Refined class number formulas for derivatives of L-series

A thesis presented

by

Henri Darmon

to

The Mathematics Department
in partial fulfillment of the requirements
for the degree of
Doctor of Philosophy
in the subject of
Mathematics.

Harvard University
Cambridge, Massachusetts

April, 1991

To my parents

Acknowledgements

I wish to thank my advisor, Benedict Gross, for guiding me with a keen mathematical instinct towards the right questions. It has been a great privilege to be his student. I was also fortunate to write this thesis standing on the shoulders of Victor Kolyvagin, Barry Mazur and John Tate. Finally, it was through a joint work with my friend Massimo Bertolini that I was initiated to the work of Kolyvagin. More than anything else, this thesis is an outgrowth of our collaboration.

It is impossible to list all the staff members, fellow students and visitors who have made Harvard a lively and exciting place in which to do mathematics. So many have contributed to the countless hours spent in the common room debating politics, mathematics and the meaning of life over tea and cookies or wine and cheese! I specifically thank Dan Abramovich, Massimo Bertolini, Eric Liverance, and Gordan Savin for their friendship and insights. Donna D'Fini provided valuable moral support through the ups and downs of graduate student life. I am also grateful to J-P. Serre who during two visits to Cambridge spent many hours explaining his ideas to me, in his wonderfully clear and relaxed way.

I owe alot to my undergraduate professors in Montreal, Joachim Lambek and John McKay for introducing me to mathematics and communicating to me early on their enthusiasm for the subject.

Most of all, I want to express my gratitude to my parents for their love and support throughout the years. This thesis is dedicated to them.

"Rien n'est plus fécond, tous les mathématiciens le savent, que ces obscures analogies, ces troubles reflets d'une théorie à une autre, ces furtives caresses, ces brouilleries inexplicables; rien aussi ne donne plus de plaisir au chercheur. Un jour vient où l'illusion se dissipe; le pressentiment se change en certitude; les théories jumelles révèlent leur source commune avant de disparaître; comme l'enseigne la Gītā *on atteint à la connaissance et à l'indifférence en même temps. La métaphysique est devenue mathématique, prête à former la matière d'un traité dont la beauté froide ne saurait plus nous émouvoir. "* André Weil.

Foreword

This thesis is inspired by the metaphysics of class number formulas. The term "metaphysics" is to be taken in the sense in which Weil uses it in his essay [We] on mathematical discovery:

> Les mathématiciens du XIII^e siècle avaient coutume de parler de la "métaphysique du calcul infinitésimal", de la "métaphysique de la théorie des équations". Ils entendaient par là un ensemble d'analogies vagues, difficilement saisissables et difficilement formulables, qui néanmoins leur semblaient jouer un rôle important à un moment donné dans la recherche et la découverte mathématiques.

The questions arising from the analytic class number formula and its conjectural analogue for elliptic curves formulated by Birch and Swinnerton Dyer are still shrouded in mystery. Rich theories have been founded in recent years by replacing the classical L-functions by their p-adic counterparts. This approach was pioneered by Iwasawa [Iw], who formulated what amounts to a p-adic analogue of Dirichlet's class number formula. Later, p-adic analogues of the Birch-Swinnerton Dyer conjectures were formulated and studied by Mazur, Tate and Teitelbaum [MTT].

The p-adic L-functions interpolate special values of the corresponding classical L-functions twisted by characters of Γ, the Galois group of a Z_p-extension. It is natural to attempt to do Iwasawa theory at a finite level in the tamely ramified setting, by replacing the Z_p-extensions by a finite tamely ramified abelian extension. The analogue of the L-function is obtained as the Fourier transform of a distribution on the finite group Γ, or equivalently an element θ in the group ring $C[\Gamma]$. In many cases these elements are known to posess strong integrality properties, and statements involving congruences for their coefficients can be made which are resonant with the class number formulas and Birch and Swinnerton-Dyer conjectures. Such refined Birch and Swinnerton-Dyer conjectures were formulated by Mazur-Tate [MT] in the case of a modular elliptic curve, and an analogue of Dirichlet's class number formula was conjectured and proved in a number of cases by Gross [Gr3].

Since the work of Dirichlet (cf. for example [Wa, p. 37]), one knows that special values of derivatives of L-series associated to even Dirichlet characters can be expressed in terms of logarithms of circular units. The formula of Gross and Zagier [GZ] shows that the Heegner points in the Mordell-Weil group of a modular elliptic curve over the Hilbert class field of an imaginary quadratic field K play a similar role, in interpolating special values of derivatives of the Hasse-Weil L-function $L'(E/K, \chi, 1)$ twisted by unramified characters χ. (A similar result certainly holds with the Hilbert class field replaced by a more general ring class field, and where the characters are allowed to be ramified.)

Using circular units or Heegner points, one can define a θ-element analogous to the one in [MT], as a kind of resolvent element belonging to the tensor product of a group of units or a Mordell-Weil group with the integral group ring of Γ. Using the formalism developed in [MT], one can define a notion of "order of vanishing" and "leading coefficient" for such θ-elements. The metaphysical principle underlying this thesis is the following:

Principle: *The θ-elements define from circular units or Heegner points should behave like the first derivative of the corresponding L-function.*

By using the methods introduced by Kolyvagin, we are able to prove a number of results which are consistent with this general principle.

The first half of this thesis is devoted to the case of circular units and a refined class number formula for real abelian number fields. The second is devoted to the case of Heegner points and the refined Birch Swinnerton-Dyer conjectures. Both parts can be read independantly of one another.

In chapter 1, we recall the results of Dirichlet and Gross' refinement of the class number formula. Sections 1.1 and 1.2 contain nothing new but provide motivation for the main conjectures and theorem which are stated in section

1.3. The proofs are given in chapter 2.

Chapters 3 and 4 are structured along similar lines. The statement of our main conjectures and results concerning Heegner points is contained in section 3.4 with the earlier paragraphs providing the necessary background notations and motivations, including the formalism of the conjectures of Mazur and Tate. Chapter 4 is devoted to the proof of the main theorems stated in section 3.4.

Contents

1 The class number formula **10**

1.1 Dirichlet's analytic class number formula 10

1.2 Gross's refined class number formula 12

1.3 A refined class number formula for derivatives of Dirichlet L-series 14

2 Partial proof of the refined class number formula for circular units **18**

2.1 The Euler system of circular units 18

2.2 Divisibility properties of the circular units 19

2.3 Formal properties of $\theta'(\omega, S)$ 24

2.4 The order of vanishing of $\theta'(\omega, S)$ 25

2.5 The leading coefficient 26

3 The Birch and Swinnerton-Dyer conjecture **31**

3.1 The classical case 31

3.2 Modular elliptic curves 33

3.3 The Mazur-Tate conjectures 35

3.4 A conjecture of Mazur-Tate type for derivatives of L-functions 39

4 Partial proof of the refined Birch and Swinnerton-Dyer conjecture for Heegner points **45**

4.1 The descent formalism 45

4.2 The Euler system of Heegner points 49

4.3 Derivatives in group rings 51

4.4 The Heegner cohomology classes 53

4.5 An application of the Chebotarev density theorem 57

4.6 A vanishing theorem for derivatives of Heegner points 59
4.7 The first non-vanishing derivatives of Heegner points 64
4.8 The order of vanishing of $\theta'(E, S)$ 68
4.9 The leading coefficient 70

Notations and conventions

If K is a number field and w is a place of K lying above a prime v of Q, we denote by K_w the localization of K at w, and let Nw be the order of its residue field. The w-adic norm $|| \, ||_w$ is normalized so that it is equal to Nw^{-1} on uniformizing elements.

Given a finite abelian extension M/K, we let

$$rec_w : K_w^* \longrightarrow \mathrm{Gal}(M/K) \tag{0.1}$$

denote the reciprocity map of local class field theory. When w is unramified in M/K, it factors through the valuation map $K_w^* \longrightarrow Z$ and maps uniformizing elements to $Frob_w$, the Frobenius element in $\mathrm{Gal}(M/K)$ characterized by

$$Frob_w(x) = x^{Nw} \pmod{\tilde{w}}, \tag{0.2}$$

where $\tilde{w}$ is any place of M above w.

We write $Div(K)$ for the free Z-module generated by the places of K, and $P(K)$ for the submodule generated by the principal divisors. The class group $C(K)$ is the quotient $Div(K)/P(K)$ and is known to be finite. Given a set S of places of K, let $\langle S \rangle$ be the Z-span of the elements of S in $Div(K)$, and let

$$C_S(K) = \langle S \rangle \backslash Div(K)/P(K). \tag{0.3}$$

Chapter 1

The class number formula

1.1 Dirichlet's analytic class number formula

We recall briefly the analytic class number formula of Dirichlet relating the behavior of the L-series of a number field at $s = 0$ to the arithmetic properties of that number field. The exposition follows closely the one in [Gr3].

Let K be a number field, and choose a finite set S of places of K containing all of the archimedean places. Let T be a finite set of places of K disjoint from S.

There is associated to this situation the local data which describes the splitting of the primes in K. This data is conveniently encoded in the Euler product

$$L_{S,T}(K, s) = \prod_{v \notin S} (1 - Nv^{-s})^{-1} \prod_{v \in T} (1 - Nv^{1-s}). \tag{1.1}$$

Here the products are taken over the non-archimedean places of K. The Euler product defines the L-function $L_{S,T}(K, s)$ in some right half plane of convergence, and it is known that $L_{S,T}(K, s)$ has a meromorphic continuation to the entire complex plane.

The number field K together with the sets S and T gives rise to more subtle global invariants.

1. The group $(\mathcal{O}_S^*)_T$ of S-units which are congruent to 1 modulo the places of T. This is a finitely generated abelian group which is free when T is large enough. Let r denote the rank of this group. By Dirichlet's unit theorem, one has $r = \#(S) - 1$.

2. The torsion subgroup $[(\mathcal{O}_S^*)_T]_{torsion}$ which is cyclic of order $w_{S,T}$. (Typically we will choose T so that $w_{S,T} = 1$.)

3. The Picard group $Pic(\mathcal{O}_S)_T$ of invertible $\mathcal{O}_S$-modules together with a trivialization at T. It is a finite extension of $C_S(K)$. Let $h_{S,T}$ denote its order.

4. The S-unit regulator $R_{S,T}$, defined as follows. Let $X = Div^0(S)$ be the free abelian group generated by the formal linear combinations of places of S of degree 0,

$$X = \{\textstyle\sum_{v\in S} n_v v, \quad \sum n_v = 0\}.$$

The logarithmic embedding $\log_S : \mathcal{O}_S^* \longrightarrow R \otimes X$ of the S-units is defined by

$$\log_S(u) = \sum_{v\in S} \log ||u||_v \otimes v. \tag{1.2}$$

Both $(\mathcal{O}_S^*)_T$ and X are of rank r. Let

$$\Lambda^r \log_S : \Lambda^r \mathcal{O}_S^* \longrightarrow \Lambda^r(R \otimes X) \tag{1.3}$$

denote the map induced by $\log_S$ on the top exterior powers, and define the regulator $R_{S,T}$ by

$$\Lambda^r \log_S(\gamma_1 \wedge \cdots \wedge \gamma_r) = R_{S,T} \otimes (v_1 \wedge \cdots \wedge v_r), \tag{1.4}$$

where $\gamma_1, \ldots, \gamma_r$ (resp. $v_1, \ldots, v_r$) are integral bases for $(O_S^*)_T$ modulo torsion (resp. X), normalized so that $R_{S,T}$ is positive.

The theorem of Dirichlet asserts that the above global invariants appear in the Taylor expansion of the L-function $L_{S,T}(K,s)$ which was constructed using purely local data. It is one of the simplest manifestations of a local global principle which is pervasive in number theory.

Theorem 1.1.1 (Dirichlet)

1. *The L-series $L_{S,T}(K,s)$ vanishes to order r at $s = 0$.*

2. *The Taylor expansion of $L_{S,T}(K,s)$ at $s = 0$ is given by:*

$$L_{S,T}(K,s) = -\frac{h_{S,T} R_{S,T}}{w_{S,T}} s^r + O(s^{r+1}).$$

1.2 Gross's refined class number formula

We now turn to the refined class number formula of Gross, following closely the account given in [Gr3].

Let L be a finite abelian extension of K which is unramified outside the places of S, and let $G = \mathrm{Gal}(L/K)$. Define a complex-valued function $\hat{\theta}_G$ on the dual group $\hat{G} = \hom(G, C^*)$ by

$$\hat{\theta}_G(\chi) = L_{S,T}(K, \chi, 0), \tag{1.5}$$

where, for a complex character $\chi : G \longrightarrow C^*$ and a complex number s with $\Re s > 1$, the complex function $L_{S,T}(K, \chi, s)$ is defined by the convergent Euler product

$$L_{S,T}(K, \chi, s) = \prod_{v \notin S} (1 - \chi(Frob_v) N v^{-s})^{-1} \prod_{v \in T} (1 - \chi(Frob_v) N v^{1-s}).$$

This function has a meromorphic continuation to the entire complex plane and is regular at $s = 0$. Let $\theta_G \in C[G]$ be the Fourier transform of $\hat{\theta}_G$,

$$\theta_G = \sum_{\chi \in \hat{G}} \hat{\theta}_G(\chi) e_\chi, \qquad e_\chi = 1/|G| \sum_{g \in G} \chi(g) g^{-1}.$$

Thus, $\theta_G = \sum_{g \in G} a(g) g$ interpolates values of $L_{S,T}(K, \chi, 0)$,

$$\sum_{g \in G} a(g) \chi(g) = L_{S,T}(K, \chi, 0). \tag{1.6}$$

For the rest of this section, we make the following assumption on T, which forces $w_{S,T} = 1$ so that the leading term in the class number formula is integral.

Hypothesis 1.2.1 *Suppose that T contains two primes of unequal residue characteristic, or that T contains a prime whose absolute ramification index in K is strictly less that the residue field characteristic minus 1.*

Under this condition, Gross [Gr3] shows that the element θ_G belongs to the integral group ring $Z[G]$.

Fact 1.2.2 (Gross) *θ_G belongs to $Z[G]$.*

The order of vanishing of θ_G: Let I denote the augmentation ideal in the group ring $Z[G]$. It is the kernel of the augmentation homomorphism $\epsilon : Z[G] \longrightarrow Z$ which sends $\sigma \in G$ to 1. The powers $I \supset I^2 \supset \cdots$ define a decreasing filtration on $Z[G]$. Because of the exact sequence

$$0 \longrightarrow I \longrightarrow Z[G] \xrightarrow{\epsilon} Z \longrightarrow 0, \tag{1.7}$$

one has $Z[G]/I = Z$. The higher quotients in the filtration are torsion. For instance, there is a natural homomorphism $G \longrightarrow I/I^2$ which sends $\sigma \in G$ to $\sigma - 1 \pmod{I^2}$. In fact, this is an isomorphism. More generally, there is a natural surjective map

$$Sym^r(G) \longrightarrow I^r/I^{r+1} \tag{1.8}$$

which sends $\sigma_1 \otimes \cdots \otimes \sigma_r$ to $(\sigma_1 - 1)\cdots(\sigma_r - 1) \pmod{I^{r+1}}$. (This map is not necessarily an isomorphism; for a detailed study of the map $Sym(G) \longrightarrow \oplus_r I^r/I^{r+1}$, the reader may consult [Pa], [H1], [H2].)

The element θ_G which interpolates special values at $s = 0$ of the twisted L-function $L_{S,T}(K, \chi, s)$ is what plays the role of the L-function in Gross's refined class number formula. To say that this element vanishes to order r is to say that it belongs to the r-th power of the augmentation ideal.

Conjecture 1.2.3 (Gross) *The element θ_G belongs to I^r.*

The leading coefficient $\tilde{\theta}_G$ in the refined class number formula is defined to be the projection of θ_G to I^r/I^{r+1}. It is natural to search for an interpretation of $\tilde{\theta}_G$ which is analogous to the analytic result of Dirichlet.

To do this, it suffices to change the definition of the regulator term $R_{S,T}$ defined in the previous section. Consider the homomorphism

$$rec_S : \mathcal{O}_S^* \longrightarrow (I/I^2) \otimes_Z X \tag{1.9}$$

defined by

$$rec_S(u) = \sum_{v \in S} (rec_v(u_v) - 1) \otimes v, \tag{1.10}$$

where $u_v \in K_v^*$ is the natural image of u. Let $\Lambda^r rec_S$ denote the induced map on the top exterior powers:

$$\Lambda^r rec_S : \Lambda^r \mathcal{O}_S^* \longrightarrow \Lambda^r(I/I^2 \otimes X) \longrightarrow (I^r/I^{r+1}) \otimes \Lambda^r X,$$

and define the regulator $R_{S,T}$ in I^r/I^{r+1} by

$$\Lambda^r rec_S(\gamma_1 \wedge \cdots \wedge \gamma_r) = R_{S,T} \otimes (v_1 \wedge \cdots \wedge v_r), \tag{1.11}$$

where $\gamma_1, \ldots, \gamma_r$ and $v_1, \ldots, v_r$ are the integral bases chosen in section 1.1.

Conjecture 1.2.4 (Gross)

$$\tilde{\theta}_G = -h_{S,T} R_{S,T}.$$

Remarks:
1. If K has a complex place v, then the Γ-factors in the functional equation force a zero at $s=0$ in the twisted L-function $L_{S,T}(K,\chi,s)$ for all χ. Hence $\theta_G = 0$. But rec_v is trivial, so that $R_{S,T} = 0$ as well. Therefore the conjecture is trivially verified. It is only interesting when K is a totally real field.
2. Because of the presence of the archimedean places, one has $2R_{S,T} = 0$ in I^r/I^{r+1}. (Also one can show that $2\tilde{\theta}_G = 0$.) Thus Gross's conjecture for number fields is really a parity statement – it was proved by Gross when S contains only the archimedean places by using the 2-adic congruences of Deligne-Ribet for totally real fields [DR].

1.3 A refined class number formula for derivatives of Dirichlet L-series

Let ω be an even primitive Dirichlet character of conductor N. In order to simplify the exposition, we assume that ω is quadratic, and let K denote the corresponding real quadratic field. Choose an auxiliary real abelian extension M of Q with conductor prime to N, and let G denote its Galois group. For all χ in $\hat{G}$, the Dirichlet L-series

$$L_S(s,\omega\chi) = \sum_{(n,S)=1}^{\infty} \omega\chi(n) n^{-s} = \prod_{p \not| S} (1 - \omega\chi(p)p^{-s})^{-1} \tag{1.12}$$

vanishes at $s=0$, because of the pole in the factor $\Gamma(\frac{1}{2}s)$ in the functional equation. One might be tempted to define a function $\hat{\theta}'_G$ on $\hat{G}$ by $\hat{\theta}'_G(\chi) = L'_S(0,\omega\chi)$, and letting $\theta'_G \in C[G]$ be its Fourier transform as in section 1.2. However, the coefficients of θ'_G are not integral, or even algebraic. This leads to the problem of finding an appropriate substitute for θ'_G, and formulating a conjecture analagous to conjectures 1.2.3 and 1.2.4 for it.

