UL 311 **J. 5006**

SESSION 2003

Filière MP

MATHÉMATIQUES

Epreuve commune aux ENS de Paris et Lyon

Durée : 6 heures

L'usage de toute calculatrice est interdit.

Aucun document n'est autorisé.

Tournez la page S.V.P.

Les symboles $\mathbf{C}$, $\mathbf{R}$, $\mathbf{Q}$, $\mathbf{Z}$ et $\mathbf{N}$ désignent respectivement le corps des nombres complexes, le corps des nombres réels, le corps des nombres rationnels, l'anneau des entiers relatifs et l'ensemble des entiers naturels.

Dans tout ce problème, D est un entier impair sans facteur carré. Si $\mathrm{S} = \{p_1, \ldots, p_s\}$, où s est le cardinal de S, est l'ensemble des nombres premiers divisant D, alors $2 \notin \mathrm{S}$ et D est le produit des p_i, pour $1 \leq i \leq s$.

L'objet du problème est l'étude de l'ensemble $\mathrm{C}(\mathbf{Q})$ des solutions $(x, y) \in \mathbf{Q}^2$ de l'équation $y^2 = x^3 - \mathrm{D}^2 x$, avec $x > 0$. Plus précisément, il s'agit de démontrer que l'on peut munir $\overline{\mathrm{C}}(\mathbf{Q}) = \mathrm{C}(\mathbf{Q}) \cup \{\infty\}$ d'une structure de groupe commutatif *de type fini* (cas particulier du *théorème de Mordell-Weil*). On note C l'ensemble des solutions dans $\mathbf{R}^2$ de l'équation $y^2 = x^3 - \mathrm{D}^2 x$, avec $x > 0$; on a donc $\mathrm{C}(\mathbf{Q}) = \mathrm{C} \cap \mathbf{Q}^2$.

La partie I donne un critère permettant de montrer qu'un groupe commutatif est de type fini. La partie II munit $\overline{\mathrm{C}} = \mathrm{C} \cup \{\infty\}$ d'une structure de groupe commutatif. La partie III donne un certain nombre de formules relatives à cette loi de groupe, et la partie IV est consacrée à la démonstration du théorème de Mordell-Weil. Ces 4 parties reposent sur des techniques différentes et peuvent se traiter de manière indépendante (pour la partie III, on n'a besoin que de la définition de la loi d'addition donnée dans la question **6.b** de la partie II, et la partie IV utilise de manière intensive les formules de la partie III mais pas leur démonstration).

Il sera tenu compte du soin apporté à la rédaction. En particulier, il est possible (et même recommandé) d'utiliser des résultats démontrés dans des questions antérieures, mais il faut indiquer la question où le résultat apparaît.

I

Dans cette partie, Γ est un groupe commutatif pour une loi notée $+$. L'élément neutre de Γ est noté 0 et l'opposé d'un élément x de Γ est noté $-x$. Si $n \in \mathbf{Z}$ et $x \in \Gamma$, on note nx l'élément de Γ évident ($0x = 0$ et $(n+1)x = nx + x$ si $n \in \mathbf{Z}$).

On dit que Γ est *de type fini* s'il existe $r \in \mathbf{N}$ et $x_1, \ldots, x_r \in \Gamma$ tels que tout élément x de Γ puisse s'écrire sous la forme $\sum_{i=1}^{r} n_i x_i$, avec $n_i \in \mathbf{Z}$, si $1 \leq i \leq r$. On dit que Γ est *de type fini modulo* 2 s'il existe un sous-ensemble fini Z de Γ tel que tout élément x de Γ puisse s'écrire sous la forme $z + 2y$, avec $z \in \mathrm{Z}$ et $y \in \Gamma$.

On appelle *hauteur* sur Γ une application $h : \Gamma \to \mathbf{R}_+$ telle qu'il existe $\mathrm{M} \geq 0$ tel que, quels que soient $(x, y) \in \Gamma^2$, on ait

$$|h(x+y) + h(x-y) - 2h(x) - 2h(y)| \leq \mathrm{M}.$$

On dit que h est *admissible* si, quel que soit $\mathrm{B} \geq 0$, l'ensemble des éléments x de Γ vérifiant $h(x) \leq \mathrm{B}$ est un ensemble fini.

