Ag 1,2,3,4 : exercices avec corrigés

I Ancienne liste oral ccp

Algèbre 1

Soient $\theta \in \mathbb{R}$ et $n \in \mathbb{N}^*$. Décomposez en produit de polynômes irréductibles dans $\mathbb{C}[X]$, puis dans $\mathbb{R}[X]$ le polynôme :

$$P = X^{2n} - 2X^n \cos(n\theta) + 1$$

Algèbre 2

On considère les polynômes $P = 3X^4 - 9X^3 + 7X^2 - 3X + 2$ et $Q = X^4 - 3X^3 + 3X^2 - 3X + 2$.

1. Décomposez P et Q en facteurs premiers sur $\mathbb{R}[X]$, puis sur $\mathbb{C}[X]$ (on pourra calculer les valeurs de P et de Q en 1 et en 2).
2. Déterminez le ppcm et le pgcd des polynômes P et Q.

Algèbre 3

On considère les polynômes de $\mathbb{C}[X]$ suivants : $P = 2X^4 - 3X^2 + 1$ et $Q = X^3 + 3X^2 + 3X + 2$.

1. Décomposez en facteurs premiers de P dans $\mathbb{C}[X]$ (on pourra calculer les valeurs de P en 1 et en -1).
2. Décomposez en facteurs premiers de Q dans $\mathbb{C}[X]$ (on pourra calculer la valeur de Q en -2).
3. (a) Déduisez des questions 1. et 2. qu'il existe deux polynômes U et V tels que $PU + QV = 1$.
   (b) Indiquez une méthode pour déterminer deux polynômes U et V en utilisant l'algorithme d'Euclide.

Algèbre 4

On considère la fraction rationnelle $R = \dfrac{X^5 + X^4}{(X-2)^2(X+1)^2}$.

1. Décomposez R en éléments simples.
2. Déterminez les primitives de la fonction $x \mapsto R(x)$ sur l'intervalle $]-1; 2[$.

II Ag1 : petits exercices

Exercice 1. Il existe une bijection entre $\mathbf{Z}$ et $\mathbf{Q}$. Montrer qu'il n'y pas d'isomorphisme entre $(\mathbf{Z}, +)$ et $(\mathbf{Q}, +)$.

Si un tel isomorphisme ϕ de $(\mathbf{Z}, +)$ sur $(\mathbf{Q}, +)$ existe, notons $r = \phi(1)$. Alors par surjectivité de ϕ et propriété de morphisme, on a

$$\mathbf{Q} = \phi(\mathbf{Z}) = \{\phi(n) \ ; \ n \in \mathbf{Z}\} = \{n\phi(1) \ ; \ n \in \mathbf{Z}\}$$

En particulier, $r/2$, qui est un rationnel, serait de la forme nr avec $n \in \mathbf{Z}$, pas possible.

Exercice 2. Soit H_1, H_2 deux sous-groupes d'un groupe $(G, *)$. Donner une condition nécessaire et suffisante pour que $H_1 \cup H_2$ soit un sous-groupe de $(G, *)$.

Si $H_1 \subset H_2$ ou $H_2 \subset H_1$, $H_1 \cup H_2$ est un sous-groupe. Réciproquement, supposons $H = H_1 \cup H_2$ sous-groupe, avec $H_1 \not\subset H_2$. Soit alors $h_1 \in H_1$ tel que $h_1 \notin H_2$. Pour tout $h_2 \in H_2$, $h_2 \circ h_1 \in H_1 \cup H_2$, or si $h_2 * h_1 \in H_2$ on en déduit que $h_1 = h_2^{-1} * (h_2 \circ h_1) \in H_2$ contradictoire. Donc $h_2 * h_1 \in H_1$, donc $h_2 = (h_2 * h_1) * h_1^{-1} \in H_1$. Donc $H_2 \subset H_1$. La condition nécessaire et suffisante cherchée est donc $H_1 \subset H_2$ ou $H_2 \subset H_1$.

Exercice 3 (Centre). Le centre d'un groupe $(G, \star)$ est

$$C = \{g \in G \ ; \ \forall h \in G \quad h \star g = g \star h\}$$

Montrer que C est un sous-groupe de $(G, \star)$.

Exercice 4 (Commutant). Soit g un élément d'un groupe $(G, *)$. Montrer que l'ensemble des éléments de G qui commutent avec g est un sous-groupe de $(G, *)$.

Exercice 5 (Nombres décimaux). Montrer que l'ensemble des nombres décimaux est un anneau (on rappelle qu'un nombre décimal est un nombre dont le développement décimal « se termine »).

On montre que c'est un sous-anneau de $(\mathbf{Q}, +, \times)$ ou de $(\mathbf{R}, +, \times)$ en vérifiant les propriétés qui caractérisent un sous-anneau. Il est commode pour cela de remarquer qu'un nombre x est décimal si et seulement s'il existe $p \in \mathbf{N}$ tel que $10^p \in \mathbf{Z}$.

III Ag2 : petits exercices

Exercice 6. Calculer, si $\theta \in \mathbf{R}$,

$$\sum_{k=0}^{n} \sin(2k+1)\theta$$

$$\begin{aligned}
\sum_{k=0}^{n} \sin(2k+1)\theta &= \operatorname{Im}\left(\sum_{k=0}^{n} e^{i(2k+1)\theta}\right) \\
&= \operatorname{Im}\left(e^{i\theta}\sum_{k=0}^{n}\left(e^{2i\theta}\right)^k\right) \\
&\textit{A partir de là on suppose } \theta \notin \pi\mathbf{Z} \\
&= \operatorname{Im}\left(e^{i\theta}\frac{1-e^{2i(n+1)\theta}}{1-e^{2i\theta}}\right) \\
&= \operatorname{Im}\left(e^{i(n+1)\theta}\frac{\sin((n+1)\theta)}{\sin\theta}\right) \\
&= \frac{\sin^2((n+1)\theta)}{\sin\theta}
\end{aligned}$$

Quand θ est un mutliple de π, on trouve 0, c'est rassurant (prendre un équivalent). On peut raffiner un peu : notant $S(\theta)$ la somme,

$$\frac{S(\theta)}{\theta} \xrightarrow[\theta\to 0]{} (n+1)^2$$

des deux manières !

Exercice 7. Calculer, sous forme cartésienne, les racines carrées de $3+4i$.

A quoi bon ?

Exercice 8. Soit $j = e^{\frac{2i\pi}{3}}$. Calculer, sous forme trigonométrique (module-argument), les racines cubiques de j. Les représenter dans le plan complexe.

Notant $\omega = e^{\frac{2i\pi}{9}}$ la plus évidente d'entre elles, les trois sont ω, $j\omega$, $j^2\omega$, situées aux trois sommets d'un triangle équilatéral inscrit dans le cercle unité.

Exercice 9. Soit $(a,b) \in \mathbf{R}^2$. A quelle condition (nécessaire et suffisante) $e^{ia} + e^{ib}$ est-il réel ?

On écrit comme d'habitude

$$e^{ia} + e^{ib} = 2\cos\left(\frac{a-b}{2}\right) e^{i(a+b)/2}$$

qui est réel si et seulement si $a+b$ est multiple de 2π ou $a-b$ de la forme $(2k+1)\pi$ avec k entier.

Exercice 10. Ecrire $2\cos t + 2\sin t$ sous la forme $A\cos(t+\phi)$

On écrit

$$2\cos t + 2\sin t = 2\sqrt{2}\cos\left(\frac{\pi}{4} - t\right)$$

IV Ag3 : petits exercices

Exercice 11. Calculer les restes respectifs des divisions euclidiennes de $X^n - nX^{n-1} + 1$ par $X-1$, par $X^2 - 3X + 2$, par $(X-1)^4$.

Notant $P = X^n - nX^{n-1} + 1$, le premier reste vaut $\widetilde{P}(1)$, le deuxième vaut $aX+b$ avec $\widetilde{P}(1) = a+b$ et $\widetilde{P}(2) = 2a+b$, ou encore le deuxième vaut $\alpha(X-1)+\beta(X-2)$ avec $\alpha = \widetilde{P}(2)$ et $-\beta = \widetilde{P}(1)$. Pour le troisième, utiliser la formule de Taylor, le reste est donc

$$\frac{(X-1)^3}{6}\widetilde{P^{(3)}}(1)(X-1)\frac{(X-1)^2}{2}\widetilde{P''}(1)(X-1) + \widetilde{P'}(1) + \widetilde{P}(1)$$

Exercice 12. Donner un exemple de polynôme dans $\mathbf{R}[X]$ qui n'est pas irréductible mais n'a pas de racine réelle.

Il faut le prendre au moins de degré 4, mais tout polynôme de degré 4 qui n'a pas de racine réelle, par exemple X^4+1, convient. Pour le factoriser, on interprète les deux termes de la somme comme les extrémités du développement d'un carré :

$$X^4 + 1 = (X^2+1)^2 - 2X^2$$

puis la formule $a^2 - b^2 = (a-b)(a+b)$ permet de factoriser. Mais bien sûr, on sait qu'il n'y a pas de polynôme irréductible de degré > 2 sur $\mathbf{R}$.

Exercice 13. Calculer la somme et le produit des racines du polynôme $X^n - nX^{n-1} + 1$.

Somme : n, produit : $(-1)^n$.

Exercice 14. Décomposer en éléments simples, sur $\mathbf{R}[X]$ et sur $\mathbf{C}[X]$,

$$\frac{X^4}{X^2+X+1}$$

Il suffit de diviser, sur $\mathbf{R}$, le numérateur par le dénominateur, pour sortir la partie entière :

$$\frac{X^4}{X^2+X+1} = \frac{(X^4+X^3+X^2)-(X^3+X^2+X)+X}{X^2+X+1} = X^2-X+\frac{X+1}{X^2+X+1}$$

Sur $\mathbf{C}$, il faut aller plus loin, on veut écrire

$$\frac{X+1}{X^2+X+1} = \frac{\alpha}{X-j}+\frac{\beta}{X-j^2}$$

et pour ce, on calcule (pôles simples) α et β avec la formule traditionnelle :

$$\alpha = \frac{j+1}{2j+1} \qquad ,\beta = \frac{j^2+1}{2j^2+1}$$

(on peut éventuellement remplacer $j+1$ par $-j^2$, j^2+1 par $-j$, ce n'est pas très utile).

V Quelques méthodes utiles

— Lorsque n est premier, l'anneau $\mathbf{Z}/n\mathbf{Z}$ est un corps ; cela permet alors d'appliquer un grand nombre de résultats : $\mathbf{Z}/n\mathbf{Z}$ est intègre, un polynôme non nul sur $\mathbf{Z}/n\mathbf{Z}$ a un nombre de zéros (comptés avec leur multiplicité) au plus égal à son degré, etc...on a aussi tous les résultats du cours d'algèbre linéaire ; si n n'est pas premier, $\mathbf{Z}/n\mathbf{Z}$ est beaucoup plus délicat à manipuler. Il faut en connaître les éléments inversibles (cours) et savoir que les autres sont des diviseurs de 0. La résolution d'une équation du second degré dans $\mathbf{Z}/n\mathbf{Z}$ est un exercice d'oral classique et instructif.

— On aime donc bien travailler avec des nombres premiers (cf rubrique précédente). Par exemple, comment exprimer que des nombres sont premiers entre eux ? en utilisant le théorème de Bezout, ou en écrivant qu'ils n'ont pas de diviseur positif commun autre que 1. Cette dernière condition sera avantageusement remplacée par : ils n'ont pas de diviseur premier commun.

— Un problème de divisibilité est souvent agréable à écrire avec des congruences : celles-ci se manipulent très facilement, presque comme des égalités, sauf pour les simplifications. Un problème de congruence peut aussi se traduire dans $\mathbf{Z}/n\mathbf{Z}$, il faut savoir passer de l'une à l'autre de ces formulations.

— Presque tous les nombres premiers sont impairs. . .mais 2 est premier et pair. Il faut faire attention à ce cas particulier. De même, $\mathbf{Z}/2\mathbf{Z}$, qui est de caractéristique 2, demande quelquefois un traitement particulier différent des $\mathbf{Z}/p\mathbf{Z}$ où p est premier impair.
— Lorsque deux polynômes interviennent dans un exercice, si l'on note P l'un d'eux, on ne doit pas noter P' l'autre (à moins que ce ne soit effectivement son polynôme dérivé).
— Un exercice sur les groupes cycliques est souvent plus facile à résoudre en pensant à $\mathbf{U}_n$ qu'à $\mathbf{Z}/n\mathbf{Z}$. Penser au morphisme canonique de $\mathbf{Z}$ sur $\mathbf{Z}/n\mathbf{Z}$ permet aussi, souvent, de trouver des raisonnements plus simples.

VI Anneaux, idéaux

Exercice 15 (Etude d'un anneau, oral Mines.)**.**
Soit $A = \left\{a + bj \ ; \ (a,b) \in \mathbf{Z}^2\right\}$ où $j = \exp(2i\pi/3)$.

1. Montrer que A est un sous-anneau de $(\mathbf{C}, +, \times)$. Est-ce un corps ?
2. On note, comme d'habitude, A^* l'ensemble des éléments inversibles (pour $\times$) de l'anneau A. Soit $u \in A$. Montrer que $u \in A^* \ \Leftrightarrow \ |u| = 1$. Enumérer les éléments inversibles de A. Que peut-on dire de $(A^*, \times)$?
3. Soit u, v dans A avec $v \neq 0$. Etablir l'existence de $(q, r) \in A^2$ vérifiant $u = qv + r$ et $|r| < |v|$ (*on pourra considérer le nombre complexe u/v, et considérer un élément de A le plus près possible de ce nombre, faire un dessin*).
4. Démontrer que A est un anneau principal, c'est-à-dire que tous les idéaux de A sont principaux.

---

1. On montre que A est stable par $-$, par $\times$ (on a besoin de $j^2 = -1 - j$), et on n'oublie pas de dire que $1 \in A$.
2. Si $|u| = 1$, alors $u \times \overline{u} = 1$, or

$$\overline{u} = a + b\overline{j} = a + bj^2 = (a - b) - bj$$

donc si $u \in A$ on a $\overline{u} \in A$. Et donc, si $u \in A$, si $|u| = 1$ on a $u \in A^*$ et $u^{-1} = \overline{u}$. Réciproquement, si $u \in A$, si $u \in A^*$, soit $v = u^{-1} \in A$. On a $uv = 1$, et donc $|u|^2 \ |v|^2 = 1$. Or, si $u = a + bj$, a et b entiers, on a

$$|u|^2 = (a + bj)(a + bj^2) = a^2 - ab + b^2 \in \mathbf{N}$$

De même $|v|^2 \in \mathbf{N}$. Or le seul produit d'entiers naturels égal à 1 est $1 \times 1 = 1$, donc $|u|^2 = 1$, donc $|u| = 1$.
l'élément $a + bj$ de A est dans A^* si et seulement si $a^2 - ab + b^2 = 1$; or $a^2 - ab + b^2 = (a - b/2)^2 + 3b^2/4$ et cette quantité est > 1 si $|b| > 1$. Pour

$b = -1$, on obtient $a^2 + a + 1 = 1$ qui donne $a = 0$ ou $a = -1$; pour $b = 0$, on obtient $a = \pm 1$. Et pour $b = 1$, $a = 0$ ou $a = 1$. Donc

$$A^* = \{-j, -1 - j, 1, -1, j, 1 + j\} = \left\{-j, j^2, -1, j, -j^2\right\}$$

Il est (vivement !) conseillé de représenter le « réseau » A pour vérifier graphiquement ce résultat.
Comme A est un anneau, $(A^*, \times)$ est un groupe.
3. $u = qv + r$ avec $|r| < |v|$ équivaut à $u/v = q + r/v$ avec $|r/v| < 1$. On cherche donc $q \in A$ tel que $|u/v - q| < 1$. Si on fait un dessin, on voit qu'il y a toujours un élément de A « assez proche » d'un nombre complexe donné. Pour le mettre en évidence, on écrit $u/v = a + jb$ avec a et b réels (la famille $(1, j)$, libre, est une base de $\mathbf{C}$ considéré comme $\mathbf{R}$-espace vectoriel). Il existe α et β entiers tels que $|a - \alpha| \leq 1/2$ et $|b - \beta| \leq 1/2$; alors

$$\begin{aligned} |u/v - (\alpha + j\beta)|^2 &= (a - \alpha)^2 - (a - \alpha)(b - \beta) + (b - \beta)^2 \\ &\leq 1/4 + 1/4 + 1/4 \\ &< 1 \end{aligned}$$

On prend alors $q = \alpha + j\beta$, $r = u - qv$, et ça marche.
4. Il suffit de reprendre la démonstration faite en cours pour $\mathbf{Z}$ ou $\mathbf{K}[X]$: on prend un idéal non nul I (si $I = (0)$, il n'y a rien à faire), on considère un élément de I de module minimal parmi les éléments non nuls de I, on l'appelle v_0, on montre par la « division euclidienne » définie dans la question précédente que $I = (v_0)$...[*Car c'est bien une division euclidienne qu'on vient de définir. Avec une originalité par rapport aux deux divisions euclidiennes que l'on connaît : le quotient, et donc le reste, ne sont pas uniques*].

