

un jeu

26 juin 2016

Soit pour $n \in \mathbb{N}$, l'ensemble $E = \{1, 2, \dots, n\}$.

On veut construire un jeu comportant n cartes C_j pour $j = 1..n$ de façon que chaque carte C_j ait comme valeur un sous ensemble de E :

$C_j \subset E$,

$\text{Card}(C_j) = m$ et

$\text{Card}(C_j \cap C_k) = 1$ pour tout j et tout $k \neq j$.

1 Le point de vue naïf

Comment choisir n ? Écrire un programme qui teste que dans un jeu on a $\text{Card}(C_j \cap C_k) = 1$

et trouver un algorithme qui renvoie la valeur des n cartes C_j $j = 1..n$.

Par exemple, en écrivant la valeur des cartes sous la forme d'une liste :

si $n = 3$ on a $m = 2$ et les 3 cartes du jeu J_2 sont : $[1, 2], [1, 3], [2, 3]$

et le jeu J_2 est $[[1, 2], [1, 3], [2, 3]]$

si $n = 4, 5, 6$ il n'y a pas de solution.

si $n = 7$ on a $p = 3$ et les 7 cartes du jeu J_3 sont : $[1, 2, 3], [1, 4, 5], [1, 6, 7], [2, 4, 6], [2, 5, 7], [3, 4, 7], [3, 5, 6]$

et le jeu J_3 est $[[1, 2, 3], [1, 4, 5], [1, 6, 7], [2, 4, 6], [2, 5, 7], [3, 4, 7], [3, 5, 6]]$

Sur chacune des n cartes il y a m nombres : on a donc en tout $n * m$ nombres et pour des raisons de symétrie, chaque nombre figure m fois donc :

il y a m cartes qui contiennent 1,

il y a m cartes qui contiennent 2,

....

il y a m cartes qui contiennent n .

L'ensemble des éléments des m cartes qui contiennent 1 est E donc :

puisque l'ensemble des éléments des m cartes qui contiennent 1 est constitué de 1 et de $m - 1$ éléments différents de 1, on a donc en tout $m(m - 1)$ éléments différents de 1, donc en tout $m(m - 1) + 1$ éléments qui constituent E donc :

$$n = m(m - 1) + 1$$

Ainsi en écrivant la valeur des cartes sous la forme d'une liste pour :

$m = 2$ on a $n = 3$ et

$J_2 := [[1, 2], [1, 3], [2, 3]]$
 $m = 3$ on a $n = 7$ et
 $J_3 := [[1, 2, 3], [1, 4, 5], [1, 6, 7], [2, 4, 6], [2, 5, 7], [3, 4, 7], [3, 5, 6]]$
 $m = 4$ on a $n = 13$ et
 $J_4 := [[1, 2, 3, 4], [1, 5, 6, 7], [1, 8, 9, 10], [1, 11, 12, 13],$
 $[2, 5, 8, 11], [2, 6, 9, 12], [2, 7, 10, 13], [3, 5, 9, 13],$
 $[3, 6, 10, 11], [3, 7, 8, 12], [4, 5, 10, 12], [4, 6, 8, 13], [4, 7, 9, 11]]$
 $m = 5$ on a $n = 21$ et
 $J_5 := [[1, 2, 3, 4, 5],$
 $[1, 6, 7, 8, 9], [1, 10, 11, 12, 13], [1, 14, 15, 16, 17], [1, 18, 19, 20, 21],$
 $[2, 6, 10, 14, 18], [2, 7, 11, 15, 19], [2, 8, 12, 16, 20], [2, 9, 13, 17, 21],$
 $[3, 6, 12, 17, 19], [3, 7, 13, 16, 18], [3, 8, 10, 15, 21], [3, 9, 11, 14, 20],$
 $[4, 6, 13, 15, 20], [4, 7, 12, 14, 21], [4, 8, 11, 17, 18], [4, 9, 10, 16, 19],$
 $[5, 6, 11, 16, 21], [5, 7, 10, 17, 20], [5, 8, 13, 14, 19], [5, 9, 12, 15, 18]]$
 $m = 6$ on a $n = 31$ et
 $J_6 := [[1, 2, 3, 4, 5, 6],$
 $[1, 7, 8, 9, 10, 11], [1, 12, 13, 14, 15, 16], [1, 17, 18, 19, 20, 21], [1, 22, 23, 24, 25, 26], [1, 27, 28, 29, 30, 31],$
 $[2, 7, 12, 17, 22, 27], [2, 8, 13, 18, 23, 28], [2, 9, 14, 19, 24, 29], [2, 10, 15, 20, 25, 30], [2, 11, 16, 21, 26, 31],$
 $[3, 7, 13, 19, 25, 31], [3, 8, 14, 20, 26, 27], [3, 9, 15, 21, 22, 28], [3, 10, 16, 17, 23, 29], [3, 11, 12, 18, 24, 30],$
 $[4, 7, 14, 21, 23, 30], [4, 8, 15, 17, 24, 31], [4, 9, 16, 18, 25, 27], [4, 10, 12, 19, 26, 28], [4, 11, 13, 20, 22, 29],$
 $[5, 7, 16, 20, 24, 28], [5, 8, 12, 21, 25, 29], [5, 9, 13, 17, 26, 30], [5, 10, 14, 18, 22, 31], [5, 11, 15, 19, 23, 27],$
 $[6, 7, 15, 18, 26, 29], [6, 8, 16, 19, 22, 30], [6, 9, 12, 20, 23, 31], [6, 10, 13, 21, 24, 27], [6, 11, 14, 17, 25, 28]]$

Écrivons un programme qui teste que dans un jeu on a :

$\text{Card}(C_j \cap C_k) = 1$ pour tout j et tout $k \neq j$.

On tape :

```

testcarte(L) := {
local j,k,s,S;
s:=size(L);
S:=set[op(L[j])] $ (j=0..s-1);
pour j de 0 jusque s-2 faire
    pour k de j+1 jusque s-1 faire
        si size(S[j] intersect S[k])!=1 alors
            retourne [j,k];
    fsi;
fpour;
retourne 1;
};

```

On tape :

```

J6:=[[1,2,3,4,5,6],[1,7,8,9,10,11],[1,12,13,14,15,16],[1,17,18,19,20,21],
[1,22,23,24,25,26],[1,27,28,29,30,31],[2,7,12,17,22,27],[2,8,13,18,23,28],
[2,9,14,19,24,29],[2,10,15,20,25,30],[2,11,16,21,26,31],[3,7,13,19,25,31],
[3,8,14,20,26,27],[3,9,15,21,22,28],[3,10,16,17,23,29],[3,11,12,18,24,30],
[4,7,14,21,23,30],[4,8,15,17,24,31],[4,9,16,18,25,27],[4,10,12,19,26,28],
[4,11,13,20,22,29],[5,7,16,20,24,28],[5,8,12,21,25,29],[5,9,13,17,26,30],

```

```
[5, 10, 14, 18, 22, 31], [5, 11, 15, 19, 23, 27], [6, 7, 15, 18, 26, 29], [6, 8, 16, 19, 22, 30],
[6, 9, 12, 20, 23, 31], [6, 10, 13, 21, 24, 27], [6, 11, 14, 17, 25, 28]]];
```

```
testcarte(J6)
```

On obtient :

```
1
```

Mais pour l'instant je n'ai pas trouvé d'algorithme...

