Arithmétique

Calculs élémentaires

Exercice 1. *De l'art de choisir ses tiroirs.*

Soit $n \in \mathbb{N}^*$ et soient $a_1, \dots, a_{n+1} \in [\![1, 2n]\!]$ deux à deux distincts.

1. Montrer qu'il existe $i, j \in [\![1, n+1]\!]$ distincts tels que $a_i \wedge a_j = 1$.
2. Montrer qu'il existe $i, j \in [\![1, n+1]\!]$ distincts tels que $a_i \mid a_j$.

Exercice 2. *Bernoulli itéré.*

Montrer que pour tout entier $n \geq 1$ et tout entier a impair on a

$$a^{2^n} \equiv 1 \pmod{2^{n+2}}.$$

◦ **Exercice 3.** *Caractérisation des racines r-ièmes.*

Soient $r \in \mathbb{N}^*$ et $n \in \mathbb{N}^*$. Montrer que

$$\exists x \in \mathbb{N}, x^r = n \Leftrightarrow \exists x \in \mathbb{Q}, x^r = n.$$

Exercice 4. *Somme des chiffres itérée.*

On note pour tout entier $n \in \mathbb{N}$, $s_{10}(n)$ la somme des chiffres de l'écriture décimale de n.
Déterminer $s_{10}\left(s_{10}\left(s_{10}\left(s_{10}\left(s_{10}\left(2^{2027}\right)\right)\right)\right)\right)$.

Exercice 5. *Une division euclidienne cachée.*

Existe-t-il des $a, b \in \mathbb{N}$ tels que $2^a - 1 \mid 2^b + 1$ et $a > 1$? Si oui, les déterminer.

Exercice 6. *Un calcul direct.*

Soit $n \in \mathbb{N}^*$ et $a, b \in \mathbb{Z}$ tels que $a \equiv b \pmod{n}$. Montrer $a^n \equiv b^n \pmod{n^2}$.

Exercice 7. *Une identité de Sophie Germain.*

Déterminer l'ensemble des $(n, m) \in (\mathbb{N}^*)^2$ tels que $n^4 + 4m^4$ est premier.

Valuations

Exercice 8. *Passage à la limite.*

Soient $a, b \in \mathbb{N}^*$.

On suppose que pour tout $n \in \mathbb{N}$, $a^n \mid b^{n+2027}$.

Montrer que $a \mid b$.

Exercice 9. *Un calcul de valuation 2-adique qui ne dit pas son nom.*

Déterminer tous les entiers $n \in \mathbb{N}^*$ tels que 2^n divise $3^n - 1$.

Exercice 10. *Théorèmes de Taeisinger (1915) et Kürschák (1918).* *X*

1. Soit p un nombre premier.
   (a) Prolonger la valuation p-adique en une fonction $v_p : \mathbb{Q} \to \mathbb{Z} \cup \{+\infty\}$ vérifiant la propriété $\forall x, y \in \mathbb{Q}, v_p(xy) = v_p(x) + v_p(y)$.
   (b) Montrer que l'on conserve la propriété $\forall x, y \in \mathbb{Q}, v_p(x+y) \geq \min(v_p(x), v_p(y))$.
2. Pour $n \geq 1$, on note $\mathrm{H}_n = \sum_{k=1}^{n} \frac{1}{k}$. Calculer $v_2(\mathrm{H}_n)$.
3. En déduire que pour tout $n > 1$, $\mathrm{H}_n \notin \mathbb{Z}$ et que pour tous $m > n \geq 1$, $\mathrm{H}_m - \mathrm{H}_n \notin \mathbb{Z}$.

Exercice 11. *LTE.*

Soit p un nombre premier différent de 2, x, y deux entiers tels que $x \neq \pm y$. On suppose de plus $v_p(x) = 0$, $v_p(y) = 0$ et $v_p(x-y) > 0$.

1. Soit $n \in \mathbb{N}$ tel que $v_p(n) = 0$.
   Montrer que pour tout $k \in [\![0, n-1]\!]$, $x^k y^{n-1-k} \equiv y^{n-1} \pmod{p}$.
2. Soit $n \in \mathbb{N}$ tel que $v_p(n) = 1$.
   Montrer que pour tout $k \in [\![1, n-1]\!]$, $x^k y^{n-1-k} \equiv y^{n-1} + k(x-y)\, y^{n-2} \pmod{p^2}$.
3. Conclure que pour tout entier $n \in \mathbb{N}^*$

$$v_p(x^n - y^n) = v_p(x-y) + v_p(n)$$

Exercice 12. *Valuation 3-adique des repunits.*

Si $n \in \mathbb{N}^*$, on note R_n le nombre s'écrivant en base 10 à l'aide de n chiffres « 1 ». Calculer $v_3(\mathrm{R}_n)$.

Factorielles et coefficients binomiaux

On adopte la convention $\binom{n}{k} = 0$ pour $n \in \mathbb{N}$ et $k \in \mathbb{Z} \setminus [\![0, n]\!]$.

♠ **Exercice 13.** *Formule de Legendre (1830).* *X*

Montrer que, pour tout nombre premier p et tout $n \in \mathbb{N}$, $v_p(n!) = \sum_{k \in \mathbb{N}^*} \left\lfloor \frac{n}{p^k} \right\rfloor$.

Exercice 14. *Deux conséquences de la formule de Legendre.* *X*

1. Par combien de zéros se termine 2027 ! ?
2. Montrer que pour tous $n, m \in \mathbb{N}$, $\dfrac{(2n)!(2m)!}{n!m!(n+m)!}$ est un entier.

Exercice 15. *Encore des coefficients binomiaux.*

Soit p un nombre premier.

Montrer que

$$\forall k \in [\![0, p-1]\!], \binom{p-1}{k} \equiv (-1)^k \pmod{p}.$$

Exercice 16. *Théorème de Lucas (1878).* *X*

Soit p un nombre premier.

1. Montrer que $\forall 0 < k < p$, p divise $\binom{p}{k}$.
2. Soit $\mathrm{Q} = 1 + \mathrm{X} \in \mathbb{F}_p[\mathrm{X}]$. Calculer Q^{p^m} (pour $m \geq 1$).
3. Soit $n = \overline{n_r n_{r-1} \cdots n_0}^p$ et $k = \overline{k_r k_{r-1} \cdots k_0}^p$ deux entiers écrits en base p. Montrer que

$$\binom{n}{k} \equiv \prod_{i=0}^{r} \binom{n_i}{k_i} \pmod{p}.$$

Exercice 17. *Un cas particulier du théorème de Lucas.* *X*

Soient $0 \leq e_1 < e_2 < \cdots < e_r$. On pose $n = \sum_{k=1}^{r} 2^{e_k}$.

1. Montrer que $v_2(n!) = n - r$.
2. Montrer que le nombre d'entiers k tels que $\binom{n}{k}$ est impair est 2^r.

Exercice 18. *Version probabiliste de la formule de Legendre.*

Soit p un nombre premier et, pour tout $n \in \mathbb{N}^*$, soit $\mathrm{X}_n \sim \mathcal{U}([\![1, n]\!])$ une variable aléatoire suivant une loi uniforme sur $[\![1, n]\!]$.

On note pour tout $\mathrm{N} \in \mathbb{N}$, $s_p(\mathrm{N})$ la somme des chiffres en base p de N.

1. Déterminer la loi de $v_p(\mathrm{X}_n)$.
2. Montrer que pour tout $k \in \mathbb{N}$

$$\lim_{n \to +\infty} \mathbb{P}(v_p(\mathrm{X}_n) = k) = \left(1 - \frac{1}{p}\right)\left(\frac{1}{p}\right)^k.$$

3. Soit $n \in \mathbb{N}^*$. À l'aide d'un calcul de $\mathbb{E}\left[v_p(\mathrm{X}_n)\right]$ montrer que

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

4. En déduire que pour tout $n \in \mathbb{N}$,

$$v_p(n!) = \frac{n - s_p(n)}{p-1}.$$

5. Soit $m \in \mathbb{N}$ et $\mathrm{Y} \sim \mathcal{U}([\![0, 2^m - 1]\!])$. Déterminer la loi de $v_2\left(\binom{2\mathrm{Y}}{\mathrm{Y}}\right)$.

Δ **Exercice 19.** *Théorème de Wilson.* *X*

Soit $n \geq 2$. Montrer que n est premier si et seulement si $(n-1)! \equiv -1 \pmod{n}$.

Exercice 20. *Variation autour de la formule de Legendre.* *ÉNS*

Soit p un nombre premier.

On pose pour tout $n \in \mathbb{N}^*$,

$$\mathrm{E}(n) = v_p\left(\prod_{k=1}^{n} k^k\right).$$

Déterminer un équivalent de $\mathrm{E}(n)$ lorsque $n \to \infty$.

Exercice 21. *Version faible du théorème de Morley.*

Soit $n \in \mathbb{N}$ tel que $2n+1$ est premier.

L'objectif de cet exercice est de montrer que

$$2^{4n}(n!)^2 \equiv (-1)^n (2n)! \pmod{(2n+1)^2}.$$

Pour tout $n \in \mathbb{N}$ on pose $\mathrm{W}_n = \displaystyle\int_0^{\frac{\pi}{2}} \cos(t)^n \mathrm{d}t$.

1. Exprimer pour tout $n \in \mathbb{N}$, W_{2n+1} à l'aide de factorielles.
2. Montrer que pour tout $n \in \mathbb{N}$

$$\mathrm{W}_{2n+1} = \frac{(-1)^n}{2^{2n}} \sum_{k=0}^{n} \frac{(-1)^k}{2n+1-2k} \binom{2n+1}{k}.$$

3. Conclure.

Remarque culturelle : on peut en fait montrer que, dès que $2n+1 \geq 5$, la congruence a lieu modulo $(2n+1)^3$ (théorème de Morley). Elle est en revanche en défaut modulo 27 pour $n = 1$.

⋆ **Exercice 22.** *Taille des p-sous-groupes de Sylow de* $\mathrm{GL}_m\left(\mathbb{F}_q\right)$. *ÉNS*

Soient p, q deux nombres premiers impairs distincts.

Pour tout $m \geq 2$ on pose $\mathrm{N}(m) = \left(q^m - 1\right)\left(q^{m-1} - 1\right) \cdots \left(q^2 - 1\right)(q-1)$.

1. Pour tout $k \in \mathbb{N}^*$ on note $\omega_{p^k}(q)$ l'ordre de q modulo p^k. Montrer que pour tout $m \geq 2$,

$$v_p(\mathrm{N}(m)) = \sum_{k=1}^{+\infty} \left\lfloor \frac{m}{\omega_{p^k}(q)} \right\rfloor.$$

2. En déduire que $v_p(\mathrm{N}(m)) = \mathrm{O}(m \ln(m))$.

⋆ **Exercice 23.** *Théorème de Wolstenholme binomial détaillé.* *ÉNS*

Soit $(m, n, p) \in (\mathbb{N}^*)^3$, avec p premier supérieur ou égal à 5, m et p premiers entre eux.

1. Montrer que $\binom{np}{m} \equiv 0 \pmod{p}$.
2. Montrer que $\binom{np}{mp} = \displaystyle\sum_{k=0}^{p} \binom{p(n-1)}{mp-k}\binom{p}{k}$.
3. Conclure que

$$\binom{np}{mp} \equiv \binom{n}{m} \pmod{p^2}.$$

On cherche désormais à montrer que pour $n = 2, m = 1$ on a la congruence plus précise :

$$\binom{2p}{p} \equiv 2 \pmod{p^3}.$$

4. Montrer que $\forall k \in [\![1, p]\!], \binom{p-1}{k-1} \equiv \pm 1 \pmod{p}$.
5. Montrer que $\sum_{k=1}^{p-1} \left(\frac{(p-1)!}{k}\right)^2 \equiv 0 \pmod{p}$.
6. Conclure.

Équations diophantiennes

Δ **Exercice 24.** *Théorème de Sylvester sur les monoïdes numériques.* *X*

Soient $a, b \in \mathbb{N}^*$ premiers entre eux tels que $a < b$. On note $\langle a, b\rangle = \{ua + vb \,|\, u, v \in \mathbb{N}\}$.

1. Montrer que $\begin{cases} \mathbb{Z}/a\mathbb{Z} \to \mathbb{Z}/a\mathbb{Z} \\ x \mapsto [b]_a\, x \end{cases}$ est un automorphisme de groupes.

On notera $\overline{h} : \mathbb{Z}/a\mathbb{Z} \to \mathbb{Z}/a\mathbb{Z}$ sa réciproque.

2. Soit $h : \mathbb{Z} \to [\![0, a-1]\!]$ l'unique application telle que $\forall n \in \mathbb{Z}, [h(n)]_a = \overline{h}([n]_a)$.
   Montrer que $\forall n \in \mathbb{N}, n \in \langle a, b\rangle \Leftrightarrow h(n)\, b \leq n$.
3. Montrer que $ab - a - b \notin \langle a, b\rangle$ mais que $[\![ab - a - b + 1, +\infty[\![\subseteq \langle a, b\rangle$.

Exercice 25. *Une équation diophantienne exponentielle.*

Soit $(x, y) \in (\mathbb{N}^*)^2$ une solution de $3^x = 8 + y^2$.

1. Déterminer les parités de x et y.
2. Conclure.

Exercice 26. *Une question du CG 1990.* *CG*

Déterminer les entiers $n \in \mathbb{N}^*$ tels que l'équation

$$\sum_{k=1}^{n} \frac{1}{x_k^2} = 1$$

admette une solution $(x_1, \dots, x_n) \in (\mathbb{N}^*)^n$.

Exercice 27. *Paramétrisation des triplets pythagoriciens.*

On appelle *triplet pythagoricien* tout triplet $(a, b, c) \in (\mathbb{N}^*)^3$ tel que $a^2 + b^2 = c^2$.
Montrer que, à l'échange de a et b près, l'ensemble des triplets pythagoriciens est

$$\left\{\left(k\left(m^2 - n^2\right), 2kmn, k\left(m^2 + n^2\right)\right), (k, m, n) \in (\mathbb{N}^*)^3, m > n\right\}.$$

Exercice 28. *Une équation diophantienne exponentielle.* *ÉNS*

Déterminer les $(a,b,c) \in \mathbb{N}^3$ tels que

$$2^a + 3^b = 5^c.$$

1. Dans le cas où b est impair.
2. Dans le cas où b est pair et c impair.
3. Dans le cas où b et c sont pairs.

Exercice 29. *Un cas particulier du théorème d'Erdős-Selfridge.*

Soit $n \geq 2$. Montrer que le produit de trois entiers > 0 consécutifs n'est jamais une puissance n-ième.

Exercice 30. *La preuve de Don Zagier du théorème des deux carrés.* *X*

Soit p un nombre premier congru à 1 modulo 4. On considère l'ensemble

$$\mathrm{S} = \left\{(a,b,c) \in \mathbb{N}^* \times \mathbb{N}^* \times \mathbb{Z}^* \,|\, 4ab + c^2 = p\right\}$$

ainsi que $\mathrm{S}_1 = \{(a,b,c) \in \mathrm{S} \,|\, a > b + c\}$ et $\mathrm{S}_2 = \{(a,b,c) \in \mathrm{S} \,|\, a < b + c\}$.

1. Montrer que S est fini non vide, est l'union disjointe de S_1 et S_2, et que S_1 et S_2 ont le même cardinal.
2. Soit $g : \mathrm{S}_1 \to \mathrm{S}_1$ définie par $g(a,b,c) = (a - b - c, b, -2b - c)$. À l'aide de g, montrer que S_1 a un cardinal impair.
3. Soit $\mathrm{S}_0 = \{(a,b,c) \in \mathrm{S} \,|\, a \neq b\}$. À l'aide de S_0, montrer que p est somme de deux carrés.
4. Montrer qu'un entier naturel non nul dont tous les diviseurs premiers sont congrus à 1 modulo 4 est somme de deux carrés d'entiers.

Fonctions des diviseurs

Exercice 31. *Somme de puissances de diviseurs ou décomposition des sigmas.*

Pour tout $s \in \mathbb{R}$ on note

$$\begin{aligned} \sigma_s : \mathbb{N}^* &\to \mathbb{R}_+ \\ n &\mapsto \sum_{d|n} d^s. \end{aligned}$$

Par exemple, pour tout entier $n \geq 1$, $\sigma_0(n)$ est le nombre de diviseurs de n tandis que $\sigma_1(n)$ est la somme des diviseurs de n.

