DETERMINATION OF MODULAR ELLIPTIC CURVES BY HEEGNER POINTS

WENZHI LUO AND DINAKAR RAMAKRISHNAN

To the memory of Olga Taussky-Todd

1. Introduction

For every integer $N \geq 1$, consider the set $\mathcal{K}(N)$ of imaginary quadratic fields such that, for each K in $\mathcal{K}(N)$, its discriminant D is an odd, square-free integer congruent to 1 modulo 4, which is prime to N and a square modulo $4N$. For each K, let $c = ([x] - [\infty])$ be the divisor class of a Heegner point x of discriminant D on the modular curve $X = X_0(N)$ as in [GZ]. (Concretely, such an x is the image of a point z in the upper half plane $\mathcal{H}$ such that both z and Nz are roots of integral, definite, binary quadratic forms of the *same* discriminant D ([B]).) Then c defines a point rational over the Hilbert class field H of K on the Jacobian $J = J_0(N)$ of X. Denote by c_K the trace of c to K.

Let f be a normalized newform of level N, weight 2 and trivial character. It is given by a Fourier expansion $\sum_{n\geq 1} a_n e^{2\pi i n z}$, $z \in \mathcal{H}$, with $a_1 = 1$. The form $2\pi i f(z)dz$ defines a differential of the first kind on the compactification of the Riemann surface $\Gamma_0(N)\backslash\mathcal{H}$, in fact a class ω_f, rational over the field $\mathbb{Q}(f)$ of coefficients, on X. There is an abelian variety factor J_f over $\mathbb{Q}$ of the Jacobian J whose cotangent space over $\mathbb{C}$ is spanned by the $[\mathbb{Q}(f) : \mathbb{Q}]$ conjugates, under $\mathrm{Aut}(\mathbb{C})$, of ω_f. For every Heegner point x coming from K, let $c_{f,K}$ denote the component of c_K in $J_f(K) \otimes \mathbb{Q} \subset J(K) \otimes \mathbb{Q}$; this is denoted by $c_{f,1}$ in [GZ], where 1 signifies the trivial character of the class group of K.

An elliptic curve E over $\mathbb{Q}$ is said to be modular if, for a newform f of weight 2 (necessarily with $\mathbb{Q}$-coefficients), E is isogenous to J_f; equivalently, by the Eichler-Shimura congruence relations and Faltings's isogeny theorem, $L(s, E) = L(s, f)$. (Modularity is known to be true for a large class of $E/\mathbb{Q}$ by the recent deep works of Wiles, Taylor-Wiles and Diamond.) When E is modular, the conductor of E agrees, by the work of Carayol ([C]), with the level N of f. In their fundamental paper, Gross and Zagier gave a formula (cf. [GZ], chap. I, section 6), for each Heegner point x, expressing the derivative at $s = 1$ of the L-function over K of such a modular elliptic curve E in terms of the canonical height $\hat{h}(c_{f,K})$ of $c_{f,K}$ over K. Our main result here is the following

Theorem A *Let E, E' be modular elliptic curves over $\mathbb{Q}$ of conductors N, M, with asssociated newforms f, g of weight 2, such that, for a non-zero scalar C, we have*

$$\hat{h}(c_{f,K}) = C\hat{h}(c_{g,K}),$$

for all Heegner divisors c_K coming from imaginary quadratic fields K in $\mathcal{K}(N) \cap \mathcal{K}(M)$. Suppose that some $c_{f,K}$ is non-zero in $J(K) \otimes \mathbb{Q}$. Then $N = M$ and E is isogenous to E' over $\mathbb{Q}$.

One can show by using [GZ] that some $c_{f,K}$ is non-zero in $J(K)\otimes\mathbb{Q}$ iff the order of zero of $L(s,E)$ at $s=1$ is ≤ 1.

The proof will be given in the next section. It uses a variant of the method of [LR], and this Note could be viewed as an addendum to [LR]. It relies, in addition to [GZ], on the important work of H. Iwaniec ([Iw]) on the quadratic twists of derivatives of modular L-series. The subject matter of ([Iw]) concerned the average values of such twists, leading to a non-vanishing result, established earlier and independently by Bump-Friedberg-Hoffstein ([BFH]) and Murty-Murty ([MM]), needed to complement Kolyvagin's work ([Ko]) on modular elliptic curves.

