Problème n° 15 : Arithmétique

Correction du problème 1 – Critères de primalité

Question préliminaire

On raisonne par l'absurde, en supposant qu'il existe des entiers naturels a et b, qu'on peut supposer premiers entre eux, tels que $\sqrt{n} = \frac{a}{b}$. On a alors $nb^2 = a^2$. On a nécessairement $b \neq 1$, sinon n serait un carré parfait. Soit alors p un facteur premier de b. L'égalité précédente permet d'affirmer que $p \mid a^2$, et d'après le lemme d'Euclide, p étant premier, $p \mid a$. Cela contredit l'hypothèse $a \wedge b = 1$ qu'on avait faite sur a et b.
Ainsi, $\boxed{\text{si } n \text{ n'est pas un carré parfait, } \sqrt{n} \text{ est irrationnel}}$.

Partie I – Anneaux $\mathbb{Z}[\xi]/(p)$

1. Soit $\mathcal{A}$ l'ensemble de tous les sous-anneaux B de $\mathbb{C}$ vérifiant $\mathbb{Z} \subset B$ et $\xi \in B$ (on peut se rendre compte qu'en fait la première condition est superflue puisque tout sous-anneau de $\mathbb{C}$ contient 1 donc tout élément de $\mathbb{Z}$). On définit
$$A = \bigcap_{B \in \mathcal{A}} B.$$
Alors A est un sous-anneau de $\mathbb{C}$, comme on le redémontre rapidement :
   - $1 \in A$ car $1 \in B$ pour tout $B \in \mathcal{A}$
   - Si $x, y \in A$, alors pour tout $B \in \mathcal{A}$, $x, y \in B$, donc $x - y \in B$ et $xy \in B$ (car ce sont des sous-anneaux de $\mathbb{C}$). Donc $x - y \in A$ et $xy \in A$.

   De plus, comme pour tout $B \in \mathcal{A}$, $\mathbb{Z} \subset B$ et $\xi \in B$, on a également $\mathbb{Z} \subset A$ et $\xi \in A$. Ainsi, A est un sous-anneau de $\mathbb{C}$ vérifiant les deux conditions requises, et si B est un autre anneau les vérifiant, $B \in \mathcal{A}$, donc $A \subset B$ par définition de A.

   Ainsi, A vérifie la propriété de minimalité requise, et $\boxed{\text{définit l'anneau } \mathbb{Z}[\xi], \text{ justifiant ainsi son existence.}}$
2. Si $\xi \in \mathbb{Z}$, $\mathbb{Z}$ est un sous-anneau contenant $\mathbb{Z}$ et ξ, donc par propriété de minimalité, $\mathbb{Z}[\xi] \subset \mathbb{Z}$. Comme $\mathbb{Z} \subset \mathbb{Z}[\xi]$ par définition, $\boxed{\mathbb{Z}[\xi] = \mathbb{Z}}$.
3. Soit $A = \{P(\xi) \mid P \in \mathbb{Z}[X]\}$.
   - Par stabilité de $\mathbb{Z}[\xi]$ par somme, différence et produit, puisque $\xi \in \mathbb{Z}[\xi]$, ses puissances successives (d'exposant positif) aussi, donc toute expression $\lambda\xi^k$, $\lambda \in \mathbb{Z}$ et $k \in \mathbb{N}$, puis par stabilité par somme, toute expression polynomiale $P(\xi)$, à coefficients entiers. Ainsi, $A \subset \mathbb{Z}[\xi]$.
   - On a clairement $\mathbb{Z} \subset A$ (étant donné $n \in \mathbb{Z}$, il suffit de considérer le polynôme constant $P = n$), ainsi que $\xi \in A$ (avec $P(X) = X$). De plus, A est un sous-anneau de $\mathbb{C}$. En effet :
     * $1 \in A$ d'après ce qu'on vient de dire,
     * si x et y sont dans A, il existe deux polynômes P et Q de $\mathbb{Z}[X]$ tels que $x = P(\xi)$ et $y = Q(\xi)$. Alors $x - y = (P - Q)(\xi)$ et $xy = PQ(\xi)$. Comme $P - Q$ et PQ sont encore de façon évidente des polynômes à coefficients entiers, on en déduit que $x - y \in A$ et $xy \in A$.

     Ainsi, par propriété de minimalité de $\mathbb{Z}[\xi]$, on a $\mathbb{Z}[\xi] \subset A$.
   - Les deux inclusions amènent l'égalité $\boxed{\mathbb{Z}[\xi] = \{P(\xi) \mid P \in \mathbb{Z}[X]\}}$.

   Considérons $\xi = \mathrm{i}$, et $x = \mathrm{i} \in \mathbb{Z}[\mathrm{i}]$. On a $x = \mathrm{i} = \mathrm{i}^5$, ce qui montre que l'écriture de x sous la forme $P(\xi)$ n'est *en général* $\boxed{\text{pas unique.}}$ Cela n'empêche pas que dans certaines situations, cette écriture est unique. Par exemple, si $\xi \in \mathbb{R}$, cette unicité caractérise les nombres transcendants.
4. La démonstration est strictement identique à celle du cours pour la relation de congruence dans $\mathbb{Z}$: soit α, β et δ dans $\mathbb{Z}[\xi]$.