1. Montrer que pour tous $n, m \in \mathbb{N}^*$ **premiers entre eux**, pour tout $s \in \mathbb{R}$,

$$\sigma_s(nm) = \sigma_s(n)\,\sigma_s(m).$$

2. Soit $n \in \mathbb{N}^*$. Montrer que

$$\sigma_s(n) = \begin{cases} \displaystyle\prod_{p \in \mathcal{P}} \left(v_p(n) + 1\right) & \text{si } s = 0 \\ \displaystyle\prod_{p \in \mathcal{P}} \frac{p^{(v_p(n)+1)s} - 1}{p^s - 1} & \text{si } s \neq 0 \end{cases}$$

Δ **Exercice 32.** *Caractérisation des carrés par le nombre de diviseurs.*

Soit $n \in \mathbb{N}^*$, on note $\sigma_0(n)$ le nombre de diviseurs de n.

Montrer que n est un carré ssi $\sigma_0(n)$ est impair.

Exercice 33. *Diviseurs et carrés.*

Pour tout $n \in \mathbb{N}^*$ on note $\sigma_0(n)$ le nombre de diviseurs de n.

Montrer que

$$\sum_{d|n} \sigma_0\left(d^2\right) = \sigma_0(n)^2.$$

Exercice 34. *Bornes sur la fonction de comptage des diviseurs.* *X (PC), ÉNS*

Pour tout entier $n \geq 1$, on note $\sigma_0(n)$ le nombre de diviseurs de n.

Montrer $\forall \varepsilon > 0, \sigma_0(n) = O(n^\varepsilon)$.

Exercice 35. *Moyenne des diviseurs.* *Mines*

Pour $n \in \mathbb{N}^*$ on note $\sigma_0(n)$ le nombre de diviseurs (positifs) de n et $\sigma_1(n)$ la somme des diviseurs (positifs) de n.

Montrer que pour tout $n \in \mathbb{N}^*$,

$$\sqrt{n} \leq \frac{\sigma_1(n)}{\sigma_0(n)} \leq \frac{n+1}{2}.$$

Exercice 36. *Moyenne du nombre de diviseurs.*

Pour $n \in \mathbb{N}^*$ on note $\sigma_0(n)$ le nombre de diviseurs (positifs) de n.

Donner un équivalent, quand $n \to +\infty$, de

$$\frac{1}{n}\sum_{k=1}^{n} \sigma_0(k).$$

Congruences

Exercice 37. *Théorème de Chevalley-Warning : un cas simple.*

Soit p un nombre premier.

1. Montrer que pour tout $k \in [\![0, p-2]\!]$ (avec la convention $a^0 = 1$, y compris pour $a = 0$),
$$\sum_{a=0}^{p-1} a^k \equiv 0 \pmod{p}.$$
2. Montrer que
$$\sum_{(a,b,c) \in [\![0,p-1]\!]^3} \left(a^2 + b^2 + c^2\right)^{p-1} \equiv 0 \pmod{p}.$$
3. Montrer que l'équation
$$a^2 + b^2 + c^2 \equiv 0 \pmod{p}$$
admet au moins une solution $(a, b, c) \in [\![0, p-1]\!]^3$ autre que $(0, 0, 0)$.

Δ **Exercice 38.** *Lemme de Hensel.*

Soit $P \in \mathbb{Z}[X]$, $p \in \mathcal{P}$ un nombre premier.

Soit $a \in \mathbb{Z}$ tel que $P(a) \equiv 0 \pmod{p}$ et $P'(a) \not\equiv 0 \pmod{p}$ (c'est-à-dire une racine simple modulo p).

Montrer que pour tout $n \in \mathbb{N}$ il existe un entier $x \in \mathbb{Z}$ tel que $x \equiv a \pmod{p}$ et $P(x) \equiv 0 \pmod{p^n}$.

Exercice 39. *Somme de puissances.* *X*

Soit $n \in \mathbb{N}^*$. Montrer que n est impair si et seulement si n divise $\sum_{k=1}^{n} k^n$.

Exercice 40. *Théorème de Vandaële.*

Soit p un nombre premier impair.

1. Soit I un ensemble de p entiers consécutifs. Montrer que p^2 divise $\sum_{k\in I} k^p$.
2. Montrer que $\sum_{k=0}^{p-1} k^p \equiv \frac{p^3 - p^2}{2} \pmod{p^3}$.

Exercice 41. *Une application du lemme chinois.*

Déterminer les $n \in \mathbb{N}$ tels que $n3^n \equiv 1 \pmod{7}$.

Exercice 42. *Désynchronisation entre l'additif et le multiplicatif.*

Soit p un nombre premier. Montrer $\exists n \in \mathbb{N} : 2^n \equiv n \pmod{p}$.

♠ **Exercice 43.** *Résidus quadratiques.*

Soit p un nombre premier différent de 2.

Soit $a \in \mathbb{Z}$. On dit que a est un *résidu quadratique modulo p* si et seulement s'il existe $b \in \mathbb{Z}$ tel que $b^2 \equiv a \pmod{p}$.

Montrer que pour tout $a \not\equiv 0 \pmod{p}$, on a

$$a \text{ est un résidu quadratique modulo } p \Leftrightarrow a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Exercice 44. *Bien choisir ses restes chinois.* *X*

Quels sont les m de $\mathbb{N}^*$ tels qu'il existe m éléments consécutifs de $\mathbb{N}^*$ divisibles par des cubes d'éléments de $\mathbb{N}^* \setminus \{1\}$?

Exercice 45. *Suite stationnaire modulo b.*

Soient $a, b > 1$ des entiers. Montrer que la suite

$$a, a^a, a^{a^a}, a^{a^{a^a}}, \ldots$$

est stationnaire modulo b.

Exercice 46. *Théorème de Leudesdorf.* *Lyon*

Soit $p \geq 5$ un nombre premier. Quand $n \wedge p = 1$, on choisit un entier n^* tel que $nn^* \equiv 1 \pmod{p^2}$.

Montrer $\sum_{k=1}^{p-1} k^* \equiv 0 \pmod{p^2}$.

Exercice 47. *Théorème de Wolstenholme.* *Centrale-Python*

Pour tout $n \in \mathbb{N}^*$ on pose

$$H_n = \sum_{k=1}^{n-1} \frac{1}{k} \in \mathbb{Q} \qquad \text{et} \qquad C_n = \sum_{k=1}^{n-1} \frac{1}{k^2} \in \mathbb{Q}$$

et on note

$$H_n = \frac{a_n}{b_n}, (a_n, b_n) \in \mathbb{Z} \times \mathbb{N}^*, a_n \wedge b_n = 1$$
$$C_n = \frac{c_n}{d_n}, (c_n, d_n) \in \mathbb{Z} \times \mathbb{N}^*, c_n \wedge d_n = 1$$

les représentations comme fractions irréductibles de H_n et C_n.

1. Montrer que, pour tout nombre premier $p \geq 5$, $a_p \equiv 0 \pmod{p^2}$.
2. Montrer que, pour tout nombre premier $p \geq 5$, $c_p \equiv 0 \pmod{p}$.

⋆ **Exercice 48.** *Un contre-exemple au principe local-global.*

On considère le polynôme

$$P = \left(X^2 - 2\right)\left(X^2 - 17\right)\left(X^2 - 34\right).$$

Montrer que pour tout $n \in \mathbb{N}^*$ il existe $a \in \mathbb{Z}$ tel que $P(a) \equiv 0 \pmod{n}$, mais que P n'admet pas de racine dans $\mathbb{Z}$.

Exercice 49. *Divisibilité des nombres de Fibonacci.*

On définit la suite $\left(F_k\right)_{k\in\mathbb{N}}$ par $(F_0, F_1) = (0, 1)$ et pour tout $k \in \mathbb{N}$, $F_{k+2} = F_{k+1} + F_k$.

1. Montrer que pour tout $n \in \mathbb{N}^*$ il existe une infinité de $k \in \mathbb{N}$ tels que $n \mid F_k$.
2. Soit p un nombre premier différent de 2 et 5.
   Montrer que $F_{p-1} + F_{p+1} \equiv 1 \pmod{p}$ et $F_p \equiv 5^{\frac{p-1}{2}} \pmod{p}$.
   En déduire que $p|F_{p-1}$ ou $p|F_{p+1}$.

Indicatrice d'Euler et fonction de Möbius

On définit la fonction de Möbius $\mu : \mathbb{N}^* \to \mathbb{Z}$ par

$$\forall n \in \mathbb{N}^*, \mu(n) = \begin{cases} 0 & \text{si } n \text{ est divisible par le carré d'un nombre premier.} \\ (-1)^r & \text{si } n \text{ est produit de } r \text{ nombres premiers distincts.} \end{cases}$$

♠ **Exercice 50.** *Convolution de Dirichlet et inversion de Möbius.*

On munit l'ensemble des fonctions $\mathbb{N}^* \to \mathbb{R}$ de l'addition et de la loi $*$ définie par

$$(f * g)(n) = \sum_{d|n} f(d)\, g\left(\frac{n}{d}\right).$$

On note 1 la fonction constante égale à 1.

1. Montrer que cela définit un anneau commutatif.
2. En déterminer les inversibles.
3. Montrer que $\mu * 1$ est l'unité de l'anneau.
4. En déduire la formule $\varphi(n) = \sum_{d|n} d\,\mu\left(\frac{n}{d}\right)$.

Exercice 51. *Probabilité d'être premiers entre eux.* *ÉNS*

Pour tout $n \in \mathbb{N}^*$, soient X_n, Y_n deux variables aléatoires i.i.d. de loi uniforme $\mathscr{U}([\![1,n]\!])$.

On note

$$p_n = \mathbb{P}(X_n \wedge Y_n = 1).$$

On définit une fonction $\mu : \mathbb{N}^* \to \mathbb{Z}$ par

$$\forall n \in \mathbb{N}^*,\ \mu(n) = \begin{cases} 0 & \text{si } n \text{ est divisible par le carré d'un nombre premier.} \\ (-1)^d & \text{si } n \text{ est produit de } d \text{ nombres premiers distincts.} \end{cases}$$

Et pour $s \in \mathbb{C}$ tel que $\Re(s) > 1$ on pose

$$\zeta(s) = \sum_{n=1}^{+\infty} \frac{1}{n^s} \text{ et } L_\mu(s) = \sum_{n=1}^{+\infty} \frac{\mu(n)}{n^s}$$

1. Montrer que pour tout $n \in \mathbb{N}^*$,
$$p_n = \frac{1}{n^2} \sum_{d=1}^{n} \mu(d) \left\lfloor \frac{n}{d} \right\rfloor^2.$$
2. Justifier la bonne définition et démontrer que pour tout $s \in \mathbb{C}$ tel que $\Re(s) > 1$,
$$\zeta(s) L_\mu(s) = 1.$$
3. Conclure que
$$p_n \xrightarrow[n\to+\infty]{} \frac{6}{\pi^2}.$$

Exercice 52. *Polynômes cyclotomiques et inversion de Möbius.* *X*

Les définitions des polynômes cyclotomiques $(\Phi_n)_{n\in\mathbb{N}^*}$ et de la fonction de Möbius $\mu : \mathbb{N}^* \to \mathbb{Z}$ sont celles du TD.

1. Montrer que pour tout $n \in \mathbb{N}^*$, $X^n - 1 = \prod_{d|n} \Phi_d$ et en déduire que pour tout $n \in \mathbb{N}^*$, $\Phi_n \in \mathbb{Z}[X]$.
2. Soit $(G, +)$ un groupe abélien et $f : \mathbb{N}^* \to G$.
On pose pour tout $n \in \mathbb{N}^*$, $F(n) = \sum_{d|n} f(d)$.
Montrer que pour tout $n \in \mathbb{N}^*$, $f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) F(d)$.
3. En déduire une expression permettant de calculer Φ_n pour $n \in \mathbb{N}^*$. Calculer Φ_{28}.

Exercice 53. *Encadrement de l'indicatrice d'Euler.* *Mines*

On note φ l'indicatrice d'Euler.

Montrer que pour tout $n \in \mathbb{N}^*$,

$$\varphi(n) \geq \frac{n}{1 + \log_2(n)}.$$

⋆ **Exercice 54.** *Déterminant de Smith.*

Soit $n \in \mathbb{N}^*$.

Montrer que

$$\det\left((i \wedge j)_{1\leq i,j\leq n}\right) = \prod_{k=1}^{n} \varphi(k).$$

Algèbre linéaire et arithmétique

Exercice 55. *Caractérisation de* $\mathrm{GL}_2(\mathbb{Z})$. *X (PC)*

Soient $A, B \in \mathrm{M}_2(\mathbb{Z})$ tels que pour tout $k \in \{0,1,2,3,4\}$, $A + kB$ est inversible, d'inverse à coefficients entiers. Montrer que $A + 5B$ est inversible, d'inverse à coefficients entiers.

Δ **Exercice 56.** *Trace et morphisme de Frobenius.* *Centrale*

1. Soit A un anneau commutatif, I un idéal de A ainsi que $M \in \mathrm{M}_n(A)$ et $N \in \mathrm{M}_n(I)$. Montrer que $\det(M+N) - \det(M) \in I$.
2. Soit p un nombre premier et $Q \in \mathbb{Z}[X]$. Montrer que $Q(X^p) - (Q(X))^p \in p\mathbb{Z}[X]$.
3. Soit $M \in \mathrm{M}_n(\mathbb{Z})$. Montrer que

$$\mathrm{tr}(M^p) \equiv \mathrm{tr}(M) \pmod{p}.$$

⋆ **Exercice 57.** *Une application du morphisme de Frobenius.* *ÉNS*

On considère la suite $(u_n)_{n\in\mathbb{N}}$ définie par $(u_0,u_1,u_2,u_3) = (4,0,0,3)$ et pour tout $n \in \mathbb{N}$, $u_{n+4} = u_{n+1} + u_n$.

Montrer que pour tout nombre premier p, p divise u_p.

Exercice 58. *Un déterminant de Vandermonde en arithmétique.*

Soient $a_1, \dots, a_n \in \mathbb{Z}$ des entiers.

Montrer que

$$\prod_{j=1}^{n-1} j! \mid \prod_{i<j} (a_j - a_i).$$

Exercice 59. *Matrices irréductibles à coefficients entiers.*

On dit que $A \in \mathrm{M}_n(\mathbb{Z})$ est « irréductible » ssi

$$A \notin \left(\mathrm{M}_n(\mathbb{Z})\right)^\times \qquad \text{et} \qquad \forall B, C \in \mathrm{M}_n(\mathbb{Z}), A = BC \Rightarrow \left(B \in (\mathrm{M}_n(\mathbb{Z}))^\times \text{ ou } C \in (\mathrm{M}_n(\mathbb{Z}))^\times\right).$$

Caractériser les irréductibles de $\mathrm{M}_n(\mathbb{Z})$ en termes de déterminant.

Δ **Exercice 60.** *L'exercice des cailloux ou des vaches.* *X (PC)*

On dispose de $2n+1$ cailloux de poids $p_1, \dots, p_{2n+1}$ vérifiant la propriété suivante : si on retire n'importe quel caillou alors les $2n$ cailloux restants peuvent être séparés en deux groupes de n cailloux de même poids.

Montrer que tous les cailloux ont le même poids.

Exercice 61. *Bézout, déterminant et compagnie.*

Soient $A, B \in \mathrm{M}_n(\mathbb{Z})$.

Montrer que

$$\det(A) \wedge \det(B) = 1 \Rightarrow \exists (U,V) \in (\mathrm{M}_n(\mathbb{Z}))^2, AU + BV = I_n.$$

Exercice 62. *Déterminant, divisibilité et transposée.* *X (PC)*

Soit $n \in \mathbb{N}$ un entier **impair**, $M \in \mathrm{M}_n(\mathbb{Z})$ et $a, b \in \mathbb{N}^*$ des entiers non nuls.

Montrer que $a + b \mid \det(aM + bM^\top)$.

Décompositions

Exercice 63. *Écriture en base $-b$.* *X*

Soit $b \geq 2$ un entier.

Montrer que pour tout $n \in \mathbb{Z}$ il existe une unique suite presque nulle $\left(c_k(n)\right) \in [\![0, b-1]\!]^{(\mathbb{N})}$ telle que

$$n = \sum_{k=0}^{+\infty} c_k(n)\,(-b)^k.$$

Exercice 64. *Fractions égyptiennes.*

Soit $r \in \mathbb{Q} \cap [0,1[$. Montrer qu'il existe $n \in \mathbb{N}$ et des entiers $a_1, \dots, a_n \in \mathbb{N}^*$ **distincts** tels que

$$r = \sum_{i=1}^{n} \frac{1}{a_i}.$$

Exercice 65. *XKCD 2835 - Décomposition en base factorielle.*

Soit $n \in \mathbb{N}$.

