INDEPENDENCE OF POINTS ON ELLIPTIC CURVES ARISING FROM SPECIAL POINTS ON MODULAR AND SHIMURA CURVES, II: LOCAL RESULTS

ALEXANDRU BUIUM AND BJORN POONEN

Abstract. In the predecessor to this article, we used global equidistribution theorems to prove that given a correspondence between a modular curve and an elliptic curve A, the intersection of any finite rank subgroup of A with the set of CM-points of A is finite. In this article we apply local methods, involving the theory of arithmetic differential equations, to prove *quantitative* versions of a similar statement. The new methods apply also to certain infinite rank subgroups, and to the situation where the set of CM-points is replaced by certain isogeny classes of points on the modular curve. Finally, we prove Shimura curve analogues of these results.

This article has been published in *Compositio Math.* **145** (2009), no. 3, 566–602.

1. Introduction

Let $N > 3$. Let S be the modular curve $X_1(N)$ over $\overline{\mathbf{Q}}$. Let $\mathrm{CM} \subseteq S(\overline{\mathbf{Q}})$ be the set of *CM-points* on S. (See Section 2 for definitions.) Let A be an elliptic curve over $\overline{\mathbf{Q}}$. Given a morphism $S \to A$, we may map the CM-points on S to points on A, and ask what relations exist among them in the group law on A. More generally, we may consider a *modular-elliptic correspondence*, a pair of non-constant morphisms $S \xleftarrow{\Pi} X \xrightarrow{\Phi} A$ of smooth connected projective curves over $\overline{\mathbf{Q}}$, where S and A are as above. On the one hand, it is easy to construct some relations by using Hecke correspondences: see (A.4). On the other hand, the following special case of Theorem 2.1 of [8] says that not too many relations exist:

Theorem 1.1. *Let $S \xleftarrow{\Pi} X \xrightarrow{\Phi} A$ be a modular-elliptic correspondence and let $\Gamma \leq A(\overline{\mathbf{Q}})$ be a finite rank subgroup. Then $\Phi(\Pi^{-1}(\mathrm{CM})) \cap \Gamma$ is finite.*

(Recall Γ is said to be of *finite rank* if the quantity $\mathrm{rank}(\Gamma) := \dim_{\mathbf{Q}}(\Gamma \otimes \mathbf{Q})$ is finite.) Theorem 2.5 of [8] implies an analogous result when S is a Shimura curve and Π is the identity.

The aim of this paper is to prove local analogues of these results in which, roughly speaking, the field $\overline{\mathbf{Q}}$ is replaced by the completion $R := \hat{\mathbf{Z}}_p^{\mathrm{ur}}$ of the maximal unramified extension of the ring $\mathbf{Z}_p$ of p-adic integers, and the set CM is replaced by either the set CL of canonical lift points or by a fixed (partial) isogeny class. The new results represent an improvement over those in [8] in that they come with effective bounds and are valid for certain groups Γ of infinite rank.

Date: October 20, 2008.

2000 *Mathematics Subject Classification.* Primary 11G18; Secondary 14G20.

Key words and phrases. modular curve, Shimura curve, CM point, canonical lift, reciprocity law.

For historical background see Section 1.2 of [8], which comments on related results in [12, 24, 28, 31, 35, 45]. Although the present article is intended as a sequel to [8], it is logically independent of [8].

Our methods are quite different from those used in [8, 12, 24, 28, 31, 35, 45]. Indeed, our local results will be proved using the theory of arithmetic differential equations in the sense of [7]: see Section 3.9.

1.1. **Main theorems.** First we introduce the following local analogue of rank, in order to treat some infinite-rank groups as if they were of finite rank.

Definition 1.2. For any abelian group G define $G_{p\text{-div}} := G_{\text{tors}} + pG$. For any subgroup $\Gamma \leq G$ define

$$\operatorname{rank}_p^G(\Gamma) := \dim_{\mathbf{F}_p}\left(\frac{\Gamma}{\Gamma \cap G_{p\text{-div}}}\right).$$

Then

$$\begin{aligned}\operatorname{rank}_p^G(\Gamma) &\leq \dim_{\mathbf{Q}}(\Gamma \otimes \mathbf{Q}) =: \operatorname{rank}\Gamma,\\ \operatorname{rank}_p^G(\Gamma) &\leq \dim_{\mathbf{F}_p}(\Gamma \otimes_{\mathbf{Z}} \mathbf{F}_p).\end{aligned}$$

Assume that we are given a modular-elliptic correspondence $S \xleftarrow{\Pi} X \xrightarrow{\Phi} A$. For each sufficiently large prime $p \in \mathbf{Z}$ one can choose a model of this correspondence over $R := \hat{\mathbf{Z}}_p^{\text{ur}}$: see Section 3. We obtain maps $S(R) \xleftarrow{\Pi} X(R) \xrightarrow{\Phi} A(R)$. Let $\text{CL} \subset S(R)$ be the set of CL-points (canonical lift points); see Section 3.3 for more on the definition of CL. In an appropriate sense, CL is a subset of CM: see Theorem 4.4.

Theorem 1.3 (Finiteness for CL points in a subgroup)**.** *Suppose that $S \xleftarrow{\Pi} X \xrightarrow{\Phi} A$ is a modular-elliptic or Shimura-elliptic correspondence (see Section 2 for definitions) and assume that p is a sufficiently large good prime in the sense of Definition 3.3. Then there exists a constant c depending on p such that for any subgroup $\Gamma \leq A(R)$ with $r := \operatorname{rank}_p^{A(R)}(\Gamma) < \infty$, the set $\Phi(\Pi^{-1}(\text{CL})) \cap \Gamma$ is finite of cardinality at most cp^r.*

Remark 1.4. Corollary 3.19 makes c explicit in the case where Π is the identity and Φ is a modular parametrization in the sense of Definition 2.3.

Remark 1.5. There are interesting examples of subgroups $\Gamma \leq A(R)$ with $\operatorname{rank}_p^{A(R)}(\Gamma) < \infty$ and $\operatorname{rank}(\Gamma) = \infty$: indeed, if $\Gamma := \Gamma_0 + pA(R)$, where $\Gamma_0 \leq A(R)$ and $\operatorname{rank}(\Gamma_0) < \infty$, then Γ is such an example; see Remark 3.11 for more on this.

If S is a modular curve and Σ is a set of prime numbers, define the *Σ-isogeny class of Q in $S(R)$* as the set of all points in $S(R)$ corresponding to elliptic curves that admit an isogeny u to E such that all the prime divisors of $\deg(u)$ are in Σ; there is a similar definition in the Shimura curve case: see Section 3.7 for details. Also, if S is a modular curve, and $Q \in S(R)$ is an ordinary point, i.e., a point corresponding to an elliptic curve E with good ordinary reduction $\overline{E}$, then let $\mathcal{K}_Q := \operatorname{End}(\overline{E}) \otimes \mathbf{Q}$; for the similar definition in the Shimura curve case, see Section 3.4.

Theorem 1.6 (Finiteness of the intersection of an isogeny class with a subgroup)**.** *Assume that $S \xleftarrow{\Pi} X \xrightarrow{\Phi} A$ is a modular-elliptic or Shimura-elliptic correspondence and that p is* *a sufficiently large good prime. Let $Q \in S(R)$ be an ordinary point. Let Σ be the set of all rational primes that are inert in the imaginary quadratic field $\mathcal{K}_Q$. Let C be the Σ-isogeny class of Q in $S(R)$. Then there exists a constant c such that for any subgroup $\Gamma \leq A(R)$ with $r := \operatorname{rank}_p^{A(R)}(\Gamma) < \infty$ the set $\Phi(\Pi^{-1}(C)) \cap \Gamma$ is finite of cardinality at most cp^r.*

Theorems 1.1, 1.3, and 1.6 suggest the following "global" conjecture:

Conjecture 1.7. *Let $S \xleftarrow{\Pi} X \xrightarrow{\Phi} A$ be a modular-elliptic or Shimura-elliptic correspondence. Let $\Gamma \leq A(\overline{\mathbf{Q}})$ be a finite rank subgroup. Let $C \subset S(\overline{\mathbf{Q}})$ be an isogeny class. Then the set $\Phi(\Pi^{-1}(C)) \cap \Gamma$ is finite.*

1.2. **Reciprocity functions.** Our local results for CL points are proved via "reciprocity theorems" (e.g., Theorem 3.5), which transform relations between certain CL-points in A into additive relations between values of a certain "reciprocity function". More precisely, one part of Theorem 3.5 (with Remark 3.7 for terminology) shows that given a modular-elliptic correspondence $S \xleftarrow{\Pi} X \xrightarrow{\Phi} A$ and a model of X over R there exist an affine dense open subscheme $X^\dagger$ of this model and a p-adic formal function $\Phi^\dagger$ on $X^\dagger$ with non-constant reduction such that for any divisor $\sum m_i P_i$ supported on $\Pi^{-1}(\mathrm{CL}) \cap X^\dagger(R)$, we have $\sum m_i \Phi(P_i) \in A(R)_{\mathrm{tors}}$ if and only if $\sum m_i \Phi^\dagger(P_i) = 0 \in R$.

Some reciprocity results have analogues for (local) isogeny classes: see Sections 3.7 and 3.8.

On the other hand, Theorems A.2, A.1, and A.10 show that there is no reciprocity in the global setting.

1.3. **Structure of the paper.** We review basic definitions in Section 2. Section 3 states all our local results beyond those already in this introduction, and Section 4 proves them. Section 4 also reviews the necessary background from the theory of arithmetic differential equations. The non-existence of global reciprocity functions is relegated to an appendix.

Remark 1.8. The proofs of the modular and Shimura cases are parallel and share some common tools, but they are logically independent in the sense that it is not necessary to follow both cases to understand only one. A similar comment applies to results for CL points versus isogeny classes.

The following *leitfaden* may help the reader seeking a quick path through the proof of the modular case of Theorem 1.3 (the result for CL points). Theorem 1.3 follows from Theorem 3.5 and its immediate Corollary 3.8. The proof of Theorem 3.5 is sketched in Section 3.9. A reader accepting parts (4) and (5) of Lemma 4.7, the isomorphism (4.48), and formula (4.15) can go directly to the first paragraphs of Section 4.9 for a complete proof of Theorem 3.5 in the modular case.

Acknowledgments. While writing this paper, the authors were partially supported by NSF grants: A.B. by DMS-0552314, and B.P. by DMS-0301280 and DMS-0841321. We are indebted to M. Kim, J. H. Silverman, and J. F. Voloch for their remarks and suggestions. The paper also benefited greatly from the advice of a referee.

2. Basic definitions

2.1. **Modular curves.** Let $N \in \mathbf{Z}$ satisfy $N > 3$. Let $X_1(N)$ over $\overline{\mathbf{Q}}$ be the complete modular curve attached to the group $\Gamma_1(N)$. If $Y_1(N) \subset X_1(N)$ is the non-cuspidal locus then $Y_1(N)(\overline{\mathbf{Q}})$ is in bijection with the set of isomorphism classes of pairs (E,α) where E is an elliptic curve over $\overline{\mathbf{Q}}$ and $\alpha\colon \mathbf{Z}/N\mathbf{Z} \hookrightarrow E(\overline{\mathbf{Q}})$ is an injection.

Definition 2.1. A CM-*point* on the curve $S := X_1(N)$ is a point in $Y_1(N)(\overline{\mathbf{Q}})$ represented by a pair (E,α) such that E has complex multiplication, i.e., $\operatorname{End}(E) \neq \mathbf{Z}$. Let $\mathrm{CM} \subset S(\overline{\mathbf{Q}})$ be the set of CM-points on S.

Definition 2.2. A *modular-elliptic correspondence* is a pair of non-constant morphisms of smooth connected projective curves over $\overline{\mathbf{Q}}$, $S \xleftarrow{\Pi} X \xrightarrow{\Phi} A$, where $S = X_1(N)$ and A is an elliptic curve. From now on, we normalize Φ by fixing $x_\infty \in X(\overline{\mathbf{Q}})$ such that $\Pi(x_\infty) = \infty$ and requiring $\Phi(x_\infty) = 0$. Call $\Phi(\Pi^{-1}(\mathrm{CM})) \subset A(\overline{\mathbf{Q}})$ the set of CM-*points* on A.

Definition 2.3. Let $f = \sum a_n q^n$ be a newform. (Unless otherwise specified, newforms in this paper are of weight 2, on $\Gamma_0(N)$, and normalized ($a_1 = 1$), with Fourier coefficients in $\mathbf{Z}$.) (For terminology on modular forms we refer to [13].) The Eichler-Shimura construction [13] yields a $\mathbf{Q}$-morphism from $X_0(N)$ to an elliptic curve A_f. By a *modular parametrization attached to* f we mean a composition $X_1(N) \to X_0(N) \to A_f \to A$ where $X_1(N) \to X_0(N)$ is the usual map and $A_f \to A$ is any isogeny of elliptic curves over $\mathbf{Q}$. A modular-elliptic correspondence is said to *arise from a modular parametrization* if it is of the form $S \xleftarrow{\Pi} X \xrightarrow{\Phi} A$ where $S = X = X_1(N)$, $\Pi = \mathrm{Id}$, and Φ is a modular parametrization.

Remark 2.4. By work of Wiles and others [47, 44, 2], together with the Isogeny Theorem of Faltings [16], any elliptic curve A over $\mathbf{Q}$ has a modular parametrization.

Definition 2.5. The *isogeny class* C of a non-cusp $Q \in S(\overline{\mathbf{Q}})$ is the set of points in $S(\overline{\mathbf{Q}})$ such that the corresponding elliptic curve admits an isogeny to the elliptic curve corresponding to Q. (The isogeny is not required to respect the points of order N.)

2.2. **Shimura curves.** Let D be a non-split indefinite quaternion algebra over $\mathbf{Q}$. Fix a maximal order $\mathcal{O}_D$ once and for all. Let $X^D(\mathcal{U})$ be the Shimura curve attached to the pair $(D,\mathcal{U})$, where $\mathcal{U}$ is a sufficiently small compact subgroup of $(\mathcal{O}_D \otimes (\varprojlim \mathbf{Z}/m\mathbf{Z}))^\times$ such that $X^D(\mathcal{U})$ is connected: see [9, 48].

Definition 2.6. A *fake elliptic curve*[1] is a pair (E,i) consisting of an abelian surface E over $\overline{\mathbf{Q}}$ and an embedding $i\colon \mathcal{O}_D \to \operatorname{End}(E)$.

The set $X^D(\mathcal{U})(\overline{\mathbf{Q}})$ is in bijection with the set of isomorphism classes of fake elliptic curves equipped with a level $\mathcal{U}$ structure in the sense of [9, 48].

Definition 2.7. The classification of endomorphism algebras [30, p. 202] shows that for any fake elliptic curve (E,i), the algebra $(\operatorname{End} E)\otimes\mathbf{Q}$ is isomorphic to either D or $D\otimes\mathcal{K} \simeq M_2(\mathcal{K})$ for some imaginary quadratic field $\mathcal{K}$ embeddable in D. In the latter case, (E,i) is called *CM*; then E is isogenous to the square of an elliptic curve with CM by an order in $\mathcal{K}$. A *CM-point* of $S(\overline{\mathbf{Q}})$ is a point whose associated (E,i) is CM. Let $\mathrm{CM} \subset S(\overline{\mathbf{Q}})$ be the set of CM-points on S.

Definition 2.8. A *Shimura-elliptic correspondence* is a pair of non-constant morphisms of smooth connected projective curves over $\overline{\mathbf{Q}}$, $S \xleftarrow{\Pi} X \xrightarrow{\Phi} A$, where S is a Shimura curve as above and A is an elliptic curve. Call $\Phi(\Pi^{-1}(\mathrm{CM})) \subset A(\overline{\mathbf{Q}})$ the set of CM-*points on A*.

[1] In the literature this is sometimes called a "false elliptic curve".

Definition 2.9. For any $Q \in S(\overline{\mathbf{Q}})$, represented by a fake elliptic curve (E, i) with level $\mathcal{U}$-structure, the *isogeny class* C of Q in $S(\overline{\mathbf{Q}})$ consists of all points in $S(\overline{\mathbf{Q}})$ represented by fake elliptic curves (E', i') with level $\mathcal{U}$-structure such that there is an isogeny $E \to E'$ compatible with the $\mathcal{O}_D$-action (but not necessarily compatible with the level $\mathcal{U}$-structures).

3. Detailed exposition of the results

3.1. **Review of Witt rings.** Fix a prime p. Let $\mathbf{Z}_p$ be the ring of p-adic integers. Let $\mathbf{Z}_p^{\mathrm{ur}}$ be the maximal unramified extension of $\mathbf{Z}_p$. Let $R := \hat{\mathbf{Z}}_p^{\mathrm{ur}}$ be the completion of $\mathbf{Z}_p^{\mathrm{ur}}$. We set $k = R/pR$ and $K := R[1/p]$. Thus $k \simeq \overline{\mathbf{F}}_p$, and R is the Witt ring $W(k)$. Let $\mathrm{Fr}\colon k \to k$ be the automorphism $\mathrm{Fr}(x) := x^p$, and let $\phi\colon R \to R$ be the unique automorphism lifting Fr.

We will use the notion of a *canonical lift* (CL) abelian scheme over R: see Section 4.1 for the definition.

3.2. **Hecke correspondences.** For any prime l let $Y_1(N, l)$ be the affine curve over $\overline{\mathbf{Q}}$ parametrizing triples (E, α, H) in which (E, α), with $\alpha\colon \mathbf{Z}/N\mathbf{Z} \hookrightarrow E(\overline{\mathbf{Q}})$, represents a point in $Y_1(N)$ and $H \leq E(\overline{\mathbf{Q}})$ is an order-l subgroup intersecting $\alpha(\mathbf{Z}/N\mathbf{Z})$ trivially: see [11, p. 207]. Define *degeneracy maps* $\sigma_1, \sigma_2\colon Y_1(N, l) \to Y_1(N)$ by $\sigma_1(E, \alpha, H) := (E, \alpha)$ and $\sigma_2(E, \alpha, H) := (E/H, u \circ \alpha)$, where $u\colon E \to E/H$ is the quotient map.

Let $X_1(N, l)$ be the smooth projective model of $Y_1(N, l)$. The σ_i extend to $\sigma_i\colon X_1(N, l) \to X_1(N)$. Define the *Hecke operator* $T(l)_*$ on $\mathrm{Div}(X_1(N)(\overline{\mathbf{Q}}))$ by $T(l)_* D := \sigma_{2*}\sigma_1^* D$. For $P \in X_1(N)(\overline{\mathbf{Q}})$ write $T(l)_* P =: \sum_i P_i^{(l)}$; the sum involves $l + 1$ or l terms according as $l \nmid N$ or $l \mid N$. If in addition $f = \sum a_n q^n \in \mathbf{Z}[[q]]$ is a newform, then the divisor $\sum_i P_i^{(l)} - a_l P$ will be called a *Hecke divisor*.

3.3. **Conventions on modular-elliptic correspondences.** The $\mathbf{Z}[1/N]$-scheme $Y_1(N)$ represents the functor taking a $\mathbf{Z}[1/N]$-algebra B to the set of isomorphism classes of pairs (E, α) where E is an elliptic curve over B and $\alpha\colon (\mathbf{Z}/N\mathbf{Z})_B \to E$ is a closed immersion of group schemes. For each $P \in Y_1(N)(B)$, let (E_P, α_P) be a pair in the corresponding isomorphism class. The $\mathbf{Z}[1/N]$-scheme $S = X_1(N)$ is the Deligne-Rapoport compactification: see [13, pp. 78–81]. The base extension of S to $\mathbf{C}$ will also be denoted S. The cusp ∞ on $X_1(N)$ is defined over $\mathbf{Q}(\zeta_N)$, where ζ_N is a primitive N^{th} root of 1.

Remark 3.1. Some of the references we cite use a modular curve parametrizing elliptic curves with an embedding of μ_N instead of $\mathbf{Z}/N\mathbf{Z}$, but the two theories are isomorphic provided we work over $\mathbf{Z}[1/N, \zeta_N]$-algebras.

Assume that we are given a modular-elliptic correspondence $S \xleftarrow{\Pi} X \xrightarrow{\Phi} A$ with $S = X_1(N)$. We may assume that A comes from a model over $\mathcal{O}_{F_0}[1/Nm]$, and that X, S, Π, Φ come from models over $\mathcal{O}_F[1/Nm]$, where $F_0 \subseteq F$ are number fields, and $\mathcal{O}_{F_0}$ and $\mathcal{O}_F$ are their rings of integers, and $m \in \mathbf{Z}_{>0}$. Then $x_\infty = \Pi(\infty)$ has a model over $\mathcal{O}_{F_1}[1/Nm]$, where F_1 is a number field containing $F(\zeta_N)$.

