Contemporary Mathematics
Volume **00**, 0000

Euler Systems and Refined Conjectures of Birch Swinnerton-Dyer Type

HENRI DARMON

Abstract. The relationship between arithmetic objects (such as global fields, or varieties over global fields) and the analytic properties of their L-functions poses many deep and difficult questions. The theme of this paper is the Birch and Swinnerton Dyer conjecture, and certain refinements that were proposed by Mazur and Tate. We will formulate analogues of these conjectures over imaginary quadratic fields involving Heegner points, and explain how the fundamental work of V.A. Kolyvagin sheds light on these new conjectures.

§1 Preliminaries.

The relationship between arithmetic objects (such as global fields, or varieties over global fields) and the analytic properties of their L-functions poses many deep and subtle questions. The theme of this paper is the Birch Swinnerton-Dyer conjecture, which concerns the case where the arithmetic object in question is an elliptic curve defined over a global field.

Let E be an elliptic curve defined over the rational numbers. The conjecture of Shimura-Taniyama-Weil asserts that E is modular, i.e., is equipped with a rational map

$$\varphi : X_0(N) \longrightarrow E,$$

where $X_0(N)$ is the modular curve of level N, defined over $\mathbf{Q}$, which parameterizes elliptic curves with a distinguished cyclic N-isogeny. We assume that E has this property. (For a specific E this can be checked by a finite computation.)

1991 *Mathematics Subject Classification.* Primary 11G40; Secondary 11G05.

The ideas for this paper are part of the author's Harvard PhD thesis; he gratefully acknowledges the support of Harvard University, and in particular of his advisor, B.H. Gross. Financial support was provided at various stages by the Natural Sciences and Enginnering Research Council and a Sloan Doctoral Dissertation Fellowship. Finally, this paper was written during a visit to the I.H.E.S. in the summer of 1991.

The pullback of the Néron differential ω on E is a cusp form of weight 2 on $X_0(N)$,

$$\varphi^*\omega = cf(q)dq/q,$$

where $f(q) = \sum_{n>0} a_n q^n$ is normalized so that $a_1 = 1$, and c denotes the Manin constant associated to the modular parametrization φ.

Let K be a number field. (In the applications we discuss, K will be either $\mathbf{Q}$, or a quadratic field.) Given a place v of K, let K_v denote the completion of K at v, and let k_v denote the residue field if v is non-archimedean.

Let S be a finite set of places of K, and let $E_S(K)$ denote the subgroup of finite index in $E(K)$ which is defined by the exact sequence

$$0 \longrightarrow E_S(K) \longrightarrow E(K) \longrightarrow \oplus_{v\in S} E_{\mathrm{ns}}(k_v) \oplus E/E_0(K) \longrightarrow J_S \longrightarrow 0,$$

where $E_{\mathrm{ns}}(k_v)$ denotes the group of non-singular points in the special fiber of E at v, and where $E/E_0(K)$ is the group of connected components in the Néron model $E_{/\mathcal{O}_K}$ of E over $\mathrm{Spec}\mathcal{O}_K$.

§1.1 Arithmetic invariants. The triple (E, K, S) gives rise to the following arithmetic data:

1. The rank r of the finitely generated abelian groups $E(K)$ and $E_S(K)$.

2. The order of the conjecturally finite Shafarevich-Tate group $\underline{Ш}(E/K)$. This is the group of elements in $H^1(K, E)$ whose restrictions in $H^1(K_v, E)$ are 0 for all places v of K. It arises naturally in descent arguments.

3. The Néron-Tate canonical height associated to the Poincaré divisor on $E \times E$; it is a positive-definite bilinear pairing

$$\langle\ ,\ \rangle_{NT} : E(K) \times E(K) \longrightarrow \mathbf{R}.$$

It gives rise to a regulator term.

We describe the general construction of the regulator suggested in [**MT2**]. While not strictly necessary for this section, the extra generality will be useful later. Let $\langle\ ,\ \rangle$ denote a G-valued pairing on $A \times B$, where G is an abelian group and A and B are subgroups of finite index in $E(K)$. We embed G as the degree one elements in the graded algebra

$$Sym(G) = \oplus_{r\geq 0} Sym^r(G).$$

If A and B are free, the regulator $R(A, B)$ in $\mathrm{Sym}(G)$ is defined to be the determinant of the $r \times r$ matrix $(\langle P_i, Q_j\rangle)$, where $P_1, \ldots, P_r$ and $Q_1, \ldots, Q_r$ denote integral bases for A and B respectively which induce compatible orientations on $E(K) \otimes \mathbf{R}$. The element $R(A, B)$ is homogeneous of degree r and can be viewed as belonging to $\mathrm{Sym}^r(G)$. If A and B are not free, one needs the hypothesis that there exist subgroups A' and B' of A and B which are free and of finite index, such that multiplication by $[A : A'][B : B']$ induces an isomorphism on G. This hypothesis is satisfied, for example, if $G = \mathbf{R}$, or if G is finite and of order prime

to the order of the torsion subgroups of A and B. One then defines $R(A,B)$ by the formula:

$$R(A,B) = [A : A']^{-1}[B : B']^{-1}R(A', B').$$

This definition is independent of the choice of A' and B'.

