Annales de l'institut Fourier

Alain Kraus

Sur les modules des points de 7-torsion d'une famille de courbes elliptiques

Annales de l'institut Fourier, tome 46, nº 4 (1996), p. 899-907

<http://www.numdam.org/item?id=AIF_1996__46_4_899_0>

Ann. Inst. Fourier, Grenoble
46, 4 (1996), 899–907

SUR LES MODULES DES POINTS DE 7-TORSION D'UNE FAMILLE DE COURBES ELLIPTIQUES

par Alain KRAUS

Introduction.

Cet article concerne la question suivante posée par B. Mazur dans [7], p. 133 :

Soit $\overline{\mathbf{Q}}$ *une clôture algébrique de* $\mathbf{Q}$*. Existe-t-il un entier* $n \geq 7$*, deux courbes elliptiques* E *et* E' *définies sur* $\mathbf{Q}$*, non isogènes sur* $\mathbf{Q}$*, tels que les groupes des points de* n*-torsion de* E *et* E' *soient isomorphes comme* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$*-modules et symplectiquement, i.e. de façon compatible aux accouplements de Weil?*

Comme le suggère B. Mazur, cette question peut être reformulée en termes d'existence de points rationnels sur $\mathbf{Q}$, de tordues galoisiennes de la courbe modulaire $Y(n)$, qui est de genre ≥ 3 pour $n \geq 7$, et qui n'a donc qu'un nombre fini de points rationnels (cf. loc. cit.).

Avec J. Oesterlé, on explicite dans [6] des exemples de couples de courbes elliptiques sur $\mathbf{Q}$ répondant positivement à cette question si $n = 7$. Une étude de surfaces modulaires liées à la courbe $Y(n)$, a récemment été faite par E. Kani et W. Schanz ([4]), permettant de prouver l'existence d'une infinité de tels couples pour $n = 7$. Par ailleurs, B. Mazur a déterminé des exemples pour $n = 11$ et $n = 13$ ([8]). Il semble que G. Frey en a aussi trouvé pour $n = 11, 13$ et 17. Dans un travail récent avec E. Halberstadt, nous en avons explicité pour $n = 10$ et 22.

Mots-clés : Courbes elliptiques – Points de torsion – Représentations de Galois.
Classification math. : 11G.

Des exemples de couples de courbes elliptiques sur $\mathbf{Q}$, non $\mathbf{Q}$-isogènes, dont les modules des points de n-torsion soient isomorphes, ont aussi été trouvés pour $n = 8$ (cf. [2], preprint, p. 22, dans lequel il y a aussi des exemples pour $n = 7$). N. Elkies a récemment démontré l'existence d'une infinité de tels couples pour $n = 7$. Par ailleurs, il se trouve dans [3] un exemple pour $n = 14$.

Dans ce travail, on se préoccupe toujours du cas où $n = 7$. Étant donné une courbe elliptique E définie sur $\mathbf{Q}$, on notera E_7 le sous-groupe des points de 7-torsion de $E(\overline{\mathbf{Q}})$; E_7 est un espace vectoriel de dimension 2 sur $\mathbf{Z}/7\mathbf{Z}$. L'action du groupe $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ sur E_7, définit une représentation continue

$$\varphi_E : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathrm{Aut}(E_7).$$

Le déterminant de φ_E est le caractère cyclotomique χ, donnant l'action de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ sur le sous-groupe des racines 7-ièmes de l'unité de $\overline{\mathbf{Q}}$ (cf. [11], 1.11).

On s'intéresse ici aux courbes elliptiques E définies sur $\mathbf{Q}$, dont la représentation φ_E possède *un quotient isomorphe à* $\mathbf{Z}/7\mathbf{Z}$. Un tel homomorphisme est représentable matriciellement sous la forme $\left(\begin{smallmatrix} \chi & * \\ 0 & 1 \end{smallmatrix}\right)$ (cf. loc. cit.). Les courbes elliptiques E ayant cette propriété sont décrites par une famille infinie à un paramètre de courbes elliptiques $E(t)$; $E(t)$ possède un modèle de Weierstrass à coefficients dans $\mathbf{Z}[t]$ (cf. §1). En décrivant le corps des points de 7-torsion de $E(t)$ (§2), on explicite une *infinité de triplets* de courbes elliptiques sur $\mathbf{Q}$, qui répondent positivement à la question posée par B. Mazur. Plus précisément, le résultat que l'on a en vue est le suivant :

