Astérisque

JOHN COATES

The work of Gross and Zagier on Heegner points and the derivatives of *L*-series

Astérisque, tome 133-134 (1986), Séminaire Bourbaki,
exp. n° 635, p. 57-72

<http://www.numdam.org/item?id=SB_1984-1985__27__57_0>

Séminaire BOURBAKI
37e année, 1984-85, n° 635 Novembre 1984

THE WORK OF GROSS AND ZAGIER ON HEEGNER POINTS AND THE DERIVATIVES OF L-SERIES

By John COATES

1 - Introduction.

The problem of determining the group of rational points on an elliptic curve defined over $\mathbb{Q}$ is one of the oldest and most intractable in mathematics. It remains unsolved today, even though a vast variety of numerical examples have been successfully computed in the literature. The most difficult part of the problem is that of constructing rational points, when numerical or theoretical evidence suggests that such points should exist. A typical case, which goes back to the Greeks and the Arabs, is the question of deciding whether a given positive integer B is the area of a right-angled triangle with rational sides. It can easily be shown that the answer is affirmative if and only if the elliptic curve

$$y^2 = x^3 - B^2x \tag{1}$$

has a rational point of infinite order (or equivalently a rational point (x,y) with $y \neq 0$). There is overwhelming evidence that (1) always admits a rational point of infinite order when B is a positive integer which is congruent to 5, 6, or 7 mod 8. Indeed it is well known that the conjecture of Birch and Swinnerton-Dyer predicts that the rank of the group of rational points on (1) is odd if and only if B is congruent to 5, 6 or 7 mod 8. An answer to even this special problem about the construction of rational points seems beyond the present resources of mathematics.

It has been known since the 19-th century that one can construct solutions of Pell's equation, using either the values of circular functions or the values of Dedekind's η-function. The great credit for the first successful attempt to use the values of elliptic modular functions to construct rational points on elliptic curves is due to Heegner [11], who, in the same paper, applied similar ideas to give the first effective determination of all imaginary quadratic fields with class number 1. After a period of obscurity and neglect, Heegner's ideas were taken up and extended by Birch [1], [2], [3]. The importance of these papers of Heegner and Birch is that they establish, for the first time, the existence of rational points

of infinite order on certain elliptic curves over $\mathbb{Q}$, without actually writing down the coordinates of these points and naively verifying that they satisfy the equation of the curve. We call these rational points provided by the Heegner-Birch construction *Heegner points* on the elliptic curve (the precise definition will be given later). However, it was already clear in this initial work that these Heegner points were not always of infinite order. In an effort to clarify this difficulty, Birch and Stephens made extensive numerical calculations (which were published only partially and after a long delay in [4]), and were led to the following two striking conjectures :

(i) the Heegner points on an elliptic curve over $\mathbb{Q}$ are of infinite order if and only if the group of rational points on the curve has rank equal to 1;

(ii) if the Hasse-Weil L-series of the elliptic curve vanishes at $s = 1$, there is a closed formula for the value at $s = 1$ of its first derivative as a product of a standard non-zero period term and the canonical Néron-Tate height of its Heegner points.

2 - Statement of results.

We now describe the work of Gross and Zagier [8], [9], which goes a long way towards proving the conjectures of Brich and Stephens, and in some sense goes further. In fact, both the construction of Heegner points and the main result of Gross and Zagier are really statements about modular forms (consequently, the applications only concern those elliptic curves over $\mathbb{Q}$, which occur as isogeny factors in the Jacobian variety of the modular curve $X_0(N)$). From now on, N will denote an integer > 1, and we recall that $X_0(N)$ is the curve over $\mathbb{Q}$ which parametrizes equivalence classes of pairs $(E_1 \xrightarrow{\alpha} E_2)$ of generalized elliptic curves, which are linked by an isogeny α, whose kernel is cyclic of order N. Following Birch [3], we define a Heegner point on $X_0(N)$ to be a pair $(E_1 \xrightarrow{\alpha} E_2)$, where the endomorphism ring of both E_1 and E_2 is isomorphic to the same order $\mathcal{O}$ in an imaginary quadratic field K. To guarantee the existence of a plentiful supply of Heegner points on $X_0(N)$, we can vary both the imaginary quadratic field K and the order $\mathcal{O}$ of K. However, for simplicity, we shall only consider in this report those Heegner points which satisfy the following hypothesis :

Hypothesis A. (i) *$\mathcal{O}$ is the maximal order of K;*
(ii) *the discriminant D of K is prime to N;*
(iii) *every prime factor of N splits in K.*

Condition (iii) implies that there exist 2^r integral ideals $\mathfrak{n}$ of K such that $\mathcal{O}/\mathfrak{n}$ is a cyclic abelian group of order N; here r denotes the number of distinct prime factors of N. It is then easy to see that the Heegner points of $X_0(N)$ are those of the form $(\mathbb{C}/\mathfrak{a} \xrightarrow{\mathrm{id}} \mathbb{C}/\mathfrak{a}\mathfrak{n}^{-1})$, where $\mathfrak{n}$ is an integral ideal with $\mathcal{O}/\mathfrak{n} \xrightarrow{\sim} \mathbb{Z}/N\mathbb{Z}$, and $\mathfrak{a}$ is an arbitrary integral ideal of K. In fact, such a point depends only on K, $\mathfrak{n}$, and the image of $\mathfrak{a}$ in the ideal class group of K. The Heegner points of $X_0(N)$ are rational over the field $H = K(j(\mathcal{O}))$, where j is the classical j-invariant of a lattice in the complex plane. By the theory of complex multiplication, H is the Hilbert class field of K (= the maximal unramified abelian extension of K), and the Artin map defines an isomorphism from the ideal class group Cl_K of K onto the Galois group G of H over K. The action of G on Heegner points can be made quite explicit; in particular, G permutes simply and transitively those Heegner points attached to a fixed $\mathfrak{n}$ with $\mathcal{O}/\mathfrak{n} \xrightarrow{\sim} \mathbb{Z}/N\mathbb{Z}$.