- $\alpha - \alpha = p \cdot 0$, donc $\alpha \equiv \alpha\ [p]$, d'où la réflexivité ;
- si $\alpha \equiv \beta\ [p]$, il existe $\gamma \in \mathbb{Z}[\xi]$ tel que $\alpha - \beta = p\gamma$. Soit $\gamma' = -\gamma \in \mathbb{Z}[\xi]$. On a alors $\beta - \alpha = p\gamma'$, donc $\beta \equiv \alpha\ [p]$, d'où la symétrie.
- Si $\alpha \equiv \beta\ [p]$ et $\beta \equiv \delta\ [p]$, alors il existe γ et γ' dans $\mathbb{Z}[\mathrm{i}]$ tels que $\alpha - \beta = p\gamma$ et $\beta - \delta = p\gamma'$. En sommant, il vient $\alpha - \delta = p(\gamma + \gamma')$. Comme $\gamma + \gamma' \in \mathbb{Z}[\xi]$, il vient $\alpha \equiv \delta\ [p]$, d'où la transitivité.

Ainsi, la relation de congruence modulo p dans $\mathbb{Z}[\xi]$ est une relation d'équivalence.

Montrons sa compatibilité avec les deux lois de $\mathbb{Z}[\xi]$. On se donne x, y, x', y' dans $\mathbb{Z}[\xi]$ tels que $x \equiv x'\ [p]$, et $y \equiv y'\ [p]$, et β et γ dans $\mathbb{Z}[\xi]$ tels que $x - x' = p\beta$, $y - y' = p\gamma$.

- $(x + y) - (x' + y') = p(\beta + \gamma)$, donc $x + y \equiv x' + y'\ [p]$
- $xy - x'y' = xy - (x - p\beta)(y - p\gamma) = p(\beta y + \gamma x - p\beta\gamma)$, donc $xy \equiv x'y'\ [p]$.

Ainsi, la congruence est compatible avec les lois de $\mathbb{Z}[\xi]$.

5. On vient de montrer que la classe de congruence de $x + y$ ne dépend que de la classe de congruence de x et de la classe de congruence de y, et de même pour le produit. En désignant par $\overline{x}$ la classe de congruence de l'élément x, on peut donc définir sans ambiguïté la somme et le produit dans $\mathbb{Z}[\xi]/(p)$ par :

$$\boxed{c + d = \overline{x + y}} \qquad \text{et} \qquad \boxed{cd = \overline{xy}},$$

où x et y sont des représentants quelconques des classes c et d, la définition ne dépendant pas du choix de ces représentants. Cette définition se traduit par le fait que pour tous $x, y \in \mathbb{Z}[\xi]$,

$$\overline{x} + \overline{y} = \overline{x + y} \qquad \text{et} \qquad \overline{x} \cdot \overline{y} = \overline{xy}.$$

Montrons que ces lois définissent une structure d'anneau sur $\mathbb{Z}[\xi]/(p)$:

- L'associativité de l'addition découle de l'associativité dans $\mathbb{Z}[\xi]$: si b, c, d sont trois éléments de $\mathbb{Z}[\xi]/(p)$ et x, y, z des représentants de ces classes, on a, par les définitions ci-dessus :

$$b + (c + d) = \overline{x} + (\overline{y} + \overline{z}) = \overline{x} + \overline{y + z} = \overline{x + (y + z)} = \overline{(x + y) + z} = \overline{x + y} + \overline{z} = (b + c) + d.$$

- L'associativité du produit, la commutativité de l'addition (et du produit) et la distributivité se démontrent de même.
- $\overline{0}$ est clairement neutre pour l'addition et $\overline{1}$ neutre pour le produit :

$$\overline{0} + \overline{x} = \overline{0 + x} = \overline{x} \qquad \text{et} \qquad \overline{1} \cdot \overline{x} = \overline{1 \cdot x} = \overline{x}.$$

- On vérifie sans peine de $\overline{-x}$ est l'opposé de $\overline{x}$ pour tout $x \in \mathbb{Z}[\xi]$, d'où l'existence des opposés.

Ainsi, $\mathbb{Z}[\xi]/(p)$ muni de ces lois est un anneau (commutatif).

6. Soit $a, b \in \mathbb{Z}[\xi]/(p)$, et x et y des représentants dans $\mathbb{Z}[\xi]$. Comme l'anneau $\mathbb{Z}[\xi]$ est commutatif, on peut utiliser la formule du binôme :

$$(x + y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{n-k}.$$

Puisque p est premier, $\binom{p}{k}$ est divisible (dans $\mathbb{Z}$) par p pour tout $k \in [\![1, p-1]\!]$, donc pour ces k, il existe $\ell \in \mathbb{Z}$ tel que

$$\binom{p}{k} x^k y^{n-k} = p\ell x^k y^{n-k} \equiv 0\ [p],$$

puisque $\ell x^k y^{n-k} \in \mathbb{Z}[\xi]$. On en déduit que

$$(x + y)^p \equiv x^p + y^p\ [p],$$

ce qui se traduit dans $\mathbb{Z}[\xi]/(p)$ par $\boxed{(a + b)^p = a^p + b^p.}$

7. Dans $\mathbb{Z}[\mathrm{i}]/(3)$, $\mathrm{i}^3 \neq \mathrm{i}$, car dans $\mathbb{C}$

$$\frac{\mathrm{i} - \mathrm{i}^3}{3} = \frac{2}{3}\,\mathrm{i} \notin \mathbb{Z}[\mathrm{i}].$$

Donc la propriété de Fermat ne se généralise pas à $\mathbb{Z}[\xi]/(p)$.

