TP 4

```
> restart;
```

Mise en place du corps K

```
> p:=3;m:=5;
```

$$p := 3$$
$$m := 5 \quad (1)$$

```
> P:=X^5+X^4+X^2+1;
```

$$P := X^5 + X^4 + X^2 + 1 \quad (2)$$

```
> alias(alpha=RootOf(P,X) mod p);#définit l'extension K=F_p[alpha]
  de degré m
```

$$\alpha \quad (3)$$

```
> p^m;
```

$$243 \quad (4)$$

```
> Power(alpha,p^m-1) mod p ;Power(alpha,(p^m-1)/2) mod p;
```

$$1$$
$$2 \quad (5)$$

```
> n:=p^m-1;
```

$$n := 242 \quad (6)$$

```
> T:=Array(0..n-1,i->Power(alpha,i) mod p):
```

```
> LD:=proc(x)
>   global T,n;
>   local i;
>  for i from 0 to n-1 do
>     if T[i]=x  then return i end if;
>   end do;
> FAIL
> end proc:
```

```
> F:=i->p*i mod n;
```

$$F := i \rightarrow p\, i \bmod n \quad (7)$$

```
> Orb:=proc(i::nonnegint)
```

```
> description "calcule les classes cyclotomipues";
> global n;local Omega,j;
> if i>=n then error "mauvais argument" end if;
> Omega:=[];j:=i;
>  do
>    Omega:=[op(Omega),j];
>    j:=F(j);
>    if member(j,Omega) then return Omega end if;
>        end do;
>   FAIL;
> end proc:
> Orb(6);
```

$$[6, 18, 54, 162, 2] \quad (8)$$

Construction du code BCH

la distance apparente du code BCH

```
> delta:=8;
```

$$\delta := 8 \quad (9)$$

```
> L:=[seq(Orb(i),i=1..delta-1)];
```

$$L := [[1, 3, 9, 27, 81], [2, 6, 18, 54, 162], [3, 9, 27, 81, 1], [4, 12, 36, 108, 82], [5, 15, 45, 135, 163], [6, 18, 54, 162, 2], [7, 21, 63, 189, 83]] \quad (10)$$

```
> J :=convert({op(map(op,L))},list);
```

$$J := [1, 2, 3, 4, 5, 6, 7, 9, 12, 15, 18, 21, 27, 36, 45, 54, 63, 81, 82, 83, 108, 135, 162, 163, 189] \quad (11)$$

(12)

les racines du code

```
> rac:=map(i -> T[i],J);
```

$$rac := [\alpha, \alpha^2, \alpha^3, \alpha^4, 2\alpha^4+2\alpha^2+2, \alpha^4+2\alpha^3+\alpha^2+2\alpha+1, \alpha^4+\alpha^3+\alpha^2+\alpha+2, \alpha^4+2\alpha^2+2\alpha, \alpha^4+\alpha^3+2\alpha^2+\alpha, \alpha^4+1, \alpha^4+2\alpha^3+\alpha^2+\alpha+2, \alpha^3+2\alpha^2+2\alpha, \alpha^3+\alpha^2+2\alpha+2, \alpha^4+\alpha+2, \alpha^4+\alpha^3+2\alpha^2+\alpha+1, \alpha^4+\alpha^3+\alpha^2+\alpha, \alpha^2+2, 2\alpha^4+\alpha^3+\alpha, 2\alpha^4+2\alpha^2+1, \alpha^4+2\alpha^3+\alpha^2+\alpha+1, \alpha^4+2\alpha^3+2\alpha^2+\alpha+2, \alpha^4+\alpha, \alpha^3+2\alpha^2+2\alpha+1, \alpha^4+2\alpha^3+2\alpha^2+\alpha, \alpha^4+2\alpha^3+\alpha^2+2\alpha] \quad (13)$$

le polynôme générateur

```
> g:=sort(Expand(mul(X-r,r in rac)) mod p,X);
```

$$g := X^{25} + X^{24} + X^{22} + X^{21} + X^{20} + 2X^{18} + 2X^{17} + 2X^{16} + 2X^{15} + X^{13} + 2X^{12} + X^{10} + 2X^{8} + X^{4} + X^{3} + X^{2} + 2X + 1 \quad (14)$$

la dimension

```
> k:=n-degree(g,X);
```

$$k := 217 \quad (15)$$

le nombre de mots du code

```
> p^k;
```

$$343014338185106544799976221490560728408063812407121477134594544147051677470\backslash 701808241506681192482333121 63 \quad (16)$$