Montrer qu'il existe une unique suite $\left(a_k\right)_{k\in\mathbb{N}^*}$ nulle à partir d'un certain rang telle que

$$n = \sum_{k=1}^{+\infty} a_k k!$$

et pour tout k, $a_k \in [\![0, k]\!]$.

Exercice 66. *Décomposition de Zeckendorf.*

On définit la suite de Fibonacci $(\mathrm{F}_n)_{n\in\mathbb{N}}$ par $\mathrm{F}_0 = 0, \quad \mathrm{F}_1 = 1$ et $\forall n \in \mathbb{N}, \mathrm{F}_{n+2} = \mathrm{F}_{n+1} + \mathrm{F}_n$.

On dit qu'un entier $n \in \mathbb{N}^*$ admet une *décomposition de Zeckendorf* s'il s'écrit

$$n = \sum_{k=1}^{r} \mathrm{F}_{i_k}$$

avec $r \in \mathbb{N}^*$ et $i_1 > i_2 > \dots > i_r \geq 2$ des indices deux à deux non consécutifs, c'est-à-dire vérifiant $i_k - i_{k+1} \geq 2$ pour tout $k \in [\![1, r-1]\!]$.

1. Montrer que tout entier $n \in \mathbb{N}^*$ admet une décomposition de Zeckendorf.
2. Montrer qu'une telle décomposition est unique.

Exercice 67. *Cas particulier du théorème d'Erdős-Surányi.* *X (PC)*

Montrer que pour tout $n \in \mathbb{N}$ il existe $m \in \mathbb{N}$ et $(\varepsilon_1, \dots, \varepsilon_m) \in \{-1, +1\}^m$ tels que

$$n = \sum_{k=1}^{m} \varepsilon_k k^2.$$

Exercice 68. *Périodicité des chiffres de n^n.* *ÉNS*

Soit $b \geq 2$ un entier.

1. Montrer que pour tout $n \in \mathbb{N}$ il existe une unique suite presque nulle $\left(c_k(n)\right)_{k\in\mathbb{N}} \in [\![0, b-1]\!]^{(\mathbb{N})}$ telle que
$$n = \sum_{k=0}^{+\infty} c_k(n)\, b^k.$$
2. Montrer que pour tout $k \in \mathbb{N}$, la suite $\left(c_k(n^n)\right)_{n\in\mathbb{N}^*}$ est périodique à partir d'un certain rang.

Plein de nombres premiers

◦ **Exercice 69.** *Nombres de Mersenne.*

Soient $a \geq 2$ et $n \geq 2$ des entiers.

1. Montrer que **si** $a^n - 1$ est premier **alors** $a = 2$ et n est premier.
2. Que dire de la réciproque ?

◦ **Exercice 70.** *Nombres de Fermat.*

1. Soit $b \in \mathbb{N}^*$.
   Montrer que **si** $2^b + 1$ est premier **alors** il existe $n \in \mathbb{N}$ tel que $b = 2^n$.

Pour $n \in \mathbb{N}$ on pose $\mathrm{F}_n = 2^{2^n} + 1$.

2. Étudier la primalité de F_n pour $n \in [\![0, 6]\!]$.
3. Montrer que $\forall (n, m) \in \mathbb{N}^2, n \neq m, \mathrm{F}_n \wedge \mathrm{F}_m = 1$.
4. En déduire une nouvelle preuve de l'existence d'une infinité de nombres premiers.

Exercice 71. *Des uns et des zéros.*

Déterminer les nombres premiers dont l'écriture en base 10 comporte en alternance des 0 et des 1.

Exercice 72. *Cas particuliers du théorème de la progression arithmétique de Dirichlet.* *ÉNS*

1. Montrer qu'il existe une infinité de nombres premiers congrus à 3 modulo 4.
2. Montrer qu'il existe une infinité de nombres premiers congrus à 5 modulo 6.

Exercice 73. *Encore un cas particulier du théorème de la progression arithmétique de Dirichlet.*

1. Soit p un nombre premier impair. Montrer que -1 est un carré modulo p ssi $p \equiv 1 \pmod 4$.
2. En déduire qu'il existe une infinité de nombres premiers congrus à 1 modulo 4.

Exercice 74. *Tranches de cardinal prescrit.* *ÉNS (PC)*

1. Soit $\mathrm{X} \subseteq \mathbb{N}$ tel que $0, 1 \in \mathrm{X}$ et $\left|\mathrm{X} \cap [\![1, n]\!]\right| = \underset{n \to +\infty}{o}(n)$.
   Montrer que pour tout $k \in \mathbb{N}^*$, il existe $j \in \mathbb{N}$ tel que $\left|\mathrm{X} \cap [\![j, j + k]\!]\right| = 2$.
2. Montrer qu'il existe un ensemble de cent entiers consécutifs contenant exactement cinq nombres premiers.

Exercice 75. *Cas particulier d'un argument cyclotomique pour montrer une version faible de Dirichlet.* *ÉNS*

Soit p un nombre premier et $n \in \mathbb{N}$.

On pose $k = \dfrac{(np)^p - 1}{np - 1}$.

1. Montrer que $k \equiv 1 \pmod p$.
2. Montrer que pour tout q diviseur premier de k on a $q \equiv 1 \pmod p$.
3. Conclure qu'il existe une infinité de nombres premiers congrus à 1 modulo p.

Exercice 76. *Majoration de valuation et combinatoire.*

Soient $p_1, \dots, p_r$ des nombres premiers distincts.
On note A l'ensemble des entiers dont les seuls facteurs premiers sont dans $\{p_1, \dots, p_r\}$.

1. Montrer que pour tout $N \in \mathbb{N}^*$,
$$|A \cap [\![1, N]\!]| \leq \left(1 + \frac{\ln(N)}{\ln(2)}\right)^r.$$
2. En déduire une nouvelle preuve de l'existence d'une infinité de nombres premiers.
3. En déduire que
$$\sum_{p \text{ premier}} \frac{1}{p} = +\infty.$$

Exercice 77. *Preuve topologique de Furstenberg.*

Pour $(a, b) \in \mathbb{N}^* \times \mathbb{Z}$ on note

$$A_{a,b} = \{an + b, n \in \mathbb{Z}\} \subseteq \mathbb{Z}.$$

Pour $U \subseteq \mathbb{Z}$ une partie de $\mathbb{Z}$ on dit que U est **ouverte** ssi

$$\forall x \in U, \exists (a, b) \in \mathbb{N}^* \times \mathbb{Z}, x \in A_{a,b} \text{ et } A_{a,b} \subseteq U.$$

Pour $F \subseteq \mathbb{Z}$ une partie de $\mathbb{Z}$ on dit que F est **fermée** ssi $\overline{F}$ est ouverte.

1. Montrer que toute union (quelconque) de parties ouvertes est ouverte, que toute intersection finie de parties ouvertes est ouverte. Que dire d'une intersection (quelconque) de parties fermées et d'une union finie de parties fermées ?
2. Montrer que pour tout $(a, b) \in \mathbb{N}^* \times \mathbb{Z}$, $A_{a,b}$ est fermée.
3. En remarquant que
$$\mathbb{Z} \setminus \{-1, 1\} = \bigcup_{p \text{ premier}} A_{p,0}$$
conclure qu'il existe une infinité de nombres premiers.

PGCD et PPCM

Exercice 78. *PGCD et suites de Fibonacci.*

On définit la suite $(F_n)_{n \in \mathbb{N}}$ par
$$(F_0, F_1) = (0, 1)$$
$$\forall n \in \mathbb{N}, F_{n+2} = F_{n+1} + F_n.$$

1. Montrer que
$$\forall p \geq 1, \forall n \in \mathbb{N}, F_{n+p} = F_p F_{n+1} + F_{p-1} F_n.$$
2. Montrer que
$$\forall (n, m) \in \mathbb{N}^2, F_n \wedge F_m = F_{n \wedge m}.$$

⋆ **Exercice 79.** *Suite récurrente et Euclide simultané.*

Soit $P \in \mathbb{Z}[X]$ (c'est-à-dire un polynôme à coefficients entiers).

On définit une suite $(a_n)_{n\in\mathbb{N}}$ par

$$a_0 = 0$$
$$\forall k \in \mathbb{N}, a_{k+1} = P\left(a_k\right).$$

Montrer que pour tout $(n, m) \in \mathbb{N}^2$,

$$a_n \wedge a_m = |a_{n\wedge m}|.$$

Exercice 80. *Plein de premiers entre eux.*

Soient α, β deux entiers naturels non nuls premiers entre eux.

Soient n et m deux entiers naturels non nuls premiers entre eux.

1. Si n et m sont impairs alors $(\alpha^n + \beta^n) \wedge (\alpha^m + \beta^m) = \alpha + \beta$,
2. Sinon,
   (a) Si α et β sont impairs alors $(\alpha^n + \beta^n) \wedge (\alpha^m + \beta^m) = 2$
   (b) Sinon $(\alpha^n + \beta^n) \wedge (\alpha^m + \beta^m) = 1$.

Extraits d'Olympiades

Exercice 81. *Une suite récurrente.* *IMO 2017*

Soit $a_0 \in \mathbb{N}$.

On considère la suite $(a_n)_{n\in\mathbb{N}}$ définie par

$$a_0 = a_0$$
$$\forall n \in \mathbb{N}, a_{n+1} = \begin{cases} \sqrt{a_n} & \text{si } a_n \text{ est un carré parfait} \\ a_n + 3 & \text{sinon} \end{cases}.$$

Expliciter une partition (P, I) de $\mathbb{N}$ telle que

1. Si $a_0 \in P$ alors $(a_n)_{n\in\mathbb{N}}$ est périodique à partir d'un certain rang.
2. Si $a_0 \in I$ alors $a_n \sim 3n$ lorsque $n \to +\infty$ (c'est-à-dire $\lim\limits_{n\to+\infty} \dfrac{a_n}{n} = 3$).

Exercice 82. *De l'arithmétique olympique.* *IMO 1990*

Trouver tous les entiers $n \in \mathbb{N}^*$ tels que n^2 divise $2^n + 1$.

⋆ **Exercice 83.** *L'exemple le plus connu de « saut de Viète ».* *IMO 1988, X*

1. Pour $k \in \mathbb{N}$ on note E_k l'équation
$$x^2 - kxy + y^2 = k$$
d'inconnue $(x, y) \in \mathbb{N}^2$.
Soit $(a, b) \in (\mathbb{N}^*)^2$. Montrer que si (a, b) est solution de E_k alors $\left(b, \dfrac{b^2 - k}{a}\right)$ est aussi solution de E_k.
2. Soient $a, b \in \mathbb{N}$. Montrer que
$$\frac{a^2 + b^2}{ab + 1} \text{ est entier} \Longrightarrow \frac{a^2 + b^2}{ab + 1} \text{ est un carré parfait.}$$

Arithmétique et algèbre

Δ **Exercice 84.** *Division euclidienne dans les entiers de Gauss.*

On rappelle que $\mathbb{Z}[i] = \{a + bi, (a,b) \in \mathbb{Z}^2\}$ est un sous-anneau de $\mathbb{C}$.

Soit $(a,b) \in \mathbb{Z}[i]^2$ tel que $b \neq 0$.

Montrer qu'il existe $(q,r) \in \mathbb{Z}[i] \times \mathbb{Z}[i]$ tels que

$$\begin{aligned} a &= bq + r \\ |r|^2 &< |b|^2 \end{aligned}$$

⋆ **Exercice 85.** *Nombres de Gauss premiers.*

On note $\mathcal{P}$ l'ensemble des nombres premiers de $\mathbb{Z}$.

On dit que $z \in \mathbb{Z}[i]$, non nul et non inversible, est premier ssi pour tous $u, v \in \mathbb{Z}[i]$ tels que $z = uv$ on a $u \in (\mathbb{Z}[i])^\times$ ou $v \in \mathbb{Z}[i]^\times$.

Montrer que $z \in \mathbb{Z}[i]$ est premier ssi

$$\begin{gathered} |z|^2 \in \mathcal{P} \\ \text{ou} \\ \exists (u,p) \in \mathbb{U}_4 \times \mathcal{P}, p \equiv 3 \pmod 4, z = up. \end{gathered}$$

Exercice 86. *Ce n'est pas juste un exercice de complexes.* *X (PC), X*

Soit $c \in \mathbb{Q} \setminus \{0\}$ et $n \in \mathbb{N}^*$ tel que $(c+i)^n = (c-i)^n$.

Montrer que $n \equiv 0 \pmod 4$ et $c = \pm 1$.

Exercice 87. *Groupe de Baer-Specker.* *Lyon*

L'ensemble $\mathbb{Z}^{\mathbb{N}}$ des suites à valeurs entières est un groupe pour l'addition, et l'ensemble $\mathbb{Z}^{(\mathbb{N})}$ des suites nulles à partir d'un certain rang en est un sous-groupe. (On ne demande pas de le vérifier.)

Soit $\varphi : \mathbb{Z}^{\mathbb{N}} \to \mathbb{Z}$ un morphisme de groupes tel que $\mathbb{Z}^{(\mathbb{N})} \subseteq \ker \varphi$. Montrer que $\varphi = 0$.

Arithmétique des polynômes

Manipulations algébriques

Δ **Exercice 88.** *Un cas particulier du fait que $\mathbb{K}[X]$ est intégralement clos.*

Soit $A \in \mathbb{K}[X]$ un polynôme.

Montrer que

$$\left(\exists F \in \mathbb{K}(X), F^2 = A\right) \Leftrightarrow \left(\exists P \in \mathbb{K}[X], P^2 = A\right).$$

♠ **Exercice 89.** *Nombre de racines distinctes.*

Soit $P \in \mathbb{C}[X]$ un polynôme non constant.

Expliquer comment calculer explicitement (par exemple par un algorithme) le nombre de racines distinctes de P.

Δ **Exercice 90.** *Polynômes à coefficients dans un anneau.*

Soit A un sous-anneau de $\mathbb{K}$.

On note $A[X]$ l'ensemble des polynômes de $\mathbb{K}[X]$ dont tous les coefficients sont dans A.

1. Montrer que $A[X]$ est un sous-anneau de $\mathbb{K}[X]$. Déterminer $(A[X])^\times$.
2. Soient $S \in A[X]$ et $T \in A[X]$ un polynôme non nul dont le **coefficient dominant est inversible** dans A.
   Montrer qu'il existe un unique couple $(Q, R) \in (A[X])^2$ tel que
   $$S = QT + R$$
   $$\deg(R) < \deg(T).$$
   Ce résultat reste-t-il vrai si on ne suppose plus l'inversibilité du coefficient dominant ?

Exercice 91. *Divisibilité et divisibilité.*

Soient $P, Q \in \mathbb{Z}[X]$, unitaires et non constants.

On suppose qu'il existe une infinité d'entiers n tels que $P(n)$ divise $Q(n)$ (dans $\mathbb{Z}$).

Montrer que P divise Q (dans $\mathbb{Z}[X]$).

Exercice 92. *Interpolation et extension de corps infinis.*

Soient $\mathbb{L}$ un corps et $\mathbb{K}$ un sous-corps infini de $\mathbb{L}$.

Soit $P \in \mathbb{L}[X]$ tel que $\forall z \in \mathbb{K}, P(z) \in \mathbb{K}$. Montrer $P \in \mathbb{K}[X]$.

♠ **Exercice 93.** *Lemme de descente pour la divisibilité.*

Soient $\mathbb{L}$ un corps et $\mathbb{K}$ un sous-corps de $\mathbb{L}$.

Soient $A, B \in \mathbb{K}[X]$ deux polynômes tels que $\exists Q \in \mathbb{L}[X] : A = QB$.

Montrer $\exists Q \in \mathbb{K}[X] : A = QB$.

Exercice 94. *Endomorphismes et automorphismes de $\mathbb{Q}[X]$.*

Déterminer les endomorphismes et les automorphismes de l'anneau $\mathbb{Q}[X]$.

Exercice 95. *Le radical d'un polynôme.*

Soient $\mathbb{K}$ un sous-corps de $\mathbb{C}$, $P \in \mathbb{K}[X]$ non constant et $x_1, \dots, x_n$ ses racines **distinctes** dans $\mathbb{C}$.

