Du cours aux exercices
Chapitre IV — Arithmétique des entiers et des polynômes

1 Aide à la révision du cours

1.1 Autre point de vue sur l'arithmétique

1.1.1 Compléments sur les anneaux, algèbres

Motivation de cette partie

On étudiera plus loin, de plus près, les propriétés de $\mathbb{Z}/n\mathbb{Z}$ comme anneau, et pour parler de systèmes de congruences (trouver x tel que $x \equiv a \bmod m$ et $x \equiv b \bmod n$) nous avons besoin de mettre une structure d'anneau sur $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Les compléments de cette section sont à cette fin. La structure d'algèbre sera pour étudier les propriétés à la fois arithmétiques et algébriques de $K[X]$.

Proposition 1 (Le groupe $A^\times$)**.**

✓	— La démontrer. C'est facile mais il y a tout de même une subtilité rédactionnelle concernant la stabilité par inverse. — Est-ce que $A^\times$ est un sous-anneau de A ?
★	Donner une condition nécessaire pour que $A^\times = \{1\}$. Ce groupe est rarement trivial. Se demander ensuite si cette condition nécessaire est suffisante (ne pas produire une démonstration : chercher des exemples ou contre-exemples).

Définition 2 (Produit fini d'anneaux)**.**

✓	— La démontrer. Il n'y a pas de subtilité majeure. Quels sont les éléments neutres pour $+$ et $\times$? — A-t-on $(A_1 \times A_2)^\times = A_1^\times \times A_2^\times$? — Si A_1 et A_2 sont commutatifs, est-ce que $A_1 \times A_2$ l'est ? Question analogue pour l'intégrité, la structure de corps, l'existence d'éléments nilpotents, etc. Attention à ne pas conclure trop vite.

Définition 3 (Algèbre, sous-algèbre, morphisme d'algèbres)**.**

✓	Se demander pourquoi on a choisi cette terminologie.

Proposition 4 (Exemples usuels)**.**

✓	Chercher d'autres exemples de K-algèbres parmi les anneaux et espaces vectoriels usuels. En fait, ils sont presque tous des K-algèbres : mettre en valeur ceux qui n'en sont pas.
★	Si X est vide, que dire de $\mathcal{F}(X, K)$? Est-ce une K-algèbre ?

Définition 5 (Polynôme en un élément d'une algèbre)**.**

✓	Vérifier *vraiment* que l'application d'évaluation est un morphisme de K-algèbres.
★	Soit $\mathbb{H}$ l'ensemble des quaternions, dont on retiendra seulement que c'est une $\mathbb{R}$-algèbre non commutative, dont tout élément non nul est inversible (en particulier elle est intègre), et qu'elle admet une $\mathbb{R}$-base $(1, i, j, k)$ telle que : $i^2 = j^2 = k^2 = ijk = -1$ (cela suffit à entièrement déterminer $\mathbb{H}$). Trouver ce qui est faux dans le raisonnement suivant, et qui met en évidence une subtilité qui passe quasiment inaperçue dans la définition de $K[u]$ et du morphisme d'évaluation : « on a : $X^2+1 = (X+i)(X-i)$. En évaluant en j cette égalité, on obtient : $0 = j^2 + 1 = (j+i)(j-i)$, et comme $\mathbb{H}$ est intègre on en déduit : $i = \pm j$. ». C'est impossible puisque (i, j) est libre, donc j'ai fait une erreur : où ? Après avoir compris d'où vient l'erreur, reprendre avec soin la vérification que l'application d'évaluation est un morphisme de K-algèbres, et voir ce qui fait que tout marche dans ce contexte.

1.1.2 Arithmétique des idéaux

Motivation de cette partie

Euler montra qu'il était possible de faire de l'arithmétique dans d'autres anneaux que $\mathbb{Z}$ et $K[X]$, puisqu'il établit l'existence de solutions entières non nulles à l'équation de Fermat $x^3+y^3=z^3$ en factorisant le membre de gauche dans $\mathbb{Z}[j]=\left\{a+bj \mid (a,b)\in\mathbb{Z}^2\right\}$ et en étudiant les relations de divisibilité que cela implique. L'objectif de cette partie est de comprendre à quelle condition il est effectivement possible de faire de l'arithmétique dans un anneau A. Nous allons voir que pour correctement définir la relation de divisibilité (pour en faire une relation d'ordre), et pour permettre les raisonnements sur le « plus petit » élément à vérifier une propriété donnée, le bon cadre est celui des idéaux.

Nous allons donc reformuler les propriétés de base de l'arithmétique en termes d'idéaux. Dans le cas où les idéaux sont tous principaux, nous retrouverons tous les théorèmes d'arithmétique connus dans $\mathbb{Z}$ et $K[X]$.

Définition 6 (Divisibilité dans un anneau intègre, éléments associés)**.**

✓	On note que l'intégrité intervient déjà dans la caractérisation des éléments associés. Et la commutativité ?

Remarque.

✓	Vérifier ces affirmations sans mystère. Et si A n'est pas supposé intègre, que dire des éléments qui divisent 0_A ?
★	Dans un anneau non intègre, proposer des éléments qui sont associés sans être égaux à un élément inversible près.

Remarque.

✓	— Vérifier que c'est effectivement une relation d'équivalence. — Vérifier que la relation de divisibilité est effectivement correctement définie sur $A/A^\times$: si a divise b et si : $a\sim a'$, alors a' divise b. De même si $b\sim b'$. Ainsi, toutes les notions fondamentales de l'arithmétique sont « aux inversibles près ». — On voit que faire de l'arithmétique dans A nécessite de connaître $A^\times$. Déterminer $A^\times$ pour les anneaux usuels.
★	— Est-ce que la notation $A/A^\times$ désigne un groupe quotient ? Un anneau quotient ? — Montrer que l'application $A^\times \to S_A$ définie par $u\mapsto(\varphi_u : a\mapsto ua)$ est un morphisme de groupes. Cela équivaut à la donnée d'une action de groupe : la notation $A/A^\times$ provient de là (c'est l'ensemble des orbites de cette action, c'est-à-dire les ensembles de la forme $\left\{\varphi_u(a) \mid u\in A^\times\right\}$).

Remarque.

✓	Pourquoi tient-on absolument à avoir une relation d'ordre ? Où cela nous est-il utile, lorsqu'on fait de l'arithmétique dans $\mathbb{Z}$ ou $K[X]$ (pour prendre des exemples connus) ?

Proposition 7 (Divisibilité en termes d'idéaux)**.**

✓	— Déduire de cette proposition que multiplier un élément par un inversible ne change pas l'idéal qu'il engendre. — Vérifier la cohérence de cet énoncé avec ce que je dis plus haut : la relation de divisibilité est correctement définie sur $A/A^\times$. — Plus généralement, dans l'intégralité de cette section : vérifier que les affirmations sur les idéaux valent aussi sur les éléments de $A/A^\times$. — En quoi cette traduction de la divisibilité en termes d'idéaux permet de résoudre le problème formulé plus haut, à savoir que la relation de divisibilité n'est pas une relation d'ordre ?
★	Reformuler les commentaires ci-dessus par la donnée d'une bijection entre $A/A^\times$ et l'ensemble des idéaux principaux, vérifiant une certaine propriété de « monotonie » qui reflète les équivalences de cette proposition. Si vous avez trouvé cette bijection, vous avez trouvé une formulation succincte et savante du fait que « raisonner avec $A/A^\times$ ou des idéaux, cela revient au même en arithmétique ».

Remarque.

★	— Proposer une autre démonstration. — En particulier, qu'est-ce que cela nous dit des idéaux d'un corps ? Et de l'intérêt arithmétique des corps ?

Définition 8 (Éléments irréductibles)**.**

✓	Est-ce que la notion d'irréductibilité peut être définie sur $A/A^\times$? C'est-à-dire : si a est irréductible, et si $a \sim a'$, est-ce que a' est irréductible ?
★	— Pourquoi exclure les inversibles ? Se poser éventuellement la question plus tard, après avoir vu plusieurs énoncés faisant intervenir des éléments irréductibles. — Reformuler cette définition en termes d'idéaux. — Si a est irréductible, que dire de l'anneau quotient A/aA ?

Exemple 1.

Définition 9 (Anneau principal)**.**

★	En introduisant les idéaux au chapitre III, je disais qu'ils étaient les « bons » analogues des sous-espaces vectoriels d'un espace vectoriel (quand on remplace les espaces vectoriels par des anneaux). Ayant ceci en tête, comprendre pourquoi un anneau principal est un candidat crédible à une généralisation de la théorie de la dimension : que serait la « dimension » de A sur A, si cela avait un sens ? Et par conséquent, à quoi devrait-on s'attendre, pour la « dimension » d'un idéal de A sur A ? À comparer avec cette définition.
☢	Trouver des exemples d'anneaux (non nécessairement intègres, mais on évitera tout de même le cas non commutatif) dont certains idéaux ne sont pas principaux. Penser à des anneaux de fonctions, de polynômes...

Définition-Proposition 10 (Définition des pgcd et des ppcm dans un anneau principal)**.**

✓	— Démontrer ce que j'ai omis. — Si $a \in A$ et p est irréductible, que dire d'un pgcd et d'un ppcm de p et a ? C'est souvent utile. — Si $a_1, \dots, a_n$ sont premiers entre eux, est-ce que pour tous $i \neq j$, les éléments a_i et a_j sont premiers entre eux ? Et réciproquement ?
★	— Après avoir démontré cette proposition : montrer que, réciproquement, si l'on définit un ppcm des a_i comme le plus petit élément (modulo $A^\times$) de l'ensemble des multiples communs des a_i (modulo $A^\times$), alors il doit nécessairement engendrer $\cap_i a_i A$. Cela permet de rendre naturelle cette définition qui semble sortir de nulle part. Même question avec les pgcd. — Pourquoi la réunion des $a_i A$ n'est pas intéressante à étudier ? — Si d et m sont un pgcd et un ppcm des $a_1, \dots, a_n$, a-t-on toujours la relation $dm = \prod_{i=1}^{n} a_i$?
☢	Si l'on n'est pas dans un anneau principal, on peut tout de même définir les pgcd et ppcm, s'ils existent, comme les grands ou plus petits éléments d'ensembles de diviseurs ou de multiples, etc. Le cas échéant : — montrer que $a_1, \dots, a_m$ admettent un ppcm si et seulement si l'idéal $\bigcap_i a_i A$ est principal ; — montrer qu'il est possible que $a_1, \dots, a_m$ admettent un pgcd sans pour autant qu'ils engendrent un idéal principal (chercher dans $\mathbb{R}[X,Y]$, ou $\mathbb{Z}[X]$) ; — montrer qu'il est possible que $a_1, \dots, a_m$ admettent un pgcd si et seulement si l'ensemble des idéaux *principaux* admet un plus petit élément ; — montrer pour tout a non nul, les a_i admettent un ppcm si et seulement si les $a \cdot a_i$ en admettent un (et donner un lien entre les deux ppcm), mais que c'est faux pour les pgcd ; — montrer que pour tout a non nul, si les $a \cdot a_i$ admettent un pgcd, alors les a_i aussi (et donner un lien entre les deux pgcd) ; — montrer que si x et y ont un ppcm, alors m divise xy, et que l'élément d tel que $xy = md$ est un pgcd (ainsi on a ppcm $\Rightarrow$ pgcd) ; — montrer qu'on peut avoir un pgcd sans avoir un ppcm, mais que, s'il existe d tel que ad soit un pgcd de ax et ay pour tout $a \in A \setminus \{0\}$, alors x et y admettent un ppcm, qui est un élément m tel que $md = xy$; — montrer que si $xA + yA$ est principal alors $xA \cap yA$ aussi ; — montrer que toute intersection de deux idéaux principaux est principale si et seulement si tout couple d'éléments admet un ppcm, si et seulement si tout couple d'éléments admet un pgcd ; et que dans ce cas $xy = \mathrm{pgcd}(x,y)\mathrm{ppcm}(x,y)$ modulo $A^\times$; — montrer que dans $\mathbb{Z}[i\sqrt{5}] = \left\{a + i\sqrt{5}b \mid (a,b) \in \mathbb{Z}^2\right\}$, les éléments 3 et $2 + i\sqrt{5}$ n'ont pas de ppcm et que 9 et $2 + i\sqrt{5}$ n'ont pas de pgcd.

Théorème 11 (Théorème de Bézout dans un anneau principal)**.**

✓	— S'il existe $u_1, \dots, u_n$ tels que : $\sum_{i=1}^{n} a_i u_i = d$, que dire de d ? (C'est très facile si on raisonne en termes d'idéaux.) — Comparer avec la démonstration du théorème de Bézout dans $\mathbb{Z}$ et $K[X]$ avec les outils de 1re année. Lorsque, plus tard, nous aurons démontré que $\mathbb{Z}$ et $K[X]$ sont principaux : quelle démonstration du théorème de Bézout est la plus simple ? Néanmoins, j'affirme que l'autre démonstration conserve un intérêt : lequel ?
☢	— Est-ce que réciproquement, si ce théorème est vrai, alors A est principal ? (Je pense qu'il est trop tôt pour répondre à cette question : l'exemple que j'ai en tête nécessite d'avoir *a minima* vu la théorie des séries entières.)

Proposition 12 (Lemme d'Euclide et théorème de Gauß dans un anneau principal)**.**

★	— Réciproquement, montrer que le lemme d'Euclide implique le théorème de Gauß. À faire éventuellement après avoir lu le reste de la section. — J'affirme que le théorème de Gauß dit quelque chose d'intéressant concernant les éléments inversibles et les diviseurs de zéro de A/aA. Quoi donc ? Même chose avec le lemme d'Euclide si a est irréductible.
☢	Est-ce que réciproquement, cet énoncé implique le théorème de Bézout ?

Théorème 13 (Existence, unicité de la décomposition en éléments irréductibles dans un anneau principal)**.**

✓	— Pourquoi exclut-on $a = 0$ de ce théorème ? — Pourquoi l'élément inversible n'est-il pas uniquement défini, dans la décomposition en facteurs irréductibles d'un élément non nul ? À ce stade, comprendre pourquoi on veut qu'un élément irréductible soit non inversible. — Revoir la démonstration de ce théorème dans le cas de $\mathbb{Z}$ et $K[X]$, afin de comprendre comment le lemme 14 permet de les imiter (faire un parallèle, étape par étape, entre les démonstrations dans $\mathbb{Z}$ et $K[X]$ et celle dans A principal). Pourquoi ne pouvait-on pas éviter de passer par des idéaux pour imiter les raisonnements de minimalité dans $\mathbb{Z}$ et $K[X]$? — Achever la démonstration de l'unicité, si je l'ai laissée en suspens. Soit par une récurrence soignée, soit *via* le commentaire ★ plus bas.
★	— Se convaincre que l'existence, dans ce théorème, équivaut exactement à l'énoncé : « tout élément non inversible admet un diviseur irréductible ». Démontrer cet énoncé équivalent à l'aide du lemme 14 (s'inspirer de la démonstration dans $\mathbb{Z}$ et $K[X]$ si vous manquez d'idée, et l'adapter en vous souvenant de la reformulation des relations de divisibilité en termes d'idéaux). — On a utilisé le lemme 14 pour l'existence. L'utiliser également pour l'unicité, afin d'éviter la rédaction elliptique à la « et ainsi de suite » en fin de démonstration. — Observer que plus généralement, le lemme 14 permet d'imiter les raisonnements par récurrence dans des ensembles autres que $\mathbb{N}$, ainsi que les raisonnements par l'absurde utilisant un plus petit ou plus grand élément. Ce parallèle devient d'autant plus évident si l'on se souvent comment fut démontré le principe de récurrence. L'illustrer en démontrant cet énoncé : « dans un anneau principal, tout idéal est intéressant ». — On a démontré l'unicité à l'aide du lemme d'Euclide. Réciproquement, montrer que l'existence et, surtout, l'unicité de la décomposition en facteurs irréductibles impliquent le lemme d'Euclide (de sorte que, finalement : théorème de Gauß, lemme d'Euclide et unicité de la décomposition, sont trois énoncés équivalents).
☢	— On a utilisé le lemme d'Euclide pour démontrer l'unicité. Cela semble indiquer que l'existence d'une décomposition n'utilise pas ce lemme, et donc pourrait être valable hors d'un anneau principal. Pourriez-vous donner des exemples d'anneaux vérifiant l'existence de la décomposition en irréductibles, sans l'unicité ? (Chercher des exemples proches de ceux que vous connaissez.) — Il reste un résultat classique non énoncé dans un anneau principal A, et pourtant valable dans $\mathbb{Z}$ et $K[X]$: l'infinité des éléments irréductibles (quoique ceci ne soit pas totalement évident dans $K[X]$ si K est fini). Qu'en pensez-vous ? On écartera rapidement les cas triviaux (A de cardinal fini, A un corps).

Lemme 14 (Un lemme qui remplace les arguments de minimalité des entiers ou polynômes)**.**

✓	— Réviser la définition d'élément maximal, pour la distinguer du plus grand élément d'un ensemble. — Prendre des exemples simples $\mathcal{I}$ d'ensembles d'idéaux dans $\mathbb{Z}$, et décrire ses éléments maximaux, afin de vous convaincre de la justesse de cette proposition. Qu'observez-vous de remarquable ?
☢	Comparer cet énoncé au lemme de Zorn (vu en Informatique, me semble-t-il : tout ensemble inductif non vide admet un élément maximal). Est-ce que ce lemme est une conséquence directe du lemme de Zorn ?

Exercice 1.

✓	Le démontrer dans les cas particuliers $\mathbb{Z}$ et $K[X]$, sans utiliser le fait qu'ils soient principaux.
★	Le faire.
☢	Est-ce que réciproquement, un anneau vérifiant cette propriété est principal ?

Proposition 15 (Caractérisation des éléments premiers entre eux)**.**

✓	— Démontrer cette proposition, si je ne l'ai pas fait. Si vous séchez : il suffit de reprendre la démonstration vue dans $\mathbb{Z}$ ou $K[X]$. — Plus généralement : reprendre TOUS les résultats d'arithmétique vus en 1re année (existence des valuations p-adiques, caractérisation de la divisibilité en termes de valuations, expression des ppcm et pgcd à l'aide de facteurs irréductibles, etc.) et qui découlent du théorème fondamental de l'arithmétique, et vérifier qu'ils se généralisent à tout anneau principal.
★	Pourquoi la dernière caractérisation (avec les diviseurs irréductibles) est très souvent préférable quand on veut montrer que des éléments sont premiers entre eux en raisonnant par l'absurde ?

Montrer qu'un anneau est principal.

✓	Réviser les démonstrations que $\mathbb{Z}$ et $K[X]$ admettent une division euclidienne. On réfléchira en particulier à la façon de définir le quotient (une fois que le quotient est correctement défini, le reste est trivial à obtenir : pourquoi ?). Cela servira d'inspiration pour tous les autres anneaux où vous voulez montrer l'existence d'une division euclidienne.

Après votre révision de cette partie

Récapituler toutes les conséquences arithmétiques de la principalité d'un idéal. Les mettre en parallèle des résultats connus dans $\mathbb{Z}$ et $K[X]$. Réviser comment vous les utilisiez dans ces deux anneaux, pour forger votre intuition dans tout anneau.