Exercice 16 (Idéaux d'un corps)**.** Un corps (commutatif) est un anneau particulier. Quels sont ses idéaux ? Démontrer qu'un anneau commutatif A dont les seuls idéaux sont $\{0\}$ et A est un corps.

Si I est un idéal non nul du corps $(\mathbf{K}, +, \times)$, et si $I \neq \{0\}$, alors soit $a \in I \setminus \{0\}$. Comme a est inversible (on est dans un corps), $a^{-1} \times a \in I$ (propriété d'idéal), donc $1 \in I$ (en notant simplement 1 l'élément neutre pour la multiplication), donc pour tout $b \in A$ on a $b \in I$. Les deux seuls idéaux sont donc $\{0\}$ et $\mathbf{K}$. Réciproquement, si les deux seuls idéaux sont $\{0\}$ et A, soit $a \in A \setminus \{0\}$. Alors $(a) \neq \{0\}$ (idéal des multiples de a), donc $(a) = A$, donc $1_A \in (a)$, ce qui montre que a est inversible.

Exercice 17. (classique à l'oral) Soit I un idéal d'un anneau commutatif $(A, +, \times)$. On définit le radical de I :

$$\sqrt{I} = \{a \in A \ / \ \exists n \in \mathbf{N} \ a^n \in I\}$$

1. Montrer que $\sqrt{I}$ est un idéal de A.
2. Si $A = \mathbf{Z}$ et $I = n\mathbf{Z}$ ($n \geq 2$), déterminer $\sqrt{I}$.

---

1. La non vacuité se déduit par exemple du fait que $I \subset \sqrt{I}$.
Si a et b sont dans $\sqrt{I}$, soit $(m, n) \in \mathbf{N}^2$ tels que $a^m \in I$ et $b^n \in I$. La formule du binôme (on est dans un anneau commutatif) donne

$$(a-b)^{m+n} = \sum_{k=0}^{m+n} \binom{m+n}{k} (-1)^{m+n-k} a^k b^{m+n-k}$$

Or si $k \geq m$, $a^k \in I$ (absorbance). Et si $k \leq m-1$, $m+n-k \geq n+1$, donc $b^{m+n-k} \in I$ (absorbance encore). Les propriétés d'idéal de I font qu'on peut en déduire

$$(a-b)^{m+n} \in I$$

et donc $a - b \in \sqrt{I}$.
Si $a \in \sqrt{I}$ et $b \in A$, soit m tel que $a^m \in I$. Comme l'anneau A est commutatif, on a

$$(ab)^m = a^m b^m \in I$$

(absorbance). Donc $ab \in \sqrt{I}$.

2. Pour utiliser les valuations p-adiques. . .désignons par $\mathcal{P}$ l'ensemble des nombres premiers ;

$$\sqrt{n\mathbf{Z}} = \left(\prod_{p \in \mathcal{P} \ ; \ \nu_p(n) > 0} p \right) \mathbf{Z}$$

Exercice 18 (Oral Mines)**.** Soit p un nombre premier. On note Z_p l'ensemble des a/b où $(a, b) \in \mathbf{Z} \times \mathbf{N}^*$ et p ne divise pas b. On note J_p l'ensemble des a/b où $(a, b) \in \mathbf{Z} \times \mathbf{N}^*$, p divise a et p ne divise pas b.

1. Montrer que Z_p est un sous-anneau de $\mathbf{Q}$.
2. Montrer que J_p est un idéal de Z_p et que tout idéal de Z_p autre que Z_p est inclus dans J_p.
3. Déterminer tous les idéaux de Z_p.

---

1. ne pose pas de difficulté particulière.
2. Pas tellement non plus de problème pour montrer que J_p est un idéal de Z_p. Soit I un idéal de Z_p non inclus dans J_p. Soit $a/b \in I$ avec p ne divisant ni a ni b. Alors $b/a \in Z_p$; donc par absorbance $1 = (a/b)(b/a) \in I$. Et, toujours par absorbance, un idéal qui contient 1 contient tout. Donc $I = Z_p$, ce qui conclut par contraposition.
3. On note J_{p^k} l'ensemble des a/b où $(a, b) \in \mathbf{Z} \times \mathbf{N}^*$, p^k divise a et p ne divise pas b ($k \in \mathbf{N}$). Il est assez simple de montrer que les J_{p^k} sont des idéaux de Z_p. Soit I un idéal de Z_p. Il existe un k_0 minimal tel que I ne soit pas inclus dans $J_{p^{k_0}}$ (car l'intersection de tous les J_{p^k} est vide). On a alors $I = J_{p^{k_0-1}}$, de la même manière que ci-dessus. On a donc trouvé tous les idéaux.

VII Divisibilité, pgcd, ppcm

Exercice 19 (Nombres de Mersenne, oral Centrale)**.** Soit a et n deux entiers naturels, $n \geq 2$; démontrer que, pour que $a^n - 1$ soit premier, il est nécessaire que a soit égal à 2 et que n soit premier.
Un tel nombre est appelé alors nombre de Mersenne ; la condition de primalité trouvée n'est pas suffisante. Il existe des tests de primalité des nombres de Mersenne performants, ce qui permet de trouver de grands nombres premiers. Par exemple, $2^{43\ 112\ 609} - 1$ *est premier. Pourquoi chercher de très grands nommbres premiers alors que l'on sait qu'il en existe une infinité ? voir par exemple les applications au codage RSA, mais pour ce codage on n'utilise certainement pas les nombres de Mersenne. . ..*

La factorisation

$$a^n - 1 = (a-1)(a^{n-1} + \cdots + 1)$$

donne la première réponse, puis

$$2^{n_1 n_2} - 1 = (2^{n_1})^{n_2} - 1 = (2^{n_1} - 1)(\ldots)$$

donne la deuxième.

Exercice 20 (Nombres de Fermat, oral Mines)**.**

1. Montrer que, pour que $2^n + 1$ soit premier, il faut que n soit une puissance de 2.
2. Si $n \in \mathbf{N}$, le nombre de Fermat d'ordre n est $F_n = 2^{2^n} + 1$. Montrer que, si $n \neq m$, F_n et F_m sont premiers entre eux.

Fermat a conjecturé que les F_n *étaient premiers. On peut trouver, avec une calculatrice ou un ordinateur, le premier nombre de Fermat non premier (Euler l'a fait sans machine. . .). Mais on ne sait pas vraiment s'il y a beaucoup de nombres de Fermat premiers. Les nombres de Fermat interviennent dans la constructibilité à la règle et au compas des polygones réguliers.*

Si n a un facteur premier impair p, on écrit

$$2^n + 1 = 2^{mp} + 1 = (2^m)^p + 1$$

Or on connaît très bien

$$a^n - b^n = (a-b)(\ldots)$$

Mais, si n est impair, remplaçant b par $-b$, on en déduit

$$a^n + b^n = (a+b)(a^{n-1} - ba^{n-2} + \cdots + b^{n-1})$$

Appliqué à notre situation, on trouve

$$2^n + 1 = (2^m + 1)(2^{m(p-1)} - 2^{m(p-2)} \cdots + 1)$$

On prend bien soin de justifier que c'est une vraie factorisation ($1 < 2^m + 1 < 2^n + 1$). Et on a résolu la première question. Comme souvent, c'est l'exercice

classique sur les nombres de Mersenne (si $a^n - 1$ est premier, $a = 2$ et n est premier) qui peut donner l'idée.
Pour la deuxième question, on peut se demander s'il est possible d'écrire une relation de Bezout. On peut aussi commencer la division de F_n par F_m, si $n > m$, pour entamer un algorithme d'Euclide...Il y a aussi les congruences, car il est facile de voir, si $n > m$:

$$2^{2^n} = 2^{2^m \times 2^{n-m}} = \left(2^{2^m}\right)^{2^{n-m}}$$

Mais $2^{2^m} \equiv -1\ [F_m]$ donc $F_n \equiv 2\ [F_m]$. Le pgcd est donc 1 ou 2. Or les F_k sont impairs...
Si l'idée des congruences peut paraître astucieuse, on a aussi la possibilité de poser la division de F_n par F_m.

Exercice 21 (**Principe des tiroirs).** Montrer que parmi n nombres on peut toujours en choisir k consécutifs (avec $1 \leq k \leq n$) dont la somme est divisible par n.

Soit $x_1, x_2, \ldots, x_n$ la suite de ces n nombres. Si l'une des sommes x_1, $x_1 + x_2$, $x_1 + x_2 + x_3$,..., $x_1 + x_2 + \ldots + x_n$ est divisible par n, c'est terminé. Sinon, les restes de la division par n de ces n sommes ne peuvent pas être deux à deux distincts (il n'y a que $n - 1$ restes non nuls possibles). On prend alors deux sommes qui ont le même reste, en soustrayant la plus courte à la plus longue on conclut. On pourrait raisonner aussi en prenant les classes dans $\mathbf{Z}/n\mathbf{Z}$, mais c'est superflu.

Exercice 22 (**Principe des tiroirs).** Montrer qu'il y a un multiple de 354 dont l'écriture en base 10 est de la forme $11\ldots10\ldots0$ (des 1, puis des 0).

Il y en a beaucoup. Il suffit de prendre deux nombres s'écrivant

$$111\ldots1$$

qui ont le même reste quand on les divise par 354. On soustrait alors le plus petit au plus grand, on conclut.

Exercice 23 (**Formule de Legendre).** Soit $n \geq 2$, p premier. Exprimer $\nu_p(n!)$ à l'aide des $\lfloor \frac{n}{p^k} \rfloor$, $k \geq 1$. Par combien de 0 se termine l'écriture décimale de 2014! ? (on pourra vérifier avec Python)
Cette formule a un certain succès à l'oral : ens, X, Centrale...

On a

$$\nu_p(n!) = \sum_{m=2}^{n} \nu_p(m)$$

Il y a dans $[\![2, n]\!]$ un nombre de multiples de p^k égal à $\lfloor \frac{n}{p^k} \rfloor$ (pour $k \geq 1$). Si on est multiple de p^{k+1} on est multiple de p^k, on obtient donc :

$$\nu_p(n!) = \sum_{k=1}^{+\infty} k \left(\lfloor \frac{n}{p^k} \rfloor - \lfloor \frac{n}{p^{k+1}} \rfloor \right)$$

(la somme est finie). Coupant la somme en deux, réindexant l'une des deux sommes obtenues, on parvient à

$$\nu_p(n!) = \sum_{k=1}^{+\infty} \lfloor \frac{n}{p^k} \rfloor$$

Comme $\nu_5(2017!) < \nu_2(2017)$, le nombre de 0 cherchés est $\nu_5(2017!)$, c'est-à-dire

$$\sum_{k=1}^{+\infty} \lfloor \frac{2017}{5^k} \rfloor$$

qui vaut $403 + 80 + 16 + 3$ c'est-à-dire 502.

Exercice 24 (Idéaux, pgcd, Bezout...Oral Centrale)**.** Soit $P = X^4 + X^2 + 1$, $Q = 1 - X^2$, $D = P \wedge Q$, dans $\mathbf{Q}[X]$.

1. Quel est le plus petit idéal de $\mathbf{Q}[X]$ qui contient à la fois P et Q ?
2. Trouver les couples (U, V) de polynômes tels que $UP + VQ = D$. Soit (U, V) l'un d'eux ; quel est le plus petit idéal de $\mathbf{Q}[X]$ contenant à la fois U et V ?

Le plus petit idéal contenant P et Q est, on le sait, (D). Ensuite, on fait l'algorithme d'Euclide :

$$X^4 + X^2 + 1 = (-X^2 + 1)(-X^2 - 2) + 3$$

donc $U = \frac{1}{3}$ et $V = \frac{1}{3}(X^2 + 2)$ conviennent. Bezout peut se lire de plusieurs manières...et U et V sont aussi bien premiers entre eux, donc le plus petit idéal qui les contient tous les deux est $\mathbf{Q}[X]$.

Exercice 25 (Résolution d'équations classiques, voir Centrale 04 Math 2)**.** On considère l'équation d'inconnues x et y nombres entiers :

$$ax + by = c$$

où a, b, c sont des entiers non nuls.

1. Donner une condition nécessaire et suffisante (faisant intervenir c et le pgcd de a et de b) pour que cette équation ait au moins une solution.
2. On se place dans le cas où équation admet au moins une solution ; dire comment on peut en déterminer une et, à partir de celle-ci, les déterminer toutes.
3. Résoudre $7x + 25y = 5$.
4. Résoudre $(X^2 + X + 1)P - (X + 2)Q = X^3$.

Il y a une solution si et seulement si

$$c \in \{ax + by \ ; \ (x, y) \in \mathbf{Z}^2\}$$

Mais on sait (c'est en fait la définition du pgcd par les idéaux) que

$$\{ax + by \ ; \ (x, y) \in \mathbf{Z}^2\} = (a \wedge b)$$

Exercice 26 (Un calcul de pgcd, par plusieurs méthodes)**.** On veut déterminer le pgcd de $X^p - 1$ et $X^q - 1$ dans $\mathbf{K}[X]$ (p et q sont deux entiers naturels non nuls).

1. On suppose que $\mathbf{K} = \mathbf{C}$. En utilisant la décomposition en facteurs irréductibles de chacun des deux polynômes, déterminer le PGCD cherché.
2. On veut démontrer que l'étude précédente permet d'obtenir la même conclusion si $\mathbf{K}$ est un sous-corps de $\mathbf{C}$ (par exemple, $\mathbf{K} = \mathbf{Q}$, $\mathbf{K} = \mathbf{R}$...). On considère deux corps $\mathbf{K}$ et $\mathbf{L}$, $\mathbf{K}$ étant un sous-corps de $\mathbf{L}$, P et Q deux éléments de $\mathbf{K}[X]$ (et donc de $\mathbf{L}[X]$). On note D (respectivement Δ) le pgcd de P et Q dans $\mathbf{K}[X]$ (respectivement dans $\mathbf{L}[X]$).
   (a) Démontrer que Δ divise D (dans $\mathbf{L}[X]$).
   (b) En utilisant le théorème de Bezout, démontrer que D divise Δ.
   (c) Conclure.
3. On se place sur un corps quelconque (pas nécessairement un sous-corps de $\mathbf{C}$) ; à l'aide de l'algorithme d'Euclide, déterminer le pgcd cherché. On commencera par montrer que, si r est le reste de la division de p par q, $X^r - 1$ est le reste de la division de $X^p - 1$ par $X^q - 1$.

VIII Congruences, $\mathbf{Z}/n\mathbf{Z}$

Exercice 27 (Oral Centrale)**.** Trouver le chiffre des unités de 1587^{413}, de 7^{7^9}.