Montrer que
$$\prod_{i=1}^{n} (X - x_i) \in \mathbb{K}[X].$$

Δ **Exercice 96.** *Inclusion de corps et surjectivité.* *Mines*

Soit $P \in \mathbb{C}[X]$.

1. À quelle condition a-t-on $P(\mathbb{C}) = \mathbb{C}$?
2. À quelle condition a-t-on $P(\mathbb{R}) \subseteq \mathbb{R}$? À quelle condition a-t-on $P(\mathbb{R}) = \mathbb{R}$?
3. À quelle condition a-ton $P(\mathbb{Q}) \subseteq \mathbb{Q}$? (∗) À quelle condition a-t-on $P(\mathbb{Q}) = \mathbb{Q}$?

Restes et divisibilités

◦ **Exercice 97.** *Calculs de reste.*

Dans les questions 1 à 5, $P \in \mathbb{K}[X]$ est quelconque. Dans les questions 6 à 9, $n \in \mathbb{N}^*$.

1. Soit $\alpha \in \mathbb{K}$. Déterminer le reste de la division euclidienne de P par $X - \alpha$.
2. Soient $\alpha, \beta \in \mathbb{K}$ **distincts**. Déterminer le reste de la division euclidienne de P par $(X - \alpha)(X - \beta)$.
3. Soit $\alpha \in \mathbb{K}$. Déterminer le reste de la division euclidienne de P par $(X - \alpha)^2$.
4. Soient $\alpha \in \mathbb{K}$ et $k \in \mathbb{N}^*$. Déterminer le reste de la division euclidienne de P par $(X - \alpha)^k$.
5. Soient $\alpha_1, \dots, \alpha_r \in \mathbb{K}$ deux à deux distincts. Déterminer le reste de la division euclidienne de P par $\prod_{i=1}^{r} (X - \alpha_i)$.

Quelques calculs explicites :

6. Déterminer le reste de la division euclidienne de X^n par $X^2 - 3X + 2$.
7. Déterminer le reste de la division euclidienne de X^n par $(X - 1)^3$.
8. Soit $\theta \in \mathbb{R}$. Déterminer le reste de la division euclidienne de $(\cos(\theta) + X\sin(\theta))^n$ par $X^2 + 1$.
9. Déterminer le reste de la division euclidienne de X^n par $X^2 + X + 1$.

Exercice 98. *Antécédents multiples.*

Trouver un polynôme $P \in \mathbb{R}[X]$ de degré 5 tel que $(X - 1)^3$ divise $P + 1$ et $(X + 1)^3$ divise $P - 1$.

Exercice 99. *Divisibilité et composition à droite.*

Soient $A, B \in \mathbb{K}[X]$ et $P \in \mathbb{K}[X]$ **non constant**.

Montrer que $A(P) \mid B(P)$ si et seulement si $A \mid B$.

Exercice 100. *Divisibilité et Bernoulli itéré.*

Soit $P \in \mathbb{K}[X]$. Montrer que pour tout $n \in \mathbb{N}^*$, $P - X$ divise $\underbrace{P \circ P \circ \cdots \circ P}_{n \text{ fois}} - X$.

Exercice 101. *Une divisibilité, et son carré.*

Soit $P \in \mathbb{K}[X]$.

1. Montrer que pour tout $Q \in \mathbb{K}[X]$, P divise $P(X + PQ)$.
2. On suppose désormais que $\mathbb{K} = \mathbb{C}$ et que les racines de P sont simples. Déterminer les $Q \in \mathbb{C}[X]$ tels que P^2 divise $P(X + PQ)$.

Exercice 102. *Divisibilité par une puissance n-ième.*

Soit $P \in \mathbb{C}[X]$ non constant et $n \in \mathbb{N}^*$ tel que P^n divise $P \circ P$.

Montrer que X^n divise P.

Exercice 103. *Trois divisibilités à paramètre.* *X (PSI) adapté*

1. Déterminer les entiers $n \in \mathbb{N}^*$ tels que $X^3 - X^2 + X - 1$ divise $\left(X^2 - X + 1\right)^n - X^{2n} + X^n - 1$.
2. Déterminer les entiers $n \in \mathbb{N}^*$ tels que $(X^2 + X + 1)^2$ divise $(X + 1)^{6n+1} - X^{6n+1} - 1$.
3. Soit $m \in \mathbb{N}^*$. Donner une condition nécessaire et suffisante sur $(p, q) \in \mathbb{C}^2$ pour que $X^8 + X^4 + 1$ divise $X^{8m} + pX^{4m} + q$.

Exercice 104. *Un triplet contraint.*

Trouver les triplets $(n, a, b) \in \mathbb{N}^* \times (\mathbb{R}_+^*)^2$ tels que $X^2 - \left(a^2 + b^2\right)$ divise $X^{2n} - (a^n + b^n)^2$.

PGCD, Bézout

Δ **Exercice 105.** *PGCD et algorithme d'Euclide.*

Soient $(n, m) \in \mathbb{N}^2$. Montrer que

$$(X^n - 1) \wedge (X^m - 1) = X^{n \wedge m} - 1.$$

♠ **Exercice 106.** *Petits couples de Bézout.*

Soient $A, B \in \mathbb{K}[X]$ premiers entre eux et non constants.

Montrer qu'il existe U, V dans $\mathbb{K}[X]$ tels que

$$AU + BV = 1$$

et

$$\deg(U) < \deg(B)$$
$$\deg(V) < \deg(A).$$

Exercice 107. *Suite périodique.*

Soit $P, Q \in \mathbb{Z}[X]$ sans racine complexe commune. Montrer que $\left(P(n) \wedge Q(n)\right)_{n \in \mathbb{N}}$ est périodique.

Exercice 108. *Inégalité de Mason–Stothers et équation de Fermat polynomiale.*

Pour $P \in \mathbb{C}[X]$ non nul, on note $r(P)$ le nombre de racines **distinctes** de P dans $\mathbb{C}$ et $\operatorname{rad}(P) = \prod_{\substack{z \in \mathbb{C} \\ P(z)=0}} (X - z)$ le produit sur ces racines distinctes.

Dans les questions 1 à 5, $A, B, C \in \mathbb{C}[X]$ sont non tous constants, premiers entre eux dans leur ensemble, et vérifient $A + B + C = 0$.

1. Montrer que A, B et C sont deux à deux premiers entre eux.
2. On pose $W = A'B - AB'$. Montrer que $W = AC' - A'C$, et que $W \neq 0$.
3. **Inégalité de Mason-Stothers.** Montrer que $A/\operatorname{rad}(A)$, $B/\operatorname{rad}(B)$ et $C/\operatorname{rad}(C)$ divisent W, et en déduire
$$r(A) + r(B) + r(C) \geq \max(\deg(A), \deg(B), \deg(C)) + 1.$$
4. **Théorème de Fermat polynomial.** En déduire que si $n \geq 3$ et $A^n + B^n = C^n$ avec $A, B, C \in \mathbb{C}[X]$ premiers entre eux dans leur ensemble, alors A, B et C sont constants.
5. **Inégalités de Davenport.** Soient $A, B, C \in \mathbb{C}[X]$ avec $A \wedge B = 1$, C non nul et $A^3 - B^2 = C$. Montrer
$$\deg(C) \geq \frac{\deg(A)}{2} + 1 \quad \text{et} \quad \deg(C) \geq \frac{\deg(B)}{3} + 1.$$
6. **Une preuve directe de Fermat, sans Mason.** Soient $n \geq 3$ et (A, B, C) un triplet de polynômes deux à deux premiers entre eux, non tous constants, tel que $A^n + B^n + C^n = 0$. Montrer que C^{n-1} divise $AB' - A'B$ et conclure.

Racines multiples, images réciproques

Exercice 109. *Racines multiples de* $A^2 + B^2$. *X*

Soient $A, B \in \mathbb{C}[X]$ premiers entre eux.

Montrer que toute racine multiple de $A^2 + B^2$ est une racine de $(A')^2 + (B')^2$.

Exercice 110. *L'équation* $P\left(X^p\right)^q = P\left(X^q\right)^p$. *Mines*

Soient $p, q \in \mathbb{N}^*$ distincts. Déterminer les $P \in \mathbb{C}[X]$ tels que

$$P\left(X^p\right)^q = P\left(X^q\right)^p.$$

Exercice 111. *Divisibilité par la dérivée, et ses puissances.*

1. Déterminer les polynômes $P \in \mathbb{C}[X]$ non constants tels que P' divise P.
2. Déterminer les polynômes $P \in \mathbb{C}[X]$ non constants pour lesquels il existe $(m, n) \in (\mathbb{N}^*)^2$ tels que

$$(P')^m \text{ divise } P^n.$$

Exercice 112. *Polynôme multiple de sa dérivée seconde.* *X*

Soit P un polynôme complexe non nul ayant au moins deux racines distinctes et tel que P'' divise P.

1. Montrer que P est à racines simples.
2. Montrer que les racines de P sont alignées.

Exercice 113. *Contrôle des images réciproques.*

Soit $P \in \mathbb{C}[X]$ de degré $d \geq 1$, que l'on identifie à sa fonction polynomiale $\mathbb{C} \to \mathbb{C}$.

1. Soit $y \in \mathbb{C}$. Montrer que y possède $d - \deg((P - y) \wedge P')$ antécédents par P.
2. En déduire que, pour toute partie finie V de $\mathbb{C}$,

$$d(|V| - 1) < \left|P^{-1}[V]\right| \leq d\,|V|$$

et donner des exemples démontrant que cet encadrement est optimal.

Δ **Exercice 114.** *Images réciproques.* *X et ÉNS (PC)*

Soit $P, Q \in \mathbb{C}[X]$ non constants tels que $P^{-1}[\{0\}] = Q^{-1}[\{0\}]$ et $P^{-1}[\{1\}] = Q^{-1}[\{1\}]$. Montrer que $P = Q$.

Exercice 115. *Théorème de De Bruijn.*

Soient $a \leq b \leq c$ et $A \leq B \leq C$ des entiers ≥ 1. On s'intéresse dans cet exercice à la possibilité de paver un pavé de taille $A \times B \times C$ par des briques de taille $a \times b \times c$. Donnons des définitions précises.

- Une *brique* est une partie de $\mathbb{N}^3$ de la forme $\mathcal{B} = [\![x, x']\!] \times [\![y, y']\!] \times [\![z, z']\!]$.
- La *taille* d'une telle brique sera le triplet de ses trois « dimensions » $x' - x + 1$, $y' - y + 1$, $z' - z + 1$, rangées par ordre croissant. Par exemple, $[\![3, 5]\!] \times [\![1, 6]\!] \times [\![2, 4]\!]$ est une brique de taille $(3, 3, 6)$.
- On se demande si le pavé $P = [\![1, A]\!] \times [\![1, B]\!] \times [\![1, C]\!]$ de taille (A, B, C) peut s'écrire comme union disjointe de briques de taille (a, b, c) : on dira alors pour simplifier que P est (a, b, c)-pavable.

1. Montrer que le pavé de taille $(5, 6, 6)$ n'est pas $(1, 2, 4)$-pavable.

Étant donné une partie finie $E \subseteq \mathbb{N}^3$, on définit son *poids* $w(E) = (X - 1)^3 \sum_{(i,j,k) \in E} X^{i+j+k} \in \mathbb{R}[X]$.

2. Calculer le poids $w(\mathrm{P})$ du pavé $\mathrm{P} = [\![1, \mathrm{A}]\!] \times [\![1, \mathrm{B}]\!] \times [\![1, \mathrm{C}]\!]$.
3. Montrer que si P est (a, b, c)-pavable, alors $(\mathrm{X}^a - 1)(\mathrm{X}^b - 1)(\mathrm{X}^c - 1) \mid w(\mathrm{P})$.
4. Montrer que le pavé de taille $(10, 10, 10)$ n'est pas $(1, 2, 4)$-pavable.
5. Montrer que le pavé de taille $(7, 8, 9)$ n'est pas $(1, 2, 4)$-pavable.
6. Montrer le *théorème de De Bruijn* (1969) : si a divise b et b divise c, alors P est (a, b, c)-pavable si et seulement si, quitte à échanger A, B et C, on a $a \mid \mathrm{A}$, $b \mid \mathrm{B}$ et $c \mid \mathrm{C}$.

Racines et factorisations dans $\mathbb{R}[\mathrm{X}]$ et $\mathbb{C}[\mathrm{X}]$

Δ **Exercice 116.** *Racines et arithmétique dans les petits degrés.*

1. Soit $\mathrm{P} \in \mathbb{K}[\mathrm{X}]$ de degré 3, possédant au moins deux racines dans $\mathbb{K}$. Montrer que P est scindé.
2. Donner un exemple de polynôme de $\mathbb{R}[\mathrm{X}]$ de degré 4 n'admettant aucune racine et n'étant pas irréductible.
3. Soit $\mathrm{P} \in \mathbb{K}[\mathrm{X}]$ tel que $\deg(\mathrm{P}) \in \{2, 3\}$. Montrer que P n'est pas irréductible si et seulement si P admet une racine dans $\mathbb{K}$.
4. Donner un exemple de corps $\mathbb{K}$ et de polynôme $\mathrm{P} \in \mathbb{K}[\mathrm{X}]$ de degré 3 irréductible.

⋆ **Exercice 117.** *Méthode de Sturm.* *X*

Soit $\mathrm{P}_0 \in \mathbb{R}[\mathrm{X}]$ non constant, sans racine réelle multiple. On pose $\mathrm{P}_1 = \mathrm{P}_0'$ puis, tant que le reste n'est pas nul,

$$\mathrm{P}_{i+1} = -\mathrm{R}_i,$$

où R_i est le reste de la division euclidienne de P_{i-1} par P_i. On note M le dernier indice pour lequel P_M est non nul.

1. Montrer que M est bien défini et que P_M est de signe strictement constant sur $\mathbb{R}$.
2. Soit $t \in \mathbb{R}$ tel que $\mathrm{P}_0(t) \neq 0$. On note $\sigma(t)$ le nombre de changements de signe de la suite $(\mathrm{P}_0(t), \dots, \mathrm{P}_\mathrm{M}(t))$, les termes nuls étant ignorés.
   Montrer que pour $a < b$ non racines de P_0, le nombre de racines de P_0 dans $]a, b]$ vaut $\sigma(a) - \sigma(b)$.

Δ **Exercice 118.** *Polynômes réciproques.* *Mines*

On dit que $\mathrm{P} \in \mathbb{R}[\mathrm{X}]$ de degré $n \geq 0$ est *réciproque* lorsque

$$\mathrm{P} = \mathrm{X}^n \mathrm{P}(1/\mathrm{X}),$$

c'est-à-dire lorsque la suite de ses coefficients est palindromique. Soit P un polynôme réciproque.

1. Soit z une racine complexe de P. Montrer que $z \neq 0$, puis que $1/z$ est racine de P avec la même multiplicité que z.
2. On note α et β les multiplicités (éventuellement nulles) de 1 et de -1 comme racines de P. Montrer que α est pair, puis qu'il existe $q \in \mathbb{N}$ et $\mathrm{Q} \in \mathbb{R}[\mathrm{X}]$ de degré q tels que

$$\mathrm{P} = (\mathrm{X} - 1)^\alpha (\mathrm{X} + 1)^\beta \mathrm{X}^q \mathrm{Q}(\mathrm{X} + 1/\mathrm{X}).$$

3. Factoriser dans $\mathbb{R}[\mathrm{X}]$ le polynôme

$$\mathrm{P} = \mathrm{X}^7 - \frac{5}{2}\mathrm{X}^6 + \frac{3}{2}\mathrm{X}^5 + \frac{3}{2}\mathrm{X}^2 - \frac{5}{2}\mathrm{X} + 1.$$

Exercice 119. *Variations autour du trinôme de Selmer.* *Mines,Centrale*

Pour $n \geq 2$, on pose $P_n = X^n - X + (-1)^n$.

1. Déterminer les racines complexes de P_n'.
2. Montrer que P_n est à racines simples. Combien P_n a-t-il de racines dans $\mathbb{C}$? Dans $\mathbb{R}$?
3. Combien P_n a-t-il de racines dans $\mathbb{Q}$?
4. On note $a_1, \dots, a_n$ les racines complexes de P_n. Calculer

$$\begin{vmatrix} 1+a_1 & 1 & \cdots & 1 \\ 1 & 1+a_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 1 \\ 1 & \cdots & 1 & 1+a_n \end{vmatrix}.$$

Polynômes à coefficients entiers ou rationnels

Remarque. Le lemme de Gauss, premier exercice de cette section, est nécessaire pour certains des exercices suivants.