Fix a choice of primitive nth roots of unity $\zeta_n \in \bar{Q}$ for each n, satisfying the compatibilities

$$\zeta_{nm}^m = \zeta_n. \tag{1.13}$$

This choice determines a complex embedding Ψ of Q^{ab}, sending ζ_n to $e^{2\pi i/n}$.

Let S be a square-free integer which is relatively prime to the conductor of ω. Let $K_S = K(\mu_S)$. The circular unit α_S in K_S is defined by

$$\alpha_S = \prod_{\sigma \in \mathrm{Gal}(Q(\mu_{SN})/Q(\mu_S))} \sigma(\zeta_{NS} - 1)^{\omega(\sigma)}. \tag{1.14}$$

Let $\Gamma_S = \mathrm{Gal}(K_S/K)$, and let I denote the augmentation ideal in the group ring $Z[\Gamma_S]$. The theta-element $\theta'(\omega, S)$ is given by the formula

$$\theta'(\omega, S) = \sum_{\sigma \in \Gamma_S} \sigma\alpha_S \otimes \sigma \quad \in K_S^* \otimes Z[\Gamma_S]. \tag{1.15}$$

Relation between θ'_S and $L'_S(0, \omega\chi)$: Let $\log : K_S^* \longrightarrow C$ be a principal branch of the logarithm map induced by the complex embedding Ψ of K_S. Extending a character $\chi \in \hat{\Gamma}_S$ by linearity to the group ring $Z[\Gamma_S]$, one combines the maps log and χ to give a linear map

$$\log \otimes \chi : K_S^* \otimes Z[\Gamma_S] \longrightarrow C.$$

The following theorem which describes the interpolation property of the circular units is due to Kummer.

Theorem 1.3.1 *Assume that χ is primitive. Then*

$$\log \otimes \chi(\theta'(\omega, S)) = \sum_{\sigma \in \Gamma_S} \chi(\sigma) \log |\sigma\alpha_S| = -2L'_S(0, \omega\chi).$$

Thus $\theta'(\omega, S)$ can be viewed as an analogue of $L'_S(s, \omega)$.

Let

$$\begin{aligned} S_{split} &= \{l | S, \quad \omega(l) = 1\} \\ S_{inert} &= \{l | S, \quad \omega(l) = -1\}. \end{aligned}$$

Let X^- be the group of divisors of K of degree 0 lying above S or ∞ on which $\mathrm{Gal}(\bar{Q}/Q)$ acts via the character ω. It is a free Z-module of rank r, where

$$r = \#(S_{split}) + 1. \qquad (1.16)$$

Let $v_\infty = \lambda_\infty - \bar{\lambda}_\infty$ be the difference of the two conjugate real places of K, and let $v_i = \lambda_i - \bar{\lambda}_i$, where $\lambda_i, \bar{\lambda}_i$ denote conjugate primes of K lying above $l_i \in S_{split}$. Then $\{v_\infty, v_1, \ldots, v_{r-1}\}$ forms a basis for X^-.

Let $(\mathcal{O}_S^*)^-$ be the group of S-units of K on which $\mathrm{Gal}(\bar{Q}/Q)$ acts via the character ω. This is also a free Z-module of rank r. Choose a basis $\omega_1, \ldots, \omega_r$ for $(\mathcal{O}_S^*)^-$ in such a way that the regulator R_S for the logarithmic embedding

$$(\mathcal{O}_S^*)^- \longrightarrow X^- \otimes R \qquad (1.17)$$

relative to the bases $\{\omega_1, \ldots, \omega_r\}$ and $\{v_\infty, v_1, \ldots, v_{r-1}\}$ is positive.

¿From the non-vanishing of the classical Dirichlet L-series at $s = 1$ combined with the functional equation for these L-series, one knows that

$$ord_{s=0} L_S'(s, \omega) = r - 1, \qquad (1.18)$$

and that

$$\lim_{s \to 0} L_S'(s, \omega)/(s^{r-1}) = -2^{\#S_{inert}+1} r h_S R_S. \qquad (1.19)$$

In the next section, we will show that a similar statement is true for the element $\theta'(\omega, S)$:

Theorem 1.3.2 (Order of vanishing) *The element $\theta'(\omega, S)$ belongs to the group $K_S^* \otimes I^{r-1}$.*

The leading coefficient $\tilde{\theta}'(\omega, S)$ is defined to be the natural projection of $\theta'(\omega, S)$ to the group $K_S^* \otimes (I^{r-1}/I^r)$. One can interpret $\theta'(\omega, S)$ by means of a kind of S-unit regulator belonging to $\mathcal{O}_S^* \otimes (I^{r-1}/I^r)$.

The regulator: Let Y^- denote the group of divisors of K of degree 0 lying above S on which $\mathrm{Gal}(\bar{Q}/Q)$ acts via the character ω. This is a free module of rank $r - 1$ with basis $\{v_1, \ldots, v_{r-1}\}$. One defines the map

$$rec_S : (\mathcal{O}_S^*)^- \longrightarrow I_S \otimes Y^- \qquad (1.20)$$

using the reciprocity law of local class field theory as in section 1.2. Define the *partial regulators* $R_i \in I_S^{r-1}/I_S^r$ by the formula

$$rec_S(\gamma_1 \wedge \cdots \wedge \gamma_{i-1} \wedge \gamma_{i+1} \wedge \cdots \wedge \gamma_r) = R_i \otimes (v_1 \wedge \cdots \wedge v_{r-1}). \qquad (1.21)$$

The regulator $R_S \in \mathcal{O}_S^* \otimes (I^{r-1}/I^r)$ is given by

$$R_S = \sum_{i=1}^{r} (-1)^{i+1} \gamma_i \otimes R_i. \tag{1.22}$$

Conjecture 1.3.3

$$\tilde{\theta}'(\omega, S) = -2^{\#(S_{inert})+1} h_S R_S.$$

This conjecture implies the induction formulas obtained by Thaine and Kolyvagin for circular units, but seems to be stronger.

We now give some evidence for conjecture 1.3.3. Let $\tilde{\theta}'(\omega, S)_2$ denote the projection of $\tilde{\theta}'(\omega, S)$ in the group $K_S^* \otimes (I_2^{r-1}/I_2^r)$, where I_2 denotes the augmentation ideal in the group ring $Z[\frac{1}{2}][\Gamma_S]$. The tensoring with the ring $Z[\frac{1}{2}]$ has been made to avoid some technical complications associated with the prime 2: observe that $(I_2^{r-1}/I_2^r) = (I^{r-1}/I^r) \otimes Z[\frac{1}{2}]$ is a finite abelian group of odd order, when $r > 1$.

Fact 1.3.4 *The natural map $K^* \otimes (I_2^{r-1}/I_2^r) \longrightarrow K_S^* \otimes (I_2^{r-1}/I_2^r)$ is an injection.*

The proof for this standard fact will be given in section 2.5.

Let $n(S)$ be the greatest odd divisor of $\gcd_{l|S}(l-1)$. The following theorem gives some evidence for conjecture 1.3.3:

Theorem 1.3.5 .

1. *Conjecture 1.3.3 is true when $r = 1$.*
2. *$\tilde{\theta}'(\omega, S)_2$ belongs to $K^* \otimes I_2^{r-1}/I_2^r$.*
3. *If $\gcd(h_S(K), n(T)) = 1$ for all $T|S$, then $\tilde{\theta}'(\omega, S)_2$ belongs to $\mathcal{O}_s^* \otimes (I_2^{r-1}/I_2^r)$.*
4. *$h_S(K)$ divides $\tilde{\theta}'(\omega, S)_2$.*
5. *Suppose that $\Gamma_S = \Gamma_l$ is cyclic, and that l is split in K/Q so that $r = 2$. Let λ be a prime of K above l, and let $k_\lambda \simeq F_l$ denote the residue field at λ. If the fundamental unit of K/Q is a generator for k_λ^*, and $\gcd(h(K), n(l)) = 1$, then*
$$\tilde{\theta}'(\omega, l)_2 = \pm 2 h_l R_l \pmod{I_2^2}.$$

The proof of this theorem will be given in section 2.5.

Chapter 2

Partial proof of the refined class number formula for circular units

2.1 The Euler system of circular units

Let $\mathcal{S}$ be the set of square-free integers prime to the conductor of K. For all $S \in \mathcal{S}$ we are given the following data:

1. An abelian extension $K_S = K(\mu_S)$ of K with Galois group $\Gamma_S = (Z/SZ)^*$.

2. The circular unit $\alpha(S)$ in K_S, given by the formula

$$\alpha(S) = \prod_{\sigma \in \mathrm{Gal}(Q(\zeta_{SN})/Q(\zeta_S))} \sigma(\zeta_{SN} - 1)^{\omega(\sigma)}. \tag{2.1}$$

Writing $S = l_1 \cdots l_s$, the extension K_S is a compositum of the fields K_{l_i} which are linearly disjoint over K. Hence there is a canonical direct product decomposition

$$\Gamma_S = \Gamma_{l_1} \times \cdots \times \Gamma_{l_s} \tag{2.2}$$

which gives inclusions $\Gamma_T \subset \Gamma_S$ for all divisors T of S. We will implicitly identify elements of Γ_T with their images in Γ_S. For any T dividing S, the partial norm operator N_T in the group ring $Z[\Gamma_S]$ is defined by

$$N_T = \sum_{\sigma \in \Gamma_T} \sigma. \tag{2.3}$$

These operators act on the field K_S in the natural way. Given $T \in \mathcal{S}$ and l a prime in $\mathcal{S}$ which is prime to T, let $\sigma_{l,T} \in \mathrm{Gal}(K_T/Q)$ be the automorphism sending the roots of unity to their lth powers.

Proposition 2.1.1

$$N_l(\alpha(Tl)) = (1 - \sigma_{l,T}^{-1})\alpha(T).$$

Proof: We can write

$$\zeta_{Tl} = \zeta_T^a \zeta_l^b, \tag{2.4}$$

where $al + bT = 1$. Hence

$$N_l(1 - \zeta_{Tl}) = (1 - \zeta_T^{al})/(1 - \zeta_T^a) = (1 - \sigma_{l,T}^{-1})(1 - \zeta_T),$$

and the proposition follows from the definition of the circular units $\alpha(T)$ and $\alpha(Tl)$.

Proposition 2.1.2 $\alpha(Tl) \equiv \sigma_{l,T}^{-1}\alpha(T) \pmod{\lambda}$, *where* λ *is any prime of* K_{Tl} *above* l.

Proof: This follows from equation (2.4) together with the fact that a is an inverse for l in $(Z/TZ)^*$ and that $\zeta_l \equiv 1 \pmod{\lambda}$.

Propositions 2.1.1 and 2.1.2 make up the axioms of an Euler system in the sense of Kolyvagin [Ko3].

2.2 Divisibility properties of the circular units

In addition to the norm operator N_l defined in the previous section, the following derivative operators in the group ring $Z[\Gamma_S]$ are a key ingredient in Kolyvagin's method. For each prime l in $\mathcal{S}$, choose a generator γ_l for Γ_l and let

$$\mathrm{D}_l = \sum_{i=1}^{l-2} i\gamma_l^i, \quad \mathrm{D}_T = \prod_{l|T} \mathrm{D}_l, \tag{2.5}$$

the product being taken in the group ring $Z[\Gamma_T]$.

Lemma 2.2.1 $(\gamma_l - 1)D_l = (l-1) - N_l$.

Proof: A direct computation.

The group ring $Z[\Gamma_T]$ operates on the group K_T^* in a natural way. Let

$$\beta(T) = \mathrm{D}_T\alpha(T) \in K_T^*, \tag{2.6}$$

and let $n(T)$ be the largest odd divisor of $\gcd_{l|T}(l-1)$.

¿From now on, we will assume that T is a product of primes which are split in K/Q. Although $\beta(T)$, unlike $N_T\alpha(T)$, need not be invariant under the action of Γ_T, it is invariant modulo $n(T)$-th powers.

Lemma 2.2.2 *$\beta(T)$ belongs to $(K_T^*/K_T^{*n(T)})^{\Gamma_T}$.*

Proof: By induction on the number of primes dividing T. Assume the lemma for all proper divisors of T, and write $T = lQ$. Modulo $n(T)$, one has:

$$\begin{aligned} (\gamma_l - 1)\mathrm{D}_T\alpha(T) &= (l-1-N_l)\mathrm{D}_Q\alpha(T) \quad \text{(lemma 2.2.1)} \\ &= (\sigma_{l,Q}^{-1} - 1)\mathrm{D}_Q\alpha(Q) \quad \text{(prop. 2.1.1)} \\ &= 0 \quad \text{by the induction hypothesis.} \end{aligned}$$

In the last step we use the fact that $\sigma_{l,Q} = 1$ in $\mathrm{Gal}(K/Q)$, so that $\sigma_{l,Q}$ belongs to Γ_Q.

Lemma 2.2.3 *The natural map $K^*/K^{*n(T)} \longrightarrow (K_T^*/K_T^{*n(T)})^{\Gamma_T}$ is an isomorphism.*

Proof: The group of $n(T)$-th roots of unity in K_T is trivial. Hence the sequence

$$1 \longrightarrow K_T^* \xrightarrow{n(T)} K_T^* \longrightarrow K_T^*/K_T^{*n_T} \longrightarrow 1 \tag{2.7}$$

is exact. Taking Γ_T-invariants gives rise to the cohomology exact sequence

$$1 \longrightarrow K^*/K^{*n(T)} \longrightarrow (K_T^*/K_T^{*n(T)})^{\Gamma_T} \longrightarrow H^1(\Gamma_T, K_T^*)_{n(T)} \longrightarrow 1, \tag{2.8}$$

and the lemma follows from Hilbert's theorem 90 ($H^1(\Gamma_T, K_T^*) = 0$).

Let $\kappa(T)$ denote the preimage of $\beta(T)$ by this isomorphism. For each prime l in $\mathcal{S}$, choose a place λ of K above it. Write

$$v_\lambda : K^* \longrightarrow Z \tag{2.9}$$

for the valuation map at λ, and $\tilde{v}_\lambda$ for the induced map on $K^*/K^{*n(T)}$, making the following diagram commute:

$$\begin{array}{ccc} K^* & \xrightarrow{v_\lambda} & Z \\ \downarrow & & \downarrow \\ K^*/K^{*n(T)} & \xrightarrow{\tilde{v}_\lambda} & Z/n(t)Z \end{array}$$

Let u_l denote the image of γ_l by the isomorphism $\Gamma_l \longrightarrow (Z/lZ)^*$. Given κ in K^*, let $red_\lambda(\kappa) \in k_\lambda^*$ be the reduction of κ mod λ, in the residue field $k_\lambda = Z/lZ$. Finally, let

$$\log_{u_l} : k_\lambda^* \longrightarrow Z/(l-1)Z \tag{2.10}$$

be the logarithm map to the base u_l. The following proposition contains the information that we will need on the ideal factorization of the $\kappa(T)$.

Proposition 2.2.4 .

1. *If l does not divide T, then $\tilde{v}_\lambda(\kappa(T)) = 0$.*
2. *If l is split in K_T/Q, then*

$$\tilde{v}_\lambda(\kappa(Tl)) = -\log_{u_l}(red_\lambda(\kappa(T))) \pmod{n(Tl)}.$$

Proof:
1. If l does not divide T, then λ is unramified in K_T/K, and hence the valuation map $\tilde{v}_\lambda$ extends from $K^*/K^{*n(T)}$ to $K_T^*/K_T^{*n(T)}$. But clearly $\tilde{v}_\lambda(\beta(T)) = 0$, since $\beta(T)$ is a unit in K_T^*.
2. Let λ' be a prime of K_T above λ, and let λ'' be the prime of K_{Tl} above λ'. Let $v_{\lambda'}$ (resp. $v_{\lambda''}$) be the valuations on K_T (resp K_{Tl}) normalized to be 1 on uniformizing elements, so that

$$v_{\lambda'}(\kappa) = \frac{1}{l-1} v_{\lambda''}(\kappa), \quad \kappa \in K_T^*. \tag{2.11}$$

Writing

$$\kappa(Tl) = \beta(Tl)\rho^{-n(Tl)}, \quad \rho \in K_{Tl}, \tag{2.12}$$

and using the fact that $\beta(Tl)$ is a unit, one finds

$$v_\lambda(\kappa(Tl)) = -\frac{n(Tl)}{l-1} v_{\lambda''}(\rho). \tag{2.13}$$

By definition of u_l, one has

$$v_{\lambda''}(\rho) = \log_{u_l}(red_{\lambda''}((\gamma_l - 1)\rho)) \pmod{l-1}. \tag{2.14}$$

But

$$\begin{aligned}
(\gamma_l - 1)\rho &= \frac{1}{n(Tl)}[(\gamma_l - 1)\beta(Tl)] \\
&= \frac{1}{n(Tl)}[(l-1)\mathrm{D}_T\alpha(Tl) + (1 - \sigma_{l,T}^{-1})\mathrm{D}_T\alpha(T)] \\
&= \frac{l-1}{n(Tl)}\mathrm{D}_T\alpha(Tl), \quad \text{since} \ \ \sigma_{l,T} = 1.
\end{aligned}$$

Hence by prop. 2.1.2,

$$red_{\lambda''}((\gamma_l - 1)\rho) = red_{\lambda'}\left(\frac{l-1}{n(Tl)}\mathrm{D}_T\alpha(T)\right), \tag{2.15}$$

and hence

$$\log_{u_l} red_{\lambda''}((\gamma_l - 1)\rho) \equiv \log_{u_l} red_{\lambda'}\left(\frac{(l-1)}{n(Tl)}\beta(T)\right) \pmod{l-1}. \tag{2.16}$$

Combining equations (2.13), (2.14) and (2.16), one obtains

$$\tilde{v}_\lambda(\kappa(Tl)) \equiv -\log_{u_l}(red_\lambda \kappa(T)) \pmod{n(Tl)} \tag{2.17}$$

as desired.