Par exemple pour $p = 7$ et $n = 43$?????

Pour $p = 6$ et $n = 31$, les cartes contenant C_1, C_2, C_3 sont obtenues systématiquement puis je fais différents raisonnements ce qui donne le programme qui suit.

On tape :

```
dobbleprog(m) := {
local n, T, L1, L2, j, Rep, LL2, L, l;
n:=m*(m-1)+1;
T:=[k$(k=1..m)];
L1:=T;
pour j:=1 jusqu' m-1 faire
  T:=[T[0], (T[k]+m-1)$(k=1..m-1)];
  L1:=L1, T;
fpour;
Rep:=L1;
L1:=[L1];
L2:=[col(L1, k)$(k=1..m-1)];
pour j:=1 jusqu' m-2 faire
  L2[j, 0]:=2;
fpour;
L2:=op(L2);
Rep:=Rep, L2;
LL2:=NULL;
pour j de 1 jusqu' m-1 faire
  LL2:=LL2, L2;
  fpour;
  LL2:=[LL2];
pour l de 3 jusqu' m faire
  L:=NULL;
  pour j de 0 jusqu' m-2 faire
    L:=L, [1, LL2[(l-2)*(k-1)+j, k]$(k=1..m-1)];
  fpour;
Rep:=Rep, L;
fpour;
retourne [Rep];
};;
```

Puis on teste en tapant :

```
D:=[dobbleprog(m)$(m=2..32)];;
```

```
testcarte(D[k])$(k=0..30)
```

On obtient :

1, 1, 1, [5, 13], 1, [7, 19], 1, [9, 25], [10, 37], [11, 31], 1,
 [13, 37], 1, [15, 43], [16, 61], [17, 49], 1, [19, 55], 1, [21, 61]
 [22, 85], [23, 67], 1, [25, 73], [26, 151], [27, 79], [28, 109],
 [29, 85], 1, [31, 91], 1

ce qui veut dire que le programme renvoie une solution pour :

$m = 2, 3, 4, 6, 8, 12, 14, 18, 20, 24, 30, 32$ c'est à dire pour :

$n = 3, 7, 13, 31, 57, 133, 183, 307, 381, 553, 871, 993$ $p = m-1 = 1, 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31$

2 Avec un peu de Mathématiques

Soit le corps $K = \mathbb{Z}/3\mathbb{Z}$. K a comme éléments 0,1,2.

Considérons le plan projectif $P = K^{3*}/K^*$.

P a 13 points qui sont :

- 4 points à l'infini :
 (1,0,0), (0,1,0), (1,1,0), (1,2,0)
- 9 points à distance finie :
 (0,0,1), (1,0,1), (2,0,1)
 (0,1,1), (1,1,1), (2,1,1)
 (0,2,1), (1,2,1), (2,2,1)

P a 13 droites :

- la droite de l'infini qui contient les 4 points à l'infini,
- 3 droites parallèles de direction (1,0,0) contenant chacune 4 points : le point à l'infini (1,0,0) et 3 points à distance finie.
 On a :
 la droite passant par les 3 points à distance finie $(0, 0, 1) + k(1, 0, 0)$ pour $k \in K$
 i.e. $k = 0, 1, 2$:
 (0,0,1), (1,0,1), (2,0,1).
 la droite passant par les 3 points à distance finie $(0, 1, 1) + k(1, 0, 0)$ pour $k \in K$
 i.e. $k = 0, 1, 2$:
 (0,1,1), (1,1,1), (2,1,1).
 la droite passant par les 3 points à distance finie $(0, 2, 1) + k(1, 0, 0)$ pour $k \in K$
 i.e. $k = 0, 1, 2$:
 (0,2,1), (1,2,1), (2,2,1).
- 3 droites parallèles de direction (0,1,0) contenant chacune 4 points : le point à l'infini (0,1,0) et 3 points à distance finie.
 On a :
 la droite passant par les 3 points à distance finie $(0, 0, 1) + k(0, 1, 0)$ pour $k \in K$
 i.e. $k = 0, 1, 2$:
 (0,0,1), (0,1,1), (0,2,1).
 la droite passant par les 3 points à distance finie $(1, 0, 1) + k(0, 1, 0)$ pour $k \in K$
 i.e. $k = 0, 1, 2$:
 (1,0,1), (1,1,1), (1,2,1) .
 la droite passant par les 3 points à distance finie $(2, 0, 1) + k(0, 1, 0)$ pour $k \in K$
 i.e. $k = 0, 1, 2$:
 (2,0,1), (2,1,1), (2,2,1).

- 3 droites parallèles de direction $(1,1,0)$ contenant chacune 4 points : le point à l'infini $(1,1,0)$ et 3 points à distance finie.
On a :
la droite passant par les 3 points à distance finie $(0, 0, 1) + k(1, 1, 0)$ pour $k \in K$
i.e. $k = 0, 1, 2$:
 $(0,0,1), (1,1,1), (2,2,1)$.
la droite passant par les 3 points à distance finie $(0, 1, 1) + k(1, 1, 0)$ pour $k \in K$
i.e. $k = 0, 1, 2$:
 $(0,1,1), (1,2,1), (2,0,1)$.
la droite passant par les 3 points à distance finie $(0, 2, 1) + k(1, 1, 0)$ pour $k \in K$
i.e. $k = 0, 1, 2$:
 $(0,2,1), (1,0,1), (2,1,1)$.
- 3 droites parallèles de direction $(1,2,0)$ contenant chacune 4 points : le point à l'infini $(1,2,0)$ et 3 points à distance finie.
On a :
la droite passant par les 3 points à distance finie $(0, 0, 1) + k(1, 2, 0)$ pour $k \in K$
i.e. $k = 0, 1, 2$:
 $(0,0,1), (1,2,1), (2,1,1)$.
la droite passant par les 3 points à distance finie $(0, 1, 1) + k(1, 2, 0)$ pour $k \in K$
i.e. $k = 0, 1, 2$:
 $(0,1,1), (1,0,1), (2,2,1)$.
la droite passant par les 3 points à distance finie $(0, 2, 1) + k(1, 2, 0)$ pour $k \in K$
i.e. $k = 0, 1, 2$:
 $(0,2,1), (1,1,1), (2,0,1)$.

