Werk

Titel: Points s-entiers des courbes elliptiques.

Autor: Ayad, Mohamed

Jahr: 1992

PURL: https://resolver.sub.uni-goettingen.de/purl?365956996_0076|log26

Kontakt/Contact

Digizeitschriften e.V.
SUB Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen

info@digizeitschriften.de

manuscripta math. 76, 305 - 324 (1992)

manuscripta
mathematica
© Springer-Verlag 1992

POINTS S-ENTIERS DES COURBES ELLIPTIQUES

Mohamed AYAD

Consider an elliptic curve defined over $\mathbb{Q}$ by a generalized weierstrass equation :

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \ ; \ a_i \in \mathbb{Z}$$

Let $M = \left(\frac{a}{d^2}, \frac{b}{d^3}\right)$; $(a,d) = 1$, be a rational point on the curve, m an integer and S a finite set of rational primes ; then the point mM is given by

$$mM = \left(\frac{\phi_m(M)}{\psi_m^2(M)}, \frac{\omega_m(M)}{\psi_m^3(M)}\right) = \left(\frac{\widehat{\phi}_m}{\widehat{\psi}_m^2}, \frac{\widehat{\omega}_m}{\widehat{\psi}_m^3}\right)$$

where $\phi_m, \psi_m, \omega_m \in \mathbb{Z}[a_1, \cdots, a_6, x, y]$ and $\widehat{\phi}_m$, $\widehat{\psi}_m$, $\widehat{\omega}_m$ are obtained from these by multipling by appropriate powers of d.
We show that the common factors of $\widehat{\phi}_m$ and $d^2\widehat{\psi}_m^2$ are those primes p of bad reduction such that $M(mod\ p)$ is singular.
Under certain conditions we show that $\widehat{\psi}_{3^N n \pm 1} \equiv \pm 1 + 3^N n (mod\ 3^{N+1})$.
These results are used to find S-integral points on elliptic curves of rank one.

1. Présentation de la méthode

Soient K un corps, E une courbe elliptique, de discriminant Δ, définie sur K par un modèle de Weierstrass généralisé.

1.1. $$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \ ; \quad a_i \in K.$$

Soit $M = (x, y)$ un point de $E(K)$; comme dans le cas du modèle de Weierstrass court, les coordonnées de mM s'expriment sous la forme :

$$mM = \left(\frac{\phi_m(M)}{\psi_m^2(M)}; \frac{\omega_m(M)}{\psi_m^3(M)}\right)$$

où $\phi_m, \psi_m, \omega_m \in \mathbb{Z}[a_1, \cdots, a_6, x, y]$ sont des polynômes définis par récurrence voir §2. En fait ϕ_m, $\psi_m^2 \in \mathbb{Z}[a_1, \cdots, a_6, x]$ et

1.2. $$(\phi_m, \psi_m^2) = 1.$$

On peut étendre la méthode utilisée dans [1] pour montrer que le résultant des polynômes ϕ_m, ψ_m^2 vaut :

1.3. $$Res(\phi_m, \psi_m^2) = \Delta^{\frac{m^2(m^2-1)}{6}}$$

Supposons que K est un corps muni d'une valuation discrète ν et que $\nu(a_i) \geq 0$; $i = 1,2,3,4,6$; alors on a le :

Théorème A. *Soit $M \in E(K)$ tel que $M \neq \infty$. On suppose que $M(mod\ \nu) \neq \infty$, alors les propriétés suivantes sont équivalentes*
(a) $\nu(\psi_2(M))$ et $\nu(\psi_3(M)) > 0$
(b) Pour tout entier $m \geq 2, \nu(\psi_m(M)) > 0$
(c) Il existe un entier $m_0 \geq 2$ tel que $\nu(\psi_{m_0}(M))$ et $\nu(\psi_{m_0+1}(M)) > 0$
(d) Il existe un entier $n_0 \geq 2$ tel que $\nu(\psi_{n_0}(M))$ et $\nu(\phi_{n_0}(M)) > 0$
(e) $M(mod\ \nu)$ est singulier.

Preuve : voir §3.

On suppose dorénavant que $K = \mathbb{Q}$ et que $a_i \in \mathbb{Z}$; $(i = 1,2,3,4,5,6)$. (Le modèle 1.1. est supposé quelconque, pas nécessairement minimal). Dans la suite nous désignons par $M(resp\ L)$ un point rationnel d'ordre infini ($resp$ d'ordre 2) et nous recherchons les points S-entiers de la courbe 1.1. appartenant au groupe $< M >$ ($resp < L, M >$) engendré par M ($resp$ par L et M) où S est un ensemble fini (peut être vide) de nombres premiers. Dans la recherche des points S-entiers nous ferons abstraction du point à l'infini.
Le théorème de Siegel montre que l'ensemble de ces points est fini [5] IX §3.
Posons

$$M = (x, y) = \left(\frac{a}{d^2}, \frac{b}{d^3}\right) \ ; \ (a, d) = 1$$

et

$$mM = \left(\frac{\phi_m(M)}{\psi_m^2(M)}, \frac{\omega_m(M)}{\psi_m^3(M)}\right) = \left(\frac{\widehat{\phi}_m}{d^2\widehat{\psi}_m^2}, \frac{\widehat{\omega}_m}{d^3\widehat{\psi}_m^3}\right)$$

avec $\widehat{\phi}_m = d^{2m^2}\phi_m(M)$; $\widehat{\psi}_m = d^{m^2-1}\psi_m(M)$; $\widehat{\omega}_m = d^{3m^2}\omega_m(M)$ de sorte que $\widehat{\phi}_m, \widehat{\psi}_m$ et $\widehat{\omega}_m$ sont des nombres entiers.
Dans cette dernière représentation des coordonnées de mM, les facteurs premiers de d ne se simplifient pas. Nous pouvons formuler cette idée sous la forme suivante :

Lemme A *Soient $m \neq 0$ un entier rationnel, M un point rationnel de 1.1. d'ordre infini et S un ensemble fini de nombres premiers. Si mM est S-entier alors M est S-entier.*

Preuve : voir §4. Ce lemme montre que si M n'est pas S-entier alors il n'y a pas de point S-entier appartenant au groupe $< M >$.
Supposons maintenant que M est lui même S-entier.
Le théorème A montre que les facteurs premiers communs de $\widehat{\phi}_m$ et $\widehat{\psi}_m$ sont les nombres premiers p de mauvaise réduction tels que $M(mod\ p)$ est singulier. Ce même théorème montre que ces nombres premiers sont ceux divisant à la fois $\widehat{\psi}_2$ et $\widehat{\psi}_3$.

Quitte à l'élargir, si nécessaire, on peut supposer que S contient l'ensemble T de nombres premiers p de mauvaise réduction tels que $M(mod\ p)$ est singulier. Du théorème A nous déduisons le résultat suivant.

Corollaire A. *Soit* $M = \left(\frac{a}{d^2}, \frac{b}{d^3}\right)$; $(a,d) = 1$, *un point S-entier d'ordre infini de 1.1 et soit $T \subset S$ l'ensemble (peut être vide) des nombres premiers p tels que $M(mod\ p)$ est singulier. Soit $m \in \mathbb{Z}\,; m \neq 0$. Pour que mM soit S-entier il faut et il suffit que :*

$$\widehat{\psi}_m = \pm \prod_{p \in S} p^{e_p} \text{ avec } e_p \text{ entier } \geq 1 \text{ si } p \in T \text{ et } e_p \text{ entier } \geq 0 \text{ si } p \in S - T.$$

Preuve : voir §4.

On suppose maintenant que la courbe 1.1 contient un point de 2 torsion rationnel $L = (u,v) = (u, \frac{1}{2}(a_1 u + a_3))$. On sait que $u \in \mathbb{Z}$ ou $4u \in \mathbb{Z}$. [5] VII. §3.
Le but du corollaire suivant est de donner une condition nécessaire et suffisante pour que $L + mM$ soit S-entier lorque M est un point rationnel de 1.1 (pas nécessairement S-entier) et m un entier $\neq 0$.
On suppose encore que S contient les nombres premiers p tels que $M(mod\ p)$ est singulier.

Corollaire B. *Soient* $M = \left(\frac{a}{d^2}, \frac{b}{d^3}\right)$ *un point rationnel d'ordre infini et $L = (u,v)$ un point de 2-torsion sur $\mathbb{Q}$ de la courbe 1.1. Soit $T \subset S$ l'ensemble (peut être vide) des nombres premiers p tels que $M(mod\ p)$ est singulier. Soit $m \in \mathbb{Z}\,; m \neq 0$. Pour que $L + mM$ soit S-entier, il faut et il suffit que :*

$$\widehat{\phi}_m - ud^2\widehat{\psi}_m^2 = \pm \prod_{p \in S} p^{e_p} \text{ si } u \in \mathbb{Z} \text{ et}$$

$$4(\widehat{\phi}_m - ud^2\widehat{\psi}_m^2) = \pm \prod_{p \in S} p^{e_p} \text{ si } u \notin \mathbb{Z}$$

avec e_p entier ≥ 1 si $p \in T$ et e_p entier ≥ 0 si $p \in S - T$.

Preuve : Voir §4.

Avant de revenir aux points S-entiers, remarquons que les simples considérations suivantes peuvent servir de critère pour affirmer qu'un entier $q \in \mathbb{Z}$ est différent de ± 1.