The principal result of Gross and Zagier gives a closed formula for the value at $s = 1$ of the first derivative of an L-series formed from the Rankin product of two modular forms. We take the first modular form $f = \sum_{n=1}^{\infty} a_n q^n$ $(q = e^{2\pi i z})$ to be any element of the vector space generated over $\mathbb{C}$ by the primitive cusp forms (i.e. newforms in the sense of [16]) of weight 2 for the subgroup $\Gamma_0(N)$ of $SL_2(\mathbb{Z})$ (recall that $\Gamma_0(N)$ consists of all matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with $c \equiv 0 \bmod N$). The second modular form is the following θ-series, which is attached to the imaginary quadratic field K and an arbitrary element σ of the Galois group G of H over K. Let $C(\sigma)$ denote the ideal class of K which corresponds to σ under the Artin isomorphism. Pick an integral ideal $\mathfrak{a}$ in $C(\sigma)$, and a $\mathbb{Z}$-basis β_1, β_2 of $\mathfrak{a}$. Then the quadratic form

$$Q_\sigma(x,y) = \frac{N(x\beta_1 + y\beta_2)}{N\mathfrak{a}}$$

has integral coefficients and discriminant D (= the discriminant of K), and its equivalence class under the action of $SL_2(\mathbb{Z})$ depends only on σ. Let w be the number of roots of unity in K, and ε the Dirichlet character modulo D of the quadratic extension $K/\mathbb{Q}$. Hecke [10] showed that the θ-series

$$\theta_\sigma(z) = \frac{1}{w} \sum_{(m,n) \in \mathbb{Z}^2} q^{Q_\sigma(m,n)}$$

is a modular form of weight 1 and character ε for $\Gamma_0(D)$, i.e. it is holomorphic at all points of the compactified upper half plane, and satisfies

(2) $$\theta_\sigma(\gamma z) = \varepsilon(d)(cz+d)\theta_\sigma(z)$$

for all $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $\Gamma_0(D)$. For each integer $n \geq 1$, write $r_\sigma(n)$ for the number of integral ideals in the class $c(\sigma)$ with norm equal to n, and let $r_\sigma(0) = w^{-1}$. Since $r_\sigma(n) = r_{\sigma^{-1}}(n)$ (because complex conjugation maps an ideal class to its inverse), we have $\theta_\sigma(z) = \sum_{n=1}^{\infty} r_\sigma(n) q^n$. The partial L-series studied by Gross and Zagier is defined in the half plane $R(s) > \frac{3}{2}$ by

(3) $$L_\sigma(f,s) = L_N(\varepsilon, 2s-1) \sum_{N=1}^{\infty} a_n r_\sigma(n) n^{-s},$$

where $L_N(\varepsilon,s)$ is the Dirichlet L-series of ε, with the Euler factors at the primes dividing N removed from its Euler product. As we shall explain later, Rankin's method shows that $L_\sigma(f,s)$ has a holomorphic continuation over the whole complex plane, and that it vanishes at $s = 1$. The novelty of Gross and Zagier's work is their proof of a remarkable closed formula for the first derivative at $s = 1$ of $L_\sigma(f,s)$ in terms of Heegner points attached to K on $X_0(N)$. The Heegner points intervene in this formula via their canonical heights, a fundamental arithmetic notion due to Néron and Tate, which we do our best to recall briefly. Assuming that N is such that $X_0(N)$ has genus $g \geq 1$, let J be the abelian variety defined over $\mathbb{Q}$ which is the Jacobian of $X_0(N)$, i.e. the group $J(\bar{\mathbb{Q}})$ of $\bar{\mathbb{Q}}$-rational points on J can be identified with the group of $\mathbb{Q}$-rational divisors on $X_0(N)$ of degree 0 modulo linear equivalence. We can construct an embedding

(4) $$\phi : J/\pm 1 \longrightarrow \mathbb{P}^{2^g-1}$$

defined over $\mathbb{Q}$ into projective space of dimension 2^g-1 as follows. Recall that a theta characteristic $\mathcal{O}$ on $X_0(N)$ is a divisor class of degree $g-1$ over $\bar{\mathbb{Q}}$ such that $2\mathcal{O}$ is the canonical class on $X_0(N)$. Let W denote the image of the $(g-1)$-th symmetric power of $X_0(N)$ in the group of divisor classes of $X_0(N)$ of degree $g-1$. Then $\Theta = W - \mathcal{O}$ is an ample and symmetric divisor on J, and the class of the divisor 2Θ in the Picard group of J is independent of the choice of $\mathcal{O}$ and is defined over $\mathbb{Q}$. The linear space $H^0(J, 2\Theta)$ has dimension $\ell = 2^g$, and gives rise to the embedding (4) on choosing a basis $x_1, \ldots, x_\ell$ of this space. For each finite extension F of $\mathbb{Q}$, let M_F denote the set all places v of F, normalized so that the restriction of $||_v$ to $\mathbb{Q}$ is the n_v-th power of the corresponding valuation of $\mathbb{Q}$, where n_v is the local degree of v. The canonical height of a point $P \in J(F)$ is then defined by the limit

$$\hat{h}_F(P) = \lim_{n\to\infty} \frac{1}{n^2} \sum_{v\in M_F} \max_{1\le i\le \ell} \{\log |x_i(nP)|_v\}.$$

