

MOHAMED KRIR

**Minorant de la dérivée au point 1 de la fonction L
attachée à une courbe elliptique de Weil**

Journal de Théorie des Nombres de Bordeaux, tome 6, n° 2 (1994),
p. 281-299

http://www.numdam.org/item?id=JTNB_1994__6_2_281_0

© Université Bordeaux 1, 1994, tous droits réservés.

L'accès aux archives de la revue « Journal de Théorie des Nombres de Bordeaux » (<http://jtnb.cedram.org/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

Minorant de la dérivée au point 1 de la fonction L attachée à une courbe elliptique de Weil

par MOHAMED KRIR

0. Introduction

Soit E une courbe elliptique définie sur \mathbf{Q} . Notons N son conducteur et $L(E, s)$ sa fonction de Hasse-Weil ([15], §8). Supposons que E est une courbe de Weil (ce qui est conjecturalement toujours le cas) et que $L(E, 1)$ est nul. En 1988, Kolyvagin (cf. [2]) a démontré que si $L'(E, 1)$ est non nul alors la courbe E est de rang 1. Considérons alors une courbe elliptique de Weil E de rang 1 et supposons que $L'(E, 1)$ est non nul. En utilisant une formule bien connue de Gross et Zagier (cf. [3]), on donne un minorant (dépendant essentiellement de N) de $L'(E, 1)$. On en déduit en particulier que pour une courbe elliptique de Weil de conducteur premier p et vérifiant la condition $L(E, 1) = 0$, on a $L'(E, 1) = 0$ ou bien

$$|L'(E, 1)| > (10^7 p^5 (1 + 1/p)^{3/2} H(E))^{-1} \log p$$

avec

$$H(E) = \sup(|c_4(E)|^{1/2}, |c_6(E)|^{1/3})$$

Dans le premier paragraphe on rappelle la formule de Gross et Zagier (*loc. cit.*). Les autres paragraphes sont consacrés à l'estimation de chacun des facteurs qui interviennent dans cette formule.

1. La formule de Gross et Zagier

Pour tout entier $N \geq 1$ on note $\Gamma_0(N)$ le sous-groupe de $SL_2(\mathbf{Z})$ formé des matrices carrés $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ telles que N divise c . Ce groupe opère sur le demi-plan de Poincaré $\mathcal{H} = \{\tau \in \mathbf{C} | \Im \tau > 0\}$ par $\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \tau \right) \mapsto \frac{a\tau + b}{c\tau + d}$.

Soit E une courbe elliptique définie sur \mathbf{Q} . Notons N son conducteur et $L(E, s)$ sa fonction de Hasse-Weil ([15] §8) et posons

$$L(E, s) = \sum_{n \geq 1} a_n n^{-s}.$$

On dit que E est une *courbe de Weil (faible)* dans la terminologie de [9]) s'il existe un morphisme φ non constant, défini sur \mathbf{Q} de la courbe modulaire $X_0(N)$ dans E . Tel est le cas si et seulement si la fonction f_E définie sur \mathcal{H} par

$$f_E(\tau) = \sum_{n \geq 1} a_n e^{2i\pi n\tau}$$

est une forme modulaire parabolique de poids 2 pour $\Gamma_0(N)$, et f_E est alors une newform de poids 2 et de niveau N au sens d'Atkin-Lehner [1], normalisée (i.e. telle que $a_1 = 1$).

Supposons que E est une courbe elliptique de Weil de conducteur N .

a) Posons $\Lambda(E, s) = (2\pi)^{-s} \Gamma(s) N^{s/2} L(E, s)$. On sait alors que cette fonction Λ vérifie l'équation fonctionnelle $\Lambda(E, s) = \epsilon \Lambda(E, 2-s)$ avec $\epsilon = 1$ ou -1 . Dans cet article on suppose que $\epsilon = -1$.

b) Le carré scalaire de Petersson de la newform f_E de poids 2 et de niveau N associée à E est par définition

$$\|f_E\|^2 = \int \int_{\mathcal{D}} |f_E(x+iy)|^2 dx dy$$

où \mathcal{D} est un domaine fondamental quelconque de \mathcal{H} modulo l'action de $\Gamma_0(N)$.

c) Soit $\varphi : X_0(N) \rightarrow E$ un morphisme non constant défini sur \mathbf{Q} . Soit ω_E une forme différentielle de Néron sur E : c'est une forme différentielle qui s'étend en une forme différentielle régulière et partout non nulle sur le modèle de Néron de E , propriété qui la caractérise au signe près. Puisque le morphisme φ est défini sur \mathbf{Q} et que la forme différentielle $2i\pi f_E(\tau) d\tau$ est rationnelle sur \mathbf{Q} , il existe un nombre rationnel non nul c_E appelé la *constante de Manin* relative à E , tel que

$$\varphi^*(\omega_E) = c_E 2i\pi f_E(\tau) d\tau.$$

Posons

$$\|\omega_E\|^2 = \int_{E(\mathbf{C})} |\omega_E \wedge \overline{\omega_E}|.$$

Le nombre $2 \|\omega_E\|^2$ est souvent appelé *l'aire* ou *le volume* de la courbe E pour la différentielle ω_E . Le degré du morphisme φ , la norme de Petersson de la newform f_E associée à E , l'aire de la courbe E pour la différentielle ω_E et la constante de Manin c_E relative à E sont liés par l'égalité

$$(1) \quad \frac{\|\omega_E\|^2}{c_E^2} = \frac{8\pi^2 \|f_E\|^2}{\deg(\varphi)}.$$

En effet on a successivement

$$\begin{aligned} \|f_E\|^2 &= \int \int_{\mathcal{D}} |f_E(x+iy)|^2 dx dy \\ &= \frac{i}{2} \int \int_{\mathcal{D}} f_E(\tau) d\tau \wedge \overline{f_E(\tau)} d\tau \\ &= \frac{i}{8\pi^2 c_E^2} \int \int_{\mathcal{D}} \varphi^*(\omega_E) \wedge \overline{\varphi^*(\omega_E)} \\ &= \frac{i}{8\pi^2 c_E^2} \deg(\varphi) \int_{E(C)} \omega_E \wedge \overline{\omega_E} \\ &= \frac{\deg(\varphi)}{8\pi^2 c_E^2} \|\omega_E\|^2 \end{aligned}$$

d) Soit K un corps quadratique imaginaire de discriminant D premier à N . On note χ_D le caractère quadratique relatif à K . On suppose que tout facteur premier de N se décompose totalement dans K . Posons

$$L(E^D, s) = \sum_{n \geq 1} a_n \chi_D(n) n^{-s}.$$

C'est la série L associée à la courbe elliptique obtenue en tordant la courbe E par le corps K , (i.e. la courbe elliptique d'équation $D y^2 = x^3 + ax + b$ si on suppose que $y^2 = x^3 + ax + b$ est une équation de Weierstrass de E).

