Corrigé de l'épreuve de mathématiques générales

Partie I

1. G étant un groupe de cardinal fini N, le théorème de Lagrange assure que $a^N = 1$ donc $\boxed{a^{N-1} \text{ est l'inverse de } a \text{ dans } G}$.

2. a) Par une récurrence immédiate : $b_i = a^{2^i}$ pour $i \in [\![0, k+1]\!]$ et $a_{i+1} = a^{\left[\sum_{j=0}^{i} x_j 2^j\right]}$ pour $i \in [\![0, k]\!]$.

   En particulier : $\boxed{a_{k+1} = a^{N-1} = a^{-1}}$.

   b) On sait que les x_i sont les restes des divisions euclidiennes successives de $N-1$ par 2. On peut donc utiliser l'algorithme suivant :
   - Initialiser trois variables $A = 1$, $B = a$ et $M = N - 1$;
   - tant que $M \neq 0$:
     - calculer le reste x de la division euclidienne de M par 2 ;
     - remplacer A par $A * B^x$ (c'est-à-dire par A ou $A * B$ selon si x vaut 0 ou 1) et B par $B * B$;
     - remplacer M par le quotient de la division euclidienne de M par 2 ;
   - fin du « tant que » ;
   - renvoyer A.

   La boucle est parcourue autant de fois qu'il y a de chiffres dans la décomposition de $N-1$ en base 2, c'est-à-dire $k+1$ fois et coûte à chaque fois deux multiplications au pire.

   $\boxed{\text{Le coût de l'algorithme est } 2(k+1)}$.

3. a) Les éléments inversibles de G sont les classes des entiers $a \in [\![0, 147]\!]$ premiers avec 148.

   En notant φ l'indicatrice d'Euler, le cardinal de G est
   $\varphi(148) = \varphi(2^2 \times 37) = \varphi(2^2)\varphi(37) = 2 \times 36$ donc $\boxed{N = 72}$.

   b) 5 est premier avec 148 donc inversible dans $\mathbb{Z}/148\mathbb{Z}$: $\boxed{5 \in G}$.

   71 s'écrit en base 2 sous la forme $72 = 2^0 + 2^1 + 2^2 + 2^6$.

   Ici : $b_0 = 5$, $b_1 = 25$, $b_2 = 33$, $b_3 = 53$, $b_4 = -3$, $b_5 = 9$, $b_6 = 81$ et

   $a_0 = 1$, $a_1 = 5$, $a_2 = 125 = -23$, $a_3 = -23 \times 33 = -19 = a_4 = a_5 = a_6$ donc $\boxed{a_7 = -19 \times 81 = -59 = a^{-1}}$.

   c) Comme 5 et 148 sont premiers entre eux, le théorème de Bézout assure l'existence d'un couple d'entiers (u, v) tel que $5u + 148v = 1$, ce qui signifie que u est inverse de 5 dans $\mathbb{Z}/148\mathbb{Z}$.

   On peut déterminer u et v par l'algorithme d'Euclide :

   $148 = 5 \times 29 + 3$ puis $5 = 3 + 2$ et $3 = 2 + 1$ donc

   $1 = 3 - 2 = 2 \times 3 - 5 = 2 \times 148 - 59 \times 5$.

   On retrouve bien que $\boxed{\text{l'inverse de 5 dans } \mathbb{Z}/148\mathbb{Z} \text{ est } -59}$.

Partie II

1. a) Considérons l'application $\boxed{\varphi_e : G^2 \to G, (x,y) \mapsto yx^{-e}}$.
   Alors, pour tout $(k,\tau) \in \mathbb{Z} \times \ G : \varphi_e \circ f_\alpha(k,\tau) = \varphi_e\left(\pi^k, \tau\alpha^k\right) = \tau\pi^{ek}\pi^{-ek} = \tau$.
   b) Il suffit que **A** fasse $\varphi_e(\lambda_i, \mu_i)$ pour retrouver τ_i.
2. a) Dans $\mathbb{F}_{29}^*$, on a $\lambda^{28} = 1$ pour tout λ donc $\lambda^{17} = \lambda^{-11}$ ce qui laisse penser que $\boxed{e = 11}$.
   On vérifie bien que $e^5 = 3$ donc $e^{11} = 2\left(2^5\right)^2 = 18$ et ça convient.
   b) En calculant pour chaque couple $\lambda_i^{17}\mu_i$ modulo 29, on trouve la suite 3, 15, 7, 9, 20, 15 donc le message est $\boxed{\text{COGITO}}$.