It can be shown that this limit exists, and defines a positive definite quadratic form $\hat{h}_F : J(F) \otimes \mathbb{R} \longrightarrow \mathbb{R}$. Let $<,>_F : J(F) \times J(F) \longrightarrow \mathbb{R}$ be the symmetric bilinear form attached to $\hat{h}_F$, i.e.

$$<P,Q>_F = \frac{1}{2} (\hat{h}_F(P+Q) - \hat{h}_F(P) - \hat{h}_F(Q)).$$

The existence of the bilinear form $<,>_F$ enables us to construct cusp forms of weight 2 for $\Gamma_0(N)$ via the following elementary lemma. For each integer $m \ge 1$, write T_m for the m-th Hecke correspondence of $X_0(N)$, which is defined by the formula

$$T_m(x) = \sum_C (x_C),$$

where $x = (E_1 \xrightarrow{\alpha} E_2)$, where the sum on the right is taken over all subgroups C of order m in E_1 which are disjoint form $\ker \alpha$, and where $x_C = (E_1/C \xrightarrow{\alpha} E_2/\alpha(C))$. This correspondence induces a $\mathbb{Q}$-endomorphism of J, which we also denote by T_m. Let $\mathbb{T}$ denote the commutative $\mathbb{Q}$-subalgebra of $\mathrm{End}_{\mathbb{Q}}(J_0(N)) \otimes \mathbb{Q}$, which is generated by the T_m for all $m \ge 1$.

Lemma 1. *Given any $\mathbb{Q}$-linear map $\phi : \mathbb{T} \longrightarrow \mathbb{C}$, there is a cusp form g_ϕ of weight 2 for $\Gamma_0(N)$ whose Fourier expansion is given by $g_\phi = \sum_{m=1}^{\infty} \phi(T_m) q^m$. Moreover, for each $t \in \mathbb{T}$, we have*

$$t(g_\phi) = \sum_{m=1}^{\infty} \phi(tT_m)\, q^m. \tag{5}$$

The proof will be postponed to paragraph 3. Let ∞ denote the rational point on $X_0(N)$ given by the cusp at infinity (recall that, classically, one identifies the complex points of $X_0(N)$ with the quotient of the compactified upper half plane by $\Gamma_0(N)$). Write x for a Heegner point attached to K on $X_0(N)$, and ξ for the point in J(H) given by the divisor class of $(x) - (\infty)$. For each $\sigma \in G$, Lemma 1 shows that

$$R_\sigma(z) = \sum_{m=1}^{\infty} <\xi, T_m \xi^\sigma>_H q^m$$

is a cusp form of weight 2 for $\Gamma_0(N)$. It is not difficult to show that, up to the addition of an old form of weight 2 on $\Gamma_0(N)$, $R_\sigma(z)$ depends only on N, D and σ, and not on the choice of the particular Heegner point x. We normalize the Peterson inner product for $\Gamma_0(N)$ via

$$(g_1, g_2)_N = \int_{\Gamma_0(N)\backslash \mathcal{H}} g_1(z)\ \overline{g_2(z)}\ dx\, dy,$$

the integral being taken over a fundamental domain for the action of $\Gamma_0(N)$ on the upper half plane $\mathcal{H}$. We can at last state the principal result of Gross and Zagier.

Theorem 2. *Let* f *be any element of the* $\mathbb{C}$*-vector space generated by the primitive cusp forms of weight* 2 *for* $\Gamma_0(N)$. *For each* $\sigma \in G$, *we have*

$$\frac{d}{ds} L_\sigma(f, s)\Big|_{s=1} = \frac{8\pi^2}{u^2 |D|^{1/2}} (f, R_\sigma)_N,$$

where $2u$ *denotes the number of roots of unity in* K.

Gross and Zagier's proof of Theorem 1 is a long, difficult, and almost miraculous calculation, much of it in the spirit of the best 19-th century mathematics. In the latter part of this report, we shall only have time to sketch some of the main ideas underlying this calculation.