Soit n un entier relatif de valeur absolue ≥ 3. Posons $a_n = 1/(1+n+n^2)$. Alors, les courbes elliptiques sur $\mathbf{Q}$, $E(a_n)$, $E(n^2 a_n)$ et $E((n+1)^2 a_n)$ sont mutuellement non isogènes sur $\mathbf{Q}$. Les représentations de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ définies par les groupes des points de 7-torsion de $E(a_n)$ $E(n^2 a_n)$ et $E((n+1)^2 a_n)$ sont symplectiquement isomorphes.

J'ai bénéficié au cours de ce travail de conversations avec J. Oesterlé et P. Satgé que je remercie ici.

1. La courbe elliptique $E(t)$.

Considérons un corps K de caractéristique 0. Soient t un élément de K de $W(t)$ la cubique affine d'équation :

$$W(t) : y^2 + a_1(t)xy + a_3(t)y = x^3 + a_2(t)x^2 + a_4(t)x + a_6(t),$$

avec :

$$\begin{aligned}
&a_1(t) = 1 + t - t^2, \quad a_2(t) = a_3(t) = t^2 - t^3,\\
&a_4(t) = 5t(1-t)(t^2 - t + 1)(t^3 + 2t^2 - 5t + 1),\\
&a_6(t) = t(1-t)(t^9 + 9t^8 - 37t^7 + 70t^6 - 132t^5 + 211t^4 - 182t^3\\
&\qquad + 76t^2 - 18t + 1).
\end{aligned}$$

Les invariants standard $c_4(t)$ et $\Delta(t)$ associés à $W(t)$ sont (cf. [13], 1) :

$$\begin{aligned}
&c_4(t) = (t^2 - t + 1)(t^6 + 229t^5 + 270t^4 - 1695t^3 + 1430t^2 - 235t + 1),\\
&\Delta(t) = t(t-1)(t^3 - 8t^2 + 5t + 1)^7.
\end{aligned}$$

Si $\Delta(t)$ n'est pas nul, $W(t)$ représente une courbe elliptique $E(t)$ définie sur K.

Soit $\overline{K}$ une clôture algébrique de K. On note μ_7 le sous-groupe des racines 7-ièmes de l'unité de $\overline{K}$.

LEMME 1. — *Soit t un élément de K tel que $\Delta(t)$ ne soit pas nul. Il existe un homomorphisme injectif $\mu_7 \to E(t)_7$ qui est compatible aux actions de* $\mathrm{Gal}(\overline{K}/K)$.

Démonstration. — Considérons la cubique affine d'équation :

$$y^2 + (1 + t - t^2)XY + (t^2 - t^3)Y = X^3 + (t^2 - t^3)X^2.$$

Son discriminant est $t^7(t-1)^7(t^3 - 8t^2 + 5t + 1)$ (cf. [13], 1); elle représente ainsi une courbe elliptique E_t sur K. Le point $(0,0)$ est d'ordre 7 (cf. par exemple [12], p. 354).

En utilisant l'algorithme de J. Vélu décrit dans [14], on constate que $E(t)$ est liée à E_t par une isogénie de degré 7. Par ailleurs, le déterminant de la représentation donnant l'action de $\mathrm{Gal}(\overline{K}/K)$ sur le groupe des points de 7-torsion de E_t, est le caractère cyclotomique χ (cf. [11], 1.11). On déduit de là qu'il existe un sous-groupe d'ordre 7 de $E(t)(\overline{K})$ sur lequel $\mathrm{Gal}(\overline{K}/K)$ opère via χ. D'où le lemme.

Remarque. — Inversement, si E une courbe elliptique définie sur K possédant une injection galoisienne de μ_7 dans E_7, il existe t dans K (non unique) tel que $\Delta(t)$ ne soit pas nul, et que E soit isomorphe sur K à $E(t)$; nous n'aurons pas besoin de cette remarque.

