Invariants des courbes de Frey-Hellegouarch et grands groupes de Tate-Shafarevich

Abderrahmane Nitaj (Saarbrücken)

1. Introduction

Soit E une courbe elliptique définie sur $\mathbb{Q}$, et Ш son groupe de Tate-Shafarevich, définie par

$$Ш = \ker\left(H^1(\mathbb{Q}, E) \longrightarrow \prod_v H^1(\mathbb{Q}_v, E)\right),$$

où v décrit l'ensemble des places finies et ∞ de $\mathbb{Q}$ (voir [30] pour une définition des groupes $H^1(\mathbb{Q}, E)$ et $H^1(\mathbb{Q}_v, E)$). Ce groupe est abélien, et sa finitude pour toute courbe elliptique est encore conjecturale, mais, en 1987, Rubin [29] a donné un exemple d'une famille infinie de courbes elliptiques pour lesquelles Ш est fini. Ces courbes sont à multiplication complexe, et définies sur un corps quadratique imaginaire. En 1989, Kolyvagin [18] a montré que Ш est fini pour toute courbe elliptique modulaire définie sur $\mathbb{Q}$ et de rang analytique 0 ou 1. D'autre part, Cassels [4] et Bölling [3] ont montré que Ш peut être arbitrairement grand (voir aussi [11] pour d'autres résultats). D'autres méthodes effectives ont été développées par Kramer [19], Mai et Murty [23] pour déterminer des courbes elliptiques ayant un grand groupe de Tate-Shafarevich, mais les premières estimations de l'ordre de Ш ont été conjecturées par Manin et Lang (voir [24] et [21]). Dans cette direction, Goldfeld et Szpiro ([14]) ont proposé la conjecture suivante :

Conjecture 1. *Pour tout $\varepsilon > 0$, il existe une constante $C_1(\varepsilon) > 0$ telle que si $E/\mathbb{Q}$ est une courbe elliptique de conducteur N et de groupe de Tate–Shafarevich* Ш*, alors*

$$|Ш| \leq C_1(\varepsilon) N^{\frac{1}{2}+\varepsilon}.$$

1991 *Mathematics Subject Classification.* 11G05, 11G40, 11Y99.

Key words and phrases. Courbe de Frey-Hellegouarch, groupe de Tate-Shafarevitch, conjecture de Goldfeld-Szpiro.

Research supported by the Marie Curie TMR programme of the European Community under contract ERBFMBICT960848.

Cette conjecture fait partie d'autres conjectures formulées en 1993 par Mai et Murty dans un travail non publié (voir par exemple [27]). D'autre part, C.S. Rajan [27] a montré son analogue pour un corps de fonctions global $K/\mathbb{F}_q$, où la caractéristique de $\mathbb{F}_q$ est impair. Par la suite, Goldfeld et Lieman ont montré que cette conjecture est vraie pour certaines familles de courbes elliptiques (voir [13]). Ces courbes sont de rangs 0 ou 1, et leurs j-invariants, différents de 0 et 1728, appartiennent à des ensembles finis. En admettant certaines conjectures, de Weger [32] a proposé la conjecture suivante.

Conjecture 2 (de Weger). *Pour tout $\varepsilon > 0$, il existe une constante $C_2(\varepsilon) > 0$ et une infinité de courbes elliptiques définies sur $\mathbb{Q}$, de conducteurs N, et de groupes de Tate-Shafarevich* Ш*, vérifiant :*

$$N \leq C_2(\varepsilon)|\text{Ш}|^{2+\varepsilon}.$$

Cette conjecture est essentiellement relative aux courbes généralisées de Frey-Hellegouarch, définies par l'équation

$$y^2 = x(x-s)(x-t) = x^3 - (s+t)x^2 + stx,$$

où s et t sont deux entiers quelconques. Pour comparer le conducteur N et l'ordre du groupe de Tate-Shafarevich $|\text{Ш}|$, on introduit le rapport :

$$\gamma = \gamma(E) = 2\frac{\log|\text{Ш}|}{\log N}. \tag{1}$$

La plus grande valeur connue actuellement de ce rapport provient de l'exemple suivant (voir Table VI) :

$$\begin{aligned} Y^2 + XY + Y =& X^3 + X^2 - 3532978428694464611454768601X \\ & - 80827582979574301299537222938555582992327, \end{aligned}$$

avec

$$\gamma = 2 \times \frac{\log 1832^2}{\log 6305720190} \approx 1.332.$$

Dans [32], de Weger a donné 11 exemples de courbes elliptiques liées aux courbes de Frey-Hellegouarch avec $|\text{Ш}|/\sqrt{N} \geq 1$, dont le meilleur vérifie $|\text{Ш}|/\sqrt{N} \approx 6.893$. Nous exhibons ici 47 autres exemples de telles courbes, dont l'exemple ci-dessus pour lequel on a $|\text{Ш}|/\sqrt{N} \approx 42.265$. En fait, comme le suggère la conjecture 2, le rapport $|\text{Ш}|/\sqrt{N}$ n'aura plus de sens si la constante $C_1(\varepsilon)$ dans la conjecture 1 vérifie $\lim_{\varepsilon\to 0} C_1(\varepsilon) = \infty$. Le choix du rapport (1) semble donc plus approprié.

On utilisera dans tout cet article les notations habituelles suivantes :

Δ le discriminant minimal de E,

N le conducteur de E,

r	le rang de E,
$\lvert Ш \rvert$	l'ordre du groupe de Tate-Shafarevich de E,
ω	l'invariant différentiel de E,
Ω	La période $\int_{E(\mathbb{R})} \lvert\omega\rvert$ de E,
R	le régulateur de E.
T	$E(\mathbb{Q})_{\mathrm{tors}}$, le groupe des points de torsion de E,
C	le nombre de Tamagawa de E.

Les conjectures 1 et 2 ont été établies pour les courbes elliptiques vérifiant la conjecture de Birch et Swinnerton-Dyer. En effet, celle-ci permet de relier la série L d'une courbe elliptique E à d'autres quantités, via la formule :

$$\lim_{s\to 1} \frac{L(s)}{(s-1)^r} = \frac{1}{r!} L^{(r)}(1) = \frac{\Omega R C \lvert Ш \rvert}{\lvert T\rvert^2}. \tag{2}$$

Le calcul de $\lvert Ш \rvert$ nécessite donc la connaissance des autres paramètres intervenant dans la relation ci-dessus. Ceci peut s'avérer très difficile si le conducteur est assez grand (voir partie 2). En utilisant la relation (2), le rapport (1) devient :

$$\gamma = 2\frac{\log\left(\frac{\lvert T\rvert^2}{\Omega C}\right)}{\log N} + 2\frac{\log\left(\frac{L^{(r)}(1)}{R r!}\right)}{\log N}.$$

Si on admet l'hypothèse de Riemann pour la fonction L (voir par exemple [14]), alors il existe une constante $C_3(\varepsilon) > 0$ telle que

$$L^{(r)}(1) \leq C_3(\varepsilon) N^{\varepsilon}.$$

D'autre part, la conjecture de Lang (voir [21]) implique qu'il existe une constante $C_4(\varepsilon) > 0$ telle que le régulateur R vérifie

$$R \geq C_4(\varepsilon) N^{-\varepsilon},$$

si le rang r est borné. Ainsi, le rapport γ vérifie :

$$\gamma \leq 2\frac{\log\left(\frac{\lvert T\rvert^2}{\Omega C}\right)}{\log N} + 2\frac{\log\left(\frac{C_3(\varepsilon)}{C_4(\varepsilon)}\right)}{\log N} + 4\varepsilon.$$

Pour les courbes elliptiques ayant un grand conducteur ($N > 10^{10}$ dans cet article) ou qui ont un rang non nul, on calculera donc le rapport

$$\delta = 2\frac{\log\left(\frac{\lvert T\rvert^2}{\Omega C}\right)}{\log N}. \tag{3}$$

Ce rapport a l'avantage d'ignorer le rang, le régulateur, la valeur de $L^{(r)}(1)$ ainsi que l'ordre du groupe de Tate-Shafarevich.

Le but de cet article est de décrire un certain nombre de propriétés des courbes de Frey-Hellegouarch et de leurs isogènes. On montre ainsi comment déterminer toutes les quantités nécessaires pour le calcul du rapport (3). On applique ensuite cette étude pour déterminer des courbes elliptiques ayant un grand groupe de Tate-Shafarevich.

Dans la partie 2, on décrit des propriétés communes à une courbe de Frey-Hellegouarch et à ses isogènes. Dans les parties 3 et 4, on explicite séparément les quantités nécessaires au rapport (3) pour chaque courbe. Dans la partie 5, on donne une méthode pour déterminer des paramètres s et t qui peuvent donner de grands rapports (3). Si le conducteur N vérifie $N \leq 10^{10}$ et le rang est nul, on calcule dans ce cas le rapport (1). Dans la partie 6, on donne des tables listant des courbes elliptiques ayant les plus grandes valeurs connues pour le rapport (1). Enfin, on donne dans la partie 7 l'expression des courbes elliptiques définies sur $\mathbb{Q}$, de sous-groupe de torsion donné. Cette partie servira pour la preuve de certaines propositions de cet article.

Tous les calculs ont été effectués à l'aide d'une combinaison du langage `C` et du système de calcul `SIMATH` [31]. Les résultats ont été ensuite vérifiés à l'aide de `PARI-GP` [2], `APECS` [6] et `MWRANK` [7].

