Heegner points, Heegner cycles, and congruences

Henri Darmon

September 9, 2007

Contents

[1]This research was funded in part by an NSERC postdoctoral fellowship.

Abstract

We define certain objects associated to a modular elliptic curve E and a discriminant D satisfying suitable conditions. These objects interpolate special values of the complex L-functions associated to E over the quadratic field $\mathbf{Q}(\sqrt{D})$, in the same way that Bernouilli numbers interpolate special values of Dirichlet L-series. Following an approach of Mazur and Tate [MT], one can make conjectures about congruences satisfied by these objects which are resonant with the usual Birch and Swinnerton-Dyer conjectures. These conjectures exhibit some surprising features not apparent in the classical case.

1 Heegner objects

1.1 Modular elliptic curves

Let E be an elliptic curve defined over $\mathbf{Q}$ by the Weierstrass equation

$$y^2 = 4x^3 - g_2 x - g_3, \quad g_2, g_3 \in \mathbf{Z},$$

and let N denote the arithmetic conductor of E, which can be computed from g_2 and g_3 by Tate's algorithm [Ta]. To simplify the discussion, let us assume that N is odd.

The group $E(\mathbf{C})$ is isomorphic to the complex torus $\mathbf{C}/\Lambda$, where Λ is a free $\mathbf{Z}$-lattice of rank 2. The lattice Λ can be computed explicitely from the coefficients g_2 and g_3, by using the arithmetic-geometric mean. An isomorphism from $\mathbf{C}/\Lambda$ to E is given by

$$z \mapsto (\wp(z), \wp'(z)),$$

where $\wp(z)$ denotes the Weierstrass $\wp$-function.

The set $E_{ns}(\mathbf{F}_p)$ of non-singular points on the reduction of E mod p is a finite abelian group. Let N_p denote its order, and define $a_p = p + \delta_p - N_p$, where $\delta_p = 0$ if E has bad reduction at p, and is equal to 1 otherwise. Extend this to a_n, for any positive integer n, by equating coefficients in the formal series identity:

$$\sum_{n \geq 0} a_n n^{-s} = \prod_p (1 - a_p p^{-s} + \delta_p p^{1-2s})^{-1}.$$

¿From the inequality of Hasse, $|a_p| \leq 2\sqrt{p}$, it follows that the Fourier series

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

converges absolutely for $\mathrm{im}(\tau) > 0$. Hence the differential $\omega_E = 2\pi i f_E(\tau) d\tau$ is a holomorphic differential on the upper half plane $\mathcal{H}$. The group $SL_2(\mathbf{R})$ of matrices of determinant 1 acts (on the left) on $\mathcal{H}$ by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau = \frac{a\tau + b}{c\tau + d}.$$

Taking pullbacks defines a right action of $\mathbf{SL}_2(\mathbf{R})$ on the space of holomorphic functions or differentials on $\mathcal{H}$.

The Atkin-Lehner involution w_N and the Hecke operators T_p act on the space of differentials by

$$T_p g(\tau) d\tau = p g(p\tau) d\tau + 1/p \sum_{k=0}^{p-1} g(\frac{\tau + k}{p}) d\tau,$$

$$w_N g(\tau) d\tau = g(-1/N\tau) d(-1/N\tau).$$

Let $\Gamma_0(N)$ denote the group of matrices in $\mathbf{SL}_2(\mathbf{Z})$ whose lower left entry is divisible by N. The following conjecture is supported by extensive computational and theoretical evidence, and is widely believed to be true:

Conjecture 1.1 (Shimura-Taniyama-Weil) .

1. *The differential ω_E is invariant under the action of $\Gamma_0(N)$, i.e.,*

$$f_E(\frac{a\tau + b}{cN\tau + d}) = (cN\tau + d)^2 f_E(\tau),$$

for all $\begin{pmatrix} a & b \\ cN & d \end{pmatrix}$ of determinant 1 with $a, b, c, d \in \mathbf{Z}$.

2. *The set L of all $\int_z^{\gamma z} \omega_E$, with $\gamma \in \Gamma_0(N)$ and $z \in \mathcal{H}$, is a lattice in $\mathbf{C}$, and there exists an integer λ such that $\lambda L \subset \Lambda$. (Hence the map $\phi : \tau \mapsto \lambda \int_{i\infty}^{\tau} \omega_E$ is a surjective analytic map from $\mathcal{H}/\Gamma_0(N)$ to $\mathbf{C}/\Lambda$.)*

3. *The differential ω_E is an eigenvalue for the Hecke operators T_p and the Atkin-Lehner involution,*

$$T_p\omega_E = a_p\omega_E, \quad (p, N) = 1, \qquad w_N\omega_E = \epsilon\omega_E, \quad \epsilon = \pm 1.$$

We assume that this conjecture is true for E - in theory, it can be checked by a finite amount of computation, cf. [Me]. All of our constructions rely crucially on the truth of the Shimura-Taniyama-Weil conjecture for E.

1.2 Binary quadratic forms

Let $D = D_0 f^2$, where D_0 is a fundamental discriminant and f is a square-free integer prime to D_0, and let $K = \mathbf{Q}(\sqrt{D}) = \mathbf{Q}(\sqrt{D_0})$ be the corresponding quadratic field with ring of integers $\mathcal{O}_K$. Let $\mathcal{O}_f$ be the order in $\mathcal{O}_K$ of conductor f, consisting of all elements in $\mathcal{O}_K$ which are congruent to a rational integer modulo f.

Definition 1.2 *The pair (E, D) satisfies the* Heegner hypothesis *if for all p dividing N, the Kronecker symbol $(\frac{D}{p})$ is equal to 1.*

Assume from now on that (E, D) satisfies the Heegner hypothesis; then there is an integer B_0 such that

$$B_0^2 \equiv D_0 \pmod{4N}.$$

Fix such a B_0 once and for all. The standard shorthand (A, B, C) will be used to denote the binary quadratic form $Ax^2 + Bxy + Cy^2$.

Definition 1.3 *A quadratic form $F = (A, B, C)$ is said to be* Heegner *if N divides the coefficient A, and $B \equiv B_0 f \pmod{2N}$.*

Let $\mathcal{F}$ denote the set of primitive binary quadratic forms of discriminant D, and let $\mathcal{F}_N$ denote the set of primitive binary quadratic forms which are Heegner. The group $\mathbf{SL}_2(\mathbf{Z})$ acts on the right on $\mathcal{F}$ by the rule:

$$F(x, y)\begin{pmatrix} a & b \\ c & d \end{pmatrix} = F(ax + by, cx + dy).$$

Proposition 1.4 .

