1 Raisonnement autour du pgcd

1. *Associativité* : Soient $a, b, c \in \mathbb{N}$, montrez que :

$$\text{pgcd}\left[\text{pgcd}\left(a, b\right), c\right] = \text{pgcd}\left[a, \text{pgcd}\left(b, c\right)\right]$$

2. *Équation diophantiennes* : Résoudre à l'aide de l'identité de Bézout dans $\mathbb{Z}^2$ l'équation :

$$10x + 15y = -365$$

3. *Généralisation* : En déduire la méthode générale pour résoudre une équation du type :

$$ux + vy = a$$

où $\text{pgcd}\left(u, v\right) = 1$.

4. *Diviseur de* 3 *?* : Soient $a, b \in \mathbb{Z}$, montrez que :

$$3|\,\text{pgcd}\left(a, b\right) \Leftrightarrow 3|a^2 + b^2$$

5. pgcd *de plus de deux nombres* : Donner le pgcd de l'ensemble des coefficient binomiaux :

$$d_n := \left\{ \binom{n}{k} \text{ pour } i \in \{1, \cdots, n-1\} \right\}$$

dans le cas où :

(a) n est premier

(b) n est une *puissance* d'un nombre premier.
Indication pour cette partie :

— Tout d'abord, utiliser la formule du Binome pour montrer que d_n divise $(k+1)^n - (1 + k^n)$ pour tout $k \geq 1$, en déduire que :

$$\forall p \geq 1, d_n | p^n - p$$

— Montrer que soit $d_n = 1$, soit d_n a des facteurs premiers d'ordre au plus 1. (Pour $d_n \neq 1$, regarder d_n comme le produit d'un nombre premier et d'un nombre quelconque.)

2 Critères de cyclicité

1. *Produit de deux groupes cycliques* : Soient H et K deux groupes cycliques.
   Montrez que $H \times K$ est cyclique si et seulement si $\text{pgcd}\left[ord\left(K\right), ord\left(H\right)\right] = 1$
2. *Cyclicité d'un groupe d'ordre fini* : Soit $(G, \cdot)$ un groupe fini d'ordre m. Soit e l'élément neutre de G pour la multiplication.
   Supposons que pour tout entier d divisant m, le cardinal de l'ensemble $A_d = \left\{x \in G | x^d = e\right\}$ est au plus d.
   Montrer que le groupe G est alors cyclique.

   Indication :
   — On veut en fait montrer que $\#A_d = \varphi\left(d\right)$ ou 0. On peut tout d'abord choisir un générateur quelconque x de g et regarder $H = \langle x \rangle$ et compter le nombre d'élément d'ordre d.
   — Voir G comme $\bigsqcup_{d|m} \left\{x \in G | x^d = e\right\}$ et utiliser que $m = \sum_{d|m} \varphi\left(d\right)$ pour montrer par l'absurde que aucun A_d n'est vide.
3. En déduire que si p est premier, alors $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique.

---

3 Théorème chinois, d'Euler et le théorème de Fermat

1. *Fonction indicatrice* : Calculer la fonction indicatrice $\varphi\left(n\right)$ pour $n = 425250000$
2. *Des modulos* : Donner les deux derniers chiffres de l'écriture décimale de :
   (a) 3^{1000}
   (b) 2^{1000}
3. *Théorème de Schinzel* : Soit $k \in \mathbb{Z} \backslash \{1\}$, montrez qu'il existe une infinité d'entiers n tels que $2^{2^n} + k$ ne soit pas premier.
   Indications/Remarques :
   (a) On ne sait pas le démontrer pour $k = 1$...
   (b) On peut exprimer k à l'aide de choses, dont des puissance de 2 et d'autres choses.
   (c) On va chercher à majorer un entier a quelconque par quelque chose de la forme $2^{2^n} + k$.