La série $L(E/K, s)$ associée à la courbe elliptique E , regardée sur K est alors égale à $L(E^D, s)L(E, s)$. Et compte tenu de l'hypothèse faite en a) sur le signe de l'équation fonctionnelle de la série $L(E, s)$, on a $L(E, 1) = 0$ et le point P_K de $E(K)$ considéré dans le théorème de Gross et Zagier ([3], th. 2.1, p.311) est tel que le point $P = 2P_K$ appartient à $E(\mathbb{Q})$. La formule énoncée dans ce même théorème s'écrit alors

$$(2) \quad L'(E, 1)L(E^D, 1) = \frac{\|\omega_E\|^2}{c_E^2 u^2 \sqrt{|D|}} \widehat{h}(P)$$

ou encore en tenant compte de (1)

$$(2') \quad L'(E, 1)L(E^D, 1) = \frac{8\pi^2 \|f_E\|^2}{\deg(\varphi)u^2\sqrt{|D|}} \widehat{h}(P)$$

où \widehat{h} est la hauteur de Néron-Tate relative au diviseur (0), définie sur $E(\mathbf{Q})$ (c.f. §2) et où $2u$ désigne le nombre de racines de l'unité dans K .

Selon que l'on dispose d'informations sur la constante de Manin ou sur le degré de φ , on utilisera la formule (2) ou (2') pour minorer le nombre $L'(E, 1)$ quand il n'est pas nul. Dans tous les cas on aura besoin de majorer $|D|$ et $L(E^D, 1)$ et de minorer $\widehat{h}(P)$, puis minorer l'aire de E ou la norme de Petersson de f_E . On a choisi ici d'utiliser la formule (2) pour minorer $L'(E, 1)$.

2. Minorant de la hauteur de Néron-Tate

Soit E une courbe elliptique (pas nécessairement de Weil) définie sur \mathbf{Q} . La hauteur de Néron-Tate, relative au diviseur (0), sur $E(\mathbf{Q})$ est une fonction $h : E(\mathbf{Q}) \rightarrow \mathbf{R}$ qui s'annule en un point P si et seulement si P est un point de torsion. Elle définit par passage au quotient une forme quadratique définie positive

$$\widehat{h} : E(\mathbf{Q})/E(\mathbf{Q})_{\text{tors}} \rightarrow \mathbf{R}$$

D'autre part, la hauteur \widehat{h} admet en tout nombre premier p une composante locale λ_p et en la place à l'infini une composante λ_∞ et pour tout point P d'ordre infini de $E(\mathbf{Q})$ on a :

$$(3) \quad \widehat{h}(P) = \sum_p \lambda_p(P) + \lambda_\infty(P)$$

2.1. Hauteur locale en p

Considérons un modèle minimal de Weierstrass à coefficients entiers, de la courbe elliptique E , d'équation

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

Écrivons $\Delta(E)$ son discriminant (cf. [15], §1 ou [14], p. 46) pour la définition de $\Delta(E)$ en fonction des a_i). Notons E_p la cubique (éventuellement singulière) dont une équation est obtenue par la réduction modulo

p de l'équation ci-dessus. Notons \mathcal{E}^0 la composante neutre du modèle de Néron de E : les points de $\mathcal{E}^0(\mathbf{Q})$ sont ceux dont la réduction modulo n 'importe quel nombre premier p est un point non singulier de E_p .

La hauteur locale en la place p est une fonction $\lambda_p : E(\mathbf{Q}_p) - \{0\} \longrightarrow \mathbf{R}$. Sa valeur en un point $P = (x(P), y(P))$ de $\mathcal{E}^0(\mathbf{Q}_p)$ est (cf. [13], p. 635)

$$\lambda_p(P) = \max\left(-\frac{1}{2}v_p(x(P)), 0\right) + \frac{1}{12}v_p(\Delta(E))$$

où v_p est la valuation de \mathbf{Q}_p (normalisée par $v_p(p) = \log(p)$). Ainsi, pour tout point P de $\mathcal{E}^0(\mathbf{Q}_p)$ on a

$$(4) \quad \sum_p \lambda_p(P) \geq \frac{1}{12} \log |\Delta(E)|$$

2.2. Hauteur locale à l'infini

Soit E une courbe elliptique définie sur \mathbf{C} . Soient τ un nombre complexe de partie imaginaire strictement positive, $\Phi : E \longrightarrow \mathbf{C}/(\mathbf{Z} \oplus \mathbf{Z}\tau)$ un isomorphisme de courbes elliptiques, P un point de $E(\mathbf{C})$ et z un nombre complexe dont la classe modulo $(\mathbf{Z} \oplus \mathbf{Z}\tau)$ est égale à $\Phi(P)$. Posons $q_u = e^{2i\pi u}$ pour tout nombre complexe u . Alors $\lambda_\infty(P)$ est égal (cf. [13], p. 635) à la fonction :

$$f(\tau, z) = -\frac{1}{2}B_2(b) \log |q_\tau| - \log |1 - q_z| - \log \prod_{n \geq 1} |(1 - q_\tau^n q_z)(1 - q_\tau^n q_z^{-1})|$$

où $B_2(T) = T^2 - T + \frac{1}{6}$ pour $0 \leq T \leq 1$ (prolongé périodiquement modulo 1).