Partie II – Adjonction d'une racine

1. Soit $A = \{a\xi + b \mid a, b \in \mathbb{Z}\}$. D'après la question I-3, $A \subset \mathbb{Z}[\xi]$, et $\mathbb{Z} \subset A$ (avec $a = 0$), ainsi que $\xi \in A$ (avec $a = 1$ et $b = 0$). Pour conclure, il suffit donc de montrer que A est un sous-anneau et d'utiliser la minimalité de $\mathbb{Z}[\xi]$. Puisque $1 \in A$, et que la stabilité par différence est évidente, il suffit de montrer que A est stable par produit. Or,
$$(a\xi + b)(a'\xi + b') = aa'\xi^2 + (ab' + a'b)\xi + bb' = (ab' + a'b)\xi + (bb' + daa'),$$
ce qui prouve la stabilité, puisque $d = \xi^2 \in \mathbb{Z}$.
Ainsi, A est un sous-anneau de $\mathbb{C}$ contenant $\mathbb{Z}$ et ξ, donc par minimalité, $\mathbb{Z}[\xi] \subset A$. Les deux inclusions amènent l'égalité $\boxed{\mathbb{Z}[\xi] = \{a\xi + b \mid a, b \in \mathbb{Z}\}}$.
2. - le cas $d = 0$ est exclus (sinon $\xi = 0 \in \mathbb{Z}$)
   - Supposons $d < 0$. Dans ce cas, $\xi \in \mathrm{i}\,\mathbb{R}^*$. On peut écrire $\xi = \mathrm{i}\,\zeta$, avec $\zeta \in \mathbb{R}^*$. Soit $x \in A$, et supposons qu'on ait deux décompositions $x = a\xi + b = a'\xi + b'$, $a, b, a', b' \in \mathbb{Z}$. Alors $a\zeta\,\mathrm{i} + b = a'\zeta\,\mathrm{i} + b'$, et par identification des parties réelles et imaginaires, on obtient donc $b = b'$ et $a\zeta = a'\zeta$. Comme $\zeta \neq 0$, $a = a'$. Cela prouve bien l'$\boxed{\text{unicité de la décomposition}}$.
   - Supposons $d > 0$. Alors $\xi \in \mathbb{R}$. Puisque $\xi \notin \mathbb{Z}$, d n'est pas un carré parfait, donc ξ est irrationnel d'après la question préliminaire. Supposons que les entiers relatifs a, a', b, b' vérifient $a\xi + b = a'\xi + b'$, à savoir $(a - a')\xi + (b - b') = 0$. Si $a - a' \neq 0$, on peut exprimer ξ comme quotient de 2 entiers, ce qui contredit son irrationnalité. Ainsi, $a = a'$, puis $b = b'$. Cela prouve l'$\boxed{\text{unicité}}$ dans ce cas également.
3. Soit $z \in \mathbb{Z}[\xi]/(p)$ tel que $z^2 = 0$. Considérons Z un représentant de z dans $\mathbb{Z}[\xi]$, et a et b deux entiers tels que $Z = a\xi + b$. On a alors $Z^2 = a^2\xi^2 + 2ab\xi + b^2 = 2ab\xi + a^2d + b^2$. L'hypothèse nous affirme que $Z^2 \equiv 0\ [p]$, donc qu'il existe des entiers c et d tels que
$$2ab\xi + a^2d + b^2 = p(c\xi + d).$$
L'unicité du développement prouvé dans la question précédente permet alors d'identifier les coefficients : $2ab = pc$ et $a^2 + db^2 = pd$. En particulier, p divise $2ab$ et $a^2 + db^2$. Comme p est différent de 2, p est premier avec 2 donc divise ab, et par le lemme d'Euclide, il divise a ou b.
   - Si $p \mid b$, alors puisque $p \mid a^2 + db^2$, on a $p \mid a^2$, et par le lemme d'Euclide, $p \mid a$.
   - Si $p \mid a$, de même, $p \mid b^2d$. Puisque p et d sont premiers entre eux, $p \mid b$.

   Ainsi, $Z = a\xi + b \equiv 0\ [p]$, donc $z = 0$ dans $\mathbb{Z}[\xi]/(p)$.
   On a bien montré : $\boxed{z^2 = 0 \Longrightarrow z = 0 \text{ dans } \mathbb{Z}[\xi]/(p)}$
4. On peut expliciter $N(x)$ pour $x = a + \xi b$:
$$N(x) = (a + \xi b)(a - \xi b) = a^2 - \xi^2 b^2 = a^2 - db^2 \in \mathbb{Z}.$$
Par ailleurs, si $y = a' + \xi b'$, on a
$$\begin{aligned} N(xy) &= N(aa' + dbb' + \xi(ab' + a'b)) = (aa' + dbb')^2 - d(ab' + a'b)^2 \\ &= a^2a'^2 + d^2b^2b'^2 - da^2b'^2 - da'^2b^2 \\ &= (a^2 - db^2)(a'^2 - db'^2) = N(x)N(y). \end{aligned}$$
Par ailleurs, on montre sans difficulté que si $x \equiv y\ [p]$, $N(x) \equiv y\ [p]$, cette dernière congruence ayant lieu dans $\mathbb{Z}$.
Si x est inversible dans $\mathbb{Z}[\xi]/(p)$, d'inverse x^{-1}, on a donc $N(1) \equiv N(x)N(x^{-1})\ [p]$. Or, $N(1) = 1$, donc $N(x)$ est inversible modulo p, c'est-à-dire (d'après le théorème de Bézout), $N(x) \wedge p = 1$.
Réciproquement si $N(x) \wedge p = 1$, alors $N(x)$ est inversible modulo p. On a alors :
$$xx^cN(x)^{-1} \equiv N(x)N(x)^{-1} \equiv 1\ [p],$$
donc x est inversible, d'inverse $x^cN(x)^{-1}$.
Ainsi, $\boxed{x \text{ est inversible dans } \mathbb{Z}[\xi]/(p) \text{ si et seulement si } N(x) \wedge p = 1}$, c'est-à-dire p ne divise pas $N(x)$ (puisque p est premier).