Let R denote the ring of germs of analytic functions of a complex variable s in a neigbourhood of $s = 1$, and let I denote the ideal of germs which vanish at $s = 1$. The choice of the local parameter $(s-1)$ determines an isomorphism $I/I^2 \simeq \mathbf{C}$, and hence the Néron-Tate height can be viewed as taking values in I/I^2. Since $\mathrm{Sym}^r(I/I^2)$ maps to I^r/I^{r+1} via a natural projection map p, one can define the regulator R_S by:

$$R_S := p(R(E(K), E_S(K))) \in I^r/I^{r+1}.$$

4. The module $H^0(E_{/\mathcal{O}_K}, \Omega^1)$ of global invariant differentials on $E_{/\mathcal{O}_K}$ is a projective $\mathcal{O}_K$-module of rank 1, and can be written as

$$H^0(E_{/\mathcal{O}_K}, \Omega^1) = \mathcal{A}\omega,$$

where $\mathcal{A}$ is a fractional ideal of K and ω is a differential for E over K. To each archimedean place of v we assign a period γ_v as follows:

$$\gamma_v = \int_{E(K_v)} |\omega| \text{ if } v \text{ is real,}$$

$$\gamma_v = 2\int_{E(K_v)} \omega \wedge \bar{\omega} \text{ if } v \text{ is complex.}$$

§1.2 The L-function. For each non-archimedean place v of K, let $\mathbf{N}v$ be the norm of v and let

$$a_v = 1 + \mathbf{N}v - \#E(k_v).$$

When E has good reduction at v, the local L-function $L(E/K_v, s)$ is defined by

$$L(E/K_v, s) = (1 - a_v\mathbf{N}v^{-s} + \mathbf{N}v^{1-2s})^{-1}.$$

A definition of the local factor $L(E/K_v, s)$ can also be given for the places of bad reduction of E, cf. [**Si**], p. 360. One always has:

$$L(E/K_v, 1) = \mathbf{N}v/\#E_{\mathrm{ns}}(k_v).$$

The L-series $L_S(E/K, s)$ is given by the Euler product

$$L_S(E/K, s) = \prod_{v \notin S} L(E/K_v, s),$$

taken over all non-archimedean places v of K which do not belong to S. The Hasse bound $|a_v| < 2\sqrt{\mathbf{N}v}$ implies that $L_S(E/K, s)$ converges in the right half plane $\Re(s) > 3/2$. One conjectures that it has a meromorphic continuation to the entire complex plane, given by a functional equation. When E is modular

and K is $\mathbf{Q}$ or a quadratic field, the functional equation is known. In particular, one can speak of the germ of $L_S(E/K, s)$ at $s = 1$. Let θ_S denote this germ.

§1.3 The Birch Swinnerton-Dyer conjecture. We give an S-integral formulation of the Birch Swinnerton-Dyer conjecture.

CONJECTURE 1.1. *1. θ_S belongs to I^r.*

2. Let $\tilde{\theta}_S$ denote the image of θ_S in I^r/I^{r+1}. Then

$$\tilde{\theta}_S = (\prod_{v \in S} \mathbf{N}v^{-1}) Disc(K)^{-1/2} (\mathbf{N}_{K/\mathbf{Q}}\mathcal{A})(\prod_v \gamma_v) \cdot \#\underline{Ш}(E/K) \# J_S R_S.$$

The arithmetic data associated to the triple (E, K, S), and the corresponding L-function $L_S(E/K, s)$ live in different worlds. The conjecture of Birch and Swinnerton-Dyer provides a mysterious bridge between them.

§1.4 The Euler System. In certain special cases, there is a sort of island between the two worlds, which Kolyvagin calls an Euler system. The bridge predicted by the Birch Swinnerton-Dyer conjecture can be constructed in two seperate stages, using the Euler sysem as a stepping stone.