1. *The set $\mathcal{F}_N$ is stable under the action of $\Gamma_0(N)$.*

2. *The natural map $\mathcal{F}_N/\Gamma_0(N) \longrightarrow \mathcal{F}/\mathbf{SL}_2(\mathbf{Z})$ is an isomorphism.*

To show surjectivity in 2, let F be a form in $\mathcal{F}$, and suppose without loss of generality that $F = (A, B, C)$ with $(C, N) = 1$. (One can bring F to this form by modifying it by an element of $\mathbf{SL}_2(\mathbf{Z})$.) Let t be an integer satisfying the congruence

$$tC \equiv \frac{B_0 f - B}{2} \pmod{N},$$

and let $\gamma = \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix}$. Then $F\gamma$ is an $\mathbf{SL}_2(\mathbf{Z})$-representative of F which belongs to $\mathcal{F}_N$. To show injectivity, one may proceed by a direct argument. This part of the proof breaks down when D is not prime to N. (In our case, $(D, N) = 1$ follows from the Heegner hypothesis.) A more general statement which also covers the cases where D and N are not assumed to be coprime is given in [GKZ], pp. 504-506.

Let $h^+(D)$ denote the number of inequivalent primitive binary quadratic forms of discriminant D. Proposition 1.4 says that the set $\mathcal{F}_N/\Gamma_0(N)$ is finite and has order $h^+(D)$. In addition, $\mathcal{F}_N/\Gamma_0(N)$ inherits a group structure from the Gaussian composition of binary quadratic forms in $\mathcal{F}/\mathbf{SL}_2(\mathbf{Z})$. Let G_D denote the set $\mathcal{F}_N/\Gamma_0(N)$ endowed with this group structure.

Class field theory interprets G_D as the Galois group of an abelian extension of K:

$$G_D = \mathrm{Gal}(K_f/K),$$

where K_f is the ring class field of K associated to the order of conductor f (cf. [Co], pp. 180-182). The following proposition gives the order of G_D in terms of h, the class number of the field K.

Proposition 1.5 .

1. *If $D < 0$, then*

$$h^+(D) = hu^{-1} \prod_{p|f} (p - (\frac{p}{D_0})),$$

where $u = \#\mathcal{O}_K^*/2$.

2. *If $D > 0$, let w be a fundamental unit of K, and let u be the smallest integer such that w^u is congruent to a rational integer modulo f, and w^u is totally positive. Then*

$$h^+(D) = hu^{-1}2\prod_{p|f}(p - (\frac{p}{D_0})).$$

Our program in the next two sections is to associate to each (not necessarily primitive) Heegner form $F = (A, B, C)$ of discriminant D a Heegner object which belongs to a certain $\mathbf{Z}$-module M_D.

The nature of the Heegner construction, and the nature of M_D, depends on whether D is positive or negative; we will treat those two cases separately.

1.3 The case $D < 0$: Heegner points

If $D < 0$, the two roots of the dehomogenized form Ax^2+Bx+C are complex conjugate and distinct, and there is a unique root τ_0 which lies in the upper half plane. Let

$$q_0 = e^{2\pi i\tau_0},$$

and let

$$z_0 = \sum_{n=1}^{\infty} \frac{a_n}{n} q_0^n.$$

Theorem 1.6 *The value of z_0 is independent of the choice of the $\Gamma_0(N)$-representative of F, up to addition of elements of $\Lambda \subset \mathbf{C}$.*

Proof: Since the root of $F\gamma$ in the upper-half plane is $\gamma^{-1}\tau_0$, the value of τ_0 is well defined in $\mathcal{H}/\Gamma_0(N)$. But $z_0 = \phi(\tau_0)$, where ϕ is the map defined in conjecture 1.1. Hence theorem 1.6 follows from conjecture 1.1 which we assumed to be true in our case.

By theorem 1.6, the point $\alpha_F = (x_0, y_0) = (\wp(z_0), \wp'(z_0))$ is a well-defined complex point on E corresponding to $F \in G_D$, and satisfying the Weierstrass equation

$$y_0^2 = 4x_0^3 - g_2x_0 - g_3.$$

Theorem 1.7 *The complex numbers x_0 and y_0 satisfy an algebraic equation of degree $2h^+(D)$ over $\mathbf{Q}$, and can be viewed as elements of the ring class field K_f. Hence α_F belongs to the Mordell-Weil group $E(K_f)$.*

This is a consequence of the theory of complex multiplication. See [Cx], chapter three, or [Sh].

Let $M_D = E(K_f)$. It is a finitely generated $\mathbf{Z}$-module by the Mordell-Weil theorem.

1.4 The case $D > 0$: Heegner cycles

When $D > 0$, the roots τ_1 and τ_2 of the dehomogenized form $Ax^2 + Bx + C$ lie on the real line. Let $\mathcal{C}$ be the geodesic in the hyperbolic plane joining τ_1 and τ_2. A geodesic joining two rational numbers on the real line maps to a cycle of finite length on $X_0(N)$, joining a cusp to a cusp. In general, an arbitrary geodesic joining irrational real numbers maps to a path with dense image on $X_0(N)$. Because τ_1 and τ_2 are real quadratic and conjugate, the image of $\mathcal{C}$ on $X_0(N)(\mathbf{C})$ is an infinite periodic cycle. More precisely, the form $Ax^2 + Bxy + Cy^2$ is preserved by an infinite abelian subgroup of $\mathbf{SL}_2(\mathbf{Z})$ of rank 1. A generator for this group modulo torsion is called an automorph of F. When F is primitive, the automorph M_F can be written down by choosing a fundamental solution to Pell's equation

$$u^2 - Dv^2 = 1,$$

and setting

$$M_F = \begin{pmatrix} u - Bv & -2Cv \\ 2Av & u + Bv \end{pmatrix}.$$

Observe that M_F belongs to $\Gamma_0(N)$, since N divides A. Now choose any point τ lying on the geodesic $\mathcal{C}$, and let $\mathcal{C}_i$ be the geodesic joining $M^i\tau$ to $M^{i+1}\tau$. Then $\mathcal{C}$ can be expressed as an infinite union

$$\mathcal{C} = \cup_{i \in \mathbf{Z}} \mathcal{C}_i,$$

and each $\mathcal{C}_i$ maps to the same basic homology cycle α_F in $M_D = H_1(E(\mathbf{C}), \mathbf{Z})$. The construction of α_F also works when F is not primitive, using the same definiton for M_F; but observe that in this case the matrix M_F could be a non-trivial power of the automorph of F.

The module M_D can be identified with the lattice Λ by the map $\alpha \mapsto \int_\alpha \omega_E$. Thus α_F can be computed by evaluating the integral

$$\int_z^{M_F z} \omega_E$$

which belongs to Λ and does not depend on the choice of z, and using the identification of Λ with $H_1(E(\mathbf{C}), \mathbf{Z})$.

