Exercices du chapitre IV (Arithmétique des entiers et des polynômes) – Indications

L'icône « (🗎) » indique que les documents *Méthodes* donnent des conseils plus généraux.
La lettre « C » indique que la *Banque des Cent* contient ou contiendra des exercices analogues.

Nombres premiers, critères de primalité

Exercice 1. (🗎)

1. Que vaut $\bar{2}^p$? Conclure grâce au fait que p soit premier.
2. Utiliser le théorème de Lagrange pour en déduire une inégalité entre p et q.

Commentaires. Cet exercice est une utilisation originale de l'ordre pour démontrer des relations de divisibilité (alors que d'habitude, c'est l'inverse : on utilise le fait que l'ordre divise un entier k vérifiant $g^k = e_G$ pour déterminer l'ordre par élimination, et le théorème de Lagrange pour trouver un tel entier k).
Cette stratégie marche sans difficulté majeure dès qu'on raisonne modulo un entier de la forme $a^k \pm 1$. En effet, on a immédiatement $a^k \equiv \mp 1 \bmod (a^k \pm 1)$, et déterminer son ordre est une affaire de routine. On raisonne ainsi dans les exercices 4, 17 et 22 par exemple.
Cette stratégie, de manière beaucoup plus élaborée (et utilisant les polynômes cyclotomiques de l'exercice 71), permet de démontrer des cas particuliers du théorème de la progression arithmétique de Dirichlet : en utilisant ces polynômes pour montrer qu'il existe une infinité de nombres premiers p tels que $\mathbb{Z}/p\mathbb{Z}$ admette un élément d'ordre n (l'entier n étant fixé), ce qui donne une infinité de nombres premiers tels que $p \equiv 1 \bmod n$ par le théorème de Lagrange.

Exercice 2. (Suite de Fibonacci)

1. Utiliser l'algorithme d'Euclide étendu. Noter que la relation $F_{n+2} = F_n + F_{n+1}$ fournit le quotient et le reste. Autre possibilité qui revient essentiellement au même : montrer que $\operatorname{pgcd}(F_{n+2}, F_{n+1}) = \operatorname{pgcd}(F_{n+1}, F_n)$ pour tout n et conclure par récurrence.
2. Faire une récurrence sur n.
3. Utiliser la question précédente pour montrer que si $m = nq + r$ avec $0 \leqslant r < n$, alors : $\operatorname{pgcd}(F_m, F_n) = \operatorname{pgcd}(F_n, F_r)$. En déduire que l'algorithme d'Euclide étendu appliqué à F_m et F_n parcourt les mêmes étapes que si on l'applique à m et n.

Commentaires. Le résultat de la dernière question a des conséquences étonnantes. Par exemple, si n divise m, alors F_n divise F_m. Sauriez-vous le démontrer sans cette méthode ? À comparer avec ce qu'on démontre dans l'exercice 18.
Le raisonnement de la dernière question apparaît aussi pour les nombres de Mersenne (définis dans l'exercice 3) ou dans l'exercice 74. Pour pressentir lorsqu'il va apparaître un tel raisonnement : c'est lorsqu'on nous demande de montrer que le pgcd de $\bigstar_m$ et $\bigstar_n$ est $\bigstar_{\operatorname{pgcd}(m,n)}$. Cela nécessite cependant de savoir expliciter chaque étape de l'algorithme d'Euclide étendu.
D'autres propriétés arithmétiques de la suite de Fibonacci sont étudiées dans l'exercice 18.

★ **Exercice 3. (Nombres premiers de Mersenne, de Fermat)**

1. Utiliser la relation $x^k - y^k = (x-y)\sum_{i=0}^{k-1} x^i y^{k-1-i}$ à bon escient. Éventuellement supposer n composé. La réciproque est fausse : chercher un contre-exemple.
2. Même principe. Supposer que n admet au moins un diviseur impair. Noter que si k est impair, alors $1 = -(-1)^k$.

Commentaires. La forme simplissime de ces nombres permet de fournir des critères de primalité qui fonctionnent spécifiquement pour ces nombres-là (notamment : les calculs de l'ordre de 2 modulo ces entiers sont élémentaires). Un exemple est le test de Lucas-Lehmer. Les plus grands nombres premiers connus sont tous des nombres de Mersenne.

Exercice 4. (Critère de Pépin) (🗎)

1. Que valent 2^{2^n} et $2^{2^{n+1}}$ modulo p ? Conclure avec le théorème de Lagrange.
2. Montrer que $\bar{a}$ est d'ordre $f_n - 1$ et engendre $(\mathbb{Z}/f_n\mathbb{Z})^\times$. En raisonnant sur le cardinal, montrer que $\mathbb{Z}/f_n\mathbb{Z}$ est un corps. Conclure.

Commentaires. C'est avec ce critère qu'Euler démontra que f_5 n'est pas un nombre premier et qu'il est divisible par 641. Pour comprendre ce qui a conduit Euler à tester la divisibilité par 641 : tout d'abord, cet exercice permet de montrer aisément que si p est un diviseur premier de f_n, alors $p \equiv 1 \bmod 2^{n+1}$ (prendre $a = 2$ et réduire modulo p). Pour $n = 65$, on doit donc avoir $p \equiv 1 \bmod 64$. On teste les nombres vérifiant cette condition (65, 129, 193, 257, 321, 385, 449, 513, 577, 641, etc.), en écartant ceux qui ne sont pas premiers, et à tâtons on tombe vite sur 641.
C'est le plus petit nombre de Fermat qui n'est pas premier, comme vous pouvez le vérifier. En fait, on ne sait pas s'il y a d'autres nombres de Fermat premiers que ceux pour $n \leqslant 4$, et on pense qu'il n'y en a qu'un nombre fini. Le plus grand nombre de Fermat composé connu est f_{23471}, et on ne sait pas ce qu'il en est pour f_{22} !

Exercice 5.

1. Noter que les diviseurs premiers de $n \equiv 3 \bmod 4$ doivent être congrus à $\pm 1 \bmod 4$. Raisonner par l'absurde.
2. Considérer $4\prod_{i=1}^{r} p_i + 3$.

Commentaires. Cette démonstration se généralise en remplaçant 4 par n'importe quel n tel que $(\mathbb{Z}/n\mathbb{Z})^\times$ soit de cardinal 2. Cela tombe bien, l'exercice 28 permet de les expliciter. La clé est en effet qu'il n'y a que deux classes de congruence possibles pour la plupart des nombres premiers modulo n, si n vérifie cette condition : soit 1, ou -1. Grâce à cela, le raisonnement des deux questions se généralise aisément pour montrer l'infinité de nombres premiers congrus à -1 modulo n. Elle est aussi vraie pour 1 modulo n mais pas aussi directement.
Le devoir des vacances d'été vous propose une démonstration analytique qui règle le problème pour toutes ces valeurs de n.
Pourquoi ne considère-t-on que $(\mathbb{Z}/n\mathbb{Z})^\times$? Un nombre premier p ne peut-il pas être dans une classe non inversible modulo n ?

★ **Exercice 6. (Théorème de Wilson et conséquence)**

1. Montrer que $\bar{k}$ est racine de $X^{p-1} - \bar{1}$ pour tout $\bar{k}$ non nul. Interpréter cela en termes d'ordre ou avec le petit théorème de Fermat.
2. Regarder le coefficient constant de $X^{p-1} - \bar{1}$.
3. Réécrire $\overline{(p-1)!} = \prod_{\bar{x} \in (\mathbb{Z}/p\mathbb{Z})^\times} \bar{x}$ avec un autre système complet de représentants, afin de pouvoir faire apparaître des termes en double dans ce produit. Les regrouper donnera le s^2 cherché.
4. Montrer que tout élément non nul de $\mathbb{Z}/n\mathbb{Z}$ est inversible.

Commentaires. Dans le traitement des questions 2 ou 3 (voire les deux, cela dépend de la façon de rédiger), apprécier encore une fois les effets des nombreuses permutations dans un groupe (et qui sont compatibles avec la loi). Ce fut déjà observé dans les exercices 22, 56 et 57 du chapitre III. Cela reviendra dans plusieurs exercices de cette feuille (voir, dans le regroupement thématique des exercices : *Sommes, produits indexés par un groupe fini*).
Cette double interprétation de $x^k = 1$ en termes d'ordre ET en termes de racines, est la grande originalité des raisonnements dans $\mathbb{Z}/p\mathbb{Z}$, et plus généralement dans n'importe quel corps fini. C'est à l'origine de plusieurs résultats remarquables, le plus remarquable d'entre eux étant la structure cyclique de $(\mathbb{Z}/p\mathbb{Z})^\times$. Voir les exercices 34 et 50 pour quelques exemples.
Le théorème de Wilson n'est pas un bon critère pratique de primalité : le calcul de $(p-1)!$ est très coûteux, même modulo p. Son intérêt est *théorique*, comme lorsqu'on l'utilise pour montrer que -1 admet une racine carrée.

★ **Exercice 7. (L'automorphisme de Frobenius pour les enfants)**

1. Montrer que $\bar{k}$ est racine de $X^{p-1} - \bar{1}$ pour tout $\bar{k}$. Interpréter cela en termes d'ordre ou avec le petit théorème de Fermat. Déduire de la factorisation trouvée : $(X+1)^p - (X+1) = X^p - X$, avec un changement d'indice convenable.
2. Utiliser la formule du binôme de Newton.

Commentaires. Derrière cet exercice en apparence anodin se cache un résultat extrêmement important : dans un anneau contenant $\mathbb{Z}/p\mathbb{Z}$, l'application $x \mapsto x^p$ est $\mathbb{Z}/p\mathbb{Z}$-linéaire ! Étonnant !
Ce n'est pas seulement un résultat intéressant parce qu'il est amusant (« le rêve du débutant »), mais parce que $x \mapsto x^p$ et ses itérés fournissent *tous* les automorphismes d'un corps fini K contenant $\mathbb{Z}/p\mathbb{Z}$. Cela implique notamment un cas particulier pour « enfants » de la théorie de Galois, que j'énonce sans démonstration mais qui n'est pas très difficile à démontrer (... si l'on utilise le fait que K^* est cyclique, ce qui n'est pas rien) : si K est de cardinal p^d (ce qui est la seule possibilité pour le cardinal d'un corps fini : voir l'exercice 54 du chapitre III), alors pour tout ℓ divisant d il existe un unique sous-corps de K de cardinal p^ℓ, et si l'on note K_ℓ ce corps alors : $\forall x \in K,\ x \in K_\ell \iff x^{p^\ell} = x$. C'est un analogue de la conjugaison complexe dont les points fixes sont exactement les réels, ou de la conjugaison $a + b\sqrt{d} \mapsto a - b\sqrt{d}$ dans $\mathbb{Q}[\sqrt{d}]$, dont les points fixes sont exactement les rationnels.
On l'utilise souvent en pratique ainsi : si on veut montrer qu'une équation dans $\mathbb{Z}/p\mathbb{Z}$ admet une solution, on en fabrique d'abord une dans un corps plus gros (de la même manière qu'on résout certaines équations réelles en se plaçant d'abord dans $\mathbb{C}$), et on vérifie son appartenance à $\mathbb{Z}/p\mathbb{Z}$ en calculant si elle est égale à sa puissance p^{e}. C'est souvent ainsi qu'on démontre le cas particulier suivant de la loi de réciprocité quadratique : 2 est un carré modulo p si et seulement si $p \equiv \pm 1 \bmod 8$ (on prend p premier impair).
Autre conséquence plus basique de la linéarité de $x \mapsto x^p$: ayant une racine α dans un corps K contenant $\mathbb{Z}/p\mathbb{Z}$ d'un polynôme $P \in \mathbb{Z}/p\mathbb{Z}[X]$, on obtient d'autres racines par simple exponentiation ! Et on les obtient toutes si P est irréductible dans $\mathbb{Z}/p\mathbb{Z}[X]$.
Bref, dans les corps finis, il est difficile de se passer de cet automorphisme. Mais dans $\mathbb{Z}/p\mathbb{Z}$ il s'agit simplement de l'identité à cause du théorème de Fermat, donc on ne se rend pas compte de son importance.

Exercice 8. (Étude d'une réciproque) Montrer que si p est un diviseur premier de n, alors $p^{v_p(n)}$ ne divise pas $\binom{n}{p}$, en étudiant la puissance de p dans l'expression $(p-1)!\binom{n}{p} = \frac{\prod_{i=0}^{p-1}(n-i)}{p}$. Conclure à une absurdité si $p \neq n$.

Commentaires. Comme souvent lorsqu'on multiplie une égalité par un certain entier, la raison pour laquelle on étudie $(p-1)!\binom{n}{p}$ au lieu de $\binom{n}{p}$ est pour n'avoir que des entiers en jeu, et se permettre des raisonnements arithmétiques. C'est une idée récurrente (voir les exercices 65 et 68 par exemple).
Cette réciproque est utilisée pour l'algorithme AKS, qui permet de déterminer en temps polynomial si un nombre entier est premier.

Exercice 9. Écrire $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ et minorer trivialement $p_i^{\alpha_i}$.

Commentaires. On peut très légèrement améliorer l'estimation en utilisant le fait que les p_i soient distincts et au moins distants de 2 (sauf 2 et 3). Néanmoins les meilleures estimations du nombre de diviseurs premiers recourent à l'analyse réelle ou complexe.

Exercice 10. (Comportement asymptotique de l'indicatrice d'Euler) Majoration triviale. Pour la minoration : écrire $\varphi(n) = n\prod_{i=1}^{r}\left(1-\frac{1}{p_i}\right)$, où $p_1,\dots,p_r$ sont les diviseurs premiers de n et minorer trivialement $-\frac{1}{p_i}$. On a besoin d'estimer r : s'inspirer de l'exercice précédent.

Commentaires. L'intérêt de la formule $\varphi(n) = n\prod_{i=1}^{r}\left(1-\frac{1}{p_i}\right)$ n'est certainement pas calculatoire (l'autre formule explicite est préférable). C'est un outil THÉORIQUE : elle facilite la comparaison entre n et $\varphi(n)$, et a l'avantage de ne pas dépendre des valuations p-adiques (éventuellement inconnues).

Relations de divisibilité, arithmétique modulaire

✓ **Exercice 11. (Inversibilité dans $\mathbb{Z}/n\mathbb{Z}$) (C)** Utiliser des relations de Bézout.

✓ **Exercice 12. (C)** Utiliser le petit théorème de Fermat. Vous aurez besoin de simplifier 10^n modulo 6 : passer par une récurrence ou le théorème chinois.

Commentaires. L'étude de 10^6 mod 6 montre les difficultés posées par le cas où l'on ne raisonne pas modulo un nombre premier. On peut avoir des choses très différentes (parfois un élément nilpotent, parfois des puissances qui « bouclent », etc.). Le seul moyen d'y voir clair sans tâtonner est de se ramener à des nombres premiers.
Passer par le théorème chinois n'est JAMAIS une mauvaise idée si vous connaissez les diviseurs premiers : le fait qu'il y ait un isomorphisme assure qu'il n'y a là aucune perte d'information. Dans le pire des cas, vous perdez un peu de temps si un raisonnement direct était possible. N'hésitez donc pas à en abuser !

✓ **Exercice 13.** Utiliser le théorème de Lagrange, et déterminer l'ordre par élimination.

Commentaires. Se demander à quelle condition sur n on a un résultat analogue dans $(\mathbb{Z}/n\mathbb{Z})^\times$ (à savoir : pour tout $a \notin \{0,\pm1\}$, soit a, soit $-a$ engendre le groupe).
Au contraire, quand est-ce que $\bar{a}$ et $-\bar{a}$ ont exactement le même ordre ? Faire le lien avec l'exercice 2 du chapitre III.