1.2 Arithmétique des entiers et des polynômes

1.2.1 Arithmétique dans $\mathbb{Z}$

Motivation de cette partie

On redémontre en seulement quelques lignes tous les résultats connus d'arithmétique dans $\mathbb{Z}$. Ce nouveau point de vue permet de prendre plus de hauteur sur ce qui fait la spécificité des entiers.

Théorème 16 ($\mathbb{Z}$ est un anneau principal)**.**

↘ III lem. 19

✓	Revoir la démonstration du lemme auquel on renvoie, et comparer à la dernière remarque de la section précédente.

Corollaire 17 (On peut faire de l'arithmétique dans $\mathbb{Z}$)**.**

✓	Comparer avec les démonstrations de ces différents résultats en 1re année. Qu'est-ce que la démonstration de cette année apporte comme plus-value ? Pourquoi, pour autant, les démonstrations de 1re année ne sont pas obsolètes ?

1.2.2 Structure d'anneau de $\mathbb{Z}/n\mathbb{Z}$

Motivation de cette partie

Pour le moment, seul le groupe additif $(\mathbb{Z}/n\mathbb{Z}, +)$ fut étudié. Nous passons à l'étude de $\mathbb{Z}/n\mathbb{Z}$ en tant qu'anneau, et c'est autrement plus intéressant pour l'arithmétique : en effet, l'arithmétique considère plutôt les produits que les sommes d'entiers. Lorsqu'on étudie un anneau, on s'intéresse à sa commutativité, ses inversibles, ses diviseurs de zéro, ses éléments nilpotents. Notre étude permet de recouvrir tous ces aspects, et de donner une condition nécessaire et suffisante remarquable pour que $\mathbb{Z}/n\mathbb{Z}$ soit un corps. Nous allons aussi généraliser le petit théorème de Fermat et donner un moyen de calculer l'indicatrice d'Euler.

Quand p est premier, $\mathbb{Z}/p^k\mathbb{Z}$ est considérablement plus simple à manipuler. Nous donnerons un théorème permettant de toujours s'y ramener : le théorème chinois.

Proposition 18 (Inversibles de $(\mathbb{Z}/n\mathbb{Z})^\times$)**.**

↘ III prop. 24

✓	— Démontrer cette équivalence sans recourir au résultat sur les générateurs de $\mathbb{Z}/n\mathbb{Z}$. — Démontrer cette équivalence en passant par d'autres implications, par exemple : $(iii) \Rightarrow (ii) \Rightarrow (i) \Rightarrow (iii)$. — Vérifier que $u \cdot \bar{x} = \bar{u} \cdot \bar{x}$ pour tout $u \in \mathbb{Z}$. — Est-ce que le même résultat serait vrai dans l'anneau $K[X]/PK[X]$? Pourquoi ?
★	Comment peut-on caractériser l'aspect générateur de $\bar{x}$ à l'aide de l'application $\bar{a} \mapsto \bar{a}\bar{x}$ de multiplication par $\bar{x}$? En déduire une équivalence entre : ne pas être diviseur de zéro dans $\mathbb{Z}/n\mathbb{Z}$, et : être inversible dans $\mathbb{Z}/n\mathbb{Z}$. On fait ainsi le lien entre deux propriétés que l'on n'aurait pas forcément rapprochées immédiatement, au vu de leurs définitions. On doit se poser régulièrement cette question, même hors du contexte de ce chapitre : les propriétés des applications de multiplication par un élément $x \in A$ fixé peuvent être étudiées grâce à des théorèmes sur les applications, afin d'en déduire des propriétés de x.

Exemple 2.

✓	Varier les exemples pour s'approprier la méthode. La *Banque des Cent* vous le permet aussi.
★	S'en inspirer pour calculer des inverses dans $K[X]/PK[X]$. Quand on applique la méthode à un élément $a + bi = \overline{a + bX}$ de $\mathbb{C} = \mathbb{R}[X]/(X^2+1)\mathbb{R}[X]$ (défini au chapitre III), qu'obtient-on ? À comparer avec ce que vous savez être $(a+bi)^{-1}$.

Corollaire 19 (Théorème d'Euler)**.**

↘ III th. 22

★	Et si x n'est pas premier avec n, peut-on dire quelque chose malgré tout ? Varier les exemples. Constater que le comportement « asymptotique » des puissances dépend de certaines choses (mais quoi ?). À la fin de la section, démontrer ce que vous avez constaté.

Corollaire 20 ($\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier, notation $\mathbb{F}_p$)**.**

✓	Il est possible de démontrer cette équivalence de plein de façons différentes. Les varier. Je trouve que dans la suite d'implications : $(iii) \Rightarrow (ii) \Rightarrow (i) \Rightarrow (iii)$, chaque raisonnement est très instructif.
★	— Caractériser les points (i) et (ii) à l'aide des applications $\bar{a} \mapsto \bar{a}\bar{x}$ de multiplication par un entier. Quelle équivalence remarquable démontre-t-on, reformulée ainsi ? — Montrer plus généralement que tout anneau commutatif fini et intègre est un corps. — Montrer que ces équivalences et la démonstration s'adaptent à $K[X]/PK[X]$, avec P polynôme non nul : c'est un corps (et un anneau intègre) si et seulement si P est irréductible. Même si cet anneau quotient n'est jamais étudié dans le programme de classes préparatoires, c'est probablement l'anneau quotient le plus riche et instructif qui soit (autant voire plus que $\mathbb{Z}/n\mathbb{Z}$). Il permet notamment de bien comprendre les anneaux de la forme $K[u]$ avec u élément d'une algèbre, *via* le théorème d'isomorphisme (voir plus loin la définition du polynôme minimal pour approfondir ce commentaire). Vous gagnerez donc en recul si vous l'étudiez systématiquement lorsque j'en fais la mention. — Montrer que ces équivalences et la démonstration s'adaptent à A/aA avec A principal et $a \in A \setminus (\{0\} \cup A^\times)$.
☢	Connaissez-vous d'autres corps finis que $\mathbb{Z}/p\mathbb{Z}$ pour p premier ?

Remarque.

✓	— Comparer avec la démonstration « antique » du petit théorème de Fermat. Selon votre façon de le démontrer en 1re année (soit par un calcul de $\prod_{i=1}^{n-1} i \bmod n$ de deux manières différentes *via* une bijection, soit avec une récurrence et la formule du binôme de Newton), la démonstration de 2e année n'en est qu'une bête reformulation : le remarquer. — On sait que le théorème de Fermat peut se reformuler : $\forall x \in \mathbb{Z}$, $x^n \equiv x \bmod n$ (pour n premier), ce qui a l'avantage de ne pas nécessiter d'hypothèse sur x. J'affirme pourtant que l'égalité $x^{n-1} \equiv 1 \bmod n$, pour x premier avec n, est préférable, par exemple en vue de simplifier des puissances de x arbitrairement grandes. Pourquoi ?
★	Si n n'est pas premier, peut-on proposer un énoncé du théorème d'Euler pour tout $x \in \mathbb{Z}$, sans hypothèse sur x ?

Théorème 21 (Théorème chinois)**.**

✓
- Pour n entier naturel non nul quelconque, qu'est-ce que cet énoncé nous dit de $\mathbb{Z}/n\mathbb{Z}$?
- Faire une liste de toutes les propriétés qui vous viennent en tête, qui sont vérifiées par $\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$ ou $\mathbb{Z}/p_i\mathbb{Z}$ pour p_i premier, et qui ne sont pas vérifiées par $\mathbb{Z}/n\mathbb{Z}$ en général. Comprendre pourquoi l'intérêt de cet énoncé est de pouvoir s'y ramener. Se poser la question plus tard éventuellement.
- Vérifier que si m_1 et m_2 sont premiers entre eux, alors effectivement : $\text{ppcm}(m_1, m_2) = m_1 m_2$. C'est la clé du raisonnement !
- Pour la récurrence : vérifier que si $m_1, \dots, m_r$ sont premiers entre eux dans leur ensemble, et non deux à deux, alors $m_1 \cdots m_{r-1}$ et m_r ne sont pas forcément premiers entre eux. Vérifier que sous l'hypothèse plus forte de l'énoncé, c'est vrai (je n'ai pas détaillé ce point).

★
- Le théorème de factorisation des morphismes devrait plutôt impliquer que $\Phi : \mathbb{Z}^2/(m_1\mathbb{Z}\times m_2\mathbb{Z}) \to \mathbb{Z}/m_1m_2\mathbb{Z}$ est bien définie, pourtant ce n'est pas ce que j'ai écrit. Se convaincre que l'anneau de départ donne bien la même chose que $\mathbb{Z}/m_1\mathbb{Z}\times\mathbb{Z}/m_2\mathbb{Z}$.
- On a montré la surjectivité par un argument sur les cardinaux. Pouvait-on la démontrer directement sans cela ?
- Réciproquement, si m et n ne sont pas premiers entre eux, comparer $\mathbb{Z}/mn\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$.
- On peut démontrer par des moyens élémentaires que si m et n sont premiers entre eux, alors $\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$ est cyclique, engendré par (1,1), et est donc isomorphe à $\mathbb{Z}/mn\mathbb{Z}$. J'affirme cependant que cet énoncé en dit bien davantage. Pourquoi ?
- Déduire de cet énoncé quelques conséquences de base sur l'intégrité, les éléments nilpotents, les diviseurs de zéro, etc. (la seule limite est votre imagination), de $\mathbb{Z}/n\mathbb{Z}$ en fonction de ses diviseurs premiers.
- Montrer que le théorème chinois a une version dans $K[X]$: si P_1 et P_2 sont premiers entre eux, alors $K[X]/P_1P_2K[X]$ est isomorphe à $K[X]/P_1K[X]\times K[X]/P_2K[X]$, de même avec r polynômes P_i. En particulier, pour $P_i = X - a_i$, j'affirme que l'existence et l'unicité d'un antécédent de ($b_1 \bmod X - a_1, \dots, b_r \bmod X - a_r$) vous renvoie à un résultat de 1re année bien connu ! Lequel ? Pourquoi la reformulation que je vous propose est-elle plus riche de conséquences ?
- Vérifier que si $m_1, \dots, m_r$ ne sont pas supposés premiers entre eux deux à deux, alors le morphisme est toujours correctement défini, mais qu'il n'est plus injectif (ni surjectif).

☢ Généraliser l'énoncé à tout anneau principal.

Interprétation en termes de congruence.

✓
- Comprendre cette reformulation. Que dit précisément l'injectivité sur ce système ? Et la surjectivité ?
- Pourquoi cette reformulation, certes très concrète, n'est pas aussi riche d'implications que celle avec un isomorphisme ?
- Donner des systèmes de congruence CONCRETS n'ayant pas de solution.

Exemple 3. ♡

✓
- Se convaincre de l'implication : $a^{561} \equiv a \bmod 561 \Rightarrow a^{561} \equiv a \bmod 3$ (ou 11, ou 17), et qu'elle ne nécessite pas le théorème chinois. Plus généralement, vérifier que si : $a \equiv b \bmod n$, et si m divise n, alors : $a \equiv b \bmod m$.
- Se convaincre que le fait d'avoir une équivalence, et non une implication directe, est bien une conséquence du théorème chinois. *C'est très important.*
- Comprendre pourquoi je n'ai pas utilisé le petit théorème de Fermat sous la forme : $a^3 \equiv a \bmod 3$, préférant la fastidieuse distinction de cas que nécessite la congruence $a^2 \equiv 1 \bmod 3$ (de même avec 11 et 17). Faire le lien avec un commentaire plus haut sur le petit théorème de Fermat (après l'avoir déduit du théorème d'Euler).

☢ En observant quelles propriétés arithmétiques de 561 ont permis ce contre-exemple au petit théorème de Fermat, conjecturer une généralisation (que vous ne serez pas en mesure de démontrer : il faut pour cela la cyclicité du groupe $(\mathbb{Z}/p\mathbb{Z})^\times$) : à quelle condition suffisante (voire nécessaire) un entier n vérifie : $\forall a \in \mathbb{Z}$, $a^n \equiv a \bmod n$?

Remarque. ♡

✓ Comprendre pourquoi Φ^{-1} vérifie effectivement la propriété de « $\mathbb{Z}$-linéarité » suivante : $\Phi^{-1}(a \bmod m, b \bmod n) = a\Phi^{-1}(1 \bmod m, 0 \bmod n) + b\Phi^{-1}(0 \bmod m, 1 \bmod n)$. Cette stratégie pour déterminer un morphisme de groupes à l'aide de son image d'une « base » se généralise-t-elle ?

★
- Peut-on construire de même la bijection réciproque de l'isomorphisme entre $\mathbb{Z}/m_1\cdots m_r\mathbb{Z}$ et $\prod_{i=1}^{r} \mathbb{Z}/m_i\mathbb{Z}$?
- On a dit plus haut que le théorème chinois est valable avec $K[X]/(P)$. Construire la bijection réciproque sur le même modèle. Dans le cas : $P_i = X - a_i$, que reconnaissez-vous de très connu ?
- Si vous avez réussi l'item précédent : comprendre pourquoi le théorème chinois avec $K[X]/(P)$ permet de créer des polynômes interpolateurs dont les évaluations ET les évaluations des dérivées (à un certain ordre), en un nombre fini de points, ont des valeurs prescrites.

Exemple 4.

✓	— Bien comprendre pourquoi $\bar{x}^2 = \bar{1} \Rightarrow \bar{x} = \pm\bar{1}$ nécessite de raisonner modulo un nombre premier (d'ailleurs, cet exemple permet bien de démontrer que c'est faux modulo 51). — Vérifier que $x^2 \equiv 1 \bmod p_1 \cdots p_r$ admet bien 2^r solutions si les p_i sont distincts, premiers et impairs, et 2^{r-1} solutions sans l'hypothèse de parité.
★	Varier les exemples. La *Banque des Cent* fournit (fournira ?) d'autres équations analogues.
☢	Donner tous les anneaux $\mathbb{Z}/n\mathbb{Z}$ dans lesquels $x^2 \equiv 1 \bmod n$ admet uniquement pour solutions 1 et -1 modulo n.

Corollaire 22 (Indicatrice d'Euler : calcul effectif)**.**

✓	— Vérifier *vraiment* l'isomorphisme entre $(\mathbb{Z}/mn\mathbb{Z})^\times$ et $(\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$. — Vérifier le dénombrement de l'ensemble des éléments non inversibles : pourquoi y a-t-il bien $p^k - p^{k-1}$ classes dans $\mathbb{Z}/p^k\mathbb{Z}$ de la forme $\overline{ap}$ avec $a \in \mathbb{Z}$? — Pourquoi ce même dénombrement dans $\mathbb{Z}/n\mathbb{Z}$ directement, avec n quelconque, est-il plus compliqué, et justifie l'approche suivie ?
★	À l'aide de ce corollaire, démontrer l'identité $n = \sum_{d\mid n} \varphi(d)$ autrement que *via* l'approche suivie en travaux dirigés. Pourquoi la démonstration que j'ai proposée en exercice est-elle conceptuellement plus instructive ?

Exemple 5.

✓	— Poursuivre le calcul pour d'autres valeurs de n. On pourra les représenter graphiquement et essayer de comprendre ce que l'on observe, effectuer différentes conjectures sur le comportement asymptotique de φ, etc. — Qu'observe-t-on sur la parité de $\varphi(n)$? L'expliquer.
★	— Quelles sont les solutions apparentes de $\varphi(n) = 2$ et $\varphi(n) = 4$? Proposer une démonstration. Ces deux équations sont intéressantes pour diverses préoccupations algébriques, dont deux que j'énonce dans proposer de démonstration : la première, pour que le cardinal de $(\mathbb{Z}/n\mathbb{Z})^\times$ soit égal à 2 (ce qui permet de démontrer sans outil sophistiqué le cas particulier suivant de la progression arithmétique de Dirichlet : il existe une infinité de nombres premiers p tels que $p \equiv -1 \bmod n$), la seconde, pour que la dimension sur $\mathbb{Q}$ de $\mathbb{Q}\left[e^{\frac{2i\pi}{n}}\right]$ soit égale à 4, et donc la dimension de $\mathbb{Q}\left[\cos\left(\frac{2\pi}{n}\right)\right]$ égale à 2 (ce qui implique concrètement que cela donne tous les angles remarquables dont le cosinus s'exprime à l'aide de rationnels et de la racine carrée d'un rationnel). — Proposer un encadrement explicite de $\varphi(n)$ pour tout $n \geqslant 1$, en fonction de n.
☢	Est-ce que φ induit une surjection de $\mathbb{N} \setminus \{0,1,2\}$ dans $2\mathbb{N} \setminus \{0\}$?

Après votre révision de cette partie

1. Commencer à comprendre quel fut l'intérêt d'introduire l'ensemble $\mathbb{Z}/n\mathbb{Z}$: après tout, en 1re année, vous saviez déjà faire du calcul modulo n, donc l'introduction de $\mathbb{Z}/n\mathbb{Z}$ pouvait d'abord s'apparenter à un simple changement de vocabulaire.
2. Effectuer les *Savoir-faire à vérifier* sur l'arithmétique des entiers, sauf celui exploitant la structure cyclique de $(\mathbb{Z}/p\mathbb{Z})^\times$ (attendre de l'avoir vue en travaux dirigés).

1.2.3 Arithmétique dans $K[X]$

Motivation de cette partie

Même motivation que dans $\mathbb{Z}$. Mais ici la situation est un peu plus nouvelle, puisque le programme de 1re année se borne à l'étude dans $\mathbb{R}[X]$ ou $\mathbb{C}[X]$. Or l'étude des polynômes dans $\mathbb{Q}[X]$ est très présente dès qu'on s'intéresse aux nombres *algébriques* (c'est-à-dire aux solutions des équations polynomiales non triviales à coefficients entiers ou rationnels). On approfondit donc l'étude des polynômes irréductibles, en donnant une classe importante de polynômes irréductibles : les polynômes minimaux, qui donnent en quelque sorte les équations polynomiales minimales vérifiées par des nombres algébriques, et donnent un moyen inédit (propre aux polynômes et sans analogue dans $\mathbb{Z}$) de montrer des relations de divisibilité.

Théorème 23 (L'anneau des polynômes sur un corps est un anneau principal)**.**

✓	— Comprendre pourquoi, au moment de chercher un polynôme qui engendre I, il était *naturel* de le prendre de degré minimal (par analyse-synthèse par exemple). — Vérifier l'inclusion réciproque « évidente ». — Il y a plusieurs choix possibles de polynôme de degré minimal. Pourtant ils engendrent le même idéal : pourquoi ? — Comparer avec la démonstration que $\mathbb{Z}$ est principal. Essayer d'en déduire une stratégie générale pour montrer que tout anneau intègre ayant une division euclidienne (en termes qu'on laisse vagues : la difficulté est de généraliser la condition sur le reste) est principal. — Dans le cas de $\mathbb{Z}$, on a même montré mieux : tous les sous-groupes de $\mathbb{Z}$ sont engendrés par un seul élément. Se convaincre que ce n'est pas le cas dans $K[X]$, et comprendre ce qui empêche la démonstration de se généraliser de $\mathbb{Z}$ à $K[X]$ (cela apparaît de manière presque voilée dans la démonstration de cette proposition).
☢	— Si l'on veut adapter la démonstration à $A[X]$ où A n'est pas un corps (par exemple $\mathbb{Z}[X]$), qu'est-ce qui coince ? Peut-on malgré tout démontrer que $A[X]$ est principal ? — Si l'on remplace $K[X]$ par $K[[X]]$ (c'est $K^{\mathbb{N}}$ muni de la même addition et multiplication que $K[X]$), obtient-on toujours un anneau principal ? (J'affirme que les propriétés arithmétiques de cet anneau sont très étonnantes, et répondent à des questions pertinentes qu'on pourrait se poser sur les irréductibles d'un anneau.)

