Examen du 4 février 2022

1 heure 30

La correction tiendra grandement compte de la clarté et de la concision de la rédaction.
L'utilisation de calculatrice, de téléphone portable et autre gadget est interdite.

Exercice 1. — Les questions de cet exercice sont indépendantes entre elles.

1) Montrer que pour tout $n \in \mathbf{Z}$, on a $n^7 \equiv n\,[42]$.

2) Pour n, m deux entiers. Montrer que $\overline{m}$ engendre le groupe $(\mathbf{Z}/n\mathbf{Z}, +)$ ssi $\overline{m}$ est inversible.

* *
*

***Exercice 2* (Nombres de Fermat et critère de Pépin)**
Soit $k \geqslant 1$ un entier.

1) Montrer que si $2^k + 1$ est premier, alors k est une puissance de 2.

Dans la suite, pour $n \geqslant 0$, on note $F_n := 2^{2^n} + 1$. Le but de l'exercice est de montrer l'équivalence :

$$F_n \text{ est premier} \quad \text{ssi} \quad 3^{2^{2^n-1}} \equiv -1[F_n].$$

2) Dans cette question, on suppose $3^{2^{2^n-1}} \equiv -1[F_n]$.

i) Montrer que 3 et F_n sont premiers entre eux.

ii) Montrer que l'ordre de 3 dans $(\mathbf{Z}/F_n\mathbf{Z})^\times$ est 2^{2^n}.

iii) En déduire que F_n est premier.

3) Réciproquement, dans cette question on suppose F_n premier.

i) En utilisant la loi de réciprocité quadratique [1], montrer que 3 n'est pas un carré modulo F_n.

ii) Conclure.

1. On rappelle que pour p, q premiers impairs, on a $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

***Exercice 3* (Agreg Docteur 2019)**. — On définit $\mathbf{Z}[i] = \{a + ib; (a, b) \in \mathbf{Z}^2\}$. On admet que c'est un sous-anneau de $\mathbf{C}$.

1) Montrer que $\mathcal{I} = \{(1 + 3i) \times z; z \in \mathbf{Z}[i]\}$ est un idéal de $\mathbf{Z}[i]$.

On définit sur $\mathbf{Z}[i]$ la relation $\mathcal{R}$ par : $\forall\,(z, z') \in \mathbf{Z}[i]^2$, $z\mathcal{R}z'$ si $(z - z') \in \mathcal{I}$.

2) Montrer que $\mathcal{R}$ est une relation d'équivalence sur $\mathbf{Z}[i]$.

Pour $z \in \mathbf{Z}[i]$ on va noter $C\ell(z)$ la classe de z pour la relation $\mathcal{R}$, et $\mathbf{Z}[i]/\mathcal{I}$ l'ensemble des classes d'équivalence de cette relation.

3) Montrer que l'on définit bien une addition et une multiplication sur $\mathbf{Z}[i]/\mathcal{I}$ en posant $C\ell\,(z + z') := C\ell(z) + C\ell\,(z')$ et $C\ell\,(z \times z') := C\ell(z) \times C\ell\,(z')$.

On admet pour la suite que l'on a une structure d'anneau sur $\mathbf{Z}[i]/\mathcal{I}$.

4) Montrer que $\mathbf{Z}/10\mathbf{Z}$ est isomorphe à $\mathbf{Z}[i]/\mathcal{I}$. [Indication : on pourra montrer que $i\mathcal{R}3$.]

5) Résoudre l'équation $X^2 + 5 = 0$ d'inconnue X dans $\mathbf{Z}[i]/\mathcal{I}$.