✓ **Exercice 14.** Écrire $p^2-1=(p-1)(p+1)$ et montrer qu'au moins un facteur est divisible par 3, et le produit par 8. Utiliser le théorème chinois.

Commentaires. Exercice en apparence anodin, qui intervient pourtant pour des questions non triviales dans les corps finis (pour montrer l'existence de solutions à $x^4=-1$, $x^8=1$, $x^{24}=1$, et d'autres variantes, etc., dans certains corps contenant $\mathbb{Z}/p\mathbb{Z}$).

✓ **Exercice 15.** Faire la liste des carrés modulo 8, et voir si la somme peut donner 7 modulo 8.

Commentaires. En fait, il y a une condition nécessaire et suffisante pour qu'un entier s'écrive comme somme de trois carrés. C'est une condition bien compliquée, si l'on compare à celle pour qu'un entier comme somme de deux ou quatre carrés : un entier naturel est une somme de trois carrés si et seulement s'il N'EST PAS de la forme $4^a(8b+7)$ avec a et b entiers. Cet exercice vous fait démontrer la partie du théorème la plus accessible...
On remarque que la connaissance des carrés (ou autres puissances) modulo n, au moins pour les petites valeurs de n, est très utile pour montrer l'impossibilité de solutions. Et pour cause : raisonner modulo n nous ramène à un ensemble fini, ou de bêtes considérations combinatoires et un recensement exhaustif permettent de montrer l'impossibilité (ou non) d'une égalité. Pour réaliser la portée de ce type d'idée, regardez en fin de document le nombre d'exercices qui l'exploitent.
Comparer la liste des carrés modulo 8 avec ce que nous enseignerait l'isomorphisme de l'exercice 39. Cet isomorphisme permet de savoir ce qu'il en est modulo 2^k pour tout k, sans calcul.

✓ **Exercice 16. (Critères de divisibilité)**

1. Écrire $n = \sum_{i=0}^{d} a_i 10^i$ et réduire modulo 3. Regarder 10 modulo 3. De même avec 9.
2. Même principe.
3. Même principe.

Commentaires. Maintenant que vous avez vu le théorème d'Euler, j'affirme que vous êtes en mesure de fournir des critères de divisibilité par tout entier n, ou presque (le cas où 10 n'est pas premier avec n est à traiter à part). Comment ? Pourquoi ceux de cet exercice sont cependant les plus agréables, en plus du critère de divisibilité par 2 et éventuellement par 4 ?

Exercice 17. (🖹) Déterminer l'ordre de a modulo $a^d - 1$. Conclure avec la caractérisation de l'ordre et l'hypothèse de l'énoncé.

Commentaires. Voir le commentaire de l'exercice 1. À noter qu'on fait ici quelque chose de très rare, pour déterminer l'ordre de a modulo $a^d - 1$: on utilise la relation d'ordre $\leqslant$ dans $\mathbb{Z}$ (je n'en dis pas plus au cas où vous n'auriez pas réussi l'exercice). Pourquoi cette nécessité ici, et qu'on ne voit presque nulle part ailleurs ?

Exercice 18. (Arithmétique de la suite de Fibonacci : relations de divisibilité)

1. Effectuer une récurrence.
2. Expliciter $\overline{F_n} \in \mathbb{Z}/5\mathbb{Z}$ *via* l'équation caractéristique, comme on le ferait dans $\mathbb{R}$ ou $\mathbb{C}$. On trouve ses racines en la mettant sous forme canonique.
3. Même principe. L'hypothèse : $p - 1|n$, sert à utiliser le petit théorème de Fermat.

Commentaires. Cet exercice doit vous débrider sur le fait que la résolution des équations polynomiales, au moins dans les cas simples, n'est pas propre à $\mathbb{R}$ ou $\mathbb{C}$: la résolution des équations de degré 2 ne nécessite en effet que de sommaires opérations (sommes, produits, quotients) qui sont valables dans tout anneau intègre (pourquoi l'intégrité ?), tant que la division par 2 est possible. De telles généralisations sont très nombreuses en algèbre (voir la construction de l'inverse de $u+n$ dans l'exercice 46, pour un autre exemple). L'important est de se demander : fait-on autre chose que des produits, différents, produits, quotients ? Si non, alors cela fonctionne dans tout cas. Si l'on a besoin d'une autre opération, mais qui reste profondément algébrique (extraire une racine n^{e} de a, ce n'est rien d'autre que manipuler une racine de $X^n - a$: c'est algébrique), alors cela se généralise potentiellement, quitte à construire l'objet dont vous avez besoin (éventuellement avec un anneau quotient : ils sont là pour ça).
Plus vous avez conscience, et plus vous serez à l'aise dans les structures en apparence abstraites, et plus vous serez capables de prendre de telles initiatives qui ont l'air audacieuses *a priori*.
Dans la dernière question, la condition que 5 est un carré est justement pour permettre l'extraction de racine carrée du discriminant de l'équation caractéristique. Si ce n'en est pas un alors, conformément à ce que je dis ci-dessus : il suffit de construire cette racine carrée. On y parvient en introduisant $K = \mathbb{Z}/p\mathbb{Z}[X]/(X^2 - 5)$ (sur le modèle de construction de $\mathbb{C}$ qui permet de fabriquer une racine carrée de -1), qui est un corps contenant $\mathbb{Z}/p\mathbb{Z}$, ou plutôt un sous-corps isomorphe à $\mathbb{Z}/p\mathbb{Z}$. On peut aussi prendre $K = \mathbb{Z}/p\mathbb{Z}[X]/(X^2 - X - 1)$ pour ne pas s'embêter à passer par le discriminant : une racine de l'équation caractéristique est simplement $\alpha = \overline{X}$ dans ce corps. On vous laisse alors poursuivre et démontrer que si $p + 1$ divise n, alors p divise F_n. Les réciproques sont fausses, hormis dans des cas particuliers comme $p = 3$ et $p = 5$.
La loi de réciprocité quadratique permet de démontrer que 5 est un carré modulo p si et seulement si $p \equiv \pm 1 \bmod 5$, ce qui achève l'étude de l'exercice.
Pour étudier la divisibilité par p^k, on a besoin du lemme de Hensel (exercice 56), et au-delà encore : du théorème chinois.

Exercice 19. (Théorème de Wilson quand n n'est pas premier) Noter que si $n = ab$ avec $1 < a, b < n$, alors a et b apparaissent dans $(n-1)!$. Sauf si...

★ **Exercice 20. (Valuation p-adique de la factorielle)**

1. Compter le nombre de multiples de p^k, pour k fixé, apparaissant dans $n!$. Compter la contribution de chacun de ces multiples à la valuation de $n!$. Attention à ne pas compter plusieurs fois un même nombre, ou bien à tenir compte de la répétition : par exemple p^2 est à la fois un multiple de p et de p^2.
   La majoration attendue découle alors de l'inégalité $\lfloor x \rfloor \leqslant x$ et du calcul d'une somme géométrique.
2. Cela revient à calculer les valuations 2-adique et 5-adique de 2023!.

Commentaires. On se demandera pour le raisonnement nécessite de prendre un nombre premier : pourquoi ne peut-on pas calculer quelle est la plus grande de puissance de 10 à diviser 2023! sans passer par 2 et 5, en imitant le raisonnement de la première question (où l'on remplace p par 10) ?
On se demandera aussi si le résultat de la première question peut être utilisé pour traiter les questions arithmétiques avec des coefficients binomiaux (exercices 7 et 8 par exemple). C'est en tout cas la raison d'être de ce résultat : affiner l'étude arithmétique des factorielles. On s'en sert dans l'exercice 38.

Exercice 21.

1. Écrire : $d\ell = 1 + kp$ avec $k \in \mathbb{Z}$, et multiplier convenablement cette égalité.

2. Raisonner dans $\mathbb{Z}/p\mathbb{Z}$. Considérer la bijection $\bar{x} \mapsto \bar{x}^{-1}$ pour simplifier la somme $\sum_{k=1}^{p-1} \bar{k}^{-1}$.

Commentaires. Nous avons plusieurs fois mis en évidence comment les sommes et produits sur des ensembles finis permettent de générer de nombreuses identités remarquables par changement d'indice (il y a beaucoup de permutations dans un ensemble fini, qui sont d'autant plus intéressantes quand elles interagissent avec les lois de la structure). Voir, dans le regroupement thématique des exercices : *Sommes, produits indexés par un groupe fini.* On se demandera si l'on est capable d'obtenir un résultat analogue en considérant $\sum_k \frac{1}{k^2}$.
La première question est un lemme purement technique. La notion « d'anneau localisé » (définie presque comme le corps de fractions d'un anneau commutatif intègre, en remplaçant $A \setminus \{0\}$ par une partie de $A \setminus \{0\}$ stable par multiplication), qui sert à rendre tout élément d'un anneau inversible sauf les puissances d'un élément irréductible fixé, permet d'éviter cette contorsion.

Exercice 22. (🗎) Regarder l'ordre de a modulo $a^n + 1$, et utiliser le théorème de Lagrange.

Commentaires. C'est une n^{e} illustration du commentaire de l'exercice 1.

✓ **Exercice 23.** Utiliser le théorème chinois et le petit théorème de Fermat.

Commentaires. Je n'ai pas choisi 2730 et 13 au hasard. Comprendre comment on pourrait généraliser cet exercice.
On ne se lassera pas de répéter qu'il ne coûte jamais rien de passer par le théorème chinois lorsqu'on connaît les diviseurs premiers : n'est-il pas agréable d'utiliser le petit théorème de Fermat ? Bien sûr, on se demandera pourquoi le théorème d'Euler, qui permet pourtant de simplifier $n^{\varphi(2730)}$ pour tout n premier avec 2730, n'est pas aussi efficace ici.

★ **Exercice 24. (Le chiffrement RSA)** Introduire $d \in \mathbb{N}$ tel que $de = 1 + k(p-1)(q-1)$. Calculer x^{de} modulo N en regardant ce que cela donne modulo p et q. Utiliser le théorème chinois.

Commentaires. On se demande pourquoi je prends $d \in \mathbb{N}$ et non $d \in \mathbb{Z}$. Globalement : il y a plein de micro-subtilités, certaines faciles à lever, sur le sens des puissances négatives modulo n. On s'efforcera de se poser la question de la légitimité des opérations sur les puissances dès qu'on en croise.
On appelle f_e l'application de chiffrement de RSA, tandis que la réciproque construite est l'application de déchiffrement. La donnée de (e, N) est publique, de sorte que tout le monde puisse chiffrer un message en utilisant f_e (après avoir converti le message en un élément de $\mathbb{Z}/N\mathbb{Z}$). C'est notamment utilisé quotidiennement lors des transactions bancaires. La donnée de (p, q) ou celle, équivalente, de $(d, \varphi(N))$, est en revanche privée. Tout le monde peut chiffrer, mais pas déchiffrer (dans le cas des transactions bancaires, seule votre banque peut déchiffrer afin de vérifier l'authenticité du compte) : on parle de cryptosystème asymétrique.
La solidité du chiffrement découle de la difficulté d'obtention de d (qui est nécessaire pour déchiffrer *a priori*) lorsqu'on ne connaît pas p et q : si on ne connaît pas p et q, on ne connaît pas $\varphi(N)$ et donc le calcul de l'inverse de e modulo $\varphi(N)$ nous échappe (on peut montrer facilement que réciproquement, si on connaît N et $\varphi(N)$, on connaît p et q).
Cependant, le jour où des algorithmes permettront de factoriser rapidement un entier, on pourra obtenir p et q à partir de n et la sûreté de ce chiffrement ne sera plus assurée.

✓ **Exercice 25. (Systèmes de congruence) (C)** La méthode est standard et vue en cours. Comme 3 n'est pas inversible modulo 12, vous aurez d'abord à simplifier la deuxième ligne du deuxième système pour y remédier (remarquer que 3, 9 et 12 sont tous divisibles par 3). Attention au fait que 63 et 12 ne soient pas premiers : se ramener d'abord à des modules premiers entre eux par une réduction convenable.

Commentaires. Plus généralement, savoir réagir *sans réfléchir* lorsqu'on est dans les situations défavorables suivantes : 1° les modules ne sont pas premiers entre eux, 2° en facteur de l'inconnue n apparaît un entier non inversible. La solution est systématiquement la même.

✓ **Exercice 26.** Utiliser le théorème chinois, en notant que soit 2, soit 3 est inversible modulo p^α pour p premier.

Commentaires. On rappelle que l'intérêt de se ramener à $\mathbb{Z}/p^\alpha\mathbb{Z}$ *via* le théorème chinois est que la description des inversibles (et non inversibles), des diviseurs de zéro, des éléments nilpotents, etc., est extrêmement simple dans ces anneaux. Illustration ici.

✓ **Exercice 27.** Lorsqu'on raisonne modulo un nombre premier p, l'intégrité de $\mathbb{Z}/p\mathbb{Z}$ permet de résoudre ces équations polynomiales « comme dans $\mathbb{R}$ ou $\mathbb{C}$ ». En cas d'équation polynomiale du second degré : mettre sous forme canonique, etc. La question se ramène à la recherche d'une racine carrée du discriminant. Si l'on n'est pas modulo un nombre premier : utiliser le théorème chinois. Seule l'étude modulo 36 ne le permet pas : pas grave. Utiliser la méthode du pivot comme on le ferait dans un corps, en évitant de « diviser » par des entiers non inversibles. Si vous avez une congruence du type : $\alpha x \equiv \beta \bmod n$, où α, β et n ne sont pas premiers entre eux : écrire la relation dans $\mathbb{Z}$ et diviser l'égalité par leur pgcd.

Commentaires. Cet exercice fait écho à la première partie de mon commentaire de l'exercice 18, sur la résolution des équations polynomiales, et plus généralement sur tout ce qui se généralise à un corps quelconque.
Observer le nombre de solutions de chaque équation, et le comparer au degré : que dire ?

✓ **Exercice 28.**

1. Soit on écrit $\varphi(n)$ en fonction des diviseurs premiers de n et on remarque qu'il apparaît au moins un facteur pair ; soit on note que pour tout $k \in [\![1, n]\!]$, on a : $\text{pgcd}(k, n) = \text{pgcd}(n - k, n)$.
2. Décomposer n en facteurs premiers et exprimer $\varphi(n)$ à l'aide d'iceux. Noter que l'équation $\varphi(n) = 2$ met déjà une contrainte sur le *nombre* de facteurs premiers, et ensuite sur leur valeur et leur valuation. Raisonnement analogue pour $\varphi(n) = 4$.

Commentaires. On se demandera si le raisonnement de la deuxième question fournit un *algorithme* pour trouver les solutions de $\varphi(n) = k$ d'inconnue n. Y a-t-il toujours une solution pour k pair ?

Exercice 29. Sens direct : utiliser le théorème chinois et le théorème d'Euler. Sens réciproque : Faire apparaître une relation de Bezout entre m et n.

✓ **Exercice 30.** Utiliser le théorème chinois (j'ai l'impression d'écrire la même chose à chaque exercice). Résoudre $x^2 \equiv 1 \bmod p$, pour p premier, est facile par intégrité de $\mathbb{Z}/p\mathbb{Z}$. Ne pas oublier le cas $p = 2$. S'inspirer d'un exemple du cours.

