Annals of Mathematics, **146** (1997), 111–147

A rigid analytic Gross-Zagier formula and arithmetic applications

By MASSIMO BERTOLINI[1] and HENRI DARMON[2]

(With an Appendix by B. Edixhoven)

Contents

Introduction

Let f be a newform of weight 2 and squarefree level N. Its Fourier coefficients generate a ring $\mathcal{O}_f$ whose fraction field K_f has finite degree over $\mathbb{Q}$. Fix an imaginary quadratic field K of discriminant prime to N, corresponding to a Dirichlet character ε. The L-series $L(f/K,s) = L(f,s)L(f\otimes\varepsilon,s)$ of f over K has an analytic continuation to the whole complex plane and a functional equation relating $L(f/K,s)$ to $L(f/K,2-s)$. Assume that the sign of this functional equation is 1, so that $L(f/K,s)$ vanishes to even order at $s=1$. This is equivalent to saying that the number of prime factors of N which are inert in K is odd. Fix any such prime, say p.

The field K determines a factorization $N = N^+N^-$ of N by taking N^+, resp. N^- to be the product of all the prime factors of N which are split, resp.

[1]Partially supported by grants from MURST, CNR, and EC.

[2]Partially supported by CICMA and by grants from CNR, FCAR, and NSERC.

inert in K. Given a ring-class field extension H of K of conductor c prime to N, write H_n for the ring-class field of conductor cp^n. It is an extension of H of degree $e_n := 2u^{-1}(p+1)p^{n-1}$, where u is the order of the group of roots of unity in the order $\mathcal{O}$ of K of conductor c. Recall that p splits in H/K, and the primes of H above p are totally ramified in H_n. For $n \geq 1$, a construction explained in [BD1, §2.5] allows us to define a compatible collection of Heegner points P_n over H_n on a certain Shimura curve X. In the notations of [BD1, §1.3], X is the curve $X_{N^+p,N^-/p}$ over $\mathbb{Q}$ attached to an Eichler order of level N^+p in the indefinite quaternion algebra of discriminant N^-/p.

Let J be the jacobian of X, $\mathcal{J}_n$ the Néron model of J over H_n, and Φ_n the group of connected components at p of $\mathcal{J}_n$. More precisely,

$$\Phi_n := \oplus_{\mathfrak{p}|p}\Phi_{\mathfrak{p}},$$

where $\Phi_{\mathfrak{p}}$ is the group of connected components of the fiber at $\mathfrak{p}$ of $\mathcal{J}_n$ and the sum is extended over all the primes $\mathfrak{p}$ of H_n above p.

Define a Heegner divisor $\alpha_n := (P_n) - (w_N P_n)$, where w_N is the Atkin-Lehner involution denoted $w_{N^+p,N^-/p}$ in [BD1, §1.8]. We view α_n as an element of $\mathcal{J}_n$, and let $\bar{\alpha}_n$ be its natural image in Φ_n.

We have found that the position of $\bar{\alpha}_n$ in Φ_n is encoded in the special values of the L-functions attached to cusp forms of weight 2 on X twisted by characters χ of $\Delta := \mathrm{Gal}(H/K)$.

More precisely, observe that the Galois group $\mathrm{Gal}(H_n/K)$ acts on $J(H_n)$ and on $\mathcal{J}_n$. Since the primes above p are totally ramified in H_n/H, the induced action on Φ_n factors through Δ. Define $e_\chi := \sum_{g\in\Delta}\chi^{-1}(g)g \in \mathbb{Z}[\chi][\Delta]$, and let $\bar{\alpha}_n^\chi := e_\chi\bar{\alpha}_n$.

The ring $\mathbb{T}$ generated over $\mathbb{Z}$ by the Hecke correspondences on X acts in a compatible way on $J(H_n)$, $\mathcal{J}_n$ and Φ_n. Write $\phi_f : \mathbb{T} \to \mathcal{O}_f$ for the homomorphism associated to f by the Jacquet-Langlands correspondence (cf. [BD1, §1.6], and let $\pi_f \in \mathbb{T}\otimes K_f$ be the idempotent corresponding to ϕ_f. Fix $n_f \in \mathcal{O}_f$ so that $\eta_f := n_f\pi_f$ belongs to $\mathbb{T}\otimes\mathcal{O}_f$, and define $\bar{\alpha}_n^{f,\chi} := \eta_f\bar{\alpha}_n^\chi$.

The group Φ_n is equipped with a canonical monodromy pairing

$$[\ ,\ ]_n\colon\ \Phi_n \times \Phi_n \to \mathbb{Q}/\mathbb{Z},$$

which we extend to a hermitian pairing on $\Phi_n \otimes \mathcal{O}_f[\chi]$ with values in $K_f[\chi]/\mathcal{O}_f[\chi]$, denoted in the same way by abuse of notation. Our main result is:

THEOREM A. *Suppose that χ is a primitive character of Δ. Then*

$$[\bar{\alpha}_n^\chi,\bar{\alpha}_n^{f,\chi}]_n = \frac{1}{e_n}\frac{L(f/K,\chi,1)}{(f,f)}\sqrt{d}\cdot u^2\cdot n_f \qquad (\mathrm{mod}\ \mathcal{O}_f[\chi]),$$

where (f,f) is the Petersson scalar product of f with itself, and d denotes the discriminant of $\mathcal{O}$.

The proof is based on Grothendieck's description of Φ_n [Groth], on the work of Edixhoven on the specialization map from $\mathcal{J}_n$ to Φ_n [Edix], and on a slight generalization of Gross' formula for special values of L-series [Gr1] (which we assume in this paper and which will be contained in [Dag]). Theorem A can be viewed as a p-adic analytic analogue of the Gross-Zagier formula, and was suggested by the conjectures of Mazur-Tate-Teitelbaum type formulated in [BD1, Ch. 5]. It is considerably simpler to prove than the Gross-Zagier formula, as it involves neither derivatives of L-series nor global heights of Heegner points.

The above formula has a number of arithmetic applications. Let A_f be the abelian variety quotient of J associated to ϕ_f by the Eichler-Shimura construction. Following the methods of Kolyvagin, we can use the Heegner points α_n to construct certain cohomology classes in $H^1(H,(A_f)_{e_n})$, whose local behaviour is related via Theorem A to $L(A_f/K,\chi,1)=\prod_\sigma L(f^\sigma/K,\chi,1)$, where σ ranges over the set of embeddings of K_f in $\bar{\mathbb{Q}}$. This can be used to study the structure of the χ-isotypical component $A_f(H)^\chi := e_\chi A_f(H) \subset A_f(H)\otimes\mathbb{Z}[\chi]$ of the Mordell-Weil group $A_f(H)$. In particular, we show:

THEOREM B. *If $L(A_f/K,\chi,1)$ is nonzero, then $A_f(H)^\chi$ is finite.*

When $\chi=\bar{\chi}$, this result also follows from the work of Gross-Zagier [GZ] and Kolyvagin-Logachev [KL], but if χ is nonquadratic the previous techniques cannot be used to study these questions.

It is worth stating the following two corollaries of Theorem B.

COROLLARY C. *Let $E/\mathbb{Q}$ be a semistable elliptic curve, and assume that $L(E/\mathbb{Q},1)$ is nonzero. Then $E(\mathbb{Q})$ is finite.*

Proof. By the fundamental work of Wiles and Taylor-Wiles (cf. [W] and [TW]), E is modular. A theorem of Waldspurger [Wald] ensures the existence of an imaginary quadratic field K such that $L(E/K,1)$ is nonzero. Then Theorem B implies that $E(K)$, and hence $E(\mathbb{Q})$, are finite.

The previously known proof invokes an analytic result of Bump-Friedberg-Hoffstein [BFH] and Murty-Murty [MM], according to which there exists an auxiliary imaginary quadratic field K such that all the primes dividing N are split in K and the first derivative $L'(E/K,1)$ is nonzero. In this setting, there is a Heegner point in $E(K)$, arising from the modular curve parametrization $X_0(N)\to E$. This point has infinite order by the formula of Gross-Zagier [GZ]. Then Kolyvagin's theorem [Ko] implies that $E(K)$ has rank one, and that $E(\mathbb{Q})$ is finite. This proof is more general than ours, since it applies to all modular elliptic curves, and also yields the finiteness of the Shafarevich-Tate group of E. Our proof depends crucially on the existence of a prime p of multiplicative reduction, and only establishes the finiteness of the p-primary part of the Shafarevich-Tate group.

Theorem B allows us to control the growth of Mordell-Weil groups over anticyclotomic $\mathbb{Z}_\ell$-extensions, addressing a conjecture of Mazur [Ma2]. Let f and K be as at the beginning of this section. Let $\ell_1, \ldots, \ell_k$ be primes not dividing N, and let K_∞ denote the compositum of all the ring-class field extensions of K of conductor of the form $\ell_1^{n_1} \ldots \ell_k^{n_k}$, where $n_1, \ldots, n_k$ are nonnegative integers. Thus, the Galois group of K_∞/K is isomorphic to the product of a finite group by $\mathbb{Z}_{\ell_1} \times \cdots \times \mathbb{Z}_{\ell_k}$.

COROLLARY D. *Assume that* $L(A_f/K,\chi,1) \neq 0$ *for almost all finite order characters of* $\mathrm{Gal}(K_\infty/K)$. *Then the Mordell-Weil group* $A_f(K_\infty)$ *is finitely generated.*

(See the details of the proof in §8.) Computations of root numbers show that $L(f/K, \chi, s)$ vanishes to even order at $s = 1$ for all χ as above, and it is expected that $L(f/K, \chi, 1)$ be nonzero for almost all χ. (For results in this direction, see [Ro1] and [Ro2].) We remark that a result similar to Corollary D for the cyclotomic $\mathbb{Z}_\ell$-extension of $\mathbb{Q}$ has been announced recently by K. Kato.

Theorems A and B provide a technique to study "analytic rank-zero situations" in terms of Heegner points of conductor divisible by powers of a prime p of multiplicative reduction for A_f and inert in K. What makes this possible, ultimately, is a "change of sign" phenomenon: If $L(f/K, s)$ vanishes to even order, and χ is an anticyclotomic character of conductor cp^n with c prime to N, then $L(f/K, \chi, s)$ vanishes to odd order, and there are Heegner points on A_f defined over the extension cut out by χ. The previous applications of the theory of Heegner points, such as the analytic formula of Gross-Zagier and the methods of Kolyvagin, occur in situations where $L(f/K, s)$ and $L(f/K, \chi, s)$ both vanish to odd order.

Acknowledgements. We are very grateful to Bas Edixhoven for writing an appendix to this paper, which provides a crucial step towards proving our results. We also thank the referee for useful remarks.

1. Gross' formula for special values of L-series

We keep the notations of the introduction. Let B be the definite quaternion algebra ramified at the primes dividing N^-. Let $R_1, \ldots, R_t$ denote representatives for the isomorphism classes of the oriented Eichler orders of level N^+ in B (see [Rob, §1.6] and [BD1, §1.1]). Define

$$\mathbb{M} := \mathbb{Z} \cdot R_1 \oplus \cdots \oplus \mathbb{Z} \cdot R_t$$

to be the free $\mathbb{Z}$-module of formal $\mathbb{Z}$-linear combinations of the R_i. (This is the module denoted by J_{N^+,N^-} in [BD1].) Let

$$\langle\ ,\ \rangle \colon \mathbb{M} \times \mathbb{M} \to \mathbb{Z}$$

be the pairing defined by the rule $\langle R_i, R_j\rangle = \delta_{ij}w_i$, where w_i is one half the order of $R_i^\times$.

Let $\mathcal{O}$ be a fixed oriented order of K of conductor c (see [BD1, §2.2]), with c prime to N. A Gross point of conductor c is an optimal embedding

$$\psi\colon\ \mathcal{O} \to R_i,$$

$i = 1, \dots, t$, preserving the orientations on $\mathcal{O}$ and R_i. Here, two R_i-valued embeddings are identified if they are conjugate under the natural action of $R_i^\times$. The set of the Gross points of conductor c is endowed with a natural free and transitive action of the group $\Delta = \mathrm{Pic}(\mathcal{O})$ (see [BD1, §2.3]).

Fix a Gross point ψ. For $g \in \Delta$, write ξ, resp. ξ^g for the natural image of ψ, resp. ψ^g in $\mathbb{M}$. Let ξ^χ be $\sum_{g\in\Delta}\chi^{-1}(g)\xi^g \in \mathbb{M}\otimes\mathbb{Z}[\chi]$ and let $\xi^{f,\chi}$ be the element $\eta_f\xi^\chi$ of $\mathbb{M}\otimes\mathcal{O}_f[\chi]$. With the notations of the introduction, we have:

THEOREM 1.1. *Suppose that χ is primitive. Then*

$$\langle\xi^\chi,\xi^{f,\chi}\rangle = \frac{L(f/K,\chi,1)}{(f,f)}\sqrt{d}\cdot(u/2)^2\cdot n_f.$$

The above formula is proved in [Gr1] only when N is a prime number and $c = 1$, so that χ is an unramified character. One can check that the methods of Gross extend directly to this more general setting; see the work in progress [Dag].

2. Bad reduction of Shimura curves

We review results on the bad reduction at p of X and $\mathcal{J}_n$, due to Deligne-Rapoport, Drinfeld, Grothendieck, and Raynaud. In [Dr], Drinfeld constructs a model $X_{\mathbb{Z}}$ of X over $\mathbb{Z}$, i.e., a projective scheme over $\mathbb{Z}$ whose generic fiber is equal to X. The definition of $X_{\mathbb{Z}}$ is via moduli: $X_{\mathbb{Z}}$ coarsely represents the moduli functor which associates to a scheme S the set of isomorphism classes of abelian schemes of dimension 2 over S, endowed with quaternionic multiplication and a suitable level N^+p-structure. (The definition of the functor is explained in [Dr] and [Rob].)

Consider the model $\mathcal{X} := X_{\mathbb{Z}}\otimes\mathbb{Z}_p$ of X over $\mathbb{Z}_p$. Let $\mathcal{X}_p$ denote the special fiber of $\mathcal{X}$. By the work of Deligne-Rapoport [DeRa] and Katz-Mazur [KaMa] (see also [Rob, Ch. 4], in particular the remark at the end of the introduction of §4), the following holds. Let X' be the Shimura curve denoted $X_{N^+,N^-/p}$ in [BD1, §1.3]. Denote by $\mathcal{X}'$ its Drinfeld model over $\mathbb{Z}_p$, and by $\mathcal{X}'_p$ the special fiber at p of $\mathcal{X}'$. The fiber $\mathcal{X}_p$ is the union of two copies of $\mathcal{X}'_p$, crossing transversally at the supersingular points of $\mathcal{X}'_p$. A point on $\mathcal{X}'_p$ is called supersingular if it corresponds to an abelian surface over $\bar{\mathbb{F}}_p$ together with its additional structure, having endomorphism ring equal to an Eichler order in a quaternion algebra. This order is necessarily an Eichler order of level N^+ in the definite quaternion algebra of discriminant N^-, by the work of Waterhouse [Wa]. By abuse of language, we call supersingular also the (ordinary) double points of $\mathcal{X}_p$. Let $s \in \mathcal{X}_p$ be any such point. It is defined either over $\mathbb{F}_p$ or over $\mathbb{F}_{p^2}$. Viewing s as a point on $\mathcal{X}$ over the ring $W(\bar{\mathbb{F}}_p)$ of Witt vectors of $\bar{\mathbb{F}}_p$, we see that its strict localization is of the form

$$W(\bar{\mathbb{F}}_p)[\![x,y]\!]/(xy-p^k),$$

where the "width of singularity" $k = k_s$ is ≥ 1. The model $\mathcal{X}$ is regular at s if and only if k_s is equal to 1.