Rappel.

✓	— Se convaincre de ce que j'affirme très brièvement. — Au regard de tout ce qui a été dit dans la section précédente sur les éléments associés : comprendre en quoi ce rappel permet de dire : « on peut toujours se ramener à des polynômes unitaires quand on fait de l'arithmétique dans $K[X]$. »

Corollaire 24 (On peut faire de l'arithmétique avec les polynômes)**.**

✓	— J'affirme que cet énoncé contient davantage que ce que vous aviez déjà démontré en 1re année (même si cela reste très proche). Quoi donc ? — Vérifier effectivement l'unicité de la constante, dans la décomposition en facteurs irréductibles unitaires. — Comprendre la plus-value de la remarque qui précède.
☢	Bien qu'on ne puisse pas montrer que $A[X]$ est principal par la méthode utilisée plus haut, j'affirme qu'on peut obtenir l'existence et unicité de la décomposition en facteurs irréductibles dans $A[X]$ si A est intègre. Pourquoi ? Prendre $A = \mathbb{Z}$ si cela vous aide à y voir clair.

Proposition 25 (Condition nécessaire pour être un polynôme irréductible)**.**

✓	Pourquoi j'exclus le degré 1 de la condition nécessaire ? Où apparaît cette nécessité dans la démonstration ?
★	— J'affirme que dans la démonstration, il apparaît subtilement, en *deux* endroits, le fait que les coefficients des polynômes soient dans un corps. Où ? (L'un de ces deux endroits ne nécessite que l'intégrité.) — Que donne cet énoncé si l'on est dans $A[X]$ avec A qui n'est pas un corps ?
☢	— Montrer que si $P \in K[X]$ est irréductible, alors il existe toujours un corps contenant K et une racine de P (s'inspirer de la construction de $\mathbb{C}$ au chapitre III ; pour vérifier que vous obtenez ainsi un corps, vous aurez besoin de mes commentaires formulés au corollaire 20). Ainsi, il faut toujours préciser dans quel corps le polynôme qu'on étudie n'admet pas de racine. Montrer de plus que la dimension minimale d'un tel corps (vu comme K-espace vectoriel) est égale au degré de P (vous aurez besoin de la construction *explicite* qui précède et du théorème d'isomorphisme). Un tel corps s'appelle un *corps de rupture* de P. Le faire pour $X^2 + \overline{1} \in \mathbb{Z}/3\mathbb{Z}[X]$ et $X^2 + X + \overline{1} \in \mathbb{Z}/2\mathbb{Z}[X]$: qu'obtenez-vous comme corps ? On peut obtenir tous les corps finis possibles par ce procédé ! — Que donne le point précédent si P n'est pas irréductible ?

Exemple 6.

✓	Fournir facilement une infinité de contre-exemples dans $\mathbb{R}[X]$.
★	Que dire d'un anneau $K[X]$ vérifiant l'équivalence entre l'irréductibilité (pour un polynôme de degré au moins 2) et l'absence de racine ? Connaissez-vous de tels anneaux ?

☢	Montrer néanmoins qu'on obtient une condition nécessaire et suffisante si l'on tient compte des corps contenant K, c'est-à-dire : montrer que si $P \in K[X]$, alors P est irréductible si et seulement si, pour tout corps L contenant K et vérifiant $\dim_K(L) \leqslant \frac{\deg(P)}{2}$, le polynôme P n'admet pas de racine dans L. La démonstration de cette équivalence nécessite de montrer l'existence des corps de rupture mentionnée ci-dessus. Retrouver, alors, grâce à cet énoncé, le fait que les polynômes irréductibles dans $\mathbb{R}[X]$ soient exactement les polynômes de degré 1 et ceux de degré 2 sans racine.

Théorème 26 (Théorème de D'Alembert-Gauß, et polynômes irréductibles sur $\mathbb{C}$)**.**

✓	Vérifier l'équivalence entre les deux formulations de ce théorème.
★	Vérifier que cet énoncé est faux avec $\mathbb{Q}[i] = \left\{a + bi \mid (a,b) \in \mathbb{Q}^2\right\}$ à la place de $\mathbb{C}$. Cela permet de comprendre pourquoi toute démonstration du théorème de D'Alembert-Gauß repose sur un argument d'analyse réelle : il nécessite $\mathbb{R}$ pour être vrai, or $\mathbb{R}$ fut construit analytiquement (soit pour avoir l'axiome de la borne supérieure, soit pour faire converger les suites de Cauchy, ce qui est équivalent).
☢	On pourrait penser que le problème avec $\mathbb{Q}(i)$ est sa dimension finie sur $\mathbb{Q}$, ou sa dénombrabilité, qui en fait un corps « trop petit » pour contenir les racines de tous les polynômes. Montrer qu'il n'en est rien, en remplaçant $\mathbb{Q}$ par l'un de ces deux corps (qui contredisent soit la dimension finie, soit la dénombrabilité, soit les deux) : 1° le plus petit sous-corps de $\mathbb{R}$ stable par $x \mapsto \sqrt{x}$ (c'est le corps des *nombres constructibles*, dont je ne demande pas de montrer l'existence ici), 2° l'élément maximal de l'ensemble $\{K \subseteq \mathbb{R} \mid K \text{ corps}, \sqrt{2} \notin K\}$ pour la relation d'inclusion, qui existe par le lemme de Zorn. Ainsi vous serez convaincus de la singularité du corps $\mathbb{R}$.

Corollaire 27 (Polynômes irréductibles sur $\mathbb{R}$)**.**

✓	Proposer une autre démonstration. Constater que dans tous les cas, on a besoin du théorème fondamental de l'algèbre, ce qui peut paraître étonnant alors que l'énoncé du corollaire ne fait pas intervenir $\mathbb{C}$.
★	Démontrer ce que j'ai laissé en suspens : *a priori* $(X-\alpha)(X-\bar{\alpha}) = X^2 - 2\mathrm{Re}(\alpha)X + |\alpha|^2$ divise P dans $\mathbb{C}[X]$ (c'est-à-dire : le quotient est dans $\mathbb{C}[X]$), et pourtant j'utilise ensuite l'irréductibilité de P dans $\mathbb{R}[X]$: pourquoi puis-je passer de $\mathbb{C}[X]$ dans $\mathbb{R}[X]$? Démontrer plus généralement que si A et B sont deux polynômes de $K[X]$, et si L est un corps contenant K, alors A divise B dans $K[X]$ si et seulement si c'est le cas dans $L[X]$. Cet énoncé a plein d'analogues (le fait d'être premiers entre eux ne dépend pas du corps K, etc.). Vous aurez probablement besoin d'utiliser l'unicité du quotient et du reste dans la division euclidienne.
☢	— Montrer plus généralement que si K et L sont deux corps tels que : $L = K(\alpha)$, où $\alpha \in L \setminus K$ est annulé par un polynôme de $K[X]$ de degré 2, alors il n'existe qu'un seul automorphisme de corps de L non trivial qui fixe les éléments de K et que, si l'on note σ cet automorphisme, alors $(X-x)(X-\sigma(x))$ est dans $K[X]$ pour tout $x \in L$, et irréductible si $x \in L \setminus K$. Achever de généraliser ce corollaire en notant que si L est algébriquement clos (c'est-à-dire : tout polynôme de $L[X]$ non constant est scindé), alors les irréductibles de $K[X]$ sont exactement les polynômes de degré 1 et ceux de degré 2 sans racine dans K. — Et si l'on reprend l'énoncé ci-dessus en supposant que α est annulé par un polynôme de $K[X]$ de degré d (où d est le plus petit degré à convenir), qu'obtient-on à la place ?

Exemple 7.

✓	— Proposer une autre démonstration que l'égalité : $\sqrt[3]{2} = \frac{a}{b}$, avec a et b entiers premiers entre eux, est impossible. Par exemple : montrer que b doit diviser a, ce qui n'est possible que si $b = \pm 1$, et conclure immédiatement. — Produire une infinité d'autres exemples, de degré supérieur à 3 et irréductibles dans $\mathbb{Q}[X]$, puis en faire autant dans $\mathbb{Z}/p\mathbb{Z}[X]$ (avec p explicite). Cela appuie mon commentaire ci-dessus concernant la forme très remarquable des irréductibles de $\mathbb{R}[X]$ (ils vous sont si familiers que le caractère exceptionnel de la proposition peut échapper).
☢	Produire des exemples de degré 4, 5, 6, etc. Certains exercices de travaux dirigés permettraient d'en produire pour des degrés quelconques.

Définition-Proposition 28 (Un idéal important : l'idéal annulateur, polynôme minimal)**.**

✓	— Connaissez-vous des exemples concrets où l'idéal I est réduit à $\{0\}$? — Définir alternativement $\pi_{z,K}$ comme le plus petit polynôme unitaire *au sens du degré*, dans $K[X]$, ayant z pour racine, et essayer de retrouver toutes ses propriétés données dans cette proposition. Comprendre pourquoi notre définition est plus satisfaisante. — Rédiger autrement notre démonstration de l'irréductibilité de $\pi_{z,K}$, pour que ce soit un raisonnement direct et non par l'absurde. — Quel aspect de la proposition nous permet de trouver le polynôme minimal d'un élément *en pratique* ?
★	— On savait déjà que $X - z$ divise P si et seulement si $P(z) = 0$. Pourquoi la relation de divisibilité de cette proposition est-elle plus instructive ? Plusieurs réponses sont possibles (y réfléchir éventuellement après avoir fini cette section ou traité quelques exercices). Quel est son *seul* défaut, par rapport à la divisibilité par $X - z$? — Le polynôme minimal d'un élément est irréductible. Réciproquement, est-ce que tout polynôme irréductible de $K[X]$ est le polynôme minimal sur K d'un élément ? — Que donne le théorème d'isomorphisme appliqué au morphisme d'évaluation ? Si vous avez bien suivi tout ce que je vous ai demandé, tout au long des commentaires de ce chapitre, vous pouvez notamment en déduire à moindre frais : une condition nécessaire et suffisante pour que $K[z]$ soit de dimension finie sur K, ou soit un corps (et le cas échéant, comment calculer un inverse en s'inspirant de ce que l'on fait dans $\mathbb{Z}/n\mathbb{Z}$). Vous pouvez aussi en déduire une démonstration élégante et très rapide que le polynôme minimal de z sur K est irréductible dans $K[X]$. C'est un des isomorphismes les plus utiles de l'algèbre. — Si K' est un autre corps tel que : $K \subseteq K' \subseteq L$, quelle relation peut-on donner entre $\pi_{z,K}$ et $\pi_{z,K'}$? — Si, au lieu de prendre $z \in L$, on prenait z dans une K-algèbre A quelconque, on pourrait toujours définir l'idéal I, et donc $\pi_{z,K}$. Quelles propriétés se généraliseraient toujours, et lesquelles disparaîtraient ? Cette observation aura une très grande importance en algèbre linéaire. — Toujours en remplaçant L par A : donner une condition suffisante simple pour que le polynôme minimal existe pour tout $z \in A$ (penser à une condition qui assurerait que le morphisme d'évaluation a un noyau non trivial).

Exemple 8.

✓	— Varier les exemples. Essayer de donner des exemples de polynômes minimaux de degré plus élevé. — Plus généralement, à quelle condition nécessaire et suffisante sur z a-t-on : $\deg(\pi_{z,K}) = 1$? — Pourquoi $X^2 - 2$ est bien irréductible ?
★	En considérant le polynôme minimal de $\sqrt{2}$ sur $\mathbb{Q}$ trouvé : comprendre pourquoi la relation de divisibilité par le polynôme minimal, dans la proposition précédente, est plus instructive que la simple divisibilité par $X - z$. Que nous enseigne la relation $P = \pi_{z,K}Q$, que ne nous enseignerait pas la relation $P = (X - z)Q$?

Exemple 9.

✓	— Et si $\theta \in \pi\mathbb{Z}$, que dire ? — Plus généralement, si $z \in \mathbb{C} \setminus \mathbb{R}$, quel est le polynôme minimal sur $\mathbb{R}$ de z ?
☢	Peut-on de même proposer un polynôme minimal sur $\mathbb{Q}$ de $e^{i\theta}$?

Remarque.

★	Essayer de construire une « dérivation » sur $\mathbb{Z}$, c'est-à-dire une application $d : \mathbb{Z} \to \mathbb{C}$ additive et vérifiant : $\delta(ab) = a\delta(b) + \delta(a)b$, pour tout $(a, b) \in \mathbb{Z}^2$. Qu'en pensez-vous ? Peut-on imiter la dérivation sur $K[X]$?
☢	Contrairement à ce que j'affirme, il y a bien une sorte de généralisation de la propriété vis-à-vis de l'évaluation : si A est un anneau principal (pour simplifier) contenant $\mathbb{Z}$, et si p est un élément irréductible de A, montrer que $pA \cap \mathbb{Z}$ est un idéal de $\mathbb{Z}$ engendré par un nombre premier q, et que p divise $a \in \mathbb{Z}$ si et seulement si q divise a. Pourquoi est-ce un analogue de la propriété du polynôme minimal ?

Exemple 10.

★	Démontrer ce résultat sans recourir aux polynômes minimaux, pour apprécier la valeur ajoutée du polynôme minimal quand on veut démontrer des relations de divisibilité.

Exemple 11.

✓	Vérifier les réductions que je n'ai pas détaillées en cours (le fait de pouvoir supposer P, Q et R premiers entre eux deux à deux, et que R est le polynôme de degré maximal).
☢	Démontrer cet autre énoncé qui est résolu dans $\mathbb{C}[X]$ mais un problème ouvert important dans $\mathbb{Z}$ (et qui implique d'ailleurs le dernier théorème de Fermat) : pour tous polynômes P, Q et R de $\mathbb{C}[X]$ premiers entre eux tels que : $P+Q=R$, on a : $\max(\deg(P),\deg(Q),\deg(R)) \leqslant N-1$, où N est le nombre de racines distinctes de PQR (théorème de Mason-Stothers). L'analogue entier s'appelle la *conjecture abc* et est l'une des conjectures les plus importantes de l'arithmétique, avec l'hypothèse de Riemann et le problème de Langlands. Ne pas croire l'annonce récente que le mathématicien japonais Mochizuki l'aurait démontrée.

Après votre révision de cette partie

1. Bien cerner les subtilités de l'irréductibilité dans $K[X]$, en évitant toutes les généralisations hâtives (concernant le lien avec le degré et les racines).
2. Faire les *Savoir-faire à vérifier* sur l'arithmétique des polynômes.

2 Savoir-faire à vérifier

Les principaux acquis à vérifier sont :

Arithmétique des entiers.

✓ 1. Démontrer qu'un entier est inversible modulo n et calculer son inverse. **(C)** ☐

✓ 2. Résoudre un système de congruence. **(C)** ☐

★ 3. Utiliser le théorème de Bézout en dehors d'un calcul d'inverse. ☐

★ 4. Utiliser le théorème chinois en dehors d'une résolution de système de congruence. ☐

☢ 5. Exploiter la structure cyclique de $(\mathbb{Z}/p\mathbb{Z})^\times$. (📄) ☐

☢ 6. Résoudre une équation diophantienne où figurent des carrés ou des cubes. ☐

☢ 7. Compter le nombre de solutions d'une équation modulo p. (📄) ☐

On veillera à revoir également ces acquis du chapitre III, que nous enrichissons ici d'exemples supplémentaires :

★ 8. Utiliser le théorème de Fermat, d'Euler ou de Lagrange pour simplifier des puissances. (📄) ☐

Arithmétique des polynômes.

✓ 1. Décomposer un polynôme de $\mathbb{R}[X]$ ou $\mathbb{C}[X]$ en facteurs irréductibles. ☐

✓ 2. Donner une relation de Bézout entre deux polynômes. ☐

★ 3. Montrer qu'un polynôme de $\mathbb{Q}[X]$ de degré raisonnable est irréductible. ☐

★ 4. Déterminer le polynôme minimal d'un nombre algébrique, cas simples. ☐

★ 5. Calculer l'inverse d'un élément de $\mathbb{Q}[\alpha]$, cas algébrique. (📄) ☐

On veillera à revoir également ces acquis du chapitre III (je vous y renvoie pour les exemples) :

✓ 6. Déterminer des automorphismes de corps en dimension finie. (📄) ☐

L'icône « (📄) » signifie que les documents *Méthodes* donnent des compléments sur ces savoir-faire.
La lettre « C » indique que la *Banque des Cent* contient ou contiendra des exercices exerçant à ce savoir-faire.

Arithmétique des entiers

✓ Démontrer qu'un entier est inversible modulo n et calculer son inverse.

Exemples.

1. Montrer que 20 est inversible modulo 37, et calculer son inverse.
2. Résoudre l'équation polynomiale : $\bar{x}^2 + \bar{x} - \bar{8} = \bar{0}$, d'inconnue $\bar{x} \in \mathbb{Z}/17\mathbb{Z}$.
3. Calculer l'inverse de -8 modulo 3^5.

✓ Résoudre un système de congruence.

Exemples. Résoudre les systèmes de congruence suivants, d'inconnue $x \in \mathbb{Z}$:

(a) $\left\{ \begin{array}{rcl} x & \equiv & 3 \bmod 17, \\ x & \equiv & 2 \bmod 31, \end{array} \right.$ (b) $\left\{ \begin{array}{rcl} x & \equiv & -1 \bmod 11, \\ 2x & \equiv & 4 \bmod 8, \\ 3x & \equiv & 1 \bmod 5, \end{array} \right.$ (c) $\left\{ \begin{array}{rcl} x & \equiv & 1 \bmod 48, \\ x & \equiv & 2 \bmod 15, \end{array} \right.$ (d) $\left\{ \begin{array}{rcl} x & \equiv & 3 \bmod 8, \\ x & \equiv & -1 \bmod 6. \end{array} \right.$

★ Utiliser le théorème de Bézout en dehors d'un calcul d'inverse.

Exemples. Soit p un nombre premier.

1. Donner la bijection réciproque de l'application $\bar{x} \mapsto \bar{x}^3$, définie de $\mathbb{Z}/23\mathbb{Z}$ dans lui-même.
2. Soient $\bar{x}$ un élément de $(\mathbb{Z}/p\mathbb{Z})^\times$ et k un nombre premier avec $p-1$. Montrer : $\langle \bar{x} \rangle = \langle \bar{x}^k \rangle$.
3. Soient P et Q deux polynômes à coefficients entiers, premiers entre eux. Montrer que pour tout nombre premier p en dehors d'un ensemble fini, ces deux polynômes n'ont pas de racine en commun dans $\mathbb{Z}/p\mathbb{Z}$.

★ Utiliser le théorème chinois en dehors d'une résolution de système de congruence.

Exemples.

1. Donner le nombre de solutions de l'équation : $\bar{x}^2 = -\bar{1}$, d'inconnue $\bar{x} \in \mathbb{Z}/130\mathbb{Z}$.
2. Soit $n \in \mathbb{N} \setminus \{0\}$. On suppose : $n = \prod_{i=1}^{r} p_i^{\alpha_i}$, où les p_i sont des nombres premiers distincts et les α_i des entiers naturels non nuls. Décrire les éléments nilpotents de $\mathbb{Z}/n\mathbb{Z}$.
3. On pose : $n = pq$. Soient $e \in \mathbb{N}$ un entier premier avec $\varphi(n)$ et $d \in \mathbb{N}$ un représentant de l'inverse de e modulo $\varphi(n)$. Montrer que $\bar{x} \mapsto \bar{x}^e$ et $\bar{x} \mapsto \bar{x}^d$, définies de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$, sont réciproques l'une de l'autre.