Commentaires. On rappelle que l'intérêt de se ramener à $\mathbb{Z}/p^\alpha\mathbb{Z}$ *via* le théorème chinois est que la description des inversibles (et non inversibles), des diviseurs de zéro, des éléments nilpotents, etc., est extrêmement simple dans ces anneaux. Mieux encore quand $\alpha = 1$, puisqu'on a un corps (qui est en particulier intègre), ce qui permet de résoudre des équations polynomiales comme dans $\mathbb{R}$. Or comment se ramener à cette situation ? Avec le théorème chinois, comme on l'illustre encore ici.

Exercice 31.

1. Raisonner par l'absurde, et réduire modulo 4.
2. Montrer : $y^2 + 1 \equiv 3 \bmod 4$ (vous aurez besoin d'une distinction de cas sur la congruence de x modulo 4, et de montrer que l'une d'elles est impossible). En déduire l'existence de p comme dans l'exercice 5. Avoir une absurdité en utilisant le petit théorème de Fermat avec y d'une part, et en montrant $(-1)^{\frac{p-1}{2}} \equiv -1 \bmod p$ d'autre part.

Commentaires. On remarque que la connaissance des carrés (ou autres puissances) modulo n, au moins pour les petites valeurs de n, est très utile pour montrer l'impossibilité de solutions. Et pour cause : raisonner modulo n nous ramène à un ensemble fini, ou de bêtes considérations combinatoires et un recensement exhaustif permettent de montrer l'impossibilité (ou non) d'une égalité. Pour réaliser la portée de ce type d'idée, regardez en fin de document le nombre d'exercices qui l'exploitent.
À cet effet, un élève de MP⋆ se doit de savoir démontrer sans aucune difficulté que -1 est un carré modulo p si et seulement si : $p \equiv 1 \bmod 4$ (outre cet exercice, il en est question dans les exercices 6 et 50). Par extension, lorsqu'il voit la condition de congruence $p \equiv \pm 1 \bmod 4$, il doit avoir ce résultat dans un coin de la tête.

Exercice 32.

1. Trouver une solution rationnelle de la forme $\left(\frac{\clubsuit}{3}, \frac{\spadesuit}{3}\right)$, et multiplier par 9, pour en déduire une solution modulo tout entier premier avec 3. Montrer ensuite l'existence d'une solution modulo 3^k pour tout $k \in \mathbb{N} \setminus \{0\}$ avec $x \equiv 0 \bmod 3^k$ et y bien choisi. Conclure modulo tout entier grâce au théorème chinois.
2. Raisonner par l'absurde. Réduire modulo 4, et en déduire que y est pair. Injecter $y = 2k$ dans l'équation et noter qu'on doit avoir $k = 0$ pour des raisons d'ordre de grandeur. Conclure.

Commentaires. Le théorème chinois fut utilisé pour résoudre des équations diophantiennes dans d'autres exercices : exercices 30 et 26 par exemple. Ici, la motivation n'est pas la même que dans l'exercice 30 (où l'on voulait un nombre premier pour utiliser l'intégrité d'un corps) : on veut « rendre inversible » certains éléments de l'équation pour faciliter la résolution. C'est ce qui dicte le choix du module auquel on réduit.

Exercice 33.

1. Réduire modulo 5 et avoir une absurdité en cas d'existence de solutions.
2. Mettre au même dénominateur x et y, sous la forme : $x = \frac{a}{c}$, $y = \frac{b}{c}$ (quitte à faire une division par le pgcd,on peut supposer que tous les entiers en jeu sont premiers entre eux), et multiplier l'égalité par ce dénominateur au carré. Réduire modulo 5. On a : $a^2 \equiv 3c^2 \bmod 5$. Montrer que si a ou c est divisible par 5, alors les trois entiers le sont, ce qui est au contraire à l'hypothèse ci-avant, et que si a et c ne sont pas divisibles par 5, alors l'absurdité de la première question se reproduit.

Commentaires. On remarquera que la connaissance des carrés (ou autres puissances) modulo n, au moins pour les petites valeurs de n, est très utile pour montrer l'impossibilité de solutions. Et pour cause : raisonner modulo n nous ramène à un ensemble fini, ou de bêtes considérations combinatoires et un recensement exhaustif permettent de montrer l'impossibilité (ou non) d'une égalité. Pour réaliser la portée de ce type d'idée, regardez en fin de document le nombre d'exercices qui l'exploitent.

Approfondissement de la structure de $(\mathbb{Z}/n\mathbb{Z})^\times$ et applications

★ **Exercice 34. ($(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique)**

1. C'est la même démonstration que l'identité analogue avec l'indicatrice d'Euler (exercice 12 du chapitre III).
2. Noter que $\langle y\rangle$ fournit d racines distinctes de X^d-1 dans $\mathbb{Z}/p\mathbb{Z}$. Conclure en remarquant que les éléments d'ordre d sont des racines de ce polynôme.
3. Utiliser la question précédente pour montrer que s'il existe un élément d'ordre d, alors il existe un unique sous-groupe de $(\mathbb{Z}/p\mathbb{Z})^\times$ de cardinal d et il doit être cyclique. On connaît son nombre de générateurs et on conclut en notant que tous les éléments d'ordre d de $(\mathbb{Z}/p\mathbb{Z})^\times$ doivent l'engendrer.
4. Noter qu'on a : $\sum_{d|p-1} N(d) = \sum_{d|p-1} \varphi(d)$. Utiliser la question précédente pour montrer que les termes généraux sont égaux pour tout d.

Commentaires. Avec cet exercice, on voit que l'interprétation algébrique de φ donné dans ce chapitre (le cardinal du groupe des inversibles) ne doit pas faire oublier que cette fonction code aussi le nombre d'éléments d'ordre donné dans un groupe cyclique.
Cette double interprétation de $x^k=1$ en termes d'ordre ET en termes de racines, est la grande originalité des raisonnements dans $\mathbb{Z}/p\mathbb{Z}$, et plus généralement dans n'importe quel corps fini. La plupart des démonstrations de la structure cyclique de $(\mathbb{Z}/p\mathbb{Z})^\times$ s'en servent. Voir les exercices 6 et 50 pour d'autres exemples.
On remarquera que ce raisonnement ne permet pas de construire explicitement un générateur. On en cherchera pour de petites valeurs de p, afin de se convaincre qu'aucune règle générale ne semble se dégager.
De tous les résultats hors programme du chapitre, celui-ci est le plus important. Il permet de transformer des problèmes multiplicatifs en problèmes additifs *via* un isomorphisme avec $\mathbb{Z}/(p-1)\mathbb{Z}$: c'est plus facile à gérer (par exemple, la résolution de $x^d=y$ d'inconnue x est ardue dans $(\mathbb{Z}/p\mathbb{Z})^\times$, elle est enfantine additivement : $dx=y$ se résout en multipliant par l'inverse de d). À cela, ajouter tous les avantages des groupes cycliques (déterminer les morphismes en raisonnant uniquement sur un générateur, etc.). Les exercices qui suivent en donnent des applications.

Exercice 35.

1. D'abord noter que $\bar{x}^m=\bar{1}$ équivaut à $\bar{x}^{\mathrm{pgcd}(m,p-1)}=\bar{1}$, ce qui permet de se ramener à un diviseur de $p-1$. Cela revient à compter le nombre d'éléments d'ordre divisant $\mathrm{pgcd}(m,p-1)$: la structure cyclique de $(\mathbb{Z}/p\mathbb{Z})^\times$ donne ce nombre d'éléments.
   Autre argument sans la structure cyclique : montrer que $X^{p-1}-\bar{1}$ est scindé et à racines simples (s'inspirer de l'exercice 6), puis que $X^{\mathrm{pgcd}(m,p-1)}-\bar{1}$ le divise. En comptant ses racines, on a répondu à la question.
2. On connaît le noyau de $\bar{x}\mapsto\bar{x}^m$ et on demande l'image : comment relier leurs cardinaux ?

Commentaires. Cette double interprétation de $x^k=1$ en termes d'ordre ET en termes de racines, est la grande originalité des raisonnements dans $\mathbb{Z}/p\mathbb{Z}$, et plus généralement dans n'importe quel corps fini. C'est à l'origine de plusieurs résultats remarquables, le plus remarquable d'entre eux étant la structure cyclique de $(\mathbb{Z}/p\mathbb{Z})^\times$. Voir les exercices 34 et 50 pour quelques exemples.
La deuxième question incite à deux choses : 1° reconnaître dans un énoncé l'image ou le noyau d'un morphisme (même quand l'énoncé n'y incite pas), 2° se souvenir que comme en algèbre linéaire, connaître le noyau permet d'en déduire l'image. Ici, c'est avec le théorème d'isomorphisme.

★ **Exercice 36. (Critère de Korselt)** Sens direct : appliquer $n|a^m-a$ avec $a=p$, pour montrer que p^2 ne divise pas n. Ensuite : raisonner modulo p avec un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$ et utiliser le théorème de Lagrange. Sens réciproque : utiliser le petit théorème de Fermat et le théorème chinois.

Commentaires. Exercice fort riche, où tous les outils principaux du chapitre sont employés. J'apprécie notamment qu'on y utilise une conséquence heureuse du théorème chinois : de pouvoir fabriquer des entiers VÉRIFIANT LES CONGRUENCES QU'ON VEUT ! En particulier, ici : être un générateur modulo le nombre premier désiré.
Ce critère de Korselt est utilisé pour trouver des nombres de Carmichael. Ce même énoncé permet par exemple de démontrer qu'un nombre de Carmichael doit avoir au moins trois facteurs premiers et être impair : pourquoi ?

Exercice 37. ($(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est cyclique)

1. Si d est l'ordre de u dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$, que dire de $u^d \bmod p^\alpha$, puis modulo p ?
2. Prendre une puissance convenable de u.
3. Récurrence par récurrence et utiliser la formule du binôme de Newton.

4. Montrer que $1+p$ est d'ordre $p^{\alpha-1}$ puis que $v(1+p)$ est d'ordre $(p-1)p^{\alpha-1}$. Comparer au cardinal de $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$.

Commentaires. La cyclicité de $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ permet de relier à la principale défaillance de l'anneau $\mathbb{Z}/p^\alpha\mathbb{Z}$ par rapport à $\mathbb{Z}/p\mathbb{Z}$: il n'est plus intègre. On ne peut notamment plus utiliser l'intégrité, ni un argument sur les racines, pour démontrer les solutions d'une équation aussi basique que $\bar{x}^2 = \bar{1}$. C'est là que le résultat de cet exercice intervient !
Cet exercice montre aussi que le plus dur est finalement de trouver un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$, puisqu'on en déduit un générateur de $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ pour tout $\alpha \geqslant 1$ à peu de frais (ce principe revient souvent : voir le lemme de Hensel dans l'exercice 56).
On se demandera pourquoi le cas $p = 2$ échappe à la méthode de l'exercice.

Exercice 38. ($(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est cyclique : démonstration « constructive »)

1. Écrire x en base p et factoriser convenablement. Le fait que x soit inversible modulo p^α donne une information sur son chiffre des unités.
2. Exprimer $v_p\left(\frac{x^n}{n!}\right)$ à l'aide de $v_p(x)$ et $v_p(n!)$. Utiliser l'exercice 20.
3. Immédiat avec la question précédente : p divise $\frac{x^n}{n!}$ (au sens donné dans l'énoncé) pour tout n assez grand.
4. Raisonnement analogue à celui de l'exercice 21, première question. Montrer que $\exp_p$ est un morphisme comme on le fait pour l'exponentielle complexe. Montrer l'injectivité et comparer les cardinaux pour conclure.
5. Comme $\exp_p$ est un isomorphisme, il conserve les ordres. L'ordre de $\bar{u}$ est aussi connu, ce qui permet de conclure car $p-1$ et p^α sont premiers entre eux.
6. Calcul naïf. Bien simplifier les quotients $\frac{3^n}{n!}$ autant que possible. Un générateur de $(\mathbb{Z}/3\mathbb{Z})^\times$ est trivial à obtenir.

Commentaires. Cet exercice est intéressant à deux égards : il montre que le plus dur est finalement de trouver un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$, puisqu'on en déduit un générateur de $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ pour tout $\alpha \geqslant 1$ à peu de frais (ce principe revient souvent : voir le lemme de Hensel dans l'exercice 56). De plus, il montre un des – nombreux – intérêts de l'expression d'une fonction usuelle sous forme de série entière : puisqu'une telle écriture ne fait intervenir que des sommes et exponentiations (pour caricaturer), elle permet de généraliser aisément des fonctions usuelles à d'autres contextes que le cas réel ou complexe. C'est essentiel si l'on veut pouvoir profiter de leurs propriétés ailleurs. On pourrait de la même manière définir un logarithme ou un cosinus p-adique, même si cette dernière fonction n'a pas un grand intérêt dans ce contexte. Nous en ferons autant dans $\mathrm{L}(E)$ et $\mathrm{M}_n(K)$ puisque nous parlerons de l'exponentielle d'un endomorphisme ou d'une matrice.
L'élève en exercice s'efforcera de comprendre ce que cette approche donne dans le cas $p = 2$. Le résultat de l'exercice 39 pourra éventuellement l'aiguiller.

Exercice 39. ($(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ n'est pas cyclique si $\alpha \geqslant 3$)

1. Par récurrence. En déduire la plus petite puissance de 5 qui donne 1 modulo 2^α.
2. Utiliser le théorème de factorisation pour avoir la bonne définition et l'injectivité. Comparer les cardinaux pour avoir la bijectivité. L'isomorphisme montre que l'ordre maximal d'un élément de $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ est $2^{\alpha-2}$. Conclure.
3. La recherche d'un générateur dans chaque cas est aisée.

Commentaires. Même si on n'obtient pas un groupe cyclique dans le cas $p = 2$, l'isomorphisme obtenu est « mieux que rien », et même très maniable. Comme dans le cas p impair, son intérêt est de de transformer des problèmes multiplicatifs en problèmes additifs *via* un isomorphisme avec $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\alpha-2}\mathbb{Z}$: c'est plus facile à gérer. Il suffit de compter le nombre de solutions de $x^2 = 1$ modulo 2^α sans cet isomorphisme, puis de le faire en résolvant $2(x, y) = (0{,}0)$ dans le groupe isomorphe, pour s'en convaincre.
De plus, un avantage ici : l'isomorphisme est explicite. Ainsi c'est un moyen *pratique* de résoudre des problèmes multiplicatifs en étudiant l'analogue additif. Par exemple, quelles sont les solutions de $x^2 \equiv 1 \bmod 2^6$?

Exercice 40. Cela revient à compter le nombre d'éléments de $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ d'ordre divisant d. Utiliser la cyclicité de $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$.

Commentaires. Le commentaire de l'exercice 35 ne serait plus valable ici, parce qu'on n'a plus de structure de corps. On ne peut plus raisonner sur les racines d'un polynôme. Ainsi la cyclicité est vraiment un recours incontournable ici !

Exercice 41. Cela revient à compter le nombre d'éléments de $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ d'ordre divisant d. L'isomorphisme de l'exercice 39 permet de ramener cette résolution à celle de : $d(y \bmod 2, y \bmod 2^{\alpha-2}) = (0 \bmod 2{,}0 \bmod 2^{\alpha-2})$: on sait résoudre explicitement cette équation.

Commentaires. Voir les commentaires de l'exercice 39, que nous mettons en application ici.

Exercice 42. (Vous savez désormais tout sur $(\mathbb{Z}/n\mathbb{Z})^\times$)

1. Utiliser le théorème chinois pour vous ramener à la situation des exercices précédents.

2. Déterminer l'ordre maximal d'un élément de $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ ou $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ grâce aux exercices précédents. Par produit, en déduire l'ordre maximal d'un élément de $\prod_i(\mathbb{Z}/p^{\alpha_i}\mathbb{Z})^\times$ (attention à ne pas aller trop vite : voir l'exercice 2 du chapitre III), et utiliser le théorème chinois pour conclure.

