Université François Rabelais Tours **2018-2019**
M1 Arithmétique

Arithmétique: Examen du 18/12/18

Durée: 4 heures.
L'évaluation de la copie tiendra compte de la qualité de sa rédaction

Exercice 1 : Soit p un nombre premier impair tel que $p \equiv 1 \bmod 3$. Montrer que $U(\mathbb{Z}/p\mathbb{Z})$ contient un élément x d'ordre 3. Vérifier que $(2x+1)^2 \equiv -3 \bmod p$ et en déduire $\left(\frac{-3}{p}\right)$ (on pourra calculer x^2+x+1 au préalable).

Exercice 2 : Polynômes cyclotomiques
On note $\mathbb{U}_n$ l'ensemble des racines n-ièmes de l'unité dans $\mathbb{C}$. On rappelle que $\Phi_n(X)$ est le polynôme cyclotomique d'indice. Soit p un nombre premier et m un entier premier avec p.

1. Démontrer que si z est racine primitive pm-ième de l'unité alors z^p est racine m-ème primitive de l'unité.
2. Démontrer que $\Phi_m(X)\Phi_{pm}(X) = \Phi_m(X^p)$ (On commencera par établir que les deux polynômes de l'égalité ci-dessus ont même degré).
3. Démontrer, en vous inspirant de la méthode ci-dessus, que pour tout entier $i \geq 1$
$$\Phi_{p^i m}(X) = \frac{\Phi_m(X^{p^i})}{\Phi_m(X^{p^{i-1}})}$$
4. En déduire Φ_{12}. Vérifier votre calcul en déterminant Δ_{12}.
5. Etablir que Φ_{12} est irréductible dans $\mathbb{Z}[X]$ et démontrer qu'il ne l'est pas dans $\mathbb{Z}/2\mathbb{Z}[X]$ ni dans $\mathbb{Z}/3\mathbb{Z}[X]$.

Exercice 3 : Equations Diophantiennes (*les questions sont indépendantes*)

1. Montrer qu'il n'y a pas de solutions en nombres entiers à l'équation $x^2 + 37y^3 = 60$ (on pourra travailler modulo m avec m bien choisi).
2. Démontrer que l'équation Diophantienne $x^2+y^2+z^2 = 4(xy+yz+zx)$ n'a pas de solution non triviale (même indication).

Problème: L'objectif de ce problème est de montrer que $\mathbb{Z}[\xi] := \{a + b\xi \mid (a,b) \in \mathbb{Z}^2\}$ où $\xi = \frac{1+i\sqrt{19}}{2}$ est un anneau principal qui n'est pas euclidien. Une norme de Dedekind-Hasse sur un anneau intègre A est une application $N : A \to \mathbb{N}$ telle que

$$\begin{cases} N(x) = 0 \text{ si et seulement si } x = 0, \\ \text{si } x, y \in A\backslash\{0\} \text{ alors } y \mid x \text{ ou il existe } (s,t) \in A^2 \text{ tel que } 0 < N(sx-ty) < N(y). \end{cases}$$

1. On suppose que A est un anneau euclidien de stathme f qui n'est pas un corps. Montrer qu'il existe un élément $y \in A$ tel que

(a) $y \neq 0$ et $y \notin U(A)$

(b) Pour tout $a \in A$, il existe $q \in A$ et $r \in U(A) \cup \{0\}$ tel que $a = qy + r$. [On prendra un élément qui minimise le stathme sur $A\backslash(U(A) \cup \{0\})$.]

2. Montrer que pour un tel y, le quotient $A/(y)$ est un corps.

3. On suppose maintenant que A est intègre et A possède une norme de Dedekind-Hasse. Montrer que A est principal.

4. On définit $N : \mathbb{Z}[\xi] \to \mathbb{N}$ par $N(a + b\xi) = |a + b\xi|^2$. Vérifier que $N(a + b\xi) = a^2 + ab + 5b^2$ et montrer que $N(xy) = N(x)N(y)$ pour tout $x, y \in \mathbb{Z}[\xi]$.

5. Déterminer l'ensemble des inversibles de $\mathbb{Z}[\xi]$.

6. En déduire que 2 et 3 sont irréductibles dans $\mathbb{Z}[\xi]$.

7. En utilisant $a = 2$ et $a = \xi$, montrer qu'il ne peut pas exister d'élément y dans A vérifiant 1)(a) et 1)(b).

8. En déduire que $\mathbb{Z}[\xi]$ n'est pas euclidien.

9. Dans cette question, on montre que N est une norme de Dedekind-Hasse sur $\mathbb{Z}[\xi]$. Soit $x, y \in \mathbb{Z}[\xi]$ deux éléments non nuls tels que y ne divise pas x. On doit trouver des éléments $s, t \in \mathbb{Z}[\xi]$ tels que $0 < N(sx - ty) < N(y)$ c'est-à-dire tels que

$$(\star) \quad 0 < N(s \cdot (\frac{x}{y}) - t) < 1.$$

On pose

$$\frac{x}{y} := \frac{a + ib\sqrt{19}}{c} = \frac{a - b}{c} + \frac{2b}{c}\xi \in \mathbb{Q}(\xi)$$

où $\text{pgcd}(a, b, c) = 1$ et $c > 1$.

(a) On suppose que $c = 2$. Montrer que le couple $(1, \frac{(a-1) + ib\sqrt{19}}{2})$ convient.

(b) On suppose que $c = 3$. Montrer que l'on peut écrire $a^2 + 19b^2 = 3q + r$ avec $1 \leq r \leq 2$ et que le couple $(a - ib\sqrt{19}, q)$ convient.

(c) On suppose que $c = 4$. Ainsi a et b ne sont pas tous les deux pairs.

- Si a et b sont impairs montrer qu'il existe $q \in \mathbb{N}$ tel que $a^2 + 19b^2 = 8q + 4$ et que le couple $(\frac{a - ib\sqrt{19}}{2}, q)$ convient.
- Si a ou b est pair montrer que $a^2 + 19b^2 = 4q + r$ avec $0 < r < 4$ et que le couple $(a - ib\sqrt{19}, q)$ convient.

(d) On supppose que $c \geq 5$. Justifier qu'il existe $n_1, n_2, n_3 \in \mathbb{Z}$ tel que

$$n_1 a + n_2 b + n_3 c = 1.$$

(e) Soit $(q, r) \in \mathbb{N}$ tel que $n_2 a - 19 n_1 b = cq + r$ avec $|r| \leq c/2$. Montrer que le couple

$$(n_2 + in_1\sqrt{19}, q - in_3\sqrt{19})$$

convient.

(f) Conclure.