Courbes elliptiques
Cours de M2, mathématiques fondamentales
Université Paris Diderot Paris 7
Marc Hindry (cours), Dominique Bernardi (TD)

UN CORRIGÉ DE L'EXAMEN DU 6 JANVIER 2016

1. Exercice 1

On considère deux courbes elliptiques et une isogénie $\phi : E_1 \to E_2$ toutes définies sur un corps K.

(1) Posons $D_\phi := \phi^*(0_{E_2}) - \deg(\phi)(0_{E_1})$. Montrer que $2D_\phi$ est un diviseur principal. Est-il toujours vrai que D_ϕ est principal?

(2) On suppose maintenant que K est un corps de nombres, et on note $\hat{h}$ la hauteur de Néron-Tate sur E_1 ou E_2; montrer que

$$\hat{h}(\phi(P)) = \deg(\phi)\hat{h}(P).$$

(3) On choisit $E = E_1 = E_2$ définie par $y^2 = x^3 + x$ sur le corps $K = \mathbb{Q}(i)$. Montrer que

$$\phi(x, y) := (-x, iy)$$

est un automorphisme de E. En déduire que $\mathrm{End}(E) = \mathbb{Z}[i]$.
En considérant l'isogénie $\psi := 1 + \phi$ (i.e. $\psi(P) = P + \phi(P)$), dont on déterminera le degré, montrer que les points P et $\phi(P)$ sont orthogonaux pour l'accouplement de Néron-Tate.

Solution

(1) Un diviseur $D = \sum n_P(P)$ est principal si et seulement si $\deg(D) = \sum n_P = 0$ et $\sum n_p P = 0 \in E$. Ici nous avons $\deg(\phi^*(O_{E_2})) = \deg(\phi)$ donc $\deg D_\phi = 0$. Ensuite en notant $G := \mathrm{Ker}\,\phi$ le groupe des points dans le noyau et e l'indice d'inséparabilité de ϕ on a $\phi^*(O_{E_2}) = e\sum_{P\in G}(P)$. Par ailleurs $2\sum_{P\in G} P = \sum_{P\in G}(P - P) = 0$ donc $2D_\phi$ est principal. Il n'est pas vrai en général que D_ϕ soit principal; en effet si T est un point d'ordre deux et $G = \{O_{E_1}, T\}$ alors $\sum_{P\in G} = T \neq 0$. De manière générale, $\sum_{P\in G} P = 0$ sauf si G est cyclique d'ordre pair.

(2) On utilise la relation de diviseur $2D_\phi = 2\phi^*(0_{E_2}) - 2\deg(\phi)(0_{E_1}) = \mathrm{div}(f)$ (avec la fonction rationnelle f dont l'existence est assurée par la question précédente) et on utilise les propriétés des hauteurs.

$$2h_{\phi^*(0_{E_2})}(P) - 2\deg(\phi)h_{0_{E_1}}(P) = h_{\mathrm{div}(f)}(P) = O(1)$$

Par ailleurs $h_{\phi^*(0_{E_2})}(P) = h_{0_{E_2}}(\phi((P))$ et on obtient donc

$$h_{0_{E_2}}(\phi((P)) - \deg(\phi)h_{0_{E_1}}(P) = O(1)$$

En appliquant cette dernière formule à $2^n P$ on en tire l'égalité voulue:

$$\hat{h}(\phi(P)) = \lim \frac{h_{0_{E_2}}(\phi(2^n P))}{4^n} = \deg(\phi)\lim \frac{h_{0_{E_1}}(2^n P)}{4^n} = \deg(\phi)\hat{h}(P).$$

