INVARIANTS OF MODULAR CURVES AND SHARIFI'S CONJECTURES

by

Jun Wang

A Dissertation Submitted to the Faculty of the

DEPARTMENT OF MATHEMATICS

In Partial Fulfillment of the Requirements

For the Degree of

DOCTOR OF PHILOSOPHY

In the Graduate College

THE UNIVERSITY OF ARIZONA

2018

THE UNIVERSITY OF ARIZONA
GRADUATE COLLEGE

As members of the Dissertation Committee, we certify that we have read the dissertation prepared by Jun Wang, titled Invariants of modular curves and Sharifi's conjectures and recommend that it be accepted as fulfilling the dissertation requirement for the Degree of Doctor of Philosophy.

Romyar Sharifi — Date: 19 June 2018

Bryden Cais — Date: 19 June 2018

Brandon Levin — Date: 19 June 2018

William McCallum — Date: 19 June 2018

Final approval and acceptance of this dissertation is contingent upon the candidate's submission of the final copies of the dissertation to the Graduate College.

I hereby certify that I have read this dissertation prepared under my direction and recommend that it be accepted as fulfilling the dissertation requirement.

Dissertation Director: Romyar Sharifi — Date: 19 June 2018

Dissertation Director: Bryden Cais — Date: 19 June 2018

STATEMENT BY AUTHOR

This dissertation has been submitted in partial fulfillment of the requirements for an advanced degree at the University of Arizona and is deposited in the University Library to be made available to borrowers under rules of the Library.

Brief quotations from this dissertation are allowable without special permission, provided that accurate acknowledgment of the source is made. Requests for permission for extended quotation from or reproduction of this manuscript in whole or in part may be granted by the head of the major department or the Dean of the Graduate College when in his or her judgment the proposed use of the material is in the interests of scholarship. In all other instances, however, permission must be obtained from the author.

SIGNED: Jun Wang

ACKNOWLEDGEMENTS

Foremost, I would like to express my sincere gratitude to my advisor Prof. Romyar Sharifi for the continuous support of my Ph.D. study and research, for his patience, motivation, enthusiasm, and immense knowledge. His guidance helped me in all the time of research and writing of this thesis. I could not have imagined having a better advisor and mentor for my Ph.D study.

Besides my advisor, I would like to thank the rest of my thesis committee: Prof. Bryden Cais, Prof. Brandon Levin and Prof. William McCallum for their encouragement, insightful comments, and hard questions. During the years in Arizona, I have learned a great deal about number theory from conversations with Prof. David Savitt, Prof. Dinesh Thakur, and Prof. Kirti Joshi.

I would like to thank Preston Wake, for answering my questions about his preprint. I would like to thank Emmanuel Lecouturier, for sending me his papers and answering my questions. I would like to thank Ashay Burungale and Yiwen Zhou, for answering my questions during all these years.

I would like to thank my friends in the department of Mathematics in the University of Arizona: Ding Ma, Sheng-Chi Shih, Shuhui Shi, Lanbo Fang, Yuan Tao, Jinjin Liang, Liang Wu, Miao Zhang, Xiyuan Wang, Hyereen Lee, Angelica Gonzalez, Cody Lee Gunton, Daniel John Rossi, Kyle Jeffery Pounder, Ryan Coatney, for the discussions, and for all the fun we have had in the last six years. I would like to thank my friends Min Xiao and Ya Lin for teaching me things outside mathematics.

Last but not the least, I would like to thank my family: my parents Cunshan Wang, Xiaoming Zhou, for understanding and supporting me throughout my life.

TABLE OF CONTENTS

TABLE OF CONTENTS – *Continued*

ABSTRACT

We compute some invariants attached to the Eisenstein quotient of an etale cohomology group of the modular curve $X_0(N)$ for $N \geq 5$. We also give a relation between one of the invariants and Sharifi's conjecture on the modular curve $X_1(N)$.

CHAPTER 1

Introduction

A modular curve is an algebraic curve obtained from a quotient space $\Gamma\backslash\mathbb{H}$, where Γ is a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ and $\mathbb{H}$ is the Poincaré half-plane. More generally, it is a moduli space of elliptic curves with additional level structure. The theory of modular curves has been widely used in number theory. In Mazur's seminal work [18], he studied the arithmetic properties of the modular curve $X_0(N)$ in detail. For example, Mazur gave a very nice description of the Eisenstein component $\mathfrak{h}$ of the p-adic cuspidal Hecke algebra of this modular curve. For a prime $p \geq 5$, he proved that there is an isomorphism $\mathbb{Z}_p/(N-1)\mathbb{Z}_p \to \mathfrak{h}/I$, and the p-adic Hecke algebra $\mathfrak{h}$ is Gorenstein. Moreover, he gave a description of the Eisenstein kernel of the p-divisible group $J[p^\infty]$ attached to the modular Jacobian $J := \mathrm{Jac}(X_0(N))$. That is, he proved that $J[I, p^\infty] \cong C \oplus \Sigma$, where $I \subset \mathfrak{h}$ is the Eisenstein ideal, C is a constant group scheme generated by the image of divisor $(0) - (\infty)$, and Σ is a multiplicative group scheme which is called the Shimura subgroup. Note that we have a Galois-equivariant

perfect pairing

$$H \times J[p^\infty] \to \mathbb{Q}_p/\mathbb{Z}_p, \tag{1.1}$$

where $H := H^1_{\text{ét}}(X_0(N)_{/\bar{\mathbb{Q}}}, \mathbb{Z}_p)$, and the Hecke operators are self-adjoint with respect to this pairing.

Thus, we get a corresponding $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module decomposition of H/IH

$$H/IH \cong H^+/IH^+ \oplus H^-/IH^-. \tag{1.2}$$

Here, $\pm$ denotes the decomposition under complex conjugation. Via (1.1), $H^+/IH^+ = \text{Hom}(C, \mathbb{Q}_p/\mathbb{Z}_p)$ and $H^-/IH^- = \text{Hom}(\Sigma, \mathbb{Q}_p/\mathbb{Z}_p)$. It is easy to see that H^+/IH^+ is a trivial $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module, and the action of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on H^-/IH^- is via χ_p^{-1}, where χ_p is the p-adic cyclotomic character.

One natural question is: what can we say about the $\mathfrak{h}[\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})]$-module H/I^2H?

Let $K = \mathbb{Q}(\zeta_q)$, where q is the highest power of p dividing $N-1$. Viewing H/I^2H as representation of $\text{Gal}(\overline{\mathbb{Q}}/K)$, we have following four **group homomorphisms**:

1. $a : \text{Gal}(\overline{\mathbb{Q}}/K) \to \text{Aut}_{\mathfrak{h}}(H^-/I^2H^-)$,

2. $b : \text{Gal}(\overline{\mathbb{Q}}/K) \to \text{Hom}_{\mathfrak{h}}(H^+/I^2H^+, H^-/I^2H^-)$,

3. $c : \text{Gal}(\overline{\mathbb{Q}}/K) \to \text{Hom}_{\mathfrak{h}}(H^-/I^2H^-, H^+/I^2H^+)$,

4. $d : \mathrm{Gal}(\overline{\mathbb{Q}}/K) \to \mathrm{Aut}_{\mathfrak{h}}(H^+/I^2H^+)$.

One can prove that the homomorphisms a and d cut out a field extension F_0, the homomorphism b cuts out a field F_{-1}, and the homomorphism c cuts out a field F_1, where F_i means that the group $\mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q})$ acts on $\mathrm{Gal}(F_i/K)$ via χ_p^i.

Let $U = \mathbb{F}_N^\times/(\mathbb{F}_N^\times)^q$. Using global class field theory, we have the following canonical isomorphisms of abelian groups:

1. $\mathrm{Gal}(F_0/K) \cong U$,

2. $\mathrm{Gal}(F_1/K) \cong \mu_q$,

3. $\mathrm{Gal}(F_{-1}/K) \cong U^{\otimes 2} \otimes \mu_q^{-1}$,

where $\mu_q^{-1} = \mathrm{Hom}(\mu_q, \mathbb{Z}/q\mathbb{Z})$. The F_i are class fields, and all of them are totally tamely ramified at N over K.

In [18], Mazur uses modular symbols to construct a canonical winding isomorphism:

$$e : I/I^2 \xrightarrow{\sim} H^-/IH^- \otimes \mu_q \xrightarrow{\sim} U. \tag{1.3}$$

In [18], Mazur also proved that H^+, H^- are both free $\mathfrak{h}$-modules of rank 1, which means that H^+/I^2H^+ and H^-/I^2H^- are free $\mathfrak{h}/I^2$-modules of rank one. We know that the images of a, d are both in $1 + I/I^2$. Since there is an canonical isomorphism

between the multiplicative abelian group $1 + I/I^2$ and the additive abelian group I/I^2, we may view a and d as homomorphisms:

1. $a : U \to I/I^2$,

2. $d : U \to I/I^2$.

By composing with the winding homomorphism (1.3), we get maps $I/I^2 \to I/I^2$ that are multiplication by an integer in $\mathbb{Z}/q\mathbb{Z}$. We use $\widetilde{a}$ and $\widetilde{d}$ to denote these two numbers. The invariants $\widetilde{a}$ and $\widetilde{d}$ have been already computed by B. Mazur, F. Calegari, R. Sharifi and W. Stein in the unpublished manuscript [19], and their results are $\widetilde{a} = -1, \widetilde{d} = 1$.

For the homomorphisms b and c, we need a more careful analysis. We carefully choose a generator of H^+/IH^+: see Remark 3.3.21. For H^-/IH^-, we can identify it with $I/I^2 \otimes \mu_q^{-1}$ using (1.3).

By (1.2), one can see that the image of b is in $\mathrm{Hom}_{\mathfrak{h}}(H^+/IH^+,\, IH^-/I^2H^-)$ and the image of c is in $\mathrm{Hom}_{\mathfrak{h}}(H^-/IH^-, IH^+/I^2H^+)$.

Since

1. $\mathrm{Hom}_{\mathfrak{h}}(H^+/IH^+,\, IH^-/I^2H^-) \cong IH^-/I^2H^- \cong I^2/I^3 \otimes \mu_q^{-1}$,

2. $\mathrm{Hom}_{\mathfrak{h}}(H^-/IH^-, IH^+/I^2H^+) \cong \mathrm{Hom}_{\mathfrak{h}}(I/I^2 \otimes \mu_q^{-1}, I/I^2) \cong \mu_q$,

we can rewrite b and c as follows:

1. $b : \mathrm{Gal}(F_{-1}/K) \cong U^{\otimes 2} \otimes \mu_q^{-1} \cong I^2/I^3 \otimes \mu_q^{-1} \to I^2/I^3 \otimes \mu_q^{-1}$,

2. $c : \mathrm{Gal}(F_1/K) \cong \mu_q \to \mu_q$.

Hence the homomorphisms b and c give us two integers in $\mathbb{Z}/q\mathbb{Z}$ which were constructed in [19]. Let's use $\widetilde{b}$ and $\widetilde{c}$ to denote them. The integers $\widetilde{b}$ and $\widetilde{c}$ are units in $\mathbb{Z}/q\mathbb{Z}$, which can be seen using [4], or [35]. What we want to understand are the exact values of $\widetilde{b}$ and $\widetilde{c}$ based on the canonical winding isomorphism $I/I^2 \cong U$ in (1.3). Our result is $\tilde{c} = 1$. For the details, see Theorem 4.3.10.

The homomorphism b has a conjectural inverse which is closely related to Sharifi's conjectures for the modular curve $X_1(N)$. In [32], Sharifi formulated a series of remarkable conjectures which relate the arithmetic of cyclotomic fields to the homology of modular curves. Roughly speaking, he used cup products of cyclotomic units to define two maps:

$$\varpi^0 : \widetilde{H}_1^+ \to H^2(\mathbb{Z}[\tfrac{1}{Np}, \zeta_N], \mathbb{Z}_p(2))^+, \quad \varpi : H_1^+ \to H^2(\mathbb{Z}[\tfrac{1}{p}, \zeta_N], \mathbb{Z}_p(2))^+, \tag{1.4}$$

where $\widetilde{H}_1 := H_1(X_1(N), \tilde{C}_\infty, \mathbb{Z}_p)$, $\tilde{C}_\infty$ is the set of cusps of $X_1(N)$ that lie above the ∞-cusp of $X_0(N)$ and $H_1 := H_1(X_1(N), \mathbb{Z}_p)$. The map ϖ^0 takes the adjusted Manin symbol $[u, v]^*$ (Defintion 4.4.11) to the cup product $(1 - \zeta_N^u, 1 - \zeta_N^v)$.

Conjecture 1.0.1 (Sharifi)**.** *Let $\mathfrak{I}_\infty$ be the ideal of the modular Hecke algebra generated by $T_l - 1 - \langle l \rangle l$ for $l \nmid N$, and $T_N - 1$, and let I_∞ be the image of $\mathfrak{I}_\infty$ in the cuspidal Hecke algebra. Then ϖ^0, ϖ induce maps:*

$$\varpi^0 : \widetilde{H}_1^+ / \mathfrak{I}_\infty \widetilde{H}_1^+ \to H^2(\mathbb{Z}[\tfrac{1}{Np}, \zeta_N], \mathbb{Z}_p(2))^+,$$

$$\varpi : H_1^+ / I_\infty H_1^+ \to H^2(\mathbb{Z}[\tfrac{1}{p}, \zeta_N], \mathbb{Z}_p(2))^+.$$

In [9], Fukaya and Kato proved these conjectures for the modular curve $X_1(N)$ when $p \mid N$. For modular curves with level not divisible by p, the conjecture is still open.

By using the following theorem in [18], one can connect the homology of $X_0(N)$ with the cohomology of $X_1(N)$,

Theorem 1.0.2 (Mazur)**.** *Let $\pi : X_1(N) \to X_0(N)$ be the natural map between modular curves. Then we have an isomorphism*

$$\pi_* : H_1^+ / (I_\infty + I_G) H_1^+ \cong I H^-(1) / I^2 H^-(1),$$

where $G = (\mathbb{Z}/N\mathbb{Z})^\times / \{\pm 1\}$.

Conjecture 1.0.3. *Viewing b as an element in* $\mathrm{Hom}(\mathrm{Gal}(F_{-1}/K), H_1^+/(I_\infty + I_G)H_1^+)$

and assuming the Eisenstein quotient conjecture, we have

$$b \circ \varpi_G = 1,$$

where ϖ_G is the map induced on G-coinvariants by ϖ.

Assuming Conjecture 1.0.1 and Conjecture 1.0.3, we use the properties of ϖ^0 to compute the invariant $\widetilde{b}$. Our result is $\widetilde{b} = 1$; for the details, see Theorem 4.4.41.

In [9], Fukaya and Kato defined a map $\infty : H^2_{\text{ét}}(\mathcal{Y}_1(N) \otimes \mathbb{Z}[\frac{1}{p}], \mathbb{Z}_p(2)) \to H^2(\mathbb{Z}[\zeta_N, \frac{1}{Np}], \mathbb{Z}_p(2))^+$, where $\mathcal{Y}_1(N)$ (Definition 2.1.1) is the moduli scheme over $\mathbb{Z}[\frac{1}{N}]$ with $\mathbb{C}$-points $Y_1(N)(\mathbb{C})$. And they proved that this map factors through the Eisenstein ideal when restricted to the submodule generated by the elements $g_{0,\frac{u}{N}} \cup g_{0,\frac{v}{N}}$, where $g_{0,\frac{u}{N}}$ and $g_{0,\frac{v}{N}}$ are Siegel units. One can check directly that

$$\infty(g_{0,\frac{u}{N}} \cup g_{0,\frac{v}{N}}) = (1 - \zeta_N^u, 1 - \zeta_N^v).$$

If we can prove that the map

$$\rho' : \widetilde{H}_1 \to H^2_{\text{ét}}(\mathcal{Y}_1(N) \otimes \mathbb{Z}[\tfrac{1}{p}], \mathbb{Z}_p(2)),$$

$$[u, v]^* \mapsto g_u \cup g_v,$$

is well-defined and Hecke-equivariant, then Conjecture 1.0.1 is true.

For $p \nmid N$, in Chapter 5, under some assumptions, we use the method in [9] to prove the well-defined property and the Hecke-equivariance of the map:

$$\rho' \otimes \mathbb{Q}_p : \widetilde{H}_1 \to H^2_{\text{ét}}(\mathcal{Y}_1(N) \otimes \mathbb{Z}[\tfrac{1}{p}], \mathbb{Z}_p(2)) \otimes \mathbb{Q}_p,$$

In Chapters 2 and 3, we review the general theory of modular curves and Mazur's work on $X_0(N)$. In Chapter 4, we compute the invariants assuming Sharifi's conjectures. In Chapter 5, we list some partial results on Sharifi's conjectures.

CHAPTER 2

Background

Notation 2.0.1. *Let $N \geq 5$ and $p \geq 5$ be prime numbers such that $N \neq p$. We fix an embedding $\overline{\mathbb{Q}} \to \mathbb{C}$ and an embedding $\overline{\mathbb{Q}} \to \overline{\mathbb{Q}_p}$.*

For $n \geq 1$, let $\zeta_n = e^{\frac{2\pi i}{n}} \in \overline{\mathbb{Q}} \subset \mathbb{C}$ and $\zeta_n^+ = \zeta_n + \zeta_n^{-1}$.

2.1 Background on modular curves and modular forms

2.1.1 Modular curves and modular forms

For general theory of modular curves, see [5], [6], [10], [26], [30].

Definition 2.1.1. Let $\mathcal{Y}_1(N)$ be the $\mathbb{Z}[\frac{1}{N}]$-scheme that represents the functor taking a $\mathbb{Z}[\frac{1}{N}]$-scheme S to the set of pairs (E, α), where E is a elliptic curve over S and α is a closed immersion $\mathbb{Z}/N\mathbb{Z} \to E$ of S-group schemes. Let $Y_1(N) := \mathcal{Y}_1(N) \otimes \mathbb{Q}$.

Fact 2.1.2. As a $\mathbb{Z}[\frac{1}{N}]$-scheme, $\mathcal{Y}_1(N)$ is a smooth and geometrically irreducible curve.

Remark 2.1.3. In [10], [30], they work with the curve $\mathcal{Y}_\mu(N)$, which classifies pairs (E, β) where $\beta : \mu_N \to E$ is a closed immersion. For the relation between $\mathcal{Y}_1(N)$ and $\mathcal{Y}_\mu(N)$, one can see [9, Section 1.4].

Definition 2.1.4. Let $\mathcal{X}_1(N)$ be the $\mathbb{Z}[\frac{1}{N}]$-scheme representating the functor taking a $\mathbb{Z}[\frac{1}{N}]$-scheme S to the set of pairs (E, α), where E is a generalized elliptic curve over S and α is a closed immersion $\mathbb{Z}/N\mathbb{Z} \to E^{reg}$ of S-group schemes. Here E^{reg} denotes the smooth locus of E/S. Let $X_1(N) := \mathcal{X}_1(N) \otimes \mathbb{Q}$.

Fact 2.1.5. The moduli scheme $\mathcal{X}_1(N)$ is proper, smooth and geometrically irreducible curve over $\mathbb{Z}[\frac{1}{N}]$.

Definition 2.1.6. Let $\mathcal{Y}_0(N)$ be the coarse moduli scheme over $\mathbb{Z}[\frac{1}{N}]$ classifying the pairs (E, C), where E is a elliptic curve over a $\mathbb{Z}[\frac{1}{N}]$-scheme S and $C \subset E[N]$ is a finite flat group scheme of order N that is locally free and of rank N. Let $Y_0(N) := \mathcal{Y}_0(N) \otimes \mathbb{Q}$.

Definition 2.1.7. Let $\mathcal{X}_0(N)$ be the coarse moduli scheme over $\mathbb{Z}[\frac{1}{N}]$ classifying generalized elliptic curves together with a locally free subgroup scheme of order N in place of α in Definition 2.1.4. Let $X_0(N) := \mathcal{X}_0(N) \otimes \mathbb{Q}$.

We give the definition of cusps. For the details, one can see [30, Section 1.1].

Definition 2.1.8 (Cusps)**.** Let $C_{/\mathbb{Z}[1/N]} := \mathcal{X}_1(N) - \mathcal{Y}_1(N)$. As a closed subscheme of $\mathcal{X}_1(N)$, it is finite étale over $\mathbb{Z}[\frac{1}{N}]$.

For $\mathcal{X}_0(N)$, its subscheme of cusps is a disjoint union of two copies of $\operatorname{Spec}\mathbb{Z}[\frac{1}{N}]$, usually called 0 and ∞ (cf. [5, Example 9.3.4] for their descriptions via Tate curves). Let $C_{0/\mathbb{Z}[1/N]}$ and $C_{\infty/\mathbb{Z}[1/N]}$ be their inverse images under the natural morphism

$$\mathcal{X}_1(N) \to \mathcal{X}_0(N).$$

One can prove that $C_{\infty/\mathbb{Z}[1/N]}$ is isomorphic to $\operatorname{Spec}\mathbb{Z}[\zeta_N^+][\frac{1}{N}]$, and $C_{0/\mathbb{Z}[1/N]}$ is isomorphic to the disjoint union of $\frac{N-1}{2}$ copies of $\operatorname{Spec}\mathbb{Z}[\frac{1}{N}]$.

Remark 2.1.9. Let $\overline{Y_i(N)} = \Gamma_i(N)\backslash\mathbb{H}$ and $\overline{X_i(N)} = \Gamma_i(N)\backslash\overline{\mathbb{H}}$ for $i = 0, 1$, where

$$\mathbb{H} = \{\tau \in \mathbb{C} | \operatorname{im}(\tau) > 0\},$$

$$\overline{\mathbb{H}} = \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q}),$$

$$\Gamma_0(N) = \left\{\alpha \in \mathrm{SL}_2(\mathbb{Z}) \mid \alpha \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \mod N\right\},$$
$$\Gamma_1(N) = \left\{\alpha \in \mathrm{SL}_2(\mathbb{Z}) \mid \alpha \equiv \begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix} \mod N\right\}.$$

One can prove that $\overline{Y_i(N)}$ and $\overline{X_i(N)}$ are all algebraic curves over $\mathbb{C}$, and $\mathcal{Y}_i(N)$ and $\mathcal{X}_i(N)$ are their $\mathbb{Z}[\frac{1}{N}]$-models. For the details, one can see [5, Section 8.2].

2.1.2 Hecke operators

In this subsection, we define Hecke correspondences on $\mathcal{X}_1(N)$. For the details, one can see [30, Section 1.2], [10, Section 3]. Let $G := (\mathbb{Z}/N\mathbb{Z})^\times/\{\pm 1\}$. For each $a \in G$, we have an automorphism $\langle a\rangle$ of $\mathcal{X}_1(N)$ over $\mathcal{X}_0(N)$ which sends (E, α) to $(E, a\alpha)$. By pullback, this action induces automorphisms on singular cohomology, de Rham cohomology and étale cohomology. We will use $\langle a\rangle$ to denote these automorphisms.