1. On note Γ_{tors} l'ensemble des $x \in \Gamma$ tels qu'il existe $n \in \mathbf{Z} - \{0\}$ tel que $nx = 0$.

1.a. Montrer que Γ_{tors} est un sous-groupe de Γ.

1.b. Le groupe Γ_{tors} est-il nécessairement fini?

2. Soit h une hauteur sur Γ.

2.a. Montrer que, si $x \in \Gamma$, la suite de terme général $4^{-n}h(2^n x)$ tend vers une limite $\widehat{h}(x)$ quand n tend vers $+\infty$, et qu'il existe $\mathrm{M}' \geq 0$ tel que $|h(x) - \widehat{h}(x)| \leq \mathrm{M}'$, quel que soit $x \in \Gamma$.

2.b. Montrer que $\widehat{h}$ vérifie l'identité:

$$\widehat{h}(x+y) + \widehat{h}(x-y) = 2\widehat{h}(x) + 2\widehat{h}(y) \quad \text{quels que soient } x, y \in \Gamma.$$

2.c. Calculer $\widehat{h}(nx)$ en fonction de $\widehat{h}(x)$, si $n \in \mathbf{Z}$.

3. On suppose que l'on peut munir Γ d'une hauteur admissible h.

3.a. Montrer que $\widehat{h}$ est une hauteur admissible sur Γ.

3.b. Montrer que $\widehat{h}(x) = 0$ si et seulement si $x \in \Gamma_{\text{tors}}$.

3.c. Montrer que Γ_{tors} est fini.

3.d. Montrer que, si $x = z + 2y$, alors $\widehat{h}(y) \leq \frac{1}{2}(\widehat{h}(x) + \widehat{h}(z))$.

3.e. Montrer que si Γ est de type fini modulo 2, alors il est de type fini.

II

On rappelle que C est l'ensemble des solutions $(x, y) \in \mathbf{R}^2$ de l'équation $y^2 = x^3 - \mathrm{D}^2 x$ avec $x > 0$. (Il n'est probablement pas inutile de faire un dessin grossier de C.) Si $(x_0, y_0) \in$ C, la tangente à C en (x_0, y_0) est la droite d'équation $2y_0(y - y_0) = (3x_0^2 - \mathrm{D}^2)(x - x_0)$.

Si $(u, v) \in \mathbf{R}^* \times \mathbf{R}$, notons (u', v') le couple défini par $u' = \frac{1}{u}$, $v' = -\frac{v}{u}$, et $\mathrm{P}_{u,v}$ et $\mathrm{Q}_{u',v'}$ les polynômes définis par

$$\mathrm{P}_{u,v}(x) = x^3 - \mathrm{D}^2 x - (ux + v)^2 \quad \text{et} \quad \mathrm{Q}_{u',v'}(y) = (u'y + v')^3 - \mathrm{D}^2(u'y + v') - y^2.$$

On note $\mathrm{D}_{u,v}$ la droite d'équation $y = ux + v$. On pourra utiliser sans démonstration les équivalences (I1) $\Leftrightarrow$ (I2) $\Leftrightarrow$ (I3), avec

(I1) $(x, y) \in \mathrm{D}_{u,v} \cap \mathrm{C}$

(I2) $x > 0$, $\mathrm{P}_{u,v}(x) = 0$ et $y = ux + v$

(I3) $\mathrm{Q}_{u',v'}(y) = 0$ et $x = u'y + v' > 0$

et, si $(x_0, y_0) \in \mathrm{C} \cap \mathrm{D}_{u,v}$, les équivalences (T1) $\Leftrightarrow$ (T2) $\Leftrightarrow$ (T3), avec

(T1) $\mathrm{D}_{u,v}$ est tangente à C en (x_0, y_0)

(T2) $\mathrm{P}_{u,v}$ a un zéro double en x_0

(T3) $\mathrm{Q}_{u',v'}$ a un zéro double en y_0.