(3) Comme ϕ est définie par des polynômes, elle donne une application rationnelle, qui se prolonge en un morphisme de E (courbe lisse) vers son image (courbe projective). Il est clair que ϕ laisse stable E et envoie le point à l'infini sur le point à l'infini, c'est donc un endomorphisme de E. Définissons $\phi'(x,y) = (-x, -iy)$, c'est aussi un endomorphisme de E et $\phi \circ \phi' = id$ donc ϕ est un automorphisme de E; de façon équivalente, on peut aussi vérifier que $\phi \circ \phi(x,y) = (x,-y) = [-1](x,y)$, ou encore $\phi^2 = [-1]$. On en déduit un homomorphisme d'anneaux $\mathbb{Z}[i] \to \mathrm{End}(E)$ défini par $m + ni \mapsto [m] + [n] \circ \phi$, qui est injectif (si $[m] + [n] \circ \phi = 0$ on aurait $[m^2] = [-n^2]$ donc $m^2 = -n^2$ et donc $m = n = 0$).
Remarquons que $\phi \circ \phi' = [1] = [\deg \phi]$ signifie que ϕ' est l'isogénie duale $\hat{\phi}$ donc $\hat{\psi} = \widehat{1+\phi} = \hat{1} + \hat{\phi} = 1 - \phi$ et $[\deg \psi] = \psi \circ \hat{\psi} = (1+\phi)(1-\phi) = 1 - \phi^2 = 2$, c'est-à-dire $\deg(\psi) = 2$. [On pouvait aussi calculer le noyau de ψ en prouvant que $\mathrm{Ker}\,\psi = \{0_E, (0,0)\}$ pour conclure que $\deg(\psi) = 2$.]
On en tire le calcul du produit scalaire suivant:
$2 < P, \phi(P) >= \hat{h}(P+\phi(P)) - \hat{h}(P) - \hat{h}(\phi(P)) = 2\hat{h}(P) - \hat{h}(P) - \hat{h}(P) = 0$.

2. Exercice 2

Soit p premier impair[1]. On considère la courbe elliptique E sur $\mathbb{F}_p$ d'équation

$$y^2 = x^3 + x = f(x)$$

(1) Soit $\left(\frac{u}{p}\right)$ le symbole de Legendre (qui vaut 0 pour $u = 0$, vaut $+1$ si u est un carré non nul et -1 si u n'est pas un carré). Rappeler pourquoi

$$|E(\mathbb{F}_p)| = p + 1 + S, \text{ avec } S := \sum_{x \in \mathbb{F}_p} \left(\frac{f(x)}{p}\right) \equiv -A_p \mod p$$

où A_p est le coefficient de x^{p-1} dans $f(x)^{(p-1)/2}$.

(2) Montrer que E est supersingulière (resp. ordinaire) si $p \equiv 3 \mod 4$ (resp. si $p \equiv 1 \mod 4$). En déduire que, si $p \equiv 3 \mod 4$, alors $|E(\mathbb{F}_p)| = p + 1$ et, en particulier, $|E(\mathbb{F}_p)| \equiv 0 \mod 4$.

(3) Si $p \equiv 1 \mod 4$ montrer que $E[2] \subset E(\mathbb{F}_p)$ et en déduire $|E(\mathbb{F}_p)| \equiv 0 \mod 4$.

(4) On admet (voir exercice 1) que l'anneau des endomorphismes de $E/\mathbb{Q}(i)$ est $\mathbb{Z}[i]$. En déduire que, lorsque $p \equiv 1 \mod 4$, l'anneau des endomorphismes de $E/\mathbb{F}_p$ est $\mathbb{Z}[i]$. [Indication: on utilisera, en le justifiant, le fait que l'homomorphisme de réduction $\mathrm{End}(E/\mathbb{Q}(i)) \to \mathrm{End}(E/\mathbb{F}_p)$ est injectif.]

(5) Soit Fr_p le Frobenius de $E/\mathbb{F}_p$, montrer qu'il s'identifie à $a + bi \in \mathbb{Z}[i] = \mathrm{End}(E)$ tel que $a^2 + b^2 = p$, avec a impair et $|E(\mathbb{F}_p)| = p + 1 - 2a$.