Partie III

1. a) On sait que $\mathbb{F}_{16}$ est un $\mathbb{F}_2$-espace vectoriel de dimension 4, construit comme $\dfrac{\mathbb{F}_2[X]}{(Q)}$ où (Q) est l'idéal engendré par un quelconque polynôme Q de degré 4 irréductible sur $\mathbb{F}_2$. En notant ω une racine de Q dans $\mathbb{F}_{16}$, $\mathbb{F}_{16}$ admet alors pour base sur $\mathbb{F}_2$ la famille $(1, \omega, \omega^2, \omega^3)$.
   Remarque : cette réponse est celle qu'il faut donner si on a lu la suite du problème mais toute autre solution juste est bien sûr acceptable ...
   b) $Q = X^4 + X^3 + 1$ est un polynôme de degré 4 sur $\mathbb{F}_2$. 0 et 1 n'en sont pas racine, donc il ne peut être réductible que s'il se décompose comme produit de deux trinômes.
   Dans ce cas, il existerait a et b dans $\mathbb{F}_2$ tels que :
   $$Q = \left(X^2 + aX + 1\right)\left(X^2 + bX + 1\right) = X^4 + (a+b)X^3 + abX^2 + (a+b)X + 1$$
   et on aurait $1 = a + b = 0$: absurde. Ainsi Q est irréductible sur $\mathbb{F}_2[X]$.

   On note ω une racine de Q : $(1, \omega, \omega^2, \omega^3)$ est une base de $\mathbb{F}_{16}$ sur $\mathbb{F}_2$.
   $\mathbb{F}_{16}^*$ est un groupe fini de cardinal 15, donc ω est d'ordre 1, 3, 5 ou 15 dans $\mathbb{F}_{16}^*$.
   La liberté de $(1, \omega, \omega^2, \omega^3)$ assure que ω et ω^3 sont différents de 1 : ω n'est d'ordre ni 1 ni 3.
   Par ailleurs, $\omega^5 = \omega\omega^4 = \omega(-1 - \omega^3) = \omega + \omega^4 = 1 + \omega + \omega^3$ est également différent de 1 car $(1, \omega, \omega^2, \omega^3)$ est libre : ω n'est pas d'ordre 5.
   Finalement ω est d'ordre 15 donc : $\boxed{\mathbb{F}_{16}^* = \left\{\omega^k, k \in [\![0, 15]\!]\right\}}$.
   c) Comme on est en caractéristique 2 : $\forall (x,y) \in \mathbb{F}_{16}, (x+y)^2 = x^2 + y^2$.
   Ainsi $\omega^4 + \omega^3 + 1 = 0$ donne en passant au carré :
   $$\omega^8 + \omega^6 + 1 = 0 \text{ puis } \omega^{16} + \omega^{12} + 1 = 0 \text{ et } \omega^{32} + \omega^{24} + 1 = 0$$
   ce qui montre que $\boxed{\omega,\ \omega^2,\ \omega^4 \text{ et } \omega^8 \text{ sont racines de } X^4 + X^3 + 1}$ et ce sont les seules puisque le polynôme est de degré 4 et qu'elles sont distinctes deux à deux.
   d) ω, ω^2, ω^4 et ω^8 sont les racines de $X^4 + X^3 + 1$ donc leur somme est $-1 = 1$.
   Vu le polynôme : $\omega^3 = 1 + \omega^4 = \omega + \omega^2 + \omega^8$, donc la famille $\left(\omega, \omega^2, \omega^4, \omega^8\right)$ engendre $(1, \omega, \omega^2, \omega^3)$ qui est une base de $\mathbb{F}_{16}$. Comme cette famille a quatre éléments, $\boxed{\left(\omega, \omega^2, \omega^4, \omega^8\right) \text{ est une base de } \mathbb{F}_{16}}$.