1. Soit $n(u,v)$ le cardinal de l'intersection de C avec la droite $\mathrm{D}_{u,v}$ d'équation $y = ux + v$.

1.a. Montrer que $n(u,v) \leq 3$.

1.b. Montrer que $\mathrm{U} = \{(u,v) \in \mathbf{R}^* \times \mathbf{R},\ n(u,v) = 3\}$ est un ouvert de $\mathbf{R}^2$.

1.c. Montrer que, si $n(u,v) \geq 2$ et si $\mathrm{D}_{u,v}$ n'est pas tangente à C, alors $n(u,v) = 3$.

1.d. Montrer que, si $(a,b) \in \mathbf{R}^2$, il n'existe qu'un nombre fini de points P de C tels que la tangente à C en P passe par (a,b).

2. Si $\mathrm{P} = (x,y) \in \mathrm{C}$, on pose $x(\mathrm{P}) = x$ et $y(\mathrm{P}) = y$.

2.a. Montrer que, si $t \in \mathbf{R}$, il existe un unique point $\mathrm{P}(t)$ de C vérifiant $y(\mathrm{P}(t)) = t$, et que, si on pose $\mathrm{F}(t) = x(\mathrm{P}(t))$, alors C est l'ensemble des couples $(\mathrm{F}(y), y)$, avec $y \in \mathbf{R}$.

2.b. Montrer que $\mathrm{F}(y) \geq \mathrm{D}$ quel que soit $y \in \mathbf{R}$, que F est paire, que l'on a $\mathrm{F}(y_1) = \mathrm{F}(y_2)$ si et seulement si $y_1 = \pm y_2$, et que F est de classe $\mathcal{C}^1$ sur $\mathbf{R}$.

2.c. Montrer que $|y|^{-2/3}\mathrm{F}(y)$ tend vers 1 quand y tend vers $+\infty$ ou vers $-\infty$.

2.d. Soient $a \in \mathbf{R}^*$ et $t \in \mathbf{R} - \{0, a, -a\}$. Notons $\mathrm{D}(a,t)$ la droite joignant $\mathrm{P}(t)$ à $\mathrm{P}(a)$ et $\mathrm{H}_a(t)$ l'élément de $\mathbf{R}$ défini par

$$a\,t\,\mathrm{H}_a(t) = -\Big(\frac{t-a}{\mathrm{F}(t)-\mathrm{F}(a)}\Big)^3\Big[\Big(\frac{t\mathrm{F}(a)-a\mathrm{F}(t)}{t-a}\Big)^3 - \mathrm{D}^2\frac{t\mathrm{F}(a)-a\mathrm{F}(t)}{t-a}\Big].$$

Montrer que l'on a les équivalences suivantes:

(i) $\mathrm{H}_a(t) \notin \{a,t\} \Leftrightarrow \mathrm{P}(\mathrm{H}_a(t))$ est le troisième point d'intersection de C et $\mathrm{D}(a,t)$;

(ii) $\mathrm{H}_a(t) = a \Leftrightarrow \mathrm{D}(a,t)$ est la tangente à C en $\mathrm{P}(a)$;

(iii) $\mathrm{H}_a(t) = t \Leftrightarrow \mathrm{D}(a,t)$ est la tangente à C en $\mathrm{P}(t)$.

2.e. Calculer la limite de $\mathrm{H}_a(t)$ quand t tend vers $+\infty$. Que devient la droite $\mathrm{D}(a,t)$?

