ACTA ARITHMETICA
XXVI (1975)

Points d'ordre $2p^h$ sur les courbes elliptiques

par

Y. HELLEGOUARCH (Caen)

1. Introduction. Etant donné un nombre premier p, on sait [10] qu'il existe une constante $C(p)$ telle qu'aucune courbe abélienne définie sur $\boldsymbol{Q}$ n'admette de point rationnel d'ordre p^h pour $h > C(p)$; cependant la valeur numérique de $C(p)$ pour p quelconque n'est pas connue.

D'autre part, il a été démontré ([4], [5]) qu'aucune courbe elliptique définie sur $\boldsymbol{Q}$ n'admet de point rationnel d'ordre $2p^2$, lorsque p est un nombre premier > 3 pour lequel l'équation de Fermat:

$$x_1^p + x_2^p + x_3^p = 0 \tag{1}$$

n'a que des solutions triviales.

On trouve aussi dans [1] la démonstration du théorème suivant: Si la courbe elliptique $y^2 = x^4 + ax^2 + b$ définie sur $\boldsymbol{Q}$ possède un point rationnel d'ordre p^2, où p désigne un nombre premier > 3, alors la courbe d'équations:

$$z^p - t^p = 1,$$
$$z^p + t^p = r^p$$

possède un point rationnel tel que $rtz \neq 0$ (1).

Or ceci équivaut à la même assertion pour une cubique d'équation $Y^2 = X(X^2 + CX + D)$ définie sur $\boldsymbol{Q}$, c'est-à-dire pour une cubique possédant (*a priori*) un point d'ordre 2 rationnel sur $\boldsymbol{Q}$.

Ainsi ce résultat a-t-il été obtenu par deux méthodes fort différentes (quant à la lettre sinon l'esprit) de sorte qu'il paraît difficile de mettre en doute sa validité.

C'est la raison pour laquelle je me bornerai à présenter les grandes lignes de la démonstration sans trop entrer dans des détails exposés dans

(1) Plus précisément Demjanenko affirme que cette courbe possède au moins $\frac{(p-1)(p-3)}{8}$ points rationnels distincts mais ne donne qu'une justification vague de cette assertion.

[1], [5], [7] et qu'on peut interpréter de plusieurs manières selon ses goûts personnels. Je ferai cependant une exception en introduisant des fonctions thêta, dont on pourrait certes se passer, mais qui me paraissent particulièrement bien adaptées à la situation.

La méthode que j'utiliserai est une variante simplifiée de celle de [4], [5] et les résultats seront un peu plus forts.

2. Préliminaires. Nous allons énoncer un certain nombre de lemmes qui seront utiles dans le paragraphe suivant.

Mais pour l'instant $\mathscr{A}$ désigne une courbe abélienne définie sur un corps l-adique $L = Q_l$ et P désigne un point d'ordre n dans le groupe des points de $\mathscr{A}$ rationnels sur L.

On suppose que $\mathscr{A}$ est donnée par un modèle de Weierstrass:

$$Y^2 = X^3 + AX + B \tag{2}$$

avec A et $B \in L$, $4A^3 + 27B^2 \neq 0$, et on désigne par $j(\mathscr{A})$ l'invariant modulaire de $\mathscr{A}$:

$$j(\mathscr{A}) = \frac{2^8 \cdot 3^3 A^3}{4A^3 + 27B^2}.$$

LEMME 1. *Désignons par v la valuation l-adique de L. Si $v(j(\mathscr{A})) \geqslant 0$ et si l'ordre n de P est un nombre impair $n > 1$ dont la valuation est nulle, alors la valuation de l'ordonnée des multiples de P est constante (on exclut le multiple égal à l'élément neutre !).*

Ce lemme peut se vérifier soit en considérant l'équation de division par n ([5], corollaire 3.1.1) soit en remarquant que l'image de P dans la réduction modulo l du modèle de Néron appartient à la composante de l'élément neutre du cycle réduit [7].

Nous nous proposons maintenant d'introduire des fonctions elliptiques l-adiques (voir [3] et [8]).