We need also consider the behaviour under base-change of $\mathcal{X}$. Given a local field F of residue characteristic p, write R for its ring of integers. Let π be a uniformizer of R, and let e be the ramification index of R over $\mathbb{Z}_p$. Consider the base change $\mathcal{X}_R = \mathcal{X} \otimes R$ of $\mathcal{X}$ to R. The singularities of the special fiber $\mathcal{X}_\pi$ of $\mathcal{X}_R$ correspond bijectively to the ordinary double points of $\mathcal{X}_p$. Suppose that the strict localization of a double point of $\mathcal{X}_p$ is of the form $W(\bar{\mathbb{F}}_p)[\![x,y]\!]/(xy-p^k)$. Then the strict localization of the corresponding point on $\mathcal{X}_\pi$ is

$$W(\bar{\mathbb{F}}_p)[\![x,y]\!]/(xy-\pi^{ek}).$$

Thus the singularities of the special fiber of $\mathcal{X}_R$ are ordinary double points, corresponding to the double points of $\mathcal{X}_p$, and their width gets multiplied by the ramification index e.

It is important for us to have a description of the group of connected components of the fiber at π of the Néron model $\mathcal{J}$ over F of the jacobian of X. Let $s_1, \ldots, s_t$ be the supersingular points of $\mathcal{X}_\pi$, with respective width $k_1, \ldots, k_t$ (relative to the uniformizer π). The work of Raynaud [Ray 1] relates the Picard scheme $\mathrm{Pic}(\mathcal{X})$ to $\mathcal{J}$. Building on this, Grothendieck [Groth] gives the following description of the group of connected components $\Phi = \Phi_\pi = \mathcal{J}_\pi/\mathcal{J}_\pi^0$ of the special fiber $\mathcal{J}_\pi$ of $\mathcal{J}$. There is a canonical identification

$$\mathcal{J}_\pi^0 = \mathrm{Pic}^0(\mathcal{X}_\pi).$$

Since the singularities of $\mathcal{X}$ are ordinary double points, $\mathrm{Pic}^0(\mathcal{X})$, and hence $\mathcal{J}$, have semistable reduction at π. The character group $\mathbb{M}_0$ of the maximal torus of $\mathcal{J}_\pi$ is equal to the group of degree zero divisors with $\mathbb{Z}$-coefficients supported on $s_1, \ldots, s_t$. The work of Waterhouse (see [Wa], and [Rob, Thm. 4.2.2]) shows that the map sending s_i to its endomorphism ring R_i induces a bijection between the set of supersingular points and the set of oriented Eichler orders $R_1, \ldots, R_t$ introduced in the previous section. Hence $\mathbb{M}_0$ is identified with the kernel of the degree map $\mathbb{M} \to \mathbb{Z}$, where $\mathbb{M}$ is the module of Section 1. Given a $\mathbb{Z}$-module Λ, we write $\Lambda^\vee$ for its $\mathbb{Z}$-dual $\mathrm{Hom}(\Lambda, \mathbb{Z})$. Let

$$\langle\ ,\ \rangle\colon\ \mathbb{M}_0 \times \mathbb{M}_0 \to \mathbb{Z}$$

be defined as the restriction to $\mathbb{M}_0$ of the pairing of the previous section, and let

$$\phi\colon\ \mathbb{M}_0 \to \mathbb{M}_0^\vee$$

be the induced map. One can show that the width of singularity k_i is equal to ew_i. (Recall that w_i is equal to $\frac{1}{2}\#(R_i^\times)$.)

THEOREM 2.1 (Grothendieck).

1. *The pairing* $e\langle\ ,\ \rangle$ *is equal to the monodromy pairing on* $\mathbb{M}_0$.
2. *There is a canonical identification*

$$\Phi = \mathrm{coker}(\mathbb{M}_0 \xrightarrow{e\phi} \mathbb{M}_0^\vee),$$

where ϕ *is the map induced by the pairing* $\langle\ ,\ \rangle$.

Proof.

1. See Grothendieck, loc. cit., Thm. 12.5, and [Ray 2, pp. 16–17].
2. Grothendieck, loc. cit., Thm. 11.5.

The monodromy pairing $e\langle\ ,\ \rangle$ on $\mathbb{M}_0$ gives rise to a pairing

$$[\ ,\ ]\colon\ \Phi \times \Phi \to \mathbb{Q}/\mathbb{Z}$$

(which we still call the monodromy pairing by abuse of terminology), in the following way. The map $e\phi$ induces an isomorphism from $\mathbb{M}_0 \otimes \mathbb{Q}$ to $\mathrm{Hom}(\mathbb{M}_0, \mathbb{Q})$, which allows us to extend the pairing $e\langle\ ,\ \rangle$ to a $\mathbb{Q}$-valued pairing on $\mathbb{M}_0^\vee \subset \mathrm{Hom}(\mathbb{M}_0, \mathbb{Q})$. The reader will check that passing to the quotient gives rise to a well-defined pairing on $\Phi = \mathbb{M}_0^\vee/e\phi(\mathbb{M}_0)$, with values in $\mathbb{Q}/\mathbb{Z}$.

As a corollary we obtain:

COROLLARY 2.2.

1. *There is an exact sequence*

$$0 \to \mathbb{M}_0 \xrightarrow{e} \mathbb{M}_0 \xrightarrow{\kappa} \Phi \to \mathbb{M}_0^\vee/\phi(\mathbb{M}_0) \to 0.$$

2. *Given* v_1 *and* v_2 *in* $\mathbb{M}_0$,

$$[\kappa v_1, \kappa v_2] = \frac{1}{e}\langle v_1, v_2\rangle \pmod{\mathbb{Z}}.$$

An alternate description of Φ, also based on the work of Raynaud, is given in [MaRa].

Example. Given a discrete valuation ring extension R of $\mathbb{Z}_{11}$, with absolute ramification degree e, and letting π denote a uniformizer of R, as an example we compute in terms of the above description the group of connected components of the fiber at π of the modular curve $X = X_0(11) = X_{11,1}$. There are two singular points s_1 and s_2 on $\mathcal{X}$, with width of singularity $k_1 = 2e$ and $k_2 = 3e$. (They correspond to supersingular elliptic curves in characteristic 11, having j-invariant equal to 1728 and 0, respectively.) The fiber $\mathcal{X}_\pi$ has two components C and C', crossing at s_1 and s_2. The character group $\mathbb{M}_0$ of the maximal torus is equal to $\mathbb{Z}(s_1 - s_2)$. The pairing $\langle\ ,\ \rangle$ is characterized by $\langle s_1 - s_2, s_1 - s_2\rangle = 5e$, so that Φ is a cyclic group of order 5e.

3. Heegner points and connected components

In this section, we describe the natural image in Φ_n of the divisors of degree zero on $X(H_n)$ supported on the Heegner points of conductor cp^n. Let G_n be $\mathrm{Gal}(H_n/H)$. The group G_n is cyclic of order e_n. Let $\mathfrak{p}$ be a prime of H_n above p, and let $\mathcal{X}_\mathfrak{p}$ be the fiber at $\mathfrak{p}$ of the base change of $\mathcal{X}$ to the ring of integers of the completion of H_n at $\mathfrak{p}$. Let P be a Heegner point of conductor cp^n. (Cf. [BD1, §2.1] for the definition of these points.)

LEMMA 3.1. *The Heegner point P reduces modulo $\mathfrak{p}$ to a supersingular point in $\mathcal{X}_\mathfrak{p}$.*

Proof. In view of the modular interpretation of X ([Rob]), the Heegner point P corresponds to an abelian surface with quaternionic multiplication and level structure, and the ring of endomorphisms of the modulus P is equal to the order $\mathcal{O}_n$ of K of conductor cp^n. This abelian surface is isogenous to a product $E \times E$, where E is an elliptic curve whose ring of endomorphisms is equal to an order of K. Since p is inert in K, the curve E has supersingular reduction at $\mathfrak{p}$. The claim follows.

Identify in the natural way the module of divisors, resp. of divisors of degree zero supported on the supersingular points of $\mathcal{X}_\mathfrak{p}$ with $\mathbb{M}$, resp. $\mathbb{M}_0$. Let Div^{hp}, resp. Div_0^{hp}, denote the module of formal divisors, resp. degree zero divisors supported on the Heegner points of conductor cp^n.

Lemma 3.1 allows us to define a reduction map

$$\rho\colon \mathrm{Div}^{hp} \to \oplus_{\mathfrak{p}|p}\mathbb{M}.$$

Corollary 2.2 gives the exact sequence

$$0 \to \oplus_{\mathfrak{p}|p}\mathbb{M}_0 \xrightarrow{e_n} \oplus_{\mathfrak{p}|p}\mathbb{M}_0 \xrightarrow{\kappa} \Phi_n \to \oplus_{\mathfrak{p}|p}(\mathbb{M}_0^\vee/\phi(\mathbb{M}_0)) \to 0,$$

where by abuse of notation we denote by κ also the map on $\oplus_{\mathfrak{p}|p}\mathbb{M}_0$.

THEOREM 3.2. *Let D be a divisor in Div_0^{hp}, and let $\bar{D}$ be the natural image of D in Φ_n. Then*

$$\bar{D} = \kappa\rho(D).$$

Proof. Given a prime $\mathfrak{p}$ of H_n above p, let $\rho_\mathfrak{p}$: $\mathrm{Div}^{hp} \to \mathbb{M}$, resp. $\kappa_\mathfrak{p}$: $\mathbb{M}_0 \to \Phi_\mathfrak{p}$, denote the $\mathfrak{p}$-component of the map ρ, resp. κ. Note that $\kappa_\mathfrak{p}$ factors as

$$\mathbb{M}_0 \subset \mathbb{M} \xrightarrow{\tilde{\phi}} \mathbb{M}^\vee \xrightarrow{\pi} \Phi_\mathfrak{p},$$

where $\tilde{\phi}$ is induced by the pairing on $\mathbb{M}$ defined in the previous section, and π is equal to the dual of $\mathbb{M}_0 \subset \mathbb{M}$ composed with the projection of $M_0^\vee$ onto $\Phi_\mathfrak{p}$ determined by Theorem 2.1. Identify $\mathbb{M}$ with the free $\mathbb{Z}$-module generated by the supersingular points $s_1, \dots, s_t$ of $\mathcal{X}_\mathfrak{p}$, and write $s_1^\vee, \dots, s_t^\vee$ for the dual basis of $\mathbb{M}^\vee$ relative to the standard scalar product. If $\rho_\mathfrak{p}(D)$ is equal to $\sum_{i=1}^t n_i \cdot s_i$, then its image $\tilde{\phi}\rho_\mathfrak{p}(D)$ in $\mathbb{M}^\vee$ is $\sum_{i=1}^t w_i n_i \cdot s_i^\vee$. Thus, by the formula (2.3) of the Appendix, Theorem 3.2 is equivalent to the equality $w_i = m(s_i)$, where the numbers $m(s_i)$ are defined in Section 2 of the Appendix. Let $H_\mathfrak{p}$ be the completion of H_n at $\mathfrak{p}$. Write $\hat{H}_\mathfrak{p}^{\mathrm{unr}}$ for the completion of the maximal unramified extension of $H_\mathfrak{p}$, R for the ring of integers of $\hat{H}_\mathfrak{p}^{\mathrm{unr}}$, and π_R for a uniformizer of R. Observe that in order to apply the results of the Appendix, we have to pull back our objects to R.

Let now P be a Heegner point of conductor cp^n. We first consider the case of modular curves. Here P corresponds to a diagram $(E \xrightarrow{\alpha} E', \beta)$, where we may assume that E, resp. E' is an elliptic curve defined over H_{n-1}, resp. H_n, and where α: $E \to E'$ is an isogeny of degree p and β denotes the prime-to-p level structure carried by P. Viewing E and E' as elliptic curves over $R/pR = R/\pi_R^{e_n} R$, we let F: $E \to E^{(p)}$ be the Frobenius morphism. By formula (3.3) of the Appendix and by the above remarks, we are reduced to showing that $E^{(p)}$ and E' are not isomorphic over $R/\pi_R^2 R$. This is a consequence of Lubin-Tate's theory of formal moduli and of Gross' work on quasi-canonical liftings of formal groups. More precisely, let $\mathfrak{m}(E') \in \pi_R R$, resp. $\mathfrak{m}(E^{(p)}) \in \pi_R(R/pR)$ denote the formal modulus of E', resp. $E^{(p)}$, defined as in [LT, §3]. By Proposition 5.3 of [Gr3, part 3], $\mathrm{ord}_{\pi_R}\mathfrak{m}(E')$ is equal to 1. On the other hand, since E is defined over H_{n-1} and H_n is totally ramified over H_{n-1}, we find that $\mathfrak{m}(E^{(p)})$ belongs to $\pi_R^{[H_n:H_{n-1}]}(R/pR)$. Since formal moduli classify liftings of formal groups up to isomorphism (see [LT, Thm. 3.1 and Prop. 3.3]), this proves Theorem 3.2 in the case of modular curves.

In the general case, the local study of Heegner points on Shimura curves reduces to similar considerations on deformations of formal groups of dimension one: See Section 4 of the Appendix, and in particular Proposition 4.2. This concludes the proof of Theorem 3.2.

4. Proof of Theorem A

Let $\mathbb{D}$ be the free $\mathbb{Z}$-module of formal linear combinations of Gross points of conductor c. Given a Heegner point P of conductor cp^n and a prime $\mathfrak{p}$ of H_n

above p, the reduction modulo $\mathfrak{p}$ of endomorphisms determines an embedding $\mathcal{O}_n \to R_i$, where R_i is one of the Eichler orders above. This embedding extends to an embedding $\psi: \mathcal{O} \to R_i$, since there are no optimal embeddings of orders of conductor divisible by p into the R_i (cf. [BD1, Lemma 2.1]).

PROPOSITION 4.1. *The embedding* ψ: $\mathcal{O} \to R_i$ *is optimal.*

Proof. Let $P_* \in X(H_1)$ be the Heegner point such that the divisors $U_p^{n-1} P_*$ and $\mathrm{Norm}_{H_n/H_1} P$ on X are equal. (See the discussion in [BD1, §2.4].) Let $P' \in X'(H)$ be the image of P_* by the natural projection. (Recall that X' is the Shimura curve introduced in §2.) Note that P' has endomorphism ring $\mathcal{O}$, and the embedding ψ is equal to the reduction modulo $\mathfrak{p}$ of the endomorphisms of P'. It is a consequence of [GZ, Proposition 7.3] that ψ is optimal. $\square$

Proposition 4.1 allows us to define a map

$$\Psi\colon\ \mathrm{Div}^{hp} \to \oplus_{\mathfrak{p}|p} \mathbb{D}.$$

We define the action of the Galois group Δ on $\oplus_{\mathfrak{p}|p}\mathbb{D}$ by permutation of the summands: $\oplus_{\mathfrak{p}|p}\mathbb{D} := \mathrm{Ind}_{(1)}^{\Delta}(\mathbb{D})$ as a Δ-module. With this definition, note that Ψ is Δ-equivariant. Recall also from Section 1 that Δ acts on $\mathbb{D}$. We may extend this action diagonally to $\oplus_{\mathfrak{p}|p}\mathbb{D}$.

LEMMA 4.2. *The two actions of* Δ *on* $\oplus_{\mathfrak{p}|p}\mathbb{D}$ *agree on* $\mathrm{Im}(\Psi)$.