2. Le corps des points de 7-torsion de $E(t)$.

On considère toujours dans ce paragraphe un corps K de caractéristique 0. Soit $\overline{K}$ une clôture algébrique de K. Étant donné un élément a de K, on désigne par $a^{1/7}$ une racine 7-ième de a dans $\overline{K}$. Soit t un élément de K tel que $\Delta(t)$ soit non nul. L'objet du §2 est de décrire l'extension $K(E(t)_7)$ de K obtenue par adjonction des coordonnées des points de $E(t)_7$. On a le résultat suivant :

THÉORÈME 1. — *Soit t un élément de K. Supposons que $t(t-1)$ (t^3-8t^2+5t+1) ne soit pas nul. Alors, on a l'égalité*

$$K(E(t)_7) = K(\mu_7, (t(t-1)^2)^{1/7}).$$

Démonstration. — Considérons le corps $L = \mathbf{Q}(T)$ des fractions rationnelles à coefficients dans $\mathbf{Q}$ en l'indéterminée T. La cubique $W(T)$ représente la courbe elliptique $E(T)$ sur L (cf. §1). D'après le lemme 1, $E(T)_7$ possède un sous-Gal$(\overline{L}/L)$-module isomorphe à μ_7. Par ailleurs, $L(\mu_7)$ est contenu dans $L(E(T)_7)$, et l'action par conjugaison de Gal$(L(\mu_7)/L)$ sur Gal$(L(E(T)_7)/L(\mu_7))$ est donnée par le caractère donnant l'action de Gal$(\overline{L}/L)$ sur μ_7. En utilisant la théorie de Kummer (cf. [1], p. 90), on déduit alors que $L(E(T)_7)$ peut s'écrire sous la forme

$$L(E(T)_7) = L(\mu_7, d(T)^{1/7}),$$

où $d(T)$ est un élément de $\mathbf{Z}[T]$ sans puissance 7-ième. Par ailleurs, la courbe elliptique $E(T)$ a mauvaise réduction de type multiplicatif en les places T, $T-1$ et T^3-8T^2+5T+1, et bonne réduction en dehors de ces places (cf. §1). D'après le critère de Néron-Ogg-Shafarevich (cf. par exemple [12], p. 184, th. 7.1), il existe donc des entiers a, b et c, bien définis modulo 7, et un nombre rationnel α, tels que l'on ait

$$d(T) = \alpha T^a (T-1)^b (T^3-8T^2+5T+1)^c.$$

Posons $g(T) = T^3-8T^2+5T+1$. L'exposant de $g(T)$ dans $\Delta(T)$ est 7. D'après la théorie de Tate, l'extension $L(E(T)_7)/L$ est donc non ramifiée en la place $g(T)$ (cf. loc. cit., p. 355, §14), et l'on peut supposer que l'on a $c=0$. En utilisant un argument de réduction, on déduit de là l'égalité

$$K(E(t)_7) = K(\mu_7, (\alpha t^a (t-1)^b)^{1/7}).$$

Un argument de spécialisation, permet alors de vérifier que l'on peut prendre $\alpha = 1$, $a = 1$ et $b = 2$. D'où le théorème 1.

3. Le résultat principal.

Soit n *un entier relatif dont la valeur absolue est* ≥ 3. On pose

$$a_n = \frac{1}{1+n+n^2}.$$

Les discriminants des cubiques $W(a_n)$, $W(n^2a_n)$ et $W((n+1)^2a_n)$ ne sont pas nuls (cf. §1). Ces cubiques représentent donc respectivement les courbes elliptiques $E(a_n)$, $E(n^2a_n)$ et $E((n+1)^2a_n)$ définies sur $\mathbf{Q}$.

Nous allons maintenant démontrer le résultat annoncé dans l'introduction :

THÉORÈME 2. — *Les courbes elliptiques $E(a_n)$, $E(n^2a_n)$ et $E((n+1)^2a_n)$ sont mutuellement non isogènes sur $\mathbf{Q}$. Les représentations de* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ *définies par les groupes des points de 7-torsion de $E(a_n)$, $E(n^2a_n)$ et $E((n+1)^2a_n)$ sont symplectiquement isomorphes.*

3.1. Lemme préliminaire.

Considérons deux courbes elliptiques E et E' définies sur $\mathbf{Q}$. Soient Δ et Δ' les discriminants minimaux de E et E' respectivement. Étant donné un nombre premier p, on note $v_p(\Delta)$ (resp. $v_p(\Delta')$) l'exposant de p dans Δ (resp. dans Δ'). Notons φ et φ' les représentations de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ dans E_7 et E'_7. Prouvons alors le lemme suivant :

LEMME 2. — *Supposons les conditions suivantes réalisées :*

(i) *les représentations φ et φ' sont isomorphes;*

(ii) *le groupe E_7 possède un sous-module isomorphe à μ_7;*

(iii) *il existe un nombre premier p distinct de 7 tel que 7 ne divise pas $v_p(\Delta)$.*

Alors, 7 ne divise pas $v_p(\Delta')$, et si les réductions modulo 7 de $v_p(\Delta)$ et $v_p(\Delta')$ diffèrent multiplicativement par un carré dans $\mathbf{Z}/7\mathbf{Z}$, les représentations φ et φ' sont symplectiquement isomorphes.

