The Conjecture of Birch and Swinnerton-Dyer for elliptic curves with complex multiplication by a nonmaximal order.

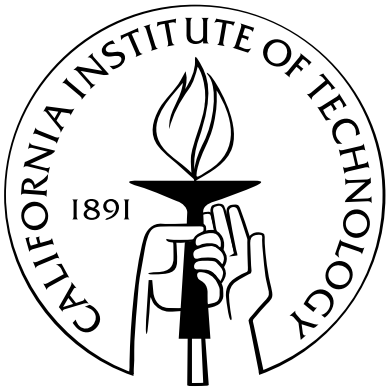
Thesis by

Jason Colwell

In Partial Fulfillment of the Requirements

for the Degree of

Doctor of Philosophy



California Institute of Technology

Pasadena, California

2004

(Defended 18 November 2003)

Acknowledgements

First, I would like to thank my advisor, Matthias Flach, for his instruction during my graduate studies, including his suggestion of this topic, and his help in the writing of this thesis. I am grateful to the Department of Mathematics at Caltech for providing a congenial environment for study and research. I would like to thank my father and mother for their support and encouragement throughout my doctoral program. Finally, I would like to thank my girlfriend, Charlene, for her constant encouragement and personal support during the writing of this thesis.

Abstract

The Conjecture of Birch and Swinnerton-Dyer relates an analytic invariant of an elliptic curve – the value of the **L-function**, to an algebraic invariant of the curve – the order of the **Tate–Šafarevič group**. Gross has refined the Birch–Swinnerton-Dyer Conjecture in the case of an elliptic curve with complex multiplication by the full ring of integers in a quadratic imaginary field. It is this version which interests us here. Gross' Conjecture has been reformulated, by Fontaine and Perrin-Riou, in the language of derived categories and determinants of perfect complexes. Burns and Flach then realized that this immediately leads to a refined conjecture for elliptic curves with complex multiplication by a nonmaximal order. The conjecture is now expressed as a statement concerning a generator of the image of a map of 1-dimensional modules. We prove this conjecture of Burns and Flach.

Contents

Chapter 0

Introduction.

The Conjecture of Birch and Swinnerton-Dyer relates an analytic invariant of an elliptic curve – the value of the **L-function**, to an algebraic invariant of the curve – the order of the **Tate–Šafarevič group**.

In our situation, the elliptic curve E is defined over a number field F. The L-function, like the classical Riemann zeta function, is defined as a product over prime ideals of F. The Tate–Shavarevich group is the group of 1-cohomology classes of E which are locally trivial at each place of F.

For most elliptic curves E, the ring of endomorphisms $\mathrm{End}(E)$ is isomorphic to $\mathbb{Z}$. However, there are some elliptic curves whose endomorphism ring is larger. In this case, E is said to have **complex multiplication**. It is elliptic curves with this additional structure which interest us here. The basic theory of the subject shows that if E has complex multiplication, then $\mathrm{End}(E)$ is isomorphic to an order $\mathcal{O}$ in a quadratic imaginary field K.

Gross has refined the Birch–Swinnerton-Dyer Conjecture in the case where $\mathcal{O}$ is the full ring of integers $\mathcal{O}_K$. It is this version which interests us here. He uses the fact that the L-function of an elliptic curve with complex mul-

tiplication agrees with the product of two L-functions of a Grössencharacter of F, associated to E, with values in K. Gross' idea is to consider the two L-functions separately, making a conjecture about each, viewing it as the K-equivariant L-function. He formulates a complex regulator in place of the real regulator used in the original conjecture. As well, he uses the order ideal of a group in place of the cardinality of the group.

Rubin has proved the $\mathfrak{p}$-part of Gross' conjecture in the case where $F = K$ (i.e., the class number of K is 1) and $\mathfrak{p}$ does not divide $|\mu_{\mathcal{O}_K}|$ (the number of roots of unity in K), under the condition $\operatorname{rank}(E(F)) = 0$. Some cases of Gross conjecture with $F \neq K$ will follow from our results below.

Gross' Conjecture has been reformulated, by Fontaine and Perrin-Riou, in the language of derived categories and determinants of perfect complexes. Burns and Flach then realized that this immediately leads to a conjecture which is a refinement in the case where $\mathcal{O} \neq \mathcal{O}_K$. The conjecture is now expressed as a statement concerning a generator of the image of a map of 1-dimensional modules. We wish to prove the p-part of this conjecture of Burns and Flach for elliptic curves with complex multiplication by a nonmaximal order, i.e., where $\mathcal{O} \neq \mathcal{O}_K$, and where necessarily $F \neq K$. We shall use Rubin's restrictions

$$\operatorname{rank}(E(F)) = 0$$

$$F(E_{\mathrm{tors}})/K \text{ is abelian}$$

$$p \not| |\mu_{\mathcal{O}_H}|$$

(H being the Hilbert Class field of K). In fact we shall also assume for simplicity that K has class number 1 (i.e., $H = K$).

The formulation of Burns–Flach naturally allows a further refinement of the conjecture, dealing with the Weil restriction B of E, and considering $\mathcal{R}_p$-modules in place of $\mathcal{O}_p$-modules, where $\mathcal{R} = \mathrm{End}(B)$. (The conjecture will be over the endomorphism algebra R of B, which is much larger than K.) We shall prove this conjecture by reducing it to the Main Conjecture for imaginary quadratic fields. At this point we need to make the further assumption that

$$p \not| [K^{\mathfrak{f}_0 p} : K],$$

where $\mathfrak{f}_0$ is the prime-to-p part of the conductor of B and $K^{\mathfrak{m}}/K$ denotes the ray class field of conductor $\mathfrak{m}$, because Rubin's proof of the Main Conjecture requires this condition.

We shall use a method of Kato to address this situation, first dualizing the modules involved, then passing to a situation universal with respect to invertible sheaves over p-adic rings. The conjecture is then seen to follow from two known results, the Explicit Reciprocity Law and Rubin's Main Conjecture.

We first discuss the conjectures which are ancestors of the Burns–Flach Conjecture under consideration, and the translation between the language of the original Birch–Swinnerton-Dyer Conjecture and that of perfect complexes. Next, a deduction of the Burns–Flach Conjecture, from the Main Conjecture and the Explicit Reciprocity Law, is given. Finally, we discuss numerical examples of the conjectures.

Chapter 1

The conjecture of Birch and Swinnerton-Dyer.

We will give the Birch–Swinnerton-Dyer Conjecture in its original generality, applying not only to elliptic curves but to abelian varieties in general. We follow [9] in our exposition.

Let A be an abelian variety of dimension g which is defined over a number field F.

Write $L(A/F, s)$ for the L-series of A over F, which is defined by the Euler product

$$L(A/F, s) = \prod_{w \not| \infty} P_w(A/F, \mathbf{N}w^{-s})^{-1},$$

where for any finite place w of F

$$P_w(A/F, x) := \det(1 - x\phi_w \mid (T_\ell(A) \otimes \mathbb{Q}_\ell)_{I_w}),$$

the characteristic polynomial of the action of Frobenius (ϕ_w) upon the inertia ℓ-adic Tate quotient module $(T_\ell(A) \otimes \mathbb{Q}_\ell)_{I_w}$ (which is the co-invariants, under the action of the inertia group I_w, of the ℓ-adic Tate module $T_\ell(A) \otimes \mathbb{Q}_\ell$).

This polynomial is independent of ℓ and has coefficients in $\mathbb{Z}$. The L-series is convergent in the half-plane $\{s \in \mathbb{C} : \mathrm{Re}(s) > \frac{3}{2}\}$.

Let $Ш(A)$ be the Tate-Šafarevič group

$$\ker\left(H^1(F,A) \to \prod_w H^1(F_w,A)\right)$$

of A over F. (The product is taken over all places w of F.) The following is conjectured to be true, and will be assumed here.

Assumption 1.0.1. $Ш(A)$ *is finite.*

A constant is defined using the Néron model, the invariant differentials on A and their period integrals, and the discriminant of $F/\mathbb{Q}$. The constant will be conjecturally related to the L-function.

Write $\mathcal{A}$ for the Néron model of A, and $\mathcal{A}_w = \mathcal{A} \otimes_{\mathcal{O}_F} k_w$ after a base change to the residue field of F at a finite place w. Write $\mathcal{A}_w^0$ for the connected component of the origin in $\mathcal{A}_w$.

Let $(\omega_1, \ldots, \omega_g)$ be an F-basis of $H^0(A, \Omega_{A/F})$. Denote the projective $\mathcal{O}_F$-module of invariant differentials on the Néron model $\mathcal{A}$ of A, by $\Omega_{\mathcal{A}}$. Then $\bigwedge^g \Omega_{\mathcal{A}}$, restricted to $H^0(A, \Omega^g_{A/F})$, is given by

$$\left(\bigwedge_{i=1}^{g} \omega_i\right) \cdot \mathfrak{D}$$

for some fractional ideal $\mathfrak{D}$ of $\mathcal{O}_F$.

For a complex place w of F, let $(h_1, \ldots, h_{2g})$ be a $\mathbb{Z}$-basis of the integral

homology $H_1(A(F_w), \mathbb{Z})$. Define

$$\Omega_w := \left| \det \left(\int_{h_i} \omega_j \left| \int_{h_i} \overline{\omega}_j \right. \right) \right|.$$

This is non-zero and depends only on $\bigwedge_{i=1}^{g} \omega_i$ and w.

For a real place w of F, corresponding to the embedding $\sigma : F \hookrightarrow \mathbb{R}$, let $(h_1, \ldots, h_g)$ be a $\mathbb{Z}$-basis of $H_1(A(F_w), \mathbb{Z})^+$, the submodule of the integral homology $H_1(A(F_w), \mathbb{Z})$ fixed by complex conjugation. Define

$$\Omega_w := \left| \frac{A^\sigma(\mathbb{R})}{A^\sigma(\mathbb{R})^0} \right| \cdot \left| \det \left(\int_{h_i} \omega_j \right) \right|.$$

This is non-zero and depends only on $\bigwedge_{i=1}^{g} \omega_i$ and w.

Fix bases $(x_1, \ldots, x_n)$ and $(y_1, \ldots, y_n)$ of respective free subgroups $X \subset A(F)$ and $Y \subset A(F)^\vee$ of finite index. (Here $\vee$ indicates the dual abelian variety.) Define the regulator

$$R := \frac{|\det(< x_i, y_j >)|}{\left| \frac{A(F)}{X} \right| \cdot \left| \frac{A^\vee(F)}{Y} \right|},$$

where $<,>$ is the canonical height pairing corresponding to the Poincaré divisor on $A \times A^\vee$. The value of $R \in \mathbb{R}^*$ is independent of X and Y and their bases.

Now we are ready to state the conjecture of Birch and Swinnerton-Dyer:

Conjecture 1.0.2 (Birch–Swinnerton-Dyer). *We have*

$$L(A/F, s) \sim c(s-1)^{\mathrm{rank}_{\mathbb{Z}} A(F)} \text{ as } s \to 1$$

for some constant $c \in \mathbb{R}_+^*$ *such that*

$$\frac{c}{R \cdot \prod_{w|\infty} \Omega_w}$$

lies in $\mathbb{Q}$ *and equals*

$$|\mathrm{disc}_{F/K}|^{-g/2} \cdot \mathbf{N}_{F/\mathbb{Q}}\mathfrak{D} \cdot |Ш(A)| \cdot \prod_{w \nmid \infty} \left| \frac{\mathcal{A}_w(k_w)}{\mathcal{A}_w^0(k_w)} \right|.$$

Note that the last product is well-defined because for all but the finite number of places w of bad reduction, we have $\mathcal{A}_w(k_w) = \mathcal{A}_w^0(k_w)$, and the multiplicand equal to 1.

We are interested in the case where $\mathrm{rank}_{\mathbb{Z}} A(F) = 0$, whereupon the assertion of the conjecture reduces to

$$\frac{L(A/F,1) \cdot |A(F)| \cdot |A^\vee(F)|}{\prod_{w|\infty} \Omega_w} = |\mathrm{disc}_{F/K}|^{-g/2} \cdot \mathbf{N}_{F/\mathbb{Q}}\mathfrak{D} \cdot |Ш(A)| \cdot \prod_{w \nmid \infty} \left| \frac{\mathcal{A}_w(k_w)}{\mathcal{A}_w^0(k_w)} \right| \in \mathbb{Q}.$$

Chapter 2

The Weil restriction.

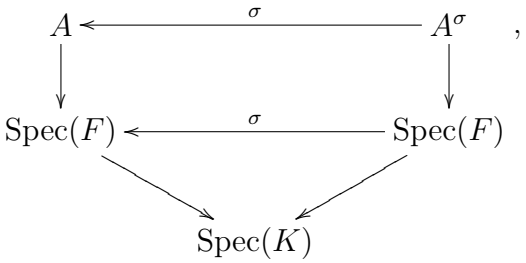
To discuss Gross' refinement of the Birch–Swinnerton-Dyer Conjecture, we will need the Weil restriction. Let A be abelian variety defined over F, an extension of a number field K. The **Weil restriction**

$$B := \mathrm{Res}_K^F A$$

is an abelian variety defined over K, whose construction we recall now.

For simplicity assume that F/K is Galois.

For each element σ of $G := \mathrm{Gal}(F/K)$, we have a commutative diagram of schemes



,

where A^σ is the fibre product of

$$\begin{array}{ccc} A & & \\ \downarrow & & \\ \mathrm{Spec}(F) & \xleftarrow{\ \sigma\ } & \mathrm{Spec}(F). \end{array}$$

Taking the fibre product over all σ, we have

$$\begin{array}{c} \tilde{B} := \prod_{\sigma \in G} A^\sigma \\ \downarrow \\ \mathrm{Spec}(F) \\ \downarrow \\ \mathrm{Spec}(K). \end{array}$$

The finite group G acts on the projective scheme $\tilde{B}$, compatibly with its action on F. Therefore, there exists a scheme B which is the quotient of $\tilde{B}$ by the G-action. B is then defined over K. This variety B is abelian, with the group law inherited from A via $\tilde{B}$. It is seen that B satisfies the desired functorial property:

Lemma 2.0.1. *B is a K-variety such that*

$$\mathrm{Hom}_{\mathrm{Spec}(K)}(Y, B) \simeq \mathrm{Hom}_{\mathrm{Spec}(F)}(Y \otimes_K F, A)$$

for any K-scheme Y. (The functor Res^F_K is the right adjoint of the extension-of-scalars functor $Y \mapsto Y \otimes_K F$.) In particular, for $Y = \mathrm{Spec}(\mathbb{C})$ and a

complex place v of K, we have

$$B(\mathbb{C}) = \mathrm{Hom}_{\mathrm{Spec}(K)}(\mathrm{Spec}(\mathbb{C}), B) \simeq \mathrm{Hom}_{\mathrm{Spec}(F)}(\mathrm{Spec}(\mathbb{C}\otimes_K F), A) = \bigoplus_{w|v} A(F_w).$$

If A is an elliptic curve with complex multiplication by an order $\mathcal{O}$ in an imaginary quadratic field K, this equality of functors provides B with multiplication by (at least) $\mathcal{O}$.

Chapter 3

The conjecture of Gross.

Gross has refined (in [9]) the conjecture of Birch–Swinnerton-Dyer for elliptic curves with complex multiplication.

Let E be an elliptic curve defined over a number field F, with complex multiplication by the ring of integers $\mathcal{O}_K$ of a quadratic imaginary field K. If we fix an isomorphism $\mathcal{O}_K \simeq \mathrm{End}_F(E)$, then the action of $\mathrm{End}_F(E)$ on $\mathrm{Lie}(E)$ gives an embedding $K \hookrightarrow F$. If we fix a complex embedding $K \hookrightarrow \mathbb{C}$, we obtain a Grössencharacter ψ of F with values in $\mathbb{C}^*$. See [21], II, §9.

We replace the $\mathbb{Q}_\ell$-action on the ℓ-adic Tate module $T_\ell(E) \otimes \mathbb{Q}_\ell$ by the $K \otimes \mathbb{Q}_\ell$-action given by complex multiplication. Now the global K-equivariant L-series of E/F is defined

$$ {}_KL(E/F, s) := \prod_{w \not| \infty} {}_KP_w(E/F, \mathbf{N}w^{-s})^{-1}, $$

where

$$ {}_KP_w(E/F, x) = \det_{K \otimes \mathbb{Q}_\ell} (1 - x\phi_w \mid (T_\ell(E) \otimes \mathbb{Q}_\ell)_{I_w}), $$

the characteristic polynomial of the action of Frobenius (ϕ_w) upon the inertia ℓ-adic Tate quotient module $(T_\ell(A) \otimes \mathbb{Q}_\ell)_{I_w}$. The product is over all finite primes of F.

On the other hand, we have the Hecke L-series

$$L(\psi, s) := \prod_{w \not| \infty \cdot \mathfrak{f}_\psi} (1 - \psi(w)\mathbf{N}w^{-s})^{-1}.$$

(The product is over the finite primes of F not dividing the conductor $\mathfrak{f}_\psi$ of ψ.) This product is convergent in the half-plane $\{s \in \mathbb{C} : \mathrm{Re}(s) > \frac{3}{2}\}$ and has an analytic continuation to the entire plane by Hecke. (See [21], II, §10.)

It is known, by a theorem of Deuring, that

$$_K L(E/F, s) = L(\psi, s).$$

Hence we also have

$$L(E/F, s) = L(\psi, s)L(\overline{\psi}, s),$$

reflecting the identity of Euler factors $\mathbf{N}_{K/\mathbb{Q}}({}_K P_w(x)) = P_w(x)$. The aim of Gross' Conjecture is to identify the leading term of $L(\psi, s)$ instead of that of $L(E/F, s)$ (whose leading term is the subject of the Birch–Swinnerton-Dyer Conjecture).

3.1 Choice of bases.

We continue to write $B = \mathrm{Res}_K^F E$ for the Weil restriction of E. The $[F : K]$-dimensional abelian variety B is canonically self-dual and has complex multiplication by $\mathcal{O}_K$. We have

$$_K L(B/K, s) = {}_K L(E/F, s).$$

As before, a "constant" is defined using the Néron model, the invariant differentials on E, and their period integrals. But this time, the "constant" is an ideal in $\mathcal{O}_K$. This ideal will again be conjecturally related to the L-function.

Write $\mathcal{B}$ for the Néron model of B, and $\mathcal{B}_v = \mathcal{B} \otimes_{\mathcal{O}_K} k_v$ after a base change to the residue field of K at a finite place v. Write $\mathcal{B}_v^0$ for the connected component of the origin in $\mathcal{B}_v$.

Let $(\omega_1, \ldots, \omega_{[F:K]})$ be an K-basis of $H^0(B, \Omega_{B/K})$. Denote the projective $\mathcal{O}_K$-module of invariant differentials on the Néron model $\mathcal{B}$ of B, by $\Omega_{\mathcal{B}}$. Then $\bigwedge^{[F:K]} \Omega_{\mathcal{B}}$, restricted to $H^0(B, \Omega_{B/K}^{[F:K]})$, is given by

$$\left(\bigwedge_{i=1}^{[F:K]} \omega_i \right) \cdot \mathfrak{d}$$

for some fractional ideal $\mathfrak{d}$ of $\mathcal{O}_K$.

The integral homology $H_1(B(\mathbb{C}), \mathbb{Z})$ is a projective $\mathcal{O}_K$-module of rank $[F : K]$. Let $(h_1, \ldots, h_{[F:K]})$ be a K-basis of $H_1(B(\mathbb{C}), \mathbb{Q})$. Then

$$\textstyle\bigwedge_{\mathcal{O}_K}^{[F:K]} H_1(B(\mathbb{C}), \mathbb{Z})$$

is given by

$$\left(\bigwedge_{j=1}^{[F:K]} h_j\right) \cdot \mathfrak{b}$$

for some fractional ideal $\mathfrak{b}$ of $\mathcal{O}_K$. Let $(\gamma_1, \ldots, \gamma_{[F:K]})$ be the dual K-basis of $H^1(B(\mathbb{C}), \mathbb{Q})$. Then

$$\bigwedge_{\mathcal{O}_K}^{[F:K]} H^1(B(\mathbb{C}), \mathbb{Z})$$

is given by

$$\left(\bigwedge_{j=1}^{[F:K]} \gamma_j\right) \cdot \mathfrak{b}^{-1}.$$

Define

$$\Omega := \det\left(\int_{h_i} \omega_j\right).$$

This is non-zero.

Fix a basis $(x_1, \ldots, x_n)$ of a free $\mathcal{O}_K$-submodule $X \subset B(K)$ of finite index. Define the complex regulator

$$R_{\mathbb{C}} := \frac{\det(< x_i, x_j >_{\mathbb{C}})}{\left|\frac{B(K)}{X}\right|},$$

where

$$<,>: B(K) \times B(K) \to \mathbb{R}$$

is the height pairing and

$$<,>_{\mathbb{C}}: B(K) \times B(K) \to \mathbb{C}$$

is

$$(x, y) \mapsto \delta < x, y > - < x, \overline{\delta} y >,$$

$\{1, \delta\}$ being a $\mathbb{Z}$-basis of $\mathcal{O}_K$, and $<,>_{\mathbb{C}}$ is independent of the choice of δ. The value of $R_{\mathbb{C}} \in \mathbb{C}^*$ is independent of X and its basis.

3.2 The conjecture.

Let "#" denote the order ideal as an $\mathcal{O}_K$-module.

Now we can state Gross' refinement of the Birch–Swinnerton-Dyer Conjecture.

Conjecture 3.2.1 (Gross). *We have*

$$L(\overline{\psi}, s) \sim c(s-1)^{\mathrm{rank}_{\mathcal{O}_K} B(K)} \text{ as } s \to 1$$

for some constant $c \in \mathbb{C}^*$ *such that*

$$\frac{c}{R_{\mathbb{C}}\Omega}$$

lies in K and generates

$$\mathfrak{b}\cdot\mathfrak{d}\cdot\#(Ш(B))\cdot\prod_{w\nmid\infty}\#\left(\frac{\mathcal{B}_v(k_v)}{\mathcal{B}_v^0(k_v)}\right).$$

We are interested in the case where $\operatorname{rank}_{\mathcal{O}_K}B(K)=0$, whereupon the assertion of the conjecture reduces to

$$\left(\frac{L(\overline{\psi},s)\cdot|B(K)|}{\Omega}\right)=\mathfrak{b}\cdot\mathfrak{d}\cdot\#(Ш(B))\cdot\prod_{w\nmid\infty}\#\left(\frac{\mathcal{B}_v(k_v)}{\mathcal{B}_v^0(k_v)}\right).$$

As explained by Gross, we have

$$\begin{aligned}
\mathbf{N}L(\overline{\psi},s)&=L(B/K,s),\\
\mathbf{N}R_{\mathbb{C}}&=R,\\
\mathbf{N}(\Omega)&=\prod_{w|\infty}\Omega_w\\
\mathbf{N}\mathfrak{b}&=|\operatorname{disc}_{F/K}|^{g/2}\\
\mathbf{N}\mathfrak{d}&=\mathbf{N}_{F/\mathbb{Q}}\mathfrak{D}\\
\mathbf{N}(\#Ш(B))&=|Ш(E)|\\
\mathbf{N}\left(\prod_{w\nmid\infty}\#\left(\frac{\mathcal{B}_v(k_v)}{\mathcal{B}_v^0(k_v)}\right)\right)&=\prod_{v\nmid\infty}\left|\frac{\mathcal{B}_v(k_v)}{\mathcal{B}_v^0(k_v)}\right|.
\end{aligned}$$

(the first three norms being the complex norm $z\mapsto\overline{z}z$, the others being the norm map on ideals) so that the original Birch–Swinnerton-Dyer Conjecture follows from Gross' Conjecture.