5. Supposons que d n'est pas un résidu quadratique modulo p. Soit $x \in \mathbb{Z}[\xi]/(p)$ non inversible. On a alors $p \mid N(x)$ d'après la question précédente. En écrivant $x = a + b\xi$, on a alors $p \mid a^2 - db^2$, c'est-à-dire

$$db^2 \equiv a^2 \ [p].$$

Si $b \not\equiv 0 \ [p]$, alors b est inversible modulo p (car $\mathbb{Z}/p\mathbb{Z}$ est un corps), et

$$d \equiv a^2 b^{-2} \equiv (ab^{-1})^2 \ [p],$$

par commutativité. cela contredit l'hypothèse faite sur d. Ainsi, $b \equiv 0 \ [p]$, puis $a^2 \equiv 0 \ [p]$, et $\mathbb{Z}/p\mathbb{Z}$ étant un corps $a \equiv 0 \ [p]$. Ainsi, $x = 0$.
Le seul élément non inversible étant $x = 0$, on en déduit que $\boxed{\mathbb{Z}[\xi]/(p) \text{ est un corps.}}$

Partie III – Conditions pour que 2 et 3 soient résidus quadratiques

1. D'après le résultat rappelé en début d'énoncé, si n est inversible modulo p (donc $n \not\equiv 0 \ [p]$), n est un carré modulo p si et seulement si $n^{\frac{p-1}{2}} \equiv 1 \ [p]$, et sinon, $n^{\frac{p-1}{2}} \equiv -1 \ [p]$. Cela correspond bien à la valeur de $(\frac{n}{p})$. Si $n \equiv 0 \ [p]$, le résultat est évident. Ainsi, pour tout $n \in \mathbb{Z}$, $\boxed{(\frac{n}{p}) \equiv n^{\frac{p-1}{2}} \ [p]}$
2. -1 est donc résidu quadratique si et seulement si $(-1)^{\frac{p-1}{2}} \equiv 1 \ [p]$. Comme $p > 2$, $1 \neq -1$, donc cette congruence est vérifiée si et seulement si $\frac{p-1}{2}$ est pair, donc $\boxed{p \equiv 1 \ [4]}$.
3. On a $2^5 = 32 \equiv -1[11]$, et $2^8 = 32 \times 8 \equiv -2 \times 8 \equiv -16 \equiv 1[17]$. Donc $\boxed{2 \text{ est un carré modulo 17, mais par modulo 11}}$. En effet, $6^2 \equiv 2[17]$.
4. De même, $3^5 = 9^2 \times 3 \equiv (-2)^3 \times 3 \equiv 12 \equiv 1 \ [11]$ et $3^8 = 27^2 \times 9 \equiv 10^2 \times 9 \equiv 100 \times 9 \equiv -2 \times 9 \equiv -18 \equiv -1 \ [18]$. Ainsi, $\boxed{3 \text{ est un carré modulo 11 (en effet, } 5^2 \equiv 3 \ [11]\text{), mais pas modulo 17}}$.
5. Soit n et n' non divisibles par p.
   (i) si n et n' sont des résidus quadratiques, il existe a et b tels que $n \equiv a^2 \ [p]$ et $n' \equiv b^2 \ [p]$, donc $nn' \equiv (ab)^2/[p]$. Donc $\boxed{nn' \text{ est un résidu quadratique}}$.
   (ii) si n est un résidu quadratique et n' un non-résidu, et $N = nn'$. Alors, n étant inversible modulo p (car non divisibles par p), en notant m son inverse modulo p, m est un résidu quadratique aussi, et $n' \equiv mN \ [p]$. Alors $\boxed{N \text{ ne peut pas être un résidu quadratique}}$, sinon d'après (i), n' le serait aussi.
   (iii) Fixons n' un non-résidu quadratique. L'application $\varphi : n \mapsto nn'$ induit une bijection de $\mathbb{F}_p^*$ dans $\mathbb{F}_p^*$. Pour tout n résidu quadratique, $\varphi(n)$ est un non-résidu quadratique d'après (ii). Or, d'après le point admis en début de sujet, il y a autant de résidus quadratiques que de non-résidus, à savoir $\frac{n-1}{2}$. Ainsi, les images par φ des $\frac{n-1}{2}$ résidus quadratiques fournissent les $\frac{n-1}{2}$ non-résidus quadratiques. Par injectivité, les images des autres éléments sont tous des résidus quadratiques. Ainsi, pour tout n non-résidu quadratique, $\varphi(n)$ est un résidu quadratique, donc $\boxed{nn' \text{ est un résidu quadratique}}$.
6. Si n ou n' est divisible par p, alors nn' est divisible par p, et par définition du symbole de Legendre,

$$(\tfrac{nn'}{p}) = 0 = (\tfrac{n}{p})(\tfrac{n'}{p}).$$

Sinon, la règle démontrée dans la question précédente sur les produits de résidus et non-résidus quadratique suit la règle des signes, donc la définition du symbole de Legendre amène directement

$$\boxed{(\tfrac{nn'}{p}) = (\tfrac{n}{p})(\tfrac{n'}{p}).}$$

7. Soit $j = \mathrm{e}^{\frac{2\,\mathrm{i}\,\pi}{3}}$.
   (a) On a $j^3 = 1$ donc $jj^2 = 1$. Or, $j^2 \in \mathbb{Z}[j]$. Ainsi, en réduisant modulo p, et en notant de la même façon les classes d'équivalence dans $\mathbb{Z}[j]/(p)$ conformément à l'énoncé, $\boxed{j \text{ est inversible}}$ dans $\mathbb{Z}[j]/(p)$ d'inverse j^2.

