)\cdot(1\cdot X^{64}+(-1)\cdot X^{32}-1)$

31 P:=X^64+X^32-1;

$X^{64}+X^{32}-1$

32 Factor(P) mod 3; #P convient

$1\cdot X^{64}+1\cdot X^{32}-1$

33 ----------------Racines carrees---

34 P:=x^64+x^32-1;

$x^{64}+x^{32}-1$

35

36 Prog Edit Ajouter | nxt | OK | Save

```
puiss:=proc(g,n)
local u,v;
u:=1;v:=g;
while n>1 do
if (n mod 2 )==0 then v:=Rem(v*v,P) mod 3; n:=n/2
else u:=Rem(u*v,P) mod 3; v:=Rem(v*v,P) mod 3; n:=(n-1)/2
fi;od;
Rem(u*v,P)mod 3;end
```

// Warning: P declared as global variable(s)
// End defining puiss

```
proc(g,n)
  local u,v;
  u:=1;
  v:=g;
  while n>1 do
    if irem(n,2)=0 then
      v:=irem(Rem(v*v,P),3);
      n:=n/2 else
      u:=irem(Rem(u*v,P),3);
      v:=irem(Rem(v*v,P),3);
      n:=(n-1)/2
    fi ;
   od;;
  irem(Rem(u*v,P),3);

end;
```

37 puiss(1+x,5^7);

$1\cdot x^{61}+1\cdot x^{60}+(-1)\cdot x^{59}+1\cdot x^{58}+0\cdot x^{57}+(-1)\cdot x^{56}+1\cdot x^{55}+0\cdot x^{54}+(-1)\cdot x^{53}+0\cdot x^{52}+0\cdot x^{51}+(-1)\cdot x^{49}+0\cdot x^{48}+1\cdot x^{47}+(-1)\cdot x^{46}+$
$1\cdot x^{40}+(-1)\cdot x^{39}+0\cdot x^{38}+0\cdot x^{37}+0\cdot x^{36}+0\cdot x^{35}+0\cdot x^{34}+(-1)\cdot x^{33}+1\cdot x^{32}+(-1)\cdot x^{31}+1\cdot x^{30}+(-1)\cdot x^{29}+1\cdot x^{28}+(-1)\cdot x^{27}+(-1)\cdot x^{25}$
$(-1)\cdot x^{19}+1\cdot x^{17}+0\cdot x^{16}+0\cdot x^{15}+1\cdot x^{13}+(-1)\cdot x^{12}+1\cdot x^{11}+(-1)\cdot x^{10}+(-1)\cdot x^{9}+(-1)\cdot x^{8}+1\cdot x^{7}+1\cdot x^{6}+(-1)\cdot x^{5}+1\cdot x^{4}+(-1)\cdot x^{3}+1\cdot$

38 puiss:=(g,n)->powmod(g,n,3,P,x);

// Warning: P x declared as global variable(s)
// End defining puiss

39 puiss(1+x,5^7); # on v'erifie

$x^{61}+x^{60}-x^{59}+x^{58}-x^{56}+x^{55}-x^{53}-x^{49}+x^{47}-x^{46}+x^{45}-x^{44}+x^{43}+x^{42}+x^{41}+x^{40}-x^{39}-x^{33}+x^{32}-x^{31}+x^{30}-x^{29}+x^{28}$

40 q:=3^64;t:=(q-1)/2^8;

(3433683820292512484657849089281 , 13412827423017626893194723005)

41 testcarre:=proc(g)
evalb(puiss(g,(q-1)/2)=1);
end proc;

// Warning: puiss q declared as global variable(s)
// End defining testcarre

```
proc(g)
  evalb(puiss(g,(q-1)/2)=1);

end;
```

42 testcarre(1+x); # 1+x ne convient pas

1

43 testcarre(1+x^5); # 1+x^5 n'est pas un carre donc g est d'ordre 2^8.

0

44 g:=puiss(1+x^5,t); # verification:

$x^{63}-x^{31}$

45 b:=[];

[]

46 for i from 0 to 8 do b:=[op(b),puiss(g,2^i)] od;

$[x^{63}-x^{31}, -x^{62}, -x^{60}-x^{28}, x^{56}+x^{24}, x^{48}+x^{16}, x^{32}+1, x^{32}-1, -1, 1]$

47 inve:=proc(v)
puiss(v,q-2)
end proc;

// Warning: q declared as global variable(s)
// End defining inve

```
proc(v)
  puiss(v,q-2);

end;
```

48 z:=1+x;testcarre(z);

(1+x, 1)

49 (u,v):=igcdex(t,2^8)[1..2];

[-107 5606142711964398740514981881]

50 dans cet exemple u est negatif, on cherche donc l'inverse de z

51 z1:=puiss(inve(z),-u*t);

$-x^{50}-x^{18}$

52 z2:=puiss(z,v*2^8);

$-x^{15}-x^{14}$

53 verification de l'isomorphisme produit on doit retrouver z:

54 Rem(z1*z2,P) mod 3;z;

$(1 \cdot x+1, 1+x)$

55 On n'etait pas oblig'e de trouver l'inverse de z, on utilise que z^(q-2)*z=1

56 z1:=puiss(z,(u*t) mod (q-1));

$-x^{50}-x^{18}$

57 Rem(z1*z2,P) mod 3;z; #attention, pour Rem mod il faut des x

$(1 \cdot x+1, 1+x)$

58 on verifie d'abord si q+1 est divisible par 4, si oui c'est tres simple.