If M is a Z-module and m belongs to M, we say that $n \in Z$ divides m if there exists $m' \in M$ with $n \cdot m' = m$. Given a rational prime p, one defines $ord_p(m)$ to be the integer M such that p^M divides m, but p^{M+1} does not. (If this integer does not exist one sets $ord_p(m) = \infty$.) Recall that $C_S(K)$ is defined to be the quotient of the ideal class group of K by the subgroup generated by the prime ideals lying above S, and that $h_S(K)$ denotes its order. The main result of Thaine and Kolyvagin gives a bound on the order of $C_S(K)$ in terms of the divisibilty of the elements $\kappa(S)$.

Theorem 2.2.5 (Thaine, Kolyvagin) *The greatest common divisor of* $n(S)$ *and* $h_S(K)$ *divides* $\kappa(S)$.

Proof: We prove this by induction on $h_S(K)$. If $h_S(K) = 1$, then the theorem is trivially true. Otherwise, choose a prime p dividing $h_S(K)$. Suppose that $ord_p(\kappa(S)) = M_0 < \infty$, and let $M = M_0 + 1$. We must whow that p^M does not divide $\gcd(n(S), h_S(K))$. If p^M does not divide $n(S)$, we are done. Hence, suppose that p^M divides $n(S)$. (So that in particular, p is odd). Now, choose a prime l in $\mathcal{S}$ not dividing S, such that

1. l splits in K/Q; let λ denote a prime of K lying above it.
2. $l \equiv 1 \pmod{P^M}$ (i.e., l splits in $Q(\mu_{p^M})/Q$).
3. $ord_p(red_\lambda(\kappa(S))) = M_0$.
4. The image of λ in $C_S(K) \otimes Z_p$ is non trivial, and the exact sequence
$$0 \longrightarrow \langle\lambda\rangle \longrightarrow C_S(K) \otimes Z_p \longrightarrow C_{Sl}(K) \otimes Z_p \longrightarrow 0$$
is split (and hence in particular $ord_p(\lambda) = 0$).

Let $F = K(\mu_{p^M}, \kappa(S)^{1/p^M})$. Conditions 2 and 3 are equivalent to the condition that $Frob_\lambda$ in $\mathrm{Gal}(F/K)$ belongs to the subgroup $\mathrm{Gal}(F/K(\mu_{p^M}))$ and is non-trivial. Condition 4 is equivalent to a condition on $Frob_\lambda$ in $\mathrm{Gal}(H_S/K)$ where H_S is a non-trivial subfield of the Hilbert class field H of K. Since F and H are linearly disjoint over K (as can be seen for example by ramification considerations), it follows from the Chebotarev density theorem that conditions 1-4 can be imposed simultaneously.

Let $m = ord_p(\kappa(Sl))$. By combining proposition 2.2.4 with condition 3 satisfied by l, one has
$$ord_p(\tilde{v}_\lambda(\kappa(Sl))) = M_0, \tag{2.18}$$
and hence a fortiori $m \leq M_0$. Moreover, since p^M divides $l-1$, it also divides $n(Sl)$. Let ρ be the natural projection of $\kappa(Sl)$ to K^*/K^{*p^M}, and let $\kappa'(Sl) = \rho^{1/p^m}$ which is well defined in $K^*/K^{*p^{M-m}}$. By equation 2.18 and condition 3, one has
$$\tilde{v}_\lambda(\kappa'(Sl)) = u \cdot p^{M_0 - m}, \tag{2.19}$$

where u is a unit in $Z/p^{M-m}Z$. Hence p^{M_0-m} annihilates the class of λ in $C(S)\otimes Z/p^{M-m}Z$. Because of condition 4, we have

$$\#\langle\lambda\rangle \leq p^{M_0-m}. \tag{2.20}$$

In particular, $m < M_0$, and by the induction hypothesis,

$$\#C_{Sl}(K)\otimes Z_p \leq p^m. \tag{2.21}$$

Combining the inequalities (2.20) and (2.21) gives

$$\#C_S(K)\otimes Z_p \leq p^{M_0}, \tag{2.22}$$

so that p^M does not divide $h_S(K)$, as was to be shown.

2.3 Formal properties of $\theta'(\omega, S)$

We now turn to the study of the element $\theta'(\omega, S)$ defined by

$$\theta'(\omega, S) = \sum_{\sigma\in\Gamma_S} \sigma\alpha(S)\otimes\sigma \in K_S^*\otimes Z[\Gamma_S]. \tag{2.23}$$

Given

$$\gamma \in \mathrm{Gal}(K_S/Q) = \Gamma_S \times \mathrm{Gal}(K/Q),$$

let $\gamma(T)$ denote its natural projection in Γ_T.

The group $\mathrm{Gal}(K_S/Q)$ acts on the left of $K_S^*\otimes Z[\Gamma_S]$ by the Galois action, and Γ_S acts on the right by multiplication in the group ring.

Lemma 2.3.1 $\gamma\theta'(\omega, S) = \omega(\gamma)\cdot\theta'(\omega, S)\cdot\gamma(S)^{-1}$.

Proof: A change of variable argument.

Given a divisor T of S, let $P_{S,T} : K_S^*\otimes Z[\Gamma_S] \longrightarrow K_S^*\otimes Z[\Gamma_S]$ be the map induced by the projection $\Gamma_S \longrightarrow \Gamma_T \subset \Gamma_S$.

Lemma 2.3.2

$$P_{S,T}(\theta'(\omega, S)) = \theta'(\omega, T)\cdot\prod_{l|S/T}(1-\omega(l)\cdot\sigma_{l,T}).$$

Proof: One has

$$P_{S,T}(\theta'(\omega,S)) = \sum_{\sigma\in\Gamma_T} \left(N_{S/T}\cdot\sigma\alpha_S\otimes\sigma\right). \tag{2.24}$$

Hence by proposition 2.1.1

$$P_{S,T}(\theta'(\omega,S)) = \left(\prod_{l|S/T}(1-\sigma_{l,T}^{-1})\right)\theta'(\omega,T), \tag{2.25}$$

which is equal to $\theta'(\omega,T)\cdot\prod(1-\omega(l)\sigma_{l,T})$ by lemma 2.3.1.

2.4 The order of vanishing of $\theta'(\omega,S)$

Let us write S as $S=PQ$, where $P=l_1\cdots l_s$ is a product of split primes in K/Q, and Q is a product of inert primes. When σ runs over Γ_S, write

$$\sigma=\sigma_1\cdots\sigma_s\tau, \tag{2.26}$$

for its unique decomposition as a product with $\sigma_i\in\Gamma_{l_i}$, and $\tau\in\Gamma_Q$.

Lemma 2.4.1

$$\begin{aligned}\theta'(\omega,S) &= \sum_{\sigma\in\Gamma_S}\sigma\alpha_S(\sigma_1-1)\cdots(\sigma_s-1)\tau \\ &\quad -\sum_{T|P,T\neq P}\left(\mu(P/T)\cdot\theta'(\omega,TQ)\cdot\prod_{l|P/T}(1-\sigma_{l,TQ})\right).\end{aligned}$$

Proof: By direct computation,

$$\sum_{\sigma\in\Gamma_S}\sigma\alpha_S(\sigma_1-1)\cdots(\sigma_s-1)\tau = \theta'(\omega,S)+\sum_{T|,T\neq P}\mu(P/T)P_{S,TQ}(\theta'(\omega,S)). \tag{2.27}$$

The formula now follows from lemma 2.3.2.

We are now ready to prove the theorem 1.3.2 of chapter 1.

Theorem 1.3.2 (Order of vanishing) *The element $\theta'(\omega,S)$ belongs to $K_S^*\otimes I^s=K_S^*\otimes I^{r-1}$.*

Proof: By induction on s, using lemma 2.4.1 for the induction step.

2.5 The leading coefficient

We now turn to the study of the element $\tilde{\theta}'(\omega, S)$ defined by projecting $\theta'(\omega, S)$ to the value group $K_S^* \otimes (I_2^{r-1}/I_2^r)$.

Lemma 2.5.1 *The leading coefficient $\tilde{\theta}'(\omega, S)_2$ belongs to the subgroup of elements in $(K_S^* \otimes (I_2^{r-1}/I_2^r))^{\Gamma_S}$ fixed by the left (Galois) action of Γ_S.*

Proof: Given σ in Γ_S, by lemma 2.3.1 we have

$$(\sigma - 1)\tilde{\theta}'(\omega, S)_2 = \tilde{\theta}'(\omega, S)_2(\sigma^{-1} - 1), \tag{2.28}$$

and lemma 2.5.1 follows.

Lemma 2.5.2 *Let Γ be a finite abelian group of odd order, and let Γ_S act on the module $K_S^* \otimes \Gamma$ by the Galois action. Then the natural map*

$$K^* \otimes \Gamma \longrightarrow (K_S^* \otimes \Gamma)^{\Gamma_S}$$

is an isomorphism.

Proof: By decomposing Γ as a direct product of cyclic groups, one reduces the proof of lemma 2.5.2 to the case where Γ is cyclic of odd order n. If K_S contains no n-th roots of unity, then we are in the situation of lemma 2.2.3. In general, one uses the fact that the restriction map

$$H^1(K, \mu_n) \longrightarrow H^1(K_S, \mu_n)^{\Gamma_S} \tag{2.29}$$

is an isomorphism.

Lemma 2.5.3 $n(S)(\gamma_{l_1} - 1) \cdots (\gamma_{l_s} - 1) = 0 \pmod{I_2^r}$.

Proof: We can write $(\gamma_{l_1} - 1) \cdots (\gamma_{l_s} - 1)$ as a sum of terms of the form $(\gamma_{l_1}^{(p)} - 1) \cdots (\gamma_{l_s}^{(p)} - 1) \pmod{I_2^r}$, where the $\gamma_{l_i}^{(p)}$ are of order a power of p (p an odd prime) and at least one of the $\gamma_{l_j}^{(p)}$ is of order exactly $q = p^{ord_p(n(S))}$. Hence it suffices to show the theorem when $n(S) = q$ is a power of a prime. In that case, one has

$$0 = \gamma_{l_j}^q - 1 = \sum_{i=1}^{q} \binom{q}{i} (\gamma_{l_j} - 1)^i,$$

so that $q(\gamma_{l_j}-1)\in I_2^2$. The result follows.

The following proposition gives an inductive formula for the leading coefficient $\tilde{\theta}'(\omega,S)_2$.

Proposition 2.5.4 .

$$\begin{aligned}\tilde{\theta}'(\omega,S)_2 &= 2^{\#(l|Q)}\kappa(P)\otimes(\gamma_{l_1}-1)\cdots(\gamma_{l_s}-1)\\ &\quad -\sum_{T|P,T\neq P}\mu(P/T)\cdot\tilde{\theta}'(\omega,T)\cdot\prod(1-\sigma_{l,T}).\end{aligned}$$

Proof: This follows from lemma 2.4.1 together with the fact that

$$\sum_{\sigma\in\Gamma_S}\sigma\alpha_S\otimes(\sigma_1-1)\cdots(\sigma_s-1)\tau = 2^{\#(l|Q)}\beta(P)\otimes(\gamma_{l_1}-1)\cdots(\gamma_{l_s}-1) \quad (2.30)$$

in $K_S^*\otimes(I^{r-1}/I^r)$. Because $(\gamma_{l_1}-1)\cdots(\gamma_{l_s}-1)$ is killed by $n(P)$ in I_2^{r-1}/I_2^r (lemma 2.5.3), one can replace $\beta(P)$ by $\kappa(P)$ in the formula.

In the remainder of this section we will prove theorem 1.3.5 which we first recall:

Theorem 1.3.5

1. *Conjecture 1.3.3 is true when $r=1$.*
2. *$\tilde{\theta}'(\omega,S)_2$ belongs to $K^*\otimes I_2^{r-1}/I_2^r$.*
3. *If $\gcd(h_S(K),n(T))=1$ for all $T|S$, then $\tilde{\theta}'(\omega,S)_2$ belongs to $\mathcal{O}_s^*\otimes(I_2^{r-1}/I_2^r)$.*
4. *$h_S(K)$ divides $\tilde{\theta}'(\omega,S)_2$.*
5. *Suppose that $\Gamma_S=\Gamma_l$ is cyclic, and that l is split in K/Q so that $r=2$. Let λ be a prime of K above l, and let $k_\lambda\simeq F_l$ denote the residue field at λ. If the fundamental unit of K/Q is a generator for k_λ^*, and $\gcd(h(K),n(l))=1$, then*

$$\tilde{\theta}'(\omega,l)_2=\pm 2h_lR_l \pmod{I_2^2}.$$

Proof:

1. When $r = 1$, we have $\tilde{\theta}'(\omega, S) = P_{S,1}(\theta'(\omega, S))$, where $P_{S,1} : Z[\Gamma_S] \longrightarrow Z$ is the augmentation map. By lemma 2.3.2,
$$P_{S,1}(\theta'(\omega, S)) = \alpha(1) \prod_{l|S}(1 - \omega(l)) = 2^{\#(l|S)}\alpha(1), \tag{2.31}$$
since all the l dividing S are inert in K/Q. We know from Dirichlet's analytic class number formula that $\alpha(1) = 2h_1R_1$, and hence the result follows.

2. Combine lemmas 2.5.1 and 2.5.2.

3. By prop 2.2.4, we have $v_\lambda(\kappa(T)) = 0 \pmod{n(T)}$ for all places λ which do not lie above S. Let $(K^*/K^{*n(T)})(S)$ denote the subgroup of elements in $K^*/K^{*n(T)}$ satisfying this property. There is a natural exact sequence
$$0 \longrightarrow \mathcal{O}_S^*/\mathcal{O}_S^{*n(T)} \longrightarrow (K^*/K^{*n(T)})(S) \longrightarrow C_S(K) \otimes Z/n(T)Z. \tag{2.32}$$
The assumption that $(h_S(K), n(T)) = 1$ for all $T|S$ implies that the natural map from $\mathcal{O}_S^*/\mathcal{O}_S^{*n(T)}$ to $(K^*/K^{*n(T)})(S)$ is an isomorphism, so that the $\kappa(T)$ are S-units modulo $n(T)$-th powers. The result follows from prop. 2.5.4.

4. This is a direct consequence of theorem 2.2.5 combined with prop. 2.5.4.

5. The fact that $\gcd(h_l(K), n(l)) = 1$ implies, by the previous fact, that $\kappa(l)$ is an l-unit of K modulo $n(l)$th powers, and hence $\tilde{\theta}'(\omega, l)$ belongs to $\mathcal{O}_l^* \otimes (I_2/I_2^2)$. We want to prove the equality of two objects in $\mathcal{O}_l^* \otimes (I/I^2)$. For this, we use two maps:
$$\phi_1 : \mathcal{O}_l^* \otimes (I_2/I_2^2) \longrightarrow I_2/I_2^2, \quad \phi_2 : \mathcal{O}_l^* \otimes (I_2/I_2^2) \longrightarrow I_2^2/I_2^3. \tag{2.33}$$
The first is induced from the map $v_\lambda : \mathcal{O}_l^* \longrightarrow Z$, and the second from the map $rec_\lambda : \mathcal{O}_l^* \longrightarrow \Gamma_l \longrightarrow I_2/I_2^2$ given by the reciprocity law of local class field theory. Because $\gcd(h(K), n(l)) = 1$, the kernel of the map ϕ_1 is just $\mathcal{O}_K^* \otimes (I_2/I_2^2)$. The assumption that the fundamental unit for K is a generator of k_λ^* means that ϕ_2 is injective on $\mathcal{O}_K^* \otimes (I_2/I_2^2)$. Hence, if two elements in $\mathcal{O}_l^* \otimes (I_2/I_2^2)$ have the same image by ϕ_1 and ϕ_2, then they are equal.

Recall that $u_l \in k_\lambda^*$ denotes the element which corresponds to the chosen generator γ_l of Γ_l by the reciprocity law of local class field theory. By prop. 2.5.4, we have

$$\tilde{\theta}'(\omega, l)_2 = \kappa(l) \otimes (\gamma_l - 1). \tag{2.34}$$

Hence, by prop. 2.2.4,

$$\phi_1(\tilde{\theta}'(\omega, l)_2) = v_\lambda(\kappa(l)) \otimes (\gamma_l - 1) = \log_{u_l}(\kappa(1))(\gamma_l - 1). \tag{2.35}$$

Let u be a fundamental unit for K. By Dirichlet's class number formula, we can write

$$\kappa(1) = u^{\pm 2h}, \tag{2.36}$$

so that $\log_{u_l}(\kappa(1)) = \pm 2h \log_{u_l}(u)$. It follows that

$$\phi_1(\tilde{\theta}'(\omega, l)_2) = \pm 2h \log_{u_l}(u)(\gamma_l - 1) = \pm 2h(rec(u) - 1). \tag{2.37}$$

Since $\kappa(l) = \beta(l)x^{n(l)}$, where x belongs to K_l^*, and since $\mathrm{norm}_{K_l/K}(\beta(l)) = 1$ by prop. 2.1.1, we have by taking norms:

$$\kappa(l)^{l-1} = \mathrm{norm}_{K_l/K} x^{n(l)}. \tag{2.38}$$

Hence $\kappa(l)^{(l-1)/n(l)} = \pm\mathrm{norm}_{K_l/K} x$, so that $\kappa(l)^{2^a}$ is a norm for some $a \geq 0$. Since norms lie in the kernel of the local reciprocity map, we find that

$$\phi_2(\tilde{\theta}'(\omega, l)_2) = 0. \tag{2.39}$$

We choose a Z-basis for $\mathcal{O}_l^*$, given by a fundamental unit u and an l-unit $u(l)$. This can be done in such a way that

$$v_\lambda(u(l)) = h/h_l, \tag{2.40}$$

since this number is the order of the class of λ in the ideal class group of K. The regulator R_l can be written explicitly as

$$R_l = \pm\left(u \otimes (rec(u(l)) - 1) - u(l) \otimes (rec(u) - 1)\right). \tag{2.41}$$

Hence,

$$\phi_1(2h_l R_l) = \pm 2h_l v_\lambda(u(l)) \otimes (rec(u) - 1) = \pm 2h(rec(u) - 1). \tag{2.42}$$

It is immediate from the definition of R_l that

$$\phi_2(4h_lR_l) = 0. \tag{2.43}$$

Combining equations (2.37), (2.39), (2.42), and (2.43) we find that

$$\tilde{\theta}'(\omega, l)_2 = \pm 2h_lR_l \pmod{I_2^2},$$

as claimed.