Commentaires. Vous l'avez compris dans ce chapitre : quand on a résolu un problème modulo p^k pour tout p premier et tout k, on en déduit les solutions modulo n par le théorème chinois. Comme $(\mathbb{Z}/n\mathbb{Z})^\times$ n'est pas cyclique en général, un raisonnement direct n'était pas possible.

Anneaux principaux

Exercice 43. Montrer que pour tout p irréductible, on a : $2v_p(a) = v_p(b) + v_p(c)$. Utiliser l'hypothèse de l'énoncé pour montrer que pour tout p, soit $v_p(b) = 0$, soit $v_p(c) = 0$. Conclure en décomposant b et c en facteurs irréductibles.

Commentaires. On se demandera ce qui pouvait nous inciter à raisonner sur la décomposition en facteurs irréductibles.
Cet exercice se généralise, en prenant 2 par n'importe quelle puissance. Il est souvent employé dans l'étude des équations diophantiennes faisant apparaître des exponentiations. On l'illustre dans l'exercice 48 mais aussi dans les *Savoir-faire à vérifier*.

Exercice 44. La vérification que c'est un anneau est facile. Si I est un idéal de $\mathbb{D}$, montrer qu'après multiplication convenable il se ramène à un idéal de $\mathbb{Z}$.

Commentaires. La méthode principale pour montrer qu'un anneau est principal, est d'utiliser une division euclidienne. On pourrait le faire ici. Mais dans les cas rares où les idéaux de l'anneau se ramènent aisément aux anneaux principaux usuels ($\mathbb{Z}$ et $K[X]$), on aurait tort de se priver.
On peut se demander : si $f : A \to B$ est un morphisme d'anneaux injectifs et si A est principal, est-ce que B l'est aussi ? Et si f est surjectif ? Dans le cas d'un isomorphisme, vous vous doutez que la réponse est positive (ou vous n'avez jamais écouté mes cours).

★ **Exercice 45. (L'anneau des entiers de Gauß, le corps des nombres de Gauß)**

1. Vérifications élémentaires, la stabilité de $\mathbb{Z}[i]$ par produit est basée sur le fait que $i^2 = -1$. Pour montrer que $\mathbb{Q}(i)$ est stable par inversion : vous savez mettre sous forme algébrique un quotient de nombres complexes.
2. L'inclusion réciproque est facile à obtenir si vous avez réussi la question précédente. L'inclusion directe s'obtient en prenant pour b un dénominateur commun convenable.

Commentaires. Les ensembles de la forme $\mathbb{Q}(\alpha)$ sont plus longuement étudiés dans l'exercice 83. Ils sont au cœur de l'arithmétique moderne. On en donne ici le cas le plus simple (en dehors de $\mathbb{Q}$). Noter que la stabilité par produit et inverse tient au fait que i soit annulé par une équation de degré 2 : c'est la clé pour les autres anneaux et corps analogues.

★ **Exercice 46. ($\mathbb{Z}[i]$ est un anneau principal)**

1. Prendre pour q un élément de $\mathbb{Z}[i]$ « aussi proche que possible » de $\frac{a}{b} \in \mathbb{Q}(i)$. La forme algébrique de $\frac{a}{b}$ et une observation géométrique vous aideront à définir q. Une fois q défini, on a r immédiatement. Il reste à vérifier l'inégalité proposée : calcul trivial si q est bien défini.
2. Imiter la démonstration faite pour $\mathbb{Z}$ et $K[X]$. On prend pour a un élément non nul de module au carré minimal.
3. Voir le cours.
4. Voir le cours. Au lieu de raisonner par l'absurde avec un ensemble non vide d'idéaux contredisant l'existence : raisonner sur un élément de $\mathbb{Z}[i] \setminus \{0\}$ minimal au sens du module au carré et qui contredirait l'existence de la décomposition.

Commentaires. C'est l'exemple le plus simple et instructif d'anneau principal parmi les non usuels. On s'attardera sur la construction géométrique de q, qui sert de modèle pour tous les autres anneaux principaux analogues (et abordables en classes préparatoires).
Puisque c'est un anneau principal, on peut y faire de l'arithmétique ; c'est l'enseignement des deux dernières questions. Mais cela est bien vain si on ne sait pas caractériser ses inversibles et irréductibles. C'est l'objet de l'exercice 47. On en donne une application dans l'exercice 48, qui figurait dans la *Présentation des chapitres de MP*.

Exercice 47. (Inversibles et irréductibles de $\mathbb{Z}[i]$)

1. Si $a \times b = 1$, prendre le module au carré dans cette égalité permet de limiter les possibilités pour a et b. Penser à vérifier la réciproque.
2. Suivre l'indication de l'énoncé. Comme p est premier, cette idée permet de montrer qu'il existe des entiers a et b tels que : $p = a^2 + b^2$. Réduire modulo 4 pour avoir une contradiction : quelles sont les valeurs possibles de carrés modulo 4 ?

3. Même idée que dans la question précédente. Noter que $\mathrm{N}(x) = 1$ est possible si et seulement si x est inversible.
4. Trouver un élément de $\mathbb{Z}[i]$ dont le module au carré égale 2.

Commentaires. L'idée de presque toutes ces questions, et qui apparaît dans d'autres anneaux principaux : utiliser le module au carré pour se ramener à des relations dans $\mathbb{Z}$ (où l'on connaît mieux l'arithmétique et les contraintes dues aux relations de divisibilité). La retenir !
La généralisation de cette stratégie à d'autres anneaux nécessite de parler de *norme* d'un entier.

Exercice 48. (Triplets pythagoriciens)

1. Vérification immédiate.
2. Si deux de ces entiers sont pairs, le troisième doit l'être aussi (réduire modulo 2 l'équation et utiliser le lien entre la parité d'un entier et celle de son carré), ce qui contredit ce qu'on sait sur a, b et c. Il ne peut pas y en avoir zéro, car la somme de deux entiers impairs est un entier pair. Supposer que c est pair et a, b impairs, et réduire modulo 4 l'équation, pour avoir une absurdité.
3. Si d est irréductible et divise $a \pm ib$, il divise leur somme et leur différence. Montrer que d ne divise pas 2 grâce à la question précédente, et utiliser le lemme d'Euclide pour avoir une absurdité. Conclure avec l'exercice 43.
4. Développer le carré et identifier parties réelles et imaginaires. Vérifier la réciproque.

Commentaires. Le traitement de cet exercice permet d'enfin comprendre, sur un exemple concret, l'intérêt de faire de l'arithmétique dans des anneaux plus gros que $\mathbb{Z}$: plus on a de nombres à disposition, et plus on peut faire de factorisations qui, interprétées en termes de divisibilité, sont suffisamment contraignantes pour expliciter les solutions (ou montrer leur inexistence).
Pour voir comment Euler put démontrer l'inexistence de solutions non triviales à l'équation de Fermat $x^3 + y^3 = z^3$, avec ce type d'idées : voir le sujet de Mathématiques Générales à l'agrégation externe de Mathématiques, année 2019. On y utilise la principalité de l'anneau $\mathbb{Z}[j]$ (que vous pouvez démontrer sur le modèle de $\mathbb{Z}[i]$).

Exercice 49. (Exemple d'anneau non principal)

1. Vérification facile.
2. Même idée que dans l'exercice 47 : écrire l'un des trois éléments de l'énoncé comme produit d'éléments de $\mathbb{Z}[i\sqrt{5}]$ et prendre le module au carré pour se ramener à une égalité dans $\mathbb{N}$.
3. Montrer que 6 s'écrit de deux façons différentes comme produit d'irréductibles de $\mathbb{Z}[i\sqrt{5}]$.

Commentaires. Comme on le disait en commentaire de l'exercice 47 : utiliser le module au carré permet de se ramener à des relations dans $\mathbb{Z}$ (où l'on connaît mieux l'arithmétique et les contraintes dues aux relations de divisibilité). Retenir cette idée !
Arriveriez-vous à trouver d'autres anneaux analogues qui ne vérifient pas l'unicité de la décomposition en facteurs irréductibles ?
Cet anneau n'est pas principal, ce qui peut paraître étonnant étant donné que $\mathbb{Z}\left[\sqrt{5}\right]$ l'est. En essayant d'imiter la démonstration valable dans $\mathbb{Z}[i]$, $\mathbb{Z}[i\sqrt{2}]$ ou encore $\mathbb{Z}[j]$, on essaiera de comprendre ce qui peut bien coincer ici.

Dénombrement des carrés, symbole de Legendre et sommes de Gauß

★ **Exercice 50. (Caractérisation des carrés dans $\mathbb{Z}/p\mathbb{Z}$, symbole de Legendre)**

1. Deux approches possibles : 1° soit on étudie le noyau de $\bar{x} \mapsto \bar{x}^2$ et on en déduit le cardinal de l'image grâce à un résultat classique, 2° soit on utilise la cyclicité de $(\mathbb{Z}/p\mathbb{Z})^\times$ (voir l'exercice 34) pour fabriquer aisément $\frac{p-1}{2}$ carrés à l'aide d'un générateur, et on utilise un argument sur les racines de $X^{\frac{p-1}{2}} - \bar{1}$ pour montrer qu'il n'y en a pas plus. On passe alors de $(\mathbb{Z}/p\mathbb{Z})^\times$ à $\mathbb{Z}/p\mathbb{Z}$ aisément.
2. Écrire $\bar{x} = \bar{y}^2$ et utiliser convenablement le petit théorème de Fermat.
3. Utiliser un argument sur les racines de $X^{\frac{p-1}{2}} - \bar{1}$ pour montrer que seuls les carrés de $(\mathbb{Z}/p\mathbb{Z})^\times$ vérifient cette congruence.
4. Appliquer les deux questions précédentes à $\bar{x} = -\bar{1}$.
5. Montrer : $\left(\frac{x}{p}\right) \equiv x^{\frac{p-1}{2}} \bmod p$. L'intégrité de $\mathbb{Z}/p\mathbb{Z}$ intervient pour montrer qu'un non carré vérifie $\bar{x}^{\frac{p-1}{2}} = -\bar{1}$.

Commentaires. Exercice fondamental, préliminaire à toute étude approfondie des carrés modulo p (et connaître ces carrés apparaît dans bien des exercices, comme vous pouvez le constater dans le regroupement thématique en fin de document). Apprécier la richesse des arguments utilisés : petit théorème de Fermat, argument sur les racines d'un polynôme, lien entre noyau et image d'un morphisme, argument d'intégrité pour déterminer le noyau.

Exercice 51. Si H est le sous-groupe des carrés de $(\mathbb{Z}/p\mathbb{Z})^\times$ (pourquoi est-ce un groupe ?) : utiliser l'exercice précédent pour montrer que $(\mathbb{Z}/p\mathbb{Z})^\times/H$ est un groupe quotient de cardinal 2. Calculer xy modulo H, où x et y ne sont pas des carrés.

Si l'on ne veut pas utiliser de groupe quotient : noter que si x et y sont deux non carrés de $(\mathbb{Z}/p\mathbb{Z})^\times$, alors $(\mathbb{Z}/p\mathbb{Z})^\times = H \sqcup xH$, donc $xy \in H$ ou $xy \in xH$. Montrer que le second cas entraînerait une contradiction.

Commentaires. Ce qu'on observe là vaut pour tous les sous-groupes d'un groupe fini G de cardinal $\frac{\mathrm{card}(G)}{2}$: penser au groupe symétrique. Si deux permutations sont de signature -1, leur produit est de signature 1 (et est donc dans le groupe alterné). Je m'en sers dans l'exercice 30 du chapitre III, où l'on montre que A_n est l'unique sous-groupe de S_n de cardinal $\frac{n!}{2}$. D'ailleurs, a-t-on le même résultat avec le sous-groupe des carrés de $(\mathbb{Z}/p\mathbb{Z})^\times$?

Dans le cas où -1 n'est pas un carré modulo p, vous en déduisez que pour tout entier a, soit a soit $-a$ est un carré modulo p. Cette considération et d'autres du même tonneau apparaissent dans certains calculs de sommes impliquant des carrés modulo p (comme celles de l'exercice 53).

Exercice 52. (Solutions de $x^2+y^2 \equiv 1 \bmod p$) (🖹) Noter que $\bar{x}^2+\bar{y}^2 = \bar{1}$ se produit si $\bar{1}-\bar{x}^2$ est un carré (et dans ce cas, deux valeurs de $\bar{y}$ conviennent, sauf si $\bar{1}-\bar{x}^2 = \bar{0}^2$), et que la fonction indicatrice des carrés de $(\mathbb{Z}/p\mathbb{Z})^\times$ est $\frac{1}{2}\left(1+\left(\frac{\cdot}{p}\right)\right)$.

Pour simplifier la somme indiquée dans l'énoncé : utiliser le fait que $\left(\frac{\cdot}{p}\right)$ soit un morphisme à valeurs dans $\{\pm 1\}$ pour se ramener au calcul de $\sum_{\bar{x}\in\mathbb{Z}/p\mathbb{Z}\setminus\{\bar{1}\}} \left(\frac{(1-x)^{-1}(1+x)}{p}\right)$. Noter que $\bar{x} \mapsto (\bar{1}-\bar{x})^{-1}(\bar{1}+\bar{x})$ est une bijection (une homographie) de $\mathbb{Z}/p\mathbb{Z}\setminus\{\bar{1}\}$ dans un certain ensemble, afin de se ramener à la somme $\sum_{\bar{x}\in\bigstar}\left(\frac{x}{p}\right)$.

La méthode pour simplifier une somme de la forme $\sum_{g\in G} f(g)$ avec $f : G \to \mathbb{C}^*$ un morphisme de groupes est alors classique (voir exercice 22 du chapitre III). Vous pouvez aussi simplifier cette somme en utilisant votre connaissance du nombre de carrés et non carrés modulo p.

Commentaires. La technique consistant de passer de $1-x^2$ à $(1-x)^{-1}(1+x)$ paraît bien astucieuse. Bien comprendre pourquoi j'ai procédé ainsi. Noter que $x \mapsto \frac{ax+b}{cx+d}$ est *presque* toujours une bijection, peu importe le corps. On appelle une telle application une homographie. Elles sont en retrait dans le programme des classes préparatoires alors qu'elles apparaissent en plusieurs domaines des mathématiques (principalement la géométrie). Voir l'exercice 37 du chapitre III.

Il est *très important* de savoir simplifier une somme de la forme $\sum_{g\in G} f(g)$ avec $f : G \to \mathbb{C}^*$ un morphisme de groupes. Si vous ne savez pas le faire, c'est à revoir impérativement !

Vous avez découvert un certain nombre de fonctions indicatrices écrites sous des formes alternatives, cf. la formule d'orthogonalité des caractères. Il est bon de s'en faire un répertoire et de comprendre pourquoi ces formules sont si utiles. D'ailleurs, est-ce que la fonction indicatrice $\frac{1}{2}\left(1+\left(\frac{\cdot}{p}\right)\right)$ ne proviendrait pas d'une formule d'orthogonalité, pour les caractères d'un groupe bien choisi ?