(6) Les conditions $p = a^2 + b^2$ et a impair déterminent a au signe près, pouvez-vous déterminer a, en spécifiant, par exemple, $a \mod 4$?

Solution

(1) Posons $f(x) = x^3 + x$. On sait que $1 + \left(\frac{u}{p}\right) = N(u)$ où $N(u)$ est le nombre de solutions dans $\mathbb{F}_p$ de $y^2 = u$. En tenant compte du point à l'infini, on a

[1] Rappel de théorie algébrique des nombres : un tel p est somme de deux carrés si et seulement si $p \equiv 1 \mod 4$ et si et seulement si p est décomposé dans l'extension quadratique $\mathbb{Q}(i)/\mathbb{Q}$

donc

$$|E(\mathbb{F}_p)| = 1 + \sum_{x\in\mathbb{F}_p} N(f(x)) = p + 1 + S, \text{ avec } S := \sum_{x\in\mathbb{F}_p} \left(\frac{f(x)}{p}\right)$$

Maintenant comme $\left(\frac{u}{p}\right) \equiv u^{(p-1)/2} \mod p$, on a que $S \equiv \sum_{x\in\mathbb{F}_p} f(x)^{(p-1)/2}$ et, en utilisant le fait que $\sum_{x\in\mathbb{F}_p} x^j = 0$ sauf si $j \neq 0$ et $p-1$ divise j (auquel cas la somme vaut -1), on vérifie que $S \equiv -A_p \mod p$, où A_p désigne le coefficient de x^{p-1} dans $f(x)^{(p-1)/2}$. [C'était essentiellement un question de cours.]

(2) On calcule

$$f(x)^{(p-1)/2} = x^{(p-1)/2}(x^2+1)^{(p-1)/2} = x^{(p-1)/2} \sum_{h=0}^{(p-1)/2} \binom{(p-1)/2}{j} x^{2j}$$

Lorsque $p \equiv 3 \mod 4$, il n'y a pas de terme en x^{p-1}, c'est-à-dire que le coefficient de x^{p-1} est nul; lorsque $p \equiv 1 \mod 4$ le coefficient de x^{p-1} est $\binom{(p-1)/2}{(p-1)/4} \not\equiv 0 \mod p$. On sait que E est supersingulière (resp. ordinaire) si et seulement si $A_p \equiv 0 \mod p$ (resp. si et seulement si $A_p \not\equiv 0 \mod p$) donc E est supersingulière (resp. ordinaire) si et seulement si $p \equiv 3 \mod 4$ (resp. si $p \equiv 1 \mod 4$). En rappelant que $|\sharp E(\mathbb{F}_p) - p - 1| \leq 2\sqrt{p}$, on voit que, dès que $p \geq 5$ la congruence $|E(\mathbb{F}_p)| \equiv p + 1 \mod p$ impose en fait $|E(\mathbb{F}_p)| = p+1$. Ainsi lorsque $p \equiv 3 \mod 4$ on obtient $|E(\mathbb{F}_p)| = p+1 \equiv 0 \mod 4$.

Pour $p = 3$ on vérifie directement que $|E(\mathbb{F}_3)| = 4$.

(3) Si $p \equiv 1 \mod 4$, alors -1 est un carré, disons $u^2 = -1$ avec $u \in \mathbb{F}_p$, et l'équation $x^3 + x = 0$ possède 3 racines 0, u et $-u$ donc

$$E[2] = \{0_E, (0,0), (u,0), (-u,0)\} \subset E(\mathbb{F}_p).$$

Par le théorème de Lagrange, on a $|E(\mathbb{F}_p)| \equiv 0 \mod 4$.