59 (q+1) mod 4; #tant pis..

60 racinez2:=puiss(z2,(t+1)/2); #racine de z2:

$x^{63}+x^{60}+x^{59}+x^{57}+x^{56}+x^{55}-x^{54}-x^{53}+x^{52}+x^{51}-x^{50}-x^{49}-x^{48}+x^{47}-x^{46}-x^{45}+x^{44}+x^{39}-x^{37}+x^{36}-x^{35}+x^{33}+x^{32}-$

$-x^{21}-x^{20}-x^{18}-x^{16}+x^{15}+x^{13}+x^{12}+x^{11}+x^{9}-x^{8}+x^{6}+x^{5}+x^{4}+x^{3}+x^{2}+x$

61 puiss(racinez2,2);z2; #verification:

$(-x^{15}-x^{14},\ -x^{15}-x^{14})$

62 m:=[seq(0,8)];xx:=z1; #on sauve z1

$([0\ 0\ 0\ 0\ 0\ 0\ 0\ 0],\ -x^{50}-x^{18})$

63 for i from 7 to 0 by -1 do if Rem(puiss(z1,2^i)+1,P) mod 3 = 0 then
m[8-i]:=1;z1:=Rem(z1*inve(b[8-i]),P) mod 3; else m[8-i]:=0;fi od;

1

64 verification:

65 z1:=1; for i from 1 to 8 do z1:=Rem(z1*puiss(b[i],m[i]),P) mod 3 od: z1;xx;#on verife que l'on trouve bien la valeur sauvee.

$(1,\ \text{Done},\ -x^{50}-x^{18},\ -x^{50}-x^{18})$

66 racinez1:=1;for i from 2 to 8 do racinez1:=Rem(racinez1*puiss(b[i-1],m[i]),P) mod 3 od:puiss(racinez1,2);z1;

$(1,\ \text{Done},\ -x^{50}-x^{18},\ -x^{50}-x^{18})$

67 racinez:=normal(Rem(racinez1*racinez2,P) mod 3);

$-x^{63}+x^{62}+x^{60}-x^{59}+x^{57}+x^{55}-x^{53}-x^{52}-x^{51}+x^{48}+x^{46}+x^{44}+x^{43}-x^{42}+x^{41}-x^{40}-x^{39}-x^{37}+x^{36}+x^{34}-x^{33}+x^{32}+x^{30}$

68 puiss(racinez,2);z;

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

69 Pour avoir la matrice (nombre premier, multiplicite), on utilise en mode xcas
maple_ifactors. En mode maple ifactors coincide avec maple_ifactors.

70 maple_ifactors(36*7)[2];

$$\begin{bmatrix}2 & 2\\ 3 & 2\\ 7 & 1\end{bmatrix}$$

71 ifactors(36*7)[2];

$$\begin{bmatrix}2 & 2\\ 3 & 2\\ 7 & 1\end{bmatrix}$$

72 transpose(ifactors(36*7)[2])[1];

$[2\ 3\ 7]$

73

74 Prog Edit Ajouter nxt OK Save

```
ordre:=proc(x,n)
local m,l,p,y;
m:=Phi(n);
l:=(maple_ifactors(m)[2])
for i from 1 to rowdim(l) do
m:=iquo(m,l[i,1]^l[i,2]);y:=powmod(x,m,n)
while y <> 1 do y:=powmod(y,l[i,1],n);m:=m*l[i,1];od;
od;
m;
end;
```

// Warning: i declared as global variable(s)
// End defining ordre

```
proc(x,n)
  local m,l,p,y;
  m:=Phi(n);
  l:=(maple_ifactors(m))[2];
  for i from 1 to rowdim(l)+1/2 do
  m:=iquo(m,(l[i,1])^(l[i,2]));
  y:=powmod(x,m,n);
  while y<>1 do
    y:=powmod(y,l[i,1],n);
    m:=m*l[i,1];
   od;;
   od;;
  m;
```

75 ordre(-1,2^1000);

2

76 pari();

All PARI functions are now defined with the pari_ prefix.
PARI functions are also defined without prefix except:
abs acos acosh arg asin asinh atan atanh binomial bitand bitor bitxor ceil charpoly concat conj content cos cosh divisors erfc eval exp fa
Note that p-adic numbers must have O argument quoted e.g. 905/7+O('7^3')
Type ?pari for short help
Inside xcas, try Help->Manuals->PARI for HTML help

77 if (pari_znorder(Mod(5,11^5*2^40*101)) == ordre(5,11^5*2^40*101)) then
print("ca marche") else print("il y a une erreur") fi;

"ca marche"

1