1 rt;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

Syntax compatibility mode xcas
Parse error line 1 at pas

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

2 factor(X^128+1 % 3);

Evaluation time: 0.47

$$(1 \% 3 \cdot X^{64} + 1 \% 3 \cdot X^{32} + -1 \% 3) \cdot (1 \% 3 \cdot X^{64} + -1 \% 3 \cdot X^{32} + -1 \% 3)$$

3 P:=(X^64+X^32-1)%3;

$$1 \% 3 \cdot X^{64} + 1 \% 3 \cdot X^{32} + -1 \% 3$$

4 factor(P); //P convient

$$1 \% 3 \cdot X^{64} + 1 \% 3 \cdot X^{32} + -1 \% 3$$

5 ----------Racines carrees----------

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

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

7

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

```
puiss:=proc(g,n)
local u,v;
u:=1;v:=g;//On suppose que g est a coeff  dans Z/3Z. (ie %3)
while(n>1){
 if irem(n , 2 )==0 then v:=rem(v*v,P) ; n:=n/2;
else u:=rem(u*v,P) ; v:=rem(v*v,P) ; n:=(n-1)/2;
fi;
}
rem(u*v,P);
end;
```

// End defining puiss

```
(g,n)->
{ local u,v;
  u:=1;
  v:=g;
  while(n>1){
    if (((irem(n,2))==0)) {
      v:=rem(v*v,P);
      n:=n/2;
    }
    else {
      u:=rem(u*v,P);
      v:=rem(v*v,P);
```

9 puiss((1+x)%3,5^7);

$$1 \% 3 \cdot x^{61} + 1 \% 3 \cdot x^{60} + -1 \% 3 \cdot x^{59} + 1 \% 3 \cdot x^{58} + 0 \% 3 \cdot x^{57} + -1 \% 3 \cdot x^{56} + 1 \% 3 \cdot x^{55} + 0 \% 3 \cdot x^{54} +$$
$$-1 \% 3 \cdot x^{49} + 0 \% 3 \cdot x^{48} + 1 \% 3 \cdot x^{47} + -1 \% 3 \cdot x^{46} + 1 \% 3 \cdot x^{45} + -1 \% 3 \cdot x^{44} + 1 \% 3 \cdot x^{43} + 1 \% 3 \cdot x^{42} +$$
$$0 \% 3 \cdot x^{38} + 0 \% 3 \cdot x^{37} + 0 \% 3 \cdot x^{36} + 0 \% 3 \cdot x^{35} + 0 \% 3 \cdot x^{34} + -1 \% 3 \cdot x^{33} + 1 \% 3 \cdot x^{32} + -1 \% 3 \cdot x^{31} +$$
$$-1 \% 3 \cdot x^{27} + -1 \% 3 \cdot x^{25} + -1 \% 3 \cdot x^{24} + 1 \% 3 \cdot x^{23} + -1 \% 3 \cdot x^{22} + -1 \% 3 \cdot x^{21} + 1 \% 3 \cdot x^{20} + -1 \% 3 \cdot x^{19}$$
$$0 \% 3 \cdot x^{15} + 1 \% 3 \cdot x^{13} + -1 \% 3 \cdot x^{12} + 1 \% 3 \cdot x^{11} + -1 \% 3 \cdot x^{10} + -1 \% 3 \cdot x^{9} + -1 \% 3 \cdot x^{8} + 1 \% 3 \cdot x^{7} + 1 \%$$

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

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

```
11 puiss((1+x)%3,5^7); // on v\'erifie
```

$$1 \% 3 \cdot x^{61} + 1 \% 3 \cdot x^{60} + -1 \% 3 \cdot x^{59} + 1 \% 3 \cdot x^{58} + -1 \% 3 \cdot x^{56} + 1 \% 3 \cdot x^{55} + -1 \% 3 \cdot x^{53} + -1 \% 3 \cdot x^{49} -1 \% 3 \cdot x^{44} + 1 \% 3 \cdot x^{43} + 1 \% 3 \cdot x^{42} + 1 \% 3 \cdot x^{41} + 1 \% 3 \cdot x^{40} + -1 \% 3 \cdot x^{39} + -1 \% 3 \cdot x^{33} + 1 \% 3 \cdot x^{32} + 1 \% 3 \cdot x^{28} + -1 \% 3 \cdot x^{27} + -1 \% 3 \cdot x^{25} + -1 \% 3 \cdot x^{24} + 1 \% 3 \cdot x^{23} + -1 \% 3 \cdot x^{22} + -1 \% 3 \cdot x^{21} + 1 \% 3 \cdot x^{20} 1 \% 3 \cdot x^{13} + -1 \% 3 \cdot x^{12} + 1 \% 3 \cdot x^{11} + -1 \% 3 \cdot x^{10} + -1 \% 3 \cdot x^{9} + -1 \% 3 \cdot x^{8} + 1 \% 3 \cdot x^{7} + 1 \% 3 \cdot x^{6} + -1 \%$$