2. a) Le cas $a = 0$ est trivial. Prenons $a \neq 0$ dans la suite.
S'il existe x tel que $x^5 = a$, alors $a^3 = x^{15} = 1$ donc
$\boxed{\text{si } a^3 \neq 1, \text{ il n'y a pas de solution}}$.
Si $a^3 = 1$, il existe $k \in \mathbb{N}$ tel que $a = \omega^{5k}$.
Alors $\boxed{x^5 = a \text{ a pour solutions } \omega^k,\ \omega^{k+3},\ \omega^{k+6},\ \omega^{k+9} \text{ et } \omega^{k+12}}$.

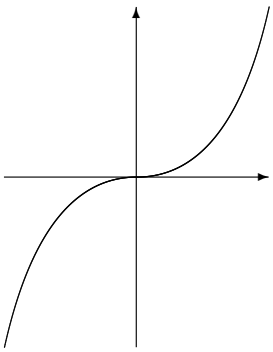
b) Si γ convient, γ^3 doit être égal à 1, γ, γ^2, γ^4 ou γ^8.
* $\gamma^3 = 1$ est impossible sinon $\gamma = \gamma^4$.
* $\gamma^3 = \gamma$ est impossible sinon on aurait $\gamma^2 = 1 = \gamma^4$.
* $\gamma^3 = \gamma^2$ ou $\gamma^3 = \gamma^4$ est impossible sinon γ serait égal à 1.
Finalement, il faut : $\gamma^5 = 1$ donc $\gamma \in \left\{\omega^3, \omega^6, \omega^9, \omega^{12}\right\}$.
Pour l'une quelconque des quatre valeurs précédentes, $\left\{\gamma, \gamma^2, \gamma^4, \gamma^8\right\}$ est la famille $\left\{\omega^3, \omega^6, \omega^9, \omega^{12}\right\}$.
ω^3 est racine de $X^5 + 1 = (X + 1)(X^4 + X^3 + X^2 + X + 1)$ et différent de 1, donc ω^3 est racine de $Q = X^4 + X^3 + X^2 + X + 1$.
0 et 1 ne sont pas racines de Q. Si celui-ci est réductible dans $\mathbb{F}_2[X]$, il doit se décomposer sous la forme :
$Q = (aX^2 + bX + c)(dX^2 + eX + f)$ avec a, b, c, d, e, f dans $\mathbb{F}_2$.
Alors : $a = d = 1$, $c = f = 1$ et les coefficients de X^3 et X imposent $b = 1 + e$.
Le coefficient de X^2 serait alors $af+cd+be = 0$ d'où contradiction : Q est irréductible dans $\mathbb{F}_2[X]$.
La famille $\left\{\omega^3, \omega^6, \omega^9, \omega^{12}\right\}$ est de la forme x, x^2, x^3, x^4 avec x racine d'un polynôme irréductible de degré 4 de $\mathbb{F}_2[X]$, donc est bien une base de $\mathbb{F}_{16}$ et elle vérifie les conditions demandées.
Il y a donc quatre éléments qui conviennent : $\boxed{\omega^3,\ \omega^6,\ \omega^9,\ \omega^{12}}$.

Les sommes se font évidemment bien et les produits aussi puisque les produits des termes de la base restent dans la base.

Partie IV

On comptera toutes les racines avec leur ordre de multiplicité. « Deux racines » peut donc en fait signifier « une racine double ».