If p is large enough to be unramified in F_1, then we fix once and for all an embedding of F_1 into K; then we obtain an embedding $\mathcal{O}_{F_1}[1/Nm] \subset R$. A point $P \in S(R)$ is called *ordinary* (respectively, a CL-*point*) if $P \in Y_1(N)(R)$ and E_P has ordinary reduction $\overline{E}_P$ (respectively, E_P is CL). If $P \in S(R)$ is ordinary let $\mathcal{K}_P$ be the imaginary quadratic field $\mathrm{End}(\overline{E}_P) \otimes \mathbf{Q}$.

Finally let CL be the set of all CL-points of $S(R)$. Call $\Phi(\Pi^{-1}(\mathrm{CL})) \subset A(R)$ the set of CL-*points* of A.

3.4. **Conventions on Shimura-elliptic correspondences.** Now suppose instead that S is a Shimura curve $X^D(\mathcal{U})$, where D and $\mathcal{U}$ satisfy the conditions in [9]; then for some $m \in \mathbf{Z}_{>0}$ the Shimura curve $S = X^D(\mathcal{U})$ is a $\mathbf{Z}[1/m]$-scheme with geometrically integral fibers, such that for any $\mathbf{Z}[1/m]$-algebra B the set $S(B)$ is in bijection with the set of isomorphism classes of triples (E, i, α) where (E, i) is a fake elliptic curve over B (i.e. E/B is an abelian scheme of relative dimension 2 and $i \colon \mathcal{O}_D \to \mathrm{End}(E/B)$ is an injective ring homomorphism) and α is a level $\mathcal{U}$ structure.

Assume that we are given a Shimura-elliptic correspondence $S \xleftarrow{\Pi} X \xrightarrow{\Phi} A$. With notation as in Section 3.3, Replacing m by a multiple if necessary, we may assume that A comes from a model over $\mathcal{O}_{F_0}[1/m]$ and that X, S, Π, Φ come from models over $\mathcal{O}_F[1/m]$, where $F_0 \subseteq F$ are number fields. Assuming that p is suitably large, we again fix an embedding $F \subset K$ hence we have an embedding $\mathcal{O}_F[1/m] \subseteq R$. A point $P \in S(R)$ is called *ordinary* (respectively a CL-*point*) if P corresponds to a triple (E_P, i_P, α_P) where E_P has ordinary reduction $\overline{E}_P$ (respectively E_P is CL). If $P \in S(R)$ is ordinary, let $\mathcal{K}_P$ be the imaginary quadratic field $\mathrm{End}(\overline{E}_P, \bar{i}_P) \otimes \mathbf{Q}$. Finally CL is the set of all CL-points of $S(R)$. Call $\Phi(\Pi^{-1}(\mathrm{CL})) \subset A(R)$ the set of CL-*points* of A.

3.5. **Reciprocity functions for** CL **points.**

Definition 3.2. Let p be a prime number. Let F_0 be a number field, and let v be a degree-1 place lying above p. Call v *anomalous* for an elliptic curve A over F_0 if the trace a_v of the p-power Frobenius on the reduction A mod v satisfies $a_v \equiv 1 \pmod{p}$. (See [27, p. 186].)

Let notation be as in Section 3.3 or Section 3.4.

Definition 3.3. A rational prime p is *good* (for our correspondence) if p splits completely in F_0, the elliptic curve A has good reduction at all primes $v|p$, and in the Shimura-elliptic case each $v|p$ is not anomalous for A.

Remark 3.4. The Chebotarev density theorem easily implies that there are infinitely many good primes.

Let p be sufficiently large and set $X_R := X \otimes R$. (More generally, throughout this paper the subscript R always means "base extension to R" and we use the same convention for any other ring in place of R. In particular, if p is a good prime, A_R comes from an elliptic curve $A_{\mathbf{Z}_p}$ over $\mathbf{Z}_p$ and we let a_p be the trace of the p-power Frobenius on $A_{\mathbf{F}_p}$.) Let $\bar{X} := X_k = X \otimes k$. For any $P \in X(R)$, let $\bar{P}$ denote the image of P in $\bar{X}(k)$. (More generally, throughout this paper, when we are dealing with a situation that is "localized at p", an upper bar always means "reduction mod p".) Let $\hat{X}_R$ the p-adic completion of X_R viewed as a formal scheme over R. (More generally, throughout this paper, an upper $\hat{}$ will denote "p-adic completion".) If $X^\dagger \subset X_R$ is an affine dense open subscheme then any global function $\Phi^\dagger \in \mathcal{O}(\hat{X}^\dagger) = \mathcal{O}(X^\dagger)\hat{}$ defines a map $\Phi^\dagger \colon X^\dagger(R) \to R$. The reduction $\overline{\Phi^\dagger} \in \mathcal{O}(\bar{X}^\dagger)$ induces a regular map $\overline{\Phi^\dagger} \colon \bar{X}^\dagger(k) \to k$.

Recall the group $A(R)_{p\text{-div}} := A(R)_{\mathrm{tors}} + pA(R)$.

Theorem 3.5 (Reciprocity functions for CL points)**.** *Assume that* $S \xleftarrow{\Pi} X \xrightarrow{\Phi} A$ *is a modular-elliptic or a Shimura-elliptic correspondence and that* p *is a sufficiently large good prime. Then there exist an affine dense open subscheme* $X^\dagger \subset X_R$ *and a function* $\Phi^\dagger \in \mathcal{O}(\hat{X}^\dagger)$ *with non-constant reduction* $\overline{\Phi^\dagger} \in \mathcal{O}(\bar{X}^\dagger) \setminus k$*, such that for any* $P_1, \dots, P_n \in \Pi^{-1}(\mathrm{CL}) \cap X^\dagger(R)$ *and any* $m_1, \dots, m_n \in \mathbf{Z}$ *we have*

$$\sum_{i=1}^n m_i \Phi(P_i) \in A(R)_{\mathrm{tors}} \iff \sum_{i=1}^n m_i \Phi^\dagger(P_i) = 0 \in R,$$

$$\sum_{i=1}^n m_i \Phi(P_i) \in A(R)_{p\text{-}div} \iff \sum_{i=1}^n m_i \overline{\Phi^\dagger}(\bar{P}_i) = 0 \in k.$$

Theorem 3.5 will be proved in Section 4. It is useful to compare Theorem 3.5 to Theorems A.1 and A.10.

Remark 3.6. As the proof of Theorem 3.5 will show, the functions $\Phi^\dagger$ will be functorially associated (in an obvious sense) to tuples $(X, S, A, \Pi, \Phi, \omega_A)$, where ω_A is a nonzero global 1-form on A defined over F_0.

Remark 3.7. Let $\mathcal{C} = \Pi^{-1}(\mathrm{CL}) \cap X^\dagger(R)$ and let $\mathrm{Div}(\mathcal{C})$ be the free abelian group generated by $\mathcal{C}$. Then one can consider the maps $\Phi_*\colon \mathrm{Div}(\mathcal{C}) \to A(R)/A(R)_{\mathrm{tors}}$ and $\Phi^\dagger_*\colon \mathrm{Div}(\mathcal{C}) \to R$ naturally induced by Φ and $\Phi^\dagger$ by additivity. Then the first equivalence in Theorem 3.5 says that $Ker(\Phi_*) = Ker(\Phi^\dagger_*)$. A similar description can be given for the second equivalence. There is a formal similarity between such a formulation of Theorem 3.5 and the way classical reciprocity laws are formulated in number theory and algebraic geometry. Indeed, in classical reciprocity laws one is usually presented with maps $\Phi : \mathcal{C} \to G$ and $\Phi^\dagger : \mathcal{C} \to G^\dagger$ from a set $\mathcal{C}$ of places of a global field to two groups G and $G^\dagger$ (typically a Galois group and a class group), and one claims the equality of the kernels of the induced maps $\Phi_* : \mathrm{Div}(\mathcal{C}) \to G$ and $\Phi^\dagger_* : \mathrm{Div}(\mathcal{C}) \to G^\dagger$.

Let us discuss some consequences of Theorem 3.5.

Corollary 3.8. *In the notation of Definition 1.2 and Theorem 3.5, we have*

$$\begin{aligned} \mathrm{rank}\left(\sum_{i=1}^n \mathbf{Z} \cdot \Phi(P_i)\right) &= \mathrm{rank}\left(\sum_{i=1}^n \mathbf{Z} \cdot \Phi^\dagger(P_i)\right) \\ \mathrm{rank}_p^{A(R)}\left(\sum_{i=1}^n \mathbf{Z} \cdot \Phi(P_i)\right) &= \dim_{\mathbf{F}_p}\left(\sum_{i=1}^n \mathbf{F}_p \cdot \overline{\Phi^\dagger}(\bar{P}_i)\right). \end{aligned}$$

Proof of Theorem 1.3. By Corollary 3.8, the $\mathbf{F}_p$-span of

$$\overline{\Phi^\dagger}(\overline{\Phi^{-1}(\Gamma) \cap \Pi^{-1}(\mathrm{CL}) \cap X^\dagger(R)})$$

has dimension $\leq r$ over $\mathbf{F}_p$. So

$$\#\overline{\Phi^{-1}(\Gamma) \cap \Pi^{-1}(\mathrm{CL}) \cap X^\dagger(R)} \leq p^r \deg(\overline{\Phi^\dagger}).$$

Now CL elliptic curves over R are uniquely determined, up to isomorphism, by their reduction mod p: see Theorem 4.3. Similarly, by loc. cit., if (E_1, i_1) and (E_2, i_2) are two fake elliptic curves such that E_1, E_2 are CL and $(\bar{E}_1, \bar{i}_1) \simeq (\bar{E}_2, \bar{i}_2)$ then $(E_1, i_1) \simeq (E_2, i_2)$. Thus

$$\Phi^{-1}(\Gamma) \cap \Pi^{-1}(\mathrm{CL}) \cap X^\dagger(R)$$

has at most $p^r \deg(\overline{\Phi^\dagger}) \cdot d_1 d_2$ elements, where $d_1 := \deg \Pi$ and d_2 is the number of level $\Gamma_1(N)$ structures (respectively, level $\mathcal{U}$ structures) on a given elliptic (respectively, fake elliptic) curve. Also, $\#\left(\Pi^{-1}(\mathrm{CL}) \setminus X^\dagger(R)\right) \leq d_1 d_2 d_3$, where $d_3 = \#\left(\Pi^{-1}(\overline{S}^{\mathrm{ord}}(k)) \setminus \bar{X}^\dagger(k)\right)$, where the *ord* superscript indicaes the ordinary locus. So

$$\#\Phi(\Pi^{-1}(\mathrm{CL})) \cap \Gamma \leq \#\Phi^{-1}(\Gamma) \cap \Pi^{-1}(\mathrm{CL}) \leq (p^r \deg(\overline{\Phi^\dagger}) + d_3) d_1 d_2, \tag{3.9}$$

which is at most cp^r, where $c := \deg(\overline{\Phi^\dagger}) + d_1 d_2 d_3$. □

Corollary 3.19 will make the bound in (3.9) explicit in the case where $S = X = X_1(N)$, $\Pi = \mathrm{Id}$, and Φ is a modular parametrization.

Remark 3.10. Let M be the algebraic closure of F in K. Then the study of $pA(M)$ is analogous to the study of *Wieferich places* in [43] and [46]: indeed, for $a \in \mathbf{Z}$ not divisible by p, the classical Wieferich condition $a^p \equiv a \pmod{p^2}$ is equivalent to $a \in M^{\times p}$, and $M^{\times p}$ is the analogue of $pA(M)$ for the multiplicative group $\mathbf{G}_m$.

Remark 3.11. Let Γ_0 be a finite-rank subgroup of $A(M)$, and let $\Gamma := \Gamma_0 + pA(M)$. Then $\operatorname{rank}_p^{A(R)}(\Gamma) < \infty$, so Theorem 1.3 applies to Γ.

On the other hand, we claim that $\operatorname{rank}(\Gamma) = \infty$. This follows from the following statement: If L is the compositum in $\overline{F}$ of all quadratic extensions of F that are unramified at all primes above p, then $A(L)$ is of infinite rank. To prove this, choose a Weierstrass equation $y^2 = f(x)$ for A, where $f(x)$ is a monic cubic polynomial with coefficients in the ring of integers $\mathcal{O}_F$ of F. Consider points with x-coordinate $x_n = 1/p^4 + n$ for $n \in \mathcal{O}_F$. Then $F(\sqrt{f(x_n)})$ is unramified at p since the equation $p^{12} f(x_n) \equiv 1 \pmod{p^4}$ implies by Hensel's lemma that $p^{12} f(x_n)$ is a square in the completion of F at any prime above p. Thus we get a collection of points in $A(L)$. We may inductively define a sequence of $n_i \in \mathcal{O}_F$ such that each $F(\sqrt{f(x_{n_i})})$ is ramified at a prime of F not ramifying in the field generated by the previous square roots, by choosing n_i so that $1/p^4 + n_i$ has valuation 1 at some prime of F splitting completely in the splitting field of f. By choosing the n_i sufficiently large, we may assume that the corresponding points $P_i \in A(L)$ have large height and hence are non-torsion. Now we claim that the Galois action forces $P_1, \ldots, P_m$ to be $\mathbf{Z}$-independent in $A(L)$. Indeed, if there were a relation $a_1 P_1 + \cdots + a_m P_m = 0$ then we could apply a Galois automorphism fixing all the P_i but P_1 to obtain $-a_1 P_1 + a_2 P_2 + \cdots + a_m P_m = 0$, and subtracting would show that $2a_1 P_1 = 0$, but P_1 is non-torsion, so $a_1 = 0$; similarly all a_i would be 0. Since m can be made arbitrarily large, $A(L)$ has infinite rank.

3.6. **Refinement of results on** CL **points for modular parametrizations.** Theorem 3.17 below is a refinement of Theorem 3.5 in the special case of a modular-elliptic correspondence $S \xleftarrow{\Pi} X \xrightarrow{\Phi} A$ arising from a modular parametrization attached to a newform $f = \sum a_n q^n$; recall that $S = X = X_1(N)$, $\Pi = \mathrm{Id}$, and we always assume f of weight 2, on $\Gamma_0(N)$, normalized, with rational Fourier coefficients. In this case we may (and will) take $F = F_0 = \mathbf{Q}$. Recall that $a_1 = 1$, that $a_n \in \mathbf{Z}$ for $n \geq 1$, and that for sufficiently large p, the coefficient a_p equals the trace of Frobenius on $A_{\mathbf{F}_p}$. One can ask if in this case the function $\Phi^\dagger$ also has a description in terms of eigenforms. This is indeed the case, as we shall explain below. Consider the series

$$f^{(-1)}(q) := \sum_{(n,p)=1} \frac{a_n}{n} q^n \in \mathbf{Z}_p[[q]]. \tag{3.12}$$

The series $f^{(-1)}(q)$ is called $f|R_{-1}$ in [38, p. 211]. Assume that $p \gg 0$ and that A_R has ordinary reduction. Then $a_p \not\equiv 0 \pmod{p}$. Let $up \in \mathbf{Z}_p^\times$ be the unique root in $p\mathbf{Z}_p$ of the equation $x^2 - a_p x + p = 0$; thus $\bar{a}_p \bar{u} = 1$. Let $V\colon \mathbf{Z}_p[[q]] \to \mathbf{Z}_p[[q]]$ be the operator $V(\sum c_n q^n) = \sum c_n q^{np}$. Define

$$f^{(-1)}_{[u]}(q) := \left(\sum_{i=0}^{\infty} u^i V^i\right) f^{(-1)}(q) = \sum_{i\geq 0} \sum_{(n,p)=1} u^i \frac{a_n}{n} q^{np^i} \in \mathbf{Z}_p[[q]]. \tag{3.13}$$

Then

$$-\left(\overline{f^{(-1)}_{[u]}(q)}\right)^p + \bar{a}_p \overline{f^{(-1)}_{[u]}(q)} = \bar{a}_p \overline{f^{(-1)}(q)}, \tag{3.14}$$

in $\mathbf{F}_p[[q]]$, where the bars denote reduction modulo p, as usual. The series $\overline{f^{(-1)}(q)}$ has a nice interpretation in terms of modular forms mod p. Indeed, recall from [17, pp. 451, 458] that if M_m is the k-linear space of modular forms over k on $\Gamma_1(N)$ of weight m then there is an injective *q-expansion map* $M_m \to k[[q]]$ and a *Serre operator* $\theta\colon M_m \to M_{m+p+1}$ that on q-expansions acts as $q\,\frac{d}{dq}$. Let $\bar{E}_{p-1} \in M_{p-1}$ be the reduction mod p of the modular form E_{p-1} over $\mathbf{Z}_{(p)}$ whose q-expansion in $\mathbf{Z}_{(p)}[[q]]$ is the normalized Eisenstein series of weight $p-1$; hence $\bar{E}_{p-1}$ is the Hasse invariant and has q-expansion 1 in $\mathbf{F}_p[[q]]$.

Define the affine curve

$$\overline{X_1(N)}^{\mathrm{ord}} := \overline{X_1(N)} \setminus \{\text{zero locus of } \bar{E}_{p-1}\}. = \overline{Y_1(N)}^{\mathrm{ord}} \cup \{\text{cusps}\}$$

where $\overline{Y_1(N)}^{\mathrm{ord}}$ is the open set of points in $\overline{Y_1(N)}$ represented by ordinary elliptic curves.

If $\alpha \in M_{m+w}$, and $\beta \in M_m$ is nonzero, call α/β a *weight-w quotient* of modular forms over k. A weight-0 quotient of modular forms is a rational function on $\overline{X_1(N)}$. In particular, $\theta^{p-2}\bar{f}, \bar{E}_{p-1}^p \in M_{p^2-p}$, and

$$\bar{f}^{(-1)} := (\theta^{p-2}\bar{f})/\bar{E}_{p-1}^p \tag{3.15}$$

is a regular function on $\overline{X_1(N)}^{\mathrm{ord}}$. Let $g \mapsto g_\infty$ be the natural q-expansion map $k(\overline{X_1(N)}) \to k((q))$. The corresponding point in $\overline{X_1(N)}(k((q)))$ will be called the *Fourier $k((q))$-point.* Then $\bar{f}^{(-1)}_\infty = \overline{f^{(-1)}(q)}$. For primes $l \neq p$, define the *Hecke operator* $T(l)\colon k[[q]] \to k[[q]]$ by $T(l)(\sum c_n q^n) = \sum c_{ln} q^n + \epsilon(l) l^{-1} \sum c_n q^{ln}$, where $\epsilon(l) = 0$ or 1 according as l divides N or not. Define the *U-operator* $U\colon k[[q]] \to k[[q]]$ by $U(\sum c_n q^n) := \sum c_{np} q^n$. By [17, p. 458], $\overline{f^{(-1)}(q)}$ is an eigenvector of T_l for every $l \neq p$; moreover, $\overline{f^{(-1)}(q)} \in \ker U$. Finally, for any open subscheme $X' \subset X_1(N)_R$ containing the ∞ section $[\infty]$ we have a natural injective q-expansion map $\mathcal{O}(X' \setminus [\infty])^\wedge \to R((q))^\wedge$, which we write as $G \mapsto G_\infty$. (See Section 4.4 for more details.)

Definition 3.16. An open subscheme of the form $X' \setminus [\infty]$ with X' as above will be called *standard.*

Let $j(x) \in k$ be the j-invariant of $x \in \overline{Y_1(N)}(k)$.

Theorem 3.17 (Explicit reciprocity functions for CL points)**.** *Assume, in Theorem 3.5, that $X = S = X_1(N)$, $\Pi = \mathrm{Id}$, and Φ is a modular parametrization attached to a newform f. Then one can choose $X^\dagger$ and $\Phi^\dagger$ in Theorem 3.5 such that*

(1) *$X^\dagger$ is standard and $\bar{X}^\dagger = \overline{Y_1(N)}^{\mathrm{ord}} \setminus \{x \mid j(x) = 0, 1728\}$.*

(2) *If A_R is not* CL *then* $\Phi^\dagger_\infty = f^{(-1)}(q)$. *In particular,* $\overline{\Phi^\dagger} = \bar{f}^{(-1)}$.

(3) *If A_R is* CL *then* $\Phi^\dagger_\infty = -uf^{(-1)}_{[u]}(q)$. *In particular,* $(\overline{\Phi^\dagger})^p - \bar{a}_p\overline{\Phi^\dagger} = \bar{f}^{(-1)}$.

In both cases, (2) and (3), the function $\overline{\Phi^\dagger}$ is integral over the integrally closed ring $\mathcal{O}(\overline{X_1(N)}^{\text{ord}})$ and belongs to the fraction field of $\mathcal{O}(\overline{X_1(N)}^{\text{ord}})$. So $\overline{\Phi^\dagger} \in \mathcal{O}(\overline{X_1(N)}^{\text{ord}})$. Theorem 3.17 will be proved in Section 4.

