Higher Eisenstein elements, higher Eichler formulas and rank of Hecke algebras

Emmanuel Lecouturier

Abstract Let \( N \) and \( p \) be primes such that \( p \) divides the numerator of \( \frac{N-1}{12} \). In this paper, we study the rank \( g_p \) of the completion of the Hecke algebra acting on cuspidal modular forms of weight 2 and level \( \Gamma_0(N) \) at the \( p \)-maximal Eisenstein ideal. We give in particular an explicit criterion to know if \( g_p \geq 3 \), thus answering partially a question of Mazur. In order to study \( g_p \), we develop the theory of higher Eisenstein elements, and compute the first few such elements in four different Hecke modules. This has applications such as generalizations of the Eichler mass formula in characteristic \( p \).

Contents

1 Introduction and results ..................................... 486
  1.1 Modular forms .................................... 489
  1.2 The supersingular module ................................ 492
  1.3 Odd modular symbols ................................ 494
  1.4 Even modular symbols ............................... 495
  1.5 Comparison ..................................... 497
2 The formalism of higher Eisenstein elements ...................... 498
  2.1 Algebraic setting .................................. 498
  2.2 The Newton polygon of \( \mathbb{T}_P \) ....................... 501
  2.3 Pairing between higher Eisenstein elements............. 502
  2.4 The special case of weight 2 and prime level ............ 503
3 The supersingular module .................................. 505

Emmanuel Lecouturier
lecoutu@tsinghua.edu.cn

Yau Mathematical Sciences Center and Tsinghua University, Beijing, China
1 Introduction and results

Let \( p \geq 2 \) and \( N \) be two prime numbers such that \( p \) divides the numerator of \( \frac{N - 1}{12} \), whose \( p \)-adic valuation is denoted by \( t \geq 1 \). This is the situation of an Eisenstein prime extensively studied in [19]. We fix in all the article a surjective group homomorphism \( \log : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{Z}/p^t\mathbb{Z} \). The various equalities stated in this paper will be independent of the choice of \( \log \) since both sides will depend on it in the same way.

Let \( \mathbb{T} \) (resp. \( \mathbb{T}^0 \)) be the \( \mathbb{Z}_p \)-Hecke algebra acting on the space of modular forms (resp. cuspidal modular forms) of weight 2 and level \( \Gamma_0(N) \). Let \( I \) (resp. \( I^0 \)) be the ideal of \( \mathbb{T} \) (resp. \( \mathbb{T}^0 \)) generated by the Hecke operators \( T_n - \sum_d d \), where the sum is over the divisors of \( n \) prime to \( N \). Let \( g_p \geq 1 \) be the rank of \( I^0 \)-adic completion of \( \mathbb{T}^0 \) as a \( \mathbb{Z}_p \)-module. Barry Mazur asked what can be said about \( g_p \) [19, p. 140]. This is one of the main motivations of this paper, and we provide a partial answer to Mazur’s question.
Loïc Merel was the first to give explicit information about $g_p$. For simplicity, in the rest of the introduction, we assume that $p \geq 5$.

**Theorem 1.1** [23, Théorème 2] *We have $g_p > 1$ if and only if*

\[ \sum_{k=1}^{N-1} k \cdot \log(k) \equiv 0 \pmod{p}. \]

We prove in Sect. 6.4 the following deceptively simple generalization.

**Theorem 1.2** *We have $g_p > 2$ if and only if*

\[ \sum_{k=1}^{N-1} k \cdot \log(k) \equiv \sum_{k=1}^{N-1} k \cdot \log(k)^2 \equiv 0 \pmod{p}. \]

The obvious generalization does not hold. More precisely, there seems to be no link between the vanishing of $\sum_{k=1}^{N-1} k \cdot \log(k)^3$ and the fact that $g_p > 3$.

For instance, if $p = 5$ and $N = 3671$, we have $g_p = 5$ but $\sum_{k=1}^{N-1} k \cdot \log(k)^3 \not\equiv 0 \pmod{p}$, and if $p = 7$ and $N = 4229$, we have $g_p = 3$ and $\sum_{k=1}^{N-1} k \cdot \log(k)^3 \equiv 0 \pmod{p}$.