When K is a quadratic imaginary field satisfying certain extra hypotheses, the Euler system is made up of Heegner points defined in the tower of ring class fields of K. The bridge between the world of the L-function and the Euler system is provided by the formula of Gross and Zagier. The work of Kolyvagin completes the picture by showing how the Euler system of Heegner points controls the arithmetic invariants r and $\underline{Ш}(E/K)$. Together, these two bridges yield the most striking evidence so far for the Birch Swinnerton-Dyer conjecture. This situation is summed up in the following diagram:

Let us now be more precise. Let K be a quadratic imaginary field of discriminant $D < -4$ such that every prime p which divides the conductor N of E splits in $K/\mathbf{Q}$, and let ω denote the corresponding odd Dirichelet character. If $N = p_1^{e_1} \cdots p_k^{e_k}$, choose for each p_i an ideal $\mathcal{P}_i$ of K above it, and set

$$\mathcal{N} = \mathcal{P}_1^{e_1} \cdots \mathcal{P}_k^{e_k}.$$

Given a positive square-free integer S which is relatively prime to N and D, let $\mathcal{O}_S$ denote the order of K of conductor T. The natural projection of complex tori

$$\mathbf{C}/\mathcal{O}_S \longrightarrow \mathbf{C}/(\mathcal{O}_S \cap \mathcal{N})^{-1}$$

corresponds to an N-isogeny of elliptic curves, and hence can be identified with a point of $X_0(N)$. By the theory of complex multiplication, this point is defined over K_S, the ring class field of K of conductor S. Let $\alpha(S)$ denote the image of this point in $E(K_S)$ by the modular parametrization φ.

Given a prime l which is split in $K/\mathbf{Q}$, let σ_l in $\mathrm{Gal}(K^l/K)$ denote the Frobenius element at λ, where K^l denotes the maximal abelian extension of K which is unramified at l, and λ is a prime of K above l. If l is inert in K, let $\sigma_l = 1$. Finally, given a square free integer T which is prime to D, let $\sigma_T = \prod_{l|T} \sigma_l$.

Now define the regularized Heegner points by the formulas:

$$y^+(S) = \sum_{T|S} \mu(T)\omega(T)\sigma_{S/T}^{-1}\alpha(T), \quad y^-(S) = \sum_{T|S} \mu(T)\sigma_{S/T}\alpha(T),$$

where μ denotes the Möbius function, $\mu(T) = (-1)^{\#(l|T)}$.

§1.5 The Gross Zagier formula. Let $G_S = \mathrm{Gal}(K_S/K)$, and let $\chi : G_S \longrightarrow \mathbf{C}^*$ denote a complex character of G_S. Let

$$e_\chi = \frac{1}{\#G_S} \sum_{\sigma \in G_S} \chi^{-1}(\sigma)\sigma$$

denote the idempotent in the group ring $\mathbf{C}[G_S]$ associated to the character χ, and let

$$y^\pm(\chi) = e_\chi y^\pm(S) \in E(K_S) \otimes \mathbf{C}$$

denote the projection of $y^\pm(S)$ to the χ-component of $E(K_S) \otimes \mathbf{C}$ for the G_S-action. Let $\langle\ ,\ \rangle_S$ denote the Néron-Tate pairing over K_S, extended to a Hermitian pairing on $E(K_S) \otimes \mathbf{C}$.

The points $y^+(\chi)$ and $y^-(\chi)$ depend on the choice of the σ_l (i.e., the choice of a prime λ of K above l for each l) but the complex number $\langle y^+(\chi), y^-(\chi)\rangle_S$ does not. From the formula of Gross and Zagier one expects this number to be related up to some simple factors to the value of $L_S'(E/K, \chi, 1)$. (By abuse of notation, we identify S with the set of primes of K which divide it, so that the L-function $L_S(E/K, s)$ has the obvious meaning.)

THEOREM 1.2. *Assume that $\chi : G_S \longrightarrow C^*$ is unramified, i.e., factors through G_1, where $G_1 = Gal(K_1/K)$ is the Galois group of the Hilbert class field of K. Then*

$$\langle y^+(\chi), y^-(\chi)\rangle_S = c^2 S \frac{\sqrt{D_S}}{h_S} \cdot \frac{L_S^{'}(E/K, \chi, 1)}{||\omega||^2}.$$

A similar result should hold for ramified characters but the computations in [**GZ**] were only carried out for characters of $\mathrm{Gal}(K_1/K)$.

§1.6 The work of Kolyvagin. V.A. Kolyvagin has established a relation between the arithmetic of E/K and the system $y^{\pm}(S)$ of Heegner points.