Our proof, which uses properties of *twisted* averages of modular L-series and their derivatives (see Theorem C), will also work for forms f with $\mathbb{Q}(f)$ different from $\mathbb{Q}$, determining the abelian variety J_f up to isogeny. The method works for forms f of higher (even) weight as well. To elaborate, Shouwu Zhang has recently proved a higher analog of the formula of Gross and Zagier (see Corollary 0.3.2 of [Z]), and applying our argument below to this situation, one gets a variant of Theorem A determining (the motive of) f by the heights of the f-components of (homologically trivial) Heegner cycles, assuming one of them has a non-trivial height.

Now let N be an odd (rational) prime, and $\mathcal{K}'(N)$ the set of imaginary quadratic fields K of discriminant D which are 1 modulo 4 and satisfy $\left(\frac{D}{N}\right)=-1$. Denote by B the quaternion division algebra over $\mathbb{Q}$ which is ramified only at N and ∞, and fix a maximal order R in B. Let Y be the associated curve of genus zero, whose points in any $\mathbb{Q}$-algebra A are given by $\{\alpha\in B\otimes A-\{0\}\mid \mathrm{tr}(\alpha)=\mathrm{Nrd}(\alpha)=0\}$, where Nrd (resp. tr) denotes the reduced norm (resp. trace). Let X be the algebraic curve defined as the double coset space $(R\otimes\hat{\mathbb{Z}})^*\backslash(B\otimes\mathbb{A}^f)^*\times Y/B^*$, where $\hat{Z}$ denotes the projective limit of $\{\mathbb{Z}/n\mathbb{Z}\}$ and $\mathbb{A}^f=\mathbb{Q}\otimes\hat{Z}$ the finite adeles of $\mathbb{Q}$. In [G], one finds a definition of *special points* x of discriminant D, for each $K\in\mathcal{K}'(N)$. Moreover, one finds there a beautiful formula relating, for each newform f of weight 2, level N and trivial character with base change f_K to $\mathrm{GL}(2)/K$, the *value* $L(1,f_K)$ $(=L(1,f)L(1,f,\chi_D))$ with an analog of the height $\langle x_{f_0,K},x_{f_0,K}\rangle$ (on $\mathrm{Pic}(X)$) of the f_0-component of x. Here f_0 denotes the Hecke eigenform on B^* associated to f by Eichler; see [JL], sec. 16, or [Sh] for a proof. (It should be noted that a generalization of this for N not prime, but still with $\left(\frac{D}{N}\right)=-1$, is sketched in [GZ], chap. V, sec. 3.) Our arguments below work (easily) in this case as well and furnish the following

Theorem B *Let E,E' be modular elliptic curves over $\mathbb{Q}$ with associated newforms f,g of weight 2 and of prime levels N,M. Suppose that for all special points x coming from the imaginary quadratic fields K in $\mathcal{K}'(N)\cap\mathcal{K}'(M)$, we have (for some non-zero scalar C)*

$$\langle x_{f_0,K},x_{f_0,K}\rangle = C\langle x_{g_0,K},x_{g_0,K}\rangle.$$

Suppose that some $\langle x_{f_0,K},x_{f_0,K}\rangle$ is non-zero. Then $N=M$ and E is isogenous to E' over $\mathbb{Q}$.

This Note is dedicated to the memory of Olga Taussky-Todd. Perhaps it is fitting that it concerns heights and special values, as it was while attending the lectures of B. Gross on this topic in Québec in June 1985 that the second author first met Olga. We would like to thank B. Gross and W. Duke for comments on an earlier version of the article. Thanks are also due to different people, Henri Darmon in

particular, for suggesting that a result such as Theorem A above might hold by a variant of [LR]. Both authors would also like to acknowledge the support of the NSF, which made this work possible.

2. The proof

Let E, E', f, g be as in Theorem A. For any imaginary quadratic field K of discriminant D, we have

$$L(s,f)L(s,f,\chi_D) = L(s,E/K) = L(s,E)L(s,E_D), \tag{2.1}$$

where $L(s,f,\chi_D)$ denotes the twisted L-function of f by the quadratic Dirichlet character χ_D associated to $K/\mathbb{Q}$ by class field theory, and E_D denotes the twist of E by D. There is a similar formula involving g and E'.