Soit ℓ un nombre premier fixé et soit $q \in \mathbb{Z}$; $q \neq \pm 1$. Les propriétés suivantes sont vérifiées :

(i) Si $\ell = 2$ et si $(q,2) = 1$, alors il existe un entier $N \geq 2$ tel que :

$$q \equiv \pm 1 + 2^N (mod\ 2^{N+1})$$

(ii) Si $\ell = 3$ et si $(q,3) = 1$, alors il existe un entier $N \geq 1$ tel que :

$$q \equiv \pm 1 + a_N 3^N (mod\ 3^{N+1})\ ;\ a_N = 1, 2$$

(iii) Si $\ell > 3$ et si $(q,\ell) = 1$ alors $q \equiv \pm a_0 (mod\ \ell)$; $a_0 = 2, \ldots, \frac{\ell - 1}{2}$ où il existe un entier $N \geq 1$ tel que :

$$q \equiv \pm 1 + a_N \ell^N (mod\ \ell^{N+1})\ ;\ a_N = 1, \ldots, \ell - 1.$$

Il est évident que réciproquement, un entier q vérifiant la conclusion de (i) ou (ii) ou (iii) est différent de ± 1.
Revenons au problème des points S-entiers et soit ℓ un nombre premier. Pour tout entier $m \neq 0$, on pose $\widehat{\psi}_m = q_m \overline{\psi}_m$ avec $q_m = \Pi p^{e_p}$ est le produit des puissances des nombres pemiers $p \in T$ et $\overline{\psi}_m$ est premier à tous ces nombres premiers.
Comme l'ensemble des points S-entiers est fini, on en déduit que l'ensemble des entiers $m \neq 0$ tels que $\overline{\psi}_m = \pm 1$ est fini.
Distinguons deux cas suivant la position de ℓ par rapport à T
(1) si $\ell \in T$ alors $(\overline{\psi}_m, \ell) = 1$
(2) si $\ell \notin T$ alors $M(mod\ \ell)$ est non singulier. Soit ρ l'ordre de M dans le groupe $E(\mathbb{F}_\ell)_{n.s}$. Le théorème A montre que $\ell \mid \overline{\psi}_m$ si et seulement si $m \equiv 0(mod\ \rho)$.

On en déduit que pour tout entier $m \in \mathbb{N} - \{0\}(resp. m \in \mathbb{N} - \rho\mathbb{N})$ dans le premier cas (resp dans le deuxième cas) sauf pour un nombre fini d'entre eux, il existe un entier $N(m)$ tel que :

(i) $\overline{\psi}_m \equiv \pm 1 + \ell^{N(m)}(mod\ \ell^{N(m)+1})$; $N(m) \geq 2$ si $\ell = 2$.
(ii) $\overline{\psi}_m \equiv \pm 1 + a_{N(m)} \ell^{N(m)}(mod\ \ell^{N(m)+1})$; $a_{N(m)} = 1, 2$; $N(m) \geq 1$ si $\ell = 3$.
(iii) $\overline{\psi}_m \equiv \pm a_0 (mod\ \ell)$; $a_0 = 2, \ldots, \dfrac{\ell - 1}{2}$ où
$\overline{\psi}_m \equiv 1 + a_{N(m)} \ell^{N(m)}(mod\ \ell^{N(m)+1})$; $a_{N(m)} = 1, \ldots, \ell - 1; N(m) \geq 1$ si $\ell > 3$.

Supposons que l'on a effectivement écrit l'une de ces formules (i), (ii), (iii) ; comment calculer les multiples de M S-entiers ?
Pour $m \neq 0$, le corollaire A montre que mM est S-entier si et seulement si $\overline{\psi}_m = \pm \prod_{p \in S - T} p^{e_p}$; e_p entier ≥ 0.
Pour tout $p \in S - T$ soit $\rho(p)$ l'ordre de M dans $E(\mathbb{F}_p)_{n.s}$.

Soit m entier > 0. Supposons que mM est S-entier et posons $m = \delta m'$ où δ est formé des puissances des nombres premiers π tels que π divise l'un des $\rho(p)$ et m' est premier à tous ces π.
Supposons que $\pi^e \mid m$ avec $e \geq 1$. Le lemme A montre que $\pi M, \ldots, \pi^e M$ sont S entiers, ce qui détermine la valeur maximale de e pour tout π. Le même argument montre que $m'M$ est S-entier donc $\overline{\psi}_{m'} = \pm 1$ et m' est l'une des valeurs exceptionnelles de m (y compris $m' = 1$) pour lesquelles (i) ou (ii) ou (iii) n'est pas vérifiée, ce qui détermine complètement les valeurs possibles de m'.
Reste à contrôler si les multiples de M de la forme $(\pi_1^{e_1} \cdots \pi_r^{e_r} m')M$ sont S-entiers en accroissant au fur et à mesure le nombre de facteurs r et les exposants e_i.
Des exemples de formules (i) ont été donnés dans [1]. Nous donnons plus loin §5 des exemples de formules (ii).
Le même raisonnement montre que si M est un point rationnel (pas nécessairement S-entier), L un point de 2-torsion rationnel de 1.1 et si on pose :

$$\widehat{\phi}_m - ud^2 \widehat{\psi}_m^2 = r_m \widehat{\theta}_m \text{ dans le cas } u \in \mathbb{Z} \text{ et}$$
$$4(\widehat{\phi}_m - ud^2 \widehat{\psi}_m^2) = r_m \widehat{\theta}_m \text{ dans le cas } u \notin \mathbb{Z}$$

(r_m et $\overline{\theta}_m$ définis semblablement à q_m et $\overline{\psi}_m$), alors pour tout entier $m \in \mathbb{N} - \{0\}(resp\ m \in \mathbb{N} - (\rho' + \rho\mathbb{N}))$ si $\ell \in T(resp.$ si $\ell \notin T)$, sauf pour un nombre fini d'entre eux, $\overline{\theta}_m$ vérifie les propositions (i), (ii), (iii) ci-dessus en remplaçant $\overline{\psi}_m$ par $\overline{\theta}_m$. L'entier ρ' que l'on définit dans le cas $\ell \notin T$ est précisé comme suit, on a : $\overline{\theta}_m \equiv 0(mod\ \ell)$ si et seulement si $L \equiv mM(mod\ \ell)$. Si cette condition est réalisée alors L appartient au groupe $< M >$ engendré par M dans $E(\mathbb{F}_\ell)_{n.s}$. Soit ρ' le plus petit entier ≥ 0 tel que $L \equiv \rho' M(mod\ \ell)$, alors $L \equiv mM(mod\ \ell)$ si et seulement si $m \equiv \rho'(mod \rho)$.
Pour déterminer les translatés $L + mM$ S-entiers, on suppose que $S - T$ ne contient aucun nombre premier p tel que $L \in < M >$ (dans $E(\mathbb{F}_p)_{n.s}$). On choisira ℓ premier de façon que la formule de récurrence (i) ou (ii) ou (iii) soit simple et que ℓ vérifie l'une des conditions $\ell \in T$ ou $L \notin < M >$ dans $E(\mathbb{F}_\ell)_{n.s}$. On fait alors un raisonnement semblable à celui fait ci-dessus.

2. Formules de multiplication

Soit E une courbe elliptique définie sur un corps K par l'équation :

2.1 $$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \ ; \ a_i \in K$$

On définit à partir des coefficients a_i les grandeurs $b_2, b_4, b_6, b_8, c_4, c_6, \Delta$ [5].
Soit $M = (x, y)$ un point de $E(K)$, alors mM s'exprime sous la forme :

$$mM = \left(\frac{\phi_m(M)}{\psi_m^2(M)}, \frac{\omega_m(M)}{\psi_m^3(M)}\right)$$

où $\phi_m, \psi_m, \omega_m \in \mathbb{Z}[a_1, \ldots, a_6, x, y]$ sont des polynômes définis par récurrence comme suit :

$$\begin{aligned}
\psi_0 &= 0 \ ; \ \psi_1 = 1 \ ; \ \psi_2 = 2y + a_1x + a_3 \\
\psi_3 &= 3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8 \\
\psi_4 &= (2y + a_1x + a_3)[2x^6 + b_2x^5 + 5b_4x^4 + 10b_6x^3 + 10b_8x^2 \\
&\quad + (b_2b_8 - b_4b_6)x + (b_4b_8 - b_6^2)] \\
\psi_2\psi_{2m} &= \psi_m(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2) \ ; \ m \geq 2 \\
\psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \ ; \ m \geq 2.
\end{aligned}$$

Pour $m < 0$, nous avons $\psi_m = -\psi_{-m}.\phi_m$ et ω_m sont définis par :

$$\begin{aligned}
\phi_m &= x\psi_m^2 - \psi_{m-1}\psi_{m+1} \\
\omega_m &= \frac{\psi_{2m}}{2\psi_m} - \frac{1}{2}\psi_m(a_1\phi_m + a_3\psi_m^2)
\end{aligned}$$

On utilisera aussi les formules suivantes :

2.2 $$\psi_{k+\ell}\psi_{k-\ell} = \psi_{k+1}\psi_{k-1}\psi_\ell^2 - \psi_{\ell+1}\psi_{\ell-1}\psi_k^2 \ ; \ k, \ell \in \mathbb{Z}$$

2.3 $$\begin{cases}
\phi_{mn}(M) = \psi_n^{2m^2}(M)\phi_m(nM); m, n \in \mathbb{Z} \\
\omega_{mn}(M) = \psi_n^{3m^2}(M)\omega_m(nM); m, n \in \mathbb{Z} \\
\psi_{mn}(M) = \psi_n^{m^2}(M)\psi_m(nM); m, n \in \mathbb{Z}
\end{cases}$$

2.4.

$$\begin{cases} \phi_{2m}(M) = \psi_m^8(M)\phi_2\left(\dfrac{\phi_m(M)}{\psi_m^2(M)}\right) = \phi_m^4(M) - b_4\phi_m^2(M)\psi_m^4(M) \\ \qquad - 2b_6\phi_m(M)\psi_m^6(M) - b_8\psi_m^8(M) \\ \psi_{2m}^2(M) = \psi_m^8(M)\psi_2^2\left(\dfrac{\phi_m(M)}{\psi_m^2(M)}\right) = \psi_m^2(M)(4\phi_m^3(M) + b_2\phi_m^2(M)\psi_m^2(M) \\ \qquad + 2b_4\phi_m(M)\psi_m^4(M) + b_6\psi_m^6(M)) \end{cases}$$

2.5 $$\psi_4 = \psi_2[-\psi_2^4 + \psi_3(6x^2 + b_2x + b_4)]$$

2.6 $[-48x^2 - 8b_2x + (b_2^2 - 32b_4)]\phi_2 - [-12x^3 + b_2x^2 + 10b_4x + 27b_6 - b_4b_2]\psi_2^2 = \Delta$

Si on pose $f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6$, alors on a :

2.7 $$a_1\frac{\partial f}{\partial y} - 2\frac{\partial f}{\partial x} = 6x^2 + b_2x + b_4$$

2.8. $$4\psi_3 = -\left(a_1\frac{\partial f}{\partial y} - 2\frac{\partial f}{\partial x}\right)^2 + (12x + b_2)\psi_2^2$$

2.9. $$4\phi_2 = \left(a_1\frac{\partial f}{\partial y} - 2\frac{\partial f}{\partial x}\right)^2 - (8x + b_2)\psi_2^2$$

On a les propriétés suivantes :
(a) Si l'on attribue les poids $i, 2, 3$ à a_i, x, y respectivement, les polynômes ϕ_m, ψ_m et ω_m sont homogènes de poids $2m^2, 2(m^2-1), 3m^2$ respectivement.