Let Z be a subring of $\mathbf{Q}$ in which the following primes are invertible:

1. The primes 2 and 3.

2. All primes p for which $\mathrm{Gal}(\mathbf{Q}(E_{p^\infty}/\mathbf{Q})$ is not isomorphic to the full $\mathbf{GL}_2(E_{p^\infty})$. By a result of Serre [**Se**], this is a finite set of primes, if E has no complex multiplications.

3. The primes p which divide $\#G_S$.

Let $Z[\chi]$ denote the ring obtained by adjoining to Z the values of the character χ. The points $y^{\pm}(\chi)$ can be viewed as belonging to the module $E(K_S) \otimes_{\mathbf{Z}[G_S]} Z[\chi]$. Let r_χ denote the rank of this module over $Z[\chi]$. It is equal to the dimension of the χ-component of $E(K_S) \otimes \mathbf{C}$ for the action of G_S, because the order of $E(K_S)_{\mathrm{tor}}$ is invertible in $Z[\chi]$. Let $\mathcal{E}(K_S) \subset E(K_S)$ denote the submodule generated be the Heegner points of $E(K_S)$.

THEOREM 1.3. *If $y^{\pm}(\chi) \neq 0$, then*

1. *$r_\chi = 1$.*
2. *The module $M = (E(K_S)/\mathcal{E}(K_S)) \otimes_{\mathbf{Z}[G_S]} Z[\chi]$ is finite.*
3. *The group $\underline{Ш}(E/K_S) \otimes_{\mathbf{Z}[G_S]} Z[\chi]$ is finite, and its order divides $(\#M)^2$.*

Kolyvagin presents the proof of this theorem when χ is the trivial character, but his methods extend to non-trivial ring class characters as well, as is shown in [**BD**].

When $L^{'}(E/K, s)$ does not vanish at $s = 1$, then theorem 1.2 shows that the Heegner point $\mathrm{Tr}_{K_1/K} y(1)$ is non-torsion, and theorem 1.3 says that $E(K)$ has rank one. It also says that $\underline{Ш}(E/K) \otimes Z$ is finite and that its order is bounded by a number which is consistent with the Birch Swinnerton-Dyer conjecture. In fact, by a more careful analysis Kolyvagin shows that $\underline{Ш}(E/K)$ is finite in this case.

§1.7 Refined conjectures. When $L^{'}(E/K, 1) = 0$, one does not know how to prove the weak Birch Swinnerton-Dyer conjecture that the rank of $E(K)$ is equal to the order of vanishing of $L(E/K, s)$ at $s = 1$. One does not even know how to exhibit a non-torsion point on $E(K)$ (although the conjecture predicts that the rank of E over K is at least 3!) Likewise, the finiteness of $\underline{Ш}(E/K)$ is still unproved in this case.

However, Kolyvagin has observed ([**Ko4**]) that from his methods it should follow that the Euler system $\{y^{\pm}(S)\}$ of all the Heegner points carries enough information to determine the structure of the Selmer groups $\mathrm{Sel}_{p^M}(E/K)$. The precise result is too technical to state here (cf. [**Ko4**] or [**Mc**]).

These results suggested that one should study the relationship between the Galois module of Heegner points and the arithmetic of E over K (the bridge on the lower left in our diagram) as an interesting question in its own right. This relationship can be formulated as a refined conjecture of Birch Swinnerton-Dyer type whose statement is motivated by the classical Birch Swinnerton-Dyer conjecture, but which avoids any mention of the complex-analytic L-function. The fundamental reference for such refined conjectures is [**MT2**].

The refined conjectures presented in [**MT2**] are a close relative of the p-adic Birch Swinnerton-Dyer conjecture (cf. [**MTT**]), where the $\mathbf{Z}_p$-extension is replaced by a finite (typically, tamely ramified) abelian extension. The analogue of the L-function is constructed using certain integral homology cycles on $E(\mathbf{C})$, the so-called modular symbols. The first section gives a slightly modified and simplified presentation of the conjectures of Mazur and Tate.

In the second section homology cycles are replaced by Heegner points, and a refined conjecture is formulated, of which much has been proved (cf. [**D1**], [**D2**]) thanks to the methods of Kolyvagin.

§2. The Mazur-Tate conjectures.

This section is devoted to an exposition of the conjectures in [**MT2**]. We ignore the extremely interesting phenomena which occur when S is divisible by a prime of multiplicative reduction for E, which are discussed in [**MT2**], leading to some simplification in the exposition. Also, we avoid the introduction of the "regularized determinant" by working with regularized modular symbols instead, which for our purposes seems more natural. Throughout this section, $K = \mathbf{Q}$, and S is a square-free integer prime to N.