Theorem 1.8 *Once a choice of a fundamental solution to Pell's equation has been made, the cycle α_F does not depend on the choice of F modulo the action of $\Gamma_0(N)$, and hence the assignment $F \mapsto \alpha_F$ is well-defined on G_D.*

Proof: Modifying F by an element γ in $\Gamma_0(N)$ has the effect of conjugating M_F by γ, i.e.,

$$M_{F\gamma} = \gamma^{-1} M_F \gamma.$$

But the map $\psi : M \mapsto \int_z^{Mz} \omega_E$ is a homomorphism from $\Gamma_0(N)$ to the abelian group Λ, and hence $\psi(M_{F\gamma}) = \psi(M_F)$.

1.5 Properties of the Heegner objects

1.5.1 Action of the Hecke operators and w_N

Let $F \in G_D$ be a class of binary quadratic forms represented by the Heegner form (A, B, C). The Hecke operators can be defined on the forms by the rule

$$T_p F = F_\infty + \sum_{k=0}^{p-1} F_k,$$

$$F_\infty = (A, Bp, Cp^2), \quad F_k = (Ap^2, (B + 2Ak)p, Ak^2 + Bk + C),$$

where the sum is to be viewed as a formal sum of (not necessarily primitive) binary quadratic forms of dicriminant Dp^2. Observe that the forms F_∞ and F_k are Heegner forms, and hence the construction of sections 1.3 or 1.4 can be applied to them. Thus one defines

$$\alpha_{T_p F} = \alpha_{F_\infty} + \sum_{k=0}^{p-1} \alpha_{F_k}.$$

Proposition 1.9 .

1. *If $D < 0$, then $\alpha_{T_p F} = a_p u \alpha_F$, where $u = \#\mathcal{O}_f^*/2$.*

2. *If $D > 0$, let u be the smallest integer such that $(v+w\sqrt{D})^u$ is congruent to a rational integer mod p, where (v, w) is a fundamental solution to the Pell equation $v^2 - Dw^2 = 1$. Then $\alpha_{T_p F} = a_p u \alpha_F$.*

The Atkin-Lehner involution w_N assigns to the Heegner form F the Heegner form $(CN, B, A/N)$.

Proposition 1.10 $\alpha_{w_N F} = -\epsilon \alpha_F$.

Propositions 1.9 and 1.10 can be verified by a direct argument, using the definition of the objects α_F in terms of ω_E, and the the action of the Hecke operators and the Atkin-Lehner involution on ω_E described in part 3 of conjecture 1.1. For more details (when $D < 0$) see [Gr1], §5 and §6, or [Gr2].

Let Frob_N be the class of quadratic forms in G_D represented by the form $(N, B_0 f, (B_0^2 f^2 - D)/(4N))$. This terminology is appropriate, because this form correponds to the Frobenius element at $\mathcal{P}_1 \cdots \mathcal{P}_k$, where $\mathcal{P}_j$ is prime ideal above $p_j | N$ given by $(p_j, (B_0 - \sqrt{D_0})/2)$. The action of the Atkin-lehner involution w_N can be written down in terms of the form Frob_N and the Gaussian composition law, as:

Proposition 1.11 $w_N F = \mathrm{Frob}_N F^{-1}$.

1.5.2 Behaviour under norms

Let p be a prime which does not divide ND, and let $F = (A, B, C)$ be an element of G_{Dp^2}. Since the ring class field K_f is contained in the ring class field K_{fp}, there is a natural homomorphism $\mu_p : G_{Dp^2} \longrightarrow G_D$. Let $\bar{F}$ denote a form in G_D which represents $\mu_p(F)$. Define the norm of F to be the formal sum

$$N_p F = \sum_{\mu_p(G) = \bar{F}} G$$

of forms in G_{Dp^2}, and define the norm of α_F to be the element

$$N_p \alpha_F = \sum_{\mu_p(G) = \bar{F}} \alpha_G,$$

where the sum is taken over all inequivalent primitive Heegner forms of discriminant Dp^2 which map to $\bar{F}$.

If p is split in K, choose an ideal $\mathcal{P}$ of K above p, and let Frob_p be the quadratic form in G_D which represents the frobenius element at $\mathcal{P}$ in $\mathrm{Gal}(K_f/K)$. Choosing a different prime of K above p replaces Frob_p by Frob_p^{-1}, so the element $\mathrm{Frob}_p + \mathrm{Frob}_p^{-1}$ in the group ring $\mathbf{Z}[G_D]$ is well-defined.

Proposition 1.12 .

1. *If* $(\frac{p}{D_0}) = 1$, *then* $N_p\alpha_F = a_p\alpha_{\bar{F}} - \alpha_{\mathrm{Frob}_p\bar{F}} - \alpha_{\mathrm{Frob}_p^{-1}\bar{F}}$.
2. *If* $(\frac{p}{D_0}) = -1$, *then* $N_p\alpha_F = a_p\alpha_{\bar{F}}$.

Proof: The formal sum N_pF can be expressed in terms of the Hecke operators T_p by

$$N_pF = u^{-1}(T_p\bar{F}) - \mathrm{Frob}_p\bar{F} - \mathrm{Frob}_p^{-1}\bar{F} \quad \text{if } (\frac{p}{D_0}) = 1,$$

and

$$N_pF = u^{-1}(T_p\bar{F}) \quad \text{if } (\frac{p}{D_0}) = -1,$$

where u is as defined in proposition 1.9; the result follows from this proposition.

2 Relation with L-functions

2.1 Root numbers

Let $L(E/K, s)$ denote the L-function of E over K, defined by the Euler product expansion

$$\prod_v (1 - a_{\mathbf{N}v}\mathbf{N}v^{-s} + \mathbf{N}v^{1-2s})^{-1},$$

where the product is taken over the places v of K. This factors as a product of two L functions

$$L(E/K, s) = L(E/\mathbf{Q}, s)L(E^{(D)}/\mathbf{Q}, s),$$

where $E^{(D)}$ is the twist of E by D defined by the equation

$$Dy^2 = 4x^3 - g_2x - g_3.$$

Let r_{an} denote the order of vanishing of $L(E/K, s)$ at $s = 1$, and let r_{an}^+ (resp. r_{an}^-) denote the order of vanishing of $L(E/\mathbf{Q}, s)$ (resp. $L(E^{(D)}/\mathbf{Q}, s)$) at $s = 1$.

Proposition 2.1 .

1. *If $D < 0$, then $r_{an}^+ \not\equiv r_{an}^- \pmod 2$, and r_{an} is odd.*
2. *If $D > 0$, then $r_{an}^+ \equiv r_{an}^- \pmod 2$, and r_{an} is even.*

Proof: Let ϵ be the eigenvalue for the Atkin-Lehner involution w_N acting on ω_E. The sign in the functional equation for $L(E/\mathbf{Q}, s)$ is $-\epsilon$, and hence $L(E/\mathbf{Q}, s)$ vanishes to odd order at the critical point $s = 1$ if $\epsilon = 1$, and to even order if $\epsilon = -1$. As explained in [Gr1], the sign in the functional equation for the L function of the twist $E^{(D)}$ can be computed explicitely, and is equal to ϵ if $D < 0$, and $-\epsilon$ if $D > 0$, when D satisfies the Heegner hypothesis. The result follows.

