UNIVERSITÉ DE BORDEAUX I 2006-2007
MASTER DE MATHÉMATIQUES *1ère année*
Option : Théorie des nombres.

Corrigé DM 2

1. Posons $P(X) = \sum_{i=0}^{m} a_i X^i$, avec $a_i \in \mathbb{Z}$ pour $i = 0, \ldots, m$. Si $a_0 = 0$, alors 0 est racine de $P(X)$ modulo p pour tout premier p, d'où la réponse à la question dans ce cas. On suppose donc désormais que $a_0 \neq 0$. Remarquons que l'ensemble $\{x \in \mathbb{Z} \mid P(x) \in \{0, \pm 1\}\}$ est fini (sinon, $P(X)$ serait constant). Ainsi, il existe $n_0 \in \mathbb{N}$ tel que, pour tout entier $n \geq n_0$ on ait $|P(n!)| > 1$. En particulier, si $n \geq n_0$, $P(n!)$ possède au moins un facteur premier p_n et $n!$ est une racine de $P(X)$ modulo p_n.
   Par ailleurs, si $a_0 = 1$, on a
   $$P(n!) = 1 + \sum_{i=1}^{m} a_i (n!)^i$$
   d'où
   $$P(n!) - 1 \in n!\mathbb{Z}.$$
   Si p est un premier $\leq n$, alors il divise $n!$ donc $P(n!) - 1$, donc il ne peut pas diviser $P(n!)$. Par conséquent, $p_n > n$. On a donc exhibé, sous l'hypothèse $a_0 = 1$, une suite infinie $(p_n)_{n \in \mathbb{N}}$ de nombres premiers tels que $P(X)$ ait une racine modulo p_n.
   Dans le cas général (et toujours sous l'hypothèse que $a_0 \neq 0$) on considère le polynôme $Q(X) = \dfrac{P(a_0 X)}{a_0}$, qui appartient à $\mathbb{Z}[X]$ et vérifie la condition $Q(0) = 1$: il possède donc des racines modulo p pour une infinité de nombres premiers. Pour $x \in \mathbb{Z}$, la condition $Q(x) \equiv 0 \mod p$ équivaut à
   $$\frac{P(a_0 x)}{a_0} \equiv 0 \mod p, \tag{1}$$
   qui entraîne que $P(a_0 x) \equiv 0 \mod p$, d'où la conclusion.

2. MEA CULPA *: l'énoncé oubliait de préciser que dans toute cette question θ* ***est un entier algébrique****, ce qui est nécessaire pour pouvoir considérer $\mathbb{Z}[\theta]$ comme sous-anneau de $\mathbb{Z}_K$...*
   (a)
   i. L'homomorphisme de $\mathbb{Z}[X]$ dans $\mathbb{F}_p$, qui à $Q(X) \in \mathbb{Z}[X]$ associe $Q(a) \mod p$, est clairement surjectif, et il est identiquement nul sur l'idéal engendré par $P(X)$, puisque $P(a) \equiv 0 \mod p$. Par conséquent il induit, par le théorème de factorisation, un homomorphisme surjectif $\phi : \mathbb{Z}[\theta] \simeq \mathbb{Z}[X] / (P(X)) \twoheadrightarrow \mathbb{F}_p$. Clairement, $I = p\mathbb{Z}[\theta] + (\theta - a)\mathbb{Z}[\theta]$

est contenu dans $\ker \phi$. Inversement, si $x = \sum_{i=0}^{m} b_i \theta^i \in \mathbb{Z}[\theta]$, on a

$$x = \sum_{i=1}^{m} b_i(\theta^i - a^i) + \sum_{i=0}^{m} b_i a^i \equiv \sum_{i=0}^{m} b_i a^i \mod I \tag{2}$$

puisque $(\theta^i - a^i) \in (\theta - a)\mathbb{Z}[\theta]$ pour $i \geq 1$. Par conséquent, $x \in \ker \phi$ si et seulement si $\sum_{i=0}^{m} b_i a^i \equiv 0 \mod p$, auquel cas l'équation (2) implique que x appartient à I. On a donc $I = \ker \phi$ et $\mathbb{Z}[\theta]/I \simeq \mathbb{F}_p$ par le théorème de factorisation.

ii. Par construction, $\mathfrak{p} \cap \mathbb{Z}[\theta]$ contient I, qui est un idéal maximal de $\mathbb{Z}[\theta]$, donc on a soit $\mathfrak{p} \cap \mathbb{Z}[\theta] = I$ soit $\mathfrak{p} \cap \mathbb{Z}[\theta] = \mathbb{Z}[\theta]$. Dans le second cas, on aurait $1 \in \mathfrak{p}$, ce qui est absurde. Donc $\mathfrak{p} \cap \mathbb{Z}[\theta] = I$, et I est le noyau de l'homomorphisme $\mathbb{Z}[\theta] \to \mathbb{Z}_K/\mathfrak{p}$ obtenu en composant l'injection canonique de $\mathbb{Z}[\theta]$ dans $\mathbb{Z}_K$ et la surjection canonique sur $\mathbb{Z}_K/\mathfrak{p}$. Par suite (théorème de factorisation), $\mathbb{Z}[\theta]/I$ s'injecte dans $\mathbb{Z}_K/\mathfrak{p}$.

iii. Posons $d = [Z_K : \mathbb{Z}[\theta]]$. Pour $x \in \mathbb{Z}_K$, on a $dx \in \mathbb{Z}[\theta]$. Si $p \nmid d$, on peut trouver $(u, v) \in \mathbb{Z}^2$ tels que $1 = du + pv$ (Bézout), auquel cas $x = dux + pvx \in \mathbb{Z}[\theta] + \mathfrak{p}$. Ainsi tout élément de $\mathbb{Z}_K$ est congru modulo $\mathfrak{p}$ à un élément de $\mathbb{Z}[\theta]$, ce qui signifie que l'injection canonique $\mathbb{Z}[\theta]/I \hookrightarrow Z_K/\mathfrak{p}$ est un isomorphisme.

