L3 Algèbre effective - Interrogation sur machine du 16 décembre 2019

Exercice 1: Une variante de RSA.

Toutes les commandes Sagemath sont autorisées pour cet exercice.

In [1]:
```
def lettreanombre(l):
    if l==' ':
        return 0
    else:
        return ord(l)-96

def nombrealettre(n):
    if n==0:
        return ' '
    else:
        return chr(n+96)

def decode(n):
    a=n
    l="";
    while (a>0):
        l=nombrealettre(a%27)+l;
        a=a//27
    return l

def encode(l):
    i=0;
    n=0;
    while (i<len(l)):
        n=lettreanombre(l[i])+27*n
        i=i+1
    return n
```

Au laboratoire de mathématiques, tous les messages que s'écrivent les chercheurs sont codés suivant le protocole suivant:

- on a choisi 3 entiers premiers p_1, p_2 et p_3 et en les multipliant, on a créé une clé publique
$$n = 313297851918307610502911324433872045797703258998425302542562974 63$$
- les messages alphanumériques sont transformés en un grand entier M (comme dans le tp2) via la fonction `encode()` donnée ci-dessus;
- Le message est crypté sous la forme $C = M^e \bmod n$ grâce à la clé publique de cryptage
$$e = 10616692270673$$

In [1]:
```
n=313297851918307610502911324433872045797703258998425302542562974 63
e=10616692270673
```

Question a)

Transmettre de façon cryptée le message suivant: "dans ce cours on apprend des choses utiles"

In [4]:
```
message="dans ce cours on apprend des choses utiles"
```

In [0]:
```

```

Question b)

Ce protocole n'est pas sûr. Vous avez intercepté un message. Décodez le, (en laissant apparents vos calculs intermédiaires)!

In [0]:
```
message="utrfqwbeutbiqjvdouvwhgebj lxuzdllvdxwyqaeechs"
```

In [0]:
```

```

Ex.2 Equations linéaires sur $\mathbb{Q}$ et $\mathbb{Z}$

Les commandes Sagemath trop évoluées telles que `A.right_kernel().basis()` *ne sont pas considérées comme des réponses possibles aux questions de cet exercice mais vous pouvez toujours tester avec ces commandes la pertinence de vos réponses.*
Vous pouvez utiliser dans vos réponses la commande donnant la forme normale de Smith d'une matrice.

a. Soit $A \in \mathrm{M}_{6,4}(\mathbb{Z})$ la matrice définie par

```
A=matrix(ZZ,6,4,[3, 4, 30, 8, -20, -32, -198, -64, -20, -34, -198, -68, -8, -14, -78, -28, -7, -12, -6
6, -24, 2, 4, 18, 8])
```

$$A = \begin{pmatrix} 3 & 4 & 30 & 8 \\ -20 & -32 & -198 & -64 \\ -20 & -34 & -198 & -68 \\ -8 & -14 & -78 & -28 \\ -7 & -12 & -66 & -24 \\ 2 & 4 & 18 & 8 \end{pmatrix}$$

Calculer la forme normale de Smith de A
Comment peut on retrouver A à partir de sa forme normale et des matrices de passage ? Vérifier votre réponse.

b. Déterminer une base du noyau de A comme $\mathbb{Z}$-module.

c. Quelle équation linéaire le vecteur colonne Y (à coefficients dans $\mathbb{Q}$) doit il vérifier pour que l'équation $AX = Y$ d'inconnue X admette une solution sur $\mathbb{Q}$ (c'est à dire à coefficients dans $\mathbb{Q}$)?

Donner le résultat sous la forme $NY = 0$ où N est une matrice adéquate ou par un système d'équations linéaires d'inconnues les coefficients $y_1, y_2, \ldots$ de Y.
Rq. On peut créer un vecteur colonne Y dont les coefficients sont des variables symboliques y_i par les instructions :

```
y = list(var('y%d' % i) for i in range(n)) #n = taille de Y
Y=matrix(y).transpose()
```

d. On suppose maintenant Y à coefficients dans $\mathbb{Z}$. A quelles conditions sur les coefficients de Y l'équation $AX = Y$ d'inconnue X admet elle une solution sur $\mathbb{Z}$?

e. Donner un exemple de vecteur colonne Y à coefficients entiers qui soit dans l'image de A comme $\mathbb{Q}$-espace vectoriel mais pas dans l'image de A comme $\mathbb{Z}$-module.