For each prime number l, we denote by $\mathcal{X}_1(N, l)$ the moduli scheme which classifies the triples (E, α, C), where (E, α) is as in Definition 2.1.4, and C is a locally free subgroup scheme of E of order l. Here we require that the group generated by the image of α and C meets every geometric irreducible component of E/S, and moreover that image of $\alpha \cap C$ is trivial when $l = N$. We have two morphisms:

$$\pi : \mathcal{X}_1(N, l) \to \mathcal{X}_1(N), \;\; \psi : \mathcal{X}_1(N, l) \to \mathcal{X}_1(N),$$

which are uniquely determined by the following rules for points of $\mathcal{Y}_1(N)$ (cf. [10, Section 3]):

$$\pi(E, P, C) = (E, P), \;\; \psi(E, P, C) = (E/C, P + C/C).$$

Then we define the following operators on the cohomology of modular curves:

$$T(l) = (\psi_l)_* \pi^*, \;\; T^*(l) = \pi_* \psi_l^*.$$

Definition 2.1.10. Let $T(1) = 1$. If $l \nmid N$, for $e \in \mathbb{Z}_{\geq 0}$, we define

$$\begin{cases} T(l^{e+2}) = T(l)T(l^{e+1}) - T(l^e)\langle l \rangle l \\ \\ T^*(l^{e+2}) = T^*(l)T^*(l^{e+1}) - T^*(l^e)\langle l \rangle^{-1} l. \end{cases}$$

We also define

$$\begin{cases} T(N^e) = T(N)^e \\ \\ T^*(N^e) = T^*(N)^e. \end{cases}$$

Proposition 2.1.11 (relative multiplicative property)**.** *We have*

$$\begin{cases} T(n_1)T(n_2) = T(n_2)T(n_1), \;\; T^*(n_1)T^*(n_2) = T^*(n_2)T^*(n_1), \\ \\ T(n)\langle a \rangle = \langle a \rangle T(n), \;\; T^*(n)\langle a \rangle = \langle a \rangle T^*(n), \\ \\ T(n) = T^*(n)\langle n \rangle \text{ if } (n, N) = 1. \end{cases}$$

Fact 2.1.12. The operators $T(n)$ and $T^*(n)$ are transposes of each other under Poincaré duality

$$H^1(X_1(N)(\mathbb{C}), \mathbb{Z}) \times H^1(X_1(N)(\mathbb{C}), \mathbb{Z}) \to \mathbb{Z}$$

and

$$H^1(Y_1(N)(\mathbb{C}),\mathbb{Z}) \times H^1_c(Y_1(N)(\mathbb{C}),\mathbb{Z}) \to \mathbb{Z}.$$

Definition 2.1.13 (Atkin-Lehner involution)**.** Let W_N denote the involution of $\overline{X_0(N)}$ induced by $\tau \to \frac{-1}{N\tau}$ on the upper half-plane. For the details, one can see [6, IV], [18, Section 6].

For the modular scheme $\mathcal{X}_1(N) \otimes \mathbb{Z}[\frac{1}{N}, \zeta_N]$, we have an involution W_{ζ_N}. For the details, one can see [10, Section 6]. For an $\mathbb{Z}[\frac{1}{N}, \zeta_N]$-algebra S, the involution W_{ζ_N} sends an S-valued point (E, α) of $\mathcal{Y}_1(N)$ to (E', α'), where $E' = E/(\text{Image of } \alpha)$ and α' sends the identity of $(\mathbb{Z}/N\mathbb{Z})_S$ to the image to E' of an N-division point s of E such that the Weil-pairing of $\alpha(1)$ and s equals ζ_N. Via the natural projection map $\overline{X_1(N)} \to \overline{X_0(N)}$, the operator W_{ζ_N} maps to W_N.

Definition 2.1.14. For $i = 0, 1$, we define

$$S_2(\Gamma_i(N), \mathbb{Q}) := H^0(X_i(N), \Omega^1_{/\mathbb{Q}}),$$

$$M_2(\Gamma_i(N), \mathbb{Q}) := H^0(X_i(N), \Omega^1_{/\mathbb{Q}}(\log\{\text{cusps}\})),$$

where $\Omega^1_{/\mathbb{Q}}$ is the sheaf of relative differential forms, and $\Omega^1_{/\mathbb{Q}}(\log\{\text{cusps}\})$ is the sheaf of differential forms which may have logarithmic poles along the cusps.

2.1.3 More on cusps

In this section, we give another description of the cusps on $\mathcal{X}_1(N)$.

Definition 2.1.15. Let P_N be the set of all pairs $(a, b) \in \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ such that the ideal (a, b) of $\mathbb{Z}/N\mathbb{Z}$ is the unit ideal.

Over $\mathbb{Q}(\zeta_N^+)$ or $\mathbb{C}$, we have the following correspondence:

$$\{\text{cusps of } X_1(N)(\mathbb{C})\} = \Gamma_1(N)\backslash\mathbb{P}^1(\mathbb{Q}) \overset{(1)}{=} (\Gamma_1(N)/(\pm 1))\backslash \operatorname{PSL}_2(\mathbb{Z})/\begin{pmatrix} 1 & \mathbb{Z} \\ 0 & 1 \end{pmatrix} \overset{(2)}{=} P_N/\sim$$

where $/\sim$ is the quotient by the equivalence relation $(a, b) \sim (a', b')$ if and only if $a' = \epsilon a$ and $b' \equiv \epsilon b \mod a$ with $\epsilon = \pm 1$. Here, the identification (1) sends the class of $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \operatorname{PSL}_2(\mathbb{Z})$ to the class of $\frac{a}{c} = g\infty \in \mathbb{P}^1(\mathbb{Q})$, and the identification (2) sends the class of $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ to the class of $(c, d) \in P_N$ (see also [9, Section 1.3]).

We then give an algebraic description of the cusps. Let $\mathbb{Z}[\zeta_N^+, \frac{1}{N}]((q^{\frac{1}{N}}))$ be the Laurent series ring. For $(a, b) \in P_N$, let

$$\infty_N(a, b) : \operatorname{Spec} \mathbb{Z}[\zeta_N^+, \tfrac{1}{N}]((q^{\frac{1}{N}})) \to \mathcal{Y}_1(N)$$

be the morphism corresponding to the N-torsion point $q^{\frac{a}{N}}\zeta_N^b \mod q^{\mathbb{Z}}$ of the Tate curve. This morphism gives the cusp of $\mathcal{X}_1(N)$ over $\mathbb{Z}[\zeta_N^+, \frac{1}{N}]$ corresponding to $(a, b) \in P_N$.

For $c \in (\mathbb{Z}/N\mathbb{Z})^{\times}$, we have $\langle c \rangle \circ \infty_N(a,b) = \infty_N(ac,bc)$.

2.2 Modular symbols and Manin symbols

In this section, we introduce modular symbols and Manin symbols. The homology and cohomology groups in this section are all singular cohomology groups. For the details, one can see [33].

Definition 2.2.1. Let $\mathbb{M}_2^{'}$ be the free abelian group generated by $\{\alpha, \beta\}$ for $\alpha, \beta \in \mathbb{P}^1(\mathbb{Q})$. Let $\mathbb{M}_2$ be the quotient of $\mathbb{M}_2^{'}$ by the relations

$$\{\alpha,\beta\} + \{\beta,\gamma\} + \{\gamma,\alpha\} = 0.$$

We define the action $\mathrm{GL}_2(\mathbb{Q})$ on $\mathbb{M}_2$ by

$$g\{\alpha,\beta\} = \{g(\alpha), g(\beta)\} \text{ for all } g \in \mathrm{GL}_2(\mathbb{Q}).$$

Definition 2.2.2. We define

$$\mathbb{M}_2(\Gamma_1(N)) = \big(\mathbb{M}_2/\langle x - g(x) \mid x \in \mathbb{M}_2, g \in \Gamma_1(N)\rangle\big)/\text{torsion}.$$

Theorem 2.2.3. *(Manin) The homomorphism*

$$\phi : \mathbb{M}_2(\Gamma_1(N)) \to H_1(X_1(N), \text{cusps}, \mathbb{Z})$$

that sends $\{\alpha, \beta\}$ *to the corresponding geodesic path in* $H_1(X_1(N), \text{cusps}, \mathbb{Z})$ *is an isomorphism.*

Proof. For the proof, see [20]. □

Proposition 2.2.4 (Manin)**.** *Let* N *be a positive integer and* $\alpha_0, \ldots, \alpha_m$ *a set of right coset representatives for* $\Gamma_1(N)$ *in* $\mathrm{SL}_2(\mathbb{Z})$*. Then* $\{\alpha_0\{0, \infty\}, \ldots, \alpha_m\{0, \infty\}\}$ *is a set of generators of* $\mathbb{M}_2(\Gamma_1(N))$ *as a* $\mathbb{Z}$*-module .*

Proof. For the proof, see [33, Section 3.3]. □

We use the following proposition to give an expression for α_i.

Proposition 2.2.5. *Let* S *be the following set*

$$\{[u, v] \in (\mathbb{Z}/N\mathbb{Z})^2 \mid (u, v) = 1 \in \mathbb{Z}/N\mathbb{Z}\}.$$

We have the following bijection of sets

$$S \xrightarrow{\psi} \Gamma_1(N) \backslash \mathrm{SL}_2(\mathbb{Z}),$$

$$\psi([u, v]) = \Gamma_1(N) \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

where $c, d \in \mathbb{Z}$ *are liftings of* u, v*.*

Proof. For the proof, see [33, Section 3.3]. □

Notation 2.2.6. *From now on, we use* $[u, v]$ *to denote* $\psi([u, v])\{0, \infty\} \in H_1(X_1(N), \text{cusps}, \mathbb{Z})$.

Remark 2.2.7. By Theorem 2.2.3, Proposition 2.2.4 and Proposition 2.2.5, we know that the pairs $[u, v]$ are generators of $H_1(X_1(N), \text{cusps}, \mathbb{Z})$, which are called Manin symbols.

It can be checked that the diamond operator $\langle l \rangle$ $(l \nmid N)$ acts on $[u, v]$ as follows:

$$\langle l \rangle [u, v] = [lu, lv].$$

It is easy to check that Manin symbols satisfy the following relations:

1. $[u, v] + [-v, u] = 0$,
2. $[u, v] = [u, u + v] + [u + v, v]$,
3. $[-u, -v] = [u, v]$,
4. $\langle j \rangle [u, v] = [ju, jv]$ for $j \in \mathbb{Z}$ prime to N.

For the details, one can see [20].

Theorem 2.2.8 (Manin)**.** *The above relations generate all the relations among the generators* $[u, v]$*, where* $u, v \in \mathbb{Z}/N\mathbb{Z}$ *and* $(u, v) = (1)$.

Proof. For the proof, see [33, Section 3.3] □

Definition 2.2.9. Define

$$[u, v]^+ = \frac{1}{2}([u, v] + [u, -v]).$$

Remark 2.2.10. We have an extra relation for symbols $[u, v]^+$:

$$[u, -v]^+ = [u, v]^+$$

The Manin symbols $[u, v]^+$ generate $H_1(X_1(N)(\mathbb{C}), \text{cusps}, \mathbb{Z}[1/2])^+$ as a $\mathbb{Z}[1/2]$-module.

Merel provided a formula for the action of Hecke operators on Manin symbols $[u, v]$. For the details, see [21].

Theorem 2.2.11 (Merel)**.** *For the Hecke operator $T(n)$, we have*

$$T(n)[u, v] = \sum_{a,b,c,d \geq 0,\, ad-bc=n,\, a>b,d>c} [au + cv, bu + dv].$$

Example 2.2.12. *We have*

$$T(2)[u, v] = [2u, v] + [2u, u + v] + [u + v, 2v] + [u, 2v] \tag{2.1}$$

and

$$T(3)[u,v] = [3u,v] + [3u,u+v] + [3u,2u+v] + [2u+v,u+2v] \\ + [u+2v,3v] + [u+v,3v] + [u,3v]. \tag{2.2}$$

2.3 Drinfeld-Manin splitting

Set $X_i = X_i(N)(\mathbb{C}), Y_i = Y_i(N)(\mathbb{C})$, and $C_i = X_i - Y_i$ for $i = 0, 1$. We have the following exact sequence in homology

$$0 \to H_1(X_i, \mathbb{Z}) \to H_1(X_i, C_i, \mathbb{Z}) \to \widetilde{H}_0(C_i, \mathbb{Z}) \to 0, \tag{2.3}$$

where $\widetilde{H}_0$ is used to denote reduced homology.

The exact sequence (2.3) does not need to split as Hecke modules. However, it does if we tensor (2.3) by $\mathbb{Q}$.

Theorem 2.3.1 (Drinfeld-Manin splitting)**.** *The exact sequence*

$$0 \to H_1(X_i, \mathbb{Q}) \to H_1(X_i, C_i, \mathbb{Q}) \to \widetilde{H}_0(C_i, \mathbb{Q}) \to 0$$

splits canonically as a sequence of Hecke modules.

Proof. For the proof, one can see [14, Section 2, Chapter IV]. □

Let N, p be as in the beginning of Chapter 1. We are interested in the following

two sequences:

$$0 \to H_1(X_0(N)(\mathbb{C}), \mathbb{Z}_p) \to H_1(X_0(N)(\mathbb{C}), \text{cusps}, \mathbb{Z}_p) \to \widetilde{H}_0(\text{cusps}, \mathbb{Z}_p) \to 0, \quad (2.4)$$

$$0 \to H_1(X_0(N)(\mathbb{C}), \mathbb{Q}_p) \to H_1(X_0(N)(\mathbb{C}), \text{cusps}, \mathbb{Q}_p) \to \widetilde{H}_0(\text{cusps}, \mathbb{Q}_p) \to 0. \quad (2.5)$$

Remark 2.3.2. Since N is prime, it is easy to see that $\widetilde{H}_0(\text{cusps}, \mathbb{Z}_p) \cong \mathbb{Z}_p$, and $e = (\infty) - (0)$ is a generator.

The Drinfeld-Manin splitting provides a map

$$\pi : H_1(X_0(N)(\mathbb{C}), \text{cusps}, \mathbb{Q}_p) \to H_1(X_0(N)(\mathbb{C}), \mathbb{Q}_p).$$

Notation 2.3.3 (Winding element)**.** *Let*

$$\{0, \infty\}_{DM} := \pi(\{0, \infty\}) \in H_1(X_0(N)(\mathbb{C}), \mathbb{Q}_p)$$

where $\{0, \infty\} \in H_1(X_0(N)(\mathbb{C}), \text{cusps}, \mathbb{Z}_p)$.

2.4 Modular units and Siegel units

2.4.1 Siegel units

Definition 2.4.1. Let $\mathcal{Y}(N)$ be the $\mathbb{Z}[\frac{1}{N}]$-scheme that represents the functor taking a $\mathbb{Z}[\frac{1}{P}]$-scheme S to a set of triples (E, P_1, P_2), where E is a elliptic curve over S and $P_1, P_2 \in E[N]$ are such that $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \to E; (a, b) \mapsto aP_1 + bP_2$ is injective. For the representable property, one can see [26].

Definition 2.4.2. Let $(\mathcal{E}, e_1, e_2)$ be the triple corresponding to the identity morphism in $\mathcal{Y}(N)(\mathcal{Y}(N))$. This $\mathcal{E}$ is called the universal elliptic curve.

In order to define Siegel units, we need to define theta functions on the universal elliptic curve first.

Theorem 2.4.3 (Kato)**.** *For any c prime to 6, there is an unique element ${}_c\theta_{\mathcal{E}} \in \mathcal{O}(\mathcal{E}\backslash\mathcal{E}[c])^\times$ with divisor $c^2(0) - \mathcal{E}[c]$ which is invariant under the norm maps induced by the following maps*

$$b : \mathcal{E}\backslash\mathcal{E}[bc] \to \mathcal{E}\backslash\mathcal{E}[c],$$

$$x \mapsto bx$$

where b is a integer prime to c.

Proof. For the proof, one can see [25, Proposition 1.3]. □

Definition 2.4.4 (Siegel units)**.** Let $\mathcal{E}$ be the universal elliptic curve over $\mathcal{Y}(N)$, $N \geq 5$. For c prime to $6N$, we define

$$ {}_cg_{\alpha,\beta} = \iota^*_{\alpha,\beta}({}_c\theta_{\mathcal{E}}) \in \mathcal{O}(\mathcal{Y}(N))^\times, $$

where $(\alpha, \beta) = (\frac{a}{N}, \frac{b}{N}) \in (\frac{\frac{1}{N}\mathbb{Z}}{\mathbb{Z}} \times \frac{\frac{1}{N}\mathbb{Z}}{\mathbb{Z}})\backslash(0,0)$, and $\iota_{\alpha,\beta} = ae_1 + be_2 : \mathcal{Y}(N) \to \mathcal{E}\backslash\mathcal{E}[c]$.

By taking c such that $c \equiv 1 \mod N$ and $c \neq \pm 1$, let $g_{\alpha,\beta} = {}_cg_{\alpha,\beta} \otimes (c^2-1)^{-1} \in \mathcal{O}(\mathcal{Y}(N))^\times \otimes \mathbb{Q}$. It can be checked that $g_{\alpha,\beta}$ is independent of the choice of c.

Definition 2.4.5. For $\begin{pmatrix} s & u \\ t & v \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, we define

$$ \begin{pmatrix} s & u \\ t & v \end{pmatrix}^* ({}_cg_{\alpha,\beta}) = {}_cg_{\alpha',\beta'}, \ (\alpha', \beta') = (\alpha, \beta) \begin{pmatrix} s & u \\ t & v \end{pmatrix}. $$

Remark 2.4.6. By the definition of $\mathcal{Y}_1(N)$, we know that ${}_cg_{0,\beta} \in \mu^*(\mathcal{O}(\mathcal{Y}_1(N))^\times)$ where μ is the natural projection of $\mathcal{Y}(N)$ to $\mathcal{Y}_1(N)$ which sends (E, e_1, e_2) to (E, e_2). For a prime number $l \nmid N, l \geq 5$, we then have elements

$$ g_{0,\beta} \in \mathcal{O}(\mathcal{Y}_1(N))^\times \otimes \mathbb{Z}_l. $$

Proposition 2.4.7. *As a meromorphic modular function on $Y_1(N)$, $g_{0,\frac{b}{N}}$ has the*

following q-expansion:

$$g_{0,\frac{b}{N}}(\tau) = q^{\frac{1}{2}\mathbb{B}_2(0)} \prod_{n\geq 0} \big(1 - q^n \zeta_N^b\big) \prod_{n>0} \big(1 - q^n \zeta_N^{-b}\big),$$

where $\mathbb{B}_2(x) = x^2 - x + \frac{1}{6}$.

Proof. For the proof, see [25, 1.9]. □

2.4.2 Modular unit of $\mathcal{Y}_0(N)$

From Remark 2.4.6, we have the Siegel unit $g_{0,\frac{1}{N}} \in \mathcal{O}(\mathcal{Y}_1(N))^\times \otimes_{\mathbb{Z}} \mathbb{Z}_p$. Let F be its norm to $\mathcal{O}(\mathcal{Y}_0(N))^\times \otimes_{\mathbb{Z}} \mathbb{Z}_p$.

Proposition 2.4.8. *The unit F has q-expansion:*

$$F = N q^{\frac{N-1}{12}} \prod_{n>0} \Big(\frac{1 - q^{Nn}}{1 - q^n}\Big)^2.$$

Proof. Since

$$g_{0,\frac{i}{N}} = q^{\frac{1}{12}}(1 - \zeta_N^i) \prod_{n>0} \big(1 - q^n \zeta_N^i\big)\big(1 - q^n \zeta_N^{-i}\big),$$

we have

$$F = \prod_{i=1}^{N-1} g_{0,\frac{i}{N}} = q^{\frac{N-1}{12}} \prod_{i=1}^{N-1} (1 - \zeta_N^i) \prod_{i=1}^{N-1} \Big(\prod_{n>0} \big(1 - q^n \zeta_N^i\big)\big(1 - q^n \zeta_N^{-i}\big)\Big).$$

It is easy to see that

1. $\prod_{i=1}^{N-1}(1-\zeta_N^i) = N$,

2. $\prod_{i=1}^{N-1}\prod_{n>0}\left(1-q^n\zeta_N^i\right) = \prod_{i=1}^{N-1}\left(1-q^n\zeta_N^{-i}\right) = \frac{1-q^{Nn}}{1-q^n}$.

So we have

$$\prod_{i=1}^{N-1} g_{0,\frac{i}{N}} = q^{\frac{N-1}{12}} N \prod_{n>0}\left(\frac{1-q^{Nn}}{1-q^n}\right)^2.$$

□

Definition 2.4.9. We define $g = \frac{F}{N}$.

Definition 2.4.10. Let $\Delta(z) \in S_{12}(\mathrm{SL}_2(\mathbb{Z}), \mathbb{C})$ be the discriminant function. For the properties of discriminant function, see [7, Section 1.1]. Define

$$f = \frac{\Delta(z)}{\Delta(Nz)}.$$

It is a modular function of $\overline{Y_0(N)}$. A similar function has already been considered by Ogg, for the details, see [27].

Proposition 2.4.11. *We have*

$$\mathrm{Div}(f) = (N-1)((0)-(\infty)).$$

Proof. Since we have

$$\Delta(z) = q\prod_{j=1}^{\infty}(1-q^j)^{24},$$

we also have

$$\Delta(Nz) = q^N \prod_{j=1}^{\infty} (1 - q^{Nj})^{24}.$$

So f has q-expansion

$$q^{-(N-1)} \prod_{j=1}^{\infty} \Big(\frac{1 - q^j}{1 - q^{Nj}} \Big)^{24},$$

and therefore it has pole of order $N - 1$ at ∞. Since $\mathrm{Div}(f)$ is a degree 0 cuspidal divisor, the divisor must be $(N - 1)((0) - (\infty))$. □

Proposition 2.4.12. *The leading coefficient of $f(z)$ at ∞ is 1, and the leading coefficient of $f(z)$ at 0 is N^{12}.*

Proof. The leading coefficient of f at ∞ can be read off from the q-expansion. We need to compute the q-expansion of g at 0. Since $\Delta(-1/z) = z^{12}\Delta(z)$ and $\Delta(-1/Nz) = (Nz)^{12}\Delta(Nz)$, we have

$$W_N(f) = \frac{\Delta(-1/(Nz))}{\Delta(-1/z)} = \frac{(Nz)^{12}\Delta(Nz)}{z^{12}\Delta(z)} = N^{12}\frac{1}{f}.$$

Since W_N changes 0 and ∞, the leading coefficient at 0 is N^{12}. □

Remark 2.4.13. From the q-expansion, we know that $f = g^{-12}$, and the leading coefficient of g at 0 is $\frac{1}{N}$.

CHAPTER 3

Mazur's work on $X_0(N)$

3.1 Mazur's result on the homology of $X_0(N)$

3.1.1 Congruence formula and the winding homomorphism

Let N, p be as Chapter 2, and assume $p \mid (N-1)$. Let q be the highest p-power dividing $N-1$. Let $\mathfrak{H}_0(N)$ be the subring of $\mathrm{End}_{\mathbb{Z}_p}(H^1(Y_0(N)(\mathbb{C}), \mathbb{Z}_p))$ generated by $T(n)\,(n \geq 1, n \nmid N)$ and W_N, and let $\mathfrak{h}_0(N)$ be its image in $\mathrm{End}_{\mathbb{Z}_p}(H^1(X_0(N)(\mathbb{C}), \mathbb{Z}_p))$.

Notation 3.1.1. *Let n be the numerator of $\frac{N-1}{12}$.*

Theorem 3.1.2. *There is a surjective algebra homomorphism:*

$$\phi : \mathfrak{h}_0(N) \to \mathbb{Z}_p/(n),$$

$$T(l) \mapsto 1 + l.$$

The kernel of ϕ is generated by $\eta_l := 1 + l - T(l)$ and $W_N + 1$. We will use I (the Eisenstein ideal) to denote this kernel.

Proof. For the proof, see [18, Proposition 9.7]. □

Let $H := H_1(X_0(N)(\mathbb{C}), \mathbb{Z}_p)$. Let H^+ be the subspace of H fixed by the complex conjugation c and H_+ be the largest quotient of H on which c acts trivially.

Remark 3.1.3. Since p is odd, we have a direct sum decomposition of H:

$$H = \frac{1+c}{2}H \oplus \frac{1-c}{2}H.$$

We identify H^+ and H_+ with $\frac{1+c}{2}H$.

Definition 3.1.4. Let

$$e^+ : I \to H^+$$

be the $\mathfrak{h}_0(N)$-morphism such that

$$x \mapsto x\{0, \infty\}_{DM}.$$

Let

$$\widetilde{e} : I\mathfrak{h}_0(N)_I \to H_I^+$$

denote the induced map on I-adic completions. We call this map the winding homomorphism.

