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

✓ : exercice d'application des méthodes, ★ : exercice classique, ☢ : exercice difficile.

Nombres premiers, critères de primalité

Exercice 1. On propose une autre démonstration de l'infinité de nombres premiers. Soient p un nombre premier et q un diviseur premier de $2^p - 1$.

1. Déterminer l'ordre de $\bar{2}$ dans $(\mathbb{Z}/q\mathbb{Z})^\times$.
2. En déduire l'existence d'une suite strictement croissante de nombres premiers.


1170-1250

Exercice 2. (Suite de Fibonacci) Soit $(F_n)_{n\geqslant 0}$ la suite de Fibonacci définie par : $F_0 = 0$, $F_1 = 1$, et : $\forall n \in \mathbb{N}$, $F_{n+2} = F_{n+1} + F_n$.

1. Montrer que F_n et F_{n+1} sont premiers entre eux pour tout $n \in \mathbb{N}$.
2. Soit $(m,n) \in \mathbb{N}^2$ tel que : $1 \leqslant m \leqslant n$. Montrer : $F_n = F_m F_{n-m+1} + F_{m-1}F_{n-m}$.
3. En déduire : $\forall (m,n) \in (\mathbb{N}\setminus\{0\})^2$, $\text{pgcd}(F_m, F_n) = F_{\text{pgcd}(m,n)}$.


1588-1648

★ **Exercice 3. (Nombres premiers de Mersenne, de Fermat)** Soient $a \geqslant 2$ et $n \geqslant 2$ deux entiers naturels.

1. Montrer que si $a^n - 1$ est un nombre premier, alors $a = 2$ et n est un nombre premier. Un tel nombre est appelé *nombre de Mersenne*. Que dire de la réciproque ?
2. Montrer que si $2^n + 1$ est un nombre premier, alors n est une puissance de 2. Un tel nombre est appelé *nombre de Fermat*.

Exercice 4. (Critère de Pépin) Soit $n \in \mathbb{N}$. On pose : $f_n = 2^{2^n} + 1$.

1. Soit p un facteur premier de f_n. Déterminer l'ordre de $\bar{2}$ dans $(\mathbb{Z}/p\mathbb{Z})^\times$, et en déduire que 2^{n+1} divise $p-1$.
2. On suppose qu'il existe $a \in \mathbb{Z}$ tel que : $a^{\frac{f_n-1}{2}} \equiv -1 \bmod f_n$. Montrer que f_n est un nombre premier.

Exercice 5. On veut montrer qu'il existe une infinité de nombres premiers congrus à 3 modulo 4.

1. Montrer que tout entier naturel congru à 3 mod 4 admet un diviseur premier congru à 3 mod 4.
2. S'inspirer de la démonstration d'Euclide de l'infinité des nombres premiers pour en déduire le résultat voulu.


1741-1793

★ **Exercice 6. (Théorème de Wilson et conséquence)** Soit p un nombre premier.

1. Justifier : $X^{p-1} - 1 = \prod_{k=1}^{p-1}(X-k)$ (dans $\mathbb{Z}/p\mathbb{Z}$).
2. En déduire : $(p-1)! \equiv -1 \bmod p$. C'est le *théorème de Wilson*.
3. Utiliser le théorème de Wilson pour démontrer que si : $p \equiv 1 \bmod 4$, alors l'équation $s^2 \equiv -1 \bmod p$ d'inconnue $s \in \mathbb{Z}$ admet une solution.
4. Montrer que réciproquement, si $n \in \mathbb{N}\setminus\{0,1\}$ vérifie : $(n-1)! \equiv -1 \bmod n$, alors n est un nombre premier.


1849-1917

★ **Exercice 7. (L'automorphisme de Frobenius pour les enfants)** Soit p un nombre premier.

1. Décomposer $X^p - X$ en facteurs irréductibles sur $\mathbb{Z}/p\mathbb{Z}$, et en déduire que dans $\mathbb{Z}/p\mathbb{Z}$, on a : $(X+\bar{1})^p = X^p + \bar{1}$.
2. En déduire que pour tout $k \in [\![1, p-1]\!]$, le nombre premier p divise $\binom{p}{k}$.

Exercice 8. (Étude d'une réciproque) Soit $n \in \mathbb{N}\setminus\{0,1\}$. On suppose que pour tout $k \in [\![1, n-1]\!]$, n divise $\binom{n}{k}$. Montrer que n est un nombre premier.

Exercice 9. Soit $n \in \mathbb{N}\setminus\{0\}$. Montrer que le nombre de diviseurs premiers de n est inférieur ou égal à $\dfrac{\ln(n)}{\ln(2)}$.

En vérité cette majoration est très grossière : le nombre de diviseurs premiers de n est plutôt de l'ordre de grandeur de $\ln(\ln(n))$. Mais c'est beaucoup plus difficile à démontrer.

Exercice 10. (Comportement asymptotique de l'indicatrice d'Euler) Soit φ l'indicatrice d'Euler. Montrer : $\forall n \in \mathbb{N}\setminus\{0,1\}$, $\dfrac{n\ln(2)}{\ln(n)+\ln(2)} \leqslant \varphi(n) \leqslant n-1$.

Avec le théorème des nombres premiers, on peut démontrer qu'il existe une constante $c > 0$ telle que pour tout n assez grand, on ait : $\varphi(n) \geqslant \dfrac{cn}{\ln(\ln(n))}$.

Relations de divisibilité, arithmétique modulaire

✓ **Exercice 11. (Inversibilité dans $\mathbb{Z}/n\mathbb{Z}$)**

1. Donner l'inverse de 148 modulo 393 et de 393 modulo 148.
2. Calculer l'inverse de 13 modulo 57.
3. Donner la liste des éléments inversibles de $(\mathbb{Z}/12\mathbb{Z})^\times$, avec leurs inverses respectifs.

✓ **Exercice 12.** Pour tout $n \in \mathbb{N} \setminus \{0\}$, montrer : $10^{10^n} \equiv 4 \bmod 7$.

✓ **Exercice 13.** Soit $\bar{a} \in (\mathbb{Z}/47\mathbb{Z})^\times \setminus \{-1,1\}$. Montrer que $\bar{a}$ ou $-\bar{a}$ engendre le groupe $(\mathbb{Z}/47\mathbb{Z})^\times$.

✓ **Exercice 14.** Soit $p \geqslant 5$ un nombre premier. Montrer que 24 divise $p^2 - 1$.

✓ **Exercice 15.** Soit $(a,b,c) \in \mathbb{Z}^3$. Montrer que $a^2 + b^2 + c^2$ n'est jamais congru à 7 modulo 8.

✓ **Exercice 16. (Critères de divisibilité)** Soit $n \in \mathbb{N}$.