On ne peut pas toujours minorer $\lambda_\infty(P)$, mais on peut le faire pour un multiple convenable de P . Plus précisément on a le lemme suivant :

LEMME 1. *Pour tout point P de $E(\mathbf{C})$ on a :*

$$(5) \quad \max(\lambda_\infty(P), \dots, \lambda_\infty(4P)) > -\frac{3}{10}$$

Démonstration. Choisissons τ dans un domaine fondamental de \mathcal{H} modulo l'action de $SL_2(\mathbf{Z})$. On a en particulier $\Im m(\tau) \geq \sqrt{3}/2$. Posons $q = |q_\tau|$. On a alors

$$(*) \quad 0 < q \leq e^{-\pi\sqrt{3}} = 0.0043342\dots$$

Considérons un isomorphisme $\Phi : E(\mathbf{C}) \longrightarrow \mathbf{C}/(\mathbf{Z} \oplus \mathbf{Z}\tau)$ de courbes elliptiques. Soit P un point de $E(\mathbf{C})$ tel que $\Phi(P) = z = a + b\tau$ avec $0 < a, b \leq 1$. Remarquons d'abord que l'on a $f(\tau, 1 + \tau - z) = f(\tau, z)$. Donc on peut restreindre les réels a et b à l'intervalle $]0, 1/2]$. D'autre part, on a $|q_z| = q^b$. D'où :

$$\lambda_\infty(P) = f(\tau, z) \geq g(q, b)$$

avec

$$g(q, b) = -\frac{1}{2}B_2(b) \log q - \log(1 + q^b) - \log \prod_{n \geq 1} (1 + q^{n-b})(1 + q^{n+b})$$

Pour démontrer le lemme il suffit de minorer $g(q, b)$ par $(-3/10)$ quand b parcourt l'intervalle $]0, 1/5]$. En effet, si P est un point de $E(\mathbf{C})$ tel que $\Phi(P)$ est la classe d'un nombre complexe $a + b\tau$ avec $0 < b \leq 1/2$, alors l'un des quatre points $\Phi(P), \dots, \Phi(4P)$ est la classe d'un nombre complexe de la forme $\alpha + \beta\tau$ avec β appartenant à $[-1/5, 1/5]$. Et comme $\lambda_\infty(-P) = f(\tau, -z) = f(\tau, z) = \lambda_\infty(P)$, on aura le résultat.

Supposons alors que $0 < b \leq 1/5$. On a :

a) La majoration

$$\begin{aligned} \log \prod_{n \geq 1} (1 + q^{n-b})(1 + q^{n+b}) &= \sum_{n \geq 1} \log(1 + q^{n+b}) + \sum_{n \geq 1} \log(1 + q^{n-b}) \\ &\leq \sum_{n \geq 1} q^{n+b} + \sum_{n \geq 1} q^{n-b} = \frac{q(q^b + q^{-b})}{(1 - q)} \\ &\leq \frac{q(q^{1/5} + q^{-1/5})}{(1 - q)} \\ &\leq 0.01443 \dots \text{ compte tenu de } (*) \end{aligned}$$

b) Posons $h(q, b) = \frac{1}{2}B_2(b) \log q + \log(1 + q^b)$. Cette fonction et ses dérivées successives par rapport à b sont données par :

$$\begin{aligned} h(q, b) &= \frac{1}{12} \log q + \log \left(q^{(b^2-b)/2} + q^{(b^2+b)/2} \right), \\ h'(q, b) &= \left(b - \frac{1 - q^b}{2(1 + q^b)} \right) \log q, \\ h^{(2)}(q, b) &= \left(1 + \frac{q^b}{(1 + q^b)^2} \log q \right) \log q, \\ h^{(3)}(q, b) &= \frac{q^b(1 - q^b)}{(1 + q^b)^3} (\log q)^3. \end{aligned}$$

Puisque b appartient à $]0, 1/5]$, on a $h^{(3)}(q, b) < 0$ et par suite $h^{(2)}(q, b)$ est strictement décroissante en b . Or, la limite en 0 de $h'(q, b)$ est nulle et $h'(q, 1/5) > 0$ compte tenu de (*). Donc $h'(q, b) > 0$ et $h(q, b)$ est croissante en b . Ainsi, on a :

$$h(q, b) \leq h(q, 1/5) = \frac{\log q}{300} + \log(1 + q^{1/5}) \leq 0.2722 \text{ compte tenu de } (*).$$

En combinant (a) et (b) on a le lemme.

2.3. Minorant de $\hat{h}(P)$

Soit E une courbe elliptique définie sur \mathbf{Q} . Rappelons que \mathcal{E}^0 désigne la composante neutre du modèle de Néron de E . Pour tout nombre premier p où E a mauvaise réduction, notons m_p le plus petit entier qui annule le groupe $E(\mathbf{Q}_p)/\mathcal{E}^0(\mathbf{Q}_p)$. On sait alors que m_p est égal à l'exposant en p de $\Delta(E)$ si E a en p mauvaise réduction de type multiplicatif et à 2, 3 ou 4 dans les autres cas. Pour les différents types de réduction (cf. [14], p. 359). Posons

$$M_E = \text{p.p.c.m.}(m_p)$$

La proposition suivante donne un minorant de la hauteur de Néron-Tate sur $E(\mathbf{Q})$.

PROPOSITION 1. *Soit E une courbe elliptique définie sur \mathbf{Q} . Notons $\Delta(E)$ son discriminant minimal. Alors pour tout point d'ordre infini de $E(\mathbf{Q})$ on a*

$$\hat{h}(P) > \frac{1}{16 M_E^2} \left(\frac{\log |\Delta(E)|}{12} - \frac{3}{10} \right)$$

Démonstration. Compte tenu de (3), (4), (5) et du fait que $\hat{h}(nP) = n^2 \hat{h}(P)$ pour tout entier n , on a pour tout point P de $\mathcal{E}^0(\mathbf{Q})$ l'inégalité $\hat{h}(P) > \frac{1}{16} \left(\frac{\log |\Delta(E)|}{12} - \frac{3}{10} \right)$. D'autre part, pour tout point d'ordre infini de $E(\mathbf{Q})$, le point $M_E P$ appartient à $\mathcal{E}^0(\mathbf{Q})$. D'où la proposition.

