```
> 7^3;
```

343

Pour travailler dans GF(343), cherchons un polynôme irréductible du type X^3+a dans Z/7Z . Comme le degré est 3, X^3+a est irréductible seulement si il n'a pas de racine.

```
> for i from 0 to 6 do i^3 mod 7; od;
```

0

1

1

6

1

6

6

Donc, X^3-2, X^3-3, X^3-4, X^3-5 sont irréductibles. Prenons, par exemple X^3+3.

```
> Irreduc(X^3+3) mod 7;
```

true

Les éléments de GF(343) sont donc les a+bX+cX^2 modulo 7 et X^3+3.

Calculons R := [1 2 3] / [4 5 6]

```
> Gcdex(4+5*X+6*X^2, X^3+3, X, 'U','V') mod 7; U;
> R:=Rem( (1+2*X+3*X^2) * U,  X^3+3, X ) mod 7;
```

Vérifions le résultat

```
> Rem( R * (4+5*X+6*X^2),  X^3+3, X ) mod 7;
```

1

$$2 X^2 + 3 X + 2$$

$$R := 3 X + 5$$

$$1 + 2 X + 3 X^2$$

Cherchons un générateur de GF(343) ; X est-il générateur ?

```
> Rem( X^3,  X^3+3, X ) mod 7;
```

4

Or nous connaissons l'ordre de 4 modulo 7

```
> 4^3 mod 7;
```

1

Donc, X est d'ordre seulement 9 (et non 342 !) dans GF(343), il n'est donc pas générateur.

```
> Rem( X^9,  X^3+3, X ) mod 7;
```

1

Voici la procédure générale pour tester si un élément de GF(q) est générateur

```
> Test_Poly_Générateur:=proc(q, Irred, A)
      local F, ordremax, i, e, Power, test, AA;

      # Au cas où A ne serait pas de degré inférieur à Irred
      AA := Gcd(Irred, A) mod q;
      if ( AA <> 1 ) then test:= false;

      else

          ordremax:=q^degree(Irred,X)-1;
          F:=map2(op, 1, op(2, ifactors( ordremax )));
          printf("Facteurs de %d : ",ordremax); lprint( op(F));

          test:=true;
          for i to nops(F) do

                e:=ordremax/F[i];
                Power:=Powmod( A, e, Irred, X) mod q ;
                printf("A^%d : ", e); lprint(Power);

                if ( Power = 1 ) then test:=false; end;

            od;
      end;
      test;
> end:
```

Testons X : [0 1 0], est-il générateur ?

```
> Test_Poly_Générateur( 7, X^3+3, X );
Facteurs de 342 : 2, 3, 19
A^171 : 1
A^114 : 2
A^18 : 1
```

false

Prenons un élément au hasard (ou presque) : [3 3 6], est-il générateur ?

```
> Test_Poly_Générateur( 7, X^3+3, 3+3*X+6*X^2 );
Facteurs de 342 : 2, 3, 19
A^171 : 6
A^114 : 2
A^18 : 2*X^2+6
```

true

$$Generator := 3 + 3\,X + 6\,X^2$$

```
> Generator:=3+3*X+6*X^2;
```

$$Generator := 3 + 3\,X + 6\,X^2$$

Création des tables de correspondance

```
> Index_To_Polynom:=Array(1..342):
  Prod:=1: for i from 1 to 342 do Prod:=Rem(Prod*Generator, X^3+3,
  X) mod 7; Index_To_Polynom[i]:=subs({X=7},Prod); od:
  Index_To_Polynom[171];
```

$$6$$

```
> Polynom_To_Index:=Array(1..342):
  for i from 1 to 342 do Polynom_To_Index[ Index_To_Polynom[i] ]:=
  i; od:
  Polynom_To_Index[1];
```

$$342$$

```
> Padic_To_Polynom:=proc(j, p)
  local Pol, Deg, q, r; Pol:=0; Deg:=1; q:=j;
  while(q>0) do
     r := q mod p;
     q := (q - r)/p;
     Pol:=Pol+Deg*r;
     Deg:=Deg*X;
  od;
  Pol;
  end:
```

Calcul de [1 2 3] / [4 5 6]

```
> Index123:=Polynom_To_Index[ subs({X=7},1+2*X+3*X^2) ];
  Index456:=Polynom_To_Index[ subs({X=7},4+5*X+6*X^2) ];
  IndexDiv:=Index123-Index456; if( IndexDiv < 0) then
  IndexDiv:=IndexDiv+342; end;
  Division:=Index_To_Polynom[ IndexDiv ];
  Padic_To_Polynom( Division, 7 );
```

$$Index123 := 36$$

$$Index456 := 268$$

$$IndexDiv := -232$$

$$IndexDiv := 110$$

$$Division := 26$$

$$3\,X + 5$$