1. Démontrer que n est divisible par 3 si, et seulement si la somme de ses chiffres (en écriture décimale) est divisible par 3. De même en remplaçant 3 par 9.
2. Démontrer que n est divisible par 4 si, et seulement si l'entier naturel formé par ses deux derniers chiffres (en écriture décimale) est divisible par 4.
3. Démontrer que n est divisible par 11 si, et seulement si la somme alternée de ses chiffres (en écriture décimale) est divisible par 11.

Exercice 17. Soit $(a,d,n) \in (\mathbb{N} \setminus \{0\})^3$, avec : $a \geqslant 2$. On suppose que $a^d - 1$ divise $a^n - 1$. Montrer que d divise n.

Exercice 18. (Arithmétique de la suite de Fibonacci : relations de divisibilité) Soit $(F_n)_{n\geqslant 0}$ la suite de Fibonacci définie par : $F_0 = 0$, $F_1 = 1$, et : $\forall n \in \mathbb{N}$, $F_{n+2} = F_{n+1} + F_n$. Il est clair que F_n est dans $\mathbb{N}$ pour tout $n \in \mathbb{N}$.

1. Montrer que F_n est un entier pair si et seulement si 3 divise n.
2. Montrer que 5 divise n si et seulement si 5 divise F_n.
3. Soit p un nombre premier impair. Montrer que si 5 est un carré dans $\mathbb{Z}/p\mathbb{Z}$, et si $p-1$ divise n, alors p divise F_n.

Exercice 19. (Théorème de Wilson quand n n'est pas premier) Soit $n \in \mathbb{N} \setminus \{0\}$. On suppose que n n'est pas un nombre premier. Simplifier $(n-1)!$ modulo n.

★ **Exercice 20. (Valuation p-adique de la factorielle)** Soient p un nombre premier et n un entier naturel.

1. Montrer : $v_p(n!) = \displaystyle\sum_{k=1}^{+\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$, et en déduire une majoration simple mais non triviale de $v_p(n!)$.
2. Par combien de zéros l'écriture décimale de 2023! se termine-t-elle ?

Exercice 21. Soit p un nombre premier IMPAIR. On pose : $H_p = \displaystyle\sum_{k=1}^{p-1} \frac{1}{k}$, et on met toutes les fractions au même dénominateur, de sorte que H_p soit de la forme : $H_p = \dfrac{A_p}{(p-1)!}$, avec $A_p \in \mathbb{N}$.

1. Montrer que pour tout entier $n \in \mathbb{N}$, et tout d diviseur de n *premier avec* p, on a : $\dfrac{n}{d} \equiv n\ell \bmod p$, où ℓ est l'inverse de d modulo p (la division de n par d « dans $\mathbb{Q}$ » équivaut à la division de n par d « dans $\mathbb{Z}/p\mathbb{Z}$ »).
2. Montrer que p divise A_p.

Exercice 22. Soient a et n deux entiers supérieurs ou égaux à 2. Montrer que $2n$ divise $\varphi(a^n + 1)$.

✓ **Exercice 23.** Soit n un entier. Montrer que 2730 divise $n^{13} - n$.

★ **Exercice 24. (Le chiffrement RSA)** Soient p et q deux nombres premiers distincts, $e \geqslant 1$ un entier, et $N = pq$. On suppose que e est inversible modulo $(p-1)(q-1)$. Montrer que l'application $f_e : \begin{cases} \mathbb{Z}/N\mathbb{Z} & \to & \mathbb{Z}/N\mathbb{Z} \\ x & \mapsto & x^e \end{cases}$ est bijective, et déterminer son application réciproque.

✓ **Exercice 25. (Systèmes de congruence)** Résoudre les systèmes de congruence :

$$\begin{cases} n \equiv 16 \bmod 47 \\ n \equiv 25 \bmod 31 \end{cases}, \qquad \begin{cases} 2n \equiv 10 \bmod 63 \\ 3n \equiv 9 \bmod 12 \end{cases}.$$

✓ **Exercice 26.** Montrer que l'équation $(2x-1)(3x-1) \equiv 0 \bmod n$, d'inconnue $x \in \mathbb{Z}$, admet des solutions pour tout entier naturel non nul n.

✓ **Exercice 27.** Résoudre les équations suivantes d'inconnue $x \in \mathbb{Z}$ ou d'inconnue $(x,y) \in \mathbb{Z}^2$:

(a) $x^3 \equiv 1 \bmod 19$, (b) $2x^2 - 3x - 2 \equiv 0 \bmod 7$, (c) $x^2 - x - 1 \equiv 0 \bmod 5$, (d) $x^2 \equiv x \bmod 34$,

(e) $x^2 - 2x + 2 \equiv 0 \bmod 5$, (f) $x^2 - 2x - 2 \equiv 0 \bmod 5$, (g) $x^2 \equiv x \bmod 30$, (h) $\begin{cases} 5x - y \equiv 11 \bmod 36, \\ 3x + 5y \equiv 1 \bmod 36. \end{cases}$

✓ **Exercice 28.** Soit φ l'indicatrice d'Euler.

1. Montrer que $\varphi(n)$ est un entier pair pour tout $n \in \mathbb{N} \setminus \{0,1,2\}$.
2. Résoudre les équations $\varphi(n) = 2$ et $\varphi(n) = 4$ d'inconnue $n \in \mathbb{N} \setminus \{0,1,2\}$.

Exercice 29. Soient m et n deux entiers naturels non nuls. Montrer que m et n sont premiers entre eux si et seulement si : $m^{\varphi(n)} + n^{\varphi(m)} \equiv 1 \bmod mn$.

✓ **Exercice 30.** Soient $p_1, \dots, p_r$ des nombres premiers distincts. On pose : $n = p_1 \cdots p_r$. Donner le nombre de solutions de l'équation $\bar{x}^2 = 1$ d'inconnue $\bar{x} \in \mathbb{Z}/n\mathbb{Z}$.

Exercice 31. En raisonnant par l'absurde, on veut montrer que l'équation diophantienne $y^2 = x^3 + 7$ d'inconnue $(x,y) \in \mathbb{Z}^2$ n'a pas de solution. Supposons l'existence d'une telle solution (x,y).

1. Montrer que x est impair.
2. Montrer que $y^2 + 1$ possède un facteur premier p congru à $3 \bmod 4$, et conclure en étudiant y^{p-1} de deux manières différentes.

Exercice 32.

1. Montrer que l'équation $x^2 + 23y^2 \equiv 41 \bmod n$ d'inconnue $(x,y) \in \mathbb{Z}^2$ admet une solution pour tout $n \in \mathbb{N} \setminus \{0\}$.
2. Montrer que l'équation $x^2 + 23y^2 = 41$ d'inconnue $(x,y) \in \mathbb{Z}^2$ n'admet pas de solution.

Exercice 33.

1. Donner l'ensemble des couples $(x,y) \in \mathbb{Z}^2$ tels que : $x^2 - 5y^2 = 33$.
2. Donner l'ensemble des couples $(x,y) \in \mathbb{Q}^2$ tels que : $x^2 - 5y^2 = 33$.