2.2 Formulas of Gross-Zagier and Waldspurger

We define a Hermitian pairing $\langle\ ,\ \rangle_D$ on $M_D \otimes \mathbf{C}$.

Definition 2.2 *The pairing $\langle\ ,\ \rangle_D : M_D \times M_D \longrightarrow \mathbf{C}$ is defined by:*

1. *If $D < 0$, let it be the Néron-Tate canonical height on $E(K_f)$, extended to a Hermitian pairing on $E(K_f) \otimes \mathbf{C}$.*
2. *If $D > 0$, let $\langle \alpha_1, \alpha_2 \rangle_D = \int_{\alpha_1} \omega_E \int_{\alpha_2} \bar{\omega}_E$.*

Given a complex character $\chi : G_D \longrightarrow \mathbf{C}^*$, let

$$\alpha_\chi = \frac{1}{h^+(D)} \sum_{F \in G_D} \chi(F)\alpha_F \in M_D \otimes \mathbf{C}.$$

To such a χ one can associate the twisted L-function

$$L(E/K, \chi, s) = \prod_v (1 - \chi(v)a_{\mathbf{N}v}\mathbf{N}v^{-s} + \chi^2(v)\mathbf{N}v^{1-2s})^{-1}.$$

It has an analytic continuation to the complex plane. Let $\omega^+, \omega^- \in \Lambda$ be the real and imaginary periods attached to E; the lattice generated by ω^+ and ω^- is of index 1 or 2 in Λ.

The following formula gives the relation between the elements α_F and the special values $L(E/K, \chi, 1)$. For $D < 0$ it is a result of Gross and Zagier, and for $D > 0$, it was proved by Waldspurger.

Theorem 2.3 (Gross-Zagier, Waldspurger) *Suppose that $D = D_0$ is a fundamental discriminant, and let $h = h^+(D)$.*

1. *If $D < 0$, then*

$$\langle \alpha_\chi, \alpha_{\bar{\chi}} \rangle_D \doteq u^2 \sqrt{D} h^{-1} (\omega^+ \omega^-)^{-1} L'(E/K, \chi, 1),$$

   where $u = \#\mathcal{O}_K^*/2$.

2. *If $D > 0$, then*

$$\langle \alpha_\chi, \alpha_{\bar{\chi}} \rangle_D \doteq \sqrt{D} h^{-1} L(E/K, \chi, 1),$$

where the symbol $\doteq$ denotes equality up to multiplication by a power of 2 which could be explicitly determined.

For the case $D < 0$, see [GZ], and for $D > 0$, see [GKZ], p. 527 and [Wal].

A similar formula certainly holds for non-fundamental D, but it has not been worked out for $D < 0$; one would need to adjust the formula to take into account the Euler factors at the primes dividing f. Since the formulas are given only to provide motivation for the later conjectures and results, we have not strived for the greatest generality and precision in writing them down.

3 A refined conjecture

3.1 Motivation and statement

Consider the formal elements

$$\theta_D = \sum_{F \in G_D} \alpha_F \cdot F, \qquad \theta_D^* = \sum_{F \in G_D} \alpha_F \cdot F^{-1},$$

viewed as elements of the tensor product $M_D \otimes \mathbf{Z}[G_D]$. Let L_D be defined by taking the formal product:

$$L_D = \theta_D \cdot \theta_D^* \in M_D^{\otimes 2} \otimes \mathbf{Z}[G_D].$$

The pairing $\langle\ ,\ \rangle_D$ of section 2.2 is a linear map of $M_D^{\otimes 2}$ to $\mathbf{C}$ and hence extends by linearity to a map from $M_D^{\otimes 2} \otimes \mathbf{Z}[G_D]$ to $\mathbf{C}[G_D]$. Applying this map to L_D gives an element $L_D^{\mathbf{C}}$ of $\mathbf{C}[G]$, which interpolates special values of the L-function of E over K; for the expression $\langle \alpha_\chi, \alpha_{\bar{\chi}} \rangle_D$ which appears in theorem 2.3 is equal to $\chi(L_D^{\mathbf{C}})$. The original element L_D has more structure than $L_D^{\mathbf{C}}$, since its coefficients are elements of a $\mathbf{Z}$-module $M_D^{\otimes 2}$. For instance, it makes sense to talk about congruences for these coefficients. Let I denote the augmentation ideal in the integral group ring $\mathbf{Z}[G_D]$. The first conjecture we make is close in spirit to the Birch and Swinnerton-Dyer conjecture, (and, even more so, to its p-adic avatars) and is inspired by a similar conjecture of Mazur and Tate in the cyclotomic case (cf. [MT], [D3]).

Conjecture 3.1 .

1. *If $D < 0$, then L_D belongs to the subgroup $M_D^{\otimes 2} \otimes I^{r-1}$ of $M_D^{\otimes 2} \otimes \mathbf{Z}[G_D]$.*
2. *If $D > 0$, then L_D belongs to the subgroup $M_D^{\otimes 2} \otimes I^{r}$ of $M_D^{\otimes 2} \otimes \mathbf{Z}[G_D]$.*

Let r denote the rank of $E(K)$. Let $E(K)^+$ and $E(K)^-$ denote the plus and minus eigenspaces of $E(K)$ under the action of the involution in $\mathrm{Gal}(K/\mathbf{Q})$. They generate a submodule of $E(K)$ of index at most 2. Let r^+ and r^- denote the ranks $E(K)^+$ and $E(K)^-$; thus r^+ is the rank of E over $\mathbf{Q}$, and $r^+ + r^- = r$. The Birch and Swinnerton-Dyer conjecture implies that $r^\pm = r_{an}^\pm$. Let $\rho = \max(r^+, r^-)$.

Guided by the main result of [D1], one is lead to make the following stronger conjecture about the "square root" θ_D of L_D.

Conjecture 3.2 .

1. *If $D < 0$, then θ_D belongs to the subgroup $M_D \otimes I^{\rho-1}$ of $M_D \otimes \mathbf{Z}[G_D]$.*
2. *If $D > 0$, then θ_D belongs to the subgroup $M_D \otimes I^{\rho}$ of $M_D \otimes \mathbf{Z}[G_D]$.*

When $D < 0$, conjecture 3.2 implies that L_D belongs to $M_D^{\otimes 2} \otimes I^{2\rho-2}$. Assuming that r is odd (which is implied by the Birch Swinnerton-Dyer conjecture $r = r_{an}$ together with proposition 2.1) one has $2\rho - 2 \geq r - 1$, with equality holding if and only if $|r^+ - r^-| = 1$. When $D > 0$, conjecture 3.2 implies that L_D belongs to $M_D^{\otimes 2} \otimes I^{2\rho}$, and $2\rho \geq r$, with equality holding if and only if $r^+ = r^-$.