Toutes les courbes elliptiques des Tables V et VI sont modulaires (voir Remarque 2.1) et sont telles que leurs fonctions L vérifient $L(1) \neq 0$. Ces courbes sont donc de rang nul. Ainsi, d'après les travaux de Kolyvagin, le rang de leurs groupes de Tate-Shafarevich est fini et toutes ces courbes vérifient la conjecture de Birch et Swinnerton-Dyer (voir [15] et [18]). Il en résulte que tous les exemples listés dans ces tables ne dépendent d'aucune conjecture.

2. Les courbes de Frey-Hellegouarch

Soient s et t deux entiers tels que (s,t) est sans facteurs carrés. Pour tout nombre premier $p | st(s-t)$, on attribue un couple (A_p, B_p) à l'aide de la table I.

Table I		
$\max(\mathrm{ord}_p(s), \mathrm{ord}_p(t), \mathrm{ord}_p(s-t))$	A_p	B_p
$\mathrm{ord}_p(s)$	s	t
$\mathrm{ord}_p(t)$	t	s
$\mathrm{ord}_p(s-t)$	$s-t$	$-t$

Dans toute la suite, $\left(\frac{\cdot}{p}\right)$ désignera le symbole de Legendre.

Les courbes de Frey-Hellegouarch sont définies par l'équation :

$$E_1 : \ y^2 = x(x-s)(x-t) = x^3 - (s+t)x^2 + stx,$$

où s et t sont deux entiers quelconques. Le discriminant minimal Δ_1 et les covariants $c_{4,1}$ et $c_{6,1}$ sont :

$$\begin{aligned}\Delta_1 &= 2^4 u_0^{-12} s^2 t^2 (s-t)^2,\\ c_{4,1} &= 2^4 u_0^{-4}(s^2 - st + t^2),\\ c_{6,1} &= 2^5 u_0^{-6}(s+t)(s-2t)(2s-t),\end{aligned}$$

avec $u_0 \in \{1, 2\}$ (voir Table II). La courbe E_1 admet au moins trois isogènes E_2, E_3 et E_4 (voir [25]). La courbe E_2 est définie par l'équation :

$$E_2 : \; y^2 = x\left(x^2 + 2(s+t)x + (s-t)^2\right),$$

avec les quantités :

$$\begin{aligned}\Delta_2 &= 2^8 u_0^{-12} st(s-t)^4,\\ c_{4,2} &= 2^4 u_0^{-4}(s^2 + 14st + t^2),\\ c_{6,2} &= 2^6 u_0^{-6}(s+t)(s^2 - 34st + t^2),\end{aligned}$$

où $u_0 \in \{1, 2, 4\}$ (voir Tables III et IV). La courbe E_3 est définie par l'équation :

$$E_3 : \; y^2 = x\left(x^2 - 2(2s-t)x + t^2\right),$$

avec :

$$\begin{aligned}\Delta_3 &= 2^8 u_0^{-12} st^4(s-t),\\ c_{4,3} &= 2^4 u_0^{-4}(16s^2 - 16st + t^2),\\ c_{6,3} &= 2^6 u_0^{-6}(2s-t)(32s^2 - 32st - t^2),\end{aligned}$$

et $u_0 \in \{1, 2, 4\}$ (voir Tables III et IV). Enfin, la courbe E_4 est définie par l'équation :

$$E_4 : \; y^2 = x\left(x^2 + 2(s-2t)x + s^2\right),$$

avec :

$$\begin{aligned}\Delta_4 &= -2^8 u_0^{-12} s^4 t(s-t),\\ c_{4,4} &= 2^4 u_0^{-4}(s^2 - 16st + 16t^2),\\ c_{6,4} &= 2^6 u_0^{-6}(s-2t)(s^2 + 32st - 32t^2),\end{aligned}$$

et $u_0 \in \{1, 2, 4\}$ (voir Tables III et IV).

Si $d \neq 0$ est un entier, la tordue quadratique par d de $E_i(s,t)$, $1 \leq i \leq 4$, est $E_i^{(d)}(s,t) = E_i(ds, dt)$. En particulier

$$E_i^{(d^2)}(s,t) = E_i(d^2 s, d^2 t) = E_i(s,t).$$

On peut se limiter alors dans la suite aux entiers s et t sans facteurs carrés communs. D'autre part, on a les isomorphismes suivants :

$$E_i(s,t) \simeq E_i(t,s), \quad i = 1, 2, \tag{4}$$

et de plus,

$$E_1(s,t) \simeq E_1(s-t,-t). \tag{5}$$

Les courbes E_3 et E_4 peuvent se ramener à E_2 grâce aux isomorphismes :

$$E_3(s,t) \simeq E_2(-s, t-s), \qquad E_4(s,t) \simeq E_2(-t, -t+s).$$

La courbe E_1 et ses différentes isogènes ont en commun un certain nombre de quantités, dont le conducteur, le rang et les coefficients de la série L et ses dérivées.

Proposition 2.1. *Soient s et t deux entiers tels que (s,t) est sans facteurs carrés. Soient A_2 et B_2 donnés par la table I. Le conducteur des courbes E_1, E_2, E_3 et E_4 est*

$$N = \prod_{p|st(s-t)} p^{f_p}, \ p \quad \textit{premier},$$

où $f_2 = f_2(A_2, B_2)$ est donné par la table II, et, pour $p \geq 3$,

$$f_p = \begin{cases} 1 & \textit{si } (s,t) \not\equiv 0 \pmod p, \\ 2 & \textit{si } (s,t) \equiv 0 \pmod p. \end{cases}$$

Preuve. Une application de l'algorithme de Tate (voir par exemple [5] ou [7]) permet de déterminer le conducteur de $E_1(s,t)$, en distinguant différents cas suivant la structure de s et t. $\square$

Remarque 2.1. Tous les points de 2-torsion de la courbe $E_1(s,t)$ sont rationnels, donc d'après Diamond et Kramer (voir [9] et [10]), $E_1(s,t)$ et ses isogènes $E_i(s,t)$, $2 \leq i \leq 4$, sont modulaires.

Soit N le conducteur commun de E_1, E_2, E_3 et E_4. On suppose que E_1 vérifie la conjecture de Birch et Swinnerton-Dyer. La fonction L, commune aussi, s'écrit $L(x) = \sum_{n\geq 1} a_n n^{-x}$. Soit Λ définie par :

$$\Lambda(x) = \left(\frac{\sqrt{N}}{2\pi}\right)^x \Gamma(x) L(x).$$

Alors le signe w de l'équation fonctionnelle $\Lambda(2-x) = w\Lambda(x)$ vérifie $w = (-1)^r$, où r est le rang de E_1. Le calcul de w peut se faire à l'aide des coefficients a_n de la série L, par la méthode exposée dans [12]. Le calcul de $\Lambda(x)$ à la précision 10^{-k}, $k \geq 1$, nécesssite le calcul de $m\sqrt{N}$ coefficients a_n, avec

$$m > \max\left(\left(\frac{4}{5\pi}\right)^{3/2} N^{1/4}, \frac{1}{\pi}\left(k \log 10 - \log(1 - e^{-\pi/\sqrt{N}})\right)\right).$$

Si E_1 admet une réduction lisse ou multiplicative en 2 ($f_2 \leq 1$ dans la table II, III ou IV), le signe w peut se calculer à l'aide de la proposition suivante.

Proposition 2.2. *Soient s et t deux entiers tels que (s,t) est sans facteurs carrés. Si A_2 et B_2, donnés par la table I, vérifient $A_2 \equiv 0, 16 \pmod{32}$ et $B_2 \equiv 3 \pmod 4$, alors le signe de l'équation fonctionnelle relative à $E_1(s,t)$ est :*

$$w = -\prod_{p \mid st(s-t)} w_p(A_p, B_p),$$

avec

$$w_p(A_p, B_p) = \begin{cases} 1 & \text{si } p = 2 \text{ et } A_2 \equiv 16 \pmod{32}, \\ -\left(\frac{-B_p}{p}\right) & \text{si } p \not| B_p(A_p - B_p), \\ \left(\frac{-1}{p}\right) & \text{si } p | B_p(A_p - B_p) \text{ et } p \geq 3, \end{cases}$$

où A_p et B_p sont donnés par la table I.

Preuve. D'après Deligne [8], le signe w de l'équation fonctionnelle d'une courbe elliptique quelquonque $E/\mathbb{Q}$ est le produit des signes locaux w_p, où p est un diviseur premier du conducteur et de $w_\infty = -1$. Ces signes dépendent du type de réduction. Si la courbe E a une réduction multiplicative en p, alors $w_p = -\left(\frac{-c_6}{p}\right)$ (voir [1]), où c_6 est le covariant habituel de la courbe. En particulier, si E_1 admet une réduction lisse en $p = 2$, on a $w_2 = 1$, et si E_1 admet une réduction multiplicative en $p = 2$, on a $u_0 = 2$ et

$$c_6 = \frac{(A_2 + B_2)(A_2 - 2B_2)(2A_2 - B_2)}{2} \equiv B_2 \pmod 2,$$

et donc $w_2 = -\left(\frac{-B_2}{2}\right)$. De même si E_1 admet en $p \geq 3$ une réduction multiplicative, alors $p \not| B_p(A_p - B_p)$ et $c_6 \equiv B_p \pmod p$. Si la courbe a une réduction additive en $p \geq 3$, alors $w_p = -\left(\frac{-q}{p}\right)$, avec $q \in \{1, 2, 3, c_6\}$, suivant le symbole de Kodaira (voir [28]). Pour E_1, si $p | B_p(A_p - B_p)$, alors le type de Kodaira pour p est de la forme I_n^* et $q = 1$. $\square$

Dans le cas où le signe de l'équation fonctionnelle de $E_1(s,t)$ est 1, on peut calculer la valeur de $L(1)$ à la précision 10^{-k} à l'aide de l'expression (voir [5] ou [12]) :

$$L(1) = 2 \sum_{n=1}^{m} \frac{a_n}{n} e^{-2\pi n/\sqrt{N}},$$

où m vérifie :

$$m \geq \frac{\sqrt{N}}{2\pi} \left(2 \log 2 + k \log 10 - \log\left(1 - e^{-2\pi/\sqrt{N}}\right)\right).$$

Le calcul de la valeur de $L(1)$ devient donc assez long pour de grandes valeurs du conducteur. Ceci est la principale raison du choix de la limite $N \leq 10^{10}$, imposée dans ce travail pour calculer $L(1)$.