Chapter 3

The Birch and Swinnerton-Dyer conjecture

3.1 The classical case

Let E be an elliptic curve defined over a number field K. Given a non-archimedean place v of K where E has good reduction, let

$$a_v = 1 + Nv - \#E(k_v). \tag{3.1}$$

The local L-function $L(E/K_v, s)$ is defined by

$$\begin{aligned} L(E/K_v, s) &= (1 - a_v Nv^{-s} + Nv^{1-2s})^{-1} \\ &\quad \text{if } E \text{ has good reduction at } v, \\ &= (1 + Nv^{-s})^{-1} \\ &\quad \text{if } E \text{ has non-split multiplicative reduction at } v, \\ &= (1 - Nv^{-s})^{-1} \\ &\quad \text{if } E \text{ has split multiplicative reduction at } v, \\ &= 1 \quad \text{if } E \text{ has additive reduction at } v. \end{aligned} \tag{3.2}$$

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

$$L(E/K, s) = \prod_v L(E/K_v, s), \tag{3.3}$$

taken over all non-archimedean places v of K. The Hasse bound $|a_v| < 2\sqrt{Nv}$ implies that $L(E/K, s)$ converges in the right half plane $\Re(s) > 3/2$.

The pair (E, K) also gives rise to some global data:

1. The rank r of the finitely generated abelian group $E(K)$.

2. The Tate-Shafarevich group (E/K) which is the kernel of the restriction map
$$\oplus_v res_v : H^1(K, E) \longrightarrow \oplus_v H^1(K_v, E). \tag{3.4}$$
This group measures the failure of the Hasse principle for principal homogeneous spaces for E over K. It is conjectured to be finite.

3. The order w of the torsion subgroup of $E(K)$.

4. The regulator $R \in R$ defined by
$$R = \det(\langle P_i, P_j \rangle_{NT}), \tag{3.5}$$
where $P_1, \ldots, P_r$ is a basis for the Mordell-Weil group $E(K)$ modulo torsion, and
$$\langle\ \ \rangle_{NT} : E(K) \times E(K) \longrightarrow R \tag{3.6}$$
denotes the Néron-Tate canonical height relative to the Poincaré divisor on $E \times E$.

5. Let $E_{/\mathcal{O}_K}$ denote the Néron model for E over the ring of integers $\mathcal{O}_K$. 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
$$H^0(E_{/\mathcal{O}_K}, \Omega^1) = \mathcal{A}\omega, \tag{3.7}$$
where $\mathcal{A}$ is a fractional ideal of K and ω is a differential for E over K.

   Let $E_0(K_v)$ denote the connected component in the fiber of the Néron model for E at v (thus, $E_0(K_v) = E(K_v)$ when E has good reduction at v). The "local constants" c_v are defined by
$$c_v = \int_{E(K_v)} |\omega| \quad \text{if } v \text{ is real}, \tag{3.8}$$
$$c_v = 2\int_{E(K_v)} \omega \wedge \bar{\omega} \quad \text{if } v \text{ is complex}, \tag{3.9}$$
$$c_v = \#(E(K_v)/E_0(K_v)) \quad \text{if } v \text{ is non-archimedean}. \tag{3.10}$$

Conjecture 3.1.1 (Birch-Swinnerton Dyer) .

1. *The L-series $L(E/K,s)$ has an analytic continuation to the entire complex plane.*
2. $ord_{s=1}L(E/K,s) = r$.
3. *The leading coefficient in the Taylor expansion of $L(E/K,s)$ at $s=1$ is equal to*

$$Disc(K)^{-1/2}w^{-2}N_{K/Q}\mathcal{A}(\prod_v c_v)\# \quad (E/K)R.$$

3.2 Modular elliptic curves

For the rest of chapter 3, we will assume that the curve E is modular, i.e., there is a morphism

$$\phi : X_0(N) \longrightarrow E \tag{3.11}$$

defined over Q, where N is a positive integer and $X_0(N)$ is the algebraic curve which classifies pairs of elliptic curves related by a cyclic N-isogeny. The modularity condition implies that E is defined over Q and has good reduction outside the primes dividing N. Conversely, the conjecture of Taniyama-Weil asserts that any elliptic curve over Q of conductor N is the image of $X_0(N)$ by an algebraic map.

The pull-back of the Néron differential ω on E is a modular form of weight 2 on $X_0(N)$. It is an eigenvalue for the Hecke operators T_p and the Fricke involution w_N which acts on modular forms g of weight 2 and level N by the formula

$$w_N(g)(\tau) = N^{-1}\tau^{-2}g(\frac{-1}{N\tau}). \tag{3.12}$$

Let us write

$$\phi^*\omega = c(\phi)f(q)dq/q, \quad q = e^{2\pi i\tau}, \tag{3.13}$$

where $c(\phi)$ is the *Manin constant* associated to the modular parametrization ϕ and f is an eigenform of weight 2 for $\Gamma_0(N)$, normalized so that its first Fourier coefficient is 1. The q-expansion of f is given by

$$f(q) = \sum_{i=1}^{\infty} a_n q^n, \quad a_1 = 1, \tag{3.14}$$

where the a_p are the integers which were defined in (3.1). In fact, if one attaches to f an L-series $L(f,s)$ by the formula

$$L(f,s)=\sum_{n=1}^{\infty}a_n n^{-s}, \tag{3.15}$$

then $L(f,s)$ has an Euler product and is equal to the L-series $L(E/Q,s)$ attached to E/Q as in section 3.1. The identification of $L(f,s)$ with $L(E/Q,s)$ allows us to derive the functional equation for the latter. Indeed, let $\epsilon=\pm1$ be the eigenvalue of the involution w_N acting on f. The identity

$$\epsilon f(\tau)=N^{-1}\tau^{-2}f(\frac{-1}{N\tau}) \tag{3.16}$$

translates into the functional equation for the L-series

$$\Lambda(f,s)=-\epsilon N^{1-s}\Lambda(f,2-s), \tag{3.17}$$

where $\Lambda(f,s)$ is the Mellin transform of f,

$$\Lambda(f,s)=\int_0^{\infty}f(i\tau)\tau^s d\tau/\tau=(2\pi)^{-s}\Gamma(s)L(f,s). \tag{3.18}$$

This functional equation allows us to extend $L(f,s)=L(E/Q,s)$ to an analytic function defined on the entire complex plane.

Choose now an auxiliary square-free integer S which for the sake of simplicity we will assume to be prime to N, and divisible by a prime p which does not divide $w=\#E(Q)_{tor}$. In analogy with section 1.1 on defines the L-series $L_S(f,s)$ by removing the Euler factors at the primes dividing S:

$$L_S(f,s)=L(f,s)\prod_{p|S}(1-a_p p^{-s}+p^{1-2s}). \tag{3.19}$$

The functional equation for $L_S(f,s)$ can be deduced from that for $L(f,s)$.

Let

$$E_S(Q)=(\cap_{l|S}E_1(Q_l))\bigcap E_0(Q), \tag{3.20}$$

where $E_1(Q_l)$ denotes the group of l-adic points of E which are in the kernel of the reduction modulo l, and $E_0(Q)$ denotes the points which have non-singular reduction everywhere. Thus $E_S(Q)$ is the kernel of the natural map

$$E(Q)\longrightarrow(\oplus_{l|S}E(F_l))\bigoplus(\oplus_p E/E_0(F_p)), \tag{3.21}$$

and is of finite index in $E(Q)$. Let J_S denote the order of the cokernel of this map. Letting r denote as before the rank of $E(Q)$, choose bases $P_1, \ldots P_r$ (resp. $Q_1, \ldots, Q_r$) for $E(Q)$ (resp $E_S(Q)$) modulo torsion, inducing compatible orientations on $E(Q)\otimes R$, and let $R_S \in R$ denote the determinant of the matrix $(\langle P_i, Q_j\rangle)$, where $\langle \ \ \rangle$ is the Néron-Tate height pairing. The Birch-Swinnerton Dyer conjecture can be formulated as follows:

Conjecture 3.2.1 *The function $L_S(f,s)$ vanishes to order r at $s=1$, and its leading coefficient is given by*

$$\lim_{s\longrightarrow 1} L_S(f,s)/(s-1)^r = \# \quad (E/Q) R_S J_S / S.$$

3.3 The Mazur-Tate conjectures

In [MT], Mazur and Tate formulate an analogue of the Birch-Swinnerton Dyer conjectures for modular elliptic curves which replaces the analytic L-series by a θ-element belonging to an integral group ring, in the manner of the Gross conjectures of section 1.2. It will be convenient, (but not essential) to make the following assumption on ϕ:

Hypothesis 3.3.1 *The modular parametrization ϕ maps the cusps of $X_0(N)$ to the origin of E.*

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

$$\Lambda \subset Z\Omega^+ \oplus iZ\Omega^-. \tag{3.22}$$

Let S be a positive square free integer which is relatively prime to N. Given a divisor T of S, and $a \in Z/SZ$, the modular symbol $[a/T]^+$ is defined by the formula

$$2\pi \int_{a/T}^{a/T+i\infty} \phi^*\omega = [a/T]^+\Omega^+ + i[a/T]^-\Omega^-. \tag{3.23}$$

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

$\phi^*\omega$. Let T' denote the inverse of S/T modulo T. It turns out to be more convenient to work with the regularized modular symbols, defined by the formula

$$[a/S]^* = \sum_{T|S} \mu(T)[aT'/T], \tag{3.24}$$

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

Let $G_S = \mathrm{Gal}(Q(\mu_S)/Q) = (Z/SZ)^*$, and let

$$G_S^+ = G_S/\tau = (Z/SZ)^*/\langle \pm 1 \rangle, \tag{3.25}$$

where τ denotes complex conjugation. Given $a \in (Z/SZ)^*$, let $\sigma(a,S)$ denote the natural image of a in G_S^+. Since $Q(\mu_S)$ is a compositum of the linearly disjoint field extensions $Q(\mu_l)$, for $l|S$, there is a canonical direct product decomposition

$$G_S = G_{l_1} \times \cdots \times G_{l_s}, \quad S = l_1 \cdots l_s \tag{3.26}$$

which allows us to implicitly view G_T as a subgroup of G_S by the componentwise embedding, for any T dividing S.

The θ-element is defined by

$$\theta_S = \frac{1}{2} \sum_{a \in (Z/SZ)^*} [\frac{a}{S}]^* \sigma(a,S) \in Z[G_S^+]. \tag{3.27}$$

Remark: In [MT], Mazur and Tate work with the θ-element defined by

$$\frac{1}{2} \sum_{a \in (Z/SZ)^*} [\frac{a}{S}]^+ \sigma(a,S) \in Z[G_S^+], \tag{3.28}$$

which we denote by θ_S^{MT} to distinguish it from our regularized one. The relationship between our θ_S and the θ_S^{MT} is given by the formula

$$\theta_S = \sum_{T|S} \mu(T)\theta_T^{MT} \sigma(S/T,T) N_{S/T}, \tag{3.29}$$

where

$$N_T = \sum_{a \in (Z/TZ)^*} \sigma(a,T) \tag{3.30}$$

is the norm element in the group ring $Z[G_T^+] \subset Z[G_S^+]$.

Let l be a prime not dividing S, and let z_l be the canonical map $Z[G_{Sl}^+] \longrightarrow Z[G_S^+]$ 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 $Z[G_S^+]$ which has the appearance of an Euler factor at l.

Lemma 3.3.2

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

where $\sigma_l = \sigma(l, S) \in G_S^+$.

Proof: This follows from the compatibility formula for modular elements

$$z_l(\theta_{Sl}^{MT}) = (a_l - \sigma_l - \sigma_l^{-1})\theta_S^{MT} \tag{3.31}$$

given in [MT], p. 717, together with equation (3.29).

Relation between θ_S *and* $L_S(f,1)$. Let χ be an even Dirichlet character of conductor dividing S. The twisted L-series

$$L_S(f,\chi,s) = \sum_{(n,S)=1} \chi(n)a_n n^{-s} = \prod_{p \nmid S}(1 - \chi(p)p^{-s} + \chi^2(p)p^{1-2s})^{-1} \tag{3.32}$$

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

$$\chi : Q[G_S^+] \longrightarrow C \tag{3.33}$$

be the ring homomorphism obtained by extending χ by linearity, and let $g = S/Cond(\chi)$.

Proposition 3.3.3

$$\chi(\theta_S) = \mu(S)\chi(g)g \cdot c(\phi)\frac{\tau(\chi)L_S(f,\bar{\chi},1)}{2\Omega^+},$$

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

Proof: For primitive characters, one has

$$\chi(\theta_S) = \mu(S)\chi(\theta_S^{MT}), \tag{3.34}$$

and the proposition follows from the formula (1) in [MT]. In the general case it follows from lemma 3.3.2.

In [MT], Mazur and Tate define a height pairing

$$\langle\ \ \rangle_S : E(Q) \times E_S(Q) \longrightarrow G_S^+. \tag{3.35}$$

The map sending σ to $\sigma - 1$ gives an identification of G_S^+ with I_S/I_S^2, where I_S is the augmentation ideal in the group ring $Z[G_S^+]$. Thus the pairing matrix $(\langle P_i, Q_j\rangle_S)$ can be viewed as an $r \times r$ matrix with entries in I_S/I_S^2; its determinant R_S in I_S^r/I_S^{r+1} is the Mazur-Tate regulator attached to E and S.

Conjecture 3.3.4 (Mazur-Tate) .

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

$$\tilde{\theta}_S = c(\phi)\#\quad(E/Q)R_S J_S.$$

Remark: The formulation of the conjecture on the leading coefficient differs slightly from the one in [MT], 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. Conjecture 4 of [MT] (reformulated to fit our notations) states that

$$\tilde{\theta}_T^{MT} = c(\phi)\#\quad(E/Q)Disc_T, \tag{3.36}$$

where

$$Disc_T = \sum_{Q|T} \mu(Q) J_Q R_Q \phi(T/Q), \tag{3.37}$$

and ϕ is the Euler function. By comparing the formulas (3.36), (3.37) with the formula (3.29) giving the relation between θ_S and θ_S^{MT}, a straigtforward computation (essentially a Möbius inversion argument) shows that the two conjectures are equivalent.

3.4 A conjecture of Mazur-Tate type for derivatives of L-functions

Fix a quadratic imaginary field K in which all primes dividing N are split, and let $\omega : \mathrm{Gal}(\bar{Q}/Q) \longrightarrow \pm 1$ denote the corresponding odd primitive Dirichlet character. One has the factorization

$$L(E/K, s) = L(f, s)L(f, \omega, s), \tag{3.38}$$

where the twisted L-function $L(f, \omega, s)$ is given by

$$L(f, \omega, s) = \sum_{n=1}^{\infty} \omega(n) a_n n^{-s}. \tag{3.39}$$

The sign in the functional equation for the twisted L-series is ϵ; in particular, $L(E/K, s)$ vanishes to odd order at $s = 1$, and hence

$$L(E/K, 1) = 0. \tag{3.40}$$

Let χ denote an idèle class character of K of finite order on which $\mathrm{Gal}(K/Q)$ acts by -1. A parity argument also shows that

$$L(E/K, \chi, 1) = 0. \tag{3.41}$$

Thus, we are in a situation similar to that of section 1.3. This time, it is the Heegner points defined over ring class fields of K which will play the role of the circular units in interpolating special values of $L'(E/K, \chi, 1)$.

If $N = p_1^{e_1} \cdots p_k^{e_k}$, we choose for each p_i an ideal P_i of K above it, and set

$$\mathcal{N} = P_1^{e_1} \cdots P_k^{e_k}.$$

Given a positive integer T which is relatively prime to N and $Disc(K)$, we let $\mathcal{O}_T$ denote the order of K of conductor T. The natural projection of complex tori

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

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_T, the ring class field of K of conductor T. Let $y(T)$ denote the image of this point in $E(K_T)$ by the modular parametrization ϕ.

Now fix a square-free integer $S = l_1 \cdots l_t$ prime to N and to $Disc(K)$. Write $G_S = \mathrm{Gal}(K_S/K_1)$, and $\Gamma_S = \mathrm{Gal}(K_S/K)$. Define the *regularized* Heegner points by the formula

$$\beta_S = \sum_{T|S} \mu(T) y(T), \quad \beta_S^{\omega} = \sum_{T|S} \mu(T)\omega(T) y(T), \tag{3.42}$$

where μ is the Möbius function as before. The element $\theta'(E,S)$ is constructed from Heegner points as follows:

$$\begin{aligned}
A(E,S) &:= \sum_{\sigma\in\Gamma_S} \sigma\beta_S \otimes \sigma \in E(K_S)\otimes Z[\Gamma_S], && (3.43)\\
A^{\omega}(E,S) &:= \sum_{\sigma\in\Gamma_S} \sigma\beta_S^{\omega} \otimes \sigma^{-1} \in E(K_S)\otimes Z[\Gamma_S], && (3.44)\\
\theta'(E,S) &:= A(E,S)\otimes_{Z[\Gamma_S]} A(E,S)^{\omega} && (3.45)\\
&= \sum_{\sigma,\tau\in\Gamma_S} \sigma\beta_S \otimes \tau\beta_S^{\omega} \otimes \sigma\tau^{-1}. && (3.46)
\end{aligned}$$

The element $\theta'(E,S)$ belongs to the triple tensor product $E(K_S)\otimes E(K_S)\otimes Z[\Gamma_S]$.

As in the case of circular units, the group G_S can be written canonically as a direct product

$$G_S = G_{l_1} \times \cdots \times G_{l_s}, \tag{3.47}$$

and one can view Γ_T as a subgroup of Γ_S when T divides S by the diagonal embedding. Let $z_l : Z[\Gamma_{Sl}] \longrightarrow Z[\Gamma_S]$ be the ring homomorphism induced by the projection $\Gamma_{Sl} \longrightarrow \Gamma_S$.

Lemma 3.4.1 .

1. $z_l(A(E,Sl)) = \begin{cases} (l+1-a_l)A(E,S) & \textit{if } \omega(l) = -1. \\ (l-1+Frob_\lambda + Frob_\lambda^{-1} - a_l)A(E,S) & \textit{if } l = \lambda\bar{\lambda}. \end{cases}$

2. $z_l(A(E,Sl)^{\omega}) = \begin{cases} (l+1+a_l)A(E,S) & \textit{if } \omega(l) = -1. \\ (l-1+Frob_\lambda + Frob_\lambda^{-1} - a_l)A(E,S) & \textit{if } \omega(l) = 1. \end{cases}$

3. $z_l(\theta'(E,Sl)) = \begin{cases} \#E(k_l)\cdot\theta'(E,S) & \textit{if } \omega(l) = -1. \\ \#E(k_\lambda)^2\cdot\theta'(E,S) & \textit{if } \omega(l) = 1. \end{cases}$

The factors which appear in the norm compatibility formulas are akin to Euler factors at l.