---

4 Exercices de fin

1. Soit G un groupe où chaque élément est son propre inverse ($\forall a \in G, a^2 = e_G$).
   (a) Montrer que G est abélien.
   (b) Montrer que on peut munir G d'une structure de $\mathbb{Z}/2\mathbb{Z}-$espace vectoriel.
   (c) Montrer que si en plus G est d'ordre fini, alors $\text{ord}\left(G\right)$ est une puissance de 2.
   (d) En déduire que si un groupe H est d'ordre 4, alors H est isomorphe à $\mathbb{Z}/4\mathbb{Z}$ ou à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

Calcul de symbole de Legendre

Utilisez trois méthodes différentes pour calculer les symboles de Legendre suivants :

Méthode 1 **:** par le critère Euler : $\left(\frac{73}{3}\right)$

Méthode 2 **:** par le loi de réciprocité quadratique : $\left(\frac{101}{641}\right)$

Exercice 1

1. *On a vu en cours que :* $\forall n \in \mathbb{N}$, $\left(\frac{n}{2}\right) \equiv n \mod 2$
   Montrez ici que
   $$\boxed{\forall n \in \mathbb{N}, \left(\frac{n}{3}\right) \equiv n \mod 3}$$
2. Soit p un nombre premier impair, et posons n le plus *petit* entier n'étant *pas* un résidu quadratique modulo p.
   Montrez que $n < 1 + \sqrt{p}$
   Indications : On veut en fait montrer que $(n-1)^2 < p$. *On pourra poser* $m \in \mathbb{N}$ *le plus petit entier tel que* $m \cdot n > p$ *et travailler sur les conditions 'le plus petit..tel que... '*

Exercice 2 : Somme de Gauss

On rappellera la construction des sommes de Gauss :
Soit q un entier premier, impair, et A un anneau commutatif, d'élément neutre 1_A.
Soit $\alpha \in A$ tel que : $\sum_{i=0}^{q-1} \alpha^i = 0$ dans A et α^i et $\left(\frac{i}{n}\right)$ ne dépendent que de $i \mod q$.
On posera la somme de Gauss τ comme étant :

$$\boxed{\tau := \sum_{i=0}^{q-1} \left(\frac{i}{q}\right) \alpha^i}$$

On a montré en cours que :

$$\tau^2 = (-1)^{\frac{q-1}{2}} \cdot q$$

Maintenant on veut montrer que :

1. Soit p un nombre premier impair, tel que $p \neq q$, supposons que $p \cdot \alpha = 0$ dans A.
   Montrez que :
   $$\boxed{\tau^p = \left(\frac{p}{q}\right) \tau}$$
2. Montrez que :
   $$\boxed{\tau = \sum_{i=0}^{q-1} \alpha^{i^2}}$$

Exercice 3

1. Montrez qu'il existe une *infinité* de nombres premiers congru à 7 modulo 8.
   Indications :
   — *Raisonner par l'absurde en posant un ensemble* $\mathcal{P} = \{p_1, \cdots, p_n\}$ *l'ensemble des tels nombres décrits.*
   — *Poser* $N = (4p_1 \cdots p_n)^2 - 2$ *et montrer qu'il existe un diviseur de* N*, congru à* 7 *modulo* 8*.*
2. Soit $n \in \mathbb{N}$, posons $F_n = 2^{2^n} + 1$ (Nombre de Fermat).
   Montrez que pour tout $n \geq 2$ entier, les facteurs premiers de F_n sont congru à 1 modulo 2^{n+2}.
   Indications :
   — *Étudier l'ordre de* 2 *dans le groupe multiplicatif* $(\mathbb{Z}/p\mathbb{Z})^*$ *pour montrer que* $p \equiv \pm 1 \mod 8$
   — *Utiliser le théorème d'Euler pour montrer que* $\dfrac{p-1}{2} \equiv 0 \mod 2^{n+1}$
3. Soit p un nombre premier. supposons que p soit de la forme $p = 4q + 1$, où q est premier.
   Montrez que 2 est un générateur du groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^*$.
   Indications : Réfléchir aux valeurs possibles de l'ordre de 2 *et ensuite, tester les possibilités (faire des disjonctions de cas)*
4. On rappelle que $\forall n \geq 1$, le nombre de Fermat s'écrit : $F_n = 2^{2^n} + 1$.
   On va montrer que F_n est premier *si et seulement si* $3^{\frac{F_n - 1}{2}} \equiv -1 \mod F_n$ par les étapes suivantes :
   (a) Soit $k \in \mathbb{N}$, montrer que si $2^k + 1$ est premier, alors k s'écrit comme une puissance de 2.
   (b) Montrer que $g \in \mathbb{N}$ est un générateur du groupe multiplicatif $(\mathbb{Z}/F_n\mathbb{Z})^*$ *si et seulement si* $\left(\dfrac{g}{F_n}\right) = -1$
   (c) Montrer que si F_n est premier *alors* 3 est un générateur du groupe multiplicatif $(\mathbb{Z}/F_n\mathbb{Z})^*$, en déduire le premier sens de la proposition.
   (d) Montrer enfin que si $3^{\frac{F_n - 1}{2}} \equiv -1 \mod F_n$ alors F_n est premier.