Chacune de ces 13 droites sont concourantes et correspondent à 13 cartes contenant chacune 4 objets.

On peut généraliser facilement pour lorsque K est le corps $K = \mathbb{Z}/p\mathbb{Z}$ pour p premier : le plan projectif $P = K^{3*}/K^*$ a $p^2 + p + 1 = p(p + 1) + 1$ points : p^2 points à distance finie et $p + 1$ points l'infini et dans ce plan on a $p + 1$ droites contenant chacune $p + 1$ points : le m du programme naïf est donc $m = p + 1$ avec p premier.

En effet :

Pour connaître les valeurs de $p = m - 1$ pour lesquelles le programme naïf renvoie une solution, on tape :

```
lesuns(D) := {
local k, M, s;
M:=NULL;
s:=size(D)-1;
pour k de 0 jusqu'à s faire
si testcarte(D[k])==1 alors M:=M, k+1; fsi;
fpour
retourne M;
} ;
```

```

On tape :
D:=[dobbleprog(m)$ (m=2..50)]
On obtient :
Done
On tape :
lesuns(D)
On obtient la liste des 16 premiers nombres premiers (Temps mis pour l'évaluation :
569.29) :
(1,2,3,5,7,11,13,17,19,23,29,31,37,41,43,47)
On tape :
ithprime(k)$ (k=0..15)
On obtient :
(1,2,3,5,7,11,13,17,19,23,29,31,37,41,43,47)

```

3 Programme lorsque K est un corps fini

Puisque le cardinal d'un corps fini K est q^n avec q premier et $n \in \mathbb{N}$, on peut trouver une solution lorsque $p = m - 1 = q^n$ avec q premier et $n \in \mathbb{N}$.

On peut construire un corps fini K de cardinal q^n avec q premier et $n \in \mathbb{N}$ en prenant : $K = \mathbb{Z}/q\mathbb{Z}[x] \bmod (P[x] \bmod q)$ où $P[x] \bmod q$ est un polynôme irréductible de $\mathbb{Z}/q\mathbb{Z}[x]$ de degré n .

Par exemple :

Pour $m - 1 = p = 4 = 2^2$, on a $K4 = \mathbb{Z}/2\mathbb{Z}[x] \bmod (x^2 + x + 1 \bmod 2)$

Pour $m - 1 = p = 8 = 2^3$, on a $K8 = \mathbb{Z}/2\mathbb{Z}[x] \bmod (x^3 + x + 1 \bmod 2)$

Pour $m - 1 = p = 9 = 3^2$, on a $K9 = \mathbb{Z}/3\mathbb{Z}[x] \bmod (x^2 + 1 \bmod 3)$

etc...

3.1 Les tables d'addition et de multiplication

Soit P le polynôme à coefficients dans $\mathbb{Z}/q\mathbb{Z}$ avec q premier tel que $\mathbb{Z}/q\mathbb{Z}[x] \bmod P$ soit un corps.

On note K la liste des éléments de $\mathbb{Z}/q\mathbb{Z}[x] \bmod P$. On représente les éléments de $\mathbb{Z}/q\mathbb{Z}[x] \bmod P$ par l'indice qu'ils ont dans K .

On a donc besoin de la commande indice qui renvoie l'indice d'un élément dans une liste et "erreur" lorsque l'élément n'est pas dans la liste.

On tape :

```

// renvoie l'indice de a dans la liste L sinon renvoie erreur
indice(a,L):={
indice(a,L):={
local k;
k:=member(normal(a),L);
si k!=0 alors

```

```

    retourne k-1;
  fsi;
  retourne "erreur";
};

```

Si $K[a] \in \mathbb{Z}/q\mathbb{Z}[x] \bmod P$ et $K[b] \in \mathbb{Z}/q\mathbb{Z}[x] \bmod P$ on a :

`addi(a,b,K,P)` est égal à l'indice de la somme de $K[a] + K[b]$ dans K et

`prod(a,b,K,P)` est égal à l'indice du produit $K[a] * K[b]$ dans K .

Par exemple si $q = 2$ et $P = (x^2 + x + 1) \bmod 2$ on a :

$K = [0\%2, 1\%2, x * 1\%2, 1\%2 + x * 1\%2]$

`addi(0,j)=j` pour $j = 0..3$

`addi(1,2)=3` car $(1\%2) + (x * 1\%2) = 1\%2 + x * 1\%2$

`prod(3,2)=1` car $(1\%2 + x * 1\%2) * (x * 1\%2) = 1\%2 \bmod (x^2 + x + 1)\%2$

On tape :

```

//addi(a,b,K,P) renvoie l'indice dans la liste K de la somme (K[a]+K[b])mod (P)
addi(a,b,K,P):={
  retourne indice((K[a]+K[b]) mod (P),K);
};
//prod(a,b,K,P)renvoie l'indice dans la liste K du produit (K[a]*K[b])mod (P)
prod(a,b,K,P):={
  retourne indice((K[a]*K[b])mod (P),K);
};

```

Lorsque L est une liste d'indice de K , on rajoute la commande `prodl(a,L,K,P)` qui renvoie la liste d'éléments $a * L[j]$ pour $j = 0..size(L) - 1$.

Lorsque L_1 et L_2 sont 2 listes d'indice de K de même longueur, on rajoute la commande `addill(L1,L2,K,P)` qui renvoie la liste d'éléments $L_1[j] + L_2[j]$ pour $j = 0..size(L_1) - 1$.

On tape :

```

//pour L une liste d'indice de taille s, prodl(a,L,K,P) renvoie
//la liste des indices dans la liste K du produit (K[a]*K[L[k]])mod (P) (k=0..s)
prodl(a,L,K,P):={
  local s;
  s:=size(L)-1;
  retourne [prod(a,L[k],K,P)$(k=0..s)];
};
//pour L1 et L2 2 listes d'indice de taille s addill(L1,L2,K,P) renvoie
//la liste des indices dans la liste K de la somme (K[L1[k]]+K[L2[k]])mod (P)
addill(L1,L2,K,P):={
  local s1,s2;
  s1:=size(L1)-1;
  s2:=size(L2)-1;
  si s1==s2 alors

```

```

    retourne [addi(L1[k],L2[k],K,P)$(k=0..s1)];
  fsi;
retourne "erreur";
};;

```

3.2 La répartition pour $p = 4$

On définit le corps $L4$ de cardinal 4 et le polygône $P4$.