Remark 3.18. If A_R is CL, then Theorem 3.17(3) implies that $\overline{f^{(-1)}_{[u]}(q)}$ is the Fourier expansion of a rational function on $\overline{X_1(N)}$, hence of a quotient α/β where $\alpha, \beta \in M_\nu$ are modular forms defined over k of some weight ν. Is there a direct argument for this?

Corollary 3.19. *Let* $\Phi\colon X_1(N) \to A$ *be a modular parametrization and let* $\Gamma \leq A(R)$ *be a subgroup with* $r := \text{rank}_p^{A(R)}(\Gamma) < \infty$. *Then the set* $\Phi(\text{CL}) \cap \Gamma$ *is finite of cardinality at most*

$$\left[(2g - 2 + \nu) \cdot \frac{p^2 - p}{2} \cdot p^r + 2\lambda\right] \lambda,$$

where g is the genus of $X_1(N)$, ν is the number of cusps of $X_1(N)$, and λ is the degree of $X_1(N) \to X_1(1)$.

Proof. By Theorem 3.17 we have $d_1 = 1$, $d_2 = \lambda$, and $d_3 \leq 2\lambda$ in (3.9). So it will be enough to check that

$$\deg(\overline{\Phi^\dagger}) \leq (2g - 2 + \nu) \cdot \frac{p^2 - p}{2}. \tag{3.20}$$

Taking degrees in parts (2) and (3) of Theorem 3.17 yields either $\deg(\overline{\Phi^\dagger}) = \deg(\bar{f}^{(-1)})$ or $p\deg(\overline{\Phi^\dagger}) = \deg(\bar{f}^{(-1)})$. In both cases, $\deg(\overline{\Phi^\dagger}) \leq \deg(\bar{f}^{(-1)})$. Now (3.20) follows from the fact that the numerator and denominator of the fraction in (3.15) are sections of the line bundle $(\Omega^1(\text{cusps}))^{\frac{p^2-p}{2}}$, where Ω^1 is the cotangent bundle on $\overline{X_1(N)}$. □

We next discuss a uniqueness property for the function $\Phi^\dagger$ in Theorem 3.17. Let $S = X_1(N)$, let $X^\dagger \subset S$ be a standard open subscheme over R such that

$$\bar{X}^\dagger \subset \overline{Y_1(N)}^{\text{ord}} \setminus \{x | j(x) = 0, 1728\} \tag{3.21}$$

and define

(3.22)

$$\mathcal{P} := \{P \in \text{CL} \mid \bar{P} \text{ is not in the isogeny class of any of the } k\text{-points of } Y_1(N) \setminus X^\dagger\}.$$

Clearly $\overline{\mathcal{P}}$ is infinite. Let M be the algebraic closure of $\mathbf{Q}$ in K and let $\wp$ be the place of M above which pR lies. We have $\mathcal{P} \subset X^\dagger(\mathcal{O}_{M,\wp})$. Let $f = \sum a_n q^n$ be a newform. Let $\sum P_i^{(l)} - a_l P$ be the Hecke divisor on $S(\overline{\mathbf{Q}})$ associated to any $P \in \mathcal{P}$ and any prime $l \neq p$ (see Section 3.2). Then $P_i^{(l)} \in \text{CL} \cap X^\dagger(\mathcal{O}_{M,\wp})$. For $d \in (\mathbf{Z}/N\mathbf{Z})^\times$, let $\langle d \rangle$ be the diamond operator acting on $\overline{X_1(N)}$ and on $\mathcal{O}(\overline{X_1(N)}^{\text{ord}})$. Consider the k-linear space

$$\mathcal{F} := \left\{\overline{\Theta} \in \mathcal{O}(\overline{X_1(N)}^{\text{ord}}) \mid \langle d \rangle \overline{\Theta} = \overline{\Theta} \text{ for all } d \in (\mathbf{Z}/N\mathbf{Z})^\times \text{ and } U\overline{\Theta}(q) = 0\right\}, \tag{3.23}$$

where $\overline{\Theta}(q) \in k[[q]]$ is the Fourier expansion of $\overline{\Theta}$. Note that $\bar{f}^{(-1)} \in \mathcal{F}$.

Theorem 3.24 (Uniqueness of reciprocity functions for CL points)**.** *Let $S = X_1(N)$, and let $\Phi\colon S \to A$ be a modular parametrization attached to a newform $f = \sum a_n q^n$ and let p be a sufficiently large good prime. Assume that $X^\dagger \subset S$ is an open subscheme over R as in* (3.21)*. Let $\mathcal{P}$ be as in* (3.22)*. Then the following conditions on $\overline{\Theta} \in \mathcal{F}$ are equivalent.*

1) For any $P_1, \dots, P_n \in \mathrm{CL} \cap X^\dagger(R)$ and any integers $m_1, \dots, m_n$ we have

$$\sum_{i=1}^n m_i \Phi(P_i) \in A(R)_{p\text{-}div} \Longrightarrow \sum_{i=1}^n m_i \overline{\Theta}(\bar{P}_i) = 0 \in k.$$

2) For any $P \in \mathcal{P}$ and any prime $l \neq p$ we have

$$\sum \overline{\Theta}(\bar{P}_i^{(l)}) - a_l \overline{\Theta}(\bar{P}) = 0.$$

3) $\overline{\Theta} = \bar{\lambda} \cdot \overline{f^{(-1)}}$ for some $\bar{\lambda} \in k$.

Proof. Condition 1 implies condition 2 by (A.5). That condition 2 implies condition 3 will be proved in Section 4: see Lemma 4.83. Finally condition 3 implies condition 1 by Theorem 3.17. □

3.7. **Reciprocity functions and finiteness for isogeny classes.** Fix a set Σ of rational primes.

Suppose that $S = X_1(N)$. Let B be a $\mathbf{Z}[1/N]$-algebra. Let Q be a B-point of $Y_1(N)$, represented by (E_Q, α_Q). The Σ-*isogeny class* (respectively, the *prime-to-*Σ *isogeny class*) of Q in $S(B)$ is the set $C = C_Q \subset S(B)$ of all B-points of $Y_1(N)$ represented by $(E_{Q'}, \alpha_{Q'})$ such that there exists an isogeny $E_Q \to E_{Q'}$ of degree divisible only by primes in Σ (respectively, outside Σ). We do not require the isogeny to be compatible with α_Q and $\alpha_{Q'}$.

The definition for $S = X^D(\mathcal{U})$ is similar. Let B be a $\mathbf{Z}[1/m]$-algebra. Let $Q \in S(B)$ be represented by (E_Q, i_Q, α_Q). The Σ-*isogeny class* (respectively, the *prime-to-*Σ *isogeny class*) of Q in $S(B)$ is the set $C = C_Q \subset S(B)$ of all B-points of S represented by $(E_{Q'}, i_{Q'}, \alpha_{Q'})$ such that there exists an isogeny $E_Q \to E_{Q'}$, compatible with the $\mathcal{O}_D$-action, and of degree divisible only by primes in Σ (respectively, outside Σ). Again the isogeny need not respect α_Q and $\alpha_{Q'}$.

Let now S be either $X_1(N)$ or $X^D(\mathcal{U})$ and let C be a Σ-isogeny class where $p \notin \Sigma$ or a prime to Σ isogeny class where $p \in \Sigma$. Say that C is *ordinary* (respectively *CL*) if it contains an ordinary point (respectively a CL point); in this case all points in C are ordinary (respectively, CL).

Theorem 3.25 (Reciprocity functions mod p for isogeny classes)**.** *Assume that $S \xleftarrow{\Pi} X \xrightarrow{\Phi} A$ is a modular-elliptic or Shimura-elliptic correspondence, assume that p is a sufficiently large good prime, and assume C is an ordinary prime-to-p isogeny class in $S(R)$. Then there exist an affine dense open subscheme $X^\dagger \subset X$, a (not necessarily connected) finite étale cover $\pi\colon \bar{X}^\ddagger \to \bar{X}^\dagger$ of degree p, a regular function $\overline{\Phi^\ddagger} \in \mathcal{O}(\bar{X}^\ddagger)$ that is non-constant on each component of $\bar{X}^\ddagger$, and a map $\sigma\colon \Pi^{-1}(C) \cap X^\dagger(R) \to \bar{X}^\ddagger(k)$ such that $\pi(\sigma(P)) = \bar{P}$ for all P, and for any $P_1, \dots, P_n \in \Pi^{-1}(C) \cap X^\dagger(R)$ and any $m_1, \dots, m_n \in \mathbf{Z}$ we have*

$$\sum_{i=1}^n m_i \Phi(P_i) \in A(R)_{p\text{-}div} \quad \Longleftrightarrow \quad \sum_{i=1}^n m_i \overline{\Phi^\ddagger}(\sigma(P_i)) = 0 \in k. \tag{3.26}$$

Theorem 3.25 will be proved in Section 4.

Remark 3.27. 1) Again, as the proof will show, the maps $\overline{\Phi^{\ddagger}}$ and σ will have a functorial nature. In Theorem 3.25 σ is simply a map of sets, but the proof will show that σ has actually an algebro-geometric flavor.

2) Theorem 3.25 is an analogue of the second equivalence in Theorem 3.5. Is there also an isogeny-class analogue of the first equivalence in Theorem 3.5?

3) The sum in the right half of (3.26) may be viewed as a function $\eta^{\ddagger}$ on $\overline{X^{\ddagger}}^{n}$ evaluated at $(\sigma(P_1), \dots, \sigma(P_n))$. If the value is zero, then so is $\eta^{\dagger}(\bar{P}_1, \dots, \bar{P}_n)$, where $\eta^{\dagger}$ is the norm of $\eta^{\ddagger}$ in the degree-p^n extension $\mathcal{O}\left(\overline{X^{\ddagger}}^{n}\right)$ of $\mathcal{O}\left(\overline{X^{\dagger}}^{n}\right)$. Here $\eta^{\dagger}$ may be expressed as a polynomial in the m_i and the coefficients of the characteristic polynomial of multiplication-by-$\Phi^{\ddagger}$ on the locally free $\mathcal{O}(\overline{X^{\dagger}})$-algebra $\mathcal{O}(\overline{X^{\ddagger}})$. Thus the left half of (3.26) implies a statement expressible in terms of evaluation of functions on $\overline{X^{\dagger}}$ instead of $\overline{X^{\ddagger}}$. Theorem 3.32(4) will show that $\eta^{\dagger}$ is not always zero (consider the case $n = 1$, for example), so the statement is not always vacuous.

Theorem 3.25 trivially implies

Corollary 3.28. *In the notation of Theorem 3.25 we have*

$$\operatorname{rank}_p^{A(R)}\left(\sum_{i=1}^{n} \mathbf{Z} \cdot \Phi(P_i)\right) = \dim_{\mathbf{F}_p}\left(\sum_{i=1}^{n} \mathbf{F}_p \cdot \overline{\Phi^{\ddagger}}(\sigma(P_i))\right).$$

Just as Corollary 3.8 implied Theorem 1.3, Corollary 3.28 applied to subsets $\{P_1, \dots, P_n\}$ of $\Phi^{-1}(\Gamma) \cap \Pi^{-1}(C) \cap X^{\dagger}(R)$ implies the first conclusion in

Corollary 3.29. *Assume $S \xleftarrow{\Pi} X \xrightarrow{\Phi} A$ is a modular-elliptic or a Shimura-elliptic correspondence and assume p is a sufficiently big, good prime. Let C be an ordinary prime-to-p isogeny class in $S(R)$. Then there exists a constant c such that for any subgroup $\Gamma \leq A(R)$ with $r := \operatorname{rank}_p^{A(R)}(\Gamma) < \infty$ the set $\overline{\Phi(\Pi^{-1}(C)) \cap \Gamma} \subseteq A(k)$ is finite of cardinality at most cp^r. In particular, the set $\Phi(\Pi^{-1}(C)) \cap A(R)_{\mathrm{tors}}$ is finite.*

The first conclusion of Corollary 3.29 implies the last because the reduction map $A(R)_{\mathrm{tors}} \to A(k)$ is injective for large p.

One can ask if the set $\Phi(\Pi^{-1}(C)) \cap \Gamma$ is finite for every Γ with $\operatorname{rank}_p^{A(R)}(\Gamma) < \infty$. Theorem 1.6 represents a partial result in this direction, with certain Σ-isogeny classes instead of prime-to-p isogeny classes. Corollary 3.29 will be used to prove Theorem 1.6 in Section 4.9.

3.8. **Refinement of results on isogeny classes for modular parametrizations.** Suppose that $S \xleftarrow{\Pi} X \xrightarrow{\Phi} A$ arises from a newform $f = \sum a_n q^n$. Our goal in this subsection is to state Theorem 3.32, which describes the cover $\overline{X^{\ddagger}}$ and the function $\overline{\Phi^{\ddagger}}$ explicitly in this case.

Let $I_1(N)$ be the Igusa curve from pp. 460–461 of [17], except that we view $I_1(N)$ as a smooth projective integral curve. It is a Galois cover of $\overline{X_1(N)}$ ramified only over supersingular points, and the Galois group is naturally isomorphic to $\mathbf{F}_p^{\times}$. Let $J := I_1(N)/\langle -1 \rangle$ be the intermediate cover of degree $(p-1)/2$ obtained by taking the quotient of $I_1(N)$ by the involution corresponding to $-1 \in \mathbf{F}_p^{\times}$. We will describe $\overline{X^{\ddagger}}$ in terms of J. There is a point ∞ on each of these covers that is unramified over $\infty \in \overline{X_1(N)}$. In particular, rational functions on $I_1(N)$ and J have Fourier expansions in $k((q))$.

Let

$$f^{(0)}(q) := \sum_{(n,p)=1} a_n q^n \in \mathbf{Z}_p[[q]]. \tag{3.30}$$

(The series $f^{(0)}(q)$ is called $f|R_0$ in [38, p. 115].) Let

$$f^{(0)}_{[a_p]}(q) := \left(\sum_{i=0}^{\infty} a_p^i V^i\right) f^{(0)}(q) = \sum_{i=0}^{\infty} \sum_{(n,p)=1} a_p^i a_n q^{np^i} \in \mathbf{Z}_p[[q]]. \tag{3.31}$$

Corollary 4.50 and Lemma 4.52 will show that for $p \gg 0$, the series $\overline{f^{(0)}_{[a_p]}(q)}$ is the Fourier expansion of some $\eta \in k(J)$. For a constant $\bar{\lambda} \in k$ to be specified later, define

$$\overline{\Phi^{\dagger\dagger}} := \begin{cases} \bar{\lambda}\eta^{p^2} - \bar{a}_p \eta^p, & \text{if } A_R \text{ is not CL} \\ \eta^p, & \text{if } A_R \text{ is CL.} \end{cases}$$

Theorem 3.32 (Explicit reciprocity functions mod p for isogeny classes)**.** *Assume, in Theorem 3.25, that $S \xleftarrow{\Pi} X \xrightarrow{\Phi} A$ arises from a modular parametrization attached to a newform f on $\Gamma_0(N)$. Then there exists $\bar{\lambda} \in k^\times$ such that $X^\dagger$, $\overline{X^\ddagger}$, and $\overline{\Phi^\ddagger}$ can be chosen to satisfy:*

1) The cover $\overline{X^\ddagger}$ of $\overline{X^\dagger}$ is a disjoint union $\overline{X^0} \coprod \overline{X^+} \coprod \overline{X^-}$, where $\overline{X^0} \simeq \overline{X^\dagger}$ is the trivial cover and $\overline{X^+}$ and $\overline{X^-}$ are each isomorphic to the inverse image of $\overline{X^\dagger}$ under $J \to \overline{X_1(N)}$.

2) The restrictions of $\overline{\Phi^\ddagger}$ to $\overline{X^0}$, $\overline{X^+}$, $\overline{X^-}$ equal

$$\overline{\Phi^\dagger}, \qquad \overline{\Phi^\dagger} + \lambda_+ \overline{\Phi^{\dagger\dagger}}, \qquad \overline{\Phi^\dagger} + \lambda_- \overline{\Phi^{\dagger\dagger}},$$

respectively, where $\lambda_\pm \in k$ are such that $\lambda_+^{(p-1)/2}, \lambda_-^{(p-1)/2}$ are the two square roots of $\bar{\lambda}$.

Theorem 3.32 will be proved in Section 4.

Corollary 3.33. *Let notation be as in Theorem 3.32. The characteristic polynomial of the endomorphism "multiplication by $\overline{\Phi^\ddagger}$" in the locally free $\mathcal{O}(\overline{X^\dagger})$-algebra $\mathcal{O}(\overline{X^\ddagger})$ is*

$$x^p - \bar{\lambda} h^2 x + (\bar{\lambda} h^2 \overline{\Phi^\dagger} - (\overline{\Phi^\dagger})^p),$$

where $h := \left(\overline{\Phi^{\dagger\dagger}}\right)^{(p-1)/2} \in k(\overline{X_1(N)})$.

Proof. The characteristic polynomial of $\overline{\Phi^\ddagger} - \overline{\Phi^\dagger}$ equals

$$x\left(x^{(p-1)/2} - \lambda_+^{(p-1)/2}\overline{\Phi^{\dagger\dagger}}^{(p-1)/2}\right)\left(x^{(p-1)/2} - \lambda_-^{(p-1)/2}\overline{\Phi^{\dagger\dagger}}^{(p-1)/2}\right) = x^p - \bar{\lambda} h^2 x.$$

In this, replace x by $x - \overline{\Phi^\dagger}$. □

3.9. **Strategy of proofs.** The proof of our local results will be an application of the theory of δ-characters [3, 4] and δ-modular forms [5, 6]. These two types of objects are special cases of *arithmetic differential equations* in the sense of [7]. Section 4 reviews the facts from this theory that are necessary for the proof. As a sample of our strategy let us explain, very roughly, the idea of our proof of Theorem 3.5. Assume for simplicity that we are dealing with a modular-elliptic correspondence $S \xleftarrow{\Pi} X \xrightarrow{\Phi} A$ arising from a modular parametrization attached to a newform f. Following [3] consider the *Fermat quotient operator* $\delta\colon R \to R$ defined by $\delta x := (\phi(x) - x^p)/p$, where $\phi\colon R \to R$ is the lift of Frobenius. We view δ

as an analogue of a derivation operator with respect to p. Recall from [3] that if Y is any smooth scheme over R then a function $g\colon Y(R) \to R$ is called a *δ-function of order r* if it is Zariski locally of the form $P \mapsto G(x, \delta x, \dots, \delta^r x)$, where G is a restricted power series with R-coefficients and $x \in R^N$ is a tuple of affine coordinates of P in some N-dimensional affine space. If A is our elliptic curve then by [3] there exists a δ-function of order 2, $\psi\colon A(R) \to R$, which is also a group homomorphism; ψ is called in [3] a *δ-character* and may be viewed as an arithmetic analogue of the "Manin map" [25, 26]. Consider the composition $f^\sharp = \psi \circ \Phi\colon X(R) \to R$. On the other hand, the theory of δ-modular forms [5] yields an open subset $X^\dagger$ of S and a δ-function of order 1, $f^\flat\colon X^\dagger(R) \to R$, that vanishes at all CL-points: see Lemma 4.37 and (4.39). Then we prove that there exist δ-functions of order 2, denoted $h_0, h_1 : X^\dagger(R) \to R$, such that the δ-function

$$\Phi^\dagger := f^\sharp - h_0 \cdot f^\flat - h_1 \cdot \delta \circ f^\flat$$

has order 0, or equivalently is a formal function in the usual sense of algebraic geometry. (Intuitively, in the system of "arithmetic differential equations" $f^\sharp = f^\flat = 0$ one can eliminate all the "derivatives" of the unknowns.) It follows that $f^\sharp$ and $\Phi^\dagger$ have the same value at each CL-point P_i. So

$$\sum m_i \Phi^\dagger(P_i) = \sum m_i f^\sharp(P_i) = \psi(\sum m_i \Phi(P_i)).$$

By the arithmetic analogue in [3, 4] of Manin's Theorem of the Kernel [25, 26], $\psi(\sum m_i \Phi(P_i))$ vanishes if and only if $\sum m_i \Phi(P_i)$ is torsion. (Actually, for our application to Theorem 1.3 we need only the "if" part, which does not require the analogue of the Theorem of the Kernel.) On the other hand we will check that $\overline{\Phi^\dagger} \notin k$ by looking at Fourier q-expansions, and this will complete the proof of the first equivalence in Theorem 3.5 in the special case we considered.