1 Petits rappels sur les corps finis

On rappellera ici quelques notions sur les corps finis :

- **Corps finis :**
  Un corps fini k est un corps **commutatif** qui est fini (*i.e.* $\#k < +\infty$).
  On notera $\mathbb{F}_p$ le corps fini à p élément, il est unique **à isomorphisme près**.
  Un corps fini k a toujours pour cardinal q la puissance d'un nombre **premier** p. Ce nombre premier s'appelle la **caractéristique** du corps fini k.
- **Cas des corps finis $\mathbb{F}_p$ où p est premier :**
  Si p est un nombre premier, alors on peut montrer que $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.
- **Autres cas :**
  Pour les cas où le cardinal q du corps fini n'est pas premier, $q = p^n$ où p est un nombre premier et $n \geq 1$. On peut alors représenter ce corps fini comme un **quotient** de $\mathbb{F}_p[X]$ avec un polynôme irréductible. En effet :

  $$\text{L'anneau } \mathbb{F}_p[X]/(P) \text{ est un corps } \textit{ssi } P \text{ est un polynôme irréductible.}$$

  Si P est irréductible, le corps $\mathbb{F}_p[X]/(P)$ est de cardinal $p^{\deg P}$.
  Pour finir, $\mathbb{F}_{p^n}$ possède un sous-corps de cardinal p^d *ssi* $d|n$. Ce corps est unique, à isomorphisme près, et est formé de l'ensemble des racines de $X^{p^d} - 1$.
- **Comment caractériser un corps ? quelle propriété peut-on en tirer ?** On rappelle que :
  — Soit k un anneau, k est un corps *ssi* l'ensemble des inversible $k^\times$ est exactement l'ensemble des éléments non nuls k^* de k, *i.e* k est un corps *ssi* $k^\times = k^*$.
  — Si $(k, +, \cdot)$ est un corps commutatif, alors $(k^\times, \cdot)$ est un groupe commutatif multiplicatif. Ce sera important pour manipuler l'ordre des éléments ! en effet la notion d'ordre est propre aux **groupes**. quand on prend un élément a dans un corps k et que l'on parle de son ordre, on parle de l'ordre de a dans le groupe multiplicatif $k^\times$.
- **Factorisation des polynômes et polynômes irréductibles sur les corps finis :**
  Soit k un corps commutatif. On rappelle que $k[X] = \left\{ \sum_{i=0}^{n} a_i X^i | a_i \in k, \forall 0 \leq i \leq n, n \in \mathbb{N} \right\}$ représente l'ensemble des polynômes à coefficients dans k.
  Soit k un corps. Un polynôme $P \in k[X]$ est réductible ssi il est le produit de deux polynômes irréductibles Q et $R \in k[X]$ avec $\deg(R) \geq 1$ et $\deg(R) \geq 1$.
  On rappelle qu'un polynôme peut être réductible dans $k[x]$ **et** n'avoir aucune racine dans le corps k. *Exemple* : $\left(X^2+1\right)^2$ est réductible dans $\mathbb{R}[X]$, pourtant ses racines sont dans $\mathbb{C}\backslash\mathbb{R}$.
  En fait, un polynôme de degré 2 ou 3 sur un corps est irréductible *ssi* il n'admet aucune racine.
  Prenons l'exemple sur un corps finis k et avec $n = 4 > 3$ **pour montrer qu'un polynôme est donc irréductible sur** $k[X]$. Soit un polynôme $P \in k[X]$ de degré 4,

supposons que P n'a aucune racine dans k. S'il était réductible dans $k[X]$, alors il faudrait qu'il soit le produit de deux polynômes irréductibles de degré 2.