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

★ **Exercice 34. ($(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique)** Soit p un nombre premier. Pour tout d divisant $p-1$, soit $N(d)$ le nombre d'éléments d'ordre d dans $(\mathbb{Z}/p\mathbb{Z})^\times$.

1. Justifier : $\displaystyle\sum_{d \mid p-1} N(d) = p - 1$.
2. Montrer que s'il existe un élément $y \in (\mathbb{Z}/p\mathbb{Z})^\times$ d'ordre d, alors TOUT autre élément d'ordre d est dans $\langle y \rangle$ (vous aurez besoin de raisonner sur le nombre de racines de $X^d - 1$ dans $\mathbb{Z}/p\mathbb{Z}$).
3. En déduire que pour tout d divisant n, l'entier $N(d)$ est soit égal à 0, soit égal à $\varphi(d)$ (indicatrice d'Euler).
4. Utiliser la première question pour en déduire : $N(p-1) = \varphi(p-1) \geqslant 1$.

Une autre démonstration est fournie par l'exercice 13 du chapitre III.

Exercice 35. Soient p un nombre premier et m un entier naturel.

1. Montrer que le nombre de solutions à l'équation $\bar{x}^m = \bar{1}$, d'inconnue $\bar{x} \in (\mathbb{Z}/p\mathbb{Z})^\times$, est $\operatorname{pgcd}(m, p-1)$.
2. En déduire que l'ensemble des puissances m^{es} de $(\mathbb{Z}/p\mathbb{Z})^\times$ est de cardinal $\frac{p-1}{\operatorname{pgcd}(m,p-1)}$.

★ **Exercice 36. (Critère de Korselt)** Soient m, $n \geqslant 2$ deux entiers. Montrer que les propriétés suivantes sont équivalentes :

— pour tout entier a, l'entier n divise $a^m - a$;

— pour tout nombre premier p divisant n, l'entier p^2 ne divise pas n et $p-1$ divise $m-1$.

Exercice 37. ($(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est cyclique) L'objectif de l'exercice est de montrer que $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est cyclique pour tout nombre premier p IMPAIR.

1. Montrer que si $u \in \mathbb{Z}$ est d'ordre $p-1$ dans $(\mathbb{Z}/p\mathbb{Z})^\times$ (pourquoi existe-t-il un tel entier ?), alors l'ordre de u dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est un multiple de $p-1$.
2. En déduire qu'il existe un élément v d'ordre $p-1$ dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$.
3. Montrer que pour tout $n \in \mathbb{N}$, on a : $(1+p)^{p^n} = 1 + \lambda p^{n+1}$, où λ est un entier naturel premier avec p.
4. Conclure.

Exercice 38. ($(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est cyclique : démonstration « constructive ») Soient p un nombre premier impair et $\alpha \geqslant 2$ un entier. On veut montrer que $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est cyclique et en donner un générateur, grâce à ceux de $(\mathbb{Z}/p\mathbb{Z})^\times$.

1. Montrer que pour tout élément $\bar{x}$ de $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$, il existe un unique couple $(u \bmod p, v \bmod p^n)$ dans $(\mathbb{Z}/p\mathbb{Z})^\times \times \mathbb{Z}/p^\alpha\mathbb{Z}$ tel que : $x \equiv u(1+pv) \bmod p^\alpha$.
2. Soit $n \geqslant 2$ un entier. Montrer que pour tout x divisible par p, on a : $v_p\left(\dfrac{x^n}{n!}\right) \geqslant \dfrac{n}{2} > 0$.

Ceci permet de définir l'application suivante, par analogie avec l'exponentielle classique : $\forall \bar{x} \in p\mathbb{Z}/p^\alpha\mathbb{Z}$, $\exp_p(\bar{x}) \equiv \sum_{n=0}^{+\infty} \dfrac{x^n}{n!} \bmod p^\alpha$, où, pour calculer une fraction $\dfrac{a}{b} \bmod p^\alpha$ avec $v_p(a) \geqslant v_p(b)$, on écrit : $a = p^{v_p(a)}a'$, $b = p^{v_p(b)}b'$, et on *pose* alors : $\dfrac{a}{b} \equiv p^{v_p(a)-v_p(b)}a'b'^{-1} \bmod p^\alpha$ (*à comparer avec la première question de l'exercice 21*).

3. Montrer que la somme a un sens, et est finie : il existe $N \in \mathbb{N}$ tel que : $\forall \bar{x} \in p\mathbb{Z}/p^\alpha\mathbb{Z}$, $\exp_p(\bar{x}) \equiv \sum_{n=0}^{N} \dfrac{x^n}{n!} \bmod p^\alpha$.
4. Montrer que pour tous $(k,\ell) \in \mathbb{N}^2$ et $(\bar{x},\bar{y}) \in (p\mathbb{Z}/p^\alpha\mathbb{Z})^2$, on a : $\dfrac{x^k y^\ell}{k!\ell!} \equiv \binom{k+\ell}{k} \dfrac{x^k y^\ell}{(k+\ell)!} \bmod p^\alpha$. En déduire que $\exp_p$ est un isomorphisme de groupes entre $(p\mathbb{Z}/p^\alpha\mathbb{Z}, +)$ et $(1+p\mathbb{Z}/p^\alpha\mathbb{Z}, \times)$.
5. En déduire que si $u \bmod p$ engendre $(\mathbb{Z}/p\mathbb{Z})^\times$, alors $\bar{u}\exp_p(\bar{p})$ engendre $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$.
6. Application : calculer $\exp_3(\bar{3}) \bmod 81$, et en déduire un générateur de $(\mathbb{Z}/81\mathbb{Z})^\times$.

Exercice 39. ($(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ n'est pas cyclique si $\alpha \geqslant 3$) Soit $\alpha \in \mathbb{N} \setminus \{0,1,2\}$.

1. Montrer : $\forall k \in \mathbb{N}$, $5^{2^k} \equiv 1 + \lambda_k 2^{k+2} \bmod 2^{k+3}$ avec $\lambda_k \in \mathbb{Z}$ impair, et en déduire l'ordre de $\bar{5}$ dans $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$.
2. Montrer que l'application $(x \bmod 2, y \bmod 2^{\alpha-2}) \mapsto (-1)^x\bar{5}^y$ est bien définie et que c'est un isomorphisme de groupes de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\alpha-2}\mathbb{Z}$ dans $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$. Conclure que $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ n'est pas cyclique.
3. Montrer que $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ est cyclique pour $\alpha \in \{1,2\}$.

Exercice 40. Cet exercice utilise les résultats de l'exercice 37. Soient p un nombre premier impair, α un entier naturel non nul, et d un diviseur de $(p-1)p^{\alpha-1}$. Donner le nombre de solutions de l'équation : $\bar{x}^d = \bar{1}$, d'inconnue $\bar{x} \in \mathbb{Z}/p^\alpha\mathbb{Z}$.