★ **Exercice 53. (Sommes de Gauß)**

1. Si a est un carré modulo p, noter que $\bar{y} \mapsto \bar{a}\bar{y}$ est une permutation de l'ensemble des carrés. Sinon, montrer que ax^2 n'est jamais un carré modulo p, et que les ensembles $\{\bar{x}^2 \mid \bar{x} \in (\mathbb{Z}/p\mathbb{Z})^\times\}$ et $\{\bar{a}\bar{x}^2 \mid \bar{x} \in (\mathbb{Z}/p\mathbb{Z})^\times\}$ partitionnent $(\mathbb{Z}/p\mathbb{Z})^\times$. L'exercice 51 peut vous inspirer.
2. On doit calculer : $\sum_{\bar{x}\in\mathbb{Z}/p\mathbb{Z}}\sum_{\bar{y}\in\mathbb{Z}/p\mathbb{Z}} \exp\left(\frac{2i\pi a(x^2-y^2)}{p}\right)$. En écrivant : $x^2-y^2 = (x-y)(x+y)$, puis en posant $u = x-y$ et $v = x+y$ (ce qui revient à considérer la bijection $(\bar{x},\bar{y}) \mapsto (\bar{x}-\bar{y},\bar{x}+\bar{y})$), se ramener à des sommes géométriques.
3. Calculer ce carré grâce aux deux questions précédentes, où l'on prend $a = -1$. Ne pas oublier que grâce à l'exercice 50, on sait exprimer autrement $\left(\frac{-1}{p}\right)$.

Commentaires. C'est un exercice de référence de calcul de sommes indexées par un groupe fini, dont des changements d'indice adéquats (compatibles avec la structure de groupe) sont la clé. Outre les bijections banales $x \mapsto xy$ et $x \mapsto x+y$ (selon que le groupe soit multiplicatif ou additif), une connaissance fine des ensembles quotients permet de songer aux bijections entre classes (on s'en sert pour démontrer le théorème de Lagrange), à condition bien entendu que la somme étudiée soit indexée par un sous-groupe ou la translation d'un sous-groupe. C'est le cas ici, puisque la somme est implicitement indexée par les carrés de $\mathbb{Z}/p\mathbb{Z}$.

Le calcul explicite de ces sommes est difficile. On peut démontrer sans trop d'effort, grâce à la dernière question, qu'elle vaut $\pm\sqrt{p}$ ou $\pm i\sqrt{p}$ selon la congruence de p modulo 4, et c'est la détermination du signe qui est un vrai défi. Les démonstrations que le signe est toujours + nécessitent des arguments en dehors de la théorie des groupes.

On utilise ces sommes de Gauß pour la démonstration d'un fameux théorème d'arithmétique (la loi de réciprocité quadratique) et le dénombrement de solutions : voir les exercices 54 et 55.

Exercice 54. (Solutions de $x^2+y^2 \equiv 1 \bmod p$, avec les sommes de Gauß) (🖹)

1. Utiliser la « formule d'orthogonalité » (exercice 12, chapitre II).

2. Immédiat avec l'exercice précédent.

Commentaires. Illustration de l'emploi de la formule d'orthogonalité. C'est en l'employant qu'on comprend la raison d'être des sommes de Gauß. La méthode de cet exercice est très efficace (à condition d'être à l'aise avec le symbole de Legendre dont les principales propriétés sont données par l'exercice 50), comme l'exercice 55 permet de le constater.

Exercice 55. (Zéros d'une forme quadratique sur $\mathbb{Z}/p\mathbb{Z}$)

1. Utiliser la « formule d'orthogonalité » (exercice 12, chapitre II).
2. Utiliser l'exercice 53.
3. Se souvenir que le symbole de Legendre est à valeurs dans $\{\pm 1\}$, et montrer que $\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = 0$ (calcul déjà effectué dans l'exercice 52 par exemple).
4. Noter que $\left(\frac{a}{p}\right)^n = 1$ pour tout a. Simplifier la somme en facteur grâce à l'exercice 53.

Commentaires. Voir le commentaire des exercices 54 et 55.

Exercice 56. (Lemme de Hensel : relèvement des solutions modulo p^k)

1. Utiliser la formule de Taylor.
2. Montrer que $P(a+p^{n-k}z) \equiv P(a) + p^{n-k}zP'(a) \bmod p^{n+1}$. Écrire $P(a) = p^n m$ et $P'(a) = p^k m'$ avec $m, m' \in \mathbb{N}$ premiers avec p. Constater que la congruence ci-dessus donne 0 si et seulement si z, m et m' vérifient une relation de congruence modulo une certaine puissance de p. Comme m et m' sont premiers avec p, ils sont inversibles et cela permet de définir z.

Commentaires. Il est conseillé de traduire ce lemme lorsque $k = 0$, ou $k = 1$ et $n \geqslant 3$. Ces deux cas suffisent souvent en pratique. Noter la ressemblance entre la démonstration proposée et la méthode de Newton : elle sert aussi dans un contexte algébrique ! Elle est même utilisée en réduction matricielle (c'est une façon d'obtenir la décomposition de Dunford d'une matrice).

☢ **Exercice 57. (Contre-exemple au principe de Hasse)**

1. Immédiat.
2. Si $n \notin \{2,17\}$ est premier : montrer que soit 2, soit 17, soit 34 est un carré modulo n. Utiliser l'exercice 51.
3. Utiliser l'exercice précédent avec $P = (X^2-2)(X^2-17)(X^2-34)$. Pour les puissances de 2, raisonner modulo 2 est insuffisant car $P'(x) \equiv 0 \bmod 2$ pour tout x entier : commencer modulo 8.
4. Utiliser le théorème chinois.

Commentaires. Le principe de Hasse, dont la démonstration dépasse très nettement le cadre du programme, dit qu'une équation quadratique ayant des solutions dans $\mathbb{R}$ et modulo n pour tout entier naturel non nul n a aussi des solutions dans $\mathbb{Q}$. Cet exercice montre qu'il devient faux si l'on enlève l'aspect « quadratique ».

Fonctions arithmétiques

Exercice 58. (Nombre de diviseurs, somme des diviseurs)

1. Noter qu'un diviseur de n est de la forme $\prod_{i=1}^{k} p^{\beta_i}$ avec $0 \leqslant \beta_i \leqslant \alpha_i$.
2. Montrer que σ est multiplicative : si a et b sont premiers entre eux, alors $\sigma(ab) = \sigma(a)\sigma(b)$. Cela nécessite d'écrire une bijection entre l'ensemble $\mathrm{Div}(ab)$ des diviseurs positifs de ab, et $\mathrm{Div}(a) \times \mathrm{Div}(b)$ (comment, partant de diviseurs d_1 et d_2 de a et b respectivement, en déduire un diviseur de ab ? Vérifier que le procédé est bijectif). Le résultat est alors immédiat en écrivant $\sigma(n) = \prod_{i=1}^{k} \sigma(p^{\alpha_i})$: il est en effet facile d'expliciter les diviseurs positifs de p^{α_i}, et de les sommer, puisqu'on reconnaît une somme usuelle.

Commentaires. Remarquons que si l'on note $*$ le produit de convolutions de fonctions arithmétiques, alors : $d = 1 * 1$, et : $\sigma = \mathrm{Id} * 1$. Or 1 et Id sont des fonctions multiplicatives : on peut démontrer que cela implique la multiplicativité de d et σ. Si vous savez le démontrer, alors le raisonnement de cet exercice peut être considérablement allégé, pour se ramener aux valeurs de d et σ en les puissances de nombres premiers.

C'est un réflexe à avoir dès qu'on étudie une fonction en arithmétique ! Est-elle multiplicative ? Si oui, cela permet d'avoir sa valeur en tout entier *via* le procédé expliqué ci-dessus (c'est ainsi qu'on a déterminé $\varphi(n)$ pour tout n dans le cours), et plus encore : cela permet d'étudier le produit eulérien de la série de Dirichlet associée : voir l'exercice 36 du chapitre II. Un intérêt est de ramener l'étude de cette série à la fonction dzêta de Riemann, que nous savons raisonnablement bien étudier. Qu'obtenez-vous comme produits eulériens impliquant d et σ ? Et φ ?

★ **Exercice 59. (Fonction de Möbius)** Écrire : $\varphi(n) = \sum_{d|n} \varphi\left(\frac{n}{d}\right) \delta_{d,1}$, et se souvenir que $\delta_{d,1}$ s'exprime en fonction de μ (exercice 39 du chapitre II). Réarranger la somme de sorte à faire apparaître $\sum_{d|n} \varphi(d)$, que l'on sait simplifier.

Commentaires. Dans cet exercice comme dans l'exercice 58, on voit que les sommes indexées par les diviseurs positifs nécessitent souvent l'emploi d'une bijection entre $\mathrm{Div}(ab)$ et $\mathrm{Div}(a) \times \mathrm{Div}(b)$ (cas a et b premiers entre eux : utile en présence de fonctions multiplicatives), ou des variantes.

On l'avait annoncé dans les commentaires de l'exercice 39 du chapitre II : l'identité vérifiée par la fonction μ est parmi les plus importantes de l'arithméticien, dans la mesure où elle permet d'inverser des formules invoquant le produit de convolution. Et il y en a beaucoup, en arithmétique ! La fonction φ en vérifie une, comme on l'a démontré dans l'exercice 12 du chapitre III.

Dans cet exercice, vous allez implicitement démontrer (dans un cas particulier) l'associativité du produit de convolution $*$ de fonctions arithmétiques. En effet, on note que l'on vous demande de montrer : $\varphi = \mu * \mathrm{Id}$. Comme : $\varphi * \bigstar(n) = n$, et : $\bigstar * \mu(n) = \delta_{1,n}$, où $\bigstar$ est une fonction que je vous laisse revoir, combiner toutes ces égalités donne immédiatement le résultat *si l'associativité de $*$ est démontrée* (et si l'on sait que $n \mapsto \delta_{1,n}$ est l'élément unité, mais c'est facile à démontrer).

Exercice 60. (Fonction de von Mangoldt) Noter que la plupart des termes de la somme sont nuls : se restreindre aux diviseurs de la forme p^k avec p divisant n. On sait alors simplifier $\Lambda(d)$. Regrouper les termes égaux, et reconnaître la décomposition en facteurs premiers de n.

Commentaires. L'étude analytique de la répartition des nombres premiers passe par cette fonction-là, qui apparaît dans l'identité suivante : $-\frac{\zeta'(s)}{\zeta(s)} = \sum_{n=1}^{+\infty} \frac{\Lambda(n)}{n^s}$, où ζ est la fonction zêta de Riemann. Vous êtes en mesure de la démontrer grâce aux exercices 37 et 39 du chapitre II, quitte à admettre que ζ' se calcule en dérivant terme à terme (comme une somme à support fini). Elle s'obtient aussi en exprimant $\ln(\zeta(s))$ grâce au produit eulérien de la fonction dzêta, et en dérivant chaque membre (sans se poser trop de question sur la légitimité de la chose).

Comme vous l'avez vu dans le devoir des vacances d'été : l'étude de $\ln \circ \zeta$ renseigne sur la répartition des nombres premiers. C'est donc aussi le cas de $-\frac{\zeta'}{\zeta}$. Par extension, Λ est une fonction incontournable lorsqu'on étudie la répartition des nombres premiers. Pour tout dire : c'est elle, et non $\pi : x \mapsto \mathrm{card}([2, x] \cap \mathbb{P})$, que l'on étudie lorsqu'on veut montrer que $\pi(x) \sim \frac{x}{\ln(x)}$ (théorème des nombres premiers) ! Une démonstration du théorème des nombres premiers par Selberg et Erdős, postérieure à celle d'Hadamard et La Vallée Poussin (mais qui a l'intérêt de s'affranchir des techniques d'analyse complexe), passe par une étude fine de produits de convolutions impliquant Λ. Le point de départ est l'identité de cet exercice.

Exercice 61. (Formule de l'hyperbole de Dirichlet) Réécrire l'indexation de la somme grâce à une bijection entre $\left\{(n, d, d') \in (\mathbb{N}^*)^3 \mid 1 \leqslant n \leqslant x,\ dd' = n\right\}$ et $\left\{(d, d') \in (\mathbb{N}^*)^2 \mid 1 \leqslant d \leqslant x,\ 1 \leqslant d' \leqslant \frac{x}{d}\right\}$. Faire ainsi apparaître $\sum_{1 \leqslant n \leqslant x} F\left(\frac{x}{n}\right) g(n)$. Séparer ensuite la somme selon que $n \leqslant y$ ou $n > y$, et remarquer que l'on a : $\left\{(n, m) \in (\mathbb{N}^*)^2 \mid y < n \leqslant x,\ 1 \leqslant m \leqslant \frac{x}{n}\right\} = \left\{(n, m) \in (\mathbb{N}^*)^2 \mid y < n \leqslant \frac{x}{m},\ 1 \leqslant m \leqslant \frac{x}{y}\right\}$.

Commentaires. Comme souvent avec les sommes indexées par des diviseurs, les sommes se simplifient grâce à des bijections convenables entre ensembles de diviseurs : voir les exercices 58 et 59.

Le membre de gauche de la formule de l'hyperbole s'écrit aussi : $\sum_{1 \leqslant n \leqslant x} (f * g)(n)$, où $*$ est le produit de convolution de fonctions arithmétiques. C'est donc une formule incontournable pour l'étude asymptotique de la moyenne de nombreuses fonctions arithmétiques s'exprimant comme un produit de convolution, telles que les fonctions σ et d définies dans l'exercice 58. Le choix $y = \sqrt{x}$ est souvent pertinent. Son intérêt est de faire disparaître les indexations par des diviseurs, qui sont toujours pénibles à gérer. Voir les exercices 62, 63 et 64. Si l'on n'a pas besoin d'une estimation aussi fine, on peut se contenter de cette formule plus simple à obtenir : $\sum_{1 \leqslant n \leqslant x} (f * g)(n) = \sum_{1 \leqslant n \leqslant x} F\left(\frac{x}{n}\right) g(n)$.

Exercice 62. (🖹) Deux pistes : 1° écrire $\sigma(n) = \sum_{k=1}^{n} k \mathbb{1}_{D(n)}(k)$ où $D(n)$ est l'ensemble des diviseurs de n, et réarranger la somme ainsi réécrite par une interversion de sommes (méthode de double comptage), 2° utiliser l'exercice précédent

avec $\sigma(n) = \sum_{k\ell=n} k = (\mathrm{Id} * 1)(n)$. Il apparaîtra des parties entières : noter que $|\lfloor u \rfloor - u| \leqslant 1$ pour tout u. Ainsi $\sum_{n\leqslant x} \sigma(n)$ s'écrit à l'aide de $\sum_{n\leqslant x} \frac{x^2}{n^2}$ plus des termes négligeables devant x^2. Conclure grâce au résultat admis de l'énoncé.

Commentaires. L'idée derrière, et qu'on peut retrouver en de nombreux exercices qui font intervenir une somme dont le terme général dépend de diviseurs inférieurs à n : écrire ce terme général sous la forme $\sum_{k=1}^{n} \mathbb{1}_{A(n)}(k)$ où $A(n)$ est l'ensemble des diviseurs apparaissant dans la définition du terme général. L'intérêt de procéder ainsi est qu'en intervertissant la double somme, on inverse la relation d'ordre de divisibilité : on ne compte plus des diviseurs (difficile) mais des multiples (très facile). Vous pouvez remplacer $\sigma(n)$ par d'autres fonctions arithmétiques dépendant de diviseurs (il y en a dans cette feuille d'exercices) pour vous convaincre de l'efficacité de l'approche.
En cas de double indexation, s'efforcer de se représenter *concrètement* (en représentant $\mathbb{N}^2$ par un quadrillage d'une partie du plan) les couples d'indices en présence. Cela vous permettra souvent de visualiser les autres façons de sommer.