(b) On a, d'après la formule du binôme (utilisable, puisque l'anneau est commutatif) :

$$b^2 = (j - j^{-1})^2 = j^2 - 2 + j^{-2}.$$

Or, $j^{-2} = j$, et $j + j^2 = -1$. Par conséquent $\boxed{b^2 = -3}$.

Attention à ne pas affirmer trop vite que -3 est un résidu quadratique, car pour cela, il faut le voir (modulo p) comme carré d'un élément de $\mathbb{Z}$, ce qui n'est pas le cas de b.

En revanche, on sait que, puisque $p > 3$ (donc p ne divise pas -3) -3 est un résidu quadratique si et seulement si $(-3)^{\frac{p-1}{2}} \equiv 1\ [p]$, donc si (dans $\mathbb{Z}[j]/(p)$) $(b^2)^{\frac{p-1}{2}} = 1$, ou encore $b^{p-1} = 1$, ce qui équivaut à $b^p = b$, à condition que b soit inversible, ce qui provient du fait que $b^2 = -3$ est inversible dans $\mathbb{Z}/p\mathbb{Z}$ (si $p \neq 3$, donc dans $\mathbb{Z}[j]/(p)$. En effet, en notant c un inverse de b^2, la relation $b^2c = 1$ montre que bc est un inverse de b.

Ainsi, -3 est un résidu quadratique si et seulement si $\boxed{b^p = b}$ dans $\mathbb{Z}[j]/(p)$.

(c) D'après I-6, on a $b^p = (j - j^{-1})^p = j^p + (-j^{-1})^p$ et comme p est impair, $\boxed{b^p = j^p - j^{-p}}$.

Ainsi, -3 est résidu quadratique si et seulement si $j^p - j^{-p} = j - j^{-1}$. Or, $j^p - j^{-p}$ est égal respectivement à 0, $j - j^{-1}$ et $j^2 - j^{-2} = j^{-1} - j$ suivant que p est congru à 0, 1 ou 2 modulo 3. Ainsi, -3 est un résidu quadratique si et seulement si $\boxed{p \equiv 1\ [3]}$.

(d) D'après la question 5, $(\frac{3}{p}) = (\frac{-3}{p})(\frac{-1}{p})$, donc 3 est résidu quadratique si et seulement si l'un des deux cas suivant se produit :

- 3 et -1 sont tous deux résidus quadratiques, ce qui équivaut à $p \equiv 1\ [3]$ et $p \equiv 1\ [4]$, donc $p \equiv 1\ [12]$;
- 3 et -1 sont tous deux non-résidus quadratiques, ce qui équivaut à $p \equiv -1\ [3]$ et $p \equiv -1\ [4]$, dont $p \equiv -1\ [12]$.

On remarquera que le cas $p \equiv 0\ [3]$ n'est pas possible, p étant supposé strictement supérieur à 3.

On en déduit que 3 est un résidu quadratique modulo p si et seulement si $\boxed{p \equiv \pm 1\ [12]}$, pour $p > 3$. Le résultat ne tient pas pour $p = 3$.

8. On fait de même, en calculant $b^2 = \omega^2 + \omega^{-2} + 2 = \mathrm{i} - \mathrm{i} + 2 = 2$.

Le même raisonnement que ci-dessus montre alors que 2 est résidu quadratique si et seulement $b^p = b$. Or, $b^p = \omega^p + \omega^{-p}$. Puisque ω est une racine 8-ième de l'unité, on a 4 cas à étudier (car p étant impair, on ne peut pas avoir $p \equiv 0, 2, 4, 6\ [8]$) :

- si $p \equiv 1[8]$, $b^p = \omega + \omega^{-1} = b$
- si $p \equiv 3[8]$, $b^p = \omega^3 + \omega^{-3} = -\omega^{-1} - \omega = -b$
- si $p \equiv 5[8]$, $b^p = \omega^5 + \omega^{-5} = \omega^{-3} + \omega^3 = -b$
- si $p \equiv 7[8]$, $b^p = \omega^7 + \omega^{-7} = \omega^{-1} + \omega = b$.

Ainsi, 2 est un résidu quadratique modulo p si et seulement si $\boxed{p \equiv \pm 1\ [8]}$.

Partie IV – Critère de primalité de Lehmer et critère de Pépin

Soit $n > 1$ un entier impair

1. Soit $a \in \mathbb{Z}/n\mathbb{Z}$ un élément inversible.
   - Si l'ordre de a est $n-1$, alors $a^{n-1} = \equiv 1\ [n]$, et pour tout diviseur premier q de $n-1$, $\frac{n-1}{q}$ n'est pas divisible par l'ordre de a, donc $\boxed{a^{\frac{n-1}{q}} \not\equiv 1\ [n]}$.
   - Si $a^{n-1} \equiv 1\ [n]$ et si pour tout diviseur premier q de $n-1$, $\frac{n-1}{q}$ n'est pas divisible par l'ordre de a, alors la première égalité implique que l'ordre de a est un diviseur d de $n-1$. S'il s'agit d'un diviseur strict, $\frac{n-1}{d}$ admet un facteur premier q dans sa décomposition, et l'ordre d de a divise $\frac{n-1}{q}$, donc $a^{\frac{n-1}{q}} = 1$, d'où une contradiction. Donc l'ordre de a est $n-1$.

