Interrogation écrite 1

Vendredi 10 octobre 2025, 11h15–12h45 (1h30)

Les documents et le matériel électronique sont interdits. Les exercices sont indépendants les uns des autres. Toutes les réponses doivent être justifiées. Le barème est indicatif.

1. On considère l'équation diophantienne $245x + 84y = d$, où $d \in \mathbb{Z}$ est fixé.
   (a) Pour quelles valeurs de d cette équation admet-elle des solutions $(x, y) \in \mathbb{Z}^2$? 1,5 pts

   Solution: L'équation admet des solutions si et seulement si d est un multiple du pgcd de 245 et 84. Or, $245 = 5 \times 7^2$ et $84 = 2^2 \times 3 \times 7$, donc $\gcd(245, 84) = 7$. Ainsi, l'équation admet des solutions si et seulement si d est un multiple de 7.

   (b) Décrire l'ensemble des solutions pour $d = 14$. 1,5 pts

   Solution: Pour $d = 14$, une solution particulière peut être trouvée en utilisant l'algorithme d'Euclide étendu. On trouve par exemple $(x_0', y_0') = (11, -32)$ pour l'équation $245x' + 84y' = 7$. En multipliant cette solution par 2, on obtient une solution particulière pour $d = 14$: $(x_0, y_0) = (22, -64)$.
   L'ensemble des solutions générales est donné par :

$$(x, y) = (x_0 + k \cdot \frac{84}{7}, y_0 - k \cdot \frac{245}{7}) = (22 + 12k, -64 - 35k)$$

   pour tout $k \in \mathbb{Z}$.

2. Résoudre le système d'équations diophantiennes 3 pts

$$\begin{cases} x \equiv 9 \pmod{15} \\ x \equiv 0 \pmod{21}. \end{cases}$$

Solution: Comme $\gcd(15, 21) = 3$ et $9 \equiv 0 \pmod 3$, le système admet des solutions. On peut écrire $x = 15k + 9$ pour un certain $k \in \mathbb{Z}$. En substituant dans la deuxième équation, on obtient :

$$15k + 9 \equiv 0 \pmod{21} \implies 15k \equiv -9 \equiv 12 \pmod{21}.$$

En divisant par 3, on a :

$$5k \equiv 4 \pmod 7.$$

En multipliant par l'inverse de 5 modulo 7 (qui est 3), on trouve :

$$k \equiv 5 \pmod 7.$$

Donc, $k = 7m + 5$ pour un certain $m \in \mathbb{Z}$. En substituant dans l'expression de x, on obtient :

$$x = 15(7m + 5) + 9 = 105m + 75 + 9 = 105m + 84.$$

Ainsi, l'ensemble des solutions est :

$$x \equiv 84 \pmod{105}.$$

3. On note que $793 = 13 \times 61$ et que 13 et 61 sont des nombres premiers.
   (a) Déterminer le cardinal de $(\mathbb{Z}/793\mathbb{Z})^\times$. 1 pt

Solution: Le cardinal de $(\mathbb{Z}/n\mathbb{Z})^\times$ est donné par la fonction indicatrice d'Euler $\varphi(n)$. Pour $n = 793 = 13 \times 61$, on a :

$$\varphi(793) = \varphi(13) \times \varphi(61) = (13 - 1)(61 - 1) = 12 \times 60 = 720.$$

Donc, le cardinal de $(\mathbb{Z}/793\mathbb{Z})^\times$ est 720.

   (b) Est-ce que les groupe $(\mathbb{Z}/13\mathbb{Z})^\times$, $(\mathbb{Z}/61\mathbb{Z})^\times$ et $(\mathbb{Z}/793\mathbb{Z})^\times$ sont cycliques ? 2 pts

Solution: Le groupe $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique pour tout nombre premier p. Donc, $(\mathbb{Z}/13\mathbb{Z})^\times$ et $(\mathbb{Z}/61\mathbb{Z})^\times$ sont cycliques. Cependant, $(\mathbb{Z}/793\mathbb{Z})^\times$ n'est pas cyclique. En fait, $(\mathbb{Z}/793\mathbb{Z})^\times$ est isomorphe à $(\mathbb{Z}/13\mathbb{Z})^\times \times (\mathbb{Z}/61\mathbb{Z})^\times$, et le produit de deux groupes cycliques n'est cyclique que si leurs ordres sont premiers entre eux. Ici, $\gcd(12, 60) = 12 \neq 1$, donc $(\mathbb{Z}/793\mathbb{Z})^\times$ n'est pas cyclique.