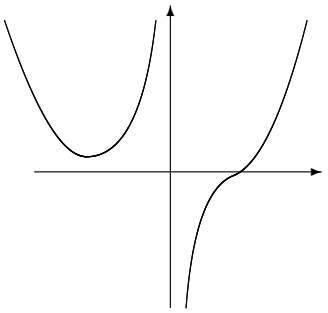
1. a) Considérons une droite D, d'équation $\alpha x + \beta y + \gamma = 0$ où α, β, γ sont des réels.
$M = (x, y)$ est point d'intersection de Γ et D si et seulement si $\begin{cases} y = x^3 \\ \alpha x + \beta y + \gamma = 0 \end{cases}$ ce qui est équivalent à résoudre $\alpha x + \beta x^3 + \gamma = 0$.
$\boxed{\text{Il y a donc une ou trois racines réelles}}$ (en comptant les multiplicités) et dans le cas où il y en a trois les relations entre coefficients et racines donnent $\boxed{x_A + x_B + x_C = 0}$.



b) En notant (x_{A*B}, y_{A*B}) les coordonnées de $A * B$, on sait que $A * B$ est déterminé par $x_{A*B} = -x_\Omega - x_C = x_A + x_B$ donc a pour coordonnées $\left(x_A + x_B, (x_A + x_B)^3\right)$.
$*$ est une loi interne à Γ par définition, associative par associativité de $+$ dans $\mathbb{R}$, a pour élément neutre $\Omega = (0, 0)$ et tout élément $A = (x_A, y_A = x_A^3)$ de Γ admet pour symétrique $(-x_A, -y_A)$: $\boxed{(\Gamma, *) \text{ est un groupe (abélien en plus)}}$.

$\varphi : \mathbb{R} \to \Gamma, x \mapsto M = (x, x^3)$ est visiblement un isomorphisme :
$\boxed{(\Gamma, *) \text{ est isomorphe à } (\mathbb{R}, +)}$.

2. a) On remarque que Γ ne contient aucun point d'abscisse nulle.
Toutes les abscisses considérées dans la suite de cette question sont non nulles.
La cubique a pour équation : $y = \dfrac{x^3-1}{3x}$.
La fonction $x \mapsto \dfrac{x^3-1}{3x}$ est définie sur $\mathbb{R}^*$, croissante sur $\mathbb{R}_+^*$ et $\left[-2^{-1/3}, 0\right[$, décroissante sur $\left]-\infty, -2^{-1/3}\right]$.
Elle admet pour limite $+\infty$ en $-\infty$, en 0 à gauche et en $+\infty$. Sa limite en 0 à droite est $-\infty$, ce qui donne l'allure sommaire ci-contre.



b) Soit D une droite quelconque, d'équation $\alpha x + \beta y + \gamma = 0$ (différente de $x = 0$).
Un point (x, y) est intersection de Γ et D si et seulement si $y = \dfrac{x^3-1}{3x}$ et $\alpha x + \beta\dfrac{x^3-1}{3x} + \gamma = 0$, ce qui revient à résoudre $\beta x^3 + 3\alpha x^2 + 3\gamma x - \beta = 0$.
Si on sait déjà qu'il existe deux solutions x_A et x_B, D n'est pas une droite « verticale » ($\beta \neq 0$) donc il existe exactement une troisième solution x_C et on trouve encore que
$\boxed{C \text{ existe et est unique}}$.
De plus, les relations entre coefficients et racines assurent que le produit des racines est 1 donc C est caractérisé par $\boxed{x_A x_B x_C = 1}$.

c) Alors $x_{A*B} = \dfrac{1}{x_\Omega x_C} = x_A x_B$: $(\Gamma, *)$ est un groupe ; l'élément neutre est Ω et le symétrique de $A = (x_A, y_A)$ est le point d'abscisse $\dfrac{1}{x_A}$.
Par l'application $\varphi : \mathbb{R} \to \Gamma, x \mapsto M = \left(x, \dfrac{x^3-1}{3x}\right)$,
$\boxed{(\Gamma, *) \text{ est un groupe commutatif isomorphe à } (\mathbb{R}^*, \times)}$.