Soit q un élément non nul de L de valuation positive. Pour tout $t \in L$ nous poserons:

$$\xi(t) = 4 \sum_{n \in Z} \frac{q^n t}{(1-q^n t)^2} + 4 \sum_{n \in Z} \frac{q^n}{(1+q^n)^2},$$

$$\eta(t) = 4 \sum_{n \in Z} \frac{q^n t(1+q^n t)}{(1-q^n t)^3}.$$

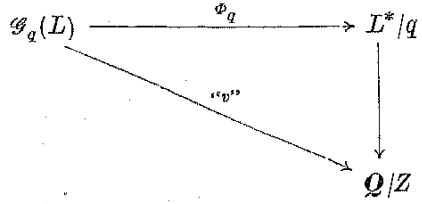
Le lieu du point $(\xi(t), \eta(t))$ est une cubique dont l'équation est de la forme:

$$\eta^2 = \xi(\xi^2 - 2S\xi + T)$$

avec S et $T \in L$; nous désignerons cette cubique par $\mathscr{T}_q$.

Désignons par $\mathscr{G}_q(L)$ le groupe des points de $\mathscr{T}_q$ rationnels sur L, on sait [8] qu'il existe un "isomorphisme de Jacobi" Φ_q entre $\mathscr{G}_q(L)$ et le groupe multiplicatif quotient L^*/q.

La valuation v de L fournit une "valuation" naturelle "v" sur $\mathscr{G}_q(L)$ suivant le diagramme:



Par abus de langage nous écrirons v au lieu de "v".

DÉFINITION. Une courbe abélienne $\mathscr{A}$ définie sur L sera appelée une *cubique de Tate* si et seulement s'il existe $q \in L^*$, de valuation positive, tel que $\mathscr{A}$ et $\mathscr{T}_q$ soient birationnellement équivalentes sur L.

Remarquons que q est alors unique et que l'on peut étendre la "valuation" v aux points de $\mathscr{A}$ rationnels sur L.

LEMME 2. *Soit une courbe abélienne $\mathscr{A}$ et soit un point P de $\mathscr{A}$ rationnel sur L et d'ordre $n = p^h$, avec p premier > 3, $p \neq l$ et $h \geqslant 1$.*

Alors si la valuation de l'ordonnée des multiples de P n'est pas constante, $\mathscr{A}$ est une cubique de Tate et $v(P) \neq 0$.

Ceci peut se vérifier analytiquement à partir de lemme 1([5] en utilisant la méthode du corollaire 1.3.2) ou bien à l'aide des modèles de Néron [7].

LEMME 3. *On suppose que l'ordre de $P = p^2$, où p est un nombre premier > 3 et on suppose que $l = p$.*

Alors $\mathscr{A}$ est une cubique de Tate et $v(pP) \neq 0$.

On peut vérifier ce résultat à l'aide de "l'hypothèse de Riemann" pour les courbes de genre 1 en utilisant les groupes quotients de Lutz ([5], ch. 2) ou, ce qui revient un peu au même, à l'aide des modèles de Néron [7].

Remarque. Quelques indications (2) pour le cas où n est une puissance de 3 sont données dans [5].

3. Points d'ordre p^h. Les résultats que nous allons énoncer dans ce paragraphe seront utilisés dans les deux paragraphes suivants.

Avant de les énoncer, nous allons introduire quelques notations.

Pour commencer donnons-nous un entier naturel n. A tout nombre réel x nous ferons correspondre le symbole $(x)_n$ qui est la distance de

(2) O. Lecacheux m'a fait remarquer que bien que proposition 3.3.1 de [5] soit essentiellement correcte, on ne peut pas dire que 3 divise C.

x à l'ensemble $n\mathbf{Z}$; remarquons que $(x)_n$ ne dépend que de la classe de x modulo $n\mathbf{Z}$. Supposons maintenant que $n = p^m$, où p est un nombre premier et m un entier $\geqslant 0$, nous désignerons par I_m l'image de l'application $x \to (x)_n$ restreinte à $\mathbf{Z}$ et par p'_m le nombre de ses éléments en sorte que:

$$p'_m = \text{Cardinal}(I_m) = \frac{p^m - 1}{2}. \tag{3}$$

Ensuite, nous dirons que deux nombres rationnels r et r' sont associés, et nous écrirons $r \sim r'$, si et seulement si $r = \pm r'$.

Soient maintenant une courbe abélienne $\mathscr{A}$ donnée sous la forme (2) avec A et $B \in \mathbf{Q}$ et un point P de $\mathscr{A}$ rationnel sur $\mathbf{Q}$ et d'ordre p^h, avec p premier >3 et $h \geqslant 2$.