(4) Lorsque $p \equiv 1 \mod 4$, on a $p\mathbb{Z}[i] = \mathfrak{p}\bar{\mathfrak{p}}$ et $\mathbb{Z}[i]/\mathfrak{p} = \mathbb{F}_p$. On sait que l'homomorphisme de réduction $\mod \mathfrak{p}$ de $\mathrm{End}(E/\mathbb{Q}(i))$ vers $\mathrm{End}(E/\mathbb{F}_p)$ est injectif; en effet cet homomorphisme est injectif sur les points de torsion d'ordre premier à p (alternativement ici on pouvait utiliser ici que, en notant u l'image de i dans $\mathbb{Z}[i]/\mathfrak{p}$, l'endomorphisme $(x,y) \mapsto (-x, uy)$ est l'image de ϕ défini dans l'exercice 1.3 et conclure). On a donc $\mathbb{Z}[i] \hookrightarrow \mathrm{End}(E/\mathbb{F}_p)$, mais, comme $E/\mathbb{F}_p$ est ordinaire on sait que ou bien $\mathrm{End}(E/\mathbb{F}_p) = \mathbb{Z}$ (impossible ici), ou bien $\mathrm{End}(E/\mathbb{F}_p)$ est un ordre dans l'anneau des entiers d'un corps quadratique imaginaire, donc un ordre dans $\mathbb{Z}[i]$ et doit donc être égal à ce dernier.

(5) Soit Fr_p le Frobenius de $E/\mathbb{F}_p$, c'est un élément de $\mathrm{End}(E/\mathbb{F}_p)$ donc, d'après la question précédente, il s'identifie à un élément $a+bi \in \mathbb{Z}[i] = \mathrm{End}(E)$. On a alors $\hat{\mathrm{Fr}}_p = a - bi$ et donc $p = \deg(\mathrm{Fr}_p) = \mathrm{Fr}_p\hat{\mathrm{Fr}}_p = \deg(a+bi) = a^2 + b^2$ et $\mathrm{Fr}_p + \hat{\mathrm{Fr}}_p = 2a$ donc $|E(\mathbb{F}_p)| = p + 1 - (\mathrm{Fr}_p + \hat{\mathrm{Fr}}_p) = p + 1 - 2a$. Enfin $|E(\mathbb{F}_p)| \equiv 0 \mod 4$ donc $0 \equiv p + 1 - 2a \equiv 2 - 2a \mod 4$ et ainsi a doit être impair.

(6) Cette question était difficile, d'autant plus qu'elle était formulée de manière ouverte. Une réponse simple est que l'on a toujours $a \equiv 1 \mod 4$. Il existe une théorie associant un "caractère de Hecke" à notre situation impliquant

une courbe elliptique à multiplication complexe, mais cela nous entraînerait loin. Voilà donc une solution plus élémentaire qui consiste à prouver directement le lemme suivant (observons que, comme on étudie le cas $p \equiv 1 \mod 4$, on a forcément $p \equiv 1$ ou 5 modulo 4):

Lemme *Soit N_p le cardinal de $E(\mathbb{F}_p)$. Si $p \equiv 1 \mod 8$ alors $N_p \equiv 0 \mod 8$; si $p \equiv 5 \mod 8$ alors $N_p \equiv 4 \mod 8$.*

Une fois prouvé le lemme on observe que, dans le premier cas, on obtient $0 \equiv N_p \equiv 2 - 2a \mod 8$ donc $a \equiv 1 \mod 4$, alors que, dans le deuxième cas, on en tire $4 \equiv N_p \equiv 6 - 2a \mod 8$ et donc on a encore $a \equiv 1 \mod 4$.