3. Courbe E_1

On commence par donner une expression pour le nombre de Tamagawa C_1 de $E_1(s,t)$. On a

$$C_1 = \prod_{p|N_1} c_p,$$

où N_1 est le conducteur de $E_1(s,t)$, et pour $p|N_1$, c_p est le nombre de Tamagawa local de $E_1(s,t)$ relatif à p.

Proposition 3.1. *Soient s et t deux entiers tels que (s,t) est sans facteurs carrés. Soient p un facteur premier de $st(s-t)$ et A_p et B_p donnés par la table I. Soit $n_p = \operatorname{ord}_p(A_p)$. Le nombre de Tamagawa c_p relatif à p pour E_1 est donné dans la table II pour $p=2$, et pour $p \geq 3$, on a*

$$c_p = \begin{cases} 2n_p & si\ (p,B_p)=1\ et\ \left(\frac{-B_p}{p}\right)=1,\ \{type\ I_{2n_p}\}, \\ 2 & si\ (p,B_p)=1\ et\ \left(\frac{-B_p}{p}\right)=-1,\ \{type\ I_{2n_p}\}, \\ 4 & si\ (p,B_p)=p,\ \{type\ I^*_{2n_p-2}\}. \end{cases}$$

Preuve. Il suffit d'appliquer l'algorithme de Tate décrit dans [5] ou [7]. □

Remarque 3.1. Si s et t sont tels que dans la table II on a $u_0 = 2$, alors $f_2 \leq 1$, et A_2 et B_2 vérifient $A_2 \equiv 0, 16 \pmod{32}$ et $B_2 \equiv 3 \pmod 4$, alors en effectuant le changement de variables $(x,y) = (4X, 8Y+4X)$, la courbe $E_1(s,t)$ devient :

$$Y^2 + XY = X^3 - \frac{A_2+B_2+1}{4}X^2 + \frac{A_2B_2}{16}X,$$

avec pour discriminant minimal $\Delta(s,t) = s^2t^2(s-t)^2/256$.

Table *II*
Courbes $E_1(s,t)$.

A_2	B_2	type	f_2	c_2	u_0
$4S+2$	$2T+1$	III	5	2	1
$8S+4$	$4T+1$	I_0^*	4	2	1
$16S+4$	$4T+3$	I_1^*	3	2	1
$16S+12$	$4T+3$	I_1^*	3	4	1
$16S+8$	$4T+1$	I_2^*	4	4	1
$16S+8$	$4T+3$	III^*	3	2	1
$32S+16$	$4T+1$	I_4^*	4	4	1
$32S+16$	$4T+3$	I_0	0	1	2
$2^{k+5}(2S+1)$	$4T+1$	I_{2k+6}^*	4	4	1
$2^{k+5}(2S+1)$	$8T+3$	I_{2k+2}	1	2	2
$2^{k+5}(2S+1)$	$8T+7$	I_{2k+2}	1	$2k+2$	2
$2^{k+2}(2S+1)$	$4T+2$	I_{2k+2}^*	6	4	1

En ce qui concerne l'ordre du sous-groupe des points de torsion de $E_1(s,t)$, on a le résultat suivant.

Théorème 3.1. *Soient s et t deux entiers tels que (s,t) est sans facteurs carrés. On désigne par (a,b) l'un des couples (s,t), (t,s), $(s-t,-t)$, $(-t,s-t)$, $(t-s,-s)$ ou $(-s,t-s)$. Alors le sous-groupe des points de torsion de $E_1(s,t)$ est :*

$$T_1 = \begin{cases} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} & \textit{si } a = -16u^4v^4,\ b = -(u+v)^4(u-v)^4, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} & \textit{si } a = 16uv^3,\ b = -(u-3v)(u+v)^3, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} & \textit{si } a = -u^2,\ b = -v^2, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \textit{sinon}, \end{cases}$$

où u et v sont des rationnels quelconques.

Preuve. Soient a et b deux entiers. La courbe $E_1(a,b)$ admet 3 points de 2-torsion non triviaux, $(0,0)$, $(a,0)$ et $(b,0)$. Le théorème de Mazur implique alors que le sous-groupe des points de torsion de $E_1(a,b)$ est de la forme $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}$, avec $1 \leq m \leq 4$. D'autre part, les courbes elliptiques ayant $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}$ pour sous-groupe de points de torsion sont classifiées (voir Appendice). Il suffit donc d'identifier $E_1(a,b)$ avec l'une de ces courbes. $\square$

Pour calculer la période Ω_1 de $E_1(s,t)$, on peut supposer $s > t$ du fait que $E_1(s,t) = E_1(t,s)$.

Proposition 3.2. *Soient s et t deux entiers avec $s > t$ et (s,t) est sans facteurs carrés. Soit u_0 donné dans la table II. Alors la période de $E_1(s,t)$ est :*

$$\Omega_1(s,t) = \frac{2u_0}{\sqrt{A}} \int_0^\infty \frac{dX}{\sqrt{X(X+1)(X+\alpha)}},$$

où $A = \max(s, s-t, -t)$ et $0 < \alpha < 1$ est donné par :

$$\alpha = \begin{cases} \frac{s-t}{s} & \textit{si } 0 < t < s, \\ \frac{s}{s-t} & \textit{si } t < 0 < s, \\ \frac{s}{t} & \textit{si } t < s < 0. \end{cases}$$

Preuve. Soit $s > t$ tels que (s,t) est sans facteurs carrés. La période de $E_1(s,t)$ est le double de sa période réelle :

$$\Omega_1 = 2u_0 \int_{\max(0,s)}^\infty \frac{dx}{\sqrt{x(x-s)(x-t)}}.$$

Si $0 < t < s$, on pose $X = (x-s)/s$. Si $t < 0 < s$, on pose $X = (x-s)/(s-t)$. Enfin si $t < s < 0$, on pose $X = -x/t$. On obtient alors l'expression de Ω_1, qui dépend du paramètre α, et qui vérifie en plus $0 < \alpha < 1$. $\square$

Remarque 3.2. Dans la pratique, on peut calculer la valeur de la période Ω_1 de $E_1(s,t)$ en utilisant la méthode de la moyenne arithmético-géométrique AGM (voir par exemple [5] ou [12]). Ainsi, avec les notations de la proposition ci-dessus et en supposant $s > t$, on a

$$\Omega_1(s,t) = \frac{2\pi u_0}{\sqrt{A}} \times \frac{1}{\mathrm{AGM}(1,\sqrt{\alpha})}.$$

4. Courbe E_2

Soient s et t deux entiers tels que (s,t) est sans facteurs carrés. Le conducteur de $E_2(s,t)$ est le même que celui de $E_1(s,t)$, donné par la proposition 2.1. Le sous-groupe des points de torsion de $E_2(s,t)$ est donné par le théorème suivant.

Théorème 4.1. *Soient s et t deux entiers tels que (s,t) est sans facteurs carrés. On désigne par (a,b) l'un des couples (s,t) ou (t,s). Le sous-groupe des points de torsion de $E_2(s,t)$ est :*

$$T_2 = \begin{cases} \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z} & si\ a = (u^2+v^2)^4,\ b = \left((u^2-v^2)^2-4u^2v^2\right)^2, \\ \mathbb{Z}/12\mathbb{Z} & si\ a = (u^2+v^2)^3(u^2+4uv+v^2), \\ & \quad b = (u+v)^6(u-v)^2, \\ \mathbb{Z}/8\mathbb{Z} & si\ a = (2u-v)^4,\ b = v^2(8u^2-8uv+v^2), \\ \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z} & si\ a = (u+v)^2,\ b = (u-v)^2, \\ \mathbb{Z}/6\mathbb{Z} & si\ a = (u+3v)(u-v)^3,\ b = (u-3v)(u+v)^3, \\ \mathbb{Z}/4\mathbb{Z} & si\ a = u^2,\ b = u(u-v), \\ \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z} & si\ a = w(u+v)^2,\ b = w(u-v)^2, \\ \mathbb{Z}/2\mathbb{Z} & sinon, \end{cases}$$

où u, v et w sont des rationnels quelconques.

Preuve. Soient a et b deux entiers. La courbe $E_2(a,b)$ admet au moins un point de 2-torsion non trivial. Le théorème de Mazur implique alors que le sous-groupe des points de torsion de $E_1(a,b)$ est de la forme $\mathbb{Z}/m\mathbb{Z}$, avec $m = 2,4,6,8,10,12$, ou $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2m\mathbb{Z}$, avec $1 \le m \le 4$. Il suffit d'identifier $E_2(a,b)$ avec l'une des courbes de l'Appendice. On va montrer cependant que $E_2(a,b)(\mathbb{Q})_{\mathrm{tors}}$ ne peut pas être de la forme $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$ ou $\mathbb{Z}/10\mathbb{Z}$.