3. Une droite D du plan projectif a une équation de la forme $\alpha X + \beta Y + \gamma Z = 0$, α, β, γ étant des réels non tous nuls. On suppose qu'on n'est pas dans le cas où la cubique contient D.
Chercher les intersections de Γ et D revient à résoudre le système $\begin{cases} \overline{P}(X, Y, Z) = 0 \\ \alpha X + \beta Y + \gamma Z = 0 \end{cases}$
Comme α, β et γ sont non tous nuls, l'une des variables peut s'exprimer en fonction des deux autres, par exemple X en fonction Y et Z. En remplaçant dans $\overline{P}$, on se ramène à une équation $Q(Y, Z) = 0$ où Q est un polynôme homogène de degré 3, de la forme :
$$Q(Y, Z) = aY^3 + bY^2Z + cYZ^2 + dZ^3.$$
On cherche des solutions (X, Y, Z) différentes de $(0, 0, 0)$ ce qui exclut que (Y, Z) soit le couple $(0, 0)$.
Premier cas : $d \neq 0$.
Alors les solutions (Y, Z) vérifient $Y \neq 0$. En posant $t = \dfrac{Z}{Y}$, résoudre le problème est, vu l'homogénéité des coordonnées, équivalent à trouver t tel que $dt^3 + ct^2 + bt + a = 0$: on a exactement une ou trois solutions réelles.
Deuxième cas : $d = 0$.

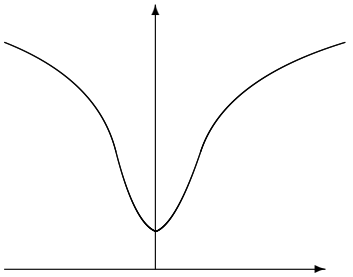
Si $a \neq 0$, on se ramène au cas précédent en échangeant les rôles de Y et Z.
Sinon, il reste à résoudre $bY^2Z + cYZ^2 = 0$ soit $YZ(bY + cZ) = 0$.
À l'homogénéité près, il y a exactement trois solutions : $(1,0)$, $(0,1)$ et $(c,-b)$.

Finalement, $\boxed{\Gamma \text{ coupe bien toute droite en exactement un ou trois points}}$.

4. a) On passe en coordonnées (« presque ») polaires : $\begin{cases} x = r\cos\theta \\ y = r\sin\theta \end{cases}$ (on autorise $r \leqslant 0$).

Un point différent de $(0,0)$ appartient à γ si et seulement si $r^3\sin^3\theta = r^2$ soit $\boxed{r = \dfrac{1}{\sin^3\theta}}$.

$\rho : \theta \mapsto \dfrac{1}{\sin^3\theta}$ est défini sur $\mathbb{R} \setminus \pi\mathbb{Z}$, 2π-périodique, impaire, ce qui permet de faire l'étude sur $]0,\pi[$ et on complètera le tracé par symétrie par rapport à l'axe Oy.
De plus : $\rho(\pi - \theta) = \rho(\theta)$ donc on limite l'étude à $\left]0, \dfrac{\pi}{2}\right]$ et on complète le tracé par symétrie par rapport à l'axe Oy.
ρ est positif sur $\left]0, \dfrac{\pi}{2}\right]$ et tend vers $+\infty$ en 0 : on a une branche infinie de direction Ox.



L'ordonnée du point de paramètre θ est $\dfrac{\sin\theta}{\sin^3\theta} = \dfrac{1}{\sin^2\theta} \xrightarrow{\theta\to 0} +\infty$ donc il n'y a pas de droite asymptote.

b) Soit (X,Y,Z) un point du plan projectif différent de $(0,0,1)$. Alors (X,Y) est différent de $(0,0)$ donc il existe des réels $\lambda \in \mathbb{R}^*$ et $\theta \in \mathbb{R}$ tels que $\begin{cases} X = \lambda\cos\theta \\ Y = \lambda\sin\theta \end{cases}$.
(X,Y,Z) appartient à Γ si et seulement si $\lambda^3\sin^3\theta - \lambda^2 Z = 0$ soit $Z = \lambda\sin^3\theta$.
Compte-tenu de l'homogénéité, on peut donc paramétrer Γ par $\begin{cases} X = \cos\theta \\ Y = \sin\theta \\ Z = \sin^3\theta \end{cases}$, θ décrivant $\mathbb{R}$.