While Theorem 2 is of the utmost technical importance for the proof, its arithmetic significance lies in a number of remarkable corollaries, which involve L-functions with Euler products. Let

$$V = J(H) \otimes \mathbb{C},$$

which is finite dimensional over $\mathbb{C}$ by the Mordell-Weil theorem. The canonical height pairing gives rise to a Hermitian inner product on V, which is defined by

$$\langle P \otimes a, Q \otimes b \rangle_H = a\bar{b} \langle P, Q \rangle_H \qquad (a, b \in \mathbb{C}).$$

Moreover, V is endowed with a natural action of both the Galois group G and the Hecke algebra $\mathbb{T}$. Write $\hat{G}$ (resp. $\hat{\mathbb{T}}$) for the group of all complex characters of G (resp. $\mathbb{T}$). The action of $\mathbb{T}$ is self-adjoint with respect to the above inner product, and commutes with the action of G. Hence we have the corresponding decompositions

$$V = \bigoplus_{\chi \in \hat{G}} V^{\chi}, \qquad V^{\chi} = \bigoplus_{\rho \in \hat{\mathbb{T}}} V^{\chi,\rho}$$

into isotypical components. An important subset of $\hat{\mathbb{T}}$ is given by the primitive normalized cusp forms of weight 2 for $\Gamma_0(N)$ (i.e. newforms of weight 2 for $\Gamma_0(N)$. whose first Fourier coefficient is equal to 1). If $f = \sum_{n=1}^{\infty} a_n q^n$ is such a form, the corresponding character of $\mathbb{T}$ sends T_m to a_m for all $m \geq 1$. Suppose for the rest of this section that f is such a primitive normalized cusp form of weight 2 for $\Gamma_0(N)$. For each $\chi \in \hat{G}$, we put

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

This L-series always admits an Euler product (the Euler product attached to the tensor product of the two ℓ-adic representations of the Galois group of $\overline{\mathbb{Q}}$ over $\mathbb{Q}$ associated with f and with the induced representation of χ). Moreover, it is well known (see [6]) that we have the functional equation

$$\Lambda(f,\chi,s) = -\Lambda(f,\chi,2-s),$$

where $\Lambda(f,\chi,s) = (ND)^{s} (2\pi)^{-2s} \Gamma(s)^2 L(f,\chi,s)$. In particular, $L(f,\chi,s)$ has a zero of odd multiplicity at $s = 1$. Recall that x denotes a Heegner point on $X_0(N)$, and ξ the point in $J(H)$ given by the divisor class of $(x) - (\infty)$. Put

$$\xi_{\chi} = \sum_{\sigma \in G} \chi^{-1}(\sigma) \xi^{\sigma},$$

so that $\xi_{\chi} \in V^{\chi}$.

Theorem 3. *Let f be a primitive normalized cusp form of weight 2 for $\Gamma_0(N)$. Then*

$$\frac{d}{ds} L(f,\chi,s)\Big|_{s=1} = \frac{8\pi^2 (f,f)_N}{u^2 h |D|^{1/2}} \langle \xi_{f,\chi}, \xi_{f,\chi} \rangle_H,$$

where $\xi_{f,\chi}$ is the projection of ξ_{χ} to the f-isotypical component of $V = J(H) \otimes \mathbb{C}$, and where h denotes the class number of K.

We note that $8\pi^2 (f,f)_N$ is equal to the period integral

$$\|\omega_f\| = \iint_{X_0(N)(\mathbb{C})} \omega_f \wedge \overline{i\omega_f}, \quad \text{where } \omega_f = 2\pi i f(z) dz.$$

Put $R = h \sum_{\sigma \in G} \chi(\sigma) R_{\sigma}$. To derive Theorem 3 from Theorem 2, we must show that $(f,R)_N = (f,f)_N \langle \xi_{f,\chi}, \xi_{f,\chi} \rangle_H$. This is a purely formal calculation using Lemma 1 and the Galois invariance of the height pairing. We omit the details.

While Theorem 3 can be applied quite generally to the simple $\mathbb{Q}$-isogeny fac-

tors of J attached to an arbitrary primitive cusp form, its most striking application is to elliptic curves over $\mathbb{Q}$ which occur in this manner. Let E be an elliptic curve defined over $\mathbb{Q}$, and, for each prime p (of good or bad reduction), let N_p denote the number of points on the reduction $\tilde{E}$ of E modulo p which are rational over $\mathbb{Z}/p\mathbb{Z}$. Put

$$a_p = 1 + p - N_p.$$

Recall that the Hasse-Weil L-series of E over $\mathbb{Q}$ is defined by the Euler product

$$L(E,s) = \prod_{p|N} (1 - a_p p^{-s})^{-1} \prod_{(p,N)=1} (1 - a_p p^{-s} + p^{1-2s})^{-1},$$

where N denotes the conductor of E (see [13]). Write $L(E,s) = \sum_{n=1}^{\infty} a_n n^{-s}$. We shall say that E is a *modular* elliptic curve over $\mathbb{Q}$ if $f(z) = \sum_{n=1}^{\infty} a_n q^n$ is a primitive cusp form of weight 2 for $\Gamma_0(N)$. If E is modular, then the function

$$\Lambda(E,s) = (2\pi)^{-s} \Gamma(s) L(E,s) = \int_0^{\infty} f(iy) y^s \frac{dy}{y}$$

is entire, and satisfies the functional equation

$$\Lambda(E,s) = w_E N^{1-s} \Lambda(E,2-s), \quad w_E = \pm 1. \tag{6}$$

It is a major open question as to which elliptic curves over $\mathbb{Q}$ are modular. Weil and Taniyama have conjectured that *every* elliptic curve over $\mathbb{Q}$ is modular, and this has now been verified numerically for some small values of the conductor $N \leq 500$. In theory it is always possible to decide in a finite number of steps whether a given elliptic curve is modular, but in practice this becomes very difficult once the conductor is at all large. The only general class of elliptic curves over $\mathbb{Q}$ which are known to be modular are those with complex multiplication (e.g. the curve (1) for all $B \in \mathbb{Q}^{\times}$). We now give the most important consequences of Theorem 3 for modular elliptic curves over $\mathbb{Q}$. If E is such a curve, we write $E(K)$ for the group of K-rational points on E, and $L(E/K,s)$ for the Hasse-Weil L-series of E over K.