Frank Calegari and Matthew Emerton have identified the $I$-adic completion of $\mathbb{T}$ with a universal deformation ring for the residual representation $\overline{\rho} = \left( \begin{array}{cc} \chi_p & 0 \\ 0 & 1 \end{array} \right)$, where $\chi_p$ is the reduction modulo $p$ of the $p$th cyclotomic character [7, Theorem 1.5]. They deduce a characterization of $g_p$ in terms of the existence of certain Galois deformations of $\overline{\rho}$. Using class field theory, they were able to prove the following result.

**Theorem 1.3** [7, Theorem 1.2 (ii)] *If $g_p \geq 2$ then the $p$-Sylow subgroup of the class group of $\mathbb{Q}(N^{1/p})$ is not cyclic.*

The converse of Theorem 1.3 happens to be false in general if $p > 5$.

Recently, Preston Wake and Carl Wang–Erickson [29] have built on the work of Calegari and Emerton. It would be interesting to compare their results to ours. In particular, they give another proof of Theorem 1.1 and they proposed our Theorem 1.2 as a conjecture.

Our work is of a different nature. If we compare to the standard conjectures on special values of L-functions, we work on the “analytic side” of the problem, while Calegari–Emerton and Wake–Wang–Erickson study the “algebraic side”.

Let us say a few words about the proof of Merel’s theorem. The essential point is the computation of the Eisenstein element of $H_1(X_0(N), \text{cusps}, \mathbb{Q})_+$. 
(the fixed part by complex conjugation of the singular homology relative to the cusps of the modular curve \(X_0(N)\) of level \(\Gamma_0(N)\)). It is an element annihilated by \(I\), which we denote by \(\tilde{m}^+_0\) (cf. Sect. 1.4). One can normalise \(\tilde{m}^+_0\) so that it has \(p\)-integral coefficients and one can show that \(g_p > 1\) if and only if \(\tilde{m}^+_0 \cdot m^-_1 \equiv 0 \pmod{p}\). Here, \(m^-_1\) is the Shimura class in \(H_1(X_0(N), \mathbb{Z}/p\mathbb{Z})\) corresponding to the covering \(X_1(N) \to X_0(N)\), and \(\cdot\) is the intersection pairing in homology. Merel was able to compute this pairing explicitly (cf. Sect. 1.5 for precise statements).

The main idea of this paper is to determine, in well-chosen Hecke modules, the so called higher Eisenstein elements, which have the property to be annihilated by a power of \(I\). Results such as Theorems 1.1 and 1.2 are by-products of our study of higher Eisenstein elements. Unfortunately we could only determine a few of them so that we do not have a general formula for \(g_p\).

Let \(\mathfrak{P} = I + (p)\), which is the unique maximal ideal of \(\mathbb{T}\) containing \(I\). We denote by \(\mathbb{T}_{\mathfrak{P}}\) the \(\mathfrak{P}\)-adic (or equivalently \(I\)-adic) completion of \(\mathbb{T}\).

**Definition 1.4** Let \(M\) be a \(\mathbb{T}\)-module such that \(M \otimes_{\mathbb{T}} \mathbb{T}_{\mathfrak{P}}\) is free of rank one over \(\mathbb{T}_{\mathfrak{P}}\). A system of higher Eisenstein elements in \(M/pM\) is a sequence \(e_0, e_1, \ldots, e_n\) satisfying the following properties.

(i) We have \(e_0 \neq 0\).

(ii) For all prime numbers \(\ell\) not dividing \(N\) and all integers \(i\) such that \(0 \leq i \leq n\), we have:

\[(T_\ell - \ell - 1)(e_i) = \frac{\ell - 1}{2} \cdot \log(\ell) \cdot e_{i-1} \pmod{\mathbb{Z} \cdot e_0 + \cdots + \mathbb{Z} \cdot e_{i-2}}\]

(with the convention \(e_{-1} = 0\)). In the case \(p = \ell = 2\) (which is excluded in this introduction but will be considered in the paper), the term \(\frac{\ell - 1}{2} \cdot \log(\ell)\) is replaced by \(\log(x)\) where \(2 = x^2 \pmod{N}\).