3. On déduit des questions **2.b** et **2.c** la convergence absolue de l'intégrale $\int_{-\infty}^{+\infty} \frac{2\,dt}{3\mathrm{F}(t)^2-\mathrm{D}^2}$. On note Ω la valeur de l'intégrale $\int_{-\infty}^{+\infty} \frac{2\,dt}{3\mathrm{F}(t)^2-\mathrm{D}^2}$, et on définit une fonction $y \mapsto \mathrm{L}(y)$ par la formule

$$\mathrm{L}(y) = \int_{-\infty}^{y} \frac{2\,dt}{3\mathrm{F}(t)^2 - \mathrm{D}^2}.$$

3.a. Montrer que L induit une bijection de $\mathbf{R}$ sur $]0,\Omega[$.

3.b. Calculer $\mathrm{L}(y) + \mathrm{L}(-y)$ si $y \in \mathbf{R}$.

4. Soient $x_1, \ldots, x_n$, des nombres complexes distincts deux à deux.

4.a. Montrer que, si $\mathrm{Q} \in \mathbf{C}[\mathrm{X}]$ est de degré $\leq n-1$, alors

$$\mathrm{Q}(\mathrm{X}) = \sum_{i=1}^{n} \mathrm{Q}(x_i)\Big(\prod_{j\neq i} \frac{\mathrm{X}-x_j}{x_i-x_j}\Big).$$

4.b. Montrer que, si $\mathrm{P}(\mathrm{X}) = \prod_{i=1}^{n}(\mathrm{X}-x_i)$, alors $\sum_{i=1}^{n} \frac{x_i^k}{\mathrm{P}'(x_i)} = 0$ si $k \in \{0,\dots,n-2\}$ (avec la convention $0^0 = 1$) et calculer $\sum_{i=1}^{n} \frac{x_i^{n-1}}{\mathrm{P}'(x_i)}$.

5.

5.a. Soit I un intervalle ouvert de $\mathbf{R}$, et soient $t \mapsto y_1(t)$, $t \mapsto y_2(t)$ et $t \mapsto y_3(t)$ des fonctions de classe $\mathcal{C}^1$ de I dans $\mathbf{R}$ telles que, quel que soit $t \in \mathrm{I}$, les points $\mathrm{P}_i(t) = (x_i(t), y_i(t)) = \mathrm{P}(y_i(t))$, $i \in \{1,2,3\}$, soient distincts deux à deux et alignés. Montrer que la fonction

$$t \mapsto \mathrm{G}(t) = \mathrm{L}(y_1(t)) + \mathrm{L}(y_2(t)) + \mathrm{L}(y_3(t))$$

est constante sur I. (On introduira l'équation $y = u(t)x + v(t)$ de la droite contenant les $\mathrm{P}_i(t)$ et on commencera par vérifier que u et v sont de classe $\mathcal{C}^1$ sur I.)

5.b. Montrer que, si $\mathrm{H}_a(t)$ est la quantité introduite à la question **2.d**, alors $\mathrm{L}(a) + \mathrm{L}(t) + \mathrm{L}(\mathrm{H}_a(t)) = 2\Omega$ quels que soient $a > 0$ et $t > a$.

5.c. Montrer que, si y_1, y_2, y_3 sont trois éléments de $\mathbf{R}$, distincts deux à deux, tels que $\mathrm{P}(y_1)$, $\mathrm{P}(y_2)$ et $\mathrm{P}(y_3)$ sont alignés, alors $\mathrm{L}(y_1) + \mathrm{L}(y_2) + \mathrm{L}(y_3) \in \{\Omega, 2\Omega\}$.

5.d. Montrer que, si $y_1 \neq y_2$, et si $\mathrm{P}(y_2)$ est sur la tangente à C en $\mathrm{P}(y_1)$, alors $2\mathrm{L}(y_1) + \mathrm{L}(y_2) \in \{\Omega, 2\Omega\}$.

5.e. Montrer que, si y_1, y_2, y_3 sont trois éléments de $\mathbf{R}$, distincts deux à deux, tels que $\mathrm{L}(y_1) + \mathrm{L}(y_2) + \mathrm{L}(y_3) \in \Omega\mathbf{Z}$, alors $\mathrm{P}(y_1)$, $\mathrm{P}(y_2)$ et $\mathrm{P}(y_3)$ sont alignés.