Remark 3.1.5. These maps are well defined since

$$IH_1(Y_0(N)(\mathbb{C}), \text{cusps}, \mathbb{Z}) \subset H_1(X_0(N)(\mathbb{C}), \mathbb{Z}).$$

Definition 3.1.6 (Shimura subgroup)**.** The Shimura covering is the maximal unramified subcover intermediate to $X_1(N) \to X_0(N)$ whose covering group is the unique quotient group of $(\mathbb{Z}/N\mathbb{Z})^\times/\{\pm 1\}$ which has order n. From the natural map $X_1(N) \to X_0(N)$, we obtain a Picard morphism $\text{Jac}(X_0(N)) \to \text{Jac}(X_1(N))$. We define the Shimura subgroup Σ to be the kernel of this map on $\overline{\mathbb{Q}}$-points.

Remark 3.1.7. Mazur proved that the Shimura subgroup is killed by the Eisenstein ideal. For the proof, see [18, Proposition 11.7].

Lemma 3.1.8 (Mazur)**.** *The group H^+/IH^+ is cyclic of order q. There is a canonical isomorphism $\phi : (\mathbb{Z}/N\mathbb{Z})^\times/((\mathbb{Z}/N\mathbb{Z})^\times)^q \to H^+/IH^+$ which identifies H^+/IH^+ with the Galois group of q-subcover of the Shimura covering.*

Proof. For the proof, see [18, Lemma 18.7]. □

Proposition 3.1.9 (Mazur)**.** *Let a and b be coprime integers with b relatively prime to N. Let $\bar{b}$ denote the image of b in $(\mathbb{Z}/N\mathbb{Z})^\times$. Let $\Phi(a/b) \in H^+/IH^+$ denote the*

image of the modular symbol $\{0, a/b\}$ *in* H^+/IH^+. *Then*

$$\Phi(a/b) = \phi(\bar{b}^{-1}).$$

Proof. For the proof, see [18, Proposition 18.8] □

Example 3.1.10. *By Proposition 3.1.9, we have*

$$\Phi([x, 1]^+) = \phi(x^{-1}),$$

where $x \in (\mathbb{Z}/N\mathbb{Z})^\times$.

Proposition 3.1.11 (Congruence formula for the winding homomorphism)**.** *Let* $\eta_l = 1 + l - T(l)$ *and* $\tilde{e}^+ : I/I^2 \to H^+/IH^+$ *be the homomorphism induced from* $\tilde{e} : I \to H_I^+$. *Then:*

$$\tilde{e}^+(\eta_l) = (l-1)\phi(\bar{l}),$$

where l *is any prime number different from* N.

Proof. For the proof, see [18, Theorem 18.10]. □

Definition 3.1.12. Let $\mathfrak{P}$ be the ideal (p, I) of $\mathfrak{h}_0(N)$. By Theorem 3.1.2, it is a maximal ideal of $\mathfrak{h}_0(N)$, and $\mathfrak{h}_0(N)/\mathfrak{P} \cong \mathbb{F}_p$.

Definition 3.1.13 (good prime)**.** Suppose that w is a prime number dividing n. Let l be a prime different from N. We say that l is good for (w, N) if either

1. one of l or w is odd, l is not a w-th power modulo N, and $\frac{l-1}{2} \not\equiv 0 \mod w$.

2. $l = w = 2$ and -4 is not an 8-th power modulo N.

Theorem 3.1.14 (Mazur)**.** *Let p be a odd prime number dividing n. Let l be a prime number different from N. Then η_l is a generator of the ideal $I_{\mathfrak{P}} = I\mathfrak{h}_0(N)_{\mathfrak{P}} \subset \mathfrak{h}_0(N)_{\mathfrak{P}}$ if and only if l is a good prime number for (p, N). Moreover, the winding homomorphism $\tilde{e}^+ : I_{\mathfrak{P}} \to H^+_{\mathfrak{P}}$ is an isomorphism of Hecke modules.*

3.1.2 Structure of the p-adic Hecke algebra of $X_0(N)$

In this section, we recall some results on the structure of $\mathfrak{h}_0(N)$. For the details, see [18].

By Theorem 3.1.14, we know that $\mathfrak{h}_0(N)_{\mathfrak{P}} = \mathbb{Z}_p[\eta_l]$ for a good prime l. Let $R_l(x) \in \mathbb{Z}_p[x]$ be the minimal monic polynomial of η_l over $\mathbb{Z}_p$. We have an isomorphism:

$$\mathfrak{h}_0(N)_{\mathfrak{P}} \cong \mathbb{Z}_p[x]/R_l(x).$$

Notation 3.1.15. *Let g_p be the degree of $R_l(x)$. It is easy to see that it is independent of the choice of good prime l.*

Corollary 3.1.16. *The Hecke algebra $\mathfrak{h}_0(N)_{\mathfrak{P}}$ is Gorenstein.*

Corollary 3.1.17. *If $p||(N-1)$, then $\mathfrak{h}_0(N)_{\mathfrak{P}}$ is a discrete valuation ring totally ramified over $\mathbb{Z}_p$.*

3.2 Galois representations attached to modular curves

Notation 3.2.1. *For a scheme C over $\mathbb{Q}$, we will use $H^i_{\text{ét}}(C)$ to denote $H^i_{\text{ét}}(C \otimes \bar{\mathbb{Q}}, \mathbb{Z}_p)$.*

Via the comparison theorem between étale cohomology and singular cohomology, we may view $H^1(X_0(N)(\mathbb{C}), \mathbb{Z}_p)$ as a Galois module. We list some well-known properties of this Galois module.

1. As a $\mathfrak{h}_0(N) \otimes \mathbb{Q}_p$-module, $H^1(X_0(N)(\mathbb{C}), \mathbb{Q}_p) \cong H^1_{\text{ét}}(X_0(N)) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is free of rank 2.

2. For a prime number $l \nmid pN$, the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is unramified at l, and we have

$$\det(1 - \mathrm{Fr}_l^{-1}\, t) = 1 - T(l)u + l\langle l\rangle u^2 = 1 - \langle l\rangle T^*(l)u + l\langle l\rangle u^2.$$

3. The determinant of $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is $\kappa(\sigma)^{-1}\langle\sigma\rangle^{-1}$, where $\kappa : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{Z}_p^\times$

is the cyclotomic character, and $\langle\sigma\rangle$ denotes $\langle a\rangle$ for $a \in (\mathbb{Z}/N\mathbb{Z})^\times$ such that $\sigma(\zeta_N) = \zeta_N^a$.

For the $\mathfrak{h}_0(N)_\mathfrak{P}[\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)]$-module structure of $H^1_{\text{ét}}(X_0(N))_\mathfrak{P}$, we have the following filtration:

$$0 \to H^1_{\text{ét}}(X_0(N))_{\mathfrak{P},\text{sub}} \to H^1_{\text{ét}}(X_0(N))_\mathfrak{P} \to H^1_{\text{ét}}(X_0(N))_{\mathfrak{P},\text{quo}} \to 0. \tag{3.1}$$

Remark 3.2.2. In fact, $H^1_{\text{ét}}(X_0(N))_{\mathfrak{P},\text{sub}}$ is a free $\mathfrak{h}_0(N)_\mathfrak{P}$-module, and $H^1_{\text{ét}}(X_0(N))^{\text{ord}}_{\mathfrak{P},\text{quo}}$ is a dualizing $\mathfrak{h}_0(N)_\mathfrak{P}$-module. Moreover, we have the following.

1. The action of $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ on $H^1_{\text{ét}}(X_0(N))_{\mathfrak{P},\text{quo}}(1)$ is unramified.

2. The action of $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ on $H^1_{\text{ét}}(X_0(N))_{\mathfrak{P},\text{sub}}$ is unramified.

3. Let α_p be the unit root of the equation $X^2 - T_pX + p = 0$ in the Hecke algebra $\mathfrak{h}_0(N)_\mathfrak{P}$. Then Fr_p acts on $H^1_{\text{ét}}(X_0(N))_{\mathfrak{P},\text{quo}}(1)$ via multiplication by α_p.

Remark 3.2.3. For the proof of the above statements, one can see [35, Proposition 3.3.4, Lemma 3.3.6].

3.3 Structure of homology modulo Eisenstein ideal

Notation 3.3.1. *Let* $H^1(X) = H^1_{\text{ét}}(X_0(N))$ *and* $H^1(Y) = H^1_{\text{ét}}(Y_0(N))$.

Remark 3.3.2. We have an isomorphism from Poincaré duality

$$H^1(X)(1) \cong H_1(X_0(N), \mathbb{Z}_p),$$

which respects complex conjugation. We use these isomorphisms to transfer from homology groups to cohomology groups.

In this section, following the method in [9, Section 6.3] and [32, Section 4], we construct a global exact sequence which gives the $\mathfrak{h}_0(N)_{\mathfrak{P}}[\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})]$-module structure of $H^1(X)/IH^1(X)$. Let $\xi = \frac{N-1}{12}$. By (2.4), we have the following exact sequence of $\mathfrak{h}_0(N)[\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})]$-modules:

$$0 \to H^1(X)(1) \to H^1(Y)(1) \to \mathbb{Z}_p e \to 0, \tag{3.2}$$

where $e = (\infty) - (0)$.

Remark 3.3.3. Via duality, the sequence (3.2) is isomorphic to the following sequence of homology groups

$$0 \to H_1(X_0(N), \mathbb{Z}_p) \to H_1(X_0(N), \mathrm{cusps}, \mathbb{Z}_p) \to \mathbb{Z}_p e \to 0.$$

For the details, see [32, Proposition 3.5].

Lemma 3.3.4. *We have*

$$H^1(Y)_{DM,\mathfrak{P}}/H^1(X)_{\mathfrak{P}} \cong \mathfrak{h}_0(N)/I \cong \mathbb{Z}_p/\xi.$$

Proof. The isomorphism

$$\mathfrak{h}_0(N)/I \cong \mathbb{Z}_p/\xi$$

is directly deduced from Theorem 3.1.2.

It is easy to see that $H^1(Y)_{DM,\mathfrak{P}}/H^1(X)_{\mathfrak{P}}$ is generated by the image of $\{0,\infty\}_{DM,\mathfrak{P}}$. The isomorphism

$$H^1(Y)_{DM,\mathfrak{P}}/H^1(X)_{\mathfrak{P}} \cong \mathfrak{h}_0(N)/I$$

follows from the fact that $(0)-(\infty)$ has order n. □

Lemma 3.3.5. *In $H^1(Y)_{DM,\mathfrak{P}}$, the element $\xi\{0,\infty\}_{DM,\mathfrak{P}}$ of $H^1(X)_{\mathfrak{P}}$ is a part of a $\mathbb{Z}_p$-basis of $H_{\mathfrak{P}}$.*

Proof. The modular symbol $\{0,\infty\}_{DM,\mathfrak{P}}$ is a generator of $H^1(Y)_{DM,\mathfrak{P}}/H^1(X)_{\mathfrak{P}}$, and via the isomorphism $H^1(Y)_{DM,\mathfrak{P}}/H^1(X)_{\mathfrak{P}} \cong \mathbb{Z}_p/\xi$, we know that $\xi\{0,\infty\}_{DM,\mathfrak{P}}$ is part of a $\mathbb{Z}_p$-basis of $H_{\mathfrak{P}}$. □

Definition 3.3.6. Using the Kummer sequence:

$$0 \to \mathbb{Z}/p^n\mathbb{Z}(1) \to G_m \to G_m \to 0$$

on the étale site of $\mathcal{Y}_0(N) \otimes \mathbb{Z}[\frac{1}{p}]$, we get a map:

$$\mathcal{O}(\mathcal{Y}_0(N))^\times \otimes \mathbb{Z}/p^n \to H^1_{\text{ét}}(\mathcal{Y}_0(N) \otimes \mathbb{Z}[\tfrac{1}{p}], \mathbb{Z}_p(1)) \to H^1(Y)(1).$$

Let $\bar{g}$ be the image of modular unit g in $H^1(Y)(1)$ via this map.

Lemma 3.3.7. *Via the map $H^1(Y)(1) \to H^1(Y)(1)_{\mathfrak{P}}/H^1(X)(1)_{\mathfrak{P}} \cong \mathbb{Z}_p e$, the element $\bar{g}$ maps to ξe.*

Proof. This is from the q-expansion of g. See Proposition 2.4.11. □

Lemma 3.3.8. *The kernel of $H^1(Y)(1)_{\mathfrak{P}} \to H^1(Y)(1)_{DM,\mathfrak{P}}$ is generated by $\bar{g}$.*

Proof. Let $U \subset H^1(Y)(1)_{\mathfrak{P}}$ be the image of $\mathcal{O}(Y_0(N))^\times \otimes \mathbb{Z}_p$ under the Kummer map. Then U is a $\mathfrak{H}_0(N)$-submodule generated by $\bar{g}$. As $\mathbb{Z}_p$-modules, $U \cong \mathbb{Z}_p$, so U maps injectively into $H^1(Y)_{\mathfrak{P}}(1)/H^1(X)_{\mathfrak{P}}(1)$. It means that $U \cap H^1(X)_{\mathfrak{P}}(1) = 0$, so U is contained in the kernel of $H^1(Y)(1)_{\mathfrak{P}} \to H^1(Y)(1)_{DM,\mathfrak{P}}$. By the definition of splitting, this kernel maps injectively into $H^1(Y)(1)/H^1(X)(1) \cong \mathbb{Z}_p$, and by Lemma 3.3.4 and the definition of congruence module (cf. [29, Lemma 1.1.4]), the image of

this kernel in $H^1(Y)(1)/H^1(X)(1) \cong \mathbb{Z}_p$ is $\xi\mathbb{Z}_p$. By Lemma 3.3.7, $\bar{g}$ maps to ξ in $H^1(Y)(1)/H^1(X)(1)$. So $\bar{g}$ generates the kernel. □

Notation 3.3.9. *Let*

$$P = H^1(X)^-/IH^1(X)^-,\ Q = H^1(X)^+/IH^1(X)^+,\ R = H^1(Y)_{DM}/H^1(X),$$

where $\pm$ is with respect to the action of complex conjugation on $X_0(N)(\mathbb{C})$.

Remark 3.3.10. The group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on R via κ^{-1}. This is because $R(1)$ is generated by the cusps of $X_0(N)$, which are both rational over $\mathbb{Q}$, so it has trivial Galois action.

Lemma 3.3.11. *We have a Galois-equivariant perfect pairing $(,)$ from the cup product of étale cohomology:*

$$H^1(X) \times H^1(X) \to \mathbb{Z}_p(-1),$$

such that

$$(tx, y) = (x, ty), x, y \in H^1(X),\ t \in \mathfrak{h}_0(N).$$

Proof. This follows from Poincaré duality of étale cohomology. □

Definition 3.3.12. We define a $\mathbb{Z}_p$-linear map from $H^1(X)/IH^1(X)$ to $\mathbb{Z}_p/(\xi)$ as

follows. Since $\xi\{0,\infty\}_{DM,\mathfrak{P}} \in H^1(X)_{\mathfrak{P}}$, we get a map:

$$H^1(X)_{\mathfrak{P}} \to \mathbb{Z}_p/\xi\mathbb{Z}_p$$

$$x \mapsto (x, W_N\xi\{0,\infty\}_{DM,\mathfrak{P}}).$$

Since $\mathfrak{h}/I \cong \mathbb{Z}_p/\xi\mathbb{Z}_p$, the above map factors through $H^1(X)/IH^1(X)$. So we get a map from $H^1(X)/IH^1(X)$ to $\mathbb{Z}_p/\xi\mathbb{Z}_p$.

Lemma 3.3.13. *The map $(-, W_N\xi\{0,\infty\}_{DM})$ is surjective.*

Proof. By Lemma 3.3.4, $\xi\{0,\infty\}_{DM,\mathfrak{P}}$ is part of a $\mathbb{Z}_p$-basis of $H^1(X)_{\mathfrak{P}}$. Since the Poincaré duality pairing is perfect, the map that we are considering is surjective. □

Notation 3.3.14. *In order to simplify the notation, let $T = H^1(X)/IH^1(X)$, $P' = \ker(T \to \mathbb{Z}_p/\xi)$, and $Q' = T/P'$.*

Proposition 3.3.15. *The group P' is a Galois submodule of T, and the Galois action on Q' is trivial.*

Remark 3.3.16. We have an exact sequence of $\mathfrak{h}_0(N)[\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})]$-modules:

$$0 \to P' \to T \to Q' \to 0. \tag{3.3}$$

Proof. For any element $x \in P'$, we have $(x, W_N\xi\{0,\infty\}_{DM,\mathfrak{P}}) \in \xi\mathbb{Z}_p$. For $\sigma \in$

$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, we need to prove that $(\sigma x, W_N\xi\{0,\infty\}_{DM,\mathfrak{P}}) \in \xi\mathbb{Z}_p$. Note that $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on R via κ^{-1}. Hence, $\sigma^{-1}\{0,\infty\}_{DM,\mathfrak{P}} = \kappa(\sigma)\{0,\infty\}_{DM,\mathfrak{P}} + y$ for some $y \in H^1(X)_{\mathfrak{P}}$. Note that

$$(\sigma x, W_N\xi\{0,\infty\}_{DM,\mathfrak{P}}) = (\sigma x, \sigma\sigma^{-1}W_N\xi\{0,\infty\}_{DM,\mathfrak{P}}).$$

By the properties of Poincaré pairing, we know that

$$\begin{aligned}(\sigma x, \sigma\sigma^{-1}W_N\xi\{0,\infty\}_{DM,\mathfrak{P}}) &= \kappa(\sigma)^{-1}(x, W_N\xi(\kappa(\sigma)\{0,\infty\}_{DM,\mathfrak{P}} + y)) \\ &= (x, W_N\xi\{0,\infty\}_{DM,\mathfrak{P}}) + \kappa(\sigma)^{-1}(x, W_N\xi y).\end{aligned}$$

Since $(x, W_N\xi\{0,\infty\}_{DM,\mathfrak{P}}) \in \xi\mathbb{Z}_p$ and $\kappa(\sigma)^{-1}(x, W_N\xi y) \in \xi\mathbb{Z}_p$, we know that $(\sigma x, W_N\xi\{0,\infty\}_{DM,\mathfrak{P}}) \in \xi\mathbb{Z}_p$. Similarly, one can prove that the Galois action on Q' is trivial. □

Using the local filtration (3.1), we try to find a local splitting of (3.3).

Let τ be an element of the inertia subgroup of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}_p)$ whose image in $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ is a generator. Let $f = \kappa(\tau)^{-1}$. Let $S = \{x \in H^1(X) \mid \tau x = fx\}$.

Proposition 3.3.17. *There is a direct sum decomposition of Hecke-modules,*

$$H^1(X)_{\mathfrak{P}} = H^1(X)_{\mathfrak{P},\mathrm{sub}} \oplus S_{\mathfrak{P}}.$$

Proof. The action of τ on $H^1(X)_{\mathfrak{P},\mathrm{sub},}$ is trivial, and the action of τ on S is multi-

plication by f. It is clear that $f \not\equiv 1 \bmod \mathfrak{P}$. □

Lemma 3.3.18. *The composition*

$$\phi : H^1(X)_{\mathfrak{P},\mathrm{sub}}/IH^1(X)_{\mathfrak{P},\mathrm{sub}} \to H^1(X)/IH^1(X) \to Q'$$

is an isomorphism. The canonical map $P' \to H^1(X)_{\mathfrak{P},\mathrm{quo}}/IH^1(X)_{\mathfrak{P},\mathrm{quo}}$ *is an isomorphism, and the action of* τ *on* P' *is multiplication by* f.

Proof. Since we have a surjection from $H_{\mathfrak{P},\mathrm{quo}}/IH_{\mathfrak{P},\mathrm{quo}}$ to $\mathrm{Coker}(\phi)$, and the action of τ on $H_{\mathfrak{P},\mathrm{quo}}$ is f, it follows that the action of τ on $\mathrm{Coker}(\phi)$ is also by f. But we know that the action of τ on Q' is trivial, so ϕ has to be a surjection. Note that $Q' \cong \mathfrak{h}_0(N)_{\mathfrak{P}}/I$ and $H_{\mathfrak{P},\mathrm{sub}}/IH_{\mathfrak{P},\mathrm{sub}} \cong \mathfrak{h}_0(N)_{\mathfrak{P}}/I$, so ϕ is an isomorphism. It follows that $P' \to H_{\mathfrak{P},\mathrm{quo}}/IH_{\mathfrak{P},\mathrm{quo}}$ is also an isomorphism, and τ acts on P' by f, and $P' = S/IS$. □

Lemma 3.3.19. *The action of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *on* P' *is given by* κ^{-1}.

Proof. Since $H^1(X)_{\mathfrak{P}} = H^1(X)_{\mathfrak{P},\mathrm{sub}} \oplus S_{\mathfrak{P}}$, we can write down the following components of $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$,

1. $a(\sigma) \in \mathrm{Hom}_{\mathfrak{h}_0(N)_{\mathfrak{P}}}(H^1(X)_{\mathfrak{P},\mathrm{sub}}, H^1(X)_{\mathfrak{P},\mathrm{sub}})$,

2. $b(\sigma) \in \mathrm{Hom}_{\mathfrak{h}_0(N)_{\mathfrak{P}}}(H^1(X)_{\mathfrak{P},\mathrm{sub}}, S_{\mathfrak{P}})$,

3. $c(\sigma) \in \mathrm{Hom}_{\mathfrak{h}_0(N)_{\mathfrak{P}}}(S_{\mathfrak{P}}, H^1(X)_{\mathfrak{P},\mathrm{sub}})$,

4. $d(\sigma) \in \mathrm{Hom}_{\mathfrak{h}_0(N)_{\mathfrak{P}}}(S_{\mathfrak{P}}, S_{\mathfrak{P}})$.

Since S/IS is stable under the action of Galois, we have $c(\sigma) \equiv 0 \bmod I$. Since $H^1(X)_{\mathfrak{P},\mathrm{sub}}$ is free of rank 1 over $\mathfrak{h}_0(N)_{\mathfrak{P}}$, we have $a(\sigma) \in \mathfrak{h}$. Since $S_{\mathfrak{P}}$ is a dualizing module, $d(\sigma) \in \mathfrak{h}_0(N)_{\mathfrak{P}}$. Since

$$\det(\sigma) = \kappa^{-1}(\sigma) = a(\sigma)d(\sigma) - b(\sigma)c(\sigma),$$

we know that $a(\sigma)d(\sigma) \equiv \kappa^{-1}(\sigma) \bmod I$. Note that $a(\sigma) \equiv 1 \bmod I$ because $H_{\mathfrak{P},\mathrm{sub}}/IH_{\mathfrak{P},\mathrm{sub}} \cong Q'$. Hence $d(\sigma) \equiv \kappa^{-1}(\sigma) \bmod I$. □

Remark 3.3.20. Since the action of complex conjugation on P' is multiplication by -1, this proves that $P' = H^1(X)^-/IH^1(X)^- = P$.

Remark 3.3.21. Since we have canonical isomorphism

$$Q = H^1(X)^+/IH^1(X)^+ \cong Q' \cong \mathbb{Z}_p/\xi\mathbb{Z}_p,$$

we call the element of $H^1(X)^+/IH^1(X)^+$ corresponding to $1 \in \mathbb{Z}_p/\xi\mathbb{Z}_p$ the *canonical generator.*

From the construction, we know that the sequence (3.3) splits locally at p. In fact, Mazur proved a stronger result.

Theorem 3.3.22 (Mazur)**.** *The exact sequence*

$$0 \to P \to T \to Q \to 0 \tag{3.4}$$

of Galois modules splits. The map

$$P \to \mathrm{Coker}(H^1(X_1(N)) \to T)$$

is an isomorphism, which gives a canonical splitting of (3.4).