Ex.3 Berlekamp

Il s'agit de factoriser un polynôme Q en mettant en oeuvre l'algorithme de Berlekamp, donc sans utiliser des instructions toutes faites comme `factor(Q)` . Vous pouvez cependant vérifier la pertinence de vos réponses avec les intructions évoluées de Sagemath tel `factor()` .

Ex. On définit $Q \in \mathbb{Z}[X]$ par :

```
X=ZZ['X'].gen()
Q=X^15 + 3*X^14 + 13*X^13 + 33*X^12 + 72*X^11 + 124*X^10 + 188*X^9 + 242*X^8 + 273*X^7 + 264*X^6 + 223*
X^5 + 160*X^4 + 96*X^3 + 45*X^2 + 15*X + 3
```

a. Le polynôme Q a t-il des facteurs multiples ? Lesquels ? Quelle factorisation de Q en déduit on (ie sans utiliser `factor()`) ?

Attention : Sagemath considère le résultat de `Q/Q1` comme un élément du corps des fractions de l'anneau de polynômes, même si Q1 divise Q. Préférer l'instruction `Q//Q1`

```
print ((X^2-1)/(X-1)).parent()
print ((X^2-1)//(X-1)).parent()
Fraction Field of Univariate Polynomial Ring in X over Integer Ring
Univariate Polynomial Ring in X over Integer Ring
```

b. Quelles sont les racines de Q dans $\mathbb{F}_7$? et dans $\mathbb{F}_2$?

Q a t-il des racines dans $\mathbb{Z}$?

Quelle factorisation de Q dans $\mathbb{F}_7[X]$ déduit on de ce qui précède ?

★ Comment se compare le quotient $Q//Q1$ de la division euclidienne dans $\mathbb{Z}[X]$ de Q par un polynôme $Q1$ avec le quotient de la division euclidienne dans $\mathbb{F}_7[X]$?

c. On pose $Q_1 = X^9 + 3 * X^8 + 3 * X^7 + 6 * X^6 + 5 * X^4 + 3 * X^3 + 3 * X^2 + 6$. Vérifier que Q_1 est un facteur de Q.

On définit l'anneau quotient $K = \mathbb{F}_7[X]/(Q_1)$ et on note x la classe de X dans K. $\mathbb{F}_7$ s'identifie aux classes des polynômes constants dans K.

```
Q1=X^9 + 3*X^8 + 3*X^7 + 6*X^6 + 5*X^4 + 3*X^3 + 3*X^2 + 6
K=GF(7)['X'].quotient(Q1,'x');x=K.gen()
print K
```

Pour a un élément de K l'instruction `a.list()` donne la liste des coordonnées de a dans la base canonique de K sur $\mathbb{F}_7$. De quelle base canonique s'agit il ?

On peut convertir cette liste en un vecteur par l'instruction `vector(a.list())` ou en une matrice par `matrix(a.list())` . Inversement on peut convertir une liste l de coefficients en un élément de K par l'instruction `K(1)` . Si C est une matrice (ligne ou colonne) de coordonnées ou un vecteur, on convertit préalablement C en liste : `K(C.list())` .
Essayer les instructions `print K([1,0,0,2,0])` , `print K([1,0,0,2,0]).list()` , `print K(matrix([1,0,0,2,0]).list())`

Combien y a t-il d'éléments dans K ? Pourquoi ?

d. Calculer la matrice M_F du Frobenius $x \mapsto x^7$ relativement à la base canonique de K comme $\mathbb{F}_7$-espace vectoriel.

e. Comment s'interprète les colonnes de la matrice N définie par l'instruction ci-dessous ?

```
N=matrix((MF-identity_matrix(Q1.degree())).right_kernel().basis()).transpose()
```

On donne

```
N=matrix(GF(7),9,4,[1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 4, 0, 0, 0, 0, 1, 0, 6, 6, 2, 0, 6, 0, 1,
0, 0, 6, 1, 0, 6, 3, 1])
```

Que dit le rang de N sur le polynôme Q_1 ?

Quels sont les éléments de $\mathbb{F}_7 \subset K$ parmi $\mathrm{Im}(N)$?

Exhiber un élément P de Im(N) qui ne soit pas dans $\mathbb{F}_7$? Combien y a t-il de tels éléments ?

Pouvez vous exhiber un $a \in \mathbb{F}_7$ tel que Q_1 et $P - a$ aient un facteur commun non trivial dans $\mathbb{F}_7[X]$?

f. ★ Calculer la décomposition de Q en facteurs irréductibles.

g. ★★ Quelles sont les racines de Q dans $\mathbb{F}_7[X]/(Q)$?