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

$$(343368382029251248465784908928 1, 1341282742301762689319472300 5)$$

```
13 testcarre:=proc(g)
   evalb(puiss(g,(q-1)/2)=1);//NB: 1%3==1 est vrai
   end proc;
// Warning: q, declared as global variable(s)
// End defining testcarre
```

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

```
14 testcarre(1%3+x); // 1+x ne convient pas
```

$$1$$

```
15 testcarre(1%3+x^5); // 1+x^5 n'est pas un carre donc g est d'ordre 2^8.
```

$$0$$

```
16 g:=puiss(1%3+x^5,t); // verification:
```

$$1 \% 3 \cdot x^{63} + -1 \% 3 \cdot x^{31}$$

```
17 b:=[];
```

$$[]$$

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

$$[1 \% 3 \cdot x^{63} + -1 \% 3 \cdot x^{31}, -1 \% 3 \cdot x^{62}, -1 \% 3 \cdot x^{60} + -1 \% 3 \cdot x^{28}, 1 \% 3 \cdot x^{56} + 1 \% 3 \cdot x^{24}, 1 \% 3 \cdot x^{48}$$

```
19 inve:=proc(v)
   puiss(v,q-2)
   end proc;
// Warning: q, declared as global variable(s)
// End defining inve
```

```
(v)->
 puiss(v,q-2);
}
```

```
20 z:=(1+x)%3;testcarre(z);
```

$$(1 \% 3 \cdot x + 1 \% 3, 1)$$

```
21 (u,v):=igcdex(t,2^8)[0..1];
```

$$[-107, 5606142711964398740514981881]$$

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

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

$$-1 \% 3 \cdot x^{50} + -1 \% 3 \cdot x^{18}$$

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

$$-1 \% 3 \cdot x^{15} + -1 \% 3 \cdot x^{14}$$

```
25 verification de l'isomorphisme  produit on doit retrouver z:
```

```
26 rem(z1*z2,P);z;
```

$$(1 \% 3 \cdot x + 1 \% 3, 1 \% 3 \cdot x + 1 \% 3)$$

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

```
28 z1:=puiss(z,irem(u*t,q-1));
```

$$50 \qquad 18$$

29 rem(z1*z2,P) ;z; //attention, pour rem il faut des pol en x ou preciser la variable

$$(1\,\%\,3 \cdot x + 1\,\%\,3,\ 1\,\%\,3 \cdot x + 1\,\%\,3)$$

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

31 (q+1) % 4; //tant pis..

$$2\,\%\,4$$

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

$$1\,\%\,3 \cdot x^{63} + 1\,\%\,3 \cdot x^{60} + 1\,\%\,3 \cdot x^{59} + 1\,\%\,3 \cdot x^{57} + 1\,\%\,3 \cdot x^{56} + 1\,\%\,3 \cdot x^{55} + -1\,\%\,3 \cdot x^{54} + -1\,\%\,3 \cdot x^{53} +$$
$$-1\,\%\,3 \cdot x^{49} + -1\,\%\,3 \cdot x^{48} + 1\,\%\,3 \cdot x^{47} + -1\,\%\,3 \cdot x^{46} + -1\,\%\,3 \cdot x^{45} + 1\,\%\,3 \cdot x^{44} + 1\,\%\,3 \cdot x^{39} + -1\,\%\,3 \cdot x^{37}$$
$$1\,\%\,3 \cdot x^{33} + 1\,\%\,3 \cdot x^{32} + -1\,\%\,3 \cdot x^{31} + 1\,\%\,3 \cdot x^{30} + 1\,\%\,3 \cdot x^{28} + 1\,\%\,3 \cdot x^{27} + -1\,\%\,3 \cdot x^{26} + -1\,\%\,3 \cdot x^{25} +$$
$$-1\,\%\,3 \cdot x^{20} + -1\,\%\,3 \cdot x^{18} + -1\,\%\,3 \cdot x^{16} + 1\,\%\,3 \cdot x^{15} + 1\,\%\,3 \cdot x^{13} + 1\,\%\,3 \cdot x^{12} + 1\,\%\,3 \cdot x^{11} + 1\,\%\,3 \cdot x^{9} +$$

33 puiss(racinez2,2);z2; //verification:

$$(-1\,\%\,3 \cdot x^{15} + -1\,\%\,3 \cdot x^{14},\ -1\,\%\,3 \cdot x^{15} + -1\,\%\,3 \cdot x^{14})$$