En identifiant $E_2(a,b)$ et $E_{2\times 6}(u,v)$, u et v doivent vérifier la relation

$$-16uv^3(u+v)^3(u-3v) = (a-b)^2,$$

et donc $-uv(u+v)(u-3v) = c^2$, pour un rationnel c. On peut supposer $(u,v) = 1$. Ainsi le point $(u/v, c/v^2)$ est rationnel sur la courbe elliptique d'équation $y^2 = -x(x+1)(x-3)$. En posant $x = -X+1$ et $y = Y$, cette courbe s'écrit :

$$Y^2 = (X-1)(X-2)(X+2).$$

Le rang de cette courbe, calculé inconditionellement par les systèmes de calcul APECS [6], MWRANK [7] et SIMATH [31] est nul. Les points de torsion non triviaux sont $(1,0)$, $(\pm 2,0)$, $(4,\pm 6)$ et $(0,\pm 2)$. On en déduit alors les possibilités $(u,v) = (0,1),(\pm 1,1),(\pm 3,1)$, pour lesquelles la courbe $E_{2\times 6}(u,v)$ est singulière. Ceci montre que $E_2(a,b)$ ne peut pas avoir un sous-groupe de torsion de la forme $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$.

En identifiant $E_2(a,b)$ et $E_{10}(u,v)$, u et v doivent vérifier la condition $16u^5(u+v)^5(u^2+3uv+v^2) = (a-b)^2$, et donc $u(u+v)(u^2+3uv+v^2) = c^2$ pour un rationnel c. On peut alors supposer que $(u,v) = 1$, et donc $(v/u, c/u^2)$ est un point rationnel sur la courbe elliptique d'équation

$$Y^2 = (X+1)(X^2+3X+1).$$

Cette courbe est aussi de rang nul, son groupe de torsion contient les points $(-1,0)$, $(0,\pm 1)$ et $(-2,\pm 1)$. Ceci donne $(u,v) = (1,-1),(1,0),(1,-2)$, mais dans ces cas, $E_{10}(u,v)$ est singulière. $\square$

Comme $E_2(s,t) = E_2(t,s)$, on peut supposer dans la proposition ci-dessous que $t < s$.

Proposition 4.1. *Soient s et t deux entiers tels que (s,t) est sans facteurs carrés et $t < s$. Soient A_2 et B_2 définis par la table I. Soit $u_0 = u_0(A_2,B_2)$ donné par la table IV si $A_2 = s-t$ et par la table III sinon. Soient $\beta = \frac{s+t}{s-t}$ et*

$$\alpha = \begin{cases} \frac{(s+t-2\sqrt{st})^2}{(s-t)^2} & si\ 0 < t < s, \\ \frac{4\sqrt{st}}{2\sqrt{st}-s-t} & si\ t < s < 0. \end{cases}$$

Alors $0 < \alpha < 1$, $-1 < \beta < 1$ et la période de $E_2(s,t)$ est :

$$\Omega_2 = \begin{cases} \frac{u_0}{2\sqrt{s-t}} \int_0^\infty \frac{dX}{\sqrt{X(X^2+2\beta X+1)}} & si\ t < 0 < s, \\ \frac{u_0}{\sqrt{|s|}+\sqrt{|t|}} \int_0^\infty \frac{dX}{\sqrt{X(X+1)(X+\alpha)}} & sinon. \end{cases}$$

Preuve. Soit $u_0 = u_0(A_2,B_2)$ donné par la table *III* ou *IV*. On pose $k = 1$ si $st < 0$ et $k = 3$ si $st > 0$. On a alors

$$\Omega_2 = \frac{(k+1)u_0}{4} \int_{x_0}^\infty \frac{dx}{\sqrt{x(x^2+2(s+t)x+(s-t)^2)}},$$

où $x_0 = 0$ si $st < 0$ et $x_0 = \max(0, -(s+t)+2\sqrt{st})$ si $st > 0$.

Si $st > 0$, on a $k = 3$, et $x^2+2(s+t)x+(s-t)^2 = (x-x_2)(x-x_3)$, avec $x_2 = -(s+t)+2\sqrt{st}$ et $x_3 = -(s+t)-2\sqrt{st}$. Si $0 < t < s$, on pose $x = -x_3X$, ce qui donne :

$$\Omega_2 = \frac{u_0}{\sqrt{s+t+2\sqrt{st}}} \int_0^\infty \frac{dX}{\sqrt{X(X+1)(X+\alpha)}},$$

avec $\alpha = x_2/x_3$. Si $t < s < 0$, on pose $x = x_2X + x_2$, ce qui donne :

$$\Omega_2 = \frac{u_0}{\sqrt{-(s+t)+2\sqrt{st}}}\int_0^\infty \frac{dX}{\sqrt{X(X+1)(X+\alpha)}},$$

avec $\alpha = (x_2 - x_3)/x_2$.

Si $st < 0$, alors $t < 0 < s$ et $k = 1$. On pose $x = (s-t)X$, ce qui donne

$$\Omega_2 = \frac{u_0}{2\sqrt{s-t}}\int_0^\infty \frac{dX}{\sqrt{X(X^2+2\beta X+1)}},$$

avec $\beta = \frac{s+t}{s-t}$. Il est facile alors de voir que $0 < \alpha < 1$ et $-1 < \beta < 1$. $\square$

Remarque 4.1. Comme dans la remarque 3.1, on peut calculer $\Omega_2 = \Omega_2(s,t)$ à l'aide de la fonction AGM par les formules :

$$\Omega_2 = \begin{cases} \frac{2\pi u_0}{\sqrt{s-t}} \times \frac{1}{\mathrm{AGM}(2,\sqrt{2}\sqrt{\beta+1})} & \text{si } t < 0 < s, \\ \frac{2\pi u_0}{\sqrt{\sqrt{|s|}+\sqrt{|t|}}} \times \frac{1}{\mathrm{AGM}(1,\sqrt{\alpha})} & \text{sinon.} \end{cases}$$

Le nombre de Tamagawa C_2 de la courbe $E_2(s,t)$ est

$$C_2 = \prod_{p|N_2} c_p,$$

où N_2 est le conducteur de $E_2(s,t)$, et pour $p|N_2$, c_p est le nombre de Tamagawa local de $E_2(s,t)$ relatif à p. Le calcul de c_p dépend de la valeur prise par $\max(\mathrm{ord}_p(st), 2\,\mathrm{ord}_p(s-t))$.

4.1. Cas où $\mathrm{ord}_p(s-t) = \min(\mathrm{ord}_p(s), \mathrm{ord}_p(t), \mathrm{ord}_p(s-t))$.

Soit p un facteur premier de $st(s-t)$. On suppose que A_p et B_p donnés par la table I vérifient $\{A_p, B_p\} = \{s,t\}$. Alors on peut déterminer le nombre de Tamagawa local c_p pour $E_2(s,t)$ à l'aide de la proposition suivante.

Proposition 4.2. *Soient s et t deux entiers tels que (s,t) est sans facteurs carrés. Soit p un nombre premier divisant $st(s-t)$ tel que les nombres A_p et B_p, donnés par la table I, vérifient $\{A_p, B_p\} = \{s,t\}$. On pose $n_p = \mathrm{ord}_p(A_p)$. Le nombre de Tamagawa local c_p de la courbe $E_2(s,t)$ est donné par la table III si $p = 2$, et si $p \geq 3$, alors :*

$$c_p = \begin{cases} n_p & \text{si } p \not| B_p \text{ et } \left(\frac{-B_p}{p}\right) = 1, \ \{\text{type } I_{n_p}\}, \\ (2, n_p) & \text{si } p \not| B_p \text{ et } \left(\frac{-B_p}{p}\right) = -1, \ \{\text{type } I_{n_p}\}, \\ 3 + \left(\frac{A_pB_pp^{-n_p-1}}{p}\right) & \text{si } p|B_p \text{ et } n_p \text{ est impair, } \{\text{type } I^*_{n_p-1}\}, \\ 3 + \left(\frac{B_pp^{-n_p}}{p}\right) & \text{si } p|B_p \text{ et } n_p \text{ est pair, } \{\text{type } I^*_{n_p-1}\}. \end{cases}$$