   On a bien démontré l'$\boxed{\text{équivalence}}$.
2. D'après la question précédente, il suffit de montrer que n est premier s'il existe un élément a dont l'ordre est $n-1$ (ce qui implique son inversibilité). Or, le résultat rappelé en début d'énoncé montre que si n est premier, $\mathbb{Z}/n\mathbb{Z}$ étant alors un corps, il existe un élément a engendrant $(\mathbb{Z}/n\mathbb{Z})^*$, donc l'$\boxed{\text{ordre sera } n-1}$.

   Réciproquement, si un tel a existe, il est inversible, ainsi que chacune de ses puissances. Comme a est d'ordre $n-1$, cela fournit $n-1$ éléments inversibles, donc tous à part 0. Ainsi, $\mathbb{Z}/n\mathbb{Z}$ est un corps, donc $\boxed{n \text{ est premier}}$.

3. • Si F_n est premier, $\mathbb{F}_n^*$ admettant autant de carré que de non carré, il existe a non carré, donc tel que $\boxed{a^{\frac{F_n-1}{2}} \equiv -1\ [F_n]}$.
   • Réciproquement, s'il existe a tel que $a^{\frac{F_n-1}{2}} \equiv -1\ [F_n]$, alors, en élevant au carré, $a^{F_n-1} \equiv 1\ [F_n]$. Comme 2 est le seul diviseur de F_n et comme $F_n \neq 2$ (donc $-1 \neq 1$), les hypothèses du critère de Lehmer sont satisfaites, donc $\boxed{F_n \text{ est premier}}$.

4. Le sens réciproque résulte de la question précédente. Supposons que F_n est premier. Le raisonnement fait dans la question précédente suggère qu'il suffit de montrer que 3 n'est pas un carré modulo F_n. Cela incite, d'après la partie III, à étudier la classe de congruence modulo 12 de F_n.

   Or, pour tout $n \geqslant 1$, $F_n \equiv 1[4]$, et puisque $F_n = 4^{2^{n-1}} + 1 \equiv 2[3]$. Ainsi, F_n est congru à $1, 5$ 9 modulo 12, ainsi qu'à 2, 5, 8 ou 11. Donc $F_n \equiv 5\ [12]$. On en déduit bien que 3 n'est pas un carré modulo F_n, se qui se traduit bien par $3^{\frac{F_n-1}{2}} \equiv -1\ [F_n]$, soit $3^{2^{2^n-1}} \equiv -1\ [F_n]$

Partie V – Suites de Lucas

1. Les égalités $V_0 = 2$ et $V_1 = a$ sont immédiates. Soit $n \geqslant 1$. On a :

$$\begin{aligned} aV_n - V_{n-1} &= (x + x^{-1})(x^n + x^{-n}) - x^{n-1} - x^{-n+1} \\ &= x^{n+1} + x^{-n+1} + x^{n-1} + x^{-n-1} - x^{n-1} - x^{-n+1} \\ &= x^{n+1} + x^{-n-1} = V_{n+1}. \end{aligned}$$

   Ainsi, pour tout $n \geqslant 1$, $\boxed{V_{n+1} = aV_n - V_{n-1}}$. Cette relation est une relation de récurrence linéaire d'ordre 2, donc l'initialisation sur les deux termes V_0 et V_1 suffit à déterminer de façon unique la suite $(V_n)_{n\in\mathbb{N}}$, qu'on complète sur $\mathbb{Z}$ par la relation évidente $V_{-n} = V_n$.

2. Par invariance du second membre par le changement d'indice $m' = -m$, et par la relation $V_m = V_{-m}$, on peut se contenter d'étudier le cas où $m \in \mathbb{N}$. De plus, si la relation est établie pour $n \geqslant 0$, alors soit $n' \leqslant 0$ et $n = -n'$. On a :

$$V_{n'+m} + V_{n'-m} = V_{-n+m} + V_{-n-m} = V_{n-m} + V_{n+m} = V_nV_m = V_{-n}V_m = V_{n'}V_n.$$

   La relation est donc alors aussi établie pour $n' \leqslant 0$. On se contente donc du cas $(n, m) \in \mathbb{N}^2$.

   Pour cela on fixe n et on montre la relation par récurrence d'ordre 2 sur $m \in \mathbb{N}$. L'initialisation pour $m = 0$ est évidente, ainsi que pour $m = 1$ (on retrouve la relation de récurrence trouvée dans la question 1). Soit $m \in \mathbb{N}$ tel que les relations $V_nV_m = V_{n+m} + V_{n-m}$ et $V_nV_{m+1} = V_{n+m+1} + V_{n-m-1}$ soient établies. On a alors

$$\begin{aligned} V_nV_{m+2} &= V_n(aV_{m+1} - V_m) = aV_nV_{m+1} - V_nV_m \\ &= a(V_{n+m+1} + V_{n-m-1}) - (V_{n+m} + V_{n-m}) \\ &= aV_{n+m+1} - V_{n+m} + aV_{n-m-1} + V_{n-m} \\ &= V_{n+m+2} + aV_{m-n+1} + V_{m-n} = V_{n+m+2} + V_{m-n+2} = V_{n+m+2} + V_{n-m-2}. \end{aligned}$$

   Ainsi, d'après le principe de récurrence, pour tout $m \in \mathbb{N}$, $\boxed{V_nV_m = V_{n+m} + V_{n-m}}$.