Théorème 1. *Soit $i \in \mathbf{Z}/p^h\mathbf{Z}$ non nul, et soit y_i l'ordonnée du point iP. Il existe (on utilise la notation (3)):*

$$\begin{aligned} &p'_1 \text{ entiers } a_{\nu_1},\ \nu_1 \in I_1,\\ &p'_2 \text{ entiers } a_{\nu_2},\ \nu_2 \in I_2,\\ &\cdots\cdots\cdots\cdots\\ &p'_h \text{ entiers } a_{\nu_h},\ \nu_h \in I_h \end{aligned}$$

tous positifs et premiers entre eux deux à deux, et il existe une constante $\gamma \in \mathbf{Q}^*$ tels que [3]:

$$y_i \sim \gamma \prod_{m=1}^{h} \prod_{\nu_m \in I_m} a_{\nu_m}^{(i\nu_m)_{p^m}}.$$

Preuve. Puisque pour presque toutes les valuations v de $\mathbf{Q}$ les y_i sont des unités, il suffit de vérifier que si $v(y_i)$ n'est pas constant lorsque i parcourt l'ensemble $\mathbf{Z}/p^h\mathbf{Z}$ moins 0, il existe $\nu_m \in I_m$ et un entier a_{ν_m} tels que:

$$v(y_i) = \text{constante} + (i\nu_m)_{p^m} v(a_{\nu_m}).$$

D'après le lemme 2, $\mathscr{A}$ est une cubique de Tate et $v(P) \neq 0$ lorsque $v(p) = 0$. D'après le lemme 3 appliqué au point $p^{h-2}P$, c'est encore vrai lorsque $v(p) > 0$.

En utilisant les fonctions thêta de Jacobi–Tate (ou le modèle de Néron) on obtient:

$$v(y_i) = \text{constante} + (v(iP))_1 v(q).$$

[3] Il s'agit bien d'un double produit [3] et non d'un simple produit comme il est dit par erreur dans [5].

Comme il existe $m \in \{1, \ldots, h\}$ et $\nu_m \in I_m$ tels que:

$$(v(P))_1 = \nu_m / p^m$$

on a:

$$v(y_i) = \text{constante} + (i\nu_m)_{p^m} \frac{v(q)}{p^m}.$$

Finalement, on définit a_{ν_m} en lui donnant pour valuation v-adique le nombre entier positif $v(q)/p^m$ lorsque $(v(P))_1 = \nu_m/p^m$; zéro pour les autres valuations.

Corollaire 1. *Posons $Q = p^{h-1}P$ et désignons par z_i l'ordonnée du point iQ lorsque $i \in \mathbf{F}_p^* = \mathbf{Z}/p\mathbf{Z}$ moins 0, on a:*

$$z_i \sim \gamma \prod_{\nu_1 \in I_1} A_{\nu_1}^{(i\nu_1)_p}$$

où les:

$$A_{\nu_1} = \prod_{(\nu_h)_p = \nu_1} a_{\nu_h}^{p^{h-1}}$$

pour $\nu_1 \in I_1$, sont des puissances d'ordre p^{h-1} de nombres entiers premiers entre eux deux à deux.

Remarque. On pourra trouver dans [4] ou [5] quelques conséquences de ce corollaire.

4. Points d'ordre $2p^h$. Le résultat essentiel de ce paragraphe est la démonstration du corollaire 2, corollaire qui implique (entre autres choses) que si une courbe abélienne $\mathscr{A}$ définie sur $\mathbf{Q}$ possède un point d'ordre $2p^2$, avec p premier > 3, l'équation de Fermat (1) possède des solutions non-triviales (et dans le "deuxième cas du théorème Fermat").

Nous nous donnerons la courbe $\mathscr{A}$ par l'équation:

$$Y^2 = X(X^2 + CX + D)$$

avec C et $D \in \mathbf{Q}$, $D(C^2 - 4D) \neq 0$.

On sait qu'à la courbe $\mathscr{A}$ est associée une courbe isogène $\mathscr{A}_1$ d'équation:

$$Y_1^2 = X_1(X_1^2 - 2CX_1 + G)$$

avec $G = C^2 - 4D$.