COROLLAIRE. *Pour toute courbe elliptique de Weil E de rang 1 et pour tout point d'ordre infini de $E(\mathbf{Q})$ on a :*

$$(6) \quad \hat{h}(P) > 10^{-5} M_E^{-2} \log |\Delta(E)|$$

Démonstration. En effet, dans ce cas $|\Delta(E)| \geq 37$ et par suite

$$\frac{1}{16} \left(\frac{\log |\Delta(E)|}{12} - \frac{3}{10} \right) \geq 10^{-5} \log |\Delta(E)|.$$

2.4. D'autres minoration de $\hat{h}(P)$

a) Dans ([5], cor. 4.3.2, p. 39) on donne également des minoration de $\hat{h}(P)$ pour une courbe elliptique quelconque définie sur \mathbf{Q} . Les résultats qu'on obtient sont plus précis que ceux présentés ici mais les démonstrations sont plus longues. Dans (*loc. cit*) les minoration obtenues sont de la forme

$$\hat{h}(P) > \frac{1}{n^2 M_E^2} \left(\frac{\log |\Delta(E)|}{12} + c \right),$$

où l'entier n et la constante c sont calculés de manière optimale et dépendent des différents signes des invariants $c_4(E)$, $c_6(E)$ et $\Delta(E)$ de la courbe E munie d'une forme différentielle non nulle quelconque. On montre en particulier que $n = 9$ et $c = 0$ conviennent à toutes les courbes elliptiques. Ce qui donne :

$$\hat{h}(P) > 10^{-3} M_E^{-2} \log |\Delta(E)|.$$

b) Hindry et Silverman démontrent dans ([4], th. 0.3) que pour toute courbe elliptique E définie sur \mathbf{Q} , de conducteur $N(E)$ et pour tout point P d'ordre infini de $E(\mathbf{Q})$ on a :

$$\hat{h}(P) > (20 \beta_E)^{-8} 10^{-1,1-4\beta_E} \quad \text{avec} \quad \beta_E = \frac{\log |\Delta(E)|}{\log N(E)}.$$

Le minorant donné dans a) est meilleur que celui de Hindry et Silverman au moins pour les courbes elliptiques de conducteur $N(E) \leq 10^{10}$.

3. Majorant de $|D|$

Il s'agit de prouver l'existence d'un entier $D < 0$, tel que le corps $\mathbf{Q}(\sqrt{D})$ vérifie les conditions du (§ 1. d)) et tel que $L(E^D, 1)$ soit non nul. Ensuite, il faut majorer la valeur absolue d'un tel entier D . On aura besoin du lemme auxiliaire suivant :

LEMME 2. Pour tout entier $N \geq 3$ on a

$$\sum_{\substack{\delta \text{ impair} \\ \delta > 0, \delta | N}} \frac{\varphi(\text{pgcd}(\delta, N/\delta))}{\delta \text{pgcd}(\delta, N/\delta)} = \prod_{\substack{p \text{ premier} \\ p \geq 3, p | N}} \left(1 + \frac{1}{p}\right),$$

où φ désigne la fonction indicatrice d'Euler.

Démonstration. Pour tout entier N et pour tout entier positif impair δ divisant N , posons :

$$A(\delta, N) = \frac{\varphi(\text{pgcd}(\delta, N/\delta))}{\delta \text{pgcd}(\delta, N/\delta)} \quad \text{et} \quad S(N) = \sum_{\delta} A(\delta, N)$$

Remarquons d'abord que si $N = 2^r N'$ avec N' impair alors on a $S(N) = S(N')$. Il suffit donc de montrer le lemme pour N impair.

a) Pour tout nombre premier impair p et pour tout entier $n \geq 1$ on a :

$$A(p^k, p^n) = \begin{cases} 1 & \text{si } k = 0, \\ \frac{p-1}{p^{k+1}} & \text{si } 1 \leq k \leq n-1 \\ \frac{1}{p^n} & \text{si } k = n \end{cases}$$

D'où

$$S(p^n) = 1 + \sum_{k=1}^{n-1} \left(\frac{1}{p^k} - \frac{1}{p^{k+1}} \right) + \frac{1}{p^n} = 1 + \frac{1}{p} = S(p).$$

b) Pour tout nombre premier p impair, pour tout entier M premier à p , pour tout diviseur δ de M et pour tout entier $n \geq 1$, on a :

$$\text{pgcd}((\delta p^k, (M p^n)/(\delta p^k)) = \text{pgcd}(M, \delta) \text{pgcd}(p^k, p^{n-k});$$

et comme la fonction φ est multiplicative, on a

$$A(\delta p^k, M p^n) = A(\delta, M) A(p^k, p^n),$$

et par suite

$$S(M p^n) = \sum_{k=1}^{n-1} \sum_{\delta|M} A(\delta p^k, M p^n) = S(M) S(p^n) = S(M) S(p).$$

D'après (a) et (b) on a le lemme.

La proposition suivante précise un majorant de $|D|$.

PROPOSITION 2. *Soit E une courbe elliptique de Weil. On note N son conducteur et on suppose que le signe de l'équation fonctionnelle de sa série $L(E, s)$ (t c.f. §1. a) est égal à (-1) . On pose*

$$N' = \prod_{\substack{p \text{ premier} \\ p \geq 3, p|N}} p \quad \text{et} \quad S(N) = \prod_{\substack{p \text{ premier} \\ p \geq 3, p|N}} \left(1 + \frac{1}{p}\right).$$

Alors il existe un entier $D < 0$ tel que tout nombre premier qui divise N se décompose totalement dans $\mathbf{Q}(\sqrt{D})$ et $L(E^D, 1) \neq 0$ (c.f. §1 pour la définition de $L(E^D, s)$). On a de plus :

$$(7) \quad |D| < 384NN'^2S(N).$$

Démonstration. Dans ([6]) on donne la démonstration de cette proposition en travaillant avec une newform f de poids 2 et de niveau N au lieu d'une courbe elliptique. On en rappelle ici le principe en apportant une amélioration en (7). Le majorant de $|D|$ donné dans (*loc. cit.*) est $384NN'^2 \log NN'^2$.

On considère la newform f_E attachée à la courbe elliptique E comme au §1. La série de Dirichlet associée à f_E est alors égale à $L(E, s)$ et pour tout caractère χ_D comme au §1, la série de Dirichlet associée à $(f_E \otimes \chi_D)$ est égale à $L(E^D, s)$.