Puis on écrit la fonction de répartition : on remarquera que pour que les indices des éléments du plan projectif PP commencent à 1 on a rajouté l'élément $[0, 0, 0]$ au début de la séquence constituée par les éléments de PP .

```

K4() := {
  local L4, j, k, s, x;
  purge(x);
  L4:=NULL;
  pour k de 0 jusque 1 faire
    pour j de 0 jusque 1 faire
      s:=x*k+j;
      L4:=L4,normal(s %2) ;
    fpour;
  fpour;
  return [L4];
};;
P4:=(x^2+x+1)%2;;
L4:=K4();;
repart4(L4,P4):={
  local k, j, L, Le, n, Rep, PP;
  PP:=[0,0,0],[1,0,0],[0,1,0],([1,k,0])$(k=1..3);
  pour k de 0 jusque 3 faire
    pour j de 0 jusque 3 faire
      PP:=PP,[j,k,1];
    fpour;
  fpour;
  PP:=[PP];
  Rep:=[1,(k+j*4)$(k=2..5)]$(j=0..4);
  pour j de 2 jusque 5 faire
    L:=NULL;
    pour k de 6 jusque 9 faire
      Le:=j;
      pour n de 0 jusque 3 faire
        Le:=Le,indice(addill(PP[k],prodl(n,PP[j],L4,P4),L4,P4),PP);
      fpour;
      L:=L,[Le];
    fpour;
  Rep:=Rep,L;

```



```

fpour;
retourne Rep;
};

```

On tape :

```
D4:=repart4(L4,P4)
```

On obtient :

```

[1,2,3,4,5],[1,6,7,8,9],[1,10,11,12,13],[1,14,15,16,17],[1,18,19,20,21],
[2,6,10,14,18],[2,7,11,15,19],[2,8,12,16,20],[2,9,13,17,21],
[3,6,11,16,21],[3,7,10,17,20],[3,8,13,14,19],[3,9,12,15,18],
[4,6,15,20,13],[4,7,14,21,12],[4,8,17,18,11],[4,9,16,19,10],
[5,6,19,12,17],[5,7,18,13,16],[5,8,21,10,15],[5,9,20,11,14]

```

On rappelle la fonction `testcarte(L)` qui permet de tester le résultat :

```

testcarte(L):={
local j,k,s,S;
s:=size(L);
S:=set[op(L[j]) $ (j=0..s-1);
pour j de 0 jusque s-2 faire
  pour k de j+1 jusque s-1 faire
    si size(S[j] intersect S[k])!=1 alors
      retourne [j,k]
  fsi;
fpour;
retourne 1;
};

```

On tape :

```
testcarte(D4)
```

On obtient :

```
1
```

3.3 La répartition pour $p = 8$

On rappelle les fonctions qui permettent d'additionner et de multiplier les éléments du corps fini, puis on définit `K8()` et on écrit la fonction de répartition `repart8` :

```

indice(a,L):={
local k;
k:=member(normal(a),L);
si k!=0 alors
  retourne k-1;
fsi;
retourne "erreur";
};
addi(a,b,K,P):={

```

```

    retourne indice((K[a]+K[b]) mod (P),K);
};;
prod(a,b,K,P):={
    retourne indice((K[a]*K[b])mod (P),K);
};;
prodl(a,L,K,P):={
    local s;
    s:=size(L)-1;
    retourne [prod(a,L[k],K,P)$(k=0..s)];
};;
addill(L1,L2,K,P):={
    local s1,s2;
    s1:=size(L1)-1;
    s2:=size(L2)-1;
    si s1==s2 alors
        retourne [addi(L1[k],L2[k],K,P)$(k=0..s1)];
    fsi;
retourne "erreur";
};;
K8():={
    local L8,j,k,m,s,x;
    purge(x);
    L8:=NULL;
    pour j de 0 jusqu' 1 faire
    pour k de 0 jusqu' 1 faire
        pour m de 0 jusqu' 1 faire
            s:=j*x^2+x*k+m;
            L8:=L8,normal(s %2) ;
        fpour;
    fpour;
    return [L8];
};;
P8:=(x^3+x+1)%2;;
L8:=K8();;
repart8(L8,P8):={
    local k,j,L,Le,n,Rep;
    PP:=[0,0,0],[1,0,0],[0,1,0],[1,k,0]$(k=1..7);
    pour k de 0 jusqu' 7 faire
        pour j de 0 jusqu' 7 faire
            PP:=PP,[j,k,1];
        fpour;
    fpour;
    PP:=[PP];
    Rep:=[1,(k+j*8)$(k=2..9)]$(j=0..8);
    pour j de 2 jusqu' 9 faire

```

```

L:=NULL;
pour k de 10 jusqu' 17 faire
  Le:=j;
  pour n de 0 jusqu' 7 faire
    Le:=Le, indice (addill (PP[k], prod1 (n, PP[j], L8, P8), L8, P8), PP);
  fpour;
  L:=L, [Le];
fpour;
Rep:=Rep, L;
fpour;
retourne Rep;
};

```

On tape :

D8:=repart8 (L8, P8)