(b) Pour m pair, $\psi_m/(2y + a_1x + a_3) \in \mathbb{Z}[a_1, \ldots, a_6][x]$ est de degré $\frac{m^2}{2} - 2$ de coefficient dominant $\frac{m}{2}$

$\phi_m \in \mathbb{Z}[a_1, \ldots, a_6][x]$ est unitaire de degré m^2

$\omega_m + \frac{1}{2}\psi_m(a_1\phi_m + a_3\psi_m^2) \in \mathbb{Z}[a_1, \ldots, a_6][x]$ est unitaire de degré $\frac{3m^2}{2}$.

(c) Pour m impair, $\psi_m \in \mathbb{Z}[a_1, \ldots, a_6][x]$ est de degré $\frac{m^2-1}{2}$ de coefficient dominant m. $\phi_m \in \mathbb{Z}[a_1, \cdots, a_6][x]$ est unitaire de degré m^2
$[\omega_m + \frac{1}{2}\psi_m(a_1\phi_m + a_3\psi_m^2)]/(2y + a_1x + a_3) \in \mathbb{Z}[a_1, \ldots, a_6][x]$ est unitaire de degré $3\frac{(m^2-1)}{2}$.

Ces formules généralisent les formules classiques valables sur un modèle de Weierstrass court [3].

3. Démonstration du Théorème A

Soit K un corps muni d'une valuation discrète ν et soit E une courbe elliptique définie sur K par l'équation :

3.1. $$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

On suppose que $\nu(a_i) \geq 0$ pour $i = 1, 2, 3, 4, 6$.

Avant d'entreprendre la preuve du théorème A, remarquons que d'après 2.6, on a :
Si $\nu(2) > 0$ et si $\nu(\psi_2(x,y)) > 0$ alors

3.2. $$a_1^4\phi_2(x) \equiv \Delta(mod\ \nu)$$

En comparant les polynômes ϕ_2 et $\frac{\partial f}{\partial x}$, nous en déduisons que :
Si $\nu(2) > 0$ et si $\nu(a_1)$ et $\nu(a_3)$ sont > 0 alors :

3.3. $$\phi_2 \equiv \left(\frac{\partial f}{\partial x}\right)^2 (mod\ \nu)$$

ie chacun des coefficients des termes de même degré des deux polynômes sont congrus entre eux modulo ν.

Preuve du Théorème A $(a) \Longrightarrow (b) \Longrightarrow (c)$ est clair
$(c) \Longleftrightarrow (d)$ comme il résulte de l'identité
$$\phi_{m_0}(M) = x\psi_{m_0}^2(M) - \psi_{m_0-1}(M)\psi_{m_0+1}(M)$$
et de l'identité homologue
$$\phi_{m_0+1}(M) = x\psi_{m_0+1}^2(M) - \psi_{m_0}(M)\psi_{m_0+2}(M)$$
qui montrent que $m_0 \in \{n_0, n_0 - 1\}$ et que l'on peut choisir pour valeur de n_0 aussi bien m_0 que $m_0 + 1$.

$(d) \Longrightarrow (e)$ Comme noté dans [5], chap. III §2, si M est non singulier $(mod\ \nu)$ il en va de même pour $mM(mod\ \nu)$ pour tout entier m.
Choisissons alors n_0 minimal dans (d).

A) Supposons que n_0 est pair et posons $n = n_0/2$.
Soient (x_n, y_n) les coordonnées de nM. Comme $\nu(\psi_{n_0}(M)) > 0$ la relation 2.4 montre que :
$$\nu(\psi_n(M)) > 0 \text{ ou } \nu(\psi_2(x_n, y_n)) > 0.$$
Mais dans le premier cas, on déduit de $\nu(\phi_{n_0}(M)) > 0$ d'après 2.4, que l'on a aussi $\nu(\phi_n(M)) > 0$ et n_0 n'avait pas été choisi minimal.
On a donc :
$$\nu(\psi_n(M)) = 0 \text{ et } \nu(\psi_2(x_n, y_n)) > 0$$
comme $\nu(\phi_{n_0}(M)) > 0$, la relation 2.4 montre aussi que $\nu(\phi_2(x_n)) > 0$. Or $\psi_2 = \frac{\partial f}{\partial y}$ de sorte que $\frac{\partial f}{\partial y}(x_n, y_n) \equiv 0(mod\ \nu)$.
Distinguons alors deux cas :
a) $\nu(2) = 0$.D'après 2.9 on voit que l'on a :
$$\left(a_1\frac{\partial f}{\partial y} - 2\frac{\partial f}{\partial x}\right)(x_n, y_n) \equiv 0(mod\ \nu)$$
et finalement $$\frac{\partial f}{\partial y}(x_n, y_n) \equiv \frac{\partial f}{\partial x}(x_n y_n) \equiv 0(mod\ \nu).$$
Le point nM et donc le point M sont singulier $(mod\ \nu)$.

b) $\nu(2) > 0$. On a alors :
$$\frac{\partial f}{\partial y}(x,y) = 2y + a_1x + a_3 \equiv a_1x + a_3(mod\ \nu)$$
de sorte que $\nu(\psi_2(x_n, y_n))$ ne peut être > 0 que si l'une ou l'autre des hypothèses suivantes

* $\nu(a_1)$ et $\nu(a_3) > 0$
* $\nu(a_1) = 0$ et $x_n \equiv -\dfrac{a_3}{a_1}(mod\ \nu)$

est vérifiée. Mais dans ce dernier cas on a d'après 3.2 :

$$a_1^4\phi_2(x_n) \equiv \Delta(mod\ \nu)$$

de sorte que l'hypothèse $\nu(\phi_2(x_n)) > 0$ assure que $\nu(\Delta) > 0$, autrement dit $E(mod\ \nu)$ est singulier et (x_n, y_n) est son point singulier.
Dans le premier cas, il est facile de vérifier c.f 3.3 que l'on a :

$$\phi_2 \equiv \left(\frac{\partial f}{\partial x}\right)^2 (mod\ \nu)$$

de sorte que l'hypothèse $\nu(\phi_2(x_n)) > 0$ assure $\nu\left(\frac{\partial f}{\partial x}(x_n, y_n)\right) > 0$ ainsi $nM = (x_n, y_n)$ et donc M est à nouveau le point singulier de $E(mod\ \nu)$ ce qui achève la démonstration de $(d) \Longrightarrow (e)$ dans le cas A.

B) Supposons que n_0 est impair.
La relation $\phi_{n_0+1}(M) = x\psi_{n_0+1}^2(M) - \psi_{n_0}(M)\psi_{n_0+2}(M)$ montre que (d) est vérifiée pour $n_0 + 1$ aussi. Maintenant $n_0 + 1$ est pair. On pose $n = (n_0 + 1)/2$ et on continue la démonstration comme précedemment d'où $(d) \Longrightarrow (e)$

$(e) \Longrightarrow (a)$ On a $\psi_2 = \dfrac{\partial f}{\partial y}$. Supposons que (x, y) est singulier $(mod\ \nu)$ de sorte que $\nu(\psi_2(M)) > 0$. On a aussi :

$$\left(a_1\frac{\partial f}{\partial y} - 2\frac{\partial f}{\partial x}\right)(x, y) \equiv 0(mod\ \nu).$$

Si $\nu(2) = 0$, on en déduit immédiatement par 2.8 que $\nu(\phi_2(M)) > 0$.
Si $\nu(2) > 0$ et si comme nous le supposons $\nu(\psi_2(M)) > 0$, on a d'après 3.2 $a_1^4\phi_2(M) \equiv \Delta(mod\ \nu)$.
Dans le cas où $\nu(a_1) = 0$ on déduit immédiatement que $\nu(\phi_2(M)) > 0$ car $\nu(\Delta) > 0$.
Dans le cas où $\nu(a_1) > 0$, l'hypothèse $\nu(\psi_2(M)) > 0$ montre que $\nu(a_3) > 0$ de sorte que 3.3 est vérifiée ie :

$$\phi_2(M) \equiv \left(\frac{\partial f}{\partial x}\right)^2 (mod\ \nu).$$

Dans ce cas aussi on conclut que $\nu(\phi_2(M)) > 0$. Finalement on a $\nu(\psi_2(M)) > 0$ et $\nu(\phi_2(M)) > 0$ dans le cas où $\nu(2) > 0$. L'égalité $\phi_2(M) = x\psi_2^2(M) - \psi_3(M)$ permet de conclure que $\nu(\psi_2(M))$ et $\nu(\psi_3(M)) > 0$. Le théorème A est donc démontré.

4. Multiples et translatés S-entiers

Nous donnons ci-dessous la démonstration du lemme A et des corollaires A et B. Soit S un ensemble fini (éventuellement vide) de nombres premiers et soit $M = \left(\dfrac{a}{d^2}, \dfrac{b}{d^3}\right)$; $(a, d) = 1$, un point rationnel d'ordre infini sur la courbe

4.1 $$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\ ;\ a_i \in \mathbb{Z}$$

On ne suppose pas que le modèle est minimal.

Preuve du lemme A :

Supposons que M n'est pas S-entier. Il existe p premier ; $p \notin S$ tel que $p \mid d$ et $p \nmid a$. On a :

$$x(mM) = \frac{\phi_m(x,y)}{\psi_m^2(x,y)} = \frac{x^{m^2} + \cdots + c_0}{m^2 x^{m^2-1} + \cdots + d_0} = \frac{a^{m^2} + \cdots + c_0 d^{2m^2}}{d^2(m^2 a^{m^2-1} + \cdots + d_o d^{2(m^2-1)})}$$

ce qui montre que p ne divise pas le numérateur de $x(mM)$; donc mM n'est pas S entier.