Chapter 4

The language of perfect complexes.

In this chapter we reformulate Gross' Conjecture using the language of perfect complexes and their determinants, essentially following Fontaine and Perrin-Riou in [6].

4.1 Determinants of perfect complexes.

By a **complex** we mean a sequence of modules $\{M^j\}_{j\in\mathbb{Z}}$ over some ring, say Q, indexed by the integers, with maps

$$M^j \xrightarrow{d_j} M^{j+1}$$

satisfying $d_{j+1} \circ d_j = 0$ for all $j \in \mathbb{Z}$.

By a **perfect complex** we mean a complex which is quasi-isomorphic to a bounded complex whose terms are finite projective modules. (These are the complexes for which it will be possible to define the determinant.)

The **determinant** of a perfect complex is the alternating tensor product

of the determinants of the modules M^j. Precisely, it is defined as

$$\bigotimes_{j\in\mathbb{Z}} (\det M^j)^{(-1)^j},$$

where M^{-1} denotes the dual of M, and $\det M$ is the highest nontrivial exterior power of M (if M is nontrivial, and Q if $M = 0$).

In the situations we will be considering, the determinant of the complex is also equal to the alternating tensor product of the determinants of the *cohomology* modules $H^j(M^\bullet)$ of the complex:

Lemma 4.1.1. *If Q is regular, then*

$$\det M^\bullet = \bigotimes_{j\in\mathbb{Z}} (\det H^j(M^\bullet))^{(-1)^j}.$$

In particular, when Q is a Dedekind ring or a field, the determinant can be computed this way. (See [14].)

We will use the following implicitly in calculating the determinants of finitely generated torsion modules.

Lemma 4.1.2. *Suppose M is a finitely generated torsion module over a discrete valuation ring Q with quotient field F Then the determinant of M is given by:*

$$\begin{array}{ccccc} \det_F(M\otimes_Q F) & = & \det_F(0) & = & F \\ \uparrow & & & & \uparrow \\ \det_Q(M) & = & & = & (\#M)^{-1} \end{array}$$

Proof. Write additively the group operation of M. Let $x_1, \ldots, x_n$ be generators of M, and M' the free module on those generators. Let M'' be the kernel of $M' \xrightarrow{\eta} M$, a submodule of M' (also free) whose generators we denote by $y_1, \ldots, y_n$. Denoting by $d : M'' \to M'$ the inclusion, we have

$$d(y_1) = a_{11}x_1 + \cdots + a_{1n}x_n,$$

$$d(y_2) = a_{21}x_1 + \cdots + a_{2n}x_n,$$

$$\vdots$$

$$d(y_n) = a_{n1}x_1 + \cdots + a_{nn}x_n,$$

for some $a_{jk} \in Q, j, k = 1, \ldots, n$. Then M has the finite projective resolution

$$\cdots \longrightarrow 0 \longrightarrow M'' \longrightarrow M' \longrightarrow M \longrightarrow 0 \longrightarrow \cdots,$$

concentrated in degrees -1 and 0. So $\det M = \det M' \otimes \det^{-1} M''$. Over F, d induces the isomorphism

$$M'' \otimes_Q F \xrightarrow[d]{\simeq} M' \otimes_Q F\ .$$

We wish to identify the invertible Q-module

$$\det M' \otimes_Q (\det M'')^{-1}$$

inside the invertible F-module

$$\Big(\det_F(M' \otimes_Q F)\Big) \otimes_F \Big(\det_F(M'' \otimes_Q F)\Big)^{-1}.$$

Now

$$\Big(\det_F(M' \otimes_Q F)\Big) \otimes_F \Big(\det_F(M'' \otimes_Q F)\Big)^{-1}$$

has canonical basis

$$d(y_1) \wedge \cdots \wedge d(y_n) \otimes (y_1 \wedge \cdots \wedge y_n)^{-1}$$

while

$$\det M' \otimes_Q (\det M'')^{-1}$$

has canonical basis

$$\det(a_{jk})^{-1} \cdot d(y_1) \wedge \cdots \wedge d(y_n) \otimes (y_1 \wedge \cdots \wedge y_n)^{-1}.$$

We have the diagram

$$\begin{array}{ccc}
\eta(y_1) \wedge \cdots \wedge \eta(y_n) \otimes (y_1 \wedge \cdots \wedge y_n)^{-1} & \longmapsto & 1 \\
\cap & & \cap \\
(\det_F(M' \otimes_Q F)) \otimes_F (\det_F(M'' \otimes_Q F))^{-1} & \xrightarrow{\simeq} & F \\
\uparrow & & \uparrow \\
\det M' \otimes_Q (\det M'')^{-1} & \xrightarrow{\simeq} & Q \cdot \det(a_{jk})^{-1} \\
\cup & & \cup \\
\det(a_{jk})^{-1} \cdot \eta(y_1) \wedge \cdots \wedge \eta(y_n) \otimes (y_1 \wedge \cdots \wedge y_n)^{-1} & \longmapsto & \det(a_{jk})^{-1},
\end{array}$$

where the isomorphisms are induced by d. As Q is a DVR, $\det(a_{jk}) \cdot Q = \#M$. The result follows. $\square$

4.2 The setting.

Let B be an abelian variety defined over the quadratic imaginary field K, and so that there is an embedding $\mathcal{O}_K \hookrightarrow \mathrm{End}_K(B)$. Denote by $B^\vee$ the dual abelian variety.

The situation we have in mind is that in which B is the Weil restriction of an elliptic curve with complex muliplication by $\mathcal{O}_K$. Here we would have $B \simeq B^\vee$. We make the same assumption about the Tate–Šafarevič group as before:

Assumption 4.2.1. $Ш(B)$ *is finite.*

Fix $K \hookrightarrow \mathbb{C}$.

4.3 Four vector spaces.

We have four finite-dimensional K-vector spaces $H^0(B, \Omega^1)$, $H_1(B(\mathbb{C}), \mathbb{Q})$, $B(K) \otimes_{\mathbb{Z}} \mathbb{Q}$, $B^\vee(K) \otimes_{\mathbb{Z}} \mathbb{Q}$ and perfect $K \otimes \mathbb{R} = \mathbb{C}$-linear pairings

$$(H^0(B, \Omega^1_{B/K}) \otimes_{\mathbb{Q}} \mathbb{R}) \times (H_1(B(\mathbb{C}), \mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{R}) \to \mathbb{C} \tag{4.1}$$

induced by integration and

$$(B(K) \otimes_{\mathbb{Z}} \mathbb{R}) \times (B^\vee(K)^{\mathrm{c}} \otimes_{\mathbb{Z}} \mathbb{R}) \to \mathbb{C} \tag{4.2}$$

given by the modified height pairing $<,>_{\mathbb{C}}$ discussed earlier. (For any K-module W we denote by W^{c} the same group W with the conjugate action of K.) Defining

$$\begin{aligned} {}_K\Xi := &\det_K H^0(B, \Omega^1_{B/K}) \otimes_K \det_K H_1(B(\mathbb{C}), \mathbb{Q}) \\ &\otimes_K (\det_K B(K) \otimes_{\mathbb{Z}} \mathbb{Q}) \otimes_K (\det_K B^\vee(K)^{\mathrm{c}} \otimes_{\mathbb{Z}} \mathbb{Q}), \end{aligned}$$

these pairings induce a $K \otimes \mathbb{R} = \mathbb{C}$-linear isomorphism

$${}_K\vartheta_\infty : {}_K\Xi \otimes_{\mathbb{Q}} \mathbb{R} \simeq K \otimes \mathbb{R}.$$

4.4 Galois cohomology.

We fix a prime number p, and a finite set S of places of K, containing the infinite place, those places above p, and all places where B has bad reduction. We denote by G_S the Galois group of the maximal extension of K unramified outside S and by $\mathcal{O}_{K,S}$ the ring of S-integers of K. For any continuous G_S-module N we put

$$R\Gamma(\mathcal{O}_{K,S}, N) = C^\bullet(G_S, N),$$

the standard complex of continuous cochains. We define

$$\begin{aligned} &R\Gamma_{\mathrm{c}}(\mathcal{O}_{K,S}, N) \\ =&\mathrm{Cone}\left(R\Gamma(\mathcal{O}_{K,S}, N) \to \bigoplus_{v \in S} R\Gamma(K_v, N) \right)[-1]. \end{aligned}$$

Suppose $v \nmid p$ is a place of K. Define

$$R\Gamma_{\mathrm{f}}(K_v, V_p(B))$$

to be the perfect complex, concentrated in degrees 0 and 1, of $K \otimes \mathbb{Q}_p$-modules

$$\cdots \longrightarrow 0 \longrightarrow V_p(B)^{I_v} \xrightarrow{1-\mathrm{Frob}_v} V_p(B)^{I_v} \longrightarrow 0 \longrightarrow \cdots . \tag{4.3}$$

Define

$$R\Gamma_{\mathrm{f}}(K_v, T_p(B))$$

to be the complex

$$\widehat{B(K_v)}[-1],$$

which is

$$\cdots \longrightarrow 0 \longrightarrow \widehat{B(K_v)} \longrightarrow 0 \longrightarrow \cdots , \tag{4.4}$$

concentrated in degree 1, where $\widehat{B(K_v)} := \varprojlim_n B(K_v)/p^n$ is the p-completion of $B(K_v)$.

For $v \mid p$, we define

$$R\Gamma_{\mathrm{f}}(K_v, V_p(B))$$

to be the perfect complex, concentrated in degrees 0 and 1, of $K \otimes \mathbb{Q}_p$-modules

$$\cdots \longrightarrow 0 \longrightarrow D_v \xrightarrow{(1-\phi,\pi)} D_v \oplus H^0(B, \Omega^1_{B/K_v})^\vee \longrightarrow 0 \longrightarrow \cdots , \tag{4.5}$$

where D_v denotes

$$D_{\mathrm{cris}}(V_p(B)) = H^0(K_v, B_{\mathrm{cris}} \otimes_{\mathbb{Q}_p} V_p(B))$$

and $\vee$ denotes the $K \otimes \mathbb{Q}_p$-dual. The K_v-vector space $H^0(K_v, B_{\mathrm{cris}} \otimes_{\mathbb{Q}_p} V_p(B))$, though invariant under the action of $\mathrm{Gal}(\overline{K_v}/K_v)$, has an additional Frobenius automorphism, which is what we mean here by ϕ. Define

$$R\Gamma_{\mathrm{f}}(K_v, T_p(B))$$

to be

$$\widehat{B(K_v)}[-1].$$

First, as in [2], we have a natural map of complexes of $\mathcal{O}_{K,p}$-modules

$$R\Gamma_{\mathrm{f}}(K_v, T_p(B)) \to R\Gamma(K_v, T_p(B))$$

and denote by

$$R\Gamma_{/\mathrm{f}}(K_v, T_p(B))$$

the cone of this map.

Whether $v \nmid p$ or $v \mid p$, we have compatibility between

$$R\Gamma(K_v, T_p(B)),$$

$$R\Gamma(K_v, V_p(B)),$$

and the natural map

$$R\Gamma_{\mathrm{f}}(K_v, T_p(B)) \to R\Gamma(K_v, T_p(B)),$$

as follows. If $v \nmid p$, then

$$R\Gamma(K_v, T_p(B)) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = \widehat{B^0(K_v)}[-1] \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$$

is the zero complex, which is quasi-isomorphic to

$$R\Gamma(K_v, V_p(B)).$$

If $v \mid p$, we have

$$R\Gamma_{\mathrm{f}}(K_v, T_p(B)) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = \widehat{B(K_v)} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p[-1],$$

which is quasi-isomorphic to the complex

$$R\Gamma_{\mathrm{f}}(K_v, V_p(B)),$$

via the exponential map

$$H^0(B, \Omega_{B_v})^\vee \xrightarrow[\exp]{\simeq} \widehat{B(K_v)} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$$

in degree 1.

Remark 4.4.1. *If B has good reduction at $v \nmid p$, then*

$$R\Gamma_{\mathrm{f}}(K_v, T_p(B))$$

could have been defined as was

$$R\Gamma_{\mathrm{f}}(K_v, V_p(B))$$

to obtain the same cohomology. Precisely,

$$R\Gamma_{\mathrm{f}}(K_v, T_p(B)) = \widehat{B(K_v)} = \widehat{B^0(K_v)}$$

is quasi-isomorphic to the complex

$$\cdots \longrightarrow 0 \longrightarrow T_p(B)^{I_v} \xrightarrow{1-\mathrm{Frob}_v} T_p(B)^{I_v} \longrightarrow 0 \longrightarrow \cdots, \tag{4.6}$$

concentrated in degrees 0 and 1, which lies inside

$$R\Gamma_{\mathrm{f}}(K_v, V_p(B)).$$

The quasi-isomorphism is compatible with the natural map

$$R\Gamma_{\mathrm{f}}(K_v, T_p(B)) \to R\Gamma(K_v, T_p(B)),$$

whose mapping cone we denote

$$R\Gamma_{/\mathrm{f}}(K_v, T_p(B)).$$

Second, we define

$$\begin{aligned} &R\Gamma_{\mathrm{f}}(K, T_p(B)) \\ =&\mathrm{Cone}\left(R\Gamma(\mathcal{O}_{K,S}, T_p(B)) \to \bigoplus_{v\in S-\{\infty\}} R\Gamma_{/\mathrm{f}}(K_v, T_p(B)) \right)[-1]. \end{aligned}$$

Third, we recall that the complex

$$R\Gamma_{\mathrm{c}}(\mathcal{O}_{K,S}, T_p(B))$$

by definition fits into the exact triangle

$$R\Gamma_{\mathrm{c}}(\mathcal{O}_{K,S}, T_p(B)) \to R\Gamma(\mathcal{O}_{K,S}, T_p(B)) \to \bigoplus_{v\in S} R\Gamma(K_v, T_p(B)).$$

Using the complexes defining $R\Gamma_{/\mathrm{f}}(K_v, T_p(B))$, $R\Gamma_{\mathrm{f}}(K, T_p(B))$, and $R\Gamma_{\mathrm{c}}(\mathcal{O}_{K,S}, T_p(B))$, we obtain a distinguished triangle

$$R\Gamma_{\mathrm{c}}(\mathcal{O}_{K,S}, T_p(B)) \to R\Gamma_{\mathrm{f}}(K, T_p(B)) \to \left(\bigoplus_{v\in S-\{\infty\}} R\Gamma_{\mathrm{f}}(K_v, T_p(B)) \right) \oplus R\Gamma(\mathbb{C}, T_p(B)). \tag{4.7}$$

We define

$$R\Gamma_{/\mathrm{f}}(K_v, V_p(B)),$$

$$R\Gamma_{\mathrm{f}}(K, V_p(B)),$$

$$R\Gamma_{\mathrm{c}}(\mathcal{O}_{K,S}, V_p(B)),$$

similarly. There is a version of triangle (4.7) with rational ($V_p(B)$) coefficients, and we have

$$R\Gamma_{\mathrm{c}}(\mathcal{O}_{K,S}, T_p(B)) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \simeq R\Gamma_{\mathrm{c}}(\mathcal{O}_{K,S}, V_p(B)).$$

Here, since we are dealing with the regular rings K, $K \otimes \mathbb{Q}_p$, and $\mathcal{O}_K \otimes \mathbb{Z}_p$, the determinants of the complexes considered are alternating tensor products of the determinants of the cohomology modules, as noted in Chapter 4.1.

4.5 Reformulation of Gross' Conjecture.

In order to reformulate Gross' Conjecture, we wish to relate $\#(Ш(B)_{p^\infty})$ to the determinant of

$$R\Gamma_{\mathrm{c}}(\mathcal{O}_{K,S}, T_p(B)),$$

viewed as an integral lattice inside the determinant of

$$R\Gamma_{\mathrm{c}}(\mathcal{O}_{K,S}, V_p(B)).$$

From the distinguished triangle (4.7), it will suffice to compute the determinants of

$$R\Gamma_{\mathrm{f}}(K_v, T_p(B)), \quad v \in S - \{\infty\} \tag{4.8}$$

$$R\Gamma_{\mathrm{f}}(K, T_p(B)), \tag{4.9}$$

$$R\Gamma(\mathbb{C}, T_p(B)), \tag{4.10}$$

describing them as lattices in the respective invertible K_p-modules

$$\det_{K_p} R\Gamma_{\mathrm{f}}(K_v, V_p(B)),$$

$$\det_{K_p} R\Gamma_{\mathrm{f}}(K, V_p(B)),$$

$$\det_{K_p} R\Gamma(\mathbb{C}, V_p(B)).$$

The determinant of the first complex (4.8) is given by the following lemma.

Lemma 4.5.1. *For $R\Gamma_{\mathrm{f}}(K_v, T_p(B)) \subset R\Gamma_{\mathrm{f}}(K_v, V_p(B))$, v finite, we have*

$$\det_{\mathcal{O}_{K,p}} R\Gamma_{\mathrm{f}}(K_v, T_p(B)) = \#\left(\frac{\mathcal{B}_v(k_v)}{\mathcal{B}_v^0(k_v)}\right) \tag{4.11}$$

$$\subset K_p \simeq \det_{K_p} R\Gamma_{\mathrm{f}}(K_v, V_p(B)) \tag{4.12}$$

if $v \nmid p$, *and*

$$\det_{\mathcal{O}_{K,p}} R\Gamma_{\mathrm{f}}(K_v, T_p(B)) = \mathfrak{d} \cdot \# \left(\frac{\mathcal{B}_v(k_v)}{\mathcal{B}_v^0(k_v)} \right) \cdot \left(\bigwedge_{j=1}^{[F:K]} \omega_j \right) \tag{4.13}$$

$$\subset K_p \cdot \left(\bigwedge_{j=1}^{[F:K]} \omega_j \right) \simeq \det_{K_p} R\Gamma_{\mathrm{f}}(K_v, V_p(B)) \tag{4.14}$$

$$\tag{4.15}$$

if $v \mid p$. *Here the isomorphisms are induced by maps between cohomology in degrees 0 and 1.*

For the proof of the lemma we use the following two results, The first is from Lemma 1 of [3], and the second is proved using [11].

Lemma 4.5.2. *Suppose*

$$\cdots \longrightarrow 0 \longrightarrow M \xrightarrow{\eta} M \longrightarrow 0 \longrightarrow \cdots,$$

is a complex of finite projective Q*-modules, concentrated in degrees 0 and 1. Then there is a commutative diagram*

$$\begin{array}{ccccc} \det(Q) & = & \det(M) \otimes \det(M)^{-1} & \xrightarrow{\simeq} & Q \\ & & \downarrow \text{Lemma 4.1.1} & & \\ & & \det_Q H^0(M) \otimes \det_Q H^1(M)^{-1} & & \downarrow \det(\eta) \\ & & \| & & \\ & & \det_Q(0) \otimes \det_Q(0)^{-1} & = & Q \end{array}$$

where the horizontal isomorphism is induced by id_M.