   (c) Déterminer le cardinal de l'ensemble des éléments $x \in \mathbb{Z}/13\mathbb{Z}$ tels que $x^{10} = 1$, et de l'ensemble des éléments $y \in \mathbb{Z}/61\mathbb{Z}$ tels que $y^{10} = 1$.

Solution: Comme 1 est inversible, on travaille dans les groupes multiplicatifs $(\mathbb{Z}/13\mathbb{Z})^\times$ et $(\mathbb{Z}/61\mathbb{Z})^\times$, qui sont cycliques d'ordre respectif 12 et 60. Le nombre d'éléments g dans un groupe cyclique d'ordre n tels que $g^k = 1$ est donné par $\gcd(n, k)$. Pour $(\mathbb{Z}/13\mathbb{Z})^\times$, on a $\gcd(12, 10) = 2$. Donc, il y a 2 éléments $x \in \mathbb{Z}/13\mathbb{Z}$ tels que $x^{10} = 1$. Pour $(\mathbb{Z}/61\mathbb{Z})^\times$, on a $\gcd(60, 10) = 10$. Donc, il y a 10 éléments $y \in \mathbb{Z}/61\mathbb{Z}$ tels que $y^{10} = 1$.

   (d) En déduire le cardinal de l'ensemble des éléments $z \in \mathbb{Z}/793\mathbb{Z}$ tels que $z^{10} = 1$. 2 pts

Solution: D'après le théorème chinois des restes, on a un isomorphisme de groupes :

$$(\mathbb{Z}/793\mathbb{Z})^\times \cong (\mathbb{Z}/13\mathbb{Z})^\times \times (\mathbb{Z}/61\mathbb{Z})^\times.$$

Donc, le nombre d'éléments $z \in \mathbb{Z}/793\mathbb{Z}$ tels que $z^{10} = 1$ est le produit des nombres d'éléments dans chaque groupe satisfaisant cette condition. On a trouvé 2 éléments dans $(\mathbb{Z}/13\mathbb{Z})^\times$ et 10 éléments dans $(\mathbb{Z}/61\mathbb{Z})^\times$. Ainsi, le nombre total est : $2 \times 10 = 20$.

Les questions suivantes sont indépendantes des précédentes.

(e) Calculer le symbole de Jacobi $\left(\frac{252}{793}\right)$. 1 pt

Solution: Comme $793 = 13 \times 61$, on a :

$$\left(\frac{252}{793}\right) = \left(\frac{252}{13}\right)\left(\frac{252}{61}\right).$$

Calculons chaque symbole séparément.
Pour $\left(\frac{252}{13}\right)$, on réduit 252 mod 13 :

$$252 \equiv 5 \pmod{13}.$$

Donc, $\left(\frac{252}{13}\right) = \left(\frac{5}{13}\right)$. En utilisant la loi de réciprocité quadratique :

$$\left(\frac{5}{13}\right) = \left(\frac{13}{5}\right)(-1)^{\frac{(5-1)(13-1)}{4}} = \left(\frac{3}{5}\right)(-1)^{12} = \left(\frac{3}{5}\right).$$

En appliquant la loi de réciprocité à nouveau :

$$\left(\frac{3}{5}\right) = \left(\frac{5}{3}\right)(-1)^{\frac{(3-1)(5-1)}{4}} = \left(\frac{2}{3}\right)(-1)^2 = \left(\frac{2}{3}\right).$$

Comme 2 n'est pas un carré mod 3 (ou bien en appliquant le second complément de la loi de réciprocité), on a $\left(\frac{2}{3}\right) = -1$. Donc, $\left(\frac{252}{13}\right) = -1$.
On trouve par des méthodes similaires que $\left(\frac{252}{61}\right) = -1$. Ainsi,

$$\left(\frac{252}{793}\right) = \left(\frac{252}{13}\right)\left(\frac{252}{61}\right) = (-1) \times (-1) = 1.$$

(f) Déterminer si $x^2 \equiv 252 \pmod{793}$ admet des solutions. 1 pt

Solution: Comme le symbole de Jacobi $\left(\frac{252}{793}\right) = 1$, l'équation $x^2 \equiv 252 \pmod{793}$ peut admettre des solutions. Cependant, pour qu'elle en ait effectivement, il faut que 252 soit un carré modulo chaque facteur premier de 793.
Nous avons déjà calculé que $\left(\frac{252}{13}\right) = -1$. Cela signifie que 252 n'est pas un carré modulo 13. Par conséquent, l'équation $x^2 \equiv 252 \pmod{793}$ n'admet pas de solutions.