Les formules de [11] montrent que si l'on choisit convenablement les périodes de $\mathscr{A}$ et si l'on pose:

$$V(t) = C_1 \frac{\theta_{01}}{\theta_{11}}(t), \qquad U(t) = C_2 \frac{\theta_{10}\theta_{00}}{\theta_{01}\theta_{11}}(t)$$

avec des constantes complexes convenables C_1 et C_2, cette isogénie est donnée par les formules:

$$(4)\qquad \begin{aligned} x(t) &= V^2(t), & x_1(2t) &= U^2(t),\\ y(t) &= V^2(t)\,U(t), & y_1(2t) &= 2U^2(t)\,V(2t), \end{aligned}$$

qui montrent que U et V jouent des rôles presque symétriques lorsque l'on passe de $\mathscr{A}$ à $\mathscr{A}_1$.

Lemme 4. *U et V sont liées par les relations d'addition suivantes:*

$$\frac{V(\alpha+\beta)+V(\alpha-\beta)}{V(\alpha+\beta)-V(\alpha-\beta)} = -\frac{U(\alpha)}{U(\beta)}.$$

Preuve. Les formules (7) de [11], § 22, nous fournissent:

$$\begin{aligned} &\theta_{00}\theta_{10}\big(\theta_{01}(\alpha+\beta)\,\theta_{11}(\alpha-\beta)+\theta_{01}(\alpha-\beta)\,\theta_{11}(\alpha+\beta)\big)\\ &\qquad = 2\theta_{01}(\alpha)\,\theta_{11}(\alpha)\theta_{00}(\beta)\,\theta_{10}(\beta),\\ &\theta_{00}\theta_{10}\big(\theta_{01}(\alpha+\beta)\theta_{11}(\alpha-\beta)-\theta_{01}(\alpha-\beta)\,\theta_{11}(\alpha+\beta)\big)\\ &\qquad = -\,2\theta_{00}(\alpha)\,\theta_{10}(\alpha)\,\theta_{01}(\beta)\,\theta_{11}(\beta) \end{aligned}$$

et en passant au quotient on obtient le résultat de l'énoncé.

Théorème 2. *Reprenons les notations du théorème* 1 *et supposons U et V liés à x et y par les relations* (4).

Pour tout $m\in\{1,\dots,h\}$ il existe $2p'_m$ entiers positifs a_{ν_m} et b_{ν_m}, $\nu_m\in I_m$, premiers entre eux deux à deux, et il existe deux constantes λ et $\mu\in\boldsymbol{Q}^*$ tels que:

$$U(it)\sim\lambda\prod_{m=1}^{h}\prod_{\nu_m\in I_m} a_{\nu_m}^{(i\nu_m)p^m},$$

$$V(it)\sim\mu\prod_{m=1}^{h}\prod_{\nu_m\in I_m} b_{\nu_m}^{(i\nu_m)p^m}$$

t désignant le paramètre d'un point P d'ordre p^h et i un élément non nul de $\boldsymbol{Z}/p^h\boldsymbol{Z}$.

Preuve. 1) La première partie de la démonstration consiste à montrer que si v est une valuation non-archimédienne de $\boldsymbol{Q}$ telle que $v\big(y(it)\big)$ et $v\big(y_1(it)\big)$ soient des constantes, alors $v\big(U(it)\big)$ et $v\big(V(it)\big)$ sont des constantes lorsque i parcourt $\boldsymbol{Z}/p^h\boldsymbol{Z}$ moins 0.

En effet cette hypothèse et les relations (4) entraînent:

$$v(2)+v\big(y^2(it)\big)-v\big(y_1(it)\big) = 4v\big(V(t)\big)-v\big(V(2t)\big) = C^{te}.$$

En posant $f(t)=v\big(V(t)\big)+K$, K étant une constante convenable, on a:

$$f(2t) = 4f(t)$$

d'où

$$f(2^nt) = 4^nf(t)$$

et $f(t)=0$, puisqu'il existe un entier n tel que $t\equiv 2^nt$ modulo les périodes.

Un raisonnement identique est valable pour U.

2) Il résulte de la première partie et de la démonstration du théorème 1, que si $v\big(U(it)\big)$ et $v\big(V(it)\big)$ ne sont pas tous les deux constants, alors $\mathscr{A}$ ou $\mathscr{A}_1$ (donc $\mathscr{A}$ et $\mathscr{A}_1$) sont des cubiques de Tate.

L'utilisation des fonctions thêta l-adiques fournit, comme pour le théorème 1, les nombres a_{ν_m} et b_{ν_m} (c.q.f.d.).