Lemma 4.5.3.

$$\widehat{\mathcal{B}(K_v)}/H^1(k_v, T_p(B)^{I_v}) \simeq \mathcal{B}_v(k_v)/\mathcal{B}^0(k_v).$$

Proof. We denote by $\mathcal{B}$ the Néron model of B/K_v, by $\mathcal{B}^0$ the zero connected component subscheme, by $\mathcal{B}_v$ the special fibre, and by $\mathcal{B}_v^0$ the zero connected component of $\mathcal{B}_v$. By [11], Lemma 2.2.1, there is a short exact sequence of group schemes

$$0 \longrightarrow \mathcal{B}^0_{p^n} \longrightarrow \mathcal{B}^0 \xrightarrow{p^n} \mathcal{B}^0 \longrightarrow 0\ .$$

We also use the short exact sequence of group schemes

$$0 \longrightarrow \mathcal{B}_{p^n} \longrightarrow \mathcal{B} \xrightarrow{p^n} \mathcal{B} \longrightarrow 0\ .$$

From these exact sequences for $\mathcal{B}^0$ and $\mathcal{B}$, we obtain the exact sequences

$$\mathcal{B}(K_v)_{p^n} \xrightarrow{p^n} \mathcal{B}(K_v)_{p^n} \longrightarrow H^1(K_v, \mathcal{B}_{p^n})\ ,$$

$$\mathcal{B}^0(\mathcal{O}_{K,v})_{p^n} \xrightarrow{p^n} \mathcal{B}^0(\mathcal{O}_{K,v})_{p^n} \longrightarrow H^1(\mathcal{O}_{K,v}, \mathcal{B}^0_{p^n})\ ,$$

$$\mathcal{B}^0_v(k_v)_{p^n} \xrightarrow{p^n} \mathcal{B}^0_v(k_v)_{p^n} \longrightarrow H^1(k_v, (\mathcal{B}^0_v)_{p^n})\ ,$$

which induce respective injections

$$\mathcal{B}(\mathcal{O}_{K,v})_{p^n} = \mathcal{B}(K_v)_{p^n} \rightarrowtail H^1(K_v, \mathcal{B}_{p^n}) = H^1(K_v, B_{p^n})\ ,$$

$$\mathcal{B}^0(\mathcal{O}_{K,v})_{p^n} \rightarrowtail H^1(\mathcal{O}_{K,v}, \mathcal{B}^0_{p^n}) \ ,$$

$$\mathcal{B}^0(k_v)_{p^n} \rightarrowtail H^1(k_v, i^*\mathcal{B}^0_{p^n}) = H^1(k_v, i^*(\mathcal{B}^0_v)_{p^n}) \ ,$$

where i here denotes the natural map $\mathrm{Spec} k_v \rightarrowtail \mathrm{Spec}\mathcal{O}_{K,v}$. Taking projective limits, we obtain, respectively,

$$\widehat{\mathcal{B}(\mathcal{O}_{K,v})} = \widehat{\mathcal{B}(K_v)} \rightarrowtail H^1(K_v, T_p\mathcal{B}) = H^1(K_v, T_p(B)) \ ,$$

$$\widehat{\mathcal{B}^0(\mathcal{O}_{K,v})} \rightarrowtail H^1(\mathcal{O}_{K,v}, T_p(\mathcal{B}^0)) \ ,$$

$$\widehat{\mathcal{B}^0(k_v)} \rightarrowtail H^1(k_v, i^*T_p(\mathcal{B}^0)) = H^1(k_v, i^*T_p(\mathcal{B}^0_v)) \ .$$

Together, these form a diagram:

$$\begin{array}{ccccc}
\widehat{\mathcal{B}(\mathcal{O}_{K,v})} & = & \widehat{\mathcal{B}(K_v)} & \rightarrowtail & H^1(K_v, T_p\mathcal{B}) = H^1(K_v, T_p(B)) \\
 & & \uparrow & & \uparrow \\
 & & \widehat{\mathcal{B}^0(\mathcal{O}_{K,v})} & \rightarrowtail & H^1(\mathcal{O}_{K,v}, T_p(\mathcal{B}^0)) \\
 & & \downarrow & & \downarrow \text{ base change} \\
 & & \widehat{\mathcal{B}^0(k_v)} & \rightarrowtail & H^1(k_v, i^*T_p(\mathcal{B}^0)) = H^1(k_v, i^*T_p(\mathcal{B}^0_v))
\end{array}$$

The injection

$$\mathcal{B}^0(k_v)_{p^n} \rightarrowtail H^1(k_v, i^*\mathcal{B}^0_{p^n}) = H^1(k_v, i^*(\mathcal{B}^0_v)_{p^n}) \ ,$$

fits into the exact sequence

$$\mathcal{B}^0(k_v)_{p^n} \rightarrowtail H^1(k_v, i^*(\mathcal{B}^0_v)_{p^n}) \longrightarrow H^1(k_v, \mathcal{B}^0_v) \ .$$

By Lang's Theorem $H^1(k_v, \mathcal{B}_v^0) = 0$, so that the map

$$\mathcal{B}^0(k_v)_{p^n} \twoheadrightarrow H^1(k_v, i^*\mathcal{B}_{p^n}^0) = H^1(k_v, i^*(\mathcal{B}_v^0)_{p^n}) \ .$$

is surjective. By [11], Proposition 2.2.5, we have

$$H^1(k_v, i^*T_p(\mathcal{B}_v^0)) = H^1(k_v, (T_p(B^0))^{I_v}),$$

The map

$$\widehat{\mathcal{B}^0(\mathcal{O}_{K,v})} \to \widehat{\mathcal{B}^0(k_v)}$$

is surjective since $\mathcal{A}^0 \to \mathcal{O}_{K,v}$ is smooth and $\mathcal{O}_{K,v}$ Henselian, injective since $v \nmid p$, making $\ker(\mathcal{B}^0(\mathcal{O}_{K,v}) \to \mathcal{B}^0(k_v))$ p-divisible. Since Speck_v is proper over Spec$\mathcal{O}_{K,v}$, then

$$H^1(\mathcal{O}_{K,v}, T_p(\mathcal{B}^0)) \simeq H^1(k_v, i^*T_p(\mathcal{B}^0)).$$

We obtain this diagram:

$$\begin{array}{ccccc}
\widehat{\mathcal{B}(\mathcal{O}_{K,v})} & = & \widehat{\mathcal{B}(K_v)} & \hookrightarrow & H^1(K_v, T_p\mathcal{B}) = H^1(K_v, T_p(B)) \\
 & & \uparrow & & \uparrow \\
 & & \widehat{\mathcal{B}^0(\mathcal{O}_{K,v})} & \hookrightarrow & H^1(\mathcal{O}_{K,v}, T_p(\mathcal{B}^0)) \\
 & & \downarrow & & \simeq \\
 & & \widehat{\mathcal{B}^0(k_v)} & \twoheadrightarrow & H^1(k_v, i^*T_p(\mathcal{B}^0)) = H^1(k_v, i^*T_p(\mathcal{B}_v^0)) \\
 & & & & \| \\
 & & & & H^1(k_v, (T_p(B))^{I_v})
\end{array}$$

From this, we conclude that

$$\widehat{\mathcal{B}(K_v)}/H^1(k_v, T_p(B)^{I_v}) \simeq \widehat{\mathcal{B}(\mathcal{O}_{K,v})}/\widehat{\mathcal{B}^0(\mathcal{O}_{K,v})} \simeq \mathcal{B}_v(\widehat{k_v)/\mathcal{B}^0}(k_v).$$

Since $\mathcal{B}_v(k_v)/\mathcal{B}^0(k_v)$ is finite, this last equality becomes

$$\widehat{\mathcal{B}(K_v)}/H^1(k_v, T_p(B)^{I_v}) \simeq \mathcal{B}_v(k_v)/\mathcal{B}^0(k_v).$$

□

Proof of Lemma 4.5.1 First suppose $v \not| p$. By Lemma 4.5.2 and the definition of

$$R\Gamma_{\mathrm{f}}(K_v, T_p(B)),$$

we see that

$$\det_{\mathcal{O}_{K,p}} R\Gamma_{\mathrm{f}}(K_v, T_p(B)) = \#\left(\widehat{B(K_v)}\right) \cdot \det(1 - \mathrm{Frob}_v)^{-1}$$

To calculate $\det(1 - \mathrm{Frob}_v)^{-1}$, we use the exact sequence

$$\begin{array}{ccccccc} T_p(B)^{\mathrm{Frob}_v=1} & \rightarrowtail & T_p(B) & \xrightarrow{1-\mathrm{Frob}_v} & T_p(B) & \twoheadrightarrow & H^1(k_v, T_p(B)^{I_v}), \\ \| & & & & & & \\ 0 & & & & & & \end{array}$$

which shows that

$$\det(1 - \mathrm{Frob}_v)^{-1} = \#H^1(k_v, T_p(B)^{I_v}).$$

We must now compute

$$\#\left(\widehat{B(K_v)}/H^1(k_v, T_p(B)^{I_v})\right).$$

But this is given by Lemma 4.5.3 to be

$$\#\left(\frac{\mathcal{B}_v(k_v)}{\mathcal{B}_v^0(k_v)}\right).$$

Now suppose $v \mid p$. The term

$$H^0(B, \Omega^1_{B/K_v})^\vee$$

in degree 1 contributes a factor of

$$\det_{\mathcal{O}_{K,p}} H^0(B, \Omega^1_{B/K_v}) = \mathfrak{d} \cdot \left(\bigwedge_{j=1}^{[F:K]} \omega_j\right)$$

to

$$\det_{\mathcal{O}_{K,p}} R\Gamma_{\mathrm{f}}(K_v, T_p(B)),$$

and the factor

$$\#\left(\frac{\mathcal{B}_v(k_v)}{\mathcal{B}_v^0(k_v)}\right)$$

is obtained as in the case $v \nmid p$. □

To deal with the second complex (4.9), we use the following lemma, obtained from the computations of Burns–Flach in [2].

Lemma 4.5.4. *The cohomology of* $R\Gamma_{\mathrm{f}}(K, T_p(B))$ *is given by*

$$H^0_{\mathrm{f}}(K, T_p(B)) = 0, \tag{4.16}$$

$$H^1_{\mathrm{f}}(K, T_p(B)) = B(K) \otimes_Z \mathbb{Z}_p, \tag{4.17}$$

$$0 \to Ш(B)_{p^\infty} \to H^2_{\mathrm{f}}(K, T_p(B)) \to \mathrm{Hom}_{\mathbb{Z}_p}(B^\vee(K)^{\mathrm{c}}, \mathbb{Z}_p) \to 0 \ \textit{(exact)}, \tag{4.18}$$

$$H^3_{\mathrm{f}}(K, T_p(B)) = (B^\vee(K)_{p^\infty})^\wedge, \tag{4.19}$$

where $\wedge$ *denotes the Pontryagin dual.*

Proof. From the definition of $R\Gamma_{\mathrm{f}}(K, T_p(B))$, it is apparent that $H^0_{\mathrm{f}}(K, T_p(B)) = H^0(\mathcal{O}_{K,S}, T_p(B))$, which is 0. This is the statement (4.16).

It is also apparent that

$$H^1_{\mathrm{f}}(K, T_p(B)) = \ker\left(H^1(\mathcal{O}_{K,S}, T_p(B)) \to \bigoplus_{v \in S - \{\infty\}} \frac{H^1(K_v, T_p(B))}{H^1_{\mathrm{f}}(K_v, T_p(B))} \oplus H^1(\mathbb{C}, T_p(B)) \right).$$

Since $\mathbb{C}$ is algebraically closed, $H^1(\mathbb{C}, T_p(B)) = 0$. Since for all v,

$$H^1_{\mathrm{f}}(K_v, T_p(B)) = \widehat{B(K_v)},$$

then the above kernel must contain

$$B(K) \otimes_{\mathbb{Z}} \mathbb{Z}_p.$$

Since Ш(B), which is finite, surjects onto the kernel of

$$\frac{H^1(\mathcal{O}_{K,S}, V_p(B)/T_p(B))}{H^1_{\mathrm{f}}(K, T_p(B)) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \to \bigoplus_{v \in S - \{\infty\}} \frac{H^1(K_v, V_p(B)/T_p(B))}{H^1_{\mathrm{f}}(K_v, T_p(B)) \otimes \mathbb{Q}_p/\mathbb{Z}_p},$$

$B(K) \otimes_{\mathbb{Z}} \mathbb{Z}_p$ is in fact all of $H^1_{\mathrm{f}}(K, T_p(B))$. This is statement (4.17).

To prove the statement (4.18), we use four pairings. The Weil pairing is

$$T_p(B) \times T_p(B^\vee) \longrightarrow \mathbb{Z}_p(1)\ .$$

Second, we have the Pontryagin pairing

$$\begin{array}{ccc} T_p(B) \times B^\vee_{p^\infty} & \longrightarrow & \mathbb{Q}_p/\mathbb{Z}_p(1)\ . \\ \| & & \\ V_p(B^\vee)/T_p(B^\vee) & & \end{array}$$

Third, we have Poitou-Tate duality

$$\begin{array}{ccc} H^2_{\mathrm{c}}(\mathcal{O}_{K,S}, T_p(B)) \times H^1(\mathcal{O}_{K,S_p}, V_p(B^\vee)/T_p(B^\vee)(1)) & \longrightarrow & H^3_{\mathrm{c}}(\mathcal{O}_{K,S}, \mathbb{Q}_p/\mathbb{Z}_p(1)) \\ & & \Big\downarrow{\scriptstyle \mathrm{trace}} \\ & & \mathbb{Q}_p/\mathbb{Z}_p. \end{array}$$

We obtain

$$0 \longrightarrow H^2_{\mathrm{f}}(K, T_p(B))^\wedge \longrightarrow H^1(\mathcal{O}_{K,S}, B^\vee_{p^\infty}) \longrightarrow \bigoplus_{v \in S - \{\infty\}} \frac{H^1(K_v, B^\vee_{p^\infty})}{H^1_{\mathrm{f}}(K_v, T_p(B))^\perp}\ .$$

Then we see that $H^2_{\mathrm{f}}(K, T_p(B))^\wedge$ is just the Selmer group $\mathrm{Sel}(B^\vee)_{p^\infty}$, and $H^1_{\mathrm{f}}(K_v, T_p(B))^\perp = (B(K_v))^\perp$, which is $B^\vee(K_v) \otimes \mathbb{Q}_p/\mathbb{Z}_p$. Consider the Galois

cohomology exact sequence

$$0 \to B^\vee(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to \mathrm{Sel}(B^\vee_{p^\infty}) \to Ш(B^\vee_{p^\infty}) \to 0. \tag{4.20}$$

We use a fourth pairing, the Cassels–Tate pairing, which says that

$$Ш(B^\vee_{p^\infty})^\wedge \sim Ш(B)_{p^\infty}.$$

Also, we know that the Pontryagin dual of $B^\vee(K)\otimes\mathbb{Q}_p/\mathbb{Z}_p$ is $\mathrm{Hom}_{\mathbb{Z}_p}(B^\vee(K), \mathbb{Z}_p)$. Therefore, dualizing (4.20), we find that

$$0 \to Ш(B)_{p^\infty} \to H^2_{\mathrm{f}}(K, T_p(B)) \to \mathrm{Hom}_{\mathbb{Z}_p}(B^\vee(K), \mathbb{Z}_p) \to 0.$$

The statement (4.19) follows from Tate–Poitou duality:

$$\begin{aligned} & H^3_{\mathrm{f}}(K, T_p(B)) \\ \simeq & H^3_{\mathrm{c}}(\mathcal{O}_{K,S}, T_p(B)) \\ \simeq & H^0(\mathcal{O}_{K,S}, V_p^\vee(B)/T_p^\vee(B)(1))^\wedge \\ \simeq & (B^\vee(K)_{p^\infty})^\wedge \end{aligned}$$

□

From this lemma we deduce a corollary which identifies the *rational* cohomology.

Corollary 4.5.5. *The cohomology of* $R\Gamma_{\mathrm{f}}(K, V_p(B))$ *is given by*

$$H^0_{\mathrm{f}}(K, V_p(B)) = 0, \tag{4.21}$$

$$H^1_{\mathrm{f}}(K, V_p(B)) \simeq B(K) \otimes_Z \mathbb{Q}_p, \tag{4.22}$$

$$H^2_{\mathrm{f}}(K, V_p(B)) \simeq (B^\vee(K)^{\mathrm{c}} \otimes_{\mathbb{Z}} \mathbb{Q}_p)^\vee, \tag{4.23}$$

$$H^3_{\mathrm{f}}(K, V_p(B)) = 0, \tag{4.24}$$

where c *denotes the conjugate* $\mathrm{Gal}(\overline{K}/K)$*-action.*

The following lemma describes (4.10), the last of the three complexes.

Lemma 4.5.6. *For* $R\Gamma(\mathbb{C}, T_p(B)) \subset R\Gamma(\mathbb{C}, V_p(B))$*, we have:*

$$\det_{\mathcal{O}_{K,p}} H^0(\mathbb{C}, T_p(B)) = \mathfrak{b}^{-1} \cdot \left(\bigwedge_{j=1}^{[F:K]} \gamma_j \right) \tag{4.25}$$

$$\subset K_p \cdot \left(\bigwedge_{j=1}^{[F:K]} \gamma_j \right) = \det_{K_p} H^0(\mathbb{C}, V_p(B)), \tag{4.26}$$

$$\det_{\mathcal{O}_{K,p}} H^j(\mathbb{C}, T_p(B)) = \mathcal{O}_{K,p} \tag{4.27}$$

$$\subset K_p = \det_{K_p} H^j(\mathbb{C}, V_p(B)) \text{ for } j \neq 0. \tag{4.28}$$

Proof. This result follows from the definition of $\mathfrak{b}$. □

The last thing we need to translate Gross' Conjecture is a map relating ${}_K\Xi$ to the determinant of the complex $R\Gamma_{\mathrm{c}}(\mathcal{O}_{K,S}, V_p(B))$.

Lemma 4.5.7. *There is a* $K \otimes_{\mathbb{Q}} \mathbb{Q}_p$*-linear isomorphism induced by the trian-*

gle (4.7):

$$ {}_K\vartheta_p : \det_{K\otimes\mathbb{Q}_p} R\Gamma_{\mathrm{c}}(\mathcal{O}_{K,S}, V_p(B))^{-1} \xrightarrow{\simeq} {}_K\Xi \otimes_{\mathbb{Q}} \mathbb{Q}_p. $$

Proof. The result will follow immediately from the triangle (4.7) if we can show that there is a natural $K \otimes_{\mathbb{Q}} \mathbb{Q}_p$-linear isomorphism

$$ \begin{aligned} &\det_{K\otimes\mathbb{Q}_p} R\Gamma_{\mathrm{f}}(K, V_p(B))^{-1} \\ &\otimes \det_{K\otimes\mathbb{Q}_p} \left(\bigoplus_{v\in S-\{\infty\}} R\Gamma_{\mathrm{f}}(K_v, V_p(B)) \right) \\ &\otimes \det_{K\otimes\mathbb{Q}_p} R\Gamma(\mathbb{C}, V_p(B)) \\ \xrightarrow{\simeq} &{}_K\Xi \otimes_{\mathbb{Q}} \mathbb{Q}_p. \end{aligned} $$

Recall that

$$ \begin{aligned} {}_K\Xi = &\det_K H^0(B, \Omega^1_{B/K}) \\ &\otimes_K \det_K H_1(B(\mathbb{C}), \mathbb{Q}) \\ &\otimes_K (\det_K B(K) \otimes_{\mathbb{Z}} \mathbb{Q}) \\ &\otimes_K (\det_K B^{\vee}(K)^{\mathrm{c}} \otimes_{\mathbb{Z}} \mathbb{Q}). \end{aligned} $$

First,

$$H^0(\mathbb{C}, V_p(B)) \simeq H_1(B(\mathbb{C}), \mathbb{Q}) \otimes \mathbb{Q}_p,$$

$$H^j(\mathbb{C}, V_p(B)) = 0 \text{ for } j \neq 0,$$

whence

$$\det_{K\otimes\mathbb{Q}_p} R\Gamma(\mathbb{C}, V_p(B)) = \det_{K\otimes\mathbb{Q}_p} (H_1(B(\mathbb{C}), \mathbb{Q}) \otimes \mathbb{Q}_p).$$

Second, for $v \mid p$,

$$H^1_{\mathrm{f}}(K_v, V_p(B))^\vee \xrightarrow[\exp^*]{\simeq} H^0(B, \Omega^1_{B/K}),$$

$$H^j_{\mathrm{f}}(K_v, V_p(B) = 0 \text{ for } j \neq 1,$$

the isomorphism being given by dual of the exponential map discussed in Section 4.4, whence

$$\det_{K\otimes\mathbb{Q}_p} \left(\bigoplus_{v|p} R\Gamma_{\mathrm{f}}(K_v, V_p(B)) \right) \simeq \det_K H^0(B, \Omega^1_{B/K}),$$

while for $v \nmid p$,

$$R\Gamma_{\mathrm{f}}(K_v, V_p(B)) \text{ is acyclic.}$$

Third, Lemma 4.5.5 says that

$$\begin{aligned} H^1_{\mathrm{f}}(K, V_p(B)) =& B(K) \otimes_{\mathbb{Z}} \mathbb{Q}_p, \\ H^2_{\mathrm{f}}(K, V_p(B)) =& (B^\vee(K)^{\mathrm{c}} \otimes_{\mathbb{Z}} \mathbb{Q}_p)^\vee, \\ H^j_{\mathrm{f}}(K, V_p(B)) =& 0 \text{ for } j \neq 1, 2, \end{aligned}$$

whence

$$\begin{aligned} \det_{K \otimes \mathbb{Q}_p} R\Gamma_{\mathrm{f}}(K, V_p(B))^{-1} =& (\det_{K \otimes \mathbb{Q}_p} B(K) \otimes_{\mathbb{Z}} \mathbb{Q}_p) \\ & \otimes_{K \otimes \mathbb{Q}_p} (\det_{K \otimes \mathbb{Q}_p} B^\vee(K)^{\mathrm{c}} \otimes_{\mathbb{Z}} \mathbb{Q}_p). \end{aligned}$$

We obtain the $K \otimes_{\mathbb{Q}} \mathbb{Q}_p$-linear isomophism

$$\begin{aligned} & \det_{K \otimes \mathbb{Q}_p} R\Gamma_{\mathrm{f}}(K, V_p(B))^{-1} \\ & \otimes \det_{K \otimes \mathbb{Q}_p} \left(\bigoplus_{v \in S - \{\infty\}} R\Gamma_{\mathrm{f}}(K_v, V_p(B)) \right) \\ & \otimes \det_{K \otimes \mathbb{Q}_p} R\Gamma(\mathbb{C}, V_p(B)) \\ \xrightarrow{\simeq}_K & \Xi \otimes_{\mathbb{Q}} \mathbb{Q}_p \end{aligned}$$

and the result follows. □

Now we can reformulate the p-part of Gross' Conjecture.

Theorem 4.5.8. *The p-part of Gross' Conjecture is equivalent to the statement that*

$$L(\overline{\psi}, s) \sim c(s-1)^{\mathrm{rank}_{\mathcal{O}_K} B(K)} \text{ as } s \to 1$$

for some constant $c \in \mathbb{C}^*$ *such that*

$$ {}_K\vartheta_\infty^{-1}(c) \in {}_K\Xi \otimes 1$$

and that

$$\mathcal{O}_{K,p} \cdot {}_K\vartheta_p^{-1}({}_K\vartheta_\infty^{-1}(c)) = \det_{\mathcal{O}_{K,p}} R\Gamma_{\mathrm{c}}(\mathcal{O}_{K,S}, T_p(B))^{-1}.$$

Proof. Let us examine the isomophism ${}_K\vartheta_\infty$. From the pairings (4.1) and (4.2), we find that the image under ${}_K\vartheta_\infty$ of the generator of ${}_K\Xi$ given by the chosen bases ($\{\gamma_j\}_j$, $\{\omega_j\}_j$, and $\{x_j\}_j$), is

$$\Omega \cdot \det_{\mathcal{O}_{K,p}}(< x_j, x_k >)_{j,k} = \Omega R_{\mathbb{C}} \left| \frac{B(K)}{X} \right|.$$

So the statements

$$ {}_K\vartheta_\infty^{-1}(c) \subset {}_K\Xi \otimes 1$$

and

$$\mathcal{O}_{K,p} \cdot {}_K\vartheta_p^{-1}({}_K\vartheta_\infty^{-1}(c)) = \det_{\mathcal{O}_{K,p}} R\Gamma_{\mathrm{c}}(\mathcal{O}_{K,S}, T_p(B))^{-1}$$

are equivalent to

$$\frac{c}{R_{\mathbb{C}}\Omega} \in K \tag{4.29}$$

and

$$\mathcal{O}_{K,p} \cdot {}_K\vartheta_\infty^{-1}\left(\frac{c}{R_{\mathbb{C}}\Omega}\right) = {}_K\vartheta_p\left(\det_{\mathcal{O}_{K,p}} R\Gamma_{\mathrm{c}}(\mathcal{O}_{K,S}, T_p(B))^{-1}\right) \tag{4.30}$$

(using for the second equality the fact that $B^\vee(K) \simeq B(K)$).

The first statement of Gross' Conjecture is just inclusion (4.29), and the p-part of the second is exactly

$$\left(\frac{c}{R_{\mathbb{C}}\Omega}\right)_p = \left(\mathfrak{b}\cdot\mathfrak{d}\cdot\#(Ш(B))\cdot\prod_{v\not|\infty}\#\left(\frac{\mathcal{B}_v(k_v)}{\mathcal{B}_v^0(k_v)}\right)\right)_p, \tag{4.31}$$

or, equivalently,

$$\mathcal{O}_{K,p}\cdot{}_K\vartheta_\infty^{-1}\left(\frac{c}{R_{\mathbb{C}}\Omega}\right) = \mathcal{O}_{K,p}\cdot{}_K\vartheta_\infty^{-1}\left(\mathfrak{b}\cdot\mathfrak{d}\cdot\#(Ш(B))\cdot\prod_{v\not|\infty}\#\left(\frac{\mathcal{B}_v(k_v)}{\mathcal{B}_v^0(k_v)}\right)\right). \tag{4.32}$$

Comparing (4.30) and(4.32), we see from the triangle (4.7) what must be proven: that

$${}_K\vartheta_p\left(\det_{\mathcal{O}_{K,p}} R\Gamma_{\mathrm{c}}(\mathcal{O}_{K,S},T_p(B))^{-1}\right)$$

is generated, in

$$\begin{aligned}&\det_{K_p} R\Gamma_{\mathrm{f}}(K,V_p(B))^{-1}\\ \otimes&\det_{K_p}\left(\bigoplus_{v\in S-\{\infty\}} R\Gamma_{\mathrm{f}}(K_v,V_p(B)\right)\\ \otimes&\det_{K_p} R\Gamma(\mathbb{C},V_p(B)),\end{aligned}$$

by

$$\mathfrak{b}\cdot\mathfrak{d}\cdot\#(Ш(B))\cdot\prod_{v\not|\infty}\#\left(\frac{\mathcal{B}_v(k_v)}{\mathcal{B}_v^0(k_v)}\right),$$

with respect to the chosen bases.