Exercice 41. Cet exercice utilise les résultats de l'exercice 39. Soient α un entier naturel non nul et d un diviseur de $2^{\alpha-1}$. Donner le nombre de solutions de l'équation : $\bar{x}^d = \bar{1}$, d'inconnue $\bar{x} \in \mathbb{Z}/2^\alpha\mathbb{Z}$.

Exercice 42. (Vous savez désormais tout sur $(\mathbb{Z}/n\mathbb{Z})^\times$) Cet exercice utilise les résultats des exercices 37 et 39. Soit $n \in \mathbb{N} \setminus \{0\}$.

1. Soit $d \in \mathbb{N} \setminus \{0\}$. Donner le nombre de solutions de l'équation : $\bar{x}^d = \bar{1}$, d'inconnue $\bar{x} \in \mathbb{Z}/n\mathbb{Z}$.
2. Donner l'ordre maximal d'un élément de $(\mathbb{Z}/n\mathbb{Z})^\times$, et en déduire à quelle condition nécessaire et suffisante sur n c'est un groupe cyclique.

Anneaux principaux

Exercice 43. Soit A un anneau principal. Soit $(a,b,c) \in A^3$ tel que : $a^2 = bc$, avec a non nul (donc b et c non plus, puisqu'un anneau principal est intègre). On suppose que b et c sont premiers entre eux. Montrer qu'il existe $(b',c') \in A^2$ et $(u,v) \in (A^\times)^2$ tels que : $b = ub'^2$, $c = vc'^2$.
Le résultat de cet exercice est employé dans l'exercice 48.

Exercice 44. Soit $\mathbb{D} = \left\{ \dfrac{a}{10^n} \mid (a,n) \in \mathbb{Z} \times \mathbb{N} \right\}$ l'ensemble des nombres décimaux. Montrer que $\mathbb{D}$ est un anneau commutatif et décrire ses idéaux.

★ **Exercice 45. (L'anneau des entiers de Gauß, le corps des nombres de Gauß)** On pose : $\mathbb{Z}[i] = \{x+iy \mid (x,y) \in \mathbb{Z}^2\}$, et : $\mathbb{Q}(i) = \{x+iy \mid (x,y) \in \mathbb{Q}^2\}$.

1. Montrer que $\mathbb{Z}[i]$ est un anneau commutatif intègre et $\mathbb{Q}(i)$ un corps.
2. Montrer : $\mathbb{Q}(i) = \left\{\frac{a}{b} \mid (a,b) \in \mathbb{Z}[i] \times (\mathbb{Z}[i] \setminus \{0\})\right\}$. C'est le *corps des fractions* de $\mathbb{Z}[i]$.

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

1. Soit $(a,b) \in \mathbb{Z}[i] \times (\mathbb{Z}[i] \setminus \{0\})$. Montrer qu'il existe $(q,r) \in \mathbb{Z}[i]^2$ tel que : $a = bq + r$, avec : $|r| < |q|$.
2. En déduire que les idéaux de $\mathbb{Z}[i]$ sont de la forme $a\mathbb{Z}[i]$ avec $a \in \mathbb{Z}[i]$.
3. Soit p un élément irréductible de $\mathbb{Z}[i]$, et soit $(a,b) \in \mathbb{Z}[i]^2$. Montrer que si p divise ab, alors p divise a ou b.
4. Montrer que pour tout $n \in \mathbb{Z}[i] \setminus \{0\}$, il existe $u \in \mathbb{Z}[i]^\times$, un unique entier $k \in \mathbb{N} \setminus \{0\}$ et un unique ensemble $\{(p_1,\alpha_1),\dots,(p_k,\alpha_k)\}$ (où, pour tout $j \in [\![1,k]\!]$, $p_j \in \mathbb{Z}[i]$ est irréductible et $\alpha_j \in \mathbb{N}\setminus\{0\}$) tel que : $n = u\prod_{j=1}^{k} p_j^{\alpha_j}$.

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

1. Montrer : $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$.
2. Montrer que si un nombre premier p vérifie : $p \equiv 3 \bmod 4$, alors p est irréductible dans $\mathbb{Z}[i]$ (*raisonner par l'absurde, et considérer le module au carré*).
3. Soit $a \in \mathbb{Z}[i]$. Montrer que $\mathrm{N}(a) = |a|^2$ est un entier naturel, et que s'il est un nombre premier alors a est irréductible.
4. Factoriser 2 comme un produit d'irréductibles de $\mathbb{Z}[i]$.

Exercice 48. (Triplets pythagoriciens) Nous donnons une application de l'arithmétique de $\mathbb{Z}[i]$, pour trouver tous les triplets pythagoriciens, c'est-à-dire tous les entiers $(x,y,z) \in \mathbb{Z}^3$ tels que : $x^2+y^2=z^2$.

1. Montrer que si $(x,y,z) \in \mathbb{Z}^3 \setminus \{(0,0,0)\}$ vérifie $x^2+y^2=z^2$, et si l'on note $d = \mathrm{pgcd}(x,y,z)$, alors : $(a,b,c) = \left(\frac{x}{d},\frac{y}{d},\frac{z}{d}\right) \in (\mathbb{Z}\setminus\{0\})^3$ est aussi un triplet pythagoricien, où a, b et c sont premiers entre eux dans leur ensemble.
2. Montrer qu'au plus un des entiers parmi a, b et c est pair. Montrer ensuite qu'il y en a exactement un, et que ce ne peut pas être c.
3. Montrer que $a+ib$ et $a-ib$ sont premiers entre eux, et en déduire qu'il existe $(u,v) \in \mathbb{Z}^2$ tel que : $a+ib = (u+iv)^2$.
4. Conclure que les triplets pythagoriciens sont exactement les triplets de la forme : $\left(d\left(u^2-v^2\right), 2duv, d\left(u^2+v^2\right)\right)$, avec $(u,v) \in \mathbb{Z}^2$ et $d \in \mathbb{Z}$.

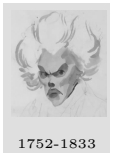
On doit la primauté de ce type d'idée à Euler – où l'on fait de l'arithmétique dans un anneau plus grand que $\mathbb{Z}$ –, qui l'eut pour démontrer le théorème de Fermat dans le cas d'un exposant égal à 3. Mais c'est plus subtil.

Exercice 49. (Exemple d'anneau non principal)

1. Montrer que $A = \left\{a+bi\sqrt{5} \mid (a,b) \in \mathbb{Z}^2\right\}$ est un anneau.
2. Montrer que $1+i\sqrt{5}$, 2 et 3 sont des éléments irréductibles de A.
3. Montrer que A n'est pas un anneau principal.

Dénombrement des carrés, symbole de Legendre et sommes de Gauß

Dans tous les exercices qui suivent, on dit que $\bar{x} \in \mathbb{Z}/p\mathbb{Z}$ est un *carré* s'il existe $\bar{y} \in \mathbb{Z}/p\mathbb{Z}$ tel que : $\bar{x} = \bar{y}^2$.