Proof. Fix a prime $\mathfrak{p}$ of H above p, and let $\Psi_{\mathfrak{p}} : \mathrm{Div}^{hp} \to \mathbb{D}$ be the natural map obtained by composing Ψ with the projection on the component at $\mathfrak{p}$. With P' as in the proof of Proposition 4.1, the claim amounts to showing that for all σ in Δ

$$\Psi_{\mathfrak{p}}((P')^{\sigma}) = \Psi_{\mathfrak{p}}(P')^{\sigma},$$

where the action of Δ on the right-hand side is the one considered in Section 1. Let $s \in \mathbb{M}$ be the reduction modulo $\mathfrak{p}$ of P', so that $\Psi_{\mathfrak{p}}(P')$ corresponds to the reduction modulo $\mathfrak{p}$ of endomorphisms

$$\psi\colon\ \mathrm{End}(P') \to \mathrm{End}(s).$$

Let $\mathfrak{a}$ be the element of $\mathrm{Pic}(\mathcal{O})$ representing σ such that

$$\mathfrak{a} = \mathrm{Hom}((P')^{\sigma}, P').$$

It follows from Proposition 7.3 of [GZ] that $\mathrm{Hom}(s^{\sigma}, s)$ is equal to $\mathrm{End}(s)\mathfrak{a}$, where we let s^{σ} denote the reduction modulo $\mathfrak{p}$ of $(P')^{\sigma}$. Observe that $\mathrm{End}(s^{\sigma})$ is the right order of $\mathrm{Hom}(s^{\sigma}, s)$, so that reduction modulo $\mathfrak{p}$ of endomorphisms gives rise to an optimal embedding

$$\psi'\colon\ \mathcal{O} = \mathrm{End}((P')^{\sigma}) \to R' = \mathrm{End}(s^{\sigma}).$$

But ψ' is equal to ψ^σ by definition; see [Gr1, p. 134].

Let ω be the natural map from $\oplus_{\mathfrak{p}|p}\mathbb{D}$ to $\oplus_{\mathfrak{p}|p}\mathbb{M}$. Then we have a natural commutative diagram of Galois and Hecke equivariant maps

$$(*) \qquad \begin{array}{ccc} \mathrm{Div}^{hp} & \xrightarrow{\rho} & \oplus_{\mathfrak{p}|p}\mathbb{M} \\ {\scriptstyle\Psi}\downarrow & & \downarrow{\scriptstyle =} \\ \oplus_{\mathfrak{p}|p}\mathbb{D} & \xrightarrow{\omega} & \oplus_{\mathfrak{p}|p}\mathbb{M}. \end{array}$$

By tensoring with $\mathcal{O}_f[\chi]$, we extend κ to a map from $\oplus_{\mathfrak{p}|p}\mathbb{M}_0 \otimes \mathcal{O}_f[\chi]$ to $\Phi_n^{f,\chi} \otimes \mathcal{O}_f[\chi]$, and denote it by the same symbol.

Proof of Theorem A. Noting that w_N acts as -1 on f ([BD1, §1.8 and 2.8]), so that $w_N\eta_f = -\eta_f$, we have the chain of equalities

$$\begin{aligned} [\bar{\alpha}_n^\chi, \bar{\alpha}_n^{f,\chi}]_n &= [\kappa\rho((P_n) - (w_N P_n))^\chi, \kappa\rho((P_n) - (w_N P_n))^{f,\chi}]_n \text{ (by Thm. 3.2)} \\ &\equiv \frac{4}{e_n}\langle(\rho P_n)^\chi, (\rho P_n)^{f,\chi}\rangle \qquad \text{(by Cor. 2.2)} \\ &= \frac{4}{e_n}\langle\omega(\Psi P_n)^\chi, \omega(\Psi P_n)^{f,\chi}\rangle \text{ (by the commutative diagram } (*)) \\ &= \frac{1}{e_n}\frac{L(f/K,\chi,1)}{(f,f)}\sqrt{d}\cdot u^2\cdot n_f \qquad (\mathrm{mod}\ \mathcal{O}_f[\chi]), \end{aligned}$$

where the last equality follows from Theorem 1.1.

Remark. We may combine the formulae of Theorem A corresponding to the various n in a single statement. Let

$$\Phi_\infty := \varprojlim_n \Phi_n,$$

where the inverse limit is with respect to the maps of multiplication by p. By Theorem 2.1, there is a surjection (which is well-defined up to sign) from Φ_∞ to $\oplus_{\mathfrak{p}|p}\mathbb{M}_0^\vee \otimes \mathbb{Z}_p$. The monodromy pairings $[\ ,\ ]_n$ give rise to a canonical pairing

$$[\ ,\ ]_\infty\colon\ \Phi_\infty \times \Phi_\infty \to \mathbb{Z}_p.$$

Denote by $\bar{\alpha}_\infty^f$ the natural image in Φ_∞ of the norm-compatible sequence of Heegner divisors (α_n^f). Then, Theorem A can be restated as follows:

THEOREM 4.3. *Suppose that χ is a primitive character of Δ. Then we have the equality in $\mathcal{O}_f[\chi]$*

$$[\bar{\alpha}_\infty^{f,\chi}, \bar{\alpha}_\infty^{f,\chi}]_\infty = \frac{L(f/K,\chi,1)}{(f,f)}\sqrt{d}\cdot u^2\cdot n_f^2.$$

5. A rigid analytic Gross-Zagier formula

In [BD1], we formulate conjectures for elliptic curves with values in anti-cyclotomic towers, which are analogues of the conjectures of Mazur, Tate and Teitelbaum for the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$ [MTT], and which contain new arithmetic features that have no counterpart in the setting of [MTT]. Here we point out that the results contained in this paper give a proof of an important special case of our conjectures, precisely Conjecture 5.5 of subsection 5.2.

Suppose that $c = 1$ and that f has rational Fourier coefficients, so that it corresponds to an isogeny class of elliptic curves defined over $\mathbb{Q}$. Any E in this isogeny class has multiplicative reduction at our fixed prime p (which is inert in K). By the Jacquet-Langlands correspondence there are maps

$$\pi_{E*}\colon J \to E, \quad \pi_E^*\colon E \to J$$

(cf. [BD1, §1.9]). Here the map π_E^* is the dual of the Shimura curve parametrization π_{E*}. We assume that π_{E*} has connected kernel, or equivalently that π_E^* is injective. We define the degree of π_{E*} to be the positive integer d_X corresponding to the endomorphism $\pi_{E*} \circ \pi_E^*$ of E. There is also a classical modular curve parametrization of minimal degree $d_{X_0(N)}$ from $X_0(N)$ to the strong Weil curve E' in the isogeny class of E. Let δ_X be the ratio $d_X/d_{X_0(N)}$, and let Ω be the complex period associated to E'.

Since p is inert in K, the curve E/K_p has split multiplicative reduction. Let

$$\Phi_n^E = \oplus_{\mathfrak{p}|p} \Phi_{\mathfrak{p}}^E$$

be the group of connected components at p of the Néron model of E over H_n. By Tate's theory, $\Phi_{\mathfrak{p}}^E$ is isomorphic (up to sign) to $\mathbb{Z}/e_n c_p \mathbb{Z}$, where $c_p := \operatorname{ord}_p(q_E)$. Let $H_{n,p}$ stand for $H_n \otimes \mathbb{Q}_p$. Define

$$\hat{E}(H_{\infty,p}) := \varprojlim_n E(H_{n,p}), \qquad \Phi_\infty^E := \varprojlim_n \Phi_n^E,$$

where the inverse limits are taken with respect to the norm and the multiplication by p maps respectively. Note that there is a surjection from Φ_∞^E to $\mathbb{Z}_p$, which induces a map

$$\lambda_{q_E}\colon \hat{E}(H_{\infty,p}) \to \mathbb{Z}_p$$

by specializing to the group of connected components.

Let $y_n := \pi_{E*}(\alpha_n) \in E(H_n)$. The Heegner points y_n are norm-compatible and, by [BD1, §2.5], $\operatorname{Norm}_{H_n/K} y_n = 0$. The reader should think of $\lambda_{q_E}((y_n))$ as the leading coefficient of the p-adic L-function associated to the sequence (y_n). (See [BD1, §2.7] for more details.)

THEOREM 5.1. *Assume that E is isolated in its isogeny class (so that $E = E'$). We have*

$$\lambda_{q_E}((y_n))^2 = \frac{L(E/K,1)}{\Omega}\sqrt{d} \cdot u^2 \cdot \delta_X \cdot c_p.$$

Proof. The group Φ_n^E is equipped with the monodromy pairing

$$[\ ,\ ]_{E,n}\colon\ \Phi_n^E \times \Phi_n^E \to \mathbb{Q}/\mathbb{Z},$$

whose $\mathfrak{p}^{\text{th}}$ component $[\ ,\ ]_{E,\mathfrak{p}}$ is characterized by $[1,1]_{E,\mathfrak{p}} = \frac{1}{e_n c_p}$. Let

$$\bar{\pi}_{E*}\colon\ \Phi_n \to \Phi_n^E$$

be the map on connected components induced by π_{E*}. Write $\mathbf{1}$ for the trivial character of Δ. The number $\lambda_{q_E}((y_n))^2$ is equal to $[\bar{\pi}_{E*}\bar{\alpha}_n^{\mathbf{1}}, \bar{\pi}_{E*}\bar{\alpha}_n^{\mathbf{1}}]_{E,n} \cdot (e_n c_p)$ modulo e_n. Hence

$$\frac{1}{c_p e_n}\lambda_{q_E}((y_n))^2 \equiv [\bar{\pi}_{E*}\bar{\alpha}_n^{\mathbf{1}}, \bar{\pi}_{E*}\bar{\alpha}_n^{\mathbf{1}}]_{E,n} = [\bar{\alpha}_n^{\mathbf{1}}, \bar{\pi}_E^*\bar{\pi}_{E*}\bar{\alpha}_n^{\mathbf{1}}]_n.$$

Observe that $\bar{\pi}_E^*\bar{\pi}_{E*}$ is equal to $d_X\pi_f$ acting on Φ_n. This can be seen by noting that $\pi_E^*\pi_{E*}$ is necessarily an integer multiple of π_f, and

$$(\pi_E^*\pi_{E*})^2 = d_X\pi_E^*\pi_{E*}.$$

Define now η_f to be $d_X\pi_f$, so that $n_f = d_X$. Then by Theorem A,

$$[\bar{\alpha}_n^{\mathbf{1}}, \bar{\pi}_E^*\bar{\pi}_{E*}\bar{\alpha}_n^{\mathbf{1}}]_n = [\bar{\alpha}_n^{\mathbf{1}}, \bar{\alpha}_n^{f,\mathbf{1}}]_n = \frac{1}{e_n}\frac{L(f/K,1)}{(f,f)}\sqrt{d}\cdot u^2 \cdot d_X \qquad (\text{mod } \mathbb{Z}).$$

Using the fact that (f,f) is equal to $d_{X_0(N)}\Omega$, we find

$$\lambda_{q_E}((y_n))^2 = \frac{L(E/K,1)}{\Omega}\sqrt{d}\cdot u^2 \cdot \delta_X \cdot c_p,$$

as was to be shown. □

Remarks. 1. The formula of Theorem 5.1 may be seen as an analogue of the formula of Gross-Zagier, in the rigid analytic setting, and of the theorem of Greenberg-Stevens [GS], in the anticyclotomic setting.

2. Theorem A shows that the sequence of Heegner points (y_n) maps non-trivially to the group of connected components Φ_∞^E precisely when $L(E/K,1)$ is nonzero. On the other hand, it is always easy to construct norm compatible sequences of local points on E whose norm to K_p is equal to zero, and whose image in Φ_∞^E is nontrivial. This follows from the fact that the period q_E is a local universal norm in the anticyclotomic $\mathbb{Z}_p$-extension of K_p.

3. The classical Birch and Swinnerton-Dyer conjecture predicts that

$$\frac{L(E/K,1)}{\Omega} = \#Ш\ (E/K)\prod_{\ell|N+} c_\ell^2 \prod_{\ell|N-} c_\ell \cdot (\#(E(K)_{\text{tors}})^2 \cdot \sqrt{d}\cdot (u/2)^2)^{-1},$$

where c_ℓ is the number of connected components of the fiber at ℓ of the Néron model of E over $\mathbb{Q}$. Combining this with Theorem 5.1 suggests that

$$(\delta_X)^{-1} = \prod_{\ell|(N^-/p)} c_\ell \pmod{(\mathbb{Q}^\times)^2}.$$

It would be interesting to investigate when this equality holds not just up to squares. In this connection, see the forthcoming work of Ribet and Takahashi [RT].

6. Kolyvagin cohomology classes

Let A denote the abelian variety A_f of the introduction. We construct cohomology classes in $H^1(H, A_{e_n})$ from Heegner points on X defined over ring-class field extensions of H_n, and we study their ramification properties. These classes will be used in the next section to bound the Mordell-Weil group $A(H)$.

Preliminaries. If L is a number field, we write G_L for its absolute Galois group, and $G_{M/L}$ for the Galois group of a finite Galois field extension M/L. We denote by $\mathrm{Frob}_\ell(M/L)$ the Frobenius element attached to a prime ℓ of L which is unramified in M. It is a well-defined conjugacy class in $G_{M/L}$.

From now on we let $\mathbb{T}$ denote the algebra generated by the Hecke operators acting on A. The map ϕ_f of the introduction induces an isomorphism of $\mathbb{T}$ onto the ring $\mathcal{O}_f$ generated over $\mathbb{Z}$ by the Fourier coefficients of f. We will write T_ℓ to denote the image of the ℓ^{th} Hecke operator in $\mathbb{T}$. The ring $\mathbb{T}$ need not be integrally closed: let $\tilde{\mathbb{T}}$ be the integral closure of $\mathbb{T}$ in its fraction field, and let ι be the exponent of $\mathbb{T}$ in $\tilde{\mathbb{T}}$. The adelic Tate module $T(A) := \varprojlim_m A_m$ is endowed with a natural action of $G_{\mathbb{Q}}$, and $T(A) \otimes_{\mathbb{T}} \tilde{\mathbb{T}}$ is free of rank 2 over $\tilde{\mathbb{T}} \otimes \hat{\mathbb{Z}}$. Choosing a basis gives Galois representations

$$\rho\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\tilde{\mathbb{T}} \otimes \hat{\mathbb{Z}}), \qquad \text{and} \qquad \rho_m\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\tilde{\mathbb{T}}/\iota m\tilde{\mathbb{T}}),$$

for all positive integers m. Let F_m denote the smallest field extension of H through which ρ_m factors. Note that A_m is defined over F_m.

Given a square-free product $t = \prod \ell$ of primes ℓ such that $(cp, \ell) = 1$, let $H_n[t]$ denote the compositum of H_n with the ring-class field $K[t]$ of conductor t. Write $\mathcal{G}_t$ for $\mathrm{Gal}(H_n[t]/H_n)$ and $\tilde{\mathcal{G}}_t$ for $\mathrm{Gal}(H_n[t]/H)$. Thus we have canonical identifications $\tilde{\mathcal{G}}_t = G_n \times \mathcal{G}_t$ and $\mathcal{G}_t = \prod_\ell \mathcal{G}_\ell$.

Definition. A prime ℓ is a *Kolyvagin prime* (relative to n) if ℓ does not divide $2c(p+1)N$, and satisfies

$$\mathrm{Frob}_\ell(F_{e_n}/\mathbb{Q}) = [\tau],$$

where τ denotes a fixed complex conjugation in $G_{\mathbb{Q}}$.

Let ℓ be a Kolyvagin prime relative to n. Then, the group $\mathcal{G}_\ell$ is cyclic of order $\ell + 1$.