Exercice 28 (Oral Mines)**.** Donner le reste de la division euclidienne de 2012^{2012} par 13.

Exercice 29 (Oral Mines)**.** Montrer, pour tout entier naturel n non nul :

$$10^{10^n} \equiv 4 \bmod 7 \ .$$

Exercice 30. Soit $n = \overline{abcdef}$ un nombre à 6 chiffres (écrit en numération décimale). Montrer que si n est divisible par 13 alors $\overline{bcdefa}$ l'est.

$$\overline{abcdef} = f + 10e + 10^2d + 10^3c + 10^4b + 10^5a$$
$$\overline{bcdefa} = 10(f + 10e + 10^2d + 10^3c + 10^4b) + a$$

Si $n = \overline{abcdef}$ est divisible par 13, alors

$$10^5a \equiv -(f + 10e + 10^2d + 10^3c + 10^4b) \ [13] \qquad (1)$$

Mais $10 \equiv -3[13]$, donc $10^2 \equiv -4[13]$, donc $10^4 \equiv 3[13]$ et $10^5 \equiv 4[13]$. Il suffit alors de multiplier par 3 la congruence (1) pour obtenir le résultat.

Exercice 31 (Oral Centrale)**.** Soit des entiers a, b, c. Montrer que si 7 divise $a^3 + b^3 + c^3$ alors 7 divise abc.

Suivant si a est congru à $0, 1, 2, 3, 4, 5$ ou 6 modulo 7, a^3 l'est à $0, 1, 1, -1, 1, -1$. Si aucun des nombres a, b, c n'est divisible par 7, $a^3 + b^3 + c^3$ est congru à $\epsilon_1 + \epsilon_2 + \epsilon_3$ modulo 7 avec chaque ϵ_k valant ± 1, la somme ne sera pas congrue à 0 modulo 7 car elle sera congrue à un entier impair compris entre -3 et 3.

Exercice 32 (Oral Mines)**.** Soit p premier, $p \geq 5$. Démontrer que 24 divise $p^2 - 1$.

---

p est congru à 1 ou à -1 modulo 3 (car $p > 3$), donc $p + 1$ ou $p - 1$ est divisible par 3. Donc $p^2 - 1$, leur produit, l'est. De plus, p, premier et impair car > 2, est congru à 1, 3, 5 ou 7 modulo 8. Donc son carré est congru à 1, 1, 1 ou 1 modulo 8. Donc $p^2 - 1$ est divisible par 3 et par 8, qui sont premiers entre eux, il est donc divisible par 24.

Exercice 33 (Conjonction de congruences)**.** Compléter l'équivalence suivante :

$$\Big(a \equiv b\ [n] \text{ et } a \equiv b\ [m]\Big) \Longleftrightarrow a \equiv b\ [\ ?\ ]$$

Exercice 34 (Oral Centrale)**.** Résoudre, dans $\mathbf{Z}$, $10\ x \equiv 14[15]$ puis $10\ x \equiv 14[18]$. Donner une condition nécessaire et suffisante pour que $ax \equiv b[n]$ ait une solution (a, b, n entiers, $n \neq 0$, inconnue entière x).

Exercice 35 (« Grand » classique, petit théorème de Fermat, indicatrice d'Euler)**.**

1. Soit p un nombre premier, k un entier naturel strictement compris entre 0 et p. Démontrer que p divise $\binom{p}{k}$.
2. Démontrer que, si x et y sont deux entiers :
$$(x+y)^p \equiv x^p + y^p\ [p]$$
3. En déduire que, pour tout nombre entier a,
$$a^p \equiv a\ [p]$$
(on suggère de faire une récurrence sur a pour $a \in \mathbf{N}$). Simplifier cette congruence si a n'est pas multiple de p.

   Ce résultat est le petit théorème de Fermat. Notons qu'il existe des nombres N non premiers tels que, pour tout entier a premier avec N,
$$a^{N-1} \equiv 1\ [N]\ .$$
   On les appelle nombres de Carmichael. Le plus petit est 561. La réciproque du petit théorème de Fermat est donc fausse.

   Dans la suite de l'exercice, on note n un entier naturel non nul. On note G_n le groupe multiplicatif des éléments inversibles de $\big(\mathbf{Z}/n\mathbf{Z}\big)$, c'est-à-dire $\big(\mathbf{Z}/n\mathbf{Z}\big)^*$. On désigne par $\phi(n)$ le nombre d'éléments de G_n (ϕ est l'indicatrice d'Euler, dont le définition est au programme).
4. Calculer, si p est premier, $\phi(p)$, $\phi(p^k)$ (k est un entier naturel non nul).
5. Soit $\overline{a}$ un élément de G_n. Démontrer que l'application $\overline{x} \mapsto \overline{a}\ \overline{x}$ est une bijection de G_n dans lui-même. En réindexant le produit des éléments de G_n à l'aide de cette bijection, en déduire que
$$a^{\phi(n)} \equiv 1\ [n]$$

et retrouver le petit théorème de Fermat.

Cette méthode consistant à faire le produit de tous les éléments d'un groupe multiplicatif en l'écrivant de deux manières différentes est classique.

Exercice 36 (Carrés dans $\mathbf{Z}/p\mathbf{Z}$)**.**

1. Faire la liste des éléments de $\mathbf{Z}/17\mathbf{Z}$ qui sont des carrés. Combien y-en-a-t-il ?
2. Soit p un nombre premier impair. On note A l'ensemble des carrés dans $\mathbf{Z}/p\mathbf{Z}$: $x \in A \Leftrightarrow \exists y \in \mathbf{Z}/p\mathbf{Z} \quad x = y^2$.
   (a) Déterminer le nombre d'éléments de A.
   (b) Démontrer que, si a est un élément non nul de A, $x \mapsto xa$ est une bijection de A sur lui-même.
   (c) Démontrer que, si a est un élément de $\mathbf{Z}/p\mathbf{Z} \setminus A$, $x \mapsto xa$ est une bijection de $A \setminus \{0\}$ sur $\mathbf{Z}/p\mathbf{Z} \setminus A$.

Exercice 37 (Résolution d'une équation du second degré dans $\mathbf{Z}/p\mathbf{Z}$)**.**

1. Résoudre l'équation
$$X^2 - \overline{13}X + \overline{8} = \overline{0}$$
dans $\mathbf{Z}/17\mathbf{Z}$. *On essayera de suivre la même démarche que sur* $\mathbf{R}$ *: mise sous forme canonique. . .reprendre donc la démarche suivie dans le cours de première*
2. Résoudre l'équation
$$X^2 - 2X + 4 = 0$$
dans $\mathbf{Z}/26\mathbf{Z}$.

Exercice 38. Discuter, suivant les valeurs de $a \in \mathbf{Z}/7\mathbf{Z}$, le nombre de solutions dans $\mathbf{Z}/7\mathbf{Z}$ de l'équation
$$x^2 + x + a = \overline{0}$$

Exercice 39 (Oral Mines, Centrale)**.** Résoudre dans $\mathbf{Z}/11\mathbf{Z}$ puis dans $\mathbf{Z}/143\mathbf{Z}$: $x^2 - 4x + 3 = 0$ (vérification avec Python à l'oral de Centrale ?).

Exercice 40 (Oral Mines)**.** Résoudre le système

$$\begin{cases} \overline{3}x + \overline{7}y &= \overline{3} \\ \overline{6}x - \overline{7}y &= \overline{0} \end{cases}$$

dans $\mathbf{Z}/36\mathbf{Z}$ puis dans $\mathbf{Z}/37\mathbf{Z}$.

Exercice 41 (Théorème chinois - version constructive)**.** Soient $m_1, m_2, \ldots, m_p$ p entiers premiers entre eux deux à deux. On note $M = \prod_{k=1}^{p} m_k$. On note enfin, pour tout i, μ_i le quotient de la division euclidienne de M par m_i.

1. Démontrer qu'il existe, pour tout i entre 1 et p, deux entiers u_i et v_i tels que $u_i m_i + v_i \mu_i = 1$
2. Construire, à partir des données précédentes, une solution du système de congruences
$$\begin{cases} x \equiv 1 \ [m_1] \\ x \equiv 0 \ [m_2] \\ \quad \vdots \\ x \equiv 0 \ [m_p] \end{cases}$$
3. Soit $(a_1, \ldots, a_p)$ une famille d'entiers. Déduire de la question précédente une solution du système de congruences
$$\begin{cases} x \equiv a_1 \ [m_1] \\ x \equiv a_2 \ [m_2] \\ \quad \vdots \\ x \equiv a_p \ [m_p] \end{cases}$$
Comment, à partir d'une solution de ce système, obtient-on toutes les solutions ?
4. Résoudre le système
$$\begin{cases} x \equiv 1[5] \\ x \equiv 6 \ [13] \\ x \equiv 3 \ [7] \end{cases}$$

IX Groupes

Exercice 42. Montrer que le groupe $\big((\mathbf{Z}/17\mathbf{Z})^*, \times\big)$ est cyclique (en cherchant, tout simplement, un générateur de ce groupe). Puis donner tous les générateurs de $\big((\mathbf{Z}/17\mathbf{Z})^*, \times\big)$.
Remarque 1 : on peut montrer que, si p est premier, $\big((\mathbf{Z}/p\mathbf{Z})^*, \times\big)$ *est cyclique.*
Remarque 2 : ne pas confondre le groupe $\big((\mathbf{Z}/p\mathbf{Z})^*, \times\big)$ *et le groupe* $(\mathbf{Z}/p\mathbf{Z}, +)$.

Exercice 43 (Sous-groupes de groupes finis : problèmes de cardinaux)**.**

1. Soit $(G, \star)$ un groupe fini. Soit H un sous-groupe de G. Si $(a, b) \in G^2$, montrer que les ensembles $a \star H = \{a \star h \ ; \ h \in H\}$ et $b \star H$ sont égaux ou disjoints. En déduire que le cardinal de H divise celui de G (Oral Centrale).

   Ce résultat est le **théorème de Lagrange**. Il n'est pas expau programme, mais est très classique. A l'oral X ou ens, il est souvent considéré comme acquis.

2. (Une version un peu plus sophistiquée) Soit $(G, \star)$ un groupe fini. Soit H un sous-groupe de G. On définit sur G la relation $\mathcal{R}$:

$$g \mathcal{R} g' \ \Leftrightarrow \ g^{-1} * g' \in H$$

   (a) Démontrer que $\mathcal{R}$ est une relation d'équivalence.

   (b) Démontrer que chaque classe d'équivalence a le même nombre d'éléments que H.

   (c) En déduire que le cardinal de H divise celui de G.

3. Soit G un groupe abélien fini d'ordre n, g_0 un élément de G, d'ordre m. Vérifier que l'application $g \mapsto g * g_0$ est une bijection de G sur lui-même. En déduire :

$$\prod_{g \in G} g = g_0^n \prod_{g \in G} g$$

   puis conclure que m divise n.

   On dit que **l'ordre d'un élément divise l'ordre du groupe**. C'est une méthode simple pour démontrer le théorème d'Euler ou le petit théorème de Fermat (probablement la plus rapide, dans le cadre du programme). Mais si G n'est pas abélien, (G fini), cette démonstration ne marche pas. Le résultat subsiste cependant : si g est un élément de G d'orde m, g engendre un sous-groupe H de cardinal m, donc m divise l'ordre de G d'après le théorème de Lagrange.

4. **Résumé :** Dans un groupe fini, l'ordre de tout sous-groupe divise l'ordre du groupe. L'ordre de tout élément divise l'ordre du groupe.

Exercice 44. *Oral Centrale* On admet le théorème de Lagrange (voir ci-dessus). Soit G un groupe fini de cardinal supérieur à 2. On définit le centre de G :

$$Z = \{x \in G \ ; \ \forall y \in G \ xy = yx\}$$

Pour $x \in G$, on définit

$$C_x = \{y \in G \ ; \ xy = yx\}$$

1. Montrer que Z et C_x sont des sous-groupes de G.

2. On suppose que $\text{Card}(G)/\text{Card}(Z)$ est un nombre premier. Montrer que G est commutatif. On pourra supposer l'existence de $x \in G \setminus Z$ et considérer le sous-groupe engendré par x et Z.

Exercice 45 (Sous-groupes de groupes finis : problèmes de cardinaux (suite))**.** Soit $(G, *)$ un groupe. On suppose que le cardinal de G s'écrit pq, p et q premiers avec $p < q$. Montrer que G contient au plus un sous-groupe de cardinal q. (Oral Centrale)

Soit H un sous-groupe de cardinal q. Tout élément de H est d'ordre divisant q, donc d'ordre 1 ou q. Donc tout élément de H qui n'est pas d'ordre 1 (donc qui n'est pas l'élément neutre) est d'ordre q, donc engendre H, qui donc est nécessairement cyclique. Supposons qu'il y ait deux sous-groupes H et H' d'ordre q, distincts. Alors $H \cap H' = \{e\}$ (car si $h \in H \cap H'$, si $h \neq e$, alors h engendre à la fois H et H', qui sont alors égaux). L'application

$$(h, h') \longmapsto h * h'$$

est alors injective. En effet, si $h_1 * h'_1 = h_2 * h'_2$, on a $h_2^{-1} * h_1 = h'_2 * (h'_1)^{-1}$, cet élément de G étant à la fois dans H et H' est donc égal à e, d'où $h_1 = h_2$ et $h'_1 = h'_2$. Il y aurait donc au moins q^2 éléments dans G, ce qui est contraire à l'hypothèse. On n'a pas utilisé la primalité de p, mais cela servait sans doute dans des questions ultérieures.

Exercice 46 (Classique)**.** Montrer qu'un sous-groupe d'un groupe cyclique est cyclique.

Classique, et très intéressant, car il y a plusieurs manières d'aborder le problème. Les deux méthodes les plus efficaces sont probablement les suivantes :
Méthode 1 : Tout groupe cyclique est isomorphe à un groupe $(\mathbf{U}_n, \times)$. Si on montre que tout sous-groupe de $(\mathbf{U}_n, \times)$ est cyclique, le résultat est démontré [*En détail : soit $(G, *)$ un groupe cyclique, ϕ un isomorphisme de G sur $\mathbf{U}_n$. Si H est un sous-groupe de G, $\phi(H)$ est un sous-groupe de $\mathbf{U}_n$. Et si on a montré que $\phi(H)$ était nécessairement un groupe cyclique, $H = \phi^{-1}(\phi(H))$ en est un*]. Soit donc K un sous-groupe de $\mathbf{U}_n$, appelons d son ordre ($d = |K|$). Tout élément z de K est d'ordre divisant d, donc vérifie $z^d = 1$. Et donc $K \subset \mathbf{U}_d$. Et donc (ils ont même cardinal) $K = \mathbf{U}_d$. C'est fini. [*C'est quand même une idée fondamentale sur les groupes cycliques : ce qui est fait pour $\mathbf{U}_n$ est fait pour tous les groupes cycliques d'ordre n. Rappelons qu'il est en général plus agréable de travailler sur $\mathbf{U}_n$ que sur $\mathbf{Z}/n\mathbf{Z}$. Par exemple, avec les notations précédentes, l'inclusion $\mathbf{U}_d \subset \mathbf{U}_n$ est très simple et ne nécessite pas l'utilisation du théorème de Lagrange, hors-programme*]

Méthode 2 : Soit $(G, *)$ un groupe cyclique d'ordre n, g un générateur de G, et utilisons le morphisme surjectif

$$\begin{array}{rccc} \phi : & \mathbf{Z} & \longrightarrow & G \\ & z & \longmapsto & g^z \end{array}$$

dont on sait que le noyau est $n\mathbf{Z}$. Si H est un sous-groupe de $(G, *)$, alors $\phi^{-1}(H)$ est un sous-groupe de $(\mathbf{Z}, +)$. Donc un certain $m\mathbf{Z}$. Donc H est engendré par g^m, or il est fini, la preuve l'est donc aussi.