Proof. See [18, Section 16]. □

Remark 3.3.23. In fact, Mazur proved that there is a decomposition of the I-torsion on the Jacobian:

$$\mathrm{Jac}(X_0(N))_{\mathfrak{P}}(I) = \Sigma_p \oplus C_p,$$

where Σ_p is the p-part of the Shimura subgroup Σ and C_p is the p-part of the cuspidal subgroup.

Remark 3.3.24. Via the duality between the étale cohomology group and the Picard group, we have

$$P \cong \mathrm{Hom}(\Sigma, \mathbb{Q}_p/\mathbb{Z}_p),$$

$$Q \cong \mathrm{Hom}(C, \mathbb{Q}_p/\mathbb{Z}_p),$$

which gives the splitting of the sequence in Theorem 3.3.22.

CHAPTER 4

Invariants of modular curves

In this chapter, we construct the extension classes we are interested in and compute the corresponding invariants. The construction of such extension classes has been considered in [19]; we revisit it in Section 4.1.

4.1 Extension classes

Let $q = p^f$ be the highest p power dividing $N-1$, and let $K = \mathbb{Q}(\zeta_q)$. Let $\Delta = \mathrm{Gal}(K/\mathbb{Q})$ and $U = \mathbb{F}_N^\times/(\mathbb{F}_N^\times)^q$.

We want to consider the following exact sequence:

$$0 \to H^1(X)/IH^1(X) \otimes I/I^2 \to H^1(X)/I^2H^1(X) \to H^1(X)/IH^1(X) \to 0. \quad (4.1)$$

By pushout and pullback, we get the following exact sequences:

(A) $0 \to Q \otimes I/I^2 \to ? \to Q \to 0$,

(B) $0 \to P \otimes I/I^2 \to ? \to Q \to 0$,

(C) $0 \to Q \otimes I/I^2 \to ? \to P \to 0$,

(D) $0 \to P \otimes I/I^2 \to ? \to P \to 0$.

Notation 4.1.1. *Let $a \in H^1(\mathbb{Z}[\frac{1}{Np}], I/I^2)$ correspond to the exact sequence (A), $b \in H^1(\mathbb{Z}[\frac{1}{Np}], P \otimes I/I^2)$ correspond to the exact sequence (B), $c \in H^1(\mathbb{Z}[\frac{1}{Np}], P^{-1} \otimes I/I^2)$ correspond to the exact sequence (C), and $d \in H^1(\mathbb{Z}[\frac{1}{Np}], I/I^2)$ correspond to the exact sequence (D).*

Definition 4.1.2. Let

1. $\chi_a \in H^1(\mathbb{Z}[1/Np, \zeta_q], I/I^2)^{\Delta}$ be the image of a,
2. $\chi_b \in H^1(\mathbb{Z}[1/Np, \zeta_q], P \otimes I/I^2)^{\Delta}$ be the image of b,
3. $\chi_c \in H^1(\mathbb{Z}[1/Np, \zeta_q], P^{-1} \otimes I/I^2)^{\Delta}$ be the image of c,
4. $\chi_d \in H^1(\mathbb{Z}[1/Np, \zeta_q], I/I^2)^{\Delta}$ be the image of d.

Proposition 4.1.3. *For $k = 1, -1, 0$, there exists a unique field extension F_k/K that is Galois over $\mathbb{Q}$, satisfying the following conditions:*

1. *Δ acts on $\mathrm{Gal}(F_k/K)$ via κ^k, where κ is the mod q cyclotomic character,*
2. *$\mathrm{Gal}(F_k/K) \cong \mathbb{Z}/q\mathbb{Z}$,*

3. *F_k/K is unramified outside p and N,*

4. *F_k/K is totally tamely ramified at N,*

5. *F_0 is the unique q-subextension of $K(\zeta_N)/K$,*

6. *F_1 is peu ramifiée at p over K and equals $K(N^{1/q})$,*

7. *F_{-1}/K splits completely at p.*

Proof. See [4, Lemma 3.9, Proposition 5.4]. □

Notation 4.1.4. *We use G_k to denote* $\mathrm{Gal}(F_k/K)$.

By Proposition 4.1.3, we know that $\chi_a, \chi_d \in \mathrm{Hom}(G_0, I/I^2)$, $\chi_b \in \mathrm{Hom}(G_{-1}, P \otimes I/I^2)$, $\chi_c \in \mathrm{Hom}(G_1, P^{-1} \otimes I/I^2)$.

Lemma 4.1.5. *There are canonical isomorphisms:*

1. *$G_0 \cong U$,*

2. *$G_1 \cong \mu_q$,*

3. *$G_{-1} \cong U^{\otimes 2} \otimes \mu_q^{-1}$.*

Proof. 1. We have $\mathrm{Gal}(K(\zeta_N)/K) \cong \mathbb{F}_N^\times$, so $G_0 \cong \mathbb{F}_N^\times/(\mathbb{F}_N^\times)^q = U$.

2. For G_1, we have the Kummer map

$$G_1 \to \mu_q, \quad \sigma \mapsto \frac{\sigma(N^{\frac{1}{q}})}{N^{\frac{1}{q}}},$$

which gives the canonical isomorphism $G_1 \cong \mu_q$.

3. For the isomorphism

$$G_{-1} \cong U^{\otimes 2} \otimes \mu_q^{-1},$$

see Remark 4.4.10.

□

Definition 4.1.6. By the winding isomorphism (Proposition 3.1.11), I/I^2 is identified with U. By Lemma 3.1.8 and Poincaré duality, P is identified with $I/I^2 \otimes \mu_q^{-1}$. Hence by Lemma (4.1.5), χ_a, χ_d are characters from U to U, χ_b is a character from $U^{\otimes 2} \otimes \mu_q^{-1}$ to $U^{\otimes 2} \otimes \mu_q^{-1}$, χ_c is a character from μ_q to μ_q. So, we have four integers attached to $\chi_a, \chi_b, \chi_c, \chi_d$, and we use $\tilde{a}, \tilde{b}, \tilde{c}, \tilde{d}$ to denote the invariants.

4.2 Computation of $\tilde{a}$ and $\tilde{d}$

The invariants $\tilde{a}$ and $\tilde{d}$ have been already computed in [19]. We review their argument here.

Fixing a basis e_+, e_- of $H^1(X)^+_{\mathfrak{P}}/I^2 \oplus H^1(X)^-_{\mathfrak{P}}/I^2$, one can write the representation as follows:

$$\rho(\sigma) = \begin{pmatrix} 1 + A(\sigma) & B(\sigma) \\ C(\sigma) & \kappa^{-1}(\sigma)(1 + D(\sigma)) \end{pmatrix}$$

for $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, where $A, B, C, D : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to I/I^2$ are homomorphisms, and κ is the p-adic cyclotomic character.

Proposition 4.2.1. *For a prime $l \not\equiv 1 \bmod q$, $l \nmid N$, we have*

$$1 + A(\mathrm{Frob}_l^{-1}) = 1 + \frac{\eta_l}{l-1},$$

where $\eta_l = 1 + l - T(l)$.

Proof. From the representation ρ, we know that $1 + A(\mathrm{Frob}_l^{-1})$ is the root of $t^2 - T(l)t + l = 0 \mod I^2$ which equal to 1 modulo I. We claim that

$$1 + A(\mathrm{Frob}_l^{-1}) \equiv 1 + \frac{\eta_l}{l-1} \bmod I^2.$$

This is seen via the following string of equalities:

$$\begin{aligned}
\left(1+\frac{\eta_l}{l-1}\right)^2-(1+l-\eta_l)\left(1+\frac{\eta_l}{l-1}\right)+l &= \left(1+\frac{\eta_l}{l-1}\right)\left(\frac{\eta_l}{l-1}+\eta_l-l\right)+l \\
&= \left(1+\frac{\eta_l}{l-1}\right)\left(\frac{l}{l-1}\eta_l-l\right)+l \\
&= l\left(\frac{\eta_l}{l-1}+1\right)\left(\frac{\eta_l}{l-1}-1\right)+l \\
&= l\left(\left(\frac{\eta_l}{l-1}\right)^2-1\right)+l \\
&\equiv 0 \mod I^2
\end{aligned}$$

□

Theorem 4.2.2 (Calegari-Mazur-Sharifi-Stein)**.** *We have* $\tilde{a}=-\tilde{d}=-1$.

Proof. Since

$$1+A(\mathrm{Frob}_l^{-1})+\kappa^{-1}(\mathrm{Frob}_l^{-1})(1+D(\mathrm{Frob}_l^{-1}))=T(l)=1+l-\eta_l,$$

and

$$1+A(\mathrm{Frob}_l^{-1})\equiv 1+\frac{\eta_l}{l-1} \mod I^2,$$

we know that

$$1+D(\mathrm{Frob}_l^{-1})=1-\frac{\eta_l}{l-1}.$$

The image of $\mathrm{Frob}_l\in U$ is l, so χ_a maps $l^{-1}\in U$ to $\frac{1}{l-1}\eta_l\in I/I^2$. Via the winding isomorphism, η_l maps to $l^{l-1}\in U$. Thus, the composite maps l^{-1} to l, which means that $\tilde{a}=-1$.

As for χ_d, it maps $l^{-1}\in U$ to $-\frac{1}{l-1}\eta_l\in I/I^2$. Via the winding isomorphism,

$-\frac{1}{l-1}\eta_l$ maps to $l^{-1} \in U$. The composite then maps l^{-1} to l^{-1}, which means that $\tilde{d} = 1$.

□

4.3 The invariant $\tilde{c}$

In this section, we use the method developed by Fukaya and Kato in [9, Section 9.6.3] to compute the invariant $\tilde{c}$.

Recall that the invariant $\tilde{c}$ (resp. cocycle c) is from the following extension class:

$$0 \to \frac{I}{I^2} \otimes \frac{H^1(X)^+}{IH^1(X)^+} \to \frac{IH^1(X)^+}{I^2H^1(X)^+} \oplus \frac{H^1(X)^-}{IH^1(X)^-} \to \frac{H^1(X)^-}{IH^1(X)^-} \to 0 \tag{4.2}$$

In this section, we will relate the sequence (4.2) to another sequence that arises from the cupsidal extension.

Let $E = H^1(Y)_{DM,\mathfrak{P}}/\operatorname{Ker}(H^1(X)_{\mathfrak{P}} \to Q)$. Then we have the following exact sequence:

$$0 \to Q \to E \to R \to 0. \tag{4.3}$$

Since

$$H^1(Y)_{DM,\mathfrak{P}}/H^1(X)_{\mathfrak{P}} \cong H^1(Y)^-_{DM,\mathfrak{P}}/H^1(X)^-_{\mathfrak{P}},\ H^1(Y)^+_{DM,\mathfrak{P}} = H^1(X)^+_{\mathfrak{P}},$$

we may rewrite (4.3) as:

$$0 \to \frac{H^1(X)^+}{IH^1(X)^+} \to \frac{H^1(Y)^-_{DM}}{IH^1(Y)^-_{DM}} \oplus \frac{H^1(X)^+}{IH^1(X)^+} \to \frac{H^1(Y)^-_{DM}}{IH^1(Y)^-_{DM}} \to 0 \qquad (4.4)$$

Note that the direct sum is with respect to the Hecke module structure.

Since there is a canonical generator $\{0,\infty\}_{DM,\mathfrak{P}}$ of $R(1)$, the sequence (4.4) gives an element c' in $H^1(\mathbb{Z}[1/Np], Q(1)) \cong H^1(\mathbb{Z}[1/Np], \mu_q)$.

Proposition 4.3.1. *We have $c = c'$ in $H^1(\mathbb{Z}[1/Np], \mu_q)$.*

Proof. We can rewrite sequence (4.2) as follows:

$$0 \to \frac{I}{I^2} \otimes \frac{H^1(X)^+}{IH^1(X)^+} \to \frac{IH^1(Y)^-_{DM}}{I^2H^1(Y)^-_{DM}} \oplus \frac{IH^1(X)^+}{I^2H^1(X)^+} \to \frac{IH^1(Y)^-_{DM}}{I^2H^1(Y)^-_{DM}} \to 0.$$

Since I is a principal ideal in the Eisenstein component and $H^1(Y)^-_{DM,\mathfrak{P}}/H^1(X)^-_{\mathfrak{P}} \cong h/I \cong I/I^2$, choosing a generator $\eta \in I/I^2$, we get the isomorphisms $\frac{H^1(X)^+}{IH^1(X)^+} \cong \frac{I}{I^2} \otimes \frac{H^1(X)^+}{IH^1(X)^+}$ and $\frac{H^1(Y)^-_{DM}}{IH^1(Y)^-_{DM}} \cong \frac{IH^1(Y)^-_{DM}}{I^2H^1(Y)^-_{DM}}$. By doing this, we identify two exact sequences. Although the identification depends on the choice of the generator, the extension class does not change. □

So, in order to compute c or $\tilde{c}$, it suffices to compute the extension class obtained from (4.3). We need to make some preparations.

Let J be the Jacobian variety of $X_0(N)$, and let GJ be the generalized Jacobian

variety of $X_0(N)$ with respect to the cusps of $X_0(N)$. For the general properties of Jacobians and generalized Jacobians of algebraic curves, one can see [28, Section 3]. We have the following exact sequence:

$$0 \to T \to GJ \to J \to 0, \tag{4.5}$$

where $T := \mathrm{Ker}(GJ \to J)$, and we have a canonical isomorphism $T \cong \mathrm{Coker}(\mathbb{G}_m \to \mathbb{G}_m \times \mathbb{G}_m)$.

Note that we have the following duality between étale cohomology groups and generalized Jacobians

$$H^1(Y) \cong GJ[p^\infty]^\wedge,\ H^1(X) \cong J[p^\infty]^\wedge.$$

where $\wedge$ is $\mathbb{Q}_p/\mathbb{Z}_p$-dual. By this duality, the sequence

$$0 \to T \to GJ \to J \to 0$$

is dual to

$$0 \to H^1(X) \to H^1(Y) \to \mathbb{Z}_p \to 0.$$

Taking the q-kernel of the first of the above two sequences, we have the following

exact sequence:

$$0 \to T[q] \to GJ[q] \to J[q] \to 0 \tag{4.6}$$

The exactness of above sequence is from the exactness of the following sequence:

$$0 \to H^1(X)/q \to H^1(Y)/q \to \mathbb{Z}_p e/q \to 0, \tag{4.7}$$

where $e = (\infty) - (0) \in \frac{H^1(Y)}{H^1(X)}$.

Notation 4.3.2. *Let $\xi = \frac{n}{m}$ and $n = vq$, where $(n, m) = 1$. Note that $\frac{\xi}{q}$ and $\frac{1}{v}$ can be viewed as elements in $(\mathbb{Z}/q\mathbb{Z})^\times$. To avoid ambiguity, we choose $\widetilde{r}, \widetilde{v} \in \mathbb{Z}$ such that $\widetilde{r} \equiv \frac{\xi}{q} \in \mathbb{Z}/q\mathbb{Z}, \widetilde{v} \equiv \frac{1}{v} \in \mathbb{Z}/q\mathbb{Z}$.*

Let $D = v(0) - v(\infty) \in J[p^\infty]$. The following lemma is from [9, section 9.6].

Lemma 4.3.3. *Let*

$$\frac{H^1(Y)(1)_{DM}}{H^1(X)(1)} \xrightarrow{\iota} H^1(X)(1) \otimes \frac{\mathbb{Q}_p}{\mathbb{Z}_p}$$

be the map induced by $H^1(Y)_{DM}(1) \to H^1(X)(1) \otimes_{\mathbb{Z}_p} \frac{\mathbb{Q}_p}{\mathbb{Z}_p}$. Then ι maps the image of $v\{0, \infty\}_{DM}$ to the image of D in $H^1(X)(1) \otimes \frac{\mathbb{Q}_p}{\mathbb{Z}_p}$.

Proof. The proof can be found in [9, Lemma 9.6.5]. For the convenience of the reader, we review the proof here. Viewing $v\{0, \infty\}$ as an element in $H^1(Y)(1)$, we know that the image of $v\{0, \infty\}$ in $\frac{H^1(Y)(1)}{H^1(X)(1)}$ is $-D$. Since the order of D is q, we have $qD =$

$\mathrm{Div}(h)$ for some $h \in \mathcal{O}(Y)^\times$. This means that $-qv\{0,\infty\} \equiv [h] \bmod H^1(X)(1)$, where $[h]$ is the Kummer class of h. We can write

$$-qv\{0,\infty\} = [h] + x \tag{4.8}$$

for some $x \in H^1(X)(1)$. We write x as a projective system $(x_1, x_2, \ldots)$, where $x_i \in \frac{H^1(X)(1)}{p^i H^1(X)(1)}$ for $i \in \mathbb{Z}_{>0}$. Modulo q, we have

$$[h] = -x_f \in \frac{H^1(Y)(1)}{qH^1(Y)(1)}.$$

From the exact sequence

$$0 \to H^1(X)(1) \to H^1(Y)(1) \to \mathbb{Z}_p \to 0,$$

we know that the map $\frac{H^1(X)(1)}{qH^1(X)(1)} \xrightarrow{i} \frac{H^1(Y)(1)}{qH^1(Y)(1)}$ is injective. By [9, Lemma 9.6.4], we know that $i(D) = [h]$ and $i(D + x_f) = x_f + [h] = 0$. Hence,

$$D = -x_f \in \frac{H^1(X)(1)}{qH^1(X)(1)}. \tag{4.9}$$

Taking the Drinfeld-Manin splitting map for (4.8), since $[h]$ maps to 0 and x maps to x, we have

$$qv\{0,\infty\}_{DM} = -x \in H^1(Y)(1)_{DM}. \tag{4.10}$$

Note that we have a canonical injection

$$\frac{H^1(Y)(1)_{DM}}{H^1(X)(1)} \xrightarrow{\iota} H^1(X)(1) \otimes \frac{\mathbb{Q}_p}{\mathbb{Z}_p}.$$

By (4.10), we have $\iota(v\{0,\infty\}_{DM}) = (-x) \otimes \frac{1}{q}$. By (4.9), we have $(-x) \otimes \frac{1}{q} = D \in H^1(X)(1) \otimes \frac{\mathbb{Q}_p}{\mathbb{Z}_p}$. □

Remark 4.3.4. The map ι maps $\{0,\infty\}_{DM}$ to $\widetilde{v}D \in J[q]$.

Lemma 4.3.5. *The map*

$$(-, W_N\xi\{0,\infty\}_{DM}) : H^1(X) \to \mathbb{Z}_p/\xi\mathbb{Z}_p \to \frac{\frac{1}{\xi\mathbb{Z}_p}}{\mathbb{Z}_p} \hookrightarrow \frac{\mathbb{Q}_p}{\mathbb{Z}_p}$$

corresponds to the element $-\widetilde{v}D$ in $J[p^\infty]$.

Proof. We identify $\frac{H^1(Y)(1)_{DM}}{H^1(X)(1)}$ with $J[p^\infty]$ using the following canonical isomorphism

$$\frac{H^1(Y)(1)_{DM}}{H^1(X)(1)} \xrightarrow{\iota} H^1(X)(1) \otimes \frac{\mathbb{Q}_p}{\mathbb{Z}_p} = J[p^\infty].$$

From the pairing

$$H^1(X) \times J[p^\infty] \to \frac{\mathbb{Q}_p}{\mathbb{Z}_p},$$

we have the following pairing

$$H^1(X) \times \frac{H^1(Y)(1)_{DM}}{H^1(X)(1)} \to \frac{\mathbb{Q}_p}{\mathbb{Z}_p}.$$

Via the isomorphism

$$\frac{H^1(Y)(1)_{DM}}{H^1(X)(1)} \to J[p^\infty],$$

$\{0,\infty\}_{DM}$ maps to $\widetilde{v}D \in J[q]$ (Remark 4.3.4). Note that the image of W_N in $\mathfrak{h}_0(N)_{\mathfrak{P}}$ is -1. Therefore, the map $(-, W_N\xi\{0,\infty\}_{DM})$ can be restated as

$$H^1(X) \xrightarrow{s} \frac{\mathbb{Q}_p}{\mathbb{Z}_p}[q] \cong \frac{\frac{1}{\xi\mathbb{Z}_p}}{\mathbb{Z}_p},$$

where the map s corresponds to $-\widetilde{v}D \in \mathrm{Hom}(H^1(X), \frac{\mathbb{Q}_p}{\mathbb{Z}_p}[q])$. Then the lemma follows. □

Corollary 4.3.6. *Taking the $\frac{\mathbb{Q}_p}{\mathbb{Z}_p}$-dual of the map $H^1(X) \to Q = \mathbb{Z}/q\mathbb{Z}$, we get a map*

$$Q^\wedge \to J[q].$$

Then the canonical generator of $Q^\wedge$ maps to $-r\widetilde{v}D \in J[q]$.

Proof. For $\frac{\mathbb{Q}_p}{\mathbb{Z}_p}[q]$, we have a canonical generator $\frac{1}{q}$. So we have a canonical isomorphism

$$Q^\wedge \cong \mathbb{Z}/q\mathbb{Z}.$$

Note that in Lemma 4.3.5, we choose a generator $\frac{1}{\xi} \in \frac{\mathbb{Q}_p}{\mathbb{Z}_p}[q]$. So the canonical generator of $Q^\wedge$ maps to $-r\widetilde{v}D$. □

Definition 4.3.7. In the sequence (4.6), pulling back by the map $\mathbb{Z}/q\mathbb{Z} \to J[q]$ which takes 1 to $-r\widetilde{v}D$, and pushing out by the map $T[q] \to \mu_q$ corresponding to e, we get an extension class:

$$0 \to \mu_q \to ? \to \mathbb{Z}/q\mathbb{Z} \to 0. \tag{4.11}$$

Remark 4.3.8. The extension class (4.3) is obtained from the sequence (4.7) via pullback by e, and pushout by the map $H^1(X) \to Q$. If we take the Pontryagin dual, it is the sequence that is obtained from the sequence (4.7) via pullback by the map of $\mathbb{Z}/q\mathbb{Z} \to J[q]$ which maps 1 to $-r\widetilde{v}D$ and pushout by e. So the extension class (4.11) is negative of the extension class given by (4.3). We will compute the extension class given by (4.11).

For the computation of the extension class given by (4.11), we have the following general proposition which is from [9, Section 9.6]:

Proposition 4.3.9. *Let C be a smooth projective curve over a field k with characteristic 0. Let Σ be a finite set of k-rational points of C. Fix two degree 0 divisors D_1 and D_2 such that both of them are supported on Σ, and D_1 is order q. Starting from the following exact sequence*

$$0 \to T[q](\bar{k}) \to GJ[q](\bar{k}) \to J[q](\bar{k}) \to 0,$$

we may pull back by the map $\mathbb{Z}/q\mathbb{Z} \to J[q]; 1 \mapsto D_1$ *and push out by the map* $D_2 : T[q] \to \mu_q$ *to obtain an exact sequence*

$$0 \to \mu_q \to ? \to \mathbb{Z}/q\mathbb{Z} \to 0. \tag{4.12}$$

Let F *be a rational function on* C *such that* $qD_1 = (F)$*, and let* h *be a rational function on* C *such that* $\mathrm{div}(h) - D_1$ *is supported away from* Σ*. Then the extension class of (4.12) coincides with the Kummer class of*

$$(\frac{F}{h^q})(-D_2) := \prod_{x \in \Sigma} \frac{F}{h^q}(x)^{-m(x)},$$

where $D_2 = \sum_{x \in \Sigma} m(x) \cdot x$

Proof. We will use the following description of $GJ(\bar{k})$:

$$GJ(\bar{k}) = \mathrm{Div}^0_\Sigma(\bar{C})/\{\mathrm{div}(f) : f \in K(\bar{C}), f \equiv 1 \bmod \Sigma\},$$

where $\mathrm{Div}^0_\Sigma(\bar{C})$ is the group of degree 0 divisors away from Σ. Choose a rational function $\alpha \in K(\bar{C})$ such that $\frac{F}{h^q \alpha^q} \equiv 1 \bmod \Sigma$, and let $A = \mathrm{div}(\alpha)$. From the assumption, we know that

$$qD_1 - q\mathrm{div}(h) - qA = 0 \in GJ(\bar{k}).$$

So we have $D_1 - \mathrm{div}(h) - A \in GJ[q](\bar{k})$. Note that $D_1 - \mathrm{div}(h) - A = D_1 \in J[q](\bar{k})$,

since $\mathrm{div}(h)$ and A are principal divisors. Hence the extension class is given by

$$\sigma \mapsto \sigma(D_1 - \mathrm{div}(h) - A) - (D_1 - \mathrm{div}(h) - A).$$

Note that $D_1 - \mathrm{div}(h)$ is k-rational, so the extension class is the class of

$$\sigma \mapsto A - \sigma A,$$

which is the Kummer class of α^{-q}. Since $\frac{F}{h^q \alpha^q} \equiv 1 \bmod \Sigma$, we have

$$\frac{F}{h^q}(x) = \alpha^q(x) \text{ for all } x \in \Sigma.$$

Hence, after pushout by D_2, the extension class is given by the Kummer class of $(\frac{F}{h^q})(-D_2)$. □

Theorem 4.3.10. *The extension class c is the Kummer class of N, and the invariant $\tilde{c}$ equals* 1.