The evidence for conjecture 3.2 is of two types. By applying the descent argument of Kolyvagin, one can prove part 1 of the conjecture (for $D < 0$) under certain mild extra hypotheses. This result will be presented in section 3.4.

The proof of the conjecture for $D > 0$ would seem to require new ideas, but it is more amenable to numerical verification on the computer, since the module M_D in this case is simpler. A summary of some of the computer calculations that were performed is given in section 3.5.

3.2 Properties of θ_D

Let ν_p denote the map $M_{Dp^2} \otimes \mathbf{Z}[G_{Dp^2}] \longrightarrow M_{Dp^2} \otimes \mathbf{Z}[G_D]$ induced by the natural homomorphism $\mu_p : G_{Dp^2} \longrightarrow G_D$.

Proposition 3.3 .

1. $\nu_p(\theta_{Dp^2}) = (a_p - \mathrm{Frob}_p - \mathrm{Frob}_p^{-1})\theta_D$ *if* $(\frac{p}{D_0}) = 1$.
2. $\nu_p(\theta_{Dp^2}) = a_p\theta_D$ *if* $(\frac{p}{D_0}) = -1$,

Proof: This is a direct consequence of proposition 1.12.

Let $\theta \mapsto \theta^*$ denote the involution which sends $\sigma \in G_D$ to σ^{-1}, extended by linearity to the group ring $\mathbf{Z}[G_D]$. The following result can be viewed as the analogue of the functional equation for the element θ_D.

Proposition 3.4 $\mathrm{Frob}_N^{-1}\theta_D^* = -\epsilon\theta_D$.

Proof: By proposition 1.10, $w_N\theta_D = -\epsilon\theta_D$, and by proposition 1.11, $w_N\theta_D = \mathrm{Frob}_N^{-1}\theta_D^*$. The result follows.

Let Z be the ring $\mathbf{Z}[\frac{1}{2}]$, and let $\underline{\theta}_D$ denote the image of θ_D in $M_D \otimes Z[G_D]$. Define the order of vanishing of $\underline{\theta}_D$ to be the greatest t such that $\underline{\theta}_D$ belongs to $M_D \otimes \underline{I}^t$.

Proposition 3.5 *If $\epsilon = 1$, then $\underline{\theta}_D$ has odd order of vanishing, and if $\epsilon = -1$, then $\underline{\theta}_D$ has even order of vanishing.*

Proof: Let t denote the order of vanishing, and let $\tilde{\underline{\theta}}_D$ and $\tilde{\underline{\theta}}^*_D$ denote the leading coefficients in $M_D \otimes (\underline{I}^t/\underline{I}^{t+1})$. Since $\tilde{\theta}^*_D = (-1)^t \tilde{\theta}_D$, the functional equation of proposition 3.4 implies that

$$(-1)^t \tilde{\underline{\theta}}_D = -\epsilon \tilde{\underline{\theta}}_D.$$

Since the group $M_D \otimes (\underline{I}^t/\underline{I}^{t+1})$ is of odd order, it follows that

$$(-1)^{t+1} = \epsilon,$$

which proves the proposition.

3.3 The leading coefficient

Assuming the truth of the order of vanishing conjectures 3.1 and 3.2, define the leading coefficient of θ_D to be the projection of θ_D to the group $M_D \otimes (I^{\rho-1}/I^{\rho})$ if $D < 0$, and to $M_D \otimes (I^{\rho}/I^{\rho+1})$ if $D > 0$. It is natural to search for an interpretation of the leading coefficient $\tilde{\theta}_D$ in terms of arithmetic data for the curve E over K. Such a conjecural interpretation can only be given at the moment for the following cases:

1. $D < 0$, $|r^+ - r^-| = 1$.
2. $D > 0$, $r^+ = r^-$.

(These represent exactly the cases for which conjecture 3.2 is no stronger than conjecture 3.1). The conjecture concerning the value of the leading coefficient in case 1 is stated in full generality in [D2]. We concentrate here on the simpler case where $D > 0$. To simplify the discussion, we will state the conjecture only in the case where f is a prime > 3 and $r > 0$, and $E(K)$ is torsion-free. (In the general case, one needs to modify the naive element θ_D by a kind of regularization process which is explained in [D2] to make the conjecture compatible under norms and take into account the Euler factors at the primes dividing f.)

In [MT], B. Mazur and J. Tate define a height pairing based on an idea of Manin and Zarhin, which takes values in $G_D = I/I^2$. This height pairing

is not defined on the full Mordell-Weil groups, but only on $E(K) \times E_f(K)$, where $E_f(K)$ denotes the subgroup of $E(K)$ of finite index in $E(K)$ defined by the exact sequence:

$$0 \longrightarrow E_f(K) \longrightarrow E(K) \longrightarrow E/E^0(K) \oplus E(k_f).$$

Here k_f denotes the residue field of K at f. Let further J_D denote the order of the cokernel of the right-hand map.

Let $P_1, \ldots, P_r$ (resp. $Q_1, \ldots Q_r$) denote integral bases for $E(K)$ (resp. $E_f(K)$) modulo torsion which induce compatible orientations on $E(K) \otimes \mathbf{R}$. Let R_D be the determinant of $r \times r$ matrix $(\langle P_i, Q_j \rangle_D$ with entries in I/I^2. It belongs naturally to I^r/I^{r+1}. The element R_D plays the role of the regulator. It is independent of the choice of bases.

Conjecture 3.6

$$\tilde{L}_D \ (= (-1)^\rho \tilde{\theta}_D^2) = \#\underline{III}(E/K) \cdot R_D \cdot J_D \cdot \omega^+ \otimes \omega^+.$$

What is the correct generalization of this conjecture when ρ is greater than $r/2$? In that case conjecture 3.2 predicts that the image of $\tilde{L}_D$ in $M_D^{\otimes 2} \otimes I^r$ is 0. It can also be shown that the Mazur-Tate regulator R_D in I^r/I^{r+1} vanishes: for the height pairing is trivial when restricted to $E(\mathbf{Q}) \times E_f(\mathbf{Q})$ or $E^-(K) \times E_f^-(K)$, and the hypothesis $r^+ \neq r^-$ implies that one of the isotropic subspaces has dimension $> r/2$.

However, one feels strongly that the leading coefficient $\tilde{\theta}_D$ in $M_D \otimes I^\rho/I^{\rho+1}$ should have an arithmetic interpretation in all cases. [1]

3.4 The case $D < 0$: theoretical evidence

We now return to the order of vanishing conjecture 3.2, and state a result which gives evidence for it in the case where $D < 0$. For details and proofs see [D2].

Suppose that E has no complex multiplications, and supppose that $D < 0$ is such that all primes dividing f are inert in $K = \mathbf{Q}(\sqrt{D})$.