On obtient :

```

[1, 2, 3, 4, 5, 6, 7, 8, 9], [1, 10, 11, 12, 13, 14, 15, 16, 17], [1, 18, 19, 20, 21, 22, 23, 24, 25],
[1, 26, 27, 28, 29, 30, 31, 32, 33], [1, 34, 35, 36, 37, 38, 39, 40, 41],
[1, 42, 43, 44, 45, 46, 47, 48, 49], [1, 50, 51, 52, 53, 54, 55, 56, 57],
[1, 58, 59, 60, 61, 62, 63, 64, 65], [1, 66, 67, 68, 69, 70, 71, 72, 73],
[2, 10, 18, 26, 34, 42, 50, 58, 66], [2, 11, 19, 27, 35, 43, 51, 59, 67],
[2, 12, 20, 28, 36, 44, 52, 60, 68], [2, 13, 21, 29, 37, 45, 53, 61, 69],
[2, 14, 22, 30, 38, 46, 54, 62, 70], [2, 15, 23, 31, 39, 47, 55, 63, 71],
[2, 16, 24, 32, 40, 48, 56, 64, 72], [2, 17, 25, 33, 41, 49, 57, 65, 73],
[3, 10, 19, 28, 37, 46, 55, 64, 73], [3, 11, 18, 29, 36, 47, 54, 65, 72],
[3, 12, 21, 26, 35, 48, 57, 62, 71], [3, 13, 20, 27, 34, 49, 56, 63, 70],
[3, 14, 23, 32, 41, 42, 51, 60, 69], [3, 15, 22, 33, 40, 43, 50, 61, 68],
[3, 16, 25, 30, 39, 44, 53, 58, 67], [3, 17, 24, 31, 38, 45, 52, 59, 66],
[4, 10, 27, 44, 61, 38, 23, 72, 57], [4, 11, 26, 45, 60, 39, 22, 73, 56],
[4, 12, 29, 42, 59, 40, 25, 70, 55], [4, 13, 28, 43, 58, 41, 24, 71, 54],
[4, 14, 31, 48, 65, 34, 19, 68, 53], [4, 15, 30, 49, 64, 35, 18, 69, 52],
[4, 16, 33, 46, 63, 36, 21, 66, 51], [4, 17, 32, 47, 62, 37, 20, 67, 50],
[5, 10, 35, 60, 53, 70, 47, 24, 33], [5, 11, 34, 61, 52, 71, 46, 25, 32],
[5, 12, 37, 58, 51, 72, 49, 22, 31], [5, 13, 36, 59, 50, 73, 48, 23, 30],
[5, 14, 39, 64, 57, 66, 43, 20, 29], [5, 15, 38, 65, 56, 67, 42, 21, 28],
[5, 16, 41, 62, 55, 68, 45, 18, 27], [5, 17, 40, 63, 54, 69, 44, 19, 26],
[6, 10, 43, 36, 69, 62, 31, 56, 25], [6, 11, 42, 37, 68, 63, 30, 57, 24],
[6, 12, 45, 34, 67, 64, 33, 54, 23], [6, 13, 44, 35, 66, 65, 32, 55, 22],
[6, 14, 47, 40, 73, 58, 27, 52, 21], [6, 15, 46, 41, 72, 59, 26, 53, 20],
[6, 16, 49, 38, 71, 60, 29, 50, 19], [6, 17, 48, 39, 70, 61, 28, 51, 18],
[7, 10, 51, 20, 45, 30, 71, 40, 65], [7, 11, 50, 21, 44, 31, 70, 41, 64],
[7, 12, 53, 18, 43, 32, 73, 38, 63], [7, 13, 52, 19, 42, 33, 72, 39, 62],
[7, 14, 55, 24, 49, 26, 67, 36, 61], [7, 15, 54, 25, 48, 27, 66, 37, 60],
[7, 16, 57, 22, 47, 28, 69, 34, 59], [7, 17, 56, 23, 46, 29, 68, 35, 58],
[8, 10, 59, 68, 21, 54, 39, 32, 49], [8, 11, 58, 69, 20, 55, 38, 33, 48],

```

```
[8,12,61,66,19,56,41,30,47],[8,13,60,67,18,57,40,31,46],
[8,14,63,72,25,50,35,28,45],[8,15,62,73,24,51,34,29,44],
[8,16,65,70,23,52,37,26,43],[8,17,64,71,22,53,36,27,42],
[9,10,67,52,29,22,63,48,41],[9,11,66,53,28,23,62,49,40],
[9,12,69,50,27,24,65,46,39],[9,13,68,51,26,25,64,47,38],
[9,14,71,56,33,18,59,44,37],[9,15,70,57,32,19,58,45,36],
[9,16,73,54,31,20,61,42,35],[9,17,72,55,30,21,60,43,34]
```

On tape :

```
testcarte(D8)
```

On obtient :

```
1
```

3.4 La répartition pour $p = 9$

On définit $K9()$ et on écrit la fonction de répartition $repart9$:

```
K9() := {
  local L9, j, k, s, x;
  purge(x);
  L9:=NULL;
  pour k de 0 jusque 2 faire
    pour j de 0 jusque 2 faire
      s:=x*k+j;
      L9:=L9,normal(s %3) ;
    fpour;
  fpour;
  return [L9];
};
P9:=(x^2+1)%3;;
L9:=K9();
repart9(L9,P9):={
  local k, j, L, Le, n, Rep, PP;
  PP:=[0,0,0],[1,0,0],[0,1,0],([1,k,0])$(k=1..8);
  pour k de 0 jusque 8 faire
    pour j de 0 jusque 8 faire
      PP:=PP,[j,k,1];
    fpour;
  fpour;
  PP:=[PP];
  Rep:=[1,(k+j*9)$(k=2..10)]$(j=0..9);
  pour j de 2 jusque 10 faire
    L:=NULL;
    pour k de 11 jusque 19 faire
      Le:=j;
      pour n de 0 jusque 8 faire
        Le:=Le,indice(addill(PP[k],prodl(n,PP[j],L9,P9),L9,P9),PP);
```

```

    fpour;
    L:=L, [Le];
    fpour;
    Rep:=Rep, L;
    fpour;
    retourne Rep;
};

```

On tape :

D9:=repart (L9,P9))