À la forme f_E , Waldspurger ([16]) associe une forme modulaire non nulle $g_E = \sum b_n q^n$ et un caractère de Dirichlet pair χ tels que g_E est de poids $3/2$ et de caractère χ . De plus, la non nullité d'un coefficient b_n de la forme g_E équivaut aux deux conditions : tout nombre premier qui divise N se décompose totalement dans $\mathbf{Q}(\sqrt{D})$ et $L(E^D, 1) \neq 0$ avec $D = -n$. Pour prouver (7), il faudrait donc majorer un entier n pour lequel on a $b_n \neq 0$. Pour cela il faudrait estimer le niveau M de la forme modulaire g_E . En suivant la construction de Waldspurger des facteurs locaux de g_E , on montre que l'on peut prendre pour M un entier divisant $2^{11}NN'^2$.

On applique enfin un lemme de Shintani ([12], lemme 3.2, p. 122) à la forme g_E pour prouver l'existence d'un entier

$$n < (3M/16) \sum_{\delta} \frac{\varphi(\gcd(\delta, N/\delta))}{\delta \text{pgcd}(\delta, N/\delta)}$$

(cf. lemme 2 pour la définition de cette somme) tel que $b_n \neq 0$. On prend alors $D = -n$ et compte tenu du même lemme et du fait que M est un diviseur de $2^{11}NN'^2$, on obtient $n < 384NN'^2S(N)$.

4. Majorant de $|L(E^D, 1)|$

LEMME 3. Pour tout entier naturel n , le nombre de diviseurs positifs de n vérifie l'inégalité :

$$d(n) \leq \sqrt{3n}.$$

Démonstration. Commençons par majorer $d(p^r)$ où p est un nombre premier et r est un entier positif.

a) Si $p = 2$, on a $d(2) = 2 < \frac{3}{2}\sqrt{2}$ et $d(2^2) = 3 = \frac{3}{2}\sqrt{4}$ et pour tout entier $r \geq 2$ l'inégalité $\frac{d(2^{r+1})}{d(2^r)} = \frac{r+2}{r+1} \leq \frac{4}{3} < \sqrt{2}$. Donc, par récurrence sur r on a $d(2^r) \leq \frac{3}{2}\sqrt{2^r}$.

b) Si $p = 3$, on a $d(3) = 2$, et pour tout entier $r \geq 1$ l'inégalité $\frac{d(3^{r+1})}{d(3^r)} = \frac{r+2}{r+1} \leq \frac{3}{2} < \sqrt{3}$. Donc, par récurrence sur r on a $d(3^r) \leq \frac{2}{\sqrt{3}}\sqrt{3^r}$.

c) Si $p \geq 5$, pour tout entier $r \geq 0$ on a $\frac{d(p^{r+1})}{d(p^r)} = \frac{r+2}{r+1} \leq 2 < \sqrt{p}$. Donc, par récurrence sur r on a $d(p^r) \leq \sqrt{p^r}$.

Ainsi si $n = \prod_{p \text{ premier}} p^{r_p}$ alors $d(n) = \prod_p d(p^{r_p}) \leq \frac{3}{2} \frac{2}{\sqrt{3}} \sqrt{n} = \sqrt{3n}$. D'où le lemme.

La proposition suivante donne un majorant de $|L(E^D, 1)|$ (cf. §1 pour la définition de $L(E^D, s)$.)

PROPOSITION 3. *Soit E/\mathbf{Q} une courbe elliptique de conducteur N et dont une équation de Weierstrass est $y^2 = x^3 + ax + b$. Soit D un entier négatif et premier à N . Alors la valeur en $s = 1$ de la série de Dirichlet $L(E^D, s)$ associée à la courbe elliptique E^D d'équation $Dy^2 = x^3 + ax + b$, vérifie l'inégalité :*

$$(8) \quad |L(E^D, 1)| \leq \frac{|D|\sqrt{3N}}{\pi}$$

Démonstration. Posons $L(E, s) = \sum_{n \geq 1} a_n n^{-s}$. D'après Manin ([7], th. 9.3, p. 61) on a l'égalité suivante :

$$L(E^D, 1) = \sum_{n \geq 1} a_n \chi_D(n) (1 - \chi_D(-N)) e^{-2\pi n / |D|\sqrt{N}},$$

et on sait que pour tout entier n , $|a_n| < d(n)\sqrt{n}$ où $d(n)$ est le nombre de diviseurs positifs de n , donc par le lemme 3, on aura $|a_n| < n\sqrt{3}$. Par ailleurs on a toujours $|\chi_D(n)(1 - \chi_D(-N))| \leq 2$, donc :

$$\begin{aligned} |L(E^D, 1)| &\leq \sum_{n \geq 1} e^{-2\pi n / |D|\sqrt{N}} \\ &\leq 2\sqrt{3} \int_0^{+\infty} e^{-2\pi x / |D|\sqrt{N}} dx = \sqrt{3N} |D| / \pi. \end{aligned}$$

5. Minorant de l'aire de E

5.1. Un lemme auxiliaire

On va commencer par démontrer un lemme auxiliaire. Rappelons d'abord quelques notations usuelles. Soit τ un nombre complexe de partie imaginaire strictement positive. Posons comme d'habitude $q_\tau = e^{2i\pi\tau}$ et considérons les séries convergentes suivantes :

$$E_4(\tau) = 1 + 240 \sum_{n \geq 1} \sigma_3(n) q_\tau^n = 1 + 240 \sum_{n \geq 1} n^3 \frac{q_\tau^n}{1 - q_\tau^n},$$

$$E_6(\tau) = 1 - 504 \sum_{n \geq 1} \sigma_5(n) q_\tau^n = 1 - 504 \sum_{n \geq 1} n^5 \frac{q_\tau^n}{1 - q_\tau^n},$$

$$\Delta(\tau) = \frac{E_4^3(\tau) - E_6^2(\tau)}{1728} \quad \text{et} \quad j(\tau) = \frac{E_4^3(\tau)}{\Delta(\tau)},$$

où pour tout entier k et pour tout entier n , $\sigma_k(n) = \sum_{d|n} d^k$.