♠ **Exercice 120.** *Contenu d'un polynôme et lemme de Gauss polynomial.*

Pour tout $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$ un polynôme à coefficients entiers, on appelle son *contenu*, noté $c(P)$ le pgcd de ses coefficients, c'est à dire $c(P) = \bigwedge_{k=0}^{n} a_k$.

1. Soient $P_1, P_2 \in \mathbb{Z}[X]$ tels que $c(P_1) = 1$ et $c(P_2) = 1$. Montrer que $c(P_1 P_2) = 1$.
2. Soient $P_1, P_2 \in \mathbb{Z}[X]$. Montrer que $c(P_1 P_2) = c(P_1)\, c(P_2)$.
3. Soient $P, Q \in \mathbb{Z}[X]$ tels que P divise Q dans $\mathbb{Q}[X]$ et $c(P) = 1$. Montrer que P divise Q dans $\mathbb{Z}[X]$.

Exercice 121. *Des antécédents en interdisent d'autres.*

Soit $P \in \mathbb{Z}[X]$ prenant au moins 3 fois la valeur 12 sur $\mathbb{Z}$.

Montrer que P ne prend jamais la valeur 13 sur $\mathbb{Z}$.

Exercice 122. *Deux valeurs opposées, prises loin l'une de l'autre.*

Soient $P \in \mathbb{Z}[X]$ et $(m_1, m_2) \in \mathbb{Z}^2$ tels que

$$P(m_1) = 1, \quad P(m_2) = -1, \quad |m_1 - m_2| > 2.$$

Montrer que P n'a aucune racine dans $\mathbb{Q}$.

Exercice 123. *Croissance de beaucoup de polynômes à coefficients entiers.*

1. Soit $P \in \mathbb{Z}[X]$ et $n \in \mathbb{N}^*$ tels que pour tout $k \in [\![0, n-1]\!]$, $P(k) = 0$.
   Montrer que $n!$ divise $P(n)$.
2. Soit $f : \mathbb{N} \to \mathbb{N}$ telle que ÀPCR, $f(n) < \frac{1}{2} n!$.
   Montrer que $E_f = \{P \in \mathbb{Z}[X] \mid \forall n \in \mathbb{N},\ |P(n)| \leq f(n)\}$ est fini.
3. Montrer que $E = \{P \in \mathbb{Z}[X] \mid \forall n \in \mathbb{N},\ |P(n)| \leq n!\}$ est infini.

⋆ **Exercice 124.** *Une réciproque partielle d'une divisibilité utile.*

1. Soient $B, Q \in \mathbb{Z}[X]$. On pose $A = Q(B)$. Montrer que pour $a, b \in \mathbb{Z}$, $B(a) - B(b)$ divise $A(a) - A(b)$.
2. Réciproquement, soient $A, B \in \mathbb{Z}[X]$ avec A non constant, tels que

$$\forall (a,b) \in \mathbb{Z}^2, \quad B(a) - B(b) \text{ divise } A(a) - A(b).$$

Montrer qu'il existe $Q \in \mathbb{Q}[X]$ tel que $A = Q(B)$.

⋆ **Exercice 125.** *Polynôme qui permute.*

1. Soient $a_1, \dots, a_r$ des éléments de $\mathbb{K}$ deux à deux distincts.
Montrer qu'il existe un polynôme $P \in \mathbb{K}[X]$ tel que pour tout $i \in [\![1, r]\!]$, $P(a_i) = a_{i+1}$ (avec la notation $a_{r+1} = a_1$).
2. Existe-t-il un polynôme $P \in \mathbb{Z}[X]$ à coefficients **entiers** et $r \geq 3$ entiers $a_1, \dots, a_r$ deux à deux distincts tels que pour tout $i \in [\![1, r]\!]$, $P(a_i) = a_{i+1}$ (avec la notation $a_{r+1} = a_1$) ?

Exercice 126. *Progression divisible.*

Soit $P \in \mathbb{Z}[X]$ un polynôme à coefficients entiers.

Montrer que pour tout $n \in \mathbb{N}^*$ il existe un entier N_n tel que

$$n \mid \sum_{k=0}^{N_n} P(k).$$

⋆ **Exercice 127.** *Théorème de Skolem (1936).* *Saclay modifié*

Soit $\mathrm{Int}(\mathbb{Z}) = \{P \in \mathbb{C}[X] \mid \forall n \in \mathbb{Z}, P(n) \in \mathbb{Z}\}$ et $A, B \in \mathrm{Int}(\mathbb{Z})$ tels que $\forall n \in \mathbb{Z}, \mathrm{pgcd}\big(A(n), B(n)\big) = 1$.

1. Soit p un nombre premier. Montrer $\dfrac{(A^{p-1} - 1)(B^{p-1} - 1)}{p} \in \mathrm{Int}(\mathbb{Z})$ et en déduire l'existence de $R, S \in \mathrm{Int}(\mathbb{Z})$ tels que $\forall n \in \mathbb{Z}, A(n)R(n) + B(n)S(n) \equiv 1 \pmod{p}$.
2. Montrer qu'il existe $d \in \mathbb{N}^*$ et $U_0, V_0 \in \mathrm{Int}(\mathbb{Z})$ tels que $AU_0 + BV_0 = d$.
3. Déduire des deux premières questions qu'il existe $U, V \in \mathrm{Int}(\mathbb{Z})$ tels que $AU + BV = 1$.

Exercice 128. *Théorème de Schur.*

Soit $P \in \mathbb{Z}[X]$.

1. Montrer que, pour tout $Q \in \mathbb{N}^*$, P induit une application $\mathbb{Z}/Q\mathbb{Z} \to \mathbb{Z}/Q\mathbb{Z}$.
2. On suppose maintenant P non constant, et on veut montrer qu'il existe une infinité de nombres premiers divisant au moins un élément de $P[\mathbb{Z}]$.
   (a) En imitant la démonstration d'Euclide, montrer le résultat en supposant en outre $P(0) = 1$.
   (b) Conclure.

⋆ **Exercice 129.** *Définition arithmétique du degré.* *ÉNS*

Soit $P, Q \in \mathbb{Q}[X]$ tels que $\{P(x) \mid x \in \mathbb{Q}\} = \{Q(x) \mid x \in \mathbb{Q}\}$. Montrer que P et Q ont le même degré.

◦ **Exercice 130.** *Théorème des racines rationnelles.*

Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$, avec $a_n \neq 0$. On suppose que P possède des racines rationnelles $\frac{p_1}{q_1}, \dots, \frac{p_r}{q_r}$ (écrites sous forme irréductible et répétées selon leur multiplicité).

1. Montrer qu'il existe $Q \in \mathbb{Z}[X]$ tel que $P = Q \prod_{j=1}^{r} (q_j X - p_j)$.
2. En déduire que $p_1 \cdots p_r$ divise a_0 et que $q_1 \cdots q_r$ divise a_n.

Δ **Exercice 131.** *What Governors Need to Know about Trigonometry.* *Mines*

1. Montrer que pour tout $n \in \mathbb{N}$ il existe un unique polynôme $P_n \in \mathbb{Z}[X]$, **unitaire** de degré n, tel que
$$P_n\left(X + \frac{1}{X}\right) = X^n + \frac{1}{X^n}.$$
2. Soit $r \in \mathbb{Q}$ tel que $\cos(\pi r) \in \mathbb{Q}$. Montrer que $2\cos(\pi r) \in \mathbb{Z}$.
3. En déduire l'ensemble des $r \in \mathbb{Q}$ tels que $\cos(\pi r) \in \mathbb{Q}$.

Exercice 132. *Irréductibilité par réduction modulo p et contre-exemple.*

Soient $P \in \mathbb{Z}[X]$ **unitaire** de degré $n \geq 1$ et p un nombre premier. On note $\overline{P} \in \mathbb{F}_p[X]$ le polynôme obtenu en réduisant les coefficients de P modulo p.

1. Montrer que si $\overline{P}$ est irréductible dans $\mathbb{F}_p[X]$, alors P est irréductible dans $\mathbb{Q}[X]$.
2. Soit p un nombre premier impair, et $a, b \in \mathbb{F}_p$. Montrer que parmi a, b, ab au moins l'un est un carré dans $\mathbb{F}_p$.
3. Montrer que $X^4 + 1$ est irréductible dans $\mathbb{Q}[X]$ mais est réductible dans $\mathbb{F}_p[X]$ pour tout nombre premier p.

⋆ **Exercice 133.** *Un exemple de polynôme irréductible dans $\mathbb{Z}[X]$.*

Soient $\lambda_1, \dots, \lambda_n$ des entiers distincts. Montrer que $P = \prod_{k=1}^{n} (X - \lambda_k) - 1$ est irréductible dans $\mathbb{Z}[X]$.

Δ⋆ **Exercice 134.** *Un critère d'irréductibilité par localisation des racines.*

1. Soit $P \in \mathbb{Z}[X]$ tel que $|P(0)|$ est premier et que toutes les racines complexes de P sont de module strictement supérieur à 1.
Montrer que P est irréductible dans $\mathbb{Z}[X]$, puis dans $\mathbb{Q}[X]$.
2. Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$ de degré $n \geq 1$. On suppose que $|a_0|$ est premier et que $|a_0| > \sum_{k=1}^{n} |a_k|$.
Montrer que P est irréductible dans $\mathbb{Q}[X]$.
3. Soient p un nombre premier, $n \in \mathbb{N}^*$.
Montrer que $P = X^n + X^{n-1} + \cdots + X + p = \sum_{i=1}^{n} X^i + p$ est irréductible dans $\mathbb{Q}[X]$.

Exercice 135. *Factorisation sur $\mathbb{Z}$ de $P^2 + 1$.* *X*

Soit $P \in \mathbb{Z}[X]$ possédant n racines distinctes $x_1, \dots, x_n \in \mathbb{Z}$.

On écrit $P^2 + 1 = Q_1 \cdots Q_r$, avec des facteurs $Q_i \in \mathbb{Z}[X]$, et on pose $R = \sum_{i=1}^{r} Q_i^2 - r$.

1. Montrer que les x_j sont racines multiples de R.
2. En déduire qu'il existe $i \in [\![1, r]\!]$ tel que $\deg(Q_i) \geq 2\left\lfloor \frac{n+1}{2} \right\rfloor$.

Exercice 136. *Théorème d'irréductibilité d'Arthur Cohn.* *ÉNS modifié*

1. Soit $P \in \mathbb{Z}[X]$ et $n \in \mathbb{N}$ tel que
   - les racines complexes de P ont toutes une partie réelle $< n - 1$;
   - $P(n)$ est premier.

   Montrer qu'alors P est un élément irréductible de $\mathbb{Z}[X]$.
2. Soit $P \in \mathbb{Z}[X]$ et $n \in \mathbb{N}$ tel que
   - les racines complexes de P ont toutes une partie réelle $< n - \frac{1}{2}$;
   - $P(n-1) \neq 0$;
   - $P(n)$ est premier.

   Montrer qu'alors P est un élément irréductible de $\mathbb{Z}[X]$.
3. En déduire le *théorème d'irréductibilité de Cohn* : si un nombre premier a pour écriture décimale $p = a_m 10^m + \cdots + a_1 10 + a_0$, alors le polynôme $a_m X^m + \cdots + a_1 X + a_0$ est irréductible.

⋆ **Exercice 137.** *Le trinôme de Selmer.*

Soit $n \geq 2$ un entier. On pose $S = X^n - X - 1$ et, pour tout $P \in \mathbb{C}[X]$ de degré $m \geq 1$ avec $P(0) \neq 0$ et de racines $z_1, \ldots, z_m$ comptées avec multiplicité, $\lambda(P) = \sum_{j=1}^{m} \left(z_j - z_j^{-1}\right)$.

1. Pour $P \in \mathbb{C}[X]$, exprimer $\lambda(P)$ en fonction des coefficients de P.
   Pour des polynômes $P_1, P_2 \in \mathbb{C}[X]$, que dire de $\lambda(P_1 P_2)$?
2. Montrer que pour tout $Q \in \mathbb{Z}[X]$ diviseur unitaire non constant de S, $\lambda(Q) \in \mathbb{Z}$.
3. Soit $z = re^{i\theta}$ une racine de S, avec $r > 0$. Montrer que $2(r - 1/r)\cos(\theta) > 1/r^2 - 1$.
4. En déduire que $\lambda(Q) > 0$ pour tout diviseur unitaire non constant Q de S dans $\mathbb{Z}[X]$.
5. Conclure que S est irréductible dans $\mathbb{Q}[X]$.

Exercice 138. *Des irréductibles de tous degrés.*

1. Montrer que pour tout $n \in \mathbb{N}^*$ il existe un polynôme de degré n irréductible dans $\mathbb{Q}[X]$.
2. ($*$) Montrer qu'on peut de plus l'exiger **scindé sur** $\mathbb{R}$, c'est à dire n'ayant que des racines réelles.

Exercice 139. *Variante autour de Hensel.* *X*

1. Soit $B \in \mathbb{C}[X]$ tel que $B(0) \neq 0$.
   Montrer que pour tout $(k, n) \in \mathbb{N}^2$ il existe $P \in \mathbb{C}[X]$ tel que X^n divise $P^k - B$.
2. Soient $A, B \in \mathbb{C}[X]$ non constants n'ayant aucune racine commune.
   Montrer que pour tout $(k, n) \in \mathbb{N}^2$ il existe $P, Q \in \mathbb{C}[X]$ tels que A^n divise $P^k - Q$.

Exercice 140. *Un cas particulier du critère d'irréductibilité de Perron.* *X détaillé*

Soit $n \in \mathbb{N}$. On cherche à déterminer si $P_n = X^{n+1} - nX^n + 1$ est irréductible dans $\mathbb{Z}[X]$.

1. Traiter les cas $n = 0$, $n = 1$ et $n = 2$.
   On supposera dans la suite que $n \geq 3$.
2. Soit $z \in \mathbb{C}$ une racine de P_n telle que $|z| \geq 1$. Montrer que $|z - n| \leq \frac{1}{(n-1)^n}$.
3. En déduire que P_n possède exactement une racine de module supérieur ou égal à 1.
4. Conclure.

Indications

Exercice 1.

1. Montrer, en faisant des petits tiroirs de deux entiers consécutifs, qu'il existe même i et j tels que a_i et a_j soient consécutifs.
2. Tout entier a_i s'écrit sous la forme $2^{r_i}q_i$ avec q_i impair.
   Si $q_i = q_j$ alors $a_i \mid a_j$ ou $a_j \mid a_i$.

Exercice 2. Effectuer des formules de Bernoulli itérées.

Exercice 3. Un sens est immédiat.

Dans l'autre sens, remarquer que si $x = \dfrac{a}{b}$ est une fraction irréductible (où $(a,b) \in \mathbb{Z} \times \mathbb{N}^*$) alors $x^r = n$ ssi $a^r = nb^r$.

Passer aux *valuations p-adiques* pour un nombre premier p.

Exercice 4. D'un point de vue algorithmique, remarquer :

1. un **invariant** : la congruence modulo 9,
2. un **variant** : la « taille », a priori $s_{10}(n)$ est bien plus petit que n.

Exercice 5. Avec la division euclidienne $b = aq + r$ constater que $2^b + 1 = 2^r(2^{aq} - 1) + (2^r + 1)$.

Exercice 6. Bernoulli. D'un côté $a - b$ est divisible par n. De l'autre côté une somme de n termes tous égaux modulo n.

Exercice 7. Remarquer que $\mathrm{X}^4 + 4 = \left(\mathrm{X}^2 - 2\mathrm{X} + 2\right)\left(\mathrm{X}^2 + 2\mathrm{X} + 2\right)$.

Par conséquent

$$n^4 + 4m^4 = \left(n^2 - 2nm + 2m^2\right)\left(n^2 + 2nm + 2m^2\right) = \left((n-m)^2 + m^2\right)\left((n+m)^2 + m^2\right)$$

d'où la seule possibilité est $m = 1$ et $n - m = 0$.

Exercice 8. Prendre les valuations p-adiques, diviser par n et passer à la limite.

Exercice 9. Vérifier que $n = 1$, $n = 2$ et $n = 4$ conviennent ; pour $n \geq 2$, regarder modulo 4 pour déduire que n est pair.

