Arithmétique - L3 - MI
Contrôle n^{0}2 - 2009
CORRIGE

Question 1

Que signifie "n est fortement pseudo-premier en base b " ? En quoi le test de Rabin-Miller est-il probabiliste ?

Question 2

Montrer que l'on a l'équivalence suivante :

$$p \text{ est premier } \iff \forall a \in \{1, 2, \cdots p-1\}, \;\; a^{p-1} \equiv 1 \bmod p.$$

Ce test sépare notamment les nombres premiers des nombres de Carmichael. Pourquoi, à votre avis, n'est-il jamais utilisé ?

Question 3

Déterminer les racines du polnôme $f = X^5 - 6X^4 + 15X^3 - 26X^2 + 36X - 24$ dans $\mathbb{Q}$.

D'apres le cours, si $\frac{p}{q}$ est une racine de f dans $\mathbb{Q}$, où p et q sont des entiers premiers entre eux, alors q divise le coefficient dominant de f et p divise le coefficient constant de f. Par conséquent, $q = \pm 1$ et $p = \pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 8, \pm 12, \pm 24$. Et on calcule avec sage :

```
x=QQ['x'].gen()
f=x^5 - 6*x^4 + 15*x^3 - 26*x^2 + 36*x - 24
for p in 24.divisors() :
  print p, f(p)
  print -p, f(-p)
```

On constate que la seule racine de f dans $\mathbb{Q}$ est 2.

Question 4

Montrer que le polynôme $f = X^6 + X + 1$ est irréductible dans $\mathbb{Z}/2\mathbb{Z}[X]$.

Remarquons tout d'abord que le polynôme f n'a pas de racine dans $\mathbb{Z}/2\mathbb{Z}$. Par conséquent, si f était réductible, il serait divisible par un polynôme sans racine de degré 2 ou 3. Ces derniers sont

$$g_1 = X^2 + X + 1$$
$$g_2 = X^3 + X + 1$$
$$g_3 = X^3 + X^2 + 1$$

On calcule les restes dans la division euclidienne de f par g_1, g_2 et g_3 pour vérifier qu'aucun de ces polynômes ne divise f :

```
x=GF(2)['x'].gen()
f=x^6+x+1
g1=x^2+x+1
g2=x^3+x+1
g3=x^3+x^2+1
f%g1
f%g2
f%g3
```

Comme les restes $f\%g1 = x$, $f\%g2 = x^2 + x$, $f\%g3 = x^2 + 1$ sont tous non nuls, f est irréductible.