On obtient :

```

[1, 2, 3, 4, 5, 6, 7, 8, 9, 10], [1, 11, 12, 13, 14, 15, 16, 17, 18, 19],
[1, 20, 21, 22, 23, 24, 25, 26, 27, 28], [1, 29, 30, 31, 32, 33, 34, 35, 36, 37],
[1, 38, 39, 40, 41, 42, 43, 44, 45, 46], [1, 47, 48, 49, 50, 51, 52, 53, 54, 55],
[1, 56, 57, 58, 59, 60, 61, 62, 63, 64], [1, 65, 66, 67, 68, 69, 70, 71, 72, 73],
[1, 74, 75, 76, 77, 78, 79, 80, 81, 82], [1, 83, 84, 85, 86, 87, 88, 89, 90, 91],
[2, 11, 20, 29, 38, 47, 56, 65, 74, 83], [2, 12, 21, 30, 39, 48, 57, 66, 75, 84],
[2, 13, 22, 31, 40, 49, 58, 67, 76, 85], [2, 14, 23, 32, 41, 50, 59, 68, 77, 86],
[2, 15, 24, 33, 42, 51, 60, 69, 78, 87], [2, 16, 25, 34, 43, 52, 61, 70, 79, 88],
[2, 17, 26, 35, 44, 53, 62, 71, 80, 89], [2, 18, 27, 36, 45, 54, 63, 72, 81, 90],
[2, 19, 28, 37, 46, 55, 64, 73, 82, 91], [3, 11, 21, 31, 41, 51, 61, 71, 81, 91],
[3, 12, 22, 29, 42, 52, 59, 72, 82, 89], [3, 13, 20, 30, 43, 50, 60, 73, 80, 90],
[3, 14, 24, 34, 44, 54, 64, 65, 75, 85], [3, 15, 25, 32, 45, 55, 62, 66, 76, 83],
[3, 16, 23, 33, 46, 53, 63, 67, 74, 84], [3, 17, 27, 37, 38, 48, 58, 68, 78, 88],
[3, 18, 28, 35, 39, 49, 56, 69, 79, 86], [3, 19, 26, 36, 40, 47, 57, 70, 77, 87],
[4, 11, 30, 22, 68, 87, 79, 44, 63, 55], [4, 12, 31, 20, 69, 88, 77, 45, 64, 53],
[4, 13, 29, 21, 70, 86, 78, 46, 62, 54], [4, 14, 33, 25, 71, 90, 82, 38, 57, 49],
[4, 15, 34, 23, 72, 91, 80, 39, 58, 47], [4, 16, 32, 24, 73, 89, 81, 40, 56, 48],
[4, 17, 36, 28, 65, 84, 76, 41, 60, 52], [4, 18, 37, 26, 66, 85, 74, 42, 61, 50],
[4, 19, 35, 27, 67, 83, 75, 43, 59, 51], [5, 11, 39, 67, 32, 60, 88, 26, 54, 82],
[5, 12, 40, 65, 33, 61, 86, 27, 55, 80], [5, 13, 38, 66, 34, 59, 87, 28, 53, 81],
[5, 14, 42, 70, 35, 63, 91, 20, 48, 76], [5, 15, 43, 68, 36, 64, 89, 21, 49, 74],
[5, 16, 41, 69, 37, 62, 90, 22, 47, 75], [5, 17, 45, 73, 29, 57, 85, 23, 51, 79],
[5, 18, 46, 71, 30, 58, 83, 24, 52, 77], [5, 19, 44, 72, 31, 56, 84, 25, 50, 78],
[6, 11, 48, 85, 59, 69, 25, 80, 36, 46], [6, 12, 49, 83, 60, 70, 23, 81, 37, 44],
[6, 13, 47, 84, 61, 68, 24, 82, 35, 45], [6, 14, 51, 88, 62, 72, 28, 74, 30, 40],
[6, 15, 52, 86, 63, 73, 26, 75, 31, 38], [6, 16, 50, 87, 64, 71, 27, 76, 29, 39],
[6, 17, 54, 91, 56, 66, 22, 77, 33, 43], [6, 18, 55, 89, 57, 67, 20, 78, 34, 41],
[6, 19, 53, 90, 58, 65, 21, 79, 32, 42], [7, 11, 57, 76, 86, 24, 43, 53, 72, 37],
[7, 12, 58, 74, 87, 25, 41, 54, 73, 35], [7, 13, 56, 75, 88, 23, 42, 55, 71, 36],
[7, 14, 60, 79, 89, 27, 46, 47, 66, 31], [7, 15, 61, 77, 90, 28, 44, 48, 67, 29],
[7, 16, 59, 78, 91, 26, 45, 49, 65, 30], [7, 17, 63, 82, 83, 21, 40, 50, 69, 34],
[7, 18, 64, 80, 84, 22, 38, 51, 70, 32], [7, 19, 62, 81, 85, 20, 39, 52, 68, 33],
[8, 11, 66, 40, 23, 78, 52, 35, 90, 64], [8, 12, 67, 38, 24, 79, 50, 36, 91, 62],
[8, 13, 65, 39, 25, 77, 51, 37, 89, 63], [8, 14, 69, 43, 26, 81, 55, 29, 84, 58],
[8, 15, 70, 41, 27, 82, 53, 30, 85, 56], [8, 16, 68, 42, 28, 80, 54, 31, 83, 57],

```

```
[8,17,72,46,20,75,49,32,87,61],[8,18,73,44,21,76,47,33,88,59],
[8,19,71,45,22,74,48,34,86,60],[9,11,75,58,50,33,70,89,45,28],
[9,12,76,56,51,34,68,90,46,26],[9,13,74,57,52,32,69,91,44,27],
[9,14,78,61,53,36,73,83,39,22],[9,15,79,59,54,37,71,84,40,20],
[9,16,77,60,55,35,72,85,38,21],[9,17,81,64,47,30,67,86,42,25],
[9,18,82,62,48,31,65,87,43,23],[9,19,80,63,49,29,66,88,41,24],
[10,11,84,49,77,42,34,62,27,73],[10,12,85,47,78,43,32,63,28,71],
[10,13,83,48,79,41,33,64,26,72],[10,14,87,52,80,45,37,56,21,67],
[10,15,88,50,81,46,35,57,22,65],[10,16,86,51,82,44,36,58,20,66],
[10,17,90,55,74,39,31,59,24,70],[10,18,91,53,75,40,29,60,25,68],
[10,19,89,54,76,38,30,61,23,69]
```

On tape :

```
testcarte(D9)
```

On obtient :

```
1
```

4 Pour un corps fini K ayant $p = q^n$ éléments avec q premier

Si $Lp = \mathbb{Z}/q\mathbb{Z}[x] \bmod Pp$ On rappelle les fonctions qui permettent d'additionner et de multiplier les éléments du corps fini, puis on écrit la fonction de répartition repartp :

```
indice(a,L):={
local k;
k:=member(normal(a),L);
si k!=0 alors
retourne k-1;
fsi;
retourne "erreur";
};
addi(a,b,K,P):={
retourne indice((K[a]+K[b]) mod (P),K);
};
prod(a,b,K,P):={
retourne indice((K[a]*K[b])mod (P),K);
};
prodl(a,L,K,P):={
local s;
s:=size(L)-1;
retourne [prod(a,L[k],K,P)$(k=0..s)];
};
addill(L1,L2,K,P):={
local s1,s2;
s1:=size(L1)-1;s2:=size(L2)-1;
```

```

    si s1==s2 alors
      retourne [addi(L1[k],L2[k],K,P)$(k=0..s1)];
    fsi;
  retourne "erreur";
};;
//si p=q^n avec q premier, Lp est la liste des poly de Z/qZ de degré<=n-1
//Pp est un poly premier du corps Lp
//PP est le plan projectif et s=p-1
repartp(Lp,Pp):={
  local k,j,L,Le,m,Rep,PP,s;
  s:=size(Lp)-1;
  PP:=[0,0,0],[1,0,0],[0,1,0],([1,k,0])$(k=1..s);
  pour k de 0 jusque s faire
    pour j de 0 jusque s faire
      PP:=PP,[j,k,1];
    fpour;
  fpour;
  PP:=[PP];
  Rep:=[1,(k+j*(s+1))$(k=2..s+2)]$(j=0..s+1);
  pour j de 2 jusque s+2 faire
    L:=NULL;
    pour k de s+3 jusque 2*s+3 faire
      Le:=j;
      pour m de 0 jusque s faire
        Le:=Le,indice(addill(PP[k],prodl(m,PP[j],Lp,Pp),Lp,Pp),PP);
      fpour;
      L:=L,[Le];
    fpour;
    Rep:=Rep,L;
  fpour;
  retourne Rep;
};;

```

Par exemple si $Lp = \mathbb{Z}/3\mathbb{Z}[x] \bmod x^3 + 2x + 1$ on construit un corps de cardinal $3^3 = 27$.