Exercice 47 (Oral Mines, X)**.**

1. Montrer que tout sous-groupe d'un groupe cyclique est cyclique.
2. Soit d, n entiers tels que $d|n$. Montrer que $\mathbf{Z}/n\mathbf{Z}$ a un unique sous-groupe d'ordre d.
3. Montrer que $n = \sum_{d|n} \phi(d)$, où ϕ désigne l'indicateur d'Euler

---

1. Méthode 1 : (Inspirée par l'observation de $\mathbf{U}_{12}$ par exemple) : soit $(G, *)$ un groupe cyclique d'ordre n, g un générateur de G. On a alors

$$G = \{g^k \ ; \ k \in \mathbf{Z}\} \ = \ \{g^k \ ; \ 0 \leq k \leq n-1\}$$

Soit H un sous-groupe de $(G, *)$ autre que $\{e\}$ (ce dernier est clairement cyclique). Comme H est fini, il suffit d'en trouver un générateur. Considérons

$$k_0 = \min(\{k \in [\![1, n-1]\!] \ / \ g^k \in H\})$$

(un dessin dans $\mathbf{U}_{12}$ justifie ce choix). Alors $h_0 = g^{k_0} \in H$ et donc

$$\langle h_0 \rangle = \{h_0^k \ ; \ k \in \mathbf{Z}\} \subset H$$

($\langle h_0 \rangle$ est le sous-groupe de $(G, *)$ engendré par h_0). Soit réciproquement h un élément de H. Soit $k \in \mathbf{Z}$ tel que $h = g^k$. Il existe q, r entiers tels que $k = k_0 q + r$, $0 \leq r < k_0$. Donc

$$h = g^k = g^{k_0 q} * g^r = \left(g^{k_0}\right)^q * g^r = h_0^q * g^r$$

Donc $g^r = h_0^{-q} * h \in H$. Et la définition de k_0 fait que $r = 0$. On en déduit que $h = h_0^q$.
Conclusion : $H = \langle h_0 \rangle$ est cyclique.

Méthode 2 : Le morphisme ϕ_g permet de transférer des résultats de $(\mathbf{Z}, +)$ sur $(G, *)$.
Les sous-groupes de $(\mathbf{Z}, +)$ sont les $n\mathbf{Z}$, $n \in \mathbf{N}$; résultat qui n'est plus au programme de mpsi, mais qui se démontre comme le résultat analogue sur les idéaux.

> soit H un sous-groupe de $(\mathbf{Z}, +)$. Si $H = \{0\}$, c'est fini : $H = 0\mathbf{Z}$. Sinon, $H \cap \mathbf{N}_* \neq \emptyset$ (en effet, si h est un élément non nul de H, $-h \in H$, et $h > 0$ ou $-h > 0$).
> Soit $h_0 = \min(H \cap \mathbf{N}_*)$; comme $h_0 \in H$ et $(H, +)$ est un groupe, $\forall q \in \mathbf{Z} \quad qh_0 \in H$ (*Il faut voir que qh_0 n'est pas du tout, ici, le « produit » de la « multiplication » (????) de q par h_0*). Réciproquement, si $h \in H$, on divise
>
> $$h = qh_0 + r \quad , \quad 0 \leq r < h_0$$
>
> et $r = h - qh_0 \in H$ donc nécessairement $r = 0$. On a donc $H = h_0\mathbf{Z}$.

Notons que les sous-groupes de $\mathbf{K}[X]$ *ne sont en revanche pas tous des idéaux.*
Soit donc $(G,*)$ un groupe cyclique d'ordre n, g un générateur de $(G,*)$. Considérons le morphisme $\phi_g \ : \ z \mapsto g^z$ de $(\mathbf{Z},+)$ dans $(G,*)$. Ce morphisme est surjectif. Son noyau est $n\mathbf{Z}$ (cours).
Si H est un sous-groupe de $(G,*)$, $\phi_g^{-1}(H)$ est un sous-groupe de $\mathbf{Z}$, donc il existe m entier naturel tel que $\phi_g^{-1}(H) = m\mathbf{Z}$. Or $\phi_g\big(\phi_g^{-1}(H)\big) = H$ (évidence ? pas tout-à-fait, c'est vrai seulement parce que ϕ_g est surjective). Donc

$$H = \phi_g(m\mathbf{Z}) = \langle g^m \rangle$$

Méthode 3 : On peut se contenter de résoudre le problème pour les sous-groupes de $(\mathbf{U}_n,\times)$, le résultat se transporte par isomorphisme...voir paragraphe suivant !
2. Méthode 1 : Déplaçons le problème vers le groupe $(\mathbf{U}_n,\times)$. Soit donc d un diviseur de n ; $(\mathbf{U}_d,\times)$ est un sous-groupe d'ordre d, il y a donc existence, reste à voir l'unicité. Soit H un sous-groupe d'ordre d de $\mathbf{U}_n$. Si $h \in H$, h est d'ordre m, et m divise d (cours !). Donc $h^d = 1$. Donc $h \in \mathbf{U}_d$.
Donc $H \subset \mathbf{U}_d$ et, comme $\mathrm{Card}(H) = \mathrm{Card}(\mathbf{U}_d)$, $H = \mathbf{U}_d$.
On a démontré que $(\mathbf{U}_n,\times)$ avait un unique sous-groupe d'ordre d. On a aussi démontré que les sous-groupes de $\mathbf{U}_n$ sont les $\mathbf{U}_d$ où $d|n$, ce qui répond aux deux premières questions !
[Soit ϕ un isomorphisme de $(\mathbf{Z}/n\mathbf{Z},+)$ sur $(\mathbf{U}_n,\times)$. ϕ transforme un sous-groupe d'ordre d de l'un en sous-groupe d'ordre d de l'autre, ce qui conclut.]

Méthode 2 : On reprend la méthode 2 précédente. De $e \in H$ on déduit que $\phi_g^{-1}(H)$ contient $\mathrm{Ker}(\phi_g)$. Et donc $n\mathbf{Z} \subset m\mathbf{Z}$. Et donc $m|n$. Or si $n = md$, on voit que l'ordre de g^m est d. Donc H est d'ordre d si et seulement si il est engendré par $g^{n/d}$. Et donc le seul sous-groupe d'ordre d est celui engendré par $g^{n/d}$.
3. L'indexation $d|n$, couramment utilisée en arithmétique, peut sembler vague. Elle désigne tous les diviseurs positifs de n, depuis 1 (compris) jusqu'à n (compris). Par exemple, si n est premier, la formule à démontrer est

$$p = \phi(p) + \phi(1)$$

qui n'est pas très difficile à voir !
Soit, si $d|n$, H_d l'unique sous-groupe d'ordre d de $(\mathbf{Z}/n\mathbf{Z},+)$. Soit A_d l'ensemble des générateurs de H_d. Comme H_d est cyclique, le cours dit que $\mathrm{Card}(H_d) = \phi(d)$.
Si $d \neq d'$, $A_d \cap A_{d'} = \emptyset$ (autrement dit : on ne peut pas engendrer deux groupes différents !)
Soit $g \in \mathbf{Z}/n\mathbf{Z}$, $\langle g \rangle$ le sous-groupe qu'il engendre. Ce sous-groupe est l'un des H_d. Donc g est dans l'un des A_d.
En conclusion on a une partition de $\mathbf{Z}/n\mathbf{Z}$:

$$\mathbf{Z}/n\mathbf{Z} = \bigcup_{d|n} A_d$$

et la réunion étant disjointe,

$$\mathrm{Card}(\mathbf{Z}/n\mathbf{Z}) = \sum_{d|n} \mathrm{Card}(A_d)$$

qui est le résultat attendu.
On peut bien entendu tout rédiger dans $\mathbf{U}_n$.

Exercice 48 (Oral X)**.** On désigne par G un groupe abélien. Soit g un élément de G d'ordre fini n, g' un élément de G d'ordre fini n', on suppose n et n' premiers entre eux. Montrer que $g * g'$ est d'ordre fini nn'.

D'abord, le plus facile :

$$(g * g')^{nn'} = g^{nn'} * (g')^{nn'} = (g^n)^{n'} * \left((g')^{n'}\right)^n = e$$

par commutativité de la loi $*$. On sait donc que $g * g'$ est d'ordre fini divisant nn'. Supposons maintenant

$$(g * g')^m = e$$

qui s'écrit par commutativité $g^m * (g')^m = e$. En élevant à la puissance n, on obtient $(g')^{mn} = e$, donc $n' \mid mn$, et par théorème de Gauss, $n' \mid m$. De même $n \mid m$. Et encore par corollaire du théorème de Gauss, $nn' \mid m$.
Le résultat s'ensuit.

Exercice 49 (Oral Centrale, Mines)**.** Soit n un entier naturel supérieur strictement à 2, soit a un entier impair. Montrer que $a^{2^{n-2}}$ est congru à 1 modulo 2^n. En déduire que, n étant un entier naturel, le groupe $G_n = \left(\mathbf{Z}/2^n\mathbf{Z}\right)^*$ est cyclique si et seulement si $n \leq 2$.

Exercice 50 (Oral Centrale)**.** Soit n un entier naturel supérieur strictement à 2 ; on note U l'ensemble des éléments inversibles de l'anneau $\mathbf{Z}/2^n\mathbf{Z}$.

1. Montrer que U est un groupe pour la multiplication.
2. Calculer $x^{2^{n-2}}$ pour tout x de U.
3. Trouver le plus petit entier $k > 0$ tel que $3^k \equiv 1 \mod 2^n$.
4. Montrer que U est isomorphe au produit des groupes additifs $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2^{n-2}\mathbf{Z}$.

1. C'est une question de cours, pas plus facile ni plus difficile à traiter pour $\mathbf{Z}/2^n\mathbf{Z}$ que pour un autre anneau.
2. On trouve $\overline{1}$...Déjà vu dans l'exercice précédent sur la feuille d'énoncés. Comment trouver ce résultat ? l'idée est d'essayer pour $n = 3$: les classes inversibles dans $\mathbf{Z}/8\mathbf{Z}$ sont $\overline{1}$, $\overline{3}$, $\overline{5}$, $\overline{7}$. Dont les carrés sont tous $\overline{1}$. Puis on fait une récurrence sur n. Rappelons que l'ordre de U est 2^{n-1} (les classes inversibles sont les classes des entiers impairs, il y en a une moitié). Voir correction de l'exercice 48 pour le détail de la récurrence.
3. L'ordre de $\overline{3}$ dans U divise donc 2^{n-2}. Par conséquent, $\overline{3}$ est d'ordre 2^{n-2} si et seulement si

$$\overline{3}^{2^{n-3}} \neq \overline{1}$$

Supposons $n > 3$, et supposons

$$3^{2^{n-2}} \equiv 1\ [2^{n+1}]$$

Alors 2^{n+1} divise $3^{2^{n-2}} - 1 = \left(3^{2^{n-3}} - 1\right)\left(3^{2^{n-3}} + 1\right)$. Mais 2^{n-3} est pair, donc

$$3^{2^{n-3}} + 1 \equiv 2\ [4]$$

(les puissances paires de 3 sont congrues à 1 modulo 4, on le déduit du simple fait que $3^2 \equiv 1\ [4]$). Donc $3^{2^{n-3}} + 1$ est divisible par 2 mais pas par 4. Et donc 2^n divise $3^{2^{n-3}} - 1$. Or 2^4 ne divise pas $3^2 - 1$, on en déduit, pour tout $n \geq 4$, que le plus petit k cherché est 2^{n-2}. Pour $n = 3$, c'est bien facile à vérifier directement.
4. Dans le groupe $\left(\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2^{n-2}\mathbf{Z}, +\right)$, l'élément $(1 \bmod 2\ , 0 \bmod 2^{n-2})$ est d'ordre 2, l'élém ent $(0 \bmod 2\ , 1 \bmod 2^{n-2})$ est d'ordre 2^{n-2}. Il n'est donc pas déraisonnable de définir

$$\phi\ :\ (x \bmod 2\ , y \bmod 2^{n-2}) \longmapsto \overline{-1}^{\,x}\ \overline{3}^{y}$$

de $\left(\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2^{n-2}\mathbf{Z}, +\right)$ dans $(U, \times)$. On vérifie sans trop de difficulté que ϕ est bien définie et est un morphisme de groupes. L'injectivité vient du fait que $\overline{-1} \notin \langle\overline{3}\rangle$, sinon on aurait

$$\overline{-1} = \overline{3}^{2^{n-3}}$$

ce qui est contradictoire avec les congruences observées à la question précédente. Notons qu'on peut remplacer $\overline{-1}$ par n'importe quel h d'ordre 2 qui n'est pas dans $\langle\overline{3}\rangle$, dont l'existence est assez facile à assurer. La surjectivité de ϕ vient enfin du fait que le cardinal est le même au départ et à l'arrivée.

Exercice 51. Démontrer que les sous-groupes finis de $\left(\mathbf{C}^*, \times\right)$ sont les $\mathbf{U}_n$ (on commencera par démontrer qu'un tel sous-groupe est inclus dans l'ensemble des nombres complexes de module 1).

Soit G un sous-groupe fini de $\left(\mathbf{C}^*, \times\right)$. Tous ses éléments sont d'ordre fini, divisant l'ordre du groupe. Soit $d = |G|$. Tous les éléments de G vérifient $z^d = 1$. Donc G est inclus dans $\mathbf{U}_d$. Mais ils ont même cardinal, ils sont donc égaux.

Exercice 52. Trouver tous les morphismes de groupes de $\left(\mathbf{Z}/n\mathbf{Z}, +\right)$ dans $\left(\mathbf{C}^*, \times\right)$.

Soit ϕ un tel morphisme. Si on connaît $\phi(\overline{1})$, on connaît ϕ.
[Plus généralement, pour connaître un morphisme d'un groupe cyclique $(G, *)$ dans un groupe $(H, .)$, il suffit de connaître l'image par ce morphisme d'un générateur de G. En effet, si g est un tel générateur, on a pour tout $n \in \mathbf{Z}$: $\phi(g^n) = (\phi(g))^n$, ce qui donne l'image par ϕ de tous les éléments de G].
Soit $\omega = \phi(\overline{1})$. On a, par propriété de morphisme (en essayant de ne pas trop se tromper de loi : au départ, l'addition, à l'arrivée la multiplication),

$$\phi(n\overline{1}) = \omega^n$$

Mais $n\overline{1} = \overline{n} = \overline{n} = \overline{0}$, et un morphisme transforme l'élément neutre du groupe de départ en l'élément neutre du groupe d'arrivée. Donc $\omega^n = 1$. Et donc $\omega \in \mathcal{U}_n$.

Réciproquement, soit ω un élément de $\mathbf{U}_n$. On montre que l'application

$$\begin{array}{rccc} \phi_\omega & : & \mathbf{Z}/n\mathbf{Z} & \longrightarrow & \mathbf{C}^* \\ & & \overline{a} & \longmapsto & \omega^a \end{array}$$

est bien définie (il s'agit pour cela de montrer que, si $a \equiv b[n]$, $\omega^a = \omega^b$, ce qui se fait sans trop de mal). C'est assez clairement un morphisme. Les ϕ_ω, $\omega \in \mathbf{U}_n$ sont les morphismes cherchés.

Exercice 53 ((Oral X))**.** Trouver à isomorphisme près tous les groupes d'ordre p^2, où p est premier.