By hypothesis, there exists an imaginary quadratic field K_0 with discriminant D_0 in $\mathcal{K}(N) \cap \mathcal{K}(M)$ and Hilbert class field H_0 such that the corresponding c_{f,K_0} is non-zero in $J_f(K_0) \otimes \mathbb{Q}$. Then c_{f,K_0} comes from a non-torsion point on $J_f(K_0)$, and hence its canonical height $\hat{h}(c_{f,K_0})$ must be non-zero (see [Si], Thm. 9.3 (d), for example). By Theorem 6.3 of Gross-Zagier [GZ], we have, for any $K \in \mathcal{K}(N)$ of discriminant D and ring of integers $\mathfrak{O}$,

$$L'(1,E/K) = \frac{8\pi^2\,(f,f)}{u^2\sqrt{|D|}}\hat{h}(c_{f,K}), \tag{2.2}$$

where u is the order of $\mathfrak{O}^*/\{\pm 1\}$, and (f,f) the Petersson norm of f.

Applying (2.2) to K_0, we get the non-vanishing of $L'(1,E/K_0)$ as $\hat{h}(c_{f,K_0}) \neq 0$. On the other hand, since $L(s,f,\chi_{D_0})$ is holomorphic at $s=1$, we see by (2.1) that the order of zero at $s=1$ of $L(s,E)$ is at most that of $L(s,E/K_0)$, which is ≤ 1. (The converse is also true, namely that the height of some Heegner point is non-zero if $L(s,E)$ vanishes to order ≤ 1, but we will not need this.) Also, since $\hat{h}(c_{f,K}) = C\hat{h}(c_{g,K})$, with $C \neq 0$, we deduce the analogous fact about $L(s,E')$. To sum, we have

$$\mathrm{ord}_{s=1}L(s,E) \leq 1 \geq \mathrm{ord}_{s=1}L(s,E'). \tag{2.3}$$

Moreover, applying (2.2) for E and E', and using the proportionality of the f- and g-components of the Heegner points, we get

$$L'(1,E/K) = \frac{C\,(f,f)}{(g,g)}L'(1,E'/K), \tag{2.4}$$

for all $K \in \mathcal{K}(N) \cap \mathcal{K}(M)$.

First suppose that $L(s,E)$ and $L(s,E')$ both vanish at $s=1$. Then by (2.1), we have

$$L'(1,E_K) = L'(1,E)L(1,E_D) \quad \text{and} \quad L'(1,E'_K) = L'(1,E')L(1,E'_D). \tag{2.5}$$

Combining (2.4) and (2.5), we then get

$$L(1,f,\chi_D) = C_1 L(1,g,\chi_D), \tag{2.6}$$

with

$$C_1 = \frac{C\,(f,f)\,L'(1,E')}{(g,g)\,L'(1,E)},$$

and this holds for *every* $K = \mathbb{Q}(\sqrt{D})$ in $\mathcal{K}(N) \cap \mathcal{K}(M)$. Applying Theorem B of our earlier paper [LR], one then concludes that $N = M$ and $f = g$. Then E is isogenous to E' over $\mathbb{Q}$, proving Theorem A in this case.

Next suppose that $L(s, E)$ and $L(s, E')$ are both non-zero at $s = 1$. In this case, $L'(1, E/K) = L(1, E)L'(1, E_D)$; similarly for E'. Then (2.4) implies ($\forall K \in \mathcal{K}(N) \cap \mathcal{K}(M)$)

$$L'(1, f, \chi_D) = C_2 L'(1, g, \chi_D), \tag{2.6}$$

with

$$C_2 = \frac{C\,(f, f)\,L(1, E')}{(g, g)\,L(1, E)}.$$

Theorem A is then a consequence of the following result with $k = m = 1$. (Note that $w(f) = 1$ here as $L(1, E) \neq 0$.)

Theorem C *Let f, g be normalized newforms of levels N, M and weights $2k, 2m$ respectively, with trivial character. Let $w(f)$ denote the sign of the functional equation (root number) of f. Suppose there is a constant C' such that*

$$L'(k, f, \chi_D) = C' L'(m, g, \chi_D),$$

for all fundamental discriminants D in the set

$$\mathcal{D} = \{D \mid Dw(f) < 0,\, D \equiv \nu^2 \,(\mathrm{mod}\, 4R),\, \text{for some}\, \nu\, \text{prime to}\, R\},$$

where R is any multiple of NM. Then

$$k = m, \quad N = M, \quad \text{and} \quad f = g.$$

Proof of Theorem C. The argument requires only a small, but straightforward, modification of the proof of Theorem B of [LR]. We will use the same notation as in section 3 of *loc. cit.*, except otherwise indicated. In particular, F will denote a smooth function with compact support in $\mathbb{R}_+^*$ with $B = \int_{\mathbb{R}_+^*} F(t)dt > 0$.