☢ Exploiter la structure cyclique de $(\mathbb{Z}/p\mathbb{Z})^\times$.

Exemples. Soient p et q des nombres premiers impairs et distincts.

1. Donner le nombre de solutions de l'équation : $\bar{x}^3 = \bar{1}$, d'inconnue $\bar{x} \in \mathbb{Z}/p\mathbb{Z}$. En déduire que $-\bar{3}$ est le carré d'un élément de $\mathbb{Z}/p\mathbb{Z}$ si et seulement si : $p \equiv 1 \bmod 3$, ou : $p = 3$.
2. On suppose : $p \equiv 1 \bmod 4$. Montrer que $(\mathbb{Z}/p\mathbb{Z})^\times$ possède un unique sous-groupe de cardinal $\frac{p-1}{4}$, et que ses éléments sont exactement les puissances quatrièmes des éléments non nuls de $\mathbb{Z}/p\mathbb{Z}$.
3. On suppose : $p \equiv 1 \bmod 4$. Montrer que -1 est un carré modulo p.
4. Montrer qu'il existe un unique morphisme non trivial de $(\mathbb{Z}/p\mathbb{Z})^\times$ dans $\{-1,1\}$, et que son noyau est exactement dans l'ensemble des carrés de $(\mathbb{Z}/p\mathbb{Z})^\times$. Il est souvent noté $\left(\frac{\cdot}{p}\right)$ et appelé *symbole de Legendre*.
5. On pose : $n = pq$. Donner l'ordre maximal d'un élément de $(\mathbb{Z}/n\mathbb{Z})^\times$. Est-ce un groupe cyclique ?

☢ Résoudre une équation diophantienne où figurent des carrés ou des cubes.

Exemples.

1. Montrer que l'équation : $x^2 - 37y^2 = 19$, d'inconnue $(x, y) \in \mathbb{Z}^2$, n'a pas de solution.
2. Montrer que l'équation : $\sum_{i=1}^{15} x_i^4 = 7936$, d'inconnue $(x_i)_{1 \leqslant i \leqslant 15} \in \mathbb{Z}^{15}$, n'a pas de solution.

3. Résoudre l'équation : $3^x - 2^y = 1$, d'inconnue $(x, y) \in \mathbb{N}^2$.
4. Montrer que l'équation : $x^2 - 3y^2 = 1$, d'inconnue $(x, y) \in \mathbb{Z}^2$, a une infinité de solutions.
5. Résoudre l'équation : $y^2 = x^3 - 2$, d'inconnue $(x, y) \in \mathbb{Z}^2$, en utilisant l'anneau $\mathbb{Z}[i\sqrt{2}] = \left\{a + i\sqrt{2}b \mid (a, b) \in \mathbb{Z}^2\right\}$.

☢ Compter le nombre de solutions d'une équation modulo p.

Exemple. Soit p un nombre premier impair. Compter le nombre de solutions de l'équation : $\bar{x}^2 - \bar{y}^2 = \bar{1}$, d'inconnue $(\bar{x}, \bar{y}) \in (\mathbb{Z}/p\mathbb{Z})^2$.

★ Utiliser le théorème de Fermat, d'Euler ou de Lagrange pour simplifier des puissances.

Exemples. Calculer 10^{1234} modulo 7, puis modulo 77, puis modulo 28.

Arithmétique des polynômes

✓ Décomposer un polynôme de $\mathbb{R}[X]$ ou $\mathbb{C}[X]$ en facteurs irréductibles.

Exemples. Décomposer en facteurs irréductibles les polynômes suivants, dans $\mathbb{C}[X]$ et $\mathbb{R}[X]$:

$$\text{(a)} \quad X^6 - 1, \quad \text{(b)} \quad X^4 + 1, \quad \text{(c)} \quad X^3 + X^2 - 2X - 8.$$

✓ Donner une relation de Bézout entre deux polynômes.

Exemples.

1. Écrire une relation de Bézout entre $X^3 - 1$ et $X^5 - 1$.
2. Écrire une relation de Bézout entre $X^3 - 6X^2 + 11X - 6$ et $X^3 - 1$.
3. Écrire une relation de Bézout entre $X^2 - X + 1$ et $X^4 + 1$.

★ Montrer qu'un polynôme de $\mathbb{Q}[X]$ de degré raisonnable est irréductible.

Exemples. Montrer que les polynômes suivants sont irréductibles dans $\mathbb{Q}[X]$:

$$\text{(a)} \quad X^3 + 2X^2 - 3X + 5, \quad \text{(b)} \quad X^4 + 1.$$

★ Déterminer le polynôme minimal d'un nombre algébrique, cas simples.

Exemples. Déterminer les polynômes minimaux sur $\mathbb{Q}$ de $2 + 3i$, $\sqrt[3]{5}$ et $\sqrt{2} - \sqrt{3}$.

★ Calculer l'inverse d'un élément de $\mathbb{Q}[\alpha]$, cas algébrique.

Exemple. Soit α une racine de $P = X^3 + 2X^2 + 2X + 2$. Simplifier $\dfrac{1}{3\alpha^2 + \alpha + 5}$, de sorte à l'écrire sous la forme $a\alpha^2 + b\alpha + c$ avec $(a, b, c) \in \mathbb{Q}^3$.

Arithmétique des entiers

✓ Démontrer qu'un entier est inversible modulo n et calculer son inverse. □

Réponse.

1. Comme 37 est un nombre premier, toute classe non nulle modulo 37 est inversible, donc $\overline{20}$ l'est. Déterminons son inverse en trouvant une relation de Bézout entre 37 et 20. On applique l'algorithme d'Euclide étendu :

$$\begin{cases} 37 &= 20 \times 1 + 17, \\ 20 &= 17 \times 1 + 3, \\ 17 &= 3 \times 5 + 2, \\ 3 &= 2 \times 1 + 1. \end{cases}$$

En remontant l'algorithme, on obtient :

$$\begin{aligned} 1 = 3 - 2 \times 1 = (20 - 17) - (17 - 3 \times 5) &= (20 - (37 - 20)) - ((37 - 20) - (20 - 17) \times 5) \\ &= (20 - (37 - 20)) - ((37 - 20) - (20 - (37 - 20)) \times 5)\,, \end{aligned}$$

c'est-à-dire : $1 = 37 \times (-7) + 20 \times 13$. En réduisant modulo 37, cela donne : $\overline{1} = \overline{20} \times \overline{13}$, donc l'inverse recherché est : $\overline{20}^{-1} = \overline{13}$.

2. La méthode est la même que dans $\mathbb{R}$ ou $\mathbb{C}$: l'important est simplement être dans un corps (pour inverser $\bar{2}$, et pour utiliser l'intégrité). Nous allons mettre sous forme canonique le polynôme. Soit $\bar{x} \in \mathbb{Z}/17\mathbb{Z}$. On a :

$$\bar{x}^2 + \bar{x} - \bar{8} = \bar{x}^2 + \bar{2}(\bar{2}^{-1}\bar{x}) + (\bar{2}^{-1})^2 - (\bar{2}^{-1})^2 - \bar{8} = \left(\bar{x} + \bar{2}^{-1}\right)^2 - (\bar{2}^{-1})^2 - \bar{8}.$$

Pour poursuivre, nous devons calculer l'inverse de $\bar{2}$. Il n'est pas difficile d'observer que : $\bar{2} \times \bar{9} = \overline{18} = \bar{1}$, donc : $\bar{2}^{-1} = \bar{9} = -\bar{8}$. On en déduit : $\left(\bar{2}^{-1}\right)^2 = (-\bar{8})^2 = \overline{64} = -\bar{4}$. On peut donc poursuivre :

$$\bar{x}^2 + \bar{x} - \bar{8} = \left(\bar{x} - \bar{8}\right)^2 - \bar{4} = \left(\bar{x} - \bar{8} - \bar{2}\right)\left(\bar{x} - \bar{8} + \bar{2}\right) = \left(\bar{x} - \overline{10}\right)\left(\bar{x} - \bar{6}\right).$$

Comme $\mathbb{Z}/17\mathbb{Z}$ est intègre (17 est un nombre premier), on peut conclure :

$$\bar{x}^2 + \bar{x} - \bar{8} = \bar{0} \iff \bar{x} \in \left\{\overline{10}, \bar{6}\right\}.$$

Remarque. En généralisant ce qu'on vient de faire, vous observerez qu'une équation polynomiale du second degré admet des solutions dans $\mathbb{Z}/p\mathbb{Z}$, avec p premier impair, si et seulement si son discriminant est un carré modulo p.

3. On pourrait procéder comme dans le premier exemple plus haut. Je choisis néanmoins de procéder autrement, pour tirer profit du fait que : $-\bar{8} = \bar{1} - \bar{9}$, avec $\bar{9}^3 = \bar{3}^6 = \bar{0}$. Il est alors facile de démontrer, en s'inspirant de la démonstration de l'identité bien connue : $(1-x)^{-1} = \sum_{n=0}^{+\infty} x^n$, que l'on a :

$$\left(-\bar{8}\right)^{-1} = (\bar{1} - \bar{9})^{-1} = \bar{1} + \bar{9} + \bar{9}^2 = \overline{91}.$$

✓ Résoudre un système de congruence. □

Réponse. Soit $x \in \mathbb{Z}$.

(a) Système de congruence $x \equiv 3 \bmod 17$ et $x \equiv 2 \bmod 31$. Comme 17 et 31 sont premiers entre eux, on peut utiliser le théorème chinois (et plus précisément l'isomorphisme réciproque de ce théorème) pour résoudre ce système de congruence. Trouvons une relation de Bézout entre ces deux entiers, grâce à l'algorithme d'Euclide étendu :

$$\begin{cases} 31 &= 17 \times 1 + 14, \\ 17 &= 14 \times 1 + 3, \\ 14 &= 3 \times 4 + 2, \\ 3 &= 2 \times 1 + 1. \end{cases}$$

En remontant l'algorithme, on obtient :

$$\begin{aligned} 1 = 3 - 2 \times 1 = (17 - 14) - (14 - 3 \times 4) &= (17 - (31 - 17)) - ((31 - 17) - (17 - 14) \times 4) \\ &= (17 - (31 - 17)) - ((31 - 17) - (17 - (31 - 17)) \times 4)\,, \end{aligned}$$

c'est-à-dire : $1 = 17 \times 11 + 31 \times (-6)$. L'isomorphisme réciproque du théorème chinois est donc défini par : $(a \bmod 17, b \bmod 31) \mapsto 187b - 186a \bmod 31 \times 17$. On peut conclure :

$$\begin{cases} x & \equiv & 3 \bmod 17 \\ x & \equiv & 2 \bmod 31 \end{cases} \iff x \equiv 187 \times 2 - 186 \times 3 \equiv 343 \bmod 527.$$

(b) Système de congruence $x \equiv -1 \bmod 11$, $2x \equiv 4 \bmod 8$ *et* $3x \equiv 1 \bmod 5$. Comme 5, 8 et 11 sont premiers entre eux deux à deux, on peut utiliser le théorème chinois. Nous allons cependant simplifier la deuxième ligne : le fait que 2 ne soit pas inversible modulo 8 peut nous embêter. On y remédie en notant que :

$$2x \equiv 4 \bmod 8 \iff \exists k \in \mathbb{Z},\ 2x = 4 + 8k \iff \exists k \in \mathbb{Z},\ x = 2 + 4k \iff x \equiv 2 \bmod 4.$$

De plus, l'inverse de 3 modulo 5 est 2, donc le système de congruence à résoudre est équivalent à :

$$\begin{cases} x & \equiv & -1 \bmod 11, \\ x & \equiv & 2 \bmod 4, \\ x & \equiv & 2 \bmod 5. \end{cases}$$

On le résout de proche en proche. Une relation de Bézout entre 11 et 4 est clairement : $11 \times (-1) + 4 \times 3 = 1$. On en déduit que l'isomorphisme réciproque du théorème chinois est ici : $(a \bmod 11, b \bmod 4) \mapsto -11b + 12a \bmod 44$. Ainsi :

$$\begin{cases} x & \equiv & -1 \bmod 11 \\ x & \equiv & 2 \bmod 4 \\ x & \equiv & 2 \bmod 5 \end{cases} \iff \begin{cases} x & \equiv & -34 \bmod 44 \\ x & \equiv & 2 \bmod 5 \end{cases} \iff \begin{cases} x & \equiv & 10 \bmod 44, \\ x & \equiv & 2 \bmod 5. \end{cases}$$

Une relation de Bézout entre 44 et 5 est : $44 \times (-1) + 5 \times 9 = 1$. Donc l'isomorphisme réciproque du théorème chinois est ici : $(a \bmod 44, b \bmod 5) \mapsto -44b + 45a \bmod 220$. On conclut :

$$\begin{cases} x & \equiv & -1 \bmod 11 \\ x & \equiv & 2 \bmod 4 \\ x & \equiv & 2 \bmod 5 \end{cases} \iff x \equiv -88 + 450 \bmod 220 \iff x \equiv -78 \bmod 220.$$

(c) Système de congruence $x \equiv 1 \bmod 48$ *et* $x \equiv 2 \bmod 15$. En réduisant les deux congruences modulo 3 (ce qui est possible puisque 3 divise 48 et 15), on obtient : $x \equiv 1 \bmod 3$, et : $x \equiv 2 \bmod 3$. C'est impossible. Donc ce système de congruence n'admet pas de solution.

(d) Système de congruence $x \equiv 3 \bmod 8$ *et* $x \equiv -1 \bmod 6$. Comme $6 = 2 \times 3$, avec 2 et 3 premiers entre eux, le théorème chinois assure l'équivalence :

$$\begin{cases} x & \equiv & 3 \bmod 8 \\ x & \equiv & -1 \bmod 6 \end{cases} \iff \begin{cases} x & \equiv & 3 \bmod 8 \\ x & \equiv & -1 \bmod 2 \\ x & \equiv & -1 \bmod 3 \end{cases}$$

La deuxième ligne est redondante : si $x \equiv 3 \bmod 8$ alors, en réduisant modulo 2 (ce qui est possible car 2 divise 8), on a : $x \equiv 1 \equiv -1 \bmod 2$. Le système de congruence à résoudre est donc équivalent à :

$$\begin{cases} x & \equiv & 3 \bmod 8, \\ x & \equiv & -1 \bmod 3. \end{cases}$$

Une relation de Bézout entre 8 et 3 étant : $8 \times (-1) + 3 \times 3 = 1$, l'isomorphisme réciproque du théorème chinois est : $(a \bmod 8, b \bmod 3) \mapsto -8b + 9a \bmod 24$. On conclut :

$$\begin{cases} x & \equiv & 3 \bmod 8, \\ x & \equiv & -1 \bmod 3. \end{cases} \iff x \equiv 8 + 27 \equiv 11 \bmod 24.$$

★ Utiliser le théorème de Bézout en dehors d'un calcul d'inverse. □

Réponse.

1. De la même manière que la réciproque de $x \mapsto x^3$, comme fonction de la variable réelle, est $x \mapsto x^{1/3}$, il est tentant de penser que la même application, vue de $\mathbb{Z}/23\mathbb{Z}$ dans elle-même, admet pour réciproque une fonction puissance dont l'exposant est l'inverse de 3... mais modulo quel entier ?

   Comme nous allons le voir, il faut prendre pour exposant l'inverse de 3 modulo 22 : cela permettra de tirer profit du petit théorème de Fermat. Calculons cet inverse. Une relation de Bézout entre 22 et 3 est : $22 \times 1 + 3 \times (-7) = 1$. On en déduit : $3 \times (-7) \equiv 1 \bmod 22$, et comme : $-7 \equiv 15 \bmod 22$, il existe $k \in \mathbb{N}$ tel que : $3 \times 15 = 1 + 22k$ (pourquoi

me ramené-je à un exposant positif ? réfléchir à ce qui poserait problème ci-dessous). Pour tout $\bar{x} \in (\mathbb{Z}/23\mathbb{Z})^\times$ on a donc, par le petit théorème de Fermat :

$$\left(\bar{x}^3\right)^{15} = \bar{x}^{3\times 15} = \bar{x}^{1+22\times k} = \bar{x} \cdot \left(\bar{x}^{22}\right)^k = \bar{x},$$

et de même : $\left(\bar{x}^{15}\right)^3 = \bar{x}$. Pour $\bar{x} = \bar{0}$ l'égalité reste trivialement vraie, donc la bijection réciproque de $\bar{x} \mapsto \bar{x}^3$ est $\bar{x} \mapsto \bar{x}^{15}$.

Remarque. Bien comprendre pourquoi il serait correct d'écrire, pour x inversible : $x^{22\times 1+3\times(-7)} \equiv x^{3\times(-7)} \bmod 23$, bien que $x^{3\times(-7)}$ ne soit pas un entier *a priori* : il ne peut pas être réduit modulo 23 ! Cette question vaut plus généralement pour toute manipulation d'exposants négatifs modulo n.

Remarque. Il y a une autre raison de penser que la réciproque d'une fonction puissance bijective, de $\mathbb{Z}/23\mathbb{Z}$ dans $\mathbb{Z}/23\mathbb{Z}$, est toujours une fonction puissance, ce qui motive d'autant plus l'heuristique ci-dessus : si $f : \bar{x} \mapsto \bar{x}^3$ est une bijection de $\mathbb{Z}/23\mathbb{Z}$ dans lui-même, c'est un élément de $S_{\mathbb{Z}/23\mathbb{Z}}$ qui est de cardinal fini 23!. Par le théorème de Lagrange : $f^{23!} = \mathrm{Id}$, donc : $f^{-1} = f^{23!-1}$ (et la réciproque de f est donc la fonction puissance $\bar{x} \mapsto \bar{x}^{3^{23!-1}}$). Cependant l'exposant obtenu avec le raisonnement ci-dessus est largement plus petit.

2. Tout d'abord, il est clair que : $\bar{x}^k \in \langle \bar{x} \rangle$, donc par minimalité du groupe engendré par $\bar{x}^k$ on a : $\left\langle \bar{x}^k \right\rangle \subseteq \langle \bar{x} \rangle$. Justifions l'inclusion réciproque. Pour cela, il suffit de montrer : $\bar{x} \in \left\langle \bar{x}^k \right\rangle$. On veut « inverser » la relation entre $\bar{x}^k$ et $\bar{x}$ (c'est $\bar{x}^k$ qui s'exprime en fonction de $\bar{x}$, et on veut l'inverse). Comme souvent, c'est une relation de Bézout qui le permet. Pour voir comment : comme k est premier avec $p-1$, il existe $(u, v) \in \mathbb{Z}^2$ tel que : $uk + v(p-1) = 1$. Alors : $\bar{x} = \bar{x}^1 = \bar{x}^{uk+v(p-1)} = \left(\bar{x}^k\right)^u \left(\bar{x}^{p-1}\right)^v$. Par le petit théorème de Fermat : $\bar{x}^{p-1} = \bar{1}$, donc finalement : $\bar{x} = \left(\bar{x}^k\right)^u \in \left\langle \bar{x}^k \right\rangle$, d'où : $\langle \bar{x} \rangle \subseteq \left\langle \bar{x}^k \right\rangle$. Ceci achève de montrer : $\langle \bar{x} \rangle = \left\langle \bar{x}^k \right\rangle$.
On a montré que si k est premier avec $p-1$, alors $\bar{x}$ et $\bar{x}^k$ ont même ordre.