§2.1 The Birch Swinnerton-Dyer conjecture. We briefly recall the statement of the classical Birch Swinnerton-Dyer conjecture when $K = \mathbf{Q}$, keeping the same notations as in section 1.3.

CONJECTURE 2.1. *1. θ_S belongs to I^r.*
2. Let $\tilde{\theta}_S$ denote the image of θ_S in I^r/I^{r+1}. Then

$$\tilde{\theta}_S = S^{-1}\gamma_\infty \cdot \#Ш(E/\mathbf{Q})\#J_S R_S.$$

Here γ_∞ denotes the period associated to the real completion of $\mathbf{Q}$ and the Néron differential for E as in section 1.1.

§2.2 The Mazur-Tate regulator. Let $G_S = \mathrm{Gal}(\mathbf{Q}(\mu_S)^+/\mathbf{Q}) = (\mathbf{Z}/S\mathbf{Z})^*/\pm 1$ be the Galois group of the maximal tamely ramified abelian extension of $\mathbf{Q}$ unramified outside S.

In [**MT2**], pp. 731-734, Mazur and Tate define a height pairing

$$\langle\ \rangle_S : E(\mathbf{Q}) \times E_S(\mathbf{Q}) \longrightarrow G_S.$$

Let Z be a subring of $\mathbf{Q}$ in which the order of $E(\mathbf{Q})_{\mathrm{tor}}$ is invertible, and let I_S be the augmentation ideal in the group ring $Z[G_S]$. The map sending σ to $\sigma - 1$ gives a homomorphism of G_S to I_S/I_S^2, and hence we can view the Mazur Tate pairing as taking values in the graded Z-algebra

$$sym(I_S/I_S^2) = \oplus_{r\geq 0} I_S^r/I_S^{r+1}.$$

(The natural convention that $I^0/I = Z$ is used.) Since multiplication by the order of $E(\mathbf{Q})_{\mathrm{tor}}$ induces an isomorphism on I_S/I_S^2, we can define

$$R_S^{\mathrm{MT}} = p(R(E(\mathbf{Q}), E_S(\mathbf{Q}))) \in I_S^r/I_S^{r+1},$$

where the regulator is computed with respect to the Mazur Tate height pairing.

§2.3 The modular symbols and the θ-element. The idea behind the Mazur Tate conjectures is to replace the analytically defined object θ_S by an algebraic object (which we denote by θ_S^{MT}) which plays the role of θ_S. This element belongs to the group ring $Z[G_S]$, and is defined using modular symbols.

§2.3.1 Modular symbols. Let $\Lambda \subset \mathbf{C}$ be the Néron lattice of E, i.e., the set of periods $\int_\gamma \omega$ where γ runs through all the 1-cycles in $H_1(E(\mathbf{C}), \mathbf{Z})$. Let Ω^+ and Ω^- be the largest positive real numbers such that

$$\Lambda \subset \mathbf{Z}\Omega^+ \oplus i\mathbf{Z}\Omega^-.$$

Given a divisor T of S, and $a \in \mathbf{Z}/S\mathbf{Z}$, the modular symbol $[a/T]^+$ is defined by the formula

$$2\pi \int_{a/T}^{a/T+i\infty} \varphi^*\omega = [a/T]^+\Omega^+ + i[a/T]^-\Omega^-.$$

Note that the symbol $[a/T]$ is indeed well defined, depending only on the value of a mod S (in fact, mod T) thanks to the modular invariance of $\varphi^*\omega$. Let T' denote the inverse of S/T modulo T. The regularized modular symbols are defined by the formula

$$[a/S]^* = \sum_{T|S} \mu(S/T)[aT'/T].$$

Given $a \in (\mathbf{Z}/S\mathbf{Z})^*$, let σ_a denote the natural image of a in G_S.

The θ-element is defined by

$$\theta_S^{\mathrm{MT}} = \frac{1}{2} \sum_{a\in(\mathbf{Z}/S\mathbf{Z})^*} [\frac{a}{S}]^* \sigma_a \in \mathbf{Z}[G_S^+].$$

Let l be a prime not dividing S, and let z_l be the canonical map $\mathbf{Z}[G_{Sl}^+] \longrightarrow \mathbf{Z}[G_S^+]$ induced by the projection $G_{Sl} \longrightarrow G_S$. The interest of working with the

regularized θ-elements is that they are compatible under the maps z_l, up to an element in $\mathbf{Z}[G_S^+]$ which has the appearance of an Euler factor at l.