   Remarquez qu'on a utilisé la relation $V_{-k} = V_k$, ainsi que la relation de récurrence pour des indices éventuellement négatifs, ce qui n'est pas gênant : la preuve de cette relation de récurrence faite dans la question 1 n'utilise pas de façon cruciale la positivité de n et reste valide en cas de négativité.

3. En particulier, pour $m = n$, on obtient : $\boxed{V_{2n} = V_n^2 - 2}$.

Partie VI – Critère de primalité de Lucas-Lehmer

1. (a) L'équation du second degré $x^2 - ax + 1 = 0$ admet Δ comme discriminant. Or Δ admet une racine ξ dans $\mathbb{Z}[\xi]/(p)$. Comme 2 est inversible modulo p, la mise sous forme canonique et la factorisation qui suit est valide et l'équation est équivalente à

$$(x - (-a - \xi) \cdot 2^{-1})(x - (-a + \xi) \cdot 2^{-1}) = 0.$$

N'ayant pas établi la régularité de l'anneau $\mathbb{Z}[\xi]/(p)$, on ne peut pas conclure que $(-a-\xi)\cdot 2^{-1}$ et $(-a+\xi)\cdot 2^{-1})$ sont les deux seules racines, mais ce sont des racines, ce qui prouve l'existence d'au moins une (et même 2 si $\Delta \neq 0$, mais éventuellement plus) solution de l'équation $\boxed{x^2 - ax + 1 = 0}$.

(b) On a alors $x(x - a) = -1$, donc x est inversible, d'inverse $\boxed{x^{-1} = a - x}$.

(c) Remarquons dans un premier temps que

$$(2x - a)^2 = 4x^2 - 4ax + a^2 = 4(ax - 1) - 4ax + a^2 = a^2 - 4 \qquad \text{soit:} \qquad \boxed{(2x - a)^2 = \Delta}.$$

Ainsi, si $\Delta^{\frac{p-1}{2}} = 1$ (égalité vue dans $\mathbb{Z}[\xi]/(p)$, alors

$$((2x - a)^2)^{\frac{p-1}{2}} = 1, \qquad \text{donc:} \qquad (2x - a)^p = (2x - a).$$

Or, d'après I-6, et l'imparité de p,

$$(2x - a)^p = 2^p x^p - a^p = 2x^p - a.$$

On a donc $2x^p - a = 2x - a$. Comme 2 est inversible modulo p, on en déduit que $x^p = x$, puis, par inversibilité de x, $\boxed{x^{p-1} = 1}$

(d) De même, si $\Delta^{\frac{p-1}{2}} \equiv -1[p]$, on obtient cette fois

$$(2x - a)^p = -(2x - a), \qquad \text{donc:} \qquad 2x^p - a = -2x + a, \qquad \text{donc:} \qquad 2x^{p+1} = 2ax - 2x^2.$$

La relation définissant x donne alors $2x^{p+1} = 2$, et par inversibilité de 2, $\boxed{x^{p+1} = 1}$.

(e) Soit $m \in \mathbb{Z}$. De façon évidente, si $x^m = 1$, alors $x^m + x^{-m} = 2$.

Réciproquement, si $x^m + x^{-m} = 2$, alors $x^{2m} - 2x^m + 1 = 0$, donc $(x^m - 1)^2 = 0$. D'après la question II-3, puisque Δ est supposé premier avec p, on en déduit que $x^m - 1 = 0$, donc $\boxed{x^m = 1}$.

2. (a) La relation $V_{N+1} = 2$ (dans $\mathbb{Z}[\xi]/(p)$) équivaut à $x^{N+1} + x^{-(N+1)} = 2$. Comme $\Delta = a^2 - 4$ et N sont premiers entre eux, il en est de même de Δ et p (p divisant N). On déduit alors de la question précédente que $\boxed{x^{N+1} = 1}$. Ainsi, l'ordre de x divise $N + 1$. Mais par ailleurs, si cet ordre était strictement plus petit que $N + 1$, il existerait (comme dans la partie IV) un diviseur premier q de $N + 1$ tel que $x^{\frac{N+1}{q}} = 1$, donc $V_{\frac{N+1}{q}} = 2$ dans $\mathbb{Z}[\xi]/(p)$. Ainsi, $V_{\frac{N+1}{q}} - 2$ et p ne sont pas premiers entre eux, donc $V_{\frac{N+1}{q}} - 2$ et N non plus, ce qui contredit les hypothèses.

On en déduit que $\boxed{\text{l'ordre de } x \text{ est exactement } N + 1}$.

(b) On sait par ailleurs que $x^{p-1} = 1$, ou $x^{p+1} = 1$, d'après la question 1 ($\Delta^{\frac{p-1}{2}}$ ne pouvant prendre que les valeurs 1 et -1, d'après le résultat rappelé en début de sujet). Ainsi, $N + 1$ divise $p - 1$ ou $p + 1$. Comme $p \leqslant N$ (c'en est un diviseur), on a nécessairement $N + 1 = p + 1$, donc $N = p$.

Ainsi, le seul diviseur premier de N est N lui même, ce qui signifie bien que $\boxed{N \text{ est premier}}$.

