Arithmétique et applications - L3 - MI

UBO – 25 juin 2009

examen - durée : 3 heures

Tout document manuscrit ou imprimé, téléphone portable, ordinateur personnel interdit.

Partie I

Exercice I : une équation diophantienne

Le but de cet exercice est de trouver tous les triplets d'entiers (x, y, z) vérifiant :

$$1009x + 345y + 56z = 1.(*)$$

1. Donner toutes les solutions entières de $1009x + 345y = 1$ puis de $1009x + 345y = a$, a étant quelconque dans $\mathbb{Z}$.
2. Donner une solution particulière de $(*)$.
3. Servez-vous de la solution particulière que vous venez de trouver pour décrire toutes les solutions de $(*)$.

Exercice II : le test $n - 1$

On décrit ici un test de primalité que l'on appliquera ensuite aux nombres de Fermat. n est un entier naturel strictement plus grand que 2.

1. Rappeler pourquoi l'ordre de tout élément a de $\mathcal{U}(\frac{\mathbb{Z}}{n\mathbb{Z}})$ divise $\varphi(n)$.
2. On suppose que l'on a trouvé un entier a tel que $a^{n-1} \equiv 1 \bmod n$ et tel que pour tout diviseur premier q de $n - 1$ on a :
$$a^{\frac{n-1}{q}} \not\equiv 1 \bmod n.$$
   (a) Montrer que l'ordre de a est $n - 1$.
   (b) En déduire que $n - 1 = \varphi(n)$ puis que n est premier.
3. Réciproquement, montrer que si n est premier, alors il existe un entier a, tel que $a^{n-1} \equiv 1 \bmod n$ et tel que pour tout diviseur premier q de $n - 1$ on a :
$$a^{\frac{n-1}{q}} \not\equiv 1 \bmod n.$$
4. On rappelle que le k-ième nombre de Fermat est le nombre $F_k = 2^{2^k} + 1$. Montrer que F_k est premier si et seulement si il existe un nombre entier a tel que
$$a^{\frac{F_k-1}{2}} \equiv -1 \bmod F_k.$$
5. Par exemple, montrer par cette méthode que $F_4 = 65537$ est premier.
   a étant choisi, quel est le coût binaire au pire de ce test de primalité de F_k en fonction de k ?

Partie II

Exercice III

Soit f le polynôme dans $\mathbb{Z}[X]$ défini par $f(X) = X^4 - 2X^2 + 9$. Le but de cet exercice est de démontrer que le polynôme f est réductible modulo tout nombre premier p, mais irréductible dans $\mathbb{Q}[X]$.

1. Montrer que f n'admet pas de racine dans $\mathbb{Q}$.
2. Montrer que si g divise f dans $\mathbb{Q}[X]$, alors $g(-X)$ le divise également.
3. En déduire que f est irréductible dans $\mathbb{Q}[X]$.
4. Montrer que f est réductible dans $\mathbb{F}_2[X]$.
5. Soit p un nombre premier impair tel qu'il existe $\delta \in \mathbb{F}_p$ avec $\delta^2 = -32$ dans $\mathbb{F}_p$. Montrer que le polynôme $x^2 - 2x + 9$ est réductible dans $\mathbb{F}_p[X]$.
6. En déduire que f est réductible dans $\mathbb{F}_p[X]$ lorsque p est un nombre premier impair tel qu'il existe $\delta \in \mathbb{F}_p$ avec $\delta^2 = -32$ dans $\mathbb{F}_p$.

Dans la suite, p désignera un nombre premier impair pour lequel il n'existe pas de $\delta \in \mathbb{F}_p$ avec $\delta^2 = -32$ dans $\mathbb{F}_p$.

7. Montrer qu'il existe un élément $\beta \in \mathbb{F}_{p^2}$ tel que $\beta^2 = -1$.
8. Montrer qu'il existe un élément $\gamma \in \mathbb{F}_{p^2}$ tel que $\gamma^2 = 2$
9. Montrer que $\alpha = \beta + \gamma$ est une racine de f dans $\mathbb{F}_{p^2}$.
10. En déduire que f est réductible dans $\mathbb{F}_p[x]$ lorsque p est un nombre premier impair pour lequel il n'existe pas de $\delta \in \mathbb{F}_p$ avec $\delta^2 = -32$.

Exercice IV

Soit $m(X) = X^6 + X^5 + X^4 + X^2 + 1 \in \mathbb{F}_2[X]$.

1. Montrer que m est irréductible dans $\mathbb{F}_2[X]$.
2. Soit $K = \mathbb{F}_2[X]/m$, et notons $\alpha = X \bmod m$. Quel est le cardinal de K ?
3. Montrer que l'élément α de $K^\star$ n'est pas générateur.
4. Déterminer un générateur β de $K^\star$.
5. Déterminer les sous-corps de K.
6. Pour chaque sous-corps L de K, préciser un générateur de $L^\star$.