Pour prouver le lemme il faut voir quand l'un des points d'ordre deux $T_0 = (0,0)$, $T_1 = (u,0)$, $T_2 = (-u,0)$ (avec $u^2 = -1$) est le double d'un point de $E(\mathbb{F}_p)$. Soit donc v tel que $v^2 = 2$; notons que, si $p \equiv 1 \mod 8$ (resp. $p \equiv 5 \mod 8$) on a $\left(\frac{2}{p}\right) = +1$ et donc $v \in \mathbb{F}_p$ (resp. $\left(\frac{2}{p}\right) = -1$ et $v \notin \mathbb{F}_p$). Posons $Q = (1, v)$ alors $Q \in E$ et $x(2Q) = 0$ donc T_0 est divisible par 2 dans $E(\mathbb{F}_p)$ (resp. ne l'est pas) si $p \equiv 1 \mod 8$ (resp. si $p \equiv 5 \mod 8$). Récrivons la formule de duplication $x(2Q) = (\frac{3x^2+1}{2y})^2 - 2x = u$. En utilisant $y^2 = x^3 + x$ cela se transforme en $x^4 - 4x^3 - 2x^2 - 4ux + 1 = (x^2 - 2ax + 1) = 0$; or l'équation $x^2 - 2ux + 1 = 0$ a ses racines dans $\mathbb{F}_p$ si et seulement si $u^2 - 1 = -2$ est un carré, c'est-à-dire ici si $p \equiv 1 \mod 8$. AInsi, lorsque $p \equiv 5 \mod 8$, il n'y a pas d'élément d'ordre 4 dans $E(\mathbb{F}_p)$ donc $N_p = 4 \times (\text{impair}) \equiv 4 \mod 8$.

Remarque. Dans notre cas $f(x) = x^3 + x$ est impair donc, si on note U l'ensemble des classes modulo p des $x \in [1, (p-1)/2]$ on peut écrire

$$S := \sum_{x \in \mathbb{F}_p} \left(\frac{f(x)}{p}\right) = \sum_{x \in U} \left(\frac{f(x)}{p}\right) + \left(\frac{-f(x)}{p}\right) = \left(1 + \left(\frac{-1}{p}\right)\right) \sum_{x \in U} \left(\frac{f(x)}{p}\right)$$

On retrouve ainsi directement que $S = 0$ lorsque $p \equiv 3 \mod 4$ et, lorsque $p \equiv 1 \mod 4$, on trouve une autre expression de a tel que $N_p = p + 1 - 2a$ comme $a = -\sum_{x \in U} \left(\frac{f(x)}{p}\right)$. Le nombre de termes de la somme est pair, car égal à $(p-1)/2$ mais l'un des termes est nul (correspondant à $x = u$ ou $x = -u$, mais un seul!) donc on retrouve que a est impair.

3. Exercice 3

On se propose d'étudier quelques propriétés de la courbe elliptique E, dont on note 0_E l'origine et dont la partie affine est définie sur $\mathbb{Q}$ par l'équation

$$y^2 + y = x^3 - 4x$$

(1) Vérifier que les points $P_1 = (0,0)$, $P_2 = (2,0)$ et $P_3 = (-2,0)$ appartiennent à $E(\mathbb{Q})$ et que $P_1 + P_2 + P_3 = 0_E$.
(2) Montrer que E a bonne réduction pour $p = 2, 3, 5$ [en fait hors de $p = 13$ et 313] et $\tilde{E}_2(\mathbb{F}_2) \cong \mathbb{Z}/3\mathbb{Z}$, $\tilde{E}_3(\mathbb{F}_3) \cong \mathbb{Z}/7\mathbb{Z}$.
(3) Montrer que le cardinal de $\tilde{E}_5(\mathbb{F}_5)$ est égal à 9. A-ton $\tilde{E}_5(\mathbb{F}_5) \cong \mathbb{Z}/9\mathbb{Z}$ ou $\tilde{E}_5(\mathbb{F}_5) \cong (\mathbb{Z}/3\mathbb{Z})^2$? [Mes excuses : il y avait une erreur dans l'énoncé qui affirmait que le cardinal était 8!]
(4) En déduire que $E(\mathbb{Q})_{\text{tor}} = \{0_E\}$ et $E(\mathbb{Q}) \cong \mathbb{Z}^r$ avec $r \geq 1$.
(5) Montrer que $E(\mathbb{R})$ possède deux composantes connexes : la composante neutre qu'on notera $\mathcal{C}_0$ et l'autre compacte dans le plan affine $\mathbb{R}^2$ qu'on

notera $\mathcal{C}_1$. Vérifier que P_1 et P_3 sont dans $\mathcal{C}_1$ (resp. P_2 dans $\mathcal{C}_0$). En déduire que P_1, P_3 n'appartiennent pas à $2E(\mathbb{Q})$.

