

Arithmétique: Examen de rattrapage 06/19

Durée: 3 heures.

L'évaluation de la copie tiendra compte de la qualité de sa rédaction

Exercice 1 (3 points) :

1. Trouver les solutions entières de $7x + 45y = 1$. En déduire celles de $7x + 45y = t$ où $t \in \mathbb{Z}$.
2. A l'aide de la question 1, trouver une expression des solutions entières de $7x + 45y + 121z = 1$.

Exercice 2 (2 points) : Montrer qu'un nombre premier $p \geq 5$ est congru à 1 modulo 3 si et seulement si -3 est un carré dans $\mathbb{Z}/p\mathbb{Z}$.

Exercice 3 (4 points) : Soient n un entier strictement positif et a_1, \dots, a_n des entiers deux à deux distincts. Le but de l'exercice est de montrer que

$$P(X) = (X - a_1) \cdots (X - a_n) - 1$$

est irréductible dans $\mathbb{Z}[X]$. Supposons $P(X) = Q(X)R(X)$ où $Q, R \in \mathbb{Z}[X]$ avec $d^\circ Q > 0$ et $d^\circ R > 0$.

1. Justifier que l'on peut supposer que les coefficients dominants de Q et R (c'est à dire les termes de plus haut degré) valent 1.
2. Montrer que pour tout $i = 1, \dots, n$, on a $Q(a_i)R(a_i) = -1$ puis que $Q(a_i) + R(a_i) = 0$.
3. En déduire que $P(X) = -Q(X)^2$.
4. Conclure.

Exercice 4 (5 points) : Soient m et n deux nombres entiers strictement positifs tels que $(m, n) = 1$.

1. Soit d un diviseur de n et ξ une racine de $\Phi_{dm}(X)$. Montrer que pour tout $a \in \mathbb{N}^*$, $\xi^{na} = 1$ ssi m divise a .
2. Montrer que $\xi^{mn} = 1$, puis à l'aide de la question précédente, que ξ^n est une racine primitive m -ième de 1.
3. Justifier que

$$n\varphi(m) = \sum_{d/n} \varphi(dm).$$

4. Déduire de ce qui précède l'identité

$$\Phi_m(X^n) = \prod_{d/n} \Phi_{dm}(X).$$

Exercice 5 (8 points): Soit $j = \exp(\frac{2i\pi}{3})$. On note $\mathbb{Z}[j] = \{a + bj \mid (a, b) \in \mathbb{Z}^2\}$.

1. Justifier que $\mathbb{Z}[j]$ est un sous-anneau commutatif unitaire de \mathbb{C} stable par la conjugaison.
2. On rappelle que $N(z) = z\bar{z}$ pour tout nombre complexe $z \in \mathbb{C}$. Justifier que $N(z_1 z_2) = N(z_1)N(z_2)$ pour tout $(z_1, z_2) \in \mathbb{Z}[j]^2$.
3. Soit $z = a + bj \in \mathbb{Z}[j]$. Montrer que $N(z) = a^2 + b^2 - ab \in \mathbb{N}$.
4. En déduire que $U(\mathbb{Z}[j])$ est l'ensemble des éléments de $\mathbb{Z}[j]$ de norme 1.
5. Montrer que $U(\mathbb{Z}[j]) = \{\pm 1, \pm j, \pm \bar{j}\}$ (on pourra remarquer que $a^2 + b^2 \geq 2|ab|$ pour tout $(a, b) \in \mathbb{Z}^2$).
6. Justifier que l'on peut paver le plan par des parallélogrammes d'aire égale à $\frac{\sqrt{3}}{2}$ dont les sommets sont les images dans le plan complexe des éléments de $\mathbb{Z}[j]$.
7. Montrer que pour tout nombre complexe z , il existe $q \in \mathbb{Z}[j]$ tel que $|z - q| < 1$.
8. En déduire que $\mathbb{Z}[j]$ est un anneau euclidien.
9. Démontrer que pour un nombre premier $p \in \mathbb{Z}$, il y a équivalence entre les trois propositions :
 - (a) p n'est pas irréductible dans $\mathbb{Z}[j]$,
 - (b) il existe un irréductible $z \in \mathbb{Z}[j]$ tel que $N(z) = p$,
 - (c) il existe $(a, b) \in \mathbb{Z}^* \times \mathbb{Z}^*$ tel que $p = a^2 + b^2 - ab$.
10. Prouver que si p est premier dans \mathbb{Z} , p n'est pas irréductible dans $\mathbb{Z}[j]$ et $p \neq 3$ alors $p \equiv 1[3]$.
11. En déduire que si $p \equiv 2[3]$ alors p est irréductible.
12. Etablir que z est irréductible dans $\mathbb{Z}[j]$ si et seulement si :
 - ou bien $N(z) = p$ où p est un nombre premier non irréductible dans $\mathbb{Z}[j]$,
 - ou bien $N(z) = p^2$ où p est un nombre premier dans \mathbb{Z} et irréductible dans $\mathbb{Z}[j]$.