But this follows from Lemma 4.5.1, Lemma 4.5.4 and its Corollary 4.5.5, and Lemma 4.5.6. □

Chapter 5

Elliptic curves with nonmaximal endomorphism ring.

In order to study an elliptic curve E with nonmaximal endomorphism ring, and its Weil restriction B, we employ another elliptic curve isogenous to E and defined over the same base field F as E.

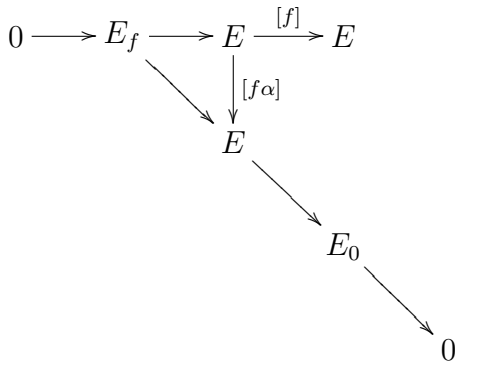
Lemma 5.0.1 ([21], Exercise II.1.2). *Suppose E is an elliptic curve over a (number) field F with $\mathrm{End}_F(E) \simeq \mathcal{O} \subseteq \mathcal{O}_K$. Then there exists an elliptic curve E_0 over F with $\mathrm{End}_F(E_0) \simeq \mathcal{O}_K$, and an isogeny $E \to E_0$ over F.*

Proof. Say that $\mathcal{O}_K$ is generated over $\mathbb{Z}$ by 1 and α, and that

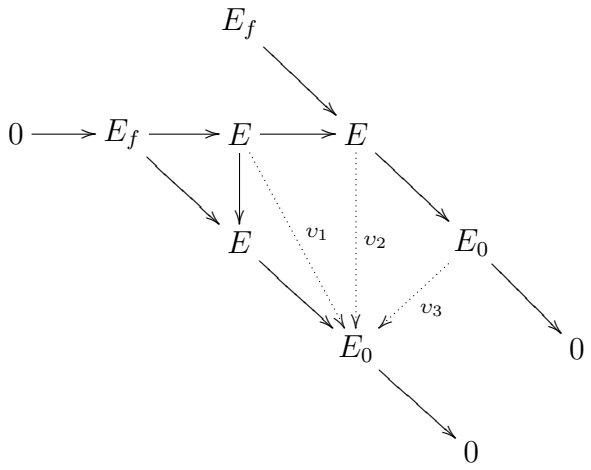
$$\mathcal{O} = \mathbb{Z} + f \cdot \mathcal{O}_K = \mathbb{Z} + f\alpha \cdot \mathbb{Z}.$$

Define E_0 by the following commutative diagram, with exact row and di-

agonal:



We shall construct an $\mathcal{O}_K$-action on E_0 which agrees with the $\mathcal{O}$-action on E . We construct morphisms υ_1, υ_2, υ_3, as shown in the following diagram:



The upper diagonal is the same as the lower diagonal. The morphism υ_1 is defined by commutativity. The morphism υ_2 is obtained by observing that the kernel of the morphism

$$E \xrightarrow{[f]} E$$

is contained in the kernel of υ_1. The morphism υ_3 is obtained as follows. The

kernel of the upper diagonal morphism

$$\begin{array}{ccc} E & & \\ & \searrow & \\ & & E_0 \end{array}$$

is the image of the composite morphism:

$$\begin{array}{ccc} E_f & \longrightarrow & E \\ & & \downarrow{\scriptstyle [f\alpha]} \\ & & E \end{array}$$

This image is

$$[f\alpha]E_f,$$

which has pre-image

$$[f\alpha]E_{f^2}$$

under

$$E \xrightarrow{[f]} E\,,$$

whose image under

$$\begin{array}{c} E \\ \downarrow{\scriptstyle [f\alpha]} \\ E \end{array}$$

is

$$\begin{aligned}
&[f\alpha]^2 E_{f^2} \\
=&[f^2\alpha^2] E_{f^2} \\
=&[f\alpha^2] E_f \\
=&[f(a\alpha + b)] E_{f^2} \text{ for some } a, b \in \mathbb{Z} \\
=&([a][f\alpha] + [b][f]) E_f \\
=&[a][f\alpha] E_f,
\end{aligned}$$

which is contained in the kernel of the lower diagonal morphism:

$$\begin{array}{ccc} E & & \\ & \searrow & \\ & & E_0 \end{array}$$

Therefore, the kernel of the upper diagonal morphism

$$\begin{array}{ccc} E & & \\ & \searrow & \\ & & E_0 \end{array}$$

(in which we were originally interested) is contained in the kernel of υ_2, and υ_3 can be constructed making the diagram commute. We then define

$$[\alpha] : E_0 \to E_0$$

to be υ_3. The morphisms

$$1 = \mathrm{id} : E_0 \to E_0$$

and

$$[\alpha] : E_0 \to E_0$$

are extended by linearity to an action of $\mathcal{O}_K$ upon E_0.

One checks that this action is a well-defined ring action and agrees with the action of $\mathcal{O}$ upon E. That is, for any $x \in \mathcal{O} \subset \mathcal{O}_K$, the diagram

$$\begin{array}{ccc} E & \xrightarrow{[x]} & E \\ \downarrow & & \downarrow \\ E_0 & \xrightarrow{[x]} & E_0 \end{array}$$

commutes. □

It is known (see for example [20], Appendix C, Theorem 11.5) that the j-invariant of E (resp. E_0) belongs to the ring class field $H(\mathcal{O})$ associated to $\mathcal{O}$ (resp .the Hilbert class field $H = H(\mathcal{O}_K)$ of K). We have a tower of fields $K \subset H \subset H(\mathcal{O}) \subset F$. The curves E and E_0 are twists over F of elliptic curves defined over $H(\mathcal{O})$ and H, respectively.

As before, we have B the Weil restriction of E, and we define B_0 to be the Weil restriction of E_0. The varieties B and B_0 are isogenous abelian varieties over K with complex multiplication by $\mathcal{O}$ and $\mathcal{O}_K$, respectively.

5.1 The Burns–Flach Conjecture.

The elliptic curve E is defined over F, with complex multiplication by the order $\mathcal{O} \subseteq \mathcal{O}_K$, with Weil restriction $B := \mathrm{Res}_K^F E$, and with E having Grössencharacter ψ. The Burns–Flach Conjecture concerns the Weil restriction B of the original elliptic curve E.

Let $\mathfrak{f}$ be the conductor of F. Fix a prime p. Let S, a set of places of K, be defined as the union of the set of prime divisors of $\mathfrak{f}p$, and the set of primes below those of bad reduction of E/F, along with the infinite place. Then by the Criterion of Néron–Ogg–Šafarevič, $S - \{\infty\}$ is the set of places where the extensions $F(E_{p^n})/K$ are ramified.

Conjecture 5.1.1 (Burns–Flach). *We have*

$$L(\overline{\psi}, s) \sim c(s-1)^{\mathrm{rank}_{\mathcal{O}_K} B(K)} \text{ as } s \to 1$$

for some constant $c \in \mathbb{C}^*$ such that

$${}_K\vartheta_\infty^{-1}(c) \in {}_K\Xi \otimes 1$$

and

$$\mathcal{O}_p \cdot {}_K\vartheta_p^{-1}({}_K\vartheta_\infty^{-1}(c)) = \det_{\mathcal{O}_p} R\Gamma_c(\mathcal{O}_{K,S}, T_p(B))^{-1}. \tag{5.1}$$

Note 5.1.2. *The Burns–Flach Conjecture is a strengthening of the p-part of Gross' Conjecture (for primes p dividing the conductor of $\mathcal{O}$). Taking tensor*

products with $\mathcal{O}_{K,p}$ in the statement of the Burns–Flach Conjecture, we have $T_p(B) \otimes_{\mathcal{O}_p} \mathcal{O}_{K,p} = T_p(B_0)$, and the determinant over $\mathcal{O}_p$ becomes a determinant over $\mathcal{O}_{K,p}$, yielding the p-part of the statement of Gross' Conjecture.

5.2 A refinement in the case $F(E_{\text{tors}})/K$ is abelian.

We wish to refine the conjecture further by considering the full endomorphism algebra of B, which can be much larger than K. Write $\mathcal{R} := \text{End}_K(B)$, $R := \mathcal{R} \otimes_{\mathbb{Z}} \mathbb{Q}$, $\mathcal{R}_p := \mathcal{R} \otimes_{\mathbb{Z}} \mathbb{Z}_p$, and $R_p := \mathcal{R} \otimes_{\mathbb{Z}} \mathbb{Q}_p = R \otimes_{\mathbb{Q}} \mathbb{Q}_p$.

Lemma 5.2.1. *Suppose $F(E_{\text{tors}})/K$ is abelian. Then R is a commutative semisimple K-algebra of rank $[F : K]$. Also, $\mathcal{R}$ is projective over $\mathcal{O}$ and $T_p(B)$ is projective over $\mathcal{R}_p$.*

Proof. $\mathcal{R}$ is computed in [8] Section 4. $\mathcal{R} = \text{End}_K(B)$ is the Galois invariants of $\text{End}_F(B)$, where B is isomorphic over F to

$$\prod_{\sigma \in G} E^{\sigma}.$$

Therefore $\mathcal{R}$ is the Galois invariants of

$$\text{Hom}_F\left(\prod_{\sigma \in G} E^{\sigma}, \prod_{\sigma \in G} E^{\sigma}\right) = \prod_{\sigma_1, \sigma_2 \in G} \text{Hom}(E^{\sigma_1}, E^{\sigma_2}),$$

which is seen to be

$$\prod_{\sigma \in G} \text{Hom}(E^{\sigma}, E) \cdot \sigma.$$

Thus $\mathcal{R}$ is projective over $\mathcal{O}$. As well, as in [8], §4, R is a commutative semisim-

ple K-algebra. (In the special case where E is isogenous to a base change from K to F (as in the examples we construct later), $R \simeq K[G]$.) We have

$$T_p(B) = \prod_{\tau \in G} T_p(E^\tau),$$

induced by the decomposition

$$B(\overline{K}) = E(\overline{K} \otimes_K F) = E(\prod_{\tau \in G} \overline{K}) = \prod_{\tau \in G} E^\tau(\overline{K}).$$

We know that $T_p(E)$ is a free $\mathcal{O}_p$-module of rank 1. Pick an $\mathcal{O}_p$-basis ξ of $T_p(E)$. And for each $\sigma \in G$, $\mathrm{Hom}_{\mathcal{O}_p}(E^\sigma, E) \otimes_{\mathbb{Z}} \mathbb{Z}_p$ is also a free $\mathcal{O}_p$-module of rank 1. Pick an $\mathcal{O}_p$-basis $b(\sigma)$ for $\mathrm{Hom}_{\mathcal{O}_p}(E^\sigma, E) \otimes_{\mathbb{Z}} \mathbb{Z}_p$, that is, an isogeny $E^\sigma \xrightarrow{b(\sigma)} E$ of degree prime to p. Composing σ with $b(\sigma)$, we obtain (since $b(\sigma)$ has a kernel prime to p) a map

$$E(\overline{K} \otimes_K F) \xrightarrow{\sigma} E^\sigma(\overline{K} \otimes_K F) \xrightarrow{b(\sigma)} E(\overline{K} \otimes_K F)\ .$$

Or, in more detail, where $B^\sigma = \mathrm{Res}^F_K E^\sigma$, we obtain

$$\begin{array}{ccccc}
B(\overline{K}) & \xrightarrow{\quad\sigma\quad} & B^\sigma(\overline{K}) & \xrightarrow{\quad b(\sigma)\quad} & B(\overline{K}) \\
\| & & \| & & \| \\
E(\overline{K} \otimes_K F) & \xrightarrow{\sigma} & E^\sigma(\overline{K} \otimes_K F) & \xrightarrow{b(\sigma)} & E(\overline{K} \otimes_K F) \\
\wr\downarrow & & \wr\downarrow & & \wr\downarrow \\
\prod_{\tau \in G} E^\tau(\overline{K}) & \xrightarrow{\sigma} & \prod_{\tau \in G} E^{\tau\sigma}(\overline{K}) & \xrightarrow{b(\sigma)^\tau} & \prod_{\tau \in G} E^\tau(\overline{K}).
\end{array}$$

The isogeny $b(\sigma)$ induces an isomorphism $T_p(B^\sigma) \simeq T_p(B)$. So, taking Tate

modules, we obtain the diagram

$$\begin{array}{ccccc}
T_p(B) & \xrightarrow{\quad\sigma\quad} & T_p(B^\sigma) & \xrightarrow{\qquad b(\sigma)\qquad} & T_p(B) \\
\| & & \| & & \| \\
\prod_{\tau\in G} T_p(E^\tau) & \xrightarrow{\sigma} & \prod_{\tau\in G} T_p(E^{\tau\sigma}) & \xrightarrow{b(\sigma)} & \prod_{\tau\in G} T_p(E^\tau) \\
\cup & & \cup & & \cup \\
(\underset{\tau=1}{\xi},0,\ldots,0) & \longmapsto & (0,\ldots,0,\underset{\tau=\sigma^{-1}}{\xi},0,\ldots,0) & \longmapsto & (0,\ldots,0,\underset{\tau=\sigma^{-1}}{b(\sigma)^{\sigma^{-1}}\xi},0,\ldots,0)
\end{array}$$

Since ξ is an $\mathcal{O}_p$-basis of $T_p(E)$, then $b(\sigma)^{\sigma^{-1}}\xi$ is also an $\mathcal{O}_p$-basis of $T_p(E)$. Suppose

$$(\alpha_\tau \cdot b(\tau)^{\tau^{-1}}\xi)_{\tau\in G}$$

is any element of

$$\prod_{\tau\in G} T_p(E^\tau) = T_p(B).$$

We can write

$$(\alpha_\tau \cdot b(\tau)^{\tau^{-1}}\xi)_{\tau\in G} = \left(\sum_{\tau\in G} \alpha_\tau \cdot b(\tau)\cdot\tau\right)(\underset{\tau=1}{\xi},0,\ldots,0)$$

with unique $\alpha_\tau \in \mathcal{O}_p$, that is, with unique

$$\left(\sum_{\tau\in G} \alpha_\tau \cdot b(\tau)\cdot\tau\right) \in \mathcal{R}_p.$$

Therefore $(\underset{\tau=1}{\xi},0,\ldots,0)$ is an $\mathcal{R}_p$-basis of $T_p(B)$. In particular, $T_p(B)$ is a projective $\mathcal{R}_p$-module. $\square$

We define an L-function for B as we did for E,

$$ {}_RL(B/K,s) := \prod_{w \not| \infty} {}_RP_w(B/K, \mathbf{N}w^{-s})^{-1} : \mathbb{C} \to R \otimes_{\mathbb{Q}} \mathbb{C}, $$

where

$$ {}_RP_w(B/K,x) = \det_{R \otimes \mathbb{Q}_\ell} (1 - x\phi_w \mid (T_\ell(B) \otimes \mathbb{Q}_\ell)_{I_w}). $$

Write φ for a Grössencharacter of K, which when pre-composed with the norm, gives ψ. Then, as in [8], the possible choices for φ are $\{\varphi\chi : \chi \in \widehat{G}\}$. Writing X for the set of orbits of $\{\varphi\chi : \chi \in \hat{G}\}$ under $\mathrm{Aut}_K\mathbb{C}$, we have

$$ R = K \otimes_{\mathcal{O}} \mathcal{R} = K \otimes_{\mathcal{O}} \mathrm{End}_K B \simeq \prod_X K(\varphi\chi), $$

where $K(\varphi\chi)$ is K with the values of $\varphi\chi$ adjoined. The L-function ${}_RL(B,s)$ corresponds to the tuple of functions

$$ (L(\sigma(\overline{\varphi\chi}), s))_{X, \sigma \in \mathrm{Hom}_K(K(\varphi\chi), \mathbb{C})}, $$

which is considered an element of $R \otimes_{\mathbb{Q}} \mathbb{C}$, where

$$ R \simeq \prod_X K(\varphi\chi). $$

Define

$$
\begin{aligned}
{}_R\Xi := &\det_R H^0(B, \Omega^1_{B/K}) \otimes_R \det_R H_1(B(\mathbb{C}), \mathbb{Q}) \\
&\otimes_R (\det_R B(K) \otimes_{\mathbb{Z}} \mathbb{Q}) \otimes_R (\det_R B^\vee(K)^{\mathrm{c}} \otimes_{\mathbb{Z}} \mathbb{Q}),
\end{aligned}
$$

As with ${}_K\vartheta_\infty$ in Section 4.3, the integration and modified height pairings induce a $R \otimes \mathbb{R}$-linear isomorphism

$$
{}_R\vartheta_\infty : {}_R\Xi \otimes_{\mathbb{Q}} \mathbb{R} \simeq R \otimes \mathbb{R}.
$$

We have a ${}_R\vartheta_p$, which is the analog of ${}_K\vartheta_p$:

Lemma 5.2.2. *There is a $R \otimes_{\mathbb{Q}} \mathbb{Q}_p$-linear isomophism:*

$$
{}_R\vartheta_p : \det_{R \otimes \mathbb{Q}_p} R\Gamma_{\mathrm{c}}(\mathcal{O}_{K,S}, V_p(B))^{-1} \xrightarrow{\simeq} {}_R\Xi \otimes_{\mathbb{Q}} \mathbb{Q}_p.
$$

Proof. This is proved in exactly the same way as Lemma 4.5.7. □

Now we can state the refined Burns–Flach Conjecture:

Conjecture 5.2.3. *We have*

$$
{}_RL(B, s) \sim {}_Rc(s-1)^{\mathrm{rank}_{\mathfrak{R}} B(K)} \text{ as } s \to 1
$$

for some ${}_Rc \in (R \otimes \mathbb{R})^*$ such that

$$
{}_R\vartheta_\infty^{-1}({}_Rc) \subset {}_R\Xi \otimes 1
$$

and

$$\mathcal{R}_p \cdot {}_R\vartheta_p^{-1}({}_R\vartheta_\infty^{-1}({}_Rc)) = \det_{\mathcal{R}_p} R\Gamma_{\mathrm{c}}(\mathcal{O}_{K,S}, T_p(B))^{-1}. \tag{5.2}$$

Note 5.2.4. *Taking norms from $\mathcal{R}_p$ to $\mathcal{O}_p$ (which is possible by Lemma 5.2.1) yields the original conjecture of Burns–Flach.*

Chapter 6

Translation into the terminology of Kato.

In this chapter we pose a conjecture in the terminology of Kato, which is equivalent to the refined Burns–Flach Conjecture for B.

Assumption 6.0.1. *We have* $\operatorname{rank}(E(F)) = 0$*, or equivalently* $\operatorname{rank}(B(K)) = 0$*. In particular, this makes*

$$ {}_R\Xi = \det_R H^0(B, \Omega^1_{B/K}) \otimes_R \det_R H_1(B(\mathbb{C}), \mathbb{Q}). $$

For ease of notation, we will now write the following:

$$T :=T_p(B)$$

$$V :=V_p(B)$$

$$\Xi :=_R \Xi$$

$$\vartheta_\infty :=_R \vartheta_\infty$$

$$\vartheta_p :=_R \vartheta_p$$

$$c :=_R c$$

The $\mathcal{R}_p$-sheaf T on Spec$\mathcal{O}_{K,S}$ is smooth and invertible. Define the invertible $\mathcal{R}_p$-module

$$\Delta_{\mathcal{R}_p}(\mathcal{O}_{K,S}, T)$$

to be

$$\left(\det_{\mathcal{R}_p}(R\Gamma(\mathcal{O}_{K,S}, T))\right)^{-1} \otimes_{\mathcal{R}_p} \left(\det_{\mathcal{R}_p}(R\Gamma(\mathcal{O}_{K,S} \otimes_{\mathbb{Z}} \mathbb{R}, T(-1)))\right)^{-1},$$

and

$$\Delta_{\mathcal{R}_p}(\mathcal{O}_{K,S}, V)$$

to be

$$\Delta_{\mathcal{R}_p}(\mathcal{O}_{K,S}, T) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$$

We compute the cohomology of $R\Gamma(\mathcal{O}_{K,S}, V)$ as follows:

Lemma 6.0.2. • *$H^1(\mathcal{O}_{K,S}, V)$ is a 1-dimensional R_p-vector space.*

- $H^j(\mathcal{O}_{K,S}, V) = 0$ *for* $j \neq 1$.