Preuve du corollaire A : La suffisance de la condition est évidente.

Supposons que mM est S-entier et qu'il existe p premier tel que $p \notin S$ et $p \mid \widehat{\psi}_m$ alors $p \mid \widehat{\phi}_m$ ce qui contredit le théorème A. Ce même théorème montre que pour tout $p \in T$ on a $e_p \geq 1$ d'où la nécessité de la condition.
On suppose maintenant que la courbe 4.1. contient un point de 2-torsion rationnel $L = (u,v) = (u, \frac{1}{2}(a_1 u + a_3))$. On sait que $u \in \mathbb{Z}$ ou $4u \in \mathbb{Z}$ [5], VII, §3.
Le but du corollaire B est de donner une condition nécessaire et suffisante pour que $L+mM$ soit S-entier lorsque M est un point rationnel de 4.1. (pas nécessairement S-entier) et m un entier $\neq 0$. On suppose encore que S contient les nombres premiers ℓ pour lesquels M est singulier $(mod\ \ell)$.

Preuve du corollaire B : Soient x_m, y_m les coordonnées de mM. Les formules d'addition sur la courbe donnent :

$$4.2. \quad x(L+mM) = \frac{(y_m - v)^2 + a_1(y_m - v)(x_m - u) - (a_2 x_m + u)(x_m - u)^2}{(x_m - u)^2}$$

$$\begin{aligned} 4.3. \ x(L+mM) = \{&(\widehat{\omega}_m - vd^3\widehat{\psi}_m^2)^2 + a_1 d\widehat{\psi}_m(\widehat{\omega}_m - vd^3\widehat{\psi}_m^3)(\widehat{\phi}_m - ud^2\widehat{\psi}_m^2) \\ &- [\widehat{\phi}_m + (a_2+u)d^2\widehat{\psi}_m^2](\phi_m - ud^2\widehat{\psi}_m^2)^2\}/d^2\widehat{\psi}_m^2(\phi_m - ud^2\widehat{\psi}_m^2)^2 \end{aligned}$$

Si L est un point entier, les termes figurant au numérateur et au dénominateur sont des entiers. Dans le cas contraire on multiplie numérateur et dénominateur par 2^6 ; on obtient :

$$\begin{aligned} 4.4. \ x(L+mM) = \{&(8\widehat{\omega}_m - 8vd^3\widehat{\psi}_m^3)^2 + 2a_1 d\widehat{\psi}_m(8\widehat{\omega}_m - 8vd^3\widehat{\psi}_m^3)(4\widehat{\phi}_m - 4ud^2\widehat{\psi}_m^2) \\ &- [4\widehat{\phi}_m + 4(a_2+u)d^2\widehat{\psi}_m^2](4\widehat{\phi}_m - 4ud^2\widehat{\psi}_m^2)^2\}/4d^2\widehat{\psi}_m^2(4\widehat{\phi}_m - 4ud^2\widehat{\psi}_m^2)^2 \end{aligned}$$

Suffisance de la condition : L'équation de la courbe permet d'écrire

$$\widehat{\omega}_m^2 + a_1 d\widehat{\psi}_m\widehat{\omega}_m\widehat{\phi}_m - \widehat{\phi}_m^3 = d^2\widehat{\psi}_m^2[a_2\widehat{\phi}_m^2 + a_4 d^2\widehat{\psi}_m^2\widehat{\phi}_m + a_6 d^4\widehat{\psi}_m^4 - a_3 d\widehat{\psi}_m\widehat{\omega}_m]$$

ce qui montre que $d^2\widehat{\psi}_m^2 \mid \widehat{\omega}_m^2 + a_1 d\widehat{\psi}_m\widehat{\omega}_m\widehat{\phi}_m - \widehat{\phi}_m^3$ dans le premier cas et $4d^2\widehat{\psi}_m^2 \mid 8^2\widehat{\omega}_m^2 + 8^2 a_1 d\widehat{\psi}_m\widehat{\omega}_m\widehat{\phi}_m - 8^2\widehat{\phi}_m^3$ dans le deuxième cas.
On en déduit que les facteurs premiers du "vrai dénominateur" de $x(L+mM)$ divisent $\widehat{\phi}_m - ud^2\widehat{\psi}_m^2 (resp\ 4\widehat{\phi}_m - 4ud^2\widehat{\psi}_m^2)$ dans le premier cas (resp. dans le deuxième cas).

Nécessité de la condition :
$L = (u,v)$ étant un point de torsion d'ordre 2, on a :

$$4.5. \qquad 0 = (2v + a_1 u + a_3)^2 = 4u^3 + b_2 u^2 + 2b_4 u + b_6$$

En utilisant cette relation et l'équation de la courbe on obtient :

$$x(L+mM) = \frac{(x_m-u)[4(x_m-u)^2+4(2u-x_m)(x_m-u)+12u^2+2b_2u+2b_4}{4(x_m-u)^2}$$

D'où

4.6. $$x(L+mM) = \{(\widehat{\phi}_m - ud^2\widehat{\psi}_m^2)[4(\widehat{\phi}_m - ud^2\widehat{\psi}_m^2)^2 + 4(2ud^2\widehat{\psi}_m^2 - \widehat{\phi}_m)(\widehat{\phi}_m - 4d^2\widehat{\psi}_m^2) + (12u^2+2b_2u+2b_4)d^4\widehat{\psi}_m^4]\}/4d^2\widehat{\psi}_m^2(\widehat{\phi}_m - ud^2\widehat{\psi}_m^2)^2$$

Ces relations étant établies, supposons que $L+mM$ est S entier et que u est entier (le raisonnement est semblable si $4u \in \mathbb{Z}$).
Supposons qu'il existe p premier ; $p \notin S$ tel que $p \mid \widehat{\phi}_m - ud^2\widehat{\psi}_m^2$ et soit $e \geq 1$ l'exposant exact tel que $p^e \mid \widehat{\phi}_m - ud^2\widehat{\psi}_m^2$.
On a :

$$\begin{aligned}\widehat{\phi}_m - ud^2\widehat{\psi}_m^2 &= d^{2m^2}[(\frac{a}{d^2})^{m^2} + \cdots + h_0 - u(m^2(\frac{a}{d^2})^{m^2-1} + \cdots + k_0)] \\ &= a^{m^2} + \cdots + h_0 d^{2m^2} - ud^2(m^2a^{m^2-1} + \cdots + k_0 d^{2(m^2-1)})\end{aligned}$$

ce qui montre que $p \nmid d$.
On a $p \nmid \widehat{\psi}_m$ sinon $p \mid \widehat{\phi}_m$ et alors $p \in S$ ce qui est contraire à l'hypothèse.
Comme $L+mM$ est S-entier on a : $p^e \mid 12u^2+2b_2u+2b_4$ si p est impair et $2^{e+2} \mid 12u^2+2b_2u+2b_4$ si $p=2$.
Pour p impair cette propriété jointe à la relation 4.5. montrer que L est singulier $(mod\ p)$.
Si $p=2$ on a $2^3 \mid 12u^2+2b_2u+2b_4$ car $e \geq 1$.
D'autre part $0 = 2v + a_1u + a_3 = \dfrac{\partial f}{\partial y}(u,v)$.
La relation $6u^2+b_2u+b_4 = a_1\dfrac{\partial f}{\partial y}(u,v) - 2\dfrac{\partial f}{\partial y}(u,v)$ montre que $2 \mid \dfrac{\partial f}{\partial y}(u,v)$.
Finalement, on conclut dans les deux cas (p impair et $p=2$) que L est singulier $(mod\ p)$.
Maintenant la relation 4.2. montre que $x_m \equiv u(mod\ p)$ et $y_m \equiv v(mod\ p)$, d'où mM est singulier $(mod\ p)$ et alors M est singulier $mod\ p$ et $p \in S$ contrairement à l'hypothèse faite sur p, ce qui achève la démonstration du corollaire B.

5. Exemples de formules (ii)

Soit $M = \left(\dfrac{a}{d^2}, \dfrac{b}{d^3}\right)$ un point rationnel d'ordre infini de :

5.1. $$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \ ; \ a_i \in \mathbb{Z}$$

Nous donnons ici des exemples de formules de (ii) dont il était question dans la présentation. Dans [1] nous avons donné des exemples de formules (i) ; c'est-à-dire des formules utilisant le nombre premier 2.
Nous conservons les notations introduites dans la présentation de la méthode.

Lemme 1 : *Soit $M = \left(\dfrac{a}{d^2}, \dfrac{b}{d^3}\right)$ un point rationnel de 5.1. On suppose que $3 \mid (b_2, b_4)$. Alors pour tout entier $N \geq 1$ et tout n premier a 3 on a :*

$$3^N \mid \widehat{\psi}_{3^N n}.$$

Preuve : On a $\widehat{\psi}_3 = 3a^4 + b_2a^3d^2 + 3b_4a^2d^4 + 3b_6ad^6 + b_8d^8 \equiv 0(mod 3)$.
La troisième formule contenue dans 2.3. montre qu'il suffit de prouver ce lemme pour $n = 1$. On complète la démonstration en raisonnant par récurrence sur N et en utilisant cette même formule.

Lemme 2 : *$M = \left(\frac{a}{d^2}, \frac{b}{d^3}\right)$ un point rationnel de 5.1. On suppose que $3 \mid (b_2, b_4)$ et que $\widehat{\psi}_2 \equiv 2(mod\ 9)$. Alors pour tout entier $N \geq 1$ et tout entier $n \geq 1$ $(n, 3) = 1$ on a :*

5.2. $$\widehat{\psi}_{3^N n \pm 1} \equiv 3^N n \pm 1 \quad (mod\ 3^{N+1})$$

Remarquons que la conclusion du lemme signifie que :

$$\widehat{\psi}_{3^N n \pm 1} \equiv 3^N n \pm 1 \quad (mod\ 3^{N+1}) \equiv \begin{cases} 3^N \pm 1 \text{ si } n \equiv 1(mod\ 3)) \\ 3^N 2 \pm 1 \text{ si } n \equiv 2(mod\ 3) \end{cases} (mod\ 3^{N+1})$$

de sorte que l'on retrouve la forme (ii) de la présentation.