LEMMA 6.1. *If ℓ is a Kolyvagin prime relative to n, then T_ℓ belongs to $e_n\mathbb{T}$ and $\ell + 1$ is divisible by e_n.*

Proof. By the Eichler-Shimura relation, the characteristic polynomial of $\rho_{e_n}(\mathrm{Frob}_\ell)$ is equal to $x^2 - T_\ell x + \ell$. The characteristic polynomial of $\rho_{e_n}(\tau)$ is equal to $x^2 - 1$. It follows that $\ell + 1$ is divisible by ιe_n, and the image of T_ℓ in $\tilde{\mathbb{T}} \otimes \hat{\mathbb{Z}}$ is divisible by ιe_n, so that T_ℓ belongs to $e_n\mathbb{T}$. □

Fix a generator σ, resp. σ_ℓ for G_n, resp. $\mathcal{G}_\ell$, and write Norm, resp. Norm_ℓ, for the associated norm operators. Define Kolyvagin's derivative operators

$$D = \sum_{i=1}^{e_n - 1} i\sigma^i, \quad D_\ell = \sum_{i=1}^{\ell} i\sigma_\ell^i.$$

The following equations hold:

$$(1) \qquad (\sigma - 1)D = e_n - \mathrm{Norm}, \quad (\sigma_\ell - 1)D_\ell = (\ell + 1) - \mathrm{Norm}_\ell.$$

Given a square-free product t of Kolyvagin primes, let $D_t \in \mathbb{Z}[\mathcal{G}_t]$, resp. $\tilde{D}_t \in \mathbb{Z}[\tilde{\mathcal{G}}_t]$ stand for $\prod_\ell D_\ell$, resp. $D\prod_\ell D_\ell$. When $t = 1$ is the empty product, we mean that $\tilde{D}_t$ is equal to D.

For all the t as before, the results of [BD1, §2.5] allow us to define Heegner points $\alpha_n(t) \in A(H_n[t])$ satisfying the relations

$$(2) \qquad \mathrm{Norm}(\alpha_n(t)) = 0, \quad \mathrm{Norm}_\ell(\alpha_n(t)) = T_\ell \alpha_n(t/\ell).$$

Let α_n denote the Heegner point corresponding to the empty product. (The point α_n is the image in A of the Heegner point α_n of the previous sections.)

Let Φ_n^A, resp. $\Phi_{n,t}^A$ be the group of connected components at p of the Néron model of A over H_n, resp. $H_n[t]$. Since the primes of H_n over p are unramified in $H_n[t]$, we have $(\Phi_{n,t}^A)^{\mathcal{G}_t} = \Phi_n^A$. Let $D_t\bar{\alpha}_n(t)$ be the image of $D_t\alpha_n(t)$ in $\Phi_{n,t}^A$.

LEMMA 6.2. 1. *The natural image $Q_n(t)$ of $\tilde{D}_t\alpha_n(t)$ in $(A(H_n[t])/e_n A(H_n[t]))$ is fixed by $\tilde{\mathcal{G}}_t$.*

2. *The element $D_t\bar{\alpha}_n(t)$ belongs to Φ_n^A.*

Proof. Part 1 follows from equations (1) and (2), combined with Lemma 6.1. To prove part 2, it is enough to show that $D_t\bar{\alpha}_n(t)$ is fixed by $\mathcal{G}_t$. Let ℓ be a prime dividing t. Then we have

$$(\sigma_\ell - 1)D_t\bar{\alpha}_n(t) = (\ell + 1)D_t\bar{\alpha}_n(t) - T_\ell D_t\bar{\alpha}_n(t/\ell).$$

Since Norm acts as multiplication by e_n on $\Phi_{n,t}^A$ and kills $\alpha_n(t)$ and $\alpha_n(t/\ell)$, we find that $\bar{\alpha}_n(t)$ and $\bar{\alpha}_n(t/\ell)$ belong to $(\Phi_{n,t}^A)_{e_n}$. The result follows from Lemma 6.1.

LEMMA 6.3. *The order of the group $A(H_n[t])_{\mathrm{tors}}$ is bounded independently of n and t.*

Proof. Choose two primes q_1 and q_2 which are inert in K and do not divide N. The residue field of $H_n[t]$ at any prime above q_1 is $\mathbb{F}_{q_1^2}$, and likewise for q_2. Since $A(H_n[t])_{\mathrm{tors}}$ injects in $A(\mathbb{F}_{q_1^2}) \oplus A(\mathbb{F}_{q_2^2})$, the claim follows.

In view of Lemma 6.3, define an absolute integer constant a which annihilates $A_{e_n}(H_n[t])$ for all n and t, and the groups $\Phi^A_{[\ell]}$ of connected components at ℓ of $A/\mathbb{Q}$, for all primes ℓ which divide N and are split in K.

Construction of the Kolyvagin classes. Recall the e_n-descent exact sequence over $H_n[t]$:

$$0 \to A(H_n[t])/e_nA(H_n[t]) \xrightarrow{\delta} H^1(H_n[t], A_{e_n}) \to H^1(H_n[t], A)_{e_n} \to 0,$$

and let $c_n(t)^{oo} = -\delta Q_n(t)$ be the natural image of $-\tilde{D}_t\alpha_n(t)$ in $H^1(H_n[t], A_{e_n})$. By Lemma 6.2, the class $c_n(t)^{oo}$ belongs to $H^1(H_n[t], A_{e_n})^{\tilde{\mathcal{G}}_t}$. The Hochschild-Serre spectral sequence $H^i(\tilde{\mathcal{G}}_t, H^j(H_n[t], A_{e_n})) \Longrightarrow H^{i+j}(H, A_{e_n})$ gives rise to the exact sequence (inflation-restriction):

$$\begin{aligned} H^1(\tilde{\mathcal{G}}_t, A_{e_n}(H_n[t])) &\xrightarrow{\text{infl}} H^1(H, A_{e_n}) \\ &\xrightarrow{\text{res}} H^1(H_n[t], A_{e_n})^{\tilde{\mathcal{G}}_t} \to H^2(\tilde{\mathcal{G}}_t, A_{e_n}(H_n[t])). \end{aligned}$$

Hence there exists a class $c_n(t)^o$ in $H^1(H, A_{e_n})$ such that $\operatorname{res}(c_n(t)^o) = ac_n(t)^{oo}$. This class is well defined in $H^1(H, A_{e_n})$, modulo the image of the inflation map. Thus the class $c_n(t) = ac_n(t)^o$ is well defined in $H^1(H, A_{e_n})$.

We call the class $c_n(t) \in H^1(H, A_{e_n})$ the *Kolyvagin cohomology class* associated to n and to the product t of Kolyvagin primes (relative to n). The class $c_n(1)$ corresponding to the empty product $t = 1$ will also be denoted by c_n. The remainder of this section is devoted to a study of the Kolyvagin classes $c_n(t)$.

Explicit description of $c_n(t)$. We will have use for the following explicit formula for the class $c_n(t)$. Let $[\frac{\tilde{D}_t\alpha_n(t)}{e_n}]$ be a (fixed) point in $A(\bar{H})$ such that $e_n[\frac{\tilde{D}_t\alpha_n(t)}{e_n}] = \tilde{D}_t\alpha_n(t)$. For all $\gamma \in G_H$, the point $(\gamma - 1)\tilde{D}_t\alpha_n(t)$ belongs to $e_nA(H_n[t])$ by Lemma 6.2. Let $\frac{(\gamma-1)\tilde{D}_t\alpha_n(t)}{e_n}$ be a point in $A(H_n[t])$ such that $e_n\frac{(\gamma-1)\tilde{D}_t\alpha_n(t)}{e_n} = (\gamma-1)\tilde{D}_t\alpha_n(t)$. This point is well defined modulo $A_{e_n}(H_n[t])$, and hence the point $a\frac{(\gamma-1)\tilde{D}_t\alpha_n(t)}{e_n}$ is uniquely defined. Define a cochain $c_n(t)'$ with values in A_{e_n} by the formula

$$c_n(t)'(\gamma) = -a(\gamma - 1)\left[\frac{\tilde{D}_t\alpha_n(t)}{e_n}\right] + a\frac{(\gamma - 1)\tilde{D}_t\alpha_n(t)}{e_n}.$$

The cochain $c_n(t)'$ is not a cocycle in general. One checks, however, that its coboundary $dc_n(t)'(\gamma_1, \gamma_2) = c_n(t)'(\gamma_1\gamma_2) - (c_n(t)'(\gamma_1) + \gamma_1c_n(t)'(\gamma_2))$ takes values in $A_{e_n}(H_n[t])$, so that the class $ac_n(t)'$ is a cocycle. As McCallum [McC] has remarked, we have:

LEMMA 6.4. *The Kolyvagin class $c_n(t)$ is represented by the cocycle $ac_n(t)'$.*

Proof. A direct computation.

Action of complex conjugation. Define a sign w to be -1 if $A/\mathbb{Q}_p$ has split multiplicative reduction, and to be $+1$ if $A/\mathbb{Q}_p$ has nonsplit multiplicative reduction.

PROPOSITION 6.5. *There exists $\gamma \in \Delta$ such that $\tau c_n(t) = (-1)^{\#\{\ell|t\}} \cdot w \cdot \gamma c_n(t)$.*

Proof. By [BD1, Prop. 2.5], we have $\tau\alpha_n(t) = -w\gamma'\alpha_n(t)$, for some element γ' of $\mathrm{Gal}(H_n[t]/K)$. Using equation (2) and Lemma 6.1, we see that a direct calculation proves the claim. (See [Gr2, Prop. 5.4].)

Descent Modules. Given a rational prime ℓ and a number field F, we let F_ℓ be $\oplus_{\lambda|\ell}F_\lambda$, where the sum is taken over the primes λ of F above ℓ and F_λ denotes the completion of F at λ. We extend additively functors defined on finite extensions of $\mathbb{Q}_\ell$. Thus, for instance, $H^1(H_\ell, A) := \oplus_{\lambda|\ell}H^1(H_\lambda, A)$, etc.

Recall the descent exact sequence:

$$0 \to A(H)/e_nA(H) \to H^1(H, A_{e_n}) \to H^1(H, A)_{e_n} \to 0.$$

For each prime ℓ of K there is also a corresponding exact sequence of local cohomology groups, obtained by replacing H by H_ℓ. Both of these sequences respect the natural actions of the Hecke algebra $\mathbb{T}$ and the Galois group Δ.

Let $W \subset H^1(H, A_{e_n})$ be the image of $A(H)/e_nA(H)$, and let $X = H^1(H, A)_{e_n}$ be the cokernel. Denote by W_ℓ and X_ℓ the local counterparts of these groups, for each prime ℓ.

We will need an explicit description of the modules W_ℓ and X_ℓ, at least when ℓ is a Kolyvagin prime relative to n and when $\ell = p$.

LEMMA 6.6. *Suppose that ℓ is a Kolyvagin prime. Then there is a canonical Δ and $\mathbb{T}$-equivariant isomorphism*

$$\psi_\ell\colon\ X_\ell \to \mathrm{Hom}(\mathcal{G}_\ell, W_\ell).$$

Proof. Let $H_\ell^{\mathrm{unr}} = \oplus_{\lambda|\ell}H_\lambda^{\mathrm{unr}}$ be the maximal unramifield extension of H_ℓ. Since ℓ is a Kolyvagin prime, we have by the inflation-restriction sequence

$$\begin{aligned} X_\ell &= H^1(H_\ell^{\mathrm{unr}}, A_{e_n})^{\mathrm{Frob}_\ell} \\ &= \mathrm{Hom}(\mathrm{Gal}(\bar{H}_\ell/H_\ell^{\mathrm{unr}}), A_{e_n})^{\mathrm{Frob}_\ell} = \mathrm{Hom}(\mathcal{G}_\ell, A_{e_n}(H_\ell)). \end{aligned}$$

Finally, we identify $A_{e_n}(H_\ell) = \oplus_{\lambda|\ell}A_{e_n}(H_\lambda)$ with $W_\ell = \oplus_{\lambda|\ell}A(H_\lambda)/e_nA(H_\lambda)$ via the map $\oplus_{\lambda|\ell}((\ell+1)\mathrm{Frob}_\lambda(H/\mathbb{Q}) - T_\ell)/e_n$. See [Gr2] for more details.

Note that the proof of Lemma 6.6 shows that the $\mathbb{T}[\Delta]$-modules X_ℓ and W_ℓ are both isomorphic to $A_{e_n}(H_\ell) = \mathrm{Ind}_{(1)}^{\Delta}A_{e_n}$.

We now turn to $\ell = p$. Let Y_p denote $H^1(G_n, A(H_{n,p}))_{e_n}$, identified by inflation with a submodule of X_p.

LEMMA 6.7. *There is a canonical Δ and $\mathbb{T}$-equivariant injection*

$$\psi_p\colon\ Y_p \to \mathrm{Hom}(G_n, \Phi_n^A).$$

Proof. The Mumford-Tate theory of p-adic uniformization gives rise to an exact sequence

$$0 \to U_{H_{n,p}} \otimes (\mathbb{M}_0^A)^\vee \to A(H_{n,p}) \to \Phi_n^A \to 0,$$

where $U_{H_{n,p}}$ is the group of units in $H_{n,p}^\times$ and $\mathbb{M}_0^A$ is the character group of A at p. Taking G_n-cohomology yields

$$0 \to \Phi^A \to \Phi_n^A \to H^1(G_n, U_{H_{n,p}} \otimes (\mathbb{M}_0^A)^\vee) \to Y_p \to \mathrm{Hom}(G_n, \Phi_n^A),$$

where Φ^A denotes the group of connected components of A over H_p. The G_n-cohomology of the natural sequence

$$0 \to U_{H_{n,p}} \otimes (\mathbb{M}_0^A)^\vee \to H_{n,p}^\times \otimes (\mathbb{M}_0^A)^\vee \xrightarrow{\mathrm{ord}} (\mathbb{M}_0^A)^\vee \to 0$$

shows that $H^1(G_n, U_{H_{n,p}} \otimes (\mathbb{M}_0^A)^\vee)$ is isomorphic to $(\mathbb{Z}/e_n\mathbb{Z})^{\dim(A)}$. Hence ψ_p is injective.

Residues and duality. Let ξ be a global cohomology class in $H^1(H, A_{e_n})$. If ℓ is a rational prime, the *residue at ℓ* of ξ, denoted $\partial_\ell\xi$, is defined to be the natural image of ξ in X_ℓ. If $\partial_\ell\xi$ is zero, then the image of ξ in $H^1(H_\ell, A_{e_n})$ belongs to W_ℓ. We denote by $v_\ell\xi$ this image, which we call the *value of ξ at ℓ*.

The class ξ has only finitely many nontrivial residues, since it is unramified for almost all primes. Define the *support* $\mathrm{Supp}(\xi)$ of ξ to be the set of primes of $\mathbb{Q}$ at which ξ has nontrivial residue.

Choose a polarization of A, i.e., a $\mathbb{Q}$-isogeny from A to its dual abelian variety $A^\vee$. This choice combined with the canonical nondegenerate Weil pairing $A_{e_n} \otimes A_{e_n}^\vee \to \mu_{e_n}$ gives rise to a pairing $A_{e_n} \otimes A_{e_n} \to \mu_{e_n}$, whose left and right radical have order bounded independently of n. The cup product followed by this modified Weil pairing gives a symmetric Galois and Hecke-equivariant local Tate pairing

$$\langle\ ,\ \rangle_\ell\colon\ H^1(H_\ell, A_{e_n}) \times H^1(H_\ell, A_{e_n}) \to H^2(H_\ell, \mu_{e_n}) \xrightarrow{\mathrm{inv}_\ell} \mathbb{Z}/e_n\mathbb{Z},$$

where inv_ℓ denotes the sum of the invariants at the primes dividing ℓ ([Mi]). By results of Tate, the radical of $\langle\ ,\ \rangle_\ell$ has order bounded independently of n. The submodule W_ℓ is isotropic for $\langle\ ,\ \rangle_\ell$, and hence the local Tate pairing gives rise to

$$\langle\ ,\ \rangle_\ell\colon\ W_\ell \times X_\ell \to \mathbb{Z}/e_n\mathbb{Z},$$

which by abuse of notation we denote in the same way.

The following reciprocity law of Poitou and Tate is fundamental.

