C. R. Acad. Sc. Paris, t. 297 (19 septembre 1983) Série I — 85

THÉORIE DES NOMBRES. — *Points de Heegner et dérivées de fonctions* L. Note (*) de **Benedict Gross** et **Don Zagier**, présentée par Jean-Pierre Serre.

Nous donnons une identité qui relie la hauteur canonique d'un point de Heegner d'une courbe modulaire à la valeur en $s=1$ de la dérivée d'une certaine fonction L. Ce résultat est en rapport avec la conjecture de Birch et Swinnerton-Dyer. Combiné à un théorème de Goldfeld, il fournit une borne inférieure effective pour le nombre de classes d'un corps quadratique imaginaire.

*NUMBER THEORY.* — Heegner Points and Derivatives of L-Functions.

*We give an identity relating the canonical heights of Heegner points on modular curves to the first derivatives at $s=1$ of* L*-series of modular forms, and we discuss connections with the conjecture of Birch and Swinnerton-Dyer. Together with a result of Goldfeld, this yields an effective lower bound for the class numbers of imaginary quadratic fields.*

Soit N un entier $\geqq 1$. La courbe modulaire $X_0(N)$, définie sur $\mathbf{Q}$, classifie les couples $(E \xrightarrow{\alpha} E')$ de courbes elliptiques généralisées liées par une isogénie cyclique $\alpha$ de degré N. D'après Birch [1], un *point de Heegner* $x \in X_0(N)$ correspond à un couple où End(E) et End(E') sont isomorphes au même ordre O d'un corps quadratique imaginaire K. Nous nous bornerons ici au cas où O est l'ordre maximal de K, et où le discriminant D de K est premier à N. Les points de Heegner sont alors de la forme $(\mathbf{C}/\mathfrak{a} \xrightarrow{\mathrm{id}} \mathbf{C}/\mathfrak{a}\mathfrak{n}^{-1})$, où $\mathfrak{a}$ et $\mathfrak{n}$ sont des idéaux de O avec $O/\mathfrak{n} \simeq \mathbf{Z}/N\mathbf{Z}$; un tel point ne dépend que de K, de $\mathfrak{n}$, et de l'image $\{\mathfrak{a}\}$ de $\mathfrak{a}$ dans le groupe $Cl_K$ des classes d'idéaux de K.

Du point de vue analytique, un point de Heegner $x$ correspond à un point $z$ du demi-plan de Poincaré, défini mod $\Gamma_0(N)$, et satisfaisant à une équation quadratique $az^2+bz+c=0$, de discriminant D, avec $a \equiv 0 \pmod{N}$. La classe de la forme $[a, b, c]$ détermine $\{\mathfrak{a}\}$, tandis que $\mathfrak{n}$ est déterminé par $b \pmod{2N}$. On sait que $x$ est rationnel sur $H=K(j(O))$, qui est le corps de classes de Hilbert de K. Le groupe de Galois G de H/K s'identifie à $Cl_K$ et permute de façon simplement transitive les points de Heegner avec $\mathfrak{n}$ donné; les différents choix de $\mathfrak{n}$ sont permutés par les involutions d'Atkin-Lehner de $X_0(N)$.

On a sur $X_0(N)$ la pointe rationnelle $\infty$. Le diviseur $y=(x)-(\infty)$, ainsi que les diviseurs $T_m y^\sigma (m \geqq 1, \sigma \in G)$, sont rationnels sur H [$T_m = m$-ième opérateur de Hecke, considéré comme endomorphisme de la jacobienne $J_0(N)$ de $X_0(N)$]. On peut donc former la série :

$$F_\sigma(z)=\sum_{m \geqq 1} \langle y, T_m y^\sigma \rangle e^{2\pi imz} \qquad (\mathrm{Im}(z)>0),$$

