Arithmétique - L3 - MI
Contrôle n°2 - 2010
CORRIGE

Question 1

Supposant que g est primitif dans $\mathbb{Z}/317\mathbb{Z}$, quel est l'ordre de g^5 ? Donner un élément différent de g qui soit aussi primitif de $\mathbb{Z}/317\mathbb{Z}$. Combien y a-t-il de tels éléments ?

Question 2

Que signifie "n est fortement pseudo-premier en base b " ? Si n est premier, combien possède-t-il de bases en lesquelles il est fortement pseudo-premier ?

Question 3

Soit $f \in \mathbb{Q}[x]$ un polynôme non nul ayant un facteur multiple m. Le polynôme $f+1$ a-t-il un facteur multiple dans $\mathbb{Q}[x]$? Si oui, lequel ? Sinon, pourquoi n'en a-t-il pas ?

Non. On construit un polynôme $f \in \mathbb{Q}[x]$ ayant une racine double en 0, et tel que $f+1$ a une racine double en 1. Un tel polynôme a une dérivée f' s'annulant en 0 et 1. Commencons donc avec un polynôme

$$g' = x(x-1) = x^2 - x$$

qui s'annule en 0 et 1. La primitive de g' s'annulant en 0 est

$$g = \frac{1}{3}x^3 - \frac{1}{2}x^2.$$

Ce polynôme a bien une racine double en 0, mais $g(1) = -\frac{1}{6}$ de sorte que 1 ne est pas racine de $g+1$. Par contre, le polynôme

$$f = 6g = 2x^3 - 3x^2$$

a bien une racine en 1. Comme $f' = 6g'$, cette racine est double. le polynôme f a également une racine double en 0. Il vient que f est un polynôme dans $\mathbb{Q}[x]$ qui a x comme facteur multiple et qui a la propriété que $x-1$ est facteur multiple de $f+1$. Ce polynôme montre donc que f et $f+1$ peuvent bien avoir tous les deux des facteurs multiples.

Question 4

Montrer qu'il existe, pour tout entier $d \geq 1$, un polynôme irréductible dans $\mathbb{Q}[x]$ de degré d.

Soit $f = x^d + 2$. D'après le critère d'Eisenstein avec $p = 2$, le polynôme f est irréductible dans $\mathbb{Q}[x]$. Comme $\deg(f) = d$, le polynôme f est irréductible dans $\mathbb{Q}[x]$ de degré d.