En effet s'il était le produit d'un polynôme irréductible de degré 1 et d'un polynôme de degré 3, tous deux dans $k[X]$, alors il aurait des racines dans k.

Pour un corps k particulier, par exemple $k = \mathbb{F}_3$,On peut alors lister la liste des polynômes irréductibles de degré 2. Les polynômes irréductibles de degré 2 dans $\mathbb{F}_3$ sont :

$$X^2 + 1, X^2 - X - 1, X^2 + X - 1$$

Ainsi, on peut vérifier que notre polynôme n'est pas le produit de deux polynômes irréductibles de degré 2.

2 Exercices de base

1. Soit p un nombre premier, montrer que pour tout $k \in \{1, \cdots, p-1\}$, p divise $\binom{p}{k}$.
2. Soit p un nombre premier, soient $a, b \in \mathbb{F}_p$, montrer que $(a+b)^p = a^p + b^p$.
3. Montrer que $\mathbb{Z}/p\mathbb{Z}$ est un corps *ssi* p est un nombre premier.
   Si p est premier, montrer que $\left|\mathbb{Z}/p\mathbb{Z}^\times\right| = \varphi(p) = p - 1$
4. Soient $a \in \mathbb{N}\backslash\{0,1\}$, et $d, n \in \mathbb{N}$, montrer que $a^d - 1 | a^n - 1$ *ssi* $d|n$

---

3 Exercice calculatoires

1. Soit $\mathbb{F}_4 = \mathbb{F}_2[X] / \left(X^2 + X + 1\right)$
   Montrer que $\forall x \in \mathbb{F}_4^\times, x^3 = 1$.
2. Soit k un corps de cardinal q. Montrer que $\forall x \in k, x^q = x$
3. Factoriser le polynôme $P = 3X^3 + 4X^2 + 2X - 4$ dans $\mathbb{F}_5[X]$ et dans $\mathbb{F}_7[X]$. Est-ce la même décomposition ? Ce polynôme a-t-il toutes ces racines dans $\mathbb{F}_7$?
4. Montrer que $X^2 + 2X + 2$ est irréductible dans $\mathbb{F}_7[X]$.

---

4 Exercice un peu plus difficile

On rappelle le critère d'Euler si k est un corps fini de cardinal $q = p^d$ où p est un nombre premier :

$$a \in k^\times \text{ est un carré } ssi\ a^{\frac{q-1}{2}} = 1 \text{ dans } k^\times$$

1. Montrer que, pour un nombre premier p :

$$P = X^2 + 1 \in \mathbb{F}_p[X] \text{ est irréducible } ssi\ p \equiv 3 \mod 4$$

---

5 Une application de la loi de réciprocité quadratique

On rappelle le théorème suivant :

Théorème 5.1 (Loi de réciprocité quadratique)**.** *Soient p et q deux entiers impairs, alors :*

1. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$
2. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$
3. $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$

1. Soit a un entier premier impair. Montrer que :
   (a) Si $a \equiv 1 \mod 4$, alors a est un résidu quadratique modulo p *ssi* $p \equiv r \mod a$ où r est un résidu quadratique modulo a
   (b) Si $a \equiv 3 \mod 4$, alors a est un résidu quadratique modulo p *ssi* $p \equiv \pm (b)^2 \mod (4a)$ où b est un entier impair premier à a.