We will prove in Theorem 2.1 that a system of higher Eisenstein element exists in \(M/pM\) for any \(1 \leq n \leq g_p\), that \(e_0\) is unique up to scalar and that \(e_i\) is uniquely determined modulo \(e_0, \ldots, e_{i-1}\) once we have fixed a choice for \(e_0\). Furthermore, there is a lift \(\tilde{e}_0\) of \(e_0\) in \(M\), unique up to \(\mathbf{Z}^x_p\), which is annihilated by \(I\).

There is an analogous definition modulo \(p^r\), for any integer \(r\) such that \(1 \leq r \leq t\), which we avoid in this introduction. All the theorems below are valid modulo appropriate powers of \(p\). The reader should consider all statements modulo \(p\) as simplifications.

In this paper, we consider four different cases for the \(\mathbb{T}\)-module \(M\), namely the modular forms, the supersingular module, the odd modular symbols and the even modular symbols. We now describe our results in each of these cases.
1.1 Modular forms

Let \( M = M_2(\Gamma_0(N), \mathbb{Z}_p) \) be the \( \mathbb{T} \)-module of modular forms of weight 2 and level \( \Gamma_0(N) \) over \( \mathbb{Z}_p \). If \( f \in M \) and \( n \geq 0 \), we denote by \( a_n(f) \in \mathbb{Z}_p \) the \( n \)th coefficient of the \( q \)-expansion of \( f \) at the cusp \( \infty \).

By \([19, \text{Corollary II.16.3}]\) and \([11, \text{Theorem 0.5 and Proposition 1.9}]\), the \( \mathbb{T}_p \)-module \( M \otimes_{\mathbb{T}} \mathbb{T}_p \) is free of rank one. Thus, there exists a system of higher Eisenstein elements \( f_0, f_1, \ldots, f_{g_p} \) in \( M/pM \). We normalize \( f_0 \) so that it is the reduction modulo \( p \) of the (unique) Eisenstein series \( E_2 \) of \( M \), whose \( q \)-expansion at the cusp \( \infty \) is

\[
E_2(q) = \frac{N - 1}{24} + \sum_{n \geq 1} \left( \sum_{\substack{d | n \\gcd(d,N) = 1}} d \right) \cdot q^n.
\]

Note that \( a_0(f_0) \equiv 0 \) (modulo \( p \)), so that \( a_0(f_1) \) is well-defined.

We prove the following result (cf. Remarks 6.4 and 6.5), from which it is possible to deduce Theorems 1.1 and 1.2.

**Theorem 1.5**

(i) We have

\[
a_0(f_1) \equiv \frac{1}{6} \cdot \sum_{k=1}^{\frac{N-1}{2}} k \cdot \log(k) \pmod{p}.
\]

(ii) Assume that \( g_p \geq 2 \). We have

\[
a_0(f_2) = \frac{1}{12} \cdot \sum_{k=1}^{\frac{N-1}{2}} k \cdot \log(k)^2 \pmod{p}.
\]

The quantity \( \sum_{k=1}^{\frac{N-1}{2}} k \cdot \log(k) \) can thus be interpreted as the constant coefficient of an higher Eisenstein series, and also as a derivative of an \( L \)-function. Similarly, we can think of \( \sum_{k=1}^{\frac{N-1}{2}} k \cdot \log(k)^2 \) as the second derivative of an \( L \)-function. This point of view has been made precise in \([15]\), where these quantities are related to derived Stickelberger elements and to the class group of the cyclotomic field \( \mathbb{Q}(\zeta_p, \zeta_N) \), proving a kind of class number number formula. Here, \( \zeta_p \) and \( \zeta_N \) are respectively \( p \)th and \( N \)th primitive roots of unity.

One may ask what are the other coefficients of the \( q \)-expansion of \( f_1 \) and \( f_2 \) at the cusp \( \infty \). We will give the result for \( f_2 \) in another paper, but let us
mention that this uses the deformation techniques of Calegari–Emerton. Since $f_1$ is uniquely defined only modulo $f_0$ and that $a_1(f_0) = 1$, we can fix $f_1$ by assuming $a_1(f_1) = 0$. If $\ell \neq N$ is a prime, we have $(T_\ell - \ell - 1)(f_1) = (\frac{\ell - 1}{2} \cdot \log(\ell) \cdot f_0$, so we get

$$a_\ell(f_1) = \frac{\ell - 1}{2} \cdot \log(\ell) .$$

We now expose another approach to prove (1), which is one of the key ideas of this paper. It also leads to a direct proof of Theorem 1.5 (i), and thus of Theorem 1.1. Since it is not used formally in the rest of the paper, we only sketch the idea.