Theorem 4. *Let E be a modular elliptic curve over $\mathbb{Q}$ of conductor N. Let K be an imaginary quadratic field of discriminant D such that $(D,N) = 1$ and each prime factor of N splits in K. Then $L(E/K,s)$ vanishes at $s = 1$, and, if this zero is simple, $E(K)$ contains a point of infinite order.*

To deduce Theorem 4 from Theorem 3, let $L(E,s) = \sum_{n=1}^{\infty} a_n n^{-s}$, so that

$f(z) = \sum_{n=1}^{\infty} a_n q^n$ is a primitive cusp form of weight 2 for $\Gamma_0(N)$. Take χ to be the trivial character χ_0 of the Galois group G. Let $L(E^{(\varepsilon)},s) = \sum_{n=1}^{\infty} a_n \varepsilon(n) n^{-s}$, where ε denotes the character of $K/\mathbb{Q}$. Then

$$L(E/K,s) = L(E,s)\, L(E^{(\varepsilon)},s) = L(f,\chi_0,s). \tag{7}$$

Hence, if $L(E/K,s)$ has a simple zero at $s = 1$, Theorem 2 shows that ξ_{f,χ_0} is non-zero in $J(K) \otimes \mathbb{C}$, whence, on picking a non-zero homomorphism from J to E, it follows that the image of ξ_{f,χ_0} in $E(K) \otimes \mathbb{C}$ is not zero, as required.

If E is an elliptic curve over $\mathbb{Q}$, we write

$$\langle , \rangle_{E,\mathbb{Q}} : E(\mathbb{Q}) \times E(\mathbb{Q}) \longrightarrow \mathbb{R}$$

for the canonical height pairing on E (the definition is entirely analogous to that for J, the analogue of the embedding (4) being given by the x-coordinate on a Weierstrass equation for E over $\mathbb{Q}$).

Theorem 5. *Let E be a modular elliptic curve over $\mathbb{Q}$ such that $L(E,s)$ vanishes at $s = 1$. Then there exists a rational point P in $E(\mathbb{Q})$ such that*

$$\frac{d}{ds} L(E,s)\Big|_{s=1} = \alpha \Omega_E \langle P,P \rangle_{E,\mathbb{Q}} , \tag{8}$$

where α denotes a non-zero rational number, and Ω_E denotes the real period of a non-zero differential of the first kind on E over $\mathbb{Q}$. In particular, if $L(E,s)$ has a simple zero at $s = 1$, then $E(\mathbb{Q})$ contains a point of infinite order.

To derive (8) from Theorem 3, we first note that a deep theorem of Waldspurger [14] proves the existence of (infinitely many) K satisfying the conditions of Theorem 4 and such that $L(E^{(\varepsilon)},1) \neq 0$. Since we can clearly suppose that $L(E,s)$ has a simple zero at $s = 1$ (otherwise take $P = 0$ in (8)), it follows that, for such a choice of K, $L(f,\chi_0,s)$ has a simple zero at $s = 1$, where χ_0 denotes the trivial character of the ideal class group of K. Hence Theorem 3 shows that ξ_{f,χ_0} is non-zero in $J(K) \otimes \mathbb{C}$. On the other hand, ξ_{f,χ_0} actually lies in $J(\mathbb{Q}) \otimes \mathbb{C}$. This follows easily from the fact that $f|_2 w_N = f$, where $w_N(z) = -1/(Nz)$, which in turn follows from the fact that $L(E,s)$ has a simple zero at $s = 1$. The equation (8) is now established by choosing a non-zero homomorphism from J to E and applying the functorial properties of heights, as well as the known algebraicity properties of $L(E^{(\varepsilon)},1)$.

Needless to say, (8) is in accord with the algebraicity properties predicted by the conjecture of Birch an Swinnerton-Dyer. However, the real importance of Theorem 5 is that it provides the first major step towards the affirmative solution of

the problem of constructing rational points on elliptic curves over $\mathbb{Q}$. Even in the function field analogue, a result of this kind was not known previously. It should also be stressed that Theorem 5 is very useful numerically, since $L'(E,1)$, when it is non-zero, can easily be calculated using a standard rapidly convergent series.

On the other hand, the limitations of Theorem 5 are also plain. When $L(E,s)$ has a zero at $s = 1$ of multiplicity > 1, Theorem 5 provides no information about the existence of rational points of infinite order on E. Even when $L(E,s)$ has a simple zero at $s = 1$, it still has not been proven that the rank of $E(\mathbb{Q})$ is equal to 1. Finally, it is not always easy to prove theoretically that $L(E,s)$ has a simple zero at $s = 1$, when this is predicted by the standard conjectures. For example, for each prime $p \equiv 5 \bmod 8$, the standard conjectures predict that the L-series of the curve

$$y^2 = x^3 + px \tag{9}$$

should have a zero at $s = 1$ of multiplicity exactly 1. It would be interesting to prove this, since it is not always easy to find a rational point of infinite order on this curve by elementary descent theory. When $p = 877$, it is shown in [5] that a generator modulo torsion of the group of rational points on (9) has x-coordinate

$$x = \frac{3754945281271621931055040699420927923462 01}{62159877768715054254632207806972380441 00},$$

which gives some idea of the limitations of using naive calculations to find rational points of infinite order.