Preuve. Ceci découle de l'algorithme de Tate(voir [5] ou [7]). $\square$

Remarque 4.2. Si s et t vérfient $s \equiv 0, 16 \pmod{32}$ et $t \equiv 3 \pmod 4$, alors $E_2(s,t)$ est stable ou semi-stable en 2. Soit $\varepsilon_0 = (t-7)/4 \pmod 2$. En posant $(x,y) = (4X+1, 8Y+4X-4\varepsilon_0)$ dans $E_2(s,t)$, on obtient la courbe :

$$\begin{aligned} Y^2 + XY - \varepsilon_0 Y = X^3 + \frac{s+t+1}{2}X^2 + \frac{(s-t)^2 + 4(s+t) + 8\varepsilon_0 + 3}{16}X \\ + \frac{(s-t)^2 + 2(s+t) - 16\varepsilon_0 + 1}{64}, \end{aligned}$$

qui est alors minimale avec pour discriminant

$$\Delta_2 = \frac{1}{16} st(s-t)^4.$$

Table III Courbe $E_2(s,t)$ avec $\{A_2,B_2\}=\{s,t\}$.					
A_2	B_2	type	f_2	c_2	u_0
$4S+2$	$4T+1$	I_0^*	5	2	1
$4S+2$	$4T+3$	I_0^*	5	1	1
$16S+4$	$4T+1$	I_2^*	4	4	1
$16S+12$	$4T+1$	I_2^*	4	2	1
$8S+4$	$4T+3$	III^*	3	2	1
$32S+8$	$4T+1$	I_3^*	4	2	1
$32S+24$	$4T+1$	I_3^*	4	4	1
$16S+8$	$4T+3$	II^*	3	1	1
$64S+16$	$4T+1$	I_4^*	4	4	1
$64S+48$	$4T+1$	I_4^*	4	2	1
$32S+16$	$4T+3$	I_0	0	1	2
$2^k(4S+1)$	$8T+1$	I_{k+5}^*	4	4	1
$2^{5+k}(4S+3)$	$8T+1$	I_{k+5}^*	4	2	1
$2^{5+k}(4S+1)$	$8T+5$	I_{k+5}^*	4	$2(2,k+3)$	1
$2^{5+k}(4S+3)$	$8T+5$	I_{k+5}^*	4	$2(2,k+4)$	1
$2^{5+k}(2S+1)$	$8T+3$	I_{k+1}	1	$(2,k+1)$	2
$2^{5+k}(2S+1)$	$8T+7$	I_{k+1}	1	$k+1$	2
$2^2(8S+3)$	$2(4T+1)$	I_5^*	6	2	1
$2^2(8S+3)$	$2(4T+3)$	I_5^*	6	4	1
$2^2(8S+7)$	$2(4T+1)$	I_5^*	6	4	1
$2^2(8S+7)$	$2(4T+3)$	I_5^*	6	2	1
$2^{3+2k}(8S+1)$	$2(8T\pm 1)$	I_{2k+6}^*	6	4	1
$2^{3+2k}(8S+1)$	$2(8T\pm 3)$	I_{2k+6}^*	6	2	1
$2^{2+2k}(8S+1)$	$2(2T+1)$	I_{2k+5}^*	6	4	1
$2^{4+2k}(8S+3)$	$2(4T+1)$	I_{2k+7}^*	6	4	1
$2^{4+2k}(8S+3)$	$2(4T+3)$	I_{2k+7}^*	6	2	1
$2^{3+2k}(8S+3)$	$2(8T+1)$	I_{2k+6}^*	6	4	1
$2^{3+2k}(8S+3)$	$2(8T+3)$	I_{2k+6}^*	6	4	1
$2^{3+2k}(8S+3)$	$2(8T+5)$	I_{2k+6}^*	6	2	1
$2^{3+2k}(8S+3)$	$2(8T+7)$	I_{2k+6}^*	6	2	1
$2^{2+2k}(8S+5)$	$2(2T+1)$	I_{2k+5}^*	6	2	1
$2^{3+2k}(8S+5)$	$2(8T\pm 1)$	I_{2k+6}^*	6	2	1
$2^{3+2k}(8S+5)$	$2(8T\pm 3)$	I_{2k+6}^*	6	4	1
$2^{4+2k}(8S+7)$	$2(4T+1)$,	I_{2k+7}^*	6	2	1
$2^{4+2k}(8S+7)$	$2(4T+3)$	I_{2k+7}^*	6	4	1
$2^{3+2k}(8S+7)$	$2(8T+1)$	I_{2k+6}^*	6	2	1
$2^{3+2k}(8S+7)$	$2(8T+3)$	I_{2k+6}^*	6	2	1
$2^{3+2k}(8S+7)$	$2(8T+5)$	I_{2k+6}^*	6	4	1
$2^{3+2k}(8S+7)$	$2(8T+7)$	I_{2k+6}^*	6	4	1

4.2. Cas où $\mathrm{ord}_p(s-t)=\max(\mathrm{ord}_p(s),\mathrm{ord}_p(t),\mathrm{ord}_p(s-t))\geq 2$**.**

Soit p un facteur premier de $st(s-t)$ tel que les valeurs A_p et B_p donnés par la table I vérifient $A_p=s-t$ et $B_p=-t$.

Proposition 4.3. *Soient s et t deux entiers tels que (s,t) est sans facteurs carrés. Soit p un nombre premier divisant $st(s-t)$ tel que $\operatorname{ord}_p(st) < 2\operatorname{ord}_p(s-t)$. On pose $n_p = \operatorname{ord}_p(s-t)$. Si $p=2$, le nombre de Tamagawa c_2 de la courbe $E_2(s,t)$ est donné par la table IV. Si $p \geq 3$, alors :*

$$c_p = \begin{cases} 4n_p & \text{si } (p,t)=1 \text{ et } \left(\frac{t}{p}\right)=1,\ \{\text{Type } I_{4n_p}\}, \\ 2 & \text{si } (p,t)=1 \text{ et } \left(\frac{t}{p}\right)=-1,\ \{\text{Type } I_{4n_p}\}, \\ 4 & \text{si } (p,t)=p,\ \{\text{Type } I^*_{4(n_p-1)}\}. \end{cases}$$

Preuve. C'est aussi une application détaillée de l'algorithme de Tate. □

Table *IV*
Courbe $E_2(s,t)$ avec $A_2 = s-t, B_2 = -t$.

$s - t$	t	type	f_2	c_2	u_0
$8S+2$	$8T\pm 1$	I_3^*	5	4	1
$8S+2$	$8T\pm 3$	I_3^*	5	2	1
$8S+6$	$8T+1$	I_3^*	5	4	1
$8S+6$	$8T+3$	I_3^*	5	4	1
$8S+6$	$8T+5$	I_3^*	5	2	1
$8S+6$	$8T+7$	I_3^*	5	2	1
$8S+4$	$4T+1$	III	3	2	2
$8S+4$	$4T+3$	II	4	1	2
$16S+8$	$8T+1$	I_1^*	3	4	2
$16S+8$	$8T+5$	I_1^*	3	2	2
$16S+8$	$4T+3$	I_0^*	4	2	2
$32S+16$	$4T+1$	I_0	0	1	4
$32S+16$	$4T+3$	I_4^*	4	4	2
$2^{k+5}(2S+1)$	$8T+1$	I_{4k+4}	1	$4k+4$	4
$2^{k+5}(2S+1)$	$8T+5$	I_{4k+4}	1	2	4
$2^{k+5}(2S+1)$	$4T+3$	I_{4k+8}^*	4	4	2
$4(2S+1)$	$4T+2$	II	6	1	2
$8(2S+1)$	$4T+2$	I_0^*	6	2	2
$2^{k+4}(2S+1)$	$4T+2$	I_{4k+4}^*	6	4	2

5. Détermination de bons paramètres s et t

Pour que le rapport (3) soit assez grand pour la courbe $E_1(s,t)$ ou $E_2(s,t)$, il faut que les quantités correspondantes Ω_i, C_i, et N_i, $i=1,2$, soient assez petites. Les propositions 3.2 et 4.1 mettent en évidence la présence d'un facteur K_i^{-1} dans l'expression de Ω_i, $i=1,2$, avec

$$K_i = \begin{cases} \sqrt{\max(|s|,|t|,|s-t|)} & \text{si } i=1, \\ \sqrt{|s-t|} & \text{si } i=2 \text{ et } st<0, \\ \sqrt{|s|}+\sqrt{|t|} & \text{si } i=2 \text{ et } st>0. \end{cases}$$

Ceci montre donc que les bons paramètres s et t pour le rapport (3) sont tels que C_i et N_i sont relativement petits en comparaison de K_i, $i = 1, 2$, et donc en comparaison du discriminant. Ainsi, on doit chercher des courbes elliptiques de la forme $E_1(s,t)$ et $E_2(s,t)$ ayant un assez grand rapport de Szpiro (voir par exemple [25]). Ce rapport est défini pour une courbe elliptique $E/\mathbb{Q}$ par :

$$\sigma = \frac{\log|\Delta|}{\log N},$$

où Δ est le discriminant minimal de E et N son conducteur. On peut utliser les *bons exemples* pour la conjecture *abc* (voir [26]) pour construire des courbes elliptiques de la forme $E_1(s,t)$ et $E_2(s,t)$, mais on donne ici une autre méthode pour exhiber des exemples plus adaptés à notre situation.

Soient x, y et z des entiers vérifiant $0 < x < y < z$, $(x, y) = 1$ et $x+y = z$. Soit d un entier sans facteurs carrés (y compris $d = \pm 1$). Compte tenu des relations d'isomorphisme (4) et (5), on calcul le rapport (3), relatif à la courbe $E_1(s,t)$, où (s,t) est l'un des couples suivants

$$(s,t) = (dx, -dy), (dx, dz),$$

avec $d \geq 1$. On calcul de même le rapport (3), relatif à la courbe $E_2(s,t)$, où (s,t) est l'un des couples suivants

$$(s,t) = (dx, -dy), (dx, dz), (dy, -dx), (dy, dz),$$

avec ici $d \in \mathbb{Z}$.

La présence du facteur d dans les couples ci-dessus correspond en fait à des tordues quadratiques. Soient s_0 et t_0 deux entiers sans facteurs carrés communs. Un résultat dû à Kohnen et Zagier [17] implique en effet l'existence de tordues quadratiques $E_1(ds_0, dt_0)$ et $E_2(ds_0, dt_0)$ de rangs nuls, avec $|d| \leq N_1^2$, où N_1 est le conducteur commun de $E_1(s_0, t_0)$ et $E_2(s_0, t_0)$. Si on admet l'Hypothèse de Riemann, alors d vérifie $|d| \leq N_1^\varepsilon$ (voir [14] ou [32]). La conjecture de Birch et Swinnerton-Dyer implique alors l'existence d'entiers d tels que $|d|$ est assez petits, pour lesquels les courbes elliptiques $E_1(s,t)$ et $E_2(s,t)$ sont de rang nuls.