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

1. Montrer qu'il y a $\frac{p-1}{2}$ carrés dans $(\mathbb{Z}/p\mathbb{Z})^\times$, et $\frac{p+1}{2}$ carrés dans $\mathbb{Z}/p\mathbb{Z}$.
2. Montrer que si $\bar{x} \in (\mathbb{Z}/p\mathbb{Z})^\times$ est un carré, alors : $x^{\frac{p-1}{2}} \equiv 1 \bmod p$.
3. Montrer que réciproquement, si $x^{\frac{p-1}{2}} \equiv 1 \bmod p$, alors $\bar{x}$ est un carré.
4. En déduire une condition nécessaire et suffisante sur p pour que -1 soit un carré modulo p.
5. En déduire que si l'on pose, pour tout $\bar{x} \in \mathbb{Z}/p\mathbb{Z}$:

$$\left(\frac{x}{p}\right) = \begin{cases} 0 & \text{si} \quad x \equiv 0 \bmod p, \\ 1 & \text{si} \quad x \not\equiv 0 \bmod p \text{ et est un carré modulo } p, \\ -1 & \text{si} \quad x \not\equiv 0 \bmod p \text{ et n'est pas un carré modulo } p, \end{cases}$$

alors l'application $\bar{x} \mapsto \left(\frac{x}{p}\right)$ induit un morphisme de groupes de $(\mathbb{Z}/p\mathbb{Z})^\times$ dans $\{-1,1\}$. C'est le *symbole de Legendre*.

Exercice 51. Soit p un nombre premier. Montrer que le produit de deux nombres non carrés dans $(\mathbb{Z}/p\mathbb{Z})^\times$ est un carré dans $(\mathbb{Z}/p\mathbb{Z})^\times$.

Exercice 52. (Solutions de $x^2+y^2\equiv 1 \bmod p$) Soit p un nombre premier impair, et soit $\left(\frac{\cdot}{p}\right)$ le symbole de Legendre défini dans l'exercice 50. En simplifiant : $\sum_{\bar{x}\in\mathbb{Z}/p\mathbb{Z}} \left(\frac{1-x^2}{p}\right)$, montrer que l'équation $\bar{x}^2+\bar{y}^2=\bar{1}$ d'inconnue $(\bar{x},\bar{y})\in(\mathbb{Z}/p\mathbb{Z})^2$ admet $p-(-1)^{\frac{p-1}{2}}$ solutions.

La méthode employée dans cet exercice atteint vite ses limites techniques. L'étude des équations plus sophistiquées suit plutôt une autre approche, basée sur ce qu'on appelle des sommes de Gauß*, elles-mêmes basées sur une formule que je qualifie « d'orthogonalité » en d'autres endroits divers (chapitres II, VII…). Les propriétés utiles pour le calcul des sommes de Gauß sont dans l'exercice 53. Nous illustrons ensuite l'utilisation des sommes de Gauß dans le décompte des solutions dans l'exercice 54, et apprécions son efficacité dans l'exercice 55 qui le généralise.*

★ **Exercice 53. (Sommes de Gauß)** Soient p un nombre premier impair et a un entier premier avec p. Soit $\left(\frac{\cdot}{p}\right)$ le symbole de Legendre défini dans l'exercice 50.

1. Montrer que pour tout $a\in\mathbb{Z}$ premier avec p, on a : $\sum_{\bar{x}\in\mathbb{Z}/p\mathbb{Z}} \exp\left(\frac{2i\pi a x^2}{p}\right) = \left(\frac{a}{p}\right) \sum_{\bar{x}\in\mathbb{Z}/p\mathbb{Z}} \exp\left(\frac{2i\pi x^2}{p}\right)$.
2. Montrer : $\left|\sum_{\bar{x}\in\mathbb{Z}/p\mathbb{Z}} \exp\left(\frac{2i\pi a x^2}{p}\right)\right|^2 = p$.
3. Montrer : $\left(\sum_{\bar{x}\in\mathbb{Z}/p\mathbb{Z}} \exp\left(\frac{2i\pi x^2}{p}\right)\right)^2 = (-1)^{\frac{p-1}{2}} p$.

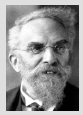
Exercice 54. (Solutions de $x^2+y^2\equiv 1 \bmod p$, avec les sommes de Gauß) Soit p un nombre premier impair. On note N le nombre de solutions de l'équation $\bar{x}^2+\bar{y}^2=\bar{1}$ d'inconnue $(\bar{x},\bar{y})\in(\mathbb{Z}/p\mathbb{Z})^2$.

1. Montrer : $N = \frac{1}{p}\sum_{a=0}^{p-1} \exp\left(-\frac{2i\pi a}{p}\right) \left(\sum_{\bar{x}\in\mathbb{Z}/p\mathbb{Z}} \exp\left(\frac{2i\pi a x^2}{p}\right)\right)^2$.
2. Conclure : $N = p-(-1)^{\frac{p-1}{2}}$.

Exercice 55. (Zéros d'une forme quadratique sur $\mathbb{Z}/p\mathbb{Z}$) Soient p un nombre premier impair et n un entier naturel non nul. Soit $(a_i)_{1\leqslant i\leqslant n}\in(\mathbb{Z}/p\mathbb{Z})^n$. On pose : $\forall \vec{x}=(x_i)_{1\leqslant i\leqslant n}\in(\mathbb{Z}/p\mathbb{Z})^n$, $q(\vec{x}) = \sum_{i=1}^n a_i x_i^2$, et : $N_q = \operatorname{card}\left(\left\{\vec{x}\in(\mathbb{Z}/p\mathbb{Z})^n \mid q(\vec{x})=\vec{0}\right\}\right)$. Soit $\left(\frac{\cdot}{p}\right)$ le symbole de Legendre défini dans l'exercice 50.

1. Justifier : $N_q = \frac{1}{p}\sum_{a=0}^{p-1} \sum_{\vec{x}\in(\mathbb{Z}/p\mathbb{Z})^n} \exp\left(\frac{2i\pi a q(\vec{x})}{p}\right)$.
2. En déduire : $N_q = p^{n-1} + \left(\frac{a_1\cdots a_n}{p}\right) \sum_{a=1}^{p-1} \left(\frac{a}{p}\right)^n \left(\sum_{\bar{y}\in\mathbb{Z}/p\mathbb{Z}} \exp\left(\frac{2i\pi y^2}{p}\right)\right)^n$.
3. En déduire que si n est un entier impair, alors : $N_q = p^{n-1}$.
4. Montrer que si n est un entier pair, alors : $N_q = p^{n-1} + \left(\frac{(-1)^{\frac{n}{2}} a_1\cdots a_n}{p}\right)(p-1)p^{\frac{n}{2}}$.

