Fédération FDP Orléans- Tours **2015-2016**
M1 Arithmétique

Arithmétique: Examen du 5/01/16
Durée: 3 heures.
L'évaluation de la copie tiendra compte de la qualité de sa rédaction

Exercice 1 (2 points): On se donne le polynôme $P(X) = X^4 - 2X^3 + 3X^2 - 2X + 1$. Calculer $P \bmod X^2 - X + 1$ puis factoriser P dans $\mathbb{Q}[X]$.

Exercice 2 (2 points): Soit $P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$. On pose $M = \max\{1, |a_0| + \cdots + |a_{n-1}|\}$. Montrer que toutes les racines rélles de P sont dans $[-M, M]$.

Exercice 3 (4 points) : Le but de l'exercice est de démontrer qu'il ne peut exister un polynôme f non constant à coefficients entiers tel que $f(n)$ soit un nombre premier pour tout $n \in \mathbb{N}$. On suppose par l'absurde l'existence d'un tel polynôme.

1. Soit $n_0 \in \mathbb{N}$ et $t \in \mathbb{N}$. Posons $f(n_0) = p_0$ où p_0 est un nombre premier. Montrer que $f(n_0 + tp_0) = f(n_0) + p_0 g(t)$ où g est un polynôme à coefficients entiers.
2. En déduire que p_0 divise $f(n_0 + tp_0)$ pour toutes les valeurs de t entières.
3. Conclure.

Exercice 4 (3 points) : Soient m et n premiers entre eux. Montrer que

$$\phi_{mn}(X) = \prod_{\alpha \in \Delta_m} \prod_{\beta \in \Delta_n} (X - \alpha\beta)$$

où Δ_m, Δ_n sont les ensembles des racines primitives m-ièmes et n-ièmes de 1.

Exercice 5 (4 points) : Soient p un entier premier et le polynôme $P(X) = X^4 - 2pX^2 + p^2 - p$ dans $\mathbb{Z}[X]$.

1. Montrer que P ne possède pas de racine dans $\mathbb{Q}$.
2. Montrer que P est irréductible dans $\mathbb{Z}[X]$.
3. Trouver les racines réelles du polynôme $P(X) = X^4 - 2pX^2 + p^2 - p$.
4. En déduire que $\sqrt{p + \sqrt{p}}$ n'est pas un rationnel.

Exercice 6 (2 points) : Caractériser tous les nombres premiers p pour lesquels la congruence quadratique $x^2 \equiv 3 \bmod p$ possède des solutions.

Exercice 7 (3 points) : Le but de l'exercice est de montrer qu'il existe une infinité de nombres premiers de la forme $4n + 1$.

1. On suppose qu'il existe seulement un nombre fini de tels nombres premiers $q_1 < \cdots < q_m$. Soit $N = (2q_1 \cdots q_r)^2 + 1$. Justifier le fait qu'il existe p premier impair qui divise N.

2. A l'aide d'un raisonnement par l'absurde et du petit théorème de Fermat, en déduire que p est de la forme $p = 4n + 1$

3. Conclure.