Montrer que si $2^{2m} \mid (3^m - 1)(3^m + 1)$ alors $2^{2m-1} \mid 3^m - 1$ ou $2^{2m-1} \mid 3^m + 1$.

Se ramener à un nombre fini de cas.

Exercice 11.

1. On a $x \equiv y \pmod{p}$, d'où $x^k \equiv y^k \pmod{p}$.
   Utiliser Bernoulli et $\displaystyle\sum_{k=0}^{n-1} x^k y^{n-1-k} \equiv n y^{n-1} \pmod{p}$.
2. On a $x^k = (y + (x-y))^k = y^k + k(x-y)y^{k-1} + \cdots$ avec les termes suivants divisibles par $(x-y)^2$ donc par p^2.
   D'où $\displaystyle\sum_{k=0}^{n-1} x^k y^{n-1-k} \equiv 0 \pmod{p}$ et $\displaystyle\sum_{k=0}^{n-1} x^k y^{n-1-k} \equiv n y^{n-1} + \frac{n(n-1)}{2}(x-y)y^{n-2} \equiv n y^{n-1} \not\equiv 0 \pmod{p^2}$
   car $p \mid \dfrac{n(n-1)}{2}$.
3. Procéder par récurrence sur $v_p(n)$, en remarquant que si $n = ab$ alors $x^n - y^n = \left((x^a)^b - (y^a)^b\right)$.

Exercice 13. La valuation p-adique d'un entier n est un cardinal – celui de $\left\{k \in \mathbb{N}^* \,\middle|\, p^k \mid n\right\}$ – et il est toujours possible d'écrire un cardinal comme une somme de 1...

Exercice 15. On rappelle que $p \mid \binom{p}{k}$ pour $1 \leq k \leq p-1$, ainsi que la formule de Pascal. Alternativement $\frac{p-j}{j}$ ressemble beaucoup à -1 modulo p.

Exercice 17.

1. Remarquer que la formule de Legendre se relie à l'écriture binaire d'un entier.
2. En notant s_2 la somme des chiffres en base 2, on a relié à la question précédente $v_2(n!)$ à $s_2(n)$. Il s'agit ici de contrôler $v_2(n!) - v_2(k!) - v_2((n-k)!)$, c'est donc un problème de retenue d'additions. Alternativement dans $(\mathbb{Z}/2\mathbb{Z})[\mathrm{X}]$ on a $(1+\mathrm{X})^n = \prod_{k=1}^{r} \left(1 + \mathrm{X}^{2^{e_k}}\right)$.

Exercice 18.

1. Pour déterminer la loi de $v_p(\mathrm{X}_n)$, calculer $\mathbb{P}(v_p(\mathrm{X}_n) \geq k)$.
2. Simple passage à la limite.
3. Formule des queues.
4. Exprimer $s_p(n)$ en fonction des $\left\lfloor \frac{n}{p^k} \right\rfloor$.
5. Utiliser par exemple la question précédente.

Exercice 20. Après une transformée d'Abel cela revient à estimer $\sum_{k=1}^{n} v_p(k!)$ et la formule de Legendre peut être utile.

Exercice 21.

1. Wallis classique, on rappelle qu'une IPP permet d'obtenir la relation de récurrence.
2. Faire Wallis « de la mauvaise façon » c'est-à-dire en linéarisant le $\cos^{2n+1}$.
3. Mettre tout ensemble en remarquant que p^2 divise beaucoup de $\frac{p}{p-2k}\binom{p}{k}$

Exercice 22.

1. Faire une preuve similaire à celle de la formule de Legendre.
2. Minorer naïvement l'ordre par la taille (c'est-à-dire passer de $|$ à $\leq$). On remarque qu'on pourrait montrer que ces ordres sont d'abord constants puis multipliés par p à chaque étape, ce qui donne vraiment Legendre et un $O(m)$.

Exercice 23.

1. Capitaines.
2. Vandermonde.
3. Remarquer qu'avec les questions précédentes, modulo p^2, en posant $C(n,m) = \binom{np}{mp}$ on a

$$C(n,m) \equiv C(n-1,m) + C(n-1,m-1) \pmod{p^2}.$$

4. C'est même $(-1)^{k-1}$.
5. Par exemple en interprétant comme une relation coefficients-racines. Ou bien se convaincre que $\sum_{k=1}^{p-1} [k]_p^{-2} = \sum_{k=1}^{p-1} [k]_p^2 = \left[\sum_{k=1}^{p-1} k^2\right]_p$.

6. Encore par Vandermonde, avec des $\binom{p}{k}^2$, puis utiliser ce qu'on vient de faire.

Exercice 26. Raisonner par majorations successives.

On pourra aussi constater que si $(x_1, \dots, x_n)$ et $(y_1, \dots, y_m)$ conviennent, alors $(x_1y_1, x_1y_2, \dots, x_1y_m, x_2, \dots, x_n)$ convient.

Exercice 27. Une inclusion est immédiate.

Pour l'autre remarquer par exemple que déterminer un triplet pythagoricien revient à déterminer un point de $\mathbb{U} \cap \mathbb{Q}^2$. Le k correspond alors à la réduction en fraction irréductible et $\frac{n}{m}$ à la tangente de l'angle moitié.

Exercice 28.

1. Modulo 4 pour forcer $a = 1$, puis modulo 9 et 7.
2. Modulo 8 pour forcer $a = 2$, puis modulo 3.
3. $A^2 - B^2 = (A - B)(A + B)$.

Exercice 30.

1. Automatique.
2. Involution avec un seul point fixe.
3. Montrer que $4 \mid |S_0|$ et en déduire qu'il existe un élément tel que $a = b$.
4. Appliquer la question précédente à chaque facteur premier, puis stabilité par produit.

Remarque : il ne s'agit pas exactement de la version historique de D. Zagier, qui considérait plutôt, pour $x, y, z \in \mathbb{N}^*$ tels que $x^2 + 4yz = p$, l'involution

$$g(x,y,z) = \begin{cases} (x + 2z, z, y - x - z) & \text{si } x < y - z \\ (2y - x, y, x - y + z) & \text{si } y - z < x < 2y \\ (x - 2y, x - y + z, y) & \text{si } x > 2y \end{cases}$$

Exercice 31.

1. Si n et m sont premiers entre eux alors tout diviseur de nm s'écrit de manière unique comme produit d'un diviseur de n et d'un diviseur de m.
   Écrire la somme sur $\mathscr{D}(nm)$ comme une somme double sur $\mathscr{D}(n) \times \mathscr{D}(m)$.
2. On a $\sigma_s(p^k) = \sum_{j=0}^{k} (p^j)^s$. Distinguer selon $s = 0$ ou $s \neq 0$.
   Écrire n comme produit de ses facteurs premiers.

Exercice 32. Grouper les diviseurs entre eux, ou bien utiliser l'expression explicite de $\sigma_0(n)$ à l'aide des valuations p-adiques.

Exercice 33.

Au choix montrer la propriété pour $n = p^k$ puis utiliser la multiplicativité de σ_0 ou bien utiliser la formule exprimant $\sigma_0(n)$ à partir de valuations p-adiques.

Exercice 35. C'est une moyenne et $\sqrt{n} \leq \frac{1}{2}\left(d + \frac{n}{d}\right) \leq \frac{n+1}{2}$.

Alternativement en utilisant la multiplicativité on obtient juste un facteur $\frac{3}{2\sqrt{2}}$ de mieux…

On pourra remarquer que la borne de droite est souvent atteinte (premiers) mais celle de gauche est asymptotiquement faible.

Exercice 36. Intervertir une somme pour obtenir $\frac{1}{n}\sum_{d=1}^{n}\left\lfloor\frac{n}{d}\right\rfloor$.

Exercice 37.

1. Au moins trois méthodes :
   - Une formule par récurrence sur les S_m,
   - une bijection astucieuse,
   - une relation coefficient/racines sur X^n-1 et des sommes de Newton (plus compliqué).
2. Ne pas hésiter à tout développer.
3. Montrer que le nombre de solutions est divisible par p.

Exercice 38. Procéder par récurrence sur n (le cas $n=0$ est trivial, le cas $n=1$ donné par $x_1=a$).

Pour l'hérédité à partir de $n\geq 1$, rechercher x_{n+1} sous la forme $x_{n+1}=x_n+p^n y_n$.

Remarquer qu'alors $P(x_{n+1})\equiv P(x_n)+p^n y_n P'(x_n) \pmod{p^{n+1}}$.

Ou alors remarquer qu'une méthode de Newton fonctionne car si $h\equiv 0 \pmod{p^k}$ alors $P(a+h)\equiv P(a)+hP'(a) \pmod{p^{2k}}$!

Exercice 43. Commencer par remarquer que $\left(a^{\frac{p-1}{2}}\right)^2\equiv 1 \pmod p$ et donc par intégrité $a^{\frac{p-1}{2}}\equiv\pm 1 \pmod p$.

Montrer ensuite une inclusion et conclure sur l'égalité par calcul des cardinaux.

Remarque : on définit souvent le symbole de Legendre $\left(\frac{a}{p}\right)$ par 0 si $p|a$, 1 si a est un résidu quadratique modulo p et -1 sinon. On a alors $\left(\frac{a}{p}\right)\equiv a^{\frac{p-1}{2}} \pmod p$.

Déterminer les résidus quadratiques modulo p est donc équivalent à déterminer les valeurs du symbole de Legendre.

Par exemple les règles des signes sont les règles usuelles.

La loi de réciprocité quadratique permet de plus de relier $\left(\frac{p}{q}\right)$ et $\left(\frac{q}{p}\right)$. Si p et q sont deux nombres premiers impairs distincts, alors

$$\boxed{\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\frac{q-1}{2}}}.$$

Exercice 44. On cherche donc k et $n_1,\dots,n_m$ tels que $k+i\equiv 0 \pmod{n_i^3}$: prendre pour n_i des nombres premiers distincts.

Exercice 47. Cela revient à étudier

$$\sum_{k=1}^{p-1}\prod_{\substack{1\leq j\leq p-1\\ j\neq k}} j$$

modulo p^2 et

$$\sum_{k=1}^{p-1}\left(\prod_{\substack{1\leq j\leq p-1\\ j\neq k}} j\right)^2$$

modulo p.

Remarquer que cela ressemble très fortement à des relations coefficients-racines pour le polynôme

$$(X-1)(X-2)\cdots(X-(p-1))$$

qui est égal dans $(\mathbb{Z}/p\mathbb{Z})[X]$ à

$$X^{p-1} - 1.$$

Exercice 48. Il faut donc montrer que, parmi 2, 17 et 34, au moins un est toujours un carré modulo n.

Par théorème des restes chinois, il suffit de montrer que pour tout nombre premier p et tout entier k, au moins un des trois nombres $2, 17, 34$ est un carré modulo p^k.

Par le lemme d'Hensel, il y a trois cas à traiter :

1. $p \notin \{2, 17\}$: le symbole de Legendre étant multiplicatif et $2 \times 17 = 34$ donc au moins l'un vaut 1,
2. $p = 17$, on a $6^2 \equiv 2 \pmod{17}$,
3. $p = 2$, le cas restant à faire, utiliser $17 \equiv 1 \pmod 8$.

Exercice 49.

1. Montrer que dans $\mathbb{Z}/n\mathbb{Z}$ la suite $\left(F_k, F_{k+1}\right)_{k\in\mathbb{N}}$ est périodique, donc repasse par $(0, 1)$.
2. On a $F_n = \dfrac{\varphi^n - \overline{\varphi}^n}{\varphi - \overline{\varphi}}$ et $F_{n-1} + F_{n+1} = \varphi^n + \overline{\varphi}^n$.

Exercice 50.

1. C'est aussi $\displaystyle\sum_{\substack{d_1,d_2\in\mathbb{N}^* \\ d_1d_2=n}} f(d_1)g(d_2)$.
2. Cela dépend de $f(1)$.
3. Par exemple, développer, pour $n \in \mathbb{N}^*$, $\displaystyle\prod_{\substack{p\in\mathcal{P} \\ p|n}} (1 - 1)$.
4. On sait que $\varphi * 1 = \mathrm{Id}$, il n'y a plus qu'à inverser.

Exercice 53. Minorer $\displaystyle\prod_{k=1}^{r}\left(1 - \frac{1}{p_k}\right)$ par $\displaystyle\prod_{k=1}^{r}\left(1 - \frac{1}{k+1}\right)$.

Il reste à majorer r par $\log_2(n)$.

Exercice 54. Montrer que

$$i \wedge j = \sum_{d\in\mathcal{D}(i)\cap\mathcal{D}(j)} \varphi(d)$$

puis en déduire qu'avec $M = \left(\delta_{i\in\mathcal{D}(j)}\right)$ une matrice d'incidence de la relation de divisibilité on a

$$A = M^\top D M$$

où D est une matrice diagonale bien choisie.

Conclure en remarquant que M est triangulaire.

Exercice 55. Que dire de $\det(A + XB)$ évalué en ces 5 points ? Et de son degré ?

Exercice 56.

1. Par exemple formule explicite.
2. Montrer que, modulo p, on a $(A + B)^p = A^p + B^p$.
3. Remarquer que la trace est un coefficient de $\det(XI_n - M)$. Alternativement, on peut le faire « à la main » en projetant dans $\mathbb{Z}/p\mathbb{Z}$ et en exprimant explicitement la trace.

Exercice 57. Il faut bien évidemment introduire le polynôme $X^4 - X - 1$. Reste ensuite à regarder pourquoi ces conditions initiales très spécifiques conviennent. Les voir comme les traces des puissances successives de la matrice compagnon, ou de manière équivalente comme les sommes de Newton. Ne reste plus qu'à appliquer le morphisme de Frobenius pour montrer que u_p est u_1 modulo p.

Exercice 58. Il suffit de montrer que le produit des factorielles divise $V(a_1, \dots, a_n)$.

Or par opérations du pivot montrer que

$$V(a_1, \dots, a_n) = \begin{vmatrix} 1 & a_1 & a_1(a_1-1) & a_1(a_1-1)(a_1-2) & \cdots & a_1(a_1-1)\cdots(a_1-n+2) \\ 1 & a_2 & a_2(a_2-1) & a_2(a_2-1)(a_2-2) & \cdots & a_2(a_2-1)\cdots(a_2-n+2) \\ 1 & a_3 & a_3(a_3-1) & a_3(a_3-1)(a_3-2) & \cdots & a_3(a_3-1)\cdots(a_3-n+2) \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & a_n(a_n-1) & a_n(a_n-1)(a_n-2) & \cdots & a_n(a_n-1)\cdots(a_n-n+2) \end{vmatrix}$$

puis conclure en remarquant que (coefficients binomiaux) on a pour tout $j \in [\![1, n-1]\!]$ et $a \in \mathbb{Z}$, $j!$ divise $a(a-1)\cdots(a-j+1)$.

Exercice 59. Commencer par montrer que les inversibles de $M_n(\mathbb{Z})$ sont ceux de déterminant dans $\mathbb{Z}^\times = \{-1, +1\}$.

Montrer que si $|\det(A)|$ est premier ou égal à 1 alors la matrice est irréductible.

Pour la réciproque (par contraposée) traiter d'abord le cas triangulaire.

S'y ramener ensuite par des transvections et donc un algorithme d'Euclide.

Exercice 60. Commencer par traduire le problème : pour tout $i \in [\![1, 2n+1]\!]$ il existe des coefficients a_{ij} tels que $a_{ii} = 0$, $a_{ij} \in \{-1, 1\}$ pour $j \neq i$, la moitié des $2n$ coefficients hors diagonale valant 1 et l'autre moitié -1 et pour tout $i \in [\![1, 2n+1]\!]$, $\sum_{j=1}^{2n+1} a_{ij} p_j = 0$.

On obtient une matrice A et il faut montrer que $\begin{matrix} 1 \\ 1 \\ \vdots \\ 1 \end{matrix}$ et $\begin{matrix} p_1 \\ p_2 \\ \vdots \\ p_{2n+1} \end{matrix}$ sont colinéaires.

Or ils appartiennent tous les deux au noyau de A.

On peut alors s'intéresser au lemme suivant : si une matrice $2n \times 2n$ de $M_{2n}(\mathbb{Z}/2\mathbb{Z})$ a une diagonale nulle et tous les autres coefficients non nuls alors elle est inversible.

Ce n'est plus qu'une question de réduction modulaire et de mineurs ensuite.

Exercice 61. On rappelle que $A\,\mathrm{Com}(A)^\top = \det(A) I_n$ et qu'il existe $(u, v) \in \mathbb{Z}^2$ tels que $\det(A)u + \det(B)v = 1$.