LEMME 4. *On a les inégalités suivantes :*

a) $1.20 < |E_4(i)|^{1/2} < 1.21$

b) $\frac{\sqrt{3}}{2} |E_6(\rho)|^{1/3} > 1.23 \quad \text{où} \quad \rho = e^{i\pi/3}$

c) $\frac{\sqrt{3}}{2} |E_6(\frac{1}{2} + i)|^{1/3} > 1$

d) *Quand τ décrit le bord de $P = \{\tau \in \mathbf{C} / 0 \leq \Re(\tau) \leq \frac{1}{2} \text{ et } |\tau| \geq 1\}$, on a*

$$\Im m(\tau) \sup \left(|E_4(\tau)|^{1/2}, |E_6(\tau)|^{1/3} \right) > 1.$$

Démonstration.

a) Posons $q = e^{-2\pi}$. On a $E_4(i) = \sum_{n \geq 1} n^3 \frac{q^n}{1 - q^n}$ et $n^3 = n(n-1)(n-2) + 3n(n-1) + n$. D'où

$$\sum_{n \geq 1} n^3 q^n = \frac{6q^3}{(1-q)^4} + \frac{6q^2}{(1-q)^3} + \frac{q}{(1-q)^2}$$

et puisque $1 - q \leq 1 - q^n < 1$, on a successivement

$$\begin{aligned} 1 + 240 \sum_{n \geq 1} n^3 q^n &\leq E_4(i) < 1 + \frac{240}{1 - q} \sum_{n \geq 1} n^3 q^n \\ 1 + 240 \frac{6q^3 + 6q^2 + q}{(1 - q)^2} &\leq E_4(i) < 1 + 240 \frac{6q^3 + 6q^2 + q}{(1 - q)^5} \\ 1.4549 &\leq E_4(i) < 1.4575 \\ 1.20 &\leq |E_4(i)|^{1/2} < 1.21. \end{aligned}$$

b) et c) On a $E_6(\frac{1}{2} + it) = 1 - 504 \sum_{n \geq 1} \sigma_5(n) (-1)^n e^{-2\pi n t}$.

Dans cette dernière somme les termes sont de signes alternés, et de valeur absolue strictement décroissante, comme il résulte des inégalités suivantes :

$$n^5 \leq \sigma_5(n) = \sum_{d|n} (n/d)^5 \leq n^5 \zeta(5) \leq \frac{5}{4} n^5 \quad \text{et}$$

$$\frac{\sigma_5(n+1)e^{-2\pi(n+1)t}}{\sigma_5(n)e^{-2\pi n t}} \leq \frac{5}{4} \left(\frac{n+1}{n} \right)^5 e^{-2\pi t} \leq 40e^{-\pi\sqrt{3}} < 1 \quad \text{pour } t \geq \sqrt{3}$$

On a par conséquent :

$$\frac{\sqrt{3}}{2} |E_6(\rho)|^{1/3} > \frac{\sqrt{3}}{2} \left[1 + 504e^{-\pi\sqrt{3}} - 504(33e^{-2\pi\sqrt{3}}) \right]^{1/3} > 1.23$$

et

$$\frac{\sqrt{3}}{2} |E_6(\frac{1}{2} + i)|^{1/3} > \frac{\sqrt{3}}{2} \left[1 + 504e^{-2\pi} - 504(33e^{-4\pi}) \right]^{1/3} > 1.$$

d) Remarquons d'abord que la fonction qui à $t \geq \sqrt{3}/2$ associe $E_6(1/2 + it)$ est strictement décroissante. En effet, la dérivée par rapport à t de cette fonction est égale à $1008 \sum_{n \geq 1} \sigma_5(n) (-1)^n e^{-2\pi n t}$ et cette somme est du signe

de son premier terme, donc négative car, pour $t \geq \sqrt{3}/2$, il vient :

$$\frac{(n+1)\sigma_5(n+1)e^{-2\pi(n+1)t}}{n\sigma_5(n)e^{-2\pi n t}} \leq \frac{5}{4} \left(\frac{n+1}{n} \right)^6 e^{-2\pi t} \leq 80e^{-\pi\sqrt{3}} < 1.$$

Posons maintenant $\psi(\tau) = \Im m(\tau) \sup \left(|E_4(\tau)|^{1/2}, |E_6(\tau)|^{1/3} \right)$, on a alors

$$\psi(\tau) = \Im m(\tau) |\Delta(\tau)|^{1/6} \sup \left(|j(\tau)|, |j(\tau) - 1728| \right)^{1/6}.$$

On va maintenant distinguer trois cas.

cas 1: Si $\tau = it$ avec $t \geq 1$, alors $j(\tau) \geq 1728$ et $\psi(\tau) = \Im m(\tau) |E_4(\tau)|^{1/2} > 1$ car $\Im m(\tau) \geq 1$ et $E_4(\tau) > 1$ (remarquons ici que l'on peut montrer que le minimum de la fonction ψ est atteint en $\tau = i$).

cas 2: Si $\tau = 1/2 + it$ avec $t \geq \sqrt{3}/2$ alors $j(\tau) \leq 0$ et $\psi(\tau) = \Im m(\tau) |E_6(\tau)|^{1/3}$ d'où si $t \geq 1$, $\psi(\tau) > 1$ car $E_6(\tau) > 1$ et, si $\sqrt{3}/2 \leq t < 1$, alors $\psi(\tau) > \sqrt{3}/2 |E_6(1/2 + i)|^{1/3} > 1$ d'après le (c).

cas 3: Si $\tau = e^{i\theta}$ avec $\pi/3 \leq \theta \leq \pi/2$, alors $0 \leq j(\tau) \leq 1728$, donc

$$\sup \left(|j(\tau)|, |j(\tau) - 1728| \right)^{1/6} \geq (864)^{1/6}$$

et par suite

$$\psi(\tau) \geq \Im m(\tau) |\Delta(\tau)|^{1/6} (864)^{1/6}.$$

Considérons alors la fonction f définie sur le demi-plan de Poincaré \mathcal{H} par :

$$f(\tau) = \Im m(\tau) |\Delta(\tau)|^{1/6}.$$

Cette fonction est à valeurs réelles, de classe (C^∞) en (x, y) (où $\tau = x + iy$), et invariante par $SL_2(\mathbf{Z})$ car la fonction Δ est une forme modulaire de poids 12.