LEMMA 2.2.

$$z_l(\theta_{Sl}^{\mathrm{MT}}) = -\sigma_l(l - \sigma_l^{-1}a_l + \sigma_l^{-2})\theta_S^{\mathrm{MT}}.$$

§2.3.2 Relation between θ_S^{MT} and $L_S(E/\mathbf{Q},1)$. Let χ be an even Dirichlet character of conductor f dividing S, and let $g = S/f$. The twisted L-series

$$L_S(E/\mathbf{Q},\chi,s) = \sum_{(n,S)=1} \chi(n)a_n n^{-s} = \prod_{p\not| S}(1 - \chi(p)a_p p^{-s} + \chi^2(p)p^{1-2s})^{-1}$$

is known to have an analytic continuation to the entire complex plane. Let

$$\chi : \mathbf{Q}[G_S^+] \longrightarrow \mathbf{C}$$

be the ring homomorphism obtained by extending χ by linearity.

PROPOSITION 2.3.

$$\chi(\theta_S^{\mathrm{MT}}) = c(\varphi)g \cdot \frac{\tau(\chi)L_S(E/\mathbf{Q},\bar{\chi},1)}{2\Omega^+},$$

where $\tau(\chi) = \sum_{a=1}^{S}\chi(a)exp(2\pi ia/S)$ is the (slightly modified) Gauss sum.

The element denoted by $\theta_{A,S}$ on p. 716 of [**MT2**] is not the same as our element θ_S^{MT}, but for characters of conductor exactly S, one does have

$$\chi(\theta_S^{\mathrm{MT}}) = \chi(\theta_{A,s}).$$

Thus the result for primitve Dirichlet characters follows from (formula (1), p. 718) of [**MT2**]. In the general case it follows from lemma 2.2.

§2.4 The refined conjecture. With the notations of sections 2.2 and 2.3, Mazur and Tate's conjecture of Birch Swinnerton-Dyer type is analogous to the classical S-integral conjecture 2.1.

CONJECTURE 2.4. *1. θ_S^{MT} belongs to I_S^r.*
2. The image $\tilde{\theta}_S^{\mathrm{MT}}$ of θ_S^{MT} in I_S^r/I_S^{r+1} is given by

$$\tilde{\theta}_S^{\mathrm{MT}} = c(\varphi)\#\underline{Ш}(E/\mathbf{Q})R_S J_S.$$

Remark: The formulation of the conjecture on the leading coefficient differs slightly from the one in [**MT2**], where the θ-element is constructed directly from modular symbols, and the leading coefficient is conjecturally equal to a regularized determinant built up from the Mazur Tate height pairings at level T for all divisors T of S. In fact, the two formulations are equivalent: see the discussion in [**D1**], pp. 37-39.

§3. Heegner points.

We keep the same notations as in section 2, but now we assume that K is an imaginary quadratic field in which all primes dividing N are split so that the Heegner points $y^{\pm}(S)$ over the ring class fields K_S of K are defined (cf. section 1.4). Under the assumptions on K, the sign in the functional equation for $L(E/K, s)$ is -1, and hence this L-function vanishes to odd order at $s = 1$. By the Birch Swinnerton-Dyer conjecture one expects that r is odd; writing $r = r^+ + r^-$, where r^+ and r^- denote the ranks of the plus and minus eignespaces of complex conjugation acting on $E(K)$, one thus expects that $r^+ \neq r^-$ (mod 2).

§3.1 The regulator term. Let $G_S = \mathrm{Gal}(K_S/K)$, and let Z denote a subring of $\mathbf{Q}$ in which $\#E(K)_{\mathrm{tor}}$ is invertible. Let I_S denote the augmentation ideal in the group ring $Z[G_S]$. Consider the Mazur Tate pairing $\langle\ ,\ \rangle_S$ on $E(K) \times E_S(K)$ with values in I_S/I_S^2.