Preuve : Commençons par écrire des formules qui nous seront utiles dans la suite et qui se déduisent toutes de 2.2. En prenant successivement
$(k, \ell) = (2.3^N n, 3^N n + 1); (k, \ell) = (2.3^N n, 3^N n - 1); (k, \ell) = (3^{N+1} n + 1, 3^{N+1} n)$;
$(k, \ell) = (3^{N+1} n, 3^{N+1} n - 1)$ on obtient :

5.3. $$\psi_{3^{N+1}n+1}\psi_{3^N n-1} = \psi_{3^N(2n)+1}\psi_{3^N(2n)-1}\psi^2_{3^N n+1} - \psi_{3^N n+2}\psi_{3^N n}\psi^2_{3^N(2n)}$$

5.4. $$\psi_{3^{N+1}n-1}\psi_{3^N n+1} = \psi_{3^N(2n)+1}\psi_{3^N(2n)-1}\psi^2_{3^N n-1} - \psi_{3^N n}\psi_{3^N n-2}\psi^2_{3^N(2n)}$$

5.5. $$\psi_{3^{N+1}(2n)+1} = \psi_{3^{N+1}n+2}\psi^3_{3^{N+1}n} - \psi^3_{3^{N+1}n+1}\psi_{3^{N+1}n-1}$$

5.6. $$\psi_{3^{N+1}(2n)-1} = \psi_{3^{N+1}n+1}\psi^3_{3^{N+1}n-1} - \psi^3_{3^{N+1}n}\psi_{3^{N+1}n-2}$$

La démonstration du lemme va être faite par récurrence sur N et sur n. Avant de l'entreprendre montrons d'abord que si la propriété du lemme est vérifiée pour le couple (N, n), elle l'est aussi pour $(N, 2n)$.
De manière précise supposons que : $\psi_{3^N n \pm 1} \equiv \pm 1 + 3^N n(mod\ 3^{N+1})$, alors posons :

5.7. $$\begin{cases} \widehat{\psi}_{3^N n-1} = -1 + 3^N n + u.3^{N+1} \\ \widehat{\psi}_{3^N n+1} = 1 + 3^N n + u'.3^{N+1} \end{cases} (mod\ 3^{N+2})$$

et montrons que :

5.8. $$\begin{cases} \widehat{\psi}_{3^N(2n)-1} = -1 + 3^N(2n) - u'.3^{N+1} \\ \widehat{\psi}_{3^N(2n)+1} = 1 + 3^N(2n) - u.3^{N+1} \end{cases} (mod\ 3^{N+2})$$

Les relations 5.5. et 5.6. donnent en tenant compte du lemme 1 :
5.9.
$$\begin{cases} \widehat{\psi}_{3^N(2n)+1} \equiv -\widehat{\psi}^3_{3^N n+1}\widehat{\psi}_{3^N n-1} \ (mod\ 3^{3N}) \\ \widehat{\psi}_{3^N(2n)-1} \equiv \widehat{\psi}_{3^N n+1}\widehat{\psi}^3_{3^N n-1} \end{cases} \begin{matrix} \equiv -\widehat{\psi}^3_{3^N n+1}\widehat{\psi}_{3^N n-1} \ (mod\ 3^{N+2}) \\ \equiv \widehat{\psi}^3_{3^N n+1}\widehat{\psi}_{3^N n-1} \end{matrix}$$

car $3N-(N+2)=2(N-1)\geq 0$ pour tout $N\geq 1$.
En utilisant 5.7. on obtient :

$$\begin{cases}\widehat{\psi}_{3^N(2n)+1}\equiv -[1+3^Nn+u'.3^{N+1}]^3[-1+3^Nn+u.3^{N+1}]\\ \widehat{\psi}_{3^N(2n)-1}\equiv [1+3^Nn+u'.3^{N+1}]\,[-1+3^Nn+u.3^{N+1}]^3\end{cases}(mod\ 3^{N+2})$$

$$\begin{cases}\widehat{\psi}_{3^N(2n)+1}\equiv -[1+3^{N+1}n]\,[-1+3^Nn+u.3^{N+1}]\\ \widehat{\psi}_{3^N(2n)-1}\equiv [1+3^Nn+u'.3^{N+1}]\,[-1+3_n^{N+1}]\end{cases}(mod\ 3^{N+2})$$

$$\begin{cases}\widehat{\psi}_{3^N(2n)+1}\equiv 1+3^N(2n)-u.3^{N+1}\\ \widehat{\psi}_{3^N(2n)-1}\equiv -1+3^N(2n)-u'.3^{N+1}\end{cases}(mod\ 3^{N+2})$$

Cela étant prouvé, nous pouvons entreprendre la démonstration proprement dite du lemme.

(1)$n=1$. Lorsque $N=1$ et que l'on a le signe - le résultat n'est autre que la condition de l'énoncé. Lorsqu'on a le signe +, la relation 2.5. donne

$$\widehat{\psi}_4\equiv -\widehat{\psi}_2^5\ mod\ 3^2\equiv -2^5(mod\ 3^2)\equiv 4(mod\ 3^2)$$

On suppose que la propriété est vraie pour N on veut la montrer pour $N+1$. Cela signifie que les relations 5.7. et 5.8. sont vérifiées pour $n=1$.
En utilisant 5.3. et 5.4. et en tenant compte du lemme 1, on obtient :

$$\begin{cases}\widehat{\psi}_{3^{N+1}+1}\widehat{\psi}_{3^N-1}\equiv \widehat{\psi}_{2.3^N+1}\widehat{\psi}_{2.3^N-1}\widehat{\psi}^2_{3^N+1}\\ \widehat{\psi}_{3^{N+1}-1}\widehat{\psi}_{3^N+1}\equiv \widehat{\psi}_{2.3^N+1}\widehat{\psi}_{2.3^N-1}\widehat{\psi}^2_{3^N-1}\end{cases}(mod\ 3^{N+2})$$

$$\begin{cases}\widehat{\psi}_{2.3^N+1}\widehat{\psi}_{2.3^N-1}\equiv [1+2.3^N-u.3^{N+1}]\,[-1+2.3^N-u'.3^{N+1}]\\ \widehat{\psi}^2_{3^N+1}\equiv (1+3^N+u'.3^{N+1})^2\\ \widehat{\psi}_{3^N-1}\equiv (-1+3^N+u.3^{N+1})^2\\ \dfrac{1}{\widehat{\psi}_{3^N+1}}\equiv \dfrac{1}{1+3^N+u'.3^{N+1}}\\ \dfrac{1}{\widehat{\psi}_{3^N-1}}\equiv \dfrac{1}{-1+3^N+u.3^{N+1}}\end{cases}(mod\ 3^{N+2})$$

Distinguons les cas $N=1$ et $N\geq 2$.

a) $N=1$; on a :

$$\begin{cases}\widehat{\psi}_7\widehat{\psi}_5\equiv -1+(u-u'+1)3^2\\ \widehat{\psi}^2_4\equiv 1+2.3+(1-u')3^2\\ \widehat{\psi}^2_2\equiv 1-2.3+(1+u)3^2\\ \dfrac{1}{\widehat{\psi}_4}\equiv 1-3+(1-u')3^2\\ \dfrac{1}{\widehat{\psi}_2}\equiv -1-3-(1+u)3^2\end{cases}(mod\ 3^3)$$

donc

$$\begin{cases} \widehat{\psi}_{3^2+1} \equiv [-1+(u-u'+1)3^2][1+2.3+(1-u')3^2][-1-3-(1+u)3^2] \\ \widehat{\psi}_{3^2-1} \equiv [-1+(u-u'+1)3^2][1-2.3+(1+u)3^2][1-3+(1-u')3^2] \end{cases}_{(mod 3^3)}$$

d'où

$$\begin{cases} \widehat{\psi}_{3^2+1} \equiv 1+3^2 \\ \widehat{\psi}_{3^2-1} \equiv -1+3^2 \end{cases} (mod\ 3^3)$$

b) $N \geq 2$ on a :

$$\begin{cases} \widehat{\psi}_{2.3^N+1}\widehat{\psi}_{2.3^N-1} \equiv -1+(u-u')3^{N+1} \\ \widehat{\psi}^2_{3^N+1} \equiv 1+2.3^N-u'.3^{N+1} \\ \widehat{\psi}^2_{3^N-1} \equiv 1-2.3^N+u3^{N+1} \\ \dfrac{1}{\widehat{\psi}_{3^N+1}} \equiv 1-3^N-u'3^{N+1} \\ \dfrac{1}{\widehat{\psi}_{3^N-1}} \equiv -1-3^N-u3^{N+1} \end{cases} \qquad (mod\ 3^{N+2})$$

donc on a les congruences suivantes $(mod\ 3^{N+2})$

$$\begin{cases} \widehat{\psi}_{3^{N+1}+1} \equiv [-1+(u-u')3^{N+1}][1+2.3^N-u'.3^{N+1}][-1-3^N-u.3^{N+1}] \\ \widehat{\psi}_{3^{N+1}-1} \equiv [-1+(u-u')3^{N+1}][1-2.3^N+u.3^{N+1}][1-3^N-u'3^{N+1}] \end{cases}$$

d'où :

$$\begin{cases} \widehat{\psi}_{3^{N+1}+1} \equiv 1+3^{N+1} \\ \widehat{\psi}_{3^{N+1}-1} \equiv -1+3^{N+1} \end{cases} (mod\ 3^{N+2})$$