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

$$\chi : Z[\Gamma_S] \longrightarrow C$$

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

$$h\otimes\chi : E(K_S)\otimes E(K_S)\otimes Z[\Gamma_S] \longrightarrow C.$$

The following theorem relates $\theta'(E,S)$ with the derivative $L'(E/K,s)$ of the L-series of E over K:

Theorem 3.4.2 (Gross-Zagier) *Suppose that $S=1$ so that K_S is the Hilbert class field of K. Then*

$$h\otimes\chi(\theta'(E,S)) = \frac{L'(E/K,\chi,1)}{\iint_{E(C)}\omega\wedge\bar{\omega}}\sqrt{Disc(K)}.$$

The computations for $S\neq 1$ have not been worked out, but it is quite likely that a similar result holds in that case as well for primitive χ. Thus, the element $\theta'(E,S)$ should be thought of as the analogue of $L'_S(E/K,s)$, the L-function of E/K with the Euler factors above the primes of S removed.

Let I denote the augmentation ideal in the group ring $Z[\Gamma_S]$. We will define a regulator term in $E(K)\otimes E(K)\otimes I^{r-1}/I^r$ which combines the ideas of sections 1.3 and 3.3. Let

$$E_S(K) = \ker\left(E(K) \longrightarrow (\oplus_{v|S}E(k_v))\bigoplus(\oplus_v E/E_0(K_v))\right), \tag{3.48}$$

and let J_S be the order of the cokernel of this map. As in the previous section, the Mazur-Tate pairing

$$\langle\ \rangle_S : E(K)\times E_S(K) \longrightarrow I/I^2 \tag{3.49}$$

is defined. Let $P_1,\ldots,P_r$ (resp. $Q_1,\ldots,Q_r$) denote integral bases for $E(K)$ modulo torsion (resp $E_S(K)$) which induce compatible orientations. The *partial regulator* R_{ij} in I^{r-1}/I^r is defined to be the Mazur-Tate determinant of the ijth minor of the pairing matrix $(\langle P_i, Q_j\rangle_S)$. The regulator R_S is given by the formula

$$R_S = \sum_{i,j=1}^{r} (-1)^{i+j} P_i \otimes Q_j \otimes R_{ij} \tag{3.50}$$

We make the following conjecture

Conjecture 3.4.3 .

1. *The element* $\theta'(E,S)$ *belongs to* $E(K_S) \otimes E(K_S) \otimes I^{r-1}$.
2. *The leading coefficient* $\tilde{\theta}'(E,S) \in E(K_S) \otimes E(K_S) \otimes (I^{r-1}/I^r)$ *belongs to* $E(K) \otimes E(K) \otimes (I^{r-1}/I^r)$.
3. $\tilde{\theta}'(E,S) = c(\phi)^2\#\quad(E/K)J_S R_S$.

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 $\mathrm{Gal}(Q(E_{p^\infty})/Q)$ is not isomorphic to $GL_2(Z_p)$.
4. All primes which divide $\prod_v c_v$, where c_v denotes the number of connected components in the Neron model at v.

Let us view $\theta'(E,S)$ as belonging to $E(K_S) \otimes E(K_S) \otimes Z[\Gamma_S]$ by extending scalars from Z to Z, and let I_* denote the augmentation ideal in the group ring $Z[\Gamma_S]$.

Theorem 3.4.4 (Main result) *Suppose that* S *is a product of primes which are inert in* K. *Then* $\theta'(E,S)$ *belongs to* $E(K_S) \otimes E(K_S) \otimes I_*^{r-1}$.

This theorem generalizes a result of Kolyvagin which can be stated as follows:

Theorem 3.4.5 (Kolyvagin) *If* $r > 1$, *then* $\theta'(E,S)$ *belongs to* $E(K_S) \otimes E(K_S) \otimes I$.

The proof uses the beautiful ideas of Kolyvagin on "Euler systems" of Heegner points. It will be described in the next chapter.

Suppose from now on that S is a product of primes which are inert in K/Q. Concerning the leading coefficient $\tilde{\theta}'(E,S)$ in $E(K_S)\otimes E(K_S)\otimes I^{r-1}/I^r$, we can prove the following results which provide evidence for our conjecture. Let p be a prime, and let $\theta'(E,S)_p$ denote the image of $\theta'(E,S)$ in $E(K_S)\otimes E(K_S)\otimes Z/pZ[\Gamma_S]$. Let $\tilde{\theta}'(E,S)_p$ denote the corresponding leading coefficient in $E(K_S)\otimes E(K_S)\otimes I_p^{r-1}/I_p^r$, where I_p denotes the augmentation ideal in the group ring $Z/pZ[\Gamma_S]$.

Theorem 3.4.6 .

1. *$\tilde{\theta}'(E,S)_p$ belongs to $E(K)\otimes E(K)\otimes(I_p^{r-1}/I_p^r)$.*
2. *If p divides $\#\ \ (E/K)J_S$, then $\tilde{\theta}'(E,S)_p=0$.*

Remarks:
1. In [BD], it is observed that Kolyvagin's methods also work to prove a special case of the Birch and Swinnerton-Dyer conjecture for Mordell-Weil groups over ring class fields of quadratic imaginary fields. More precisely, let c denote a fixed conductor prime to B, and let $\chi : \mathrm{Gal}(K_c/K)\longrightarrow C^*$ be a character. Let R denote the ring obtained by adjoining to Z the character values and inverting $\#\Gamma_c$. Given an integer S prime to Bc, let $\alpha^\chi(S)$ be the projection of the Heegner point $\alpha(cS)$ onto the χ-component $E(K_{cS})^\chi$ of $E(K_{cS})\otimes R$ for the action of Γ_c. Let I_χ denote the augmentation ideal in the group ring $R[\Gamma_S]$, and let

$$\theta'(E,S,\chi)\in E(K_{cS})^\chi\otimes E(K_{cS})^\chi\otimes R[\Gamma_S]$$

denote the theta-element made with $\alpha^\chi(S)$ instead of $\alpha^{reg}(S)$, and let r_χ denote the R-rank of $(E(K_c)^\chi$. The main result of [BD] is:

Proposition 3.4.7 *If $r_\chi>1$, then $\theta'(E,S,\chi)$ belongs to $E(K_{cS})\otimes E(K_{cS})\otimes I_\chi$.*

The main difficulty in tackling this case is that complex conjugation does not act on the relevant Galois modules, when χ is different from $\bar{\chi}$. However, one expects that the modification in Kolyvagin's argument presented in [BD], combined with the ideas in this thesis, would give evidence for the following:

Conjecture 3.4.8 *$\theta'(E,S,\chi)$ belongs to $E(K_{cS})\otimes E(K_{cS})\otimes I_{\chi}^{r_\chi - 1}$.*

However, in proving the result in this thesis we have followed Kolyvagin's original approach, and relied heavily on the decomposition of certain Galois modules into eigencomponents for the action of complex conjugation. This simplifies many of the arguments.

2. The philosophy of refined Birch and Swinnerton Dyer formulas can be used to formulate other kinds of conjectures, which have not been touched upon in this thesis. For example, in [Gr2], it is shown that the heights of certain special points on Shimura curves interpolate special values of the L-function of a corresponding elliptic curve (and not its derivative). One can form a θ-element from these points in the same way as with the Heegner points, and one obtains a conjecture which in some ways lies between the original Mazur-Tate conjectures and the conjectures of this thesis. Unfortunately, the techniques of Kolyvagin do not seem to be applicable (at least directly), and even the statement about the order of vanishing remains entirely conjectural in this setting, just as in that of the original Mazur-Tate conjectures.

Another analogue is gotten by replacing the imaginary quadratic field by a real quadratic field K, and still requiring that all the primes dividing the conductor of E split in K. In that case, one can define certain objects, which share features of both modular symbols, and Heegner points: like modular symbols, they belong naturally to $H_1(E,C)$, and interpolate special values of $L(E/K,1)$ (cf. [Wal]). Like Heegner points, they correspond naturally to elements in the Galois group of the ring class field of the quadratic field K, and they are defined computationally in a manner very analogous to Heegner points. It seems that a beautiful analogy exists between these real quadratic modular symbols and Stickelberger elements, just as there is between Heegner points and circular units. It is striking that so much more can be proved, from the point of view of Mazur-Tate conjectures, in the latter setting than in the former.

Chapter 4

Partial proof of the refined Birch and Swinnerton-Dyer conjecture for Heegner points

4.1 The descent formalism

This section is devoted to the formalism of descent and the cohomological tools that enter into Kolyvagin's method. All the statements in this section are valid for an arbitrary elliptic curve E (not necessarily parametrized by a modular curve) defined over a number field K. We let p be a rational prime and let $q = p^M$ be a power of p. Multiplication by q gives an isogeny of E whose kernel is the group E_q of points of order q on E. To simplify matters, we assume the following:

Hypothesis 4.1.1 *$Gal(K(E_q)/K) = GL_2(Z/qZ)$.*

Note that, if q does not satisfy this hypothesis, then it is invertible in the ring Z of section 3.4.

Lemma 4.1.2 *The cohomology groups $H^i(GL_2(Z/qZ), (Z/qZ)^2)$ are trivial, where the action of $GL_2(Z/qZ)$ is the obvious one.*

Proof: Let $T \subset GL_2(Z/qZ)$ be the subgroup of order 2 generated by the matrix $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$. Since q is odd, $H^i(T, (Z/qZ)^2) = 0$ and the Hochschild-

Serre spectral sequence

$$H^m(GL_2(Z/qZ)/T, H^n(T,(Z/qZ)^2)) \Rightarrow H^{m+n}(GL_2(Z/qZ),(Z/qZ)^2) \quad (4.1)$$

implies that $H^i(GL_2(Z/qZ),(Z/qZ)^2) = 0$. (cf. [Gr4]).

Taking the Galois cohomology of the short exact sequence

$$0 \longrightarrow E_q(\bar{K}) \longrightarrow E(\bar{K}) \xrightarrow{q} E(\bar{K}) \longrightarrow 0 \qquad (4.2)$$

gives the exact cohomology sequence, analogous to the Kummer sequence, which is the starting point for the descent formalism:

$$0 \longrightarrow E(K)/qE(K) \longrightarrow H^1(K,E_q) \longrightarrow H^1(K,E)_q \longrightarrow 0. \qquad (4.3)$$

To control the image of $E(K)/qE(K)$ inside $H^1(K,E_q)$, one introduces the subgroup of cohomology classes whose restrictions in $H^1(K_v,E_q)$ come from elements in $E(K_v)/qE(K_v)$ for all places v of K. This is the q-Selmer group $Sel_q(E/K)$:

$$Sel_q(E/K) = \ker(H^1(K,E_q) \longrightarrow \oplus_v H^1(K_v,E)_q). \qquad (4.4)$$

The Tate-Shafarevich group is defined by

$$(E/K) = \ker(H^1(K,E) \longrightarrow \oplus_v H^1(K_v,E)). \qquad (4.5)$$

Thus one has the following exact sequence:

$$0 \longrightarrow E(K)/qE(K) \longrightarrow Sel_q(E/K) \longrightarrow \quad (E/K)_q \longrightarrow 0. \qquad (4.6)$$

By definition of the Selmer group there is a map:

$$Sel_q(E/K) \longrightarrow \prod_v E(K_v)/qE(K_v), \qquad (4.7)$$

where the product is taken over all places v of K.

Lemma 4.1.3 *The map (4.7) is an injection.*

Proof: Let $F = K(E_q)$, and consider the commutative diagram

$$\begin{array}{ccc} H^1(K,E_q) & \longrightarrow & H^1(F,E_q) \\ \downarrow & & \downarrow \\ \oplus_v H^1(K_v,E_q) & \longrightarrow & \oplus_w H^1(F_w,E_q) \end{array}$$

The kernel of the top horizontal map in the inflation-restriction sequence is

$$H^1(\mathrm{Gal}(F/K),E_q) \simeq H^1(GL_2(Z/pZ),(Z/qZ)^2), \tag{4.8}$$

which is trivial, by lemma 4.1.2. The right vertical map is also injective by the Chebotarev density theorem, because $H^1(F,E_q) = \mathrm{hom}(\mathrm{Gal}(\bar{F}/F),E_q)$. The result follows.

Given a Z/qZ-module M, let M^* denote its Pontrjagin dual,

$$M^* = \mathrm{hom}(M, Z/qZ). \tag{4.9}$$

Taking Pontrjagin duals of the injective map (4.7), we get a surjective map

$$\oplus_v (E(K_v)/qE(K_v))^* \longrightarrow Sel_q(E/K)^*. \tag{4.10}$$

Theorem 4.1.4 (Tate) *The groups $(E(K_v)/qE(K_v))^*$ and $H^1(K_v,E)_q$ are canonically isomorphic.*

Proof: The cup product in cohomology combined with the Weil pairing gives rise to a pairing $\langle\ ,\ \rangle_v$:

$$\begin{aligned} \langle\ ,\ \rangle_v :\ & H^1(K_v,E_q) \times H^1(K_v,E_q) \xrightarrow{cup} H^2(K_v, E_q \otimes E_q) \\ & \xrightarrow{Weil} H^2(K_v,\mu_q) = \mathrm{Br}_q(K_v) \xrightarrow{\mathrm{inv}_v} Z/qZ. \end{aligned} \tag{4.11}$$

It is a result of Tate [Mi] that the above pairing is non-degenerate. By using the local q-descent exact sequence,

$$0 \longrightarrow E(K_v)/qE(K_v) \longrightarrow H^1(K_v,E_q) \longrightarrow H^1(K_v,E)_q \longrightarrow 0, \tag{4.12}$$

we view $E(K_v)/qE(K_v)$ as a subspace of $H^1(K_v,E_q)$. It is not hard to show that this subspace is maximal isotropic for the pairing $\langle\ ,\ \rangle_v$, and by passing to the quotient one defines the non-degenerate local Tate pairing:

$$\langle\ ,\ \rangle_v : E(K_v)/qE(K_v) \times H^1(K_v,E)_q \longrightarrow Z/qZ. \tag{4.13}$$

Combining the map (4.10) with theorem 4.1.4 yields the surjective map:

$$\phi : \oplus_v H^1(K_v, E)_q \longrightarrow Sel_q(E/K)^*. \tag{4.14}$$

The next step is to identify elements in the kernel of the map ϕ in (4.14), by using the reciprocity law of global class field theory.

Proposition 4.1.5 *If $(c_v) \in \oplus_v H^1(K_v, E)_q$ is the image of a global class $c \in H^1(K, E)_q$ by the natural restriction map:*

$$\oplus res_v : H^1(K, E)_q \longrightarrow \oplus_v H^1(K_v, E)_q,$$

then $\phi((c_v)) = 0$ in $Sel_q(E/K)^*$.

Proof: Let $\tilde{c}$ be any lift of c to a class in $H^1(K, E_q)$. Given $s \in Sel_q(E/K)$, write $s_v = res_v(s) \in H^1(K_v, E_q)$, and let $\tilde{s}_v$ be the lift of s_v to $E(K_v)/qE(K_v)$. By definition of the map ϕ and of the local Tate pairing, we have:

$$\phi((c_v))(s) = \sum_v \langle \tilde{s}_v, c_v \rangle_v = \sum_v inv_v(s \cup \tilde{c}) = 0. \tag{4.15}$$

The last equality results from the global reciprocity law of class field theory: the sum of local invariants of an element in the Brauer group of a global field is 0.

Let $\ {}_q(E/K)$ denote the cokernel which fits into the following exact sequence:

$$0 \longrightarrow \quad (E/K)_q \longrightarrow H^1(K, E)_q \longrightarrow \oplus_v H^1(K_v, E)_q \longrightarrow \quad {}_q(E/K) \longrightarrow 0. \tag{4.16}$$

We have constructed a surjective map which is at the heart of Kolyvagin's descent method:

$$ {}_q(E/K) \longrightarrow Sel_q(E/K)^*. \tag{4.17}$$

When E is a modular elliptic curve and K is a quadratic imaginary field satisfying suitable assumptions, Kolyvagin succeeds in contructing certain global cohomology classe in $H^1(K, E_q)$ from Heegner points.

If $\mathcal{L}$ is a set of primes of K, let $H^1_{\mathcal{L}}(K, E)_q$ denote the set of classes which are concentrated above places of $\mathcal{L}$, i.e.,

$$H^1_{\mathcal{L}}(K, E)_q = \{c \in H^1(K, E)_q \text{ such that } \mathrm{res}_v(c) = 0 \quad \forall v \notin \mathcal{L}\}, \tag{4.18}$$

and let

$$_{\mathcal{L}} = \oplus_{v \in \mathcal{L}} H^1(K_v, E)_q / H^1_{\mathcal{L}}(K, E)_q \subset \quad _q(E/K). \tag{4.19}$$

Kolyvagin exhibits a set $\mathcal{L}$ of primes such that the map

$$_{\mathcal{L}} \longrightarrow Sel^*_q(E/K) \tag{4.20}$$

is still surjective. The main ingredient in the proof of surjectivity is the Chebotarev density theorem, as in the proof of lemma 4.1.3.

When the point P in $E(K)$ obtained from Heegner's construction is non-trivial, and when q is large enough (so that P remains non-trivial in $E(K)/qE(K)$, and so that the field generated by the q-torsion points has as big a Galois group as possible), Kolyvagin constructs enough classes in $H^1_{\mathcal{L}}(K, E)_q$ to show that that $\quad_{\mathcal{L}}$ is a quotient of a group of the form $Z/qZ \times T$, where $\#T \leq p^{2a}$ and p^a is the largest power of p dividing P. He concludes that the rank of $E(K)$ is less than 1, and that the order of $\quad(E/K)_q$ is less than p^{2a}, as one expected from the Birch-Swinnerton Dyer conjecture, given the result of Gross and Zagier.

Our approach will be to search for a converse to Kolyvagin's result. Assuming a priori information about the Selmer group, say, that

$$Sel_q(E/K) = (Z/qZ)^{r_q} \times T, \tag{4.21}$$

where T is of exponent less than q, Kolyvagin's result tells us that P is divisible by q when $r_q > 1$. In fact, the bigger r_q is, the more the global cohomology classes constructed by Kolyvagin must tend to vanish. This statement can be made precise and translates into divisibility properties by powers of p of certain combinations of Heegner points over ring class fields. These divisibility properties are exactly what one needs to prove the order of vanishing statements for the element $\theta'(E, S)$ introduced in section 3.4.

4.2 The Euler system of Heegner points

¿From now on, we place ourselves in the situation described in section 3.4. Let $B = NDisc(K)$. Let $\mathcal{S}$ be the set of square-free integers prime to B which are products of primes which are inert in K. For all $T \in \mathcal{S}$ recall that we are given the following data:

1. An abelian extension K_T of K, the ring class field of K associated to the order of conductor T. It is ramified only at the places of K which lie above the primes dividing T. Thus K_1 is the Hilbert class field of K. One writes $G = \mathrm{Gal}(K_1/K)$, $G_T = \mathrm{Gal}(K_T/K_1)$ and $\Gamma_T = \mathrm{Gal}(K_T/K)$.