This pairing vanishes when it is restricted to the spaces $E(K)^+ \times E_S(K)^+$ or $E(K)^- \times E_S(K)^-$ (cf [**MT1**], p. 216). Thus when $r^+ \neq r^-$ the regulator term $R(E(K), E_S(K))$ belonging to I_S^r/I_S^{r+1} formed from the pairing $\langle\ ,\ \rangle_S$ is equal to 0. One is thus lead to search for a more sophisticated version of this regulator. Define the extended pairing

$$\langle\ ,\ \rangle_S^{'} : E(K) \times E_S(K) \longrightarrow (I_S/I_S^2) \oplus E(K)^{\otimes 2}$$

$$(P, Q) \mapsto (\langle P, Q\rangle_S, P \otimes Q).$$

We view the group $(I_S/I_S^2) \oplus E(K)^{\otimes 2}$ as the group of homogeneous elements of degree one in the graded algebra

$$sym^{'}(G_S) = \oplus_{r\geq 0}[\ (I_S^r/I_S^{r+1})\ \oplus\ (E(K)^{\otimes 2} \otimes (I_S^{r-1}/I_S^r))\ ].$$

The multiplication on this algebra is defined as follows: if $\alpha = (\alpha_1, \alpha_2)$ and $\beta = (\beta_1, \beta_2)$ are homogeneous elements of degrees r and s respectively (so that

$$\alpha_1 \in I_S^r/I_S^{r+1},\ \alpha_2 \in E(K)^{\otimes 2} \otimes I_S^{r-1}/I_S^r,$$

$$\beta_1 \in I_S^s/I_S^{s+1},\ \beta_2 \in E(K)^{\otimes 2} \otimes I_S^{s-1}/I_S^s),$$

define the product $\alpha \cdot \beta$ as the homogeneous element of degree $r + s$ given by the formula:

$$\alpha \cdot \beta = (\alpha_1\beta_1, \beta_2\alpha_1 + \alpha_2\beta_1).$$

The regulator $R_S^{'}$ is the term $R(E(K), E_S(K))$ associated to this pairing. It is a homogeneous element of degree r. However, if r is odd, then the I_S^r/I_S^{r+1}-component of this regulator term vanishes, and hence

$$R_S^{'} \text{ belongs to } E(K)^{\otimes 2} \otimes (I_S^{r-1}/I_S^r).$$

§3.2 The θ-element. We construct the θ-element $\theta_S^{'}$ from the Heegner points $y^{\pm}(S)$ as follows. Let A_S^+ and A_S^- be the resolvent elements associated to the

Heegner points $y^+(S)$ and $y^-(S)$ respectively,

$$A_S^+ = \sum_{\sigma \in G_S} \sigma y^+(S) \otimes \sigma \in E(K_S) \otimes Z[G_S],$$

$$A_S^- = \sum_{\sigma \in G_S} \sigma y^-(S) \otimes \sigma^{-1} \in E(K_S) \otimes Z[G_S].$$

The element $\theta_S^{'}$ is the tensor (over the ring $Z[G_S]$) of the elements A_S^+ and A_S^-; it belongs to $E(K_S)^{\otimes 2} \otimes Z[G_S]$,

$$\theta_S^{'} = A_S^+ \otimes A_S^- = \sum_{\sigma,\tau \in G_S} \sigma y^+(S) \otimes \tau y^-(S) \otimes (\sigma\tau^{-1}).$$

Let z_l be the natural map from $E(K_{Sl})^{\otimes 2} \otimes Z[G_{S1}]$ to $E(K_{Sl})^{\otimes 2} \otimes Z[G_S]$ induced by the homomorphism $G_{Sl} \longrightarrow G_S$. The following lemma is the analogue of lemma 2.2.

LEMMA 3.1.

$$z_l(\theta_{Sl}^{'}) = \theta_S^{'}(l - a_l + 1)(l + a_l + 1) \text{ if } l \text{ is inert in } K,$$

$$z_l(\theta_{Sl}^{'}) = \theta_S^{'}(l - a_l\sigma_l^{-1} + \sigma_l^{-2})(l - a_l\sigma_l + \sigma_l^{-2}) \text{ if } l \text{ is split in } K.$$

Relation between $\theta_S^{'}$ and $L_S^{'}(E/K, 1)$: Let $h : E(K_S)^{\otimes 2} \longrightarrow \mathbf{R}$ be the canonical Néron-Tate height, and let $\chi : \Gamma_S \longrightarrow \mathbf{C}^*$ be a complex character of Γ_S. As before, we denote by

$$\chi : Z[\Gamma_S] \longrightarrow \mathbf{C}$$

the ring homomorphism obtained by sending $\sigma \in \Gamma_S$ to $\chi(\sigma)$. By combining h and χ one gets a natural linear map:

$$h \otimes \chi : E(K_S)^{\otimes 2} \otimes Z[\Gamma_S] \longrightarrow \mathbf{C}.$$

The following theorem is a restatement of the Gross Zagier formula (theorem 1.2).