Soit $(G, .)$ un tel groupe. S'il y a dans G un élément d'ordre p^2, G est cyclique, isomorphe donc à $(\mathbf{Z}/p^2\mathbf{Z}, +)$.
Supposons dorénavant G non cyclique. Tous les éléments de G autres que l'élément neutre e sont d'ordre p. Soit $a \neq e$, et $b \notin \langle a \rangle$. Si $b^k \neq e$, alors b^k engendre $\langle b \rangle$ (dans un groupe cyclique d'ordre premier p, tous les éléments sauf le neutre sont générateurs). Donc $b^k \notin \langle a \rangle$, sinon on aurait $\langle b \rangle \subset \langle a \rangle$. On en déduit que les $a^k b^\ell$, $0 \leq k \leq p-1$, $0 \leq \ell \leq p-1$, sont deux à deux distincts. On pourrait avoir l'idée de montrer que

$$\begin{array}{rccc} \phi & : & \mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z} & \longrightarrow & G \\ & & (\overline{k}, \overline{\ell}) & \longmapsto & a^k b^\ell \end{array}$$

est un isomorphisme de groupes (la loi au départ étant bien sûr l'addition). Mais cela pose un problème de commutation de a et b. On va essayer de trouver un élément a qui commute avec tous les autres, en arrivant par des moyens si

possibles modestes à une application classique de l'action d'un groupe sur un ensemble et de l'équation aux classes.
Le centre de G, c'est

$$C = \{a \in G \ ; \ \forall x \in G \quad ax = xa\} = \{a \in G \ ; \ \forall x \in G \quad xax^{-1} = a\}$$

c'est un sous-groupe de $(G, .)$, il est donc de cardinal 1, p ou p^2.
Fixons a dans G, et remarquons donc que a est dans le centre si et seulement si le cardinal de

$$D_a = \{xax^{-1} \ ; \ x \in G\}$$

vaut 1. D_a n'est pas un sous-groupe, mais on va quand même pouvoir dire des choses sur son cardinal. En effet, on note que

$$xax^{-1} = yay^{-1} \ \Leftrightarrow \ y^{-1}x \in C(a)$$

où $C(a)$ est le commutant de a (l'ensemble des éléments qui commutent avec a).
Reprenons alors la démonstration du classique théorème de Lagrange : il existe $x_1, \ldots, x_m$ tels que

$$G = \bigcup_{i=1}^{m} x_i C(a)$$

(la réunion étant disjointe). On a alors

$$D_a = \{x_i a x_i^{-1}\}_{1 \leq i \leq m}$$

les éléments étant distincts, et donc $|D_a| = m$.
Comme m divise $|G|$, on en déduit l'essentiel : $|D_a|$ divise $|G|$, donc vaut 1, p ou p^2. Mais facilement, les D_a sont deux à deux disjoints ou confondus, et leur réunion est G. Il existe donc $a_1, \ldots, a_r$ tels que

$$G = \bigcup_{i=1}^{r} D_{a_i}$$

(réunion disjointe) ; il y a au moins un D_a réduit à un singleton : D_e. Il n'est pas le seul, sinon on aurait

$$|G| \equiv 1 \ [p]$$

Ce qui permet de conclure...car si a est dans le centre, l'application ϕ donnée plus haut est bien un isomorphisme de groupes. On en déduit que tout groupe de cardinal p^2 est commutatif. Et aussi que le centre d'un p-groupe (un groupe dont le cardinal est une puissance de p) n'est pas réduit au seul élément neutre.

Exercice 54 (Groupe diedral). On considère les transformations suivantes du plan complexe (on note comme d'habitude $j = e^{\frac{2i\pi}{3}}$) :

$$s \ : \ z \mapsto \overline{z}$$

$$r \ : \ z \mapsto jz$$

1. Quelle est la nature géométrique des transformations r et s ?

Rotation de centre 0 et d'angle $2\pi/3$ et réflexion d'axe réel, respectivement.

---

2. Trouver les plus petits entiers naturels non nuls m et n tels que $s^m = r^n = \mathrm{Id}$.

---

1 et 3, respectivement.

---

3. Exprimer $s \circ r \circ s$ (qu'on pourra noter srs) comme une puissance de r.

Si $z \in \mathbf{C}$,

$$(s \circ r \circ s)(z) = (s \circ r)(\overline{z}) = \overline{j\overline{z}} = \overline{j}z = j^2 z = r^2(z)$$

---

4. On veut montrer que

$$G = \{\mathrm{Id}, r, r^2, s, s \circ r, s \circ r^2\}$$

est stable par $\circ$.

(a) Trouver deux entiers naturels u et v tels que

$$s \circ r = r^u \circ s \qquad \text{et} \qquad r \circ s = s \circ r^v$$

En composant $s \circ r \circ s = r^2$ par s à droite, on obtient

$$s \circ r = r^2 \circ s$$

et en composant par s à gauche,

$$r \circ s = s \circ r^2$$

(b) Compléter le tableau page suivante (à l'intersection de la ligne de g_i et de la colonne de g_j, inscrire $g_i \circ g_j$) pour montrer la stabilité de G par $\circ$.

5. Montrer que $(G, \circ)$ est un groupe non commutatif.

La table montre que $(G, \circ)$ est bien un groupe. Mais $r \circ s \neq s \circ r$, sinon on aurait $s \circ r \circ s = r$ ce qui n'est pas vrai.

---

6. Montrer que $(G, \circ)$ est isomorphe à $(\mathfrak{S}_3, \circ)$.

On considère $\tau = (12)$ (transposition) et $c = (123)$ (3-cycle). Alors $(\sigma_3, \circ) = \{Id, c, c^2, \tau, \tau \circ c, \tau \circ c^2\}$ et on a la relation $\tau \circ c \circ \tau = c^2$ qui permet d'obtenir la même table que celle de $(G, \circ)$. Il y a un isomorphisme unique ϕ de $(G, \circ)$ sur $(\mathfrak{S}_3, \circ)$ tel que $\phi(r) = c$ et $\phi(s) = \tau$.

---

7. Faire la liste des sous-groupes de $(G, \circ)$.

Si un sous-groupe contient r, il contient r^2, et réciproquement car $r = (r^2)^2$. S'il contient en plus s ou $s \circ r$ ou $s \circ r^2$, il contient r et s donc c'est le groupe entier. Si un sous-groupe contient deux éléments parmi s, $s \circ r$, $s \circ r^2$, il contient r (le plus dur est de le voir si le groupe contient $s \circ r$ et $s \circ r^2$. Dans ce cas il contient $s \circ r \circ s \circ r^2 = r^4 = r$). Finalement, les sous-groupes sont

$$G, \{Id\}, \{Id, s\}, \{Id, s \circ r\}, \{Id, s \circ r^2\}, \{Id, r, r^2\}$$

---

8. Tracer le triangle équilatéral de sommets 1, j, j^2. Tracer les axes des réflexions qui le laissent invariant. Déterminer les angles des rotations de centre 0 qui le laissent invariant.

Intéressant : le groupe $(G, \circ)$ est le groupe des isométries laissant le triangle équilatéral invariant.

$\circ$	Id	r	r^2	s	$s \circ r$	$s \circ r^2$
Id						
r						
r^2						
s						
$s \circ r$						
$s \circ r^2$						

$\circ$	Id	r	r^2	s	$s\circ r$	$s\circ r^2$
Id	Id	r	r^2	s	$s\circ r$	$s\circ r^2$
r	r	r^2	Id	$s\circ r^2$	s	$s\circ r$
r^2	r^2	Id	r	$s\circ r$	$s\circ r^2$	s
s	s	$s\circ r$	$s\circ r^2$	Id	r	r^2
$s\circ r$	$s\circ r$	$s\circ r^2$	s	r^2	Id	r
$s\circ r^2$	$s\circ r^2$	s	$s\circ r$	r	r^2	Id

X POLYNÔMES, NOMBRES COMPLEXES

Exercice 55 (Oral Mines)**.** Dans $\mathbf{R}[X]$, quel est le reste de la division de $X^n + 3X^{n-1} + 2$ par $(X-1)^2$?

Exercice 56 (Oral Centrale)**.** Soit P un polynôme à coefficients rationnels, irréductible sur $\mathbf{Q}[X]$. Montrer que les racines complexes de P sont toutes simples (on pourra penser à utiliser le théorème de Bezout !)

Exercice 57 (Oral Centrale, Mines)**.** On cherche les polynômes réels non nuls tels que $P(X^2) = P(X-1)P(X)$. (N.B. Cet exercice, classique de l'oral, est en général donné sans indication. Sa résolution repose sur une idée : scinder le polynôme sur $\mathbf{C}$, et raisonner sur les racines)

1. Soit z une racine complexe de P. Montrer que $z = 0$ ou $|z| = 1$.
2. Montrer que, si z est une racine complexe de P, alors $(z+1)^2$ l'est aussi.
3. En déduire que les seules racines possibles pour P sont 0, -1 et deux racines de l'unité que l'on précisera.
4. Trouver, à l'aide des questions précédentes, tous les polynômes P qui vérifient la condition donnée.

Enoncés analogues : trouver les polynômes $P \in \mathbf{R}[X]$ tels que
$(X+3)P(X) = XP(X+1)$ (oral centrale),
trouver les polynômes de $\mathbf{C}[X]$ tels que
$(X+4)P(X) = XP(X+1)$ (oral mines).

Exercice 58. Soit $P = \sum_{k=0}^{n} a_i X^i$ un polynôme scindé de degré n, $\alpha_1, \ldots, \alpha_n$ ses racines (répétées avec leur ordre de multiplicité), supposées non nulles.

1. Construire un polynôme Q de degré n dont les racines sont $1/\alpha_1, \ldots, 1/\alpha_n$. En déduire une expression de $\sum_{i=1}^{n} \frac{1}{\alpha_i}$ à l'aide des a_i.
2. Calculer directement $\sum_{i=1}^{n} \frac{1}{\alpha_i}$ à l'aide des a_i, en réduisant au même dénominateur.

Exercice 59. Soit $P = \sum_{i=0}^{n} a_i X^i$ un polynôme scindé de degré n. Calculer en fonction des a_i la somme des carrés des racines de P.

Exercice 60. Soit n un entier ≥ 2. Calculer
$\prod_{k=1}^{n-1} \left(1 - e^{2ik\pi/n}\right)$ (oral mines)
$\prod_{k=1}^{n-1} \left(1 + e^{2ik\pi/n}\right)$ (oral X)
$\prod_{k=1}^{n-1} \left(\frac{1+\omega^k}{1-\omega^k}\right)$ où $\omega = e^{2i\pi/n}$ (oral X, oral Centrale)

Exercice 61 (Oral Centrale)**.** Soit $P = X^3 + aX^2 + bX + c$ un polynôme complexe de racines α, β, γ. Calculer

$$\frac{\alpha}{\beta+\gamma} + \frac{\beta}{\alpha+\gamma} + \frac{\gamma}{\beta+\alpha}$$

Exercice 62 (Polynômes de Tchebitcheff, classique)**.**
Les polynômes de Tchebitcheff (ou Tchebychev, ou...) ont beaucoup de propriétés intéressantes. Il n'est donc pas étonnant de les retrouver fréquemment dans des énoncés. Les questions 1 à 4 sont classiques et intéressantes.

1. Montrer avec la formule de De Moivre que, pour tout entier naturel n, il existe un unique polynôme T_n à coefficients réels tel que

$$\forall \theta \in \mathbf{R} \qquad \cos n\theta = T_n(\cos\theta)\ .$$

2. En utilisant la formule $\cos(n+1)\theta + \cos(n-1)\theta\ = \cdots$, redémontrer l'existence des T_n et trouver une relation de récurrence entre T_{n+1}, T_n, T_{n-1}.
3. Trouver tous les zéros de T_n.
4. Trouver une équation différentielle linéaire du second ordre vérifiée par T_n.
5. (*Oral Centrale*) Décomposer en éléments simples la fraction $\dfrac{1}{T_n}$.
6. (*Oral X*) Calculer

$$\sum_{k=0}^{n-1} \frac{1}{\cos^2\left(\frac{\pi}{2n} + \frac{k\pi}{n}\right)}$$

---

3. On résout, pour θ réel,

$$\begin{aligned} T_n(\cos\theta) = 0 &\Leftrightarrow \cos(n\theta) = 0 \\ &\Leftrightarrow n\theta \equiv \pi/2\ [\pi] \end{aligned}$$

Les $\cos\left(\dfrac{\pi}{2n} + \dfrac{k\pi}{n}\right)$ sont donc racines de T_n. Pour $k = 0, \ldots, n-1$ cela donne n racines distinctes (cos est injective sur $[0, \pi]$ car strictement décroissante). Or T_n est de degré n, on a donc toutes les racines.
5. C'est une fraction à pôles simples. Donc on peut appliquer la formule

$$\frac{1}{T_n} = \sum_{k=1}^{n} \frac{1}{T_n'(c_k)(X - c_k)}$$

où $c_1, \ldots, c_n$ sont les racines trouvées en 3. Mais on a par dérivation :

$$-n\sin(n\theta) = -\sin\theta\ T_n'(\cos\theta)$$

qui, appliquée à $\dfrac{\pi}{2n} + \dfrac{k\pi}{n}$, donne

$$T_n'(c_k) = n\frac{(-1)^k}{s_k}$$

en notant $c_k = \cos\left(\dfrac{\pi}{2n} + \dfrac{k\pi}{n}\right)$ et $s_k = \sin\left(\dfrac{\pi}{2n} + \dfrac{k\pi}{n}\right)$. Avec ces notations on a donc

$$\frac{1}{T_n} = \frac{1}{n}\sum_{k=1}^{n} \frac{(-1)^k s_k}{X - c_k}$$

6. Plus astucieux. Remarquer que le problème n'a de sens que si n pair (sinon il y a un c_k nul). Supposons donc n pair, les $1/c_k$ sont les racines du polynôme $X^n T_n(1/X)$, la somme de leurs carrés vaut le carré de la somme à laquelle on soustrait les doubles produits, bref une sorte de $\sigma_1^2 - 2\sigma_2$. Il n'y a plus qu'à appliquer les relations entre polynômes et racines au polynôme $X^n T_n(1/X)$.

Exercice 63 (cours, programme mpsi)**.** Décomposer en éléments simples le polynôme $\dfrac{P'}{P}$

Un cas très particulier de décomposition, à bien voir car il ne se traite pas suivant les méthodes habituelles. Tout en étant très simple. Remarquons que le cas de pôles simples s'obtient bien par la formule habituelle, et permet de retrouver le cas général. P'/P est la « dérivée logarithmique » de P, on demande parfois à l'oral de montrer qu'elle transforme produit en somme, ce qui donne l'indication pour parvenir au résultat.

Si $P = \prod_{k=1}^{r}(X-\alpha^k)^{m_k}$, alors $P' = \sum_{k=1}^{r} m_k \left((X-\alpha_k)^{m_k-1} \prod_{j\neq k}(X-\alpha^j)^{m_j} \right)$ ce qui donne

$$\frac{P'}{P} = \sum_{k=1}^{r} \frac{m_k}{X-\alpha_k}$$

On peut aussi partir de l'expression $P = \prod_{k=1}^{d}(X-\beta_k)$ (on ne suppose pas les racines distinctes, mais on les répète autant de fois que leur ordre de multiplicité), on a alors $P' = \sum_{k=1}^{d} \left(\prod_{j\neq k}(X-\beta_j) \right)$ et

$$\frac{P'}{P} = \sum_{j=1}^{d} \frac{1}{X-\beta_j}$$

qui est bien la même formule.

Exercice 64 (Oral Mines)**.** Décomposer en éléments simples le polynôme $\dfrac{X^{n-1}}{X^n-1}$.

On reconnaît qu'à un facteur près c'est une fraction P'/P. Si on n'y pense pas, ce n'est pas grave, on utilise la formule avec les pôles simples. On trouve

$$\frac{1}{n}\sum_{\zeta\in\mathbf{U}_n} \frac{1}{X-\zeta}$$

ou encore, si on préfère les indexations plus standard :

$$\frac{1}{n}\sum_{k=1}^{n} \frac{1}{X-\exp(2ik\pi/n)}$$

(l'indexation peut aussi se faire pour k allant de 0 à $n-1$).