---

6 Un test de primalité : Les suites de Lucas

6.1 Énoncé du théorème

On va tout d'abord définir **la suite de Lucas** $(V_k)_{k\in\mathbb{N}}$ associées à l'entier relatif $a \in \mathbb{Z}$:

$$\boxed{V_0 = 2, V_1 = a, V_{k+1} = aV_k - V_{k-1}, \forall k \geq 1}$$

On va vouloir montrer le critère de primalité suivant :

Théorème 6.1. *soit $n \in \mathbb{N}\setminus\{0,1\}$ tel que n est impair. Soit $b \in \mathbb{N}$ impair, et $a \in \mathbb{Z}$ et $(V_k)_{k\in\mathbb{N}}$ sa suite de Lucas associée.*
supposons que :

1. $\left(a^2-4\right)$ *est premier avec n*
2. $V_{n+1} \equiv 2 \mod n$
3. *Pour tout diviseur premier q de $n+1$, $V_{\frac{n+1}{q}} - 2$ est premier avec n.*

Alors, n est un nombre ***premier.***

6.2 Notations des exercices préliminaires

Pour ce faire, on aura tout d'abord besoin de résoudre deux premiers exercices où l'on doit définir quelques objets : Soit p un nombre **premier impair**, et $\overline{a}$ la classe de a modulo p.
On définit l'anneau polynomial $A := \mathbb{F}_p[X]/\left\langle X^2 - \overline{a}X + 1\right\rangle$. On notera que $\mathbb{F}_p$ est alors un sous-anneau de A.
Posons α la classe de X modulo $\left(X^2 - \overline{a}X + 1\right)$. On obtient alors que $\alpha \in A^\times$ et que :

$$\alpha^2 - \overline{a}\cdot\alpha + 1 = 0, \alpha + \alpha^{-1} = a$$

6.3 Exercices préliminaires

Une fois que ces notations sont posées, on peut donc prouver ces deux premiers exercices : (dans l'ordre que l'on veut, le deuxième étant le plus facile)

1. **Premier exercice :**
   Soit $\Delta := a^2 - 4$, supposons que le nombre premier impair p définit plus haut (s. 6.2) ne divise **pas** Δ.
   Montrer alors qu'on a $\Delta^{\frac{p-1}{2}} \equiv \pm 1 \mod p$, montrer que :
   (a) — Si $\Delta^{\frac{p-1}{2}} \equiv 1 \mod p$, alors $\alpha^{p-1} = 1$
   — Si $\Delta^{\frac{p-1}{2}} \equiv -1 \mod p$, alors $\alpha^{p+1} = 1$
   (b) $\forall m \in \mathbb{Z}$, on a l'équivalence suivante :

$$\boxed{\alpha^m = 1 \Leftrightarrow \alpha^m + \alpha^{-m} = 2.}$$

2. **Deuxième exercice :** Montrer la relation de récurrence suivante :

$$\boxed{\forall k \in \mathbb{N}, V_k + p\mathbb{Z} = \alpha^k + \alpha^{-k}.}$$

Indications pour le premier exercice :
— Montrer que $\Delta^{p-1} \equiv 1 \mod p$.
— Se rappeler que A est un corps de caractéristique p, cela signifie que $\forall a_1, a_2 \in A$, $(a_1 + a_2)^p = a_1^p + a_2^p$. Comme $\overline{a}$ est calculé modulo p, donc $a^p \equiv a \mod p$.
— Pour la (b) : considérer la base $(1, \alpha)$ du $\mathbb{F}_p-$espace vectoriel A et montrer que

$$\boxed{\forall x \in A, x^2 = 0 \Rightarrow x = 0.}$$

6.4 Démonstration du théorème

Maintenant que ces deux exercices sont prouvés/admis, on va vouloir démontrer le théorème (les notations de la section 6.2 ne sont pas utilisées, elles serviront à la preuve.) :

Théorème 6.2. *soit $n \in \mathbb{N}\setminus\{0,1\}$ tel que n est impair. Soit $b \in \mathbb{N}$ impair, et $a \in \mathbb{Z}$ et $(V_k)_{k\in\mathbb{N}}$ sa suite de Lucas associée.*
supposons que :