(2) $n > 1$. On suppose que le lemme est vrai pour tout $N \geq 1$ et tout $k < n$, on veut le démontrer pour $\widehat{\psi}_{3^N n \pm 1}$.
(2.a) On suppose que $N = 1$
(2.a.1) Si n est impair
En prenant $(k,\ell) = \left(\dfrac{3(n+1)}{2}, \dfrac{3n-1}{2}\right)$ puis $(k,\ell) = \left(\dfrac{3n+1}{2}, \dfrac{3(n-1)}{2}\right)$ dans 2.2. on obtient

$$\begin{cases} \widehat{\psi}_{3n+1}\widehat{\psi}_2 = \widehat{\psi}_{\frac{3n+5}{2}}\widehat{\psi}_{\frac{3n+1}{2}}\widehat{\psi}^2_{\frac{3n-1}{2}} - \widehat{\psi}_{\frac{3n+1}{2}}\widehat{\psi}_{\frac{(3n-1)}{2}}\widehat{\psi}^2_{\frac{3(n+1)}{2}} \\ \widehat{\psi}_{3n-1}\widehat{\psi}_2 = \widehat{\psi}_{\frac{3(n+1)}{2}}\widehat{\psi}_{\frac{3n-1}{2}}\widehat{\psi}^2_{\frac{3(n-1)}{2}} - \widehat{\psi}_{\frac{3n-1}{2}}\widehat{\psi}_{\frac{3n-5}{2}}\widehat{\psi}^2_{\frac{3n+1}{2}} \end{cases}$$

donc :

$$\begin{cases} \widehat{\psi}_{3n+1}\widehat{\psi}_2 = \widehat{\psi}_{\frac{3n+5}{2}}\widehat{\psi}_{\frac{3n+1}{2}}\psi^2_{\frac{3n-1}{2}} \\ \widehat{\psi}_{3n-1}\widehat{\psi}_2 = -\widehat{\psi}_{\frac{3n-1}{2}}\widehat{\psi}_{\frac{3n-5}{2}}\widehat{\psi}^2_{\frac{3n+1}{2}} \end{cases} (mod\ 3^2)$$

Supposons que $n \equiv 1(mod\ 3)$ (les calculs sont semblables dans le cas $n \equiv -1(mod\ 3)$) et posons $n = 3^M q + 1$; $M \geq 1$; $(3,q) = 1$, q pair alors :

$$\frac{3n+5}{2} = 3\left(3^M\frac{q}{2}+1\right)+1\ ;\ \frac{3n+1}{2} = 3\left(3^M\frac{q}{2}+1\right)-1$$
$$\frac{3n-1}{2} = 3^{M+1}\frac{q}{2}+1\ ;\ \frac{3n-5}{2} = 3^{M+1}\frac{q}{2}-1$$

Il est évident que les coefficients $\frac{q}{2}, 3^M\frac{q}{2}+1$ sont des entiers $< n$ de sorte que l'hypothèse de récurrence s'applique aux entiers $\frac{3n+5}{2}, \frac{3n+1}{2}, \frac{3n-1}{2}, \frac{3n-5}{2}$, donc :

$$\widehat{\psi}_{\frac{3n+5}{2}} \equiv \frac{3n+5}{2}(mod\ 3^2)\ ;\ \widehat{\psi}_{\frac{3n+1}{2}} = \frac{3n+1}{2}\ (mod\ 3^2)$$

$$\widehat{\psi}_{\frac{3n-1}{2}} \equiv \frac{3n-1}{2}\ mod\ 3^{M+2} \equiv 1\ (mod\ 3^2)$$

$$\widehat{\psi}_{\frac{3n-5}{2}} \equiv \frac{3n-5}{2}\ mod\ 3^{M+2} \equiv -1(mod\ 3^2) \quad \text{d'où}$$

$$\begin{cases} \widehat{\psi}_{3n+1}\widehat{\psi}_2 \equiv \dfrac{(3n+5)}{2}\dfrac{(3n+1)}{2} \\ \widehat{\psi}_{3n+1}\widehat{\psi}_2 \equiv \left(\dfrac{3n+1}{2}\right)^2 \end{cases} (mod\ 3^2)$$

et

$$\begin{cases} \widehat{\psi}_{3n+1} \equiv 3n+1 \\ \widehat{\psi}_{3n-1} \equiv 3n-1 \end{cases} (mod\ 3^2)$$

(2.a.2) si n est pair

On prend $(k,\ell) = \left(3\frac{n}{2}+1,\ 3\frac{n}{2}\right)$ puis $(k,\ell) = \left(3\frac{n}{2}, 3\frac{n}{2}-1\right)$ dans 2.2. on obtient :

$$\begin{cases} \widehat{\psi}_{3n+1} = \psi_{3\frac{n}{2}+2}\psi^3_{3\frac{n}{2}} - \psi^3_{3\frac{n}{2}+1}\psi_{3\frac{n}{2}-1} \\ \widehat{\psi}_{3n-1} = \psi_{3\frac{n}{2}+1}\psi^3_{3\frac{n}{2}-1} - \psi^3_{3\frac{n}{2}}\psi_{3\frac{n}{2}-2} \end{cases}$$

donc :

$$\begin{cases} \widehat{\psi}_{3n+1} \equiv -\widehat{\psi}^3_{3\frac{n}{2}+1}\widehat{\psi}_{3\frac{n}{2}-1} \\ \widehat{\psi}_{3n-1} \equiv \widehat{\psi}_{3\frac{n}{2}+1}\widehat{\psi}^3_{3\frac{n}{2}-1} \end{cases} (mod\ 3^2)$$

L'hypothèse de récurrence montre que :

$$\begin{matrix} \widehat{\psi}_{3n+1} \equiv -[3\frac{n}{2}+1]^3[3\frac{n}{2}-1] \\ \widehat{\psi}_{3n-1} \equiv [3\frac{n}{2}+1][3\frac{n}{2}-1]^3 \end{matrix} \quad mod\ 3^2 \begin{matrix} \equiv 3n+1 \\ \equiv 3n-1 \end{matrix} (mod\ 3^2)$$

(2.b) On suppose que le lemme est vrai pour N et on veut le montrer pour $N+1$ (n étant toujours fixé > 1).

La démonstration faite dans (1) peut être reproduite mot pour mot en remplaçant $3^N \pm 1$ par $3^N n \pm 1$; $2.3^N \pm 1$ par $3^N(2n) \pm 1$ et $3^{N+1} \pm 1$ par $3^{N+1}n \pm 1$.

En utilisant la même méthode on peut démontrer les 3 lemmes suivants :

Lemme 3 : *Soit $M = \left(\frac{a}{d^2}, \frac{b}{d^3}\right)$ un point rationnel de 5.1. On suppose que $3 \mid (b_2, b_4)$ et que $\widehat{\psi}_2 \equiv 4(mod\ 3^2)$.*

Alors pour tout entier $N \geq 1$ et tout $n \geq 1, (n,3) = 1$ on a :

5.10. $$\begin{cases} \widehat{\psi}_{3^N n\pm 1} \equiv \mp 1 + 3^N n(mod\ 3^{N+1}) \text{ si } n \text{ est impair} \\ \widehat{\psi}_{3^N n\pm 1} \equiv \pm 1 - 3^N n(mod\ 3^{N+1}) \text{ si } n \text{ est pair} \end{cases}$$

Lemme 4 : *Soit* $M = \left(\frac{a}{d^2}, \frac{b}{d^3}\right)$ *un point rationnel de 5.1. On suppose que* $3 \mid (b_2, b_4)$ *et que* $\widehat{\psi}_2 \equiv -2(mod\ 3^2)$.
Alors pour tout entier $N \geq 1$ *et tout* $n \geq 1, (n,3) = 1$ *on a :*

5.11. $$\begin{cases} \widehat{\psi}_{3^N n \pm 1} \equiv 3^N n \pm 1 (mod\ 3^{N+1}) \text{ si } n \text{ est pair} \\ \widehat{\psi}_{3^N n \pm 1} \equiv \mp 1 - 3^N n (mod\ 3^{N+1}) \text{ si } n \text{ est impair} \end{cases}$$

Lemme 5 : *Soit* $M = \left(\frac{a}{d^2}, \frac{b}{d^3}\right)$ *un point rationnel de 5.1. On suppose que* $3 \mid (b_2, b_4)$ *et que* $\widehat{\psi}_2 \equiv -4(mod\ 3^2)$.
Alors pour tout entier $N \geq 1$ *et tout* $n \geq 1, (n,3) = 1$ *on a :*

5.12. $$\widehat{\psi}_{3^N n \pm 1} \equiv \pm 1 - 3^N n \ \ (mod\ 3^{N+1})$$

Nous allons montrer à travers trois exemples complètement traités comment ces lemmes techniques peuvent être employés dans la recherche des points S-entiers.

6. Points S-entiers sur la courbe $y^2 = x^3 - 6x + 6$

Cette courbe a mauvaise réduction en 2 et 3 seulement. Nous prendrons $S = \{2, 3, 5, 7\}$.
Cette courbe apparaît dans les tables de Birch et Swinnerton-Dyer [2]. Son groupe des points rationnels est de rang 1. En réduisant $(mod\ 7)$ nous voyons que cette courbe est sans torsion sur $\mathbb{Q}$.

Lemme 1 : *Le point* $M = (1,1)$ *engendre le groupe des points rationnels de cette courbe.*

Preuve : Soit $Q = (x, y)$ un générateur. Posons $M = mQ$; $m \neq 0$. Comme M est un point entier, alors Q l'est aussi (voir lemme A §1).
On a $2M = 2mQ = \left(\frac{1}{4}, \frac{-17}{8}\right)$ est 2-entier donc $2Q$ l'est aussi. On en déduit d'après le théorème A§1 que $\psi_2^2(x) = 4y^2 = 4(x^3 - 6x + 6) = 2^e 3^h$ avec $e \geq 2, h \geq 0$.
Si $3 \mid x$ alors $3 \parallel \psi_2^2(x)$ ce qui est impossible, donc $h = 0$.
Si $2 \mid x$ alors $8 \parallel \psi_2^2(x)$ ce qui est impossible donc $e = 2$.
Si $(x, 6) = 1$ alors $(x^3 - 6x + 6, 6) = 1$.
D'où $y^2 = 1$ et $Q = \pm M$.

Théorème 1 : *Soit* $S = \{2, 3, 5, 7\}$. *Les points* S *entiers sur la courbe* $y^2 = x^3 - 6x + 6$ *sont* $\pm M = (1, \pm 1)$; $\pm 2M = (\frac{1}{4}, \mp\frac{17}{8})$; $\pm 3M = \left(\frac{145}{3^2}, \mp\frac{1727}{3^3}\right)$.