On décrit maintenant une méthode pour déterminer des entiers x, y et z, qui donneront des paramètres s et t comme ci-dessus. Soient $2 = p_1 < p_2 < \cdots < p_n$ les n premiers nombres premiers. Soient A, B et C des entiers premiers entre eux deux à deux, donnés par :

$$A = \prod_{i=1}^{n} p_i^{k_i}, \quad B = \prod_{i=1}^{n} p_i^{l_i}, \quad C = \prod_{i=1}^{n} p_i^{m_i},$$

où, pour $i = 1, \cdots, n$, k_i, l_i et m_i sont des entiers. On considère l'équation linéaire

$$AX - BY = CZ, \tag{6}$$

en entiers non nuls X, Y et Z, vérifiant $(AX, BY) = 1$. S'il y a une solution (X, Y, Z) vérifiant cette condition, alors $T = XY^{-1} \pmod{C}$, avec $0 < T < C$, vérifie la congruence

$$T \equiv BA^{-1} \pmod{C}. \tag{7}$$

Il existe donc deux entiers U et Q tels que $AT - B = CQ$ et $X = TY - CU$, ce qui donne $Z = QY - AU$. Ceci montre donc que l'équation (6) admet une infinité de solutions. On doit cependant fixer une limite X_0, Y_0 et Z_0 pour chacune des variables X, Y et Z. On peut alors déterminer des entiers X, Y et Z en considérant le système d'inéquations :

$$\begin{cases} |TY - CU| \le X_0, \\ |QY - AU| \le Z_0, \\ |Y| \le Y_0, \end{cases}$$

en entiers Y et U. Ce système peut être résolu par exemple en utilisant l'algorithme LLL (voir [22]). D'autre part, le Théorème de Minkowski sur les formes linéaires assure l'existence d'une solution de ce système vérifiant $(Y, U) \ne (0, 0)$ si $X_0 Y_0 \ge C$, $X_0 Z_0 \ge B$ et $Y_0 Z_0 \ge A$. Les entiers x, y et z recherchés pour les paramètres s et t seront alors :

$$\begin{aligned} &x = \min\left(|AX|, |BY|, |CZ|\right)/D, \\ &z = \max\left(|AX|, |BY|, |CZ|\right)/D, \\ &y = z - x, \end{aligned}$$

où $D = (AX, BY)$.

6. Résultats numériques

On donne dans cette partie des exemples de courbes elliptiques $E_i(s, t)$, $i = 1, 2$, ayant un grand groupe de Tate-Shafarevich. Les tables V et VI concernent le cas où le rang est nul et le conducteur est inférieur à 10^{10}. Dans ce cas, on calcule la valeur de l'ordre du groupe de Tate-Shafarevich sous forme d'un carré, ainsi que le rapport (1).

Les valeurs de s et t vérifient $s > t$, sont sans facteurs carrés communs, et sont déterminées par la méthode décrite dans la partie 5, avec les données suivantes :

$$\begin{aligned} &2 = p_1 < p_2 < \cdots < p_{46} = 199, \\ &0 < A = p_i^{k_i}, B = p_j^{k_j}, C = p_h^{k_h} \le 2^{32}, \\ &X_0 = Y_0 = Z_0 = 2^{16}, \\ &-21 \le d \le 21. \end{aligned}$$

Pour les tables V et VI, certaines valeurs de s et t ne forment pas de bons exemples pour la conjecture abc (voir [26]). Ainsi, dans la table VI, la courbe $E_2(3\cdot 5^8\cdot 83\cdot 107, -2^8\cdot 3\cdot 41^3)$ est telle que $\gamma = 1.1422$, mais le rapport de Oesterlé-Masser (voir par exemple [26]) de la relation correspondante $2^8\cdot 41^3 + 5^8\cdot 83\cdot 107 = 3^{20}$ est

$$\frac{\log 3^{20}}{\log(2\cdot 3\cdot 5\cdot 41\cdot 83\cdot 107)} \approx 1.355773,$$

et donc *n'est pas un bon exemple* pour la conjecture *abc*. Signalons enfin un exemple remarquable. Les courbes

$$E_1(3\cdot 83^2\cdot 103^2, -2^3\cdot 3),\ E_2(3\cdot 83^2\cdot 103^2, -2^3\cdot 3),$$
$$E_2(-3\cdot 83^2\cdot 103^2, 3^6\cdot 67^3),\ E_2(3^6\cdot 67^3, 2^3\cdot 3),$$

sont isogènes, ont le même rapport $\gamma \approx 1.0187$, et donc le même ordre du groupe de Tate-Shafarevich $|\text{Ш}| = 87^2$.

Table V

Courbes E_1, $r_1 = 0$ et $N_1 \le 10^{10}$, $\gamma \ge 1$.

s t	N_1	$\|T_1\|$ C_1	Ω_1	$L(1)$	$\|\text{Ш}\|$	γ
$-2^{35}\cdot 11$ $-11\cdot 19^5\cdot 13883$	1532016816	4 128	0.1022×10^{-5}	14.9757	428^2	1.1459
$2^5\cdot 3\cdot 7^{13}\cdot 11$ $-5^{14}\cdot 11\cdot 19$	6305720190	4 512	0.1238×10^{-5}	8.3133	458^2	1.0861
$5^9\cdot 7^2$ 5	287175	4 64	0.1285×10^{-2}	3.2113	25^2	1.0245
$3\cdot 83^2\cdot 103^2$ $-2^3\cdot 3$	41240376	4 64	0.4243×10^{-3}	12.8470	87^2	1.0187

Table VI

Courbes E_2, $r_2 = 0$ et $N_2 \leq 10^{10}$, $\gamma \geq 1$.

s t	N_2	$\lvert T_2 \rvert$ C_2	Ω_2	$L(1)$	$\lvert Ш \rvert$	γ
$-2^5 \cdot 3 \cdot 7^{13} \cdot 11$ $-11^8 \cdot 37^2 \cdot 353$	6305720190	2 16	0.6192×10^{-6}	8.3133	1832^2	1.3318
$-2^{35} \cdot 11$ $-11 \cdot 19^5 \cdot 13883$	1532016816	2 16	0.5109×10^{-5}	14.9757	856^2	1.2770
$-5 \cdot 101^5$ $-2^5 \cdot 13^5 \cdot 4423$	406517930	2 2	0.2741×10^{-4}	3.5366	508^2	1.2572
$-2^4 \cdot 3^7 \cdot 5 \cdot 547$ $-5^9 \cdot 7^2$	287175	2 8	0.6423×10^{-3}	3.2113	50^2	1.2451
$-5^{13} \cdot 181$ $-2^4 \cdot 3 \cdot 11 \cdot 13^2 \cdot 19^5$	51636585	2 4	0.1337×10^{-4}	0.6707	224^2	1.2189
$-3^5 \cdot 5 \cdot 7^3 \cdot 67^2$ $-2^5 \cdot 3 \cdot 11^7$	17179470	2 8	0.1453×10^{-3}	7.0705	156^2	1.2125
$2^5 \cdot 3 \cdot 7^{13} \cdot 11$ $-5^{14} \cdot 11 \cdot 19$	6305720190	2 64	0.6192×10^{-6}	8.3133	916^2	1.2090
$-2^{26} \cdot 5 \cdot 29^2$ $-3^3 \cdot 7^{10} \cdot 37$	1137465840	2 16	0.5914×10^{-5}	6.7962	536^2	1.2055
$-3^{17} \cdot 7$ $-2^3 \cdot 3 \cdot 11 \cdot 23 \cdot 53^3$	6758136	2 4	0.1045×10^{-3}	1.2188	108^2	1.1909
$-2^9 \cdot 3^{18} \cdot 13^2$ $-3 \cdot 11^5 \cdot 17 \cdot 31^3 \cdot 137$	7433609040	2 96	0.5426×10^{-6}	7.6809	768^2	1.1692
$2^5 \cdot 5 \cdot 41$ -1	1230	2 2	0.7757×10^{-1}	2.4823	8^2	1.1691
$-2^5 \cdot 5 \cdot 41$ -3^8	1230	2 2	0.7757×10^{-1}	2.4823	8^2	1.1691
$-3 \cdot 5^{11} \cdot 7 \cdot 29 \cdot 97$ $-2^4 \cdot 13^9 \cdot 17$	718032315	2 22	0.3700×10^{-5}	2.5211	352^2	1.1502
$11 \cdot 19^5 \cdot 13883$ $3^2 \cdot 11^7$	1532016816	2 16	0.2044×10^{-4}	14.9757	428^2	1.1459
$3 \cdot 5^8 \cdot 83 \cdot 107$ $-2^8 \cdot 3 \cdot 41^3$	32770890	2 16	0.6151×10^{-4}	4.8225	140^2	1.1422
$-2^9 \cdot 3^{17} \cdot 13^2$ $-11^5 \cdot 17 \cdot 31^3 \cdot 137$	309733710	2 24	0.1880×10^{-5}	0.7624	260^2	1.1377
$-7 \cdot 11^5 \cdot 13^2$ $-2^{15} \cdot 7^3 \cdot 17$	1191190	2 8	0.4549×10^{-3}	2.4600	52^2	1.1297
$-3 \cdot 19 \cdot 509^3$ $-2^{19} \cdot 3^5 \cdot 59$	10270602	2 2	0.7247×10^{-4}	0.3067	92^2	1.1203
$2^5 \cdot 13^5 \cdot 4423$ 7^7	406517930	2 4	0.5482×10^{-4}	3.5366	254^2	1.1173
$-2 \cdot 19 \cdot 509^3$ $-2^{20} \cdot 3^4 \cdot 59$	109553088	2 8	0.4438×10^{-4}	2.2722	160^2	1.0966
$2^6 \cdot 5 \cdot 17 \cdot 41 \cdot 193$ -1	4035630	2 4	0.9577×10^{-3}	3.9226	64^2	1.0937