THEOREM 3.2. *Suppose that $S = 1$ so that K_S is the Hilbert class field of K. Then*

$$h \otimes \chi(\theta_S^{'}) = c^2 Sh_S \sqrt{D_S} \frac{L_S^{'}(E/K, \chi, 1)}{||\omega||^2}.$$

§3.3 The refined conjecture. The Mazur Tate type conjecture is:

CONJECTURE 3.3. *1. $\theta_S^{'}$ belongs to $E(K_S)^{\otimes 2} \otimes I_S^{r-1}$.*

2. The image $\tilde{\theta}_S^{'}$ of $\theta_S^{'}$ in $E(K_S)^{\otimes 2} \otimes I_S^{r-1}/I_S^r$ belongs to the image of the natural map

$$t : E(K)^{\otimes 2} \otimes I_S^{r-1}/I_S^r \longrightarrow E(K_S)^{\otimes 2} \otimes I_S^{r-1}/I_S^r.$$

3. $\tilde{\theta}_S^{'} = t(c^2 \# \underline{III}(E/K) \# J_S R_S)$.

Unlike conjecture 2.4, much evidence can be given for conjecture 3.3.

Let Z denote a ring in which the following are invertible:

1. The primes 2 and 3.
2. All primes $p < (r-1)/2$.
3. All primes p such that $\mathrm{Gal}(\mathbf{Q}(E_{p^\infty})/\mathbf{Q})$ is not isomorphic to $\mathbf{GL}_2(\mathbf{Z}_p)$.

The methods of Kolyvagin [**Ko1,Ko2,Ko3**] allow one to show:

THEOREM 3.4. *Suppose that S is a product of primes which are inert in K. Then parts 1 and 2 of conjecture 3.3 are true.*

A proof of this result is given in [**D1**] and [**D2**]. In fact, more precise information can be derived about the order of vanishing of $\theta_S^{'}$; cf. [**D2**].

An analogue of conjecture 3.3 can be made for elliptic curves over real quadratic fields, replacing Heegner points by certain geodesic cycles associated to binary quadratic forms of positive discriminant. See the paper [**D3**] where computational data in support of this conjecture is given.

References

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

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

[**D2**] Darmon, H., *A refined conjecture of Mazur-Tate type for Heegner points*, Invent. Math. **110** (1992), 123–146.

[**D3**] Darmon, H., *Heegner points, Heegner cycles, and congruences*, Proceedings of a conference on elliptic curves and related topics, Ste-Adèle, Québec.

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

[**Gr3**] Gross, B.H., *Kolyvagin's work on modular elliptic curves*, Proc. Durham symposium on L-functions and arithmetic, Cambridge University Press, 1991, pp. 235–256.

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

[**Ko1**] Kolyvagin, V.A., *Finiteness of $E(\mathbf{Q})$ and $\underline{III}(E/\mathbf{Q})$ for a subclass of Weil curves*, Izv. Akad. Nauk. SSSR Ser Mat. **52** (1988), 522–540.

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

[**Ko3**] Kolyvagin, V.A., *Euler Systems*, The Grothendick Festschrift II, Progresss in Mathematics 87, Birkhaüser, Boston, Basel, Berlin, 1990, pp. 435–483.

[**Ko4**] Kolyvagin, V.A., *On the structure of Selmer groups*, Math. Annalen **291** (1991), 253–259.

[**Ma1**] Mazur, B., *Courbes elliptiques et symbole modulaire*, LNM 317, Springer-Verlag, Berlin.

[**Ma2**] Mazur, B., *Modular curves and arithmetic*, Proceedings of the International Congress of Mathematicians, Warszawa, 1983.

[**MS**] Mazur, B. and Swinnerton-Dyer, P., *Arithmetic of Weil curves*, Invent. Math. **25** (1974), 1–61.

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

[**MT1**] Mazur, B. and Tate, J., *Canonical height pairings via biextensions*, Arithmetic and Geometry, Volume I, Michael Artin and John Tate, eds., Birkhauser, Boston, pp. 195–238.

[**MT2**] Mazur, B. and Tate, J., *Refined conjectures of the "Birch and Swinnerton-Dyer type"*, Duke Math Journal **54** (1987), 711.

[**Mc**] McCallum, W.G., *Kolyvagin's work on Shafarevich-Tate groups*, Proc. Durham symposium on L-functions and arithmetic, Cambridge University Press, 1991, pp. 295–316.

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

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

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

[**Z**] Zagier, D., *Modular points, modular curves, modular surfaces and modular forms*, Springer Lecture Notes 1111, pp. 225–248.

Department of Mathematics, Princeton University, Princeton, NJ 08544

E-mail address: darmon@math.princeton.edu