Preuve : Commençons par quelques remarques.
La courbe a bonne réduction $(mod\ 5)$. $E(\mathbb{F}_5)$ est cyclique d'ordre 8 et M engendre ce groupe. Donc $\psi_m \equiv 0(mod\ 5)$ si et seulement si $m \equiv 0(mod\ 8)$. Le même argument s'applique pour 7. On a $\psi_m \equiv 0(mod\ 7)$ si et seulement si $m \equiv 0(mod\ 11)$. On a $M \in E(\mathbb{F}_2)_{n.s}$ et $\psi_m \equiv 0(mod\ 2)$ si et seulement si $m \equiv 0(mod\ 2)$. Les conditions des lemmes 1 et 2 (§5) sont satisfaites donc $3^N \mid \psi_{3^N n}$ et

6.1. $$\psi_{3^N n \pm 1} \equiv 3^N n \pm 1 \ (mod\ 3^{N+1})$$

pour tout entier $N \geq 1$ et tout entier $n \geq 1, (n,3) = 1$.

Supposons que mM est S entier avec $m > 0$ et posons $m = 2^{e_1}.3^{e_2}11^{e_3}m'$ avec $(m', 66) = 1$ et $e_1, e_2, e_3 \geq 0$.
Le lemme A montre que $m'M$ est S-entier. Les nombres $2,3,5,7$ ne divisent pas $\psi_{m'}$; donc $\psi_{m'} = \pm 1$. La relation 6.1. montre alors que $m' = 1$. Si $e_1 \geq 1$ alors $2M, \ldots, 2^{e_1}M$ sont S-entiers.
Nous avons $2M = \left(\frac{1}{2^2}, \frac{-17}{2^3}\right)$ est S-entier et $\psi_4 \equiv -4.17$ donc $4M$ n'est pas S-entier d'où $e_1 = 0$ ou 1.

Si $e_2 \geq 1$ alors $3M, \ldots, 3^{e_2}M$ sont S-entiers.
Nous avons $3M = \left(\frac{145}{3^2}, \frac{-1727}{3^3}\right)$ est S-entier et $\psi_9 \equiv 3^2 + 3^4 (mod\ 3^5)$ donc $\psi_9 \neq \pm 3^e$ d'où $9M$ n'est pas S-entier et $e_2 = 0$ ou 1.

Si $e_3 \geq 1$ alors $11M$ est S-entier ie. : $\psi_{11} = \pm 7^h (h \geq 1)$.
Quelques calculs $(mod\ 7^2)$ donnent : $\psi_4 \equiv -19 (mod\ 7^2)$; $\psi_5 \equiv -32 (mod\ 7^2)$; $\psi_6 \equiv -23 (mod\ 7^2)$; $\psi_7 \equiv 16 (mod\ 7^2)$ et donc $\psi_{11} = \psi_7\psi_5^3 - \psi_4\psi_6^3 \equiv -28\ mod\ 7^2$ ce qui contredit la relation $\psi_{11} = \pm 7^h$ donc $e_3 = 0$.
Il reste à considérer le point $6M$. On a $\psi_6 = -6(1727)$ donc $6M$ n'est pas S-entier.
Nous avons montré que les valeurs > 0 de m sont $1,2,3$, ce qui achève la démonstration du théorème.
Nous conservons le même ensemble S et nous étudions ci-dessous les points S-entiers d'une courbe vérifiant les lemmes 1 et 5 (§5).

7. Points S-entiers sur la courbe $y^2 = x^3 + 40$

Cette courbe apparaît dans les tables de [4]. Elle est de rang 1 sur Q sans torsion. Son groupe des points rationnels est engendré par $M = (6, 16)$. Cette courbe a mauvaise réduction en $2,3,5$ et le point M est singulier $(mod\ 2)$.
On pose pour tout $m > 0$; $\psi_m(6,16) = 2^{em}\overline{\psi}_m$ où $\overline{\psi}_m$ est impair alors on a le :

Lemme 1 : *Les exposants $e(m)$ sont donnés par :*

7.1. $$e(m) = \begin{cases} \dfrac{m^2-1}{2} \text{ si } m \text{ est impair} \\ \dfrac{m^2}{2} + M + 2 \text{ si } m = 2^M n \ ; \ (n \text{ impair}, \ M \geq 1) \end{cases}$$

Preuve : Par récurrence en utilisant les relations définissant ψ_{2m} et ψ_{2m+1} (voir §2 ou [3]).

Théorème 1 : *Soit $S = \{2,3,5,7\}$. Les points S-entiers sur la courbe $y^2 = x^3 + 40$ sont $\pm M = (6, \pm 16)$ et $\pm 2M = \left(\frac{-39}{2^6}, \pm\frac{3229}{2^9}\right)$.*

Preuve : M est non singulier $(mod\ 5)$ et M engendre $E(\mathbb{F}_5)_{n.s}$.

De même M est non singulier $(mod\ 7)$ et M engendre $E(\mathbb{F}_7)$.
On en déduit que $\psi_m \equiv 0(mod\ 5)$ si et seulement si $m \equiv 0(mod\ 5)$ et $\psi_m \equiv 0(mod\ 7)$ si et seulement si $m \equiv 0(mod\ 7)$.
Les conditions des lemmes 1 et 5 (§5) sont satisfaites par cette courbe et par M ; donc $3^N \mid \psi_{3^N n}$ et

7.2. $$\psi_{3^N n \pm 1} \equiv 1 - 3^N n (mod\ 3^{N+1})$$

Supposons que mM est S-entier avec $m > 0$ et posons $m = 2^{e_1}.3^{e_2}.5^{e_3}.7^{e_4}m'$ avec $(m', 2.3.5.7.) = 1$.
Si $e_1 > 0$ alors $2M, \ldots, 2^{e_1}\ M$ sont S-entiers.
On a $\psi_2 = 2^5$ et $\psi_4 = 2^{12}.3229$ d'où $2M$ est S-entier et $4M$ ne l'est pas, donc $e_1 = 0$ ou 1.
Si $e_2 > 0$ alors $3M$ est S-entier. Or $\psi_3 = 2^4.3^2.47$ donc $3M$ n'est pas S-entier d'où $e_2 = 0$.
Si $e_3 > 0$ alors $5M$ est S-entier. Or $\psi_5 = 2^{12}.5.6024181$ donc $5M$ n'est pas S-entier d'où $e_3 = 0$.
Si $e_4 > 0$ alors $7M$ est S-entier. Or $\psi_7 = -2^{24}.7^2(43531391759777)$ donc $7M$ n'est pas S-entier d'où $e_4 = 0$.
De plus, $m'M$ est S-entier. Si $m' \neq 1$ posons $m' = 3^N(2n) \pm 1$; $(n, 3) = 1$ car $(m', 6) = 1$.
Puisque $(m', 2.3.5.7) = 1$ on a $\psi_{m'} = 2^{e(m')}\overline{\psi}_{m'} = \pm 2^{e(m')}$.
D'autre part, la relation 7.2. montre que $\psi_{m'} \equiv \pm 1 - 3^N(2n)(mod\ 3^{N+1})$.
On en déduit que : $\pm 2^{e(m')} \equiv \pm 1 - 3^N(2n) mod\ 3^{N+1}$ (les signes $\pm$ de part et d'autre de l'égalité étant indépendants). En tenant compte de 7.1. on a :

$$\pm 2^{\frac{m'^2-1}{2}} \equiv \pm 1 - 3^N(2n)\ (mod\ 3^{N+1})$$
$$\pm 2^{3^N 2n(3^N n \pm 1)} \equiv \pm 1 - 3^N(2n)\ (mod\ 3^{N+1})$$

Il est facile de vérifier par récurrence sur N que $2^{2.3^N} \equiv 1(mod\ 3^{N+1})$ donc $\pm 1 \equiv 1 - 3^N(2n)\ (mod 3^{N+1})$ ce qui est impossible d'où $m' = 1$. Finalement les seuls
points S-entiers sont $\pm M = (6, \pm 16)$ et $\pm 2M = \left(\frac{-39}{2^6}, \pm\frac{3229}{2^9}\right)$.
On peut utiliser la même méthode pour déterminer les points S-entiers des courbes $y^2 = x^3 - 4$ et $y^2 = x^3 - 21$ toutes deux de rang 1 sans torsion [4].
Le groupe des points rationnels de la première courbe est engendré par le point (2,2).
Les conditions des lemmes 1 et 3 §5 sont vérifiées par cette courbe et ce point.
Le groupe des points rationnels de la seconde est engendré par $\left(\frac{37}{3^2}, \frac{188}{3^3}\right)$. Les conditions des lemmes 1 et 4 §5 sont satisfaites.
Nous allons maintenant traiter complètement le cas d'une courbe de rang 1 sur $\mathbb{Q}$ avec un point de 2-torsion rationnel.

8. Points S-entiers sur la courbe $y^2 = x^3 - 15x$

Cette courbe possède le point de 2-torsion rationnel $L = (0, 0)$. Elle apparaît dans les tables de [2] et est de rang 1 sur $\mathbb{Q}$.

On a $E(\mathbb{F}_7) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ donc $Tors\ E(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}$. La courbe contient le point d'ordre infini $M = (4,2)$.

Lemme 1 : *On a* $E(Q) =< L, M >$.

Preuve : On fait la démonstration en deux étapes.

1) Le point M n'est pas multiple d'un point rationnel ie. :
$$M = mM' \Longrightarrow m = \pm 1.$$

Supposons que $M = mM'$ avec $m \in \mathbb{Z} - \{0\}$ et $M' = (x,y)$ un point rationnel sur la courbe. M étant entier, on a d'après le lemme A que M' est entier. De plus $\psi_2(M) = 2^2$ donc $2M$ est 2-entier or $2M = 2mM'$ donc $2M'$ est 2-entier (par application de ce même lemme A. On en déduit que $\psi_2^2(M') = 4y^2 = 4(x^3 - 15x) = 2^e 3^f 5^h$; ($e \geq 2$ f et $h \geq 0$) d'après le corollaire A.
On notera par $\nu_p(a)$ la valuation en p du rationnel a.
Supposons que $\nu_3(x) \geq 2$ alors $3^4 \mid \psi_2^2(M')$.
La relation $\phi_2(M') = x\psi_2^2(M') - \psi_3(M')$ montre en utilisant le corollaire A que $3^4 \mid \psi_3(M') = 3x^4 - 6.15x^2 - 15$ ce qui est impossible donc $\nu_3(x) = 0$ ou 1 d'où $f = 0$ ou 2. Le même raisonnement pour 5 montre que $h = 0$ ou 2.
Supposons que $x \equiv \pm 1 (mod\ 4)$ alors $y^2 \equiv x^3 + x \equiv 2 (mod\ 4)$ ce qui est impossible donc x est pair.
La relation $y^2 = x^3 - 15x$ montre que $\nu_2(x) \geq 2$.
On a $\psi_3(M') = 3x^4 - 6.15x^2 - 15$ est impair donc $\phi_2(M') = x\psi_2^2(M') - \psi_3(M')$ est impair.
De plus $x\ (2M') = \dfrac{\phi_2(M')}{4y^2}$ et $\nu_2(x(2M')) = -(2 + \nu_2(y^2)) \leq -4$.
Comme $2M = 2mM' = \left(\dfrac{31^2}{4^2}, \dfrac{-31.959}{4^3}\right)$, il est clair qu'on ne peut avoir $\nu_2(x) > 2$ d'où $\nu_2(x) = 2 = \nu_2(y^2)$ et $e = 2$.
Il reste à examiner les différents cas : $y^2 = x^3 - 15x = 4$; $y^2 = x^3 - 15x = 4.9$ $y^2 = x^3 - 15x = 4.25$; $y^2 = x^3 - 15x = 4.9.25$.
Seule l'équation $x^3 - 15x = 4$ possède une solution entière donc $M' = \pm M$.