PROPOSITION 6.8 (Global reciprocity). *Suppose that ξ_1 and ξ_2 are global classes in $H^1(H,A_{e_n})$ with disjoint support. Then we have:*

$$\sum_{\ell\in\mathrm{Supp}(\xi_2)} \langle v_\ell\xi_1,\partial_\ell\xi_2\rangle_\ell = -\sum_{\ell\in\mathrm{Supp}(\xi_1)} \langle v_\ell\xi_2,\partial_\ell\xi_1\rangle_\ell.$$

Proof. By the formula for the local Tate pairing we have $\langle v_\ell\xi_1, \partial_\ell\xi_2\rangle_\ell = \mathrm{inv}_\ell(\xi_1 \cup \xi_2)$, for all ℓ in the support of ξ_2, and likewise for ξ_1. Hence

$$\sum_{\ell\in\mathrm{Supp}(\xi_2)} \langle v_\ell\xi_1, \partial_\ell\xi_2\rangle_\ell + \sum_{\ell\in\mathrm{Supp}(\xi_1)} \langle v_\ell\xi_2, \partial_\ell\xi_1\rangle_\ell = \sum_\ell \mathrm{inv}_\ell(\xi_1 \cup \xi_2).$$

The last sum is 0, by the global reciprocity law of class field theory ([Mi]). □

Local behaviour of the Kolyvagin classes. We turn to the behaviour of the classes $c_n(t)$ under localization. It might help the reader already familiar with Kolyvagin's theory to notice that the classes $c_n(t)$ differ from the cohomology classes considered by Kolyvagin (see for example [Gr2]) for the fact that they may be nontrivial not only at tamely ramified (Kolyvagin) primes, but also at the wildly ramified prime p.

PROPOSITION 6.9.

1. *If ℓ does not divide pt, then $\partial_\ell c_n(t) = 0$.*

2. *If ℓ divides t, then:*

   (a) (*Induction formula*). $\psi_\ell(\partial_\ell c_n(t))(\sigma_\ell) = v_\ell c_n(t/\ell)$.

   (b) (*Orthogonality relation*). $\langle v_\ell\mathbb{T}[\Delta]c_n(t/\ell),\partial_\ell c_n(t)\rangle_\ell = 0$.

3. *The residue $\partial_p c_n(t)$ belongs to Y_p, and*

$$\psi_p(\partial_p c_n(t))(\sigma) = a^2 D_t\bar{\alpha}_n(t),$$

where $D_t\bar{\alpha}_n(t)$ denotes the image of $D_t\alpha_n(t)$ in Φ_n^A.

Proof.

1. Observe that the extension $H_n[t]/H$ is unramified outside pt. Then, by [Ma1, Prop. 4.3], the group $H^1(\mathrm{Gal}((H_n[t])_\ell/H_\ell), A((H_n[t])_\ell))$ is naturally isomorphic to $H^1(\mathrm{Gal}(\mathbb{F}_{(H_n[t])_\ell}/\mathbb{F}_{H_\ell}), \Phi^A_{[\ell]})$. If ℓ is a prime of good reduction for A, then $\Phi^A_{[\ell]}$ is trivial, and hence $\partial_\ell c_n(t) = 0$. If ℓ is inert in K, then $H_n[t]/H$ has trivial residue field extension at ℓ, and thus $c_n(t)$ restricts to zero at ℓ. Finally, if ℓ splits in K and divides N, then our choice of a guarantees that $\partial_\ell c_n(t) = 0$.

2. By the explicit description of $c_n(t)$, and the description of X_ℓ given in the proof of Lemma 6.6, we have the equality

$$\partial_\ell c_n(t)(\sigma_\ell) = a^2 \frac{(\sigma_\ell - 1)\tilde{D}_t \alpha_n(t)}{e_n}$$

in $A_{e_n}(H_\ell)$. Equations (1) and (2) yield

$$\frac{(\sigma_\ell - 1)\tilde{D}_t \alpha_n(t)}{e_n} = \frac{(\ell+1)\tilde{D}_{t/\ell}\alpha_n(t) - T_\ell \tilde{D}_{t/\ell}\alpha_n(t/\ell)}{e_n}.$$

Part (a) now follows from the description of the map ψ_ℓ given in Proposition 6.6, and the congruence

$$\alpha_n(t) \equiv \mathrm{Frob}_{\lambda'}(H_n[t]/\mathbb{Q})\alpha_n(t/\ell) \pmod{\lambda'}$$

for all primes λ' of $H_n[t]$ above ℓ. (The above congruence is a consequence of equation (2), combined with the Eichler-Shimura relation. See [Gr2, Prop. 3.7 and 6.2] for more details.)

The proof of (b) in a special case is contained in Proposition 3.6(b) of [B2]. The general case is proved along similar lines.

3. It follows from Lemma 6.4, combined with equation (1).

Given a character $\chi\colon \Delta \to \mathbb{Z}[\chi]^\times$, let $[\chi]$ be the Galois orbit of χ, and define the operator $e_{[\chi]} \in \mathbb{Z}[\Delta]$ to be $e_{[\chi]} := \sum_{\chi^\sigma \in [\chi]} e_{\chi^\sigma}$. Let V be a $\mathbb{Z}[\Delta]$-module. Unlike the previous sections, we now define $V^\chi := e_{[\chi]}V$. It is a $\mathbb{Z}[\Delta]$-submodule of V. The action of the group ring $\mathbb{Z}[\Delta]$ on V^χ factors through the map $\mathbb{Z}[\Delta] \to \mathbb{Z}[\chi]$ induced by χ. In this way, V^χ can and will be viewed as a $\mathbb{Z}[\chi]$-module. Suppose in addition that V is a $\mathbb{Z}[G_{H/\mathbb{Q}}]$-module. Then the complex conjugation τ acts on V^χ and this action is skew-linear with respect to the action of $\mathbb{Z}[\chi]$, i.e., $\tau\alpha v = \bar{\alpha}\tau v$ for all $v \in V^\chi$ and $\alpha \in \mathbb{Z}[\chi]$. Let $V^{\chi,\pm}$ be the $\pm$-eigenspace for τ acting on V^χ.

Let $c_n(t)^\chi$ be the class $e_{[\chi]}c_n(t)$ in $H^1(H, A_{e_n})^\chi$.

PROPOSITION 6.10. *If $L(A/K,\chi,1) \neq 0$, then the $\mathbb{T}[\chi]$-submodule of Y_p^χ generated by $\partial_p c_n^\chi$ has index bounded independently of n.*

Proof. Since $L(A/K,\chi,1)$ is nonzero, then $L(f^\sigma/K,\chi,1)$ is nonzero for all the Galois conjugate forms f^σ of f. Proposition 6.10 follows from Theorem A combined with part 3 of Proposition 6.9.

7. Bounding Mordell-Weil groups

Assuming that $L(A/K,\chi,1) \neq 0$, we show in this section that the image of $A(H)/p^n A(H)$ in $H^1(H, A_{p^n})^\chi$ is bounded independently of n, thus proving Theorem B.

We will make a shift in notation, letting W^χ, resp. X^χ be $(A(H)/p^nA(H))^\chi$, resp. $H^1(H,A)^\chi_{p^n}$, and likewise for their local counterparts W^χ_ℓ and X^χ_ℓ. Moreover, we replace the class $c_n(t)$ defined in Section 6 with its natural image in $H^1(H,A_{p^n})$.

Given a $\mathbb{Z}[\chi]$-module V, let V^{dual} be the Pontryagin dual $\mathrm{Hom}(V,\mathbb{Q}/\mathbb{Z})$ of V, viewed as a $\mathbb{Z}[\chi]$-module via the rule $\alpha(f(v)) = f(\alpha v)$ for all $\alpha \in \mathbb{Z}[\chi]$ and v in V. Consider the natural map

$$\nu_n\colon\ W^\chi \longrightarrow (Y^\chi_p)^{\mathrm{dual}},$$

equal to the composite map $W^\chi \xrightarrow{v_p} W^\chi_p \to (X^\chi_p)^{\mathrm{dual}} \to (Y^\chi_p)^{\mathrm{dual}}$, where the second map is induced by the local Tate duality, and the third map is the dual of the natural inclusion $Y^\chi_p \hookrightarrow X^\chi_p$. Our proof of Theorem B divides naturally in two steps: first we bound uniformly the image of ν_n, and then its kernel.

PROPOSITION 7.1. *The order of the image of ν_n is bounded independently of n.*

Proof. Let $\mathcal{C}$ be the submodule of $H^1(H,A_{p^n})^\chi$ generated over $\mathbb{T}[\chi]$ by the Kolyvagin class c^χ_n. Let P be a point of W^χ. By Proposition 6.9, the classes in $\mathcal{C}$ have support only above p, and by definition P has empty support. Hence by Proposition 6.8, we have

$$\langle v_pP, x\rangle_p = 0 \quad \forall x \in \partial_p(\mathcal{C}).$$

By Proposition 6.10, the index of $\partial_p(\mathcal{C})$ in Y^χ_p is bounded independently of n. The result follows.

Recall that w is the sign defined in Section 6.

COROLLARY 7.2. *Suppose that $\chi = \bar\chi$. Then $A(H)^{\chi,w}$ is finite.*

Proof. When $\chi = \bar\chi$ the module Y^χ_p is identified with a submodule of $X^{\chi,w}_p$, whose index in $X^{\chi,w}_p$ is bounded independently of n. Since ν_n is τ-equivariant, Proposition 7.1 shows that the map $W^{\chi,w} \to (X^{\chi,w}_p)^{\mathrm{dual}}$ induced by ν_n has image bounded independently of n. Hence, by the τ-equivariance of the local Tate duality, the natural image of $A(H)^{\chi,w}$ in $A(H_p)^{\chi,w}\otimes\mathbb{Z}_p$ is finite. Since the natural map $A(H)^{\chi,w} \to A(H_p)^{\chi,w}\otimes\mathbb{Z}_p$ has finite kernel, the claim follows.

It is worth recording the following consequence of Corollary 7.2.

THEOREM 7.3. *Let E be a semistable elliptic curve, having a prime p of nonsplit multiplicative reduction. If $L(E/\mathbb{Q},1)$ is nonzero, then $E(\mathbb{Q})$ is finite.*

Proof. By [Wi] and [TW], E is modular. One chooses an auxiliary imaginary quadratic field K such that p is inert in K and $L(E/K,1)$ is nonzero.

This is possible by a theorem of Waldspurger [Wald]. In this case, the sign w is 1 and $E(H)^{\mathbf{1},w} = E(\mathbb{Q})$ is finite by Corollary 7.2.

Remark. Note that the proofs of Proposition 7.1, Corollary 7.2 and Theorem 7.3 do not use the Kolyvagin primes ℓ, but only the wildly ramified prime p. Bounding the kernel of ν_n requires a more involved argument, based on the use of Kolyvagin primes and the Chebotarev density theorem.

Preliminaries. We begin with proving two lemmas, which are used to establish the important technical Proposition 7.6, stating that a global cohomology class is essentially determined by its restriction at the Kolyvagin primes. The key ingredient in the proof of Proposition 7.6 is the Chebotarev density theorem.

From now on we denote the field F_n defined in the previous section by F. Recall that A_{p^n} is defined over F.

LEMMA 7.4. *The order of $H^1(G_{F/H}, A_{p^n})$ divides an integer b_1 independent of n.*

Proof. This is proved in [KL, Prop. 5.10] along the following lines. By a result of Serre [Se], the image Π of the Galois representation ρ_{p^n} contains a group Π_0 of scalar matrices equal to the natural image of $1 + b_1'\mathbb{Z}_p$ in $\tilde{\mathbb{T}}/p^n\tilde{\mathbb{T}}$, where b_1' is a nonzero integer independent of n. The Hochschild-Serre spectral sequence for $\Pi_0 \lhd \Pi$ gives the exact sequence

$$0 \to H^1(\Pi/\Pi_0, A_{p^n}^{\Pi_0}) \to H^1(\Pi, A_{p^n}) \to H^1(\Pi_0, A_{p^n}).$$

Now $A_{p^n}^{\Pi_0}$ is contained in $A_{b_1'}$, and $H^1(\Pi_0, A_{p^n})$ is contained in $A_{p^n}/b_1'A_{p^n}$, so that the order of $H^1(\Pi, A_{p^n})$ divides the order of $A_{b_1'}^2$. Since b_1' does not depend on n, the result follows upon taking $b_1 = \#A_{b_1'}^2$. □

LEMMA 7.5. *There exists a constant b_2 independent of n such that the following holds*:

(a) *Let U be a submodule of A_{p^n} which is stable under the action of $G_{F/H}$. Then we can find $u \in U^+$ so that b_2 annihilates the quotient $U/\mathbb{Z}[G_{F/H}]u$.*

(b) *Let U be a submodule of $\mathrm{Hom}_{\mathbb{T}}(\mathbb{T}[\chi]^2, A_{p^n})$ which is stable under the action of $\mathbb{Z}[\chi][G_{F/H}]$. Then we can find $u \in U^+$ so that b_2 annihilates the quotient $U/\mathbb{Z}[\chi][G_{F/H}]u$.*

Proof.

(a) By replacing U by its pre-image under the natural projection $T_p(A) \to A_{p^n}$, where $T_p(A)$ denotes the p-adic Tate module of A, we are reduced to proving the claim for a submodule U of $T_p(A)$, which is stable under the action of $\mathbb{Z}_p[G_H]$.

The Galois group G_H acts naturally on $T_p(A)$: Let R be the image of the group ring $\mathbb{Z}_p[G_H]$ in $\mathrm{End}(T_p(A))$. By a result of Serre [Se], R has finite index in $\mathrm{End}(T_p(A))$. Let $\tilde{\mathbb{T}}$ be as before the integral closure of $\mathbb{T}$ in its fraction field. Note that $T_p(A) \otimes_{\mathbb{T}} \tilde{\mathbb{T}}$ is isomorphic to $(\tilde{\mathbb{T}} \otimes \mathbb{Z}_p)^2$. Since $\mathbb{T}$ has finite index in $\tilde{\mathbb{T}}$, the natural inclusion of R in $\mathrm{End}(T_p(A)) \otimes \tilde{\mathbb{T}} \simeq M_2(\tilde{\mathbb{T}} \otimes \mathbb{Z}_p)$ has finite cokernel of order independent of n: let $b_2 \in \mathbb{Z}_p$ be an annihilator.

Let $\bar{U}$ be $M_2(\tilde{\mathbb{T}} \otimes \mathbb{Z}_p)U$, viewed as a submodule of $T_p(A) \otimes_{\mathbb{T}} \tilde{\mathbb{T}}$. Then b_2 annihilates $\bar{U}/U$, and $\bar{U} = M_2(\tilde{\mathbb{T}} \otimes \mathbb{Z}_p)\bar{u}$, for $\bar{u} \in \bar{U}^+$. Defining u to be $b_2\bar{u}$ concludes the proof of part (a).