Let Z be a subring of $\mathbf{Q}$ such that the following are invertible:

[1] Note: Since this paper was submitted, such an interpretation has been found. See the forthcoming publication by Massimo Bertolini and the author on "Derived Height Pairings".

1. All primes $p|6$.

2. All primes $p < \rho$.

3. All primes p such that $\mathrm{Gal}(\mathbf{Q}(E_{p^\infty})/\mathbf{Q})$ is smaller than the full group of $\mathbf{Z}_p$-linear automorphisms of the Tate module $T_p(E)$.

4. All p which divide $[E : E^0]$.

By a result of Serre [Se], the set of primes satisfying condition 3 is a finite set (in the case where N is squarefree, it consists at most of the primes ≤ 11). Let $\underline{\theta}_D$ be the image of θ_D in the group $M_D \otimes Z[G_D]$, and let $\underline{I}$ denote the augmentation ideal in the group ring $Z[G_D]$.

Theorem 3.7 *$\underline{\theta}_D$ belongs to the subgroup $M_D \otimes (\underline{I}^{\rho-1}/\underline{I}^{\rho})$ of $M_D \otimes Z[G_D]$.*

A key ingredient in the proof of this result is the descent method of Kolyvagin [Ko1], [Ko2].

3.5 The case $D > 0$: computational evidence

The conjecture for $D > 0$ is closer to the original cyclotomic conjecture of Mazur and Tate formulated in [MT] in terms of modular symbols, which remains unproved. One must thus content oneself with numerical verification on the computer. Fortunately, the module M_D is much simpler than when $D < 0$, making such calculations feasible.

Because of the close analogy between Heegner cycles and Heegner points, it is hoped that the numerical study of Heegner cycles will provide insights into the behaviour of Heegner points in the anticyclotomic tower. An understanding of this behaviour is crucial if one wants to extend Kolyvagin's methods to modular elliptic curves of higher rank.

We now give three representative examples, involving modular elliptic curves of conductor 11, 37 and 5077.

3.5.1 The curve $X_0(11)$

Let E be the modular curve $X_0(11)$, given by the equation

$$y^2 + y = x^3 - x^2 - 10x - 20.$$

Its Mordell-Weil group has rank 0 over $\mathbf{Q}$, and the eigenvalue of the Atkin-Lehner involution w_{11} is $\epsilon = -1$.

A list of values of $D_0 \leq 500$ which satisfy the Heegner hypothesis for E and for which $L(E/K, s)$ has a (non-trivial) zero at $s = 1$ can be found in the tables compiled by Glenn Stevens [St], p. 171. They are: $D_0 = 232, 265, 273, 364, 401, 421, 476, 488$. If f is prime to $11D_0$, and if $D = D_0 f^2$, conjecture 3.2 predicts that

$$\theta_D \in M_D \otimes I^2.$$

In this case much of it can be proved. Let $\underline{\theta_D}$ denote as in section 3.2 the image of θ_D in $M_D \otimes Z[G_D]$, where Z is the ring $\mathbf{Z}[\frac{1}{2}]$.

Proposition 3.8 *$\underline{\theta_D}$ belongs to $M_D \otimes \underline{I}^2$.*

Proof: Waldspurger's formula (theorem 2.3) implies that $\underline{\theta_D}$ belongs to $M_D \otimes \underline{I}$. The result follows from proposition 3.5 and the fact that $\epsilon = -1$ for the curve $X_0(11)$.

A verification of the full vanishing conjecture by computation remains interesting nonetheless, since it enables us to compute the values of the mysterious leading terms $\tilde{\theta}_D \in M_D \otimes (I^2/I^3)$.

A summary of some of these computations is presented in table 1.

1. Column 1 of the table indicates the value of D, written in the form $D_0 f^2$. In some cases the full θ_D was not computed, but only its projection in $\mathbf{Z}[G_D^{(2)}]$, where $G_D^{(2)}$ is the quotient of G_D by its 2-primary part. These cases are indicated by an asterisk next to the value of D.

2. Column 2 indicates the order, and structure, of the class group G_D by giving the factorization $h^+(D) = h_1 \cdots h_k$, where

   $$G_D = \mathbf{Z}/h_1 \times \cdots \times \mathbf{Z}/h_k\mathbf{Z},$$

   and h_i is divisible by h_j whenever $j > i$. The integers h_i are determined uniquely by G_D and determine the structure of G_D completely. In the cases where the 2-part was ignored, the similar factorization is given, but only for the odd part of the class group.

3. Column 3 indicated generators σ_1, ..., σ_k for each of the cyclic pieces of the class group.

4. Column 4 gives the leading coefficient of the θ-element. The expressions $\sigma_1, \ldots, \sigma_k$ refer to the corresponding generators given in column 3. We have omitted the factor of ω^+ which appears in all of the leading coefficients.

3.5.2 The curve $X_0(37)^+$

Let E be the elliptic curve of conductor 37 given by the equation

$$y^2 - y = x^3 - x.$$

The curve E is modular; in fact, it is the quotient of the modular curve $X_0(37)$ of genus 2 by the Atkin-Lehner involution w_{37}, and hence the map ϕ of conjecture 1.1 is of degre 2.

If D satisfies the Heegner hypothesis for E, then conjecture 3.2 predicts that

$$\theta_D \text{ belongs to } M_D \otimes I.$$

In this case the conjecture follows from the formula (theorem 2.3) of Waldspurger. It is interesting to check that this predicted order of vanishing is sharp, i.e., that the leading coefficients of $\tilde{\theta}_D$ are in general non-trivial in $M_D \otimes (I/I^2)$.

Since $\rho = r^+ = r^- = 1$, conjecture 3.6 of section 3.3 gives a precise prediction for the value of the leading coefficient. We plan to verify this conjecture by finding rational points on the relevant twists of $X_0(37)^+$ and computing the Mazur-Tate height pairing between them, but have not carried out this computation at present.

The first 10 positive fundamental discriminants which satisfy the Heegner hypothesis are 12, 21, 28, 33, 40, 41, 44, 53, 65, and 73. We have limited our computations to discriminants of the form $D_0 f^2$ where D_0 is one of these ten fundamental discriminants, and f is prime. The results of the computation are summarized in table 2, with the same conventions as for the previous table.