Table VI (suite)
Courbes E_2, $r_2 = 0$ et $N_2 \leq 10^{10}$, $\gamma \geq 1$.

s t	N_2	$\lvert T_2\rvert$ C_2	Ω_2	$L(1)$	$\lvert Ш\rvert$	γ
$-2^6 \cdot 5 \cdot 17 \cdot 41 \cdot 193$ -3^{16}	4035630	2 4	0.9577×10^{-3}	3.9226	64^2	1.0937
$-2 \cdot 7 \cdot 11^8$ $-2^{21} \cdot 3^3 \cdot 53$	69736128	2 16	0.5735×10^{-4}	4.2428	136^2	1.0881
$2^{21} \cdot 3^3 \cdot 53$ $2 \cdot 89$	69736128	2 8	0.1147×10^{-3}	4.2428	136^2	1.0881
$-2^4 \cdot 3 \cdot 5 \cdot 7^{11}$ $-3 \cdot 11^4 \cdot 29^3 \cdot 443$	1023841665	2 8	0.9121×10^{-5}	1.4301	280^2	1.0864
$-2^2 \cdot 3 \cdot 281^3$ $-2 \cdot 7^5 \cdot 89^2$	33612096	2 12	0.1925×10^{-3}	6.7370	108^2	1.0807
$5 \cdot 31^5 \cdot 73$ $-2^{11} \cdot 5231$	355132590	2 2	0.6145×10^{-4}	1.2290	200^2	1.0765
$-5^9 \cdot 17^3$ $-2^{10} \cdot 5 \cdot 37^4$	7516550	2 32	0.6414×10^{-4}	2.5144	70^2	1.0734
$2^{26} \cdot 5 \cdot 29^2$ -631	1137465840	2 64	0.5914×10^{-5}	6.7962	268^2	1.0725
$3^8 \cdot 227$ $-2^{13} \cdot 13^3$	194766	2 4	0.2451×10^{-2}	1.6571	26^2	1.0700
$2^4 \cdot 3^3 \cdot 41^4$ $7^2 \cdot 523$	2251515	2 16	0.3597×10^{-3}	3.5967	50^2	1.0698
$5 \cdot 11^5 \cdot 13 \cdot 17^3$ $-2^7 \cdot 5^7$	87151350	2 8	0.2770×10^{-4}	0.9654	132^2	1.0683
$2^3 \cdot 3^3 \cdot 5 \cdot 7^3 \cdot 127$ -1	2026920	2 18	0.4580×10^{-3}	4.7488	48^2	1.0663
$2^4 \cdot 3 \cdot 11 \cdot 13^2 \cdot 19^5$ 7^3	51636585	2 8	0.2673×10^{-4}	0.6707	112^2	1.0627
$-2^6 \cdot 3 \cdot 5 \cdot 7 \cdot 13^5 \cdot 17$ $-13 \cdot 239^4$	144195870	2 32	0.3051×10^{-4}	5.0609	144^2	1.0582
$3^{15} \cdot 5 \cdot 17$ $-2^2 \cdot 17$	29790120	2 16	0.8996×10^{-4}	3.0456	92^2	1.0510
$-3^2 \cdot 5^5 \cdot 47^2$ $-2^{18} \cdot 3 \cdot 79$	334170	2 16	0.7971×10^{-3}	2.4998	28^2	1.0479
$3 \cdot 11^5 \cdot 17 \cdot 31^3 \cdot 137$ $3 \cdot 5^3$	7433609040	2 96	0.2170×10^{-5}	7.6809	384^2	1.0472
$-2^3 \cdot 3 \cdot 7^2 \cdot 13^5$ $-3^5 \cdot 5^7 \cdot 23$	334170	2 16	0.1503×10^{-3}	3.1175	82^2	1.0382
$-2^5 \cdot 3 \cdot 5^2$ -7^4	210	2 4	0.1282	2.0519	4^2	1.0371
$2^5 \cdot 3 \cdot 5^2$ -1	210	2 4	0.1282	2.0519	4^2	1.0371
$5^9 \cdot 7^2$ 5	287175	4 32	0.2569×10^{-2}	3.2113	25^2	1.0245

Table VI (suite) Courbes E_2, $r_2 = 0$ et $N_2 \leq 10^{10}$, $\gamma \geq 1$.						
s t	N_2	$\lvert T_2\rvert$ C_2	Ω_2	$L(1)$	$\lvert Ш\rvert$	γ
$2^4 \cdot 3^7 \cdot 5 \cdot 547$ -5	287175	2 32	0.6423×10^{-3}	3.2113	25^2	1.0245
$2^{17} \cdot 3 \cdot 17$ $-17 \cdot 29^3$	251430	2 8	0.2394×10^{-2}	2.7576	24^2	1.0223
$3 \cdot 83^2 \cdot 103^2$ $-2^3 \cdot 3$	41240376	2 32	0.2122×10^{-3}	12.8470	87^2	1.0187
$-3 \cdot 83^2 \cdot 103^2$ $-3^6 \cdot 67^3$	41240376	2 16	0.4243×10^{-3}	12.8470	87^2	1.0187
$3^6 \cdot 67^3$ $2^3 \cdot 3$	41240376	2 16	0.4243×10^{-3}	12.8470	87^2	1.0187
$-19 \cdot 509^3$ $-2^{19} \cdot 3^4 \cdot 59$	27388272	2 24	0.6276×10^{-4}	2.2911	78^2	1.0176
$2^{35} \cdot 11$ $-3^2 \cdot 11^7$	1532016816	2 256	0.5109×10^{-5}	14.9757	214^2	1.0148
$2^3 \cdot 3 \cdot 11 \cdot 23 \cdot 53^3$ 3	6758136	2 8	0.2090×10^{-3}	1.2188	54^2	1.0146
$3 \cdot 5^{11} \cdot 7 \cdot 29 \cdot 97$ -11^3	718032315	2 44	0.7399×10^{-5}	2.5211	176^2	1.0142
$-2^5 \cdot 5^{11} \cdot 19^2$ $-3 \cdot 5 \cdot 7^5 \cdot 11^3 \cdot 41^2$	2231367600	2 66	0.4183×10^{-5}	3.6023	232^2	1.0121
$-2 \cdot 3^{12}.5^2$ $-3 \cdot 5 \cdot 7 \cdot 13$	7207200	2 8	0.6094×10^{-3}	3.2959	52^2	1.0009
$-2^{13} \cdot 5 \cdot 29^2 \cdot 37^3$ $-5^{10} \cdot 11^4 \cdot 13$	529364550	2 32	0.4682×10^{-5}	0.8653	152^2	1.0004

7. Appendice

On donne dans cette partie l'expression générale des courbes elliptiques définies sur $\mathbb{Q}$, suivant la forme de leur sous-groupe de torsion (voir [16], [20] ou [25]). Les paramètres u et v représentent des rationnels pour lesquels le discriminant correspondant n'est pas nul. Ces discriminants peuvent être non minimaux.

1. Courbes de sous-groupe de torsion de la forme $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$,

$$E_{2\times 8}: \; Y^2 = X(X + 16u^4v^4)(X + (u^2 - v^2)^4).$$

Le discriminant est alors

$$\Delta_{2\times 8} = 2^{12}u^8v^8(u^2 - v^2)^8(u^2 + v^2)^4(u^2 - 2uv - v^2)^2(u^2 + 2uv - v^2)^2.$$

2. Courbes de sous-groupe de torsion de la forme $\mathbb{Z}/12\mathbb{Z}$,

$$E_{12}:\ Y^2 = X(X^2 + a_2X + a_4),$$

avec

$$\begin{aligned} a_2 &= \frac{1}{4}(u^4 - v^4)^2 + uv(u^4 + v^4)(u^2 + uv + v^2), \\ a_4 &= u^6v^6(u^2 + uv + v^2)^2. \end{aligned}$$

Le discriminant est

$$\Delta_{12} = u^{12}v^{12}(u-v)^2(u+v)^6(u^2+v^2)^3(u^2+uv+v^2)^4(u^2+4uv+v^2).$$

3. Courbes de sous-groupe de torsion de la forme $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$,

$$E_{2\times 6}:\ Y^2 = X(X - 16uv^3)(X + (u-3v)(u+v)^3),$$

et de discriminant

$$\Delta_{2\times 6} = u^2v^6(u+v)^6(u-v)^6u + 3v)^2(u-3v)^2.$$

4. Courbes de sous-groupe de torsion de la forme $\mathbb{Z}/10\mathbb{Z}$,

$$E_{10}:\ Y^2 = X(X^2 + a_2X + a_4),$$

avec

$$\begin{aligned} a_2 &= -(2u^2 + 2uv + v^2)(4u^4 + 12u^3v + 6u^2v^2 - 2uv^3 - v^4), \\ a_4 &= 16u^5(u+v)^5(u^2 + 3uv + v^2), \end{aligned}$$

et de discriminant

$$\Delta_{10} = -2^{12}u^{10}v^5(u+v)^{10}(2u+v)^5(u^2+3uv+v^2)^2(4u^2+2uv-v^2).$$