Remarquer que la réciproque est fausse.

Exercice 62. Remarquer que $\det(M - M^\top) = 0$ dans $\mathbb{Z}$ et donc dans $\mathbb{Z}/(a+b)\mathbb{Z}$.

Remarquer aussi que dans $\mathbb{Z}/(a+b)\mathbb{Z}$, $b = -a$.

Exercice 63. Faire comme la base b mais avec un signe $-$…

Exercice 64. Voir sous l'angle algorithmique de construction d'une telle suite. Ici un algorithme glouton fonctionne (à montrer).

Exercice 65. Raisonner par analyse-synthèse.

Comme pour une décomposition en base b, a_1 est le reste de la division euclidienne de n par 2.

Puis a_2 est le reste de la division euclidienne de $\frac{1}{2}(n-a_1)$ par 3, etc.

Exercice 67. Remarquer que pour tout $n \in \mathbb{N}$, $(n+4)^2-(n+3)^2-(n+2)^2+(n+1)^2=4$ et procéder par récurrence d'ordre 4.

Exercice 68.

1. RAS (écriture en base b)
2. Se convaincre que cela revient à la périodicité de $[n^n]_{b^{k+1}}$ puis, par le théorème des restes chinois, à celle de $[n^n]_{p^\alpha}$ pour p^α facteur de la décomposition de b^{k+1}. Deux termes bougent de périodes différentes mais montrer que $p^\alpha \vee \varphi(p^\alpha)$ (ou $p^\alpha \times \varphi(p^\alpha)$) convient.

Exercice 69. Bernoulli.

Exercice 70. Écrire une relation de récurrence de la forme $F_n = \prod_{k=0}^{n-1} F_k + 2$ ou $F_{n+b} = (F_n-1)^{2^b}+1$.

Exercice 72. Adapter la preuve d'Euclide, en remarquant qu'un nombre premier assez grand est congru à 1 ou 3 modulo 4 (resp. à 1 ou 5 modulo 6) et qu'un produit de 1 fait toujours 1.

Exercice 73.

1. C'est un cas particulier de l'exercice sur les résidus quadratiques.
2. Adapter la preuve d'Euclide à $(2p_1\cdots p_r)^2+1$.

Exercice 75.

1. Explicite.
2. Que dire de l'ordre de np dans $(\mathbb{Z}/q\mathbb{Z})^\times$? Montrer que c'est 1 ou p mais pas 1.
3. Adapter la preuve usuelle d'Euclide.

Exercice 76. Remarquer que si $n \leq N$, alors pour tout p premier, $v_p(n) \leq \frac{\ln(N)}{\ln(p)} \leq \frac{\ln(N)}{\ln(2)}$.

Si la série converge alors remarquer que pour toute partie B de $\mathcal{P}$, $|\{n \in [\![1,N]\!], \exists p \in B, p|n\}| \leq (\sum_{p\in B}\frac{1}{p})N$.

Exercice 77.

1. Rédaction automatique pour l'un, il « suffit » de faire pour 2 pour l'autre et conclure par récurrence.
   Remarquer que pour tout $\tilde{b} \in A_{a,b}$, $A_{a,b} = A_{a,\tilde{b}}$.
   Pour U_1 et U_2 deux ouverts remarquer que si $U_1 \cap U_2 \neq \emptyset$ alors il existe $\tilde{b} \in U_1 \cap U_2$.
   Prendre ensuite tout multiple commun des deux raisons.
   Puis passage au complémentaire des propriétés sur les ouverts.
2. Écrire $\overline{A_{a,b}}$ comme l'union de $a-1$ ouverts.
3. Si l'ensemble des nombres premiers est fini, alors $\{-1,1\}$ est le complémentaire d'une union finie de fermés, donc ouvert.
   Mais il est non vide fini.

Exercice 78.

1. Par récurrence sur p.
2. Par exemple reparamétrer en $F_{n+p} \wedge F_n = F_{(n+p)\wedge n} = F_{p\wedge n}$ et procéder par récurrence.

Exercice 79. S'inspirer des exercices précédents.

Par exemple pour $k \in \mathbb{N}$, pour tout n on a $a_{n+k} = \underbrace{P \circ P \circ \cdots \circ P}_{k \text{ fois}}(a_n)$ et en particulier (comme pour tout polynôme R à coefficients entiers $R(a_n) \equiv R(0) \pmod{a_n}$), on a une écriture de la forme

$$a_{n+k} = a_n q_{n,k} + a_k.$$

Procéder par algorithme d'Euclide simultané.

Exercice 80. Poser pour tout $n \in \mathbb{N}$, $a_n = \alpha^n + \beta^n$.
Constater que pour tout $m \geq 2n$, $a_n a_{m-n} = a_m + (\alpha\beta)^n a_{m-2n}$.
Procéder alors à un algorithme d'Euclide simultané.

Exercice 81. Remarquer que la suite est autonome et travailler modulo 3.

1. Si $a_0 \equiv 0 \pmod 3$ alors pour tout n, $a_n \equiv 0 \pmod 3$. Et si $a_0 \leq (3m)^2$ alors pour tout $n \in \mathbb{N}$, $a_n \leq (3m)^2$.
2. Si $a_0 \equiv 2 \pmod 3$ alors pour tout n, $a_n \equiv 2 \pmod 3$ et $a_n = a_0 + 3n$.
3. Il reste le cas $a_0 \equiv 1 \pmod 3$.
   Traiter à la main les petits cas.
   Remarquer que si $a_0 = 3k+1$ alors comme $(3k-1)^2 = (3k+1) + 9\left(k^2 - k\right)$, si $k \geq 9$ alors il existera un rang où $a_n < a_0$.
   Si ce a_n est congru à 2 modulo 3 alors on a terminé.
   Conclure par récurrence forte dans le cas de congruence à 1.

Exercice 83.

1. Utiliser les relations coefficients/racines.
2. Faire un principe de descente infinie.

Exercice 84. Remarquer que tout point de $\mathbb{C}$ est à distance au plus $\frac{\sqrt{2}}{2} < 1$ d'un point de $\mathbb{Z}[i]$.

Exercice 85. Il y a plusieurs points à remarquer :

1. Montrer que si $|z|^2 \in \mathcal{P}$ alors z est premier est un simple constat,
2. Montrer que si z est premier, il existe $p \in \mathcal{P}$ tel que $z|p$ (dans $\mathbb{Z}[i]$)
3. Pour $p \in \mathcal{P}$, p est premier dans $\mathbb{Z}[i]$ ssi -1 n'est pas un carré modulo p.

Exercice 86. Se ramener à montrer que $\mathbb{U}_n \cap \mathbb{Q}(i) \subseteq \mathbb{U}_4$. Pour cela remarquer que le polynôme minimal d'une racine n-ième est à coefficients entiers et que celui d'un élément de $\mathbb{Q}(i)$ est de degré ≤ 2.

Exercice 88. Faire exactement la même preuve que pour $\mathbb{Q}$ et $\mathbb{Z}$ (par exemple descente infinie, ou irréductibilité et Euclide, ou parité des valuations associées aux facteurs irréductibles, etc.).

On peut montrer de manière générale que si F est racine d'un polynôme unitaire à coefficients dans $\mathbb{K}[X]$, alors $F \in \mathbb{K}[X]$ (avec la preuve usuelle de caractérisation des racines rationnelles).

Exercice 89. Cela revient à calculer $\deg(P) - \deg(P \wedge P')$.

Exercice 90.

1. Vérifier la définition de sous-anneau. On a $(A[X])^\times = A^\times$, en identifiant un polynôme constant à la constante associée.
2. Faire la même preuve que pour un corps, et noter l'utilisation de l'inversibilité du coefficient dominant. Le résultat est faux de manière générale. Ainsi, dans $\mathbb{Z}[X]$, la division euclidienne de X^2 par $2X$ n'existe

pas.

Exercice 91. Comme il s'agit de polynômes unitaires, on peut effectuer une division euclidienne dans $\mathbb{Z}[X]$, soient A et B dans $\mathbb{Z}[X]$ tels que

$$Q = AP + B$$

et $\deg(B) < \deg(P)$.

Alors il existe une infinité d'entiers n tels que $P(n)$ divise $B(n) = Q(n) - A(n)P(n)$.

Comme $\deg(P) > \deg(B)$, on a de plus $|P(n)| > |B(n)|$ pour $|n|$ assez grand.

L'ensemble des entiers considérés étant infini, il en existe donc une infinité pour lesquels $B(n) = 0$.

Exercice 92. Lagrange.

Exercice 93. Existence de la division euclidienne dans le petit corps et unicité de la division euclidienne dans le grand.

Exercice 94. Tout endomorphisme de $\mathbb{Q}[X]$ fixe $\mathbb{Q}$: c'est donc un endomorphisme de $\mathbb{Q}$-algèbre, entièrement déterminé par l'image de X. Réciproquement, toute image de X dans $\mathbb{Q}[X]$ définit un endomorphisme. Il s'agit d'un automorphisme si et seulement si cette image est de la forme $aX + b$, avec $a \in \mathbb{Q}^*$ et $b \in \mathbb{Q}$.

Exercice 95. Le produit cherché est, à une constante multiplicative près, le quotient $P/(P \wedge P')$.

Méditer sur le lien avec $\sqrt{P\mathbb{K}[X]}$.

Exercice 96.

1. D'Alembert-Gauss
2. Décomposer $P = A + iB$ puis dire qqchose sur le degré de A après avoir montré que B est nul.
3. Lagrange.
   Il reste l'autre question.
   Écrire $P \in \mathbb{Q}[X]$, et l'on écrit $P = A/c$ avec $A = \sum_{k=0}^{n} \alpha_k X^k \in \mathbb{Z}[X]$ et $c \in \mathbb{N}^*$.
   Montrer que $\mathscr{S} = P^{-1}(\mathbb{Z}) \subseteq \frac{1}{a_n}\mathbb{Z}$.
   Et donc (progression arithmétique, comptage et asymptotique) on obtient
   $$P(\mathscr{S}) \cap [\![1, N = O(N^{\frac{1}{n}})$$
   et donc P de degré 1.

Exercice 97.

1. Évaluer en α : $R = P(\alpha)$.
2. Évaluer en α et en β ; R est affine et passe par deux points :
   $$R = P(\alpha)\frac{X-\beta}{\alpha-\beta} + P(\beta)\frac{X-\alpha}{\beta-\alpha}.$$
3. Évaluer, puis dériver et évaluer, en α : $R = P'(\alpha)(X-\alpha) + P(\alpha)$.
4. Dériver j fois et évaluer en α pour $0 \leq j \leq k-1$, ou plus directement écrire la formule de Taylor de P en α et tronquer :
   $$R = \sum_{j=0}^{k-1} \frac{P^{(j)}(\alpha)}{j!}(X-\alpha)^j.$$
5. C'est le polynôme d'interpolation de Lagrange de P aux points α_i :
   $$R = \sum_{i=1}^{r} P(\alpha_i) \prod_{j \neq i} \frac{X-\alpha_j}{\alpha_i - \alpha_j}.$$

6. Appliquer ce qui précède avec le bon découpage du diviseur. Ici $X^2 - 3X + 2 = (X-1)(X-2)$: deux racines simples, donc question 2. Réponse : $(2^n - 1)X + 2 - 2^n$.
7. Racine triple en 1, donc question 4 : $R = 1 + n(X-1) + \binom{n}{2}(X-1)^2$.
8. $X^2 + 1 = (X-i)(X+i)$ dans $\mathbb{C}[X]$: deux racines simples, donc question 2 après passage à $\mathbb{C}$. Utiliser $\cos(\theta) + i\sin(\theta) = e^{i\theta}$, d'où $R(i) = e^{in\theta}$ et $R(-i) = e^{-in\theta}$. Réponse : $R = \sin(n\theta)X + \cos(n\theta)$.
9. $X^2 + X + 1 = (X-j)\left(X - \bar{j}\right)$: évaluer en j et discuter selon n modulo 3. Réponse : 1, X ou $-X-1$ selon que $n \equiv 0, 1, 2\ [3]$.

On notera, sur les questions 8 et 9, que le reste est à coefficients réels bien qu'on ait travaillé dans $\mathbb{C}$: c'est le changement de corps, le reste étant unique.

Exercice 99. Par exemple déduire la division euclidienne de $B(P)$ par $A(P)$ de celle de B par A.

Exercice 100.

On peut montrer que pour tout $R \in \mathbb{K}[X]$, il existe $Q_R \in \mathbb{K}[X]$ tel que

$$R(P(X)) - R(X) = Q_R(X)(P(X) - X)$$

et appliquer cette relation aux itérées successives de P, puis télescoper.

Alternativement, appliquer l'identité $R \mid R(X+R)$ au polynôme $R = P - X$, puis raisonner par récurrence.

Alternativement remarquer que modulo $P - X$, $P \equiv X\,[P-X]$ et itérer.

Exercice 101.

1. On peut par exemple appliquer la formule de Bernoulli à $P(X+PQ) - P(X)$. Voir le lien avec la divisibilité de $P \circ P - X$ par $P - X$, ou encore avec le développement $P(X+H) \equiv P(X) \pmod{H}$.
2. Remarquer que $P(X+H) \equiv P(X) + P'(X)H \pmod{H^2}$; cela revient donc à $P \mid 1 + P'Q$.
   Les racines de P étant simples, $P \wedge P' = 1$. Si (U, V) vérifie $PU + P'V = 1$, la condition s'écrit $Q \equiv -V\ [P]$.

Exercice 103.

1. On a $X^3 - X^2 + X - 1 = (X-1)\left(X^2+1\right)$, de racines 1, i, $-i$.
   En 1, on a $0 = 0$. En i, on trouve $(-i)^n - (-1)^n + i^n - 1 = 2\cos(n\pi/2) - (-1)^n - 1$ et $-i$ s'en déduit par conjugaison. Discuter selon n modulo 4.
   Réponse : les entiers n tels que $n \not\equiv 2\ [4]$.
2. Cela revient à vérifier que j est une racine double du dividende. Calculer sa valeur et celle de sa dérivée en j. Tous les entiers $n \in \mathbb{N}^*$ conviennent.
3. Remarquer que
   $$X^8 + X^4 + 1 = \frac{X^{12} - 1}{X^4 - 1},$$
   donc que ses racines sont les racines douzièmes de l'unité qui ne sont pas des racines quatrièmes, c'est à dire celles d'ordre 3, 6 ou 12 et elles sont simples.
   Soit ζ une telle racine et $\omega = \zeta^{4m}$: alors $\omega^3 = \zeta^{12m} = 1$, et la condition s'écrit $\omega^2 + p\omega + q = 0$. Discuter selon m modulo 3 : si $3 \mid m$, la condition est $p + q = -1$; sinon, c'est $(p, q) = (1, 1)$.

Exercice 104. Cela revient à résoudre

$$\left(a^2 + b^2\right)^n = \left(a^n + b^n\right)^2.$$

Par homogénéité et positivité, poser $t = b/a > 0$ et étudier

$$g(t) = n\ln(1+t^2) - 2\ln(1+t^n).$$

En déduire que $n = 2$ et que tout couple convient.

Exercice 105. Cf le TD d'arithmétique.

Montrer que, pour tous $a \in \mathbb{N}$ et $b \in \mathbb{N}^*$, si r est le reste de la division euclidienne de a par b, alors $X^r - 1$ est le reste de la division euclidienne de $X^a - 1$ par $X^b - 1$.

Faire tourner un algorithme d'Euclide.

Exercice 106. Comme dans $\mathbb{Z}$, déterminer la structure de tous les couples de Bézout, et montrer qu'au moins un convient.

Exercice 107. Montrer l'existence de $t \in \mathbb{N}^*$ et $U, V \in \mathbb{Z}[X]$ tels que $PU+QV = t$. En posant $d_n = P(n) \wedge Q(n)$, vérifier alors que

$$d_n = P(n) \wedge Q(n) \wedge t.$$

Utiliser enfin les congruences $P(n+t) \equiv P(n)\ [t]$ et $Q(n+t) \equiv Q(n)\ [t]$.

Exercice 108.