Soit D une droite du plan, d'équation $\alpha X + \beta Y + \gamma Z = 0$.
Un point de Γ de paramètre θ appartient à Γ si et seulement si : $\alpha\cos\theta + \beta\sin\theta + \gamma\sin^3\theta = 0$.
Ceci est équivalent à :

$$\alpha(e^{i\theta} + e^{-i\theta}) - i\beta(e^{i\theta} - e^{-i\theta}) + i\frac{\gamma}{4}\left[e^{3i\theta} - 3e^{i\theta} + 3e^{-i\theta} - e^{3i\theta}\right] = 0.$$

En posant $T = e^{2i\theta}$, c'est équivalent à résoudre :

$$\gamma T^3 + (4\alpha + 3i\gamma - 4i\beta)T^2 + (4\alpha - 3i\gamma + 4i\beta)T - \gamma = 0.$$

Pour $\gamma \neq 0$, il y a exactement trois solutions T_1, T_2, T_3 dans $\mathbb{C}$ dont le produit vaut 1.
Le cas $\gamma = 0$ est exclu dans la suite par le fait qu'il n'y aurait qu'une solution T non nulle.

Soit A et B deux points de Γ, de paramètres θ_A et θ_B. Le résultat précédent montre que la droite AB coupe Γ en un troisième point C de paramètre θ_C caractérisé par :

$$e^{2i(\theta_A+\theta_B+\theta_C)} = 1.$$

En remarquant que Ω est le point de paramètre 0, on en déduit que $A * B$ est le point de paramètre θ caractérisé par $e^{2i\theta_C+2i\theta} = 1$ soit $e^{2i\theta} = e^{2i(\theta_A+\theta_B)}$.

Deux paramètres égaux modulo π donnent le même point (cela multiplie toutes les coordonnées par -1), donc $A * B$ est le point de paramètre $\boxed{\theta = \theta_A + \theta_B}$.

c) L'application qui au point M de Γ de paramètre θ associe $e^{2i\theta}$ est un isomorphisme de $(\Gamma, *)$ sur $(\mathscr{U}, \times)$, où $\mathscr{U}$ est l'ensemble des nombres complexes de module 1.

Les points d'ordre 6 sont ceux qui sont associés par l'isomorphisme précédent aux points d'ordre 6 dans $\mathscr{U}$, *i.e.* qui correspondent à $\theta = \dfrac{\pi}{6}$ ou $\theta = \dfrac{5\pi}{6}$ ce qui donne $\boxed{\text{les deux points } (\pm 4\sqrt{3}, 4, 1)}$.

Partie V

1. Pour chaque $x \in \mathbb{F}_{16}$, l'équation $y^2 + y = x^3 + x$ d'inconnue y a au plus deux solutions. Ainsi, lorsque x parcourt $\mathbb{F}_{16}$,

$$\boxed{\text{il existe au plus 32 couples } (x, y) \text{ vérifiant } x^3 + x = y^2 + y}.$$

2. Considérons Γ dans le plan projectif ; elle contient, en plus des points de Γ', le point à l'infini $\Omega = (0, 1, 0)$.

Comme en IV, intersecter Γ avec une droite projective d'équation $\alpha X + \beta Y + \gamma Z = 0$ revient à résoudre une équation homogène de degré 3 par exemple en Y et Z.

S'il y a déjà deux points d'intersection A et B, il y en a donc également un troisième C. De même, le point $A * B$, troisième intersection de ΩC avec Γ, est toujours bien défini.