5. Courbes de sous-groupe de torsion de la forme $\mathbb{Z}/9\mathbb{Z}$,

$$E_9:\ Y^2 = X^3 + a_2X^2 + a_4X + a_6,$$

avec

$$\begin{aligned} a_2 &= u^6 - 6u^5v - 10u^3v^3 + 9u^4v^2 + 6u^2v^4 + v^6, \\ a_4 &= 8(u^3 - u^2v - v^3)u^2v^4(u-v)(u^2 - uv + v^2), \\ a_6 &= 16u^4v^8(u-v)^2(u^2 - uv + v^2)^2. \end{aligned}$$

Le discriminant est alors

$$\Delta_9 = 2^{12}u^9v^9(u-v)^9(u^2-uv+v^2)^3(u^3-6u^2v+3uv^2+v^3).$$

6. Courbes de sous-groupe de torsion de la forme $\mathbb{Z}/8\mathbb{Z}$,

$$E_8 : \ Y^2 = X(X^2 + a_2 X + a_4),$$

avec

$$\begin{aligned} a_2 &= \frac{1}{4}\left(8u^4 - 16u^3v + 16u^2v^2 - 8uv^3 + v^4\right), \\ a_4 &= u^4(u-v)^4. \end{aligned}$$

et tels que $a_2^2 - 4a_4 = (2u-v)^4v^2(8u^2-8uv+v^2)$ n'est pas un carré parfait. Le discriminant est alors

$$\Delta_8 = u^8v^2(u-v)^8(2u-v)^4(8u^2-8uv+v^2).$$

7. Courbes de sous-groupe de torsion de la forme $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$,

$$E_{2\times 4} : \ Y^2 = X(X^2 + u^2)(X + v^2),$$

tels qu'il n'existe pas de rationnels p et q vérifiant $E_{2\times 4}(u,v) = E_{2\times 8}(p,q)$. Le discriminant est alors

$$\Delta_{2\times 4} = 16u^4v^4(u+v)^2(u-v)^2.$$

8. Courbes de sous-groupe de torsion de la forme $\mathbb{Z}/7\mathbb{Z}$,

$$E_7 : \ Y^2 = X^3 + a_2X^2 + a_4X + a_6,$$

avec

$$\begin{aligned} a_2 &= u^4 - 6u^3v + 3u^2v^2 + 2v^3u + v^4, \\ a_4 &= 8u^2v^3(u-v)(u^2 - uv - v^2), \\ a_6 &= 16u^4v^6(u-v)^2. \end{aligned}$$

Le discriminant est alors

$$\Delta_7 = 2^{12}u^7v^7(u-v)^7(u^3 - 8u^2v + 5uv^2 + v^3).$$

9. Courbes de sous-groupe de torsion de la forme $\mathbb{Z}/6\mathbb{Z}$,

$$E_6 : \ Y^2 = X(X^2 - \frac{1}{4}(8u^2 - 12uv + 3v^2)X + u(u-v)^3),$$

tels que $-v(8u-9v)$ n'est pas un carré parfait. Le discriminant est alors

$$\Delta_6 = -u^2v^3(u-v)^6(8u-9v).$$

10. Courbes de sous-groupe de torsion de la forme $\mathbb{Z}/4\mathbb{Z}$,

$$E_4 : \; Y^2 = X(X^2 + 2u(2u - v)X + u^2v^2),$$

et tels que $u(u - v)$ n'est pas un carré parfait. Le discriminant est alors

$$\Delta_4 = 2^8u^7v^4(u - v).$$

11. Courbes de sous-groupe de torsion de la forme $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$,

$$E_{2\times 2} : \; Y^2 = X(X - u)(X - v),$$

tels qu'il n'existe pas de rationnels p et q vérifant $E_{2\times 2}(u, v) = E_{2\times 4}(p, q)$ ou $E_{2\times 2}(u, v) = E_{2\times 6}(p, q)$ ou $E_{2\times 2}(u, v) = E_{2\times 8}(p, q)$. Le discriminant est alors

$$\Delta_{2\times 2} = 2^4u^2v^2(u - v)^2.$$

References

1. A.O.L. Atkin and J. Lehner, *Hecke operators on* $\Gamma_0(m)$, Math. Ann. **185** (1970), 134–160.
2. C. Batut, D. Bernardi, H. Cohen and M. Olivier, *PARI-GP*, a computer system for number theory, Version 2.0, `ftp://megrez.ceremab.u-bordeaux.fr/pub/pari/`.
3. R. Bölling, *Die Ordnung der Schafarewitsch-Tate-Gruppe kann beliebig gro werden*, Math. Nachr. **67** (1975), 157–179.
4. J.W.S. Cassels, *Arithmetic on curves of genus 1. VI: The Tate-Safarevic group can be arbitrarily large*, J. Reine Angew. Math. **214/215** (1964), 65–70.
5. H. Cohen, *A Course in Computational Algebraic Number Theory*, Graduate Texts in Math., vol. 138, Springer-Verlag, Berlin, 1993.
6. I. Connell, *APECS*, Version 4.36, 1998, `ftp://math.mcgill.ca/pub/apecs/`.
7. J. Cremona, *Algorithms for Modular Elliptic Curves*, Cambridge University Press, Cambridge, 1992.
8. P. Deligne, *Les constantes des équations fonctionnelles des fonctions L*, in Antwerp II: Modular Functions of One Variable, Lecture Notes in Math., Springer-Verlag **349** (1973), 501–597.
9. F. Diamond, *On deformation rings and Hecke rings*, Ann. Math. **144** (1996), 137–166.
10. F. Diamond and K. Kramer, *Modularity of a family of elliptic curves*, Math. Res. Lett. **2** (1995), 299–304.
11. G. Frey, *Some aspects of the theory of elliptic curves over number fields*, Expo. Math. **4** (1986), 35–66.
12. J. Gebel and H.G. Zimmer, *Computing the Mordell-Weil group of an elliptic curve over* $\mathbb{Q}$, CRM Proc. Lect. Notes **4** (1994), 61–83.
13. D. Goldfeld and D. Lieman, *Effective bounds on the size of the Tate-Shafarevich group*, Math. Research Letters **3** (1996), 309–318.
14. D. Goldfeld and L. Szpiro, *Bounds for the order of the Tate-Shafarevich group*, Compos. Math. **97** (1995), 71–87.
15. B.H. Gross, *Kolyvagin's work on modular elliptic curves*, in L-functions and arithmetic, Proc. Symp., Durham/UK 1989, Lond. Math. Soc. Lect. Note Ser. **153** (1991), 235–256.
16. D. Husemöller, *Elliptic Curves*, Graduate Texts in Math., vol. 111, Springer-Verlag, Berlin, Heidelberg, New York, 1986.
17. W. Kohnen and D. Zagier, *Values of L-series of modular forms at the center of the critical strip*, Invent. Math. **64** (1981), 175–198.

18. V.A. Kolyvagin, *Finiteness of $E(\mathbb{Q})$ and $Ш(E/\mathbb{Q})$ for a subclass of Weil curves*, Math. USSR, Izv. **32** (1989), 523–541.
19. K. Kramer, *A family of semistable elliptic curves with large Tate-Shafarevitch groups*, Proc. Am. Math. Soc. **89** (1983), 379–386.
20. D.S. Kubert, *Universal bounds on the torsion of elliptic curves*, Proc. London Math. Soc. **33** (1976), 193–237.
21. S. Lang, *Conjectured diophantine estimates on elliptic curves*, Prog. Math. **35** (1983), 155–172.
22. A.K. Lenstra, H.W. Lenstra, and L. Lovász, *Factoring polynomials with rational coefficients*, Math. Ann. **261** (1982), 515–534.
23. L. Mai and M.R. Murty, *A note on quadratic twists of an elliptic curve*, in Elliptic curves and related topics, AMS, CRM Proc. Lect. Notes **4** (1994), 121–124.
24. Y. Manin, *Cyclotomic fields and modular curves*, Russian Math. Surveys **26** (1971), 7-78.
25. A. Nitaj, *Détermination de courbes elliptiques pour la conjecture de Szpiro*, Acta Arith. **85** (1998), 351-376.
26. ———, *Tables of good abc-examples*, preprint (1997), Saarbrücken.
27. C.S. Rajan, *On the size of the Shafarevich-Tate group of elliptic curves over function fields*, Compos. Math. **105** (1997), 29–41.
28. D.E. Rohrlich, *Galois theory, elliptic curves, and root numbers*, Compos. Math. **100** (1996), 311–349.
29. K. Rubin, *Tate-Shafarevich groups and L-functions of elliptic curves with complex multiplication*, Invent. Math. **89** (1987), 527–560.
30. J.H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Math., vol. 106, Springer Verlag, Berlin and New York, 1986.
31. Simath Group, *SIMATH*, a computer algebra system, Version 4.2, Saarbrüken, 1998 `ftp://ftp.math.uni-sb.de:/pub/simath`.
32. B.M.M. de Weger, *$A + B = C$ and big Sha's*, Quart. J. Math. Ser. (2), **49** (1998), 105–128.

Fb 9, Mathematik
Universität des Saarlandes
Postfach 15 1150
D-66041 Saarbrücken, Germany

E-mail address: `nitaj@math.uni-sb.de`