Cet exercice et les précédents donnent plusieurs exemples de décompte des solutions d'une équation modulo un nombre premier p. Et modulo un entier non nul n quelconque ? Il semble qu'il suffise d'utiliser le lemme des restes chinois… Mais que faire s'il apparaît des facteurs carrés dans la décomposition en facteurs premiers de n ? Le lemme de Hensel, dans l'exercice 56, montre que les solutions modulo p en induisent de nouvelles modulo p^k, avec plus ou moins de précision selon les hypothèses. Ainsi le plus dur est souvent fait lorsqu'on a trouvé les solutions modulo p.


1861-1941

Exercice 56. (Lemme de Hensel : relèvement des solutions modulo p^k) Soit $P \in \mathbb{Z}[X]$. On suppose qu'il existe $a \in \mathbb{Z}$, $n \in \mathbb{N}$ et $k \in \mathbb{N}$ tels que : $k < \dfrac{n}{2}$, et : $P(a) \equiv 0 \bmod p^n$, $P'(a) \equiv 0 \bmod p^k$, $P'(a) \not\equiv 0 \bmod p^{k+1}$.

1. Soit $z \in \mathbb{Z}$. Montrer qu'il existe $b \in \mathbb{Z}$ tel que : $P\left(a + p^{n-k}z\right) = P(a) + p^{n-k}zP'(a) + p^{2n-2k}b$.
2. En déduire, par un choix adéquat de z, l'existence de $a_0 \in \mathbb{Z}$ congru à a modulo p^{n-k} et tel que : $P(a_0) \equiv 0 \bmod p^{n+1}$, $P'(a) \equiv 0 \bmod p^k$, et : $P'(a_0) \not\equiv 0 \bmod p^{k+1}$.


1898-1979

☢ **Exercice 57. (Contre-exemple au principe de Hasse)** On s'intéresse à l'équation $(x^2-2)(x^2-17)(x^2-34) \equiv 0 \bmod n$ d'inconnue $x \in \mathbb{Z}$, selon les valeurs de n.

1. Montrer qu'il existe une solution à cette équation si $n \in \{2,17\}$.
2. Montrer qu'il existe une solution à cette équation si n est un nombre premier quelconque.
3. Montrer qu'il existe une solution à cette équation si n est une puissance d'un nombre premier. On traitera à part le cas d'une puissance de 2.
4. Conclure dans le cas où n est un entier naturel non nul quelconque.

Fonctions arithmétiques

Dans toute cette partie, le symbole $\displaystyle\sum_{d|n}$ signifie que la somme est indexée par tous les diviseurs d *positifs* de n.

Exercice 58. (Nombre de diviseurs, somme des diviseurs) Soit $n \in \mathbb{N} \setminus \{0,1\}$. On note $d(n)$ le nombre de diviseurs positifs de n et $\sigma(n)$ la somme des diviseurs positifs de n. Supposons que la décomposition en facteurs premiers de n s'écrive : $n = \displaystyle\prod_{i=1}^{k} p_i^{\alpha_i}$, avec p_i premier et α_i entier naturel non nul pour tout $i \in [\![1,k]\!]$.

1. Montrer : $d(n) = \displaystyle\prod_{i=1}^{k}(\alpha_i+1)$.
2. Montrer : $\sigma(n) = \displaystyle\prod_{i=1}^{k}\frac{p_i^{\alpha_i+1}-1}{p_i-1}$.

★ **Exercice 59. (Fonction de Möbius)** On note $\mu : \mathbb{N}\setminus\{0\} \to \mathbb{R}$ la fonction définie ainsi : si $n \in \mathbb{N}\setminus\{0\}$, alors $\mu(n) = 0$ si n est divisible par un carré (dans le cas contraire, on dit que n est *quadratfrei*), et $\mu(n) = (-1)^r$ si n est *quadratfrei* et admet exactement r diviseurs premiers. Soit φ l'indicatrice d'Euler. Montrer : $\forall n \in \mathbb{N}\setminus\{0\}$, $\varphi(n) = \displaystyle\sum_{d|n}\mu(d)\frac{n}{d}$.


1854-1925

Exercice 60. (Fonction de von Mangoldt) On note $\Lambda : \mathbb{N}\setminus\{0\} \to \mathbb{R}$ la fonction définie par :

$$\Lambda(n) = \begin{cases} \ln(p) & \text{si : } \exists (p,k) \in \mathbb{P}\times(\mathbb{N}\setminus\{0\}),\ n = p^k, \\ 0 & \text{sinon.} \end{cases}$$

Montrer que pour tout $n \in \mathbb{N}\setminus\{0\}$, on a : $\displaystyle\sum_{d|n}\Lambda(d) = \ln(n)$.

Exercice 61. (Formule de l'hyperbole de Dirichlet) Soient f et g deux applications de $\mathbb{N}\setminus\{0\}$ dans $\mathbb{C}$. On pose : $\forall x \in \mathbb{R}_+^*$, $F(x) = \displaystyle\sum_{1\leqslant n\leqslant x} f(n)$, et : $\forall x \in \mathbb{R}_+^*$, $G(x) = \displaystyle\sum_{1\leqslant n\leqslant x} g(n)$. Montrer :

$$\forall x \in \mathbb{R}_+^*,\ \forall y \in]1,x[,\quad \sum_{1\leqslant n\leqslant x}\ \sum_{\substack{(k,\ell)\in\mathbb{N}^2\\ k\ell=n}} f(k)g(\ell) = \sum_{1\leqslant n\leqslant y} F\left(\frac{x}{n}\right)g(n) + \sum_{1\leqslant n\leqslant \frac{x}{y}} f(n)G\left(\frac{x}{n}\right) - F\left(\frac{x}{y}\right)G(y).$$

Exercice 62. Pour tout $n \in \mathbb{N}\setminus\{0\}$, on note $\sigma(n)$ la somme des diviseurs positifs de n. Montrer : $\displaystyle\sum_{n\leqslant x}\sigma(n) \underset{x\to+\infty}{\sim} \frac{\pi^2x^2}{12}$.

On admet : $\displaystyle\sum_{n=1}^{+\infty}\frac{1}{n^2} = \frac{\pi^2}{6}$ (*voir l'exercice 16 du chapitre II pour une démonstration*).

Exercice 63. Pour tout $n \in \mathbb{N}\setminus\{0\}$, on note $d(n)$ le nombre de diviseurs positifs de n. Soit γ la constante d'Euler. Montrer : $\displaystyle\sum_{n\leqslant x} d(n) = x\ln(x) + (2\gamma-1)x + \underset{x\to+\infty}{O}\left(\sqrt{x}\right)$.

Exercice 64. (Comportement asymptotique moyen de l'indicatrice d'Euler) Soient φ l'indicatrice d'Euler et μ la fonction de Möbius définie dans l'exercice 59.