Let ℓ be 1 or a odd prime not dividing R. Our main tool is the twisted sum (for $T > 0$)

$$S_{f,\ell}(T) = \sum L'(k, f, \chi_D) F(\frac{|D|}{T}) \chi_D(\ell), \tag{2.7}$$

where the sum runs over D in $\mathcal{D}$ with $\mu(D) \neq 0$. When $\ell = 1$, this sum was analyzed in [Iw], establishing a strong asymptotic formula in T (compare [MM]). We make use of (only) [Iw], and assume familiarity with its contents.

Arguing as in section 3 of [LR], we deduce that

$$S_{f,\ell}(T) = BC_0 L_{f,\ell}(k) T \log T + \beta_f T + O(T^{\frac{13}{14}+\epsilon}), \tag{2.8}$$

for some constant β_f, with C_0 and $Ł_{f,\ell}(s)$ as in Proposition 3.6 of [LR]. For $\ell = 1$, this is Iwaniec's formula. (It is likely that the error term can be improved by using the recent work of Heath-Brown [H], but this is not necessary for us here.)

In the proof of (2.8), we need only redefine $V(x)$ (compare (3.13) of [LR]) as follows:

$$V(x) = \frac{1}{2\pi i} \int_{\Re(s) = 4/5} \frac{\Gamma(k + s)}{\Gamma(k)} x^{-s} \frac{ds}{s^2}.$$

With this change, the proof of Proposition 3.6 of [LR] goes through verbatim.

We next recall that, when ℓ is prime to N, Lemma 3.7 of [LR] shows that $L_{f,\ell}(k)$ is $L_{1,\ell}(k)$ times a rational function of $\tilde{a}_\ell(f) = a_\ell(f)\ell^{(1-2k)/2}$, which determines the normalized Hecke eigenvalue $\tilde{a}_\ell(f)$. Now applying the hypothesis of Theorem C, we get the equality of $\tilde{a}_\ell(f)$ and $\tilde{a}_\ell(g)$ for almost all primes ℓ. Thus, by the strong multiplicity one theorem, f and g coincide, resulting in the equality of N and M and the $\mathbb{Q}$-isogeny of E and E'.

$\square$

To complete the proof of Theorem A, it remains for us to consider the possibility that the orders of zero at $s = 1$ of $L(s, E)$ and $L(s, E')$ are different. If we are in such a case, we may, after interchanging E and E' if necessary, assume, thanks to (2.3), that

$$\mathrm{ord}_{s=1}L(s, E) = 0 \quad \text{and} \quad \mathrm{ord}_{s=1}L(s, E') = 1.$$

Then $L'(1, E/K) = L(1, E)L'(1, E_D)$, while $L'(1, E'/K) = L'(1, E')L(1, E'_D)$. Applying (2.4), we get $(\forall K \in \mathcal{K}(N) \cap \mathcal{K}(M))$

$$L'(1, f, \chi_D) = C_3 L(1, g, \chi_D), \tag{2.9}$$

with

$$C_3 = \frac{C\,(f, f)\,L'(1, E')}{(g, g)\,L(1, E)}.$$

Sum both sides over discriminants D in $\mathcal{D}$, weighted by $F(\frac{|D|}{T})$. Then the left hand side has the asymptotic given by (2.8) (with $\ell = 1$), hence with leading term a (non-zero) multiple of $T\log T$, while the leading term of the asymptotic of the right hand side is, by Proposition 3.6 of [LR], a multiple of T. This gives a contradiction. Hence the hypotheses of Theorem A prevent $L(s, E)$ and $L(s, E')$ from having different orders of zero at $s = 1$. We note that we are justified in applying the results of [LR] to g as $w(g) = -1$, so that the set $\mathcal{D}^w$ used in *loc. cit.*, (3.2), is the same as $\mathcal{D}$.

This finishes the proof of Theorem A.

The proof of Theorem B is very similar, in fact simpler. Indeed, since by hypothesis, there exists some $K_0 \in \mathcal{K}'(N)$ such that $\langle x_{f_0,K_0}, x_{f_0,K_0}\rangle$ is non-zero, we must have, by Proposition 11.2 of [G], that

$$L(1, E/K_0) = L(1, f)L(1, f, \chi_{D_0}) \neq 0,$$

where D_0 is the discriminant of K_0. Hence $L(1, f)$ is non-zero. (The converse is also true; indeed, if $L(1, f)$ is non-zero, then $w(f)$ must be 1, and by using [W], for example, we can find some $K \in \mathcal{K}_1(N)$ for which $L(1, E/K_0) \neq 0$, and hence, by [G], that $\langle x_{f_0,K}, x_{f_0,K}\rangle$ is non-zero.) Now since $\langle x_{f_0,K}, x_{f_0,K}\rangle$ is a non-zero multiple of $\langle x_{g_0,K}, x_{g_0,K}\rangle$, $L(1, g)$ is also non-zero. Applying Gross's result again, we get