où $\langle \ , \ \rangle$ est la forme hermitienne sur $\mathbf{C} \otimes J_0(N)(H)$ qui prolonge la hauteur globale de Néron-Tate sur $J_0(N)(H)$. La fonction $F_\sigma$ est une forme parabolique de poids 2 sur $\Gamma_0(N)$; elle ne dépend que de N, D et $\sigma$ (et non des choix de $\{\mathfrak{a}\}$ et de $\mathfrak{n}$). D'autre part, pour toute forme parabolique $f=\sum a_n q^n$ appartenant à l'espace engendré par les formes primitives (newforms) de poids 2 et de niveau N, on peut former la série de Dirichlet :

$$L_\sigma(f, s)=L(\varepsilon, 2s-1) \sum_{n \geqq 1} a_n b_n n^{-s},$$

où $b_n$ est le nombre des idéaux de O de norme $n$ dans la classe correspondant à $\sigma$, et $L(\varepsilon, s)$ est la série L du caractère $\varepsilon$ correspondant à $K/\mathbf{Q}$. Cette série converge pour $\mathrm{Re}(s)>3/2$. Notre résultat principal est alors le suivant :

THÉORÈME 1. — *La fonction* $L_\sigma(f, s)$ *se prolonge en une fonction entière s'annulant en* $s=1$, *et sa dérivée en ce point est :*

$$L'_\sigma(f, 1)=\frac{16\pi^2 h}{u^2 |D|^{1/2}} (f, F_\sigma),$$

*où $2u$ et $h$ sont le nombre d'unités et le nombre de classes de* O, *et* ( , ) *est le produit scalaire de Petersson.*

Pour démontrer ce résultat, on utilise la méthode de Rankin-Selberg pour représenter $L_\sigma(f, s)$ comme produit scalaire $(f, E_s \cdot \theta)$, où $E_s$ est une série d'Eisenstein non holomorphe de poids 1 et de caractère $\varepsilon$, et $\theta$ est la série thêta de poids 1 associée à $\sigma$. A l'aide de cette représentation, et d'un opérateur de projection convenable, on obtient :

$$L'_\sigma(f, 1) = 16\pi^2 u^{-2} |D|^{-1/2} (f, \Phi),$$

où $\Phi = \sum c_m q^m$ est une forme parabolique holomorphe de poids 2 et de niveau N avec des coefficients $c_m$ explicites. Il suffit alors de prouver que $c_m = h \langle y, T_m y^\sigma \rangle$ pour $(m, N) = 1$, ce qui se fait en calculant les hauteurs locales (à la Néron) des points de Heegner.

Supposons maintenant que $f$ soit une forme primitive normalisée $(a_1 = 1)$, et soit $\chi$ un caractère de G. On a alors une série de Dirichlet avec produit eulérien :

$$L(f, \chi, s) = \sum_{\sigma \in G} \chi(\sigma) L_\sigma(f, s),$$

correspondant au produit tensoriel des représentations $l$-adiques de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ associées à $f$ et à Ind $\chi$. Le théorème 1 entraîne :

THÉORÈME 2. — *La fonction* $L(f, \chi, s)$ *s'annule en* $s = 1$, *et l'on a* :

$$L'(f, \chi, 1) = \frac{16\pi^2 (f, f)}{u^2 |D|^{1/2}} \langle v_{f,\chi}, v_{f,\chi} \rangle,$$

*où* $v_{f,\chi}$ *est la composante de* $\sum_{\sigma \in G} \chi^{-1}(\sigma) \otimes y^\sigma$ *dans le sous-espace propre de* $\mathbf{C} \otimes J_0(N)(H)$ *correspondant à* $f$.

Comme $\langle\ ,\ \rangle$ est positif non dégénéré, on en déduit :

COROLLAIRE 1. — $L'(f, \chi, 1) \geqq 0$.

Ceci serait une conséquence immédiate de l'hypothèse de Riemann pour $L(f, \chi, s)$.