Exercice 63. Mêmes pistes que dans l'exercice 62. La constante d'Euler apparaît au moment de simplifier une somme de la forme $\sum_{1\leqslant n\leqslant x} \frac{x}{n}$.

Commentaires. Même commentaire que dans l'exercice 62.

Exercice 64. (Comportement asymptotique moyen de l'indicatrice d'Euler)

1. Voir l'exercice 59.
2. S'inspirer du raisonnement de l'exercice 61 (en plus simple), pour montrer : $\sum_{n=1}^{N} \varphi(n) = \sum_{n=1}^{N} \left(\sum_{k\leqslant \frac{n}{x}} k \right) \mu(n)$.
3. Pour faire disparaître les parties entières, noter que $|\lfloor u \rfloor - u| \leqslant 1$ pour tout u. On est ramené à l'étude de $\sum_{k=1}^{N} \frac{\mu(k)}{k}$ et $\sum_{k=1}^{N} \frac{\mu(k)}{k^2}$: on estime la première somme trivialement en la comparant à une somme harmonique (que, elle-même, on estime *via* une comparaison série-intégrale ou par le théorème de sommation des équivalents), et la deuxième somme a été étudiée dans l'exercice 39 du chapitre II.

Commentaires. On jugera encore de l'intérêt de la formule de l'exercice 61 (ou de sa variante plus simple, donnée en commentaire) : faire disparaître les indexations par des diviseurs, qui sont toujours pénibles à gérer. Cela a cependant un coût : faire apparaître la fonction de Möbius, dont le comportement est assez erratique. À cet effet, il vaut mieux avoir en tête l'exercice 39 du chapitre II(on peut aussi calculer les sommes de la forme $\sum_{n=1}^{+\infty} \frac{\mu(n)}{n^s}$ avec un produit eulérien).
Inutile de chercher à améliorer la majoration triviale de $\sum_{k=1}^{N} \frac{\mu(k)}{k}$ par $\sum_{k=1}^{N} \frac{1}{k} \approx \ln(N)$: c'est extrêmement difficile ! De bonnes estimations de cette somme entraînent en effet la justesse d'énoncés très profonds de l'arithmétique (comme le théorème des nombres premiers).
On a vu d'autres produits de convolution dans cette section, par exemple dans l'exercice 60. On pourra vérifier qu'on a compris la méthode en estimant $\sum_{n\leqslant x} \Lambda(n)$ comme on a estimé la somme $\sum_{n\leqslant x} \varphi(n)$.

Exercices généraux sur les polynômes

★ **Exercice 65.** Écrire $x = \frac{p}{q}$ avec p et q premiers entre eux, et ramener l'égalité $P(x) = 0$ à une égalité n'impliquant que des nombres entiers. Regarder les relations de divisibilité obtenues. De l'arithmétique élémentaire permet de montrer que $q = \pm 1$.

Commentaires. Cet exercice montre davantage : une analyse fine nous permet d'avoir une condition de divisibilité sur p, ce qui donne un nombre fini de possibilités pour les valeurs de x. Ainsi, par recensement exhaustif et élimination, on obtient toutes les racines rationnelles d'un polynôme de $\mathbb{Z}[X]$. La méthode s'étend aux polynômes de $\mathbb{Q}[X]$. C'est très commode pour démontrer l'irréductibilité d'un polynôme de $\mathbb{Q}[X]$ de degré raisonnable.

Exercice 66. L'hypothèse revient à dire que P et Q, et $P-1$ et $Q-1$, ont les mêmes racines. En déduire une minoration du nombre de racines de $P - Q = (P-1) - (Q-1)$ qui excède le degré de ce polynôme (il dépend du degré de P ou Q : introduire des notations appropriées). Pour compter le nombre de racines, vous devrez : 1° prendre garde à la possibilité de racines multiples, 2° utiliser le fait que P et $P-1$ soient premiers entre eux (ils n'ont en particulier pas de racine commune), 3° noter que P et $P-1$ ont même dérivée (sachant que c'est la dérivée qui contrôle la multiplicité des racines).

Commentaires. Le résultat reste valable en remplaçant 0 et 1 par deux complexes distincts quelconques.

Exercice 67. Une base intéressante, lorsqu'on connaît les évaluations d'un polynôme en suffisamment de points et qu'on veut le reconstituer, est la base des polynômes interpolateurs de Lagrange.

Un choix est encore plus avisé ici : la base des polynômes de la forme $\frac{1}{n!}\prod_{i=0}^{n-1}(X-i)$. Montrer qu'ils sont à valeurs entières sur $\mathbb{Z}$, et que les coordonnées de P dans cette base le sont aussi.

Commentaires. On se demandera pourquoi le premier choix, pourtant très naturel, n'est pas celui que je recommande : quelle difficulté rencontre-t-on ? J'affirme qu'on peut résoudre cette difficulté... avec les polynômes de la seconde base.
Même si l'interpolation de Lagrange n'est pas le choix privilégié, on ne perdra pas de vue que lorsqu'on veut reconstituer un polynôme à partir de ses évaluations, y penser doit être un RÉFLEXE.
Les polynômes de la seconde base proposée sont incontournables lorsqu'on étudie les polynômes à valeurs entières, quitte à affaiblir les hypothèses de cet exercice. On notera par ailleurs, grâce à ces mêmes polynômes, qu'un polynôme à valeurs entières n'est pas nécessairement à coefficients entiers.

Exercice 68.

1. Quelle base est pertinente à introduire, lorsqu'on veut reconstituer un polynôme à partir de ses évaluations en suffisamment de points ?
2. La question précédente montre déjà qu'un tel polynôme P est dans $\mathbb{Q}[X]$. Noter que les polynômes de degré 1 conviennent. Pour un degré n supérieur ou égal à 2 : d'abord se ramener à $P \in \mathbb{Z}[X]$. Si $r \in \mathbb{Q}$ est tel que : $P(r) = \frac{1}{p}$, avec p premier : effectuer des multiplications convenables pour avoir uniquement des entiers dans cette égalité. En déduire que si $r = \frac{a}{b}$ avec a et b premiers entre eux, alors p divise b. En déduire que p divise $b^n P(r)$, puis que p divise le coefficient dominant de P. Par contraposée, en déduire que tout nombre premier ne divisant pas le coefficient dominant de P n'a pas d'antécédent, et donc que P n'est pas surjective.

Commentaires. La subtilité de la seconde question ne doit pas faire perdre de vue qu'on a déjà effectué des raisonnements semblables : voir l'exercice 65 pour un analogue beaucoup plus simple, ou encore l'exercice 32 où l'on passe de $\mathbb{Q}$ à $\mathbb{Z}$ pour faire de l'arithmétique.

Exercice 69. Si P convient, alors l'ensemble R des racines de P est stable par $x \mapsto x^2$ et $x \mapsto (x-1)^2$. Conclure sur la nature de R en utilisant le fait qu'un polynôme non nul a un nombre fini de racines, puis en déduire P en écrivant sa décomposition en irréductibles dans $\mathbb{C}[X]$ et en vérifiant la réciproque.

Commentaires. La plupart des équations fonctionnelles vérifiées par des polynômes s'étudient d'abord en comparant des choses triviales (coefficient dominant, degré) et, si ce n'est pas instructif, en essayant de fabriquer de nouvelles racines à partir d'une racine donnée (sachant qu'il en existe toujours pour un polynôme non constant dans $\mathbb{C}[X]$). La condition de finitude des racines assure que notre procédé de construction doit finir par « boucler », et c'est ce qui assure qu'on peut finir par se ramener à un nombre fini de possibilités de racines. Le plus dur est alors fait.

Exercice 70.

1. Écrire $P = \sum_{i=0}^{d} a_i X^i$, et calculer $P(n + P(n))$ modulo $P(n)$.
2. L'hypothèse de l'énoncé et la question précédente permettent de montrer que $P(X+P(X))-P(X)$ a une infinité de racines. La contradiction s'obtient en inspectant les degrés.

Commentaires. Comme le comportement des nombres premiers est très difficile à cerner (étant donné un nombre premier p, on ne peut pas prédire, en gros, quand apparaîtra le suivant), même si l'on connut des avancées majeures depuis le XIX$^{\text{e}}$ siècle : certains mathématiciens ont essayé de produire des « suites logiques » constitués uniquement de nombres premiers, afin d'en engendrer facilement. C'est dans ce contexte qu'on put légitimement se demander s'il existait une fonction polynomiale à valeurs dans l'ensemble des nombres premiers (si l'on se restreint aux entiers). Cet exercice montre que ce n'est pas possible. Cependant Euler montra qu'il était possible de proposer un polynôme tel que $P(n)$ soit entier pour tout $0 \leqslant n \leqslant 39$ (et on ne peut pas faire beaucoup mieux). Le polynôme en question est $X^2 + X + 41$.

★ **Exercice 71. (Polynôme cyclotomique)**

1. Noter que l'ensemble des racines de Φ_n est exactement l'ensemble des éléments d'ordre n dans $\mathbb{U}_n$, qui est un groupe cyclique.
2. Raisonnement analogue à celui de l'exercice 34, première question.

3. Raisonner par récurrence forte à l'aide de l'identité de la question précédente. Une étape nécessite l'unicité du quotient dans la division euclidienne.
4. Il s'agit de montrer que si $\bar{a} \in \mathbb{Z}/p\mathbb{Z}$ est racine de $\overline{\Phi_n}$, alors $\bar{a}^n = \bar{1}$ et $\bar{a}^d \neq \bar{1}$ pour tout diviseur strict d de n (et réciproquement). Noter que cela revient à dire que $\bar{a}$ est racine de $X^n - \bar{1}$ sans être racine de $X^d - \bar{1}$: cela incite à utiliser l'identité de la seconde question. Raisonner par récurrence sur n.

   Le miracle est qu'un polynôme défini à l'aide d'éléments d'ordre n dans $\mathbb{C}$ puisse donner les éléments d'ordre n dans $\mathbb{Z}/p\mathbb{Z}$ pour tout p, alors que ces anneaux n'ont *a priori* rien à voir entre eux : ce miracle est permis par l'universalité de l'identité $X^n - 1 = \prod_{d|n} \Phi_d$. Comme elle est à coefficients dans $\mathbb{Z}$, on peut à moindre frais l'injecter dans tout anneau.

Commentaires. Toutes les propriétés des polynômes cyclotomiques découlent de la première question. On remarquera que l'on peut se passer systématiquement de l'expression explicite des racines primitives de l'unité avec la forme exponentielle. Il importe seulement de savoir que l'ensemble des racines n^{es} est un groupe cyclique (ce qui vaut dans n'importe quel corps), et qu'une racine primitive n^{e} z donne toutes les autres en calculant z^k pour tous entiers k premiers avec n. Ainsi les polynômes cyclotomiques sont des objets purement formels, qu'on pourrait manipuler en remplaçant $\mathbb{C}$ par n'importe quel corps.
La beauté de la relation de la première question, et du fait que les polynômes cyclotomiques soient à coefficients entiers, est qu'elle est universelle. Partant de celle-ci, on peut la réduire modulo n'importe quel entier n, et (à quelques précautions près) toutes les relations entre polynômes cyclotomiques restent valables modulo n. D'où le miracle polynomial de la dernière question. N'est-il pas surprenant qu'un objet construit à partir des éléments d'ordre n dans $\mathbb{C}^*$ puisse permettre de calculer les éléments d'ordre n dans des anneaux qui n'ont, *a priori*, aucun rapport avec $\mathbb{C}$? *Un seul objet*, à savoir Φ_n, qui permet d'avoir les éléments d'ordre n de *tous les anneaux* $\mathbb{Z}/p\mathbb{Z}$? C'est cette universalité des propriétés des polynômes à coefficients entiers qui les rend si essentiels aux mathématiques (cette idée est encore exploitée en mathématiques contemporaines).
C'est une idée utilisée pour l'une des démonstrations classiques du théorème de la progression arithmétique de Dirichlet dans un cas particulier : si $n \in \mathbb{N} \setminus \{0\}$, alors il existe une infinité de nombres premiers p tels que : $p \equiv 1 \bmod n$. Dans les grandes lignes, l'idée est de produire un élément d'ordre n dans $(\mathbb{Z}/p\mathbb{Z})^\times$ pour une infinité de nombres premiers p (puisque dans ce cas, par le théorème de Lagrange, n divise $p-1$). Pour ce faire, il suffit de noter que si $a \in \mathbb{Z}$ et si p est un nombre premier divisant $\Phi_n(a)$ (il faut pour cela choisir a de sorte que $\Phi_n(a) \neq \pm 1$, ce qui est possible puisque Φ_n tend vers l'infini en l'infini), alors $\overline{\Phi_n(a)} = \bar{0}$ dans $\mathbb{Z}/p\mathbb{Z}$, donc a est d'ordre n dans $(\mathbb{Z}/p\mathbb{Z})^\times$ comme toutes les racines de $\overline{\Phi_n}$ (à une subtilité près dont je ne parle pas), et donc $n \equiv 1 \bmod p$. Si l'on choisit convenablement a, on s'assure que procédé de construction permet de fabriquer une suite strictement croissante de nombres premiers p vérifiant cette congruence.
Les polynômes cyclotomiques apparaissent dans bien d'autres considérations encore. Il serait vain d'en faire l'inventaire. Un dernier exemple d'utilisation : comme Φ_n est de degré $\varphi(n)$ (facile à démontrer, si l'on a compris ce qu'est μ_n), et que c'est le polynôme minimal de $e^{\frac{2i\pi}{n}}$ (c'est en effet une racine primitive de l'unité), on sait donner une condition nécessaire et suffisante simple sur n pour que $e^{\frac{2i\pi}{n}}$ soit solution d'une équation polynomiale à coefficients rationnels et de degré au plus 4 (cela revient à résoudre $\varphi(n) = k$ pour tout $k \in [\![1,4]\!]$: voir l'exercice 28), et par extension on sait en déduire une condition nécessaire et suffisante simple sur n pour que $\cos\left(\frac{2\pi}{n}\right)$ soit solution d'une équation polynomiale de degré au plus 2. Cela tombe bien, puisque vous savez résoudre une telle équation. On retrouve alors que, hormis les angles remarquables que vous connaissez depuis longtemps, on sait aussi calculer, uniquement à l'aide d'une racine carrée, et de sommes, produits et quotients de rationnels : $\cos\left(\frac{2k\pi}{5}\right)$, et il n'y en a pas d'autres (si l'on s'autorise plusieurs racines carrées, ou des racines cubiques, etc., il suffit de changer la condition recherchée sur $\varphi(n) = \deg(\Phi_n)$).
En résumé : dès qu'il est question de polynômes irréductibles dans $\mathbb{Q}[X]$, il y a une probabilité non négligeable de croiser des polynômes cyclotomiques.

Arithmétique dans $K[X]$, nombres algébriques, polynômes irréductibles

★ **Exercice 72. (L'anneau $A[X]$ n'est pas principal en général)** Raisonner par l'absurde. Noter que si $aA[X] + XA[X] = D \cdot A[X]$, alors D divise a et X. Utiliser ces deux relations de divisibilité pour en déduire $D = 1$. Conclure à une absurdité en évaluant une relation entre a, X et D en un élément bien choisi de A.