(b) As before, we may replace U by its pre-image in $\mathrm{Hom}_{\mathbb{T}}(\mathbb{T}[\chi]^2, T_p(A))$. Let $\bar{U}$ be $M_2(\tilde{\mathbb{T}} \otimes \mathbb{Z}_p)U$, viewed as a submodule of

$$\mathrm{Hom}_{\mathbb{T}}(\mathbb{T}[\chi]^2, T_p(A)) \otimes_{\mathbb{T}} \tilde{\mathbb{T}} \simeq \mathrm{Hom}_{\tilde{\mathbb{T}}}(\tilde{\mathbb{T}}[\chi]^2, \tilde{\mathbb{T}}^2) \otimes \mathbb{Z}_p.$$

The last module is identified with $(\tilde{\mathbb{T}}^2 \otimes \mathbb{Z}_p[\chi]^\vee) \oplus (\tilde{\mathbb{T}}^2 \otimes \mathbb{Z}_p[\chi]^\vee) \simeq \mathcal{T}^2 \oplus \mathcal{T}^2$, where $\mathcal{T}$ is the ring $\tilde{\mathbb{T}} \otimes \mathbb{Z}_p[\chi]$, and the action of $M_2(\mathcal{T})$ on $\mathcal{T}^2$ is by left multiplication, viewing $\mathcal{T}^2$ as column vectors. Note that $\mathcal{T}$ is a semilocal principal ideal ring, equal to the product of discrete valuation rings which are finite extensions of $\mathbb{Z}_p$. By working component by component, we may, and will from now on, assume that $\mathcal{T}$ is a discrete valuation ring. Projection onto the second factor gives an exact sequence of $M_2(\mathcal{T})$-modules

$$0 \to \bar{U}' \to \bar{U} \to \bar{U}'' \to 0.$$

The modules $\bar{U}'$ and $\bar{U}''$ are either zero or isomorphic to $\mathcal{T}^2$ as $M_2(\mathcal{T})$-modules. If $\bar{U}''$ is zero, then $\bar{U} = \bar{U}'$. Assume that $\bar{U}''$ is nonzero, and let (ξ, η) be an element of $\bar{U}$ such that η generates $\bar{U}''$ as an $M_2(\mathcal{T})$-module. If the vectors ξ and η are not multiples of each other by an element of $\mathcal{T} \otimes \mathbb{Q}$, we may find a matrix $A \in M_2(\mathcal{T})$ such that $A(\xi, \eta) = (0, \eta)$. Thus, $M_2(\mathcal{T})(0, \eta)$ is a submodule of $\bar{U}$ isomorphic to $\bar{U}''$. If ξ and η are proportional by an element of $\mathcal{T} \otimes \mathbb{Q}$, the submodule $M_2(\mathcal{T})(\xi, \eta)$ is isomorphic to $\bar{U}''$. In all cases, we have

$$\bar{U} = \bar{U}' \oplus \bar{U}''$$

as $M_2(\mathcal{T})$-modules. A direct computation now shows that $\bar{U}$ is generated over $M_2(\mathcal{T})$ by an element of $\bar{U}^+$. The result follows as in the proof of part (a).

Let b denote the integer (independent of n) $b_1\#(\mathbb{T}[\chi]/2b_2\mathbb{T}[\chi])^2$.

PROPOSITION 7.6. *Let ξ_1 and ξ_2 be cohomology classes in $H^1(H, A_{p^n})^\chi$, and let $\mathcal{C}$ be the $\mathbb{T}[\chi]$-module they generate. Assume that $\mathcal{C}$ is stable under the action of τ, and, if $\chi = \bar{\chi}$, suppose further that ξ_1 and ξ_2 belong to different eigenspaces for the action of τ. Then there exist infinitely many Kolyvagin primes ℓ such that $\partial_\ell \xi_1 = \partial_\ell \xi_2 = 0$ and such that the order of the kernel of the* *natural map*

$$v_\ell\colon\ \mathcal{C} \to W_\ell^\chi$$

divides the constant b.

Proof. It is convenient to treat the case when $\chi = \bar{\chi}$ separately from the case when $\chi \neq \bar{\chi}$.

Suppose first that $\chi = \bar{\chi}$, so that ξ_1 and ξ_2 belong to different eigenspaces for τ. This enables us to prove the Proposition for the $\mathbb{T}$-modules generated by ξ_1 and ξ_2, considered one at a time. Let $\xi \in H^1(H, A_{p^n})^\chi$ be one of the cohomology classes ξ_1 and ξ_2, and let $\xi' \in \operatorname{Hom}(G_F, A_{p^n})^\chi$ be its natural image by restriction. Call L_ξ the Galois extension of F cut out by ξ', and $U_\xi = \operatorname{Gal}(L_\xi/F)$ its Galois group. The map ξ' is a $\mathbb{Z}[G_{F/H}]$-equivariant homomorphism, and it identifies U_ξ with a submodule of A_{p^n}. Let u be the element of U_ξ^+ produced by Lemma 7.5 (a) applied to the module U_ξ. By the Chebotarev density theorem, there exist infinitely many primes ℓ such that

$$\operatorname{Frob}_\ell(L_\xi/\mathbb{Q}) = [\tau u].$$

Observe that ℓ is a Kolyvagin prime relative to n, and that

$$\operatorname{Frob}_\ell(L_\xi/K) = [\tau u \tau u] = [u^2].$$

If an element φ of $\mathbb{T}\xi$ is in the kernel of the map v_ℓ, then its restriction φ' to G_F satisfies $\varphi'(\operatorname{Frob}_\lambda(L_\xi/F)) = 0$ for all primes λ of F above ℓ, and hence vanishes on $\mathbb{Z}[G_{F/H}]u^2$. The claim when $\chi = \bar{\chi}$ now follows from Lemma 7.4 and the choice of u.

Suppose that $\chi \neq \bar{\chi}$. Let $\mathcal{C}$ be the module generated over $\mathbb{T}[\chi]$ by the classes ξ_1 and ξ_2, and let $\mathcal{C}' \subset \operatorname{Hom}(G_F, A_{p^n})$ be the natural restriction of $\mathcal{C}$. Let L be the extension cut out by $\mathcal{C}'$, and let $U = G_{L/F}$. Consider the left and right nondegenerate Kummer pairing

$$(\ ,\ )\colon\ \mathcal{C}' \times U \to A_{p^n}.$$

The modules appearing in this pairing are each endowed with various structures coming from the natural action of $G_{F/K}$ and from Hecke operators. More precisely, $\mathcal{C}'$ is a $\mathbb{T}[\chi]$-module; the module U is a module over $\mathbb{Z}[\chi][G_{F/H}]$; and A_{p^n} is equipped with a natural action of $\mathbb{T}[G_{F/H}]$. The pairing $(\ ,\ )$ obeys the following compatibilities with respect to these actions:

(1) $(Tc, u) = T(c, u)$, for all $T \in \mathbb{T}$.
(2) $(c, gu) = g(c, u)$, for all $g \in G_{F/H}$.
(3) $(\alpha c, u) = (c, \bar{\alpha} u)$, for all $\alpha \in \mathbb{Z}[\chi]$.

Hence the Kummer pairing induces an injection of $\mathbb{Z}[\chi][G_{F/H}]$-modules

$$U \hookrightarrow \operatorname{Hom}_{\mathbb{T}}(\mathcal{C}', A_{p^n}) \hookrightarrow \operatorname{Hom}_{\mathbb{T}}(\mathbb{T}[\chi]^2, A_{p^n}).$$

The last injection is induced by our choice of the two $\mathbb{T}[\chi]$-module generators of $\mathcal{C}'$ coming from ξ_1 and ξ_2. Let u be the element of U^+ produced by Lemma 7.5 (b) applied to the module U. By the Chebotarev density theorem, there exist infinitely many primes ℓ such that

$$\mathrm{Frob}_\ell(L_\xi/\mathbb{Q}) = [\tau u].$$

Observe that ℓ is a Kolyvagin prime relative to n. The reader will check as in the case $\chi = \bar{\chi}$ that the kernel of the map from $\mathcal{C}$ to W_ℓ has order dividing b.

PROPOSITION 7.7. *The order of the kernel of ν_n is bounded independently of n.*

Proof. Let P be an element in $\ker(\nu_n)$. Let $\mathcal{C}$ be the submodule of $H^1(H, A_{p^n})^\chi$ generated over $\mathbb{T}[\chi]$ by P and the Kolyvagin class c_n^χ. Observe that if χ is a quadratic character, P and c_n^χ belong to different eigenspaces for the action of τ. Choose a Kolyvagin prime ℓ satisfying the conclusion of Proposition 7.6 applied to our module $\mathcal{C}$. By Kolyvagin's induction formula of Proposition 6.9 and our choice of ℓ, combined with Proposition 6.10, it follows that the ratio of the orders of $\mathbb{T}[\chi]\partial_\ell c_n(\ell)^\chi$ and Y_p^χ is bounded independently of n. Since $\partial_p c_n(\ell)^\chi$ belongs to Y_p^χ and P belongs to $\ker(\nu_n)$, it follows that $\langle v_p P, \partial_p(\mathbb{T}[\chi]c_n(\ell)^\chi)\rangle_p = 0$. Hence, by Proposition 6.8 we have

$$\langle v_\ell P, \partial_\ell(\mathbb{T}[\chi]c_n(\ell)^\chi)\rangle_\ell = 0.$$

By the Kolyvagin orthogonality relation of Proposition 6.9,

$$\langle v_\ell c_n^\chi, \partial_\ell(\mathbb{T}[\chi]c_n(\ell)^\chi)\rangle_\ell = 0.$$

Since by our choice of ℓ the orders of $\mathbb{T}[\chi]v_\ell c_n^\chi$ and Y_p^χ differ by an integer independent of n, the claim follows from a counting argument.

The proof of Theorem B now follows by combining Proposition 7.1 and 7.7.

Remark. (Suppose for simplicity that A is an elliptic curve.) If the sign of the functional equation of $L(A/K, \chi, s)$ is -1, then one can construct a canonical Heegner point in $A(H)^\chi$, and it is expected that this point has infinite order precisely when $L'(A/K, \chi, 1) \neq 0$. Assuming this, it is shown in [BD2] that the rank over $\mathbb{Z}[\chi]$ of $A(H)^\chi$ is equal to 1. The methods of [BD2] build directly on the fundamental ideas of Kolyvagin, which were used in [Ko] to handle the case $\chi = \bar{\chi}$.

8. Mordell-Weil groups in anticyclotomic towers

In this section, we prove that the Mordell-Weil group of A over very general anticyclotomic towers is finitely generated, under the assumption that "generically" A has analytic rank equal to zero. The precursor of this kind of investigations is Mazur's conjecture stating that $A(\mathbb{Q}_\infty)$ is finitely generated, $\mathbb{Q}_\infty$ being the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$. A proof of this conjecture, based on the use of cohomology classes made from Steinberg symbols of modular units, has been announced by K. Kato [K].

As before, let K be an imaginary quadratic field such that $L(A/K, s)$ vanishes to even order at $s = 1$. Fix primes $\ell_1, \ldots, \ell_k$ of good reduction for A, and let K_∞ denote the compositum of all the ring-class field extensions of K of conductor of the form $\ell_1^{n_1}, \ldots, \ell_k^{n_k}$, where $n_1, \ldots, n_k$ are nonnegative integers. Thus the Galois group of K_∞/K is equal to the product of a finite group by $\mathbb{Z}_{\ell_1} \times \cdots \times \mathbb{Z}_{\ell_k}$. We now prove Corollary D of the introduction.

THEOREM 8.1. *Assume that $L(A/K,\chi,1)$ is nonzero for all but finitely many finite order characters χ of $\mathrm{Gal}(K_\infty/K)$. Then the Mordell-Weil group $A(K_\infty)$ is finitely generated.*

Proof. Given χ factoring through a finite extension H of K and such that the special value $L(A/K, \chi, 1)$ is nonzero, Theorem B shows that $A(H)^\chi$ is finite. This implies that $\mathrm{rank}_{\mathbb{Z}} A(K_\infty)$ is finite. Theorem 8.1 now follows from Lemma 6.3.

Remark.

1. It is expected that the nonvanishing assumption on the $L(A/K, \chi, 1)$ always holds in our setting. See [Ro1] and [Ro2] for computations germane to our study.
2. Note that it is not necessary to assume, as customary in Iwasawa theory, that the ℓ_i are primes of ordinary reduction for A.
3. Let ℓ be a prime of good ordinary reduction for A, and let K_∞ be the anticyclotomic $\mathbb{Z}_\ell$-extension of an imaginary quadratic field K. Suppose that all the primes dividing N are split in K, so that the $L(A/K, \chi, s)$ vanishes to odd order at $s = 1$ for all finite order characters χ of $\mathrm{Gal}(K_\infty/K)$. The results of [B1] (where A is an elliptic curve) show, under a mild nontriviality assumption on a Iwasawa module built up from Heegner points, that the Pontryagin dual of $A(K_\infty) \otimes \mathbb{Q}_\ell/\mathbb{Z}_\ell$ and of $\mathrm{Sel}_{\ell^\infty}(A/K_\infty)$ has rank 1 over the Iwasawa algebra $\mathbb{Z}_\ell[\![\mathrm{Gal}(K_\infty/K)]\!]$. The method of proof of these results builds on Kolyvagin's theory.

UNIVERSITÁ DI PAVIA, ITALY
E-mail address: MASSIMO@DRAGON.IAN.PV.CNR.IT

MCGILL UNIVERSITY, MONTREAL, CANADA
E-mail address: DARMON@MATH.MCGILL.CA

REFERENCES

[B1] M. BERTOLINI, Selmer groups and Heegner points in anticyclotomic $\mathbb{Z}_p$-extensions, Compositio Math. **99** (1995), 153–182.

[B2] ———, Growth of Mordell-Weil groups in anticyclotomic towers, *Proc. Symp. Arithmetic Geometry*, F. Catanese, ed., Symposia Math. XXXVII, Cambridge Univ. Press, 1997.

[BD1] M. BERTOLINI and H. DARMON, Heegner points on Mumford-Tate curves, Inv. Math. **126** (1996) no. 3, 413–456.

[BD2] ———, Kolyvagin's descent and Mordell-Weil groups over ring class fields, J. für die Reine und angew. Math., **412** (1990), 63–74.

[Dag] H. DAGHIGH, Modular forms, quaternion algebras, and special values of L-functions, McGill University Ph.D. thesis, in progress.

[BFH] D. BUMP, S. FRIEDBERG, and J. HOFFSTEIN, Eisenstein series on the metaplectic group and nonvanishing theorems for automorphic L-functions and their derivatives, Annals of Math. **131** (1990), 53–127.

[DeRa] P. DELIGNE and M. RAPOPORT, *Les Schémas de Modules de Courbes Elliptiques*, LNM **349**, Springer-Verlag, New York, 1973, 143–316.

[Dr] V. G. DRINFELD, Coverings of p-adic symmetric regions, Funct. Anal. Appl. **10** (1976), 29–40.

[Edix] B. EDIXHOVEN, Appendix to this paper.

[GS] R. GREENBERG and G. STEVENS, p-adic L-functions and p-adic periods of modular forms, Inv. Math. **111** (1993), 407–447.

[Gr1] B. H. GROSS, Heights and special values of L-series, *CMS Conference Proc.*, H. Kisilevsky, and J. Labute, eds., Vol. 7, 1987.

[Gr2] ———, Kolyvagin's work on modular elliptic curves, In: *L-functions and Arithmetic*, J. Coates and M. Taylor, eds., Cambridge University Press, 1991, 235–256.

[Gr3] ———, On canonical and quasi-canonical liftings, Inv. Math. **84** (1986), 321–326.

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

[Groth] A. GROTHENDIECK, *Groupes de Monodromie en Geometrie Algébrique*, Sém. de Géom. Alg. 7 I, LNM **288**, Springer-Verlag, New York, 1972.

[K] K. KATO, Forthcoming work.

[KaMa] N. KATZ and B. MAZUR, *Arithmetic moduli of elliptic curves*, Annals of Math. Studies 108, Princeton Univ. Press, 1985.

[Ko] V. A. KOLYVAGIN, Euler Systems, In: *The Grothendieck Festschrift*, P. Cartier, et al., eds., vol. II, Progr. in Math. **87**, Birkhäuser, 1990, 435-483.

[KL] V. A. KOLYVAGIN and D. YU. LOGACHEV, Finiteness of the Shafarevich-Tate group and the group of rational points for some modular abelian varieties, Leningrad Math. J. **1** (1990), 1229–1253.

[LT] J. LUBIN and J. TATE, Formal moduli for one-parameter formal Lie groups, Bull. Soc. Math. Fr. **94** (1966), 49–60.

[Ma1] B. MAZUR, Rational points of abelian varieties with values in towers of number fields, Inv. Math. **18** (1972), 183–266.

[Ma2] ———, Modular curves and arithmetic, *Proc. of the Int. Congress of Math.*, 1983, Warszawa.

[MaRa] B. MAZUR and M. RAPOPORT, Behaviour of the Néron model of the jacobian of $X_0(N)$ at bad primes, Appendix to "Modular curves and the Eisenstein ideal", Pub. Math. I.H.E.S. **47** (1977), 173–186.

