Examen du 11 décembre 2018

Le sujet est composé de 3 exercices indépendants.

Sauf mention explicite du contraire dans l'exercice 3, vous avez le droit d'utiliser toutes les fonctions Sage sans avoir à les recoder.

Exercice 1.

On donne les 3 vecteurs u, v et $w \in \mathbf{Z}^5$ suivants:

In [1]:
```
u=vector(ZZ,range(5)); u
```
Out[1]: `(0, 1, 2, 3, 4)`

In [2]:
```
v=vector(ZZ,[2*i^2+4 for i in range(5,10)]); v
```
Out[2]: `(54, 76, 102, 132, 166)`

In [3]:
```
w=vector(ZZ,[i^3+6 for i in range (-2,3)]); w
```
Out[3]: `(-2, 5, 6, 7, 14)`

a) Donner un système "d'équations-congruences" du $\mathbf{Z}$-module $E := < u, v, w >$ engendré par ces vecteurs.

In [0]:

In [0]:

b) Soit z le vecteur suivant:

In [4]:
```
z=vector(ZZ,[28, 37, 51, 67, 82]); z
```
Out[4]: `(28, 37, 51, 67, 82)`

b-i) z est-il combinaison linéaire *à coefficients dans* $\mathbf{Q}$ de u, v, w? Si oui, laquelle?

b-ii) z est-il combinaison linéaire *à coefficients dans* $\mathbf{Z}$ de u, v, w? Si oui, laquelle?

In [0]:

In [0]:

c) Quels sont les multiples entiers du vecteur z qui sont dans E (le $\mathbf{Z}$-module engendré par u, v, w)?

In [0]:

In [0]:

Exercice 2.

a) Quel est le pgcd d de la famille d'entiers m, n, p, q suivante?

In [3]:
```
m=1096013; n=1127843; p=1098079;m,n,p
```
Out[3]: `(1096013, 1127843, 1098079)`

In [0]:

b) Trouver une relation de Bezout pour cette famille, c'est-à-dire des entiers u, v, w tels que

$$um + vn + wp = d.$$

In [0]:

c) Pour les valeurs de a, b, c ci-dessous, quelles sont les solutions des systèmes de congruence suivants?

$$\begin{cases} x \equiv a[m] \\ x \equiv b[n] \\ x \equiv c[p] \end{cases}$$

c-i) Premier jeu de valeurs:

In [7]:
```
a,b,c=1,2,3; a,b,c
```
Out[7]:
```
(1, 2, 3)
```

In [0]:
```

```

c-ii) Second jeu de valeurs:

In [9]:
```
a,b,c=33896, 1066249, 27698; a,b,c
```
Out[9]:
```
(33896, 1066249, 27698)
```

In [0]:
```

```

In [0]:
```

```

Exercice 3. *Les questions a), b) et c) sont indépendantes.*

Soit p le nombre premier ci-dessous:

In [17]:
```
p=7;p
```
Out[17]:
```
7
```

a) Faire la liste des polynômes *unitaires* (c'est-à-dire de coefficient dominant 1) de degré 3 de $\mathbf{Z}/p\mathbf{Z}[X]$ qui n'ont pas de racine dans $\mathbf{Z}/p\mathbf{Z}$.

In [0]:
```

```

b) On pose $Q := X^4 + 1$ et on note R l'anneau$(\mathbf{Z}/p\mathbf{Z}[X])/(Q)$.

b-i) L'anneau R est-il un corps?

b-ii) L'élément $\overline{X^3 + X + 1}$ est-il inversible dans R? Si oui, donner son inverse.

In [0]:
```

```

In [0]:
```

```

c) Pour $k \geq 1$, on note N_k le nombre de polynômes unitaires (c'est-à-dire de coefficient dominant 1) irréductibles de degré k dans $\mathbf{Z}/p\mathbf{Z}[X]$.

On admet la formule suivante:

$$N_k = \frac{1}{k} \sum_{d|k} \mu(\frac{k}{d}) p^d,$$

où $\mu : \mathbf{N} \to \mathbf{N}$ est la fonction de Moebius, définie par:

$$\mu(\ell) := \begin{cases} 0 \text{ si } \ell \text{ a un facteur carré} \\ (-1)^r \text{ où } r \text{ est le nombre de facteurs premiers divisant } \ell \text{ sinon.} \end{cases}$$

c-i) Coder la fonction μ *sans utiliser la fonction prédéfinie de Sage " `moebius` "*

In [13]:
```
def mu(n):
    return 0
```

In [15]:
```
moebius(23), moebius(23^2), moebius(1)
```
Out[15]:
```
(-1, 0, 1)
```

c-ii) Ecrire un programme calculant la valeur de N_k.

En déduire la valeur de N_{100}.