Démonstration. — Il résulte des conditions (ii) et (iii) que E a en p réduction de type multiplicatif (cf. par exemple [5], p. 361, lemme 2). Par ailleurs, la condition (i) et le fait que 7 ne divise pas $v_p(\Delta)$, impliquent que E' a aussi en p réduction de type multiplicatif. La proposition 2 de [6] entraîne alors le résultat.

3.2. La courbe elliptique $E(a/b)$.

Soit t un élément de $\mathbf{Q}$ distinct de 0 et 1; $\Delta(t)$ n'est pas nul. On se propose ici d'expliciter un modèle entier de la courbe elliptique $E(t)$.

Posons pour cela $t = a/b$, où a et b sont deux *entiers premiers entre eux*. Rappelons que x et y désignent les fonctions coordonnées de Weierstrass de $E(t)$ dans le modèle $W(t)$. En effectuant le changement de variables

$$\begin{cases} X = b^4x \\ Y = b^6y, \end{cases}$$

on constate que la courbe elliptique $E(a/b)$ admet un modèle de Weierstrass $W(a,b)$ de la forme :

$$W(a,b) : Y^2 + A_1XY + A_3Y = X^3 + A_2X^2 + A_4X + A_6,$$

avec :

$$\begin{aligned}
&A_1 = b^2 + ab - a^2, \qquad A_2 = a^2b(b-a), \qquad A_3 = a^2b^3(b-a),\\
&A_4 = 5ab(b-a)(a^2 - ab + b^2)(a^3 + 2a^2b - 5ab^2 + b^3),\\
&A_6 = ab(b-a)(a^9 + 9a^8b - 37a^7b^2 + 70a^6b^3 - 132a^5b^4 + 211a^4b^5\\
&\qquad - 182a^3b^6 + 76a^2b^7 - 18ab^8 + b^9).
\end{aligned}$$

Le discriminant $\Delta(a,b)$ associé à ce modèle est (cf. [13], 1) :

$$\Delta(a,b) = ab(a-b)(a^3 - 8a^2b + 5ab^2 + b^3)^7.$$

On utilisera l'énoncé suivant (cf. [9], p. 30, prop. II.3.1) :

LEMME 3. — *L'équation $W(a,b)$ est minimale en tout nombre premier distinct de 7.*

En effet, l'invariant standard $c_4(a,b)$ associé à $W(a,b)$ est :

$$c_4(a,b) = (a^2 - ab + b^2)(a^6 + 229a^5b + 270a^4b^2 - 1695a^3b^3 + 1430a^2b^4 - 235ab^5 + b^6).$$

Les entiers a et b étant par hypothèse premiers entre eux, on vérifie alors que 7 est le seul diviseur premier commun possible à $c_4(a,b)$ et $\Delta(a,b)$.

3.3. Démonstration du théorème 2.

Signalons d'abord l'idée qui nous a permis de trouver l'énoncé du théorème 2. Elle repose sur la remarque suivante, qui est une application directe du théorème 1 : soient u et v sont des nombres rationnels distincts de 0 et 1. Si l'on a $u(u-1)^2 = v(v-1)^2$, les $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-modules des points de 7-torsion des courbes elliptiques $E(u)$ et $E(v)$ sur $\mathbf{Q}$, sont isomorphes.