1. Montrer : $\forall n \in \mathbb{N} \setminus \{0\}$, $\varphi(n) = \sum_{d|n} d \cdot \mu\left(\frac{n}{d}\right)$.
2. En déduire : $\forall N \in \mathbb{N} \setminus \{0\}$, $\sum_{n=1}^{N} \varphi(n) = \frac{1}{2} \sum_{k=1}^{N} \mu(k) \left(\left\lfloor \frac{N}{k} \right\rfloor + \left\lfloor \frac{N}{k} \right\rfloor^2 \right)$.
3. En déduire : $\lim_{N \to +\infty} \frac{1}{N^2} \sum_{n=1}^{N} \varphi(n) = \frac{3}{\pi^2}$. On admet : $\sum_{n=1}^{+\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$ (*voir l'exercice 16 du chapitre II pour une démonstration*).

Exercices généraux sur les polynômes

★ **Exercice 65.** Soit $P \in \mathbb{Z}[X]$ un polynôme unitaire. Montrer que si $x \in \mathbb{Q}$ est racine de P, alors : $x \in \mathbb{Z}$.

Exercice 66. Soient P et Q deux polynômes non constants de $\mathbb{C}[X]$. On suppose : $P^{-1}(\{0\}) = Q^{-1}(\{0\})$, et : $P^{-1}(\{1\}) = Q^{-1}(\{1\})$. Montrer : $P = Q$.

Exercice 67. Soit $P \in \mathbb{C}[X]$ un polynôme de degré $n \in \mathbb{N} \setminus \{0\}$, tel que : $P(\llbracket 0, n \rrbracket) \subseteq \mathbb{Z}$. Montrer : $P(\mathbb{Z}) \subseteq \mathbb{Z}$. *Introduire une base convenable de $\mathbb{C}_n[X]$ dont les éléments vérifient cette propriété.*

Exercice 68.

1. Décrire les polynômes de $\mathbb{C}[X]$ vérifiant : $P(\mathbb{Q}) \subseteq \mathbb{Q}$.
2. ☢ Déterminer les polynômes de $\mathbb{C}[X]$ qui induisent une surjection de $\mathbb{Q}$ dans $\mathbb{Q}$. *On se ramènera au cas de polynômes de $\mathbb{Z}[X]$, et on considérera les images réciproques de $\frac{1}{p}$ par de tels polynômes, où p est un nombre premier.*

Exercice 69. Déterminer tous les polynômes $P \in \mathbb{C}[X]$ vérifiant : $P(X^2) = P(X)P(X+1)$.

Exercice 70. Soit $P \in \mathbb{Z}[X]$ un polynôme non constant tel que pour tout $n \in \mathbb{N}$, l'entier $P(n)$ soit un nombre premier.

1. Montrer que pour tout $n \in \mathbb{N}$, le nombre $P(n + P(n))$ est divisible par $P(n)$.
2. Montrer : $P(X + P(X)) = P(X)$, et en déduire une contradiction.

★ **Exercice 71. (Polynôme cyclotomique)** Pour tout $n \in \mathbb{N} \setminus \{0\}$, on pose : $\Phi_n = \prod_{\substack{k=1 \\ k \wedge n = 1}}^{n} \left(X - e^{\frac{2i\pi k}{n}} \right)$.

1. Montrer que pour tout $n \in \mathbb{N} \setminus \{0\}$, le polynôme Φ_n est de degré $\varphi(n)$, où φ est l'indicatrice d'Euler.
2. Montrer : $\forall n \in \mathbb{N} \setminus \{0\}$, $\prod_{d|n} \Phi_d = X^n - 1$.
3. Montrer : $\forall n \in \mathbb{N} \setminus \{0\}$, $\Phi_n \in \mathbb{Z}[X]$.
4. ☢ *Un miracle polynomial.* Soit $n \in \mathbb{N} \setminus \{0\}$. On note $\overline{\Phi}_n$ le polynôme de $\mathbb{Z}/p\mathbb{Z}[X]$ obtenu en réduisant modulo p les coefficients de Φ_n. Montrer que les racines de $\overline{\Phi}_n$ dans $\mathbb{Z}/p\mathbb{Z}$ sont exactement les éléments d'ordre n de $(\mathbb{Z}/p\mathbb{Z})^\times$. Quelle émotion ! Pourquoi parlé-je de « miracle polynomial » ?

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

★ **Exercice 72. (L'anneau $A[X]$ n'est pas principal en général)** Soit A un anneau commutatif intègre qui n'est pas un corps, et soit $a \in A \setminus A^\times$. Montrer que l'idéal $aA[X] + XA[X]$ n'est pas principal.

Exercice 73. Décrire les polynômes de $\mathbb{C}[X]$ divisibles par leur dérivée.

★ **Exercice 74.** Soient m et n deux entiers naturels non nuls. Calculer le pgcd de $X^m - 1$ et $X^n - 1$.

Exercice 75. Déterminer l'ensemble des polynômes $P \in \mathbb{R}[X]$ tels que $(X-1)^3$ divise $P-1$ et $(X+1)^3$ divise $P+1$.

Exercice 76. Soient K un corps et A un polynôme de $K[X]$ non constant. Soit $(m, n) \in (\mathbb{N} \setminus \{0\})^2$. Montrer que $A^2 + A$ divise $A^{2m} + (A+1)^n - 1$.

Exercice 77. Soient $a_1, \ldots, a_n$ des entiers distincts. Montrer que $\prod_{i=1}^{n} (X - a_i) - 1 \in \mathbb{Z}[X]$ est irréductible dans $\mathbb{Z}[X]$.

Exercice 78. Soit $P = X^4 + 1$.

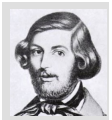
1. Décomposer P en éléments irréductibles dans $\mathbb{R}[X]$ et $\mathbb{C}[X]$.
2. Montrer que P est irréductible dans $\mathbb{Q}[X]$.
3. ☢ Montrer que pour tout nombre premier p, le polynôme P n'est pas irréductible dans $\mathbb{Z}/p\mathbb{Z}[X]$.

★ **Exercice 79.** Soit $P \in \mathbb{Q}[X]$ un polynôme irréductible. Montrer que ses racines dans $\mathbb{C}$ sont simples.

Exercice 80. Soit $P \in \mathbb{Q}[X]$. On suppose qu'il existe une racine complexe de P, notée λ, dont l'ordre de multiplicité est strictement supérieur à $\frac{\deg(P)}{2}$. Montrer : $\lambda \in \mathbb{Q}$.

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

1. Soient $P, Q \in \mathbb{Z}[X]$ et p un nombre premier. On suppose que p divise tous les coefficients de PQ. Montrer que p divise tous les coefficients de P ou tous ceux de Q.
2. Pour tout $P \in \mathbb{Z}[X]$, on appelle $c(P)$ le pgcd des coefficients de P. Montrer : $\forall (P, Q) \in \mathbb{Z}[X]^2$, $c(PQ) = c(P)c(Q)$.
3. Montrer que si $P \in \mathbb{Z}[X]$ est irréductible dans $\mathbb{Z}[X]$, il l'est dans $\mathbb{Q}[X]$.
4. Soient $n \in \mathbb{N}\setminus\{0\}$ et $P = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$. On suppose qu'il existe un nombre premier p tel que : $\forall k \in [\![0, n-1]\!]$, $p \mid a_k$, et : $p \nmid a_n$, $p^2 \nmid a_0$. Montrer que P est irréductible dans $\mathbb{Q}[X]$. C'est le critère d'Eisenstein.