Exercice 65 (Décomposition en éléments simples avec pôles simples)**.**

1. Soit P un polynôme scindé simple, $\alpha_1, \ldots, \alpha_n$ ses racines ; écrire la décomposition en éléments simples de $1/P$.
2. Décomposer en éléments simples sur $\mathbf{C}$ la fraction rationnelle
$$\frac{1}{X^n - 1}\ .$$
3. Si P est un polynôme à racines simples non nulles $\alpha_1, \ldots, \alpha_n$, trouver une relation entre $P(0)$ et $\displaystyle\sum_{k=1}^{n} \frac{1}{\alpha_k P'(\alpha_k)}$.

---

1. On utilise la formule pour les pôles simples :
$$1/P = \sum_{k=1}^{n} \frac{1}{P'(\alpha_k)(X - \alpha_k)}$$

2. C'est un exemple d'application de la formule précédente. On peut présenter le résultat de diverses manières. Par exemple, en notant $\omega = \exp(2i\pi/n)$,
$$\frac{1}{X^n - 1} = \sum_{k=1}^{n} \frac{1}{n(\omega^k)^{n-1}(X - \omega^k)} = \frac{1}{n} \sum_{k=1}^{n} \frac{\omega^k}{X - \omega^k}$$
Mais le plus élégant est l'indexation par l'ensemble $\mathbf{U}_n$ des racines n-ièmes de l'unité :
$$\frac{1}{X^n - 1} = \frac{1}{n} \sum_{\zeta \in \mathbf{U}_n} \frac{\zeta}{X - \zeta}$$

3. Il suffit de réécrire la formule du 1 et d'appliquer la relation entre fonctions rationnelles associées à la valeur 0 de la variable.

Exercice 66 (Théorème de Lucas)**.** Soit P un polynôme de $\mathbf{C}[X]$, de degré au moins 2. En utilisant la décomposition en éléments simples de P'/P (on pourra considérer la conjuguée de cette décomposition), démontrer que les racines de P' se trouvent dans l'enveloppe convexe de celles de P (autre formulation : démontrer que toute racine de P' est barycentre à coefficients positifs de celles de P).

Soit $(\alpha_i, m_i)_{1 \leq i \leq r}$ la famille des racines de P comptées avec leur multiplicité. Alors, si z n'est pas racine de P,
$$\frac{P'(z)}{P(z)} = \sum_{i=1}^{r} \frac{m_i}{z - \alpha_i}$$

Supposons que z soit une racine de P' qui ne soit pas une racine de P. Alors $0 = \sum_{i=1}^{r} \frac{m_i}{z-\alpha_i}$ et donc $0 = \sum_{i=1}^{r} \frac{m_i}{\overline{z-\alpha_i}}$. Réécrivons cette relation :

$$\sum_{i=1}^{r} \frac{m_i}{|z-\alpha_i|^2}(z-\alpha_i) = 0$$

et donc le point d'affixe z est barycentre de la famille de points (A_i, k_i), où les $k_i = \frac{m_i}{|z-\alpha_i|^2}$ sont des réels positifs, et les A_i les points d'affixes α_i.

Exercice 67 (Centrale)**.** Soit $P \in \mathbf{R}_n[X]$ scindé à racines simples $(x_1, \ldots, x_n)$. Montrer que

$$\sum_{k=1}^{n} \frac{P''(x_k)}{P'(x_k)} \;=\; 0.$$

Un genre d'exercice assez astucieux, où il peut être utile de se souvenir de la formule de décomposition en éléments simples de P/Q dans le cas de pôles simples. On commence par dire que, d'après le théorème de Rolle par exemple, si P est scindé simple alors P' l'est aussi (c'est faux sur un corps autre que $\mathbf{R}$, prendre par exemple $X^n - 1$ dans $\mathbf{C}[X]$). On décompose en éléments simples la fraction P''/P, on multiplie par X, on fait tendre la variable vers $+\infty$ dans l'égalité entre fonctions polynômes associées...

Exercice 68. Dans $\mathbf{Z}/p\mathbf{Z}$ (p premier), montrer que la fonction polynôme associée à $X^p - X$ est la fonction nulle.

C'est une conséquence du théorème de Fermat.

Exercice 69 (Oral X)**.** Soit a, b, c trois nombres complexes de même module, $a \neq c$. Montrer que $\frac{a}{b}\frac{(c-b)^2}{(c-a)^2}$ est un réel positif.

On écrit $a = re^{i\alpha}$, $b = re^{i\beta}$, $c = re^{i\gamma}$, puis on utilise des factorisations du type

$$e^{i\gamma} - e^{i\beta} = e^{i(\beta+\gamma)/2}(\ldots)$$

Exercice 70. Ecrire sous forme factorisée la somme

$$\sum_{k=0}^{n} \sin(2k+1)x$$

Techniques habituelles : on l'écrit comme partie imaginaire d'une somme géométrique, puis on utilise des factorisations du type

$$e^{ia} \pm e^{ib} = e^{i(a+b)/2}(\dots)$$

Exercice 71 (Oral X)**.** Calculer $\cos\dfrac{\pi}{13} + \cos\dfrac{3\pi}{13} + \cdots + \cos\dfrac{11\pi}{13}$.

Il s'agit de la partie réelle de

$$\sum_{k=0}^{5} e^{i(2k+1)\pi/13}$$

qui est une somme géométrique, valant

$$e^{i\pi/13}\frac{1-e^{12i\pi/13}}{1-e^{2i\pi/13}}$$

c'est-à-dire

$$e^{i\pi/13}\frac{e^{6i\pi/13}}{e^{i\pi/13}}\frac{\sin(6\pi/13)}{\sin(\pi/13)}$$

La partie réelle vaut donc

$$\frac{1}{2}\frac{\sin(12\pi/13)}{\sin(\pi/13)}$$

c'est-à-dire $1/2$, tout simplement !

Exercice 72 (Noyau de Dirichlet, noyau de Féjer)**.**

1. On définit, si $n \in \mathbf{N}_*$, pour tout réel x,

$$D_n(x) = \sum_{k=-n}^{n} e^{ikx}$$

Démontrer que, si x n'est pas un multiple de 2π,

$$D_n(x) = \frac{\sin\left((n+\frac{1}{2})x\right)}{\sin\left(\frac{x}{2}\right)} \tag{1}$$

Combien vaut $D_n(x)$ si x est un multiple de 2π ? Vérifier la cohérence en regardant la limite quand $x \to 0$ de l'expression (1).

2. On définit, si $n \in \mathbf{N}_*$, pour tout réel x,

$$F_n(x) = \frac{1}{n} \sum_{k=0}^{n-1} D_k(x)$$

Montrer que, si x n'est pas un multiple de 2π,

$$F_n(x) = \frac{1}{n} \left(\frac{\sin\left(\frac{nx}{2}\right)}{\sin\left(\frac{x}{2}\right)} \right)^2 \tag{2}$$

Calculer d'autre part $F_n(x)$ si x n'est pas un multiple de 2π. Vérifier de nouveau la cohérence en regardant la limite quand x tend vers 0 de l'expression (2).

D'abord, pas trop dur, le noyau de Dirichlet, si $x \not\equiv 0[2\pi]$, i.e. si $e^{ix} \neq 1$, on se contente des techniques habituelles :

$$\begin{aligned} D_n(x) &= \sum_{k=-n}^{n} e^{ikx} \\ &= \frac{e^{-inx} - e^{i(n+1)x}}{1 - e^{ix}} \\ &= \frac{e^{-i(n+1/2)x} - e^{i(n+1/2)x}}{e^{-ix/2} - e^{ix/2}} \\ &= \frac{\sin\left((n + \frac{1}{2})x\right)}{\sin\left(\frac{x}{2}\right)} \end{aligned}$$

La limite en 0 de cette expression est $2n + 1$, ça tombe bien c'est précisément la valeur en 0 de D_n, et aussi sa valeur en tout multiple de 2π car D_n est 2π-périodique.
Pour le noyau de Féjer, c'est une autre histoire. Il y a plusieurs manières de s'y prendre, et certaines donnent des calculs pas évidents. On va partir du principe qu'en général, quand on demande le noyau de Féjer, on connaît celui de Dirichlet. L'avantage, c'est qu'on continue avec les techniques classiques. On multiplie tout par n, parce que le $1/n$ n'a pas l'air de compter beaucoup, on le retrouve intact entre le début et la fin.

$$\begin{aligned} nF_n(x) \sin\left(\frac{x}{2}\right) &= \sum_{k=0}^{n-1} \sin\left(\left(k + \frac{1}{2}\right) x\right) \\ &= \operatorname{Im}\left(\sum_{k=0}^{n-1} \exp\left(i \left(k + \frac{1}{2}\right) x \right) \right) \\ &= \operatorname{Im}\left(e^{ix/2} \frac{1 - e^{inx}}{1 - e^{ix}} \right) \\ &= \operatorname{Im}\left(e^{inx/2} \frac{\sin\left(\frac{nx}{2}\right)}{\sin\left(\frac{x}{2}\right)} \right) \end{aligned}$$

ce qui amène le résultat. De nouveau vérifiable en 0 car

$$\frac{1}{n}\sum_{k=0} n - 1(2k+1) = \frac{1}{n}\left((n-1)n+n\right) = n$$

qui est bien la limite en 0 de l'expression au second membre de (2).

XI Exercices divers

Exercice 73 (Indicatrice d'Euler : méthode probabiliste).
Soit $n \geq 2$, on munit $\Omega = \{1, 2, \ldots, n\}$ de la probabilité uniforme P. On note $\{p_1, \ldots, p_r\}$ l'ensemble des diviseurs premiers de n. On désigne par ϕ l'indicatrice d'Euler.

1. Soit d un diviseur de n ($d \geq 1$), A_d l'ensemble des multiples de d dans Ω. Calculer $P(A_d)$.
2. (a) Montrer que les évènements A_{p_i} ($1 \leq i \leq r$) sont mutuellement indépendants.
   (b) En déduire que
   $$\frac{\phi(n)}{n} = \prod_{i=1}^{r}\left(1 - \frac{1}{p_i}\right)$$
   (c) Calculer $\phi(36)$

---

1. Comme P est la probabilité uniforme sur Ω,

$$P(A_d) = \frac{\mathrm{Card}(A_d)}{\mathrm{Card}(\Omega)}$$

Or $A_d = \left\{d, 2d, \ldots, \frac{n}{d}d\right\}$. Donc $\mathrm{Card}(A_d) = \frac{n}{d}$, et

$$P(A_d) = \frac{1}{d}$$

2.a. Attention à ne pas se contenter de montrer qu'ils sont indépendants deux à deux. Soit $\{i1, \ldots, im\}$ ($1 \leq m \leq r$) une partie finie de $\{1, \ldots, r\}$. On a (c'est une conséquence du théorème de Gauss) :

$$\bigcap_{k=1}^{m} A_{p_{ik}} = A_{p_{i1}\ldots p_{im}}$$

(les p_{ik} sont des nombres premiers distincts, être divisible par leur produit c'est être divisible par chacun d'eux) ; donc

$$P\left(\bigcap_{k=1}^{m} A_{p_{ik}}\right) = \frac{1}{p_{i1}\ldots p_{im}} = \prod_{k=1}^{m} P\left(A_{p_{ik}}\right)$$

On en déduit l'indépendance mutuelle. Soit alors B l'ensemble des éléments de Ω premiers avec n. Ecrivant

$$B = \bigcap_{i=1}^{r} \overline{A_{p_i}}$$

et utilisant le fait que des complémentaires d'événements indépendants le sont, on trouve la formule. Et donc

$$\phi(36) = 36 \times \left(1 - \frac{1}{2}\right) \times \left(1 - \frac{1}{3}\right) = 12$$

Exercice 74. Une belle formule de dénombrement, oral ens
Soit p un nombre premier ≥ 3, $n \in \mathbf{N}_*$, $a_1, \ldots, a_n \in \mathbf{N}$, $r_1, \ldots, r_n \in \mathbf{N} \setminus \{0, 1\}$ et

$$\begin{array}{rccc} F & : & (\mathbf{Z}/p\mathbf{Z})^n & \longrightarrow & \mathbf{Z}/p\mathbf{Z} \\ & & (x_1, \ldots, x_n) & \longmapsto & \displaystyle\sum_{i=1}^{n} a_i x_i^{r_i} \end{array}$$

Soit enfin N le nombre de solutions de l'équation $F(x_1, \ldots, x_n) = 0$. Prouver que

$$N = p^{n-1} + \frac{1}{p} \left(\sum_{x \in (\mathbf{Z}/p\mathbf{Z})^*} \left(\prod_{i=1}^{n} \left(\sum_{y \in \mathbf{Z}/p\mathbf{Z}} \zeta^{a_i x y^{r_i}} \right) \right) \right)$$

où $\zeta = e^{2i\pi/p}$.

On n'y comprend rien...dans ce cas, une bonne idée peut être d'examiner des cas particuliers...mais ici, on va essayer de démêler un peu la grosse expression dans le membre de droite. On va développer, si $x \in (\mathbf{Z}/p\mathbf{Z})^*$,

$$\psi(x) = \prod_{i=1}^{n} \left(\sum_{y \in \mathbf{Z}/p\mathbf{Z}} \zeta^{a_i x y^{r_i}} \right)$$

par distributivité. On le transformera ainsi en une somme :

$$\psi(x) = \sum_{(y_1, \ldots, y_n) \in (\mathbf{Z}/p\mathbf{Z})^n} \left(\zeta^{a_1 x y_1^{r_1}} \zeta^{a_2 x y_2^{r_2}} \ldots \zeta^{a_n x y_n^{r_n}} \right)$$

ce qui gagne à être écrit :

$$\psi(x) = \sum_{(y_1, \ldots, y_n) \in (\mathbf{Z}/p\mathbf{Z})^n} \zeta^{xF(y_1, \ldots, y_n)}$$

Intervertir deux sommes finies ne pose pas de problème, donc

$$\sum_{x \in (\mathbf{Z}/p\mathbf{Z})^*} \psi(x) = \sum_{(y_1, \ldots, y_n) \in (\mathbf{Z}/p\mathbf{Z})^n} \left(\sum_{x \in (\mathbf{Z}/p\mathbf{Z})^*} \zeta^{xF(y_1, \ldots, y_n)} \right)$$

Bien sûr, si $F(y_1, \ldots, y_n) = \overline{0}$,

$$\sum_{x \in (\mathbf{Z}/p\mathbf{Z})^*} \zeta^{xF(y_1, \ldots, y_n)} = p - 1$$

en revanche, si $F(y_1,\dots,y_n) \neq \overline{0}$, l'application $x \mapsto xF(y_1,\dots,y_n)$ est une bijection de $(\mathbf{Z}/p\mathbf{Z})^*$ sur lui-même. Or

$$\sum_{u\in(\mathbf{Z}/p\mathbf{Z})^*} \zeta^u = \sum_{k=1}^{p-1} \zeta^k = -1$$

Il ne reste plus qu'à calculer :

$$\frac{1}{p}\left(N\times(p-1)+(p^n-N)\times(-1)\right) = N - p^{n-1}$$

qui donne le résultat cherché.

Exercice 75 (Oral X)**.** Soit des complexes $z_1,\dots,z_n$. Montrer l'existence d'une partie I de $[1,n]$ telle que $\left|\sum_{k\in I} z_k\right| \geq \frac{1}{6}\sum_{k=1}^{n}|z_k|$.

L'idée de départ n'est pas très compliquée : il y a égalité dans l'inégalité triangulaire lorsque les nombres complexes qui y figurent ont même argument. On essaye ici de faire un paquet le plus gros possible de complexes ayant des arguments pas trop différents. Il vaut mieux se représenter les choses graphiquement. Quitte à appliquer une rotation (qui ne change rien au problème), on peut supposer, en notant

$$I = \{k\in[\![1,n]\!]\ ;\ \mathrm{Arg}(z_k)\in[-\pi/3,\pi/3]\}$$

que

$$\sum_{k\in I}|z_k| \geq \frac{1}{3}\sum_{k=1}^{n}|z_k|$$

Mais, d'autre part,

$$\left|\sum_{k\in I} z_k\right| \geq \mathrm{Re}\left(\sum_{k\in I} z_k\right) \geq \sum_{k\in I}\mathrm{Re}(z_k) \geq \frac{1}{2}\sum_{k\in I}|z_k|$$

Exercice 76 (Oral X)**.** *Un grand classique, intéressant, mais pas si facile...*
Soit $P\in\mathbf{R}[X]$ scindé à racines simples.