Proof. We apply Proposition 4.3.9 to the case that the curve is the modular curve $X_0(N)$, and $D_1 = -r\widetilde{v}D = -r\widetilde{v}v((0) - (\infty))$ and $D_2 = (\infty) - (0)$. We need to find a function F such that $\mathrm{div}(F) = -qr\widetilde{v}D$. By Remark 2.4.13, we know that $\mathrm{div}(g^{-1}) = \xi((0) - (\infty))$. Hence $\mathrm{div}(g^{\frac{m}{v} r\widetilde{v}v}) = -qr\widetilde{v}v((0) - (\infty))$. It is easy to see

that $\frac{m}{v} r\widetilde{v}v \equiv 1 \bmod q$. Again by Remark 2.4.13, we have

$$\frac{g^{\frac{m}{v} r\widetilde{v}v}(0)}{g^{\frac{m}{v} r\widetilde{v}v}(\infty)} = N^a,$$

where $a \equiv -1 \bmod q$, which means that the extension class (4.11) is given by the Kummer class of N^{-1}. Therefore, the extension class (4.3) is given by the Kummer class of N. By the isomorphism of Lemma 4.1.5 (2), the invariant $\tilde{c}$ equals 1. $\square$

4.4 The cocycle χ_b

Recall the cocycle $\chi_b \in \mathrm{Hom}(G_{-1}, P \otimes I/I^2) \cong \mathrm{Hom}(G_{-1}, I^2/I^3 \otimes \mu_q^{-1})$. In this section, we try to give a conjectural inverse map to χ_b.

4.4.1 K-theory of integer rings

In this section, we review some basic facts in K-theory. For details, one can see [31]. For any scheme X, there is a Grothendieck group $K_0(X)$. It is defined as the abelian group generated by symbols $[\mathcal{E}]$, where $\mathcal{E}$ runs over all isomorphism classes of vector bundles on X, with relations of the form

$$[\mathcal{E}] = [\mathcal{E}'] + [\mathcal{E}'']$$

for every exact sequence $0 \to \mathcal{E}' \to \mathcal{E} \to \mathcal{E}'' \to 0$. For a ring R, one defines $K_0(R)$ to be $K_0(\mathrm{Spec}\,(R))$.

Quillen showed that $K_0(X)$ is the first of an infinite sequence of K-groups which are the higher homotopy groups of certain spaces attached to X.

We list some important properties of K-groups that we will use:

1. There are products $K_p(X) \times K_q(X) \to K_{p+q}(X)$.

2. The unit group $\mathcal{O}(X)^\times$ injects into $K_1(X)$, with equality if $X = \operatorname{Spec} F$ is the spectrum of a field.

3. The K-groups of finite fields are finite:

$$K_{2n-1}(\mathbb{F}_q) \cong \mathbb{Z}/(q^n - 1)\mathbb{Z}, \;\; K_{2n}(\mathbb{F}_q) = 0 \; (n > 0).$$

For a number field F, we have the following exact sequence:

$$\ldots \to K_q(\mathfrak{o}_F) \to K_q(\mathfrak{o}_{F,S}) \to \prod_{\mathfrak{p} \in S} K_{q-1}(\mathfrak{o}_F/\mathfrak{p}) \to K_{q-1}(\mathfrak{o}_F) \to \ldots,$$

where $\mathfrak{o}_F$ is the algebraic integer ring of F and $\mathfrak{o}_{F,S}$ is the S-integer ring of F.

There is another type of K-group which is called a Milnor K-group:

Definition 4.4.1. For a unital ring R, define

$$K_*^M(R) = T^* R^\times / \langle a \otimes (1 - a) \mid a \in R^\times - \{1\} \rangle$$

to be the quotient of the tensor algebra over $\mathbb{Z}$ by the two-sided ideal generated by the elements $a \otimes (1-a), a \neq 0, 1$. Let $K_n^M(R)$ be the the n-th graded quotient of $K_*^M(R)$.

Remark 4.4.2. If F is a field, then $K_2(F) \cong K_2^M(F)$. In general, they are different.

We will use the following theorem to identify K-groups with étale cohomology groups:

Theorem 4.4.3. *For a number field F, let S be a finite set of places containing the places above p. Then there is a étale Chern character inducing an isomorhism:*

$$K_2(\mathfrak{o}_{F,S}) \otimes \mathbb{Z}_p \to H^2_{\text{ét}}(\mathfrak{o}_{F,S}, \mathbb{Z}_p(2)).$$

For the proof, one can see [34].

Remark 4.4.4. We may identify Galois cohomology groups with étale cohomology groups: for the details, see [17].

4.4.2 Cohomological interpretation of G_{-1}

Lemma 4.4.5. *We have the following exact sequence:*

$$0 \to K_2(\mathbb{Z}[\zeta_N]) \otimes \mathbb{Z}_p \to K_2(\mathbb{Z}[\zeta_N, \tfrac{1}{N}]) \otimes \mathbb{Z}_p \to K_1(\mathbb{F}_N) \otimes \mathbb{Z}_p \to 0.$$

Proof. This is from the localization sequence of K-groups and the facts that

1. $K_2(\mathbb{F}_N) = 0$,

2. $K_1(\mathbb{Z}[\zeta_N]) \otimes \mathbb{Z}_p \hookrightarrow K_1(\mathbb{Z}[\zeta_N, \frac{1}{N}]) \otimes \mathbb{Z}_p$.

□

Corollary 4.4.6. *Using the Chern class maps of Theorem 4.4.3, we have the following exact sequence in étale cohomology:*

$$0 \to H^2(\mathbb{Z}[\zeta_N, \tfrac{1}{p}], \mathbb{Z}_p(2)) \to H^2(\mathbb{Z}[\zeta_N, \tfrac{1}{Np}], \mathbb{Z}_p(2)) \to \mathbb{F}_N^\times \otimes \mathbb{Z}_p \to 0.$$

Let $G = \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$. We have the following lemma:

Lemma 4.4.7. *Via the injection of Corollary 4.4.6, we have*

$$H^2(\mathbb{Z}[\zeta_N, \tfrac{1}{p}], \mathbb{Z}_p(2)) = I_G H^2(\mathbb{Z}[\zeta_N, \tfrac{1}{Np}], \mathbb{Z}_p(2)).$$

Proof. It suffices to show that the map induced on coinvariants

$$H^2(\mathbb{Z}[\zeta_N, \tfrac{1}{Np}], \mathbb{Z}_p(2))_G \to \mathbb{F}_N^\times \otimes \mathbb{Z}_p$$

from the exact sequence of Corollary 4.4.6 is an isomorphism. But

$$H^2(\mathbb{Z}[\zeta_N, \tfrac{1}{Np}], \mathbb{Z}_p(2))_G \cong H^2(\mathbb{Z}[\tfrac{1}{Np}], \mathbb{Z}_p(2))$$

by [24, Proposition 3.3.11] and

$$H^2(\mathbb{Z}[\tfrac{1}{Np}], \mathbb{Z}_p(2)) \cong K_2(\mathbb{Z}[\tfrac{1}{Np}]) \otimes \mathbb{Z}_p = \mathbb{F}_N^\times \otimes \mathbb{Z}_p,$$

so the surjection is an isomorphism by equality of orders. □

Corollary 4.4.8. *Fix the isomorphism*

$$I_G/I_G^2 \to G,$$

$$g - 1 \mapsto g.$$

We have canonical isomorphisms:

$$H^2(\mathbb{Z}[\zeta_N, \tfrac{1}{p}], \mathbb{Z}_p(2))_G \cong \frac{I_G H^2(\mathbb{Z}[\zeta_N, \frac{1}{Np}], \mathbb{Z}_p(2))}{I_G^2 H^2(\mathbb{Z}[\zeta_N, \frac{1}{Np}], \mathbb{Z}_p(2))} \cong I_G/I_G^2 \otimes \mathbb{F}_N^\times \otimes \mathbb{Z}_p \cong U^{\otimes 2}.$$

Proposition 4.4.9. *We have a canonical isomorphism:*

$$H^2(\mathbb{Z}[\zeta_N, \tfrac{1}{p}], \mathbb{Z}_p(2))_G \cong G_{-1} \otimes \mu_q.$$

Proof. Let $\Delta = \mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q})$. Since $H^2(\mathbb{Z}[\zeta_N, \frac{1}{p}], \mathbb{Z}_p(2))_G \cong U^{\otimes 2} \cong \mathbb{Z}/q\mathbb{Z}$ and $\operatorname{Spec} \mathbb{Z}[\zeta_N, \frac{1}{p}]$ has p-cohomological dimension 2 (see [24, Proposition 8.3.18]), we know that

$$H^2(\mathbb{Z}[\zeta_N, \tfrac{1}{p}], \mathbb{Z}_p(2))_G \cong H^2(\mathbb{Z}[\zeta_N, \tfrac{1}{p}], \mu_q^{\otimes 2})_G.$$

Since

$$H^2(\mathbb{Z}[\zeta_N, \tfrac{1}{p}], \mu_q^{\otimes 2}) \cong H^2(\mathbb{Z}[\zeta_{Nq}, \tfrac{1}{p}], \mu_q^{\otimes 2})_\Delta$$

by [24, Proposition 3.3.11], we only need to understand $H^2(\mathbb{Z}[\zeta_{Nq}, \frac{1}{p}], \mu_q^{\otimes 2})_{G\times\Delta}$. By [24, Proposition 8.3.11], we have the following sequence

$$0 \to A_{\mathbb{Q}(\zeta_{Nq}),p} \otimes \mathbb{Z}/q\mathbb{Z} \to H^2(\mathbb{Z}[\tfrac{1}{p}, \zeta_{Nq}], \mu_q) \to \bigoplus_{v|p} H^2(\mathbb{Q}(\zeta_{Nq})_v, \mu_q) \to \mathbb{Z}/q\mathbb{Z} \to 0,$$

where $A_{\mathbb{Q}(\zeta_{Nq}),p}$ is ideal class group of $\mathbb{Q}(\zeta_{Nq})$ modulo the ideal classes $[\mathfrak{p}]$, for $\mathfrak{p}|p$. Taking the κ^{-1}-eigenquotient, where κ is the modulo q cyclotomic character, since $H^2(\mathbb{Q}(\zeta_{Nq})_v, \mu_q^{\otimes 2}) \cong \mu_q$ and Δ does not permute the $v \mid p$, we have $(\bigoplus_{v|p} H^2(\mathbb{Q}(\zeta_{Nq})_v, \mu_q^{\otimes 2})_\Delta = 0$. Thus, we have the following:

$$(A_{\mathbb{Q}(\zeta_{Nq}),p})_{\kappa^{-1}} \otimes \mu_q \cong H^2(\mathbb{Z}[\zeta_{Nq}, \tfrac{1}{p}], \mu_q^{\otimes 2})_\Delta.$$

Hence

$$H^2(\mathbb{Z}[\zeta_{Nq}, \tfrac{1}{p}], \mu_q^{\otimes 2})_{G\times\Delta} \cong (A_{\mathbb{Q}(\zeta_{Nq}),p})_{\kappa^{-1},G} \otimes \mu_q.$$

Now let $F/\mathbb{Q}(\zeta_{Nq})$ be the field extension that corresponds to $(A_{\mathbb{Q}(\zeta_{Np}),p})_{\kappa^{-1}}$. Note that by Proposition 4.1.3, we have

$$G_{-1} \cong \mathrm{Gal}(F_{-1}/K),$$

where F_{-1} is tamely ramified at N and split completely at the prime dividing p. Hence, $F_{-1}\mathbb{Q}(\zeta_{Nq})$ is unramfied over $\mathbb{Q}(\zeta_{Nq})$ with κ^{-1}-action and split completely at

the primes dividing p. Then, we have $F_{-1}\mathbb{Q}(\zeta_{Nq}) \subset F$, which means that G_{-1} is a quotient of $(A_{\mathbb{Q}(\zeta_{Nq}),p})_{\kappa^{-1},G}$, but they have the same size, so we have

$$(A_{\mathbb{Q}(\zeta_{Nq}),p})_{\kappa^{-1},G} \cong G_{-1}.$$

□

Remark 4.4.10. By Corollary 4.4.8 and Proposition 4.4.9, we have a canonical isomorphism:

$$G_{-1} \cong U^{\otimes 2} \otimes \mu_q^{-1}.$$

4.4.3 The map from homology to Galois cohomology

Definition 4.4.11 (Adjusted Manin symbol)**.** For $u, v \in \mathbb{Z}/N\mathbb{Z}$ with $(u, v) = 1$, we let

$$[u, v]' = W_N[u, v] = \left\{\frac{-d}{bN}, \frac{-c}{aN}\right\},$$

where $a, b, c, d \in \mathbb{Z}$ satisfy $ad - bc = 1, u = c \mod N, v = d \mod N$.

Let $[u, v]^* := W_N[u, v]^+ = \frac{1}{2}([u, v]' + [u, -v]')$

Lemma 4.4.12. *The diamond operator $\langle j \rangle$ $(j \in \mathbb{F}_N^\times)$ acts on $[u, v]'$ as follows:*

$$\langle j \rangle [u, v]' = [j^{-1}u, j^{-1}v]'.$$

Proof. We have

$$\langle j\rangle[u,v]' = \langle j\rangle W_N[u,v] = W_N\langle j\rangle^*[u,v] = [j^{-1}u, j^{-1}v]'.$$

□

Theorem 4.4.13. *The relative homology group $H_1(X_1(N), \text{cusps}, \mathbb{Z}_p)^+$ has a presentation as a $\mathbb{Z}_p[\mathbb{F}_N^\times]$-module with generators $[u,v]^*$ for $u, v \in \mathbb{F}_N$ and $(u,v) = (1)$, subject to the following relations:*

1. $[u,v]^* + [-v,u]^* = 0$,
2. $[u,v]^* = [u, u+v]^* + [u+v, v]^*$,
3. $[-u,-v]^* = [u,v]^* = [u,-v]^*$,
4. $\langle j\rangle[u,v]^* = [j^{-1}u, j^{-1}v]^*$ *for* $j \in \mathbb{F}_N^\times$.

Remark 4.4.14. We have the following isomorphisms via Poincaré duality

$$H^1(X_1(N)(\mathbb{C}), \mathbb{Z}_p) \cong H_1(X_1(N)(\mathbb{C}), \mathbb{Z}_p),$$

$$H^1(Y_1(N)(\mathbb{C}), \mathbb{Z}_p) \cong H_1(X_1(N)(\mathbb{C}), \text{cusps}, \mathbb{Z}_p).$$

Note that these isomorphisms are not Hecke compatible, they transfer from the $T(l)^*$-action to the $T(l)$-action. For the details, one can see [32, Proposition 3.5].

Remark 4.4.15. If we identify $H^1(X_1(N)(\mathbb{C}), \mathbb{Z}_p)$ (resp. $H^1(Y_1(N)(\mathbb{C}), \mathbb{Z}_p)$) with $H^1_{\text{ét}}(X_1(N))$ (resp. $H^1_{\text{ét}}(Y_1(N))$), Poincaré duality also changes the Galois action. In fact we have an isomorphism

$$H^1_{\text{ét}}(X_1(N))(1) \cong H_1(X_1(N)(C), \mathbb{Z}_p),$$

which respects complex conjugation. For the details, one can see [32, Section 3.5].

Lemma 4.4.16. *Let $\tilde{C}_0$ denote the cusps of $X_1(N)(\mathbb{C})$ that lie above the 0 cusp in $X_0(N)$, and let $\tilde{C}_\infty$ denote the cusps of $X_1(N)(\mathbb{C})$ that lie above the ∞ cusp in $X_0(N)$. The Manin symbols $[u, v]$ $(u \neq 0, v \neq 0)$ generate the relative homology group $H_1(X_1(N), \tilde{C}_0, \mathbb{Z}_p)$, and Manin symbols $[u, v]'$ generate the relative homology group $H_1(X_1(N), \tilde{C}_\infty, \mathbb{Z}_p)$.*

Proposition 4.4.17 (Sharifi)**.** *There exists a homomorphism*

$$\varpi^0 : H_1(X_1(N), \tilde{C}_\infty, \mathbb{Z}_p)^+ \to H^2(\mathbb{Z}[\zeta_N, \tfrac{1}{Np}], \mathbb{Z}_p(2))^+.$$

$$[u, v]^* \mapsto (1 - \zeta_N^u, 1 - \zeta_N^v)^+.$$

Proof. We only need to check the relations of Theorem 4.4.13 can be realized in $H^2(\mathbb{Z}[\zeta_N, \frac{1}{Np}], \mathbb{Z}_p(2))^+$. It is proved in [32]. We review the the proof here.

1. For $[u:v]^* + [-v,u]^* = 0$, we need to check that

$$(1-\zeta_N^u, 1-\zeta_N^v)^+ + (1-\zeta_N^{-v}, 1-\zeta_N^u)^+ = 0.$$

This follows from the equality

$$1-\zeta_N^v = -\zeta_N^v(1-\zeta_N^{-v})$$

and the fact that roots of unity pair with cyclotomic units trivially in the plus part.

2. For $[u:v]^* = [u,u+v]^* + [u+v,v]^*$, note that

$$\frac{1-\zeta_N^u}{1-\zeta_N^{u+v}} + \zeta_N^u \frac{1-\zeta_N^v}{1-\zeta_N^{u+v}} = 1,$$

so we have

$$\left(\frac{1-\zeta_N^u}{1-\zeta_N^{u+v}}, \frac{1-\zeta_N^v}{1-\zeta_N^{u+v}}\right)^+ = 0,$$

which gives

$$\left(1-\zeta_N^u, 1-\zeta_N^v\right)^+ = \left(1-\zeta_N^u, 1-\zeta_N^{u+v}\right)^+ + \left(1-\zeta_N^{u+v}, 1-\zeta_N^v\right)^+.$$

□

Definition 4.4.18. Since $H_1(X_1(N),\mathbb{Z}_p)^+ \subset H_1(X_1(N),\tilde{C}_\infty,\mathbb{Z}_p)^+$, via restriction,

we have the following homomorphism:

$$\varpi : H_1(X_1(N), \mathbb{Z}_p)^+ \to H^2(\mathbb{Z}[\zeta_N, \tfrac{1}{Np}], \mathbb{Z}_p(2))^+.$$

Definition 4.4.19. (Eisenstein ideal for $X_1(N)$) Let $\mathfrak{I}_0$ be the ideal of $\mathrm{End}_{\mathbb{Z}_p}(H_1(X_1(N), \tilde{C}_\infty, \mathbb{Z}_p))$ generated by $T(l) - l - \langle l \rangle$, for $l \neq N$, and $T(N) - N$, and let I_0 be the image of $\mathfrak{I}_0$ in $\mathrm{End}_{\mathbb{Z}_p}(H_1(X_1(N), \mathbb{Z}_p))$. Let $\mathfrak{I}_\infty$ be the ideal of $\mathrm{End}_{\mathbb{Z}_p}(H_1(X_1(N), \tilde{C}_\infty, \mathbb{Z}_p))$ generated by $T(l) - 1 - l\langle l \rangle$, for $l \neq N$, and $T(N) - 1$, and let I_∞ be the image of $\mathfrak{I}_\infty$ in $\mathrm{End}_{\mathbb{Z}_p}(H_1(X_1(N), \mathbb{Z}_p))$.

Lemma 4.4.20. *We have* $\mathfrak{I}_0 H_1(X_1(N), \tilde{C}_\infty, \mathbb{Z}_p) \subset H_1(X_1(N), \mathbb{Z}_p)$.

Proof. One can check that $\mathfrak{I}_0$ kills $\tilde{C}_\infty$. For the Hecke action on cusps, one can see [30, Section 1.2]. □

4.4.4 Topological boundary and arithmetic boundary

In this section, we compare the following three exact sequences:

$$0 \to H^2(\mathbb{Z}[\tfrac{1}{p}, \zeta_N^+], \mathbb{Z}_p(2)) \to H^2(\mathbb{Z}[\tfrac{1}{Np}, \zeta_N^+], \mathbb{Z}_p(2)) \xrightarrow{\partial} H^2(\mathbb{Q}(\zeta_N^+)_N, \mathbb{Z}_p(2)) \to 0, \tag{4.13}$$

where $\mathbb{Q}(\zeta_N^+)_N$ is the completion of $\mathbb{Q}(\zeta_N^+)$ at the place dividing N,

$$0 \to K_2(\mathbb{Z}[\zeta_N^+]) \otimes \mathbb{Z}_p \to K_2(\mathbb{Z}[\zeta_N^+, \tfrac{1}{N}]) \otimes \mathbb{Z}_p \xrightarrow{\partial} K_1(\mathbb{F}_N) \otimes \mathbb{Z}_p \to 0, \tag{4.14}$$

$$0 \to H_1(X_1(N), \mathbb{Z}_p)^+ \to H_1(X_1(N), \tilde{C}_\infty, \mathbb{Z}_p)^+ \xrightarrow{\partial'} \bigoplus\nolimits^0_{\tilde{C}_\infty} \mathbb{Z}_p \to 0, \tag{4.15}$$

where $\bigoplus^0$ denotes the elements which sum to zero.

Remark 4.4.21. We identify sequence (4.13) with the sequence (4.14) via the étale chern class map.

Proposition 4.4.22. *In sequence (4.13), the residue map ∂ satisfies*

$$\partial(1 - \zeta_N^u, 1 - \zeta_N^v)^+ = \frac{u}{v} \in \mathbb{F}_N^\times \otimes \mathbb{Z}_p.$$

Proof. By the definition of tame symbol, we have

$$\partial(1 - \zeta_N^u, 1 - \zeta_N^v) = (-1)\frac{1 - \zeta_N^u}{1 - \zeta_N^v} \equiv -\frac{u}{v} \in \mathbb{F}_N^\times \otimes \mathbb{Z}_p.$$

Note that -1 is trivial in $\mathbb{F}_N^\times \otimes \mathbb{Z}_p$. □

Proposition 4.4.23. *In sequence (4.15), the boundary map ∂' satisfies*

$$\partial'([u, v]^*) = \Big(\frac{-c}{Na}\Big) - \Big(\frac{-d}{Nb}\Big),$$

where $a, b, c, d \in \mathbb{Z}$ with $ad - bc = 1$, and $(u, v) \equiv (c, d) \bmod N$.

