Du cours aux exercices (Savoir-faire à vérifier)

Chapitre IV — Arithmétique des entiers et des polynômes

Les principaux acquis à vérifier sont :

Arithmétique des entiers.

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

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

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

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

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

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

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

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

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

Arithmétique des polynômes.

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

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

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

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

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

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

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

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

Arithmétique des entiers

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

Exemples.

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

✓ Résoudre un système de congruence.

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

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

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

Exemples. Soit p un nombre premier.

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

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

Exemples.

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

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

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

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

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

Exemples.

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

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

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

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

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

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

Arithmétique des polynômes

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

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

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

✓ Donner une relation de Bézout entre deux polynômes.

Exemples.

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

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

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

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

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

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

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

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

Arithmétique des entiers

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

Réponse.

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

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

En remontant l'algorithme, on obtient :

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

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

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

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

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

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

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

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

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

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

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

✓ Résoudre un système de congruence. □

Réponse. Soit $x \in \mathbb{Z}$.

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

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

En remontant l'algorithme, on obtient :

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Réponse.

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

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

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

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

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

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

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

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

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

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

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

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

Réponse.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Réponse.

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

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

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

donc par unicité dans le théorème chinois on a : $x^m \bmod n \equiv 1 \bmod n$. Tout élément de $(\mathbb{Z}/n\mathbb{Z})^\times$ est donc d'ordre divisant $m = \text{ppcm}(p-1, q-1)$, donc tout ordre d vérifie $d \leqslant \text{ppcm}(p-1, q-1)$.
Montrons l'inégalité inverse : soient $\bar{\omega}_p$ un élément d'ordre $p-1$ dans $(\mathbb{Z}/p\mathbb{Z})^\times$ et $\bar{\omega}_q$ un élément d'ordre $q-1$ dans $(\mathbb{Z}/q\mathbb{Z})^\times$ (de tels éléments existent parce que ces groupes sont cycliques). Grâce à l'existence des solutions à tout système de congruence modulo p et q (d'après le théorème chinois), il existe $\bar{x} \in (\mathbb{Z}/n\mathbb{Z})^\times$ tel que : $(x \bmod p, x \bmod q) = (\omega_p \bmod p, \omega_q \bmod q)$, ce qui signifie que $\bar{x}$ est d'ordre $p-1$ dans $(\mathbb{Z}/p\mathbb{Z})^\times$ et d'ordre $q-1$ dans $(\mathbb{Z}/q\mathbb{Z})^\times$. Soit d' son ordre dans $(\mathbb{Z}/n\mathbb{Z})^\times$; alors $x^{d'} \equiv 1 \bmod n$ implique $x^{d'} \equiv 1 \bmod p$ et $x^{d'} \equiv 1 \bmod q$. On en déduit que l'ordre de $\bar{x}$ dans $(\mathbb{Z}/p\mathbb{Z})^\times$ et l'ordre de $\bar{x}$ dans $(\mathbb{Z}/q\mathbb{Z})^\times$ divisent d', c'est-à-dire : $p-1$ et $q-1$ divisent d'. Ainsi d' est un multiple commun à $p-1$ et $q-1$, donc par définition du ppcm m divise d'. On en déduit : $\text{ppcm}(p-1, q-1) \leqslant d'$. L'inégalité inverse fut démontrée tantôt, donc : $d' = \text{ppcm}(p-1, q-1)$.
L'ordre maximal d'un élément de $(\mathbb{Z}/n\mathbb{Z})^\times$ est donc $\text{ppcm}(p-1, q-1)$ (puisque tout autre ordre doit le diviser donc lui être inférieur, d'après ce qui précède). Notons qu'on a aussi démontré que l'ordre de tout élément divise l'ordre maximal : c'est un cas particulier d'un résultat valable dans tout groupe commutatif fini.
Concluons : $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique si et seulement si : $\text{ppcm}(p-1, q-1) = \text{card}((\mathbb{Z}/n\mathbb{Z})^\times) = (p-1)(q-1)$, si et seulement si $p-1$ et $q-1$ sont premiers entre eux. Mais, si p et q sont des nombres premiers impairs, alors $p-1$ et $q-1$ sont tous les deux pairs, donc ils ne sont pas premiers entre eux : on en déduit que $(\mathbb{Z}/n\mathbb{Z})^\times$ n'est pas cyclique.