Theorem 6. *There exist modular elliptic curves* E *over* $\mathbb{Q}$ *such that* $L(E,s)$ *has a zero at* $s = 1$ *of multiplicity* 3.

Let E be a modular elliptic curve over $\mathbb{Q}$ such that the sign in the functional equation of $L(E,s)$ is equal to -1. If the point P constructed in Theorem 5 is zero in $E(\mathbb{Q}) \otimes \mathbb{Q}$, it follows that $L(E,s)$ has a zero at $s = 1$ of multiplicity ≥ 3. In fact, Gross and Zagier prove that P is zero for the curve

$$-139y^2 = x^3 + 10x^2 - 20x + 8,$$

which, as we would expect, is known to have rank 3. Goldfeld's work (which has been so beautifully simplified by Oesterlé in his Bourbaki report of last June) shows that Theorem 6 enables us to solve the major classical problem of effectively determining all imaginary quadratic fields with given class number.

3 - An indication of the proof of Theorem 2.

We first say a word about the proof of Lemma 1. Let S be the vector space over $\mathbb{Q}$ of cusp forms of weight 2 on $\Gamma_0(N)$ with rational Fourier coefficients. The algebra $\mathbb{T}$ acts faithfully on S, because S can be identified with the cotangent space to the origin of the Jacobian $J/\mathbb{Q}$. The assertion of Lemma 1 is an almost immediate consequence of the following fact. The pairing $\mathbb{T} \times S \longrightarrow \mathbb{Q}$ which associates to each pair (t,g) the first Fourier coefficient of $t(g)$ is a perfect pairing of $\mathbb{Q}$-vector spaces (use the definition of the pairing and the fact that the action of $\mathbb{T}$ on S is faithful).

Two basic ideas underly the proof of Theorem 2, namely Néron's [12] decomposition of the global height of J/H as a sum of local components, and Rankin's method for analytically continuing the function $L_\sigma(f,s)$. The proof is very indirect, and can be fairly described as showing that Theorem 2 is true because no other alternative is possible. Indeed, after two beautiful and ingenious computations, one of an arithmetic nature involving local height calculations on $X_0(N)$, and the other of an analytic nature involving Rankin's method, Gross and Zagier succeed in proving that both terms appearing in Theorem 2 reduce to the same explicit, complicated, and mysterious expression. We only have space to indicate a few of the salient features of these remarkable calculations, without going into any detail. To simplify the formulae, we assume henceforth

Hypothesis. $D = -p$ *where* $p > 3$ *is a prime with* $p \equiv 3 \bmod 4$.

Néron's theory (see also [7]) proves the existence, for each place v of H, of a unique local symbol $\langle \mathfrak{a},\mathfrak{b} \rangle_v$ with values in $\mathbb{R}$, which is defined on pairs of relatively prime divisors $\mathfrak{a},\mathfrak{b}$ of degree 0 of $X_0(N)$ over the completion of H at v. This symbol is characterized by being bi-additive, symmetric, continuous, and given by

$$\langle \mathfrak{a},\mathfrak{b} \rangle_v = \sum_p m_p \log |g(P)|_v ,$$

whenever $\mathfrak{a} = \sum_p m_p(P)$, and $\mathfrak{b}$ is the divisor of a function g. In [7], it is explained how to extend the definition of this local symbol to a pair $\mathfrak{a},\mathfrak{b}$ of divisors of degree 0 which are not relatively prime, and, at least in theory, how to compute this local symbol. The connexion between the local symbols and the global height pairing is simply

$$\langle \alpha,\beta \rangle_H = \sum_{v \in M_H} \langle \mathfrak{a},\mathfrak{b} \rangle_v , \tag{10}$$

where $\mathfrak{a},\mathfrak{b}$ are arbitrary divisors of degree 0 on $X_0(N)$ over H, and α,β are

the points in $J(H)$ given by their corresponding divisor classes. Now take x to be a Heegner point on $X_0(N)$ attached to K, and let $\mathfrak{a} = (x)-(\infty)$, $\mathfrak{h} = (x)-(0)$. Since the class of $(0)-(\infty)$ is known to have finite order in $J(H)$, it follows that, for all integers $m \geq 1$,

$$\langle \xi, T_m \xi \rangle_H = \sum_{v \in M_H} \langle \mathfrak{a}, T_m \mathfrak{h}^\sigma \rangle_v ,$$

where, as before, ξ denotes the class of $\mathfrak{a}$ in $J(H)$. Unfortuneately, we do not have space to go into the highly interesting calculation of the local symbols $\langle \mathfrak{a}, T_m \mathfrak{h}^\sigma \rangle_v$ which is carried out in [9] (we only note that the divisors $\mathfrak{a}$ and $T_m \mathfrak{h}^\sigma$ are relatively prime if and only if $r_\sigma(m) = 0$). The final result is as follows. Recall (see [15], Chapter 15) that the Legendre function of the second kind

$$Q_s(z) = \frac{1}{2^{s+1}} \int_{-1}^{1} (1-t^2)^n (z-t)^{-s-1} dt \quad (R(s) > -1)$$