Posons :

$$E_2(\tau) = 1 - 24 \sum_{n \geq 1} \sigma_1(n) q_\tau^n \quad \text{et} \quad E_2^*(\tau) = E_2(\tau) - \frac{3}{\pi y}.$$

On a alors :

$$\frac{1}{2} \left(\frac{\partial f}{\partial x} - i \frac{\partial f}{\partial y} \right) = \frac{\partial f}{\partial \tau} = \frac{i}{24\pi} E_2^*(\tau).$$

Pour que la différentielle de f s'annule en τ , il faut et il suffit que $E_2^*(\tau) = 0$, c'est à dire d'après Masser ([8], lemme 3.2) que τ appartienne l'orbite de i

ou de ρ sous $SL_2(\mathbf{Z})$. Cette différentielle en $e^{i\theta}$ est nulle sur la normale au cercle unité. Par conséquent la fonction $\theta \mapsto f(e^{i\theta})$ admet sur $] \pi/3, \pi/2[$ une dérivée non nulle, de signe constant ; ce signe est négatif puisque l'on a

$$f(i) = |\Delta(i)|^{1/6} = |E_4(i)|^{1/2}(1728)^{-1/6}$$

$$f(\rho) = (\sqrt{3}/2)|\Delta(\rho)|^{1/6} = (\sqrt{3}/2)|E_6(\rho)|^{1/3}(1728)^{-1/6}$$

et d'après (a) et (c) on a $f(i) < f(\rho)$. Ainsi, quand θ varie dans $] \pi/3, \pi/2[$, on a

$$\psi(e^{i\theta}) \geq f(i)(864)^{1/6} = |E_4(i)|^{1/2}(2)^{-1/6} > 1 \quad \text{d'après (a).}$$

Ceci achève la démonstration du lemme.

5.2. Minorant de l'aire de E

Considérons maintenant une courbe elliptique E définie sur \mathbf{Q} , et dont un modèle de Weierstrass minimal à coefficients entiers a pour équation

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

Prenons comme d'habitude $\omega_E = dx/2y + a_1x + a_3$ pour forme différentielle de Néron sur E . Soient $c_4(E) = c_4(E, \omega_E)$ et $c_6(E) = c_6(E, \omega_E)$ les invariants habituels attachés à E . Pour leurs définitions en fonction des a_i , voir par exemple ([14], p. 46). Rappelons que l'on a posé :

$$\|\omega_E\|^2 = \int_{E(\mathbf{C})} |\omega_E \wedge \overline{\omega_E}|.$$

PROPOSITION 4. *Pour toute courbe elliptique E définie sur \mathbf{Q} on a*

$$(9) \quad \|\omega_E\|^2 > \frac{8\pi^2}{H(E)} \quad \text{où} \quad H(E) = \sup(|c_4(E)|^{1/2}, |c_6(E)|^{1/3})$$

Démonstration. À la paire (E, ω_E) est associé un réseau de \mathbf{C} de la forme $\Omega(\mathbf{Z} \oplus \mathbf{Z}\tau)$ où Ω est un réel positif et τ est un nombre complexe de partie imaginaire > 0 et qui est de la forme $\tau = it$ si $\Delta(E) > 0$ et $\tau = (1/2) + it$ si $\Delta(E) < 0$. Posons $q = e^{2i\pi\tau}$ et $\lambda = \Omega/2i\pi$. Alors (E, ω_E) est isomorphe à $(\mathbf{C}^*/q^{\mathbf{Z}}, \Omega du/u)$ et on a :

$$c_4(E) = \lambda^{-4}E_4(\tau), \quad c_6(E) = -\lambda^{-6}E_6(\tau) \quad \text{et} \quad \|\omega_E\|^2 = 8\pi^2|\lambda|^2\Im \tau.$$

D'où :

$$\|\omega_E\|^2 H(E) = 8\pi^2 \psi(\tau) \quad \text{où} \quad \psi(\tau) = \Im m(\tau) \sup \left(|E_4(\tau)|^{1/2}, |E_6(\tau)|^{1/3} \right)$$

est la fonction définie au lemme 4. Cette fonction est invariante par $SL_2(\mathbf{Z})$ car les fonctions E_4 et E_6 sont des formes modulaires de poids respectifs 4 et 6. Et puisque la courbe E est définie sur \mathbf{Q} alors pour minorer $\psi(\tau)$ il suffit de faire varier τ sur le bord du demi-domaine fondamental $P = \{\tau \in \mathbf{C} / 0 \leq \Re(\tau) \leq \frac{1}{2} \text{ et } |\tau| \geq 1\}$. Et par le lemme précédent on sait alors que $\psi(\tau) > 1$. D'où le résultat.

6. La constante de Manin

Soit E une courbe elliptique définie sur \mathbf{Q} . Notons N son conducteur. On dit que E est une courbe de *Weil forte* s'il existe $\varphi : X_0(N) \rightarrow E$ un morphisme non constant défini sur \mathbf{Q} et qui ne se factorise pas par une isogénie $E' \rightarrow E$ de courbes elliptiques de degré > 1 . Un tel morphisme φ est appelé une *paramétrisation de Weil forte* de E . On sait que toute courbe de *Weil* (c.f. §1) est \mathbf{Q} -isogène à une unique courbe de *Weil forte*.

Soit E une courbe de *Weil forte* de conducteur N . Rappelons que la constante de Manin c_E relative à E est définie par la relation

$$\varphi^*(\omega_E) = c_E 2\pi i f_E(\tau) d\tau$$

où ω_E est une forme différentielle de Néron sur E et f_E est la newform de poids 2 et de niveau N associée à E (cf. §1). Quitte à changer ω_E en son opposé, on peut supposer que $c_E > 0$. On conjecture que la constante c_E est toujours égale à 1. Dans cette direction, on a les résultats suivants (cf. [10]) :

- a) la constante c_E est un entier naturel ;
- b) si p est un nombre premier impair et p^2 ne divise pas N alors p ne divise pas c_E ;
- c) si 4 ne divise pas N alors 4 ne divise pas c_E . Si de plus a_2 (le deuxième coefficient de Fourier de f_E) est pair alors 2 ne divise pas c_E ;
- d) si N est sans facteur carré on déduit de (b) et (c)

$$(10) \quad c_E = 1 \quad \text{ou} \quad 2.$$

Récemment, Edixhoven a démontré (mais pas encore publié) que pour un conducteur N quelconque, tous les nombres premiers > 7 ne divisent

pas c_E . En suivant la même méthode on doit pouvoir majorer les exposants en 5 et 7 de c_E . Mais pour les exposants en 2 et 3, on ne sait rien à l'heure actuelle.