[MTT] B. MAZUR, J. TATE, and J. TEITELBAUM, On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer, Inv. Math. **84** (1986), 1–48.

[McC] W. McCallum, Kolyvagin's work on the structure of the Shafarevich-Tate group, In: *L-functions and Arithmetic*, J. Coates and M. Taylor, eds., Cambridge University Press, 1991.

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

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

[Ray1] M. Raynaud, Spécializations du foncteur de Picard, Publ. Math. I.H.E.S. **38** (1970), 27–76.

[Ray2] ———, Jacobienne des courbes modulaires et opérateurs de Hecke, Astérisque **196–197**, 1991.

[RT] K. Ribet and S. Takahashi, Parametrizations of elliptic curves by Shimura curves and classical modular curves, preprint.

[Ro1] D. Rohrlich, On L-functions of elliptic curves and anti-cyclotomic towers, Inv. Math. **75** (1984), 383–408.

[Ro2] ———, On L-functions of elliptic curves and cyclotomic towers, Inv. Math. **75** (1984), 409–423.

[Rob] D. Roberts, Shimura curves analogous to $X_0(N)$, Harvard Ph.D. Thesis, 1989.

[Se] J-P. Serre, *Resumé des cours de* 1984–85 *et* 1985–86, Annuaire du Collège de France, Paris, 1985 and 1986.

[TW] R. Taylor and A. Wiles, Ring theoretic properties of certain Hecke algebras, Annals of Math. **141** (1995), 553–572.

[Vi] M-F. Vignéras, *Arithmétique des algèbres des quaternions*, LNM **800**, Springer-Verlag, New York, 1980.

[Wa] W. C. Waterhouse, Abelian varieties over finite fields, Ann. Sci. Ecole Norm. Sup., Série **4** (1969), 521–560.

[Wald] J-L. Waldspurger, Correspondances de Shimura et quaternions, preprint.

[Wi] A. Wiles, Modular elliptic curves and Fermat's last theorem, Annals of Math. **141** (1995), 443–551.

(Received October 2, 1995)

Appendix

By Bas Edixhoven

1. Various descriptions of groups of connected components

Let R be a complete discrete valuation ring, with fraction field K and algebraically closed residue field k. Let X_K be a smooth, proper, geometrically connected curve over K. Suppose that X is a nodal model of X_K over R, i.e., X is a proper flat R-scheme, its generic fibre is X_K and the only singularities of the special fibre X_k are ordinary double points. We will suppose, for simplicity, that the irreducible components of X_k are smooth. Let J_K be the jacobian of X_K, J the Néron model over R of J_K, and $\Phi := J_k/J_k^o$ the group of connected components of J_k. Let $\widetilde{X} \to X$ be the minimal resolution of X. We associate a graph $\tilde{G}$ to $\widetilde{X}$ as follows. The set of vertices is the set $\tilde{\mathcal{C}}$ of irreducible components of $\widetilde{X}_k$, the set of edges is the set $\tilde{\mathcal{S}}$ of singular points of $\widetilde{X}_k$. The vertices meeting an edge x are the two irreducible components containing x. The elements of $\tilde{\mathcal{C}}$ are Cartier divisors on $\widetilde{X}$; hence for any two of them, say C and C', we have an intersection number $(C \cdot C')$. This intersection pairing defines a morphism of free $\mathbb{Z}$-modules:

$$(1.1) \qquad \alpha\colon \mathbb{Z}^{\tilde{\mathcal{C}}} \longrightarrow \mathbb{Z}^{\tilde{\mathcal{C}}}, \qquad f \mapsto \Bigl(C \mapsto \sum_{C'} (C \cdot C')\, f(C')\Bigr).$$

A theorem of Raynaud (see [1, Thm. 9.6/1]) says that Φ is canonically isomorphic to the homology of the complex:

$$(1.2) \qquad \mathbb{Z}^{\tilde{\mathcal{C}}} \xrightarrow{\ \alpha\ } \mathbb{Z}^{\tilde{\mathcal{C}}} \xrightarrow{\ +\ } \mathbb{Z},$$

where the map "+" sends f to $\sum_C f(C)$. The isomorphism works as follows. Let P be in $J(K)$, let D be a divisor on $\widetilde{X}$ such that P is the class of the restriction of D to X_K. Then P specializes to the element of Φ given by $C \mapsto (C \cdot D)$.

Grothendieck gave another description of Φ in terms of the monodromy pairing in [6, Thm. 11.5]; see also [7]. Our aim is to compare these two descriptions.

We choose an orientation on the graph $\tilde{G}$; i.e, we choose two maps s and t from $\tilde{\mathcal{S}}$ to $\tilde{\mathcal{C}}$ (s for source and t for target) such that for all edges x, $s(x)$ and $t(x)$ are the vertices meeting x. We get induced maps:

$$(1.3) \qquad s_*, t_*\colon \mathbb{Z}^{\tilde{\mathcal{S}}} \longrightarrow \mathbb{Z}^{\tilde{\mathcal{C}}}, \qquad s^*, t^*\colon \mathbb{Z}^{\tilde{\mathcal{C}}} \longrightarrow \mathbb{Z}^{\tilde{\mathcal{S}}},$$

where $(s_*f)C = \sum_{s(x)=C} f(x)$, $(s^*f)x = f(s(x))$, etc. Note that s^* is the adjoint, with respect to the standard inner products on $\mathbb{Z}^{\tilde{\mathcal{S}}}$ and $\mathbb{Z}^{\tilde{\mathcal{C}}}$, of s_*. With this notation, we can define the usual boundary and coboundary maps:

$$(1.4) \qquad d_* := t_* - s_*\colon \mathbb{Z}^{\tilde{\mathcal{S}}} \longrightarrow \mathbb{Z}^{\tilde{\mathcal{C}}}, \qquad d^* := t^* - s^*\colon \mathbb{Z}^{\tilde{\mathcal{C}}} \longrightarrow \mathbb{Z}^{\tilde{\mathcal{S}}}.$$

By definition, $\ker(d_*)$ is the homology group $\mathrm{H}_1(\tilde{G}, \mathbb{Z})$ and $\operatorname{coker}(d^*) = \mathrm{H}^1(\tilde{G}, \mathbb{Z})$ (the isomorphisms depend on the orientation chosen). Since $\tilde{G}$ is connected, $\ker(d^*) = \mathrm{H}^0(\tilde{G}, \mathbb{Z})$ is the diagonal in $\mathbb{Z}^{\tilde{\mathcal{C}}}$, and $\operatorname{coker}(d_*) = \mathrm{H}_0(\tilde{G}, \mathbb{Z})$ is $\mathbb{Z}$, via the map $+\colon \mathbb{Z}^{\tilde{\mathcal{C}}} \to \mathbb{Z}$. A simple computation shows:

$$(1.5) \qquad \alpha = t_*s^* + s_*t^* - s_*s^* - t_*t^* = -(t_* - s_*)(t^* - s^*) = -d_*d^*.$$

Let T be the maximal torus of J_k^o, and let $M := \mathrm{Hom}(T, \mathrm{G}_{\mathrm{m},k})$ be its character group. We denote the $\mathbb{Z}$-linear dual of M by $M^\vee$. It is well known, e.g.

[6, 12.3.7] or [1, §9.2, Ex. 8], that M and $\mathrm{H}_1(\tilde{G},\mathbb{Z})$ are canonically isomorphic. Let us give an isomorphism. The torus T is the kernel of the pull-back map $\mathrm{Pic}_{\widetilde{X}_k/k} \to \mathrm{Pic}_{\widetilde{X}_k^{\mathrm{nor}}/k}$, where nor: $\widetilde{X}_k^{\mathrm{nor}} \to \widetilde{X}_k$ is the normalization map. For each x in $\tilde{\mathcal{S}}$ we can distinguish the two elements of $\mathrm{nor}^{-1}\{x\}$ because one of them lies on $s(x)$ and one on $t(x)$; we denote these two points by s_x and t_x. Let f be a k^*-valued function on $\tilde{\mathcal{S}}$. Then we can construct a line bundle on $\widetilde{X}_k$ whose class is in $T(k)$ as follows: Take the trivial line bundle on $\widetilde{X}_k^{\mathrm{nor}}$, and, for each x in $\tilde{\mathcal{S}}$, identify the fiber at s_x with the fibre at t_x via multiplication by $f(x)$. This construction induces an isomorphism between $M^\vee$ and $\mathrm{H}^1(\tilde{G},\mathbb{Z})$ which does not depend on the orientation chosen. Passing to duals gives the desired isomorphism. From (1.5) we get the following commutative diagram:

(1.6)
$$\begin{tikzcd}
 & 0 \arrow[dr] & & & 0 \arrow[d] & & \\
 & & \mathbb{Z} \arrow[rr, "0"] \arrow[dr, "\mathrm{diag}"] & & M \arrow[d] \arrow[dr, "i"] & & \\
0 \arrow[r] & \mathbb{Z} \arrow[ur, "\mathrm{id}"] \arrow[rr, "\mathrm{diag}"] & & \mathbb{Z}^{\tilde{\mathcal{C}}} \arrow[r, "d^*"] \arrow[dr, "-\alpha"] & \mathbb{Z}^{\tilde{\mathcal{S}}} \arrow[r] \arrow[d, "d_*"] & M^\vee \arrow[r] \arrow[dd] & 0 \\
 & & & & \mathbb{Z}^{\tilde{\mathcal{C}}}[+] \arrow[dr] \arrow[dd] & & \\
 & & & & & \Phi \arrow[dl] \arrow[dr] & \\
 & & & & 0 & & 0.
\end{tikzcd}$$

As a consequence, we have the short exact sequence:

$$0 \longrightarrow M \xrightarrow{\;i\;} M^\vee \longrightarrow \Phi \longrightarrow 0. \tag{1.7}$$

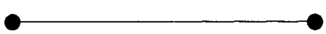
A computation shows that for all m_1 and m_2 in M:

$$(i(m_1))\,(m_2) = \sum_{x\in\tilde{\mathcal{S}}} m_1(x)\,m_2(x), \tag{1.8}$$

which is exactly the value at (m_1,m_2) of the monodromy pairing; see [6, Thm. 12.5] and [7]. Equations (1.7) and (1.8) together are Grothendieck's description of Φ. It follows that the diagram (1.6) gives a translation between Raynaud's and Grothendieck's descriptions of Φ.

Our next objective is to give the relation between the descriptions of M in terms of $\widetilde{X}$ and X. Let G be the graph associated to X: The set of vertices is the set $\mathcal{C}$ of irreducible components of X_k, the set of edges is the set $\mathcal{S}$ of singular points of X_k, and the vertices meeting an edge x are the two components containing x. Let r: $\widetilde{X} \to X$ denote the resolution morphism; it is the composition of blowing ups in the singular points. For x in $\mathcal{S}$ let $w(x)$ be the "width" of the singularity at x: If π is a uniformizer of R then, locally at x for the étale topology, X is given by the equation $uv = \pi^{w(x)}$. Let x be in $\mathcal{S}$. It is well known that $r^{-1}\{x\}$ is a chain of $w(x) - 1$ projective lines. In terms of graphs, this means that $\tilde{G}$ is obtained from G by replacing each edge x of G by a path of $w(x)$ edges:

(1.9)

 becomes 

It is clear that an orientation on G induces an orientation on $\tilde{G}$. We will assume that the orientation that we already have on $\tilde{G}$ comes from an orientation on G; the corresponding two maps $\mathcal{S} \to \mathcal{C}$ will also be denoted by s and t. It is also clear that $\mathrm{H}_1(G, \mathbb{Z})$ and $\mathrm{H}_1(\tilde{G}, \mathbb{Z})$ are canonically isomorphic, and that this isomorphism is compatible with the identifications of both of them with M (there is an isomorphism between M and $\mathrm{H}_1(G, \mathbb{Z})$ defined just as for $\tilde{G}$).

Picture (1.9) suggests for us to consider the following maps:

$$h_{\mathcal{C}}\colon \mathbb{Z}^{\mathcal{C}} \longrightarrow \mathbb{Z}^{\tilde{\mathcal{C}}}, \quad C \mapsto \tilde{C}, \qquad h_{\mathcal{S}}\colon \mathbb{Z}^{\mathcal{S}} \longrightarrow \mathbb{Z}^{\tilde{\mathcal{S}}}, \quad x \mapsto \sum_{y \in r^{-1}x} y, \tag{1.10}$$

with $\tilde{C}$ the strict transform of C. By construction, we get a commutative diagram:

$$\begin{array}{ccccccccccc} 0 & \longrightarrow & M & \longrightarrow & \mathbb{Z}^{\mathcal{S}} & \xrightarrow{d_*} & \mathbb{Z}^{\mathcal{C}} & \xrightarrow{+} & \mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle h_{\mathcal{S}}} & & \downarrow{\scriptstyle h_{\mathcal{C}}} & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 0 & \longrightarrow & M & \longrightarrow & \mathbb{Z}^{\tilde{\mathcal{S}}} & \xrightarrow{d_*} & \mathbb{Z}^{\tilde{\mathcal{C}}} & \xrightarrow{+} & \mathbb{Z} & \longrightarrow & 0. \end{array} \tag{1.11}$$

Dualization gives another such diagram:

$$\begin{array}{ccccccccccc} 0 & \longrightarrow & \mathbb{Z} & \xrightarrow{\mathrm{diag}} & \mathbb{Z}^{\tilde{\mathcal{C}}} & \xrightarrow{d^*} & \mathbb{Z}^{\tilde{\mathcal{S}}} & \longrightarrow & M^\vee & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle h_{\mathcal{C}}^\vee} & & \downarrow{\scriptstyle h_{\mathcal{S}}^\vee} & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 0 & \longrightarrow & \mathbb{Z} & \xrightarrow{\mathrm{diag}} & \mathbb{Z}^{\mathcal{C}} & \xrightarrow{d^*} & \mathbb{Z}^{\mathcal{S}} & \longrightarrow & M^\vee & \longrightarrow & 0. \end{array} \tag{1.12}$$

In this diagram $h_{\mathcal{S}}^{\vee}$ and $h_{\mathcal{C}}^{\vee}$ are given by:

$$(1.13) \qquad h_{\mathcal{S}}^{\vee}\colon \mathbb{Z}^{\tilde{\mathcal{S}}} \longrightarrow \mathbb{Z}^{\mathcal{S}}, \quad y \mapsto r(y), \qquad h_{\mathcal{C}}^{\vee}\colon \mathbb{Z}^{\tilde{\mathcal{C}}} \longrightarrow \mathbb{Z}^{\mathcal{C}}, \quad C \mapsto r_*(C),$$

where $r_*(C)$ is zero if $r(C)$ is a point, and $r(C)$ otherwise.

The map $h_{\mathcal{S}}$ from (1.10) is injective; the standard inner product on $\mathbb{Z}^{\tilde{\mathcal{S}}}$ induces the following inner product on $\mathbb{Z}^{\mathcal{S}}$:

$$(1.14) \qquad \langle \cdot, \cdot \rangle\colon \mathbb{Z}^{\mathcal{S}} \times \mathbb{Z}^{\mathcal{S}} \longrightarrow \mathbb{Z}, \quad (f,g) \mapsto \sum_{x \in \mathcal{S}} w(x)\, f(x)\, g(x).$$

It follows that, when we view M as a submodule of $\mathbb{Z}^{\mathcal{S}}$ and $M^{\vee}$ as a quotient of it, the map (1.7) $i\colon M \to M^{\vee}$ is given by:

$$(1.15) \qquad (i(m_1))(m_2) = \sum_{x \in \mathcal{S}} w(x)\, m_1(x)\, m_2(x).$$

The discussion up to here allows us to translate between Raynaud's description of Φ in terms of $\widetilde{X}$ and Grothendieck's description in terms of the Picard-Lefschetz formula for X.