satisfies the differential equation

$$(1-z^2)y'' - 2zy' + s(s+1)y = 0 .$$

Put

$$\eta_N = \frac{12}{N \prod_{q|N} (1+q^{-1})} , \quad \gamma_N = \sum_{q|N} \frac{\log q}{q^2-1} ,$$

where q runs over the prime factors of N. Put

$$A_\varepsilon = \frac{L'(\varepsilon,1)}{L(\varepsilon,1)} , \quad B = C + \log \pi,$$

where C denotes Euler's constant. Write $\delta(m)$ for the function whose value is 1 or 2, according as p does not or does divide m. Let $\rho(m)$ denote the sum $\rho(m) = \sum_{c|m} c$. Finally, $\zeta(s)$ denotes the Riemann zeta function.

Theorem 7. *For each integer $m \geq 1$, the value of the height pairing $\langle \xi, T_m \xi^\sigma \rangle_H$ is given by*

$$\begin{aligned}
(11) \qquad & 2h\, r_\sigma(m) \left\{A_\varepsilon - B + \frac{1}{2} \log \left(\frac{Np}{m}\right)\right\} \\
& - \sum_{n=1}^{\frac{mp}{N}} \delta(n) \Big(\sum_{d|n} \varepsilon(d) \log \left(\frac{n}{d}\right)^2 \Big) r_\sigma(mp-nN) \\
& + \lim_{s \to 1} \left\{ \frac{h\rho(m)\eta_N}{s-1} - 2 \sum_{n=1}^{\infty} \delta(n) \Big(\sum_{d|n} \varepsilon(d) \Big) r_\sigma(mp+nN) Q_{s-1}\left(1 + \frac{2nN}{mp}\right) \right\} \\
& + 2h\rho(m)\eta_N \left\{ A_\varepsilon - \frac{\zeta'(2)}{\zeta(2)} - 1 - \gamma_N + \frac{1}{2} \log \left(\frac{mp}{N}\right) \right\} - 2h\eta_N \sum_{d|m} \frac{m}{d} \log d.
\end{aligned}$$

We now sketch the analytic arguments used to calculate $L'_\sigma(f,1)$ via Rankin's method. The Eisentein series

$$G_\varepsilon(z,s) = \sum_{\substack{(m,n)\in\mathbb{Z}^2 \\ (m,n)\neq(0,0)}} \frac{\varepsilon(n)y^s}{(mpz+n)\,|mpz+n|^{2s}} \qquad (z = x+iy)$$

has a holomorphic continuation as a function of s over the whole complex plane, and, as a function of z, $G_\varepsilon(z,s)$ is a non-holomorphic modular form of weight 1 and character ε for $\Gamma_0(p)$. Classical arguments yield the following integral representation for

$$\Xi(s) = (4\pi)^{-s}\,\Gamma(s)\,L_\sigma(f,s)\ .$$

Proposition 8. *Put* $\Phi(z,s) = \theta_\sigma(z)G_\varepsilon(Nz,s)$ *and* $M = Np$. *Then*

$$\Xi(s) = \frac{1}{2}\,(f,\Phi(z,\bar{s}-1))_M = \frac{1}{2}\int_{\Gamma_0(M)\backslash H} f(z)\overline{\Phi(z,\bar{s}-1)}\,dx\,dy\ .$$

Recall that, for each (possibly non-holomorphic) modular form g of weight 2 for $\Gamma_0(M)$, the trace of g to $\Gamma_0(N)$ is defined by

$$\mathrm{Tr}(g) = \sum_{\alpha\in W} g|_2\alpha\ ,$$

where W denotes a set of representatives of the right cosets of $\Gamma_0(M)$ in $\Gamma_0(N)$. Supposing henceforth that s is real, we put

$$\Omega(z,s) = \mathrm{Tr}\,(\Phi(z,s-1))\ , \tag{12}$$

whence it is clear from Proposition 8 that

$$\Xi(s) = \frac{1}{2}\,(f,\Omega(z,s))_N.$$

Since $L_\sigma(f,s)$ vanishes at $s=1$, we conclude that

$$L'_\sigma(f,1) = 2\pi(f,\psi(z))_N, \quad \text{where} \quad \psi(z) = \frac{\partial}{\partial s}\,\Omega(z,s)\,|_{s=1}\ . \tag{13}$$

Although it is technically quite difficult, one can explicitly calculate the Fourier series of $\psi(z)$. Define

$$Y(u) = \int_1^\infty e^{-ux}x^{-1}dx\ .$$

Proposition 9. *We have* $\psi(z) = \sum_{m\in\mathbb{Z}} b_m(y)q^m$, *where*

$$b_m(y) = h r_\sigma(m)\,(\log(Npy) + 2A_\varepsilon - C)$$
$$- \sum_{n=1}^{\frac{mp}{N}} r_\sigma(mp-nN)\,\delta(n)\,\Big(\sum_{d|n} \varepsilon(d) \log\big(\frac{n}{d^2}\big)\Big)$$
$$- \sum_{n=1}^{\infty} r_\sigma(mp+nN)\,\delta(n)\,Y\big(\frac{4\pi nNy}{p}\big)\,\Big(\sum_{d|n} \varepsilon(d)\Big).$$