In particular, our proof of the (effective) finiteness of $\Phi(\mathrm{CL}) \cap \Gamma$ in the case $\Gamma = A(R)_{\mathrm{tors}}$ can be intuitively described as follows. The points of CL are solutions of the "arithmetic differential equation" $f^\flat = 0$ whereas the points of $\Phi^{-1}(\Gamma)$ are solutions of the "arithmetic differential equation" $f^\sharp = 0$. Hence the points of $\mathrm{CL} \cap \Phi^{-1}(\Gamma)$ are solutions of the system of "arithmetic differential equations" $f^\flat = f^\sharp = 0$. By what was said above one can eliminate, in this system, the "derivatives" of the unknowns and hence one is left with a (non-differential) algebraic equation mod p, whose "degree" can be estimated. There are only finitely many solutions to this algebraic equation and their number is effectively bounded by the "degree".

4. Proofs

Fix a prime $p \geq 5$. Recall that $R = \hat{\mathbf{Z}}_p^{\mathrm{ur}}$, $k = R/pR$, $K := R[1/p]$, and $\phi\colon R \to R$ is the Frobenius automorphism.

4.1. **Review of CL and CM points.**

This section reviews facts we need about CL abelian schemes and their relation with CM points; see [22, 15, 29]. Expert readers should skip this discussion.

Definition 4.1. An abelian scheme E/R is CL (a *canonical lift*) if its reduction $\bar{E} := E \otimes k$ is ordinary and there exists an R-homomorphism $E \to E^\phi := E \otimes_{R,\phi} R$ whose reduction mod p is the relative Frobenius k-homomorphism $\bar{E} \to \bar{E}^{\mathrm{Fr}} := \bar{E} \otimes_{k,\mathrm{Fr}} k$.

Theorem 4.2. *The following are equivalent for an elliptic curve E over R:*

(1) *E is* CL.

(2) *E has ordinary reduction and Serre-Tate parameter $q(E) = 1$ (with respect to some, and hence any, basis of the physical Tate module).*

(3) *There exists a morphism of* $\mathbf{Z}$-schemes *$E \to E$ whose reduction mod p is the absolute Frobenius $\mathbf{F}_p$-morphism $\bar{E} \to \bar{E}$. (In* [7] *this situation was referred to by saying that E has a lift of Frobenius.)*

Proof. The equivalence between 2 and 1 is essentially the definition of the CL property in [22]. The implication 1 $\implies$ 3 is trivial. For 3 $\implies$ 1, note first that $\bar{E}$ must be ordinary: this follows, for instance, from Proposition 7.15 and Corollaries 8.86 and 8.89 in [7]. Finally, the $\mathbf{Z}$-morphism $E \to E$ induces an R-morphism $E \to E^{\phi}$; the Néron model property shows that the latter is a composition of a homomorphism u with translation by an R-point reducing to the identity mod p. But then u mod p is the relative Frobenius. □

Theorem 4.3 (Existence and uniqueness of CL abelian schemes)**.**

(1) *Fix a prime p and an ordinary abelian variety $\bar{E}$ over k. Then there exists a unique* CL *abelian scheme E over R with $E \otimes k \simeq \bar{E}$ (unique up to isomorphism).*

(2) *If E and E' are* CL *abelian schemes over R, then the natural map $\mathrm{Hom}_R(E, E') \to \mathrm{Hom}_k(\bar{E}, \bar{E}')$ is an isomorphism.*

(3) *If two elliptic curves over R are related by an isogeny of degree prime to p and one of them is* CL*, then so is the other.*

Proof. This is due to Serre and Tate: see [22, 15]. □

The *conductor* of an order in a quadratic number field is the index of the order in the maximal order.

Theorem 4.4 (Relation between CL and CM)**.**

(1) (a) *If E is a* CL *elliptic curve over R, then E has* CM *(part of this claim is that E is definable over $M = K \cap \overline{\mathbf{Q}}$). Thus we have the relation* CL $\subseteq$ CM *between subsets of $Y_1(N)(\overline{\mathbf{Q}})$.*

(b) *Conversely, if $Q = (E, \alpha) \in Y_1(N)(\overline{\mathbf{Q}})$ is in* CM*, and p is split in* $\mathrm{End}\, E \otimes \mathbf{Q}$ *and does not divide the conductor of* $\mathrm{End}\, E$*, then $Q \in$* CL.

(2) (a) *If (E, i) is a* CL *fake elliptic curve over R, then (E, i) is CM. Thus we have the relation* CL $\subseteq$ CM *between subsets of $X^D(\mathcal{U})(M)$.*

(b) *Conversely, for any* CM*-point $Q \in X^D(\mathcal{U})(\overline{\mathbf{Q}})$, we know that the associated abelian surface E is the square of an elliptic curve with* CM *by an order in some $\mathcal{K}$; if p splits in $\mathcal{K}$ and p does not divide the conductor of the order, then $Q \in$* CL.

Proof.

(1) (a) If E/R is a CL elliptic curve, then $\mathrm{End}_R(E) \simeq \mathrm{End}_k(\bar{E}) \neq \mathbf{Z}$.

(b) This follows from the theorem in the middle of p. 293 in [36].

(2) (a) Let $\mathcal{E} := \mathrm{End}_R(E) \otimes \mathbf{Q} \simeq \mathrm{End}_k(\bar{E}) \otimes \mathbf{Q}$. Since $\bar{E}$ is ordinary, the center of $\mathcal{E}$ contains an imaginary quadratic field $\mathcal{K}$: see [7, p. 247], say. In particular, $\mathcal{E} \not\simeq D$, so (E, i) is CM.

(b) Apply Theorem 4.4(1)(b) to the elliptic curve.

□

4.2. **δ-functions.** See [3, 7]. Let $\delta\colon R \to R$ be the *Fermat quotient map* $\delta x := (\phi(x) - x^p)/p$. Then

$$\begin{array}{rcl} \delta(x+y) & = & \delta x + \delta y + C_p(x,y) \\ \delta(xy) & = & x^p \cdot \delta y + y^p \cdot \delta x + p \cdot \delta x \cdot \delta y, \end{array} \tag{4.5}$$

where $C_p(X,Y) := \frac{X^p+Y^p-(X+Y)^p}{p} \in \mathbf{Z}[X,Y]$. Following [3] we think of δ as a "derivation with respect to p". If $P \in \mathbf{A}^N(R) = R^N$, then δP is defined by applying δ to each coordinate.

Let X be a smooth R-scheme and let $f\colon X(R) \to R$ be a map of sets. Following [7, p. 41], we say that f is a *δ-function of order r* if for any point in $X(R)$ there is a Zariski open neighborhood $U \subset X$, a closed immersion $u\colon U \hookrightarrow \mathbf{A}^N_R$, and a restricted power series F with R-coefficients in $(r+1)N$ variables such that

$$f(P) = F(u(P), \delta(u(P)), \dots, \delta^r(u(P))) \quad \text{for all } P \in U(R).$$

(*Restricted* means that the coefficients converge p-adically to 0.) Let $\mathcal{O}^r(X)$ be the ring of δ-functions of order r on X.

We have natural maps $\delta\colon \mathcal{O}^r(X) \to \mathcal{O}^{r+1}(X)$, $f \mapsto \delta f := \delta \circ f$, and natural ring homomorphisms $\phi\colon \mathcal{O}^r(X) \to \mathcal{O}^{r+1}(X)$, $f \mapsto \phi(f) = f^\phi := \phi \circ f$. The maps δ above still satisfy the identities in (4.5). Let X be affine, and let x be a system of étale coordinates on X, that is to say there exists an étale map $X \to \mathbf{A}^d$ such that x is the d-tuple of elements in $\mathcal{O}(X)$ obtained by pulling back the coordinates on $\mathbf{A}^d$. Let $x', x'', \dots, x^{(r)}$ be d-tuples of variables and let $\hat{}$ denotes p-adic completion, as usual. Then the natural map

$$\mathcal{O}(X)\hat{}\,[x', x'', \dots, x^{(r)}]\hat{} \to \mathcal{O}^r(X) \tag{4.6}$$

sending $x' \mapsto \delta x$, $x'' \mapsto \delta^2 x$,…,$x^{(r)} \mapsto \delta^r x$ is an isomorphism: see Propositions 3.13 and 3.19 in [7].

4.3. **δ-characters.** We recall facts from [3, 7]. If G is a smooth group scheme over R, then by a *δ-character of order r* we understand a δ-function $\psi\colon G(R) \to R$ of order r which is also a group homomorphism into the additive group of R. Following [3], we view δ-characters of abelian schemes as arithmetic analogues of the Manin maps [25, 26]. Let $\mathbf{X}^r(G)$ be the R-module of δ-characters of order r on G. By [3, pp. 325-326], the following hold for an elliptic curve E/R:

(1) If E is CL, then $\mathbf{X}^1(E)$ is free of rank 1.
(2) If E is not CL, then $\mathbf{X}^2(E)$ is free of rank 1.

We will need to review (and complement) some results in [3, 4] that can be viewed as an arithmetic analogue of Manin's Theorem of the Kernel [26, 10]. For any abelian group G, we set $p^\infty G := \cap_{n=1}^\infty p^n G$ and we let $p^\infty G : p^\infty$ be the group of all $x \in G$ for which there exists an integer $n \geq 1$ with $p^n x \in p^\infty G$. Also recall that we set $G_{p\text{-div}} = G_{\text{tors}} + pG$.

Lemma 4.7. *Let E be an elliptic curve over $\mathbf{Z}_p$. Let r be 1 or 2 according as E is* CL *or not. Let $\psi\colon E(R) \to R$ be a generator of $\mathbf{X}^r(G)$. Then*

(1) *ψ is surjective and defined over $\mathbf{Z}_p$.*
(2) $\ker\psi = p^\infty E(R) : p^\infty$.
(3) $\ker\psi + pE(R) = E(R)_{\text{tors}} + pE(R) =: E(R)_{p\text{-}div}$.
(4) $\psi^{-1}(pR) = E(R)_{\text{tors}} + pE(R) =: E(R)_{p\text{-}div}$.
(5) $(\ker\psi) \cap E(\mathbf{Z}_p^{\text{ur}}) = E(\mathbf{Z}_p^{\text{ur}})_{\text{tors}}$.

Proof.

1. Surjectivity follows from [4, Theorem 1.10]. That ψ is defined over $\mathbf{Z}_p$ follows from its construction in [3].
2. If E has ordinary reduction, then [3, Theorem B', p. 312] shows that $(\ker\psi)/p^\infty E(R)$ is a finite cyclic p-group; this implies the non-trivial inclusion "$\subset$". If E has supersingular reduction, we are done by [4, Corollary 1.12].
3. The non-trivial inclusion is "$\subset$". If $P \in \ker\psi$, by (2) there exists n such that $p^nP = p^{n+1}Q$ for some $Q \in E(R)$. So $P - pQ \in E(R)_{\text{tors}}$ and we are done.
4. This follows from (3) and (1).
5. If E has ordinary reduction, then by Theorem 1.2 and Remark 1.3 on p. 209 of [4], we have $p^\infty E(R) \cap E(\mathbf{Z}_p^{\text{ur}}) \subset E(\mathbf{Z}_p^{\text{ur}})_{\text{tors}}$; combining this with (2) yields the nontrivial inclusion $(\ker\psi) \cap E(\mathbf{Z}_p^{\text{ur}}) \subset E(\mathbf{Z}_p^{\text{ur}})_{\text{tors}}$ of (5). Now assume that E has supersingular reduction. If a_p is the trace of Frobenius on $E_{\mathbf{F}_p}$ then the map $\phi^2 - a_p\phi + p\colon R \to R$ is injective. By [4, Theorem 1.10, p. 212], the restriction of ψ to the kernel of the reduction map red: $E(R) \to E(k)$ is injective. In other words, $\ker(\psi) \cap \ker(\text{red}) = \{0\}$. Equivalently, red restricts to an injection $\ker\psi \to E(k)$. Since $E(k)$ is torsion, so is $\ker\psi$.

□

We now describe an explicit generator ψ of $\mathbf{X}^r(A_R)$, where A is an elliptic curve over $\mathbf{Z}_p$, and r is 1 or 2 according as A_R is CL or not. Fix a 1-form ω generating the $\mathbf{Z}_p$-module $H^0(A, \Omega^1)$. This uniquely specifies a Weierstrass model $y^2 = x^3 + ax + b$ for A over $\mathbf{Z}_p$ such that $\omega = dx/y$. Let $T := -x/y$. So T is an étale coordinate at the origin 0 of A, vanishing at 0. Let $L(T) \in \mathbf{Q}_p[[T]]$ be the logarithm of the formal group of A associated to T, so $dL(T) = \omega \in \mathbf{Z}_p[[T]]\,dT$ and $L(0) = 0$. If A is CL, let up be the unique root in $p\mathbf{Z}_p$ of the polynomial $x^2 - a_px + p$. By [7, Theorem 7.22] and [4, Theorem 1.10], we may take

$$\psi := \begin{cases} \frac{1}{p}(\phi^2 - a_p\phi + p)L(T) \in R[[T]][T', T'']\hat{}, & \text{if } A \text{ is not CL;} \\ \frac{1}{p}(\phi - up)L(T) \in R[[T]][T']\hat{}, & \text{if } A \text{ is CL.} \end{cases} \tag{4.8}$$

4.4. **δ-Fourier expansions.** See [5]. We start by reviewing background on *classical* Fourier expansions as in [13, p. 112]. (The discussion there involves the modular curve parametrizing elliptic curves with an embedding of μ_N rather than $\mathbf{Z}/N\mathbf{Z}$ as here. But, the two modular curves are isomorphic over $\mathbf{Z}[1/N, \zeta_N]$: see [13, p. 113].) The cusp ∞ on $S := X_1(N)$ arises from a $\mathbf{Z}[1/N, \zeta_N]$-valued point; so if $p \gg 0$ (specifically, $p \nmid N$), then it gives rise to an R-point, which may be viewed as a closed immersion $s_\infty\colon \operatorname{Spec} R \to S_R$. Let $[\infty] = s_\infty(\operatorname{Spec} R)$. Let $\tilde{S}_R$ be the completion of S_R along $[\infty]$. The Tate generalized elliptic curve $\text{Tate}(q)/R[[q]]$ equipped with the standard immersion α_{can} of $\mu_{N,R} \simeq (\mathbf{Z}/N\mathbf{Z})_R$ is a point in $S(R[[q]])$ that reduces mod q to s_∞. For $p \gg 0$ there is an induced isomorphism $\operatorname{Spf} R[[q]] \simeq \tilde{S}_R$. Therefore, for any open subset $U \subset S_R$ containing $[\infty]$ we have an induced *Fourier q-expansion* homomorphism

$$\mathcal{O}(U \setminus [\infty]) \to R((q)) := R[[q]][1/q].$$

More generally, suppose that we are given a modular-elliptic correspondence $S \xleftarrow{\Pi} X \xrightarrow{\Phi} A$. Let M be the ramification index of Π at x_∞. As before, we assume $p \gg 0$. Then we have $\operatorname{Spf} R[[\mathfrak{q}]] \simeq \tilde{X}_R$, where $\mathfrak{q} := q^{1/M}$ and $\tilde{X}_R$ is the completion of X_R along the closure $[x_\infty]$

of x_∞. Moreover, for any open set $U \subset X_R$ containing $[x_\infty]$ we have a *Fourier q-expansion* homomorphism

$$\mathcal{O}(U \setminus [x_\infty]) \to R((\mathfrak{q})).$$

Next we move to the "δ-theory". Let $q', q'', \dots, q^{(r)}, \dots$ be new indeterminates. Define

$$S^r_\infty := R((q))\hat{}[q', q'', \dots, q^{(r)}]\hat{}.$$

For each r, extend $\phi\colon R \to R$ to a ring homomorphism $\phi\colon S^r_\infty \to S^{r+1}_\infty$ denoted $F \mapsto F^\phi$ by requiring

$$q^\phi := q^p + pq', \quad (q')^\phi := (q')^p + pq'', \quad \dots,$$

and define $\delta\colon S^r_\infty \to S^{r+1}_\infty$ by

$$\delta F := \frac{F^\phi - F^p}{p}. \tag{4.9}$$

By the universality property of the sequence $\{\mathcal{O}^r(U \setminus [\infty])\}_{r \geq 0}$ (see [7, Proposition 3.3]), there exists a unique sequence of ring homomorphisms

$$\mathcal{O}^r(U \setminus [\infty]) \to S^r_\infty, \tag{4.10}$$

called *δ-Fourier expansion* maps and denoted $g \mapsto g_\infty$, such that $(\delta g)_\infty = \delta(g_\infty)$ for all g.

More generally, given a modular-elliptic correspondence $S \xleftarrow{\Pi} X \xrightarrow{\Phi} A$, define rings

$$S^r_{x_\infty} := R((\mathfrak{q}))\hat{}[\mathfrak{q}', \dots, \mathfrak{q}^{(r)}]\hat{}$$

where $\mathfrak{q}', \dots, \mathfrak{q}^{(r)}$ are new variables. Again there are natural maps $\phi, \delta\colon S^r_{x_\infty} \to S^{r+1}_{x_\infty}$ defined exactly as above and there are *δ-Fourier expansion* maps

$$\mathcal{O}^r(U \setminus [x_\infty]) \to S^r_{x_\infty}$$

commuting with δ, and denoted $g \mapsto g_{x_\infty}$. There are natural maps $S^r_\infty \to S^r_{x_\infty}$. Since $\operatorname{Spec} R[\mathfrak{q}, \mathfrak{q}^{-1}] \to \operatorname{Spec} R[q, q^{-1}]$ is étale, (4.6) implies

$$S^r_{x_\infty} \simeq R((\mathfrak{q}))\hat{}[q', \dots, q^{(r)}]\hat{}.$$

4.5. **δ-Serre-Tate expansions.** See [6, 7]. Assume that we are given a Shimura-elliptic correspondence $S \xleftarrow{\Pi} X \xrightarrow{\Phi} A$, and that $p \gg 0$. By the proof of Lemma 2.6 in [6], there exist infinitely many k-points $\bar{y}_0 \in S(k)$ whose associated triple $(\bar{Y}, \bar{i}, \bar{\alpha})$ is such that

(1) $\bar{Y}$ is ordinary, and
(2) if $\bar{\theta}$ is the unique principal polarization compatible with $\bar{i}$, then $(\bar{Y}, \bar{\theta})$ is isomorphic to the polarized Jacobian of a genus-2 curve.

So we may choose a point $\bar{y}_0 \in S(k)$ as above such that moreover, there exists $\bar{x}_0 \in \bar{X}(k)$ with $\Pi(\bar{x}_0) = \bar{y}_0$ such that both Π and Φ are étale at $\bar{x}_0$: here we use $p \gg 0$ to know that $\Pi \otimes k$ and $\Phi \otimes k$ are separable.

Let Y be the canonical lift of $\bar{Y}$. Since $\operatorname{End}(Y) \simeq \operatorname{End}(\bar{Y})$, the embedding $\bar{i}\colon \mathcal{O}_D \to \operatorname{End}(\bar{Y})$ induces an embedding $i\colon \mathcal{O}_D \to \operatorname{End}(Y)$. Also the level $\mathcal{U}$ structure $\bar{\alpha}$ lifts to a level $\mathcal{U}$ structure on (Y, i). Let $y_0 := (Y, i, \alpha) \in S(R)$. Since Π is étale at $\bar{x}_0$, there exists $x_0 \in X(R)$ such that $x_0 \bmod p = \bar{x}_0$ and $\Pi(x_0) = y_0$.

Let $\bar{Y}^\vee$ be the dual of $\bar{Y}$. By [6, Lemma 2.5], there exist $\mathbf{Z}_p$-bases of the Tate modules $T_p(\bar{Y})$ and $T_p(\bar{Y}^\vee)$, corresponding to each other under $\bar{\theta}$, such that any fake elliptic curve over R lifting $(\bar{Y}, \bar{i})$ has a diagonal Serre-Tate matrix $\operatorname{diag}(q, q^{disc(D)})$ with respect to these bases. Fix such bases. They define an isomorphism between the completion of S_R along the section y_0 and $\mathrm{Spf}\, R[[t]]$. The Serre-Tate parameter q corresponds to the value of $1+t$. Since Π is étale at $\bar{x}_0$ we have an induced isomorphism between the completion of X along the section x_0 and $\mathrm{Spf}\, R[[t]]$. As in Section 4.4 define rings

$$S^r_{x_0} \simeq R[[t]][t', \dots, t^{(r)}]\hat{}$$

and maps $\phi, \delta\colon S^r_{x_0} \to S^{r+1}_{x_0}$; then for any affine open set $U \subset X$ containing the image of the section x_0 we have natural *δ-Serre-Tate expansion maps*

$$\mathcal{O}^r(U) \to S^r_{x_0}, \tag{4.11}$$

denoted $g \mapsto g_{x_0}$, that commute with ϕ and δ.