Table 1: The curve $X_0(11)$

$D = D_0 f^2$	$h^+(D)$	Generators of G_D	Leading term
$232 \cdot 13^2$	$14 \cdot 2$	$(33, 134, -161)$,	$11 \cdot (\sigma_1 - 1)^2$
		$(69, 142, -69)$	$+(\sigma_1 - 1)(\sigma_2 - 1)$
$232 \cdot 35^2$	$6 \cdot 2$	$(-3, 530, 275)$	$4(\sigma_1 - 1)^2$
		$(-2, 532, 147)$	
$232 \cdot 323^2$	$18 \cdot 2 \cdot 2$	$(-3, 4916, 3106)$	$8(\sigma_1 - 1)^2$
		$(1673, 3116, -2166)$	
		$(-1847, 2974, 2079)$	
$232 \cdot 7841^2$	$2614 \cdot 2$	$(40293, 41732, -77694)$,	$486(\sigma_1 - 1)^2$
		$(-50919, 84196, 35226)$	$+(\sigma_1 - 1)(\sigma_2 - 1)$
$232 \cdot 146329^2(*)$	$21 \cdot 21$	$(9, 2228804, -1600486)$	$9(\sigma_1 - 1)^2$
		$(57121, 2174902, -1039137)$	$+15(\sigma_2 - 1)^2$
$265 \cdot 373^2$	$372 \cdot 2$	$(-60, 6065, 354)$	$294(\sigma_1 - 1)^2$
		$(-1320, 4465, 3207)$	
$273 \cdot 727^2$	$364 \cdot 2 \cdot 2$	$(2, 12009, -9042)$	$284(\sigma_1 - 1)^2$
		$(-21, 11991, 6004)$	
		$(-6028, 12009, 3)$	
$401 \cdot 1601^2$	2670	$(-1502, 29659, 24665)$	$2520(\sigma_1 - 1)^2$
$421 \cdot 97^2$	96	$(15, 1967, -1535)$	$42(\sigma_1 - 1)^2$
$421 \cdot 139^2$	138	$(15, 2849, -289)$	$2(\sigma_1 - 1)^2$
$421 \cdot 331^2$	166	$(15, 6791, -125)$	$138(\sigma_1 - 1)^2$
$421 \cdot 4337^2$	4338	$(-5, 88983, 42713)$	$3147(\sigma_1 - 1)^2$
$488 \cdot 97^2$	$32 \cdot 2$	$(-118, 2040, 911)$	$5(\sigma_1 - 1)^2$
		$(-61, 2074, 1189)$	$+(\sigma_1 - 1)(\sigma_2 - 1)$

Table 2: The curve $X_0(37)^+$

$D = D_0 f^2$	$h^+(D)$	Generators of G_D	Leading term
$12 \cdot 607^2$	$38 \cdot 2$	$(-1034, 2066, 37)$ $(3, 2100, -949)$	$8 \cdot (\sigma_1 - 1)$
$12 \cdot 2131^2$	$164 \cdot 2$	$(-3351, 6042, 1342)$ $(2, 7382, -1)$	$128(\sigma_1 - 1)$
$12 \cdot 3691^2$	$284 \cdot 2$	$(3489, 8136, -6971)$ $(3, 12780, -12781)$	$12(\sigma_1 - 1)^3$
$21 \cdot 2089^2$	$190 \cdot 2$	$(-3617, 4923, 4659)$ $(3, 9573, -1)$	$94(\sigma_1 - 1)$
$21 \cdot 3191^2$	$290 \cdot 2$	$(-1433, 14047, 2881)$ $(3, 14619, -9745)$	$34(\sigma_1 - 1)$
$28 \cdot 271^2$	$54 \cdot 2$	$(498, 538, -887)$ $(7, 1428, -613)$	$36(\sigma_1 - 1)$
$28 \cdot 617^2$	$88 \cdot 2$	$(-3, 3260, 2641)$ $(7, 3262, -666)$	$8(\sigma_1 - 1)$
$33 \cdot 151^2$	$38 \cdot 2$	$(-2, 867, 93)$ $(62, 867, -3)$	$26(\sigma_1 - 1)$
$33 \cdot 2069^2$	$414 \cdot 2$	$(-3284, 7875, 6033)$ $(-3, 11883, 4952)$	$140(\sigma_1 - 1)$
$40 \cdot 281^2$	$56 \cdot 2$	$(-6, 1772, 769)$ $(-5, 1770, 1277)$	$24(\sigma_1 - 1)$
$40 \cdot 3221^2$	$358 \cdot 2$	$(-7734, 10576, 9799)$ $(-5, 20370, 2837)$	$102(\sigma_1 - 1)$
$41 \cdot 241^2$	80	$(-206, 1347, 688)$	$128(\sigma_1 - 1)$
$41 \cdot 1493^2$	166	$(2, 9557, -6845)$	$128(\sigma_1 - 1)$
$41 \cdot 99241^2$	6616	$(-1112, 634453, 285344)$	$5808(\sigma_1 - 1)$
$44 \cdot 199^2$	$50 \cdot 2$	$(-10, 1318, 133)$ $(11, 1320, -1)$	$18(\sigma_1 - 1)$
$44 \cdot 379^2$	$76 \cdot 2$	$(-659, 1460, 1589)$ $(11, 2508, -685)$	$68(\sigma_1 - 1)$
$44 \cdot 419^2$	$84 \cdot 2$	$(-7, 2768, 2245)$ $(11, 2772, -925)$	$60(\sigma_1 - 1)$

Table 2 (cont'd): The curve $X_0(37)^+$.

$D = D_0 f^2$	$h^+(D)$	Generators of G_D	Leading term
$53 \cdot 2549^2$	510	$(-11, 18537, 16861)$	$40(\sigma_1 - 1)$
$53 \cdot 3581^2$	398	$(-11, 26055, 17857)$	$186(\sigma_1 - 1)$
$65 \cdot 89^2$	$18 \cdot 2$	$(244, 249, -464)$	$4(\sigma_1 - 1)$
		$(-5, 715, 182)$	
$65 \cdot 149^2$	$30 \cdot 2$	$(-10, 1185, 971)$	$14(\sigma_1 - 1)$
		$(-5, 1195, 752)$	
$65 \cdot 181^2$	$20 \cdot 2$	$(-10, 1445, 1036)$	$8(\sigma_1 - 1)$
		$(-5, 1455, 622)$	
$65 \cdot 257^2$	$86 \cdot 2$	$(-14, 2059, 959)$	$38(\sigma_1 - 1)$
		$(-5, 2065, 1448)$	
$65 \cdot 353^2$	$32 \cdot 2$	$(-14, 2823, 2326)$	$8(\sigma_1 - 1)$
		$(-5, 2845, 278)$	
$65 \cdot 449^2$	$30 \cdot 2$	$(-1316, 1663, 1964)$	$12(\sigma_1 - 1)$
		$(-5, 3615, 1792)$	
$73 \cdot 1901^2$	380	$(-12, 16225, 11601)$	$232(\sigma_1 - 1)$

3.5.3 The curve of conductor 5077

Let E be the elliptic curve of conductor 5077 given by the equation

$$y^2 + y = x^3 - 7x + 6.$$

It was proved by Mestre [Me], p. 232, that E is modular. (In fact, the degree of the map ϕ of conjecture 1.1 was computed by Zagier [Z], and is equal to 1984.)

If D satisfies the Heegner hypothesis for E, then conjecture 3.2 predicts that

$$\theta_D \text{ belongs to } M_D \otimes I^3.$$

This has been checked for a number of values of D; the results of the computation are summarized in table 3.