2. The Heegner point $y(T)$ in $E(K_T)$.

Writing $T = l_1 \cdots l_s$, the extension K_T is a compositum of the fields K_{l_i} which are linearly disjoint over K_1. Hence there is a canonical direct product decomposition

$$G_T = G_{l_1} \times \cdots \times G_{l_s} \tag{4.22}$$

which gives inclusions $G_S \subset G_T$ and $\Gamma_S \subset \Gamma_T$ for all divisors S of T. We will implicitly identify elements of G_S with their images in G_T. For any S dividing T, the partial norm operator N_S in the group ring $Z[G_T]$ is defined by

$$N_S = \sum_{\sigma \in G_S} \sigma. \tag{4.23}$$

These operators act on the field K_T and on the Mordell-Weil group $E(K_T)$ in the natural way. Given $S \in \mathcal{S}$ and l a prime in $\mathcal{S}$ which is prime to S, let λ denote a prime of K above l and let $\sigma_{\lambda,S} \in \Gamma_S$ be the frobenius automorphism associated to λ.

Proposition 4.2.1 $N_l(y(Sl)) = a_l y(S)$.

The proof of this statement can be found in [Gr4].

Proposition 4.2.2 $y(Sl) \equiv \sigma_{\lambda,S}\, y(S) \pmod{\lambda'}$, *where* λ' *is any prime of* K_{Sl} *above* λ.

Proof: See [Gr4].

Propositions 4.2.1 and 4.2.2 make up the axioms of an Euler system for Heegner points in the sense of Kolyvagin [Ko3].

Complex conjugation τ acts on the Galois extension K_T and on the Mordell-Weil group $E(K_T)$.

Proposition 4.2.3 $\tau y(T) = \epsilon \sigma_0 y(T) + (torsion)$ *for some* $\sigma_0 \in \Gamma_T$.

Proof: See [Gr4].

4.3 Derivatives in group rings

We begin by setting up some notation. Let $[\tau]$ denote the class of complex conjugation in $\mathrm{Gal}(\bar{Q}/Q)$. By abuse of notation, we identify frobenius elements with their images in quotients of $\mathrm{Gal}(\bar{Q}/Q)$. We define sets $\mathcal{L}_q$ and $\mathcal{L}_{q,E}$ of rational primes as follows:

$$\mathcal{L}_q = \{l \text{ rational prime} \mid l \not| Bp \text{ and } Frob_l = [\tau] \text{ in } K(\mu_q)/Q\}, \tag{4.24}$$

and

$$\mathcal{L}_{q,E} = \{l \text{ rational prime} \mid l \not| Bp \text{ and } Frob_l = [\tau] \text{ in } K(E_q)/Q\}. \tag{4.25}$$

Lemma 4.3.1 *The prime l not dividing Bp belongs to $\mathcal{L}_q$ if and only if l is inert in K/Q and q divides the order of G_l. The prime l belongs to $\mathcal{L}_{q,E}$ if and only if it belongs to $\mathcal{L}_q$ and in addition q divides a_l.*

Proof: If $Frob_l = [\tau]$ in $K(\mu_q)/Q$, then l is inert in K/Q and q divides $l+1$. But $G_l = k_\lambda^*/(Z/lZ)^*$ and hence is cyclic of order $l+1$. Hence q divides $\#G_l$. If $l \in \mathcal{L}_{q,E}$, we have the equalities of the minimal polynomials of $Frob_l$ and τ acting on E_q:

$$x^2 - a_l x + l = x^2 - 1 \pmod{\mathrm{q}}.$$

The lemma follows by equating coefficients of these two polynomials.

For each l in $\mathcal{L}_q$, choose a generator σ_l of G_l, and define the kth derivative in the group ring $Z[G_l]$ by the formula

$$\mathrm{D}_l^k = \sum_{i=1}^{\#G_l} \binom{i}{k} \sigma_l^i. \tag{4.26}$$

Thus $\mathrm{D}_l^0 = N_l$ is the norm element in the group ring, and D_l^1 is the derivative operator studied by Kolyvagin. One also introduces higher derivatives in the group ring $Z[G]$ when q divides the exponent of the class group of K. In this case, write

$$G = Z/p^{t_1} \times \cdots \times Z/p^{t_a} \times G' \tag{4.27}$$

where $p^{t_1} \geq \cdots \geq p^{t_a} \geq q$, and q does not divide the exponent of G'. Such a decomposition exists, by the structure theory of finite abelian groups. Now choose generators $\xi_1, \ldots, \xi_a$ for the first factors in this decomposition and let the derivatives be defined by

$$\mathrm{D}^k_{\xi_j} = \sum_{i=1}^{p^{t_j}} \binom{i}{k} \xi^i_j, \quad \mathrm{D}^0_{G'} = \sum_{\sigma \in G'} \sigma. \tag{4.28}$$

One has the following formula:

Lemma 4.3.2 .

$(\sigma_l - 1) D^1_l = (l+1) - D^0_l.$

2. For all $0 < k < p$,

$$(\sigma_l - 1) D^k_l = -D^{k-1}_l \pmod q,$$

and a similar formula hold for the $D^k_{\xi_j}$.

Proof: An easy computation, using the fact that q divides the order of G_l (lemma 4.3.1) and of ξ_j.

Given $S = l_1 \cdots l_s$ a product of distinct primes in $\mathcal{L}_q$, the general derivative operator in the group ring $Z/qZ[\Gamma_S]$ is of the form:

$$\mathrm{D}_{\underline{k}} = \mathrm{D}^0_{G'} \mathrm{D}^{j_1}_{\xi_1} \cdots \mathrm{D}^{j_a}_{\xi_a} \mathrm{D}^{k_1}_{l_1} \cdots D^{k_s}_{l_s}, \tag{4.29}$$

where $\underline{k} = (j_1, \ldots, j_a, k_1, \ldots, k_s)$ is an $(a+s)$-tuple of positive integers. One defines the support of $\mathrm{D}_{\underline{k}}$ to be the integer S, its conductor S' to be the product of the l_i with $k_i > 0$, and its order to be $j_1 + \cdots + j_a + k_1 + \cdots + k_s$. There is an obvious partial ordering on the set of derivatives with support S. Given $\underline{k}' = (j'_1, \ldots, j'_a, k'_1, \ldots, k'_s)$, one says that $\mathrm{D}_{\underline{k}'}$ is less than $\mathrm{D}_{\underline{k}}$ if

$$j'_t \leq j_t, \quad k'_t \leq k_t \quad \forall t.$$

The group $\mathrm{Gal}(K_S/Q)$ is a semi-direct product of $\mathrm{Gal}(K/Q) = \langle \tau \rangle$ with Γ_S. Complex conjugation τ acts on Γ_S by the formula:

$$\tau \sigma \tau^{-1} = \sigma^{-1}. \tag{4.30}$$

Extending this action to the group ring $Z/qZ[\Gamma_S]$, one has the following action of τ on $\mathrm{D}_{\underline{k}}$:

Lemma 4.3.3 $\tau D_{\underline{k}}\tau^{-1} = (-1)^k D_{\underline{k}} +$ *(lower order derivatives).*

Proof: It suffices to show this for a derivative operator of the form D_l^k. In this case, one has

$$\tau \mathrm{D}_l^k \tau^{-1} - (-1)^k \mathrm{D}_l^k = \sum_{i=0}^{\#G_l} f(i)\sigma_l^i, \tag{4.31}$$

where $f(i) = \binom{\#G_l - i}{k} - (-1)^k \binom{i}{k}$. The function $f(i)$ is the reduction mod q of a polynomial with rational coefficients taking integral values at integral arguments. Moreover the degree of f is strictly less than k. The Z-module of all such polynomial functions is spanned by the $\binom{i}{k'}$ with $k' < k$. Hence the left hand side of (4.31) can be expressed as a linear combination of derivatives of lower order.

4.4 The Heegner cohomology classes

Assume from now on that q is not invertible in the ring Z defined in section 3.4. In particular, p does not divide any of the c_v's and

Lemma 4.4.1 *If L is a solvable extension of Q, then $E_q(L) = 0$.*

Proof: Suppose $E_p(L) \neq 0$. Since $\mathrm{Gal}(\bar{Q}/Q)$ acts transitively on the p-torsion in E, this implies that L contains all of the p-torsion points, which is implossible since $GL_2(Z/pZ)$ is not solvable when $p > 3$.

Let $\mathrm{D}_{\underline{k}} \in Z[G_S]$ be a derivative operator of order k, with support S where S is a product of primes in $\mathcal{L}_q$. Let $S'|S$ be the conductor of $\mathrm{D}_{\underline{k}}$.

Choose a prime l not dividing S which satisfies the following condition:

$$l \not| B \cdot p \cdot S, \quad Frob_l = [\tau] \text{ in } K_S(E_q)/Q. \tag{4.32}$$

Clearly this implies that l belongs to $\mathcal{L}_{q,E}$. Let P denote the class of $\mathrm{D}_{\underline{k}} y(S)$ in $E(K_S)/qE(K_S)$. Let $T = Sl$, and let $P(l)$ denote the class of $\mathrm{D}_{\underline{k}} \cdot \mathrm{D}_l^1 y(T)$ in $E(K_T)/qE(K_T)$. We make the following assumption:

Hypothesis 4.4.2 *For all the derivatives D' which are strictly less than $D_{\underline{k}} D_l^1$, the class of $D' y(T)$ is 0 in the group $E(K_T)/qE(K_T)$.*

Under hypothesis 4.4.2, one has:

Lemma 4.4.3 *The class of $P(l)$ is fixed under the action of Γ_T.*

Proof: Let $\sigma = \sigma_l$ for some l dividing T or $\sigma = \xi_j$ for some j. Then $(1-\sigma)\mathrm{D}_{\underline{k}}\mathrm{D}_l^1 = \mathrm{D}'$, where D' is some derivative which is strictly less than $\mathrm{D}_{\underline{k}}\mathrm{D}_l^1$, by lemma 4.3.2. Hence $(1-\sigma)P(l) = 0$, by hypothesis 4.4.2.

¿From lemma 4.4.1, the following sequence is exact:

$$0 \longrightarrow E(K_T) \xrightarrow{q} E(K_T) \longrightarrow E(K_T)/qE(K_T) \longrightarrow 0. \tag{4.33}$$

Taking Γ_T-invariants yields an exact cohomology sequence

$$0 \longrightarrow E(K)/qE(K) \longrightarrow (E(K_T)/qE(K_T))^{\Gamma_T} \xrightarrow{\delta} H^1(\Gamma_T, E(K_T))_q. \tag{4.34}$$

Let $d(l) = \delta P(l)$. We will identify $d(l)$ with its image by inflation in $H^1(K,E)_q$.

The class $d(l)$ is the global cohomology class which plays a key role in Kolyvagin's method. We now undertake to analyze its properties.

Behavior of the class $d(l)$ under complex conjugation: Complex conjugation τ acts on the group $H^1(K,E)_q$ in the natural way. Let $\delta = (-1)^k$ be the parity of the order of $\mathrm{D}_{\underline{k}}$.

Proposition 4.4.4 *The class $d(l)$ is in the $-\epsilon\delta$–eigenspace for the action of τ.*

Proof: By lemma 4.4.1, the group $E(K_T)$ has no q-torsion, and hence the torsion subgroup $E(K_T)_{tor}$ is killed in $E(K_T)/qE(K_T)$. Hence by lemma 4.2.3 we have

$$\tau[y(T)] = \epsilon\sigma_0[y(T)], \tag{4.35}$$

where $[y(T)]$ denotes the image of $y(T)$ in $E(K_T)/qE(K_T)$. Combining lemma 4.3.3 with the hypothesis 4.4.2 that all lower order derivatives of $y(T)$ vanish, we find:

$$\tau P(l) = -\epsilon\delta\sigma_0 P(l) = -\epsilon\delta P(l). \tag{4.36}$$

The last equality follows from lemma 4.4.3. Since the map δ used to construct the class $d(l)$ from $P(l)$ is equivariant with respect to the Galois actions, it follows that $d(l)$ is in the $-\epsilon\delta$-eigenspace for τ.

Local behavior of the class $d(l)$: Given a place v of K, let $d(l)_v$ denote the restriction of $d(l)$ in $H^1(K_v, E)_q$. ¿From condition (4.32), one sees that the prime l is inert in K/Q. Let λ be the place of K above it. The prime λ splits completely in K_S/K; choose a place λ' of K_S above λ. Finally, the extension K_T/K_S is completely ramified at λ'; let λ'' denote the unique place of K_T above λ'. The localization $d(l)_\lambda$ belongs to

$$H^1(\mathrm{Gal}((K_T)_{\lambda''}/K_\lambda), E((K_T)_{\lambda''}))_q = H^1(G_l, E((K_T)_{\lambda''})).$$

Fact 4.4.5 *The choice of generator σ_l of G_l determines a canonical inclusion of $H^1(G_l, E((K_T)_{\lambda''}))_q$ inside $E_q(k_\lambda)$.*

Proof: Since the kernel of the reduction map $E((K_T)_{\lambda''}) \longrightarrow E(k_\lambda)$ is a pro-l group, the group $H^1(G_l, E((K_T)_{\lambda''}))_q$ injects into $H^1(G_l, E(k_\lambda))_q = \hom(G_l, E(k_\lambda))_q$. The latter group can be identified with $E(k_\lambda)_q$ thanks to the chosen generator σ_l of G_l.

Theorem 4.4.6 .

1. *For all archimedean places and all places which do not divide l or the conductor S' of $D_{\underline{k}}$, the class $d(l)_v$ is equal to 0.*

2. *The image of $d(l)_\lambda$ in $E(k_\lambda)_q$ is equal to*

$$\frac{(l+1)\tau - a_l}{q}\tilde{P},$$

where $\tilde{P}$ is the reduction of P mod λ'.

Proof:

1. If v is archimedean, then $K_v = C$ and E/K_v has trivial Galois cohomology. Suppose now that v is a non-archimedean place not lying above $S'l$. By construction the class $d(l)_v$ is inflated from a class in $H^1(K_{S'l}/K, E)_q$. Since the extension $K_{S'l}$ is unramified at v, the class $d(l)_v$ comes from a class in $H^1(K_v^{unram}/K_v, E)_q$. Let E^0 denote the connected component of the Néron model at v, and let $J_v = E/E_0$. The group $H^1(K_v^{unram}/K_v, E^0)$ vanishes, (cf. [Mi] ch. I, prop. 3.8), and hence $H^1(K_v^{unram}/K_v, E)_q$ injects into $H^1(K_v^{unram}/K_v, J_v)_q$. But this group is trivial because J_v has order prime to q. Hence the class $d(l)_v$ vanishes.

2. The image of $d(l)_\lambda$ in $E(k_\lambda)$ by the isomorphism defined above is the point

$$red_{\lambda''}\left(\frac{(\sigma_l - 1)P(l)}{q}\right) = red_{\lambda''}\left(\frac{(\sigma_l - 1)\mathrm{D}_l\mathrm{D}_{\underline{k}}y(T)}{q}\right),$$

where $red_{\lambda''} : E((K_T)_{\lambda''}) \longrightarrow E(k_\lambda)$ is the reduction map. But

$$\begin{aligned}(\sigma_l - 1)\mathrm{D}_l\mathrm{D}_{\underline{k}}y(T) &= (l + 1 - N_l)\mathrm{D}_{\underline{k}}y(T) \text{ (by lemma 4.3.2)} &(4.37)\\ &= (l+1)\mathrm{D}_{\underline{k}}y(T) - a_l\mathrm{D}_{\underline{k}}y(S) \text{ (by prop. 4.2.1)} &(4.38)\end{aligned}$$

Hence,

$$red_{\lambda''}\left(\frac{(\sigma_l - 1)P(l)}{q}\right) = red_{\lambda''}\left(\frac{l+1}{q}\tau\mathrm{D}_{\underline{k}}y(S) - \frac{a_l}{q}\mathrm{D}_{\underline{k}}y(S)\right), \quad (4.39)$$

by prop. 4.2.2 combined with the fact that $Frob_{\lambda'} = \tau$. Since $\tilde{P} = red_{\lambda''}(\mathrm{D}_{\underline{k}}y(S))$, the lemma is proved.

We will be exploiting the cohomology class $d(l)$ in the following way. Let $Sel_q(S') \subset Sel_q(E/K)$ be the kernel of the map

$$Sel_q(E/K) \longrightarrow \oplus_{v|S'} E(K_v)/qE(K_v) \quad (4.40)$$

As explained in section 4.1, the local Tate duality gives a map

$$H^1(K_\lambda, E)_q \longrightarrow Sel_q(S')^*. \quad (4.41)$$

Corollary 4.4.7 *The local class $d(l)_\lambda$ is in the kernel of the map*

$$H^1(K_\lambda, E)_q^{-\epsilon\delta} \longrightarrow (Sel_q(S')^*)^{-\epsilon\delta}.$$

Proof: This is a consequence of part 1 of theorem 4.4.6, combined with the orthogonality relations between global classes and the Selmer group which are described in proposition 4.1.5.

4.5 An application of the Chebotarev density theorem

We make the following hypothesis:

Hypothesis 4.5.1 *The point $P = D_{\underline{k}}y(S)$ is not the q–th power of a point in $E(K_S)$.*

If M is a finite Z/qZ-module, it can be decomposed as a direct product

$$M = (Z/qZ)^{r_q(M)} \times M', \tag{4.42}$$

where M' is of exponent strictly dividing q. The integer $r_q(M)$ is well-defined.

Hypothesis 4.5.2 $r_q(Sel_q(S')^{-\epsilon\delta}) \geq 1$.

Set $F = K_S(E_q)$. We start with a few cohomological lemmas.

Lemma 4.5.3 *The fields K_S and $K(E_q)$ are linearly disjoint over K.*

Proof: The intersection of the K_S and $K(E_q)$ is a subfield of $K(E_q)$ which is abelian over K and hence is contained in $K(\mu_q)$, since $\mathrm{Gal}(K(E_q)/K) = GL_2(Z/qZ)$. But $K_S \cap K(\mu_q) = K$, since S and q are relatively prime.

Lemma 4.5.4 *The restriction map $H^1(K, E_q) \longrightarrow H^1(K_S, E_q)$ is injective.*

Proof: Its kernel is the group $H^1(K_S/K, E_q(K_S))$ which is trivial since $E_q(K_S) = 0$ by lemma 4.5.3.