(6) En utilisant la formule de duplication (que l'on justifiera):

$$x(2P) = \left(\frac{3x^2(P)-4}{2y(P)+1}\right)^2 - 2x(P),$$

montrer que P_2 n'appartient pas à $2E(\mathbb{Q})$. [Indication : on pourra montrer que si $2P = P_2$ alors P est à coordonnées entières, avec $x(P)$ pair et considérer les valuations 2-adiques.]

(7) Conclure que P_1, P_2, P_3 engendrent un groupe isomorphe à $\mathbb{Z}^2$. [Nota : en fait ces points engendrent $E(\mathbb{Q})$ qui est donc de rang 2 – ce que l'on ne demande pas de démontrer.]

Solution

(1) Il est immédiat que les points $P_1 = (0,0)$, $P_2 = (2,0)$ et $P_3 = (-2,0)$ appartiennent à $E(\mathbb{Q})$; par ailleurs ils sont alignés car il sont tous les trois sur la droite d'équation $y = 0$, donc on a bien $P_1 + P_2 + P_3 = 0_E$.

(2) On peut calculer le discriminant $\Delta = 64 \cdot 2^6 - 27 = 13 \cdot 313$ et conclure que E a bonne réduction hors de $p = 13$ ou 313. Alternativement on pouvait écrire les équations d'un point singulier $2y + 1 = 3x^2 - 4 = 0$, qui donnent immédiatement la bonne réduction en $p = 2$ ou 3 et, pour $p = 5$, noter que cela impose $y = 2$ et $x^2 = 3$ donc $y^2 + y = 1 = x^3 - 4x = -x$ mais $(-1)^2 \neq 3$. Un calcul direct donne
$\tilde{E}_2(\mathbb{F}_2) = \{0_E, (0,0), (0,-1)\}$
$\tilde{E}_3(\mathbb{F}_3) = \{0_E, (0,0), (0,-1)(1,0)(1,-1), (-1,0), (-1,-1)\}$
donc $\tilde{E}_2(\mathbb{F}_2) \cong \mathbb{Z}/3\mathbb{Z}$, $\tilde{E}_3(\mathbb{F}_3) \cong \mathbb{Z}/7\mathbb{Z}$.

(3) De même on vérifie que [De nouveau, mes excuses pour l'erreur dans l'énoncé initial, il y a neuf points et non huit!]
$\tilde{E}_5(\mathbb{F}_5) = \{0_E, (0,0), (0,-1), (1,1)(1,-2), (2,0), (2,-1), (-2,0), (-2,-1)\}$
A priori ce groupe de cardinal 9 est isomorphe à $(\mathbb{Z}/3\mathbb{Z})^2$ ou $\mathbb{Z}/9\mathbb{Z}$. Un point P est d'ordre trois si $3P = 0$ donc si c'est un point d'inflexion; la tangente au point $P = (0,0)$ s'écrit $y = -4x = x$ et le troisième point d'intersection est $(1,1)$, donc P n'est pas d'ordre 3 et $\tilde{E}_5(\mathbb{F}_5) \cong \mathbb{Z}/9\mathbb{Z}$. Alternativement, en invoquant le pairing de Weil, on voit que si $(\mathbb{Z}/3\mathbb{Z})^2 \subset E(\mathbb{F}_5)$ alors les racines troisièmes de l'unité seraient contenues dans $\mathbb{F}_5$, ce qui est faux, puisque $\mathbb{F}_5^\times$, qui est cyclique d'ordre 4, ne contient pas de sous-groupe d'ordre 3.

