

Examen de l'Unité Arithmétique dans \mathbb{Z} et $\mathbb{K}[X]$

Deuxième session : Lundi 14 Juin 2010

Durée : 3h

Deux pages recto-verso de résumé de cours autorisées
Calculatrices et matériels électroniques interdits.

Il est rappelé que la qualité de la rédaction compte pour une part non négligeable dans l'appréciation de la copie et que les réponses non justifiées n'ont pas de valeur. Les notations sont celles du cours .

Questions brèves

- 1) Etablir que l'équation $x^2 + 23y^2 = 14$ ne possède pas de solution entière.
- 2) Etablir que l'équation diophantienne (E) $x^4 + 5y^4 + 25z^4 = 125t^4$ n'a pas de solution non triviale en nombre entiers .
- 3) Résoudre $\varphi(n) = 22$.
- 4) Déterminer les pgcd des entiers de Gauss $z_1 = -7 + 4i$ et $z_2 = 1 + 8i$.

Exercice 1 : Polynômes cyclotomiques et irréductibilité :

On rappelle que le polynôme cyclotomique d'indice n est donné par

$$\Phi_n(X) = \prod_{\zeta \in \Delta_n} (X - \zeta)$$

où Δ_n désigne l'ensemble des racines primitives n èmes de l'unité dans \mathbb{C} ie l'ensemble des générateurs du sous-groupe \mathbb{U}_n des racines n èmes de l'unité dans \mathbb{C}

Soit p un nombre premier et m un entier premier avec p . On note \mathbb{U}_n l'ensemble des racines n -èmes de l'unité dans \mathbb{C} .

1)a)Etablir que si z est racine primitive pm -ième de l'unité alors z^p est racine m -ème primitive de l'unité.

b) Démontrer que $\Phi_{pm}(X) = \frac{\Phi_m(X^p)}{\Phi_m(X)}$.

On commencera par déterminer le degré du polynôme Q , $Q(X) = \Phi_{pm}(X)\Phi_m(X)$.

2) a)Démontrer de même que pour tout entier $i \geq 1$ $\Phi_{p^i m}(X) = \frac{\Phi_m(X^{p^i})}{\Phi_m(X^{p^{i-1}})}$

b) En déduire Φ_{12} .

c) Etablir que Φ_{12} est irréductible dans $\mathbb{Z}[X]$ mais qu'il ne l'est pas dans $\mathbb{Z}/2\mathbb{Z}[X]$ ni dans $\mathbb{Z}/3\mathbb{Z}[X]$.

Exercice 2 : Autour de la fonction ν

On rappelle que l'on désigne par $\nu(n)$ le nombre de diviseurs de n , par i_k la fonction puissance k ième et $\sigma(n)$ la somme des diviseurs du nombre n . On désigne par μ la fonction de Möbius.

1)a) Redémontrer que ν et σ sont multiplicatives.

b)Etablir que

$$\sum_{d/n} \sigma(d) = n \sum_{d/n} \frac{\nu(d)}{d},$$

puis que

$$n\nu(n) = \sum_{d|n} \varphi(d)\sigma\left(\frac{n}{d}\right).$$

2) Etant donné une fonction arithmétique f on définit :

$$\bar{f}(n) = \frac{1}{\nu(n)} \sum_{d|n} f(d)$$

2) a) Démontrer que si f est multiplicative, \bar{f} l'est aussi.

b) Que sont les fonctions $\bar{1}$ et $\bar{\mu}$?

c) On désigne par $\tau(n)$ le nombre de diviseurs premiers de n . Calculer $\bar{\tau}$.

d) On désigne par ψ la fonction $\psi(n) = 2^{\tau(n)}$. Démontrer que :

$$\bar{\psi}(n) = \frac{\nu(n^2)}{\nu(n)}.$$

3) a) Etablir qu'étant donné g une fonction multiplicative, il existe f multiplicative telle que $g = \bar{f}$.

b) Calculer f pour la fonction ψ .

Exercice 3 : entiers modulo p^2 :

Soit p un nombre premier et m un entier non divisible par p . On désigne par m^* un entier tel que $mm^* \equiv 1[p^2]$.

1) a) Etant donné m un entier, décrire l'ensemble des éléments que l'on peut choisir pour m^* . Combien en existe-t-il dans $\{0, \dots, p^2 - 1\}$?

b) Démontrer que si $p > 2$, $1^* + 2^* + \dots + (p-1)^* \equiv 0[p]$.

2) Soit P le polynôme $P(X) = (X - (p-1))(X - (p-2)) \dots (X - 1) = X^{p-1} - a_{p-2}X^{p-2} + \dots + a_0$.

a) Etablir que p divise tous les a_i , $i > 0$ puis que si $p > 3$, $a_1 \equiv 0[p^2]$.

b) En déduire, en calculant $P(0)$ que si $p > 3$, $1^* + 2^* + \dots + (p-1)^* \equiv 0[p^2]$.

3) a) Démontrer que si $1 \leq i \leq p-1$, p divise C_p^i puis que $\frac{C_p^i}{p} \equiv (-1)^{i-1} i^* [p]$.

b) Démontrer, après avoir justifié que pour $p > 2$, $\frac{2^{p-1}-1}{p}$ est un entier, que,

$$\frac{2^{p-1}-1}{p} \equiv 1^* + 3^* + 5^* + \dots + (p-2)^* [p]$$

(Ind : calculer le nombre entier $\frac{2^p-2}{p}$ à l'aide des nombres de la question précédente)

Quel est le résidu de 2^{p-1} modulo p^2 ?

4) a) Etablir, si $p > 2$, la généralisation de la formule de Wilson :

$$(p-1)! \equiv (-1)^{\frac{p-1}{2}} 2^{2p-2} \left(\frac{p-1}{2}\right)!^2 [p^2]$$

On calculera le résidu modulo p^2 du nombre $(p-2)(p-4) \dots (p-2k) = \frac{(2k)!}{2^k k!}$ si $p = 2k + 1$.

5) On suppose $p > 2$. Démontrer qu'une condition nécessaire et suffisante pour que -1 soit un carré modulo p^2 est que p soit congru à 1 modulo 4.

On s'inspirera du cours pour construire une racine carrée de -1 modulo p^2 à l'aide d'une racine carrée de -1 modulo p .