1. $\left(a^2 - 4\right)$ *est premier avec n*
2. $V_{n+1} \equiv 2 \mod n$
3. *Pour tout diviseur premier q de $n+1$, $V_{\frac{n+1}{q}} - 2$ est premier avec n.*

Alors, n est un nombre ***premier.***

On peut démontrer le théorème avec les étapes suivantes :

1. Poser p **un diviseur premier de** n, le but sera de montrer que $n = p$.
2. Utiliser les exercices précédents pour montrer que $\alpha^{n+1} = 1$ et $\alpha^{\frac{n+1}{q}} \neq 1$ pour tout diviseur q premier de $n+1$.
3. En déduire l'ordre de α dans le groupe multiplicatif $A^\times$.
4. Montrer ensuite que soit $\alpha^{p+1} = 1$, soit α^{p-1}
5. En déduire que $n+1$ divise $p \pm 1$ et conclure.

1 Un test de primalité.

1. théorème de Wilson :
   Soit $p \in \mathbb{N} \setminus \{0, 1\}$, on a l'équivalence suivante :

   $$\boxed{p \text{ est un nombre premier } \textit{ssi } p \text{ divise } (p-1)! + 1}$$

   avec l'indication suivante : montrer que $1 + (-1)^{p-1}(p-1)! \equiv 0 \mod p$ en étudiant les racines de $X^{p-1} - 1$.

---

2 Exercices sur les corps finis.

1. Inverser des éléments sur des anneaux et des corps finis :
   Soit A **l'anneau** $A = \mathbb{F}_2[X] / \langle X^3 + 1 \rangle$.
   (a) Factoriser $X^3 + 1$ dans $\mathbb{F}_2[X]$
   (b) Lister les éléments inversibles de A, leur ensemble étant noté $A^\times$. Hormis 1, ont-ils un lien l'un envers l'autre ?
   (c) On rappelle que l' on peut déterminer l'inversibilité et l'inverse d'un élément via l'identité de Bézout.
   Déterminer l'inverse de $X^2 + 1$ dans le corps $\mathbb{F}_2[X] / \langle X^4 + X + 1 \rangle$.
2. Des polynômes irréductibles dans $\mathbb{F}_2[X]$:
   (a) Montrer que $X^2 + X + 1$ est **l'unique** polynôme irréductible de degré 2 sur $\mathbb{F}_2[X]$.
   (b) Lister tous les polynômes irréductibles de $\mathbb{F}_2[X]$ de degré $1, 2, 3$.
   (c) Montrer que $X^4 + X + 1 \in \mathbb{F}_2[X]$ est irréductible.
   Soit $K = \mathbb{F}_2[X] / (P)$. Quel est le cardinal de K ? sa caractéristique ?
   (d) Soit α la classe de X modulo P.
   Montrer que α est un générateur de K^*.
   (e) Combien de générateurs possède K^* ? Écrire les coordonnées de chacun de ces générateurs dans la base $\left(1, \alpha, \alpha^2, \alpha^3\right)$ de K en tant que $\mathbb{F}_2-$espace vectoriel.
3. Construire son propre corps finis :
   Construire les corps $\mathbb{F}_4, \mathbb{F}_8, \mathbb{F}_{16}$ et $\mathbb{F}_{25}$. *Il n'y a pas de procédé général pour trouver un polynôme irréductible de degré n, donc pour construire un corps* $\mathbb{F}_{p^n}$
4. Isomorphisme entre deux corps finis :
   On sait que tout corps finis d'ordre p^n sont isomorphe.
   Donner un isomorphisme explicite entre $\mathbb{F}_2[X] / \langle X^4 + X + 1 \rangle$ et $\mathbb{F}_2 / \langle X^4 + X^3 + 1 \rangle$
5. Quelques petites factorisations :

(a) Factoriser $X^2 + X \in \mathbb{F}_2[X]$ en produit de polynômes irréductibles dans $\mathbb{F}_2[X]$.

(b) Puis $X^4 + X$ dans le même corps....

(c) Puis $X^8 + X$...

(d) Enfin, $X^{16} + X$ dans ce même corps.