Étant donné u dans $\mathbf{Q}$ distinct de 0 et 1, on a ainsi été amené à déterminer les racines rationnelles du polynôme $T(T-1)^2 - u(u-1)^2$. On a le lemme suivant :

LEMME 4. — *Soit u un nombre rationnel autre que* 0 *et* 1. *Supposons que $u(4-3u)$ soit le carré dans $\mathbf{Q}$ d'un élément a. Alors, $v = (2-u+a)/2$ et $w = (2-u-a)/2$ sont distincts de* 0 *et* 1, *et les courbes elliptiques $E(u)$, $E(v)$ et $E(w)$ sur $\mathbf{Q}$, ont leurs* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$*-modules des points de 7-torsion isomorphes.*

Démonstration. — Le fait que v et w soient distincts de 0 et 1 se vérifie directement. Par ailleurs, les racines du polynôme $T(T-1)^2 - u(u-1)^2$ sont u, v et w. Les corps des points de 7-torsion de $E(u)$, $E(v)$ et $E(w)$ sont donc égaux, ce qui entraîne l'assertion.

Démontrons maintenant le théorème 2. Rappelons que n désigne un entier relatif dont la valeur absolue est ≥ 3.

a) Les représentations de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ définies par les groupes des points de 7-torsion de $E(a_n)$, $E(n^2a_n)$ et $E((n+1)^2a_n)$ sont isomorphes; en effet, cela résulte du lemme 4 appliqué avec $u = a_n$ (avec les notations de ce lemme, avec $a = (2n+1)/(1+n+n^2)$, on a $v = (n+1)^2a_n$ et $w = n^2a_n$).

b) Démontrons que les courbes elliptiques $E(a_n)$, $E(n^2a_n)$ et $E((n+1)^2a_n)$ sont mutuellement non isogènes sur $\mathbf{Q}$. Il suffit pour cela de prouver que leurs conducteurs sont distincts (pour la définition du conducteur d'une courbe elliptique, voir par exemple [12], p. 361).

Considérons les discriminants des modèles entiers $W(1, 1+n+n^2)$, $W(n^2, 1+n+n^2)$ et $W((n+1)^2, 1+n+n^2)$ représentant respectivement $E(a_n)$, $E(n^2a_n)$ et $E((n+1)^2a_n)$ (cf. 3.2); on a les égalités (cf. loc. cit.) :

$$\Delta(1, 1+n+n^2) = -n(n+1)(1+n+n^2)\alpha(n)^7,$$

où $\alpha(n) = n^6 + 3n^5 + 11n^4 + 17n^3 + 13n^2 + 5n - 1$,

$$\Delta(n^2, 1+n+n^2) = n^2(n+1)(1+n+n^2)\beta(n)^7,$$

où $\beta(n) = n^6 - 5n^5 - 13n^4 - 17n^3 - 11n^2 - 3n - 1$, et

$$\Delta((n+1)^2, 1+n+n^2) = -n(n+1)^2(1+n+n^2)\delta(n)^7,$$

où $\delta(n) = n^6 + 11n^5 + 27n^4 + 35n^3 + 27n^2 + 11n + 1$.

Prouvons que les trois ensembles formés des diviseurs premiers distincts de 7, respectivement de $\alpha(n)$, $\beta(n)$ et $\delta(n)$, sont deux à deux distincts. Les deux entiers $\alpha(n)\beta(n)\delta(n)$ et $n(n+1)(1+n+n^2)$ étant premiers entre eux, l'assertion de l'alinéa b) résultera alors du lemme 3. Démontrons pour cela que les entiers $\alpha(n)$, $\beta(n)$ et $\delta(n)$ vérifient les deux propriétés suivantes :

(i) ils ne sont pas divisibles par 2;

(ii) ils ne sont pas des puissances 7-ièmes.

L'assertion (i) se vérifie directement. Prouvons que l'on a

$$7^3 \nmid \alpha(n), \quad 7^3 \nmid \beta(n), \quad \text{et} \quad 7^3 \nmid \delta(n). \tag{1}$$

Si $n \not\equiv 1 \bmod 7$ et $n \not\equiv -2 \bmod 7$, 7 ne divise pas $\alpha(n)$. Supposons $n \equiv 1 \bmod 7$ ou $n \equiv -2 \bmod 7$. On a alors $\alpha(n) \equiv 7^2 \bmod 7^3$, et en particulier 7^3 ne divise pas $\alpha(n)$.

Si $n \not\equiv 1 \bmod 7$ et $n \not\equiv 3 \bmod 7$, 7 ne divise pas $\beta(n)$. Si l'on a $n \equiv 1 \bmod 7$ ou $n \equiv 3 \bmod 7$, alors $\beta(n) \equiv -7^2 \bmod 7^3$, et dans ce cas $7^3 \nmid \beta(n)$.