Dans le corollaire suivant, $\mathscr{C}$ désigne la courbe projective d'équations:

$$(5)\qquad \begin{aligned} x_1^{p^{h-1}}+x_2^{p^{h-1}} &= x_3^{p^{h-1}},\\ x_1^{p^{h-1}}-x_2^{p^{h-1}} &= x_4^{p^{h-1}}. \end{aligned}$$

Corollaire 2. *Si $\mathscr{A}$ admet un point rationnel d'ordre $2p^h$, la courbe $\mathscr{C}$ possède au moins $(p-1)/2$ points distincts non triviaux dans l'espace projectif $\boldsymbol{P}_3(\boldsymbol{Q})$.*

Remarque. On dit qu'un point (x_1,x_2,x_3,x_4) de $\boldsymbol{P}_3(\boldsymbol{Q})$ est trivial si et seulement si on peut choisir les x_i dans l'ensemble $\{0,1,-1\}$.

Preuve. Désignons par P un point de $\mathscr{A}$, d'ordre p^h, rationnel sur $\boldsymbol{Q}$, et posons $Q=p^{h-1}P$. Comme dans la démonstration du corollaire 1, on déduit du théorème 2 que pour $i\in\boldsymbol{F}_p^*$, on a:

$$U(ip^{h-1}t)\sim\lambda\prod_{\nu_1\in I_1} A_{\nu_1}^{(i\nu_1)p},$$

$$V(ip^{h-1}t)\sim\mu\prod_{\nu_1\in I_1} B_{\nu_1}^{(i\nu_1)p}$$

où les A_{ν_1} et B_{ν_1} sont des puissances d'ordre p^{h-1} d'entiers positifs premiers entre eux deux à deux.

En portant ce résultat dans le lemme 4, avec $\alpha=3ip^{h-1}t$ et $\beta=ip^{h-1}t$, on a:

$$(6)\qquad \frac{\prod_{\nu_1\in I_1} B_{\nu_1}^{(4i\nu_1)p}+\prod_{\nu_1\in I_1} B_{\nu_1}^{(2i\nu_1)p}}{\prod_{\nu_1\in I_1} B_{\nu_1}^{(4i\nu_1)p}-\prod_{\nu_1\in I_1} B_{\nu_1}^{(2i\nu_1)p}} = -\frac{\prod_{\nu_1\in I_1} A_{\nu_1}^{(3i\nu_1)p}}{\prod_{\nu_1\in I_1} A_{\nu_1}^{(i\nu_1)p}}.$$

Nous devons maintenant distinguer deux cas suivant que les B_{ν_1} ne sont pas tous impairs, ou qu'ils le sont.

Dans le premier cas l'équation (6) donne (5) en écrivant les fractions sous forme irréductible et en égalant numérateurs et dénominateurs.

Dans le second cas on obtient par le même procédé les relations:

$$y_1^{p^{h-1}} + y_2^{p^{h-1}} = 2y_3^{p^{h-1}},$$
$$y_1^{p^{h-1}} - y_2^{p^{h-1}} = 2y_4^{p^{h-1}}.$$

En ajoutant et retranchant ces relations membre à membre, et en divisant par 2, on obtient:

$$y_1^{p^{h-1}} = y_3^{p^{h-1}} + y_4^{p^{h-1}},$$
$$y_2^{p^{h-1}} = y_3^{p^{h-1}} - y_4^{p^{h-1}}$$

ce qui redonne les équations (5).

Il reste à voir qu'on obtient $(p-1)/2$ solutions non triviales distinctes.

Pour cela déduit du lemme 3 que l'un des nombres A_{ν_1} ou $B_{\nu_1'}$ est divisible par p (la même observation vaudrait pour 2). Alors on déduit des formules (6) et du calcul de la valuation de $x_1 x_2 x_3 x_4$ que lorsque i parcourt I_1 les solutions de (5) sont distinctes. En particulier on trouve que pour $p = 5$ une solution au moins est telle que $x_1 x_2 x_3 x_4 \equiv 0$ (modulo p) alors que pour $p > 5$ elles possèdent toutes cette propriété.