1. RAS.
2. Constater que $W = \left(\frac{A}{B}\right)' B^2$. Substituer $B = -A - C$.
3. Les facteurs irréductibles de $A/\operatorname{rad}(A)$ sont exactement ceux qui apparaissent à la fois dans A et dans A'.
   Ces trois quotients sont deux à deux premiers entre eux, donc leur produit divise W. Comparer les degrés en utilisant $\deg(W) \leq \deg(A) + \deg(B) - 1$, après avoir supposé (quitte à renommer) que $\deg(C)$ est le plus grand des trois.
4. Appliquer l'inégalité de Mason–Stothers au triplet $(A^n, B^n, -C^n)$, en remarquant $r(A^n) = r(A) \leq \deg(A)$.
5. Appliquer l'inégalité de Mason–Stothers au triplet $\left(A^3, -B^2, -C\right)$, après avoir vérifié qu'il est admissible.
6. Multiplier $A^n + B^n + C^n = 0$ par B', multiplier la relation dérivée

   $$A^{n-1}A' + B^{n-1}B' + C^{n-1}C' = 0$$

   par B, et soustraire. Il vient

   $$A^{n-1}\left(AB' - A'B\right) = -C^{n-1}\left(CB' - BC'\right),$$

   et l'on conclut avec $A \wedge C = 1$ et le lemme de Gauss.
   Supposer $\deg(C)$ maximal et comparer les degrés :

   $$(n-1)\deg(C) \leq \deg(A) + \deg(B) - 1 \leq 2\deg(C) - 1,$$

   d'où $(n-3)\deg(C) \leq -1$, absurde pour $n \geq 3$ sauf si $AB' - A'B = 0$ — cas qui force A et B proportionnels, donc constants.

Exercice 109. On pourra profiter d'être sur $\mathbb{C}$ pour factoriser $A^2 + B^2$.

Exercice 110. Le polynôme nul convient. Les autres solutions sont les cX^m, avec $m \in \mathbb{N}$, $c \in \mathbb{C}^*$ et $c^p = c^q$.

Si $P \neq 0$, écrire $P = X^k R$ avec $R(0) \neq 0$; on a alors aussi $R\left(X^p\right)^q = R\left(X^q\right)^p$.

Quitte à échanger p et q, supposer $q > p$. Si $z \neq 0$ est une racine de R de multiplicité maximale M, choisir $u \in \mathbb{C}^*$ tel que $u^p = z$. L'égalité montre que u^q est une racine de R, de multiplicité N vérifiant $pN = qM$. Ainsi $N > M$, contradiction. Donc R est constant ; l'égalité initiale donne alors $c^p = c^q$.

Exercice 111.

1. Classique : si $d = \deg(P)$, soit, par le degré, le quotient est $\frac{1}{d}(X - \lambda)$, soit on utilise $\frac{P'}{P} = \frac{d}{X - \lambda}$.

2. On a alors que toute racine de P' est racine de P.
   Faire un comptage : si P est de degré d et possède r racines distinctes de multiplicités $\alpha_1, \dots, \alpha_r$, alors P' admet ces racines avec les multiplicités $\alpha_i - 1$, ce qui en fait $d - r$ comptées avec multiplicité. Comme $\deg(P') = d - 1$, il reste exactement $r - 1$ racines de P', comptées avec multiplicité, qui ne sont **pas** racines de P.
   Donc $r = 1$.

Exercice 112. Pour la deuxième question, on pourra utiliser le théorème de Gauss–Lucas et faire des dessins !

Exercice 116.

1. Factoriser, le quotient est de degré 1.
2. N'importe quel polynôme de signe constant convient, que dire par exemple de $X^4 + 1$?
3. Remarquer que si $a + b \in \{2, 3\}$ avec a et b dans $\mathbb{N}^*$ alors au moins l'un des deux vaut 1.
4. Par exemple $\mathbb{K} = \mathbb{Q}$ et $P = X^3 - 2$.

Exercice 117.

1. Remarquer que
   $$(P_{i+1}, P_i) = (-R_i, P_i)$$
   ressemble à un algorithme bien connu.
   En déduire que P_M est associé à $\operatorname{pgcd} P_0 P_0'$. Montrer alors que P_M n'a aucune racine réelle.
2. Observer que
   - Deux polynômes consécutifs P_i, P_{i+1} n'ont aucune racine réelle commune.
   - Si x est une racine de P_i, avec $0 < i < M$, alors $P_{i-1}(x)$ et $P_{i+1}(x)$ sont non nuls et de signes opposés. En déduire que σ ne change pas lorsque t traverse x.
   - Si x est une racine de P_0, alors $P_1(x) = P_0'(x) \neq 0$ et σ diminue de 1 lorsque t traverse x.

   Ainsi σ est constante entre les racines de P_0 et diminue exactement de 1 à chaque racine de P_0.

Exercice 118.

1. Le coefficient constant de P est son coefficient dominant, non nul : donc $P(0) \neq 0$. Pour la multiplicité avec $P = (X - z)^m R$ avec $R(z) \neq 0$, écrire $X^n P(1/X)$ en remarquant que $(1 - zX)^m = (-z)^m (X - 1/z)^m$.
2. Poser $R = P / \left((X-1)^\alpha (X+1)^\beta\right)$, de degré $n - \alpha - \beta$. Vérifier que $X - 1$ est *anti*-réciproque et $X + 1$ réciproque, donc que
   $$X^{n-\alpha-\beta} R(1/X) = (-1)^\alpha R.$$
   Évaluer en 1 pour obtenir α pair.
   D'après la première question, le degré de R est pair, disons $2q$. Écrire $R = \sum_{k=0}^{2q} r_k X^k$ avec $r_k = r_{2q-k}$ puis
   $$R = X^q \left(r_q + \sum_{k=1}^{q} r_{q+k} \left(X^k + X^{-k} \right) \right).$$
   Il reste à montrer que $X^k + X^{-k}$ est un polynôme en $X + X^{-1}$, par exemple par récurrence sur k ou avec Tchebychev.
3. Le polynôme P est bien réciproque, de degré impair.
   On obtient à la fin
   $$P = (X-1)^4 (X+1) \left(X^2 + \frac{1}{2} X + 1 \right).$$

Exercice 119.

1. $P_n' = nX^{n-1} - 1$, d'où, à un module près, les racines $(n-1)$-ièmes de l'unité.
2. Pour une racine z de P_n' qui serait aussi racine de P_n, on a $z^n = z/n$; en réinjectant dans P_n, on obtient une contradiction.
   Pour le cas réel, faire une étude de fonction et montrer que, dans le cas pair, la fonction est strictement positive en son minimum et qu'elle s'annule une fois dans le cas impair.
3. Pour le cas rationnel, utiliser un critère bien connu sur les racines rationnelles d'un polynôme à coefficients entiers.
4. Montrer que le déterminant d'une matrice $D + J$, où $D = \operatorname{diag}(a_1, \dots, a_n)$ et J est la matrice de rang 1 dont tous les coefficients valent 1, vaut
$$\prod_{i=1}^{n} a_i + \sum_{j=1}^{n} \prod_{i \neq j} a_i$$
et utiliser les relations entre coefficients et racines.

Remarque. Cet exercice tombe parfois au concours avec $X^n - X - 1$ ou $X^n - X + 1$ à la place de P_n.

Exercice 120.

1. Prendre un diviseur premier de $c(P_1P_2)$ et regarder modulo p. Alternativement regarder le premier coefficient non divisible par p dans P_1 et P_2.
2. Se ramener à un contenu de 1.
3. Le plus simple est d'étendre le contenu à $\mathbb{Q}[X]$.

Exercice 121. On a $P - 12 = (X - a_1)(X - a_2)(X - a_3)Q$ avec $a_1, a_2, a_3 \in \mathbb{Z}$ distincts et $Q \in \mathbb{Z}[X]$ (division euclidienne par un unitaire).
Si $P(b) = 13$, parmi $b - a_1$, $b - a_2$ et $b - a_3$, au moins un n'est pas ± 1.

Exercice 122. Si p/q est une racine de P avec $\operatorname{pgcd}(p, q) = 1$, on a, par le lemme de Gauss,
$$P = (qX - p)Q, \quad Q \in \mathbb{Z}[X].$$
Évaluer en m_1 et m_2 : les entiers $qm_1 - p$ et $qm_2 - p$ divisent respectivement 1 et -1, donc valent ± 1.
Mais $|q(m_1 - m_2)| \geq |m_1 - m_2| > 2$.

Exercice 123.

1. Faire la division par le polynôme unitaire $X(X-1)\cdots(X-(n-1))$.
2. Si P et Q coïncident sur $[\![0, N-1]\!]$, alors N! divise $P(N) - Q(N)$, et $|P(N) - Q(N)| \leq 2f(N) < N!$. Puis une récurrence.
3. Exhiber une famille infinie, au hasard $X(X-1)\cdots(X-k+1)$.

Remarque. On a probablement que le « seuil » critique est $(1 - e^{-1})n!$.

Exercice 124.

1. Bernoulli.
2. Écrire (par divisions euclidiennes successives dans $\mathbb{Q}[X]$) $A = \sum_{k=0}^{m} C_k B^k$, où les C_k sont dans $\mathbb{Q}_{\deg(B)-1}[X]$ (écriture « en base B »). On veut montrer que les C_k sont constants.
   Montrer qu'il existe N (indépendant de a et b) tel que, pour tous a, b, $B(b) - B(a)$ divise (dans $\mathbb{Z}$) $N \sum_{k=0}^{m} (C_k(a) - C_k(b))B(a)^k$. D'où une inégalité sur les tailles qui, en faisant $b \to +\infty$, montre que les C_k sont constants.

Exercice 125.

1. Lagrange.
2. Il n'existe pas de telle configuration.
   En effet, pour tout $i \in [\![1, r]\!]$, en posant $a_{r+2} = a_2$, comme $a_{i+1} - a_i \mid \mathrm{P}(a_{i+1}) - \mathrm{P}(a_i)$, on a en particulier $a_{i+1} - a_i \mid a_{i+2} - a_{i+1}$.
   Donc en particulier, pour tout i, $|a_{i+1} - a_i| = |a_{i+2} - a_{i+1}|$. De plus, si $a_{i+1} - a_i = -(a_{i+2} - a_{i+1})$, alors $a_i = a_{i+2}$, ce qui contredit le caractère distinct des a_i.
   Donc, pour tout i, $a_{i+2} - a_{i+1} = a_{i+1} - a_i$.
   En notant $\delta = a_2 - a_1$ la valeur commune de ces écarts, on obtient $a_r - a_1 = (r-1)\,\delta$; mais le cas $i = r$ donne aussi $a_1 - a_r = \delta$, d'où $r\delta = 0$ puis $\delta = 0$, ce qui est absurde.

Exercice 126. On remarque que pour tout entier k, $\mathrm{P}(n+k) \equiv \mathrm{P}(k)\,[n]$.

Donc, en regroupant les termes, on a

$$\sum_{k=0}^{n^2-1} \mathrm{P}(k) = \sum_{r=0}^{n-1} \sum_{q=0}^{n-1} \mathrm{P}(qn + r)$$

qui est divisible par n.

Exercice 129. Regarder des valuations p-adiques pour de grands p.

Exercice 131.

1. Cela ressemble fortement à Tchebychev.
2. Remarquer que $\mathrm{P}_{2q}(2\cos(\pi p/q))$, et que dire des racines rationnelles d'un polynôme unitaire à coefficients entiers.
3. L'intersection $\mathbb{Z} \cap [-2, 2]$ n'est pas bien grande.

Exercice 132.

1. Par Gauss on se ramène à une factorisation dans $\mathbb{Z}[\mathrm{X}]$, puis dans $\mathbb{F}_p[\mathrm{X}]$.
2. Avec les symboles de Legendre, on a $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.
3. Pour l'irréductibilité dans $\mathbb{Q}[\mathrm{X}]$, par exemple Eisenstein.
   Pour $p = 2$ un petit Frobenius.
   Pour p premier impair, parmi -1, 2 et -2, au moins l'un est un carré dans $\mathbb{F}_p$.
   Et très formellement $\mathrm{X}^4 + 1 = (\mathrm{X}^2)^2 - \sqrt{-1}^2 = (\mathrm{X}^2 - \sqrt{2}\mathrm{X} + 1)(\mathrm{X}^2 + \sqrt{2}\mathrm{X} + 1) = (\mathrm{X}^2 - \sqrt{-2}\mathrm{X} - 1)(\mathrm{X}^2 + \sqrt{-2}\mathrm{X} - 1)$.

Exercice 133. Supposons $\mathrm{P} = \mathrm{AB}$ avec A et B dans $\mathbb{Z}[\mathrm{X}]$ non constants.

Pour tout k, $\mathrm{A}(\lambda_k)\,\mathrm{B}(\lambda_k) = -1$ donc $(\mathrm{A} + \mathrm{B})(\lambda_k) = 0$.

Conclure par degré et en comptant les racines que $\mathrm{P} = -\mathrm{A}^2$ ce qui est impossible par coefficient dominant.

Exercice 134.

1. Avec $\mathrm{P} = \mathrm{AB}$ dans $\mathbb{Z}[\mathrm{X}]$, parmi $\mathrm{A}(0)$ et $\mathrm{B}(0)$ l'un est de module 1. Par relations coefficients racines il est alors sans racine i.e constant.
   Pour passer à $\mathbb{Q}[\mathrm{X}]$, on a $c(\mathrm{P}) = 1$ ou p, et de même $\mathrm{P} = p\tilde{\mathrm{P}}$ donne un problème sur $\tilde{\mathrm{P}}(0)$ et ses racines.
2. Il suffit de montrer que toutes les racines sont de module strictement supérieur à 1, ce qui se fait en écrivant $\mathrm{P}(z) = 0$ et en appliquant l'inégalité triangulaire.
3. Calcul direct : $(\mathrm{X} - 1)\sum_{i=1}^{n} \mathrm{X}^i = \mathrm{X}^{n+1} - \mathrm{X}$, puis ajouter $p(\mathrm{X} - 1)$.
4. Montrer que si $z^{n+1} = p - (p-1)\,z$ et $|z| \leq 1$ alors $|z| = 1$ puis que $z = 1$.
   Donc toutes les racines sont de module strictement supérieur à 1.

Exercice 136. Pour la dernière question, on pourra majorer le module des racines de P dont la partie réelle est > 0.

Exercice 137.

1. Par relations coefficients racines on obtient $\lambda(P) = -\frac{a_{m-1}}{a_m} + \frac{a_1}{a_0}$.
   On somme sur les racines comptées avec multiplicité, d'où $\lambda(P_1P_2) = \lambda(P_1) + \lambda(P_2)$.
2. Le coefficient dominant et le constant sont ± 1.
3. Utiliser $z^n = z + 1$ puis calcul de complexes.
4. On a $\lambda(Q) \in \mathbb{R}$, d'où $\lambda(Q) = \sum_j \left(r_j - 1/r_j\right)\cos(\theta_j)$.
   Comme $|Q(0) = 1$, par IAG $\sum_j 1/r_j^2 \geq m$.
5. Par Gauss il suffit de montrer l'irréductibilité dans $\mathbb{Z}[X]$.
   Remarquer que $\lambda(S) = 1$ et qu'il est difficile d'écrire 1 comme somme d'entiers strictement positifs.

Exercice 138.

1. Par exemple $X^n - 2$ convient (Einsenstein en 2).
2. Cf l'exercice sur $\prod_{i=1}^{n}(X - a_i) - 1$ d avec $a_1 < \cdots < a_n$ entiers.
   Il reste à montrer qu'on peut choisir les a_i pour que P change suffisamment de fois de signe.
   Sur $]a_i, a_{i+1}[$, le produit est du signe de $(-1)^{n-i}$, et son extremum a une valeur absolue qui tend vers $+\infty$ quand les écarts $a_{i+1} - a_i$ grandissent. Prendre donc les a_i suffisamment espacés.

Exercice 139.

1. À k fixé, passer de $P^k \equiv B \pmod{X^n}$ à $(P + X^nQ)^k \equiv B \pmod{X^{2n}}$.
2. Restes chinois sur les $(X - a_i)^k$.

Exercice 140.

1. On a $X^3 - 2X^2 + 1 = (X - 1)\left(X^2 - X - 1\right)$.
2. Utiliser $|z - n| \leq \frac{1}{|z|^n}$ et bootstraper.
3. Utiliser la somme de racines : si aucune de module ≥ 1 alors le module est trop petit, si au moins deux de module ≥ 1 elles sont dans le cercle de centre n et de rayon $\frac{1}{(n-1)^n}$, donc la somme des racines est trop grande.
4. Si $P = AB$ avec $A, B \in \mathbb{Z}[X]$ non constants, alors A ou B a toutes ses racines de module < 1, ce qui pose problème pour le coefficient constant.