Université François Rabelais Tours **2016-2017**
M1 Arithmétique

Arithmétique: Examen du 4/01/17
Durée: 3 heures.
L'évaluation de la copie tiendra compte de la qualité de sa rédaction

Exercice 1 (3 points) : Soit p un nombre premier impair.

1. Exprimer $\left(\frac{3}{p}\right)$ en fonction de $\left(\frac{p}{3}\right)$.
2. Peut-on dire que 3 est un carré modulo 29 ?
3. Montrer que 3 est un carré modulo p si et seulement si $p = 3$ ou $p \equiv \pm 1 \bmod 12$.
4. Montrer que 5 est un carré modulo p si et seulement si $p = 5$ ou $p \equiv \pm 1 \bmod 5$.

Exercice 2 (4 points) : On considère le polynôme $P(X) = X^4 + 1$.

1. Justifier que $\sqrt{2}$ n'est pas un nombre rationnel.
2. Factoriser P dans $\mathbb{C}$ et dans $\mathbb{R}$. En déduire que P est irréductible dans $\mathbb{Q}[X]$.
3. Soit p un nombre premier. Justifier que -1, 2 ou -2 est un carré dans $\mathbb{Z}/p\mathbb{Z}$.
4. En déduire que P n'est pas irréductible dans $\mathbb{Z}/p\mathbb{Z}[X]$.

Exercice 3 (7 points): Soit $j = \exp(\frac{2i\pi}{3})$. On note $\mathbb{Z}[j] = \{a + bj \mid (a, b) \in \mathbb{Z}^2\}$.

1. Justifier que $\mathbb{Z}[j]$ est un sous-anneau commutatif unitaire de $\mathbb{C}$ stable par la conjugaison.
2. Vérifier que l'application $f : \mathbb{Z}[X] \to \mathbb{Z}[j]$ telle que $f(P) = P(j)$ est un morphisme d'anneaux. En déduire que $\mathbb{Z}[X]/(X^2 + X + 1)$ est isomorphe à $\mathbb{Z}[j]$.
3. L'idéal $(X^2 + X + 1)$ de $\mathbb{Z}[X]$ est-il maximal ? Si ce n'est pas le cas, déterminer un idéal I de $\mathbb{Z}[X]$ tel que $(X^2 + X + 1) \subsetneq I \subsetneq \mathbb{Z}[X]$.
4. On rappelle que $N(z) = z\overline{z}$ pour tout nombre complexe $z \in \mathbb{C}$. Justifier que $N(z_1 z_2) = N(z_1)N(z_2)$ pour tout $(z_1, z_2) \in \mathbb{Z}[j]^2$.
5. Soit $z = a + bj \in \mathbb{Z}[j]$. Montrer que $N(z) = a^2 + b^2 - ab \in \mathbb{N}$. En déduire que $U(\mathbb{Z}[j])$ est l'ensemble des éléments de $\mathbb{Z}[j]$ de norme 1.
6. Montrer que $U(\mathbb{Z}[j]) = \{\pm 1, \pm j, \pm\overline{j}\}$ (on pourra remarquer que $a^2 + b^2 \geq 2\,|ab|$ pour tout $(a, b) \in \mathbb{Z}^2$).
7. Dans la suite, on admet que $\mathbb{Z}[j]$ est un anneau euclidien (la preuve est analogue à celle pour $\mathbb{Z}[i]$). Soit J l'idéal de $\mathbb{Z}[j]$ engendré par $1 - j$. Montrer que $\mathbb{Z}[j]/J$ est un corps isomorphe à $\mathbb{Z}/3\mathbb{Z}$.

Exercice 4 (6 points) : On se donne deux entiers naturels $m \geq 0$ et $n > 0$ ainsi qu'un nombre premier p. Notons k le corps $\mathbb{Z}/p\mathbb{Z}$. On pose $S_m = \sum_{x \in k} x^m$.

1. On suppose (seulement dans cette question) que m n'est pas divisible par $p-1$. Justifier qu'il existe α dans k tel que $\alpha^m - \overline{1} \neq \overline{0}$. Montrer que l'on a alors $S_m = \alpha^m S_m$. En déduire que $S_m = \overline{0}$.

2. Montrer que si m est nul ou si il n'est pas divisible par $p-1$, alors $S_m = \overline{0}$.

3. Soit $(m_1, \ldots, m_n) \in \mathbb{N}^n$ établir que

$$S_{(m_1,\ldots,m_n)} = \sum_{(x_1,\ldots,x_n) \in k^n} x_1^{m_1} \times \cdots \times x_n^{m_n} = \overline{0}$$

dès que l'un des entiers m_i est nul ou non divisible par $p-1$. On suppose que $m_1 + \cdots + m_n < (p-1)n$. Justifier que $S_{(m_1,\ldots,m_n)} = \overline{0}$.

4. Soit $Q \in k[X_1, \ldots, X_n]$ tel que $\deg(Q) < n(p-1)$. Que vaut

$$S_Q = \sum_{(x_1,\ldots,x_n) \in k^n} Q(x_1, \ldots, x_n) \ ?$$

5. On se donne maintenant un polynôme P dans $k[X_1, \ldots, X_n]$ tel que $d(P) < n$ et on pose $Q = \overline{1} - P^{p-1}$. Justifier que pour tout $(x_1, \ldots, x_n) \in k^n$, on a $Q(x_1, \ldots, x_n) = \overline{1}$ si $P(x_1, \ldots, x_n) = \overline{0}$ et $Q(x_1, \ldots, x_n) = \overline{0}$ sinon.

6. En déduire que $\mathrm{card}\{(x_1, \ldots, x_n) \in k^n \mid P((x_1, \ldots, x_n) = \overline{0}\}$ est divisible par p dès que $d(P) < n$ (théorème de Chevalley-Warning).