Proof. Use the exact triangle

$$R_{\mathrm{f}}\Gamma(\mathcal{O}_{K,S}, V) \to R\Gamma(\mathcal{O}_{K,S}, V) \to \bigoplus_{v \in S} R_{/\mathrm{f}}\Gamma(K_v, V)$$

(see [4], §3.2), which is the complex

$$\begin{aligned}
0 \to & H^0_{\mathrm{f}}(K, V) \to H^0(\mathcal{O}_{K,S}, V) \to \bigoplus_{v \in S} H^0_{/\mathrm{f}}(K_v, V) \\
\to & H^1_{\mathrm{f}}(K, V) \to H^1(\mathcal{O}_{K,S}, V) \to \bigoplus_{v \in S} H^1_{/\mathrm{f}}(K_v, V) \\
\to & H^2_{\mathrm{f}}(K, V) \to H^2(\mathcal{O}_{K,S}, V) \to \bigoplus_{v \in S} H^2_{/\mathrm{f}}(K_v, V) \\
\to & H^3_{\mathrm{f}}(K, V) \to \cdots .
\end{aligned}$$

Now $H^0(\mathcal{O}_{K,S}, V) = 0$, and since $R\Gamma_{\mathrm{f}}(K, V)$ is acyclic by Assumption 6.0.1, we have

$$\begin{aligned}
H^1(\mathcal{O}_{K,S}, V) &\simeq \bigoplus_{v \in S} H^1_{/\mathrm{f}}(K_v, V), \\
H^2(\mathcal{O}_{K,S}, V) &\simeq \bigoplus_{v \in S} H^2_{/\mathrm{f}}(K_v, V),
\end{aligned}$$

the second giving us by duality

$$\begin{aligned} H^2(\mathcal{O}_{K,S}, V) &\simeq \bigoplus_{v\in S} H^2_{/\mathrm{f}}(K_v, V) \\ &\simeq \bigoplus_{v\in S} H^2(K_v, V) \\ &\simeq \bigoplus_{v\in S} H^0(K_v, V^*(1))^* \\ &\simeq \bigoplus_{v\in S} H^0(K_v, V)^* \\ &\quad \text{since } V \text{ is the Weil restriction of an elliptic curve} \\ &=0. \end{aligned}$$

Consider the exact sequence

$$0 \longrightarrow \underset{\|}{H^1_{\mathrm{f}}(K_v, V)} \longrightarrow H^1(K_v, V) \longrightarrow H^1_{/\mathrm{f}}(K_v, V) \longrightarrow 0\,.$$
$$\qquad\quad 0$$

If $v \nmid p$, then $H^1(K_v, V) = 0$, and for $v \mid p$, we compute

$$\begin{aligned} \dim_{\mathcal{R}_p} H^1(\mathcal{O}_{K,S}, V) &= \sum_{v|p} \dim_{\mathcal{R}_p} H^1_{/\mathrm{f}}(K_v, V) \\ &= \sum_{v|p} \dim_{\mathcal{R}_p} H^1(K_v, V). \end{aligned}$$

Using $K_p = \prod_{v|p} K_v$ we rewrite this:

$$\begin{aligned}\dim_{\mathcal{O}_p} \mathcal{R}_p \cdot \dim_{\mathcal{R}_p} H^1(\mathcal{O}_{K,S}, V) &= \dim_{\mathcal{O}_p} \mathcal{R}_p \cdot \sum_{v|p} \dim_{\mathcal{R}_p} H^1(K_p, V) \\ &= \sum_{v|p} \dim_{\mathcal{O}_p} H^1(K_p, V)\end{aligned}$$

Applying Tate's Euler characteristic formula

$$\begin{aligned}&\dim_{\mathcal{O}_p} H^0(K_v, V) - \dim_{\mathcal{O}_p} H^1(K_v, V) + \dim_{\mathcal{O}_p} H^2(K_v, V) \\ =& - [K_v : \mathbb{Q}_p] \dim_{\mathcal{O}_p},\end{aligned}$$

with

$$H^0(K_v, V) = H^2(K_v, V) = 0,$$

we obtain

$$\begin{aligned}\dim_{\mathcal{O}_p} \mathcal{R}_p \cdot \dim_{\mathcal{R}_p} H^1(\mathcal{O}_{K,S}, V) =& [K_p : \mathbb{Q}_p] \dim_{\mathcal{O}_p} V \\ =& [K_p : \mathbb{Q}_p] \dim_{\mathcal{O}_p} \mathcal{R}_p,\end{aligned}$$

where the last equality follows from

$$\dim_{\mathcal{R}_p} V = 1.$$

Further, we find

$$\begin{aligned}\dim_{\mathcal{O}_p} \mathcal{R}_p \cdot \dim_{\mathcal{R}_p} H^1(\mathcal{O}_{K,S}, V) =& [K_p : \mathbb{Q}_p] \dim_{\mathcal{O}_p} \mathcal{R}_p, \\ =& [K_p : \mathbb{Q}_p] \dim_{\mathcal{O}_p} B \\ =& \dim_{\mathcal{O}_p} \widehat{B(K_p)} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p, \\ \Rightarrow \dim_{\mathcal{R}_p} H^1(\mathcal{O}_{K,S}, V) =& \dim_{\mathcal{R}_p} \widehat{B(K_p)} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p,\end{aligned}$$

so that

$$H^1(\mathcal{O}_{K,S}, V)$$

has dimension 1 over R_p. □

The dual exponential map (see [13] Chapter II §1.2-§1.4) is

$$\exp^* : H^1(K, V) \to H^0(B, \Omega^1_{B/K}),$$

and gives us a map

$$\det_{\mathcal{R}_p}(\exp^* \otimes \mathrm{id}) : \Delta_{\mathcal{R}_p}(\mathcal{O}_{K,S}, V) \to \Xi \otimes \mathbb{Q}_p,$$

the determinant of Kato's $\exp^* \otimes \mathrm{id}$.

Note that for $v \in S - \{\infty\}$, all terms in $R\Gamma_{\mathrm{f}}(K_v, V)$ are zero except for possibly $H^1_{\mathrm{f}}(K_v, V)$, and that all terms in $R\Gamma(\mathbb{C}, V)$ are zero except for possibly $H^0(\mathbb{C}, V)$.

The modules involved in the refined Burns–Flach Conjecture are in fact isomorphic to those just defined above. We summarize the situation in the

following two lemmata.

Lemma 6.0.3.

$$\det_{\mathcal{R}_p} R\Gamma_{\mathrm{c}}(\mathcal{O}_{K,S},T)^{-1} \simeq \Delta_{\mathcal{R}_p}(\mathcal{O}_{K,S},T)$$

Proof. We use the complex $\widetilde{R\Gamma}_{\mathrm{c}}(\mathcal{O}_{K,S},T)$ which is defined in this case by the exact triangle

$$\widetilde{R\Gamma}_{\mathrm{c}}(\mathcal{O}_{K,S},T) \to R\Gamma(\mathcal{O}_{K,S},T) \to \bigoplus_{v\in S-\{\infty\}} R\Gamma(K_v,T).$$

We consider the following exact triangle which it satisfies:

$$R\Gamma_{\mathrm{c}}(\mathcal{O}_{K,S},T) \longrightarrow \widetilde{R\Gamma}_{\mathrm{c}}(\mathcal{O}_{K,S},T) \longrightarrow R\Gamma(\mathbb{C},T) \tag{6.1}$$

Tate–Poitou duality gives

$$\det_{\mathcal{R}_p} \widetilde{R\Gamma}_{\mathrm{c}}(\mathcal{O}_{K,S},T) \simeq \det_{\mathcal{R}_p} R\Gamma(\mathcal{O}_{K,S},T^*(1))^*[-3]$$

So from (6.1),

$$\begin{aligned}
\det_{\mathcal{R}_p} R\Gamma_{\mathrm{c}}(\mathcal{O}_{K,S}, T(1)) &\simeq \det_{\mathcal{R}_p} \widetilde{R\Gamma}_{\mathrm{c}}(\mathcal{O}_{K,S}, T) \otimes_{\mathcal{R}_p} \det_{\mathcal{R}_p} R\Gamma(\mathcal{O}_{K,S} \otimes \mathbb{R}, T)^{-1} \\
&\simeq \det_{\mathcal{R}_p} R\Gamma_{\mathrm{c}}(\mathcal{O}_{K,S}, T^*(1))^*[-3] \otimes_{\mathcal{R}_p} \det_{\mathcal{R}_p} R\Gamma(\mathcal{O}_{K,S} \otimes \mathbb{R}, T)^{-1} \\
&\simeq \det_{\mathcal{R}_p}^{-1} R\Gamma_{\mathrm{c}}(\mathcal{O}_{K,S}, T^*(1))^* \otimes_{\mathcal{R}_p} \det_{\mathcal{R}_p} R\Gamma(\mathcal{O}_{K,S} \otimes \mathbb{R}, T)^{-1} \\
&\simeq \det_{\mathcal{R}_p} R\Gamma_{\mathrm{c}}(\mathcal{O}_{K,S}, T^*(1))^{\#} \otimes_{\mathcal{R}_p} \det_{\mathcal{R}_p} R\Gamma(\mathcal{O}_{K,S} \otimes \mathbb{R}, T(-1)) \\
&\quad \text{since } T^*(1) \simeq T^{\#}, \text{ whence } T^{*\#} \simeq T(-1), \\
&\simeq \det_{\mathcal{R}_p} R\Gamma_{\mathrm{c}}(\mathcal{O}_{K,S}, T) \otimes_{\mathcal{R}_p} \det_{\mathcal{R}_p} R\Gamma(\mathcal{O}_{K,S} \otimes \mathbb{R}, T(-1))
\end{aligned}$$

where "$*$" denotes $R\mathrm{Hom}(\bullet, \mathbb{Z}_p)$ and "$\#$" means changing the $\mathcal{R}_p$-action via the (Rosati) involution on $\mathcal{R}_p$. We conclude that

$$\begin{aligned}
&\det_{\mathcal{R}_p} R\Gamma_{\mathrm{c}}(\mathcal{O}_{K,S}, T)^{-1} \\
&= \left(\det_{\mathcal{R}_p}(R\Gamma(\mathcal{O}_{K,S}, T))\right)^{-1} \otimes_{\mathcal{R}_p} \left(\det_{\mathcal{R}_p}(R\Gamma(\mathcal{O}_{K,S} \otimes \mathbb{R}, T(-1)))\right)^{-1}
\end{aligned}$$

is isomorphic to

$$\Delta_{\mathcal{R}_p}(\mathcal{O}_{K,S}, T).$$

This proves Lemma 6.0.3. □

Lemma 6.0.4. *The diagram*

$$\begin{array}{ccc}
\det_{R_p} R\Gamma_c(\mathcal{O}_{K,S}, V)^{-1} & \xrightarrow{\vartheta_p} & \Xi \otimes \mathbb{Q}_p \\
\Big\downarrow{\scriptstyle \text{Lemma 6.0.3}} & & \Big\| \\
\Delta_{\mathcal{R}_p}(\mathcal{O}_{K,S}, V) & \xrightarrow{\det_{\mathcal{R}_p}(\exp^* \otimes \mathrm{id})} & \Xi \otimes \mathbb{Q}_p
\end{array}$$

commutes, where

$$\det_{\mathcal{R}_p}(\exp^* \otimes \mathrm{id})$$

the determinant of Kato's $\exp^* \otimes \mathrm{id}$.

Proof. The map ϑ_p is constructed from the dual exponential maps

$$H^1_{\mathrm{f}}(K_v, V_p(B))^\vee \xrightarrow[\exp^*]{\simeq} H^0(B, \Omega^1_{B/K}),$$

for $v \mid p$. The left vertical arrow is obtained from dualities and defining exact triangles, so that the composition of the left vertical map and the lower horizontal map $\det_{\mathcal{R}_p}(\exp^* \otimes \mathrm{id})$ is another exponential map, which at $v \mid p$ is $\exp^*$. □

Knowing that the last two results are true, we can now pose the refined Burns–Flach Conjecture in the terminology of Kato.

Conjecture 6.0.5. *We have*

$$\vartheta_\infty^{-1}({}_R L(B,1)) \subset \Xi \otimes 1 \tag{6.2}$$

and

$$\mathcal{R}_p \cdot \det(\exp^* \otimes \mathrm{id})^{-1}(\vartheta_\infty^{-1}({}_R L(B,1)) = \Delta_{\mathcal{R}_p}(\mathcal{O}_{K,S}, T). \tag{6.3}$$

Chapter 7

Proof of the conjecture.

The proof will be indicated in this chapter, with more details being given in the following chapters.

7.1 A universal situation.

Following Kato, we now pass to a situation universal with respect to invertible sheaves over p-adic rings such as $T_p(B)$ over $\mathcal{R}_p$.

Write $K^{\mathfrak{m}}$ for the ray class field modulo $\mathfrak{m}$, and let $\mathfrak{f}$ be the conductor of B. Recall that S is the set of places of K dividing $\infty\mathfrak{f}p$. Put

$$\Lambda_n := \mathbb{Z}_p[\mathrm{Gal}(K^{\mathfrak{f}p^n}/K)],$$

$$\Lambda_\infty := \varprojlim_n \Lambda_n = \mathbb{Z}_p[\mathrm{Gal}(K^{\mathfrak{f}p^\infty}/K)] \text{ (the completed Galois group algebra)},$$

$$\mathcal{F}_n := (f_{K^{\mathfrak{f}p^n}})_*(f_{K^{\mathfrak{f}p^n}})^*(\mathbb{Z}_p(1)_{\mathrm{Spec}\mathcal{O}_{K,S}})$$

(f_L being the canonical morphism $\mathrm{Spec}\mathcal{O}_{L,S} \to \mathrm{Spec}\mathcal{O}_{K,S}$),

$$\mathcal{F}_\infty := \varprojlim_n \mathcal{F}_n$$

We write $\Delta_{\Lambda_\infty}(\mathcal{O}_{K,S},\mathcal{F})$ for the invertible Λ_∞-module

$$\left(\det_{\Lambda_\infty}(R\Gamma(\mathcal{O}_{K,S},\mathcal{F}))\right)^{-1}\otimes_{\Lambda_\infty}\left(\det_{\Lambda_\infty}(R\Gamma(\mathcal{O}_{K,S}\otimes_{\mathbb{Z}}\mathbb{R},\mathcal{F}(-1)))\right)^{-1}.$$

The action of $\mathrm{Gal}(\overline{K}/K)$ on $T_p(B)(-1)$ is given by a character

$$\mathrm{Gal}(\overline{K}/K)\twoheadrightarrow\mathrm{Gal}(K^{\mathfrak{f}p^\infty}/K)\longrightarrow\mathcal{R}_p^\times,$$

inducing a ring homomorphism $\Lambda_\infty\to\mathcal{R}_p$, so that

$$T\simeq\mathcal{F}_\infty\otimes_{\Lambda_\infty}\mathcal{R}_p$$

and

$$\Delta_{\Lambda_\infty}(\mathcal{O}_{K,S},\mathcal{F}_\infty)\otimes_{\Lambda_\infty}\mathcal{R}_p\simeq\Delta_{\mathcal{R}_p}(\mathcal{O}_{K,S},T).$$

To better describe

$$\Delta_{\Lambda_\infty}(\mathcal{O}_{K,S},\mathcal{F}_\infty),$$

we calculate the cohomology of $\mathcal{O}_{K,S}$ with $\mathcal{F}_\infty$-coefficients:

Lemma 7.1.1.

- $H^0(\mathcal{O}_{K,S},\mathcal{F}_\infty)=0$
- $H^1(\mathcal{O}_{K,S},\mathcal{F}_\infty)=\varprojlim_n\mathcal{O}^\times_{K^{\mathfrak{f}p^n},S}\otimes\mathbb{Z}_p$
- *There is a natural short exact sequence*

$$\varprojlim_n\mathrm{Pic}\mathcal{O}_{K^{\mathfrak{f}p^n},S}\otimes_{\mathbb{Z}}\mathbb{Z}_p\longrightarrow H^2(\mathcal{O}_{K,S},\mathcal{F}_\infty)\twoheadrightarrow\varprojlim_n\left(\bigoplus_{w|\mathit{finite}\ v\in S}\mathbb{Z}_p\right)^{\mathrm{sum}=0}.$$

Proof. We use the short exact sequence

$$0 \longrightarrow \mu_{p^k} \longrightarrow \mathbb{G}_{\mathrm{m}} \xrightarrow{p^k} \mathbb{G}_{\mathrm{m}} \longrightarrow 0\ ,$$

for which the Kummer sequence yields the following exact sequences:

$$0 \longrightarrow H^0(\mathcal{O}_{K\mathfrak{f}p^n,S}, \mu_{p^k}) \twoheadrightarrow H^0(\mathcal{O}_{K\mathfrak{f}p^n,S}, \mathbb{G}_{\mathrm{m}})_{p^k}$$

$$H^0(\mathcal{O}_{K\mathfrak{f}p^n,S}, \mathbb{G}_{\mathrm{m}})/p^k \rightarrowtail H^1(\mathcal{O}_{K\mathfrak{f}p^n,S}, \mu_{p^k}) \twoheadrightarrow H^1(\mathcal{O}_{K\mathfrak{f}p^n,S}, \mathbb{G}_{\mathrm{m}})_{p^k}$$

$$H^1(\mathcal{O}_{K\mathfrak{f}p^n,S}, \mathbb{G}_{\mathrm{m}})/p^k \longrightarrow H^2(\mathcal{O}_{K\mathfrak{f}p^n,S}, \mu_{p^k}) \longrightarrow H^2(\mathcal{O}_{K\mathfrak{f}p^n,S}, \mathbb{G}_{\mathrm{m}})_{p^k}$$
$$\| $$
$$\mathrm{Br}_S(\mathcal{O}_{K\mathfrak{f}p^n})_{p^k}$$

Take projective limits $\varprojlim_k$ to obtain the following exact sequences:

$$0 \longrightarrow H^0(\mathcal{O}_{K\mathfrak{f}p^n,S}, \mathbb{Z}_p(1)) \longrightarrow 0$$

$$\mathcal{O}_{K\mathfrak{f}p^n,S} \otimes_{\mathbb{Z}} \mathbb{Z}_p \rightarrowtail H^1(\mathcal{O}_{K\mathfrak{f}p^n,S}, \mathbb{Z}_p(1)) \twoheadrightarrow 0$$

$$\mathrm{Pic}\mathcal{O}_{K\mathfrak{f}p^n,S} \otimes_{\mathbb{Z}} \mathbb{Z}_p \rightarrowtail H^2(\mathcal{O}_{K\mathfrak{f}p^n,S}, \mathbb{Z}_p(1)) \twoheadrightarrow \left(\bigoplus_{w|\text{finite } v\in S} \mathbb{Z}_p \right)^{\text{sum}=0}$$

Take projective limits again, this time $\varprojlim_n$, we find

$$H^0(\mathcal{O}_{K,S}, \mathcal{F}_\infty) = 0$$

and

$$\varprojlim_n \mathcal{O}_{K^{\mathfrak{f}p^n},S} \otimes_{\mathbb{Z}} \mathbb{Z}_p = H^1(\mathcal{O}_{K,S}, \mathcal{F}_\infty),$$

and obtain another exact sequence:

$$\varprojlim_n \mathrm{Pic}\mathcal{O}_{K^{\mathfrak{f}p^n},S} \otimes_{\mathbb{Z}} \mathbb{Z}_p \longrightarrow H^2(\mathcal{O}_{K,S}, \mathcal{F}_\infty) \longrightarrow \varprojlim_n \left(\bigoplus_{w|\text{finite } v\in S} \mathbb{Z}_p \right)^{\text{sum}=0}$$

Thus the result is proved. □

We now use a construction of Kato ([13], III, §1.2). We will use his

Assumption 7.1.2. *K has class number 1.*

Kato's E, and its Grössencharacter ν, we will denote by E_0 and φ, respectively. Now, our E_0/K is an elliptic curve isogenous to our E of Chapter 5 and Chapter 6, and with complex multiplication by the full ring of integers $\mathcal{O}_K$. Then our "φ" here is consistent with that of those chapters.

We use the following proposition of Kato (written using our notation).

Proposition 7.1.3 ([13], III, 1.1.5). *Suppose $a \in \mathrm{End}(E_0^\chi)$, $(a, 6) = 1$. Then there exists a unique rational function $\theta_a \in K(E_0^\chi)^\times$ satisfying the following two conditions:*

$$\mathbf{N}_b(\theta_a) = \theta_a \text{ for any } b \in \mathrm{End}(E_0^\chi) \text{ such that } (a, b) = 1. \tag{7.1}$$

$$\text{The divisor of } \theta_a \text{ is } \deg(a)(e) - \ker(a). \tag{7.2}$$

Choose a non-zero ideal $\mathfrak{a}$ of $\mathcal{O}_K$ prime to $6\mathfrak{f}p$, and such that $\mathbf{N}(\mathfrak{a})\psi(a)^{-1}$ is not a root of 1. Set $a = \psi(\mathfrak{a})$. Let

$$\Upsilon_{a,n} : H^0(K^{\mathfrak{f}p^n} \otimes_K \mathbb{R}, \mathbb{Z}_p) \simeq \bigoplus_{\iota} H^0(\mathbb{C}, \mathbb{Z}_p) \to H^1(\mathcal{O}_{K^{\mathfrak{f}p^n},S}, \mathbb{Z}_p(1))$$

be the homomorphism

$$(a_\iota)_\iota \mapsto \sum_\iota a_\iota(\iota^{-1}(\theta_a(\exp(h_n)))),$$

where ι ranges over all embeddings $K^{\mathfrak{f}p^n} \to \mathbb{C}$ whose restriction to K concides with the given embedding of K into $\mathbb{C}$ (i.e., over all finite places of $K^{\mathfrak{f}p^n}$), and where $h_n = \pi^{-n}g^{-1}h$, $\pi = \psi(p)$, g a generator of $\mathfrak{f}$. Now h_n will be an $\mathcal{O}_K$-basis of $(\mathfrak{f}p^n)^{-1}H_1(E_0(\mathbb{C}), \mathbb{Z})$. (And $\theta_a(\exp(h_n))$ is independent of the choice of h and g because $\theta_a \circ [u] = \theta_a$ for any $u \in (\mathcal{O}_K)^\times$.) Then

$$\varprojlim_n \Upsilon_{a,n} : H^0(\mathbb{C}, \mathcal{F}_\infty(-1)) \to H^1(\mathcal{O}_{K,S}, \mathcal{F}_\infty)$$

corresponds to an element of

$$H^1(\mathcal{O}_{K,S}, \mathcal{F}_\infty) \otimes_{\Lambda_\infty} H^0(\mathbb{C}, \mathcal{F}_\infty(-1))^{-1},$$

which we denote by $z_{a,\Lambda_\infty}(\mathcal{O}_{K,S}, \mathcal{F}_\infty)$. Define

$$z_{a,\mathcal{R}_p}(\mathcal{O}_{K,S}, T) \in H^1(\mathcal{O}_{K,S}, T) \otimes_{\mathcal{R}_p} H^0(K \otimes \mathbb{R}, T(-1))^{-1}$$

to be the image of $z_{a,\Lambda_\infty}(\mathcal{O}_{K,S},\mathcal{F}_\infty)$ under the map

$$\begin{array}{c} H^1(\mathcal{O}_{K,S},\mathcal{F}_\infty)\otimes_{\Lambda_\infty} H^0(K\otimes\mathbb{R},\mathcal{F}_\infty(-1))^{-1} \\ \downarrow \\ H^1(\mathcal{O}_{K,S},T)\otimes_{\mathcal{R}_p} H^0(K\otimes\mathbb{R},T(-1))^{-1}. \end{array}$$

Define

$$z_{\mathcal{R}_p}(\mathcal{O}_{K,S},T)\in H^1(\mathcal{O}_{K,S},T)\otimes_{\mathcal{R}_p} H^0(\mathbb{C},T(-1))^{-1}$$

to be

$$\left(\mathbf{N}(\mathfrak{a})-\mathbf{N}(\mathfrak{a})\chi_T(\sigma_\mathfrak{a})^{-1}\right)^{-1} z_{a,\mathcal{R}_p}(\mathcal{O}_{K,S},T),$$

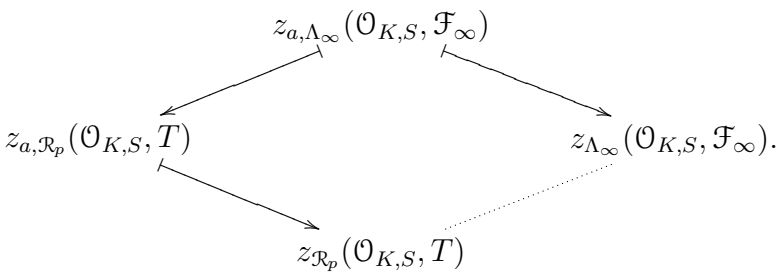
where χ_T is the action on T. Here $\mathbf{N}(\mathfrak{a})-\mathbf{N}(\mathfrak{a})\chi_T(\sigma_\mathfrak{a})$ is invertible in $\mathcal{R}_p$ because $\chi_T(\sigma_\mathfrak{a})=\mathbf{N}(\mathfrak{a})\psi(\mathfrak{a})^{-1}\alpha$ for a root α of 1 in $K[G]$. Then $z_{\mathcal{R}_p}(\mathcal{O}_{K,S},T)$ is independent of the choice of $\mathfrak{a}$. Define

$$z_{\Lambda_\infty}(\mathcal{O}_{K,S},\mathcal{F}_\infty)\in H^1(\mathcal{O}_{K,S},\mathcal{F}_\infty)\otimes_{\Lambda_\infty} H^0(\mathbb{C},\mathcal{F}_\infty(-1))^{-1}\otimes_{\Lambda_\infty}\mathrm{quot}(\Lambda_\infty)$$

to be

$$(\mathbf{N}(\mathfrak{a})-\sigma_\mathfrak{a})^{-1}\, z_{a,\Lambda_\infty}(\mathcal{O}_{K,S},\mathcal{F}_\infty).$$

Observe that we have constructed elements



7.2 The strategy of proof.

The rest of our exposition has two parts. First, following the approach of Kato, we show in §8 that $z_{\Lambda_\infty}(\mathcal{O}_{K,S}, \mathcal{F}_\infty)$ is an Λ_∞-basis of $\Delta_{\Lambda_\infty}(\mathcal{O}_{K,S}, \mathcal{F}_\infty)$, which allows us to conclude that $z_{\mathcal{R}_p}(\mathcal{O}_{K,S}, T)$ is a $\mathcal{R}_p$-basis of $\Delta_{\mathcal{R}_p}(\mathcal{O}_{K,S}, T)$. Second, we find (Theorem 9.0.2), using [13], III, Theorem 1.2.6, that the image of $z_{\mathcal{R}_p}(\mathcal{O}_{K,S}, T)$ under the map

$$\det_{\mathcal{R}_p}(\exp^* \otimes \mathrm{id}) : \det_{\mathcal{R}_p} \Delta_{\mathcal{R}_p}(\mathcal{O}_{K,S}, V) \to \Xi \otimes \mathbb{Q}_p$$

is sent by ϑ_∞ to $(L_S((\varphi\chi)^{-1}, 0))_{\chi \in \hat{G}}$, where $L_S((\varphi\chi)^{-1}, 0)$ equals the L-value $L(\overline{\varphi\chi}, 1)$, deprived of the Euler factors at primes dividing $\mathfrak{f}$. But the Euler factors at primes of bad reduction are 1, and we shall assume that the Euler factors at any other primes dividing $\mathfrak{f}$, are also units at p. So we may disregard the missing Euler factors.