---

3 Trouver des inverses dans un corps avec de l'algèbre linéaire.

Soit $K = \mathbb{Q}$ et $P = X^3 + X + 1 \in K[X]$, on note A la $\mathbb{Q}-$algèbre $K[X]/(P)$. A est de dimension 3.
On note α la classe de X modulo P. On sait que $\left(1, \alpha, \alpha^2\right)$ est une $\mathbb{Q}-$base de A.

1. Exprimer $X^5 + 1$ dans cette base.
2. On admettra que A est un corps.
   NB :en fait, on peut montrer que P est irréductible via le lemme suivant :

   Lemme 3.1. Si $\sum_{i=0}^{n-1} a_i X^i \in \mathbb{Z}[X]$ a une racine dans $\mathbb{Q}$, alors cette racine est également dans $\mathbb{Z}$ et divise a_0.

   Comme on a ici un polynôme de degré 3, il suffit de montrer qu'on a pas de racine dans $\mathbb{Q}$.
3. On veut déterminer l'inverse de $1 + \alpha$ dans la base $\left(1, \alpha, \alpha^2\right)$ avec de l'algebre linéaire :
   (a) Poser l'endomorphisme f :

$$\begin{array}{ccc} \mathbb{Q}[X]/(P) & \to & \mathbb{Q}[X]/(P) \\ a & \mapsto & a(\alpha+1) \end{array}$$

   Montrer que cet endomorphisme est bijectif.

   (b) Donner la matrice de f dans la base $\left(1, \alpha, \alpha^2\right)$.

   (c) En déduire l'inverse de $(1 + \alpha)$.

   (d) Retrouver ce résultat avec l'algorithme d'Euclide.

---

4 Fonction de Möbius et polynômes irréductibles sur $\mathbb{F}_q$.

Dans cette partie, on va chercher à dénombrer le nombre de polynômes irréductible d'un corps finis $\mathbb{F}_q[X]$. Le premier exercice portera sur la **fonction de Möbius** :

1. Fonction de Möbius :
   On définit la fonction de Möbius μ de la manière suivante :

$$\begin{array}{rccl} \mu : & \mathbb{N}^* & \to \{-1,0,1\} & \\ & n & \mapsto & \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{si } n \text{ a un facteur carré} \\ (-1)^r & \text{si } n = p_1 \cdots p_r \text{ (premiers distincts)} \end{cases} \end{array}$$

(a) Montrer que μ est multiplicative, *i.e* $\forall n, m \in \mathbb{N}^*$ tel que $m \wedge n = 1$, $\mu(mn) = \mu(m)\mu(n)$.

(b) Montrer que $\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{sinon} \end{cases}$.

(c) Montrer la FORMULE D'INVERSION DE MÖBIUS : si $g(n) = \sum_{d|n} f(d)$ alors :

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

2. APPLICATION N^{o}1 :FONCTION D'EULER ET DE MÖBIUS :
Montrer que pour $n \in \mathbb{N}^*$:

$$\frac{\varphi(n)}{n} = \sum_{d|n} \frac{\mu(d)}{d}$$

3. APPLICATION N^{o}2 :DÉNOMBRER LES POLYNÔMES IRRÉDUCTIBLES DE $\mathbb{F}_q$:
On va donc chercher à montrer le théorème suivant :

Théorème 4.1. Soit $n \in \mathbb{N}^*$.
Notons $A(n,q)$ l'ensemble des polynômes irréductibles unitaire de degré n de $\mathbb{F}_q[X]$. On note $I(n,q) = \#A(n,q)$.
On rappelle que :

$$X^{q^n} - X = \prod_{d|n} \prod_{P \in A(d,q)} P$$

Alors :

- Si μ est la fonction de Möbius, $I(n,q) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d$
- On a l'équivalent suivant :

$$I(n,q) \underset{n \to +\infty}{\sim} \frac{q^n}{n}$$

- En déduire la probabilité de choisir un polynôme unitaire irréductible lorsque l'on choisit un polynôme au hasard, de degré n, dans $\mathbb{F}_q[x]$.