4. Soit A un anneau factoriel. Démontrer que si $p \in A$ est irréductible, alors l'idéal (p) est premier. 3 pts

Solution: Soit $a, b \in A$ tels que $ab \in (p)$. Cela signifie qu'il existe un élément $c \in A$ tel que $ab = pc$. On décompose a et b en facteurs irréductibles :

$$a = u \prod_{i=1}^{m} p_i^{\alpha_i}, \quad b = v \prod_{j=1}^{n} q_j^{\beta_j},$$

où u, v sont des unités dans A, et p_i, q_j sont des éléments irréductibles de A. Ainsi,

$$ab = uv \prod_{i=1}^{m} p_i^{\alpha_i} \prod_{j=1}^{n} q_j^{\beta_j} = pc.$$

Par unicité de la décomposition en facteurs irréductibles dans un anneau factoriel, le facteur irréductible p doit apparaître dans la décomposition de ab, donc dans la décomposition de a ou de b. Par conséquent, p divise a ou p divise b, ce qui signifie que $a \in (p)$ ou $b \in (p)$. Ainsi, l'idéal (p) est premier.

5. Soit p un nombre premier impair. On considère l'anneau quotient $\mathbb{Z}[X]/(p, X^2 + 13)$.
   (a) Démontrer que cet anneau est intègre si et seulement si $X^2 + 13$ est irréductible dans $(\mathbb{Z}/p\mathbb{Z})[X]$. 2 pts

Solution: Cet anneau est isomorphe à $(\mathbb{Z}/p\mathbb{Z})[X]/(X^2 + 13)$. Un anneau quotient R/I est intègre si et seulement si l'idéal I est premier dans R. L'anneau de polynômes sur un corps est principal (euclidien), donc un idéal engendré par un polynôme est premier si et seulement si ce polynôme est irréductible. Ainsi, $(\mathbb{Z}/p\mathbb{Z})[X]/(X^2 + 13)$ est intègre si et seulement si $X^2 + 13$ est irréductible dans $(\mathbb{Z}/p\mathbb{Z})[X]$.

   (b) On suppose que $p \equiv 23 \pmod{52}$. Est-ce que l'anneau est intègre dans ce cas ? 2 pts

Solution: Le polynôme $X^2 + 13$ est irréductible dans $(\mathbb{Z}/p\mathbb{Z})[X]$ si et seulement si -13 n'est pas un carré modulo p. Pour déterminer si -13 est un carré modulo p, on utilise le symbole de Legendre :

$$\left(\frac{-13}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{13}{p}\right).$$

Comme $p \equiv 3 \pmod{4}$, on a $\left(\frac{-1}{p}\right) = -1$. Ensuite, en utilisant la réciprocité quadratique et le fait que $13 \equiv 1 \pmod{4}$, on obtient :

$$\left(\frac{13}{p}\right) = \left(\frac{p}{13}\right) = \left(\frac{10}{13}\right) = \left(\frac{2}{13}\right)\left(\frac{5}{13}\right).$$

En utilisant le complément de la loi de réciprocité, on trouve que $\left(\frac{2}{13}\right) = -1$. De plus, par réciprocité quadratique, on trouve que $\left(\frac{5}{13}\right) = \left(\frac{13}{5}\right) = \left(\frac{3}{5}\right) = -1$. On en déduit que

$\left(\frac{10}{13}\right) = (-1)(-1) = 1$. Donc, $\left(\frac{-13}{p}\right) = (-1)(1) = -1$. Ainsi, -13 n'est pas un carré modulo p, et donc $X^2 + 13$ est irréductible dans $(\mathbb{Z}/p\mathbb{Z})[X]$. Par conséquent, l'anneau est intègre lorsque $p \equiv 23 \pmod{52}$.