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

$$([0, 0, 0, 0, 0, 0, 0, 0],\ -1\,\%\,3 \cdot x^{50} + -1\,\%\,3 \cdot x^{18})$$

35 for ii from 7 to 0 by -1 do if rem(puiss(z1,2^ii)+1,P) = 0 then
m[7-ii]:=1;z1:=rem(z1*inve(b[7-ii]),P); else m[7-ii]:=0;fi od;

$$1\,\%\,3$$

36 verification:

37 om 0 to 7 do z1:=rem(z1*puiss(b[ii],m[ii]),P) od:; z1;xx;//on verife que l'on trouve bien la valeur sauvee.

$$(1,\ \text{Done},\ -1\,\%\,3 \cdot x^{50} + -1\,\%\,3 \cdot x^{18},\ -1\,\%\,3 \cdot x^{50} + -1\,\%\,3 \cdot x^{18})$$

38 racinez1:=1;for ii from 1 to 7 do racinez1:=rem(racinez1*puiss(b[ii-1],m[ii]),P) od:; puiss(racinez1,2);z1;

$$(1,\ \text{Done},\ -1\,\%\,3 \cdot x^{50} + -1\,\%\,3 \cdot x^{18},\ -1\,\%\,3 \cdot x^{50} + -1\,\%\,3 \cdot x^{18})$$

39 racinez:=normal(rem(racinez1*racinez2 ,P));

$$-1\,\%\,3 \cdot x^{63} + 1\,\%\,3 \cdot x^{62} + 1\,\%\,3 \cdot x^{60} + -1\,\%\,3 \cdot x^{59} + 1\,\%\,3 \cdot x^{57} + 1\,\%\,3 \cdot x^{55} + -1\,\%\,3 \cdot x^{53} + -1\,\%\,3 \cdot x^{52}$$
$$1\,\%\,3 \cdot x^{44} + 1\,\%\,3 \cdot x^{43} + -1\,\%\,3 \cdot x^{42} + 1\,\%\,3 \cdot x^{41} + -1\,\%\,3 \cdot x^{40} + -1\,\%\,3 \cdot x^{39} + -1\,\%\,3 \cdot x^{37} + 1\,\%\,3 \cdot x^{36}$$
$$1\,\%\,3 \cdot x^{30} + -1\,\%\,3 \cdot x^{29} + 1\,\%\,3 \cdot x^{28} + -1\,\%\,3 \cdot x^{26} + -1\,\%\,3 \cdot x^{25} + -1\,\%\,3 \cdot x^{24} + -1\,\%\,3 \cdot x^{23} + 1\,\%\,3 \cdot x^{19}$$
$$1\,\%\,3 \cdot x^{16} + 1\,\%\,3 \cdot x^{15} + -1\,\%\,3 \cdot x^{13} + 1\,\%\,3 \cdot x^{12} + -1\,\%\,3 \cdot x^{10} + -1\,\%\,3 \cdot x^{7} + 1\,\%\,3 \cdot x^{6} + -1\,\%\,3 \cdot x^{4} + -1\,\%$$

40 puiss(racinez,2);z;

$$(1\,\%\,3 \cdot x + 1\,\%\,3,\ 1\,\%\,3 \cdot x + 1\,\%\,3)$$

41 ----------Exercice: Ordre d'un element----------

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

43 maple_ifactors(36*7)[1];

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

44 ifactors(36*7);

$$[2, 2, 3, 2, 7, 1]$$

45 transpose(maple_ifactors(36*7)[1])[0];

$$[2, 3, 7]$$

46

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

```
ordre:=proc(x,n)
local m,l,p,y;
m:=Phi(n);
l:=(maple_ifactors(m)[1]);
for ii from 0 to rowdim(l)-1 do
m:=iquo(m,l[ii,0]^l[ii,1]);y:=powmod(x,m,n);
while(y <> 1){ y:=powmod(y,l[ii,0],n);m:=m*l[ii,0];
od;
m;
end;
```

```
(x,n)->
{ local m,l,p,y;
  m:=Phi(n);
  l:=(maple_ifactors(m))[1];
  for (ii:=0;ii<=(rowdim(l)-1);ii:=ii+abs(1)) {
     m:=iquo(m,(l[ii,0])^(l[ii,1]));
     y:=powmod(x,m,n);
     while(y!=1){
        y:=powmod(y,l[ii,0],n);
        m:=m*l[ii,0];
      };
```

M

48 ordre(-1,2^1000);

2

M

49 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 divi
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
```

M

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

ca marche

1

M