Remarques. 1) Les équations (5) sont équivalentes aux équations:

$$x_3^{p^{h-1}} + x_4^{p^{h-1}} = 2x_1^{p^{h-1}},$$
$$x_3^{p^{h-1}} - x_4^{p^{h-1}} = 2x_2^{p^{h-1}}. \tag{7}$$

2) La courbe d'équations (5) se trouve sur la surface:

$$x_1^{2p^{h-1}} - x_2^{2p^{h-1}} = (x_3 x_4)^{p^{h-1}} \tag{8}$$

et sur la surface:

$$x_3^{2p^{h-1}} - x_4^{2p^{h-1}} = 4(x_1 x_2)^{p^{h-1}}. \tag{9}$$

3) Dans [1] il est dit que, pour $h = 2$, la courbe (5) possède au moins $\frac{(p-1)(p-3)}{8}$ points distincts (qu'on obtiendrait en portant dans le le lemme 4 toutes les valeurs possibles de α et β); cela me paraît plus délicat à démontrer rigoureusement par la méthode précédente.

4) Un théorème de Hubert [6] permet de montrer que si une courbe abélienne $\mathscr{A}$ définie sur $\boldsymbol{Q}$ admet un point P d'ordre $2p^h$ rationnel sur un corps de nombres galoisien L de degré m et si $(m, 3p(p-1)) = 1$, alors P est rationnel sur $\boldsymbol{Q}$. Cette remarque permet d'étendre le domaine d'application du corollaire 2.

5. Groupe $(2, 2p^h)$. Lorsque la courbe $\mathscr{A}$ possède trois points rationnels d'ordre 2, son équation peut s'écrire (de trois manières différentes) sous la forme:

$$Y^2 = X(X-b)(X+c) \tag{10}$$

avec b et $c \in \boldsymbol{Q}$ et $bc(b+c) \neq 0$.

Le théorème 5 de [3] montre que les nombres a_{ν_m} du théorème 2 sont alors des carrés de nombres entiers.

En choisissant parmi les équations de la forme (10) une de celles pour lesquelles tous les a_{ν_h} du théorème 2 sont impairs, on obtient le corollaire suivant dans lequel $\mathscr{D}$ désigne la courbe projective d'équation:

$$z_1^{2p^{h-1}} + z_2^{2p^{h-1}} = z_3^{2p^{h-1}}. \tag{11}$$

Corollaire 3. *Si $\mathscr{A}$ admet un sous-groupe de points rationnels du type $(2, 2p^h)$, la courbe $\mathscr{D}$ possède au moins $(p-1)/2$ points distincts non triviaux dans le plan projectif $\boldsymbol{P}_2(\boldsymbol{Q})$.*

Preuve. La démonstration du corollaire 2 fournit les relations:

$$x_1^{p^{h-1}} + x_2^{p^{h-1}} = x_3^{2p^{h-1}},$$
$$x_1^{p^{h-1}} - x_2^{p^{h-1}} = x_4^{2p^{h-1}}$$

et l'équation (8) donne:

$$x_1^{2p^{h-1}} - x_2^{2p^{h-1}} = (x_3 x_4)^{2p^{h-1}}.$$

Remarques. 1) L'équation (9) donne:

$$r_1^{4p^{h-1}} - r_2^{4p^{h-1}} = 4r_3^{p^{h-1}}.$$

2) Si l'on choisit l'équation (10) pour laquelle un a_{ν_h} est pair, les équations (8) et (9) fournissent encore:

$$s_1^{2p^{h-1}} - s_2^{2p^{h-1}} = 4s_3^{2p^{h-1}}$$

et

$$t_1^{4p^{h-1}} - t_2^{4p^{h-1}} = t_3^{p^{h-1}}.$$

6. Réciproque partielle du corollaire 3. On considère l'équation diophantienne:

$$ax^{2p^h} + by^{2p^h} + cz^{2p^h} = 0 \tag{12}$$

dans laquelle les inconnues sont x, y, z et les données sont le nombre premier impair p, l'exposant $h > 0$ et les trois entiers non nuls et premiers entre eux deux à deux a, b, c.

Nous dirons qu'une solution (α, β, γ) de (12) est "primitive" lorsque α, β, γ sont des entiers non nuls tels que $a\alpha$, $b\beta$, $c\gamma$ soient premiers entre eux deux à deux.

A toute solution primitive (a, β, γ) de (12) nous associerons la courbe abélienne $\mathscr{A}_{a,\beta,\gamma}$ d'équation:

$$Y^2 = X(X - b\beta^{2p^h})(X + c\gamma^{2p^h}).$$

La "réciproque partielle du corollaire 3" que nous avons en vue est le théorème suivant.