Commentaires. Noter qu'on n'est pas obligé de raisonner par l'absurde : en adaptant le raisonnement proposé, on peut plutôt en déduire que a est inversible pour tout $a \neq 0$.
Cet exercice donne un exemple d'anneau où deux éléments peuvent avoir un pgcd (un plus grand commun diviseur modulo $A^\times$) sans pour autant qu'ils engendrent un idéal principal. Une des subtilités des anneaux non principaux...
Ainsi il est facile de produire des exemples d'anneaux intègres non principaux : $\mathbb{Z}[X]$ par exemple. Cependant il reste vrai dans $\mathbb{Z}[X]$ que tout polynôme non nul s'écrit comme produit de facteurs irréductibles, même si la démonstration doit être adaptée. Si on veut un anneau intègre dans lequel cette propriété est fausse : regarder l'exercice 49.

Exercice 73. Par le théorème de D'Alembert-Gauß, P est scindé sur $\mathbb{C}$. Exprimer $\text{pgcd}(P', P)$ en fonction des facteurs irréductibles de P, et regarder à quelle condition on a : $\text{pgcd}(P', P) = P'$. Les seuls polynômes à convenir sont ceux que vous avez probablement trouvés par des essais à tâtons.

Commentaires. On note qu'une relation du type $P = P'Q$ est une équation différentielle linéaire du premier ordre : pourquoi ne pas exploiter cette idée ?
L'arithmétique des polynômes ressemble à celle des entiers lorsqu'on raisonne sur une décomposition en facteurs irréductibles. On remarquera cependant que des considérations sur le degré sont plus faciles à faire que les considérations sur la taille des entiers. Cela intervient souvent quand on étudie la décomposition d'un polynôme à expliciter, ou lorsqu'on veut montrer son irréductibilité.

★ **Exercice 74.** Trouver le pgcd en utilisant l'algorithme d'Euclide étendu. Remarquer que la division euclidienne de $X^m - 1$ par $X^n - 1$ est faisable explicitement, et que l'algorithme d'Euclide étendu suit les mêmes étapes que si on l'appliquait aux entiers m et n. On trouve comme pgcd : $X^{\mathrm{pgcd}(m,n)} - 1$.

Commentaires. Voir les commentaires de l'exercice 2, où il apparaît un raisonnement analogue.

Exercice 75. S'inspirer de la technique employée pour résoudre un système de congruence avec des entiers *via* une relation de Bézout. En effet, ce qui est demandé revient à trouver P tel que : $P \equiv 1 \bmod (X-1)^3$, et : $P \equiv -1 \bmod (X+1)^3$.

Commentaires. Les anneaux $K[X]/QK[X]$ et $\mathbb{Z}/n\mathbb{Z}$ (avec Q polynôme) ont de très nombreux points communs (et c'est normal : ce sont tous les deux des anneaux quotients issus d'anneaux principaux). Je vous encourage à les remarquer dans l'aide à la révision du cours du chapitre IV. Cela vous permettra de prendre par le bon bout des énoncés *en apparence* originaux. En utilisant le théorème d'isomorphisme avec un morphisme d'évaluation, vous pourrez même vous inspirer de raisonnements dans $\mathbb{Z}/n\mathbb{Z}$ pour résoudre des exercices dans $K[z]$ (cet anneau est introduit dans l'exercice 83).

Exercice 76. Factoriser $A^{2m} - 1$ et en déduire que A et $A+1$ divisent $A^{2m} + (A+1)^n - 1$. Conclure en montrant que A et $A+1$ sont premiers entre eux.

Commentaires. Si l'on avait remplacé A par un entier, on aurait pu traiter cette question avec de l'arithmétique modulaire et le théorème chinois. On remarquera que l'indication ci-dessus revient implicitement à en faire autant dans un contexte polynomial. On se garde simplement de raisonner dans $K[X]/(A)$ puisque le programme ne contient aucun résultat sur ces anneaux quotients (pourtant très proches de $\mathbb{Z}/n\mathbb{Z}$ comme vous l'avez constaté en suivant de près l'aide à la révision du cours).

Exercice 77. Raisonner par l'absurde. Si P est le polynôme de l'énoncé, et si $P = QR$ avec Q et R dans $\mathbb{Z}[X]$ de degré strictement inférieur à celui de P, alors noter montrer $Q(a_i) = \pm 1$ et $R(a_i) = \mp 1$. Conclure que $Q = -R$ par un argument sur les racines. En déduire une absurdité.

Commentaires. Il est rare d'étudier des polynômes irréductibles de degré strictement plus grand que 3 en classes préparatoires, parce qu'on manque de théorèmes (pour le degré 4 ou 5, on peut parfois s'en sortir à tâtons très péniblement, parce qu'un polynôme réductible de tel degré admet un facteur de degré 2 ou 3 dont on sait caractériser l'irréductibilité).
Lorsqu'on vous demande d'y parvenir, en particulier avec un degré n quelconque, il s'agit souvent d'un polynôme à coefficients entiers. Cette condition met en effet des contraintes arithmétiques fortes sur une décomposition en facteurs non triviaux, dont on espère qu'elle débouche sur une absurdité. Outre le raisonnement de cet exercice, cela donne notamment le très efficace critère d'Eisenstein de l'exercice 81.

Exercice 78.

1. Deux pistes : 1° commencer par décomposer P dans $\mathbb{C}[X]$ en calculant ses racines (on sait résoudre $z^4 = -1$ pour $z \in \mathbb{C}$), et en déduire la décomposition dans $\mathbb{R}[X]$ en regroupant les racines conjuguées ; 2° ajouter et soustraire un polynôme convenable pour factoriser directement P dans $\mathbb{R}[X]$ grâce à une identité remarquable.
2. Montrer que P n'a pas de racine rationnelle, puis que, s'il avait un facteur irréductible de degré 2 dans $\mathbb{Q}[X]$, il serait égal à l'un des facteurs trouvés dans $\mathbb{R}[X]$, ce qui est impossible car ses coefficients ne sont pas tous rationnels.
3. ☢ Montrer qu'au moins un entier parmi -1, 2 et -2 est un carré modulo p. S'inspirer alors de la décomposition dans $\mathbb{R}[X]$ pour trouver une décomposition dans $\mathbb{Z}/p\mathbb{Z}[X]$. Pour montrer que l'un de ces trois nombres est un carré modulo p : utiliser les résultats des exercices 50 et 51.

Commentaires. La deuxième question pose la difficile question de l'irréductibilité dans $\mathbb{Q}[X]$ lorsque le polynôme étudié est de degré strictement supérieur à 3 : une simple étude des racines ne suffit plus. L'approche à la main que l'on propose est à peu près la seule à votre disposition (raisonnement par l'absurde, recensement exhaustif des possibilités de facteurs irréductibles selon leur degré, comparaison avec la décomposition dans $\mathbb{R}[X]$).

★ **Exercice 79.** Cela revient à montrer que P et P' n'ont pas de racine commune. D'abord montrer qu'ils sont premiers

entre eux grâce à l'irréductibilité de P : si D divise P' et P, montrer que le cas $D = P$ entraîne une bizarrerie. Conclure en écrivant une relation de Bézout entre P et P', puis en l'évaluant en une racine de P.

Autre piste : noter que si z est racine de P, alors P est le polynôme minimal de z sur $\mathbb{Q}$. Conclure qu'en cas de racine double, P divise P' ce qui est impossible.

Commentaires. La seconde piste illustre bien comme il est plus instructif de caractérisation l'annulation en z avec le polynôme minimal plutôt qu'avec la divisibilité par $X - z$.
Cet exercice implique en particulier que le polynôme minimal sur $\mathbb{Q}$ d'un nombre complexe admet toujours autant de racines (dans $\mathbb{C}$) que son degré. C'est utilisé dans les exercices 80 et 85 (pour dénombrer des morphismes de corps).

Exercice 80. Si π est le polynôme minimal de P sur $\mathbb{Q}$, alors π divise P et λ est racine simple de π par l'exercice 79. En déduire que, si d est l'ordre de multiplicité de λ comme racine de P, alors π^d divise P. Conclure à une absurdité, si $\lambda \notin \mathbb{Q}$, en comparant les degrés de π^d et P.

Commentaires. Cet exercice illustre bien comme il est plus instructif de caractérisation l'annulation en z avec le polynôme minimal plutôt qu'avec la divisibilité par $X - z$.

★ **Exercice 81. (Lemme de Gauß et critère d'irréductibilité d'Eisenstein)**

1. On a $\overline{P} \cdot \overline{Q} = \bar{0}$ dans $\mathbb{Z}/p\mathbb{Z}[X]$. Utiliser l'intégrité de cet anneau pour conclure.
2. Se ramener au cas où $c(P) = c(Q) = 1$. Montrer que $c(PQ) = 1$ en raisonnant par l'absurde et en utilisant la question précédente.
3. Si $P = QR$ avec $Q, R \in \mathbb{Q}[X]$, se ramener à des polynômes à coefficients entiers après multiplication par un entier convenable qui élimine tous les dénominateurs. En utilisant la question précédente, se ramener à une égalité du type $P = Q_0 R_0$ avec Q_0 et R_0 dans $\mathbb{Z}[X]$, pour utiliser l'irréductibilité de P dans $\mathbb{Z}[X]$.
4. D'après la question précédente, il suffit de montrer l'irréductibilité dans $\mathbb{Z}[X]$. Si $P = QR$ avec $Q, R \in \mathbb{Z}[X]$ non constants, réduire modulo p cette égalité, et utiliser l'hypothèse de l'énoncé pour simplifier. Obtenir une expression très simple de $\overline{Q}$ et $\overline{R}$ par unicité de la décomposition en facteurs irréductibles dans $\mathbb{Z}/p\mathbb{Z}[X]$ (pourquoi est-ce unique ?). Regarder ce que cela implique sur les coefficients constants de Q et R, puis sur celui de P ; conclure à une absurdité.

Commentaires. On utilise l'anneau $\mathbb{Z}/p\mathbb{Z}[X]$ dans cet exercice : on comprend ici pourquoi on ne pouvait pas se borner à faire de l'arithmétique dans $\mathbb{R}[X]$ ou $\mathbb{C}[X]$ comme en 1re année. On se privait de raisonner modulo p avec des polynômes.
Ce critère est *très* efficace pour l'irréductibilité des polynômes de haut degré ! On l'applique dans l'exercice 82.
Pour comprendre l'intérêt du lemme très fastidieux des questions 2 et 3 : réfléchir aux relations entre l'irréductibilité dans $\mathbb{Z}[X]$ et $\mathbb{Q}[X]$: quelle propriété est la plus forte ? Comment passer de l'une à l'autre ? Remarquer que la réponse n'est pas si simple.
Pour pressentir l'intérêt de s'intéresser au *contenu* d'un polynôme (c'est le nom donné au pgcd de ses coefficients) : notons que si tous les coefficients d'un polynôme admettent un diviseur commun non trivial d, alors $P = d \cdot Q$ et il n'est pas irréductible dans $\mathbb{Z}[X]$... Mais on sent bien que c'est une factorisation artificielle (qui d'ailleurs n'implique pas la réductibilité dans $\mathbb{Q}[X]$ puisque d y est inversible) et dont on ne veut pas tenir compte. Diviser P par $c(P)$, comme on le fait dans cet exercice, évite ce genre de factorisation.

Exercice 82. (Applications du critère d'Eisenstein)

1. Construire un polynôme dans $\mathbb{Z}[X]$, de degré n, tel que 2 divise tous ses coefficients sauf le coefficient dominant, et tel que 2^2 ne divise pas le coefficient constant. Il y a l'embarras du choix.
2. Appliquer le critère d'Eisenstein à $\Phi_p(X + 1)$.

Commentaires. Illustration de l'efficacité du critère d'Eisenstein. La deuxième question peut paraître astucieuse. Cela permet d'avoir l'irréductibilité des polynômes cyclotomiques au moins dans le cas particulier d'un indice premier (cela peut être demandé : voir l'épreuve de six heures de l'ENS de Paris en 2019), à moindre frais. La démonstration pour un entier quelconque est particulièrement difficile.

★ **Exercice 83. (Un exercice ULTRA important)**

1. Cas non algébrique : considérer l'application linéaire naturelle $\mathbb{Q}[X] \to \mathbb{Q}[z]$. Cas algébrique : trouver une base « canonique » explicite de $\mathbb{Q}[z]$.
2. Cas non algébrique : considérer le morphisme d'anneaux naturel $\mathbb{Q}[X] \to \mathbb{Q}[z]$. Cas algébrique : si $\omega \in \mathbb{Q}[z]$ est non nul et s'écrit $\omega = P(z)$, montrer que π_z et P sont premiers entre eux, et écrire une relation de Bézout entre ces deux polynômes. Conclure que ω est inversible dans $\mathbb{Q}[z]$ par une évaluation convenable.
   Avec les anneaux quotients (hors programme) : utiliser le théorème d'isomorphisme pour avoir un isomorphisme entre $\mathbb{Q}[z]$ et $\mathbb{Q}[X]/(\pi_z)$. Imiter la démonstration que $\mathbb{Z}/p\mathbb{Z}$ est un corps si et seulement si p est premier, pour montrer que $\mathbb{Q}[X]/(\pi_z)$ est un corps.

Commentaires. Cet exercice est un lemme préparatoire à toute étude des solutions des équations polynomiales rationnelles (qu'on appelle *nombres algébriques*). Il permet de démontrer qu'un nombre algébrique par un argument indirect ne nécessitant pas d'expliciter un polynôme annulateur non nul. On jugera de l'efficacité de l'approche dans l'exercice 84, où l'on montre que la somme et le produit de deux nombres algébriques est encore algébrique : y parvenir par construction de polynômes annulateurs explicites vous mettrait bien en difficulté, même si c'est possible. La théorie de la dimension est très puissante.

Le fait que $\mathbb{Q}[z]$ soit un corps généralise ce que vous saviez déjà pour les nombres complexes : $\frac{a+ib}{c+id}$ peut être mis sous la forme algébrique $\alpha + i\beta \in \mathbb{Q}[i]$. De même, vous savez mettre $\frac{a+b\sqrt{n}}{c+d\sqrt{n}}$ sous la forme $\alpha + \beta\sqrt{n}$ en « multipliant par le conjugué ». En fait, ce n'est pas une propriété propre aux racines carrées mais aux nombres algébriques : l'inverse d'un élément de $\mathbb{Q}[z]$ est un élément de $\mathbb{Q}[z]$. Selon votre façon de procéder, vous avez même trouvé un moyen explicite d'écrire un inverse dans $\mathbb{Q}[z]$, et qui n'est pas sans rappeler la méthode dans $\mathbb{Z}/n\mathbb{Z}$ (aucune surprise là derrière : les anneaux $\mathbb{Q}[z]$ et $\mathbb{Q}[X]/(\pi_z)$ sont isomorphes, et ce dernier anneau partage de nombreuses propriétés avec $\mathbb{Z}/n\mathbb{Z}$ du fait d'être des quotients d'anneaux principaux).

★ **Exercice 84. (Théorème de la base télescopique et application)**

1. Pour trouver une famille génératrice : écrire $x \in M$ en fonction d'une L-base de M, puis écrire les scalaires de la relation, qui sont dans L, dans une K-base de L. Vous avez ainsi obtenu une famille génératrice de M sur K. Montrer qu'elle est libre en écrivant une relation de dépendance linéaire sur K : en regroupant convenablement les termes, vous aurez une relation de dépendance linéaire vérifiée par la L-base de M introduite ci-avant, ce qui vous permettra de conclure à la nullité des scalaires. Conclure est facile à partir de là.
2. Montrer que si α et β sont algébriques sur $\mathbb{Q}$, alors $\mathbb{Q}[\alpha+\beta]$ et $\mathbb{Q}[\alpha\beta]$ sont inclus dans un espace vectoriel de dimension finie (c'est là qu'intervient la question précédente).