4.6. **Pullbacks by Φ of δ-characters.** Assume that we are given a modular-elliptic or a Shimura-elliptic correspondence $S \xleftarrow{\Pi} X \xrightarrow{\Phi} A$. Recall that A is defined over a number field F_0. We suppose that $p \gg 0$ and p splits completely in F_0. Then A_R comes from an elliptic curve over $\mathbf{Z}_p$. Define a_p and (if A_R is CL) u as in Section 4.3. Let ψ be as in (4.8). The composition

$$f^\sharp\colon X(R) \xrightarrow{\Phi} A(R) \xrightarrow{\psi} R. \tag{4.12}$$

is in $\mathcal{O}^r(X_R)$. In what follows we compute the δ-Fourier expansion $f^\sharp_{x_\infty} \in S^r_{x_\infty}$ (in the modular-elliptic case) or the δ-Serre-Tate expansion $f^\sharp_{x_0} \in S^r_{x_0}$ (in the Shimura-elliptic case).

4.6.1. *Modular-elliptic case.* Suppose that $S = X_1(N)$. We have $\Phi^*\colon R[[T]] \to R[[\mathfrak{q}]]$. Define $b_n \in F_0 \cap R$ by

$$\left(\sum_{n \geq 1} b_n \mathfrak{q}^{n-1}\right) d\mathfrak{q} := d(\Phi^*(L(T))) = \Phi^*(dL(T)) = \Phi^*\omega.$$

so

$$\sum_{n \geq 1} \frac{b_n}{n} \mathfrak{q}^n = \Phi^*(L(T)). \tag{4.13}$$

Applying Φ^* to (4.8) and substituting (4.13) yields

$$f^\sharp_{x_\infty} = \Phi^*\psi = \begin{cases} \frac{1}{p} \sum_{n \geq 1} \left(\frac{b_n^{\phi^2}}{n} \mathfrak{q}^{n\phi^2} - a_p \frac{b_n^{\phi}}{n} \mathfrak{q}^{n\phi} + p \frac{b_n}{n} \mathfrak{q}^n \right), & \text{if } A \text{ is not CL;} \\ \frac{1}{p} \sum_{n \geq 1} \left(\frac{b_n^{\phi}}{n} \mathfrak{q}^{n\phi} - up \frac{b_n}{n} \mathfrak{q}^n \right), & \text{if } A \text{ is CL.} \end{cases} \tag{4.14}$$

In both cases, $f^\sharp_{x_\infty} \in R[[\mathfrak{q}]][\mathfrak{q}', \mathfrak{q}'']\hat{}$. Applying the substitution homomorphism

$$\begin{aligned} R[[\mathfrak{q}]][\mathfrak{q}', \mathfrak{q}'']\hat{} &\to R[[\mathfrak{q}]] \\ G &\mapsto G_\natural := G(\mathfrak{q}, 0, 0) = G|_{\mathfrak{q}'=\mathfrak{q}''=0}, \end{aligned}$$

we obtain

$$(f^\sharp_{x_\infty})_\natural = \begin{cases} \frac{1}{p} \sum_{n \geq 1} \left(\frac{b^{\phi^2}_{n/p^2}}{n/p^2} - a_p \frac{b^{\phi}_{n/p}}{n/p} + p \frac{b_n}{n} \right) q_M^n, & \text{if } A \text{ is not CL;} \\ \frac{1}{p} \sum_{n \geq 1} \left(\frac{b^{\phi}_{n/p}}{n/p} - up \frac{b_n}{n} \right) \mathfrak{q}^n, & \text{if } A \text{ is CL,} \end{cases} \tag{4.15}$$

where $b_\gamma := 0$ if $\gamma \in \mathbf{Q} \setminus \mathbf{Z}$. (In particular, the right hand side of (4.15) has coefficients in R, which is not a priori obvious.)

Let us consider the special case when $S \xleftarrow{\Pi} X \xrightarrow{\Phi} A$ arises from a modular parametrization associated to the newform $f = \sum a_n q^n$, so $S = X = X_1(N)$, $\Pi = \mathrm{Id}$, $x_\infty = \infty$, $M = 1$, and $\mathfrak{q} = q$. We may take ω so that $\Phi^*\omega = \sum a_n q^{n-1} dq$; then $b_n = a_n$ for all n. Since f is a newform, the a_n satisfy the usual relations [41, Theorem 3.43] (we use $p \gg 0$ to know that $p \nmid N$):

$$a_{p^i m} = a_{p^i} a_m \quad \text{for } (p, m) = 1, \tag{4.16}$$

$$a_{p^{i-1}} a_p = a_{p^i} + p a_{p^{i-2}} \quad \text{for } i \geq 2. \tag{4.17}$$

Lemma 4.18. *Assume that $S \xleftarrow{\Pi} X \xrightarrow{\Phi} A$ arises from a modular parametrization attached to f.*

(1) *With notation as in* (3.12) *and* (3.13), *the following holds in $\mathbf{Z}_p[[q]]$:*

$$(f^\sharp_\infty)_\natural = \begin{cases} f^{(-1)}(q), & \text{if } A \text{ is not CL;} \\ -u f^{(-1)}_{[u]}(q), & \text{if } A \text{ is CL.} \end{cases} \tag{4.19}$$

(2) *With notation as in* (3.30) *and* (3.31), *the following holds in $k[[q]][q', q'']$:*

$$\overline{f^\sharp_\infty} = \begin{cases} \overline{f^{(-1)}(q)} + \left(\frac{q'}{q^p}\right)^p \left(\overline{f^{(0)}_{[a_p]}(q)}\right)^{p^2} - \bar{a}_p \left(\frac{q'}{q^p}\right) \left(\overline{f^{(0)}_{[a_p]}(q)}\right)^p, & \text{if } A \text{ is not CL;} \\ \\ -\bar{u}\overline{f^{(-1)}_{[u]}(q)} + \left(\frac{q'}{q^p}\right) \left(\overline{f^{(0)}_{[a_p]}(q)}\right)^p, & \text{if } A \text{ is CL.} \end{cases} \tag{4.20}$$

Proof. We shall prove (4.20) in the case where A_R is not CL. The other three statements are proved similarly (and are actually easier).

To simplify notation, let $\Box$ stand for any element of $\mathbf{Z}_p[[q]][q^{-1}, q', q'']\hat{}$. For any $\gamma, \beta \in \mathbf{Z}_p[[q]][q^{-1}, q', q'']\hat{}$, any $\ell \in \mathbf{Z}_{\geq 2}$, and any $m \in \mathbf{Z}_{\geq 1}$ we have

$$(1 + p\gamma + p^2\beta)^{mp^{\ell-2}} = 1 + mp^{\ell-1}\gamma + p^\ell \Box. \tag{4.21}$$

(Writing $(1 + p\gamma + p^2\beta)^m$ as $1 + p\gamma'$ lets us reduce to the case $\beta = 0$ and $m = 1$, which is proved by induction on ℓ.)

By (4.14) we get

$$\begin{aligned} f^\sharp_\infty &= \frac{1}{p}\left[\sum \frac{a_n}{n}\left(q^{p^2} + p(q')^p + p^2\Box\right)^n - a_p \sum \frac{a_n}{n}\left(q^p + pq'\right)^n + p\sum \frac{a_n}{n} q^n\right] \\ &= \frac{1}{p}\left[\sum \frac{a_n}{n}\left(1 + p(\frac{q'}{q^p})^p + p^2\Box\right)^n q^{p^2 n} - a_p \sum \frac{a_n}{n}\left(1 + p\frac{q'}{q^p}\right)^n q^{pn} + p\sum \frac{a_n}{n} q^n\right] \\ &= \sum \left[\frac{a_{n/p^2}}{n/p}\left(1 + p\left(\frac{q'}{q^p}\right)^p + p^2\Box\right)^{n/p^2} - a_p \frac{a_{n/p}}{n}\left(1 + p\frac{q'}{q^p}\right)^{n/p} + \frac{a_n}{n}\right] q^n \\ &=: \sum \gamma_n q^n, \end{aligned}$$

where $a_r = 0$ for $r \in \mathbf{Q} \setminus \mathbf{Z}$.

If $(n, p) = 1$, then $\gamma_n = a_n/n$.

If $n = pm$ with $(m,p) = 1$, then (4.16) and (4.21) yield

$$\gamma_n = \frac{a_p a_m}{pm} - a_p \frac{a_m}{pm}\left(1 + pm\frac{q'}{q^p} + p^2\Box\right) \equiv -a_p a_m \frac{q'}{q^p} \pmod{p}.$$

If $n = p^\ell m$ with $\ell \geq 2$ and $(m,p) = 1$, then (4.16), (4.17), and (4.21) yield

$$\begin{aligned}\gamma_n &= \frac{a_{p^{\ell-2}} a_m}{p^{\ell-1} m}\left(1 + mp^{\ell-1}\left(\frac{q'}{q^p}\right)^p + p^\ell\Box\right) - \frac{a_p a_{p^{\ell-1}} a_m}{p^\ell m}\left(1 + mp^\ell \frac{q'}{q^p} + p^{\ell+1}\Box\right) + \frac{a_{p^\ell} a_m}{p^\ell m}\\ &\equiv a_p^{\ell-2} a_m \left(\frac{q'}{q^p}\right)^p - a_p^\ell a_m \frac{q'}{q^p} \pmod{p}.\end{aligned}$$

Therefore

$$f_\infty^\sharp \equiv \sum_{(m,p)=1} \frac{a_m}{m} q^m - a_p \frac{q'}{q^p} \sum_{(m,p)=1} a_m q^{mp} + \sum_{\ell \geq 2} \sum_{(m,p)=1} a_m \left(a_p^{\ell-2}\left(\frac{q'}{q^p}\right)^p - a_p^\ell \frac{q'}{q^p}\right) q^{mp^\ell} \pmod{p},$$

and the first case of (4.20) follows via a trivial algebraic manipulation. □

Remark 4.22. The right hand side of (4.20) belongs to the subring $k[[q]][q']$ of $k[[q]][q', q'']$. In the case where $S \xleftarrow{\Pi} X \xrightarrow{\Phi} A$ does not necessarily arise from a modular parametrization, an argument similar to the one in the proof of Lemma 4.18 still yields

$$\overline{f_{x_\infty}^\sharp} \in k[[\mathfrak{q}]][\mathfrak{q}']. \tag{4.23}$$

4.6.2. *Shimura-elliptic case.* Suppose that $S = X^D(\mathcal{U})$. Recall that we fixed $x_0 \in X(R)$ and a corresponding δ-Serre-Tate expansion map $\mathcal{O}^2(X_R) \to S_{x_0}^2 = R[[t]][t', t'']\hat{}$, denoted $G \mapsto G_{x_0}$. Let $z_0 = \Phi(x_0) \in A(R)$. Let $\lambda\colon A_R \to A_R$ be the translation by $-z_0$. Recall the étale coordinate T on A_R at 0; use $T_{z_0} := \lambda^* T$ as étale coordinate at z_0. Now we have $R[[T]] \xrightarrow{\lambda^*} R[[T_{z_0}]] \xrightarrow{\Phi^*} R[[t]]$. Define $b_n \in F_0 \cap R$ by

$$\left(\sum_{n \geq 1} b_n t^{n-1}\right) dt := d(\Phi^* \lambda^* (L(T))) = \Phi^* \lambda^* d(L(T)) = \Phi^* \lambda^* \omega,$$

so

$$\sum_{n \geq 1} \frac{b_n}{n} t^n = \Phi^* \lambda^* (L(T)). \tag{4.24}$$

Since Φ is étale at x_0, we have $b_1 \neq 0$; scaling ω, we may assume that $b_1 = 1$. Since ψ is a group homomorphism, we have $\psi - \psi(z_0) = \lambda^* \psi$. Add the constant $\psi(z_0)$ to both sides, and apply Φ^* to obtain

$$f_{x_0}^\sharp = \Phi^* \psi = \psi(z_0) + \Phi^* \lambda^* \psi.$$

Evaluate $\Phi^* \lambda^* \psi$ by applying $\Phi^* \lambda^*$ to (4.8) and substituting (4.24) into the right hand side: the final result is

$$f_{x_0}^\sharp = \begin{cases} \psi(z_0) + \frac{1}{p}\sum_{n\geq 1}\left(\frac{b_n^{\phi^2}}{n} t^{n\phi^2} - a_p \frac{b_n^\phi}{n} t^{n\phi} + p\frac{b_n}{n} t^n\right), & \text{if } A \text{ is not CL;}\\ \psi(z_0) + \frac{1}{p}\sum_{n\geq 1}\left(\frac{b_n^\phi}{n} t^{n\phi} - up\frac{b_n}{n} t^n\right), & \text{if } A \text{ is CL.}\end{cases} \tag{4.25}$$

An argument similar to the one in the proof of Lemma 4.18 shows that

$$\overline{f_{x_0}^\sharp} \in k[[t]][t']. \tag{4.26}$$

4.7. **δ-modular forms: modular-elliptic case.** We recall some concepts from [5, 7, 1]. The ring of *δ-modular functions* [5] is

$$M^r := R[a_4^{(\leq r)}, a_6^{(\leq r)}, \Delta^{-1}]\hat{},$$

where $a_4^{(\leq r)}$ is a tuple of variables $(a_4, a_4', a_4'', \ldots, a_4^{(r)})$ and $a_6^{(\leq r)}$ is similar, and $\Delta := -2^6 a_4^3 - 2^4 3^3 a_6^2$. If $g \in M^0 \setminus pM^0$, define

$$M_{\{g\}}^r := M^r[g^{-1}]\hat{} = R[a_4^{(\leq r)}, a_6^{(\leq r)}, \Delta^{-1}, g^{-1}]\hat{}.$$

An element of M^r or $M_{\{g\}}^r$ is *defined over* $\mathbf{Z}_p$ if it belongs to the analogously defined ring with $\mathbf{Z}_p$ in place of R. Define $\delta\colon M^r \to M^{r+1}$ and $\delta\colon M_{\{g\}}^r \to M_{\{g\}}^{r+1}$ as $\delta\colon S_\infty^r \to S_\infty^{r+1}$ was defined in Section 4.4. Let $j : -2^{12}3^3 a_4^3/\Delta$, let $i := 2^6 3^3 - j$, and let $t := a_6/a_4$. (This t is unrelated to the t used in δ-Serre-Tate expansions.) By [5, Proposition 3.10], we have

$$M_{\{a_4 a_6\}}^r = R[j^{(\leq n)}, j^{-1}, i^{-1}, t^{(\leq r)}, t^{-1}]\hat{}.$$

If $w = \sum n_i \phi^i \in \mathbf{Z}[\phi]$, define $\deg w = \sum n_i$. If moreover $\lambda \in R$, define $\lambda^w := \prod (\lambda^{\phi^i})^{n_i}$. For $w \in \mathbf{Z}[\phi]$, say that f in M^r or $M_{\{g\}}^r$ is of *weight* w if

$$f(\lambda^4 a_4, \lambda^6 a_6, \delta(\lambda^4 a_4), \delta(\lambda^6 a_6), \ldots) = \lambda^w f(a_4, a_6, a_4', a_6', \ldots), \tag{4.27}$$

for all $\lambda \in R$. Let $M^r(w)$ be the set of $f \in M^r$ of weight w, and define $M_{\{g\}}^r(w)$ similarly. In [5], elements of $M_{\{g\}}^r(w)$ were called *δ-modular forms of weight w* (holomorphic outside $g = 0$).

If $f \in M_{\{g\}}^r(w)$ and E is an elliptic curve given by $y^2 = x^3 + Ax + B$ with $A, B \in R$ and $g(A, B) \in R^\times$, then define $f(A, B) \in R$ by making the substitutions $a_4 \mapsto A$, $a_6 \mapsto B$, $a_4' \mapsto \delta A$, $a_6' \mapsto \delta B$, $a_4'' \mapsto \delta^2 A$, and so on. Recall from [5] that f is called *isogeny covariant* if for any isogeny u of degree prime to p from an elliptic curve $y^2 = x^3 + A_1 x + B_1$ with $g(A, B) \in R^\times$ to an elliptic curve $y^2 = x^3 + A_2 x + B_2$ with $g(A_2, B_2) \in R^\times$ that pulls back dx/y to dx/y we have

$$f(A_1, B_1) = \deg(u)^{-\deg(w)/2} f(A_2, B_2).$$

By [5, Corollary 3.11], $M_{\{a_4 a_6\}}^r(0) = R[j^{(\leq r)}, j^{-1}, i^{-1}]\hat{}$. More generally, if $m \in 2\mathbf{Z}$ and $g \in M^0(m)$, define $\tilde{g} := g t^{-m/2}$; then

$$M_{\{a_4 a_6 g\}}^r(0) = R[j^{(\leq r)}, j^{-1}, i^{-1}, \tilde{g}^{-1}]\hat{}. \tag{4.28}$$

Also define the open subscheme $Y(1)^g := \operatorname{Spec} R[j, j^{-1}, i^{-1}, \tilde{g}]$ of the modular curve $Y(1)_R := \operatorname{Spec} R[j]$. If we define

$$b := a_6^2/a_4^3 = -2^2 3^{-3} + 2^8 j^{-1}. \tag{4.29}$$

then $R[j, j^{-1}, i^{-1}] = R[b, b^{-1}, (4+27b)^{-1}]$, so b is an étale coordinate on $Y(1)^g$, and $Y_1(N)_R \to Y(1)_R$ is étale over $Y(1)^g$. Suppose that in addition we are given a modular-elliptic correspondence $S \xleftarrow{\Pi} X \xrightarrow{\Phi} A$. Then we may (and do) choose g so that the composition $v\colon X_R \overset{\Pi}{\to} X_1(N)_R \to X(1)_R$ is étale above $Y(1)^g$. Set

$$X^\dagger := v^{-1}(Y(1)^g). \tag{4.30}$$

The pull-back of b to $X^\dagger$, which we will still call b, is an étale coordinate on $X^\dagger$. By (4.6), we have natural isomorphisms

$$\mathcal{O}(X^\dagger)\hat{}[b',\dots,b^{(r)}]\hat{} \simeq \mathcal{O}^r(X^\dagger), \tag{4.31}$$

where $b',\dots,b^{(r)}$ are new indeterminates. We view (4.31) as an identification. Similarly, since j is an étale coordinate on $Y(1)$, (4.6) and (4.28) yield

$$M^r_{\{a_4a_6g\}}(0) \simeq \mathcal{O}^r(Y(1)^g) \subset \mathcal{O}^r(X^\dagger). \tag{4.32}$$

Since $X^\dagger$ is standard in the sense of Definition 3.16, we have the δ-Fourier expansion map

$$\mathcal{O}^r(X^\dagger) \to S^r_{x_\infty}. \tag{4.33}$$

Composing (4.32) and (4.33) yields δ-Fourier expansion maps

$$M^r_{\{a_4a_6g\}}(0) \to S^r_{x_\infty}. \tag{4.34}$$

Let $E_4(q)$ and $E_6(q)$ be the normalized Eisenstein series of weights 4 and 6: "normalized" means with constant coefficient equal to 1. We have natural ring homomorphisms, also referred to as *δ-Fourier expansion maps* [5],

$$\begin{aligned} M^r &\to S^r_\infty \\ g &\mapsto g_\infty = g(q,q',\dots,q^{(r)}), \end{aligned} \tag{4.35}$$

characterized by the properties that they send a_4 and a_6 to $-2^{-4}3^{-1}E_4(q)$ and $2^{-5}3^{-3}E_6(q)$, respectively, and commute with δ. There exists a unique $E_{p-1} \in M^0(p-1)$ such that $E_{p-1}(q)$ is the normalized Eisenstein series of weight $p-1$.

By (4.1) and (7.26) in [5], there exists a unique $f^1 \in M^1(-1-\phi)$, defined over $\mathbf{Z}_p$, such that

$$f^1(q,q') = \frac{1}{p}\log\frac{q^\phi}{q^p} := \sum_{n\geq 1}(-1)^{n-1}n^{-1}p^{n-1}\left(\frac{q'}{q^p}\right)^n \in R((q))\hat{}[q']\hat{}. \tag{4.36}$$

As explained in [5, pp. 126–129], f^1 is isogeny covariant and may be interpreted as a (characteristic zero) *arithmetic Kodaira-Spencer class.*

Lemma 4.37. *Let E be an elliptic curve given by $y^2 = x^3 + Ax + B$ with $A, B \in R$. With notation as above, $f^1(A,B) = 0$ if and only if E is* CL.