3. (a) En reprenant les notations de la partie V, on remarque que $L_1 = V_1$, $L_2 = V_1^2 - 2 = L_2$, et plus généralement, en itérant la relation V-3, pour tout $n \in \mathbb{N}$, $L_n = V_{2^{n-1}}$.

Ainsi, $L_{s-1} \equiv 0\ [M_s]$ équivaut à $V_{2^{s-2}} \equiv 0\ [M_s]$. On a alors

$$V_{2^{s-1}} = L_s = L_{s-1}^2 - 2 = -2 \neq 2\ [n] \qquad \text{et} \qquad V_{2^s} = L_s^2 - 2 = 2.$$

Comme $2^s = M_s - 1$, et que le seul diviseur premier de $M_s - 1$ est 2, et comme $-2 \neq 2$ modulo M_s, on est dans les conditions d'application du critère de Lucas-Lehmer. On peut donc conclure que $\boxed{M_s \text{ est premier}}$.

(b) Pour montrer que le choix de $a = 4$ convient, il suffit de montrer que $a^2 - 4$ est premier à $M_s = 2^s - 1$. Or, avec $a = 4$, $a^2 - 4 = 12$. Cherchons donc le reste de M_s modulo 12 :

- pour $s \geqslant 2$, $2^s \equiv 0$ [4], donc $M_s \equiv -1[4]$
- pour $s \geqslant 2$ *impair*, on a $2^s \equiv -1$ [3], donc $M_2 \equiv -2 \equiv 1$ [3].

En énumérant les classes de congruence modulo 12, on se rend compte que la seule possibilité est $M_s \equiv 7$ [12]. Ainsi, M_s est premier avec $12 = a^2 - 4$. On est donc dans les conditions d'application du critère de Lucas. Ainsi, le choix de $a = 4$ convient.

Dans le cas où s est pair, on a une factorisation $M_s = (2^{s/2} - 1)(2^{s/2} + 1)$, qui montre que M_s est composé (sauf pour $s = 2$).

4. (a) On calcule :

$$(1+\beta)^2 = (x-1)^2 = x^2 - 2x + 1,$$

et puisque $x^2 - 4x + 1 = 0$, $\boxed{(1+\beta)^2 = 2x}$ De même,

$$(1-\beta)^2 = (3-x)^2 = x^2 - 6x + 9 = -2x + 8 = 2(4-x).$$

Or, la relation satisfaite par x se réécrit $x(4-x) - 1 = 0$, donc $4 - x = x^{-1}$. ainsi, $\boxed{(1-\beta)^2 = 2x^{-1}}$.

(b) On a donc :

$$(1+\beta)^{M_s+1} + (1-\beta)^{M_s+1} = (2x)^{\frac{M_s+1}{2}} + (2x^{-1})^{\frac{M_s+1}{2}},$$

ce qui a un sens puisque les exposants sont entiers positifs. Ainsi,

$$(1+\beta)^{M_s+1} + (1-\beta)^{M_s+1} = 2^{\frac{M_s+1}{2}}(x^{\frac{M_s+1}{2}} + x^{-\frac{M_s+1}{2}}) = 2^{\frac{M_s+1}{2}} V_{2^{s-1}},$$

donc, puisque, comme on l'a déjà dit, $L_s = V_{2^{s-1}}$,

$$\boxed{(1+\beta)^{M_s+1} + (1-\beta)^{M_s+1} = 2^{\frac{M_s+1}{2}} L_s.}$$

(c) Puisque M_s est supposé premier,

$$(1+\beta)^{M_s+1} = (1+\beta)(1+\beta)^{M_s} = (1+\beta)(1+\beta^{M_s})$$

et de même,

$$(1-\beta)^{M_s+1} = (1-\beta)(1-\beta^{M_s}),$$

par imparité de M_s. On a alors après développement et simplification

$$2^{\frac{M_s+1}{2}} L_s = 2 + 2\beta^{M_s+1} = 2(1 + 3^{\frac{M_s+1}{2}}),$$

puisque $\beta^2 = (x-2)^2 = x^2 - 4x + 4 = 3$. Or, comme montré ci-dessus, M_s étant premier, s est impair, et donc $M_s \equiv 7$ [12]. Ainsi, d'après III-7, 3 n'est pas résidu quadratique, donc $3^{\frac{M_s-1}{2}} \equiv -1$ $[M_s]$ puis $3^{\frac{M_s+1}{2}} \equiv -3$ $[M_s]$. De plus, s étant impair au moins égal à 3, $M_s \equiv -1$ [8], donc d'après III-8, 2 est résidu quadratique modulo M_s, donc $2^{\frac{M_s-1}{2}} \equiv 1$ $[M_s]$, donc $2^{\frac{M_s+1}{2}} \equiv 2$ $[M_s]$. On obtient donc

$$2L_s \equiv -4\ [M_s] \qquad \text{donc:} \qquad L_s \equiv -2\ [M_s],$$

2 étant inversible modulo M_s. On a donc $L_{s-1}^2 \equiv L_s + 2 \equiv 0$ $[M_s]$, et $\mathbb{Z}/M_s\mathbb{Z}$ étant un corps, $\boxed{L_{s-1} \equiv 0\ [M_s]}$. En déduire que $L_{s-1} \equiv 0$ $[M_s]$.

On a ainsi démontré le théorème de Lucas-Lehmer affirmant qu'avec les notations et les conditions de la question 3 et le choix de $a = 4$, M_s est premier si et seulement si $L_{s-1} \equiv 0$ $[M_s]$.