Let $\mathfrak{M}$ (resp. S) denote the space of non-holomorphic modular forms (resp. holomorphic cusp forms) of weight 2 for $\Gamma_0(N)$. Recall that the holomorphic projection operator is the unique linear map $\Pi : \mathfrak{M} \longrightarrow S$ satisfying

$$(w,g)_N = (w,\Pi(g))_N \quad \text{for all} \quad w \in S .$$

In order to give an analytic formula for the effect of Π on the Fourier coefficients of a modular form, we are obliged to introduce the subset $\mathfrak{N}$ of $\mathfrak{M}$ consisting of all $g \in \mathfrak{M}$ such that, for each $\gamma \in SL_2(\mathbb{Z})$, there exists $\varepsilon > 0$ such that

$$(g|_2\gamma)(z) = O(y^{-\varepsilon}) \quad \text{for} \quad z \longrightarrow i\infty . \tag{14}$$

Lemma 10. *Assume that* $g = \sum_{m\in\mathbb{Z}} c_m(y) q^m$ *belongs to* $\mathfrak{N}$. *Then* $\Pi(g) = \sum_{m=1}^{\infty} c_m q^m$, *where*

$$c_m = 4\pi m \times \lim_{s\to 0} \int_0^\infty e^{-4\pi m y} y^s c_m(y)\, dy .$$

A new major technical difficulty arises because the form $\psi(z)$ in $\mathfrak{M}$ does not belong to $\mathfrak{N}$. The ingenious argument used to overcome this difficulty is as follows. For each positive divisor e of N, let

$$E_e(z,s) = \Sigma'' \frac{y^s}{(cz+d)^2|cz+d|^{2s}} ,$$

where Σ'' denotes summation over all pairs of integers (c,d) modulo ± 1, satisfying $(c,d) = 1$, $e|c$, and $(c/e, N/e) = 1$. This Eisenstein series can be continued over the whole s-plane, and we define

$$E_e(z) = E_e(z,0), \quad F_e(z) = \frac{\partial}{\partial s} E_e(z,s)\Big|_{s=0} .$$

Proposition 11. *Let*

$$\phi(z) = \psi(z) - \frac{4\pi h}{\sqrt{p}} \sum_{e|N} \frac{e}{N} \{F_e(z) + (\log(\tfrac{pe^2}{N}) + 2A_\varepsilon - B) E_e(z)\} .$$

Then $\phi \in \mathfrak{N}$ *and* $\Pi(\phi) = \Pi(\psi)$.

In view of (13), and the fact that f belongs to the space generated by the primitive forms of weight 2 for $\Gamma_0(N)$, the proof of Theorem 2 is now completed by the

following (again technically difficult) calculation of the Fourier coefficients of $\Pi(\phi)$.

Proposition 12. *Assume that* $\Pi(\phi) = \sum_{m=1}^{\infty} c_m q^m$. *Then, for each integer* $m \geq 1$ *with* $(m,N) = 1$, *we have that* $\frac{\sqrt{p}}{4\pi} c_m$ *is given by the expression* (11) *of Theorem* 7.

Acknowledgement. I am grateful to B. Gross, D. Zagier, and P. Colmez for their help in the preparation of this report.

BIBLIOGRAPHIE

[1] B. Birch.- Diophantine analysis and modular functions, Proceedings of Bombay Colloquium on Algebraic Geometry (1968), 35-42.

[2] B. Birch.- Elliptic curves and modular functions, Symposia Mathematica (1970), 27-32.

[3] B. Birch.- Heegner points of elliptic curves, Symposia Mathematica (1975), 441-445.

[4] B. Birch and N. Stephens.- Heegner's construction of points on the curve $y^2 = x^3 - 1728e^3$, Progress in Mathematics Vol. 38 (1983), 1-19.

[5] J. Cassels and A. Bremmer.- On the equation $y^2 = x(x^2+p)$, Math. of Computation Vol. 42 (1984), 257-264.

[6] B. Gross.- Heegner points on $X_0(N)$, to appear in Proceedings of the Durham Conference on Modular Forms (1983).

[7] B. Gross.- Local Heights on Curves, to appear in Proceedings of the Storrs Conference on Algebraic Geometry (1984).

[8] B. Gross and D. Zagier.- Points de Heegner et dérivées de fonctions L, CRAS 297 (1983), 85-87.

[9] B. Gross and D. Zagier.- Heegner points and derivatives of L-series, to appear in Invent. Math.

[10] E. Hecke.- Zur Theorie der elliptischen Modulfunktionen, Math. Werke, 428-460.

[11] K. Heegner.- Diophantische Analysis und Modulfunktionen, Math. Zeitschrift 56 (1952), 227-253.

[12] A. Néron.- Quasi-fonctions et hauteurs sur les variétés abéliennes, Ann. of Math. 82 (1965), 249-331.

[13] J. Tate.- The arithmetic of elliptic curves, Invent. Math. 23 (1974), 179-206.

[14] J.-L. Waldspurger.- Correspondance de Shimura et Quaternions, to appear.

[15] Whittaker and Watson.- *Modern Analysis*, Cambridge University Press (4th edition) (1952).

[16] A. Atkin and J. Lehner.- Hecke operators on $\Gamma_0(m)$, Math. Ann. Vol. 185 (1970), 134-160.

John COATES
Mathématiques, Bât. 425
Université de Paris-Sud
F-91405 ORSAY