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

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

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

2. Soit $(x_i)_{1 \leqslant i \leqslant 15} \in \mathbb{Z}^{15}$. On suppose : $\sum_{i=1}^{15} x_i^4 = 7936$. Comme : $7936 = 8000 - 64 = 16 \cdot 500 - 16 \cdot 4$, réduire cette égalité modulo 16 donne : $\sum_{i=1}^{15} x_i^4 \equiv 0 \bmod 16$. Or les seuls puissances quatrièmes modulo 16 sont $\bar{0} = \bar{0}^4 = (\pm\bar{2})^4 = (\pm\bar{4})^4 = (\pm\bar{6})^4 = \bar{8}^4$ et $\bar{1} = (\pm\bar{1})^4 = (\pm\bar{3})^4 = (\pm\bar{5})^4 = (\pm\bar{7})^4$ (savoir que $(\mathbb{Z}/2^4\mathbb{Z})^\times$ est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ permet d'avoir ce résultat immédiatement, mais cela nécessite plus de recul et, surtout, un résultat très largement hors programme). Le seul moyen d'obtenir zéro modulo 16 en sommant quinze $\bar{0}$ ou $\bar{1}$ est d'avoir uniquement des zéros, donc : $\forall i \in [\![1,15]\!]$, $x_i^4 \equiv 0 \bmod 16$. D'après notre description des puissances ci-dessus, cela signifie que tous les x_i sont pairs. Pour tout $i \in [\![1,15]\!]$, écrivons donc : $x_i = 2k_i$, avec k_i entier. L'équation : $\sum_{i=1}^{15} x_i^4 = 7936$, devient après simplifications : $\sum_{i=1}^{15} k_i^4 = 496$. En réduisant modulo 16, on obtient encore : $\sum_{i=1}^{15} k_i^4 \equiv 0 \bmod 16$, donc par le même raisonnement on parvient à l'existence d'entiers $m_1, \ldots, m_{15}$ tels que : $\sum_{i=1}^{15} m_i^4 = 31$. À ce stade, deux façons de conclure :
   — du fait que $3^4 = 81$, aucun des m_i ne peut être strictement supérieur à 2 ; de plus, vu que : $2^4 = 16$, on voit qu'il est impossible d'avoir deux entiers m_i supérieurs ou égaux à 2 en valeur absolue ; mais s'il y en a au plus un (avec, donc, tous les autres inférieurs ou égaux à 1 en valeur absolue), alors : $\sum_{i=1}^{15} m_i^4 \leqslant 2^4 + 14 \cdot 1^4 = 30 < 31$, ce qui est impossible ;

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

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

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

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

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

4. Notons déjà que l'équation $x^2 - 3y^2 = 1$, d'inconnue $(x, y) \in \mathbb{Z}^2$, admet au moins une solution non triviale (i.e. différente de (1,0)), à savoir : $(x, y) = (2,1)$. La clé est d'observer que cette solution suffit à en engendrer d'autres par exponentiation (phénomène très fréquent pour les équations de la forme $x^2 - dy^2 = 1$).

   En effet, si $(x, y) \in \mathbb{Z}^2$, alors :

$$x^2 - 3y^2 = 1 \iff \mathrm{N}(x + \sqrt{3}y) = 1,$$

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

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

   Remarque. On peut également inclure les puissances négatives.

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

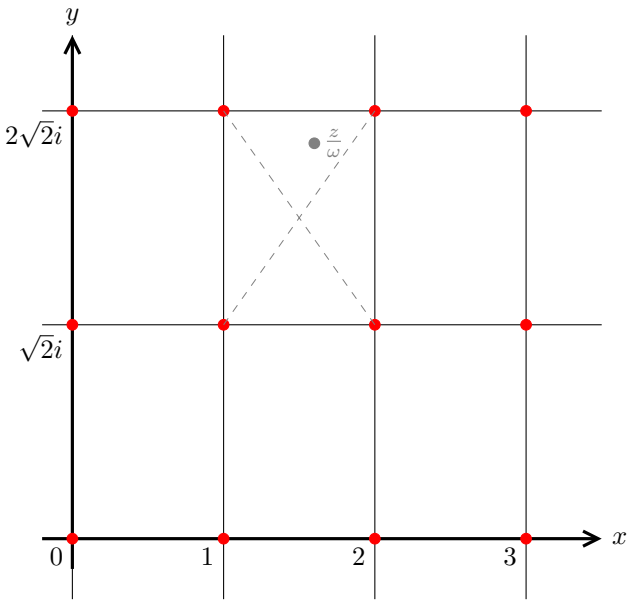
y est aussi pair. Mais c'est absurde : l'équation $y^2 = x^3 - 2$ donnerait, modulo 4, l'égalité : $0 \equiv -2 \bmod 4$. De même si y est pair. Par l'absurde, x et y sont impairs.
Pour poursuivre, on utilise l'indication de l'énoncé, qui n'est exploitable que si $\mathbb{Z}[i\sqrt{2}]$ est un anneau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

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

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

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

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



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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Réponse.

