UNIVERSITÉ D'ÉVRY VAL D'ESSONNE
L3 MATHÉMATIQUES

ANNÉE UNIVERSITAIRE 2008-2009
MODULE : M54

Lundi 26 Janvier 2009
Partiel d'algèbre et arithmétique

Exercice 1 (4,5 points)

1. *Enoncé du théorème d'Euler-Fermat.*
2. *Enoncé du théorème d'isomorphisme entre anneaux.*
3. *Définition d'un anneau principal*
4. *Montrer que $\mathbb{Z}[X]$ n'est pas un anneau principal.*
5. *Définition d'un anneau euclidien*
6. *Donner un exemple d'anneau euclidien.*
7. *Quels sont les corps de fractions de $A = \mathbb{Z}, \mathbb{Z}[i]$.*
8. *Quels sont les polynômes irréductibles $(\mathbb{R}[X], +, \times)$?*
9. *Quels sont les idéaux maximaux de $(\mathbb{R}[X], +, \times)$?*

Exercice 2 (8 points). *Dans ce qui suit, si p est un nombre premier, on désignera par $\mathbb{F}_p$ le corps fini à p éléments $\mathbb{Z}/p\mathbb{Z}$.*

1. *Montrer que $(\mathbb{F}_2[X], +, \times)$ est un anneau principal.*
2. *Montrer que le polynôme $X^2 + X + 1$ est irréductible sur $\mathbb{F}_2$.*
3. *Décrire les éléments de $\mathbb{F}_2[X]/(X^2 + X + 1)$.*
   Indication : Faire la division euclidienne d'un $P(X) \in \mathbb{F}_2[X]$ par $X^2 + X + 1$, ceci vous donnera $P(X)$ modulo $X^2 + X + 1$.
4. *Ecrire les tables d'addition et de multiplication de $\mathbb{F}_2[X]/(X^2 + X + 1)$.*
   On pose dans la suite $\mathbb{F}_4 := F_2[X]/(X^2 + X + 1)$.
5. *Soit p un nombre premier. Montrer que le polynôme $P(X) = X^2 + 1$ est irrt'ductible sur $\mathbb{F}_p$ si et seulement si p est congru à 3 modulo 4.*
   (indication : utiliser le fait que -1 est un carré dans $\mathbb{F}_p$ si et seulement si p est congru à 3 modulo 4)
6. *Déduire de la question précédente, que, si p est congru à 3 modulo 4, $\mathbb{F}_p[X]/(X^2 + 1)$ est un corps à p^2 éléments.*
7. *Ecrire les tables de $\mathbb{F}_9$.*
8. *Montrer que le polynôme $X^3 + X^2 + 1$ est irréductible sur $\mathbb{F}_2$. Donner la liste des éléments de $\mathbb{F}_8$ et la méthode pour obtenir la table de $\mathbb{F}_8$.*

Exercice 3 (14 points). *Soit $A = \mathbb{Z}[i]$ muni de l'application $\varphi(a + bi) = a^2 + b^2, a, b \in \mathbb{Z}$.*

1. *Montrer que $(A, +, \times, \varphi)$ est un anneau euclidien.*
2. *Déterminer les inversibles de A ?* $\{1, -1, i, -i\}$
3. *Déterminer les éléments z irréductibles de A tels que : $\varphi(z) = 2$ ou 3.*
4. *Soit p un nombre premier impair. Montrer que les applications :*

$$\phi : \mathbb{Z}/p\mathbb{Z}\backslash\{0\} \to \mathbb{Z}/p\mathbb{Z}\backslash\{0\} \quad , \quad x \mapsto x^2$$

$$\psi : \mathbb{Z}/p\mathbb{Z}\backslash\{0\} \to \{-\bar{1}, \bar{1}\} \quad , \quad x \mapsto x^{\frac{p-1}{2}}$$

   sont des morphismes de groupes multiplicatifs.
5. *Montrer que $Ker(\psi) = Im(\phi)$. Calculer le cardinal de $Ker(\psi)$?*
6. *En déduire que : $-\bar{1} \in Ker(\psi) \iff p \equiv 1 \pmod 4$.*

7. *Montrer que* $\mathbb{Z}/p\mathbb{Z}[X]/(X^2+1)) \simeq \mathbb{Z}[i]/(p)$ *(isomorphes en tant qu'anneaux)*
   Indication : Montrer que l'application

$$\phi : \mathbb{Z}[X] \to \mathbb{Z}[i]/(p) \quad , \quad P(X) \mapsto P(i) \pmod{(p)}$$

   est un morphisme d'anneaux surjectif. Puis, appliquer le théorème d'isomorphisme.