6. Soit $\mathbf{G}$ le groupe des nombres complexes de module 1 et soit $\mathrm{E} : \overline{\mathrm{C}} \to \mathbf{G}$ l'application définie par $\mathrm{E}(\infty) = 1$ et $\mathrm{E}(\mathrm{P}(y)) = \exp(\frac{2i\pi}{\Omega}\mathrm{L}(y))$ si $y \in \mathbf{R}$.

6.a. Montrer qu'il existe, sur $\overline{\mathrm{C}}$, une unique loi de groupe commutatif $+$ telle que l'on ait $\mathrm{E}(\mathrm{P}+\mathrm{Q}) = \mathrm{E}(\mathrm{P})\mathrm{E}(\mathrm{Q})$. Montrer de plus, que, si $\mathrm{P}+\mathrm{Q} \neq \infty$, alors $\mathrm{L}(y(\mathrm{P}+\mathrm{Q})) = \mathrm{L}(y(\mathrm{P})) + \mathrm{L}(y(\mathrm{Q}))$ si $\mathrm{L}(y(\mathrm{P})) + \mathrm{L}(y(\mathrm{Q})) < \Omega$ et $\mathrm{L}(y(\mathrm{P}+\mathrm{Q})) = \mathrm{L}(y(\mathrm{P})) + \mathrm{L}(y(\mathrm{Q})) - \Omega$ si $\mathrm{L}(y(\mathrm{P})) + \mathrm{L}(y(\mathrm{Q})) > \Omega$.

6.b. Montrer que ∞ est l'élément neutre pour $+$ et que, si $\mathrm{P}_1 = (x_1, y_1)$, $\mathrm{P}_2 = (x_2, y_2)$ et $\mathrm{P}_3 = (x_3, y_3)$ sont trois éléments distincts de C, alors $\mathrm{P}_1 + \mathrm{P}_2 + \mathrm{P}_3 = \infty$ si et seulement si P_1, P_2 et P_3 sont alignés.

6.c. Montrer que, si $\mathrm{P} \in \mathrm{C}$, alors l'opposé $-\mathrm{P}$ de P pour la loi $+$ est le symétrique de P par rapport à l'axe des x.

6.d. Montrer que si $\mathrm{P} \in \overline{\mathrm{C}}$, l'équation $2\mathrm{Q} = \mathrm{P}$ a toujours des solutions; combien en a-t-elle?

6.e. Montrer que, si $y_1 + y_2 \neq 0$, et si z_1 tend vers y_1 et z_2 tend vers y_2, alors $y(\mathrm{P}(z_1) + \mathrm{P}(z_2))$ tend vers $y(\mathrm{P}(y_1) + \mathrm{P}(y_2))$. Que se passe-t-il si $y_1 + y_2 = 0$?

III

Dans les questions **1.b**, **2.b** et **4**, les formules que l'on cherche à établir vont par groupe; dans chaque groupe, on démontrera la formule qui n'est pas entre crochets, et on admettra les autres.

1. Soient $\mathrm{P}_1 = (x_1, y_1)$ et $\mathrm{P}_2 = (x_2, y_2)$ deux éléments de C, avec $x_1 \neq x_2$, et soit $\mathrm{P}_3 = (x_3, y_3) \in \mathrm{C}$ défini par $\mathrm{P}_1 + \mathrm{P}_2 + \mathrm{P}_3 = \infty$.

1.a. Montrer que x_1, x_2, x_3 sont les racines du polynôme

$$\mathrm{P}(x) = x^3 - \mathrm{D}^2 x - \Big(y_1 + \frac{y_2 - y_1}{x_2 - x_1}(x - x_1)\Big)^2.$$

En déduire que l'on a

$$x_3 = \big(\frac{x_1^2 + x_1 x_2 + x_2^2 - \mathrm{D}^2}{y_1 + y_2}\big)^2 - x_1 - x_2 \quad \text{et} \quad y_3 = \frac{x_1^2 + x_1 x_2 + x_2^2 - \mathrm{D}^2}{y_1 + y_2}(x_3 - x_1) + y_1.$$

(On commencera par supposer que P_1, P_2 et P_3 sont distincts.)