Our result on the image of

$$z_{\mathcal{R}_p}(\mathcal{O}_{K,S}, T)$$

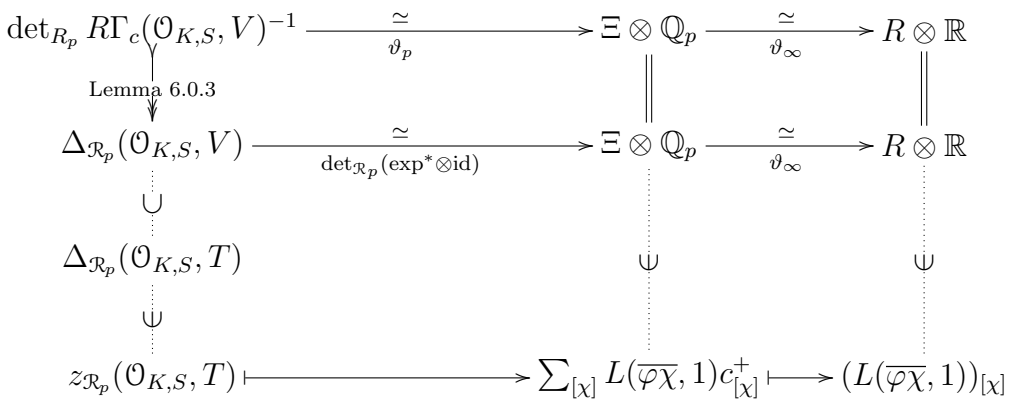
shows that the image of

$$\det_{\mathcal{R}_p} \Delta_{\mathcal{R}_p}(\mathcal{O}_{K,S}, T)$$

under $\exp^*$ is generated by $(\vartheta_\infty)^{-1}({}_R L(B/K, 1))$, as asserted by the Burns–Flach Conjecture.

We summarize the strategy of proof, including the translation of the re-

fined Burns–Flach Conjecture into the terminology of Kato, in the following diagram:



The first line depicts the morphisms involved in the refined Burns–Flach Conjecture. The second line shows the translation into the terminology of Kato. On the third line is given the integral submodule of the vector space just above. On the fourth line is a basis for the integral submodule (on the left), and its images under the two maps of the second line. The element $c^+_{[\chi]}$ is defined to be the pre-image, under ϑ_∞, of the element of R with $[\chi]$-component 1 and all other components 0.

Chapter 8

A Λ_∞-basis of $\Delta_{\Lambda_\infty}(\mathcal{O}_{K,S}, \mathcal{F}_\infty)$.

We will make an

Assumption 8.0.1.

- *K has class number 1.*
- *$p \not| [K(\mathfrak{f}_0 p) : K]$, where $\mathfrak{f}_0 \mid \mathfrak{f}$ is the prime-to-p part of $\mathfrak{f}$.*
- *$p \not| \mu(H_K)$, where H_K is the Hilbert Class Field of K.*

In this chapter we prove the following

Theorem 8.0.2. *Recall that the finite places of S are exactly those dividing $\mathfrak{f}p$. Then*

$$z_{\Lambda_\infty}(\mathcal{O}_{K,S}, \mathcal{F}_\infty)$$

is an Λ_∞-basis of

$$\Delta_{\Lambda_\infty}(\mathcal{O}_{K,S}, \mathcal{F}_\infty).$$

To work more easily with the element

$$z_{\Lambda_\infty}(\mathcal{O}_{K,S}, \mathcal{F}_\infty) \in H^1(\mathcal{O}_{K,S}, \mathcal{F}_\infty) \otimes_{\mathcal{R}_p} H^0(K \otimes \mathbb{R}, \mathcal{F}_\infty(-1))^{-1},$$

we fix a basis

$$y_{\Lambda_\infty}(\mathcal{O}_{K,S}, \mathcal{F}_\infty)$$

of

$$H^0(K \otimes \mathbb{R}, \mathcal{F}_\infty(-1))^{-1}.$$

Here $y_{\Lambda_\infty}(\mathcal{O}_{K,S}, \mathcal{F}_\infty)$ is an inverse system of embeddings

$$K^{\mathfrak{f}p^n} \hookrightarrow \mathbb{C}$$

which could come, for example, from a fixed embedding $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$. Now also fix

$$x_{a,\Lambda_\infty}(\mathcal{O}_{K,S}, \mathcal{F}_\infty) \in H^1(\mathcal{O}_{K,S}, \mathcal{F}_\infty)$$

such that

$$z_{a,\Lambda_\infty}(\mathcal{O}_{K,S}, \mathcal{F}_\infty) = x_{a,\Lambda_\infty}(\mathcal{O}_{K,S}, \mathcal{F}_\infty) \otimes_{\mathcal{R}_p} y_{\Lambda_\infty}(\mathcal{O}_{K,S}, \mathcal{F}_\infty)$$

and

$$y_{\Lambda_\infty}(\mathcal{O}_{K,S}, \mathcal{F}_\infty)$$

is a basis of $H^0(K \otimes \mathbb{R}, \mathcal{F}_\infty(-1))^{-1}$. Correspondingly, we express

$$z_{\Lambda_\infty}(\mathcal{O}_{K,S}, \mathcal{F}_\infty) = x_{\Lambda_\infty}(\mathcal{O}_{K,S}, \mathcal{F}_\infty) \otimes_{\mathcal{R}_p} y_{\Lambda_\infty}(\mathcal{O}_{K,S}, \mathcal{F}_\infty),$$

where

$$x_{\Lambda_\infty}(\mathcal{O}_{K,S}, \mathcal{F}_\infty) = (\mathbf{N}(\mathfrak{a}) - \sigma_\mathfrak{a})^{-1} x_{a,\Lambda_\infty}(\mathcal{O}_{K,S}, \mathcal{F}_\infty).$$

The primary result we will be using is the

Theorem 8.0.3 ([17], Theorem 4.1: Main Conjecture).

$$\mathrm{char}(A_\infty) = \mathrm{char}(U_\infty/\mathcal{C}_\infty),$$

where

$$A_\infty = \varprojlim_n A_n$$

$$U_\infty = \varprojlim_n U_n$$

$$\mathcal{C}_\infty = \varprojlim_n \mathcal{C}_n,$$

where A_n is the p-part of the ideal class group of $K^{\mathfrak{f}p^n}$, U_n is the global units, and $\mathcal{C}_n$ is the elliptic units. The inverse limits are all with respect to the norm maps.

We need a lemma to permit us to deal with modules over discrete valuation ring, instead of with the Λ_∞-modules themselves.

Lemma 8.0.4. *Let N be a local Noetherian integral domain and suppose $I, J \subset M$ are two invertible N-submodules of an invertible* quot$N$*-submodule M. (Since N and* quot$N$ *are local, "invertible" means free of rank 1.) If N is Cohen-Macaulay then $I = J$ if and only if $I_\mathfrak{q} = J_\mathfrak{q}$ for all height-1 prime ideals $\mathfrak{q}$ of N.*

Proof. The result would follow if we could show that

$$I = \bigcap_{\mathrm{ht}\mathfrak{q}=1} I_{\mathfrak{q}} \subset M \text{ and } J = \bigcap_{\mathrm{ht}\mathfrak{q}=1} J_{\mathfrak{q}} \subset M.$$

Since $I_{\mathfrak{q}} = N_{\mathfrak{q}} \otimes_N I$ and $J_{\mathfrak{q}} = N_{\mathfrak{q}} \otimes_N J$, then this would in turn be implied by

$$N = \bigcap_{\mathrm{ht}\mathfrak{q}=1} N_{\mathfrak{q}} \subset \mathrm{quot}N.$$

The inclusion

$$N \subseteq \bigcap_{\mathrm{ht}\mathfrak{q}=1} N_{\mathfrak{q}}$$

is obvious. To prove

$$N \supseteq \bigcap_{\mathrm{ht}\mathfrak{q}=1} N_{\mathfrak{q}},$$

let

$$\mathrm{quot}N \ni \frac{x}{y} \notin N,$$

where $x, y \in N$. Then $y \notin N^*, \Rightarrow (y) \neq N$, so that y is a (1-term) N-regular sequence. By [15] §15 Lemma 4, we find that

$$\dim N/(y) = \dim N - 1.$$

But [15] §16 Theorem 31(i) implies that

$$\dim N/(y) = \dim N - \mathrm{ht}(y).$$

We conclude that $\mathrm{ht}(y)$=1, which means that y lies in some height-1 prime

ideal $\mathfrak{q}$ of N. Therefore $\frac{x}{y} \notin N_{\mathfrak{q}}$ and in particular

$$\frac{x}{y} \notin \bigcap_{\mathrm{ht}\mathfrak{q}=1} N_{\mathfrak{q}}.$$

□

Note 8.0.5. *The ring Λ_∞ is*

$$\mathbb{Z}_p[\mathrm{Gal}(K^{\mathfrak{f}_0 p}/K)][[\mathrm{Gal}(K^{\mathfrak{f}_0 p^\infty}/K^{\mathfrak{f}_0 p})]] \simeq \mathbb{Z}_p[\mathrm{Gal}(K^{\mathfrak{f}_0 p}/K)][[x,y]],$$

where $\mathfrak{f}_0$ is the prime-to-p part of $\mathfrak{f}$. If $p \nmid [K^{\mathfrak{f}_0 p} : K]$ then $\mathbb{Z}_p[\mathrm{Gal}(K^{\mathfrak{f}_0 p}/K)]$ is a product of discrete valuation rings; hence Λ_∞ is regular. If $p \mid [K^{\mathfrak{f}_0 p} : K]$ then Λ_∞ is no longer regular. But the ring Λ_∞ is a complete intersection and in particular is Cohen–Macaulay.

We will use the Main Conjecture to analyze $\Delta_{\Lambda_\infty}(\mathcal{O}_{K,S}, \mathcal{F}_\infty)$. The following lemma relates the cohomology of $\mathcal{O}_{K,S}$ to Rubin's Iwasawa modules, to which we will then be able to apply the Main Conjecture.

Lemma 8.0.6.

- $H^1(\mathcal{O}_{K,S}, \mathcal{F}_\infty) \simeq U_{S,\infty}$
- $0 \longrightarrow A_{S,\infty} \longrightarrow H^2(\mathcal{O}_{K,S}, \mathcal{F}_\infty) \longrightarrow X_{S,\infty} \longrightarrow 0$ *(exact)*

Note 8.0.7. *The Main Conjecture deals with modules U_∞ and A_∞, whereas here we are using the respectively corresponding modules $U_{S,\infty}$ and $A_{S,\infty}$, where the finite primes above those of S are inverted. We have the exact sequence*

$$0 \to U_\infty \to U_{S,\infty} \to Y'_{S,\infty} \to A_\infty \to A_{S,\infty} \to 0$$

of Λ_∞-modules, which gives rise to the following exact sequence of Λ_∞-modules

$$0 \to U_\infty/\mathcal{C}_\infty \to U_{S,\infty}/\mathcal{C}_\infty \to Y'_{S,\infty} \to A_\infty \to A_{S,\infty} \to 0.$$

Moreover, for any height-1 prime $\mathfrak{q}$ we have $\mathrm{char}(Y'_{S,\infty,\mathfrak{q}}) = 0$. (To see this, consider a place v of K. If v has infinite inertial degree, we have $Y'_{\{w|v\},\infty}$ itself being 0 since the norm maps on units (the maps between the various components of the projective limit) correspond to multiplication by the inertial degrees on the corresponding valuations. On the other hand, if $v = p$, then since there only finitely many places above p in K_∞, then $Y'_{\{w|v\},\infty}$ is finitely generated over $\mathbb{Z}_p$, hence pseudonull.)

Proof of Lemma 8.0.6. Since

$$\varprojlim_n \mathcal{O}^\times_{K^{\mathfrak{f}p^n},S} \otimes \mathbb{Z}_p \simeq \varprojlim_n U_{S,n} = U_{S,\infty},$$

$$\varprojlim_n \mathrm{Pic}\mathcal{O}_{K^{\mathfrak{f}p^n},S} \otimes_{\mathbb{Z}} \mathbb{Z}_p \simeq \varprojlim_n A_{S,n} = A_{S,\infty},$$

and

$$\begin{array}{ccccccccc} 0 & \longrightarrow & X_{S,\infty} & \longrightarrow & Y_{S,\infty} & \longrightarrow & \mathbb{Z}_p & \longrightarrow & 0\,, \\ & & & & \| & & & & \\ & & & & \varprojlim_n \left(\bigoplus_{\text{finite } w|v\in S} \mathbb{Z}_p \right) & & & & \end{array}$$

then Lemma 7.1.1 immediately yields the desired result. □

Another lemma relates the constructed element

$$x_{a,\Lambda_\infty}(\mathcal{O}_{K,S},\mathcal{F}_\infty)\in H^1(\mathcal{O}_{K,S},\mathcal{F}_\infty)$$

to the Iwasawa modules:

Lemma 8.0.8. *For all height-1 prime ideals $\mathfrak{q}$ of Λ_∞, we have*

$$\mathrm{length}_{\Lambda_\infty,\mathfrak{q}}(\Lambda_{\infty,\mathfrak{q}}/x_{\Lambda_\infty}(\mathcal{O}_{K,S},\mathcal{F}_\infty)\cdot\Lambda_{\infty,\mathfrak{q}})+\mathrm{length}_{\Lambda_\infty,\mathfrak{q}}X_{S,\infty,\mathfrak{q}}=\mathrm{length}_{\Lambda_\infty,\mathfrak{q}}\mathcal{C}_{\infty,\mathfrak{q}}.$$

Proof of Lemma 8.0.8. The ideal $\mathfrak{q}$ induces a character

$$\mathrm{Gal}(K_{\mathfrak{f}p}/K)=G_\infty^{\mathrm{tor}}\subset\Lambda\to\Lambda_\mathfrak{q}\to\Lambda_\mathfrak{q}/\mathfrak{q}\Lambda_\mathfrak{q}\simeq\mathbb{Q}_p(\psi),$$

(where the last is some finite extension of $\mathbb{Q}_p$) the prime-to-p part of which we denote $\mathfrak{d}\mid\mathfrak{f}_0$. Now $\mathcal{C}_{\infty,\mathfrak{q}}$ is spanned by an elliptic unit $x_{\mathfrak{d}p^\infty}$, while

$$x_{\mathfrak{f}_0p^\infty}=x_{\Lambda_\infty}(\mathcal{O}_{K,S},\mathcal{F}_\infty)$$

(both denoted using notation of the form $\Theta(v;L,\mathfrak{a})$ in [19], II, §2), satisfying the Euler relations

$$\mathbf{N}_{K^{\mathfrak{f}_0}/K^{\mathfrak{d}}}(x_{\mathfrak{f}_0p^\infty})=\left(\prod_{\mathfrak{p}\mid\mathfrak{f}_0,\nmid\mathfrak{d}}(1-\mathrm{Frob}_\mathfrak{p}^{-1})\right)x_{\mathfrak{d}p^\infty},$$

where

$$\mathbf{N}_{K^{\mathfrak{f}_0}/K^{\mathfrak{d}}} = \sum_{\sigma \in \mathrm{Gal}(K^{\mathfrak{f}_0}/K^{\mathfrak{d}})} \sigma \in \Lambda.$$

Localizing at $\mathfrak{q}$, the norm element $N_{K^{\mathfrak{f}_0}/K^{\mathfrak{d}}}$ becomes a unit in $\Lambda_{\mathfrak{q}}$ and thus $x_{\mathfrak{f}_0 p^\infty}$ a multiple of $x_{\mathfrak{d}p^\infty}$. Moreover, the element

$$\prod_{\mathfrak{p}|\mathfrak{f}_0, \nmid \mathfrak{d}} (1 - \mathrm{Frob}_{\mathfrak{p}}^{-1})$$

is also the charactistic ideal of $X_{S,\infty,\mathfrak{q}}$. The result follows. □

Now we are ready to give the

Proof of **Theorem 8.0.2**. We will consider the situation locally, one prime at a time. (We will use the fact that

$$\mathrm{char}(M) = \prod_{\mathrm{ht}\,\mathfrak{q}=1} \mathfrak{q}^{\mathrm{length}_{R_{\mathfrak{q}}} M_{\mathfrak{q}}}$$

for any finitely generated torsion Λ_∞-module M.) We aim to prove that

$$z_{\Lambda_\infty}(\mathcal{O}_{K,S}, \mathcal{F}_\infty)$$

is a $(\Lambda_\infty)_{\mathfrak{q}}$-basis of

$$\Delta_{\Lambda_\infty}(\mathcal{O}_{K,S}, \mathcal{F}_\infty)_{\mathfrak{q}},$$

for any height-1 prime $\mathfrak{q}$. We will then conclude from Lemma 8.0.4 that $z_{\Lambda_\infty}(\mathcal{O}_{K,S}, \mathcal{F}_\infty)$ is a Λ_∞-basis of $\Delta_{\Lambda_\infty}(\mathcal{O}_{K,S}, \mathcal{F}_\infty)$.

Fix a height-1 prime $\mathfrak{q}$ of Λ_∞. We may apply Lemma 8.0.4 here.

Considering the integral complex

$$R\Gamma(\mathcal{O}_{K,S},\mathcal{F}_\infty)_{\mathfrak{q}},$$

the result will follow if we can show that

$$H^1(\mathcal{O}_{K,S},\mathcal{F}_\infty)_{\mathfrak{q}}/((\Lambda_\infty)_{\mathfrak{q}}\cdot x_{\Lambda_\infty}(\mathcal{O}_{K,S},\mathcal{F}_\infty))$$

and

$$\simeq H^2(\mathcal{O}_{K,S},\mathcal{F}_\infty)_{\mathfrak{q}}$$

have the same length as $\Lambda_{\infty,\mathfrak{q}}$-modules.

By the first assertion of Lemma 8.0.6, and 8.0.8, this last statement is equivalent to

$$\begin{aligned}&\mathrm{char}_{\Lambda_{\infty,\mathfrak{q}}}(U_{S,\infty,\mathfrak{q}}/\mathcal{C}_{\infty,\mathfrak{q}})\cdot\mathrm{char}_{\Lambda_{\infty,\mathfrak{q}}}X_{S,\infty,\mathfrak{q}}\\ =&\mathrm{char}_{\Lambda_{\infty,\mathfrak{q}}}H^2(\mathcal{O}_{K,S},\mathcal{F}_\infty)_{\mathfrak{q}}\cdot\mathrm{char}_{\Lambda_{\infty,\mathfrak{q}}}Y'_{S,\infty,\mathfrak{q}},\end{aligned}$$

then by the second assertion of Lemma 8.0.6, to

$$\begin{aligned}&\mathrm{char}_{\Lambda_{\infty,\mathfrak{q}}}(U_{S,\infty,\mathfrak{q}}/\mathcal{C}_{\infty,\mathfrak{q}})\cdot\mathrm{char}_{\Lambda_{\infty,\mathfrak{q}}}X_{S,\infty,\mathfrak{q}}\\ =&\mathrm{char}_{\Lambda_{\infty,\mathfrak{q}}}X_{S,\infty,\mathfrak{q}}\cdot\mathrm{char}_{\Lambda_{\infty,\mathfrak{q}}}A_{S,\infty,\mathfrak{q}}\cdot\mathrm{char}_{\Lambda_{\infty,\mathfrak{q}}}Y'_{S,\infty,\mathfrak{q}},\end{aligned}$$

which is rephrased

$$\begin{aligned}&\mathrm{length}_{\Lambda_{\infty,\mathfrak{q}}}(U_{S,\infty,\mathfrak{q}}/\mathcal{C}_{\infty,\mathfrak{q}})\\ =&\mathrm{length}_{\Lambda_{\infty,\mathfrak{q}}}A_{S,\infty,\mathfrak{q}}+\mathrm{length}_{\Lambda_{\infty,\mathfrak{q}}}Y'_{S,\infty,\mathfrak{q}}.\end{aligned}$$

In view of Note 8.0.7, the last statement becomes

$$\mathrm{length}_{\Lambda_{\infty,\mathfrak{q}}}(U_{\infty,\mathfrak{q}}/\mathcal{C}_{\infty,\mathfrak{q}})=\mathrm{length}_{\Lambda_{\infty,\mathfrak{q}}}A_{\infty,\mathfrak{q}}.$$

Consequently, the statement to be proved follows from the Main Conjecture. □

Chapter 9

The image of the basis.