$$L(1, f, \chi_D) = C_4 L(1, g, \chi_D),$$

for a non-zero scalar C_4, for all $K \in \mathcal{K}'(M) \cap \mathcal{K}'(N)$. So Theorem B of [LR] applies, resulting in the equality of N and M and the $\mathbb{Q}$-isogeny of E and E'.

$\square$

3. Questions

In Theorem A, one should probably only need the equality of $\hat{h}(c_{f,K})$ with $C\hat{h}(c_{g,K})$ for a *finite* set of K, depending on C, N, M. It will be interesting to know if it sufices, for $C = 1$, to know this equality for one single K_0 with c_{f,K_0} of infinite order.

It will also be of interest to know if a p-adic analog of Theorem A can be proven, i.e., with $\hat{h}$ replaced by the corresponding p-adic height, for a prime p not dividing N, M. When p is ordinary for E, there isa p-adic analog of the Gross-Zagier formula due to Bernadette Perrin-Riou ([PR]), for all $K \in \mathcal{K}(N)$ in which p splits. We have learnt recently of an assertion of D. Bertrand ([Be], Prop. 1), determining any *CM curve* E (up to isogeny) by the knowledge of the p-adic height of any point of infinite order.

Bibliography

[Be]: D. Bertrand, Relations d'orthogonalité sur les groupes de Mordell-Weil, *Sém. Th. Nombres, Paris 84-85*, Progress in Math. **63** (1986), 33-39.

[B]: B. Birch, Heegner points on elliptic curves, Symposia Mathematica, vol. XV, Academic Press (1975), 441-445.

[BFH]: D. Bump, S.Friedberg and J. Hoffstein, Non-vanishing theorems for $L-$functions of modular forms and their derivatives, Inventiones Mathematicae **102,** (1990) 543-618.

[C]: H. Carayol, Courbes de Shimura, Formes automorphes et Représentations Galoisiennes, Thèse de Doctorat d'Etat, Univ. Paris VII (1984).

[G]: B. Gross, Heights and the special values of L-series, in *Number Theory*, ed. by H. Kisilevsky and J. Labute, CMS Proceedings **7** (1987), 115-187.

[GZ]: B. Gross and D. Zagier, Heegner points and derivatives of L-series, Inventiones Mathematicae **84** (1986), 225-320.

[H]: R. Heath-Brown, A mean value estimate for real character sums, Acta Arithmetica **72** (1995), 235-275.

[IW]: H. Iwaniec, On the order of vanishing of modular L- functions at the critical point, Séminaire de Théorie des Nombres, Bordeaux **2** (1990), 365–376.

[JL]: H. Jacquet and R. P. Langlands, *Automophic Forms on GL*(2), Springer Lecture Notes **114** (1970).

[K]: V. Kolyvagin, Finiteness of $E(\mathbb{Q})$ and Sha$(E, \mathbb{Q})$ for a subclass of Weil curves, Math. USSR Izvestiya **32** (1989), no.3, 523-541 (English translation from Russian).

[LR]: W. Luo and D. Ramakrishnan, Determination of modular forms by twists of critical L-values, Inventiones Mathematicae, to appear (1997).

[MM]: V. K. Murty and M.R. Murty, Mean values of derivatives of modular $L-$series, Annals of Math. **133** (1991), 447-475.

[PR]: B. Perrin-Riou, Points de Heegner et derivées de fonctions L p-adiques, Inventiones Math. **89** (1987), no. 3, 455-510.

[Sh]: H. Shimizu, Zeta functions of quaternion algebras, Ann. Math. **81** (1965), 166-193.

[Si]: J. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Math. **106** (1986), Springer-Verlag, NY.

[W]: J.-L. Waldspurger, Correspondances de Shimura et Shintani, J. Math. Pures Appl. **59** (1980), 1–133.

[Z]: S. Zhang, Heights of Heegner cycles and derivatives of L-series, Inventiones Mathematicae, to appear.

Wenzhi Luo
Department of Mathematics
Princeton University
Princeton, NJ 08544

Dinakar Ramakrishnan
Department of Mathematics
California Institute of Technology
Pasadena, CA 91125