Commentaires. La première question donne des relations surprenantes de divisibilité entre dimensions, qui n'est pas sans rappeler les contraintes de divisibilité impliquées par le théorème de Lagrange : $\mathrm{card}(G) = \mathrm{card}(H)\mathrm{card}(G/H)$. Ce parallèle peut paraître boiteux, mais c'est loin d'être le cas (le théorème de correspondance de Galois l'éclaire). Ce théorème de la base télescopique est utilisé tout autant que le théorème de Lagrange lorsqu'on étudie la théorie des corps.

On en déduit à moindre frais, par exemple, que si p est un entier non carré, $\sqrt{p}$ n'est pas une combinaison linéaire de racines cubiques d'un entier donné (appliquer l'exercice aux corps $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{p}] \subseteq \mathbb{Q}[\sqrt[3]{q}]$). Apprécier la puissance de la théorie de la dimension.

Pour juger de l'efficacité de la méthode de la seconde question : étant donné deux nombres algébriques α et β, même très simples, arriveriez-vous à fabriquer un polynôme annulateur non nul de $\mathbb{Q}[X]$ pour $\alpha+\beta$ et $\alpha\beta$? Prendre par exemple $\alpha = \sqrt{2}$ et $\beta = \sqrt[3]{3}$. Noter que le théorème de cet exercice nous permet de conjecturer le degré de polynômes qui conviendraient.

Exercice 85. (Théorie de Galois pour bébés)

1. Utiliser l'exercice 79.
2. Écrire : $\pi_{\mathbb{Q}}(\alpha) = 0$, et prendre l'image par f de cette égalité. Vous aurez besoin de montrer qu'un automorphisme de corps de L fixe les rationnels. Un morphisme injectif de $\mathrm{Aut}(L)$ dans S_R est donné par $f \mapsto f_{|R}$. Comme R est de cardinal n, on conclut.
3. Il faut montrer que $f_x(z)$ ne dépend pas du choix du polynôme P tel que $z = P(\alpha)$. Pour cela : si $z = P(\alpha) = Q(\alpha)$, montrer que $\pi_{\mathbb{Q}}$ divise $P-Q$ et en déduire : $P(z) = Q(z)$. Cette vérification étant faite, c'est une opération de routine de montrer que c'est un morphisme de corps.
4. Constater qu'un morphisme de $\mathbb{Q}[\alpha]$ dans $\mathbb{C}$ est entièrement caractérisé par l'image de α. Utiliser la deuxième question pour conclure.
5. Montrer qu'un automorphisme de $\mathbb{Q}[\sqrt{2}]$ est caractérisé par l'image de $\sqrt{2}$. Utiliser la deuxième question pour constater que seuls deux choix sont possibles.

Commentaires. Avec cet exercice, vous ne serez plus pris au dépourvu au moment de déterminer les morphismes de corps d'une extension de $\mathbb{Q}$. Comme dans l'exercice 53 du chapitre III : une fois qu'on a compris qu'un morphisme de corps fixe le sous-corps premier, on étend progressivement son explicitation du sous-corps premier au corps entier par adjonction d'éléments (pour passer de $\mathbb{R}$ à $\mathbb{C}$, on doit « ajouter i »), et en considérant l'image de ces éléments par ce morphisme. C'est en général possible sans trop d'effort si le corps est un espace vectoriel de dimension FINIE (en tant qu'espace vectoriel sur le sous-corps). C'est ainsi que de la même manière, vous pourriez obtenir tous les automorphismes de corps de $\mathbb{Q}(\sqrt{d})$ avec d qui n'est pas un carré de rationnel, ou $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}\left(e^{\frac{2i\pi}{n}}\right)$, etc. Pour déterminer $f(i)$ dans cet exercice, ou $f(\sqrt{d})$, ou $f(\sqrt[3]{2})$, etc., on imite le raisonnement de l'exercice 52, puisque c'est à chaque fois la même idée : utiliser une équation vérifiée par α pour en déduire une équation vérifiée par $f(\alpha)$, ce qui limite le nombre de possibilités.
Remarquer que dans la troisième question, il est plus malin de travailler avec un élément de $\mathbb{Q}[\alpha]$ sous la forme $P(\alpha)$ avec $P \in \mathbb{Q}[X]$ de degré quelconque, bien que le raisonnement de l'exercice 83 assure qu'on puisse se borner à P de degré $\deg(\pi_{\mathbb{Q}}) - 1$. C'est potentiellement contre-intuitif. Comprendre pourquoi on procède ainsi en peinant, voire en échouant, sur des exemples concrets : si l'on prend $\alpha = \sqrt[3]{2}$, vérifier que $f : a + b\sqrt[3]{2} + c\sqrt[3]{2}^2 \mapsto a + bj\sqrt[3]{2} + cj^2\sqrt[3]{2}^2$ est un morphisme de corps de $\mathbb{Q}[\sqrt[3]{2}]$ dans $\mathbb{C}$ sans passer par la méthode de l'exercice. C'est pire encore avec les morphismes de corps de $\mathbb{Q}\left[\exp\left(\frac{2i\pi}{n}\right)\right]$ dans $\mathbb{C}$ par exemple.
Les automorphismes d'un corps L fixant un sous-corps K forment le *groupe de Galois* de l'extension (L, K) (du moins, on utilise cette terminologie lorsque (L, K) est *galoisienne*, ce que je ne définirai mais qui consiste essentiellement à dire qu'il ne « manque pas d'automorphismes de L fixant K » par rapport à ce qu'on pourrait théoriquement espérer : les questions 1 et 4 donnent une idée de ce que j'entends par là), et le théorème de correspondance de Galois formule, de manière plus explicite et plus impressionnante, qu'en connaissant ce groupe et tous ses sous-groupes, on connaît aussi tous les sous-corps contenant K et contenus dans L ; on les obtient tous en considérant les corps de la forme $\{x \in L \mid \forall \sigma \in G,\ \sigma(x) = x\}$ avec G un sous-groupe du groupe de Galois. Autrement dit : ce sont les points fixes des automorphismes de L fixant K qui permettent de décrire tous les sous-corps. Au fond, on le sait déjà dans certains cas particuliers : par exemple, le groupe de Galois de $\mathbb{C}/\mathbb{R}$ est $G = \{\mathrm{Id}_{\mathbb{C}}, \sigma\}$, où $\sigma : z \mapsto \bar{z}$ est la conjugaison complexe. Ici, G n'a que deux sous-groupes : le sous-groupe réduit à l'élément neutre et lui-même. En considérant les points fixes dans $\mathbb{C}$ du sous-groupe $\{\mathrm{Id}_{\mathbb{C}}\}$, on obtient trivialement $\mathbb{C}$. En considérant les points fixes de G (ce qui revient à prendre les points fixes de la conjugaison complexe), on obtient $\mathbb{R}$. On obtient ainsi deux corps, et il n'y en a pas d'autre par un argument dimensionnel : si $\mathbb{R} \subseteq K \subseteq \mathbb{C}$, alors K est de dimension 1 ou 2 sur $\mathbb{R}$, donc par un argument dimensionnel il est égal à $\mathbb{R}$ ou $\mathbb{C}$. On a illustré la correspondance de Galois dans ce cas particulier (même si cette correspondance donne beaucoup plus de liens entre les sous-groupes du groupe de Galois et les corps intermédiaires entre K et L).

Polynômes de $K[X]$ avec K un corps fini

★ **Exercice 86.** Trouver un polynôme non constant qui vaut 1 en tout élément de K. Si vous n'avez pas d'idée : comment caractériser, en termes de divisibilité, le fait que $P(x) = 1$, si P est un tel polynôme et $x \in K$?

Commentaires. Ainsi un corps fini n'est jamais algébriquement clos. On démontre en passant que $P \mapsto \tilde{P}$, où $\tilde{P}$ est l'application polynomiale associée à P, n'est pas injective : voir l'exercice 88 pour une étude plus approfondie de cette application.

Exercice 87. Dans les deux cas : l'étude des polynômes de degré 1 est triviale. Pour celle des polynômes de degré 2 : il y en a 2^2 et 3^2, respectivement, à énumérer. Parmi ceux-ci, chercher ceux qui n'ont pas de racine. De même pour le degré 3. Pour le degré 4 : d'abord faire en sorte qu'ils n'ont pas de racine. Ensuite : les polynômes irréductibles de degré 2 ayant été explicités, vous pouvez en déduire la forme des polynômes de degré 4 qui se décomposent en produit de deux polynômes irréductibles de degré 2. Conclure en prenant le complémentaire.

Commentaires. Rien de bien original : on y fait au fond la même chose que sur $\mathbb{R}$ ou $\mathbb{C}$, avec cependant la différence que la recherche de racines est plus facile : on peut procéder par recensement exhaustif.
Vous avez peut-être eu l'occasion d'utiliser le résultat de l'exercice 89 pour vous simplifier la vie et avoir des réductibilités en un coup d'œil !

★ **Exercice 88.** Pour le noyau (dont on sait qu'il est un idéal engendré par un polynôme : il s'agit de le déterminer) : comment traduire $P(x) = 0$, pour tout $x \in K$, en termes de divisibilité ? Pour l'image : soit vous montrez que c'est surjectif en obtenant le cardinal de l'image grâce au théorème d'isomorphisme (attention, $\mathbb{Z}/p\mathbb{Z}[X]$ n'est pas fini, vous ne pouvez pas utiliser la formule $\mathrm{card}(G) = \mathrm{card}(\ker(f))\mathrm{card}(\mathrm{im}(f))$), soit vous écrivez explicitement une application quelconque f de $\mathbb{Z}/p\mathbb{Z}$ dans lui-même comme étant égale à une application polynomiale. Pour ce faire : vous avez un outil pour fabriquer un polynôme prenant exactement les valeurs $f(x)$ en tous les $x \in K$.

Commentaires. L'idéal est engendré par un polynôme non irréductible, au contraire de l'idéal engendré par le polynôme minimal d'un nombre algébrique (cf. le cours). Est-ce que vous pouvez l'expliquer ?
Cet exemple donne la différence majeure entre l'étude des polynômes sur un corps contenant $\mathbb{Q}$ et ceux sur un corps contenant $\mathbb{Z}/p\mathbb{Z}$. L'autre différence majeure concerne les polynômes de dérivée nulle (exercice 90). En revanche, quasiment tout le reste de la théorie des polynômes est valable quel que soit le corps. Plus généralement, si vous avez un doute sur ce qui se généralise à un corps quelconque : dites-vous que tout résultat dans $K[X]$ se démontrant par l'algèbre linéaire, et par des calculs n'impliquant aucune division par p, restent valables quel que soit le corps (seule exception à ce principe : l'exercice qu'on vient de traiter). Pour des exemples concrets pouvant nécessiter une division par p, il y a : la résolution des équations polynomiales de degré 2 (division par 2 pour la mise sous forme canonique), le calcul de primitive (division par $k+1$ si l'on intègre X^k, ce qui explique la bizarrerie de l'exercice 90) et la formule de Taylor (division par $k!$, ce qui explique la bizarrerie de l'exercice 92).

★ **Exercice 89.** Utiliser la formule du binôme de Newton, et montrer que les coefficients binomiaux $\binom{p}{k}$ sont nuls modulo p (voir l'exercice 7 si besoin). Simplifier l'exponentiation des coefficients de P grâce au petit théorème de Fermat.

Commentaires. On a déjà croisé ce résultat dans l'exercice 7. C'était un cas particulier. Il a deux applications sympathiques : 1° il permet de montrer en un clin d'œil que des polynômes sont réductibles (par exemple : $X^4+X^2+1=(X^2+X+1)^2$ dans $\mathbb{Z}/2\mathbb{Z}[X]$, ou $\sum_{k=0}^{p-1} X^k = \frac{X^p-1}{X-1} = (X-1)^{p-1}$ dans $\mathbb{Z}/p\mathbb{Z}[X]$), 2° il montre que si x est une racine de P, alors x^p également (ce qui est sans intérêt si $x \in \mathbb{Z}/p\mathbb{Z}$ car $x^p = x$, mais c'est autrement plus utile dans un corps contenant strictement $\mathbb{Z}/p\mathbb{Z}$), et en réitérant x^{p^2}, etc., sont aussi racines. Si P est irréductible dans $\mathbb{Z}/p\mathbb{Z}[X]$, on obtient ainsi toutes les racines !
C'est ce qui est utilisé dans les démonstrations (difficiles) que les polynômes cyclotomiques, définis dans l'exercice 71, sont irréductibles dans $\mathbb{Q}[X]$.

Exercice 90.

1. Écrire $P = \sum_i a_i X^i$, et regarder à quelle condition on peut avoir $P' = 0$.
2. Immédiat grâce à la question précédente et la linéarité de la dérivation.

Commentaires. Voir le commentaire de l'exercice 88 pour l'origine des bizarreries dans les corps finis. Le résultat de cet exercice doit notamment vous rendre critiques lorsque j'écris des arguments tels que : « P divise P', ce qui est impossible pour des raisons de degré ». Ceci est tout à fait possible si P' est nul, et on veut que cela peut arriver même si P n'est pas constant.
On doit aussi être plus prudent lorsqu'on affirme qu'un polynôme est à racines simples. Par exemple $X^p - 1$ admet des racines multiples dans $\mathbb{Z}/p\mathbb{Z}$ puisque sa dérivée est nulle (faire le lien avec les exercices 89 et 92).

Exercice 91.

1. Montrer que X^4+X+1 n'a pas de racine dans $\mathbb{Z}/2\mathbb{Z}$. S'il est réductible, il est donc produit de deux polynômes irréductibles de degré 2. Comme il n'y a qu'un seul polynôme irréductible de degré 2 dans $\mathbb{Z}/2\mathbb{Z}[X]$ (vous pouvez le trouver par recensement exhaustif des polynômes de degré 2, en testant à chaque fois s'ils ont une racine), il suffit de vérifier si X^4+X+1 est différent de ce polynôme au carré pour en déduire s'il est irréductible. Vous pouvez accélérer le calcul de ce carré avec le résultat de l'exercice 89.
2. Montrer que ses facteurs irréductibles doivent être de degré 2 et 3. Il n'y en a qu'un seul de degré 2. Obtenir le dernier facteur par une division euclidienne.

Commentaires. Rien de très original par rapport aux raisonnements dans $\mathbb{R}$ ou $\mathbb{C}$, à ceci près que la recherche de racines peut se faire par une étude exhaustive.

Exercice 92.

1. S'inspirer de la démonstration valable dans $\mathbb{R}[X]$ ou $\mathbb{C}[X]$.
2. Écrire $P = (X-\alpha)^m Q$ et dériver avec la formule de dérivation de Leibniz.

Commentaires. Voir le commentaire de l'exercice 88 pour l'origine des bizarreries dans les corps finis. Une étude plus approfondie permet de voir que pour des polynômes P bien choisis, la réciproque de la deuxième question reste vraie.

Exercice 93.

1. Comme P est irréductible, le pgcd de P' et P, qui doit diviser P, ne peut prendre que deux valeurs différentes. Montrer que l'une de ces deux valeurs implique une relation de divisibilité impossible pour des raisons de degré, à moins d'avoir $P' = 0$.
2. Faire le lien avec les exercices 89 et 90.

Commentaires. Cet exercice est à comparer avec l'exercice 79, qui démontre la même chose avec un polynôme de $\mathbb{Q}[X]$. Pourquoi le raisonnement est-il si différent ici, malgré une conclusion semblable ? Voir aussi mon commentaire de l'exercice 90.

Classement des exercices par thèmes