(b) Soit $\mathcal{P}_0 = \{p \text{ premier }, P(X) \text{ admet une racine } \mod p \text{ et } p \nmid [\mathbb{Z}_K : \mathbb{Z}[\theta]]\}$. D'après la question 1, cet ensemble est infini ($[\mathbb{Z}_K : \mathbb{Z}[\theta]]$ n'a qu'un nombre fini de facteurs premiers), et d'après(a), pour tout $p \in \mathcal{P}_0$ il existe un idéal premier $\mathfrak{p}$ au-dessus de p tel que $\mathbb{Z}_K/\mathfrak{p} \simeq \mathbb{F}_p$, c'est-à-dire tel que $f(\mathfrak{p}) = 1$.

3. Tout d'abord, si K est une extension finie de $\mathbb{Q}$, le théorème de l'élément primitif permet d'affirmer qu'il existe $\theta \in K$ tel que $K = \mathbb{Q}(\theta)$. Qui plus est, quitte à multiplier θ par un entier convenable, on peut supposer que θ est un entier algébrique. On est donc ramené aux hypothèses de la question 2. Si K est galoisienne, les degrés résiduels des idéaux premiers $\mathfrak{p}_1 \cdots \mathfrak{p}_g$ au-dessus d'un premier p sont tous égaux, ainsi que leurs indices de ramification. Ainsi, on a

$$p\mathbb{Z}_K = (\mathfrak{p}_1 \cdots \mathfrak{p}_g)^e \tag{3}$$

où e est l'indice de ramification commun à tous les $\mathfrak{p}_i$. De plus, en notant f le degré résiduel commun des $\mathfrak{p}_i$ on a

$$efg = [K : \mathbb{Q}]. \tag{4}$$

Avec les notations précédentes, on sait que f vaut 1 si $p \in \mathcal{P}_0$, auquel cas l'équation 4 devient $eg = [K : \mathbb{Q}]$. Il reste à justifier que $g = [K : \mathbb{Q}]$ (ou, ce qui revient au même, que $e = 1$) pour une infinité de $p \in \mathcal{P}_0$. Or on sait qu'il n'y a qu'un nombre fini de premiers ramifiés (c'est-à-dire tels que $e > 1$) dans K, d'où la conclusion.

4. Soit $K = \mathbb{Q}(\zeta_m)$. Le polynôme minimal de ζ_m est le $m$ième polynôme cyclotomique $\Phi_m(X)$. On note $\mathcal{P}_m$ l'ensemble des nombres premiers tels que $\Phi_m(X)$ admette une racine modulo p, qui est infini d'après la question 1. Montrons que tous les éléments de $\mathcal{P}_m$, sauf un nombre fini, satisfont la congruence $p \equiv 1 \mod m$ ce qui permettra de conclure puisque $\mathcal{P}_m$ est infini. Soit donc $p \in \mathcal{P}_m$ et $x \in \mathbb{F}_p$ tel que $\overline{\Phi}_m(x) = 0$, où $\overline{\Phi}_m(X)$ désigne

la réduction modulo p de $\Phi_m(X)$. Rappelons que $X^m - 1$ se décompose dans $\mathbb{Z}[X]$ sous la forme

$$X^m - 1 = \prod_{d|m} \Phi_d(X) \tag{5}$$

d'où, en réduisant modulo p,

$$X^m - 1 = \prod_{d|m} \overline{\Phi}_d(X). \tag{6}$$

Par conséquent, si $\overline{\Phi}_m(x) = 0$, on a également $x^m = 1$. En particulier x est non nul, ce qui implique que $x^{p-1} = 1$ (le groupe multiplicatif $\mathbb{F}_p^\times$ est cyclique d'ordre $p-1$). Ainsi, l'ordre de x dans $\mathbb{F}_p^\times$ est un diviseur commun d de m et $p-1$. Si $d = m$, on a alors $m \mid p-1$, comme souhaité. Sinon, en remarquant que

$$X^d - 1 = \prod_{d'|d} \overline{\Phi}_{d'}(X) \tag{7}$$

on conclut que $\overline{\Phi}_{d'}(x) = 0$ pour au moins un diviseur d' de d. Cela implique, en utilisant (6), que x est une racine double de $X^m - 1$ (x est racine de $\overline{\Phi}_m(X)$ et $\overline{\Phi}_{d'}(X)$ qui sont deux facteurs distincts du produit $\prod_{d|m} \overline{\Phi}_d(X)$). Par suite, x est racine de mX^{m-1}, ce qui implique ($x \neq 0$) que p divise m. Ceci n'est possible que pour un nombre fini de premiers p (les facteurs premiers de m), par conséquent, on a bien $m \mid p-1$ pour une infinité de $p \in \mathcal{P}_m$.