3. a) La définition ci-dessus ne fait pas intervenir l'ordre du couple (A, B) :

$$\boxed{\text{l'opération * est commutative}}.$$

Vu la définition également, $\boxed{\Omega \text{ est élément neutre pour } *}$ et tout élément A admet un inverse A^{-1} qui est la troisième intersection de ΩA avec Γ.

b) Avec le Ω ci-dessus, si $A = (\alpha, \beta)$ est un point de Γ', chercher B tel que (AB) ait la direction de Ω revient à faire en sorte que AB soit une droite « verticale », *i.e.* on cherche B de coordonnées (α, y) telles que $y^2 + y = \alpha^3 + \alpha$.

On sait que β est l'une des solutions de cette équation et $-1 = 1$ est la somme des racines donc la deuxième solution est $1 + \beta$.

Ainsi $\boxed{A^{-1} \text{ est le point de coordonnées } (\alpha, 1 + \beta)}$.

4. a) Une droite d'équation $ax + by + c = 0$ intersecte Γ' aux points de coordonnées (x, y) tels que :

$$\begin{cases} ax + by + c = 0 \\ y^2 + y = x^3 + x \end{cases}$$

La droite passe par A si et seulement si $c = a\alpha + b\beta$ ce qui ramène au système équivalent, lorsque $a \neq 0$ par exemple :

$$\begin{cases} a(x - \alpha) + b(y - \beta) = 0 \\ P\left(\dfrac{-by - c}{a}, y\right) = 0 \end{cases}$$

et la droite est tangente en A à Γ' si et seulement s'il y a racine double, i.e. :

$$\frac{d}{dy} P\left(\frac{-b(y - \beta) - a\alpha}{a}, y\right)_{|y=\beta} = 0 \text{ soit } -\frac{b}{a} P'_X(\alpha, \beta) + P'_Y(\alpha, \beta) = 0.$$

On remarque que, pour le polynôme $P(X,Y) = Y^2 + Y - X^3 - X$, il n'existe aucun point singulier dans Γ (tel que $P'_X(\alpha,\beta) = P'_Y(\alpha,\beta) = 0$) et on déduit la condition nécessaire et suffisante de tangence :

$$bP'_X(\alpha,\beta) - aP'_Y(\alpha,\beta) = 0$$

qui donne une tangente d'équation $\boxed{P'_X(\alpha,\beta)(x-\alpha) + P'_Y(\alpha,\beta)(y-\beta) = 0}$.

b) La tangente à Γ' en A a pour équation :
$(2\beta+1)(y-\beta) = (3\alpha^2+1)(x-\alpha)$ soit $y - \beta = (1+\alpha^2)(x-\alpha)$.
En éliminant y dans $x^3 + x = y^2 + y$, on trouve :

$$x^3 + x = (1+\alpha^2)(x-\alpha) + \beta + (1+\alpha^2)^2(x-\alpha)^2 + \beta^2$$

La somme des abscisses des points A, $B = A$ et C est donnée par le coefficient de x^2 : c'est $(1+\alpha^4)$.

C est donc le point de coordonnées
$\left(1+\alpha^4, \beta + (\alpha^2+1)\left(1+\alpha^4-\alpha\right)\right) = \left(1+\alpha^4, \beta+1+\alpha+\alpha^2+\alpha^3+\alpha^4+\alpha^6\right)$
et $A * A$ est le point de coordonnées
$\left(1+\alpha^4, 1+\beta+(\alpha^2+1)\left(1+\alpha^4-\alpha\right)\right) = \left(1+\alpha^4, \beta+\alpha+\alpha^2+\alpha^3+\alpha^4+\alpha^6\right)$.
Comme $\alpha^3 + \alpha = \beta + \beta^2$ et $\alpha^2 + \alpha^6 = (\alpha+\alpha^3)^2 = \beta^2 + \beta^4$, les coordonnées de $A * A$ sont

$$\boxed{\left(1+\alpha^4, \alpha^4+\beta^4\right)}.$$

c) Alors A^4 a pour abscisse $1 + \left(1+\alpha^4\right)^4 = \alpha^{16} = \alpha$ et pour ordonnée $\left(1+\alpha^4\right)^4 + \alpha^{16} + \beta^{16} = 1+\beta$ donc

$$\boxed{A^4 = A^{-1}}.$$

d) Pour tout $A \in \Gamma'$ et même pour $A = \Omega$: $A^5 = \Omega$ donc A peut être d'ordre 1 (dans le cas de Ω) ou 5.