1.b. Établir les formules (la formule entre crochets sera admise sans démonstration):

$$(x_1 + \mathrm{D})(x_2 + \mathrm{D})(x_3 + \mathrm{D}) = \Big(\frac{(x_1 + \mathrm{D})y_2 - (x_2 + \mathrm{D})y_1}{x_2 - x_1}\Big)^2$$
$$\Big[x_1 x_2 x_3 = \Big(\frac{x_1 y_2 - x_2 y_1}{x_2 - x_1}\Big)^2\Big].$$

2. Soit $\mathrm{P} = (x, y) \in \mathrm{C}$, avec $y \neq 0$ et $2\mathrm{P} = (x', y')$.

2.a. Établir les formules :

$$x' = \big(\frac{3x^2 - \mathrm{D}^2}{2y}\big)^2 - 2x \quad \text{et} \quad -y' = \frac{3x^2 - \mathrm{D}^2}{2y}(x' - x) + y.$$

2.b. Montrer que l'on a $x' = \big(\frac{x^2 + \mathrm{D}^2}{2y}\big)^2$. On admettra que, de même,

$$\Big[x' + \mathrm{D} = \Big(\frac{x^2 + 2\mathrm{D}x - \mathrm{D}^2}{2y}\Big)^2 \quad \text{et} \quad x' - \mathrm{D} = \Big(\frac{x^2 - 2\mathrm{D}x - \mathrm{D}^2}{2y}\Big)^2\Big].$$

3. Montrer que $\overline{\mathrm{C}}(\mathbf{Q})$ est un sous-groupe de $\overline{\mathrm{C}}$.

4. Soient $\mathrm{P}_1 = (x_1, y_1)$ et $\mathrm{P}_2 = (x_2, y_2)$ deux éléments de $\mathrm{C}(\mathbf{Q})$, avec $x_1 \neq x_2$, et soient $\mathrm{P}_3 = \mathrm{P}_1 + \mathrm{P}_2 = (x_3, y_3)$ et $\mathrm{P}_4 = \mathrm{P}_1 - \mathrm{P}_2 = (x_4, y_4)$. Établir les formules (la formule entre crochets sera admise sans démonstration):

$$(x_3 + \mathrm{D})(x_4 + \mathrm{D}) = \Big(\frac{x_1x_2 + \mathrm{D}(x_1 + x_2) - \mathrm{D}^2}{x_2 - x_1}\Big)^2 \quad \text{et} \quad \Big[x_3x_4 = \Big(\frac{x_1x_2 + \mathrm{D}^2}{x_2 - x_1}\Big)^2\Big].$$

IV

IV. A

1. Si p est un nombre premier et $a \in \mathbf{Z} - \{0\}$, on définit l'entier $v_p(a)$ comme le plus grand entier n tel que p^n divise a (par exemple $48 = 3 \cdot 2^4$ et donc $v_2(48) = 4$, $v_3(48) = 1$ et $v_p(48) = 0$ si $p \notin \{2, 3\}$). On a $v_p(ab) = v_p(a) + v_p(b)$, ce qui permet d'étendre v_p à $\mathbf{Q}^*$ grâce à la formule $v_p(ab^{-1}) = v_p(a) - v_p(b)$. Si $a \in \mathbf{Q}^*$, alors $v_p(a) = 0$ sauf pour un nombre fini de nombres premiers p et, si a est positif, alors $a = \prod_p p^{v_p(a)}$. Si $v \in \mathbf{Z}$, on note $\overline{v}$ son image dans $\mathbf{Z}/2\mathbf{Z}$.

1.a. Montrer que $a \in \mathbf{Q}^*$ est un carré si et seulement si $a > 0$ et $\overline{v_p(a)} = 0$ quel que soit le nombre premier p.

