

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

Mardi 4 Janvier 2011

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)a) Démontrer que 561 divise $2^{561} - 2$.
- b) Si a est un entier premier avec 561, a-t-on $a^{561} - a$ divisible par 561 ? Expliquez.
- 2) Donner toutes les preuves que vous connaissez de l'irréductibilité dans $\mathbb{Z}[X]$ du polynôme $P = X^3 + 6X^2 - 27X + 3$.
- 3) **A voir** Etablir qu'il existe une infinité de nombres premiers dont l'écriture décimale se termine par 43. Indiquez quels sont les deux plus petits (on commencera par donner une liste des nombres premiers inférieurs ou égaux à 30).

Exercice 1 :

- 1)a) Pour quelles valeurs de m le groupe $\mathbb{U}(Z/m\mathbb{Z})$ est-il cyclique ?
- b) On prend m comme ci-dessus. Etablir que si n est un entier premier avec $\varphi(m)$ alors l'équation de congruence $x^n \equiv a[m]$ a pour tout entier a une unique solution.
- 2) Etablir que 2 est une racine primitive modulo 13.
- 3) Résoudre l'équation $x^3 \equiv 21[715]$.

Exercice 2 : Polynômes cyclotomiques

On note $\mathbb{U}_n$ l'ensemble des racines n -ièmes de l'unité dans $\mathbb{C}$.

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 -ièmes de l'unité dans $\mathbb{C}$ ie l'ensemble des générateurs du sous-groupe $\mathbb{U}_n$ des racines n -ièmes de l'unité dans $\mathbb{C}$.

Soit p un nombre premier et m un entier premier avec p .

- 1)a) Démontrer 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 $\Phi_m(X)\Phi_{pm}(X) = \Phi_m(X^p)$.

On commencera par établir que les deux polynômes de l'égalité ci-dessus ont même degré.

- 2) a) Démontrer, en vous inspirant de la méthode ci-dessus, que pour tout entier $i \geq 1$

$$\Phi_{p^i m}(X) = \frac{\Phi_m(X^{p^i})}{\Phi_m(X^{p^{i-1}})}$$

- b) En déduire Φ_{12} . Vérifier votre calcul en déterminant Δ_{12} .
- c) 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 $\mathbb{Z}/3\mathbb{Z}[X]$.

T.S.V.P

Exercice 3 : Equations Diophantiennes :

les questions sont indépendantes

1) Déterminer tous les triplets Pythagoriciens dont la longueur d'un côté est 172. On commencera par ceux qui sont primitifs.

2) 23 est-il un carré modulo 37 ? En déduire qu'il n'y a pas de solutions en nombres entiers à l'équation $x^2 + 37y^3 = 60$.

3) Démontrer que l'équation Diophantienne $x^2 + y^2 + z^2 = 4(xy + yz + zx)$ n'a pas de solutions non triviales.

Exercice 4 : Autour de la valeur moyenne m_n des diviseurs du nombre n :

On désigne par $\tau(n)$ le nombre de diviseurs de n et $\sigma(n) = \sum_{d|n} d$ tandis que μ désigne la fonction de Möbius et φ l'indicatrice d'Euler.

On veut donner un encadrement de $m_n = \frac{\sigma(n)}{\tau(n)}$.

1)a) **Cours** Redémontrer, par exemple en écrivant que chaque fonction est un produit de convolution, que les fonctions τ et σ sont multiplicatives.

b) En déduire que m_n est multiplicative. Calculer m_{88} .

c) Montrer que τ est strictement croissante par rapport à la division ie si m divise n et $m \neq n$ alors $\tau(m) < \tau(n)$.

2)a) **Cours** Démontrer que $\sum_{d|n} \left(\frac{n}{d}\right) \mu(d) = \varphi(n)$. On pourra commencer par donner l'identité polynomiale qui permet d'assurer que $n = \sum_{d|n} \varphi(d)$

b) En déduire que $\sum_{d|n} \varphi\left(\frac{n}{d}\right) \frac{\tau(d)}{\tau(n)} = \frac{\sigma(n)}{\tau(n)}$.

3) Démontrer que , pour tout $n \geq 2$, $m_n < n$.

4)a) Etant donnés k entiers positifs , $a_1, \dots, a_k$, démontrer que :

$$(a_1 a_2 \dots a_k)^{\frac{1}{k}} \leq \frac{a_1 + a_2 + \dots + a_k}{k}.$$

b) Démontrer pour tout $n \geq 2$, $m_n \geq \sqrt{n}$. Peut-on avoir égalité ?