Proof. It is almost immediate from the definition. □

Definition 4.4.24. Let $s = \frac{c}{a}$ be an element of $\mathbb{Q} \cup \{\infty\}$ with $\gcd(a, c) = 1$ and $N \mid a$. We define a map t as follows:

$$t : \mathbb{Z}_p[\widetilde{C}_\infty] \to \mathbb{F}_N^\times \otimes \mathbb{Z}_p,$$

$$t(s) = c \in \mathbb{F}_N^\times \otimes \mathbb{Z}_p.$$

Remark 4.4.25. The map t is well defined. One can check this by using [7, Proposition 3.8.3].

Proposition 4.4.26. *The following diagram commutes:*

$$\begin{array}{ccc} H_1(X_1(N), \tilde{C}_\infty, \mathbb{Z}_p) & \xrightarrow{\partial} & \bigoplus_{\widetilde{C}_\infty}^{0} \mathbb{Z}_p \\ \downarrow{\scriptstyle \varpi^0} & & \downarrow{\scriptstyle t} \\ K_2(\mathbb{Z}[\zeta_N^+, \tfrac{1}{N}]) \otimes \mathbb{Z}_p & \xrightarrow{\partial'} & \mathbb{F}_N^\times \otimes \mathbb{Z}_p. \end{array} \tag{4.16}$$

Proof. Using Proposition 4.4.23, we know that

$$t(\partial([u, v]^*)) = \frac{u}{v}.$$

And using Proposition 4.4.22 and the definition of ϖ, we know that

$$\partial' \varpi^0([u, v]^*) = \frac{c}{d} = \frac{u}{v} \in \mathbb{F}_N^\times \otimes \mathbb{Z}_p.$$

□

So we have the following proposition.

Proposition 4.4.27. *The image of ϖ is in $H^2(\mathbb{Z}[\zeta_N, \frac{1}{p}], \mathbb{Z}_p(2))^+$ or $K_2(\mathbb{Z}[\zeta_N^+]) \otimes \mathbb{Z}_p$.*

Proof. This is the map on kernels of the horizontal maps in the commutative diagram (4.16). □

Remark 4.4.28. By Remark 4.4.15, we may also view ϖ as a map:

$$\varpi : H^1(X_1(N), \mathbb{Z}_p)^-(1) \to H^2(\mathbb{Z}[\tfrac{1}{p}, \zeta_N], \mathbb{Z}_p(2))^+.$$

4.4.5 Sharifi's conjecture

In this section, we list several conjectures made by Sharifi.

Conjecture 4.4.29. *The map ϖ^0 satisfies*

$$\varpi^0(\eta x) = 0$$

for all $\eta \in \mathfrak{I}_\infty$ and $x \in H_1(X_1(N), \tilde{C}_\infty, \mathbb{Z}_p)$.

Lemma 4.4.30 (Busuioc, Sharifi)**.** *We have*

$$\varpi^0 \circ (T(2) - 1 - 2\langle 2 \rangle) = 0,$$

$$\varpi^0 \circ (T(3) - 1 - 3\langle 3\rangle) = 0.$$

Proof. For the proof, one can see [3, Theorem 1.2]. □

Remark 4.4.31. Conjecture 4.4.29 has been proved under the assumption $p \mid N$: see [9, Theorem 5.2.3].

Let $\widetilde{I} = I_\infty + I_G$. Then we have the following map of exact sequences which gives the relationship between the cohomology of $X_1(N)$ and $X_0(N)$:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \frac{H^1(X_1(N),\mathbb{Z}_p)^-}{\widetilde{I}H^1(X_1(N),\mathbb{Z}_p)^-} & \longrightarrow & \frac{H^1(X_1(N),\mathbb{Z}_p)}{\widetilde{I}H^1(X_1(N),\mathbb{Z}_p)} & \longrightarrow & \frac{H^1(X_1(N),\mathbb{Z}_p)^+}{\widetilde{I}H^1(X_1(N),\mathbb{Z}_p)^+} & \longrightarrow & 0 \\ & & \downarrow \pi & & \downarrow \cong & & \downarrow \cong & & \\ 0 & \longrightarrow & \frac{IH^1(X_0(N),\mathbb{Z}_p)^-}{I^2H^1(X_0(N),\mathbb{Z}_p)^-} & \longrightarrow & \frac{IH^1(X_0(N))^- \oplus H^1(X_0(N))^+}{I^2H^1(X_0(N))^- \oplus IH^1(X_0(N))^+} & \longrightarrow & \frac{H^1(X_0(N),\mathbb{Z}_p)^+}{IH^1(X_0(N),\mathbb{Z}_p)^+} & \longrightarrow & 0 \end{array}$$

Remark 4.4.32. The surjectivity of the vertical maps is from Theorem 3.3.22. The injectivity of the vertical maps is from [16, Proposition 4.5].

Remark 4.4.33. Note that the sequence

$$0 \to \frac{H^1(X_1(N),\mathbb{Z}_p)^-}{\widetilde{I}H^1(X_1(N),\mathbb{Z}_p)^-} \to \frac{H^1(X_1(N),\mathbb{Z}_p)}{\widetilde{I}H^1(X_1(N),\mathbb{Z}_p)} \to \frac{H^1(X_1(N),\mathbb{Z}_p)^+}{\widetilde{I}H^1(X_1(N),\mathbb{Z}_p)^+} \to 0$$

also gives the same extension class as b in $H^1(\mathbb{Z}[\frac{1}{Np}], P \otimes I/I^2)$. It gives a character

$$\chi_b : G_{-1} \to \frac{H^1(X_1(N),\mathbb{Z}_p)^-}{\tilde{I}H^1(X_1(N),\mathbb{Z}_p)^-} \cong \frac{IH^1(X_0(N),\mathbb{Z}_p)^-}{I^2H^1(X_0(N),\mathbb{Z}_p)^-} \cong I/I^2 \otimes P.$$

In [32], Sharifi made a general conjecture about the relationship between homol-

ogy of modular curves and Galois cohomology of number fields. We just express the related form that we need here.

Conjecture 4.4.34 (Sharifi). *1. The map ϖ induces an isomorphism:*

$$\frac{H^1(X_1(N),\mathbb{Z}_p)^-(1)}{I_\infty H^1(X_1(N),\mathbb{Z}_p)^-(1)} \cong \frac{H_1(X_1(N),\mathbb{Z}_p)^+}{I_\infty H_1(X_1(N),\mathbb{Z}_p)^+} \xrightarrow{\varpi} H^2(\mathbb{Z}[\zeta_N^+,\tfrac{1}{p}],\mathbb{Z}_p(2)).$$

2. Let ϖ_G be the map induced by ϖ on G-coinvariants. It is a map

$$\frac{IH^1(X_0(N),\mathbb{Z}_p)^-(1)}{I^2H_1(X_0(N),\mathbb{Z}_p)^-(1)} \to H^2(\mathbb{Z}[\zeta_N,\tfrac{1}{p}],\mathbb{Z}_p(2))_G \cong G_{-1}\otimes\mu_q.$$

Twisting the coefficients, we have a map

$$\varpi_G\otimes\mu_q^{-1} : \frac{IH^1(X_0(N),\mathbb{Z}_p)^-}{I^2H_1(X_0(N),\mathbb{Z}_p)^-} \to H^2(\mathbb{Z}[\zeta_N^+,\tfrac{1}{p}],\mathbb{Z}_p(2))_G\otimes\mu_q^{-1} \cong G_{-1}.$$

Then

$$\chi_b\circ(\varpi_G\otimes\mu_q^{-1}) = (\varpi_G\otimes\mu_q^{-1})\circ\chi_b = 1.$$

Remark 4.4.35. The analogous conjecture for modular curves of level divisible by p has been proved by Takako Fukaya and Kazuya Kato when certain hypotheses hold. For details, one can see [9].

Lemma 4.4.36. *In the following diagram*

$$\begin{array}{ccc} H_1(X_1(N), \tilde{C}_\infty, \mathbb{Z}_p)^+ & \xrightarrow{\varpi^0} & H^2(\mathbb{Z}[\zeta_N^+, \frac{1}{Np}], \mathbb{Z}_p(2)) \\ \downarrow \pi & & \downarrow \\ H_1(X_0(N), \mathbb{Z}_p)^+ & \xrightarrow{\varpi_G^0} & H^2(\mathbb{Z}[\frac{1}{Np}], \mathbb{Z}_p(2)), \end{array}$$

the vertical maps are both surjective. The map ϖ_G^0 factors through the quotient by $IH_1(X_0(N), \mathbb{Z}_p)^+$.

Proof. The surjectivity of vertical maps is from the definitions and the fact that there are only two cusps on $X_0(N)$. Let us compute $\pi([u,v]^*) = \pi(W_{\zeta_N}([u,v])) = W_N\pi([u,v])$. Using Hensel's lemma, we have that the image of W_N in $\mathfrak{h}_0(N)_{\mathfrak{P}}$ with $\mathfrak{P}$ as in Definition 3.1.12 is -1. Hence, in $H_1(X_0(N), \mathbb{Z}_p)^+_{\mathfrak{P}}$, we have $\pi([u,v]^*) = -\pi(\langle v\rangle[\frac{u}{v}, 1]) = -[\frac{u}{v}, 1]$. Let $x \in \mathbb{Z}$ be a lifting of $\frac{u}{v}$. By computation, we have $[\frac{u}{v}, 1] = \{0, \frac{1}{x}\}$. Using Proposition 3.1.9, we know that the element $-\{0, \frac{1}{x}\}$ corresponds to $\frac{u}{v} \in U$. By Proposition 4.4.22, we know that $[u,v]^*$ maps to $\frac{u}{v} \in U \cong H^2(\mathbb{Z}[\frac{1}{Np}], \mathbb{Z}_p(2))$. So ϖ_G^0 maps $-\{0, \frac{1}{x}\}$ to $\frac{u}{v}$. From this, we know that $\varpi_G^0 = \phi$, where ϕ is the map defined in Proposition 3.1.9. Since ϕ factors through $IH_1(X_0(N), \mathbb{Z}_p)^+$, we know that ϖ_G^0 factors through $IH_1(X_0(N), \mathbb{Z}_p)^+$. □

Remark 4.4.37. We also have the following commutative diagram

$$\begin{array}{ccc} H_1(X_1(N),\mathbb{Z}_p)^+ & \xrightarrow{\varpi} & H^2(\mathbb{Z}[\zeta_N^+,\frac{1}{p}],\mathbb{Z}_p(2)) \\ \downarrow{\scriptstyle \pi} & & \downarrow \\ IH_1(X_0(N),\mathbb{Z}_p)^+ & \xrightarrow{\varpi_G} & H^2(\mathbb{Z}[\zeta_N^+,\frac{1}{p}],\mathbb{Z}_p(2))_G. \end{array}$$

However, we cannot prove that ϖ_G factors through the quotient by $I^2H_1(X_0(N),\mathbb{Z}_p)^+$. If we know that 2 or 3 are good prime numbers, we can conclude that it does by Theorem 3.1.14.

4.4.6 Computation of b

In this section, assuming Conjecture 4.4.29 and Conjecture 4.4.34, we compute the invariant $\tilde{b}$. Recall that in Lemma 3.1.8, we have a canonical isomorphism:

$$\phi : U \to H_1(X_0(N),\mathbb{Z}_p)^+/IH_1(X_0(N),\mathbb{Z}_p)^+$$

We identify the two groups by ϕ.

Lemma 4.4.38. *For $u,v \in \mathbb{F}_N^\times$, the image of $(l+\langle l\rangle - T(l))[u,v]^*$ in $\frac{IH_1(X_0(N),\mathbb{Z}_p)^+}{I^2H_1(X_0(N),\mathbb{Z}_p)^+} \cong I/I^2 \otimes \frac{H_1(X_0(N),\mathbb{Z}_p)^+}{IH_1(X_0(N),\mathbb{Z}_p)^+}$ is $\eta_l \otimes \frac{u}{v}$, where we view $\frac{u}{v}$ as an element in $U \cong \frac{H_1(X_0(N),\mathbb{Z}_p)^+}{IH_1(X_0(N),\mathbb{Z}_p)^+}$.*

Proof. By definition, we have $\pi((l+\langle l\rangle - T(l))[u,v]^*) = \eta_l\pi([u,v]^*)$. From the proof of Lemma 4.4.36, we know that $\pi([u,v]^*) = \frac{u}{v}$. Then we can conclude that the image

of $(l+\langle l\rangle - T(l))[u,v]^*$ in $\frac{IH_1(X_0(N),\mathbb{Z}_p)^+}{I^2H_1(X_0(N),\mathbb{Z}_p)^+}$ is $\eta_l \otimes \frac{u}{v}$. □

Lemma 4.4.39. *Via $\partial \circ \varpi^0$, $[u,v]^*$ maps to $\frac{u}{v}$ in $H^2(\mathbb{Q}_N(\zeta_N),\mathbb{Z}_p(2)) \cong U$.*

Proof. The image of $\varpi^0([u,v]^*)$ in $H^2(\mathbb{Q}_N(\zeta_N),\mathbb{Z}_p(2))$ is $(1-\zeta_N^u, 1-\zeta_N^v)$ by definition. Via the map $H^2(\mathbb{Q}_N(\zeta_N),\mathbb{Z}_p(2)) \cong U$, the image of $(1-\zeta_N^u, 1-\zeta_N^v)$ is exactly $\frac{u}{v}$ by Proposition 4.4.22. □

Since $(l+\langle l\rangle - T(l))[u,v]^* \in H_1(X_1(N),\mathbb{Z}_p)$, via ϖ, it maps into

$$I_G/I_G^2 \otimes H^2(\mathbb{Z}[\tfrac{1}{Np},\zeta_N],\mathbb{Z}_p(2)) \cong G \otimes U.$$

Lemma 4.4.40. *Via ϖ, the element $(l+\langle l\rangle - T(l))[u,v]^*$ maps to $l^{l-1} \otimes \frac{u}{v}$.*

Proof. Note that by definition, we have

$$\varpi((l+\langle l\rangle - T(l))[u,v]^*) = \varpi^0((l+\langle l\rangle - T(l))[u,v]^*).$$

If we assume the Eisenstein quotient conjecture for ϖ^0 and note that

$$l+\langle l\rangle - T(l) \equiv (l-1)(1-\langle l\rangle) \mod I_\infty. \tag{4.17}$$

We have

$$\varpi^0((l+\langle l\rangle - T(l))[u,v]^*) = \varpi^0((l-1)(1-\langle l\rangle)[u,v]^*) = (l-1)(1-\sigma_l^{-1})\varpi^0([u,v]^*).$$

By the isomorphism in Corollary 4.4.8, $(l-1)(1-\sigma_l^{-1})$ maps to $l^{l-1} \in G \otimes \mathbb{Z}_p$. Since $\partial\varpi^0([u,v]^*) = \frac{u}{v} \in U$, we have proved that $\varpi((l+\langle l\rangle - T(l))[u,v]^*) = l^{l-1} \otimes \frac{u}{v}$. □

Theorem 4.4.41. *Suppose that Conjecture 4.4.29 and Conjecture 4.4.34 hold. Then the invariant $\tilde{b}$ equals 1.*

Proof. By Lemma 4.4.38 and Lemma 4.4.40, we know that

$$\varpi_G(\eta_l \otimes \frac{u}{v}) = l^{l-1} \otimes \frac{u}{v}.$$

Assuming Conjecture 4.4.34, we know that

$$\chi_b(l^{l-1} \otimes \frac{u}{v} \otimes \zeta_q) = \eta_l \otimes \frac{u}{v} \otimes \zeta_q.$$

Since the winding isomorphism identifies l^{l-1} with η_l (Proposition 3.1.11), we know that $\tilde{b} = 1$.

□

CHAPTER 5

Sharifi's conjecture

5.1 Eisenstein quotient conjecture

5.1.1 Goncharov and Brunault's map and the ∞-map

In [2], Brunault constructed a map from the first homology group of a modular curve to the second K-group of a modular variety tensored with $\mathbb{Q}$. In [11], Goncharov constructed a similar map to the second K-group of a modular variety without tensoring with $\mathbb{Q}$.

Theorem 5.1.1 (Brunault, Goncharov)**.** *There is a well-defined map* ρ

$$\rho' : H_1(X_1(N), \text{cusps}, \mathbb{Z}) \to K_2(Y_1(N)) \otimes \mathbb{Z}[\tfrac{1}{N}],$$

$$\rho'([u, v]) = g_{0,\frac{u}{N}} \cup g_{0,\frac{v}{N}}.$$

Corollary 5.1.2. *Since* $p \nmid N$*, we have a map*

$$H_1(X_1(N), \text{cusps}, \mathbb{Z}_p) \to K_2(Y_1(N)) \otimes \mathbb{Z}_p.$$

Remark 5.1.3. Composing ρ' with the étale chern class map, we get a map from a homology group to $H^2_{\text{ét}}(Y_1(N))(2)$. We still use ρ' to denote this map.

Remark 5.1.4. It is easy to see that $g_{0,\frac{u}{N}} \cup g_{0,\frac{v}{N}}$ lies in $H^2_{\text{ét}}(\mathcal{Y}_1(N) \otimes \mathbb{Z}[\frac{1}{p}], \mathbb{Z}_p(2))$. And the map $H^2_{\text{ét}}(\mathcal{Y}_1(N) \otimes \mathbb{Z}[\frac{1}{p}], \mathbb{Z}_p(2)) \to H^2_{\text{ét}}(Y_1(N))(2)$ is injective, which can be seen from the commutative diagram

$$\begin{array}{ccccccccc} 0 & \to & H^2(\mathbb{Z}[\frac{1}{Np}], \mathbb{Z}_p(2)) & \to & H^2_{\text{ét}}(\mathcal{Y}_1(N) \otimes \mathbb{Z}[\frac{1}{p}], \mathbb{Z}_p(2)) & \to & H^1(\mathbb{Z}[\frac{1}{Np}], H^1_{\text{ét}}(Y_1(N))(2)) & \to & 0 \\ & & \downarrow{\scriptstyle (1)} & & \downarrow & & \downarrow{\scriptstyle (2)} & & \\ 0 & \longrightarrow & H^2(\mathbb{Q}, \mathbb{Z}_p(2)) & \longrightarrow & H^2_{\text{ét}}(Y_1(N), \mathbb{Z}_p(2)) & \longrightarrow & H^1(\mathbb{Q}, H^1_{\text{ét}}(Y_1(N))(2)) & \longrightarrow & 0, \end{array}$$

where the rows of the diagram are from the Hochschild-Serre spectral sequence and the maps $(1), (2)$ are both injective. We can view ρ' as a map from a homology group to $H^2_{\text{ét}}(\mathcal{Y}_1(N) \otimes \mathbb{Z}[\frac{1}{p}], \mathbb{Z}_p(2))$.

Remark 5.1.5. The element $g_{0,\frac{u}{N}} \cup g_{0,\frac{v}{N}}$ is called a Beilinson-Kato element. See [1], [9], [25].

In [9], Fukaya and Kato defined a map $\infty(a, b)$ attached to the cusp $\infty_N(a, b)$:

$$H^2_{\text{ét}}(\mathcal{Y}_1(N)_{/\mathbb{Z}[1/Np]}, \mathbb{Z}_p(2)) \to H^2(\mathbb{Z}[\tfrac{1}{Np}, \zeta_N^+], \mathbb{Z}_p(2)).$$

And also, they proved in [9] the following theorem.

Theorem 5.1.6 (Fukaya-Kato)**.** *We have*

$$\varpi([u,v]^*) = \infty(0,1)(g_{0,\frac{u}{N}} \cup g_{0,\frac{v}{N}}).$$

The key property of $\infty(0,1)$ is found in the following proposition.

Proposition 5.1.7 (Fukaya-Kato)**.** *Restricted to the image of the Beilinson-Kato elements, the map $\infty(0,1)$ is killed by the Eisenstein ideal $\mathfrak{I}_\infty$.*

Proof. For the proof, see [9, Proposition 5.1.5, Proposition 5.1.7, Theorem 5.1.9]. □

Conjecture 5.1.8. *The map ρ is Hecke-equivariant.*

Corollary 5.1.9. *If Conjecture 5.1.8 is true, then Conjecture 4.4.29 is true.*

Note that we have the following exact sequence from the Hochschild-Serre spectral sequence:

$$0 \to H^2(\mathbb{Z}[\tfrac{1}{Np}], \mathbb{Z}_p(2)) \to H^2_{\text{ét}}(\mathcal{Y}_1(N) \otimes \mathbb{Z}[\tfrac{1}{p}], \mathbb{Z}_p(2)) \xrightarrow{g} H^1(\mathbb{Z}[\tfrac{1}{Np}], H^1_{\text{ét}}(Y_1(N))(2))) \to 0. \tag{5.1}$$

We define ρ:

$$\rho : H_1(X_1(N), \tilde{C}_\infty, \mathbb{Z}_p) \to H^2_{\text{ét}}(\mathcal{Y}_1(N) \otimes \mathbb{Z}[\tfrac{1}{p}], \mathbb{Z}_p(2)) \otimes \mathbb{Q}_p \cong H^1(\mathbb{Z}[\tfrac{1}{Np}], H^1_{\text{ét}}(Y_1(N))(2)).$$

In this section, we prove that the map

$$\rho : H_1(X_1(N), \tilde{C}_\infty, \mathbb{Z}_p) \to H^2_{\text{ét}}(\mathcal{Y}_1(N) \otimes \mathbb{Z}[\tfrac{1}{p}], \mathbb{Z}_p(2)) \otimes \mathbb{Q}_p$$

is well-defined and Hecke-equivariant.

5.1.2 Beilinson-Kato elements on $Y(M, N)$

Let $M, N \in \mathbb{Z}_+, M + N \geq 5$. Let $\mathcal{Y}(M, N)$ be the $\mathbb{Z}[\frac{1}{MN}]$-scheme that represents the functor of triples (E, e_1, e_2), where e_1 has order M, e_2 has order N, and $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \to E : (a, b) \mapsto ae_1 + be_2$ is injective. Similarly to Siegel units on $\mathcal{Y}(N)$, we can define Siegel units on $\mathcal{Y}(M, N)$.

Let $\mathcal{E}$ be the universal elliptic curve over $\mathcal{Y}(M, N)$.

Definition 5.1.10. For $(\alpha, \beta) = (\frac{a}{M}, \frac{b}{N}) \in (\frac{\frac{1}{M}\mathbb{Z}}{\mathbb{Z}} \times \frac{\frac{1}{N}\mathbb{Z}}{\mathbb{Z}})\backslash(0, 0)$ and for an integer $c > 1$ prime to $6MN$, we define the Siegel unit ${}_cg_{\alpha,\beta}$ as

$${}_cg_{\alpha,\beta} = \iota^*_{\alpha,\beta}({}_c\theta_{\mathcal{E}}) \in \mathcal{O}(\mathcal{Y}(M, N))^\times,$$

where $\iota_{\alpha,\beta} = ae_1 + be_2 : \mathcal{Y}(M, N) \to \mathcal{E}\backslash_c\mathcal{E}$. We define

$$g_{\alpha,\beta} = {}_cg_{\alpha,\beta} \otimes (c^2 - 1)^{-1} \in \mathcal{O}(\mathcal{Y}(M, N))^\times \otimes \mathbb{Q}.$$

In [9], the following objects are defined.

Definition 5.1.11 (Fukaya-Kato)**.** For a matrix $R = \left(\begin{smallmatrix} s & u \\ t & v \end{smallmatrix}\right) \in M_2(\mathbb{Z})$ such that $(s,u) \neq (0,0)$ and $(t,v) \neq (0,0)$, define:

$$ {}_{c,d}z_{m,M}(R) := {}_c g_{\frac{s}{m},\frac{u}{M}} \cup {}_d g_{\frac{t}{m},\frac{v}{M}} \in K_2(\mathcal{Y}(m,M)). $$

Let $z_{m,M}(R) = g_{\frac{s}{m},\frac{u}{M}} \cup g_{\frac{t}{m},\frac{v}{M}} \in K_2(\mathcal{Y}(m,M)) \otimes \mathbb{Q}$.