3. Comme P et Q sont premiers entre eux dans $\mathbb{Q}[X]$, il existe $(U, V) \in \mathbb{Q}[X]^2$ tel que : $UP + VQ = 1$. Quitte à multiplier cette égalité par un entier convenable (le ppcm des dénominateurs des coefficients de U et V), on a l'existence de $d \in \mathbb{Z} \setminus \{0\}$ et $(U_0, V_0) \in \mathbb{Z}[X]^2$ tels que : $U_0 P + V_0 Q = d$. Soit S l'ensemble des nombres premiers divisant d, et considérons un nombre premier p qui N'EST PAS dans S (il en existe, puisque S est un ensemble fini et qu'il existe une infinité de nombres premiers). Alors, quand on réduit modulo p l'égalité ci-dessus, ce qui est possible puisque tous les polynômes sont à coefficients entiers, on obtient : $\overline{U_0} \cdot \overline{P} + \overline{V_0} \cdot \overline{Q} = \bar{d}$. Cela permet de démontrer ce qui est demandé : s'il existe une racine commune $\bar{a} \in \mathbb{Z}/p\mathbb{Z}$ à $\overline{P}$ et $\overline{Q}$, alors évaluer en $\bar{a}$ l'égalité précédente donnerait : $\bar{0} = \bar{d}$, et donc p diviserait d : faux par hypothèse sur p. Par l'absurde, $\overline{P}$ et $\overline{Q}$ n'admettent pas de racine commune dans $\mathbb{Z}/p\mathbb{Z}$ (en fait, par la réciproque du théorème de Bézout, on a bien mieux : ils sont premiers entre eux dans $\mathbb{Z}/p\mathbb{Z}[X]$).

Remarque. On a illustré là un aspect remarquable de l'universalité des polynômes et des relations de Bézout (elles traduisent algébriquement une propriété arithmétique, c'est-à-dire en des égalités où l'on peut évaluer, réduire modulo un entier, etc.), qui permettent de transférer des égalités valables dans $\mathbb{Z}[X]$ à presque n'importe quel anneau.

Remarque. Comme $\mathbb{Z}[X]$ n'est pas principal ($\mathbb{Z}$ n'est pas un corps), on ne peut pas utiliser de relation de Bézout avec des polynômes de $\mathbb{Z}[X]$. Cette contrainte ne peut pas être levée.

★ Utiliser le théorème chinois en dehors d'une résolution de système de congruence. □

Réponse.

1. Soit $\bar{x} \in \mathbb{Z}/130\mathbb{Z}$. On a : $130 = 2 \cdot 5 \cdot 13$. Par le théorème chinois, on a donc l'équivalence :

$$\bar{x}^2 = -\bar{1} \iff \begin{cases} x^2 \equiv -1 \bmod 2, \\ x^2 \equiv -1 \bmod 5, \\ x^2 \equiv -1 \bmod 13. \end{cases} \iff \begin{cases} x^2 \equiv 1 \bmod 2, \\ x^2 \equiv 4 \bmod 5, \\ x^2 \equiv 25 \bmod 13. \end{cases}$$

J'ai changé les représentants afin de faciliter l'extraction de racines carrées, puisque : $1 = 1^2$, $4 = 2^2$, et : $25 = 5^2$. Comme $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z}$ et $\mathbb{Z}/13\mathbb{Z}$ sont intègres, on a :

$$\bar{x}^2 = -\bar{1} \iff \exists (\varepsilon_1, \varepsilon_2) \in \{-1,1\}^2, \begin{cases} x \equiv 1 \bmod 2, \\ x \equiv \varepsilon_1 2 \bmod 5, \\ x \equiv \varepsilon_2 5 \bmod 13. \end{cases}$$

(Bien comprendre pourquoi l'intégrité est essentielle : tout passer dans le membre de gauche, factoriser, etc. Noter que $1 \equiv -1 \bmod 2$.)
Cela fournit quatre solutions de l'équation : $\bar{x}^2 = -\bar{1}$, dans $\mathbb{Z}/130\mathbb{Z}$. On peut les expliciter, quitte à utiliser l'isomorphisme réciproque du théorème chinois. Ce sont les classes : $\bar{1}$, $-\bar{1}$, $\overline{57}$ et $-\overline{57}$.

Remarque. Si on ne trouve pas à tâtons une racine carrée de -1 modulo 13 par exemple, rappelons qu'un exercice de travaux dirigés vous fait montrer que, si p est un nombre premier congru à 1 modulo 4, alors :

$-1 \equiv \left(\left(\frac{p-1}{2}\right)!\right)^2 \bmod p$. Cela fournit une racine carrée explicite (c'est hélas très rapidement calculatoire, mais on ne peut guère faire mieux en classes préparatoires). Un autre algorithme, « probabiliste » : prendre un nombre au hasard entre -6 et 6 (éviter 0 et ± 1), et l'élever à la puissance 6 modulo 13. Il a une chance sur deux de donner -1 (pourquoi ?). Si ce n'est pas le cas, retenter avec un autre nombre. Si c'est le cas : ce nombre à la puissance 3 est une racine carrée de -1 modulo 13.

2. Soit $\bar{x} \in \mathbb{Z}/n\mathbb{Z}$. Par le théorème chinois, on a :

$$\exists k \in \mathbb{N},\ \bar{x}^k = \bar{0} \iff \exists k \in \mathbb{N},\ \forall i \in [\![1, r]\!],\ x^k \equiv 0 \bmod p_i^{\alpha_i} \iff \forall i \in [\![1, r]\!],\ \exists k_i \in \mathbb{N},\ x^{k_i} \equiv 0 \bmod p_i^{\alpha_i}.$$

Justifions la dernière équivalence : le sens direct est évident, et pour le sens réciproque il suffit de poser : $k = \max_{1 \leqslant i \leqslant r} k_i$.

Ainsi on est ramené à déterminer les éléments nilpotents de $\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$ pour tout $i \in [\![1, r]\!]$. Soient $i \in [\![1, r]\!]$ et $k_i \in \mathbb{N}$. Notons d'abord que si x modulo $p_i^{\alpha_i}$ est nilpotent, alors il n'est pas inversible dans $\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$, et donc il n'est pas premier avec $p_i^{\alpha_i}$: on en déduit que x est un multiple de p_i. Réciproquement, soit $m_i \in \mathbb{Z}$ tel que : $x = m_i p_i$. Alors : $x^{\alpha_i} = m_i^{\alpha_i} p_i^{\alpha_i} \equiv 0 \bmod p_i^{\alpha_i}$, donc x modulo $p_i^{\alpha_i}$ est nilpotent si et seulement si p_i divise x. On en déduit :

$$\exists k \in \mathbb{N},\ \bar{x}^k = \bar{0} \iff \forall i \in [\![1, r]\!],\ p_i | x \iff \mathrm{ppcm}(p_1, \ldots, p_r) | x \iff p_1 \cdots p_r | x.$$

En conclusion : les éléments nilpotents de $\mathbb{Z}/n\mathbb{Z}$ sont les classes des multiples de $\prod_{i=1}^{r} p_i$.

3. On doit montrer : $\forall \bar{x} \in \mathbb{Z}/n\mathbb{Z}$, $\left(\bar{x}^d\right)^e = \left(\bar{x}^e\right)^d = \bar{x}^{de} = \bar{x}$. Tout d'abord, notons que par définition de d, on a : $de \equiv 1 \bmod \varphi(n)$, donc il existe $k \in \mathbb{Z}$ tel que : $de = 1 + k\varphi(n) = 1 + k(p-1)(q-1)$. Donc : $\forall \bar{x} \in \mathbb{Z}/n\mathbb{Z}$, $\bar{x}^{de} = \bar{x}^{1+k(p-1)(q-1)}$. Pour simplifier cela, nous allons raisonner modulo p et q.

Raisonnons d'abord modulo p. Si p ne divise pas x alors, par le petit théorème de Fermat : $x^{de} \equiv x \cdot \left(x^{p-1}\right)^{k(q-1)} \equiv x \bmod p$. Si p divise x, alors $x^{de} \equiv 0 \bmod p$ et $x \equiv 0 \bmod p$, donc on a $x^{de} \equiv x \bmod p$ dans tous les cas.

Raisonnement analogue modulo q. Puisque l'on a : $x^{de} \equiv x$ modulo p et q, par le théorème chinois on a : $x^{de} \equiv x \bmod n$. D'où le résultat.

☢ Exploiter la structure cyclique de $(\mathbb{Z}/p\mathbb{Z})^\times$. □

Réponse.

1. On nous demande de donner le nombre d'éléments d'ordre divisant 3 dans $(\mathbb{Z}/p\mathbb{Z})^\times$. Comme $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique, on sait que l'ensemble des éléments dont l'ordre divise 3 est exactement l'unique sous-groupe de cardinal 3 si 3 divise $p-1$, et c'est l'ensemble $\{\bar{1}\}$ sinon (par le théorème de Lagrange) : si 3 divise $p-1$, il y a donc trois solutions à l'équation : $\bar{x}^3 = \bar{1}$, d'inconnue $\bar{x} \in (\mathbb{Z}/p\mathbb{Z})^\times$ (et comme $\bar{0}$ n'est pas solution, cela donne aussi les solutions dans $\mathbb{Z}/p\mathbb{Z}$). Si 3 ne divise pas $p-1$, il n'y en a qu'une seule.
   Or : $\bar{x}^3 = \bar{1} \iff (\bar{x}-\bar{1})(\bar{x}^2+\bar{x}+\bar{1}) = \bar{0} \iff \bar{x} = \bar{1}$ ou $\bar{x}^2+\bar{x}+\bar{1} = \bar{0}$. Le fait que l'équation $\bar{x}^3 = \bar{1}$ ait trois solutions équivaut donc au fait que $\bar{x}^2+\bar{x}+\bar{1}$ en ait deux, et donc au fait que le discriminant de $X^2+X+\bar{1}$ soit un carré non nul. Or ce discriminant vaut : $-\bar{3}$. Par ce qui précède, $-\bar{3}$ est un carré non nul si et seulement si 3 divise $p-1$, si et seulement si : $p \equiv 1 \bmod 3$.
   Il reste le cas où $-\bar{3} = \bar{0}^2$: c'est vrai si et seulement si $p = 3$.
   Remarque. On peut se passer de la structure cyclique ici (ce qui a l'avantage d'éviter le recours à un gros théorème hors programme). Il suffit pour cela d'utiliser le théorème de Lagrange pour démontrer que $X^{p-1}-\bar{1}$ est scindé à racines simples : $X^{p-1}-\bar{1} = \prod_{\bar{k}\in(\mathbb{Z}/p\mathbb{Z})^\times} (X-\bar{k})$. Or, si 3 divise $p-1$, alors $X^3-\bar{1}$ divise $X^{p-1}-\bar{1}$ en vertu de l'égalité : $X^{p-1}-\bar{1} = (X^3-\bar{1}) \sum_{i=0}^{(p-1)/3-1} X^{3k}$. Par unicité de la décomposition en facteurs irréductibles, $X^3-\bar{1}$ doit être scindé et à racines simples : il admet donc trois racines, d'où le résultat.
2. Comme $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique, pour tout diviseur d de $p-1$ il existe un unique sous-groupe de cardinal $\frac{p-1}{d}$: c'est le groupe engendré par $\bar{g}^d$, où $\bar{g}$ est un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$. Or, par hypothèse sur p, l'entier 4 divise $p-1$, donc il existe un unique sous-groupe G de cardinal $\frac{p-1}{4}$, qui est engendré par $\bar{g}^4$. Comme ses éléments sont de la forme $\left(\bar{g}^4\right)^k = \left(\bar{g}^k\right)^4$, ce sont tous des puissances quatrièmes d'éléments de $(\mathbb{Z}/p\mathbb{Z})^\times$, et réciproquement toutes les puissances quatrièmes de ce groupe sont dans G : en effet, si $\bar{x} \in (\mathbb{Z}/p\mathbb{Z})^\times$ est une puissance quatrième d'un élément de $(\mathbb{Z}/p\mathbb{Z})^\times$, alors il existe $\bar{y} \in (\mathbb{Z}/p\mathbb{Z})^\times$ tel que : $\bar{x} = \bar{y}^4$, et alors : $\bar{x}^{\frac{p-1}{4}} = \bar{y}^{p-1} = \bar{1}$, donc $\bar{x}$ appartient à G (rappelons que ce fut également démontré lorsqu'on a explicité la structure des sous-groupes de $(\mathbb{Z}/n\mathbb{Z},+)$: l'unique sous-groupe de cardinal d, pour d divisant n, est exactement l'ensemble des éléments d'ordre divisant d ; on l'applique ici avec $d = \frac{p-1}{4}$, en ne perdant pas de vue qu'ici la loi est multiplicative). Ayant montré l'inclusion réciproque : G est exactement l'ensemble des puissances quatrièmes de $(\mathbb{Z}/p\mathbb{Z})^\times$.
3. Soit $\bar{g}$ un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$. Il en existe car c'est un groupe cyclique. On a : $\bar{g}^{p-1} = \bar{1}$, donc : $\left(\bar{g}^{\frac{p-1}{2}}-\bar{1}\right)\left(\bar{g}^{\frac{p-1}{2}}+\bar{1}\right) = \bar{0}$. Or : $g^{\frac{p-1}{2}} \neq \bar{1}$ (sinon $\bar{g}$ serait d'ordre divisant $\frac{p-1}{2}$ et non d'ordre $p-1$), donc par intégrité de $\mathbb{Z}/p\mathbb{Z}$ on a : $\bar{g}^{\frac{p-1}{2}} = -\bar{1}$. Comme $\frac{p-1}{2}$ est pair par hypothèse sur p, cela peut se réécrire : $-\bar{1} = \left(\bar{g}^{\frac{p-1}{4}}\right)^2$, ce qui démontre bien que -1 est un carré modulo p.
   Remarque. Réciproquement, si -1 est un carré modulo p alors $p \equiv 1 \bmod 4$ ou $p = 2$. Ce sens est plus facile à montrer (en élevant à la puissance $\frac{p-1}{2}$ une égalité du type $-\bar{1} = \bar{x}^2$).
4. Comme $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique, il existe un générateur $\bar{g}$ de ce groupe, et un morphisme f de $(\mathbb{Z}/p\mathbb{Z})^\times$ dans $\{-1,1\}$ est entièrement caractérisé par l'image de $\bar{g}$. Il y a deux possibilités : soit $f(\bar{g}) = 1$, et dans ce cas f est le morphisme trivial (puisqu'il coïncide avec lui sur un générateur), soit $f(\bar{g}) = -1$ (et dans ce cas f n'est pas trivial).
   Réciproquement, l'application $f : \bar{g}^k \mapsto (-1)^k$ est correctement définie, puisqu'elle ne dépend pas de la façon d'écrire un élément de $(\mathbb{Z}/p\mathbb{Z})^\times$ sous la forme : $\bar{x} = \bar{g}^k$. En effet, si $\bar{x} = \bar{g}^k = \bar{g}^\ell$ avec k et ℓ deux entiers, alors : $\bar{g}^{k-\ell} = \bar{1}$, donc l'ordre de $\bar{g}$, c'est-à-dire $p-1$, divise $k-\ell$. Il existe donc $m \in \mathbb{Z}$ tel que : $k = \ell + m(p-1)$. On a alors : $(-1)^k = (-1)^\ell(-1)^{m(p-1)}$, et comme $p-1$ est pair il en résulte : $(-1)^k = (-1)^\ell$. Bref, l'application f est correctement définie et est clairement un morphisme de groupes de $(\mathbb{Z}/p\mathbb{Z})^\times$ dans $\{-1,1\}$. On a bien montré l'existence et l'unicité.
   Son noyau est de cardinal $\frac{p-1}{2}$: cela revient à compter les classes $\bar{k}$ qui sont paires dans $\mathbb{Z}/(p-1)\mathbb{Z}$. Il est plus précisément égal à : $\langle\bar{g}^2\rangle$, ce qui permet de se convaincre que $\ker(f)$ est inclus dans l'ensemble des carrés de $(\mathbb{Z}/p\mathbb{Z})^\times$. Réciproquement, si $\bar{x} \in (\mathbb{Z}/p\mathbb{Z})^\times$, et s'il existe $\bar{y} \in (\mathbb{Z}/p\mathbb{Z})^\times$ tel que : $\bar{x} = \bar{y}^2$, alors : $\bar{x}^{\frac{p-1}{2}} = \bar{y}^{p-1} = \bar{1}$, donc $\bar{x}$ est inclus dans l'unique sous-groupe de cardinal $\frac{p-1}{2}$ de $(\mathbb{Z}/p\mathbb{Z})^\times$ (c'est la structure cyclique qui nous l'enseigne : l'unique sous-groupe de cardinal $\frac{p-1}{2}$ est exactement l'ensemble des éléments dont l'ordre divise $\frac{p-1}{2}$), or ce sous-groupe est $\ker(f)$ d'après ce qui précède. On a donc l'inclusion réciproque, et $\ker(f)$ est exactement l'ensemble des carrés de $(\mathbb{Z}/p\mathbb{Z})^\times$.
   Remarque. On montre plus classiquement l'existence de ce morphisme sans recourir à la structure cyclique, mais en étudiant l'image de $\bar{x} \mapsto \bar{x}^2$ et le noyau de $\bar{x} \mapsto \bar{x}^{\frac{p-1}{2}}$.
5. Par le théorème chinois, déterminer l'ordre maximal d'un élément de $(\mathbb{Z}/n\mathbb{Z})^\times$ revient à déterminer l'ordre maximal d'un élément de $(\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times$.

Remarquons que $x^{p-1} \equiv 1 \bmod p$ et $x^{q-1} \equiv 1 \bmod q$ pour tout $x \in \mathbb{Z}$ inversible modulo n. Alors, si l'on prend pour exposant un multiple à la fois de $p-1$ et $q-1$, disons leur ppcm qu'on note m, on a :

$$(x^m \bmod p-1, x^m \bmod q-1) = (1 \bmod p-1, 1 \bmod q-1),$$

donc par unicité dans le théorème chinois on a : $x^m \bmod n \equiv 1 \bmod n$. Tout élément de $(\mathbb{Z}/n\mathbb{Z})^\times$ est donc d'ordre divisant $m = \text{ppcm}(p-1, q-1)$, donc tout ordre d vérifie $d \leqslant \text{ppcm}(p-1, q-1)$.