Si $n \not\equiv 3 \bmod 7$ et $n \not\equiv -2 \bmod 7$, 7 ne divise pas $\delta(n)$. Si l'on a $n \equiv 3 \bmod 7$ ou $n \equiv -2 \bmod 7$, alors $\delta(n) \equiv -7^2 \bmod 7^3$. D'où l'assertion (1).

Or puisque $|n|$ est ≥ 3, on a les inégalités $|\alpha(n)| > 7^2$, $|\beta(n)| > 7^2$ et $|\delta(n)| > 7^2$. Cela démontre l'assertion (ii).

Par ailleurs, le résultant de deux quelconques des polynômes α, β et δ est $-2^6 7^6$. Par suite, un diviseur premier commun à $\alpha(n)$ et $\beta(n)$ est nécessairement 2 ou 7. Les entiers $\alpha(n)$ et $\delta(n)$, ainsi que $\beta(n)$ et $\delta(n)$, possèdent la même propriété. Les assertions (i) et (ii) entraînent alors le résultat annoncé.

c) Démontrons maintenant que les représentations de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ définies par les points de 7-torsion de $E(a_n)$, $E(n^2 a_n)$ et $E((n+1)^2 a_n)$ sont *symplectiquement* isomorphes.

c.1) Supposons d'abord que 7 ne divise pas $1+n+n^2$. Le fait que n soit distinct de -1 et 0, implique que $1+n+n^2$ n'est pas la puissance 7-ième d'un entier (cf. [10], 1). Notre assertion dans ce cas, résulte alors du lemme 2.

c.2) Supposons que 7 divise $1+n+n^2$. Alors, 7 ne divise pas n. Si n n'est pas la puissance 7-ième d'un entier, le lemme 2 entraîne encore le résultat; sinon, $n+1$ n'est pas la puissance 7-ième d'un entier, et le même argument en ce qui concerne l'entier $n+1$ prouve dans ce cas notre assertion. Cela démontre le théorème 2.

BIBLIOGRAPHIE

[1] B.J. Birch, Cyclotomic fields and Kummer extensions, dans : Algebraic Number Theory, édité par J.W.S. Cassels et A. Fröhlich, Academic Press (1967), 85–93.

[2] H. Darmon et A. Granville, On the equations $z^m = F(x,y)$ and $Ax^p + By^q = Cz^r$, preprint, 1995.

[3] E. Halberstadt et A. Kraus, Sur la comparaison galoisienne des points de torsion des courbes elliptiques, C. R. Acad. Sci. Paris, Série I, 322 (1996), 313–316.

[4] E. Kani et W. Schanz, Diagonal quotient surfaces, preprint, 1995.

[5] A. Kraus, Sur le défaut de semi-stabilité des courbes elliptiques à réduction additive, Manuscripta Math., 69 (1990), 353–385.

[6] A. Kraus et J. Oesterlé, Sur une question de B. Mazur, Math. Ann., 293 (1992), 259–275.

[7] B. Mazur, Rational isogenies of prime degree, Invent. Math., 44 (1978), 129–162.

[8] B. Mazur, Questions about number, New directions in mathematics, 1995 (à paraître).

[9] J.-F. Mestre, Courbes elliptiques et groupe des classes d'idéaux, J. Crelle, 343 (1983), 23–35.

[10] T. Nagell, Des équations indéterminées $x^2+x+1=y^n$ et $x^2+x+1=3y^n$, Norsk. M. F. Skriffer, Série I (1921).

[11] J.-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Invent. Math., 15 (1972), 259–331.

[12] J. Silverman, The arithmetic of elliptic curves, G.T.M. 106, Springer-Verlag (1986).

[13] J. Tate, Algorithm for determining the type of a singular fiber in an elliptic pencil, Modular functions of one variable IV, Lecture Notes in Math. 476, Springer-Verlag (1975), 33–52.

[14] J. Vélu, Isogénies entre courbes elliptiques, C. R. Acad. Sci. Paris, Série I, 273 (1971), 238–241.

Manuscrit reçu le 6 novembre 1995,
accepté le 8 mars 1996.

Alain KRAUS,
Université de Paris VI
Institut de Mathématiques
Case 247
4, place Jussieu
75252 Paris Cedex 05 (France).
kraus@mathp6.jussieu.fr