Proof. See [7, Proposition 7.15]. □

Define

$$t^{\frac{\phi+1}{2}} := t^{\frac{p+1}{2}}\left(\frac{t^\phi}{t^p}\right)^{1/2} = t^{\frac{p+1}{2}}\left(1+p\frac{\delta t}{t^p}\right)^{1/2} = t^{\frac{p+1}{2}}\sum_{j\geq 0}\binom{1/2}{j}p^j\left(\frac{\delta t}{t^p}\right)^j; \tag{4.38}$$

this function is an element of $M^1_{\{a_4a_6\}}(1+\phi)$. Next define

$$f^\flat := f^1 \cdot t^{\frac{\phi+1}{2}} \in M^1_{\{a_4a_6\}}(0) \subset M^1_{\{a_4a_6g\}}(0) \subset \mathcal{O}^1(X^\dagger). \tag{4.39}$$

The maps in (4.34) and (4.35) are compatible, so

$$f^\flat_\infty \in q'R((q))\hat{}[q']\hat{} \subset \mathfrak{q}'R((\mathfrak{q}))\hat{}[\mathfrak{q}']\hat{}. \tag{4.40}$$

Finally, by the main theorem of [20],

$$f^1 = cE_{p-1}\Delta^{-p}(2a_4^p a_6' - 3a_6^p a_4') + f_0 + pf_1, \tag{4.41}$$

for some $c \in R^\times$, $f_0 \in M^0(-1-p)$, and $f_1 \in M^1$. On the other hand, (4.29) implies

$$b^\phi = \left(\frac{a_6^2}{a_4^3}\right)^\phi = \frac{(a_6^p + pa_6')^2}{(a_4^p + pa_4')^3},$$

so a calculation using the definition in (4.9) yields

$$\delta b = a_4^{-4p} a_6^p (2a_4^p a_6' - 3a_6^p a_4') + ph \tag{4.42}$$

for some $h \in M^1_{\{a_4 a_6\}}$. Set $a_0 := cE_{p-1}\Delta^{-p} a_4^{4p} a_6^{-p}$. Then combining (4.41) and (4.42) yields

$$f^\flat = f^1 \cdot t^{\frac{\phi+1}{2}} = a_0 t^{\frac{p+1}{2}} \delta b + f_0 t^{\frac{p+1}{2}} + ph_1, \tag{4.43}$$

for some $h_1 \in M^1_{\{a_4 a_6\}}$. Let $\alpha = a_0 t^{\frac{p+1}{2}} \in M^0_{\{a_4 a_6\}}(0)$. Then by (4.43) and (4.5), respectively, we obtain, for $n = 0$ and $n = 1$,

$$\delta^n f^\flat = \alpha^{p^n} \delta^{n+1} b + \beta_n + p\gamma_n, \tag{4.44}$$

for some $\beta_n \in M^n_{\{a_4 a_6\}}(0)$ and $\gamma_n \in M^{n+1}_{\{a_4 a_6\}}(0)$.

Lemma 4.45. *Assume that the element $g \in M^0(m)$ is in $E_{p-1}M^0$. Then $\overline{f^\flat}$ and $\overline{\delta f^\flat}$ are algebraically independent over $\mathcal{O}(\bar{X}^\dagger)$, and the natural maps*

$$\mathcal{O}(\bar{X}^\dagger)[\overline{f^\flat}] \to \mathcal{O}^1(X^\dagger) \otimes_R k \tag{4.46}$$

$$\mathcal{O}(\bar{X}^\dagger)[\overline{f^\flat}, \overline{\delta f^\flat}] \to \mathcal{O}^2(X^\dagger) \otimes_R k \tag{4.47}$$

$$\mathcal{O}(X^\dagger)\hat{\ } \to \mathcal{O}^2(X^\dagger)/(f^\flat, \delta f^\flat) \tag{4.48}$$

are isomorphisms.

Proof. By (4.36), (4.38), and (4.39), we have

$$\overline{f^\flat_\infty} = t_\infty^{\frac{p+1}{2}} q'/q^p, \tag{4.49}$$

which involves q', so the algebraic independence follows. Reducing (4.31) mod p gives isomorphisms like (4.46) and (4.47) but with $\overline{b'}$ and $\overline{b''}$ on the left in place of $\overline{f^\flat}$ and $\overline{\delta f^\flat}$. To change variables, observe that since $g \in E_{p-1}M^0$, the element α is invertible in $\mathcal{O}(X^\dagger)$; thus (4.44) implies $\mathcal{O}(\bar{X}^\dagger)[\overline{f^\flat}] \simeq \mathcal{O}(\bar{X}^\dagger)[\overline{b'}]$ and $\mathcal{O}(\bar{X}^\dagger)[\overline{f^\flat}, \overline{\delta f^\flat}] \simeq \mathcal{O}(\bar{X}^\dagger)[\overline{b'}, \overline{b''}]$. This proves (4.46) and (4.47).

Now (4.47) implies that (4.48) induces an isomorphism mod p, Since both sides of (4.48) are p-adically complete and separated rings, (4.48) is surjective. The δ-Fourier expansion map $\mathcal{O}^2(X^\dagger) \to R((\mathfrak{q}))\hat{\ }[\mathfrak{q}', \mathfrak{q}'']\hat{\ }$ followed by the evaluation map mapping $\mathfrak{q}'$ and $\mathfrak{q}''$ to 0 induces a map $\mathcal{O}^2(X^\dagger)/(f^\flat, \delta f^\flat) \to R((\mathfrak{q}))$, by (4.40). The composition of (4.48) with this is simply the Fourier expansion map, since elements of $\mathcal{O}(X^\dagger)\hat{\ }$ have Fourier expansions in $R((\mathfrak{q}))$. So the Fourier expansion principle implies that (4.48) is injective. □

Corollary 4.50. *The series $\overline{f^{(0)}(q)}$ and $\overline{f^{(0)}_{[a_p]}(q)}$ are Fourier expansions of weight-2 quotients of modular forms.*

Proof. We have $\overline{f^{(0)}(q)} = \left(\theta^{p-1}\bar{f}\right)/\bar{E}_{p-1}^{p+1}$, which is the Fourier expansion of a weight-2 quotient. We handle the second series in an indirect way, using $f^\sharp$. Although $f^\sharp \in \mathcal{O}^2(X^\dagger)$, we have $\overline{f^\sharp} \in \mathcal{O}^1(X^\dagger) \otimes_R k$ by (4.23). So (4.46) identifies $\overline{f^\sharp}$ with a polynomial in $\mathcal{O}(\bar{X}^\dagger)[\overline{f^\flat}] \subset L[\overline{f^\flat}]$, where $L := k(\overline{X_1(N)})$. We can find this polynomial explicitly from the δ-Fourier expansion, since elements of L have expansions in $k((q))$ while $\overline{f^\flat_\infty}$ involves q': see (4.49). By Lemma 4.20 and (4.49),

$$\overline{f^\sharp_\infty} = \begin{cases} \overline{f^{(-1)}(q)} + t_\infty^{-\frac{p^2+p}{2}} \left(\overline{f^{(0)}_{[a_p]}(q)}\right)^{p^2} \overline{f^\flat_\infty}^{\,p} - \bar{a}_p t_\infty^{-\frac{p+1}{2}} \left(\overline{f^{(0)}_{[a_p]}(q)}\right)^{p} \overline{f^\flat_\infty}, & \text{if } A \text{ is not CL;} \\ -\bar{u}\overline{f^{(-1)}_{[u]}(q)} + t_\infty^{-\frac{p+1}{2}} \left(\overline{f^{(0)}_{[a_p]}(q)}\right)^{p} \overline{f^\flat_\infty}, & \text{if } A \text{ is CL.} \end{cases}$$

In either case, taking the coefficient of $\overline{f^\flat_\infty}$ shows that $\bar{a}_p t_\infty^{-\frac{p+1}{2}} \left(\overline{f^{(0)}_{[a_p]}(q)}\right)^{p}$ is the Fourier expansion of an element of L. Since t is a weight 2 quotient, $\bar{a}_p \left(\overline{f^{(0)}_{[a_p]}(q)}\right)^{p}$ is the Fourier expansion of a weight $p+1$ quotient, and hence (by dividing by $\bar{E}_{p-1}$) also of a weight-2 quotient. By (3.31),

$$-\bar{a}_p \left(\overline{f^{(0)}_{[a_p]}(q)}\right)^{p} + \overline{f^{(0)}_{[a_p]}(q)} = \overline{f^{(0)}(q)};$$

now $\overline{f^{(0)}_{[a_p]}(q)}$ is the Fourier expansion of a weight-2 quotient since the other terms are. □

Remark 4.51. The proof that $\overline{f^{(0)}_{[a_p]}(q)}$ is a Fourier expansion of a quotient of modular forms used the theory of δ-modular forms; we know no direct proof.

Recall the Igusa curve $I_1(N)$ and its quotient J defined in Section 3.8.

Lemma 4.52. *The Fourier series of any modular form f on $X_1(N)$ over k is also the Fourier series of a rational function $g \in k(I_1(N))$. If the weight of f is even, then we may take $g \in k(J)$.*

Proof. By [17, Proposition 2.2], there is a line bundle ω on $\overline{X_1(N)}$ such that for each $i \in \mathbf{Z}$, the global sections of ω^i are the modular forms of weight i. We denote by ω also the pullback of ω to $I_1(N)$ or J. By [17, p. 461], the sections of ω^i on $I_1(N)$ or J have naturally defined Fourier expansions, compatible with the Fourier expansions of modular forms on $X_1(N)$. There is a section a of ω on $I_1(N)$ whose Fourier expansion is 1: see [17, Proposition 5.2]. Given a modular form f of weight i on $X_1(N)$, let $g := f/a^i \in k(I_1(N))$.

The action of $\mathbf{F}_p^\times$ on $I_1(N)$ lifts to an action of $\mathbf{F}_p^\times$ on ω, and $-1 \in \mathbf{F}_p^\times$ sends a to $-a$ (see [17, Proposition 5.2(5)]), so if i is even, $f/a^i \in k(J)$. □

Recall the definition of $M^r_{\{g\}}(w)$ from the end of the first paragraph of Section 4.7. By Construction 3.2 and Theorem 5.1 of [1], there exist unique δ-modular forms $f^\partial \in M^1_{\{E_{p-1}\}}(\phi-1)$ and $f_\partial \in M^1_{\{E_{p-1}\}}(1-\phi)$, defined over $\mathbf{Z}_p$, with δ-Fourier expansions identically equal to 1. Moreover, these forms are isogeny covariant and $f^\partial \cdot f_\partial = 1$. Furthermore, the reduction $\overline{f^\partial} \in M^1 \otimes k$ equals the image of $\bar{E}_{p-1} \in M_{p-1}$ in $M^1 \otimes k$. For $\lambda \in R^\times$, define

$$f_\lambda := (f^1)^\phi - \lambda f^1 (f^\partial)^{-\phi-1} \in M^2_{\{E_{p-1}\}}(-\phi-\phi^2). \tag{4.53}$$

Since f_1 and f^∂ are isogeny covariant, so is f_λ. Furthermore consider the series

$$t^{\frac{\phi^2+\phi}{2}} := t^{\frac{p^2+p}{2}} \left(\frac{t^\phi}{t^p}\right)^{1/2} \left(\frac{t^{\phi^2}}{t^{p^2}}\right)^{1/2} \in M^2_{\{a_4a_6\}}(\phi+\phi^2),$$

and define

$$f^\flat_\lambda := f_\lambda \cdot t^{\frac{\phi^2+\phi}{2}} \in M^2_{\{a_4a_6E_{p-1}\}}(0). \tag{4.54}$$

The main reason for considering these forms comes from the following

Lemma 4.55. *Let E_1 be an elliptic curve $y^2 = x^3+A_1x+B_1$ over R with ordinary reduction. Then*

1. *There exists $\lambda \in R^\times$ such that $f_\lambda(A_1, B_1) = 0$.*
2. *If λ is as in (1) and there is an isogeny of degree prime to p between E_1 and an elliptic curve E_2 over R given by $y^2 = x^3 + A_2x + B_2$, then $f_\lambda(A_2, B_2) = 0$.*
3. *If in addition, $A_2B_2 \not\equiv 0 \pmod{p}$, then $f^\flat_\lambda(A_2, B_2) = (\delta f^\flat_\lambda)(A_2, B_2) = \cdots = 0$.*

Proof.

1. If $f^1(A_1, B_1) = 0$, any $\lambda \in R^\times$ will do. If $f^1(A_1, B_1) \neq 0$, set
$$\lambda := \frac{f^1(A_1, B_1)^\phi}{f^1(A_1, B_1)} f^\partial(A_1, B_1)^{\phi+1};$$
the numerator and denominator of the first factor have the same p-adic valuation and $\overline{f^\partial(A_1, B_1)} \equiv \bar{E}_{p-1}(\bar{A}, \bar{B}) \neq 0$, so $\lambda \in R^\times$.
2. Scaling A_2 and B_2 by suitable elements of $R^\times$, we may assume that the isogeny pulls back dx/y to dx/y. Now use the isogeny covariance of f_λ.
3. By (4.54), $f^\flat_\lambda(A_2, B_2) = 0$. Now use $\delta 0 = 0$.

□

Set $\sigma := q'/q^p$. Then (4.36), (4.53), and (4.54) yield

$$\overline{f^1_\infty} = \sigma, \qquad \overline{f_{\lambda,\infty}} = \sigma^p - \overline{\lambda}\sigma, \qquad \text{and} \qquad \overline{f^\flat_{\lambda,x_\infty}} = t_\infty^{\frac{p^2+p}{2}}(\sigma^p - \overline{\lambda}\sigma). \tag{4.56}$$

In what follows we assume that $X^\dagger = U \setminus [x_\infty]$ where U has an étale coordinate $\tau \in \mathcal{O}(U)$ such that $[x_\infty]$ is scheme-theoretically given by τ: we can arrange this by shrinking $X^\dagger$. Then $R[[\mathfrak{q}]] = R[[\tau]]$, so

$$R((\tau))\hat{}[\tau', \ldots, \tau^{(r)}]\hat{} = R((\mathfrak{q}))\hat{}[\mathfrak{q}', \ldots, \mathfrak{q}^{(r)}]\hat{} = R((\mathfrak{q}))\hat{}[q', \ldots, q^{(r)}]\hat{}.$$

Also $\mathcal{O}^r(X^\dagger) = \mathcal{O}(X^\dagger)\hat{}[\tau', \ldots, \tau^{(r)}]\hat{}$. Since

$$\overline{f^\flat_\lambda} \in \mathcal{O}(\bar{X}^\dagger)[\tau', \tau''] \cap k((\tau))[\tau'] = \mathcal{O}(\bar{X}^\dagger)[\tau'] = \mathcal{O}^1(X^\dagger) \otimes_R k, \tag{4.57}$$

we may define a quotient ring

$$\mathcal{A}^\ddagger := (\mathcal{O}^1(X^\dagger) \otimes_R k)/(\overline{f^\flat_\lambda}) \tag{4.58}$$

and a scheme $\bar{X}^\ddagger := \operatorname{Spec} \mathcal{A}^\ddagger$. View $\mathcal{A}^\ddagger$ as an algebra over $\mathcal{A}^\dagger := \mathcal{O}(X^\dagger) \otimes k = \mathcal{O}(\bar{X}^\dagger)$.

Lemma 4.59. *The $k((\mathfrak{q}))$-algebra $\mathcal{A}^\ddagger \otimes_{\mathcal{A}^\dagger} k((\mathfrak{q}))$ is a product of p copies of $k((\mathfrak{q}))$.*

Proof. We have

$$\begin{aligned}\mathcal{A}^\ddagger \otimes_{\mathcal{A}^\dagger} k((\mathfrak{q})) &= \left(\mathcal{O}(\bar{X}^\dagger)[\tau']/(\overline{f^\flat_\lambda})\right) \otimes_{\mathcal{A}^\dagger} k((\tau)) \\ &= k((\tau))[\tau']/(\overline{f^\flat_\lambda}) \\ &= k((\mathfrak{q}))[q']/(\overline{f^\flat_{\lambda,x_\infty}}) \\ &= k((\mathfrak{q}))[\sigma]/(\sigma^p - \bar{\lambda}\sigma) \\ &\simeq \prod_{i=1}^{p} k((\mathfrak{q})),\end{aligned}$$

since $\sigma^p - \bar{\lambda}\sigma = \prod_{i=1}^p (\sigma - \lambda_i)$ for some $\lambda_i \in k$. Explicitly, the last isomorphism is given by

(4.60) $$q' \mapsto (\lambda_1 q^p, \ldots, \lambda_p q^p).$$

□

Lemma 4.61. *One can choose $X^\dagger$ so that $\bar{X}^\ddagger \to \bar{X}^\dagger$ is a finite étale cover of degree p.*

Proof. By definition, $\bar{X}^\ddagger \to \bar{X}^\dagger$ is of finite type. Lemma 4.59 shows that it is étale of degree p above the generic point of $\bar{X}^\dagger$. Therefore $\bar{X}^\ddagger \to \bar{X}^\dagger$ is finite étale of degree p over some open neighborhood of the generic point. □

In case our correspondence arises from a modular parametrization one has the following variant of Lemma 4.59.

Lemma 4.62. *Assume $S \xleftarrow{\Pi} X \xrightarrow{\Phi} A$ arises from a modular parametrization and let $L = k(\overline{X_1(N)})$. Then*

$$\mathcal{A}^\ddagger \otimes_{\mathcal{A}^\dagger} L \simeq L \times \mathcal{A}^+ \times \mathcal{A}^-$$

where

$$\mathcal{A}^\pm := L[y]/\left(y^{(p-1)/2} - \bar{E}_{p-1}/t^{(p-1)/2}\right).$$

Proof. By (4.46), we have $\mathcal{A}^\ddagger \otimes_{\mathcal{A}^\dagger} L \simeq L[\overline{f^\flat}]/(\overline{f^\flat_\lambda})$. On the other hand

$$\begin{aligned}\overline{f^\flat_\lambda} &= t^{\frac{p^2+p}{2}}\left[(\overline{f^1})^p - \bar{\lambda}\overline{f^1}(\overline{f^\partial})^{-p-1}\right] \\ &= (\overline{f^\flat})^p - \lambda t^{\frac{p^2-1}{2}}\bar{E}_{p-1}^{-p-1}\overline{f^\flat} \\ &= \overline{f^\flat}\left[(\overline{f^\flat})^{(p-1)/2} + \sqrt{\lambda}t^{(p-1)/2}\bar{E}_{p-1}^{-1}(t^{(p-1)/2}/\bar{E}_{p-1})^{(p-1)/2}\right] \\ &\quad\cdot\left[(\overline{f^\flat})^{(p-1)/2} - \sqrt{\lambda}t^{(p-1)/2}\bar{E}_{p-1}^{-1}(t^{(p-1)/2}/\bar{E}_{p-1})^{(p-1)/2}\right],\end{aligned}$$

so the result follows. □

4.8. **δ-modular forms: Shimura-elliptic case.** We continue using the notation and assumptions of Sections 4.5 and 4.6. Assume that the U in (4.11) is small enough that the *line bundle of fake* 1*-forms* on U is trivial. (See [7, p. 230] for the definition of this line bundle: there it is called the "line bundle of false 1-forms".) Let $q := 1+t \in R[[t]]$ and write $q' = \delta(1+t)$, $q'' = \delta^2(1+t)$, and so on. Define

$$\Psi = \Psi(t,t') := \frac{1}{p}\log\frac{q^\phi}{q^p} = \frac{q'}{q^p} - \frac{p}{2}\left(\frac{q'}{q^p}\right)^2 + \cdots \in R[[t]][t']\hat{}.$$

Lemma 4.63. *There exists $f^\flat \in \mathcal{O}^1(U)$ such that*

$$f^\flat_{x_0} = u(t)^{\phi+1} \cdot \Psi(t,t') \in q'R[[t]][t']^{\widehat{\ }} \tag{4.64}$$

for some $u(t) \in R[[t]]^\times$, and

$$f^\flat(P) = 0 \quad \text{for } P \in \Pi^{-1}(\mathrm{CL}) \cap U(R). \tag{4.65}$$

Proof. Use (8.116), (8.82), and Proposition 8.61 in [7]. (In the notation of [7], one takes $f^\flat$ to be the value of the "δ-modular form" f^1_{crys} at the pull back to U of the universal fake elliptic curve equipped with some invertible fake 1-form; again f^1_{crys} should be viewed as an arithmetic Kodaira-Spencer class.) □

Lemma 4.66. *There exists a neighborhood $X^\dagger \subset U$ of the section x_0 such that $\overline{f^\flat}$ and $\overline{\delta f^\flat}$ are algebraically independent over $\mathcal{O}(\bar{X}^\dagger)$ and the natural maps*

$$\mathcal{O}(\bar{X}^\dagger)[\overline{f^\flat}] \to \mathcal{O}^1(X^\dagger) \otimes_R k \tag{4.67}$$

$$\mathcal{O}(\bar{X}^\dagger)[\overline{f^\flat}, \overline{\delta f^\flat}] \to \mathcal{O}^2(X^\dagger) \otimes_R k \tag{4.68}$$

$$\mathcal{O}(X^\dagger)^{\widehat{\ }} \to \mathcal{O}^2(X^\dagger)/(f^\flat, \delta f^\flat) \tag{4.69}$$

are isomorphisms.