8. *Montrer que pour tout premier impair* $p \equiv 1 \pmod 4$, *p n'est pas irréductible dans* $\mathbb{Z}[i]$.
   (Utiliser les deux questions précédentes).
9. *En déduire que pour tout premier impair* $p \equiv 1 \pmod 4$, *il existe un couple* $(x,y) \in \mathbb{Z}^2$ *tels que :* $p = x^2 + y^2$.
10. *Soit p premier avec* $p \equiv 3 \pmod 4$.
    . Montrer que X^2+1 *est irréductible dans* $\mathbb{Z}/p\mathbb{Z}[X]$.
    . En déduire que, pour $p \equiv 3 \pmod 4$ *premier, on a : p est irréductible dans* $\mathbb{Z}[i]$.
11. *Soit* $z \in \mathbb{Z}[i]$, *dont* $\varphi(z) = p$ *premier impair. Montrer que z est irréductible dans* $\mathbb{Z}[i]$.
12. *Soit* $z \in \mathbb{Z}[i]$ *irréductible, dont* $\varphi(z)$ *est divisible par un nombre premier* $p \equiv 3 \pmod 4$. *Montrer que* $z = \pm p$ *ou* $\pm ip$.
13. *Soit* $z \in \mathbb{Z}[i]$ *irréductible, dont* $\varphi(z)$ *est divisible par un nombre premier* $p \not\equiv 3 \pmod 4$.
    Montrer que $\varphi(z) = p$.
14. *Déterminer les irréductibles de* $\mathbb{Z}[i]$.

Exercice 4 (10 points). *Soit* $A = \mathbb{Z}[i\sqrt{2}] := \{P(i\sqrt{2}) : P(X) \in \mathbb{Z}[X]\}$.

1. *Montrer que* $A = \{a + bi\sqrt{2} : a, b \in \mathbb{Z}\}$.
2. *En munissant A de l'application :* $\varphi(a+bi\sqrt{2}) = a^2 + 2b^2, a, b \in \mathbb{Z}$. *Montrer que* $(A, +, \times, \varphi)$ *est un anneau euclidien.*
3. *Déterminer le corps des fractions de A.*
4. *Déterminer les inversibles de A ?*
5. $i\sqrt{2}$ *est-il irréductible dans A ?*
6. *Trouver tous les éléments* $c + id\sqrt{2}$ *de* $\mathbb{Z}[i\sqrt{2}]$ *tel que :* $c^2 + 2d^2 = 2$. *Montrer qu'ils sont tous irréductibles dans A.*
7. *Déterminer les diviseurs de* $2i\sqrt{2}$ *dans A ? Préciser ceux qui sont irréductibles dans A ?*
8. *Soit* $(x_0, y_0) \in \mathbb{Z}^2$ *une solution de l'équation :*

$$y^2 + 2 = x^3.$$

   – *Montrer que* x_0 *et* y_0 *sont impairs.*
   – *Montrer que* $y_0 + i\sqrt{2}$ *et* $y_0 - i\sqrt{2}$ *sont premiers entre eux dans l'anneau* $\mathbb{Z}[i\sqrt{2}]$.

9. *En déduire que si* $(x_0, y_0) \in \mathbb{Z}^2$ *est une solution de l'équation :*

$$y^2 + 2 = x^3$$

   il existe des entiers a et b vérifiant

$$y_0 + i\sqrt{2} = (a + ib\sqrt{2})^3.$$

10. *Résoudre dans* $\mathbb{Z}^2$ *l'équation :* $x^3 - y^2 - 2 = 0$.