1. En considérant la fraction rationnelle P'/P, montrer que $P'^2 - PP''$ n'a pas de racine réelle.
2. On écrit $P = \sum_{i=0}^{n} a_i X^i$. Montrer que, pour tout k entre 1 et $n-1$, $a_{k-1}a_{k+1} < a_k^2$ (commencer par $k=1$).

1. On commence par se poser la question : quel lien peut-il y avoir entre P'/P et $P'^2 - PP''$? il faut penser à la dérivation :

$$\Big(\frac{P'}{P}\Big)' = \frac{P''P - P'^2}{P^2}$$

Comment en déduire qu'il n'y a pas de racine réelle ? une autre idée est utile ici : décomposer en éléments simples P'/P. La dérivation de cette décomposition donne

$$\Big(\frac{P'}{P}\Big)' = \sum_{i=1}^{n} \frac{-1}{(X - x_i)^2}$$

où les x_i sont les racines de P. En passant aux fonctions rationnelles associées, on obtient que

$$(P'^2 - PP'')(x) > 0$$

(on note de la même manière polynôme et fonction polynôme associée)...mais ce n'est valable que pour $x \neq x_i$ $(1 \leq i \leq n)$ a priori, car les fonctions rationnelles considérées ne sont pas définies en les x_i qui sont pôles. Mais d'autre part, comme $P(x_i) = 0$, si x_i est un zéro de $P''P - P'^2$ il sera aussi zéro de P', ce qui contredit le fait que toutes les racines de P sont simples.
2. On vient de voir que $P'^2 - PP''$ était à valeurs strictement positives ; en particulier en 0, ce qui permet d'affirmer que

$$a_1^2 > 2a_0a_2$$

inégalité plus forte que celle demandée, mais gardons-la prudemment.
Comment continuer ? en utilisant le théorème de Rolle (décidément, il y a beaucoup d'idées à avoir, dans cet exercice...), on montre que si P est un polynôme réel scindé à racines simples, P' aussi (entre deux racines consécutives de P, il y a au moins une racine de P', ce qui donne au moins autant de racines distinctes pour P' que son degré, il ne peut d'autre part pas y en avoir plus). En appliquant l'inégalité qu'on vient de trouver à P', on obtient :

$$(2a_2)^2 > (2a_1)(3a_3)$$

d'où l'on tire $a_2^2 > 3a_1a_3/2$ ce qui conclut pour $k = 2$. Il n'est guère plus difficile de dire, pour $r \leq n - 2$, que $P^{(r)}$ est scindé simple (application récurrente du théorème de Rolle), et d'appliquer l'inégalité $a_1^2 > 2a_0a_2$ à $P^{(r)}$ pour obtenir la conclusion voulue.

Exercice 77 (Oral X)**.** Le polynôme X^4+4 est-il irréductible sur $\mathbf{Q}[X]$? Quels sont les entiers naturels n tels que $n^4 + 4$ soit premier ?

Il n'est pas trop difficile de montrer que le polynôme n'a pas de racine rationnelle ; s'il y a une factorisation, c'est en un produit de deux polynômes de degré 2. Mais

$$X^4 + 4 = (X^2 + 2)^2 - 4X^2 = (X^2 - 2X + 2)(X^2 + 2X + 2)$$

Si n est pair, n^4+4 l'est. Et il ne vaut pas 2. Si $5 \not| n$, n^4+4 est divisible par 5. Si $n=1$, cela ne l'empêche pas d'être premier. Mais si $n \neq 1$, si. Si n^4+4 est premier, la factorisation

$$n^4+4 = (n^2-2n+2)(n^2+2n+2)$$

n'en est pas une « vraie ». Or, si $n \geq 2$, $1 < n^2-2n+2 < n^2-2n+2$, la factorisation en est donc une vraie. La seule possibilité est $n=1$.

Exercice 78 (Oral Cachan)**.** Soit P un polynôme ; montrer que $P(X)-X$ divise $P(P(X))-X$.

Il revient au même de montrer que $P(X)-X$ divise $P\left(P(X)\right)-P(X)$, qui est combinaison linéaire de termes du type $(P(X))^n - X^n$ dans lesquels on peut bien factoriser $P(X)-X$.

Exercice 79 (Oral X)**.** Soit $x_1, \ldots, x_k$ des nombres complexes, on pose $u_n = \sum_{i=1}^{k} x_i^n$ (les u_n sont appelés sommes de Newton).

1. Trouver une relation de récurrence linéaire satisfaite par la suite u.
2. On suppose les x_i distincts, on pose $P = \prod_{i=1}^{k}(X-x_i)$. Calculer $\sum_{i=1}^{k} \frac{1}{P'(x_i)}$.
3. Avec les hypothèses et notations du **b.**, donner un système permettant de calculer, pour $n \in [0, k-1]$, la valeur de u_n en fonction de $u_0, \ldots, u_{n-1}$.

---

1. Utilisons déjà les notations de 2., et posons

$$P = \prod_{i=1}^{k}(X-x_i) = X^k + a_1 X^{k-1} + \cdots + a_k$$

(on sait par ailleurs que

$$a_j = (-1)^j \sigma_j$$

où les σ_j sont les fonctions symétriques élémentaires de $x_1, \ldots, x_k$. On a alors, pour tout i,

$$x_i^k + a_1 x_i^{k-1} + \ldots + a_1 x_i + a_k$$

et, en multipliant par x_i^{n-k} et en ajoutant xes relations pour $i \in [\![1,k]\!]$, on obtient

$$\forall n \geq k \qquad u_n + a_1 u_{n-1} + \ldots + a_k u_{n-k} = 0$$

2. Quelques réminiscences de la formule de décomposition simple d'une fraction à pôles simples peuvent aider. On décompose donc $1/P$, on multiplie par X,

on fait tendre la variable vers $+\infty$ dans l'égalité entre fractions rationnelles associées, on obtient le résultat : 0 (en supposant $k \geq 2$, mais le cas $k = 1$ n'est pas très intéressant !).
3. Il n'est pas vraiment restrictif de supposer les x_i non nuls. On développe alors en série entière $1/P$ à partir de sa décomposition en éléments simples, on multiplie par P, on écrit un produit de Cauchy et on utilise l'unicité du DSE...

Exercice 80 (Théorème de Wolstenholme, oral Centrale, X)**.**

1. Soit p un nombre premier ≥ 5. Montrer que $x \mapsto 1/x$ est une permutation de $\mathbf{Z}/p\mathbf{Z} \setminus \{\overline{0}\}$.
2. On écrit le rationnel $\displaystyle\sum_{i=1}^{p-1} \frac{1}{i}$ sous forme irréductible a/b. Montrer que p^2 divise a.

Exercice 81 (Théorème de Wolstenholme, oral Centrale)**.** Soit p un nombre premier, $S_p = \displaystyle\sum_{k=1}^{p-1} \frac{(p-1)!}{k(p-k)}$. On écrit $\displaystyle\sum_{k=1}^{p-1} \frac{1}{k} = \frac{a_p}{b_p}$ où a_p et b_p sont deux entier naturels premiers entre eux. La classe de $a \in \mathbf{Z}$ modulo p est notée $\overline{a}$.

1. Montrer que $(p-1)! \equiv -1\ [p]$.
2. Montrer : $\overline{S_p} = \displaystyle\sum_{x \in (\mathbf{Z}/p\mathbf{Z})^*} x^{-2} = \sum_{x \in (\mathbf{Z}/p\mathbf{Z})^*} x^2$.
3. Montrer que, pour $p \geq 5$, p divise S_p.
4. Montrer que, pour $p \geq 5$, p^2 divise a_p.

---

1. La congruence de Wilson est un classique.
2. Remarquons d'abord que $k(p-k)$ divise $(p-1)!$ pour tout k entre 1 et $p-1$; en effet, $(p-1)!$ est un produit de facteurs dont k et $p-k$ font partie (et ces deux facteurs sont bien distincts : $k = p-k$ donnerait p pair, d'où $p = 2$, cas trop évident pour être intéressant). Notons alors m_k le quotient de la division de $(p-1)!$ par $k(p-k)$:

$$(p-1)! = k(p-k)m_k$$

Alors, en prenant les classes modulo p (c'est-à-dire dans $\mathbf{Z}/p\mathbf{Z}$) :

$$\overline{(p-1)!} = \overline{k} \times \overline{p-k} \times \overline{m_k}$$

ou encore, tenant compte de la congruence de Wilson,

$$\overline{-1} = \overline{k} \times (\overline{-k}) \times \overline{m_k}$$

ce qui donne $\overline{m_k} = \overline{k}^{-2}$ et la formule attendue :

$$\overline{S_p} = \sum_{x \in (\mathbf{Z}/p\mathbf{Z})^*} x^{-2}$$

Mais l'application $x \mapsto x^{-1}$ est une permutation de $(\mathbf{Z}/p\mathbf{Z})^*$, on a donc bien

$$\overline{S_p} = \sum_{x \in (\mathbf{Z}/p\mathbf{Z})^*} x^{2}$$

Il importe dans cette question de supprimer les fractions pour bien faire de l'arithmétique avec des entiers, c'est ce qui motive l'introduction des m_k
3. La formule précédente montre :

$$\overline{S_p} = \sum_{k=1}^{p-1} \overline{k}^2 = \overline{\Big(\frac{(p-1)p(2p-1)}{6}\Big)}$$

grâce à une formule sommatoire « connue » (mais qu'il faut savoir démontrer...). En notant que, si m est un entier, $\overline{6m} = 6\ \overline{m}$, on en déduit que $\overline{6} \times \overline{S_p} = \overline{p-1} \times \overline{p} \times \overline{2p-1} = \overline{0}$ Mais p ne vaut ici ni 2 ni 3, donc est premier avec 6, on conclut bien $\overline{S_p} = \overline{0}$, donc p divise S_p.
4. Remarquons la décomposition en éléments simples :

$$\frac{1}{k(p-k)} = \frac{1}{p}\big(\frac{1}{k} + \frac{1}{p-k}\big)$$

d'où l'on déduit

$$pS_p = \sum_{k=1}^{p-1} (p-1)!\Big(\frac{1}{k} + \frac{1}{p-k}\Big) = 2(p-1)!\frac{a_p}{b_p}$$

ou encore (toujours pour supprimer les fractions)

$$b_p p S_p = 2(p-1)! a_p$$

p^2 divise le membre de gauche (car S_p est multiple de p), et donc celui de droite, et est premier avec $2(p-1)!$ (qui est produit de nombre premiers avec p, donc avec p^2). Le théorème de Gauss permet alors de conclure.

Exercice 82 (Oral Centrale)**.** Combien y-a-t-il de morphismes de $(\mathbf{Z}/n\mathbf{Z}, +)$ dans $(\mathbf{Z}/m\mathbf{Z}, +)$?

Remarque : comme souvent dans les problèmes sur les groupes cycliques, on peut déplacer le problème et étudier les morphismes de $\mathbf{U}_n$ dans $\mathbf{U}_m$. Il est d'ailleurs intéressant de réécrire le raisonnement ci-dessous dans ces termes.
On commence par analyser la situation : si ϕ est un tel morphisme, on a $\phi(0 \bmod n) = 0 \bmod m$. Et comme $1 \bmod n$ engendre le groupe cyclique $\mathbf{Z}/n\mathbf{Z}$, le tout est de connaître $\phi(1 \bmod n)$. Notons-le x. On a $nx = \phi\left(n(1 \bmod n)\right) =$

$\phi(n \bmod n) = 0 \bmod m)$, donc x est un élément de $\mathbf{Z}/m\mathbf{Z}$ dont l'ordre divise n. Mais son ordre divise aussi m. Donc son ordre divise $d = m \wedge n$. Réciproquement, soit x un élément de $\mathbf{Z}/m\mathbf{Z}$ d'ordre d. Il est alors légitime de définir

$$\phi(a \bmod n) = ax$$

pour $a \in \mathbf{Z}$ (on vérifie en effet que si $a \bmod n = b \bmod n$, alors $ax = bx$). Et cela définit bien un morphisme de $\mathbf{Z}/n\mathbf{Z}$ dans $\mathbf{Z}/m\mathbf{Z}$.
Conclusion : il y a autant de morphismes que d'éléments dont l'ordre divise d dans $\mathbf{Z}/m\mathbf{Z}$. Or, si a est un entier,

$$d(a \bmod m) = 0 \bmod m \ \Leftrightarrow \ m|da \ \Leftrightarrow \frac{m}{d} \mid a$$

Il y a donc d élements dont l'ordre divise d (ce sont : $0 \bmod m$, $\frac{m}{d} \bmod m$,..., $\frac{(d-1)m}{d} \bmod m$).

Exercice 83 (Oral X)**.** Soit G un groupe commutatif d'ordre pq, p et q premiers distincts. Montrer qu'il y a dans G un élément d'ordre pq.

On remarquera que dans les deux groupes commutatifs d'ordre pq que l'on connaît, il y a un élément d'ordre pq. Ces deux groupes sont en effet $\mathbf{Z}/pq\mathbf{Z}$ et $\mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/q\mathbf{Z}$. Dans le premier cas, $\overline{1}$ convient. Dans le second, $(1 \bmod p, 1 \bmod q)$ convient.
Soit $(G, *)$ un groupe commutatif. Ses éléments, à part l'élément neutre, sont d'ordre p, q ou pq. On montre que si x est d'ordre p et y d'ordre q, alors $x * y$ est d'ordre pq (pour cela, on n'utilise pas le fait que p et q soient premiers, mais seulement le fait qu'ils sont premiers entre eux et que le groupe est commutatif). En effet, si $(x * y)^m = e$, alors $(x * y)^{mp} = e$, or, par commutativité, $(x * y)^{mp} = x^{mp} * y^{mp} = y^{mp}$, donc $q \mid mp$, donc $q \mid m$, idem pour p, ce qui conclut.
On utilisera dans la suite le théorème de Lagrange : l'ordre d'un sous-groupe divise l'ordre du groupe. Ce n'est pas au programme, mais c'est un grand classique, il est bien de savoir le démontrer (voir exercice classique). Supposons que x soit un élément de G d'ordre p, soit y n'appartenant pas au sous-groupe $\langle x \rangle$. On note r l'ordre de y ($r = p$ ou $r = q$, nécessairement). Soit H le sous-groupe engendré par x et y. On a facilement

$$H = \{x^a * y^b \ ; \ (a, b) \in [\![0, p-1]\!] \times [\![0, m-1]\!]\}$$

Mais, d'autre part,

$$x^a * y^b = x^{a'} * y^{b'} \Leftrightarrow x^{a-a'} = y^{b'-b}$$

et, comme $y \notin \langle x, \rangle$, $\langle x \rangle \cap \langle y \rangle = \{e\}$ (c'est en effet un sous-groupe de $\langle y \rangle$ qui ne contient pas y, or $\langle y \rangle$ est un nombre premier). Donc H est d'ordre mp, qui divise pq, et $m > 1$, donc $m = q$, ce qui conclut.