THÉORÈME 4. *Si l'équation* (12) *admettait une infinité de solutions primitives* (a, β, γ) *telles que* $a\beta\gamma$ *soit divisible par* $2p$, *il existerait un corps de nombres algébriques* L *ne dépendant que de* a, b, c *et* p^h *dans lequel toutes les courbes* $\mathscr{A}_{a,\beta,\gamma}$ *admettraient un groupe complet de points d'ordre* $2p^h$.

Preuve. Nous nous bornerons à présenter les grandes lignes de la démonstration, renvoyant à [5], ch. 5, pour les détails.

1) Soit un corps de nombres K contenu dans une clôture algébrique $\overline{Q}$ de Q et contenant toutes les racines d'ordre $4p^h$ de 2^8, a^2, b^2 et c^2 et soit une valuation non-archimédienne v de K telle que:

$$v(abc\alpha\beta\gamma) > 0.$$

Alors on vérifie par un calcul direct que $\mathscr{A}_{a,\beta,\gamma}$ est une cubique de Tate sur K_v et que son paramètre q est puissance d'ordre $4p^h$ d'un élément de K_v^*.

2) Soit $P = (x, y)$ un point d'ordre p^h sur $\mathscr{A}_{a,\beta,\gamma}$ rationnel sur $\overline{Q}$. On vérifie que l'extension $K(x, y)/K$ est non ramifiée.

Lorsque $v(abc\alpha\beta\gamma) = 0$, cela se voit en montrant que le discriminant de l'équation de division par p^h est de valuation nulle.

Lorsque $v(abc\alpha\beta\gamma) > 0$, cela se voit en utilisant les fonctions thêta de Jacobi–Tate.

3) Les degrés des extensions $K(x, y)/K$ sont tous majorés par $p^{2h}-1$.

Finalement il existe un corps de nombres L ne dépendant que de K et de p^{2h} tel que toute extension non ramifiée M de K de degré $\leqslant p^{2h}-1$ et contenue dans $\overline{Q}$ soit contenue dans L (on peut utiliser un théorème bien connu de Hermite [9]).

Remarques. 1) Une réciproque véritable du corollaire 3 consisterait à établir que pour $(a, b, c) = (1, 1, -1)$ et pour une solution (α, β, γ) de (12) la courbe $\mathscr{A}_{a,\beta,\gamma}$ possède un point d'ordre p^{h+1} rationnel sur Q.

Il serait déjà très intéressant de pouvoir montrer qu'elle possède un point d'ordre p^h rationnel sur Q.

2) Dans le même ordre d'idée, il serait intéressant de démontrer que l'équation modulaire qui relie $j(\tau)$ à $j(2p^h\tau)$ n'admet qu'un nombre fini de solutions dans tout corps de nombres.

Références

[1] V. A. Demjanenko, *Points d'ordre fini sur les courbes elliptiques* (Russe), Acta Arith. 19 (1971), p. 185–194.

[2] Y. Hellegouarch, *Points d'ordre fini sur les variétés abéliennes*, Bulletin Soc. Math. de France, Mémoire n° 25, 1969, p. 107–112.

[3] — *Etude des points d'ordre fini des variétés abéliennes de dimension un définies sur un anneau principal*, Journ. Reine. Angew. Math. 244 (1970), p. 20–36.

[4] — *Points d'ordre fini sur les courbes elliptiques*, C. R. Acad. Sc. Paris, 273 (1971), p. 540–543.

[5] — *Courbes elliptiques et équation de Fermat*, Thèse, Université de Besançon (1972).

[6] M. Hubert, *Torsion des courbes elliptiques*, C. R. Acad. Sc. Paris, 276 (1973), p. 661–663.

[7] A. Néron, *Modèles minimaux des variétés abéliennes*, Publications Mathématiques I. H. E. S. n° 21 (1964).

[8] P. Roquette, *Analytic theory of elliptic functions over local fields*, 1970.

[9] P. Samuel, *Théorie algébrique des nombres*, Paris 1967.

[10] J.-P. Serre, *p-torsion des courbes elliptiques*, Séminaire Bourbaki, n° 380, (1969/1970), p. 1–14.

[11] H. Weber, *Lehrbuch der Algebra*, t. III, New York 1908.

Reçu le 29. 9. 1973 (464)