COROLLAIRE 2. — $\mathrm{ord}_{s=1} L(f, \chi, s) > 1 \Leftrightarrow \mathrm{ord}_{s=1} L(f^\alpha, \chi^\alpha, s) > 1$ *pour tout* $\alpha \in \mathrm{Aut}(\mathbf{C})$.

En effet, $L'(f, \chi, 1) = 0 \Leftrightarrow v_{f,\chi} = 0 \Leftrightarrow v_{f^\alpha, \chi^\alpha} = 0 \Leftrightarrow L'(f^\alpha, \chi^\alpha, 1) = 0$.

Ce résultat est en accord avec la conjecture de Deligne-Gross [2] selon laquelle l'ordre d'une fonction L motivique de poids impair au point de symétrie de son équation fonctionnelle est indépendant du plongement complexe de ses coefficients.

Pour $\chi = 1$, on a $L(f, \chi, s) = L(f, s) L(f \otimes \varepsilon, s)$, et l'on obtient :

COROLLAIRE 3. — $\mathrm{ord}_{s=1}(L(f, s) L(f \otimes \varepsilon, s)) = 1 \Rightarrow \mathrm{rg} A_f(K) \geqq \dim A_f$, *où* $A_f$ *est le quotient de* $J_0(N)$ *correspondant à* $f$.

Supposons en outre que $f | W_N = f$. L'ordre de $L(f, s)$ en $s = 1$ est alors impair, et celui de $L(f \otimes \varepsilon, s)$ est pair. D'après un théorème de Waldspurger ([5], *voir* aussi [4]) on peut choisir K tel que $L(f^\alpha \otimes \varepsilon^\alpha, 1) \neq 0$ pour tout $\alpha \in \mathrm{Aut}(\mathbf{C})$. Les corollaires 2 et 3 donnent alors :

COROLLAIRE 4. — $\mathrm{ord}_{s=1} L(f, s) > 1 \Rightarrow \mathrm{ord}_{s=1} L(f^\alpha, s) > 1$ *pour tout* $\alpha \in \mathrm{Aut}(\mathbf{C})$.

COROLLAIRE 5. — $\mathrm{ord}_{s=1} L(f, s) = 1 \Rightarrow \mathrm{rg} A_f(\mathbf{Q}) \geqq \dim A_f$.

La conjecture de Birch et Swinnerton-Dyer donnerait les corollaires 3 et 5 avec égalité de dimensions. Inversement, si l'on suppose l'égalité des dimensions en question et la finitude du groupe de Tate-Šafarevič, le théorème 2 implique la forme précise de ladite conjecture, à un facteur rationnel non nul près.

COROLLAIRE 6. — *Soit f l'unique forme primitive de niveau* 37 *et de poids* 2 *telle que* $f \mid W_{37} = -f$, *et soit g la forme tordue de f par le caractère* $\left(\frac{\cdot}{139}\right)$. *Alors* $L(g, s)$ *a un zéro d'ordre* 3 *en* $s=1$.

*Démonstration.* — La fonction modulaire $u(z)=\eta(z)^2/\eta(37z)^2=q^{-3}+\ldots$ donne une application $u: X_0(37) \to \mathbf{P}^1$, définie sur $\mathbf{Q}$, de diviseur $3(0)-3(\infty)$. Le discriminant $D=-139$ a les propriétés suivantes :

(i) 37 est norme d'un élément $\lambda$ de l'ordre O de discriminant D;

(ii) D n'est divisible ni par 2 ni par 3;

(iii) $h(D)=3$.

