UNIVERSITÉ DE BORDEAUX I 2007-2008
MASTER DE MATHÉMATIQUES *1ère année*
Option : Théorie algébrique des nombres.

DM 1
À remettre le 19 février.

Exercice 1. Pour tout entier naturel $n > 0$ on définit $H_n = \sum_{k=1}^{n} \frac{1}{k}$. Le but de cet exercice est de démontrer la propriété suivante, connue sous le nom de *théorème de Wolstenholme* :

"Si p est un nombre premier ≥ 5, le numérateur de H_{p-1} est divisible par p^2."

Dans la suite, p est un nombre premier impair. On note S la partie mutiplicative $\mathbb{Z} \setminus p\mathbb{Z}$ de $\mathbb{Z}$. L'anneau $S^{-1}\mathbb{Z}$ est alors un anneau local noté $\mathbb{Z}_{(p)}$, d'idéal maximal $\mathfrak{m} = p\mathbb{Z}_{(p)}$. L'anneau $\mathbb{Z}_{(p)}$ peut s'identifier au sous-anneau de $\mathbb{Q}$ constitué des rationnels dont le dénominateur est étranger à p, autrement dit

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \in \mathbb{Q}, p \nmid b \right\}.$$

On rappelle enfin (voir TD) que les quotients $\mathbb{Z}/p\mathbb{Z}$ et $\mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)}$ sont isomorphes.

1. Montrer que le théorème de Wolstenholme est équivalent à la propriété "$H_{p-1} \in p^2\mathbb{Z}_{(p)}$".
2. En regroupant convenablement les termes de la somme définissant H_{p-1}, montrer que

$$H_{p-1} = \sum_{i=1}^{\frac{p-1}{2}} \frac{p}{i(p-i)} \tag{1}$$

3. Montrer que

$$\sum_{i=1}^{\frac{p-1}{2}} \frac{1}{i(p-i)} \equiv -\frac{1}{2} \sum_{1}^{p-1} i^2 \mod p\mathbb{Z}_{(p)} \tag{2}$$

(*noter que 2 est inversible dans $\mathbb{Z}_{(p)}$ puisque p est un premier impair*).

4. En déduire que, si $p \geq 5$, alors $H_{p-1} \in p^2\mathbb{Z}_{(p)}$.

Exercice 2. Soit k un corps. L'anneau $k[X, Y]$ est-il un anneau de Dedekind (justifier) ?

(suite...) ►

Exercice 3. Soit $P(X) = X^n + a_{n-1} + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$ un polynôme d'Eisenstein en p pour un certain premier p. On considère l'extension $K = \mathbb{Q}(\theta)$ engendrée par une racine θ de $P(X)$ dans $\mathbb{C}$. On note $\mathbb{Z}_K$ l'anneau des entiers de K.

1. Montrer que $\mathbb{Z}_K \supset \mathbb{Z}[\theta]$ et que l'indice $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$ est fini.
2. Soit $x = c_0 + c_1\theta + \cdots + c_{n-1}\theta^{n-1} \in \mathbb{Z}[\theta]$. Montrer que $\mathbb{N}_{K/\mathbb{Q}}(x) \equiv c_o^n \mod p$ (*considérer la matrice de la multiplication par x dans la base $\{1, \theta, \cdots, \theta^{n-1}\}$*).
3. On souhaite montrer que l'indice $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$ est premier à p. Supposons, par l'absurde, que ce ne soit pas le cas.
   (a) Montrer que $\mathbb{Z}_K$ contient un élément y de la forme $y = \frac{c_0 + c_1\theta + \cdots + c_{n-1}\theta^{n-1}}{p}$, où les c_i sont des entiers non tous divisibles par p.
   (b) En utilisant la question 1, montrer que c_0 est divisible par p (*utiliser le fait que la norme d'un entier algébrique est un entier*).
   (c) Montrer, de proche en proche, que tous les c_i sont divisibles par p, et conclure à une contradiction.
4. Application : déterminer l'anneau des entiers $\mathbb{Z}_K$ de $K = \mathbb{Q}(\theta)$, où θ est une racine du polynôme $P(X) = X^3 - 3$.
   On pourra utiliser, sans la redémontrer (voir TD), la relation

$$\textit{Disc}(\mathbb{Z}[\theta]) = \textit{Disc}\,(P(X)) = [\mathbb{Z}_K : \mathbb{Z}[\theta]]^2\, \textit{Disc}(\mathbb{Z}_K)$$

   .