Montrons l'inégalité inverse : soient $\bar{\omega}_p$ un élément d'ordre $p-1$ dans $(\mathbb{Z}/p\mathbb{Z})^\times$ et $\bar{\omega}_q$ un élément d'ordre $q-1$ dans $(\mathbb{Z}/q\mathbb{Z})^\times$ (de tels éléments existent parce que ces groupes sont cycliques). Grâce à l'existence des solutions à tout système de congruence modulo p et q (d'après le théorème chinois), il existe $\bar{x} \in (\mathbb{Z}/n\mathbb{Z})^\times$ tel que : $(x \bmod p, x \bmod q) = (\omega_p \bmod p, \omega_q \bmod q)$, ce qui signifie que $\bar{x}$ est d'ordre $p-1$ dans $(\mathbb{Z}/p\mathbb{Z})^\times$ et d'ordre $q-1$ dans $(\mathbb{Z}/q\mathbb{Z})^\times$. Soit d' son ordre dans $(\mathbb{Z}/n\mathbb{Z})^\times$; alors $x^{d'} \equiv 1 \bmod n$ implique $x^{d'} \equiv 1 \bmod p$ et $x^{d'} \equiv 1 \bmod q$. On en déduit que l'ordre de $\bar{x}$ dans $(\mathbb{Z}/p\mathbb{Z})^\times$ et l'ordre de $\bar{x}$ dans $(\mathbb{Z}/q\mathbb{Z})^\times$ divisent d', c'est-à-dire : $p-1$ et $q-1$ divisent d'. Ainsi d' est un multiple commun à $p-1$ et $q-1$, donc par définition du ppcm m divise d'. On en déduit : $\text{ppcm}(p-1, q-1) \leqslant d'$. L'inégalité inverse fut démontrée tantôt, donc : $d' = \text{ppcm}(p-1, q-1)$.

L'ordre maximal d'un élément de $(\mathbb{Z}/n\mathbb{Z})^\times$ est donc $\text{ppcm}(p-1, q-1)$ (puisque tout autre ordre doit le diviser donc lui être inférieur, d'après ce qui précède). Notons qu'on a aussi démontré que l'ordre de tout élément divise l'ordre maximal : c'est un cas particulier d'un résultat valable dans tout groupe commutatif fini.

Concluons : $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique si et seulement si : $\text{ppcm}(p-1, q-1) = \text{card}((\mathbb{Z}/n\mathbb{Z})^\times) = (p-1)(q-1)$, si et seulement si $p-1$ et $q-1$ sont premiers entre eux. Mais, si p et q sont des nombres premiers impairs, alors $p-1$ et $q-1$ sont tous les deux pairs, donc ils ne sont pas premiers entre eux : on en déduit que $(\mathbb{Z}/n\mathbb{Z})^\times$ n'est pas cyclique.

☢ Résoudre une équation diophantienne où figurent des carrés ou des cubes. □

Réponse. Pour la plupart de ces résolutions, on réduit l'équation modulo un entier bien choisi, afin de profiter du fait que les carrés, cubes, etc., soient en nombre fini et faciles à décrire. Pour avoir une intuition du bon choix des modules, encore faut-il avoir une connaissance fine du nombre de carrés, cubes, etc., modulo chaque entier, et idéalement les connaître explicitement. À cet égard, il est souvent utile de connaître à quelle condition nécessaire et suffisante -1 est un carré modulo p.

1. Soit $(x, y) \in \mathbb{Z}^2$. On suppose : $x^2 - 37y^2 = 19$. On réduit cette égalité modulo 19. On obtient : $\bar{x}^2 + \bar{y}^2 = \bar{0}$, donc : $\bar{x}^2 = -\bar{y}^2$. On en déduit que si $\bar{x}$ ou $\bar{y}$ est nul, alors l'autre classe aussi, donc x et y sont divisibles par 19. Donc x^2 et y^2 sont divisibles par 19^2. Mais dans ce cas, l'égalité : $x^2 - 37y^2 = 19$, réduite modulo 19^2, donne : $0 \equiv 19 \bmod 19^2$, ce qui est faux. On en déduit que ni $\bar{x}$, ni $\bar{y}$ n'est nul. Comme 19 est premier, $\mathbb{Z}/19\mathbb{Z}$ est un corps, donc $\bar{y}$ est inversible : l'égalité $\bar{x}^2 = -\bar{y}^2$ équivaut donc à : $(\bar{x}\bar{y}^{-1})^2 = -\bar{1}$, donc $-\bar{1}$ est un carré dans $(\mathbb{Z}/19\mathbb{Z})^\times$. C'est impossible puisque : $19 \equiv 3 \bmod 4$. Redémontrons pourquoi : il suffit d'élever à la puissance 9 l'égalité précédente. On a alors : $-\bar{1} = (-\bar{1})^9 = (\bar{x}\bar{y}^{-1})^{18} = \bar{1}$ (petit théorème de Fermat), donc : $\bar{2} = \bar{0}$. C'est impossible puisque 19 ne divise pas 2.

   Dans tous les cas on a une absurdité, donc l'équation : $x^2 - 37y^2 = 19$, d'inconnue $(x, y) \in \mathbb{Z}^2$, n'a pas de solution.

2. Soit $(x_i)_{1 \leqslant i \leqslant 15} \in \mathbb{Z}^{15}$. On suppose : $\sum_{i=1}^{15} x_i^4 = 7936$. Comme : $7936 = 8000 - 64 = 16 \cdot 500 - 16 \cdot 4$, réduire cette égalité modulo 16 donne : $\sum_{i=1}^{15} x_i^4 \equiv 0 \bmod 16$. Or les seuls puissances quatrièmes modulo 16 sont $\bar{0} = \bar{0}^4 = (\pm\bar{2})^4 = (\pm\bar{4})^4 = (\pm\bar{6})^4 = \bar{8}^4$ et $\bar{1} = (\pm\bar{1})^4 = (\pm\bar{3})^4 = (\pm\bar{5})^4 = (\pm\bar{7})^4$ (savoir que $(\mathbb{Z}/2^4\mathbb{Z})^\times$ est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ permet d'avoir ce résultat immédiatement, mais cela nécessite plus de recul et, surtout, un résultat très largement hors programme). Le seul moyen d'obtenir zéro modulo 16 en sommant quinze $\bar{0}$ ou $\bar{1}$ est d'avoir uniquement des zéros, donc : $\forall i \in [\![1,15]\!]$, $x_i^4 \equiv 0 \bmod 16$. D'après notre description des puissances ci-dessus, cela signifie que tous les x_i sont pairs. Pour tout $i \in [\![1,15]\!]$, écrivons donc : $x_i = 2k_i$, avec k_i entier. L'équation : $\sum_{i=1}^{15} x_i^4 = 7936$, devient après simplifications : $\sum_{i=1}^{15} k_i^4 = 496$. En réduisant modulo 16, on obtient encore : $\sum_{i=1}^{15} k_i^4 \equiv 0 \bmod 16$, donc par le même raisonnement on parvient à l'existence d'entiers $m_1, \ldots, m_{15}$ tels que : $\sum_{i=1}^{15} m_i^4 = 31$. À ce stade, deux façons de conclure :

   — du fait que $3^4 = 81$, aucun des m_i ne peut être strictement supérieur à 2 ; de plus, vu que : $2^4 = 16$, on voit qu'il est impossible d'avoir deux entiers m_i supérieurs ou égaux à 2 en valeur absolue ; mais s'il y en a au plus un (avec, donc, tous les autres inférieurs ou égaux à 1 en valeur absolue), alors : $\sum_{i=1}^{15} m_i^4 \leqslant 2^4 + 14 \cdot 1^4 = 30 < 31$, ce qui est impossible ;

— ou bien on s'amuse encore à réduire modulo 16, pour avoir : $\sum_{i=1}^{15} m_i^4 \equiv 15 \bmod 16$: ce n'est possible d'obtenir cette égalité que si tous les m_i^4 sont égaux à 1 modulo 16 (vu qu'ils valent soit 0, soit 1), et donc si tous les m_i sont des entiers impairs (d'après la description des bicarrés donnée ci-dessus) ; or les plus petits entiers impairs (en valeur absolue) sont 1 et 3 : comme dans la première méthode ci-dessus, il est impossible que l'un d'eux soit supérieur ou égal à 3, donc tous les m_i sont égaux à 1 en valeur absolue ; dans ce cas, on a : $\sum_{i=1}^{15} m_i^4 = 15 \neq 31$, et c'est absurde.

On a montré qu'il n'existe pas de solution à l'équation : $\sum_{i=1}^{15} x_i^4 = 7936$.

Remarque. Pour savoir comment j'ai été amené à réduire modulo 16 : d'abord, il s'agissait de réduire modulo un diviseur de $7936 = 2^8 \cdot 31$ pour se ramener à un bête problème combinatoire (puisqu'il n'y a qu'un nombre fini de puissances quatrièmes modulo n). Pour savoir quel module choisir, il vaut mieux prendre un module suffisamment petit pour que les calculs soient simples et qu'il y ait peu de puissances quatrièmes (pour qu'on puisse rapidement énumérer toutes les possibilités, et résoudre l'équation par recensement exhaustif), mais aussi suffisamment grand pour que l'égalité voulue soit réellement contraignante, et laisse peu de possibilités de valeurs des x_i. Il y a beaucoup trop de puissances quatrièmes modulo 31 (il y en a $\frac{30}{\text{pgcd}(4,30)} = 15$, comme on peut le montrer en étudiant l'image de $\bar{x} \mapsto \bar{x}^4$ ou grâce à la structure cyclique de $(\mathbb{Z}/31\mathbb{Z})^\times$), donc on exclut cette étude. Pour choisir la puissance de 2 à laquelle réduire l'équation : modulo 2, 4 ou 8, cela laisse trop de possibilités. Par exemple, si j'avais réduit modulo 8, j'aurais été contrarié au moment d'interpréter les situations qui donnent : $\sum_{i=1}^{15} x_i^4 \equiv 0 \bmod 8$. Cela se produit si tous les x_i^4 sont égaux à 0 modulo 8, mais aussi si huit d'entre eux sont égaux à 1 (et les autres à 0). Avoir un second cas (par ailleurs difficile à résoudre) alourdit considérablement le raisonnement ci-dessus. Si j'avais voulu effectuer le raisonnement ci-dessus, mais modulo 8, j'aurais pu avoir jusqu'à quatre cas différents à traiter (selon que sept x_i ou les quinze soient pairs, puis selon que sept k_i ou les quinze sont pairs). Voilà pourquoi je n'ai pas voulu suivre cette idée. Si j'avais voulu réduire modulo 32 ou davantage, alors les puissances quatrièmes n'auraient pas toutes été égales à $\bar{0}$ ou $\bar{1}$ (par exemple : $3^4 = 81 \equiv 17 \bmod 32$) et il y aurait encore eu trop de cas à considérer. Voilà pourquoi 16 était le meilleur choix.

3. Soit $(x,y) \in \mathbb{N}^2$. Supposons : $3^x - 2^y = 1$. En réduisant modulo 3 cette équation, on a : $(-1)^y \equiv -1 \bmod 3$, donc y est un entier impair (en particulier, $y \geqslant 1$). Si $y = 1$, alors $3^x = 1 + 2^1$ est vérifié pour $x = 1$. Supposons à présent $y \neq 1$. En particulier : $y \geqslant 3$. Donc 2^y est divisible par 4, et réduire modulo 4 l'équation donne : $(-1)^x \equiv 1 \bmod 4$, donc x est pair. Écrivons : $x = 2k$, avec $k \in \mathbb{N} \setminus \{0\}$. On a : $2^y = 3^x - 1 = (3^k - 1)(3^k + 1)$. Par unicité de la décomposition en facteurs premiers, il existe donc $\ell \in \mathbb{N}$ tel que : $3^k - 1 = 2^\ell$, et : $3^k + 1 = 2^{y-\ell}$. On a logiquement : $\ell < y - \ell$. Mais alors : $2 = (3^k + 1) - (3^k - 1) = 2^{y-\ell} - 2^\ell = 2^\ell(2^{y-2\ell} - 1)$. Comme 2 est un nombre premier, ceci impose : $2^{y-2\ell} - 1 = 1$, et : $2^\ell = 2$. À partir de là, on conclut facilement que $\ell = 1$ et $y = 3$. On a déterminé y. Pour avoir x, on rappelle que l'on a : $3^x = 1 + 2^y = 9$, donc : $x = 2$. Réciproquement, $(x,y) = (2,3)$ est bien solution.

   En conclusion, cette équation diophantienne admet deux solutions : (1,1) et (2,3).

4. Notons déjà que l'équation $x^2 - 3y^2 = 1$, d'inconnue $(x,y) \in \mathbb{Z}^2$, admet au moins une solution non triviale (i.e. différente de (1,0)), à savoir : $(x,y) = (2,1)$. La clé est d'observer que cette solution suffit à en engendrer d'autres par exponentiation (phénomène très fréquent pour les équations de la forme $x^2 - dy^2 = 1$).
   En effet, si $(x,y) \in \mathbb{Z}^2$, alors :
   $$x^2 - 3y^2 = 1 \iff \mathrm{N}(x + \sqrt{3}y) = 1,$$
   où N est l'application définie sur $\mathbb{Z}[\sqrt{3}] = \left\{a + \sqrt{3}b \mid (a,b) \in \mathbb{Z}^2\right\}$ et à valeurs dans $\mathbb{Z}$, qui à $a + \sqrt{3}b$ associe $a^2 - 3b^2 = (a + \sqrt{3}b)(a - \sqrt{3}b)$. L'intérêt de cette réécriture est que la fonction N est multiplicative : pour tout $(x,y,x',y') \in \mathbb{Z}^4$, on a : $\mathrm{N}((x + \sqrt{3}y)(x' + \sqrt{3}y')) = \mathrm{N}(x + \sqrt{3}y)\mathrm{N}(x' + \sqrt{3}y')$. Cela se démontre grâce au fait que l'application $a + \sqrt{3}b \mapsto a - \sqrt{3}b$ est un automorphisme d'anneaux de $\mathbb{Z}[\sqrt{3}]$ dans lui-même, comme vous pouvez le vérifier aisément. Cela implique en particulier : $\forall n \in \mathbb{N}$, $\mathrm{N}\left((2 + \sqrt{3})^n\right) = \mathrm{N}\left(2 + \sqrt{3}\right)^n = 1^n = 1$. Par conséquent, si l'on note, pour tout $n \in \mathbb{N}$, les entiers a_n et b_n tels que : $(2 + \sqrt{3})^n = a_n + \sqrt{3}b_n$ (on peut les expliciter *via* la formule du binôme de Newton, où l'on regroupe les puissances paires et les puissances impaires de $\sqrt{3}$), alors $(a_n, b_n) \in \mathbb{Z}^2$ est solution de l'équation $x^2 - 3y^2 = 1$ pour tout $n \in \mathbb{N}$, d'après l'équivalence ci-dessus. Cela fournit une infinité de solutions, puisqu'on vérifie sans peine que $(a_n)_{n \geqslant 0}$ tend vers l'infini (on a en effet, par la formule du binôme de Newton : $a_n \geqslant 2^n$) : d'où le résultat.

   Remarque. On peut montrer (mais c'est difficile) que les solutions de cette équation sont exactement celles obtenues par cette méthode. Pour $n = 2$, on a par exemple : $(2 + \sqrt{3})^2 = 7 + 4\sqrt{3}$, et on vérifie que (7,4) est effectivement solution de : $x^2 - 3y^2 = 1$.

   Remarque. On peut également inclure les puissances négatives.

5. Avant d'utiliser l'indication de l'énoncé, notons que si x et y sont solutions, alors ils doivent être tous les deux impairs. En effet, si x est pair (par exemple), alors $y^2 \equiv 0 \bmod 2$, donc $y \equiv 0 \bmod 2$ (car $\mathbb{Z}/2\mathbb{Z}$ est intègre), et y

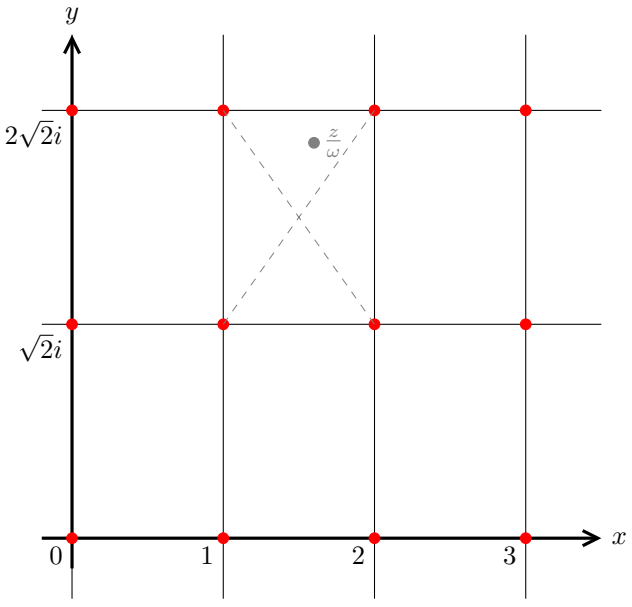
est aussi pair. Mais c'est absurde : l'équation $y^2 = x^3 - 2$ donnerait, modulo 4, l'égalité : $0 \equiv -2 \bmod 4$. De même si y est pair. Par l'absurde, x et y sont impairs.
Pour poursuivre, on utilise l'indication de l'énoncé, qui n'est exploitable que si $\mathbb{Z}[i\sqrt{2}]$ est un anneau principal (afin d'y faire de l'arithmétique). Admettons-le *provisoirement*, afin de comprendre en quoi cela nous permet de résoudre cette équation. Si $(x, y) \in \mathbb{Z}^2$ vérifie : $y^2 = x^3 - 2$, alors on a également :

$$(y + i\sqrt{2})(y - i\sqrt{2}) = x^3.$$

Démontrons que les deux facteurs du membre de gauche sont premiers entre eux. Si $d \in \mathbb{Z}[i\sqrt{2}]$ divise $y + i\sqrt{2}$ et $y - i\sqrt{2}$, alors il divise la différence $-2i\sqrt{2} = (i\sqrt{2})^3$. Or $i\sqrt{2}$ est irréductible dans $\mathbb{Z}[i\sqrt{2}]$ (car l'égalité $i\sqrt{2} = ab$, avec $(a, b) \in \mathbb{Z}[i\sqrt{2}]^2$, implique : $2 = |a|^2|b|^2$, et comme $|a|^2$ et $|b|^2$ sont des entiers naturels on a par exemple : $|a|^2 = 1$, ce qui n'est possible dans $\mathbb{Z}[i\sqrt{2}]$ que si $a = \pm 1$ est inversible), donc l'unicité de la décomposition en facteurs premiers dans $\mathbb{Z}[i\sqrt{2}]$ implique qu'il existe $u \in \mathbb{Z}[i\sqrt{2}]^\times$ et $k \in [\![0,3]\!]$ tels que : $d = u(i\sqrt{2})^k$. Justifions que $k = 0$: si $k \geqslant 1$ alors, du fait que d divise $y + i\sqrt{2}$ et $y - i\sqrt{2}$, son carré d^2 divise leur produit, c'est-à-dire x^3 ; or : $d^2 = u^2(i\sqrt{2})^{2k} = (-1)^k u^2 2^k$: par conséquent, si $k \geqslant 1$, alors 2 divise x^3 dans $\mathbb{Z}[i\sqrt{2}]$ (et donc aussi dans $\mathbb{Z}$, en prenant la partie réelle dans une relation de divisibilité entre 2 et x^3), et donc x est pair. C'est impossible, on a affirmé tantôt que x est impair ! Par l'absurde : $k = 0$, donc $d = u$ est inversible.
Ainsi $y + i\sqrt{2}$ et $y - i\sqrt{2}$ sont premiers entre eux, et leur produit est un cube, donc ils sont eux-mêmes des cubes (raisonner sur la décomposition en facteurs irréductibles de x^3, et de $y \pm i\sqrt{2}$, pour le comprendre). Soit $(a, b) \in \mathbb{Z}^2$ tel que : $y + i\sqrt{2} = (a + i\sqrt{2}b)^3$. En développant cette puissance et en identifiant parties réelles et imaginaires, on obtient :

$$y = a^3 - 6ab^2 = a(a^2 - 6b^2), \quad 1 = 3a^2b - 2b^3 = b(3a^2 - 2b^2).$$

Partant de là, on déduit : $b = 1$, $a^2 = \frac{1+2b^2}{3} = 1$, le cas $b = -1$ étant impossible (sinon on aurait $a^2 = \frac{1}{3} \notin \mathbb{Z}$) et il n'est plus difficile d'en déduire que les solutions $(x, y) \in \mathbb{Z}^2$ de l'équation initiale sont (3,5) et $(3, -5)$ (la réciproque est triviale).
Pour que cette résolution soit licite, il faut s'assurer que $\mathbb{Z}[i\sqrt{2}]$ est en effet principal (le fait que ce soit un anneau commutatif et intègre étant facile à vérifier). On y parvient en démontrant l'existence d'une division euclidienne : soient $z = a + i\sqrt{2}b \in \mathbb{Z}[i\sqrt{2}]$ et $\omega = c + i\sqrt{2}d \in \mathbb{Z}[i\sqrt{2}]$. On suppose ω non nul. Montrons l'existence de $(q, r) \in \mathbb{Z}[i\sqrt{2}]^2$ tel que : $z = \omega q + r$, avec : $|r| < |\omega|$. Pour cela, on note que si q et r conviennent, on a : $\left|q - \frac{z}{\omega}\right| = \left|\frac{r}{\omega}\right| < 1$. Il s'agit de montrer qu'il est possible de choisir ainsi q. Quitte à faire une multiplication convenable par le conjugué, on peut écrire : $\frac{z}{\omega} = x + i\sqrt{2}y$, avec $(x, y) \in \mathbb{Q}^2$. C'est cette quantité qu'on veut approcher au mieux par q. Une observation graphique semble indiquer comment faire (les éléments de $\mathbb{Z}[i\sqrt{2}]$ sont les points de concours des arêtes du quadrillage) : la distance entre $\frac{z}{\omega}$, et l'un des quatre sommets du rectangle le contenant, est inférieure ou égale à la longueur d'une demi-diagonale, c'est-à-dire $\frac{\sqrt{1^2+\sqrt{2}^2}}{2} = \frac{\sqrt{3}}{2} < 1$:



Concrètement : soit x' un entier tel que : $|x - x'| \leqslant \frac{1}{2}$, et de même soit y' un entier tel que : $|y - y'| \leqslant \frac{1}{2}$: il en existe. Ce sont les entiers les plus proches de x et y. Vérifions que $q = x + iy$ et $r = z - \omega q$ conviennent. On a évidemment : $z = \omega q + r$, et surtout :

$$|r| = |\omega| \left|\frac{z}{\omega} - q\right| = |\omega| \left|(x - x') + i\sqrt{2}(y - y')\right| = |\omega|\sqrt{(x - x')^2 + 2(y - y')^2} \leqslant |\omega|\sqrt{\frac{1}{4} + 2\frac{1}{4}} = \frac{\sqrt{3}}{2}|\omega| < |\omega|,$$

d'où l'existence d'une division euclidienne. Une fois celle-ci établie, montrer que $\mathbb{Z}[i\sqrt{2}]$ est principal suit la même stratégie que pour $\mathbb{Z}$ et $K[X]$: soit I un idéal de $\mathbb{Z}[i\sqrt{2}]$. Si $I = \{0\}$ alors il n'y a rien à raconter. Supposons donc : $I \neq \{0\}$. L'ensemble $\left\{|\omega|^2 \mid \omega \in I \setminus \{0\}\right\}$ est une partie de $\mathbb{N}$ non vide puisque $I \neq \{0\}$, donc elle admet un plus petit élément : soit ω un élément de $I \setminus \{0\}$ qui réalise ce minimum. Montrons que ω engendre I. Soit $z \in I$. Par ce qui précède, il existe $(q, r) \in \mathbb{Z}[i\sqrt{2}]^2$ tel que : $z = \omega q + r$, et : $|r| < |\omega|$. Le fait que q et z soient dans I, qui est un idéal, implique : $r = z - \omega q \in I$. Ainsi r est un élément de I tel que : $|r|^2 < |\omega|^2$: cela impose $r = 0$, sinon la minimalité de $|\omega|^2$ serait contredite. Ainsi : $z = \omega q \in \omega\mathbb{Z}[i\sqrt{2}]$, donc : $I \subseteq \omega\mathbb{Z}[i\sqrt{2}]$. L'inclusion réciproque est évidente par propriété d'absorption d'un idéal, d'où : $I = \omega\mathbb{Z}[i\sqrt{2}]$. Tous les idéaux de $\mathbb{Z}[i\sqrt{2}]$ sont principaux, ce qu'il restait à démontrer.

☢ Compter le nombre de solutions d'une équation modulo p. □

Réponse. Nous allons compter le nombre de solutions de l'équation : $\bar{x}^2 - \bar{y}^2 = \bar{1}$, d'inconnue $(\bar{x}, \bar{y}) \in (\mathbb{Z}/p\mathbb{Z})^2$, par plusieurs méthodes différentes. La première est la plus rapide et simple, mais la moins généralisable. Nous vous recommandons de faire d'abord des exercices sur les sommes de Gauß ou le symbole de Legendre auparavant, ou de lire *Méthodes* aux pages consacrées. Autrement, la stratégie de décompte vous paraîtra obscure.

Première méthode : avec un changement de variable. Soit $(x, y) \in \mathbb{Z}^2$. On a : $\bar{x}^2 - \bar{y}^2 = \bar{1} \iff (\bar{x} - \bar{y})(\bar{x} + \bar{y}) = \bar{1}$. On en déduit que l'application $(\bar{x}, \bar{y}) \mapsto (\bar{x} - \bar{y}, \bar{x} + \bar{y})$, définie sur $\{(\bar{x}, \bar{y}) \in (\mathbb{Z}/p\mathbb{Z})^2 \mid \bar{x}^2 - \bar{y}^2 = \bar{1}\}$ et à valeurs dans $\{(\bar{u}, \bar{v}) \in (\mathbb{Z}/p\mathbb{Z})^2 \mid \bar{u}\bar{v} = \bar{1}\}$, est correctement définie. Elle est bijective puisqu'elle admet pour réciproque $(\bar{u}, \bar{v}) \mapsto \left(\bar{2}^{-1}(\bar{v} + \bar{u}), \bar{2}^{-1}(\bar{v} - \bar{u})\right)$. Ainsi il revient au même de compter les solutions de : $\bar{u}\bar{v} = \bar{1}$, d'inconnue $(\bar{u}, \bar{v}) \in (\mathbb{Z}/p\mathbb{Z})^2$. C'est trivial : il suffit de compter les $\bar{u}$ inversibles (il y en a $p - 1$: ce sont les éléments de $(\mathbb{Z}/p\mathbb{Z})^\times$) et de prendre $\bar{v} = \bar{u}^{-1}$. Ainsi il y a $p - 1$ solutions à cette équation, et donc $p - 1$ à l'équation initiale $\bar{x}^2 - \bar{y}^2 = \bar{1}$.

Deuxième méthode : avec le symbole de Legendre. On note que si $(x, y) \in \mathbb{Z}^2$, alors $\bar{x}^2 - \bar{y}^2 = \bar{1}$ si et seulement si : $\bar{y}^2 = \bar{x}^2 - \bar{1}$, si et seulement si $\bar{x}^2 - \bar{1}$ est un carré (et dans ce cas, il y a deux valeurs de $\bar{y}$ qui conviennent, sauf si $\bar{x}^2 - \bar{1} = \bar{0}$: c'est ce qui expliquera la disparition du facteur $\frac{1}{2}$ dans le calcul de N ci-dessous). Or on remarque que, si l'on note $\left(\frac{\cdot}{p}\right)$ le symbole de Legendre, on a :

$$\forall \bar{a} \in \mathbb{Z}/p\mathbb{Z}, \quad \frac{1}{2}\left(1 + \left(\frac{a}{p}\right)\right) = \begin{cases} \frac{1}{2} & \text{si} \quad \bar{a} = \bar{0}, \\ 1 & \text{si} \quad \bar{a} \text{ est un carré mod } p, \\ 0 & \text{si} \quad \bar{a} \text{ n'est pas un carré mod } p, \end{cases}$$

donc : $\forall \bar{a} \in (\mathbb{Z}/p\mathbb{Z})^\times$, $\frac{1}{2}\left(1 + \left(\frac{a}{p}\right)\right) = \mathbb{1}_{(\text{carrés}\setminus\{0\})}(a)$. Par conséquent, si l'on note N le nombre de solutions dans $(\mathbb{Z}/p\mathbb{Z})^2$ de : $\bar{x}^2 - \bar{y}^2 = \bar{1}$, on a, en mettant à part les cas $\bar{x} = \pm\bar{1}$ (qui donnent le carré $\bar{0}^2$) :

$$N = 2 + \sum_{\bar{x} \in \mathbb{Z}/p\mathbb{Z}\setminus\{\bar{1}, -\bar{1}\}} \left(1 + \left(\frac{x^2 - 1}{p}\right)\right) = p + \sum_{\bar{x} \in \mathbb{Z}/p\mathbb{Z}\setminus\{\bar{1}, -\bar{1}\}} \left(\frac{x^2 - 1}{p}\right) = p + \sum_{\bar{x} \in \mathbb{Z}/p\mathbb{Z}\setminus\{\bar{1}\}} \left(\frac{x^2 - 1}{p}\right).$$

Pour simplifier cette somme, nous utilisons d'une part la propriété de morphisme du symbole de Legendre, et d'autre part une permutation adéquate afin de se ramener à la somme simplifiable $\sum_{x \in (\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{x}{p}\right)$ (qui vaut zéro et c'est valable en remplaçant le symbole de Legendre par n'importe quel morphisme non trivial : exercice classique). Faisons :

$$N = p + \sum_{\bar{x} \in \mathbb{Z}/p\mathbb{Z}\setminus\{\bar{1}\}} \left(\frac{x^2 - 1}{p}\right) = p + \sum_{\bar{x} \in \mathbb{Z}/p\mathbb{Z}\setminus\{\bar{1}\}} \left(\frac{x - 1}{p}\right)\left(\frac{x + 1}{p}\right) = p + \sum_{\bar{x} \in \mathbb{Z}/p\mathbb{Z}\setminus\{\bar{1}\}} \left(\frac{(x - 1)^{-1}}{p}\right)\left(\frac{x + 1}{p}\right),$$

où $(x - 1)^{-1}$ représente l'inverse de $\bar{x} - \bar{1}$. Cette dernière égalité est valable parce que le symbole de Legendre vaut 1 ou -1, donc il est égal à son inverse. La propriété de morphisme fait le reste. L'intérêt de la manœuvre est de faire apparaître une homographie, dont on sait que c'est bijectif (au contraire de $\bar{x} \mapsto \bar{x}^2 - \bar{1}$ dont on était parti initialement). Plus précisément, l'application $\bar{x} \mapsto (\bar{x} - \bar{1})^{-1}(\bar{x} + \bar{1})$ est une bijection de $\mathbb{Z}/p\mathbb{Z} \setminus \{\bar{1}\}$ dans lui-même, sa réciproque étant $\bar{y} \mapsto (\bar{y} - \bar{1})^{-1}(\bar{y} + \bar{1})$. Donc :

$$N = p + \sum_{\bar{x} \in \mathbb{Z}/p\mathbb{Z}\setminus\{\bar{1}\}} \left(\frac{(x - 1)^{-1}(x + 1)}{p}\right) = p + \sum_{\bar{x} \in \mathbb{Z}/p\mathbb{Z}\setminus\{\bar{1}\}} \left(\frac{x}{p}\right).$$

Or : $\sum_{\bar{x} \in (\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{x}{p}\right) = 0$, parce qu'il y a autant de carrés que de non carrés dans $(\mathbb{Z}/p\mathbb{Z})^\times$ (à savoir $\frac{p-1}{2}$). On peut aussi démontrer cette relation en faisant un changement d'indice grâce à la permutation $\bar{x} \mapsto \bar{a}\bar{x}$, où $\bar{a} \in (\mathbb{Z}/p\mathbb{Z})^\times$ est un *non* carré quelconque fixé. On peut donc conclure :

$$N = p + \sum_{\bar{x} \in \mathbb{Z}/p\mathbb{Z}} \left(\frac{x}{p}\right) - \left(\frac{1}{p}\right) = p - 1.$$

Troisième méthode : avec les sommes de Gauß. On va utiliser la formule d'orthogonalité suivante :

$$\forall (x,y)\in\mathbb{Z}^2,\quad \frac{1}{p}\sum_{k=0}^{p-1}\exp\left(\frac{2i\pi k(x^2-y^2-1)}{p}\right)=\begin{cases}1 & \text{si } x^2-y^2\equiv 1 \bmod p,\\ 0 & \text{si } x^2-y^2\not\equiv 1 \bmod p.\end{cases}$$

Par conséquent, si l'on note N le nombre de solutions dans $(\mathbb{Z}/p\mathbb{Z})^2$ de : $\bar{x}^2-\bar{y}^2=\bar{1}$, on a :

$$\begin{aligned}N&=\sum_{x=0}^{p-1}\sum_{y=0}^{p-1}\frac{1}{p}\sum_{k=0}^{p-1}\exp\left(\frac{2i\pi k(x^2-y^2-1)}{p}\right)\\&=p+\frac{1}{p}\sum_{k=1}^{p-1}\exp\left(-\frac{2i\pi k}{p}\right)\sum_{x=0}^{p-1}\exp\left(\frac{2i\pi kx^2}{p}\right)\sum_{y=0}^{p-1}\exp\left(-\frac{2i\pi ky^2}{p}\right).\end{aligned}$$

Pour poursuivre, nous devons savoir calculer les sommes de Gauß. Nous utilisons sans démonstration des identités qu'il faut bien entendu savoir démontrer si on y recourt (on note $\left(\frac{\cdot}{p}\right)$ le symbole de Legendre) :

$$N=p+\frac{1}{p}\sum_{k=1}^{p-1}\exp\left(-\frac{2i\pi k}{p}\right)\cdot\left(\frac{k}{p}\right)\left(-\frac{k}{p}\right)\left(\frac{-1}{p}\right)p=p+\sum_{k=1}^{p-1}\exp\left(-\frac{2i\pi k}{p}\right)=p-1.$$

★ Utiliser le théorème de Fermat, d'Euler ou de Lagrange pour simplifier des puissances. □

Réponse.

Modulo 7. Comme 7 ne divise pas 10, on a par le petit théorème de Fermat : $10^6\equiv 1 \bmod 7$. Pour simplifier 10^{1234} modulo 7, nous allons effectuer la division euclidienne de 1234 par 6. On trouve : $1234=1200+34=6\cdot 200+6\cdot 5+4=6\cdot 205+4$. On a donc : $10^{1234}=\left(10^6\right)^{205}\cdot 10^4\equiv 10^4\equiv(-3)^4\equiv 9^2\equiv(-2)^2\equiv 4 \bmod 7$.

Modulo 77. Il y a deux façons de traiter ce cas : soit on utilise le théorème d'Euler au lieu du théorème de Fermat, et on imite le raisonnement ci-dessus ; soit on utilise le théorème chinois avec $77=7\cdot 11$ (en effet 7 et 11 sont premiers entre eux) :

— avec le théorème d'Euler : comme 77 est premier avec 10, on a par le théorème d'Euler : $10^{\varphi(77)}=10^{\varphi(7)\varphi(11)}=10^{60}\equiv 1 \bmod 77$, donc l'ordre de 10 dans $(\mathbb{Z}/77\mathbb{Z})^\times$ divise 60 ; or $10^6\equiv 1 \bmod 7$ et $10^6\equiv 1 \bmod 11$, donc par le théorème chinois qu'on utilise finalement ici aussi : $10^6\equiv 1 \bmod 77$; pour simplifier 10^{1234} modulo 77, nous allons effectuer la division euclidienne de 1234 par 6 ; on trouve : $1234=6\cdot 205+4$; on a donc, comme ci-dessus : $10^{1234}\equiv 10^4\equiv 100^2\equiv 23^2\equiv 529\equiv -10 \bmod 77$;

— avec le théorème chinois : on a $10\equiv -1 \bmod 11$, donc : $10^{1234}\equiv(-1)^{1234}\equiv 1 \bmod 11$; or $10^{1234}\equiv 4 \bmod 7$; il suffit donc d'utiliser l'isomorphisme réciproque du théorème chinois pour trouver un antécédent de $(1 \bmod 11, 4 \bmod 7)$, et cela donne la valeur de $10^{1234} \bmod 77$; je court-circuite cette recherche en notant que l'entier 67 vérifie $67\equiv 1 \bmod 11$ et $67\equiv 4 \bmod 7$, donc par unicité de la solution modulo 77 on a : $10^{1234}\equiv 67\equiv -10 \bmod 77$.

Voyez que l'exposant 60 utilisé dans la première méthode peut considérablement être abaissé. Même lorsque le théorème d'Euler fournit une puissance égale à 1, il vaut le coup de chercher (parmi les diviseurs de $\varphi(n)$) s'il y a une puissance plus petite qui convient : cela simplifie les calculs qui suivent !

Modulo 28. On ne peut pas utiliser le théorème d'Euler cette fois-ci, puisque 10 n'est pas premier avec 28 (ils ont 2 pour diviseur commun, qui est aussi leur pgcd). Pas grave : on utilise le théorème chinois, avec : $28=4\cdot 7$, étant donné que 4 et 7 sont premiers entre eux. On a : $10^{1234}=10^2\cdot 10^{1232}\equiv 0 \bmod 4$ (car $100=4\cdot 25$), et : $10^{1234}\equiv 4 \bmod 7$ (calcul effectué ci-dessus), et un entier vérifiant ces deux congruences est évidemment 4, donc par unicité dans le théorème chinois : $10^{1234}\equiv 4 \bmod 28$.

Arithmétique des polynômes

✓ Décomposer un polynôme de $\mathbb{R}[X]$ ou $\mathbb{C}[X]$ en facteurs irréductibles. □

Réponse.

(a) Le polynôme X^6-1. On a, *via* différentes identités remarquables :

$$X^6-1=(X^3-1)(X^3+1)=(X-1)(X^2+X+1)(X+1)(X^2-X+1),$$

et les polynômes $X^2 \pm X + 1$ sont de discriminant $-3 < 0$, donc sans racine réelle et de degré 2 : ils sont irréductibles. On a donc factorisé $X^6 - 1$ sur $\mathbb{C}[X]$. Il reste à calculer les racines complexes de $X^2 \pm X + 1$ pour factoriser le polynôme sur $\mathbb{C}$:

$$X^6 - 1 = (X-1)(X+1)\left(X - \frac{-1+i\sqrt{3}}{2}\right)\left(X - \frac{-1-i\sqrt{3}}{2}\right)\left(X - \frac{1+i\sqrt{3}}{2}\right)\left(X - \frac{1-i\sqrt{3}}{2}\right)$$

On pouvait aussi procéder à l'inverse : trouver les racines complexes de $X^6 - 1$ (ce sont les racines sixièmes de l'unité), puis regrouper chaque racine avec sa conjuguée pour avoir la décomposition sur $\mathbb{R}$.