We wish to consider the $[\chi]$-components of R individually, where $[\chi]$ is the orbit of $\chi \in \hat{G}$ under $\mathrm{Aut}_K\mathbb{C}$. Accordingly, choose for each $[\chi]$ a pre-image $c^+_{[\chi]}$, under ϑ_∞ in Ξ, of the element of R with $[\chi]$-component 1 and the other components 0.

We rephrase a result of Kato to identify the image of the basis $z_\Lambda(\mathcal{O}_{K,S}, T)$. In his setting, it is assumed that the class number of K is 1, but that assumption is not actually used in the result we apply here.

First we introduce Kato's notation. Let A be a finite product of finite extensions of K. Let $\Lambda = A \otimes \mathbb{Q}_p$. Let $\mathcal{F}$ be an invertible smooth Λ-sheaf on $X = \mathrm{Spec}(\mathcal{O}_{K,S})$ such that there exists an integer $r \geq 1$ and a homomorphism $\lambda : \mathrm{Gal}(K^{\mathrm{ab},S}/K) \to A^\times$ which is continuous for the discrete topology of $A^\times$ satisfying the condition that $\chi_\mathcal{F} = \chi_{\mathrm{cyclo}}(\sigma)\chi_E(\sigma)\lambda(\sigma)^{-r}$ for all $\sigma \in \mathrm{Gal}(K^{\mathrm{ab},S}/K)$, where $\chi_\mathcal{F} : \mathrm{Gal}(K^{\mathrm{ab},S}/K) \to (\mathcal{O}_K \otimes \mathbb{Z}_p)^\times \subset A^\times$ is the action on $\mathcal{F}$. Define $\Sigma = H_1(B(\mathbb{C}), \mathbb{Q})^{-1}$ and $\Omega = H^0(B, \Omega^1_{B/K})$.

The result, in the notation of Kato, is:

Theorem 9.0.1 ([13], Theorem III.1.2.6). *The element $z_\Lambda(X, \mathcal{F})$ is sent*

by the map

$$\exp^* \otimes \mathrm{id} : H^1(X, \mathcal{F}) \otimes_A \Sigma^{-1} \to (\Omega \otimes_A \Sigma^{-1}) \otimes \mathbb{Q}_p$$

to an element of $\Omega \otimes_A \Sigma^{-1}$ *whose image in* $A \otimes \mathbb{R}$ *coincides with*

$$(-1)^{r-1} L_{A,S}(X, \mathcal{F}^*(1), 0).$$

In our case $r = 1$, $\mathcal{F} = T$, $A = R$, and $L_{A,S}(X, \mathcal{F}^*(1), 0) = L_S((\varphi\chi^{-1}, 0)$. Kato's result becomes:

Theorem 9.0.2. *The image of* $z_\Lambda(\mathcal{O}_{K,S}, T)$ *under the map*

$$\exp^* \otimes \mathrm{id} : H^1(\mathcal{O}_{K,S}, T) \otimes_R H_1(B(\mathbb{C}), \mathbb{Q}) \to H^0(B, \Omega^1_{B/K}) \otimes_R H_1(B(\mathbb{C}), \mathbb{Q}) \otimes \mathbb{Q}_p,$$

with respect to the chosen bases, has $[\chi]$*-component* $L_S((\varphi\chi)^{-1}, 0)$.

We recall in this chapter the proof of this theorem. Fix, for the proof, an embedding $\iota : K^{\mathrm{ab},S} \to \mathbb{C}$, and thus, by restriction, embeddings $\iota_n : K^{\mathfrak{p}^n} \to \mathbb{C}$.

Denote by $u := (u_n)_n$ the norm-compatible system

$$(\iota_n^{-1}(\theta_a(\exp(h_n))))_n \in ((K^{\mathfrak{p}^n})^\times)_n.$$

Define the $\mathcal{O}_{K,p}$-basis ξ of $H^0(K^{\mathrm{ab},S}, T)$ to be the image of $g^{-1}h$ under the isomorphisms

$$H_1(E_0^\chi(\mathbb{C}), \mathbb{Z}) \otimes \mathbb{Z}_p \simeq H^0(\mathbb{C}, T) \simeq H^0(K^{\mathrm{ab},S}, T)$$

(where the right-hand isomorphism is induced by ι). Let $\xi_n = \pi^{-n}\xi \bmod T \in V/T$. Then the Coleman power series $g_{u,\xi}$ associated to u and ξ is the function

$$z \mapsto \theta_a(z + \iota^{-1}(\exp(g^{-1}h)))$$

on $\widehat{E_0^\chi}$.

Fix n for the rest of the proof. Define $s \in H^1(K^{\mathfrak{f}p^n}, T^\vee(1))$ to be the image of u under

$$\begin{array}{ccc} \varprojlim_m (K^{\mathfrak{f}p^n})^\times & \longrightarrow & \varprojlim_m H^1(K^{\mathfrak{f}p^n}, \mathbb{Z}_p(1)) \\ & & \downarrow \cup(\xi_m)_m^\vee \\ \varprojlim_m H^1(K^{\mathfrak{f}p^n}, T^\vee(1)/\pi^m) & \xleftarrow[\text{trace}]{} & \varprojlim_m H^1(K^{\mathfrak{f}p^n}, T^\vee(1)/\pi^m) \\ \simeq \downarrow & & \\ H^1(K^{\mathfrak{f}p^n}, T^\vee(1)) & & \end{array}.$$

We will shortly apply the

Theorem 9.0.3 (Explicit Reciprocity Law). *([13], II, 2.1.7) The function*

$$\exp^* : H^1(K^{\mathfrak{f}p^n}, T^\vee(1)) \to \mathrm{coLie}(E_0^\chi) \otimes_{\mathcal{O}_K} K^{\mathfrak{f}p^n}$$

sends s to

$$\pi^{-n}\omega \otimes \left(\left(\frac{d}{\omega}\right)\log(\varphi^{-n}(g_{u,\xi}))\right)(\xi_n)$$

(Here ω can be taken to be any $\mathcal{O}_K$-basis of $\mathrm{coLie}(E_0^\chi)$*.)*

Consider the composite map

$$\begin{aligned} H^0(B, \Omega^1_{B/K})^\vee \to & H^1(\mathcal{O}_{K,S}, T) \\ \to & H^1(\mathcal{O}_{K^{\mathfrak{f}p^n},S}), T^{-1}(1)) \\ \to & H^1((K^{\mathfrak{f}p^n})_p, T^{-1}(1)), \end{aligned}$$

where the first arrow is defined by the element $z_{a,\Lambda}(\mathcal{O}_{K,S}, T)$.

Consider the element of $H^\vee_{\mathrm{B}}$ whose v-component is h_v^{-1} if v agrees with our embedding $\iota : K^{\mathrm{ab},S} \to \mathbb{C}$ and is 0 if v does not. This element is sent to

$$g^{-1} \cdot s \in H^1(K^{\mathfrak{f}p^n} K_p, T^{-1}(1))$$

by the above composite map. (We have related the Coleman power series $g_{u,\xi}$ to the element $z_{a,\Lambda}(\mathcal{O}_{K,S}, T)$.)

Applying the Explicit Reciprocity Law, we find that this element is sent by $\exp^*$ to

$$g^{-1} \cdot \pi^{-n}\omega \otimes \left(\left(\frac{d}{\omega} \right) \log(\varphi^{-n}(g_{u,\xi})) \right) (\xi_n) \in \mathrm{coLie}(E_0^\chi) \otimes_{\mathcal{O}_K} K^{\mathfrak{f}p^n},$$

where ξ_n denotes ξ restricted to $K^{\mathfrak{f}p^n}$.

To put this expression in useful form we apply a lemma. We use $\theta_{(\varphi\chi)(\mathfrak{a})}$, as described by Proposition 7.1.3:

Lemma 9.0.4. *([13], III, 1.1.6) Write* $\tau = \left(\frac{K^{\mathfrak{f}p^n}/K}{\mathfrak{a}} \right) \in \mathrm{Gal}(K^{\mathfrak{f}p^n}/K)$, *and let*

$\alpha = \exp(h_n) \in (E_0^\chi)_{\mathfrak{f}p^n}(\mathbb{C}) = (E_0^\chi)_{\mathfrak{f}p^n}(K^{p^n})$, $\sigma \in \mathrm{Gal}(K^{\mathfrak{f}p^n}/K)$. *The value of*

$$\left(\frac{d}{\omega}\right)\log(\theta_{(\varphi\chi)(\mathfrak{a})})$$

at $\sigma\alpha$ *is equal to*

$$\left(\int_{h_n}\omega\right)^{-1}\cdot\left(\mathbf{N}(\mathfrak{a})L_{\sigma\text{-}part}((\varphi\chi)^{-1},0)-(\varphi\chi)(\mathfrak{a})L_{\sigma\tau\text{-}part}((\varphi\chi)^{-1},0)\right).$$

Choose $\mathfrak{a}\equiv 1(\mod \mathfrak{f})$, so that $\tau = 1$ and the above expression is simplified. The image of $z_{a,\Lambda}(\mathcal{O}_{K,S},T)$ we wish to ascertain is

$$g^{-1}\cdot\pi^{-n}\omega\otimes\left(\int_{h_n}\omega\right)^{-1}\cdot\left(\mathbf{N}(\mathfrak{a})-(\varphi\chi)(\mathfrak{a})\right)L_S((\varphi\chi)^{-1},0)$$

It follows that the image of

$$z_\Lambda(\mathcal{O}_{K,S},T)=\left(\mathbf{N}(\mathfrak{a})-\mathbf{N}(\mathfrak{a})\chi_T(\sigma_\mathfrak{a})^{-1}\right)^{-1}z_{a,\Lambda}(\mathcal{O}_{K,S},T)$$

is

$$\begin{aligned}
&g^{-1}\cdot\pi^{-n}\omega\otimes\left(\int_{h_n}\omega\right)^{-1}\cdot L_S((\varphi\chi)^{-1},0)\\
=&g^{-1}\cdot\pi^{-n}\omega\otimes\left(\int_{\pi^{-n}g^{-1}h}\omega\right)^{-1}\cdot L_S((\varphi\chi)^{-1},0),\\
=&\omega\otimes\left(\int_{h}\omega\right)^{-1}\cdot L_S((\varphi\chi)^{-1},0),\\
=&c^+_{[\chi]}\cdot L_S((\varphi\chi)^{-1},0)\\
=&c^+_{[\chi]}\cdot L_S(\overline{\varphi\chi},1).
\end{aligned}$$

This proves Theorem 9.0.2.

Chapter 10

Examples.

In this chapter we will find examples, or show the existence of examples, of elliptic curves to which the our main theorem applies.

We search for elliptic curves E/F, having complex multiplication by a nonmaximal order $\mathcal{O} = \mathbb{Z} + f \cdot \mathcal{O}_K$, for which the Mordell-Weil group $E(F)$ has rank 0.

We will make some simplifying assumptions:

Assumption 10.0.1.

- *K has class number 1.*
- *f is a prime ≥ 3.*

The field F contains the j-invariant of E. The **ring class group** is $G_f := \frac{I_f}{Z_f P_f}$, where I_f is the group of fractional ideals prime to f, Z_f is the group of principal ideals with a generator in $\mathbb{Q} \subset K$, and P_f is the group of principal ideals with a generator $\equiv 1 \mod f$. The **ring class field** of $\mathcal{O}$ is a field H_f such that $\mathrm{Gal}(H_f/K) \simeq G_f$. The theory of complex multiplication shows that we may take also:

- $F = H_f$.

10.1 Elliptic curves with rank 0.

Note 10.1.1. *If E/F and E_0/F are two elliptic curves isogenous over F, then*

$$L(E/F, s) = L(E_0/F, s).$$

We have the following theorem of Coates and Wiles ([5]), a generalization of a result of Arthaud:

Theorem 10.1.2. *If* $\operatorname{rank}(E_0(F)) \geq 1$ *then* $L(E_0/F, 1) = 0$.

Accordingly, we search for elliptic curves E_0 for which

$$L(E_0/F, 1) \neq 0.$$

Then we will try to show the existence of elliptic curves E/F, isogenous over F, with complex multiplication by $\mathcal{O} = \mathbb{Z} + f \cdot \mathcal{O}_K$.

10.2 Elliptic curves with complex multiplication by a nonmaximal order.

Suppose E_0/K is an elliptic curve with complex multiplication by $\mathcal{O}_K$. There exists an elliptic curve $E/\overline{K}$, with complex multiplication by $\mathcal{O}$, fitting into the short exact sequence

$$0 \longrightarrow C \longrightarrow E_0 \longrightarrow E \longrightarrow 0\ ,$$

with C finite.

Theorem 10.2.1. *E is defined over H_f.*

To prove this theorem we use the following

Lemma 10.2.2. *There exists a short exact sequence*

$$0 \longrightarrow T_f E_0 \longrightarrow T_f E \longrightarrow C \longrightarrow 0.$$

Proof of lemma. For each $n \geq 1$, we have the diagram, with exact rows and columns:

$$\begin{array}{ccccccccc}
 & & & & 0 & & 0 & & \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & E_{0,f^n} & \longrightarrow & E_{f^n} & \longrightarrow & C'_n \longrightarrow 0 \\
 & & & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & C & \longrightarrow & E_0 & \longrightarrow & E & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \cdot f^n} & & \downarrow{\scriptstyle \cdot f^n} & & \downarrow{\scriptstyle \cdot f^n} & & \\
0 & \longrightarrow & C & \longrightarrow & E_0 & \longrightarrow & E & \longrightarrow & 0 \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & 0 & & 0 & &
\end{array}$$

The leftmost vertical map is 0 since C is f-torsion. By diagram-chasing, we get an isomorphism $C'_n \to C$. Chasing the diagram

$$\begin{array}{ccccccc}
E_{0,f^n} & \longrightarrow & E_{f^n} & \longrightarrow & C'_n & \longrightarrow & 0 \\
\downarrow{\scriptstyle \cdot f} & & \downarrow{\scriptstyle \cdot f} & & & & \\
E_{0,f^{n-1}} & \longrightarrow & E_{f^{n-1}} & \longrightarrow & C'_{n-1} & \longrightarrow & 0 \\
\downarrow & & \downarrow & & & & \\
0 & & 0 & & & &
\end{array}$$

shows that there is an isomorphism $C'_n \to C'_{n-1}$ which is compatible with the isomorphisms $C'_n \to C$ and $C'_{n-1} \to C$ constructed above, in that the diagram

$$\begin{array}{ccc} C'_n & \xrightarrow{\simeq} & C'_{n-1} \\ & {\scriptstyle\simeq}\searrow \quad \swarrow{\scriptstyle\simeq} & \\ & C & \end{array}$$

commutes. Then, taking the projective limit over diagrams

$$\begin{array}{ccccccc} E_{0,f^n} & \longrightarrow & E_{f^n} & \longrightarrow & C'_n & \longrightarrow & 0 \\ \downarrow{\scriptstyle\cdot f} & & \downarrow{\scriptstyle\cdot f} & & \downarrow & & \\ E_{0,f^{n-1}} & \longrightarrow & E_{f^{n-1}} & \longrightarrow & C'_{n-1} & \longrightarrow & 0, \end{array}$$

we conclude that there is an exact sequence

$$0 \longrightarrow T_f E_0 \longrightarrow T_f E \longrightarrow C \longrightarrow 0.$$

□

Proof of Theorem 10.2.1. Consider the action of $\mathcal{O}_{K,f}$ upon $T_f E_0$. It gives rise to a representation

$$\mathbb{Z}_f[\mathrm{Gal}(\overline{K}/K)] \to \mathcal{O}_{K,f}^{\times}.$$

The image of

$$\mathbb{Z}_f[\mathrm{Gal}(\overline{K}/H_f)]$$

lies in $(\mathbb{Z}_f + f\mathcal{O}_{K,f})^{\times}$. Therefore, $\mathrm{Gal}(\overline{K}/H_f)$ acts on $T_f E$, compatibly with

the $\mathrm{Gal}(\overline{K}/H_f)$-action on $T_f E_0$. As a result of the exact sequence

$$0 \longrightarrow C \longrightarrow E_0 \longrightarrow E \longrightarrow 0\,,$$

$\mathrm{Gal}(\overline{K}/H_f)$ acts on C. The short exact sequence

$$0 \longrightarrow T_f E_0 \longrightarrow T_f E \longrightarrow C \longrightarrow 0$$

from Lemma 10.2.2 illustrates that C is $\mathrm{Gal}(\overline{K}/H_f)$-stable. Consequently, we see from the previous exact sequence

$$0 \longrightarrow C \longrightarrow E_0 \longrightarrow E \longrightarrow 0$$

that E is also $\mathrm{Gal}(\overline{K}/H_f)$-stable. The result follows. □

Our strategy will be to find ring class fields H_f and elliptic curves E_0 over $F := H_f$ with

$$L(E_0/F, 1) \neq 0.$$

These will be examples of rank-0 elliptic curves, to which Gross' Conjecture applies. Moreover, this will show the existence of rank-0 elliptic curves E with nonmaximal endomorphism ring, to which only the more general Burns–Flach Conjecture applies.

By Theorem 10.2.1, we may as well search for E_0 with complex multiplication by $\mathcal{O}_K$. We will in fact use curves E_0 which are defined over K.

Write, as before, φ for a Grössencharacter of K, which when pre-composed

with the norm, gives the associated Grössencharacter ψ of E_0 over H_f. Then, as explained in [8], we have

$$L(\psi, s) = \prod_{\chi \in \widehat{\mathrm{Gal}(H_f/K)}} L(\varphi\chi, s).$$

Since, by a result of Deuring for elliptic curves E_0 with $\mathrm{End}(E_0) = \mathcal{O}_K$ (see [21], II, Theorem 10.5(a)), we have

$$L(E_0/F, s) = L(\psi, s)L(\overline{\psi}, s),$$

then we must verify exactly that

$$L(\varphi\chi, 1) \neq 0 \quad \forall \chi \in \widehat{\mathrm{Gal}(H_f/K)}.$$

Let us examine the characters φ and χ more closely. We know, by the property of the associated Grössencharacter, that for $x \equiv 1 \mod \mathfrak{c}_0$, where $\mathfrak{c}_0$ is the conductor of E_0/K,

$$\varphi((x)) = x.$$

Since $\mathcal{O}_K$ by assumption is a principal ideal domain, then φ is essentially the identity function on $K^\times$. Now χ may be considered a map

$$G_f \simeq \mathrm{Gal}(H_f/K) \to \mathbb{C}^\times$$

Lemma 10.2.3. *G_f is a group of order*

$$\frac{2\Phi(f)}{\phi(f)w},$$

where $w = |\mathcal{O}_K^\times|$, ϕ is Euler's ϕ-function, and Φ is its obvious analog defined on ideals of $\mathcal{O}_K$.

(A more precise description of this group will be given for examples we find.)

Proof. First,

$$G_f = \frac{I_f}{Z_f P_f} \simeq \frac{(\mathcal{O}_K/f)^\times}{(\mathbb{Z}/f)^\times \mathrm{im}(\mathcal{O}_K^\times)}.$$

Consider the archimedean absolute value. We observe that $1 + f \cdot \mathcal{O}_K$ intersects the unit circle at only 1 point if $f > 2$, which is true here by assumption. Therefore, the group homomorphism $\mathcal{O}_K^\times \to (\mathcal{O}_K/f)^\times$ is an injection, and $|\mathrm{im}(\mathcal{O}_K^\times)| = |\mathcal{O}_K^\times| = w$. Since there are two roots of unity in $\mathbb{Z}^\times$, the image of $(\mathbb{Z}/f)^\times$ in $\frac{(\mathcal{O}_K/f)^\times}{\mathrm{im}(\mathcal{O}_K^\times)}$ has order $\frac{\phi(f)}{2}$. Since

$$\left| \frac{(\mathcal{O}_K/f)^\times}{\mathrm{im}(\mathcal{O}_K^\times)} \right| = \frac{\Phi(f)}{w},$$

the order of

$$\frac{(\mathcal{O}_K/f)^\times}{(\mathbb{Z}/f)^\times \mathrm{im}(\mathcal{O}_K^\times)}$$

is

$$\frac{2\Phi(f)}{\phi(f)w},$$

as desired. □

10.3 A first attempt.

Here we examine a first and mostly unsuccessful attempt to find examples. We also explain why many of the curves of the class searched, can be ruled out by theory alone.

Use $K = \mathbb{Q}(i)$, which has class number 1. If $f \equiv 1 \mod 4$, then f is split in K, and $|G_f| = \frac{2(f-1)^2}{4(f-1)} = \frac{f-1}{2}$. If $f \equiv 3 \mod 4$, then f is inert in K, and $|G_f| = \frac{2(f^2-1)}{4(f-1)} = \frac{f+1}{2}$.

Consider the Gauss curve $y^2 = x^3 - x$, which we denote E_0. It has abelian torsion, so that the above considerations for ψ apply. If we knew that $L(\varphi\chi, 1) \neq 0$ for all $\chi \in \widehat{G_f}$, then we would be guaranteed the existence of an elliptic curve E, defined over H_f, with complex multiplication by exactly $\mathbb{Z} + f \cdot \mathcal{O}_K$ and $\mathrm{rank}_{\mathbb{Z}} E(H_f) = 0$.

As a preliminary search, a necessary (though insufficient) condition was checked. The L-function satisfies the functional equation

$$\Lambda(\varphi\chi, s) = T(\varphi\chi)\Lambda(\overline{\varphi\chi}, 2 - s),$$

where

$$\Lambda(\varphi\chi, s) = (D\mathbf{N}(\varphi\chi))^{\frac{s}{2}}(2\pi)^{-s}\Gamma(s)L(\varphi\chi, s),$$

where $\mathbf{N}(\varphi\chi) \in \mathbb{N}$ is the norm of the conductor $c(\varphi\chi)$ (an ideal of $\mathcal{O}_K$) and D is the discriminant of K. And $T(\varphi\chi)$ is related to the root number $W(\varphi\chi)$ by

$$T(\varphi\chi) = -i\frac{W(\varphi\chi)}{\sqrt{\mathbf{N}(\varphi\chi)}}.$$

Since E_0 is defined over $\mathbb{Q}$, then φ is anticyclotomic, i.e., $\varphi(\overline{\mathfrak{n}}) = \overline{\varphi(\mathfrak{n})}$. The same is true of χ. On the ideals of $\mathbb{Z}$, χ is trivial (since all ideals of $\mathbb{Z}$ represent the trivial class in the ring class group). The Grössencharacter φ satisfies

$$\varphi((a)) = a \text{ for } a \equiv 1 \mod (1+i)^3,$$

so that for $a \in \mathbb{Z}$, $\varphi((a)) = a$ for $a \equiv 1 \mod 4$ and $\varphi((a)) = -a$ for $a \equiv 3 \mod 4$. This means that the value of φ is real on the ideals of $\mathbb{Z}$. Thus $L(\varphi\chi, 1) = L(\overline{\varphi\chi}, 1)$, which means that any root number $W(\varphi\chi)$ being unequal to 1 will force the L-value to be 0.