2. Specialization of divisors of degree zero

We keep the notation of the previous section. Since X and $\widetilde{X}$ are proper over R, we can identify $X(K)$, $X(R)$ and $\widetilde{X}(R)$. The closure in $\widetilde{X}$ of an effective divisor on X_K is a Cartier divisor. Extending this by linearity we associate to each divisor D on X_K a Cartier divisor $\tilde{D}$ on $\widetilde{X}$.

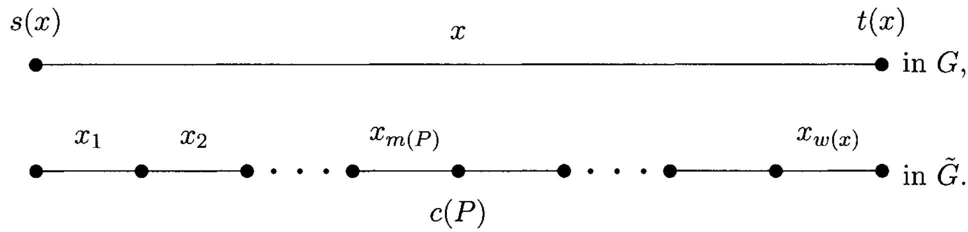
Suppose now that D is a divisor of degree zero on X_K. Then the class of D under linear equivalence corresponds to an element, say $[D]$, of $J(K) = J(R)$. Let $\phi(D)$ denote the image of $[D]$ in Φ. By Raynaud's description of Φ, (see (1.2)), $\phi(D)$ is given by the element $(C \mapsto (C \cdot \tilde{D}))$ of $\mathbb{Z}^{\tilde{\mathcal{C}}}$. Our aim is to get an expression for $\phi(D)$ in terms of $\mathbb{Z}^{\mathcal{C}}$ and $\mathbb{Z}^{\mathcal{S}}$. For simplicity, we suppose that D has support in the set of K-rational points of X (note that since X is semistable, one can always reduce to this case by extending K). Let us write:

$$(2.1) \qquad D = \sum_P n_P\, P,$$

where the sum ranges through the set $X(K)$ (of course, almost all n_P are zero, and their sum is zero). Each P in $X(K)$ specializes to a unique element $c(P)$ of $\tilde{\mathcal{C}}$, since $\widetilde{X}$ is regular. With this notation, $\phi(D)$ is given by the element $\sum_P n_P\, c(P)$ of $\mathbb{Z}^{\tilde{\mathcal{C}}}$.

Suppose now that P is such that $c(P)$ is not in $\mathcal{C}$. Let x in $\mathcal{S}$ be the image of $c(P)$ under the morphism r: $\widetilde{X} \to X$. Then we have the following situation:

(2.2)



Note that the integer $m(P)$ is defined by the condition that $c(P)$ is the $m(P)^{\text{th}}$ projective line in the chain of projective lines from $s(x)$ to $t(x)$ in $\widetilde{X}$.

Using (1.6) it follows that $\phi(D)$ is represented by the sum of the following two contributions:

$$(2.3)\qquad \sum_{c(P)\in\mathcal{C}} n_P\, c(P) + \sum_{c(P)\notin\mathcal{C}} n_P\, s(r(c(P))) \quad \text{and} \quad \sum_{c(P)\notin\mathcal{C}} n_P\, m(P)\, r(c(P)),$$

where the first contribution comes from the subgroup $\mathbb{Z}^{\mathcal{C}}[+]$ of $\mathbb{Z}^{\tilde{\mathcal{C}}}[+]$ and the second from $\mathbb{Z}^{\mathcal{S}}$.

The last thing we want to do in this section is to give a useful interpretation of the integers $m(P)$. Suppose that P in $X(K)$ is such that $c(P)$ is not in $\mathcal{C}$. Let x denote the element $r(c(P))$ of $\mathcal{S}$. Let π be a uniformizer of R. Let u and v be elements of the complete local ring $\widehat{\mathcal{O}}_{X,x}$ such that $\widehat{\mathcal{O}}_{X,x} = R[[u,v]]/(uv - \pi^{w(x)})$. By interchanging u and v, if necessary, we may and do suppose that (u,π) is the ideal of the branch $s(x)$. Let $c_0,\ldots,c_{w(x)}$ be the irreducible components of $r^{-1}x$, numbered such that $s(x_i) = c_{i-1}$ and $t(x_i) = c_i$. For the divisor $\operatorname{div}(v)$ of v on the completion of $\widetilde{X}$ along $r^{-1}x$ one has:

$$(2.4)\qquad \operatorname{div}(v) = \sum_{i=0}^{w(x)} i\, c_i.$$

To see this, note that blowing up $R[u,v]/(uv - \pi^n)$ in the ideal (u,v,π) gives the singularity $R[\pi^{-1}u, \pi^{-1}v]/(\pi^{-1}u\pi^{-1}v - \pi^{n-2})$. Equation (2.4) gives the following interpretation of $m(P)$:

$$(2.5)\qquad m(P) = P\cdot(m(P)c(P)) = P\cdot \sum_{i=0}^{w(x)} i\, c_i = P\cdot \operatorname{div}(v) = \operatorname{val}_R(P^*(v)),$$

where val_R denotes the valuation on R such that $\operatorname{val}_R(\pi) = 1$, and where P^* is the morphism of rings $\widehat{\mathcal{O}}_{X,x} \to R$ induced by the morphism of schemes P: $\operatorname{Spec}(R) \to X$.

3. Modular curves

The aim of this section is to give a moduli theoretic interpretation of the integer $m(P)$ in (2.5), in the case where X_K is a certain modular curve.

From now on, let p be a prime number. We suppose that K has characteristic zero and that k has characteristic p. Let X be the compactified coarse moduli scheme for the algebraic stack with objects $((\alpha\colon E \to E')/S/R, \beta)$, with S an R-scheme, E and E' elliptic curves over S, α an isogeny of degree p, and β some prime-to-p level structure (of a fixed type) on E. By [5, V.1] or [9, 13.4], the R-scheme X is proper and flat, X_K is smooth, and the only singularities of X_k are ordinary double points. We suppose that the level structure β is such that X_K is geometrically irreducible. Then X satisfies the hypotheses of the beginning of Section 1. The special fibre X_k has two irreducible components; we call them C_∞ and C_0, with C_∞ containing the cusp ∞ and C_0 the cusp 0. Over C_∞, the isogeny α is isomorphic to the relative Frobenius $F\colon E \to E^{(p)}$. Over C_0, α is isomorphic to the Verschiebung $V\colon (E')^{(p)} \to E'$. We choose the following orientation on the graph G of X: For every double point x of X_k, $s(x) = C_0$ and $t(x) = C_\infty$.

Let $((\alpha\colon E \to E')/R, \beta)$ be an R-valued point of the stack mentioned above, and let P in $X(R)$ denote the induced R-valued point of X. We suppose that P specializes to a singular point x of X_k; this just means that E_k is supersingular. Let A be the deformation ring of the object corresponding to x (we consider deformations over complete local R-algebras with residue field k). By [5, V, 1.19] or [9, Thms. 5.1.1 and 13.4.7], we can take y and z in A such that $A = R[[y,z]]/(yz-p)$. Let G be the group of k-automorphisms of the object corresponding to x. Then G acts on A, and by [5, I, 8.2.1] we have $\widehat{\mathcal{O}}_{X,x} = A^G$. The two branches at x of X_k are fixed by G; hence for all g in G, $g(y)/y$ and $g(x)/x$ are units in A. Let $\bar{G}$ be the image of G in $\mathrm{Aut}(A)$, and $|\bar{G}|$ its order. We get a subring $R[[u,v]]/(uv - p^{|\bar{G}|})$ of A^G by sending u to $\prod_{g\in\bar{G}} g(y)$ and v to $\prod_{g\in\bar{G}} g(z)$. This subring is normal, and the field extension given by the fraction fields of this subring and of A has degree $|\bar{G}|$. It follows that:

$$\widehat{\mathcal{O}}_{X,x} = R[[u,v]]/(uv - p^{|\bar{G}|}). \tag{3.1}$$

As in Section 2, we assume that u vanishes on the branch C_0, and v on C_∞. Let $((\alpha_{\mathrm{univ}}\colon E_{\mathrm{univ}} \to E'_{\mathrm{univ}})/A, \beta_{\mathrm{univ}})$ denote the universal deformation. Then z is an equation for the maximal closed subscheme of $\mathrm{Spec}(A/pA)$ over which E'_{univ} is isomorphic to $E^{(p)}_{\mathrm{univ}}$ (use that the analogous statement is true for the deformation ring over the Witt vectors of k; see [9, Thm. 13.4.7]). Since P in $X(R)$ arises from the object $((\alpha\colon E \to E')/R, \beta)$, the morphism $P^*\colon \widehat{\mathcal{O}}_{X,x} \to R$ is induced from a morphism $\tilde{P}^*\colon A \to R$. The element $\tilde{P}^*(z)$ is an equation for the maximal closed subscheme of $\mathrm{Spec}(R/pR)$ over which E' and $E^{(p)}$ are isomorphic. In other words, $\mathrm{val}_R(\tilde{P}^*(z))$ is the maximal integer n such that E' and $E^{(p)}$ are isomorphic over $R/\pi^n R$ (as before, π is a uniformizer of R). We have:

$$(3.2)\quad \mathrm{val}_R(P^*(v)) = \mathrm{val}_R(\tilde{P}^*(v)) = \sum_{g\in\tilde{G}} \mathrm{val}_R(\tilde{P}^*(g(z))) = |\tilde{G}|\cdot \mathrm{val}_R(\tilde{P}^*(z)).$$

Equation 3.1 implies that $w(x) = |\tilde{G}|\cdot \mathrm{val}_R(p)$. Putting everything together, we see that

$$(3.3)\qquad m(P) = \frac{w(x)}{\mathrm{val}_R(p)}\cdot \max\{n \leq \mathrm{val}_R(p) \mid E' \cong E^{(p)} \text{ over } R/\pi^n R\}.$$

4. Shimura curves

We will now adapt the arguments of Section 3 to the case of certain Shimura curves.

Let p and K be as in Section 3. Let $B_{\mathbb{Q}}$ be an indefinite quaternion algebra over $\mathbb{Q}$, of discriminant prime to p. Let B be a maximal order in $B_{\mathbb{Q}}$. First we consider the algebraic stack $\mathcal{M}$ with objects $(E/S/R, i\colon B \to \mathrm{End}_S(E), \beta)$, where S is an R-scheme, E/S an abelian scheme of relative dimension two, i a morphism of rings, and β some prime-to-p level structure. See [2] for the proof that this category is indeed an algebraic stack, and that it is proper and smooth of relative dimension one over R. We suppose that the level structure β is such that the fibres of $\mathcal{M}/R$ are geometrically irreducible. We combine [2, p. 54] with [3, III, 1.5] and see that each such E/S with B-action has a canonical principal polarization (the unique principal $*$-polarization).

In [5, Introduction, §7] it is explained how the results of [5] and [9] for modular curves imply results for $\mathcal{M}$. Let e be a nontrivial idempotent in $\mathbb{Z}_p\otimes B$ (recall that B is split at p). Let $(E/S, i, \beta)$ be an object of $\mathcal{M}$. Since $\mathbb{Z}_p \otimes B$ acts on the p-divisible group $E[p^\infty]$ of E, we get a direct sum decomposition

$$(4.1)\qquad E[p^\infty] = eE[p^\infty] \oplus (1-e)E[p^\infty].$$

The two terms in this decomposition are isomorphic, since e and $1-e$ are conjugates. The construction $G \mapsto eG$ defines an equivalence between the category of p-divisible S-groups with an action by B and the category of p-divisible S-groups. Via this equivalence, we can apply the Drinfeldian level structures of [9, §1.9] to $\mathcal{M}$. We will only consider the level structure corresponding to the $\Gamma_0(p)$ level structure in the modular curve case: It associates to $(E/S/R, i)$ the set of finite locally free subgroup schemes of rank p of $eE[p^\infty]$, or, equivalently, the set of isogenies α: $(E, i) \to (E', i')$ (up to isomorphism) of degree p^2, with $i'\colon B \to \mathrm{End}(E')$ and α compatible with i and i'.

Let X be the coarse moduli space for the algebraic stack with objects $((\alpha\colon E \to E')/S/R, \beta)$, with S an R-scheme, E and E' abelian S-schemes of relative dimension two, equipped with an action by B, α as isogeny of degree p^2, and β a prime-to-p level structure as above. Let x be a closed point of X_k. Let $\tilde{x} := ((\alpha\colon E \to E')/k, \beta)$ be the object corresponding to x. Then $eE[p^\infty]$ is a p-divisible group over k, of height two and with associated formal group of dimension one. The classification of p-divisible groups over algebraically closed fields implies that $eE[p^\infty]$ is isomorphic to the p-divisible group of some elliptic curve F over k (in fact, if $eE[p^\infty]$ is purely local, then any supersingular elliptic curve will do, otherwise any ordinary elliptic curve does the job). By the theorem of Serre and Tate [8] and the equivalence above, the deformation theory of $\tilde{x}$ is equivalent to that of $(F/k, e\ker(\alpha))$ (again, we consider deformations to complete local R-algebras). It follows that the deformation ring of $\tilde{x}$ is isomorphic to that of $(F/k, e\ker(\alpha))$. It follows that the only singularities of X_k are ordinary double points. One now easily shows, by constructing an ample divisor, that the algebraic space X is in fact a projective curve over R, satisfying the hypotheses of the beginning of Section 1. (An other way to see that X is a quasi-projective scheme is to prove that the morphism from $\mathcal{M}$ to the stack of two-dimensional principally polarized abelian varieties is representable and projective (use Hilbert schemes); see [4, §5.3].) We orient the graph G of X by demanding that for each singular point x of X_k, $s(x)$ is the branch on which α is generically étale. The following proposition is now a direct consequence of the results of the preceding sections.

PROPOSITION 4.2. *Let P in $X(R)$ be induced by an object $((\alpha\colon E \to E')/R,\beta)$. Suppose that P specializes to a singular point x of X_k. Then the integer $m(P)$ of* (2.5) *is given by:*

$$m(P) = \frac{w(x)}{\mathrm{val}_R(p)} \cdot \max\{n \leq \mathrm{val}_R(p) \mid E' \cong E^{(p)} \text{ over } R/\pi^n R\}.$$

INSTITUT MATHÉMATIQUE, CAMPUS DE BEAULIEU, RENNES, FRANCE
E-mail address: EDIX@CAMPAGNARDE.UNIV-RENNES1.FR

REFERENCES

[1] S. BOSCH, W. LÜTKEBOHMERT, and M. RAYNAUD, *Néron Models*, Ergebnisse der Mathematik und Ihre Grenzgebiete 3. Folge, Band 21, Springer (1990).

[2] J.-F. BOUTOT, *Variétés de Shimura et Fonctions L*, Breen and Labesse (eds.), Exposé III, Publications Mathématiques de l'université de Paris VII, 1979.

[3] J.-F. BOUTOT and H. CARAYOL, *Courbes de Shimura et Courbes Modulaires*, Exposé III, Astérisque **196–197**, SMF, 1991.

[4] H. Carayol, Sur la mauvaise réduction des courbes de Shimura, Comp. Math. **59** (1986), 151–230.

[5] P. Deligne and M. Rapoport, *Les schémas de modules des courbes elliptiques*, LNM **349**, Springer-Verlag, New York, 1973, 143–316.

[6] A. Grothendieck. SGA 7, exposé IX, LNM **288**, Springer-Verlag, New York 1972, 313–523.

[7] L. Illusie, Réalisation l-adique de l'accouplement de monodromie, d'après A. Grothendieck, Astérisque **196–197**, 1991, 27–44.

[8] N. Katz, *Serre-Tate local moduli*, LNM **868**, Springer-Verlag, New York 1981, 138–202.

[9] N. Katz and B. Mazur, *Arithmetic Moduli of Elliptic Curves*, Annals of Math. Studies 108, Princeton University Press, Princeton, NJ, 1985.

(Received October 2, 1995)