Si $x \in X_0(37)$ est le point de Heegner correspondant à $\mathfrak{a}=O$ et $\mathfrak{n}=(\bar{\lambda})$, on a $u(x) \in H^*$ et $u(x)^{12}=\Delta(O)/\Delta(\lambda O)=\lambda^{12}$; d'après (ii), H n'a pas d'autres racines de l'unité que $\pm 1$; on a donc $u(x)=\pm\lambda \in K^*$, d'où $u(x^\sigma)=u(x)$ pour tout $\sigma \in G$. La propriété (iii) implique maintenant que le diviseur de la fonction $u-u(x)$ est $\sum_{\sigma \in G}(x^\sigma)-3(\infty)$, donc $y_1=0$ dans $J_0(37)(K)$. D'après le théorème 2 (et l'équation fonctionnelle), on a $\mathrm{ord}_{s=1} L(f, 1, s) \geqq 3$. Un calcul numérique donne $L(f, 1) \neq 0$ et $L'''(g, 1) \neq 0$, d'où l'énoncé puisque $L(f, 1, s)=L(f, s)\,L(g, s)$.

*Remarque.* — Ce corollaire est lui aussi en accord avec la conjecture de Birch et Swinnerton-Dyer, car $L(g, s)$ est la fonction L d'une courbe elliptique de rang 3 sur $\mathbf{Q}$ (donnée par l'équation $-139y^2=x^3+10x^2-20x+8$). Le conducteur de cette courbe est égal à $37 \cdot 139^2=714\,877$; on connaît d'autres courbes de rang 3 sur $\mathbf{Q}$ ayant un conducteur plus petit (e. g. 5 077), mais nous n'avons pas vérifié que ce sont des courbes de Weil.

Le corollaire 6, combiné avec les résultats de Goldfeld [3], mène à une *borne inférieure effective* pour les nombres de classes des corps quadratiques imaginaires :

THÉORÈME 3. — *Pour tout nombre réel* $\delta>0$, *il existe une constante effectivement calculable* $c_\delta>0$ *telle que :*

$$h_F > c_\delta (\log |d_F|)^{1-\delta}$$

*pour tout corps quadratique imaginaire* F.

(Ici, $h_F$ et $d_F$ désignent respectivement le nombre de classes, et le discriminant, du corps F.)

*Démonstration.* — Soit $\varepsilon$ le caractère quadratique associé à l'extension $F/\mathbf{Q}$, et soit $g$ la forme modulaire du corollaire 6. La série L tordue $L(g \otimes \varepsilon, s)$ satisfait à une équation fonctionnelle avec signe $+1$ si $\varepsilon(37)=1$ et signe $-1$ si $\varepsilon(37)=0$ ou $-1$. Dans le premier cas, on a $4 \cdot 37^{h_F}=a^2+b^2 |d_F|$ avec $b \neq 0$, d'où $h_F>\log(|d_F|/4)/\log 37$. Dans le deuxième cas, on a $\mathrm{ord}_{s=1}(L(g, s)\,L(g \otimes \varepsilon, s)) \geqq 4$, et le théorème de Goldfeld donne le résultat voulu.

(*) Reçue le 18 juillet 1983, acceptée le 19 septembre 1983.

[1] B. J. BIRCH, *Heegner Points of Elliptic Curves* (*Symp. Math.*, Ist. d. Alta Mat., 15, 1975, p. 441-445).

[2] P. DELIGNE, *Valeurs de fonctions* L *et périodes d'intégrales*, (*Symp. Pure Math.*, *A.M.S.*, 33, II, 1979, p. 313-346).

[3] D. M. GOLDFELD, *The Conjectures of Birch and Swinnerton-Dyer and the Class Numbers of Quadratic Fields* (S.M.F., *Astérisque*, 41-42, 1977, p. 219-227).

[4] M.-F. VIGNÉRAS, *Valeur au centre de symétrie des fonctions* L *associées aux formes modulaires* (*Sém. D.P.P.*, 1979-1980, Birkhäuser, 1981, p. 331-356).

[5] J.-L. WALDSPURGER, *Correspondance de Shimura et Quaternions* (à paraître).

*Dept. of Math., Brown University, Providence, RI* 02912, *U.S.A.;*
*Dept. of Math., Univ. of Maryland, College Park, MD* 20742, *U.S.A.*
et *Max-Planck-Institut, Gottfried-Claren-Str.* 26, 5300 *Bonn, R.F.A.*