Proof. By (4.64),

$$\overline{f^\flat_{x_0}} = \frac{\bar{u}(t)^{p+1}}{(1+t)^p} t' + S_0 \in k[[t]][t'], \tag{4.70}$$

for some $S_0 \in k[[t]]$. Using (4.5) one obtains

$$\overline{\delta f^\flat_{x_0}} = \frac{\bar{u}(t)^{p^2+p}}{(1+t)^{p^2}} t'' + S_1 \in k[[t]][t',t''] \tag{4.71}$$

for some $S_1 \in k[[t]][t']$. We may assume that there is an étale coordinate τ on U such that x_0 is given scheme-theoretically by $\tau = 0$. Then $R[[t]] = R[[\tau]]$ (and $R[[t]][t',t'']^{\widehat{\ }} = R[[\tau]][\tau',\tau'']^{\widehat{\ }}$) so $t = S(\tau) := \sum_{n\geq 1} c_n \tau^n$ for some $c_n \in R$ with $c_1 \in R^\times$. One can easily see that

$$t' = \frac{1}{p}\left[\sum c_n^\phi (\tau^p + p\tau')^n - \left(\sum c_n \tau^n\right)^p\right] = (\partial S/\partial \tau)^p \tau' + B_0 + pB_1$$

for some $B_0 \in R[[\tau]]$ and $B_1 \in R[[\tau]][\tau']^{\widehat{\ }}$. Using (4.5) we obtain

$$t'' = (\partial S/\partial \tau)^{p^2} \tau'' + B_1^* + pB_2$$

for some $B_1^* \in R[[\tau]][\tau']^{\widehat{\ }}$ and $B_2 \in R[[\tau]][\tau',\tau'']^{\widehat{\ }}$. Combining with (4.70) and (4.71) and setting

$$\bar{v}(\tau) := \frac{\bar{u}(\bar{S}(\tau))^{p+1} (\partial \bar{S}/\partial \tau)^p}{(\bar{S}(\tau)+1)^p} \in k[[\tau]],$$

we obtain

$$\tag{4.72} \begin{aligned} \overline{f^\flat_{x_0}} &= \bar{v}(\tau)\tau' + C_0(\tau) \in k[[\tau]][\tau'], \\ \overline{\delta f^\flat_{x_0}} &= \bar{v}(\tau)^p \tau'' + C_1(\tau,\tau') \in k[[\tau]][\tau',\tau'']. \end{aligned}$$

where $C_0(\tau) \in k[[\tau]]$ and $C_1(\tau,\tau') \in k[[\tau]][\tau']$. On the other hand, by (4.6), we have $\overline{f^\flat} \in \mathcal{O}(\bar{U})[\tau']$ and $\overline{\delta f^\flat} \in \mathcal{O}(\bar{U})[\tau',\tau'']$. Thus $\bar{v}(\tau)$, $C_0(\tau)$, and $C_1(\tau,\tau')$ are images of elements $\bar{v} \in \mathcal{O}(\bar{U})$, $C_0 \in \mathcal{O}(\bar{U})$, and $C_1 \in \mathcal{O}(\bar{U})[\tau']$, respectively, such that

$$\overline{f^\flat} = \bar{v}\tau' + C_0, \qquad \text{and} \qquad \overline{\delta f^\flat} = \bar{v}^p\tau'' + C_1. \tag{4.73}$$

Lift $\bar{v}$ to $v \in \mathcal{O}(U)$. Let $X^\dagger$ be the complement in U of the closed subscheme defined by v. Since $\bar{v}(\tau)$ has a nonzero constant term, $\bar{v}$ does not vanish at $\bar{x}_0$, so $X^\dagger$ contains the section x_0. The proof now follows the proof of Lemma 4.45, using (4.73) in place of (4.44). □

Remark 4.74. Using [7, pp. 268–269], for $\bar{U}$ contained in the ordinary locus one can construct forms $f^\flat_\lambda \in \mathcal{O}^2(U)$ analogous to the ones in (4.54). (In the notation of [7], one takes $f^\flat_\lambda$ to be the Shimura analogues of the forms in (4.53) evaluated at a basis of the module of fake 1-forms on U.) The analogues of Lemmas 4.55, 4.59, and 4.61 still hold with Fourier expansions replaced by Serre-Tate expansions. The corresponding statements and their proofs are analogous to the ones in the modular-elliptic case.

4.9. **Proofs of the local results.**

Proof of Theorem 3.5. Assume that we are given either a modular-elliptic or a Shimura-elliptic correspondence $S \xleftarrow{\Pi} X \xrightarrow{\Phi} A$. Assume that p is sufficiently large and p splits completely in F_0. In the Shimura-elliptic case we also assume that the places $v|p$ are not anomalous for A. In the modular-elliptic case, choose g as in Lemma 4.45 and define $X^\dagger$ as in (4.30). In the Shimura-elliptic case, choose $X^\dagger$ as in Lemma 4.66. By Lemma 4.45 or 4.66, there exists $\Phi^\dagger \in \mathcal{O}(X^\dagger)\hat{}$ such that

$$f^\sharp - \Phi^\dagger = h_0 f^\flat + h_1 \delta f^\flat, \tag{4.75}$$

for some $h_j \in \mathcal{O}^2(X^\dagger)$. Suppose that $P_1, \ldots, P_n \in \Pi^{-1}(\mathrm{CL}) \cap X^\dagger(R)$ and $m_1, \ldots, m_n \in \mathbf{Z}$. By Lemma 4.37 or 4.63, we have $f^\flat(P_i) = 0$, so $\delta f^\flat(P_i) = 0$. Thus

$$f^\sharp(P_i) = \Phi^\dagger(P_i). \tag{4.76}$$

Now (4.76) implies

$$\sum m_i \Phi^\dagger(P_i) = \sum m_i f^\sharp(P_i) = \sum m_i \psi(\Phi(P_i)) = \psi\left(\sum m_i \Phi(P_i)\right). \tag{4.77}$$

Equation (4.77) and Lemma 4.7(4) imply the second of the two equivalences in Theorem 3.5.

We now prove the first equivalence in Theorem 3.5. Let $Q := \sum m_i \Phi(P_i)$. If $Q \in A(R)_{\mathrm{tors}}$, then $\psi(Q) = 0$ and (4.77) implies $\sum m_i \Phi^\dagger(P_i) = 0$. Conversely, suppose that $\sum m_i \Phi^\dagger(P_i) = 0$; then $Q \in \ker \psi$. Since $\mathrm{CL} \subseteq S(\overline{\mathbf{Q}})$, we have $P_i \in X(\overline{\mathbf{Q}}) \cap X(R)$, so $Q \in A(\overline{\mathbf{Q}}) \cap A(R) \subset A(\mathbf{Z}_p^{\mathrm{ur}})$. So Lemma 4.7(5) implies $Q \in A(R)_{\mathrm{tors}}$.

To complete our proof, we need to check that $\overline{\Phi^\dagger} \notin k$.

Assume first that we are in the modular-elliptic case. By (4.40),

$$\delta f^\flat_\infty \in (\mathfrak{q}', \mathfrak{q}'')R((\mathfrak{q}))\hat{}[\mathfrak{q}', \mathfrak{q}'']\hat{}. \tag{4.78}$$

Taking δ-Fourier expansions in (4.75), taking $\natural$ (i.e., setting $\mathfrak{q}' = \mathfrak{q}'' = 0$), and using (4.40) and (4.78), we obtain

$$\Phi^\dagger_{x_\infty} = (f^\sharp_{x_\infty})_\natural. \tag{4.79}$$

Let e be the ramification index of $\Phi\colon X \to A$ at x_∞. Then the $b_e \in F_0$ of Section 4.6.1 is nonzero. We may assume that p is large enough that $e, b_e \not\equiv 0 \pmod{p}$. By (4.79) and (4.15), the coefficient of $\mathfrak{q}^e$ in $\Phi^\dagger_{x_\infty}$ is $\frac{b_e}{e}$ or $-u\frac{b_e}{e}$, where $u \not\equiv 0 \pmod{p}$; in either case this coefficient is nonzero mod p. Thus $\overline{\Phi^\dagger_{x_\infty}} \notin k$. Hence $\overline{\Phi^\dagger} \notin k$.

Finally, assume that we are in the Shimura-elliptic case. By (4.64),

$$\delta f^\flat_{x_0} \in (q', q'')R[[t]][t', t'']\hat{}. \tag{4.80}$$

By (4.5),

$$\begin{array}{rcl} q' & = & t' - G_1(t) \\ q'' & = & t'' - G_2(t, t'), \end{array} \tag{4.81}$$

for some $G_1(t) \in \mathbf{Z}[t]$ and $G_2(t, t') \in \mathbf{Z}[t, t']$. Denote by $G \mapsto G_\natural$ the substitution homomorphism

$$R[[t]][t', t'']\hat{} \to R[[t]]$$

sending t' to $G_1(t)$ and t'' to $G_2(t, t')$. Then $(q')_\natural = (q'')_\natural = 0$, so (4.64) and (4.80) imply $(f^\flat_{x_0})_\natural = (\delta f^\flat_{x_0})_\natural = 0$. Taking δ-Serre-Tate expansions in (4.75), taking $\natural$, and substituting (4.25), we obtain

$$\Phi^\dagger_{x_0} = \begin{cases} \psi(z_0) + \frac{1}{p}\sum_{n\geq 1}\left(\frac{b_n^{\phi^2}}{n}((t^{\phi^2})_\natural)^n - a_p\frac{b_n^\phi}{n}((t^\phi)_\natural)^n + p\frac{b_n}{n}t^n\right), & \text{if } A \text{ is not CL;} \\ \psi(z_0) + \frac{1}{p}\sum_{n\geq 1}\left(\frac{b_n^\phi}{n}((t^\phi)_\natural)^n - up\frac{b_n}{n}t^n\right), & \text{if } A \text{ is CL.} \end{cases} \tag{4.82}$$

Substituting the two formulas

$$(t^\phi)_\natural = (q^\phi - 1)_\natural = (q^p + pq' - 1)_\natural = q^p - 1 = (1+t)^p - 1 = pt + \cdots + t^p, \text{ and}$$
$$(t^{\phi^2})_\natural = (q^{\phi^2} - 1)_\natural = ((q^p + pq')^p + p((q')^p + pq'') - 1)_\natural = q^{p^2} - 1 = (1+t)^{p^2} - 1 = p^2t + \cdots + t^{p^2},$$

and recalling from Section 4.6.2 that $b_1 = 1$, we deduce that the coefficient of t in $\Phi^\dagger_{x_0}$ is $1 - a_p + p$ if A_R is not CL, and $1 - u$ if A_R is CL. This coefficient is nonzero mod p, since our non-anomalous assumption implies $a_p \not\equiv 1 \pmod{p}$ and we have $\bar{u}\bar{a}_p = 1$ in the CL case. So $\Phi^\dagger_{x_0} \notin R + pR[[t]]$. Hence $\overline{\Phi^\dagger} \notin k$. □

Proof of Theorem 3.17. Assume, in the proof of Theorem 3.5, that our modular-elliptic correspondence $S \xleftarrow{\Pi} X \xrightarrow{\Phi} A$ satisfies $S = X = X_1(N)$, $\Pi = \mathrm{Id}$, and Φ is a modular parametrization attached to a newform f. We may choose $g := E_{p-1}$ in Section 4.7; then $\bar{X}^\dagger = \overline{Y_1(N)}^{\mathrm{ord}} \setminus \{x \mid j(x) = 0, 1728\}$. Now (4.19) and (4.79) give the formula for $\Phi^\dagger_\infty$. □

The following lemma was needed to prove Theorem 3.24; the notation is as in Theorem 3.24.

Lemma 4.83. *Suppose that $\overline{\Theta} \in \mathcal{F}$. Assume that for every $P \in \mathcal{P}$ and every prime $l \neq p$ we have*

$$\sum_i \overline{\Theta}(\bar{P}_i^{(l)}) - a_l\overline{\Theta}(\bar{P}) = 0. \tag{4.84}$$

Then $\overline{\Theta} = \bar{\lambda}\overline{f^{(-1)}}$ for some $\bar{\lambda} \in k$.

Proof. Since $\overline{\Theta}$ is regular on $\overline{X_1(N)}^{\mathrm{ord}}$, there exists $m \in \mathbf{Z}_{\geq 1}$ such that $\bar{G} := \bar{E}_{p-1}^m \overline{\Theta}$ is a modular form over k on $\Gamma_1(N)$. View modular forms as functions on the set of triples (E, α, ω) where E is an elliptic curve over k, where $\alpha \colon \mathbf{Z}/n\mathbf{Z} \hookrightarrow E(k)$ is an injective homomorphism, and ω is a nonzero 1-form on E. Given $P \in \mathcal{P}$ and a prime $l \neq p$, choose (E, α, ω) such that (E, α) represents P, and choose $(E_i, \alpha_i, \omega_i)$ such that (E_i, α_i) represents $P_i^{(l)}$ and such that ω_i pulls back to ω under the l-isogeny $E \to E_i$. Then $\bar{E}_{p-1}(E_i, \alpha_i, \omega_i) = \bar{E}_{p-1}(E, \alpha, \omega)$ by [7, p. 269], for instance. Multiplying (4.84) by this yields

$$\sum_i \bar{G}(E_i, \alpha_i, \omega_i) = a_l \bar{G}(E, \alpha, \omega).$$

By [17, p. 452] or [21, p. 90], the left hand side equals $(lT(l)\bar{G})(E, \alpha, \omega)$. Since $\mathcal{P}$ is infinite, it follows that $lT(l)\bar{G} = a_l \bar{G}$ for all $l \neq p$. On the other hand, $\bar{G}(q) = \overline{\Theta}(q)$, and $U\overline{\Theta} = 0$, so $U\bar{G} = 0$. Furthermore $\bar{G}$ is invariant under the diamond operators. Thus $\bar{G}$ is a Hecke eigenform with the same eigenvalues as $\theta^{p-2}\bar{f}$, so by [17, p. 453], we have $\bar{G}(q) = \bar{\lambda} \cdot (\theta^{p-2}\bar{f})(q)$ for some $\bar{\lambda} \in k$. Thus $\overline{\Theta}(q) = \bar{\lambda}\overline{f^{(-1)}}(q)$, so $\overline{\Theta} = \bar{\lambda}\overline{f^{(-1)}}$. □

Proof of Theorem 3.25. Assume that we have a modular-elliptic correspondence. Pick $Q \in C$ represented by (E_Q, α_Q) where E_Q is given by $y^2 = x^3 + Ax + B$. By Lemma 4.55(1), there exists $\lambda \in R^\times$ such that $f_\lambda(A, B) = 0$. Let $X^\dagger \subset X$ satisfy the conclusions of Lemmas 4.45 and 4.61. View $f_\lambda^\flat$ and $f^\sharp$ as elements of $\mathcal{O}^2(X^\dagger)$; then $\overline{f_\lambda^\flat}, \overline{f^\sharp} \in \mathcal{O}^1(X^\dagger) \otimes_R k$ by (4.57) and (4.23), respectively. Let $\overline{\Phi^\sharp}$ be the image of $\overline{f^\sharp}$ in the ring $\mathcal{A}^\ddagger = \mathcal{O}(\bar{X}^\ddagger)$ of (4.58).

Claim. $\overline{\Phi^\ddagger}$ is non-constant on each irreducible component of $\bar{X}^\ddagger$.

If not, there is a minimal prime $\mathcal{P}$ of $\mathcal{A}^\ddagger$ such that the image of $\overline{\Phi^\ddagger}$ in $\mathcal{A}^\ddagger/\mathcal{P}$, and hence in $(\mathcal{A}^\ddagger/\mathcal{P}) \otimes_{\mathcal{A}^\dagger} k((\mathfrak{q}))$, is in k. By Lemma 4.59, $(\mathcal{A}^\ddagger/\mathcal{P}) \otimes_{\mathcal{A}^\dagger} k((\mathfrak{q}))$ is a nonzero product of copies of $k((\mathfrak{q}))$. By (4.60), the element

$$\overline{f_{x_\infty}^\sharp} \in k[[\mathfrak{q}]][\mathfrak{q}'] \subset k((\mathfrak{q}))[q']$$

is sent into an element of k by at least one of the $k((\mathfrak{q}))$-algebra homomorphisms

$$k((\mathfrak{q}))[q'] \to k((\mathfrak{q})), \tag{4.85}$$

denoted $s \mapsto s_*$ and defined by $(q')_* := \lambda_i q^p$. Since $q = \mathfrak{q}^M$, we have

$$q' = \delta(\mathfrak{q}^M) = \frac{(\mathfrak{q}^p + p\mathfrak{q}')^M - \mathfrak{q}^{pM}}{p} \equiv M\mathfrak{q}^{p(M-1)}\mathfrak{q}' \pmod{p},$$

so $\mathfrak{q}' \equiv M^{-1}\mathfrak{q}^{-p(M-1)}q' \pmod{p}$. Thus

$$(\mathfrak{q}')_* = M^{-1}\mathfrak{q}^{-p(M-1)}\lambda_i q^p = M^{-1}\lambda_i\mathfrak{q}^p \in \mathfrak{q}^p k[[\mathfrak{q}]].$$

Hence

$$(\overline{f_{x_\infty}^\sharp})_* \in (\overline{f_{x_\infty}^\sharp})_\natural + \mathfrak{q}^p k[[\mathfrak{q}]],$$

where we recall that $\natural$ means setting $\mathfrak{q}' = 0$. Let e be the ramification index of Φ at x_∞. Exactly as in the proof of Theorem 3.5, since $p \gg 0$, the coefficient of $\mathfrak{q}^e$ in $(\overline{f_{x_\infty}^\sharp})_\natural$ is nonzero. So $(\overline{f_{x_\infty}^\sharp})_*$ is not in k, a contradiction. This ends the proof of our Claim.

Now consider the set $\mathcal{C} := \Pi^{-1}(C) \cap X^\dagger(R)$ and let $P_1 \in \mathcal{C}$, $Q_1 := \Pi(P_1)$. Let E_{Q_1} be given by $y^2 = x^3 + A_1 x + B_1$. By choice of $X^\dagger$, we have $A_1 B_1 \not\equiv 0 \pmod{p}$. By Lemma 4.55, $f_\lambda^\flat(P_1) = 0$. Therefore the homomorphism $\mathcal{O}^1(X^\dagger) \to R$ sending a function to its value at P_1 induces a homomorphism $\mathcal{A}^\ddagger \to k$, which may be viewed as a point $\sigma(P_1) \in \bar{X}^\ddagger(k)$ mapping to $P_1 \in \bar{X}^\dagger(k)$. This defines $\sigma\colon \mathcal{C} \to\to \bar{X}^\ddagger(k)$. By definition of $\sigma(P_1)$ and $\Phi^\ddagger$, $\overline{f^\sharp(P_1)} = \overline{\Phi^\ddagger}(\sigma(P_1))$. Now, for $P_1, \dots, P_n \in \mathcal{C}$,

$$\begin{aligned} \sum_{i=1}^n m_i \overline{\Phi^\ddagger}(\sigma(P_i)) &= \sum_{i=1}^n m_i \overline{f^\sharp(P_i)} \\ &= \sum_{i=1}^n m_i \overline{\psi(\Phi(P_i))} \\ &= \overline{\psi\left(\sum_{i=1}^n m_i \Phi(P_i)\right)}, \end{aligned}$$

so the desired equivalence follows from Lemma 4.7(4).

The case of Shimura-elliptic correspondences is entirely similar, given Remark 4.74. We skip the details but point out one slight difference in the computations. The proof of the analogue of the Claim above, uses a $k[[t]]$-algebra homomorphism

$$k[[t]][t'] \to k[[t]],$$

denoted $s \mapsto s_*$, defined by requiring $(q')_* = \lambda_i q^q$, where $q = 1 + t$ and $q' = \delta(1 + t)$. Then one must check that for $f^\sharp_{x_0}$ as in (4.25), the coefficient of t in $(f^\sharp_{x_0})_*$ is nonzero mod p. This coefficient can be computed explicitly, and, unlike in the modular-elliptic case, its expression has contributions from all the terms with $n \geq 1$. Nevertheless all the contributions from terms with $n \geq 2$ turn out to be 0 mod p, and the coefficient in question turns out to be congruent mod p to either $1 - a_p$ or $1 - u$, and hence is nonzero mod p. □

The following will be used to prove Theorem 1.6:

Lemma 4.86. *Under the assumptions of Theorem 1.6 there is a constant γ depending only on N such that all the fibers of the reduction mod p map $C \to \overline{C}$ are finite of cardinality at most γ.*

Proof. Assume that we are in the modular-elliptic case; the Shimura-elliptic case follows by the same argument. Suppose that $Q_1, Q_2 \in C$ are such that $\bar{Q}_1 = \bar{Q}_2 \in S(k)$. Let Q_i be represented by (E_i, α_i), so there is an isogeny $u\colon E_1 \to E_2$ of degree $\prod l_j^{e_j}$ where the l_j are inert in $\mathcal{K}_Q$.