Lemma 4.5.5 *The restriction map $H^1(K_S, E_q) \longrightarrow H^1(F, E_q)$ is injective.*

Proof: By lemma 4.5.3, we have $\mathrm{Gal}(F/K_S) = GL_2(Z/qZ)$, and the kernel of the restriction map is the group

$$H^1(F/K_S, E_q) = H^1(GL_2(Z/qZ), E_q). \tag{4.43}$$

This group is trivial by lemma 4.1.2, and the result follows.

Lemma 4.5.6 *The restriction map $H^1(K, E_q) \longrightarrow H^1(F, E_q)$ is injective.*

Proof: Combine lemmas 4.5.4 and 4.5.5.

Let l be a rational prime satisfying the condition

Condition 4.5.7 *$l \not| B \cdot p \cdot S$, $\quad Frob_l = [\tau]$ in F/Q.*

In this case, l is inert in K/Q. Let λ be the unique prime of K above l. The prime λ splits completely in F/K. Choose a prime λ_F of F above it. The residue field of F at λ_F is identified with k_λ.

Proposition 4.5.8 *There exists a prime l satisfying the condition 4.5.7 such that*

1. *The image of $\tilde{P}$ in $E(k_\lambda)/qE(k_\lambda)$ is non-zero.*
2. *The map $Sel_q(S')^{-\epsilon\delta} \longrightarrow (E(k_\lambda)/qE(k_\lambda))^{-\epsilon\delta}$ is surjective.*

Proof: By the hypothesis 4.5.1, the class P in $E(K_S)/qE(K_S)$ is non-trivial. Complex conjugation acts on $E(K_S)/qE(K_S)$ in a natural way, and P can be written uniquely as a sum of projections onto the $+$ and $-$ eigencomponents for this action. At least one of these projections is non-trivial: call it P'. The cohomology class in $H^1(K_S, E_q)$ corresponding to P' is also non trivial; hence, so is its restriction in $H^1(F, E_q)$, by lemma 4.5.5. Let ζ_1 denote this restriction.

By hypothesis 4.5.2, we may choose an element of order exactly q in $Sel_q(S')^{-\epsilon\delta}$, and the image ζ_2 of this element in $H^1(F, E_q)$ is still of order exactly q, by lemma 4.5.6.

Both ζ_1 and ζ_2 are homomorphisms from $\mathrm{Gal}(F^{ab}/F)$ into E_q. Let $\tilde{F}$ be the smallest extension of F which is cut out by ζ_1 and ζ_2 and is Galois over Q. Let $U = \mathrm{Gal}(\tilde{F}/F)$. There is an exact sequence

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathrm{Gal}(\tilde{F}/F) & \longrightarrow & \mathrm{Gal}(\tilde{F}/K_S) & \longrightarrow & \mathrm{Gal}(F/K_S) & \longrightarrow & 1 \\ & & \| & & & & \| & & \\ & & U & & & & GL_2(Z/qZ) & & \end{array} \tag{4.44}$$

which determines a $GL_2(Z/qZ)$-action on U. Similarly, complex conjugtion τ acts on U by inner automorphisms. The cohomology classes ζ_1, and ζ_2 are fixed under the action of $GL_2(Z/qZ)$ on $\hom(U, E_q)$, since they come from classes in $H^1(K_S, E_q)$ by inflation. Let U^+ denote the subspace of U which is fixed by τ. The class ζ_1 belongs to a fixed eigenspace of $\hom(U, E_q)$ for the action of τ, by construction. The class ζ_2 belongs to the $\epsilon\delta$–eigenspace, since it comes from a class in $Sel_q(S')^{-\epsilon\delta}$. Hence both ζ_1 and $p^{M-1}\zeta_2$ are non-zero on U^+. Otherwise, they would map U onto a given eigenspace of E_q for the τ-action, contradicting the $GL_2(Z/qZ)$-invariance of the image. Thus, we can find $\gamma \in U^+$ such that

$$\zeta_1(\gamma) \neq 0, \quad \zeta_2(\gamma) \text{ is of order exactly } q. \tag{4.45}$$

Now choose l such that

$$Frob_l = [\tau\gamma] \text{ in } \tilde{F}/Q. \tag{4.46}$$

One can find such a prime, by the Chebotarev density theorem. Clearly, l satisfies the condition 4.5.7. In addition,

$$\zeta_1(Frob_{\lambda_F}) = \zeta_1(Frob_l^2) = \zeta_1(\gamma^\tau \cdot \gamma) = \zeta_1(\gamma^2) \neq 0. \tag{4.47}$$

Hence, P is not a q-th power in $E(k_\lambda)/qE(k_\lambda)$, and condition 1 is satisfied. By the same computation, one shows that $\zeta_2(Frob_{\lambda_F})$ is of order exactly q in E_q, which implies that the image of ζ_2 in $H^1(K_\lambda, E_q)^{-\epsilon\delta}$ is itself of order exactly q, so that condition 2 is satisfied as well, since

$$(E(K_\lambda)/qE(K_\lambda))^{-\epsilon\delta} \simeq Z/qZ. \tag{4.48}$$

This proves the proposition.

4.6 A vanishing theorem for derivatives of Heegner points

Given a Z/qZ-module M, define $r_p(M)$ to be

$$r_p(M) = \dim_{F_p}(M \otimes F_p). \tag{4.49}$$

Lemma 4.6.1 *If* $0 \longrightarrow A' \longrightarrow A \xrightarrow{f} A''$ *is an exact sequence of* Z/qZ*-modules, then*

$$r_q(A) \leq r_q(A') + r_p(A'').$$

Proof: We may assume without loss of generality that f is surjective. Let N denote the image of $A_{p^{M-1}}$ in A''. Because of the surjectivity assumption, the module A''/N is annihilated by p. There is a natural exact sequence of F_p-vector spaces:

$$\begin{array}{ccccc} 0 \longrightarrow p^{M-1}A' \longrightarrow & p^{M-1}A & \longrightarrow & A''/N \\ & p^{M-1}a & \mapsto & f(a). \end{array} \tag{4.50}$$

Hence

$$\dim_{F_p}(p^{M-1}A) \leq \dim_{F_p}(p^{M-1}A') + \dim_{F_p}(A''/N). \tag{4.51}$$

The lemma now follows from the fact that $\dim_{F_p}(p^{M-1}A) = r_q(A)$ (and likewise for A') and from the inequality $\dim_{F_p}(A''/N) \leq r_p(A'')$.

Lemma 4.6.2 *For any prime v of K which lies above a prime of $\mathcal{L}_q$,*

$$r_p(E(K_v)/qE(K_v)^{-\epsilon\delta}) \leq 1.$$

Proof: We have

$$r_p(E(K_v)/qE(K_v)) = r_p(E(K_v)/pE(K_v)) = r_p(E(k_v)/pE(k_v)), \tag{4.52}$$

because the norm of v is prime to p. Since $E(k_v)$ is a finite group, the group $E(k_v)/pE(k_v)$ is isomorphic to $E_p(k_v)$ which is at most 2 dimensional. Moreover, we know that

$$\# E(k_v)^{\pm} = l + 1 \mp a_l. \tag{4.53}$$

Since p divides $l+1$, the order of $E(k_v)$ is divisible by p if and only if p divides a_l, and then p divides the order of each eigenspace so that $r_p(E(k_v)/pE(k_v)^{\pm}) = 1$.

Let $\mathrm{D}_{\underline{k}}$ be as in the previous section a derivative with support S and conductor S'. Let $\delta = (-1)^{\mathrm{order}(\mathrm{D}_{\underline{k}})}$ be the parity of the order of $\mathrm{D}_{\underline{k}}$. The main result of this section relates the vanishing of the derivatives $P = \mathrm{D}_{\underline{k}}y(S)$ of Heegner points to the size of the q-Selmer group Sel_q of E over K. Let $Sel_q^{\pm}$ denote the plus and minus eigenspaces of the q- Selmer group for the action of complex conjugation.

Theorem 4.6.3 *If $order(D_{\underline{k}}) < r_q(Sel_q^{-\epsilon\delta})$, then $D_{\underline{k}}y(S) = 0$.*

Proof: The *weight* of $\mathrm{D}_{\underline{k}}$ is defined to be

$$wt(\mathrm{D}_{\underline{k}}) = \mathrm{order}(\mathrm{D}_{\underline{k}}) - \#\{l|S \text{ such that } l \text{ belongs to } \mathcal{L}_{q,E}\ \}. \tag{4.54}$$

We will show theorem 4.6.3 by induction on $wt(\mathrm{D}_{\underline{k}})$.

Step 1: Case where $wt(\mathrm{D}_{\underline{k}}) < 0$. In that case, $\mathrm{D}_{\underline{k}}$ contains a factor of the form D_l^0, with $l \in \mathcal{L}_{q,E}$. But then, by proposition 4.2.1,

$$\mathrm{D}_l^0 y(S) = a_l \cdot y(S/l), \tag{4.55}$$

which is 0, since q divides a_l by lemma 4.3.1. Thus one always has $\mathrm{D}_{\underline{k}} y(S) = 0$, without assuming any inequality between the order of $\mathrm{D}_{\underline{k}}$ and $r_q(Sel_q^{-\epsilon\delta})$!

Step 2: Proof for $wt(\mathrm{D}_{\underline{k}}) = w \geq 0$: We make the induction hypothesis that theorem 4.6.3 holds in weight strictly less than w. We argue by contradiction, assuming that $P = \mathrm{D}_{\underline{k}} y(S)$ is non-zero but that

$$\mathrm{order}(\mathrm{D}_{\underline{k}}) < r_q(Sel_q^{-\epsilon\delta}). \tag{4.56}$$

Lemma 4.6.4 $r_q(Sel_q(S')^{-\epsilon\delta}) > 0$.

Proof: From the exact sequence

$$0 \longrightarrow Sel_q(S')^{-\epsilon\delta} \longrightarrow Sel_q^{-\epsilon\delta} \longrightarrow \oplus_{v|S'}(E(K_v)/qE(K_v))^{-\epsilon\delta}, \tag{4.57}$$

we find from lemma 4.6.1

$$\begin{aligned} r_q(Sel_q^{-\epsilon\delta}) &\leq r_q(Sel_q(S')^{-\epsilon\delta}) + r_p(\oplus_{v|S'} E(K_v)/qE(K_v)^{-\epsilon\delta}) \\ &\leq r_q(Sel_q(S')^{-\epsilon\delta}) + \#\{l|S'\} \quad \text{(by lemma 4.6.2)} \\ &\leq r_q(Sel_q(S')^{-\epsilon\delta}) + \mathrm{order}(\mathrm{D}_{\underline{k}}). \end{aligned}$$

It follows that

$$r_q(Sel_q(S')^{-\epsilon\delta}) \geq r_q(Sel_q^{-\epsilon\delta}) - \mathrm{order}(\mathrm{D}_{\underline{k}}) > 0, \tag{4.58}$$

as was to be shown.

By proposition 4.5.8 we can choose a prime l satisfying the conditions

Conditions 4.6.5 .

1. *$Frob_l = \tau$ in $K_S(E_q)/Q$.*
2. *$\tilde{P} \neq 0$ in $E(k_\lambda)/qE(k_\lambda)$.*
3. *The map $Sel_q(S')^{-\epsilon\delta} \longrightarrow (E(K_\lambda)/qE(K_\lambda))^{-\epsilon\delta}$ is surjective.*

The crucial observation is that the hypothesis 4.4.2 of section 4.4 is still satisfied in our new setting.

Lemma 4.6.6 *The derivative $D_{\underline{k}}D_l^1$ satisfies the hypothesis 4.4.2 of section 4.4.*

Proof: Let D' be a derivative which is strictly less than $\mathrm{D}_{\underline{k}}\mathrm{D}_l^1$. We assume without loss of generality that the order of D' is equal to k, the order of $\mathrm{D}_{\underline{k}}$. Thus in particular the parities of these orders are the same, and we have

$$order(\mathrm{D}') < r_q(Sel_q^{-\epsilon\delta}). \tag{4.59}$$

Since the support of D' is divisible by an extra prime in $\mathcal{L}_{q,E}$,

$$wt(\mathrm{D}') < wt(\mathrm{D}_{\underline{k}}) \tag{4.60}$$

Thus we may apply the induction hypothesis to conclude that $\mathrm{D}'y(T) = 0$.

Because of this lemma, we can apply the general construction of section 4.4, to obtain a class $d(l)$ in $H^1(K,E)_q$. Combining 1 and 2 of conditions 4.6.5 satisfied by l with theorem 4.4.6, we find

$$d(l)_\lambda \neq 0. \tag{4.61}$$

By corollary 4.4.7, it follows that the map

$$H^1(K_\lambda, E)_q^{-\epsilon\delta} \longrightarrow (Sel_q(S')^{-\epsilon\delta})^* \tag{4.62}$$

fails to be injective. Taking duals and using the perfect local Tate duality, this shows that $Sel_q(S')^{-\epsilon\delta}$ does not surject onto $(E(K_\lambda)/qE(K_\lambda))^{-\epsilon\delta}$, contradicting the third of the conditions 4.6.5 on l. This contradiction proves the theorem.

We now derive some consequences of the main result.

Proposition 4.6.7 *If order*$(D_{\underline{k}}) < r_q(Sel_q^{\epsilon\delta}) - 1$, *then* $D_{\underline{k}}y(S) = 0$.

Proof: Suppose that $P = \mathrm{D}_{\underline{k}}y(S) \neq 0$. Then, by proposition 4.5.8, we can choose a prime l such that

1. $Frob_l = \tau$ in $K_S(E_q)/Q$.
2. $\tilde{P} \neq 0$ in $E(k_\lambda)/qE(k_\lambda)$.

We observe that the point $\mathrm{D}_{\underline{k}}\mathrm{D}_l^1 y(T) = P(l)$ is non-zero in $E(K_T)/qE(K_T)$. For, either there is a derivative D' strictly less than $\mathrm{D}_{\underline{k}}\mathrm{D}_l^1$ such that $\mathrm{D}'y(T)$ is non-zero, in which case we are done by lemma 4.3.2; or $\mathrm{D}_{\underline{k}}\mathrm{D}_l^1$ satisfies the hypothesis 4.4.2, in which case we can apply the general construction of section 4.4 to obtain a cohomology class $d(l)$ in $H^1(K,E)_q$. By theorem 4.4.6, this class is non-zero locally at λ, and hence a fortiori globally. Hence the point $P(l)$ from which it comes is non-zero as well. But the parity δ' of the order of $\mathrm{D}_{\underline{k}}\mathrm{D}_l^1$ is $-\delta$. Hence we have

$$\mathrm{order}(\mathrm{D}_{\underline{k}}\mathrm{D}_l^1) = \mathrm{order}(\mathrm{D}_{\underline{k}}) + 1 < r_q(Sel_q^{-\epsilon\delta'}), \tag{4.63}$$

but theorem 4.6.3 tells us that $P(l) = 0$, which is a contradiction.

Proposition 4.6.8 *If order*$(D_{\underline{k}}) < \max(r_q(Sel_q^+), r_q(Sel_q^-)) - 1$, *then* $D_{\underline{k}}y(S) = 0$.

Proof: If this inequality is true, then either

$$\mathrm{order}(\mathrm{D}_{\underline{k}}) < r_q(Sel_q^{-\epsilon\delta}) \quad \text{or} \quad \mathrm{order}(\mathrm{D}_{\underline{k}}) < r_q(Sel_q^{\epsilon\delta}) - 1. \tag{4.64}$$

The result then follows from either theorem 4.6.3 or proposition 4.6.7.

Proposition 4.6.9 *If* 2*order*$(D_{\underline{k}}) < r_q(Sel_q) - 1$, *then* $D_{\underline{k}}y(S) = 0$.

Proof: The inequality can be rewritten

$$2\mathrm{order}(\mathrm{D}_{\underline{k}}) < r_q(Sel_q^{-\epsilon\delta}) + (r_q(Sel_q^{\epsilon\delta}) - 1). \tag{4.65}$$

Hence order$(\mathrm{D}_{\underline{k}})$ must be less than at least one of the two terms in the above sum. The result follows from either theorem 4.6.3 or proposition 4.6.7.

4.7 The first non-vanishing derivatives of Heegner points

We now examine more closely what happens in the limiting situation of theorem 4.6.3 when order($\mathrm{D}_{\underline{k}}$) $= r_q(Sel_q^{-\epsilon\delta})$. We will make the following assumption:

Hypothesis 4.7.1 *The integer $q = p$ is prime.*

This asumption is made because there are some technical difficulties in dealing with the general case of prime power order. One expects however that similar methods would work in that case as well, at the cost of some further technical complications.

Let $J_{S,p}^{\pm}$ be defined as the cokernel which fits into the following exact sequence:

$$0 \longrightarrow Sel_p(S)^{\pm} \longrightarrow Sel_p^{\pm} \longrightarrow \oplus_{v|S}(E(K_v)/pE(K_v))^{\pm} \longrightarrow J_{S,p}^{\pm} \longrightarrow 0. \tag{4.66}$$

Proposition 4.7.2 *If order($D_{\underline{k}}$) $= r_p(Sel_p^{-\epsilon\delta})$, and $J_{S,p}^{-\epsilon\delta}$ is non-trivial, then $D_{\underline{k}}y(S) = 0$.*

Proof: As in the proof of theorem 4.6.3, we will show theorem 4.7.2 by induction on $wt(\mathrm{D}_{\underline{k}})$.

Step 1: Case where $wt(\mathrm{D}_{\underline{k}}) < 0$. Exactly as in the proof of theorem 4.6.3, one finds that $\mathrm{D}_{\underline{k}}(y(S)) = 0$, without assuming any inequality between the order of $\mathrm{D}_{\underline{k}}$ and $r_p(Sel_p^{-\epsilon\delta})$.

Step 2: Proof for $wt(\mathrm{D}_{\underline{k}}) = w \geq 0$: We make the induction hypothesis that proposition 4.7.2 holds in weight strictly less than w. We reason by contradiction, assuming that $P = \mathrm{D}_{\underline{k}}y(S)$ is non-zero. This implies in particular that $S = S'$ and that $\#\{l|S\} <$ order($\mathrm{D}_{\underline{k}}$).

Lemma 4.7.3 *$r_p(Sel_p(S)^{-\epsilon\delta}) > 0$.*

Proof: From the exact sequence

$$0 \longrightarrow Sel_p(S)^{-\epsilon\delta} \longrightarrow Sel_p^{-\epsilon\delta} \longrightarrow \oplus_{v|S}(E(K_v)/pE(K_v))^{-\epsilon\delta} \longrightarrow J_{S,p}^{-\epsilon\delta} \longrightarrow 0, \tag{4.67}$$

we find

$$\begin{aligned} r_p(Sel_p(S)^{-\epsilon\delta}) &= r_p(Sel_p^{-\epsilon\delta}) - r_p(\oplus_{v|S}(E(K_v)/pE(K_v))^{-\epsilon\delta}) + r_p(J_{S,p}) \\ &\geq r_p(Sel_p^{-\epsilon\delta}) - \#\{l|S\} + r_p(J_{S,p}^{-\epsilon\delta}) \quad \text{(by lemma 4.6.2)} \\ &\geq r_p(J_{S,p}^{-\epsilon\delta}) > 0. \end{aligned}$$

This proves the lemma.