1.b. Montrer que, si $a, b \in \mathbf{Q}^*$ vérifient $v_p(a) < v_p(b)$, alors $v_p(a + b) = v_p(a)$.

2. Soit $\mathrm{P} = (x, y) \in \mathrm{C}(\mathbf{Q})$, et soit $c \in \{1, 4, 9, 16, \ldots\}$ le plus petit carré (d'entier) tel que $a = cx \in \mathbf{Z}$.

2.a. Montrer que, si $v_p(c) \geq 1$, alors $v_p(c) \geq 2$ et $v_p(a) \in \{0, 1\}$.

2.b. Montrer que $a(a - \mathrm{D}c)(a + \mathrm{D}c)$ est un carré.

2.c. Montrer que, si $p \notin \mathrm{S} \cup \{2\}$, alors $v_p(a)$ et $v_p(a + \mathrm{D}c)$ sont des nombres pairs.

3. Soit $\varphi : \overline{\mathrm{C}}(\mathbf{Q}) \to (\mathbf{Z}/2\mathbf{Z})^{2s+2}$ l'application qui envoie ∞ sur $(0, \ldots, 0)$ et $\mathrm{P} = (x, y)$ sur

$$(\overline{v_2(x)}, \overline{v_{p_1}(x)}, \ldots, \overline{v_{p_s}(x)}, \overline{v_2(x + \mathrm{D})}, \overline{v_{p_1}(x + \mathrm{D})}, \ldots, \overline{v_{p_s}(x + \mathrm{D})}).$$

3.a. Montrer que φ est un morphisme de groupes de $\overline{\mathrm{C}}(\mathbf{Q})$ dans $(\mathbf{Z}/2\mathbf{Z})^{2s+2}$.

3.b. Montrer que, si $\mathrm{P} = (x', y') \in \mathrm{C}(\mathbf{Q})$ est tel que x', $x' - \mathrm{D}$ et $x' + \mathrm{D}$ sont des carrés dans $\mathbf{Q}$, et si $\mathrm{Q} \in \mathrm{C}$ est une solution de l'équation $2\mathrm{Q} = \mathrm{P}$, alors $\mathrm{Q} \in \mathrm{C}(\mathbf{Q})$.

3.c. Caractériser le noyau de φ.

3.d. Montrer que $\overline{\mathrm{C}}(\mathbf{Q})$ est de type fini modulo 2.

IV. B

IV. B

On définit une fonction $h : \overline{\mathrm{C}}(\mathbf{Q}) \to \mathbf{R}_+$ en envoyant ∞ sur 0 et $\mathrm{P} = (x, y)$ sur $\log(a + \mathrm{D}c) = \log(c(x + \mathrm{D}))$, si c est le plus petit carré rendant $a = cx$ entier.

1. Montrer que, quel que soit $\mathrm{P} \in \overline{\mathrm{C}}(\mathbf{Q})$, on a

$$h(2\mathrm{P}) \leq 4h(\mathrm{P}).$$

2. Soient $\mathrm{P}_1 = (x_1, y_1)$ et $\mathrm{P}_2 = (x_2, y_2)$ deux éléments de $\mathrm{C}(\mathbf{Q})$, avec $x_1 \neq x_2$, et soient $\mathrm{P}_3 = \mathrm{P}_1 + \mathrm{P}_2 = (x_3, y_3)$ et $\mathrm{P}_4 = \mathrm{P}_1 - \mathrm{P}_2 = (x_4, y_4)$. Soit c_1 (resp. c_2) le plus petit carré rendant $a_1 = c_1 x_1$ (resp. $a_2 = c_2 x_2$) entier.

2.a. Montrer que, si d divise $\mathrm{T} = a_1 a_2 + \mathrm{D}^2 c_1 c_2$, $\mathrm{U} = a_1 a_2 - \mathrm{D}^2 c_1 c_2 + \mathrm{D}(a_1 c_2 + a_2 c_1)$ et $\mathrm{V} = a_1 c_2 - a_2 c_1$, alors d divise aussi $2a_1(a_2 + \mathrm{D}c_2)$ et $2a_2(a_1 + \mathrm{D}c_1)$ ainsi que $4\mathrm{D}^2 a_1 c_2^2$ et $4\mathrm{D}^2 a_2 c_1^2$.