Les éléments de Γ sont tous d'ordre 5, sauf Ω, donc le cardinal de Γ doit être une puissance de 5.

Le cardinal de Γ est celui de Γ' auquel on ajoute 1 à cause de Ω : il doit être inférieur à 33 et ne peut donc être que 5 ou 25.

Or Ω, $(0,0)$, $(0,1)$, $(1,0)$, $(1,1)$ sont dans Γ. D'après les calculs faits dans la partie III :

$$\omega + \omega^3 = 1 + \omega + \omega^4 = \omega^2 + \omega^8 = (\omega^2+\omega^4) + (\omega^2+\omega^4)^2$$

donc $(\omega, \omega^2+\omega^4)$ est un sixième point de Γ.

Finalement : $\boxed{\operatorname{Card}\Gamma = 25}$ et $\boxed{\Gamma \sim (\mathbb{Z}/5\mathbb{Z})^2}$.

5. On choisit un point A de Γ et un entier e ; on calcule $B = A^e$. On travaille dans le groupe $H = \left\{A^k ; k \in \mathbb{N}\right\}$.

On rend publics H, les points A et B. On demande à l'expéditeur de coder son message par un point $M \in H$, de choisir un entier k (qu'il garde secret) et d'envoyer $(A^k, MB^k) = (Y, Z)$. Les espions ne peuvent alors déterminer ni e ni k, mais le destinataire sait calculer $ZY^{-e} = M$.

Rapport des correcteurs

Les candidats ont principalement abordé les parties I, II et IV ; la partie III s'est révélée extrêmement discriminante.

Dans la partie I, il est utile de rappeler aux candidats que l'on attend d'eux une démonstration précise, même lorsqu'il suffit de faire une récurrence « évidente » : il est tout aussi rapide et beaucoup plus rigoureux de poser précisément la récurrence que de faire un vague discours sur la récurrence que l'on pourrait faire.

L'algorithme demandé est souvent très mal décrit. On attendait la description précise des initialisations de variables et des structures de contrôles utilisées ; il est par contre mal venu de s'encombrer de déclarations d'entrées-sorties, d'appels de bibliothèques ... surtout lorsqu'ils sont liés à un langage particulier.

La partie II a posé peu de problèmes, à part une erreur très courante dans la définition de $\varphi_e : (x, y) \mapsto \dfrac{y}{x^e}$.

La partie III a été la moins bien traitée en général et n'a souvent pas été abordée. $\mathbb{F}_{16}$ a été défini de façon fantaisiste : $\mathbb{Z}/16\mathbb{Z}$ ou $(\mathbb{Z}/17\mathbb{Z})^*$ entre autres.

En partie IV, dans 50% des copies, le tracé de $y = x^3$ est incorrect : la tangente à l'origine n'est pas horizontale. Il faut que dans un tracé, même sommaire, les candidats mettent en évidence les éléments remarquables de la courbe.

L'étude de l'intersection courbe-droite en IV.1.b) a souvent été faite de façon extrêmement compliquée, avec des études multiples de cas particuliers ($y = b$, $y = ax$, $y = ax + b$ ...) et d'énormes difficultés pour discuter le nombre de racines d'un polynôme de degré 3.

Les relations entre coefficients et racines sont très mal connues ce qui rend difficile la détermination des relations entre x_A, x_B, x_C demandées en IV.1 et IV.2.

La question IV.3 était posée de façon incorrecte et a été notée généreusement.

Le tracé de la courbe en coordonnées polaires du IV.4 a souvent été un obstacle insurmontable et la fin du problème n'est pratiquement jamais abordée.