Exercice 84. Soit p premier et n divisible par p. Soit $(G,*)$ un groupe d'ordre n, de neutre e et $E = \left\{(x_1,\dots,x_p) \in G^p \ / \ x_1 * x_2 * \cdots * x_p = e\right\}$. On définit la relation $\mathcal{R}$ sur E par

$$(x_1,\dots,x_p)\mathcal{R}(y_1,\dots,y_p) \ \Leftrightarrow \ \exists k \in [1,p] \ (y_1,\dots,y_p) = (x_k,\dots,x_p,x_1,\dots,x_{k-1}).$$

1. Montrer que $\mathcal{R}$ est une relation d'équivalence sur E.
2. Montrer que les classes d'équivalence de $\mathcal{R}$ ont 1 ou p éléments.
3. Montrer que $s + pq = n^{p-1}$ où s est le nombre de classes d'équivalence à un élément et q est le nombre de classes d'équivalence à p élḿents.
4. En déduire qu'il existe dans G au moins un élément d'ordre p.

---

1. Peut se montrer directement, ou utiliser le cycle

$$\sigma = (1\ 2\ \dots\ p)$$

En effet,

$$(x_1,\dots,x_p)\mathcal{R}(y_1,\dots,y_p) \Longleftrightarrow \exists k \in \mathbf{Z} \qquad (y_1,\dots,y_p) = (x_{\sigma^k(1)},\dots,x_{\sigma^k(p)})$$

Cette remarque rend la vérification plus simple.
2. Comme c est d'ordre p, la classe de x est l'ensemble des p-uplets $(x_{\sigma^k(1)},\dots,x_{\sigma^k(p)})$ pour $k = 0,1,\dots,p-1$.
Si tous les x_i sont égaux, la classe d'équivalence de $x = (x_1,\dots,x_p)$ a un élément.
Supposons qu'il existe $0 \leq k < k' \leq p-1$ tels que

$$(x_{\sigma^k(1)},\dots,x_{\sigma^k(p)}) = (x_{\sigma^{k'}(1)},\dots,x_{\sigma^{k'}(p)})$$

On aurait alors, pour tout i,

$$x_{\sigma^k(i)} = x_{\sigma^{k'}(i)}$$

ou encore, pour tout j,

$$x_j = x_{\sigma^{k'-k}(j)}$$

Donc, notant $c = \sigma^{k'-k}$,

$$x_1 = x_{c(1)} = \ldots = x_{c^{p-1}(1)}$$

Mais $c(j) \equiv j + (k'-k)\ [p]$, donc

$$c^m(1) = c^{m'}(1) \Longrightarrow \ 1 + (k'-k)m \equiv 1 + (k'-k)m'\ [p] \ \Longrightarrow \ m' \equiv m\ [p]$$

(car $(k'-k) \wedge p = 1$). On en déduit que $1, c(1), \dots, c^{p-1}(1)$ sont deux à deux distincts, donc ce sont tous les éléments de $[\![1,p]\!]$, donc on obtient bien

$$x_1 = x_2 = \ldots = x_n$$

et donc, si la classe de x a moins de p éléments, elle en a un seul.
3. Les classes d'équivalence forment une partition de E. Mais l'application $(x_1,\dots,x_p) \longmapsto (x_1,\dots,x_{p-1})$ est assez facilement une bijection de E sur G^{p-1}.

En effet, on peut écrire la bijection réciproque $(x_1, \ldots, x_{p-1}) \longmapsto (x_1, \ldots, x_{p-1}, (x_1 * \cdots * x_{p-1})^{-1})$. Donc $\mathrm{Card}(E) = n^{p-1}$, ce qui permet de conclure.
4. Et donc $s \equiv 0\ [p]$. Mais $s \neq 0$, car la classe de $(e, \ldots, e)$ est à un élément. Donc il y a une autre classe à un élément, i.e. un élément x_1 qui n'est pas e et qui vérifie $x_1^p = e$. Donc un élément d'ordre divisant p et qui n'est pas d'ordre 1, ce qui conclut.

Exercice 85 (Fonction de Möbius, extrait d'un problème d'ens)**.** On définit la fonction de Möbius sur $\mathbf{N} \setminus \{0\}$ par : $\mu(1) = 1$; si $n = p_1 p_2 \ldots p_r$ où les p_i sont premiers deux à deux distincts ($r \geq 1$), alors $\mu(n) = (-1)^r$. Dans tous les autres cas, $\mu(n) = 0$.

1. Soit n un entier naturel supérieur ou égal à 2. Démontrer que $\sum_{d|n} \mu(d) = 0$ ($\sum_{d|n}$ signifie la somme sur tous les diviseurs positifs de n).
2. Soit G une application de $\mathbf{N} \setminus \{0\}$ dans $\mathbf{C}$. On définit, sur $\mathbf{N} \setminus \{0\}$, F par
$$F(n) = \sum_{d|n} G(d)\ .$$
Démontrer qu'alors, pour tout entier naturel non nul n :
$$G(n) = \sum_{d|n} \mu(d) F\Big(\frac{n}{d}\Big)$$

C'est la formule d'inversion de Möbius ; la fonction de Möbius a été introduite par Euler, avant d'être étudiée par Möbius. Elle a des applications en arithmétique.

---

1. On décompose n en facteurs premiers :
$$n = \prod_{i=1}^{d} p_i^{m_i}$$
Un diviseur positif de n est un nombre de la forme
$$n' = \prod_{i=1}^{d} p_i^{m_i'}$$
où chaque m_i' est dans $[\![0, m_i]\!]$. Si l'un des m_i' est ≥ 2, n a un facteur carré, donc $\mu(n') = 0$. Donc, en ne gardant que les termes non nuls :
$$\begin{aligned}\sum_{d|n} \mu(d) &= \sum_{(\epsilon_1, \ldots, \epsilon_d) \in \{0,1\}^d} \mu\left(p_1^{\epsilon_1} \ldots p_d^{\epsilon_d}\right) \\ &= \sum_{(\epsilon_1, \ldots, \epsilon_d) \in \{0,1\}^d} (-1)^{\epsilon_1 + \ldots + \epsilon_d}\end{aligned}$$

Si $d = 1$, on trouve $\mu(n) = 1 - 1 = 0$. Sinon,

$$\begin{aligned}\sum_{d|n} \mu(d) &= \sum_{(\epsilon_2,\ldots,\epsilon_d)\in\{0,1\}^{d-1}} (-1)^{\epsilon_2+\ldots+\epsilon_d} \quad - \sum_{(\epsilon_2,\ldots,\epsilon_d)\in\{0,1\}^{d-1}} (-1)^{\epsilon_2+\ldots+\epsilon_d} \\ &= 0\end{aligned}$$

(on fait deux paquets : les termes pour $\epsilon_1 = 0$ et ceux pour $\epsilon_1 = 1$).
2. On calcule

$$\begin{aligned}\sum_{d|n} \mu(d) F\Big(\frac{n}{d}\Big) &= \sum_{d|n} \left(\mu(d) \sum_{d'|\frac{n}{d}} G(d') \right) \\ &= \sum_{d|n} \left(\sum_{d'|\frac{n}{d}} \mu(d) G(d') \right) \\ &= \sum_{dd'=n} \mu(d) G(d') \\ &= \sum_{d'|n} \left(G(d') \sum_{d|\frac{n}{d'}} \mu(d) \right) \\ &= G(n)\end{aligned}$$

On peut trouver l'indexation $\displaystyle\sum_{dd'=n}$ un peu floue, elle n'est pas si difficile à préciser : c'est

$$\sum_{(d,d')\in\{(k,\ell)\in N_*^2 \ ; \ k\ell=n\}}$$

Exercice 86 (Contenu d'un polynôme)**.** On se place sur l'anneau $\mathbf{Q}[X]$ des polynômes à coefficients rationnels. On note naturellement $\mathbf{Z}[X]$ l'ensemble des polynômes à coefficients entiers. Il est facile de voir que c'est un sous-anneau de $\mathbf{Q}[X]$.
Pour tout polynôme non nul $P = \sum a_i X^i \in \mathbf{Z}[X]$, on note $c(P)$ le pgcd de la famille (a_i) de ses coefficients. On dit que P est primitif lorsque $c(P) = 1$.

1. Si $n \in \mathbf{N}^*$ et P polynôme non nul à coefficients entiers, exprimer $c(nP)$ à l'aide de n et de $c(P)$.
2. Pour tout entier a et tout nombre premier p, on note $a \bmod p$ la classe de a dans $\mathbf{Z}/p\mathbf{Z}$. Vérifier que l'application

$$\begin{array}{rccc} \phi_p \ : & \mathbf{Z}[X] & \longrightarrow & \mathbf{Z}/p\mathbf{Z}[X] \\ & \sum a_i X^i & \longmapsto & \sum (a_i \bmod p) X^i \end{array}$$

est un morphisme d'anneaux. Ou, si l'on trouve cela trop fatigant, dire que c'est évident.

3. Soient A, B deux polynômes primitifs. Démontrer que, pour tout nombre premier p, $\phi_p(AB) \neq 0$. En déduire que le produit de deux polynômes primitifs est primitif.
4. En déduire que, si P et Q sont dans $\mathbf{Z}[X]$, $c(PQ) = c(P)c(Q)$.
5. Soit $A \in \mathbf{Z}[X]$, unitaire, et $P \in \mathbf{Q}[X]$, unitaire, tels que P divise A dans $\mathbf{Q}[X]$. Montrer que $P \in \mathbf{Z}[X]$.
6. Soit $P = 1 + X + \cdots + X^{p-1}$ où p est premier. Montrer que P est irréductible dans $\mathbf{Q}[X]$ (étudier l'irréductibilité de $R(X) = P(X+1)$ à l'aide du morphisme ϕ_p). *Il s'agit d'un cas d'irréductibilité des polynômes cyclotomiques.*
7. Le but de cette question est de retrouver le résultat de la deuxième question sans recours aux ϕ_p et à $\mathbf{Z}/p\mathbf{Z}$. Soit $A = \sum_{i=0}^{d} a_i X^i$ et $B = \sum_{j=0}^{\delta} b_j X^j$ deux polynômes de $\mathbf{Z}[X]$ primitifs. Soit p un nombre premier ; on pose $i_0 = \min\{i \in [0,d] \,/\, p \text{ nedivisepas } a_i\}$ et $j_0 = \min\{j \in [0,\delta] \,/\, p \text{ nedivisepas } b_j\}$. Jusitfier l'existence de i_0 et j_0, et en déduire qu'il existe au moins un coefficient de AB non divisible par p.
   Conclure

1.Par propriété du pgcd, c(nP)=nc(P)

2.Pas de difficulté, c'est un morphisme pour + et ×, qui transforme 1 en $\overline{1}$.

3. Si A et B sont primitifs, et si p est premier, alors $\phi_p(A) \neq 0$ et $\phi_p(B) \neq 0$. Par intégrité de $\mathbf{Z}/p\mathbf{Z}[X]$, $\phi_p(A)\phi_p(B) \neq 0$. Et donc $\phi_p(AB) \neq 0$. Il n'existe aucun nombre premier, donc, qui divise tous les coefficients de AB. Et donc le pgcd de ces coefficients est 1. Ce qui signifie que AB est primitif.

4. Les polynômes $\frac{1}{c(P)}P$ et $\frac{1}{c(Q)}Q$ sont primitifs, donc leur produit aussi. Donc :

$$c(PQ) = c(c(P)c(Q)\frac{1}{c(P)}P\frac{1}{c(Q)}Q = c(P)c(Q) \times 1$$

(on utilise **1.**).

5.Ecrivons

$$A = PQ$$

(Q est nécessairement unitaire) et soit p (respectivement q) le plus petit entier naturel non nul tel que pP (respectivement qQ) soit dans $\mathbf{Z}[X]$. Alors pP et qQ sont primitifs, et donc

$$pPqQ = pqA$$

l'est aussi. Ce qui, tous les coefficients de pqA étant divisibles par pq, donne nécessairement $pq = 1$, donc $p = q = 1$. Et donc $P \in \mathbf{Z}[X]$.

6. Ecrivons

$$R(X) = P(X+1) = \frac{(X+1)^p - 1}{X} = \sum_{k=1}^{p} \binom{p}{k} X^{k-1}$$

Supposons $R = AB$ où A, B sont dans $\mathbf{Z}[X]$; alors

$$\phi_p(A)\phi_p(B) = \phi_p(R) = X^{p-1}$$

Donc $\phi_p(A) = X^k$ et $\phi_p(B) = X^{p-1-k}$ pour un certain $k \in [\![1, p-2]\!]$. Mais alors les coefficients constants de A et de B sont nécessairement divisibles par p, or leur produit est p (le coefficient constant de R), ce qui est contradictoire.
Finalement, R est irréductible dans $\mathbf{Z}[X]$, donc dans $\mathbf{Q}[X]$ d'après **5.**.

Exercice 87 (Cyclotomie)**.** *Les polynômes « cyclotomiques » peuvent être utilisés pour la construction des corps finis ; il est simple de montrer que si* $\mathbf{K}$ *est un corps fini, il a* p^n *éléments, où* p *est premier, mais il est moins évident de montrer que pour tout* $n \geq 1$ *et* p *premier, il existe un corps à* p^n *éléments.*
On note, dans tout l'exercice, si $n \geq 1$, $\mathbf{U}_n$ l'ensemble des racines n-ièmes de 1 dans $\mathbf{C}$, et $\mathbf{V}_n$ l'ensemble des racines primitives n-ièmes de 1 dans $\mathbf{C}$ ($\mathbf{V}_n$ est l'ensemble des générateurs du groupe $(\mathbf{U}_n, \times)$). On définit

$$\Phi_n = \prod_{\zeta \in \mathbf{V}_n} (X - \zeta)$$

1. Calculer Φ_1, Φ_2, Φ_3, Φ_4, Φ_6.
2. Calculer Φ_p si p est premier.
3. Exprimer le degré de Φ_n à l'aide de la constante d'Euler.
4. Montrer que, si $n \geq 1$,
$$X^n - 1 = \prod_{d|n} \Phi_d$$
5. On veut montrer que Φ_n est à coefficients entiers.
   (a) Montrer que, si A et B sont dans $\mathbf{Q}[X]$, si $A = BC$ où $C \in \mathbf{C}[X]$, alors $C \in \mathbf{Q}[X]$.
   (b) On suppose de plus A et B dans $\mathbf{Z}[X]$, unitaires. Montrer que C est dans $\mathbf{Z}[X]$.
   (c) Démontrer que les Φ_n sont à coefficients entiers.

   On peut montrer que les polynômes cyclotomiques sont irréductibles dans $\mathbf{Q}[X]$*, c'est un théorème de Gauss, assez technique.*

---

1. $\Phi_1 = X-1$, $\Phi_2 = X+1$, $\Phi_3 = (X-j)(X-j^2) = (X^3-1)/(X-1) = X^2+X+1$, $\Phi_4 = X^2+1$, $\Phi_6 = \big(X-\exp(i\pi/3)\big)\big(X-\exp(5i\pi/3)\big) = X^2-X+1$
2. $\Phi_p = (X^p-1)/(X-1) = 1 + X + X^2 + \cdots + X^{p-1}$
3. C'est $\phi(n)$.
4. Signalons que l'indexation $d|n$, usuelle en arithmétique, est un raccourci de « d diviseur de n, compris entre 1 et n ». On a
$$\mathbf{U}_n = \bigcup_{d|n} \mathbf{V}_d$$
(si z est une racine n-ième de l'unité, z est d'ordre d pour un unique diviseur d de n) et cette union est disjointe, ce qui permet de conclure.

5. (a) Plusieurs méthodes possibles ; on peut diviser A par B dans $\mathbf{Q}[X]$: $A = BQ + R$ avec $\deg(R) < \deg(B)$ où Q et R sont dans $\mathbf{Q}[X]$. Mais tous ces polynômes sont aussi dans $\mathbf{C}[X]$, or il y a unicité de la division euclidienne dans $\mathbf{C}[X]$, donc $C = Q$ et $R = 0$.

   (b) Voir exercice sur le contenu, ou, directement, remarquer que le coefficient dominant de C est entier (il vaut 1), puis par récurrence (descendante et finie) montrer que tous les coefficients de C sont entiers.

   (c) Récurrence (hypothèse « forte »).