Table 3: The curve of conductor 5077

$D = D_0 f^2$	$h^+(D)$	Generators of G_D	Leading term
$12 \cdot 71^2$	$10 \cdot 2$	$(13, 238, -74)$	0
		$(2, 242, -241)$	
$21 \cdot 2089^2$	$190 \cdot 2$	$(-1915, 5749, 7649)$	$122(\sigma_1 - 1)^3$
		$(7, 9669, -2735)$	
$21 \cdot 3191^2$	$290 \cdot 2$	$(3527, 13205, -2797)$	$286(\sigma_1 - 1)^3$
		$(-1, 14621, 14615)$	
$28 \cdot 17^2$	$6 \cdot 2$	$(3, 86, -58)$	0
		$(-27, 44, 57)$	
$53 \cdot 2549^2$	510	$(6773, 12507, -6937)$	$194(\sigma_1 - 1)^3$
$53 \cdot 4481^2$	640	$(97, 32603, -3223)$	$560(\sigma_1 - 1)^3$
$53 \cdot 3581^2$	398	$(211, 25745, -19957)$	$393(\sigma_1 - 1)^3$
$57 \cdot 151^2$	$76 \cdot 2$	$(2, 1137, -861)$	$4(\sigma_1 - 1)^3$
		$(-1, 1139, 584)$	
$61 \cdot 761^2$	254	$(3, 5941, -2575)$	$30(\sigma_1 - 1)^3$
$61 \cdot 5209^2$	1042	$(827, 39703, -23829)$	$472(\sigma_1 - 1)^3$
$61 \cdot 3373^2$	482	$(19, 26335, -6219)$	$198(\sigma_1 - 1)^3$
$65 \cdot 257^2$	$86 \cdot 2$	$(2, 2069, -1553)$	$8(\sigma_1 - 1)^3$
		$(-622, 1657, 622)$	
$76 \cdot 113^2$	$38 \cdot 2$	$(3, 980, -837)$	$10(\sigma_1 - 1)^3$
		$(2, 982, -765)$	
$85 \cdot 1361^2$	$272 \cdot 2$	$(3, 12547, -1673)$	$32(\sigma_1 - 1)^3$
		$(5, 12545, -3513)$	
$88 \cdot 197^2$	$98 \cdot 2$	$(3, 1844, -1238)$	$8(\sigma_1 - 1)^3$
		$(22, 1848, -1)$	
$89 \cdot 53^2$	52	$(2, 497, -374)$	$8(\sigma_1 - 1)^3$
$89 \cdot 101^2$	34	$(2, 949, -911)$	$4(\sigma_1 - 1)^3$
$97 \cdot 569^2$	570	$(388, 5529, -538)$	$482(\sigma_1 - 1)^3$
$97 \cdot 401^2$	134	$(3, 3949, -258)$	$4(\sigma_1 - 1)^5$

References

[BD] M. Bertolini and H. Darmon, *Kolyvagin's descent and Mordell-Weil groups over ring class fields*, Journall für die Reine und Angewandte Mathematik 412 (1990), pp. 63-74.

[Co] H. Cohn, *A classical invitation to algebraic numbers and class fields*, Universitext, Springer-Verlag, 1988.

[Cx] D.A. Cox, Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication, John Wiley and sons, 1989.

[D1] H. Darmon, *Refined class number formulas for derivatives of L-series*, PhD thesis, Harvard University, May 1991.

[D2] H. Darmon, *A refined conjecture of Mazur-Tate type for Heegner points*, to appear in Invent. Math.

[D3] H. Darmon, *Euler Systems and refined conjectures of Birch Swinnerton-Dyer type*, to appear, in Proceedings of a Workshop on p-adic monodromy and the Birch Swinnerton-Dyer conjecture, held at Boston University, August 1991, B. Mazur and G. Stevens, eds.

[Gr1] B.H. Gross, *Heegner points on* $X_0(N)$, in Modular Forms, ed. by R.A. Rankin, Ellis Horwood limited, (1984) 87-105.

[Gr2] B.H. Gross, *Kolyvagin's work on modular elliptic curves*, Proceedings of the Durham symposium on L-functions and arithmetic, July, 1989, J. Coates and M.J. Taylor eds., Cambridge University Press, 1991, pp. 235-256.

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

[GKZ] B.H. Gross, W. Kohnen, and D. Zagier, *Heegner points and derivatives of L-series. II*, Math. Ann. 278, pp. 497-562 (1987).

[Ko1] V.A. Kolyvagin, *Finiteness of* $E(\mathbf{Q})$ *and* $\underline{III}(E/\mathbf{Q})$ *for a subclass of Weil curves*, Izv. Akad. Nauk. SSSR Ser Mat. 52 (3) (1988), 522-540; Math USSR Izvestiya 32 (1989), 523-541.

[Ko2] V.A. Kolyvagin, *On the Mordell-Weil group and Shafarevich-Tate group of Weil elliptic curves*, Izv. Akad. Nauk. SSSR Ser Mat. 52 (6) (1988), 1154-1179.

[Ko3] V.A. Kolyvagin, *Euler Systems*, (1988). Grothendieck Festschrift, vol. 2, Progr. in Math, vol. 87, Boston: Birkhaüser 1991, pp. 435-483.

[Ko4] V.A. Kolyvagin, *On the structure of Selmer groups*, to appear in Math. Ann.

[MTT] B. Mazur, J. Tate and J. Teitelbaum, *On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer*, Invent. Math. 84 (1986), 1-48.

[MT] B. Mazur and J. Tate, *Refined conjectures of the "Birch and Swinnerton-Dyer type"*, Duke Math Journal, Vol. 54, No. 2, 1987, p. 711.

[Me] J.-F. Mestre, *La méthode des graphes. Exemples et applications.* Proceedings of the international conference on class numbers and fundamental units of algebraic number fields. June 24-28, 1986, Katata, Japan.

[Si] J.H. Silverman, The arithmetic of elliptic curves, Springer-Verlag, GTM 106, 1986.

[Se] J-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. Invent. Math. 15 (1972), 259-331.

[Sh] G. Shimura, Arithmetic theory of automorphic functions, Princeton University Press, Princeton, New Jersey, 1971.

[St] G. Stevens, Arithmetic on Modular Curves, Progress in Mathematics, Vol. 20, J. Coates, S. Helgason, ed.

[Ta] J. Tate, *Algorithm for determining the singular fiber in an elliptic pencil*, in "Modular functions of one variable IV," Lecture Notes in Mathematics 476, Springer-Verlag, 1975.

[Wal] J-L. Waldspurger, *Sur les valeurs de certaines fonctions L automorphes en leur centre de symétrie*, Comp. math. 54, pp. 173-242, 1985.

[Z] D. Zagier, *Modular points, modular curves, modular surfaces and modular forms*, Springer Lecture Notes 111, pp. 225-248.