5.1.3 Beilinson-Kato elements on $Y_1(M) \otimes \mathbb{Q}(\zeta_m)$ and zeta values

In this section, we assume that $M \geq 4$ and $m \geq 1$.

Definition 5.1.12 (Fukaya-Kato)**.** Let $u, v \in \mathbb{Z}/M\mathbb{Z}$. Take lifts $u', v' \in \mathbb{Z}$ of u and v and integers s, t such that $sv' - tu' = 1$. Let ${}_{c,d}z_{1,M,m}(u,v)$ be the image of ${}_{c,d}z_{m,Mm}\left(\begin{smallmatrix} s & u' \\ t & v' \end{smallmatrix}\right)$ under the norm map $K_2(\mathcal{Y}(m,Mm)) \to K_2(\mathcal{Y}_1(M) \otimes \mathbb{Z}[\frac{1}{Mm}, \zeta_m])$.

We have the following two propositions that are from [9].

Proposition 5.1.13. *Let $N, M \geq 1$, and assume $N + M \geq 5$. Assume that the prime divisors of N are prime divisors of M. Let $L \geq 1$. Let $R \in \mathrm{GL}_2(\mathbb{Z}/L\mathbb{Z})$. Let $c, d \in \mathbb{Z}$ and assume that $(cd, 6NML) = 1$. Then the norm map $K_2(\mathcal{Y}(NL, ML)) \to K_2(\mathcal{Y}(N,M) \otimes \mathbb{Z}[\frac{1}{L}])$ sends ${}_{c,d}z_{NL,ML}(R)$ to*

$$ \left(\prod_{l \mid L, l \nmid N} P_l \right) \cdot {}_{c,d}z_{N,M}(R), $$

where

1. $P_l = 1 - T^*(l) \begin{pmatrix} \frac{1}{l} & 0 \\ 0 & 1 \end{pmatrix}^* + \begin{pmatrix} \frac{1}{l} & 0 \\ 0 & \frac{1}{l} \end{pmatrix}^* l$ *if* $l \nmid M$,
2. $P_l = 1 - T^*(l) \begin{pmatrix} \frac{1}{l} & 0 \\ 0 & 1 \end{pmatrix}^*$ *if* $l \mid M$.

Proposition 5.1.14. *Let $L \geq 1$, and let m, M be as in the beginning of this section. Then the norm map $K_2(Y_1(M) \otimes \mathbb{Z}[\frac{1}{mL}, \zeta_{mL}]) \to K_2(Y_1(M) \otimes \mathbb{Z}[\frac{1}{mL}, \zeta_m])$ sends ${}_{c,d}z_{1,M.mL}(u,v)$ to*

$$\prod_{l \in C'} (1 - \sigma_l^{-1} \otimes T^*(l) + \sigma_l^{-2} \otimes \langle l^{-1} \rangle l) \prod_{l \in C} (1 - \sigma_l^{-1} \otimes T^*(l))_{c,d} z_{1,M,m}(u,v),$$

where C' denotes the set of all prime numbers which divide L but do not divide mM, and C denotes the set of all primes which divide LM but do not divide m.

Definition 5.1.15 (Fukaya-Kato)**.** Let $Z_{1,M,m}(s) = \prod_l P_l(l^{-s})^{-1}$ be the operator-valued zeta function acting on

$$\mathbb{Z}[\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})] \otimes_{\mathbb{Z}[\{\pm 1\}]} H^1(Y_1(M)(\mathbb{C}), \mathbb{C}),$$

where

$$P_l(t) = 1 - \sigma_l^{-1} \otimes T^*(l)t + \sigma_l^{-2} \otimes \langle l \rangle^{-1} l t^2 \text{ if } l \nmid mM,$$

$$P_l(t) = 1 - \sigma_l^{-1} \otimes T^*(l)t \text{ if } l \nmid m, l \mid M,$$

$$P_l(t) = 1 \text{ if } l \mid m.$$

Remark 5.1.16. The zeta function $Z_{1,M,m}(s)$ converges when $\mathrm{Re}(s) > 2$, and has meromorphic continuation to the whole complex plane and is holomorphic except at $s = 2$.

Definition 5.1.17. Let ${}_{c,d}[u, v] \in \mathbb{Z}[\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})] \otimes H^1(Y_1(M)(\mathbb{C}), \mathbb{Z})$ be

$${}_{c,d}[u, v] = c^2 d^2 \otimes [u, v] - c^2 \sigma_d \otimes [u, dv] - d^2 \sigma_c \otimes [cu, v] + \sigma_{cd} \otimes [cu, dv],$$

where c, d are prime to $6Mm$.

Let $M \geq 5$. For $\alpha, \beta \in \mathbb{P}^1(\mathbb{Q})$, let $\{\alpha, \beta\} \in H_1(X_1(M)(\mathbb{C}), \mathrm{cusps}, \mathbb{Z})$ be the class of the geodesic line on the upper half plane from α to β. Via the canonical isomorphism of Poincare duality, we regard it as an element in $H^1(Y_1(M)(\mathbb{C}), \mathbb{Z})(1)$.

Definition 5.1.18. Let $M_2(M)_{\mathbb{Q}}$ be the space of all modular forms of weight 2 and

level M defined over $\mathbb{Q}$. We have the period map

$$\mathrm{per}' : M_2(M)_{\mathbb{Q}} \to H^1(Y_1(M)(\mathbb{C}), \mathbb{C}),$$

$$f \mapsto \phi_f : \{\alpha, \beta\} \mapsto \frac{1}{2\pi i} \int_\alpha^\beta f dz.$$

Definition 5.1.19. Define the equivariant period map,

$$\mathrm{per} : M_2(M)_{\mathbb{Q}} \otimes \mathbb{Q}(\zeta_m) \to \mathbb{Z}[\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})] \otimes H^1(X_1(M)(\mathbb{C}), \mathbb{C}),$$

$$x \otimes y \mapsto \sum_{g \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})} g \otimes g^{-1}(y)\mathrm{per}'(x).$$

We review some facts in p-adic Hodge theory. For the details, one can see [25, Section 9].

Definition 5.1.20. Let K be a local field that $[K : \mathbb{Q}_p] < \infty$. Let B_{dR} be p-adic field defined by Fontaine. It is a complete discrete valuation field with $\mathrm{Gal}(\bar{K}/K)$-action, and

$$H^0(K, B_{\mathrm{dR}}) = K.$$

Definition 5.1.21. For a finite dimensional $\mathbb{Q}_p$-vector space V with a continuous action of $\mathrm{Gal}(\bar{K}/K)$, let

$$D_{\mathrm{dR}}(V) = H^0(K, B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V).$$

Then $D_{\mathrm{dR}}(V)$ has a descending filtration $D^i_{\mathrm{dR}}(V)_{i\in\mathbb{Z}}$ defined by

$$D^i_{\mathrm{dR}}(V) = H^0(K, B^i_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V),$$

where B^i_{dR} denotes the subring of B_{dR} generates by the elements whose normalized valuation is $\geq i$.

If $\dim_K(D_{\mathrm{dR}}(V)) = \dim_{\mathbb{Q}_p}(V)$, we say that the representation V is a de Rham representation.

Example 5.1.22. *1. Let X be a smooth projective variety over K, let $m \in \mathbb{Z}_{\geq 0}$, and let $V = H^m(X \otimes \overline{K}, \mathbb{Q}_p)$. Then V is a de Rham representation, and $D_{\mathrm{dR}}(V) \cong H^m_{\mathrm{dR}}(X/K)$.*

2. Let $V = H^1_{\text{ét}}(Y_1(N), \mathbb{Q}_p)$. Then V is a de Rham representation and satisfies

$$D^i_{\mathrm{dR}}(V) = D_{\mathrm{dR}}(V), \;\; i \leq 0,$$

$$D^i_{\mathrm{dR}}(V) = 0, \;\; i \geq 2,$$

$$D^1_{\mathrm{dR}}(V) = M_2(\Gamma_1(N), \mathbb{Q}_p).$$

3. If V is de Rham representation, then $V(i)$ is also a de Rham representation

for $i \in \mathbb{Z}$, and

$$D^j_{\mathrm{dR}}(V(i)) = D^{i+j}_{\mathrm{dR}}(V).$$

Definition 5.1.23. Let V be a de Rham representation, we define a canonical homomorphism:

$$\exp^* : H^1(K, V) \to D^0_{\mathrm{dR}}(V).$$

as the composition

$$H^1(K, V) \to H^1(K, B^0_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V) \xleftarrow{\sim} H^0(K, B^0_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V) = D^0_{\mathrm{dR}}(V),$$

where the first map is induced by $v \mapsto 1 \otimes v$ for $v \in V$, and the second map is the cup product with the element

$$\log(\chi) \in H^1(K, \mathbb{Z}_p),$$

where χ is the p-adic cyclotomic character.

Definition 5.1.24. Consider the following composition:

$$\varprojlim_n K_2(\mathcal{Y}_1(Mp^n)) \xrightarrow{(1)} \varprojlim_n H^2(\mathcal{Y}_1(Mp^n), \mathbb{Z}_p(2)) \overset{(2)}{\cong} \varprojlim_n H^2(\mathcal{Y}_1(Mp^n), \mathbb{Z}_p(1))$$
$$\xrightarrow{(3)} H^2(\mathcal{Y}_1(M) \otimes \mathbb{Z}[\tfrac{1}{p}], \mathbb{Z}_p(1)) \xrightarrow{(4)} H^1(\mathbb{Z}[\tfrac{1}{pM}], H^1_{\text{ét}}(Y_1(M))(1)) \xrightarrow{(5)} H^1(\mathbb{Q}_p, H^1_{\text{ét}}(Y_1(M))(1))$$
$$\overset{\exp^*}{\to} M_2(M)_{\mathbb{Q}_p}$$

Remark 5.1.25. In 5.1.24, the map (1) is the étale Chern class map, the map (2) is defined by $\otimes(\zeta_{p^n}^{\otimes(-1)})_n$, the map (3) is the map corresponding the natural projection $Y_1(Mp^n) \to Y_1(M)$, the map (4) is the map from the spectral sequence, and the map (5) is the restriction map.

Theorem 5.1.26 (Fukaya-Kato)**.** *Assume $p \mid m$. Then the map* exp* *in Definition 5.1.24 sends $\left({}_{cd}z_{1,M,mp^n}(u,v)\right)_{n\geq 0}$ to an element of $M_2(M)_{\mathbb{Q}} \otimes \mathbb{Q}(\zeta_m)$ whose period image in $\mathbb{Z}[\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})] \otimes H^1(Y_1(M)(\mathbb{C}), \mathbb{C})$ coincides with $-Z_{1,M,m}(1)_{c,d}[u,v]^*$.*

Remark 5.1.27. This is Theorem 2.4.9 in [9], but we drop the assumption $p \mid M$, since the condition $p \mid M$ is not used.

5.1.4 The map z_{1,N,p^∞}

In this section, we focus on the modular curve $Y_1(N)$. Let $p \nmid N$ and let

$$\Lambda := \mathbb{Z}_p[[\mathbb{Z}_p^\times]] \cong \mathbb{Z}_p[[\mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q})]].$$

Let

$$\widetilde{\mathfrak{T}} := \varprojlim_n H^1(\mathbb{Z}[\tfrac{1}{Np}, \zeta_{p^n}], H^1_{\text{ét}}(Y_1(N))(1)).$$

Lemma 5.1.28. *The kernel of*

$$\exp^* : \widetilde{\mathfrak{T}} \to \varprojlim_n M_2(N) \otimes \mathbb{Q}(\zeta_{p^n}) \otimes \mathbb{Q}_p$$

coincides with the Λ*-torsion of* $\widetilde{\mathfrak{T}}$*.*

Proof. For the proof, see [9, Lemma 3.1.4]. □

Theorem 5.1.29 (Fukaya-Kato)**.** *There exists a unique Hecke-equivariant* Λ*-module homomorphism*

$$z'_{1,N,p^\infty} : \Lambda \otimes H^1(Y_1(M)(\mathbb{C}), \mathbb{Z}) \to \widetilde{\mathfrak{T}} \otimes Q(\Lambda)$$

satisfying the following conditions:

1. *For any* $\gamma \in \Lambda \otimes H^1(Y_1(M)(\mathbb{C}), \mathbb{Z})$ *and for any* c, d *such that* $(cd, 6Np) = 1$ *and* $c \equiv d \equiv 1 \mod N$*,* $(\sigma_c - c)(\sigma_d - d)z'_{1,N,p^\infty}(\gamma)$ *belongs to the image of* $\widetilde{\mathfrak{T}}$ *in* $\widetilde{\mathfrak{T}} \otimes Q(\Lambda)$*.*

2. *For* $n \geq 1$*, consider the dual exponential map*

$$\exp^*_{p^n} : H^1(\mathbb{Z}[\tfrac{1}{Np}, \zeta_{p^n}], H^1_{\acute{e}t}(Y_1(N))(1)) \otimes \mathbb{Q}_p \to M_2(N) \otimes \mathbb{Q}(\zeta_{p^n}) \otimes \mathbb{Q}_p$$

and the period map

$$\mathrm{per}_{p^n} : M_2(M) \otimes \mathbb{Q}(\zeta_{p^n}) \to \mathbb{Z}[\mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q})] \otimes H^1(Y_1(N)(\mathbb{C}), \mathbb{C}).$$

Then for any $\gamma \in H^1(Y_1(N)(\mathbb{C}), \mathbb{Z})$*, the image of* $z'_{1,N,p^\infty}(1 \otimes \gamma)$ *in* $M_2(N) \otimes \mathbb{Q}(\zeta_{p^n}) \otimes \mathbb{Q}_p$ *under* $\exp^*$ *is an element of* $M_2(M)_{\mathbb{Q}} \otimes \mathbb{Q}(\zeta_{p^n})$ *whose image in* $\mathbb{Z}[\mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q})] \otimes H^1(Y_1(N)(\mathbb{C}), \mathbb{C})$ *under* per_{p^n} *coincides with*

$$Z_{1,N,p^n}(1) \cdot \gamma.$$

Proof. The uniqueness is from Lemma 5.1.28 and the injectivity of the period map.

Let $\gamma \in H^1(Y_1(N)(\mathbb{C}), \mathbb{Z}_p)$. Suppose $\gamma = \sum a_i [u_i, v_i]^*$ where $a_i \in \mathfrak{h}_N$ and the $[u_i, v_i]^*$ are adjusted Manin symbols. Take $c, d \in \mathbb{Z} \backslash \{\pm 1\}$ such that $(cd, 6Mm) = 1$. Then $c - \sigma_c$ and $d - \sigma_d$ are non-zero divisors in Λ. Let

$$z'_{1,N,p^\infty}(\gamma) = (c - \sigma_c)^{-1}(d - \sigma_d)^{-1} \sum_i a_i \mathrm{tw}_{-1}({}_{c,d}z_{1,N,p^\infty}(u_i, v_i)) \in \widetilde{\mathfrak{T}} \otimes Q(\Lambda).$$

Here tw_{-1} is the twist by $\mathbb{Z}_p(-1)$. From the definition, we know that if this map is well defined, then it is Hecke-equivariant. Suppose we have two different expressions for γ:

$$\gamma = \sum_i a_i [u_i, v_i]^* = \sum_j b_j [u_j, v_j]^*. \tag{5.2}$$

Let

$$A = (c - \sigma_c)^{-1}(d - \sigma_d)^{-1} \sum_i a_i \mathrm{tw}_{-1}({}_{c,d}z_{1,N,p^\infty}(u_i, v_i)), \tag{5.3}$$

and

$$B = (c' - \sigma_{c'})^{-1}(d' - \sigma_{d'})^{-1} \sum_j b_j \mathrm{tw}_{-1}({}_{c,d}z_{1,N,p^\infty}(u_j, v_j)). \tag{5.4}$$

By Theorem 5.1.26, $\mathrm{per} \circ \exp^*$ maps both A and B to $Z_{1,N,p}(1)\gamma$. Then by Lemma 5.1.28 and the injectivity of period map, we know that $z'_{1,N,p^\infty}(\gamma)$ is well-defined. Then it is easy to check that $z'_{1,N,p^\infty}(\gamma)$ satisfies the properties in Theorem 5.1.29. □

Remark 5.1.30. This theorem is exactly the same as Theorem 3.1.5 in [9]. Here we don't require that $p \mid N$, but the proof is exactly the same.

By twisting coefficients, we have the following corollary.

Corollary 5.1.31. *We have a Hecke-equivariant Λ-homomorphism*

$$z_{1,N,p^\infty} : \Lambda \otimes H^1(Y_1(N)(\mathbb{C}), \mathbb{Z})(1) \to \widetilde{\mathfrak{T}}(1) \otimes Q(\Lambda)$$

induced by z'_{1,N,p^∞} such that

1. *z_{1,N,p^∞} sends ${}_{c,d}[u,v]^*$ to $({}_{c,d}z_{1,N,p^n}(u,v))_n$, and*

2. *the image of $[u,v]^*$ in $H^1(\mathbb{Z}[\frac{1}{Np}, \zeta_{p^n}], H^1_{\acute{e}t}(Y_1(N))(2)) \otimes \mathbb{Q}_p$ is $-z_{1,N,p^n}(u,v)$.*

So in the first layer of this tower, we have a Hecke-equivariant map:

$$\mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})] \otimes H^1(Y_1(N)(\mathbb{C}), \mathbb{Z})(1) \to H^1(\mathbb{Z}[\tfrac{1}{Np}, \zeta_p], H^1_{\text{ét}}(Y_1(N))(2)) \otimes \mathbb{Q}_p,$$

which induces a map

$$Z : H_1(Y_1(N)(\mathbb{C}), \mathbb{Z}) \to H^1(\mathbb{Z}[\tfrac{1}{Np}, \zeta_p], H^1_{\text{ét}}(Y_1(N))(2)) \otimes \mathbb{Q}_p$$

which sends $1 \otimes [u, v]^*$ to $-z_{1,N,p}(u, v)$.

Proposition 5.1.32. *The norm map*

$$H^1(\mathbb{Z}[\tfrac{1}{Np}, \zeta_p], H^1_{\text{ét}}(Y_1(N))(2)) \otimes \mathbb{Q}_p \to H^1(\mathbb{Z}[\tfrac{1}{Np}], H^1_{\text{ét}}(Y_1(N))(2)) \otimes \mathbb{Q}_p,$$

takes $z_{1,N,p}(u, v)$ *to* $(1 - T^*(p) + p\langle p\rangle^{-1})z_{1,N,1}(u, v)$.

Proof. It is immediate from Proposition 5.1.14. □

Remark 5.1.33. We have a Hecke-equivariant map

$$Z' : H_1(X_1(N)(\mathbb{C}), \widetilde{C}_\infty, \mathbb{Z}_p) \to H^1(\mathbb{Z}[\tfrac{1}{Np}], H^1_{\text{ét}}(Y_1(N))(2)) \otimes \mathbb{Q}_p$$

which sends $[u, v]^*$ to $(1 - T^*(p) + p\langle p\rangle^{-1})z_{1,N,1}(u, v)$.

Proposition 5.1.34. *The operator*

$$1 - T^*(p) + p\langle p\rangle^{-1} \in \text{End}_{\mathbb{Q}_p}\left(H^1(\mathbb{Z}[\tfrac{1}{Np}], H^1(\mathbb{Z}[\tfrac{1}{Np}], H^1_{\text{ét}}(X_1(N))(2))) \otimes \mathbb{Q}_p\right)$$

is injective.

Proof. For simplicity of notation, let $\eta_p = 1 - T^*(p) + p\langle p\rangle^{-1}$ and $V = H^1_{\text{ét}}(X_1(N))(1) \otimes \mathbb{Q}_p$. We have $V \cong \bigoplus_{f_i} T_p(A_{f_i}) \otimes \mathbb{Q}_p$, where the f_i are weight 2 newforms of $\Gamma_1(N)$. Note that Hecke action changes in the above isomorphism, so η_p acts on $T_p(A_{f_i}) \otimes \mathbb{Q}_p$ by multiplying by $1 - a_p(f) + p\chi_i(p)$, where χ_i is the character of f_i.

It is easy to see that $1 - a_p(f) + p\chi_i(p) \neq 0$. That is because the root of the polynomial $x^2 - a_p(f)x + p\chi_i(p)$ has absolute value $p^{1/2}$ (cf. [25, 14.10.5]). We know that η_p acts injectively on $V(1)$. Since $V(1)$ is a finite dimensional vector space, η_p is an isomorphism of $V(1)$. We can conclude that η_p is injective on $H^1(\mathbb{Z}[\frac{1}{Np}], V(1))$. $\square$

Proposition 5.1.35. *We have a Hecke-equivariant map*

$$\rho : H_1(X_1(N)(\mathbb{C}), \widetilde{C}_\infty, \mathbb{Z}_p) \to H^1(\mathbb{Z}[\tfrac{1}{Np}], H^1_{\text{ét}}(Y_1(N))(2)) \otimes \mathbb{Q}_p$$

which sends $[u, v]^*$ *to* $z_{1,N,1}(u, v)$.

Proof. We have the following exact sequence

$$0 \to H^1_{\text{ét}}(X_1(N))(2) \otimes \mathbb{Q}_p \to H^1_{\text{ét}}(Y_1(N))(2) \otimes \mathbb{Q}_p \to C(1) \to 0,$$

where $C = \bigoplus_{\text{cusps}}^0 \mathbb{Q}_p$. Note that $H^0(\mathbb{Z}[\frac{1}{Np}], C(1)) = 0$ since $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\zeta_N))$ acts triv-

ially on C. Taking Galois cohomology, we have the following exact sequence

$$0 \to H^1(\mathbb{Z}[\tfrac{1}{Np}], H^1_{\text{ét}}(X_1(N))(2) \otimes \mathbb{Q}_p) \to H^1(\mathbb{Z}[\tfrac{1}{Np}], H^1_{\text{ét}}(Y_1(N))(2) \otimes \mathbb{Q}_p) \tag{5.5}$$
$$\xrightarrow{t} H^1(\mathbb{Z}[\tfrac{1}{Np}], C(1)).$$

Let $\gamma \in H_1(X_1(N)(\mathbb{C}), \widetilde{C}_\infty, \mathbb{Z}_p)$. Suppose we have two different expressions for γ:

$$\gamma = \sum_i a_i[u_i, v_i]^* = \sum_j b_j[u_j, v_j]^*,$$

where a_i, b_j are elements in the Hecke algebra. Let $A = \sum_i a_i z_{1,N,1}(u_i, v_i)$ and $B = \sum_j b_j z_{1,N,1}(u_j, v_j)$. By [9, Theorem 3.9.3 (iii)], we have $t(A - B) = 0$. By (5.5), we have $A - B \in H^1(\mathbb{Z}[\frac{1}{Np}], H^1_{\text{ét}}(X_1(N))(2) \otimes \mathbb{Q}_p)$. By Remark 5.1.33, we know that $\eta_p(A - B) = 0$. From Proposition 5.1.34, we know that η_p is injective on $H^1(\mathbb{Z}[\frac{1}{Np}], H^1_{\text{ét}}(X_1(N))(2) \otimes \mathbb{Q}_p)$. So, we can conclude that $A = B$. □

Proposition 5.1.36. *The group $H^1(\mathbb{Z}[\frac{1}{Np}], H^1_{ét}(Y_1(N))(2))$ is $\mathbb{Z}_p$-torsion-free.*

Proof. Consider the exact sequence

$$0 \to H^1_{\text{ét}}(X_1(N)) \xrightarrow{i} H^1_{\text{ét}}(Y_1(N)) \to C \to 0,$$

where C is the cokernel of i. In order to prove that $H^1(\mathbb{Z}[\frac{1}{Np}], H^1_{\text{ét}}(Y_1(N))(2))$ is $\mathbb{Z}_p$-torsion-free, it suffices to prove that both $H^1(\mathbb{Z}[\frac{1}{Np}], H^1_{\text{ét}}(X_1(N))(2))$ and

$H^1(\mathbb{Z}[\frac{1}{Np}], C(2))$ are $\mathbb{Z}_p$-torsion-free. From the sequence

$$0 \to \mathbb{Z}_p(2) \xrightarrow{p} \mathbb{Z}_p(2) \to \mu_p^{\otimes 2} \to 0,$$

it suffices to prove that

1. $H^0(\mathbb{Z}[\frac{1}{Np}], H^1_{\text{ét}}(X_1(N))(2) \otimes \mathbb{F}_p) = 0$,

2. $H^0(\mathbb{Z}[\frac{1}{Np}], C(2) \otimes \mathbb{F}_p) = 0$.