2) On n'a pas $M = L + mM'$ avec $m \neq \pm 1$ et M' rationnel.
Supposons que $M = L + mM'$ avec M' rationnel ; $m \neq 0, \pm 1$ et posons $m = 2^N n, N \geq 0$; n impair. Alors $M = n(L + 2^N M')$. Le 1) montre que $n = \pm 1$ et $M = L \pm 2^N M'$.
Si $N \neq 1$ alors $M + L = \pm 2^N M' \in 2E(\mathbb{Q})$ donc $M + L \in 2E(\mathbb{F}_7)$.
Or $M = \left(\dfrac{-15}{4}, \dfrac{15}{8}\right) \equiv (-2,1) mod\ 7$.
D'autre part $E(\mathbb{F}_7) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \simeq < (0,0) > \times < (-2,1) >$ donc $M + L \notin 2E(\mathbb{F}_7)$ et on déduit que $N = 1$ et $M = L \pm M'$.

Théorème 1 : *Soit* $S =< 2,3,5,7 >$. *Les points* S*-entiers sur la courbe* $y^2 = x^3 - 15x$ *sont*
$$L = (0,0)\ ;\ \pm M = (4, \pm 2)\ ;\ \pm 2M = \left(\frac{31^2}{4^2}, \pm\frac{31.959}{4^3}\right),\ L \pm M = \left(\frac{-15}{4}\ ;\ \mp\frac{15}{8}\right).$$

Preuve : On procède en deux étapes.

1) Supposons que mM est S-entier avec $m > 0$.
M engendre $E(\mathbb{F}_2)_{n.s}$ donc $2 \mid \psi_m$ si et seulement si $m \equiv 0(mod\ 2)$.
Le même argument s'applique pour les nombres premiers 3 et 5.
On a $3 \mid \psi_m(resp\ 5 \mid \psi_m)$ si et seulement si $m \equiv 0(mod\ 3)(resp\ mod\ 5)$.
La courbe est non singulière $(mod\ 7)$ et M est d'ordre 4 dans $E(\mathbb{F}_7)$ donc $\psi_m \equiv 0(mod\ 7)$ si et seulement si $m \equiv 0(mod\ 4)$.
Posons $m = 2^{e_1}.3^{e_2}.5^{e_3}m'$ avec $(m', 2.3.5) = 1$.
On a $\psi_2 = 2^2$; $\psi_4 = -2^3.7.31.137$. d'où $2M$ est S-entier et $4M$ ne l'est pas. On en déduit que $e_1 = 0$ ou $e_1 = 1$.
On a $\psi_3 = -3.13.23$ ce qui montre que $3M$ n'est pas S-entier d'où $e_2 = 0$.
On a $\psi_5 = 5^2.28260521$ donc $5M$ n'est pas S-entier d'où $e_3 = 0$.
De même $m'M$ est S-entier. Comme $(m', 2.3.5) = 1$ on en déduit que $\psi_{m'} = \pm 1$.
Comme les conditions du lemme 3 §5 sont vérifiées on a $m' = 1$. Finalement les valeurs > 0 de m sont $m = 1, 2$.

2) Supposons maintenant que $L + mM$ est S-entier avec $m > 0$ et posons $m = 2^N n$; n impair, $N \geq 0$. On a $L + mM = n(N + 2^N M)$ donc $L + 2^N M$ est S-entier.
Supposons que $N \geq 1$; le corollaire B montre que $\phi_{2^N} = \pm 2^{h_1} 3^{h_2} 5^{h_3} 7^{h_4}$.
Revenons au cas général des polynômes $\phi_m(a_1, \ldots, a_6, x, y)$ nous voyons en tenant compte du fait que ce polynôme est unitaire en x et des valeurs particulières de $a_1, \ldots, a_6, x, y$ que $(\phi_{2^N}, 3.5) = 1$ et $h_2 = h_3 = 0$.
On a $\phi_{2^N} = 4\psi_{2^N}^2 - \psi_{2^N-1}\psi_{2^N+1}$ est impair, donc $h_1 = 0$.
Pour $p = 7$ on a : $7 \mid \phi_m$ si et seulement si $mM \equiv T(mod\ 7)$.
Or $M \equiv (-2, 1)(mod\ 7)$; $2M \equiv (-1, 0)(mod\ 7)$; $3M \equiv -M \equiv (-2, 1)(mod\ 7)$
$4M = \infty(mod\ 7)$ donc $mM \not\equiv L$ pour tout m et $h_4 = 0$.
Finalement on a $\phi_{2^N} = \pm 1$.
Les formules 2.4. donnent :

$$\phi_{2^N} = \phi_{2^N-1}^4 + 30\phi_{2^N-1}^2\psi_{2^N-1}^4 + 15^2\psi_{2^N-1}^8 = \left(\phi_{2^N-1}^2 + 15\psi_{2^N-1}^4\right)^2 > 1.$$

On en déduit que $N = 0$ et $m = n$ est impair.
Il faut donc regarder les multiples impairs de $L + M$, S-entiers. On a $L + M = \left(\frac{-15}{4}, \frac{15}{8}\right)$;
$2^8\psi_3(L + M) = \widehat{\psi}_3(L + M) = 3.15^4 - 6.15^3.4^2 - 15^2.4^4 \equiv -1 + 2^2(mod\ 2^3)$ de sorte que les hypothèses du lemme 3 §3 [1] sont vérifiées, donc :

8.1. $$\widehat{\psi}_{2^N n \pm 1}(L + M) \equiv \pm 1 + 2^N\ (mod\ 2^{N+1})$$

On a $L + M$ est singulier $(mod\ 3)$ et $(mod\ 5)$ et $M + L$ est d'ordre 4 dans $E(\mathbb{F}_7)$ donc $7 \not\mid \widehat{\psi}_{2^N n \pm 1}(L + M)$. On conclut que si $(2^N n \pm 1)(M + L)$; $N \geq 2$, n impair est S-entier alors $\widehat{\psi}_{2^N n \pm 1}(M + L) = \pm 3^{e_1}.5^{e_2}$. Considérons le polynôme $\psi_m(a_1, \ldots, a_6, X, Y)$. Il est homogène de poids $m^2 - 1$ si on attribue les poids $i, 2, 3$ à a_i, X, Y respectivement. Lorsque l'indice m est impair ce polynôme est indépendant de Y. Considérons plus particulièrement le polynôme déduit du précédent $\psi_{2^N n \pm 1}(0, 0, 0, a_4, 0, X)$.
On peut vérifier par récurrence que le terme indépendant de X est $\pm(a_4)^{\frac{(2^N n \pm 1)^2 - 1}{4}}$.

Dans le cas qui nous intéresse $a_4 = -15$ donc le terme constant de $\psi_{2^N n\pm 1}(0,0,0,-15,0,X)$ est égal à $\pm 15^{\frac{(2^N n\pm 1)^2-1}{4}} = \pm 15^{n^2 2^{2(N-1)} \pm n.2^{N-1}}$.
On voit facilement que $\nu_3(\widehat{\psi}_{2^N n\pm 1})$ $(resp\ \nu_5(\widehat{\psi}_{2^N n\pm 1}))$ est égal à la valuation en 3(resp en 5) de ce terme indépendant de X.
On en déduit que si $(2^N n \pm 1)(M+L)$ est S-entier, alors :

$$\widehat{\psi}_{2^N n\pm 1} = \pm 3^{e_1} 5^{e_2} = \pm 15^{n^2 2^{2(N-1)} \pm n 2^{N-1}}.$$

Il est facile de vérifier que $15^{2^{N-1}} \equiv 1 (mod\ 2^{N+1})$ donc $\widehat{\psi}_{2^N n\pm 1} \equiv \pm 1 (mod\ 2^{N+1})$, ce qui contredit la relation 8.1.
Finalement on a que les seuls multiples de $L+M$, S-entiers sont $L \pm M$ ce qui achève la démonstration du théorème.

Remerciements

Je remercie les professeurs Y. Hellegouarch, G. Robert et P. Toffin pour m'avoir aidé dans ce travail.

Bibliographie

[1] **Ayad, M.** : Points Δ entiers sur les courbes elliptiques.
Journal of number theory 39 (1991) 323-337

[2] **Birch, B.J. et Swinnerton-Dyer, H.P.F.** : Notes on elliptic curves I
J. Reine Angew. Math 212 (1963) 7-25.

[3] **Cassels, J.W.S.** : A note on the division values of $\mathcal{P}(u)$
Proc. Cambridge Phil. Soc. 45 (1949), 167-172

[4] **Cassels, J.W.S.** : The rational solutions of the diophantine equation :
$y^2 = x^3 - D$. *Acta. Math. 82 (1950) 243-273*

[5] **Silverman, J.H.** : The arithmetic of elliptic curves.
Springer Verlag (1986)

Université de Caen - Faculté des Sciences
Département de Mathématiques
Esplanade de la Paix 14032 CAEN

(Reçu le 23. Octobre 1991;
la version révisée reçu le 19. Mars 1992)