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

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

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

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

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

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

Arithmétique des polynômes

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

Réponse.

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

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

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

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

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

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

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

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

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

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

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

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

On obtient évidemment la même chose par les deux méthodes.

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

✓ Donner une relation de Bézout entre deux polynômes. □

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

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

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

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

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

Réponse.

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

(b) Le polynôme X^4+1. Tout d'abord, le fait que $x^4+1\geqslant 1$ pour tout $x\in\mathbb{R}$ assure que X^4+1 n'admet pas de racine rationnelle (ni même réelle), donc X^4+1 n'admet pas de facteur irréductible de degré 1 dans $\mathbb{Q}[X]$. Par conséquent, si c'est un polynôme réductible dans $\mathbb{Q}[X]$, il admet deux facteurs irréductibles P et Q dans $\mathbb{Q}[X]$ de degré 2. On l'a dit, X^4+1 n'admet pas de racine réelle, donc P et Q n'en ont pas non plus : étant de degré 2, cela assure qu'ils sont aussi irréductibles dans $\mathbb{R}[X]$. Or on a décomposé X^4+1 en facteurs irréductibles de $\mathbb{R}[X]$ à la page 14 ; par unicité de la décomposition, on a : $P=X^2\pm\sqrt{2}X+1\notin\mathbb{Q}[X]$: absurde. Ceci montre que X^4+1 est irréductible dans $\mathbb{Q}[X]$.

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

Réponse.

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

Polynôme minimal de $\sqrt[3]{5}$. On a : $\sqrt[3]{5}^3=5$, donc $X^3-5\in\mathbb{Q}[X]$ admet $\sqrt[3]{5}$ pour racine. Justifions qu'il est irréductible dans $\mathbb{Q}[X]$: comme il est de degré 3, il suffit pour cela de montrer qu'il n'a pas de racine rationnelle. Or une étude banale de variation montre que $x\mapsto x^3-5$ ne s'annule qu'une seule fois sur $\mathbb{R}$, et c'est en $\sqrt[3]{5}$: justifions que $\sqrt[3]{5}$ n'est pas rationnel en raisonnant par l'absurde. S'il existe deux entiers naturels non nuls p et q, premiers entre eux, tels que : $\sqrt[3]{5}=\frac{p}{q}$, alors : $5q^3=p^3$. On en déduit que 5 divise p^3, donc par le lemme d'Euclide 5 divise p. Il existe donc $k\in\mathbb{N}$ tel que : $p=5k$. En injectant ceci dans l'égalité précédente, et en simplifiant, on obtient : $q^3=5^2k^3$, donc par un argument analogue 5 divise q, et par conséquent p et q admettent un diviseur commun strictement supérieur à 1 : c'est impossible, puisque p et q sont premiers entre eux. Par l'absurde : $\sqrt[3]{5}\notin\mathbb{Q}$. L'étude qui précède permet d'en déduire que X^3-5 est irréductible dans $\mathbb{Q}[X]$, donc c'est le polynôme minimal sur $\mathbb{Q}$ de $\sqrt[3]{5}$.

Polynôme minimal de $\sqrt{2}-\sqrt{3}$. Posons :
$$\begin{aligned} P&=\left(X-\left(\sqrt{2}-\sqrt{3}\right)\right)\left(X-\left(\sqrt{2}+\sqrt{3}\right)\right)\left(X-\left(-\sqrt{2}-\sqrt{3}\right)\right)\left(X-\left(-\sqrt{2}+\sqrt{3}\right)\right)\\ &=\left(\left(X-\sqrt{2}\right)^2-(\sqrt{3})^2\right)\left(\left(X+\sqrt{2}\right)^2-(\sqrt{3})^2\right)\\ &=\left(X^2-2\sqrt{2}X-1\right)\left(X^2+2\sqrt{2}X-1\right)\\ &=\left(X^2-1\right)^2-\left(2\sqrt{2}X\right)^2\\ &=\left(X^2-1\right)^2-8X^2.\end{aligned}$$

On a : $P\in\mathbb{Q}[X]$, et P admet $\sqrt{2}-\sqrt{3}$ pour racine. Il reste à justifier qu'il est irréductible. Tout d'abord, il n'admet pas de racine rationnelle parce que $\pm\sqrt{2}\pm\sqrt{3}$ est irrationnel (c'est à démontrer : voir plus bas), donc si P est réductible, ses facteurs irréductibles (que l'on prend unitaires) doivent être de degré 2. Or, si l'on note Q et R ces facteurs, de sorte que :

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

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

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

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

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

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

Donc, en remontant l'algorithme :

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

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