(b) Le polynôme X^4+1. On peut soit commencer par décomposer dans $\mathbb{C}[X]$ en notant que les racines de X^4+1 sont exactement les racines primitives huitièmes de l'unité, soit commencer par $\mathbb{R}[X]$ en faisant ingénieusement apparaître une identité remarquable :

— avec les racines primitives : pour tout $x \in \mathbb{C}$, on a : $x^4 + 1 = 0$, si et seulement si : $x^4 = -1 = e^{i\pi}$, si et seulement s'il existe $k \in \mathbb{Z}$ tel que : $x = e^{\frac{i\pi}{4} + \frac{2i\pi k}{4}} = e^{\frac{i\pi(2k+1)}{4}}$; cela fournit quatre racines distinctes, à savoir : $e^{\frac{i\pi}{4}}$, $e^{-\frac{i\pi}{4}}$, $e^{\frac{3i\pi}{4}}$, et $e^{-\frac{3i\pi}{4}}$, ce qui permet de factoriser $X^4 + 1$ dans $\mathbb{C}[X]$:

$$X^4 + 1 = \left(X - e^{\frac{i\pi}{4}}\right)\left(X - e^{-\frac{i\pi}{4}}\right)\left(X - e^{\frac{3i\pi}{4}}\right)\left(X - e^{-\frac{3i\pi}{4}}\right),$$

et il suffit de regrouper chaque racine avec sa conjuguée pour avoir une factorisation réelle :

$$\begin{aligned} X^4 + 1 &= \left(X^2 - 2\mathrm{Re}\left(e^{\frac{i\pi}{4}}\right)X + e^{\frac{i\pi}{4}}e^{-\frac{i\pi}{4}}\right)\left(X^2 - 2\mathrm{Re}\left(e^{\frac{3i\pi}{4}}\right)X + e^{\frac{3i\pi}{4}}e^{-\frac{3i\pi}{4}}\right) \\ &= \left(X^2 - \sqrt{2}X + 1\right)\left(X^2 + \sqrt{2}X + 1\right) ; \end{aligned}$$

— avec une identité remarquable : on a $X^4 + 1 = X^4 + 2X^2 + 1 - 2X^2 = (X^2+1)^2 - 2X^2 = (X^2 + 1 - \sqrt{2}X)(X^2 + 1 + \sqrt{2}X)$, et on vérifie que ces deux polynômes ont pour discriminant $-2 < 0$: ils n'ont pas de racine réelle et sont de degré 2, donc ils sont irréductibles dans $\mathbb{R}[X]$; on les décompose dans $\mathbb{C}[X]$ en cherchant leurs racines, et on obtient :

$$X^4 + 1 = \left(X - \frac{\sqrt{2}+i\sqrt{2}}{2}\right)\left(X - \frac{\sqrt{2}-i\sqrt{2}}{2}\right)\left(X - \frac{-\sqrt{2}+i\sqrt{2}}{2}\right)\left(X - \frac{-\sqrt{2}-i\sqrt{2}}{2}\right).$$

On obtient évidemment la même chose par les deux méthodes.

(c) Le polynôme $X^3 + X^2 - 2X - 8$. À tâtons, on trouve que 2 est racine de ce polynôme. On trouve le quotient de X^3+X^2-2X-8 par $X-2$ *via* une division euclidienne, et on en déduit : $X^3+X^2-2X-8 = (X-2)(X^2+3X+4)$. Le discriminant de $X^2 + 3X + 4$ est $-7 < 0$, donc il n'admet pas de racine réelle et est de degré 2 : il est donc irréductible. On a factorisé X^3+X^2-2X-8 dans $\mathbb{R}[X]$. Pour la factorisation dans $\mathbb{C}[X]$, il suffit de calculer les racines X^2+3X+4, et on conclut : $X^3 + X^2 - 2X - 8 = (X-2)\left(X - \frac{-3+i\sqrt{7}}{2}\right)\left(X - \frac{-3-i\sqrt{7}}{2}\right)$.

✓ Donner une relation de Bézout entre deux polynômes. □

Réponse. On utilise l'algorithme d'Euclide étendu dans chaque cas.

1. On a :
$$\left\{\begin{array}{rcl} X^5 - 1 &=& (X^3-1)\times X^2 + X^2 - 1, \\ X^3 - 1 &=& (X^2-1)\times X + X - 1, \\ X^2 - 1 &=& (X-1)\times(X+1) + 0. \end{array}\right.$$
On en déduit d'abord que le pgcd de $X^5 - 1$ et $X^3 - 1$ est $X - 1$. Ensuite, en remontant l'algorithme, on a :
$$X - 1 = X^3 - 1 - (X^2-1)X = X^3 - 1 - \left((X^5-1) - (X^3-1)X^2\right)X = (X^3-1)(X^3+1) + (X^5-1)\cdot(-X).$$
Remarque. Vous observerez que les étapes de l'algorithme d'Euclide sont exactement les mêmes que si on l'applique aux entiers 5 et 3.

2. On a :
$$\left\{\begin{array}{rcl} X^3 - 6X^2 + 11X - 6 &=& (X^3-1)\times 1 - 6X^2 + 11X - 5, \\ X^3 - 1 &=& (-6X^2 + 11X - 5)\times\left(-\frac{1}{6}X - \frac{11}{36}\right) + \frac{91}{36}(X-1), \\ -6X^2 + 11X - 5 &=& \frac{91}{36}(X-1)\times\left(-\frac{216}{91}X + \frac{180}{91}\right) + 0. \end{array}\right.$$
Le pgcd de $X^3 - 6X^2 + 11X - 6$ et $X^3 - 1$ est donc $X - 1$. En remontant l'algorithme :
$$X - 1 = (X^3-1)\cdot\frac{1}{91}(-6X+25) + \left(X^3 - 6X^2 + 11X - 6\right)\cdot\frac{1}{91}(6X+11).$$

3. On a :
$$\left\{\begin{array}{rcl} X^4+1 & = & (X^2-X+1)\times(X^2+X)-X+1,\\ X^2-X+1 & = & (-X+1)\times(-X)+1,\\ -X+1 & = & 1\times(-X+1)+0.\end{array}\right.$$
Le pgcd de X^4+1 et X^2-X+1 est donc 1. En remontant l'algorithme :
$$1=(X^4+1)\cdot X+\left(X^2-X+1\right)\left(-X^3-X^2+1\right).$$

★ Montrer qu'un polynôme de $\mathbb{Q}[X]$ de degré raisonnable est irréductible. □

Réponse.
(a) Le polynôme $P=X^3+2X^2-3X+5$. Comme ce polynôme est de degré 3, il suffit de montrer qu'il n'admet pas de racine rationnelle pour en déduire qu'il est réductible dans $\mathbb{Q}[X]$. Montrons-le par l'absurde : s'il existe p et q deux entiers premiers entre eux tels que $\frac{p}{q}$ soit racine de P, alors : $q^3P\left(\frac{p}{q}\right)=0$. Ceci équivaut à : $p^3+2p^2q-3pq^2+5q^3=0$. En réduisant cette équation modulo p, on a : $5q^3=0 \bmod p$, donc p divise $5q^3$. Or p est premier avec q, donc p divise 5. On a donc : $p\in\{\pm1,\pm5\}$. Le même raisonnement, mais modulo q, montre que q divise 1. Ainsi, si P admet une racine rationnelle, elle est dans l'ensemble $\{\pm1,\pm5\}$. Mais une évaluation de P en ces quatre entiers donne une quantité non nulle, donc P n'admet pas de racine rationnelle. Étant de degré 3 et sans racine rationnelle, c'est donc un polynôme irréductible dans $\mathbb{Q}[X]$.

(b) Le polynôme X^4+1. Tout d'abord, le fait que $x^4+1\geqslant 1$ pour tout $x\in\mathbb{R}$ assure que X^4+1 n'admet pas de racine rationnelle (ni même réelle), donc X^4+1 n'admet pas de facteur irréductible de degré 1 dans $\mathbb{Q}[X]$. Par conséquent, si c'est un polynôme réductible dans $\mathbb{Q}[X]$, il admet deux facteurs irréductibles P et Q dans $\mathbb{Q}[X]$ de degré 2. On l'a dit, X^4+1 n'admet pas de racine réelle, donc P et Q n'en ont pas non plus : étant de degré 2, cela assure qu'ils sont aussi irréductibles dans $\mathbb{R}[X]$. Or on a décomposé X^4+1 en facteurs irréductibles de $\mathbb{R}[X]$ à la page 26 ; par unicité de la décomposition, on a : $P=X^2\pm\sqrt{2}X+1\notin\mathbb{Q}[X]$: absurde. Ceci montre que X^4+1 est irréductible dans $\mathbb{Q}[X]$.

★ Déterminer le polynôme minimal d'un nombre algébrique, cas simples. □

Réponse.
Polynôme minimal de $2+3i$. Le polynôme $(X-2-3i)(X-2+3i)=(X-2)^2+9\in\mathbb{Q}[X]$ admet $2+3i$ pour racine. Il est irréductible dans $\mathbb{Q}[X]$ puisqu'il n'a pas de racine rationnelle et est de degré 2. C'est donc le polynôme minimal de $2+3i$ sur $\mathbb{Q}$.

Polynôme minimal de $\sqrt[3]{5}$. On a : $\sqrt[3]{5}^3=5$, donc $X^3-5\in\mathbb{Q}[X]$ admet $\sqrt[3]{5}$ pour racine. Justifions qu'il est irréductible dans $\mathbb{Q}[X]$: comme il est de degré 3, il suffit pour cela de montrer qu'il n'a pas de racine rationnelle. Or une étude banale de variation montre que $x\mapsto x^3-5$ ne s'annule qu'une seule fois sur $\mathbb{R}$, et c'est en $\sqrt[3]{5}$: justifions que $\sqrt[3]{5}$ n'est pas rationnel en raisonnant par l'absurde. S'il existe deux entiers naturels non nuls p et q, premiers entre eux, tels que : $\sqrt[3]{5}=\frac{p}{q}$, alors : $5q^3=p^3$. On en déduit que 5 divise p^3, donc par le lemme d'Euclide 5 divise p. Il existe donc $k\in\mathbb{N}$ tel que : $p=5k$. En injectant ceci dans l'égalité précédente, et en simplifiant, on obtient : $q^3=5^2k^3$, donc par un argument analogue 5 divise q, et par conséquent p et q admettent un diviseur commun strictement supérieur à 1 : c'est impossible, puisque p et q sont premiers entre eux. Par l'absurde : $\sqrt[3]{5}\notin\mathbb{Q}$. L'étude qui précède permet d'en déduire que X^3-5 est irréductible dans $\mathbb{Q}[X]$, donc c'est le polynôme minimal sur $\mathbb{Q}$ de $\sqrt[3]{5}$.
Polynôme minimal de $\sqrt{2}-\sqrt{3}$. Posons :
$$\begin{aligned} P&=\left(X-\left(\sqrt{2}-\sqrt{3}\right)\right)\left(X-\left(\sqrt{2}+\sqrt{3}\right)\right)\left(X-\left(-\sqrt{2}-\sqrt{3}\right)\right)\left(X-\left(-\sqrt{2}+\sqrt{3}\right)\right)\\ &=\left(\left(X-\sqrt{2}\right)^2-(\sqrt{3})^2\right)\left(\left(X+\sqrt{2}\right)^2-(\sqrt{3})^2\right)\\ &=\left(X^2-2\sqrt{2}X-1\right)\left(X^2+2\sqrt{2}X-1\right)\\ &=\left(X^2-1\right)^2-\left(2\sqrt{2}X\right)^2\\ &=\left(X^2-1\right)^2-8X^2.\end{aligned}$$
On a : $P\in\mathbb{Q}[X]$, et P admet $\sqrt{2}-\sqrt{3}$ pour racine. Il reste à justifier qu'il est irréductible. Tout d'abord, il n'admet pas de racine rationnelle parce que $\pm\sqrt{2}\pm\sqrt{3}$ est irrationnel (c'est à démontrer : voir plus bas), donc si P est réductible, ses facteurs irréductibles (que l'on prend unitaires) doivent être de degré 2. Or, si l'on note Q et R ces facteurs, de sorte que : $P=QR$, on a : $QR=\left(X^2-2\sqrt{2}X-1\right)\left(X^2+2\sqrt{2}X-1\right)$. L'unicité de la décomposition en éléments irréductibles

implique, dans $\mathbb{R}[X]$, l'égalité : $Q = \left(X^2 - 2\sqrt{2}X - 1\right)^\alpha \left(X^2 + 2\sqrt{2}X - 1\right)^\beta$, avec $(\alpha, \beta) \in \{0,1\}^2$. Cependant, si $(\alpha, \beta) = (1,0)$ ou $(\alpha, \beta) = (0,1)$, on n'obtient pas un polynôme à coefficients rationnels ; ceci impose $Q = 1$ ou $Q = P$, donc P est irréductible dans $\mathbb{Q}[X]$ et admet $\sqrt{2} - \sqrt{3}$ pour racine : c'est donc le polynôme minimal de $\sqrt{2} - \sqrt{3}$ sur $\mathbb{Q}$.

Ce qu'on a fait là marche souvent : prendre un polynôme dont les racines sont l'élément voulu, ainsi que ses « conjugués » (je ne cherche pas à définir rigoureusement le terme ici), donne un polynôme de $\mathbb{Q}[X]$ si l'on s'y prend bien. C'est d'ailleurs ce qu'on a fait pour $2 + 3i$ ci-dessus.

Démonstration que $\varepsilon_1\sqrt{2}+\varepsilon_2\sqrt{3}$ est irrationnel pour $(\varepsilon_1, \varepsilon_2) \in \{-1,1\}^2$. S'il existe $r \in \mathbb{Q}$ tel que : $\varepsilon_1\sqrt{2}+\varepsilon_2\sqrt{3} = r$, alors l'égalité : $\varepsilon_1\sqrt{3} = r - \varepsilon_2\sqrt{2}$, implique après élévation au carré : $3 = r^2 + 2 - 2r\varepsilon_2\sqrt{2}$, si $r = 0$, alors cette égalité est absurde puisque $3 \neq 2$, et si $r \neq 0$ alors on a : $\sqrt{2} = -\frac{3-r^2-2}{2r\varepsilon_2} \in \mathbb{Q}$, ce qui est absurde également. Ainsi r n'existe pas et $\varepsilon_1\sqrt{2} + \varepsilon_2\sqrt{3}$ est irrationnel.

★ Calculer l'inverse d'un élément de $\mathbb{Q}[\alpha]$, cas algébrique. □

Réponse. Pour comprendre ce qui motive l'approche ci-dessous, notons que : $\dfrac{1}{3\alpha^2 + \alpha + 5} = a\alpha^2+b\alpha+c$, si et seulement si : $(3\alpha^2+\alpha+5)(a\alpha^2+b\alpha+c)-1 = 0$, si et seulement si le polynôme minimal de α (qui est P si tout se passe bien) divise $(3X^2 + X + 5)(aX^2 + bX + c) - 1$, si et seulement s'il existe $U \in \mathbb{Q}[X]$ tel que : $(3X^2 + X + 5)(aX^2 + bX + c) = 1 + UP$ (toujours en partant du principe que P est le polynôme minimal de P : ce n'est pas nécessaire mais cela simplifie la discussion). On reconnaît une relation de Bézout. On va donc trouver $aX^2 + bX + c$ en trouvant une relation de Bézout entre P et $3X^2 + X + 5$. On y parvient *via* l'algorithme d'Euclide étendu :

$$\left\{\begin{array}{rcl} P & = & (3X^2 + X + 5) \times \left(\frac{X}{3} + \frac{5}{9}\right) - \frac{2X}{9} - \frac{7}{9}, \\ 3X^2 + X + 5 & = & \left(-\frac{2X}{9} - \frac{7}{9}\right) \times \left(-\frac{27}{2}X + \frac{171}{4}\right) + \frac{153}{4}, \\ -\frac{2X}{9} - \frac{7}{9} & = & \frac{153}{4}(X - 1) \times \left(\frac{4}{51}X^2 + \frac{4}{153}X + \frac{20}{153}\right) + 0. \end{array}\right.$$

Donc, en remontant l'algorithme :

$$1 = \frac{1}{17}(6X - 19)P + \frac{1}{17}\left(-2X^2 + 3X + 11\right)\left(3X^2 + X + 5\right).$$

On évalue cette égalité en α. Comme $P(\alpha) = 0$, on obtient : $1 = \frac{1}{17}\left(-2\alpha^2 + 3\alpha + 11\right)\left(3\alpha^2 + \alpha + 5\right)$. On en déduit le résultat voulu : $\dfrac{1}{3\alpha^2 + \alpha + 5} = \dfrac{1}{17}\left(-2\alpha^2 + 3\alpha + 11\right)$.

3 Feuilles d'exercices

3.1 Indications et commentaires

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 $a \notin \{0, \pm 1\}$, 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)

4. Vérification immédiate.
5. 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.
6. 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.
7. 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 **??** 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^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 : $X^{\text{pgcd}(m,n)} - 1$.

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 $P = Q_0R_0$ 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.

3.2 Classement des exercices par thèmes

Anneaux principaux	43, 44, 46, 47, 48, 49, 72, 81
Calcul d'ordre, en déduire une divisibilité	1, 4, 17, 22, 36, 37
Carrés et racines carrées modulo n	6, 15, 18, 27, 31, 32, 33, 47, 48, 50, 51, 52, 53, 54, 55, 57, 78
Carrés mod 4, nombres premiers mod 4	5, 6, 31, 32, 47, 48, 50
Décomposer en facteurs irréductibles	3, 5, 9, 10, 28, 42, 43, 58, 60, 73, 78
Développements asymptotiques	62, 63, 64
Équation $x^d \equiv 1 \bmod n$	30, 35, 40, 41, 42, 50
Équation diophantienne	31, 32, 33
Équation polynomiale du 2$^{\text{e}}$ degré $\bmod n$	18, 27
Groupes cycliques, cyclicité de $(\mathbb{Z}/p\mathbb{Z})^\times$	4, 34, 36, 37, 38, 40, 50, 71, 78
Interpolation de Lagrange	67, 68, 88
Irréductibilité dans $\mathbb{Z}[X]$ et $\mathbb{Q}[X]$	77, 78, 81, 82
Opérer par translation : $g \mapsto gx$	6, 7, 53
Ordre d'un élément : calcul	1, 4, 13, 17, 22, 37, 38, 39
Polynôme minimal	79, 80, 83, 85
Produit de convolution	58, 59, 60, 61, 62, 63, 64
Quasi-démonstration du cours	16, 46
Racines de $X^k - \bar{1}$ dans $\mathbb{Z}/p\mathbb{Z}$	6, 7, 34, 35, 50, 71, 78
Raisonner sur les racines d'un polynôme	6, 7, 34, 35, 50, 65, 70, 71, 77, 78, 86, 88
Réduction modulo $a^n \pm 1$	1, 4, 17, 22
Relation de Bézout	11, 24, 29, 72, 75, 79, 83
Sommes, produits sur un groupe fini	6, 7, 21, 52, 53, 54, 55
Théorème chinois	12, 14, 23, 24, 25, 26, 29, 30, 32, 36, 42, 57
Théorème d'isomorphisme	35, 39, 50, 88
Théorème de Lagrange, Euler ou Fermat	1, 4, 6, 12, 13, 18, 22, 23, 24, 29, 36
$\mathbb{Z}/n\mathbb{Z}$ corps $\Rightarrow n$ premier	4, 6

Table des matières