1823-1852

Exercice 82. (Applications du critère d'Eisenstein)

1. Montrer que pour tout $n \in \mathbb{N} \setminus \{0\}$, il existe un polynôme de degré n irréductible dans $\mathbb{Q}[X]$.
2. Soit p un nombre premier. On pose : $\Phi_p = \sum_{k=0}^{p-1} X^k$. Montrer que Φ_p est irréductible dans $\mathbb{Q}[X]$.

★ **Exercice 83. (Un exercice ULTRA important)** Soit $z \in \mathbb{C}$. S'il existe $P \in \mathbb{Q}[X]$ non nul tel que : $P(z) = 0$, alors on dit que z est un *nombre algébrique*, et dans le cas contraire qu'il est *transcendant*. S'il est algébrique, on note $\pi_z \in \mathbb{Q}[X]$ son polynôme minimal sur $\mathbb{Q}$. On pose : $\mathbb{Q}[z] = \{P(z) \mid P \in \mathbb{Q}[X]\}$.

1. Montrer que $\mathbb{Q}[z]$ est un $\mathbb{Q}$-espace vectoriel de dimension finie si et seulement si z est un nombre algébrique, et que le cas échéant on a : $\dim(\mathbb{Q}[z]) = \deg(\pi_z)$.
2. Montrer que $\mathbb{Q}[z]$ est un corps si et seulement si z est un nombre algébrique.

★ **Exercice 84. (Théorème de la base télescopique et application)** Soient K, L et M trois corps tels que : $K \subseteq L \subseteq M$. On munit M d'une structure de L-espace vectoriel en prenant pour loi de composition externe l'application $(\ell, m) \mapsto \ell m$. De la même manière, L et M sont munis d'une structure de K-espace vectoriel.

1. Montrer : $\dim_K(M) = \dim_L(M) \cdot \dim_K(L)$.
2. Montrer que l'ensemble des nombres algébriques est un corps. *Voir l'exercice 83 pour la définition d'un nombre algébrique.*

Exercice 85. (Théorie de Galois pour bébés) Soit $\alpha \in \mathbb{C}$ un nombre algébrique sur $\mathbb{Q}$ (*voir la définition dans l'exercice 83*). On note $\pi_{\mathbb{Q}}$ son polynôme minimal et n son degré. Soit R l'ensemble des racines dans $\mathbb{C}$ de $\pi_{\mathbb{Q}}$. Soit L le plus petit sous-corps de $\mathbb{C}$ contenant R. On note $\mathrm{Aut}(L)$ l'ensemble des automorphismes de corps de L.

1. Justifier : $\mathrm{card}(R) = n$.
2. Montrer que pour tout $x \in R$ et pour tout $f \in \mathrm{Aut}(L)$, on a : $f(x) \in R$. En déduire l'existence d'un morphisme injectif de $\mathrm{Aut}(L)$ dans S_n.
3. Pour tout $z \in \mathbb{Q}[\alpha]$, il existe $P \in \mathbb{Q}[X]$ tel que : $z = P(\alpha)$, et l'on pose : $\forall x \in R$, $f_x(z) = P(x)$. Vérifier que pour tout $x \in R$, l'application f_x est correctement définie et est un morphisme de corps de $\mathbb{Q}[\alpha]$ dans $\mathbb{C}$ (l'exercice 83 assure que $\mathbb{Q}[\alpha]$ est bien un corps).
4. Montrer que les morphismes de corps de $\mathbb{Q}[\alpha]$ dans $\mathbb{C}$ sont exactement les morphismes de la question précédente. Il y en a donc n.
5. Montrer que $\mathrm{Aut}(\mathbb{Q}[\sqrt{2}])$ est isomorphe à $\mathbb{Z}/2\mathbb{Z}$.

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

Dans tous les exercices ci-dessous, p est un nombre premier.

★ **Exercice 86.** Soit K un corps fini. Montrer qu'il existe un polynôme non constant de $K[X]$ sans racine dans K.

Exercice 87. Dénombrer et expliciter :

— les polynômes irréductibles et unitaires de degrés 1, 2, 3, 4 sur $\mathbb{Z}/2\mathbb{Z}$;

— les polynômes irréductibles et unitaires de degrés 1, 2, 3 sur $\mathbb{Z}/3\mathbb{Z}$.

★ **Exercice 88.** Montrer que l'application de $\mathbb{Z}/p\mathbb{Z}[X]$ dans $(\mathbb{Z}/p\mathbb{Z})^{\mathbb{Z}/p\mathbb{Z}}$, qui à un polynôme associe son application polynomiale associée, n'est pas injective. Décrire son noyau et son image (il est clair que c'est un morphisme d'anneaux).

★ **Exercice 89.** Soit $P \in \mathbb{Z}/p\mathbb{Z}[X]$. Montrer : $(P(X))^p = P(X^p)$.

Exercice 90. Soit $P \in \mathbb{Z}/p\mathbb{Z}[X]$.

1. Montrer que $P' = 0$ si et seulement s'il existe $Q \in \mathbb{Z}/p\mathbb{Z}[X]$ tel que : $P = Q(X^p)$.
2. En déduire une condition nécessaire et suffisante pour que deux polynômes de $K[X]$ aient même dérivée.

Exercice 91.

1. Montrer que $X^4 + X + 1$ est irréductible dans $\mathbb{Z}/2\mathbb{Z}[X]$.
2. Factoriser $X^5 + X^4 + 1$ dans $\mathbb{Z}/2\mathbb{Z}[X]$.

Exercice 92. Soit $P \in \mathbb{Z}/p\mathbb{Z}[X]$. Soit K un corps contenant $\mathbb{Z}/p\mathbb{Z}$. On suppose qu'il existe $\alpha \in K$ tel que : $P(\alpha) = 0$.

1. Montrer que α est une racine double de P si et seulement si : $P'(\alpha) = 0$.
2. Soit $m \in \mathbb{N} \setminus \{0,1,2\}$. Montrer que si $(X - \alpha)^m$ divise P, alors : $\forall k \in [\![0, m-1]\!]$, $P^{(k)}(\alpha) = 0$, mais que la réciproque est fausse.

Exercice 93. Soit $P \in \mathbb{Z}/p\mathbb{Z}[X]$ un polynôme irréductible. Soit K un corps contenant $\mathbb{Z}/p\mathbb{Z}$. On veut montrer que les racines de P dans K, s'il en existe, sont simples.

1. Montrer que soit : $P' = 0$, soit : $\text{pgcd}(P, P') = 1$.
2. Montrer que si P admet des racines multiples dans K, alors il existe $Q \in \mathbb{Z}/p\mathbb{Z}[X]$ tel que $P(X) = Q(X^p)$. En déduire une contradiction.