(4) On sait en général que la réduction modulo un idéal premier de bonne réduction est injective sur la torsion d'ordre premier à la caractéristique résiduelle. Le lemme de Cassels, dans le cas $E/\mathbb{Q}$ est plus précis et indique que le noyau de la réduction ne contient aucun point de torsion, sauf éventuellement un point d'ordre 2 pour $p = 2$. Comme $\tilde{E}_2(\mathbb{F}_2) \cong \mathbb{Z}/3\mathbb{Z}$, on en tire que $E(\mathbb{Q})_{\text{tor}}$ est un sous-groupe de $\mathbb{Z}/6\mathbb{Z}$; comme $\tilde{E}_3(\mathbb{F}_3) \cong \mathbb{Z}/7\mathbb{Z}$, on en tire que $E(\mathbb{Q})_{\text{tor}}$ est un sous-groupe de $\mathbb{Z}/7\mathbb{Z}$, et donc $E(\mathbb{Q})_{\text{tor}} = \{0_E\}$ et $E(\mathbb{Q}) \cong \mathbb{Z}^r$. De plus $E(\mathbb{Q}) \neq \{0\}$ donc $r \geq 1$ (les points P_1, P_2 et P_3 sont tous d'ordre infini).

(5) En récrivant l'équation de E sous la forme $(y + \frac{1}{2})^2 = x^3 - 4x + \frac{1}{4} = g(x)$ et en vérifiant que le polynôme membre de droite possède trois racines réelles $\alpha_1 < \alpha_2 < \alpha_3$, il est immédiat que $E(\mathbb{R})$ possède deux composantes réelles

$\mathcal{C}_1$ et $\mathcal{C}_0$ correspondant respectivement à $x \in [\alpha_1, \alpha_2]$ et $x \in [\alpha_3, +\infty]$. Comme $\alpha_1 < -2 < 0 < \alpha_2$ et $\alpha_3 < 2$ on voit que $P_1, P_3 \in \mathcal{C}_1$ et $P_2 \in \mathcal{C}_0$. Notons que, comme le groupe des composantes est de cardinal 2, on a $2E(\mathbb{R}) \subset \mathcal{C}_0$ et donc P_1 et P_3 ne sont pas des doubles dans $E(\mathbb{R})$ et a fortiori dans $E(\mathbb{Q})$.

(6) La formule de duplication s'écrit:

$$x(2P) = \left(\frac{3x^2(P) - 4}{2y(P) + 1}\right)^2 - 2x(P),$$

En effet la tangente au point P a pour équation $(2y(P) + 1)(y - y(P)) = (3x(P)^2 - 4)(x - x(P))$. S'il existait un point P tel que $P_2 = 2P$ alors P est à coordonnées entières [si P non entier en un premier p, il est dans le noyau de la réduction modulo p et donc ses multiples également.] On a donc que $2y(P) + 1$ est impair et divise $3x^2(P) - 4$ qui doit être pair et donc $x(P)$ est pair. Mais alors 4 divise $(\frac{3x^2(P)-4}{2y(P)+1})^2$ et donc $2 - 2x(P)$ qui est congru à 2 modulo 4, contradiction.

(7) Les points P_1 et P_2 engendrent le même groupe G que P_1, P_2, P_3; ils tous deux d'ordre infini et G est sans torsion, donc ou bien les points sont indépendants et engendrent un groupe isomorphe à $\mathbb{Z}^2$, ou bien ils sont liés et $G \cong \mathbb{Z}$. Mais on vient de voir que les points $0, P_1, P_3$ et $P_1 + P_3 = -P_2$ ne sont pas des doubles et sont donc distincts modulo $2E(\mathbb{Q})$ et donc $|G/2G| \geq 4$ et $G \cong \mathbb{Z}^2$.