2.b. Montrer que, si $p \notin \mathrm{S} \cup \{2\}$, alors p ne divise pas $4\mathrm{D}^2 a_1 c_2^2$, $4\mathrm{D}^2 a_2 c_1^2$ ou $a_1 a_2 + \mathrm{D}^2 c_1 c_2$ (on commencera par montrer que p ne divise ni le p.g.c.d. de a_1 et c_1, ni celui de a_2 et c_2).

2.c. Montrer que, si $p \in \mathrm{S} \cup \{2\}$, alors p^4 ne divise pas $4\mathrm{D}^2 a_1 c_2^2$, $4\mathrm{D}^2 a_2 c_1^2$ ou $a_1 a_2 + \mathrm{D}^2 c_1 c_2$.

2.d. Montrer que le p.g.c.d. de $a_1 a_2 + \mathrm{D}^2 c_1 c_2$, $a_1 a_2 - \mathrm{D}^2 c_1 c_2 + \mathrm{D}(a_1 c_2 + a_2 c_1)$ et $a_1 c_2 - a_2 c_1$ divise $(2\mathrm{D})^3$.

2.e. Montrer que, si $x_3 x_4 = \frac{d}{e}$ et $(x_3 + \mathrm{D})(x_4 + \mathrm{D}) = \frac{d'}{e}$, où d, d' et e sont des entiers, si c_3 (resp. c_4) est le plus petit carré rendant $a_3 = c_3 x_3$ (resp. $a_4 = c_4 x_4$) entier, et si $\delta = \text{p.g.c.d.}(d, d', e)$, alors $\frac{c_3 c_4 \delta}{e}$ est entier et $h(\mathrm{P}_3) + h(\mathrm{P}_4) \geq \log d' - \log \delta$.

2.f. Montrer que, quels que soient $(\mathrm{P}_1, \mathrm{P}_2) \in \mathrm{C}(\mathbf{Q})^2$ avec $\mathrm{P}_1 \pm \mathrm{P}_2 \neq \infty$, on a

$$h(\mathrm{P}_1 + \mathrm{P}_2) + h(\mathrm{P}_1 - \mathrm{P}_2) \geq 2(h(\mathrm{P}_1) + h(\mathrm{P}_2)) - 2\log(2(2\mathrm{D})^3).$$

3. On suppose dorénavant que le groupe $\overline{\mathrm{C}}(\mathbf{Q})$ est infini.

3.a. Montrer que les seules solutions de l'équation $2\mathrm{P} = \infty$ sont $\mathrm{P} = \infty$ et $\mathrm{P} = (\mathrm{D}, 0)$.

3.b. Montrer que $h(2\mathrm{P}) \geq 4h(\mathrm{P}) - 6\log(2(2\mathrm{D})^3)$ quel que soit $\mathrm{P} \in \overline{\mathrm{C}}(\mathbf{Q})$.

3.c. Montrer qu'il existe $\mathrm{A} > 0$ tel que, quels que soient $(\mathrm{P}, \mathrm{Q}) \in \overline{\mathrm{C}}(\mathbf{Q})^2$, on ait

$$h(\mathrm{P} + \mathrm{Q}) + h(\mathrm{P} - \mathrm{Q}) \geq 2(h(\mathrm{P}) + h(\mathrm{Q})) - \mathrm{A}.$$

3.d. Montrer que h est une hauteur sur $\overline{\mathrm{C}}(\mathbf{Q})$.

3.e. Montrer que h est une hauteur admissible sur $\overline{\mathrm{C}}(\mathbf{Q})$.

3.f. Montrer que $\overline{\mathrm{C}}(\mathbf{Q})_{\mathrm{tors}}$ est un groupe fini et que $\overline{\mathrm{C}}(\mathbf{Q})$ est de type fini.