For each prime f between 3 and 250, the root number $W(\varphi\chi)$ was checked numerically for all characters χ of G_f. $W(\varphi\chi)$ was found to be -1 for at least one χ for each $f \neq 3$. This can in fact be proven for all $f > 3$:

Proposition 10.3.1. *Let f be any prime > 3. Then there exists $\chi \in \widehat{G_f}$ such that $W(\varphi\chi) \neq 1$.*

Proof. We shall restrict our attention to nontrivial χ. We have as in Miyake ([16], 3.3.11), the formula for the root number of $\varphi\chi$:

$$W(\varphi\chi) = W(\varphi)W(\chi)\frac{\varphi(c_\chi)}{|\varphi(c_\chi)|}\chi(c_\varphi),$$

where c_φ and c_χ are the respective conductors of φ and χ. Let us examine the factors $W(\varphi)$, $W(\chi)$, $\frac{\varphi(c_\chi)}{|\varphi(c_\chi)|}$, and $\chi(c_\varphi)$. We shall determine the first two, and show that the fourth can be chosen, depending on the third, making the whole product -1.

We know that $W(\varphi) = 1$ since the Gauss curve is a rank-0 elliptic curve.

Second, let us examine $W(\chi)$. The character χ is a character of the Galois group of the extension $F = H_f/K$. Consider the representation

$$\mathrm{Res}_K^{\mathbb{Q}}\mathrm{Ind}_K^{\mathbb{Q}}\chi$$

formed by induction and then restriction. It is

$$x \mapsto \begin{pmatrix} \chi(x) & 0 \\ 0 & \chi(\overline{x}) \end{pmatrix}.$$

Now since $x\overline{x} \in \mathbb{Z}$ for $x \in \mathcal{O}_K$, and since the image of $\mathbb{Z}$ in G_f is trivial, then

$$\chi(\overline{x})\chi(x) = \chi(\overline{x}x) = 1,$$

so that χ is anti-cyclotomic (i.e., $\chi(\overline{x}) = \overline{\chi(x)}$). It follows that the character associated to the representation

$$\mathrm{Res}_K^{\mathbb{Q}}\mathrm{Ind}_K^{\mathbb{Q}}\chi$$

is

$$\begin{aligned}\mathrm{tr}(\mathrm{Res}_K^{\mathbb{Q}}\mathrm{Ind}_K^{\mathbb{Q}}\chi) =& \mathrm{tr}\begin{pmatrix}\chi(x) & 0\\ 0 & \chi(\overline{x})\end{pmatrix}\\ =& \mathrm{tr}\begin{pmatrix}\chi(x) & 0\\ 0 & \overline{\chi(x)}\end{pmatrix}\\ =& \chi(x)+\overline{\chi(x)}\\ \in& \mathbb{R}.\end{aligned}$$

One also checks that $\mathrm{tr}(\mathrm{Ind}_K^{\mathbb{Q}}\chi)(x) \in \mathbb{R}$ for $x \in G_{\mathbb{Q}}\backslash G_K$. The work of Fröhlich and Queyrut ([7]) tells us that for a real character which comes from a real representation, the root number is 1. Though the representation $\mathrm{Ind}_K^{\mathbb{Q}}\chi$ is not itself real, it is conjugate to a real representation. Thus its root number is also 1. Since the L-function is unchanged by induction or restriction of characters, we see that $W(\chi)$ must be 1.

Next, we examine the factor $\frac{\varphi(c_\chi)}{|\varphi(c_\chi)|}$. Since the conductor of χ is f if χ is nontrivial, then $\varphi(c_\chi) \in \mathbb{Z}$, and the factor $\frac{\varphi(c_\chi)}{|\varphi(c_\chi)|}$ is ± 1 .

The class of $c_\varphi = (1+i)^3$ is of order exactly 2 in G_f since its square is the class of the ideal (8), which is trivial, while the class of $(1+i)^3$ is itself nontrivial. Therefore, there exists a character χ of G_f which has value -1 at c_φ. Since $f > 3$, then $G_f \neq < 1+i >$, so that there is a nontrivial character of G_f which factors through $G_f/ < 1+i >$.

Whether $\frac{\varphi(c_\chi)}{|\varphi(c_\chi)|}$ is 1 or -1, we find a $\chi \in \widehat{G_f}$ for which the product

$$\frac{\varphi(c_\chi)}{|\varphi(c_\chi)|}\chi(c_\varphi),$$

and thus the product

$$\frac{\varphi(c_\chi)}{|\varphi(c_\chi)|}\chi(c_\varphi)W(\varphi)W(\chi),$$

is -1. Thus, for $f > 3$, there exists $\chi \in \widehat{G_f}$ such that $W(\varphi\chi) = -1$. □

The curve E_0/H_3 turned out to have non-zero L-value, and so E_3 was the lone example obtained from this search.

10.4 A second search.

A different class of curves was searched, yielding 15 elliptic curves over ring class fields $F := H_f$ with

$$L(E_0/F, 1) \neq 0.$$

These are examples of rank-0 elliptic curves, to which Gross' Conjecture applies. Moreover, this shows the existence of 15 rank-0 elliptic curves E with nonmaximal endomorphism ring, to which only the more general Burns–Flach Conjecture applies.

Here the Gauss curve E_0 is replaced by a quartic twist thereof. Let $E_{4,0}$ be given by the equation

$$y^2 = x^3 - (1 + 4i)x.$$

This curve is isomorphic to the Gauss curve over $F(\sqrt[4]{1+4i})$, using the co-ordinate change $(x, y) = (\beta^2 x', \beta^3 y')$, where $\beta = \sqrt[4]{1+4i}$. Since the Gauss curve $y^2 = x^3 - x$ has abelian torsion, then $E_{4,0}$ does also. If we knew that $L(\varphi'\chi, 1) \neq 0$ for all $\chi \in \widehat{G_f}$, where φ' is the Grössencharacter of $E_{4,f}$, then we would be guaranteed the existence of an elliptic curve $E_{4,f}$, defined over H_f, with complex multiplication by exactly $\mathbb{Z} + f \cdot \mathcal{O}_K$.

The Grössencharacter of $E_{4,0}$ is $\varphi' = \varphi\epsilon$, where ϵ is the character associated to the quartic twist $E_0 \mapsto E_{4,0}$. We have

$$\varphi'((\alpha)) = \overline{\left(\frac{1+4i}{\alpha}\right)}_4 \alpha, \quad \alpha \equiv 1 \mod (1+i)^3.$$

(See [12], Chapter 19, Theorem 5.) The conductor of ϵ is $1+4i$, which is prime to the conductor of φ, and to the conductor of χ if $f \neq 17$. In this case, the root number of $\xi = \varphi'\chi$ can be calculated using the formula

$$W(\varphi'\chi) = \frac{\varphi'(c_\chi)}{|\varphi'(c_\chi)|}\epsilon(c_{\varphi'})W(\varphi')W(\chi),$$

where the root number of $\varphi' = \varphi\epsilon$ is calculated using the formula

$$W(\varphi\epsilon) = \frac{\varphi(c_\epsilon)}{|\varphi(c_\epsilon)|}\epsilon(c_\varphi)W(\varphi)W(\epsilon).$$

The values of $L(\varphi'\chi, 1)$ were checked for all ring class characters χ, for all primes f between 3 and 61, excluding 17. The values $L(\varphi'\chi, 1)$ were found all to be non-zero, except when $f = 5$ and χ was the non-trivial character of the two-element group G_5. In this case, $L(\varphi'\chi, 1)$ appeared to be zero, though

this could not be deduced from the numerical calculations. In any case, it was determined that $E_{4,0}/H_f$ had non-zero L-value for the following 15 values of f:

$$3, 7, 11, 13, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61.$$

Thus there exists an example $E_{4,f}$ for each of these values of f.

10.5 The code.

Here we give the code used in PARI to find the examples. With some modification, many other similar classes of elliptic curves could be searched. Explanation is given interspersed with the code. Comments generally follow the line or lines to which they refer.

```
bnf=bnfinit(y^2+1);
```

Initializes the number field 'bnf'= $\mathbb{Q}(i)$.

```
bnr2=bnrinit(bnf,[1,4]~,1);
```

Initializes 'bnr2', which is $\mathbb{Q}(i)$ with the structure of the ray class group modulo $1 + 4i$.

```
initialize(f)=
```

Initializes the data involving f ='eff'.

```
{
eff=f;
```

Sets f, called 'eff'.

```
bnr=bnrinit(bnf,eff,1);
```

Initializes 'bnr', which is $\mathbb{Q}(i)$ with the structure of the ray class group modulo f.

```
bnr3=bnrinit(bnf,eff*[1,4]~,1);
```

Initializes 'bnr3', which is $\mathbb{Q}(i)$ with the structure of the ray class group modulo $f(1+4i)$.

```
prim=znprimroot(eff);
for(index=1,eff,
    if(prim==Mod(index,eff),
        prim=index
        )
    );
prim=bnrisprincipal(bnr,prim)[1];
```

Sets a generator 'prim' of $(\mathbb{Z}/f\mathbb{Z})^*$.

```
chi=vector(length(bnr.clgp[2]));
```

Sets χ to be the trivial character.

}

```
h1generator(bnf,ideal)=
```

Extracts a generator of 'ideal' in 'bnr', assuming the class number of 'bnr' is 1.

{

```
dec=factor(idealnorm(bnf,ideal));
```

```
gen=1;
for(index=1,matsize(dec)[1],
    fac1=[dec[index,1],0]~;
    fac2=[1,0]~;
    for(a=1,sqrt(dec[index,1]),
        for(b=1,a,
            if(a^2+b^2==dec[index,1],
                fac1=[a,b]~;
                fac2=[a,-b]~;
                )
            )
        );
    gen=nfeltmul(bnf,gen,
        nfeltpow(bnf,fac1,idealval(bnf,
            ideal,idealfactor(bnf,fac1)[1,1]))
        );
    if(fac1!=[1,1]~& fac2!=[1,0]~,
        gen=nfeltmul(bnf,gen,
            nfeltpow(bnf,fac2,idealval(bnf,
                ideal,idealfactor(bnf,fac2)[1,1]))
            );
        );
    );
gen
```

```
}
```

```
phieval(ideal)=
```

Evaluates the character φ =‘phi’ (factor of the Grössencharacter) at ‘ideal’, given by a generator, expressed as a column vector on the integral basis.

```
{
for(o=0,3,
    if(nfeltmod(bnf,
        nfeltmul(bnf, ideal,nfeltpow(bnf,[0,1]~,o))-[1,0]~,
            nfeltpow(bnf,[1,1]~,3))
        ==[0,0]~,
        ideal=nfeltmul(bnf, ideal,nfeltpow(bnf,[0,1]~,o));
        );
    );
if(nfeltmod(bnf,ideal,[1,1]~)==[0,0]~,
    ideal=[0,0]~;
    );
ideal[1]+ideal[2]*I
}
```

```
epsiloneval(ideal)=
```

Evaluates the character ϵ =‘epsilon’, associated to the quartic twist of E by $1+4i$, at ‘ideal’. We know the character is either [1] or [3] as a character of the cyclic 4-group ‘bnr2.clgp’, and, twisting three times if necessary, we may

assume without loss of generality that it is [1].

```
{
if(idealnorm(bnr2,idealcoprime(bnr2,[1,4]~,ideal))!=1,
    0,
    exp(2*Pi*I*bnrisprincipal(bnr2,ideal)[1][1]
        *1/bnr2.clgp[2][1])
    )
}
```

```
rnepsilon=bnrrootnumber(bnr2,[1]);
```

Calculates the (fixed) root number of ϵ =‘epsilon’.

```
phiprimeeval(ideal)=
```

Evaluates φ' =‘phiprime’= $\varphi\epsilon$ at ‘ideal’.

```
{
phieval(ideal)*epsiloneval(ideal)
}
```

```
cophiprime=nfeltmul(bnf,[1,4]~,nfeltpow(bnf,[1,1]~,3));
```

Calculates the conductor of φ' =‘phiprime’= $\varphi\epsilon$.

```
rnphiprime=(1+4*I)/sqrt(17)
    *epsiloneval(nfeltpow(bnf,[1,1]~,3))
    *1*rnepsilon;
```

Calculates the (fixed) root number of ‘phiprime’=‘phi’·‘epsilon’. (At 1+4i, the conductor of ‘epsilon’, ‘phi’ takes the value 1+4i.)

```
chieval(ideal)=
```

Evaluates the character χ =‘chi’ of the ray class group modulo f, at ideal.

```
{
if(idealnorm(bnr,bnrconductorofchar(bnr,chi))==1,
    1,
    if(idealnorm(bnr,idealcoprime(bnr,
        bnrconductorofchar(bnr,chi),ideal))!=1,
        0,
        exp(2*Pi*I*(
            sum(index=1,length(bnr.clgp[2]),
                bnrisprincipal(bnr,ideal)[1][index]*chi[index]
                /bnr.clgp[2][index]
                )
            ))
        )
    )
}
```

```
xieval(ideal)=
```

Evaluates the character ξ =‘xi’= $\varphi'\chi = \varphi\epsilon\chi$ at the ideal generated by ‘ideal’.

```
{
```

```
phiprimeeval(ideal)*chieval(ideal)
}
```

```
rnxi()=
```

This calculates the root number (varying with χ) of ξ ='xi'= $\phi'\chi = \phi\epsilon\chi$.

```
{
cochi=h1generator(bnr,bnrconductorofchar(bnr,chi));
fact=phiprimeeval(cochi);
if(fact==0,0,
    fact/sqrt(norm(fact))
    *chieval(cophiprime)
    *rnphiprime
    *bnrrootnumber(bnr,chi)
    )
}
```

```
isring(upsilon)=
```

Tests whether 'upsilon', a character of the ray class group modulo f ('bnr.clgp'), factors through the ring class group modulo f, and thus is a valid χ to consider. Uses the constant 'prim', which is a generator of $(\mathbb{Z}/f\mathbb{Z})^*$, expressed as an element of 'bnr.clgp'.

```
{
if(length(bnr.clgp[2])==1,
    upsilon[1]*prim[1]%(bnr.clgp[2][1])==0,
```

```
    (upsilon[1]*prim[1]*bnr.clgp[2][2]
        +upsilon[2]*prim[2]*bnr.clgp[2][1])
        %(bnr.clgp[2][1]*bnr.clgp[2][2])==0;
```

Tests whether 'upsilon' factors through the quotient by $(\mathbb{Z}/f\mathbb{Z})^*$,i.e., whether it gives character on the ring class group as well as the ray class group.

```
    )
}
```

```
getapbp(p)=
```

Sets a_p ='ap' and b_p ='bp' for the modular form.

```
{
if(idealprimedec(bnr,p)[1][4]==2,
    ap=0;
    bp=-xieval([p,0]~);
    );
if(idealprimedec(bnr,p)[1][3]==2,
    for(i=1,sqrt(p),
        for(j=1,i,
            if(i^2+j^2==p,
                ap=xieval([i,j]~);
                bp=0
                );
            );
        );
```

```
    );
if(length(idealprimedec(bnr,p))==2,
    for(i=1,sqrt(p),
        for(j=1,i,
            if(i^2+j^2==p,
                v1=xieval([i,j]~);
                v2=xieval([i,-j]~);
                ap=(v1+v2);
                bp=(v1*v2)
                );
            );
        );
    );
}
```

`add(n,P,y,z)=`

This function calls itself, and is the heart of the Gross–Buhler recursion.

```
{
Sum=Sum+y*expq^n/n;
forprime(p=2,min(P,bound/n),
    getapbp(p);
    x=y*ap;
    if(p==P,x=x-z*bp);
    add(p*n,p,x,y);
```

```
    )
}

GB(bound)=
{
f1=expq;
a1=1;
Sum=a1*f1;
forprime(p=2,bound,
    getapbp(p);
    add(p,p,ap,1);
    );
Sum
}
```

The preceding two functions comprise the algorithm of Gross and Buhler, as described in [1]. This algorithm can be described as "computationally minimal" in the sense that, using the known relations between the various a_n and b_n (surely the most efficient way to calculate the terms), the minimum number of them necessary for the rest to be calculated, are kept in memory at once.

```
Lval(xx,bound)=
```

This function approximates the L-value $L(\xi, 1)$, using the formula

$$L(\xi,1) = \sum_{n=1}^{\infty} \frac{a_n}{n} e^{-\frac{2\pi n x}{\sqrt{N}}} + T(\xi) \sum_{n=1}^{\infty} \frac{\overline{a}_n}{n} n e^{-\frac{2\pi n}{x\sqrt{N}}},$$

where $N = |D|\mathbf{N}(\xi)$, D being the discriminant of K. The computaion uses the cutoff point $x =$'xx' ≈ 1, and 'bound' terms of each series. Varying x does not change the infinite sum, of course, and this was used as a way to check the correctness of the calculation.

```
{
expq=exp(-2*Pi/sqrt(4*2^3*17*idealnorm(bnf,
    bnrconductorofchar(bnr,chi)))*xx);
term1=GB(bound);
expq=exp(-2*Pi/sqrt(4*2^3*17*idealnorm(bnf,
    bnrconductorofchar(bnr,chi)))*(1/xx));
term2=conj(GB(bound));
term1+rnxi*term2
}
```

`multichi1()=`

Checks the L-value for fixed f and all possible χ, for cyclic ray class group modulo f. Note that in all cases the ring class group modulo f is cyclic, but it is more convenient here to examine the characters of the ray class group, finding the L-value only for those which factor through the ring class group. (In some cases, the ray class group is not cyclic.)

```
{
indicator=1;
for(a=0,bnr.clgp[1]-1,
    if((isring([a])==1)&(indicator==1),
        chi=[a];
        if(truncate(norm(1000*Lval(1,500)))==0,
            indicator=0
            );
        );
    );
if(indicator==1,
    print("GOOD f=" eff ),
    print("BAD f=" eff)
    )
```

Prints "GOOD" if E_f is an elliptic curve of the desired type, and "BAD" otherwise.

}

`multichi2()=`

Checks the L-value for fixed f and all possible χ, for ray class group modulo f with 2 cyclic components. Again, only those characters which factor through the ring class group are considered.

```
{
for(a=0,bnr.clgp[2][1]-1,
```

```
    for(b=0,bnr.clgp[2][2]-1,
        if((isring([a,b])==1)&(indicator==1),
            chi=[a,b];
            if(truncate(norm(1000*Lval(1,500)))==0,
                indicator=0
                );
            );
        );
    );
if(indicator==1,
    print("GOOD f=" eff ),
    print("BAD f=" eff)
    )
```

Prints "GOOD" if E_f is an elliptic curve of the desired type, and "BAD" otherwise.

}

`multieff(lower,upper)=`

Checks the L-value for all (prime) f from 'lower' to 'upper'. Note that for all $f \equiv 3 \mod 4$, f is inert, which implies that the ray class group modulo f is cyclic. For all $f > 5, \equiv 1 \mod 4$, f is non-inert and the ray class group has two cyclic components. For f=5, the ray class group is cyclic. We do not wish to examine $f = 2$ or 17 because they are not prime to the conductors of ϕ and ϵ, respectively. Thus ranges ['lower','upper'] are chosen, when this code

is used, which exclude 2 and 17.

```
{
forprime(index=lower,upper,
    initialize(index);
    if(length(bnr.clgp[2])==1,
        multichi1,
        multichi2
        );
    );
}
```

Bibliography

[1] Buhler, J. and Gross, B., "Arithmetic on elliptic curves with complex multiplication. II." *Invent. Math.* **79** (1985), 223—251.

[2] Burns, D. and Flach, M., "Motivic L-functions and Galois module structures." *Math. Ann.* **305** (1996), 65—102.

[3] Burns, D. and Flach, M., "On Galois structure invariants associated to Tate motives." *American Journal of Mathematics* **120** (1998), 1343—1397.

[4] Burns, D. and Flach, M., "Tamagawa numbers for motives with (non-commutative) coefficients." *Documenta Math.* **6** (2001), 501—570.

[5] Coates, J. and Wiles, A., "On the Conjecture of Birch and Swinnerton-Dyer." *Invent. Math.* **39** (1977), 223—251.

[6] Fontaine, J.-M. and Perrin-Riou, B., "Autour des conjectures de Bloch et Kato: cohomologie galoisienne et valeurs de fonctions L." (French) (Seattle, WA, 1991), 599—706, Proc. Sympos. Pure Math., **55**, Part 1, Amer. Math. Soc., Providence, RI, 1994.

[7] Fröhlich A. and Queyrut, J., "On the functional equation of the Artin L-function for characters of real representations." *Invent. Math.* **20** (1973), 125—138.

[8] Goldstein, C. and Schappacher, N., "Séries d'Eisenstein et fonctions L de courbes elliptiques multiplication complexe." (French) J. Reine Angew. Math. **327** (1981), 184—218.

[9] Gross, B., "On the conjecture of Birch and Swinnerton-Dyer for elliptic curves with complex multiplication." (Cambridge, Mass., 1981), 219—236, Progr. Math., **26**, Birkhäuser, Boston, Mass., 1982.

[10] Gross, B., *Arithmetic on elliptic curves with complex multiplication.* Springer Lecture Notes Math. 776.

[11] Grothendieck, A., "Modèles de Néron et monodromie." Exposé IX, SGA 7I, Springer–Verlag, 1972.

[12] Ireland, K. and Rosen, M,, *A Classical Approach to Modern Number Theory.* Springer GTM 84, 1982.

[13] Kato, K., *Lectures on the approach to Iwasawa theory for Hasse-Weil L-functions via* B_{dR}*. I.* (Trento, 1991), 50—163, Lecture Notes in Math., 1553, Springer, Berlin, 1993.

[14] Knudsen, F. and Mumford, D., "The projectivity of the moduli space of stable curves I: Preliminaries on 'det' and 'Div'." Math. Scand **39** (1976) 19—55.

[15] Matsumura, H., *Commutative Algebra.* Benjamin Cummings, 1980.

[16] Miyake, T., *Modular Forms.* Springer–Verlag, 1989.

[17] Rubin, K., "The 'main conjectures' of Iwasawa theory for quadratic imaginary fields." Invent. Math. **103** (1991), no. 1, 25—68.

[18] Rubin, K., *Euler Systems.* Annals of Mathematics Studies, 147. Hermann Weyl Lectures. The Institute for Advanced Study. Princeton University Press, Princeton, NJ, 2000.

[19] de Shalit, E., *Iwasawa theory of elliptic curves with complex multiplication.* Orlando: Academic Press (1987).

[20] Silverman, J. H., *The Arithmetic of Elliptic Curves.* New York: Springer-Verlag (1986).

[21] Silverman, J. H., *Advanced Topics in the Arithmetic of Elliptic Curves.* New York: Springer-Verlag (1994).