TP 3

Exercice 1

```
> restart;
> with(numtheory):
> racines:=proc(p::prime,m::posint)
>   local L;
>   L:=convert(divisors(p^m-1),list)[2..-1];
>   return select(n->order(p,n)=m,L)
>   end proc:
```

```
> p:=5;
```

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

```
> m:=6;
```

$$m := 6 \quad (2)$$

```
> p^m;
```

$$15625 \quad (3)$$

```
> N:=racines(p,m);
```

$$N := [7, 9, 14, 18, 21, 28, 36, 42, 56, 63, 72, 84, 93, 126, 168, 186, 217, 248, 252, 279, 372, 434, 504, 558, 651, 744, 868, 1116, 1302, 1736, 1953, 2232, 2604, 3906, 5208, 7812, 15624] \quad (4)$$

```
> F:=map(n->iquo(phi(n),m),N);
```

$$F := [1, 1, 1, 1, 2, 2, 2, 2, 4, 6, 4, 4, 10, 6, 8, 10, 30, 20, 12, 30, 20, 30, 24, 30, 60, 40, 60, 60, 60, 120, 180, 120, 120, 180, 240, 360, 720] \quad (5)$$

```
> add(n,n in F); # nombre de corps finis distincts (mais tous
  isomorphes entre eux) de cardinal 15625
```

$$2580 \quad (6)$$

Exercice 2

```
> n:=N[19];
```

$$n := 252 \quad (7)$$

```
> F[19];
```

$$12 \quad (8)$$

```
> Phi:=cyclotomic(n,X);
```

$$\Phi := 1 + X^6 - X^{18} - X^{24} + X^{36} - X^{48} - X^{54} + X^{66} + X^{72} \quad (9)$$

```
> d:=iquo(phi(n),m);  # modulo p F se factorise en 12 facteurs tous
  de degré 6
```

$$d := 12 \quad (10)$$

```
> FF:=Factors(Phi) mod p;
```

$$FF := [1, [[X^6 + 3X^5 + 3X^4 + 2X^2 + 3X + 4, 1], [X^6 + X^5 + 3X^4 + X^3 + 2X^2 + X + 4, 1], [X^6 + 4X^5 + 2X^4 + 3X^2 + 4X + 4, 1], [X^6 + X^5 + 2X^4 + 3X^2 + X + 4, 1], [X^6 + 4X^4 + 4X^3 + X^2 + 4, 1], [X^6 + 4X^5 + 2X^4 + X^3 + 3X^2 + 4X + 4, 1], [X^6 + X^5 + 4X^3 + X \quad (11)$$

$$+4,1],[X^6+2X^5+3X^4+2X^2+2X+4,1],[X^6+X^5+2X^4+4X^3+3X^2+X+4,1],[X^6+4X^5+3X^4+4X^3+2X^2+4X+4,1],[X^6+4X^4+X^3+X^2+4,1],[X^6+4X^5+X^3+4X+4,1]]]$$

```
> LFF:=map(F->F[1],FF[2]);
```

$$LFF := [X^6+3X^5+3X^4+2X^2+3X+4, X^6+X^5+3X^4+X^3+2X^2+X+4, X^6+4X^5+2X^4+3X^2+4X+4, X^6+X^5+2X^4+3X^2+X+4, X^6+4X^4+4X^3+X^2+4, X^6+4X^5+2X^4+X^3+3X^2+4X+4, X^6+X^5+4X^3+X+4, X^6+2X^5+3X^4+2X^2+2X+4, X^6+X^5+2X^4+4X^3+3X^2+X+4, X^6+4X^5+3X^4+4X^3+2X^2+4X+4, X^6+4X^4+X^3+X^2+4, X^6+4X^5+X^3+4X+4] \quad (12)$$

```
> P:=LFF[4];  # on choisit l'un des facteurs irréductibles de F mod p
```

$$P := X^6+X^5+2X^4+3X^2+X+4 \quad (13)$$

```
> alias(x=RootOf(P,X) mod p);  # définit l'élément primitif x de K= F_p[x]$
```

$$x \quad (14)$$

```
> Power(x,6) mod p;
```

$$4x^5+3x^4+2x^2+4x+1 \quad (15)$$

```
> Power(x,n) mod p;Power(x,n/2) mod p;  # x est bien d'ordre 256
```

$$1$$

$$4 \quad (16)$$

```
> d:= trunc(sqrt(n));
```

$$d := 15 \quad (17)$$

```
> n_sur_d:=iquo(n,d);
```

$$n\_sur\_d := 16 \quad (18)$$

```
> U:=[seq(Power(x,r) mod p, r=0..d-1)];
```

$$U := [1, x, x^2, x^3, x^4, x^5, 4x^5+3x^4+2x^2+4x+1, 4x^5+2x^4+2x^3+2x^2+2x+4, 3x^5+4x^4+2x^3+4, x^5+x^4+x^2+x+3, 3x^4+x^3+3x^2+2x+1, 3x^5+x^4+3x^3+2x^2+x, 3x^5+2x^4+2x^3+2x^2+2x+3, 4x^5+x^4+2x^3+3x^2+3, 2x^5+4x^4+3x^3+3x^2+4x+4] \quad (19)$$

```
> y:=Power(x,n-d) mod p;
```

$$y := 3x^4+x^2+4x \quad (20)$$

```
> V:=[seq(Power(y,q) mod p, q=0..n_sur_d)];
```

$$V := [1, 3x^4+x^2+4x, x^3+3x^2+4x+2, x^5+x^4+2x^3+2x^2+1, 3x^3, 4x^5+3x^3+3x^2+3x+1, x^5+x^4+x^3+x^2+2x+3, x^5+x^4+3x^2, x^5+2x^4+3x^2+x+4, x^5+4x^4+2x^3+3x^2+x+2, x^5+3x^4+x^3+2x^2+3x+2, 3x^4+2x^3+x^2+x+4, 2x^5+2x^4+2x^2+2x+1, 2x^4+x^3+x^2+3x+1, 3x^5+3x^4+4x^2+1, 3x^5+4x^4+2x+2, 3x^5+2x^4+2x^3+2x^2+2x+3] \quad (21)$$

```
> z1:=x^5+2*x^2+x+3;
```

$$z1 := x^5+2x^2+x+3 \quad (22)$$

```
> for v in V do
>        zz:=evala(z1*v) mod p;
>        if member(zz,U,'r') then
>                                  member(v,V,'q');q:=q-1;r:=r-1;
>                                  break;
>                                  end if;
>        end do:
> k:=q*d+r:
> q,r,k,evalb(z1=Power(x,k) mod p);
```

$$8,\ 3,\ 123,\ true \qquad \textbf{(23)}$$

```
> z2:=3*x^4+3*x^3+x^2+2*x+4;
```

$$z2 := 3\,x^4 + 3\,x^3 + x^2 + 2\,x + 4 \qquad \textbf{(24)}$$

```
> unassign('q','r');
> for v in V do
>        zz:=evala(z2*v) mod p;
>        if member(zz,U,'r') then
>                                  member(v,V,'q');q:=q-1;r:=r-1;
>                                  break;
>                                  end if;
>        end do:
> k:=q*d+r:
> q,r,k;
```

$$q,\ r,\ 15\,q + r \qquad \textbf{(25)}$$