On tape :

```

K27():={
  local Lp,j,k,l,s,x;
  purge(x);
  Lp:=NULL;
  pour j de 0 jusque 2 faire
    pour k de 0 jusque 2 faire
      pour l de 0 jusque 2 faire
        s:=j*x^2+x*k+l;
        Lp:=Lp,normal(s % 3) ;

```

```

        fpour;
    fpour;
    fpour;
    return [Lp];
};
L27:=K27();
P27:=(x^3+2*x+1)%3;

On tape D27:=repartp(L27,P27);
On obtient (Temps mis pour l'évaluation : 80)
Done
On tape size(L27),size(D27)
On obtient car  $27 * 28 + 1 = 757$  :
27,757
On a donc 757 objets différents et D27 donne la répartition de  $27+1=28$  objets sur
chacune des 757 cartes.
On tape pour vérifier :
textcarte(D27)
On obtient 1

```

5 Exercice

Trouver la répartition lorsque l'on veut un jeu ayant :

1. 6 objets par carte et $5*6+1=31$ cartes
2. 12 objets par carte et $11*12+1=133$ cartes
3. 17 objets par carte et $16*17+1=273$ cartes
4. 26 objets par carte et $25*26+1=651$ cartes

Solution

1. 6 objets par carte et $5*6+1=31$ cartes
On tape puisque 11 est premier :


```

K5() := {
    local Lp, j, s, x;
    purge(x);
    Lp:=NULL;
    pour j de 0 jusque 4 faire
        s:=j;
        Lp:=Lp,normal(s %5) ;
    fpour;
    return [Lp];
};
P5:=(x)%5;
L5:=K5();

```


On tape D5:=repartp(L5,P5) ;;

On obtient :

Done

On tape :

size(L5), size(D5)

On obtient car $5 * 6 + 1 = 31$:

5, 31

On tape pour vérifier :

testcarte(D5)

On obtient :

1

On tape :

D5

On obtient :

[1, 2, 3, 4, 5, 6], [1, 7, 8, 9, 10, 11], [1, 12, 13, 14, 15, 16], [1, 17, 18, 19, 20, 21],
[1, 22, 23, 24, 25, 26], [1, 27, 28, 29, 30, 31], [2, 7, 12, 17, 22, 27], [2, 8, 13, 18, 23, 28],
[2, 9, 14, 19, 24, 29], [2, 10, 15, 20, 25, 30], [2, 11, 16, 21, 26, 31], [3, 7, 13, 19, 25, 31],
[3, 8, 14, 20, 26, 27], [3, 9, 15, 21, 22, 28], [3, 10, 16, 17, 23, 29], [3, 11, 12, 18, 24, 30],
[4, 7, 18, 29, 15, 26], [4, 8, 19, 30, 16, 22], [4, 9, 20, 31, 12, 23], [4, 10, 21, 27, 13, 24],
[4, 11, 17, 28, 14, 25], [5, 7, 23, 14, 30, 21], [5, 8, 24, 15, 31, 17], [5, 9, 25, 16, 27, 18],
[5, 10, 26, 12, 28, 19], [5, 11, 22, 13, 29, 20], [6, 7, 28, 24, 20, 16], [6, 8, 29, 25, 21, 12],
[6, 9, 30, 26, 17, 13], [6, 10, 31, 22, 18, 14], [6, 11, 27, 23, 19, 15]

2. 12 objets par carte et $11 * 12 + 1 = 133$ cartes

On tape puisque 11 est premier

```
K11() := {
  local Lp, j, s, x;
  purge(x);
  Lp:=NULL;
  pour j de 0 jusque 10 faire
    s:=j;
    Lp:=Lp,normal(s %11) ;
  fpour;
  return [Lp];
};;
```

P11:=(x)%11;;

L11:=K11() ;;

On tape D11:=repartp(L11,P11) ;;

On obtient (Temps mis pour l'évaluation : 1.8) :

Done

On tape :

size(L11), size(D11)

On obtient car $11 * 12 + 1 = 133$:

11, 133

On tape pour vérifier :

testcarte(D11)

On obtient :

1

3. 17 objets par carte et $16 \cdot 17 + 1 = 273$ cartes

On définit le corps K_{16} ayant 16 éléments :

On tape puisque $16 = 2^4$:

```
K16() := {
  local Lp, j, k, l, m, s, x;
  purge(x);
  Lp := NULL;
  pour m de 0 jusqu'à 1 faire
    pour j de 0 jusqu'à 1 faire
      pour k de 0 jusqu'à 1 faire
        pour l de 0 jusqu'à 1 faire
          s := m*x^3 + j*x^2 + x*k + l;
          Lp := Lp, normal(s % 2);
        fpour;
      fpour;
    fpour;
  return [Lp];
};
L16 := K16();
P16 := (x^4 + x + 1) % 2;
```

On tape $D16 := \text{repartp}(L16, P16)$;

On obtient (Temps mis pour l'évaluation : 13.78) :

Done

On tape :

$\text{size}(L16), \text{size}(D16)$

On obtient car $16 \cdot 17 + 1 = 273$:

16, 273

On tape pour vérifier :

$\text{testcarte}(D16)$

On obtient :

1

4. 26 objets par carte et $25 \cdot 26 + 1 = 651$ cartes

On tape puisque $25 = 5^2$:

```
K25() := {
  local Lp, j, k, s, x;
  purge(x);
  Lp := NULL;
  pour k de 0 jusqu'à 4 faire
    pour j de 0 jusqu'à 4 faire
      s := x*k + j;
```

```

        Lp:=Lp,normal(s %5) ;
    fpour;
    fpour;
    return [Lp];
};;
P25:=(x^2+2)%5;;
L25:=K25() ;;
On tape :
D25:=repartp(L25,P25) ;;
On obtient (Temps mis pour l'évaluation : 48.21) :
Done
On tape :
size(L25),size(D25)
On obtient car  $25 * 26 + 1 = 651$  :
25, 651
On tape pour vérifier :
testcarte(D25)
On obtient :
1

```

6 En utilisant la commande GF de Xcas

Tout d'abord il faut construire le corps Lp de cardinal $p = q^n$ (q premier), puis la commande GF nous donnera un polynôme irréductible Pp de $\mathbb{Z}/q\mathbb{Z}[x]$ de degré n , puis on réécrit un programme de répartition `repart(p)` ayant un seul paramètre $p = q^n$ avec q premier.

— Construction de Lp .