Note that the $\text{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$-representation $H^1_{\text{ét}}(X_1(N))(2) \otimes \mathbb{Q}_p$ is crystalline. Then (1) is deduced from the statement that $H^0(\mathbb{Q}_p, H^1_{\text{ét}}(X_1(N))(2) \otimes \mathbb{F}_p) = 0$. For the details, see [8, Section 3.2]. For (2), it is true because $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\zeta_N))$ acts trivially on $C(1)$. □

Corollary 5.1.37. *If $p \nmid N\phi(N)$, then the Eisenstein quotient conjecture is true.*

Proof. If $p \nmid N\phi(N)$, it is easy to see that $H^2(\mathbb{Z}[\frac{1}{Np}], \mathbb{Z}_p(2)) = 0$. From (5.1), we have

$$H^2_{\text{ét}}(\mathcal{Y}_1(N) \otimes \mathbb{Z}[\tfrac{1}{p}], \mathbb{Z}_p(2)) \xrightarrow{\sim} H^1(\mathbb{Z}[\tfrac{1}{Np}], H^1_{\text{ét}}(Y_1(N))(2)).$$

Then the corollary follows from Proposition 5.1.35 and Proposition 5.1.36. □

5.2 Sharifi's conjecture for the modular curve $X_1(N)^{(p)}$

In this section, enlightened by Lecouturier's work [16], we consider Sharifi's conjecture for $X_1(N)^{(p)}$. We try to give some evidence for this conjecture.

Notation 5.2.1.

1. *Let* $G := (\mathbb{Z}/N\mathbb{Z})^\times/\{\pm 1\} = G_p \times G'$, *where* G_p *is the Sylow* p*-subgroup of* G *and* G' *is the maximal subgroup which has order not divisible by* p. *Let* $\Lambda = \mathbb{Z}_p[G]$ *and* $\Lambda_p = \mathbb{Z}_p[G_p]$.

2. *Let*
$$\widetilde{\xi} := \frac{N}{2}\sum_{i=1}^{N-1} \mathbb{B}_2(\frac{i}{N})[i] \in \Lambda,\ \tau = \sum_{\sigma \in G_p} \sigma.$$

3. *Let* $X_1(N)^{(p)}$ *(resp.,* $Y_1(N)^{(p)}$*) be the compact modular curve (resp., modular curve) corresponding to the congruence subgroup*
$$\Gamma_1(N)^{(p)} := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) \mid a \in G' \bmod N, d \in G' \bmod N \right\}.$$
We still use $\tilde{C}_\infty$ *to denote the cusps that lie above the* ∞ *cusp of* $X_0(N)$. *Let* $\mathfrak{H}$ *be the subring of* $\mathrm{End}_{\mathbb{Z}_p}(H_1(X_1(N)^{(p)}(\mathbb{C}), \tilde{C}_\infty, \mathbb{Z}_p))$ *generated by* $T^*(n)\,(n \geq 1)$ *and* $\langle n \rangle\,((n, N) = 1)$.

Let $\mathfrak{h}$ *be the subring of* $\mathrm{End}_{\mathbb{Z}_p}(H_1(X_1(N)^{(p)}(\mathbb{C}), \mathbb{Z}_p))$ *generated by* $T^*(n)$ $(n \geq 1)$ *and* $\langle n \rangle$ $((n, N) = 1)$.

4. *Let* $\mathbb{Q}(\zeta_N^{(p)})$ *be the maximal p-power subextension of* $\mathbb{Q}(\zeta_N)/\mathbb{Q}$, *and let* $\mathbb{Z}[\zeta_N^{(p)}]$ *be its integer ring. Note that this field is totally real.*

Lemma 5.2.2. *The natural maps of homology groups give the following isomorphisms:*

$$H_1(X_1(N)^{(p)}, \mathbb{Z}_p) \cong H_1(X_1(N), \mathbb{Z}_p)_{G'},$$

$$H_1(X_1(N)^{(p)}, \tilde{C}_\infty, \mathbb{Z}_p) \cong H_1(X_1(N), \tilde{C}_\infty, \mathbb{Z}_p)_{G'}.$$

Proof. By [16, Lemma 4.3], we know that

1. $I_{G'} H_1(X_1(N), \tilde{C}_\infty, \mathbb{Z}_p)$ is the kernel of the map
$$H_1(X_1(N), \tilde{C}_\infty, \mathbb{Z}_p) \to H_1(X_1(N)^{(p)}, \tilde{C}_\infty, \mathbb{Z}_p).$$
2. $I_{G'} H_1(X_1(N), \mathbb{Z}_p)$ is the kernel of the map
$$H_1(X_1(N), \mathbb{Z}_p) \to H_1(X_1(N)^{(p)}, \mathbb{Z}_p).$$

From [16, Corollary 4.2], we know that

$$H_1(X_1(N), \tilde{C}_\infty, \mathbb{Z}_p) \to H_1(X_1(N)^{(p)}, \tilde{C}_\infty, \mathbb{Z}_p)$$

is surjective.

$$H_1(X_1(N)^{(p)}, \tilde{C}_\infty, \mathbb{Z}_p) \cong H_1(X_1(N), \tilde{C}_\infty, \mathbb{Z}_p)_{G'}.$$

Since the order of G' is prime to p, we know that the map

$$H_1(X_1(N), \mathbb{Z}_p) \to H_1(X_1(N)^{(p)}, \mathbb{Z}_p)$$

is also surjective.

$$H_1(X_1(N)^{(p)}, \mathbb{Z}_p) \cong H_1(X_1(N), \mathbb{Z}_p)_{G'}.$$

□

Notation 5.2.3. *Let* $H_p = H_1(X_1(N)^{(p)}, \mathbb{Z}_p)$ *and* $\widetilde{H}_p = H_1(X_1(N)^{(p)}, \tilde{C}_\infty, \mathbb{Z}_p)$.

Theorem 5.2.4 (Lecouturier)**.** *The map* $\Lambda_p \to \mathfrak{H}$ *given by* $[d] \mapsto \langle d \rangle^{-1}$ *gives isomorphisms of* Λ_p*-modules*

$$\Lambda_p/\widetilde{\xi} \cong \mathfrak{H}/\mathfrak{I}_\infty \cong \widetilde{H}_p^+/\mathfrak{I}_\infty \widetilde{H}_p^+,$$

$$\Lambda_p/(\widetilde{\xi}, \tau) \cong \mathfrak{h}/I_\infty \cong H_p^+/I_\infty H_p^+.$$

Proof. For the proof, see [16, Theorem 4.6, Theorem 4.9]. □

Lemma 5.2.5. *We have the following exact sequence of* Λ_p*-modules*

$$0 \to H_p^+/I_\infty H_p^+ \to \widetilde{H}_p^+/\mathfrak{I}_\infty \widetilde{H}_p^+ \to \frac{I_{G_p}}{I_{G_p}^2} \cdot (\infty) \to 0. \tag{5.6}$$

Proof. From the definition, we have the following exact sequence

$$0 \to H_p^+ \to \widetilde{H}_p^+ \to I_{G_p} \cdot (\infty) \to 0.$$

Tensoring with $\mathfrak{H}/\mathfrak{I}_\infty$, we have the following exact sequence

$$H_p^+/I_\infty H_p^+ \xrightarrow{j} \widetilde{H}_p^+/\mathfrak{I}_\infty \widetilde{H}_p^+ \to \mathfrak{H}/\mathfrak{I}_\infty \otimes_{\mathfrak{H}} I_{G_p} \cdot (\infty) \to 0.$$

It is easy to see that $\mathfrak{H}/\mathfrak{I}_\infty \otimes_{\mathfrak{H}} I_{G_p} \cdot (\infty) \cong \frac{I_{G_p}}{I_{G_p}^2} \cdot (\infty)$. From Theorem 5.2.4, we know that

$$|H_p^+/I_\infty H_p^+| \cdot q = |\widetilde{H}_p^+/\mathfrak{I}_\infty \widetilde{H}_p^+|.$$

So, the map j has to be an injection. □

Similar to the case of the modular curve $X_1(N)$, we can define maps

$$\varpi_{G'} : H_p^+ \to H^2(\mathbb{Z}[\zeta_N^{(p)}, \tfrac{1}{p}], \mathbb{Z}_p(2)),$$

$$\varpi_{G'}^0 : \widetilde{H}_p^+ \to H^2(\mathbb{Z}[\zeta_N^{(p)}, \tfrac{1}{Np}], \mathbb{Z}_p(2)).$$

Lemma 5.2.6. *We have the following commutative diagrams:*

$$\begin{array}{ccc} H_1(X_1(N), \tilde{C}_\infty, \mathbb{Z}_p)^+ & \xrightarrow{\varpi^0} & H^2(\mathbb{Z}[\zeta_N^+, \frac{1}{Np}], \mathbb{Z}_p(2)) \\ \downarrow & & \downarrow \\ \widetilde{H}_p^+ & \xrightarrow{\varpi_{G'}^0} & H^2(\mathbb{Z}[\zeta_N^{(p)}, \frac{1}{Np}], \mathbb{Z}_p(2)), \end{array}$$

$$\begin{array}{ccc} H_1(X_1(N),\mathbb{Z}_p)^+ & \xrightarrow{\varpi} & H^2(\mathbb{Z}[\zeta_N^+,\tfrac{1}{p}],\mathbb{Z}_p(2)) \\ \downarrow & & \downarrow \\ H_p^+ & \xrightarrow{\varpi_{G'}} & H^2(\mathbb{Z}[\zeta_N^{(p)},\tfrac{1}{p}],\mathbb{Z}_p(2)). \end{array}$$

Proof. The diagram of $\varpi^0_{G'}$ commutes since ϖ^0 is G-equivariant, using the facts that $H_1(X_1(N),\tilde{C}_\infty,\mathbb{Z}_p)^+_{G'} \cong \widetilde{H}_p^+$ and $H^2(\mathbb{Z}[\zeta_N^+,\frac{1}{Np}],\mathbb{Z}_p(2))_{G'} \cong H^2(\mathbb{Z}[\zeta_N^{(p)},\frac{1}{Np}],\mathbb{Z}_p(2))$. Via restriction, we get the diagram for $\varpi_{G'}$ □

Similar to the case of the modular curve $X_1(N)$, we have the following conjecture.

Conjecture 5.2.7. *1. The map $\varpi^0_{G'}$ factors through the Eisenstein ideal.*

2. The map $\varpi_{G'}$ induces an isomorphism from $H_p^+/I_\infty H_p^+$ to $H^2(\mathbb{Z}[\zeta_N^{(p)},\frac{1}{p}],\mathbb{Z}_p(2))$.

Proposition 5.2.8. *The map $\varpi^0_{G'}$ is surjective.*

Proof. Note that ϖ^0_G takes values in $H^2(\mathbb{Z}[\zeta_N^+,\frac{1}{Np}],\mathbb{Z}_p(2))_G \cong H^2(\mathbb{Z}[\frac{1}{Np}],\mathbb{Z}_p(2)) \cong U$. The map $(\varpi^0_{G'})_{G_p} = \varpi^0_G$ is surjective since $\varpi^0_G([u,v]^*) = \frac{u}{v} \in U$. Then the proposition follows from Nakayama's lemma. □

Remark 5.2.9. Without using the Eisenstein quotient conjecture, we cannot prove that $\varpi_{G'}$ is surjective. If we assume the Eisenstein quotient conjecture, we can even prove that $\varpi_{G'}$ is an isomorphism. See Proposition 5.2.14.

Proposition 5.2.10. *As Λ_p-modules, we have an isomorphism*

$$H^2(\mathbb{Z}[\zeta_N^{(p)}, \tfrac{1}{Np}], \mathbb{Z}_p(2)) \cong \Lambda_p/(\widetilde{\xi}).$$

Proof. Since

$$H^2(\mathbb{Z}[\zeta_N^{(p)}, \tfrac{1}{Np}], \mathbb{Z}_p(2))_G \cong H^2(\mathbb{Z}[\tfrac{1}{Np}], \mathbb{Z}_p(2)) \cong \mathbb{F}_N^\times \otimes \mathbb{Z}_p,$$

$H^2(\mathbb{Z}[\zeta_N^{(p)}, \frac{1}{Np}], \mathbb{Z}_p(2))$ is a cyclic Λ_p-module. We only need to prove that the Fitting ideal of $H^2(\mathbb{Z}[\zeta_N^{(p)}, \frac{1}{Np}], \mathbb{Z}_p(2))$ is $\widetilde{\xi}$. This follows directly from the Coates-Sinnott conjecture for $\mathbb{Q}(\zeta_N)/\mathbb{Q}$ proven in [12, Theorem 6.19]. □

For the convenience of the reader, we review the Coates-Sinnott conjecture. Let K/k be abelian extension of number fields of Galois group $\tilde{G}$, and let S be a finite set of primes in k that contains all the ramified primes and all the primes over ∞.

Definition 5.2.11.

1. Set $e_n(K/k) := \prod_{v \in S_\infty} \frac{(1+(-1)^n \sigma_v)}{2}$ if k is totally real. Here, σ_v is complex conjugation.

2. Set $e_n(K/k) := 0$ if k is not totally real.

In [12], the following theorem is proved.

Theorem 5.2.12 (Greither, Popescu)**.** *If k is totally real, $p > 2$ and the classical Iwasawa μ-invariant associated to the maximal CM-subfield of $K(\mu_p)$ is zero, then we have*

$$\mathrm{Ann}_{\mathbb{Z}_p[G]}(H^1(\mathcal{O}_{K,S}[\tfrac{1}{p}],\mathbb{Z}_p(n))_{\mathrm{tors}})\Theta_{S,K/k}(1-n) = e_n(K/k).\mathrm{Fitt}(H^2(\mathcal{O}_{K,S}[\tfrac{1}{p}],\mathbb{Z}_p(n)), \tag{5.7}$$

where $\Theta_{S,K/k}(1-n) = \frac{1}{n}N^{n-1}\sum \mathbb{B}_n(\frac{i}{N})[i]$.

Now let $k = \mathbb{Q}, K = \mathbb{Q}(\zeta_N^{(p)}), n = 2, S = \{N, \infty\}$. Since K is abelian, the μ-invariant vanishes. As in proven in [12], one can show that

$$H^1(\mathcal{O}_{K,S}[\tfrac{1}{p}],\mathbb{Z}_p(2))_{\mathrm{tors}} = (\mathbb{Q}_p/\mathbb{Z}_p(2))^{G_K} = 0.$$

Since $K = \mathbb{Q}(\zeta_N^{(p)})$ is already totally real, $e_2(K/k)$ acts on the Fitting ideal trivially, so we get

$$\mathrm{Fitt}(H^2(\mathbb{Z}[\zeta_N^{(p)},\tfrac{1}{Np}],\mathbb{Z}_p(2))) = \Theta_{S,K/k}(-1)$$

In the case we are interested in, we have

$$\Theta_{S,K/k}(1-2) = \frac{1}{2}N\sum \mathbb{B}_2(\frac{i}{N})[i] = \tilde{\xi}.$$

By Theorem 5.2.12, we have

$$\mathrm{Fitt}(H^2(\mathbb{Z}[\zeta_N^{(p)}, \tfrac{1}{Np}], \mathbb{Z}_p(2))) = \widetilde{\xi}.$$

Corollary 5.2.13. *As Λ_p-modules; we have*

$$H^2(\mathbb{Z}[\zeta_N^{(p)}, \tfrac{1}{p}], \mathbb{Z}_p(2)) \cong (I_{G_p} + \widetilde{\xi})/\widetilde{\xi} \cong \Lambda_p/(\widetilde{\xi} + \tau).$$

Proof. From the localization sequence

$$0 \to H^2(\mathbb{Z}[\zeta_N^{(p)}, \tfrac{1}{p}], \mathbb{Z}_p(2)) \to H^2(\mathbb{Z}[\zeta_N^{(p)}, \tfrac{1}{Np}], \mathbb{Z}_p(2)) \to \mathbb{F}_N^{\times} \otimes \mathbb{Z}_p \to 0,$$

we know that

$$H^2(\mathbb{Z}[\zeta_N^{(p)}, \tfrac{1}{p}], \mathbb{Z}_p(2)) = I_{G_p} H^2(\mathbb{Z}[\zeta_N^{(p)}, \tfrac{1}{Np}], \mathbb{Z}_p(2)) = (I_{G_p} + \widetilde{\xi})/\widetilde{\xi}.$$

□

Proposition 5.2.14. *Assuming Conjecture 5.2.7 (1), the map $\varpi_{G'}^0$ induces an isomorphism*

$$\widetilde{H}_p^+/\mathfrak{I}_\infty \widetilde{H}_p \cong H^2(\mathbb{Z}[\zeta_N^{(p)}, \tfrac{1}{Np}], \mathbb{Z}_p(2)),$$

and $\varpi_{G'}$ induces an isomorphism

$$H_p^+/I_\infty H_p^+ \cong H^2(\mathbb{Z}[\zeta_N^{(p)}, \tfrac{1}{p}], \mathbb{Z}_p(2)).$$

Proof. From Theorem 5.2.4 and Proposition 5.2.10, we know that as Λ_p-modules, $\widetilde{H}_p^+/\mathfrak{I}_\infty\widetilde{H}_{(p)}$ and $H^2(\mathbb{Z}[\zeta_N^{(p)}, \frac{1}{Np}], \mathbb{Z}_p(2))$ are both isomorphic to $\Lambda_p/\widetilde{\xi}$. It suffices to prove that $\varpi_{G'}^0$ is a surjection, which is from Proposition 5.2.8. The statement on $\varpi_{G'}$ follows directly from the statement of $\varpi_{G'}^0$ and the exact sequence (5.6). □

Remark 5.2.15. A similar result has been obtained in [16, Proposition 4.34] assuming [15, Conjecture 1.10] and Eisenstein quotient conjecture for $\varpi_{G'}^0$. By using the theorem of Greither-Popescu, we can prove Conjecture 1.10 in [15].

REFERENCES

[1] A. Beilinson, Higher regulators and values of L-functions, Journal of Soviet Mathematics 30 (1985), 2036-2070.

[2] F. Brunault, Beilinson-Kato elements in K_2 of modular curves, Acta Arith. 134 (2008), 283-298.

[3] A. Busuioc, The Steinberg symbol and special values of L-functions, Trans. Amer. Math. Soc. 360 (2008), 5999-6015.

[4] F. Calegari and M. Emerton, On the ramification of Hecke algebras at Eisenstein primes, Invent. Math. 160 (2005), 97-144.

[5] F. Diamond and J. Im, Modular forms and modular curves, In: Seminar on Fermat's Last Theorem, (ed. V. Kumar Murty), CMS Conf. Proc. 17, Amer. Math. Soc. Providence, RI, 1995, 39-133.

[6] P. Deligne and M. Rapoport, Les schemas de modules de courbes elliptiques, In: Modular Functions of One Variable, II, Antwerp, 1972, (eds. P. Deligne and W. Kuyk), Lecture Notes in Math. 349, Springer-Verlag, Berline, 1973, 143-316.

[7] F. Diamond and J. Shurman, A first course in modular forms, Grad. Texts in Math 228, Springer, 2007.

[8] J. Fontaine and W. Messing, p-adic periods and p-adic étale cohomology, In: Current trends in arithmetical algebraic geometry, Contemp. Math. 67, Amer. Math. Soc. Providence, RI, 1987, 179-207.

[9] T. Fukaya and K. Kato, On conjectures of Sharifi, preprint.

[10] B. H. Gross, A tameness criterion for Galois representations associated to modular forms (mod p), Duke Math. J. 61 (1990), 445-517.

[11] A. Goncharov, Euler complexes and geometry of modular varieties, Geom. Funct. Anal. 17 (2008), 1872-1914.

[12] C. Greither and C. D. Popescu, An Equivariant Main Conjecture in Iwasawa theory and applications, J. Algebraic Geom. 24 (2015), 629-692.

[13] H. Hida, Elementary theory of L-functions and Eisenstein series, 2nd ed., London Mathematical Society Student Texts 26, Cambridge University Press, 1993.

[14] S. Lang, Introduction to Modular Forms, Grundlehren Math. Wiss, vol. 222, Springer-Verlag, Berlin-Heidelberg, 1987.

[15] E. Lecouturier, On the galois structure of the class group of certain kummer extensions, to appear in Journal of the London Mathematical Society.

[16] E. Lecouturier, Higher Eisenstein elements, higher Eichler formulas and ranks of Hecke algebras, arXiv:1709.09114v1, 2017.

[17] B. Mazur, Notes on étale cohomology of number fields, Ann. Sci. Ecole Norm. Sup. (4) 6 (1973), 521-552.

[18] B. Mazur, Modular curves and the Eisenstein ideal, Publ. Math. IHES 47 (1997), 33-186.

[19] B. Mazur, F. Calegari, R. Sharifi, W. Stein, The Square of the Eisenstein ideal and primitive roots, unpublished note.

[20] J. I. Manin, Parabolic points and zeta functions of modular curves, Izv. Akad. Nauk SSSR Ser. Mat 36 (1972), 19-66.

[21] L. Merel, Universal Fourier expansions of modular forms, On Artin's conjecture for odd 2-dimensional representations, Lecture Notes in Math. 1585, Springer, Berlin, 1994, 59-94.

[22] L. Merel, L'accouplement de Weil entre le sous-groupe de Shimura et le sous-groupe cuspidal $J_0(N)$, J. reine angew. Math. 477 (1996), 71-115.

[23] B. Mazur and A. Wiles, Class fields of abelian extensions of $\mathbb{Q}$, Invent. Math. 76 (1984), 179-330.

[24] J. Neukirch, A. Schmidt, and K. Wingberg, Cohomology of Number Fields, second ed., Grundl. Math. Wissen. 323, Springer-Verlag, Berlin, 2008.

[25] K. Kato, p-adic Hodge theory and values of zeta functions of modular forms, Astérisque 295 (2004), 117-290.

[26] N. Katz, B. Mazur, Arithmetic moduli of elliptic curves, Ann. of Math. Stud. 108, Princeton Univ. Press, Princeton, NJ, 1985.

[27] A. Ogg, Rational points on certain elliptic modular curves, Proc. Symp. Pure Math. 24 (1973), 221-231.

[28] M. Ohta, Ordinary p-adic étale cohomology groups attached to towers of elliptic modular curves, Compositio Math. 115 (1999), 241-301.

[29] M. Ohta, Congruence modules related to Eisenstein series, Ann. Sci. École Norm Sup. (4) 36 (2003), 225-269.

[30] M. Ohta, Eisenstein ideals and the rational torsion subgroups of modular Jacobian varieties, J. Math. Soc. Japan 65 (2013), 733-772.

[31] D. Quillen, Higher algebraic K-theory I, Lecture Notes in Math. 341 (1973), 85-147.

[32] R. Sharifi, A reciprocity map and the two-variable p-adic L-function, Ann. of Math. 173 (2011), 251-300.

[33] W. Stein, Modular forms, a computational approach, Graduate studies in Math. 79, Amer. Math. Soc, 2007.

[34] C. Soulé, Régulateurs. Séminaire Bourbaki, exposé 644, Astérisque 133/134 (1986), 237-253.

[35] P. Wake and C. Wang-Erickson, The rank of Mazur's Eisenstein ideal, arXiv:1707.01894v2, 2017.