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 (x-1)*(x+1)%5;// Attention le % developpe automatiquement

$$1\,\%\,5\cdot x^2+-1\,\%\,5$$

3 factor(x^2-1)%5;// ca factorise dans Z puis developpe dans Z/5Z

$$1\,\%\,5\cdot x^2+-1\,\%\,5$$

4 factor(x^2-1%5);//ici ca factorise dans Z/5Z

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

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

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

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

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

7 a:=F729(a); //On note a cette classe.

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

8 (1+a)^17

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

9 factor(x^3-x+1%3);

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

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

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

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

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

12 factor((x^(3^5)-x)%3);

Evaluation time: 0.52

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

13 GF(3,20,a); //c'est trop gros:No irreducible primitive polynomial found Error:

No irreducible primitive polynomial found Error: Bad Argument Value

14 factor(X^8+1); factor(X^8+1%3);

$$(X^8+1,\ (1\%3\cdot X^4+1\%3\cdot X^2+-1\%3)\cdot(1\%3\cdot X^4+-1\%3\cdot X^2+-1\%3))$$

15 l:=%{1,2,3,4,3,4%};

[[1, 2, 3, 4]]

16 l:=set[1,2,3,4,3,4];

[[1, 2, 3, 4]]

17 l minus %{1,3%};

[[2, 4]]

18 l minus l;

%{ %}

19

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

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

// End defining orbites

(n)->

21 factor(X^32-1%3);

$$(1\%3\cdot X+1\%3)\cdot(1\%3\cdot X+-1\%3)\cdot(1\%3\cdot X^2+1\%3)\cdot(1\%3\cdot X^2+1\%3\cdot X+-1\%3)\cdot(1\%3\cdot X^2$$
$$(1\%3\cdot X^4+1\%3\cdot X^2+-1\%3)\cdot(1\%3\cdot X^4+-1\%3\cdot X^2+-1\%3)\cdot(1\%3\cdot X^8+1\%3\cdot X^4+-1\%3)\cdot(1$$

22 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 factor(X^14-1%3);

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

24 orbites(14);

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

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

26
```
for ii from 1 to 8 do print(nops(orbites(2^ii)),2^ii) od;
```

```
2,2
3,4
5,8
7,16
9,32
11,64
13,128
15,256
```

1

27
```
(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
```

28
```
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
```

29
```
znorder(3%8);
```

2

30
```
for ii from 1 to 8 do print(znorder(3%2^ii),2^ii) od;
```

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

1

31
```
for ii from 1 to 8 do print(factor(X^(2^ii)-1),2^ii) 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: 0.43
```

1

32
```
le poly cyclo Phi_2^n est phi(n)
```

33
```
phi:=n->X^(2^(n-1))+1;
```

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

2^{n-1}

```
34 for ii from 1 to 8 do print(factor(phi(ii) % 3)) od;
```

```
(1 % 3)*X+1 % 3
(1 % 3)*X^2+1 % 3
((1 % 3)*X^2+(1 % 3)*X-1 % 3)*((1 % 3)*X^2+(-1 % 3)*X-1 % 3)
((1 % 3)*X^4+(1 % 3)*X^2-1 % 3)*((1 % 3)*X^4+(-1 % 3)*X^2-1 % 3)
((1 % 3)*X^8+(1 % 3)*X^4-1 % 3)*((1 % 3)*X^8+(-1 % 3)*X^4-1 % 3)
((1 % 3)*X^16+(1 % 3)*X^8-1 % 3)*((1 % 3)*X^16+(-1 % 3)*X^8-1 % 3)
((1 % 3)*X^32+(1 % 3)*X^16-1 % 3)*((1 % 3)*X^32+(-1 % 3)*X^16-1 % 3)
((1 % 3)*X^64+(1 % 3)*X^32-1 % 3)*((1 % 3)*X^64+(-1 % 3)*X^32-1 % 3)
```

$$1$$

M

```
35 Remarquons aussi que l'ordre de 3 dans le groupe multiplicatif de (Z/2^iZ)
   est le degre des facteurs irreductibles de cyclotomic(2^i) dans Z/3Z[x]
```

```
36 for ii from 1 to 100 do if ((3^ii-1) % 2^8) == 0  then print(ii) fi; od;
```

```
ii:64
```

undef

M

```
37 on prend ii=64
```

```
38 factor(X^128+1 % 3);
```

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

M

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

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

M

```
40 factor(P) ; //P convient
```

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

M

41