On utilise `a .+ L` pour renvoyer une liste d'éléments `a+L[k]` pour $k=0 \dots \text{size}(L)-1$
 On tape :

```

polyp(p):={
    local L1,j,m,Lp,P,x,f,n,q;
    f:=ifactors(p);
    si size(f)==2 alors (q,n):=f; sinon return "erreur"; fsi;
    L1:=[(j % q)$(j=0..q-1)];
    Lp:=L1;
    purge(x);
    P:=x;
    pour m de 1 jusque n-1 faire
        pour j de 1 jusque q-1 faire
            Lp:=append(Lp,op(L1[j]*P .+ L1));
        fpour;
        L1:=Lp;
        P:=P*x;
    finpour;
}

```

```

    fpour;
    return normal(LP);
};;
On tape pour  $p = 2^3 = 8$ :
polyp(8)
On obtient :
[0 % 2, 1 % 2, (1 % 2)*x, 1 % 2+1 % 2*x, (1 % 2)*x^2, 1 % 2+(1
% 2)*x^2, (1 % 2)*x+(1 % 2)*x^2, 1 % 2+(1 % 2)*x+(1 % 2)*x^2]
Ou bien on utilise l'écriture en base  $q$  des  $q^n$  entiers  $0, 1, \dots, \text{size}(Lp)-1$ 
c'est alors la fonction poly(p) (cf ci dessous). On tape  $p = 2^3 = 8$  donc
 $q = 2$  et  $n = 3$ :
L:=[j$(j=0..7)]
PP:=revlist(convert(L[j],base,2))$(j=0..7)
[normal(poly2symb(PP[j] % 2,x))$(j=0..7)]
On obtient :
[[0 % 2, 1 % 2, (1 % 2)*x, 1 % 2+(1 % 2)*x, (1 % 2)*x^2, 1
% 2+(1 % 2)*x^2, (1 % 2)*x+(1 % 2)*x^2, 1 % 2+(1 % 2)*x+(1
% 2)*x^2]]
— Pour obtenir un polynôme irréductible  $Pp$  de  $\mathbb{Z}/q\mathbb{Z}[x]$  de degré  $n$  si  $p = q^n$ . La
commande GF nous donne un polynôme irréductible  $Pp$  de  $\mathbb{Z}/q\mathbb{Z}[x]$  de degré
 $n$  lorsque  $p = q^n$ .
Par exemple pour  $p = 2^3 = 8$ , on tape :
purge(g);GF(8)
On obtient :
GF(2,k^3+k^2+1,[k,Q,g],undef)
On tape :
Pp:=normal(poly2symb(pmin(g),x))
On obtient :
1 % 2+(1 % 2)*x^2+(1 % 2)*x^3
— Réécriture du programme de répartition ayant comme seul paramètre  $p$  Si
 $Lp = \mathbb{Z}/q\mathbb{Z}[x] \bmod Pp$  On rappelle les fonctions qui permettent d'additionner
et de multiplier les éléments du corps fini, puis on écrit la fonction poly(p)
qui renvoie  $Lp$  et on écrit la fonction repartip(p) qui renvoie la répartition
lorsque  $p = q^n$  avec  $q$  premier à savoir : on a  $p*(p+1)+1$  cartes et  $p*(p+1)+1$ 
objets différents (ici les objets sont les entiers  $1..p*(p+1)+1$ ) et on place sur
chaque carte  $p+1$  objets de façon que 2 cartes quelconques aient en commun
1 et 1 seul objet.
indice(a,L):={
local k;
k:=member(normal(a),L);
si k!=0 alors
retourne k-1;
fsi;
retourne "erreur";
};;
addi(a,b,K,P):={

```

```

    retourne indice((K[a]+K[b]) mod (P),K);
};;
prod(a,b,K,P):={
    retourne indice((K[a]*K[b])mod (P),K);
};;
prodl(a,L,K,P):={
    local s;
    s:=size(L)-1;
    retourne [prod(a,L[k],K,P)$(k=0..s)];
};;
addill(L1,L2,K,P):={
    local s1,s2;
    s1:=size(L1)-1;
    s2:=size(L2)-1;
    si s1==s2 alors
        retourne [addi(L1[k],L2[k],K,P)$(k=0..s1)];
    fsi;
retourne "erreur";
};;
poly(p):={
    local Lp,j,L,L1,x,f,n,q,s;
    f:=ifactors(p);
    purge(x);
    si size(f)==2 alors (q,n):=f; sinon return "erreur"; fsi;
    s:=p-1;
    L:=[j$(j=0..s)];
    L1:=revlist(convert(L[j],base,q))$(j=0..s);
    Lp:=[normal(poly2symb(L1[j] % q,x))$(j=0..s)];
    return Lp;
};;
repartip(p):={
    local k,j,L,Le,Rep,PP,s,Lp,Pp,q,n,m,f,G,g,x;
    purge(x);
    f:=ifactors(p);
    si size(f)==2 alors (q,n):=f; sinon return "erreur1"; fsi;
    si est_premier(q)!=1 alors retourne "erreur2" fsi;
    Lp:=poly(p);
    s:=p-1;
    si n==1 alors Pp:=x; sinon
        purge(g);
        G:=GF(p);
        Pp:=normal(poly2symb(pmin(g),x));
    fsi;
    PP:=[0,0,0],[1,0,0],[0,1,0],([1,k,0])$(k=1..s);
    pour k de 0 jusque s faire
        pour j de 0 jusque s faire

```

```

        PP:=PP,[j,k,1];
    fpour;
fpour;
PP:=[PP];
Rep:=[1,(k+j*(s+1))$(k=2..s+2)]$(j=0..s+1);
pour j de 2 jusque s+2 faire
    L:=NULL;
    pour k de s+3 jusque 2*s+3 faire
        Le:=j;
        pour m de 0 jusque s faire
            Le:=Le,indice(addill(PP[k],prodl(m,PP[j],Lp,Pp),Lp,Pp),PP);
        fpour;
        L:=L,[Le];
    fpour;
    Rep:=Rep,L;
fpour;
retourne Rep;
};

```

Par exemple si $Lp = \mathbb{Z}/3\mathbb{Z}[x] \bmod x^3 + 2x + 1$ on construit un corps de cardinal $3^3 = 27$.

On tape :

D3:=repartip(3) ;; On obtient :

Done

On tape pour vérifier :

testcarte(D3)

On obtient :

1 On tape :

D4:=repartip(4) ;;

On obtient :

Done

On tape pour vérifier :

testcarte(D4) ;;

On obtient :

1

On tape :

D27:=repartip(27) ;;

On obtient (Temps mis pour l'évaluation : 78.48) :

Done

On tape :

size(D27)

On obtient car $27 * 28 + 1 = 757$:

757

On tape pour vérifier :

testcarte(D27) ;;

On obtient (Temps mis pour l'évaluation : 10.4) :

1