Applying proposition 4.5.8 we can choose a prime l satisfying the conditions

Conditions 4.7.4 .

1. *$Frob_l = \tau$ in $K_S(E_p)/Q$.*
2. *$\tilde{P} \neq 0$ in $E(k_\lambda)/pE(k_\lambda)$.*
3. *The map $Sel_p(S)^{-\epsilon\delta} \longrightarrow (E(K_\lambda)/pE(K_\lambda))^{-\epsilon\delta}$ is surjective.*

Lemma 4.7.5 *The derivative $D_{\underline{k}}D_l^1$ satisfies the hypothesis 4.4.2 of section 4.4.*

Proof: Let D' be a derivative which is strictly less than $\mathrm{D}_{\underline{k}}\mathrm{D}_l^1$. We assume without loss of generality that the order of D' is equal to k, the order of $\mathrm{D}_{\underline{k}}$. Thus in particular the parities of these orders are the same, and

$$order(\mathrm{D}') = r_p(Sel_p^{-\epsilon\delta}). \tag{4.68}$$

Since $J_{S,p}$ is non trivial, then a fortiori $J_{T,p}$ is non trivial. Also, because the support of D' is divisible by an extra prime in $\mathcal{L}_{p,E}$,

$$wt(\mathrm{D}') < wt(\mathrm{D}_{\underline{k}}). \tag{4.69}$$

Thus we may apply the induction hypothesis to conclude that $\mathrm{D}'y(T) = 0$.

This lemma allows us to apply the construction of section 4.4, to obtain a class $d(l)$ in $H^1(K, E)_p$. Combining 1 and 2 of conditions 4.7.4 satisfied by l with theorem 4.4.6, we find

$$d(l)_\lambda \neq 0. \tag{4.70}$$

By corollary 4.4.7, it follows that the map

$$H^1(K_\lambda, E)_p^{-\epsilon\delta} \longrightarrow (Sel_p(S)^{-\epsilon\delta})^* \tag{4.71}$$

fails to be injective. Taking duals and using the perfect local Tate duality, this shows that $Sel_p(S)^{-\epsilon\delta}$ does not surject onto $(E(K_\lambda)/pE(K_\lambda))^{-\epsilon\delta}$, contradicting the third of the conditions 4.7.4 on l. This contradiction proves the theorem.

Proposition 4.7.6 *If order*$(D_{\underline{k}}) = r_q(Sel_q^{\epsilon\delta}) - 1$, *and* $J_{S,p}^{\epsilon\delta}$ *is non trivial, then* $D_{\underline{k}} y(S) = 0$.

Proof: Suppose that $P = \mathrm{D}_{\underline{k}} y(S) \neq 0$. Then, by proposition 4.5.8, we can choose a prime l such that

1. $Frob_l = \tau$ in $K_S(E_p)/Q$.
2. $\tilde{P} \neq 0$ in $E(k_\lambda)/pE(k_\lambda)$.

We observe that the point $\mathrm{D}_{\underline{k}} \mathrm{D}_l^1 y(T) = P(l)$ is non-zero in $E(K_T)/pE(K_T)$. For, either there is a derivative D' strictly less than $\mathrm{D}_{\underline{k}}\mathrm{D}_l^1$ such that $\mathrm{D}' y(T)$ is non-zero, in which case we are done by lemma 4.3.2; or $\mathrm{D}_{\underline{k}}\mathrm{D}_l^1$ satisfies the hypothesis 4.4.2, in which case we can apply the general construction of section 4.4 to obtain a cohomology class $d(l)$ in $H^1(K, E)_p$. By theorem 4.4.6, this class is non-zero locally at λ, and hence a fortiori globally. Hence the point $P(l)$ from which it comes is non-zero as well. But the parity δ' of the order of $\mathrm{D}_{\underline{k}}\mathrm{D}_l^1$ is $-\delta$. Hence we have

$$\mathrm{order}(\mathrm{D}_{\underline{k}}\mathrm{D}_l^1) = \mathrm{order}(\mathrm{D}_{\underline{k}}) + 1 = r_q(Sel_q^{-\epsilon\delta'}). \tag{4.72}$$

Since in addition $J_{Sl,p}^{-\epsilon\delta'}$ is non-trivial, prop. 4.7.2 tells us that $P(l) = 0$, which is a contradiction.

Proposition 4.7.7 *If* 2*order*$(D_{\underline{k}}) = r_p(Sel_p) - 1$, *and* $J_{S,p}$ *is non-trivial, then* $D_{\underline{k}} y(S) = 0$.

Proof: If $\mathrm{D}_{\underline{k}} y(S) \neq 0$, then by theorem 4.6.3 and proposition 4.6.7, we have the inequalities:

$$\mathrm{order}(\mathrm{D}_{\underline{k}}) \geq r_p(Sel_p^{-\epsilon\delta}), \quad \mathrm{order}(\mathrm{D}_{\underline{k}}) \geq r_p(Sel_p^{\epsilon\delta}) - 1. \tag{4.73}$$

The equality

$$2\text{order}(\mathrm{D}_{\underline{k}}) = r_p(Sel_p^{-\epsilon\delta}) + (r_p(Sel_p^{\epsilon\delta}) - 1) \tag{4.74}$$

implies that equalities hold everywhere in (4.73). Since at least one of $J_{S,p}^{-\epsilon\delta}$ or $J_{S,p}^{\epsilon\delta}$ is non-trivial, we can apply either proposition 4.7.2 or proposition 4.7.6 to conclude.

Let r denote the rank of the Mordell-Weil group of $E(K)$. The main result of this section is the following:

Theorem 4.7.8 *If* $2\mathit{order}(D_{\underline{k}}) = r - 1$, *then* $D_{\underline{k}}y(S)$ *belongs to the image of the map* $E(K)/pE(K) \longrightarrow E(K_S)/pE(K_S)$.

Proof: Since all derivatives of lower order than $\mathrm{D}_{\underline{k}}$ vanish on $y(S)$, we have

$$\mathrm{D}_{\underline{k}}y(S) \in (E(K_S)/pE(K_S))^{\Gamma_S}. \tag{4.75}$$

On the other hand there is an exact sequence (cf. equation (4.34) of section 4.4):

$$0 \longrightarrow E(K)/pE(K) \longrightarrow (E(K_S)/pE(K_S))^{\Gamma_S} \longrightarrow H^1(K, E)_p \tag{4.76}$$

The image $d(S)$ of $\mathrm{D}_{\underline{k}}y(S)$ in $H^1(K, E)_p$ has the property (by theorem 4.4.6) that its image in $H^1(K_v, E)_p$ is 0 for all v not dividing S. Since $d(S)$ is a global cohomology class, its image in $\oplus_{\lambda|S}H^1(K_\lambda, E)_p$ belongs to the kernel of the natural map

$$\oplus_{\lambda|S}H^1(K_\lambda, E)_p \longrightarrow Sel_p^* \tag{4.77}$$

given by the local Tate duality, by proposition 4.1.5. Suppose that $\mathrm{D}_{\underline{k}}y(S)$ is non zero. Then by prop. 4.6.9 $r_p = r$ and hence $\ {}_p(E/K) = 0$. Also, by prop. 4.7.7, the cokernel $J_{S,p}$ is trivial, so that Sel_p surjects onto $\oplus_{\lambda|S}E(K_\lambda)/pE(K_\lambda)$. By the Tate duality, this means that the map (4.77) is injective, so that the cohomology class $d(S)$ is trivial locally everywhere. Since $\ {}_p(E/K) = 0$, this implies that $d(S) = 0$, and hence, the obstruction to $\mathrm{D}_{\underline{k}}y(S)$ coming from $E(K)/pE(K)$ vanishes.

The previous theorem tells us that the $(r-1)/2$nd derivatives of Heegner points give rise to points in the Mordell-Weil group $E(K)$ by p-descent.

4.8 The order of vanishing of $\theta'(E,S)$

In this section, we will show how proposition 4.6.9 translates into the order of vanishing statement for the element $\theta'(E,S)$ (theorem 3.4.4). To lighten our notations, we will assume that the field K has class number 1 so that $K_1 = K$. It will be clear to the reader that this convention was made only for typographical reasons and could easily be dispensed with.

Let r denote the rank of $E(K)$, and let ρ be the smallest integer greater or equal to $(r-1)/2$. (Since $L(E/K,s)$ vanishes to odd order at $s=1$, the parity conjectures imply that r is odd so that in fact $\rho = (r-1)/2$.)

Let $\Lambda(E,T)$ be the element in $E(K_T) \otimes Z[\Gamma_T]$ made directly from the Heegner points $y(T)$,

$$\Lambda(E,T) = \sum_{\sigma \in \Gamma_T} \sigma y(T) \otimes \sigma. \tag{4.78}$$

We observe that the elements $A(E,S)$ and $A^{\omega}(E,S)$ can be written in terms of these, by the formulas

$$\begin{aligned} A(E,S) &= \sum_{T|S} \mu(T)\Lambda(E,T) \cdot N_{S/T}, & (4.79)\\ A^{\omega}(E,S) &= \sum_{T|S} \mu(T)\omega(T)\Lambda(E,T) \cdot N_{S/T}. & (4.80) \end{aligned}$$

Thus, to prove the order of vanishing statement for $\theta'(E,S)$ in $E(K_S) \otimes E(K_S) \otimes Z[G_S]$, it will be enough to concentrate our attention on the elements $\Lambda(E,T)$.

The essential step in the translation is the following proposition which is analogous to the Taylor theorem in several variables. It gives an expansion for the element $\Lambda(E,T)$ around the augmentation ideal in terms of the derivative operators with support $T = l_1 \cdots l_t$.

Proposition 4.8.1

$$\Lambda(E,T) = \sum_{\underline{k}} D_{\underline{k}} y(T) \otimes (\sigma_{l_1} - 1)^{k_1} \cdots (\sigma_{l_t} - 1)^{k_t},$$

where the sum runs over all s-tuples $\underline{k} = (k_1, \ldots, k_s)$ of positive integers.

Proof: Note that this sum is in fact a finite sum, since the derivative operator $\mathrm{D}_{\underline{k}}$ becomes zero once its order is large enough. The proof is based on the binomial theorem and on rearranging terms in finite sums. It is straightforward, but somewhat messy to write down.

Fix a derivative $\mathrm{D}_{\underline{k}}$ with support T. Let T' denote the conductor of $\mathrm{D}_{\underline{k}}$, and let

$$n(\mathrm{D}_{\underline{k}}) = \gcd_{l|T'}(l+1). \tag{4.81}$$

Lemma 4.8.2 *$n(D_{\underline{k}})(\sigma_{l_1}-1)^{k_1}\cdots(\sigma_{l_t}-1)^{k_t} \in I^{\rho}$.*

Proof: The proof is also straightforward, using the fact that all primes less than ρ are invertible in Z, together with the fact that, if σ is an element of order p, where p is a prime, then $p(\sigma-1)$ belongs to the pth power of the augmentation ideal.

Proposition 4.8.3 *If $order(D_{\underline{k}}) < \rho$, then $n(D_{\underline{k}})$ divides $D_{\underline{k}}y(T)$.*

Proof: We can write

$$\mathrm{D}_{\underline{k}} = \mathrm{D}' \cdot N_{T/T'}, \tag{4.82}$$

where D' is a derivative of support T'. Hence by proposition 4.2.1,

$$\mathrm{D}_{\underline{k}}y(T) = (\prod_{l|(T/T')} a_l) \cdot \mathrm{D}'y(T'). \tag{4.83}$$

If q is a prime power that divides $n(\mathrm{D}_{\underline{k}})$, then all the primes dividing T' are in $\mathcal{L}_q$. Furthermore, since $\rho \leq (r_q(Sel_q)-1)/2$, we have

$$2 \cdot order(\mathrm{D}') < r_q(Sel_q) - 1. \tag{4.84}$$

Hence, by proposition 4.6.9, q divides $\mathrm{D}'y(T')$ and therefore also $\mathrm{D}_{\underline{k}}y(T)$. Since this is true for all q dividing $n(\mathrm{D}_{\underline{k}})$, the result follows.

Proposition 4.8.4 *The element $\Lambda(E,T)$ belongs to $E(K_T) \otimes I^{\rho}$.*

Proof: By considering the Taylor-like expansion of proposition 4.8.1, it suffices to show that the terms

$$\mathrm{D}_{\underline{k}} y(T) \otimes (\sigma_{l_1} - 1)^{k_1} \cdots (\sigma_{l_t} - 1)^{k_t} \tag{4.85}$$

belong to I^ρ. When the order of $\mathrm{D}_{\underline{k}}$ is greater or equal to ρ, this is clear. Otherwise, $n(\mathrm{D}_{\underline{k}})$ divides $\mathrm{D}_{\underline{k}} y(T)$ by proposition 4.8.3. Hence by lemma 4.8.2, the term (4.85) belongs to $E(K_T) \otimes I^\rho$.

We now come to the proof of the theorem 3.4.4 of section 3.4, which we recall:

Theorem 3.4.4 *$\theta'(E, S)$ belongs to $E(K_S) \otimes E(K_S) \otimes I^{r-1}$.*
Proof: ¿From the formulas (4.79) and (4.80) expressing the elements $A(E, S)$ and $A^\omega(E, S)$ in terms of the $\Lambda(E, T)$, it follows that

$$A(E, S) \in E(K_S) \otimes I^\rho, \quad A^\omega(E, S) \in E(K_S) \otimes I^\rho. \tag{4.86}$$

Therefore, $\theta'(E, S)$ belongs to $E(K_S) \otimes E(K_S) \otimes I^{2\rho}$. Since $2\rho = r - 1$ if r is odd, and $r + 1$ is r is even, we are done.

4.9 The leading coefficient

We now turn to the analysis of the leading coefficient $\tilde{\theta}'(E, S)_p$ reduced mod p, and give the prof of theorem 3.4.6.
Theorem 3.4.6

1. *$\tilde{\theta}'(E, S)_p$ belongs to $E(K) \otimes E(K) \otimes (I_p^{r-1}/I_p^r)$.*

2. *If p divides $\#$ $(E/K) J_S$, then $\tilde{\theta}'(E, S)_p = 0$.*

Proof: The first part follows from theorem 4.7.8, combinde with the Taylor expansion of prop. 4.8.1.

If $p|\#$ (E/K), then $r_p > r$, and prop. 4.6.9 implies that $\tilde{\theta}'(E, S)_p = 0$. Likewise, if $p|J_S$, then the group $J_{S,p}$ is non-trivial, and hence by prop. 4.7.7, $\tilde{\theta}'(E, S)_p = 0$.

Bibliography

[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.

[BFH] D. Bump, S. Friedberg and J. Hoffstein, *A non-vanishing theorem for derivatives of automorphic L-functions with applications to elliptic curves*, Bull. AMS Math. Soc. 21 (1989), 89-93.

[DR] P. Deligne and K. Ribet, *Values of abelian L-functions at negative integers over totally real fields*, Invent. Math. 59 (1980), pp. 227-286.

[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, *Heights and the special values of L-series*, Proceedings of the 1985 Montreal conference on number theory, June 17-29, 1985, Canadian Mathematical Society, pp. 115-188.

[Gr3] B.H. Gross, *On the values of abelian L-functions at* $s = 0$, Journal of the Faculty of Science, the University of Tokyo, Sect. IA, Math. Vol. 35, No. 1, pp. 177-197, March, 1988.

[Gr4] B.H. Gross, *Kolyvagin's work on modular elliptic curves*, Proc. Durham symposium on L-functions and arithmetic, 1989, to appear.

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

[H1] Alfred W. Hales, *Augmentation terminals of finite abelian groups*, in SLN 1006, 1983, pp. 720-733.

[H2] Alfred W. Hales, *Stable augmentation quotients of abelian groups*, Pacific Journal of Math, vol 118, no. 2, 1985, pp. 401-410.

[Iw] K. Iwasawa, *On Z_l-extensions of algebraic number fields*, Annals of Mathematics, second series, vol. 98, no. 2, 1973.

[Ko1] V.A. Kolyvagin, *Finiteness of $E(Q)$ and (E/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). To appear in a Birkhäuser volume in honor of Grothendieck.

[La] S. Lang, Cyclotomic fields I and II, combined second edition, GTM 121, Springer-Verlag 1990.

[Ma1] B. Mazur, *Courbes elliptiques et symbole modulaire*, Séminaire Bourbaki 414 (1971/1972), in LNM 317, Springer-Verlag, Berlin.

[Ma2] B. Mazur, *Modular curves and arithmetic*, Proceedings of the International Congress of Mathematicians, August 16-24, 1983, Warszawa.

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

[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.

[MW] B. Mazur and A. Wiles, *Class fields of abelian extensions of Q*, Invent. Math. 76, (1984) pp. 179-330.

[Mi] J.S. Milne, Arithmetic duality theorems. Perspectives in mathematics. Academic Press, 1986.

[MM] M. Ram Murty and V. Kumar Murty, *Mean values of derivatives of modular L-series* , Annals of Math., to appear.

[Pa] I.B.S. Passi, Group rings and their augmentation ideals, SLN 715, Berlin-New York, 1979.

[Ru1] K.C. Rubin, *Global units and ideal class groups*, Invent. Math. 89, 511-526, (1987).

[Ru2] K.C. Rubin, *Tate-Shafarevich groups and L-functions of elliptic curves with complex multiplication*, Invent. Math. 89, 527-560, (1987).

[Ru3] K.C. Rubin, *On the main conjecture of Iwasawa theory for imaginary quadratic fields*, Invent. Math. 93, 701-713, (1988).

[Ru4] K. Rubin, Appendix to S. Lang, Cyclotomic Fields I and II, combined second edition, GTM 121, Springer-Verlag, 1990.

[Ru5] K. Rubin *Kolyvagin's system of Gauss sums*, unpublished.

[Sch] R. Schoof, preprint.

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

[Th] F. Thaine, *On the ideal class groups of real abelian number fields*, Ann. of Math. 128 (1988), pp. 1-18.

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

[Wa] L. Washington, Introduction to cyclotomic fields, GTM 83, New York, Springer-Verlag (1982).

[We] A. Weil, *De la métaphysique aux mathématiques*, Sciences, p. 52-56, 1960.