We claim that $E_1 \simeq E_2$. Since $\bar{E}_1 \simeq \bar{E}_2$, we may view $\bar{u}$ as an element of $\operatorname{End} \bar{E}_1$, which may be identified with a subring of the ring of integers $\mathcal{O}$ of $\mathcal{K}_Q$. The norm of this element equals $\deg \bar{u} = \deg u$, but the only elements of $\mathcal{O}$ whose norm is a product of inert primes are those in $\mathbf{Z} \cdot \mathcal{O}^\times$. Hence u factors as $E_1 \overset{n}{\to} E_1 \overset{\epsilon}{\to} E_2$ for some $n \in \mathbf{Z}$ and ϵ of degree 1. In particular, $E_1 \simeq E_2$.

By the claim, Lemma 4.86 holds with γ equal to the number of possible $\Gamma_1(N)$-structures on an elliptic curve. □

Proof of Theorem 1.6. By Lemma 4.86, the map

$$\Phi(\Pi^{-1}(C)) \cap \Gamma \to \overline{\Phi(\Pi^{-1}(C)) \cap \Gamma}$$

has finite fibers of cardinality bounded by a constant independent of Γ. On the other hand, by Corollary 3.29, the target of this map has cardinality at most cp^r for some c independent of Γ. □

Proof of Theorem 3.32. Assume, in the proof of Theorem 3.25, that we have a modular-elliptic correspondence arising from a modular parametrization attached to f. Part (1) follows from Lemma 4.62. Part (2) follows comparing Fourier expansions of the two sides: apply the substitution maps as in (4.85) to $\overline{f^{\sharp}_{\infty}}$ given in (4.14) to obtain the p different series

$$\overline{\Phi^{\ddagger}}_{\infty i} = (\overline{f^{\sharp}_{\infty}})_* = \overline{\Phi^{\dagger}}(q) + \overline{\lambda}_i \overline{\Phi^{\dagger\dagger}}(q) \in k((q))$$

where $\lambda_1, \dots, \lambda_p \in k$ are the zeros of $x^p - \bar{\lambda}x$ as in the proof of Lemma 4.59. □

Appendix A. Non-existence of reciprocity in the global case

Let $S \xleftarrow{\Pi} X \xrightarrow{\Phi} A$ be a modular-elliptic or a Shimura-elliptic correspondence and let $X^\dagger \subset X$ be a dense open subscheme. Ideally we would like a description of the group of divisors $\sum m_i P_i$ on $X^\dagger$ supported in $\Pi^{-1}(\mathrm{CM})$ such that $\sum m_i \Phi(P_i) \in A(\overline{\mathbf{Q}})_{\mathrm{tors}}$. More precisely, in analogy with the "local" result Theorem 3.5, one may ask if there exists a regular function $\Phi^\dagger$ on $X^\dagger$ such that for any divisor $\sum m_i P_i$ on $X^\dagger$ supported in $\Pi^{-1}(\mathrm{CM})$ we have that $\sum m_i \Phi(P_i) \in A(\overline{\mathbf{Q}})_{\mathrm{tors}}$ if and only if $\sum m_i \Phi^\dagger(P_i) = 0$. We could refer to such a $\Phi^\dagger$ as a *reciprocity function for* CM *points.*

A.1. Non-existence of global reciprocity functions for isogeny classes and CM points.

But even in the "most classical" case of modular-elliptic correspondences arising from a newform, no such function exists:

Theorem A.1 (Non-existence of reciprocity functions for CM points)**.** *Let $\Phi : X_1(N) \to A$ be a modular parametrization. Assume that there is a non-empty open subscheme $X^\dagger \subset X_1(N)$ and a regular function $\Phi^\dagger \in \mathcal{O}(X^\dagger)$ having the property that for any $P_1, \dots, P_n \in \mathrm{CM} \cap X^\dagger(\overline{\mathbf{Q}})$ and any $m_1, \dots, m_n \in \mathbf{Z}$ we have*

$$\sum_{i=1}^{n} m_i \Phi(P_i) \in A(\overline{\mathbf{Q}})_{\mathrm{tors}} \quad \Rightarrow \quad \sum_{i=1}^{n} m_i \Phi^\dagger(P_i) = 0 \in \overline{\mathbf{Q}}.$$

Then $\Phi^\dagger = 0$.

Theorem A.1 follows immediately from the following isogeny class analogue applied to an isogeny class of CM points.

Theorem A.2 (Non-existence of reciprocity functions for isogeny classes)**.** *Let $\Phi \colon S = X_1(N) \to A$ be a modular parametrization. Let $C \subset S(\overline{\mathbf{Q}})$ be an isogeny class and let $\Phi^\dagger$ be a rational function on S none of whose poles is in C. Assume that for any $P_1, \dots, P_n \in C$ and any $m_1, \dots, m_n \in \mathbf{Z}$ we have*

$$\sum_{i=1}^{n} m_i \Phi(P_i) \in A(\overline{\mathbf{Q}})_{\mathrm{tors}} \quad \Rightarrow \quad \sum_{i=1}^{n} m_i \Phi^\dagger(P_i) = 0 \in \overline{\mathbf{Q}}. \tag{A.3}$$

Then $\Phi^\dagger = 0$.

Proof. We use Hecke correspondence notation as in Section 3.2. Extend Φ linearly to a homomorphism $\Phi_*\colon \operatorname{Div}^0(X_1(N)(\overline{\mathbf{Q}})) \to A(\overline{\mathbf{Q}})$. Then $\Phi_* \circ T(l)_* = a_l \cdot \Phi_*$; see [14, p. 242]. For any point $P \in C$ we have $T(l)_*(P - \infty) = \sum P_i^{(l)} - \sum P_{i0}^{(l)}$ with $P_{i0}^{(l)}$ cusps. We get

$$\begin{aligned} a_l \cdot \Phi(P) &= a_l(\Phi_*(P-\infty)) \\ &= \Phi_*(T(l)_*(P-\infty)) \\ &= \Phi_*(\textstyle\sum P_i^{(l)} - \sum P_{i0}^{(l)}) \\ &= \textstyle\sum \Phi(P_i^{(l)}) - \sum \Phi(P_{i0}^{(l)}) \end{aligned} \tag{A.4}$$

By the Manin-Drinfeld theorem (see [23, p. 62], for instance), $\Phi(P_{i0}^{(l)}) \in A(\overline{\mathbf{Q}})_{\mathrm{tors}}$, so (A.4) yields

$$\sum \Phi(P_i^{(l)}) - a_l \cdot \Phi(P) \in A(\overline{\mathbf{Q}})_{\mathrm{tors}}. \tag{A.5}$$

By (A.3), we obtain $\sum_i \Phi^\dagger(P_i^{(l)}) - a_l \cdot \Phi^\dagger(P) = 0$. Now Lemma A.6 below implies $\Phi^\dagger = 0$. □

Lemma A.6. *Let $S = X_1(N)$. Let $f = \sum a_n q^n$ be a weight-2 newform on $\Gamma_1(N)$. let $C \subset S(\overline{\mathbf{Q}})$ be an isogeny class. Let $\Phi^\dagger$ be a rational function on S none of whose poles are in C. Assume that for infinitely many primes l and for any $P \in C$ we have*

$$\sum_i \Phi^\dagger(P_i^{(l)}) - a_l \Phi^\dagger(P) = 0. \tag{A.7}$$

Then $\Phi^\dagger = 0$.

Proof. Assume that $\Phi^\dagger \neq 0$. The function

$$(T(l)\Phi^\dagger)(x) := \sum \Phi^\dagger(x_i^{(l)}),$$

defined for all but finitely many $x \in S(\mathbf{C})$, is a rational function on S by [39, p. 55]. For the infinitely many given l, the rational functions $T(l)\Phi^\dagger$ and $\Phi^\dagger$ agree on the infinite set C so they coincide. Since $\Phi^\dagger$ may be viewed as a ratio of modular forms over $\overline{\mathbf{Q}}$, each of which is a $\overline{\mathbf{Q}}$-linear combination of newforms whose Fourier coefficients are algebraic integers, the Fourier expansion $\varphi(q)$ of $\Phi^\dagger$ is in $\mathcal{O}_{\mathcal{K},\mathcal{S}}((q))$ for some ring of $\mathcal{S}$-integers in some number field $\mathcal{K}$, with $\mathcal{S}$ finite. We may restrict attention to primes $l \nmid N$ not lying under any prime in $\mathcal{S}$. We may assume also that the leading coefficient of $\varphi(q)$ is prime to l. The q-values corresponding to the elliptic curves l-isogenous to the one corresponding to q itself are q^l and the l-th roots of q, so taking Fourier expansions in $T(l)\Phi^\dagger = \Phi^\dagger$ yields

$$\varphi(q^l) + \sum_{b=0}^{l-1} \varphi(\zeta^b q^{1/l}) = a_l \varphi(q), \tag{A.8}$$

where ζ is a primitive l-th root of 1. Let v_q be the valuation on $\overline{\mathbf{Q}}((q))$. Comparing leading terms in (A.8) yields $v_q(\varphi) \geq 0$; and if $v_q(\varphi) = 0$, then $l + 1 = a_l$, which contradicts $|a_l| \leq 2\sqrt{l} < l + 1$. Thus $v_q(\varphi) > 0$.

The series $\sum_{b=0}^{l-1} \varphi(\zeta^b q^{1/l})$ is divisible by l, so

$$\varphi(q^l) \equiv a_l \varphi(q) \pmod{l\mathcal{O}_{\mathcal{K},\mathcal{S}}[[q]].)} \tag{A.9}$$

The leading coefficient of $\varphi(q^l)$ equals that of $\varphi(q)$, so it is prime to l. Then (A.9) shows that a_l is prime to l. Now (A.9) contradicts $v_q(\varphi) > 0$. $\square$

A.2. **Non-existence of geometric reciprocity functions.** Finally we prove that there are no purely geometric reasons for the existence of reciprocity functions; thus the existence of reciprocity functions in the local setting is a truly arithmetic phenomenon.

Theorem A.10 (Non-existence of geometric reciprocity functions). *Let $\Phi\colon X \to A$ be a non-constant morphism between smooth projective curves over an algebraically closed field k of characteristic $p \geq 0$, where A is an elliptic curve. Let $n \geq 3$, and let $a_1, \ldots, a_n$ be nonzero integers not all divisible by p. Suppose that $X^\dagger \subset X$ is an affine open subset and $\Phi^\dagger \in \mathcal{O}(X^\dagger)$ is a regular function such that for any $P_1, \ldots, P_n \in X^\dagger(k)$ we have*

$$\text{(A.11)} \qquad \sum_{i=1}^{n} a_i \Phi(P_i) = 0 \quad \Longrightarrow \quad \sum_{i=1}^{n} a_i \Phi^\dagger(P_i) = 0.$$

Then $\Phi^\dagger$ is constant. In particular, if $\sum_{i=1}^n a_i$ is not divisible by p, then $\Phi^\dagger = 0$.

Remark A.12. Theorem A.10 fails for both $n = 1$ and $n = 2$. Let A be any elliptic curve over k, let $X = A$, let Φ be the identity, and let $X^\dagger \subsetneq X$ any nonempty affine open subset. For $n = 1$, one obtains a counterexample by taking $a_1 = 1$ and $\Phi^\dagger \in \mathcal{O}(X^\dagger)$ any non-constant regular function vanishing at the origin (if the origin is in $X^\dagger$). For $n = 2$, one obtains a counterexample by taking $a_1 = 1$, $a_2 = -1$, and $\Phi^\dagger \in \mathcal{O}(X^\dagger)$ any non-constant regular function. Alternatively, for $n = 2$, one can take $a_1 = a_2 = 1$ and $\Phi^\dagger$ a nonconstant rational function that is anti-invariant for the negation map on X (shrink $X^\dagger$ if necessary), such as the y-coordinate on a short Weierstrass model in characteristic not 2; this shows that the final sentence of Theorem A.10 can fail too.

Proof of Theorem A.10. Without loss of generality, $p \nmid a_1$. To prove that $\Phi^\dagger$ is constant, it will suffice to show that $\Phi^\dagger$ is regular at every $P \in X(k)$.

Fix P. Let Y be the inverse image of $\{0\}$ under the morphism

$$\begin{aligned} \beta\colon X \times (X^\dagger)^{n-1} &\to A \\ (P_1, \ldots, P_n) &\mapsto \sum a_i \Phi(P_i). \end{aligned}$$

Let $\pi_i\colon Y \to X$ be the i-th projection. The morphism $\pi_1\colon Y \to X$ is surjective since given P_1, if we choose $P_4, \ldots, P_n \in X^\dagger(k)$ arbitrarily, then there are only finitely many choices of $P_2 \in X^\dagger$ such that the equation $\beta(P_1, \ldots, P_n) = 0$ forces $P_3 \notin X^\dagger$. In particular, we can find a smooth irreducible curve C and a morphism $\gamma\colon C \to Y$ such that $\pi_1(\gamma(C))$ is a dense subset of X containing P.

By (A.11), we have $\sum a_i \Phi^\dagger(P_i) = 0$ for all $(P_1, \ldots, P_n) \in Y \cap (X^\dagger)^n$. In particular,

$$\sum_{i=1}^{n} a_i \Phi^\dagger(\pi_i(\gamma(c))) = 0$$

is an identity of rational functions of $c \in C$. Since $\Phi^\dagger$ is regular on $X^\dagger$, the last $n - 1$ summands are regular on C. Therefore the first summand is regular too. So $a_1 \Phi^\dagger$ is regular on $\pi_1(\gamma(C))$. Since $a_1 \neq 0$ in k, and $P \in \pi_1(\gamma(C))$, the function $\Phi^\dagger$ is regular at P. $\square$

References

1. Barcau, M.:Isogeny covariant differential modular forms and the space of elliptic curves up to isogeny, Compositio Math. **137** (2003), 237–273.
2. Breuil C., Conrad B., Diamond F., Taylor R.: On the modularity of elliptic curves over **Q**: wild 3-adic exercises, J. Amer. Math. Soc. **14** (2001), no. 4, 843–939.
3. Buium, A.: Differential characters of abelian varieties over p-adic fields, Invent. Math. **122** (1995), 309–340.
4. Buium, A.: Differential characters and characteristic polynomial of Frobenius, J. reine angew. Math. **485** (1997), 209–219.
5. Buium, A.: Differential modular forms, J. reine angew. Math., **520** (2000), 95–167.
6. Buium, A.: Differential modular forms on Shimura curves, I, Compositio Math. **139** (2003), 197–237.
7. Buium, A.: Arithmetic Differential Equations. Math. Surveys and Monographs **118**, AMS (2005).
8. Buium, A., Poonen, B.: Independence of points on elliptic curves arising from special points on modular and Shimura curves, I: global results, to appear in *Duke Math. J.*
9. Buzzard, K.: Integral models of certain Shimura curves, Duke Math J. **87** (1997), no. 3, 591–612.
10. Chai C-L.: A note on Manin's Theorem of the Kernel, Amer. J. Math. **113** (1991), no. 3, 387–389.
11. Conrad, B.: The Shimura Construction in weight 2. Appendix to: Ribet, K. A., Stein, W.: Lectures on Serre's conjecture. In: Arithmetic Algebraic Geometry, Conrad, B., Rubin K., Eds., IAS/Park City Math Series, Vol. 9, AMS (2001).
12. Cornut, C.: Mazur's conjecture on higher Heegner points, Invent. Math. **148** (2002), 495–523.
13. Diamond, F., and Im, J.: Modular forms and modular curves. In: Seminar on Fermat's Last Theorem, Conference Proceedings, Volume 17, Canadian Mathematical Society, pp. 39–134 (1995).
14. Diamond, F., Shurman, J.: A first course in modular forms. GTM 228, Springer (2005)
15. Dwork, B., Ogus, A.: Canonical liftings of Jacobians, Compositio Math. **58** (1986), 111–131.
16. Faltings, G.: Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, Invent. Math. **73** (1983), 349–366.
17. Gross B.: A tameness criterion for Galois representations associated to modular forms mod p, Duke Math. J. **61** (1990), no. 2, 445–517.
18. Gross B., Zagier D.: Heegner points and derivatives of L-series, Invent. Math. **84** (1986), no. 2, 225–320.
19. Gross B., Kohnen W., Zagier D.: Heegner points and derivatives of L-series II, Math. Ann. **278** (1987), nos. 1–4, 497–562.
20. Hurlburt, C.: Isogeny covariant differential modular forms modulo p, Compositio Math., **128** (2001), no. 1, 17–34.
21. Katz, N.: p-adic properties of modular schemes and modular forms, LNM 350, Springer 1973, 69–190.
22. Katz, N.: Serre-Tate local moduli, Springer LNM 868 (1981), 138–202.
23. Lang, S.: Introduction to Modular forms. Springer, Heidelberg (1976)
24. Kolyvagin, V. A.: Finiteness of $E(\mathbf{Q})$ and $SH(E,\mathbf{Q})$ for a subclass of Weil elliptic curves, Izv. Akad. Nauk SSSR Ser. Mat. **52** (1988), no. 3, 522–540.
25. Manin, Yu. I.: Algebraic curves over fields with differentiation, Izv. Akad. Nauk SSSR, Ser. Mat. **22**, 737–756 (1958)
26. Manin Yu. I.: Rational points of algebraic curves over function fields, Izv. Akad. Nauk SSSR Ser. Mat. **27** (1963), 1395–1440.
27. Mazur, B.: Rational points of abelian varieties with values in towers of number fields, Invent. Math. **18** (1972), 183–266.
28. Mazur, B.: Modular curves and arithmetic, Proc. ICM, Warsaw, 1983, PWN (1984), 185–211.
29. Messing, W.: The Crystals Associated to Barsotti-Tate Groups, LNM 264, Springer 1972.
30. Mumford, D.: Abelian varieties, Oxford University Press, 1970.
31. Nekovár, J. and Schappacher, N.: On the asymptotic behaviour of Heegner points, Turkish J. Math. **23** (1999), 549–556.
32. Ogus, A.: Hodge cycles and crystalline cohomology, pp. 357–414. In: Hodge cycles, motives and Shimura varieties, by P. Deligne, J. Milne, A. Ogus, and K.-y. Shih, Lecture Notes in Math. **900**, Springer-Verlag, 1982.

33. Pink, R.: A combination of the conjectures of Mordell-Lang and André-Oort, pp. 251–282. In: Geometric methods in algebra and number theory, Progr. Math. **235**, Birkhäuser, 2005.
34. Poonen, B.: Mordell-Lang plus Bogomolov, Invent. Math. **137** (1999), 413–425.
35. Rosen, M., and Silverman, J. H.: On the independence of Heegner points associated to distinct imaginary fields, arXiv.math.NT/0508259v2, 15 August 2005, to appear in J. Number Theory.
36. Serre, J.-P.: Complex multiplication, pp. 292–296 in Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), Thompson, 1967.
37. Serre, J.-P.: Propriétés galoisennes des point d'ordre fini des courbes elliptiques, Invent. Math. **15** (1972), 259–331.
38. Serre, J.-P.: Formes modulaires et fonctions zéta p-adiques. In: Springer Lecture Notes in Math. **350** (1973).
39. Serre, J.-P.: Algebraic groups and class fields, GMT 117, Springer, Heidelberg, New York, 1988.
40. Serre, J.-P.: Topics in Galois theory, Jones and Bartlett, Boston, 1992.
41. Shimura, G.: Introduction to the arithmetic theory of automorphic functions, Princeton Univ. Press, 1971.
42. Silverman, J. H.: Hecke points on modular curves, Duke Math. J. **60** (1990), 401–423.
43. Silverman, J. H.: Wieferich criterion and the abc conjecture, J. Number Theory **30** (1988), 226–237.
44. Taylor R., Wiles A.: Ring-theoretic properties of certain Hecke algebras, Annals of Math. (2) **141** (1995), no. 3, 553–572.
45. Vatsal V.: Uniform distribution of Heegner points, Invent. Math. **148** (2002), 1–48.
46. J.F.Voloch: Elliptic Wieferich primes, J. Number Theory **81** (2000), no. 2, 205-209.
47. Wiles, A.: Modular elliptic curves and Fermat's Last Theorem, Annals of Math. (2) **141** (1995), no. 3, 443–551.
48. Zhang, S.: Heights of Heegner points on Shimura curves, Annals of Math. (2) **153** (2001), 27–147.

University of New Mexico, Albuquerque, NM 87131
E-mail address: `buium@math.unm.edu`
URL: `http://math.unm.edu/~buium`

Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139-4307, USA
E-mail address: `poonen@math.mit.edu`
URL: `http://math.mit.edu/~poonen`