7. Les résultats

Rappelons les données et notations des paragraphes précédents. On considère une courbe elliptique E définie sur \mathbf{Q} . On note N son conducteur, $\Delta(E)$ son discriminant minimal, $c_4(E)$, $c_6(E)$ les invariants habituels associés à E et enfin $L(E, s)$ sa série de Dirichlet. On suppose que E est une courbe de Weil et qu'elle vérifie comme au §1. (a) l'hypothèse :

(S) *le signe de l'équation fonctionnelle de sa série $L(E, s)$ est -1 .*

Rappelons aussi que c_E désigne la constante de Manin relative à E (cf. §6) et que le conducteur N et le discriminant $\Delta(E)$ sont divisibles par les mêmes nombres premiers. Écrivons alors

$$\Delta(E) = \pm \prod_{p|N} p^{d_p},$$

et posons :

$$d_E = \text{ppcm}(d_p) \quad \text{et} \quad H(E) = \sup(|c_4(E)|^{1/2}, |c_6(E)|^{1/3})$$

$$N' = \prod_{\substack{p \text{ premier} \\ p \geq 3, p|N}} p \quad \text{et} \quad S(N) = \prod_{\substack{p \text{ premier} \\ p \geq 3, p|N}} \left(1 + \frac{1}{p}\right).$$

Le théorème suivant traite le cas général d'une courbe elliptique de Weil.

THÉORÈME 1. *Soit E une courbe elliptique de Weil de conducteur N et vérifiant l'hypothèse (S). Alors on a $L'(E, 1) = 0$ ou bien*

$$|L'(E, 1)| > \left(10^9 N^3 N'^2 S(N)^{3/2} H(E) c_E^2 d_E^2\right)^{-1} \log |\Delta(E)|.$$

Démonstration. L'hypothèse (S) veut dire que $L(E, 1)$ est nul. Si $L'(E, 1)$ est non nul alors en utilisant la formule (2) et les inégalités (6), (7), (8) et (9) on a le théorème : remarquons ici que l'entier M_E intervenant dans (6) est un diviseur de $12 d_E$ et que le nombre u intervenant dans la formule (2) est égal à 1 dès que $|D| > 4$.

Les deux théorèmes qui suivent traitent successivement le cas d'une courbe elliptique de Weil semi-stable (i.e. de conducteur sans facteur carré) et le cas d'une courbe elliptique de conducteur premier.

THÉORÈME 2. *Soit E une courbe elliptique de Weil vérifiant l'hypothèse (S). Supposons que son conducteur N est sans facteur carré. Alors on a $L'(E, 1) = 0$ ou bien*

$$|L'(E, 1)| > \left(10^7 N^5 S(N)^{3/2} H(E) d_E^2 \right)^{-1} \log |\Delta(E)|.$$

Démonstration. Comme N est sans facteur carré la constante M_E intervenant dans (6) est alors égale à d_E et la constante de Manin relative à E est égale à 1 ou 2 d'après (10). Enfin, l'entier N' est égal à N ou $N/2$ suivant que N est impair ou pair.

THÉORÈME 3. *Soit E une courbe elliptique de Weil vérifiant l'hypothèse (S). Supposons que son conducteur est un nombre premier p . Alors on a $L'(E, 1) = 0$ ou bien*

$$|L'(E, 1)| > \left(10^7 p^5 \left(1 + \frac{1}{p} \right)^{3/2} H(E) \right)^{-1} \log p.$$

Démonstration. Si $L'(E, 1)$ est non nul alors d'après ([2], th.1.3, p. 236) la courbe E est de rang 1. Et d'après Oesterlé et Mestre ([11], th.2, p.183) on a $\Delta(E) = \pm p$. Par suite on a $d_E = 1$ et le théorème.

BIBLIOGRAPHIE

- [1] A. O. L Atkin et J. Lehner, *Hecke operators on $\Gamma_0(M)$* , Math. Ann. **185** (1970), 134–160.
- [2] B. H. Gross, *Kolyvagin's work on modular elliptic curves*, in: L- functions and Arithmetic London Math. Soc. Lectures Notes series, **153** (1991), 235–256.
- [3] B. H. Gross et D. B. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84**, Fasc. 2 (1986), 225–320.
- [4] M. Hindry et J. H. Silverman, *The canonical height and integral points on elliptic curves*, Invent. Math. (1987).
- [5] M. Krir, *Contributions à l'étude des courbes elliptiques et modulaires*, thèse, Université Paris VI, Octobre (1992).
- [6] M. Krir, *Une version effective d'un théorème de Waldspurger*, C. R. Acad. Sci. Paris **316**, série I (1993).
- [7] Yu. I. Manin, *Cyclotomic fields and modular curves*, Russian Math. Surveys **26** (1978), 7–78.
- [8] D. Masser, *Elliptic functions and transcendence*, Springer Lectures Notes **437** (1975).

- [9] B. Mazur, *Courbes elliptiques et symboles modulaires*, Séminaire Bourbaki exposé 414, Lectures Notes in Math. **317** (1973).
- [10] J. Oesterlé et J.-F. Mestre, *Courbes elliptiques supersingulières et courbes modulaires*, à paraître.
- [11] J. Oesterlé et J.-F. Mestre, *Courbes de Weil semi-stables de discriminant une puissance m -ième*, J. reine angew. Math. **400** (1989), 173–184.
- [12] T. Shintani, *On construction of holomorphic cusp form of half integral weight*, Nogoya Math. J. **58** (1975), 83–126.
- [13] J. H. Silverman, *Lower bound for the canonical height on elliptic curves*, Ducke Math. J. **48** (1981), 633–648.
- [14] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Math. **106** (1986), Springer-Verlag, New-York.
- [15] J. Tate, *The Arithmetic of Elliptic Curves*, Inv. Math. **23** (1974), 179–206.
- [16] J. L. Waldspurger, *Sur les coefficients de Fourier des formes modulaires de poids demi-entiers*, J. Math. Pures et Appliquées **60**, Fasc. 4 (1981), 375–484.

Mohamed KRIR
 URA 763 du CNRS
 Université Paris VI
 UFR 920, Tour 45-46, 5e étage
 4, place Jussieu
 75252 Paris Cedex 05