It is well-known (cf. [10, Theorem 4.6.2]) that for any non-trivial even Dirichlet character $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$, there exists two Eisenstein series $E_{1,\chi}$ and $E_{\chi,1}$ in $M_2(\Gamma_1(N))$ whose $q$-expansion at the cusp $\infty$ are

$$E_{1,\chi}(q) = \frac{L(-1, \chi)}{2} + \sum_{n \geq 1} \left( \sum_{d|n} \chi(d) \cdot d \right) \cdot q^n$$

and

$$E_{\chi,1}(q) = \sum_{n \geq 1} \left( \sum_{d|n} \chi(\frac{n}{d}) \cdot d \right) \cdot q^n .$$

It is also well-known (cf. [30, Theorem 4.2]) that

$$L(-1, \chi) = -\frac{N}{2} \cdot \sum_{k=1}^{N-1} \chi(k) \cdot B_2(\frac{k}{N})$$

where $B_2(X) = X^2 - X + \frac{1}{6}$ is the second Bernoulli polynomial.

There exists an eigenform $E_0 \in M_2(\Gamma_1(N), \mathbb{Z}_p[(\mathbb{Z}/N\mathbb{Z})^\times/ \pm 1])$ interpolating $E_{1,\chi}$ at any $\chi$ as above and interpolating $E_2$ at the trivial character. For any prime $\ell \neq N$, we have

$$T_\ell(E_0) = (\ell[\ell] + 1) \cdot E_0 .$$

Furthermore, we have

$$a_0(E_0) = -\frac{N}{4} \cdot \sum_{k=1}^{N-1} [k] \cdot B_2(\frac{k}{N}) .$$
Similarly, there exists an eigenform \( E_\infty \in M_2(\Gamma_1(N), \mathbb{Z}_p[(\mathbb{Z}/N\mathbb{Z})^\times / \pm 1]) \) interpolating \( E_{\chi,1} \) at any \( \chi \) as above and interpolating \( E_2 \) at the trivial character. For any prime \( \ell \neq N \), we have

\[
T_\ell(E_\infty) = (\ell + [\ell]) \cdot E_\infty.
\]

Furthermore, we have

\[
a_0(E_\infty) = \frac{1}{24} \cdot \left( \sum_{k=1}^{N-1} [k] \right).
\]

Let \( J \) be the kernel of the augmentation map \( \mathbb{Z}_p[(\mathbb{Z}/N\mathbb{Z})^\times / \pm 1] \to \mathbb{Z}_p \). We have a group homomorphism \( \varphi : J \to \mathbb{Z}/p\mathbb{Z} \) defined by \( \varphi([a] - 1) = \log(a) \). The modular form

\[
F = \frac{E_0 - E_\infty}{2}
\]

belongs to \( J \cdot M_2(\Gamma_1(N), \mathbb{Z}_p[(\mathbb{Z}/N\mathbb{Z})^\times / \pm 1]) \) and its image \( \overline{F} \) in \( M_2(\Gamma_1(N), \mathbb{Z}/p\mathbb{Z}) \) via \( \varphi \) is an element of \( M_2(\Gamma_0(N), \mathbb{Z}/p\mathbb{Z}) \).

By (2) and (4), for any prime \( \ell \neq N \) we have

\[
(T_\ell - \ell - 1)(\overline{F}) = \frac{\ell - 1}{2} \cdot \log(\ell) \cdot f_0.
\]

Since \( a_1(\overline{F}) = 0 \), we conclude that \( \overline{F} = f_1 \). This proves (1) since

\[
a_\ell(\overline{F}) = \frac{1}{2} \varphi(\ell[\ell] + 1 - [\ell] - \ell) = \frac{\ell - 1}{2} \cdot \log(\ell).
\]

By (3) and (5), we have in \( \mathbb{Z}/p\mathbb{Z} \):

\[
a_0(f_1) = -\frac{1}{8} \cdot \sum_{k=1}^{N-1} B_2\left(\frac{k}{N}\right) \cdot \log(k)
\]

\[
= -\frac{1}{8} \cdot \sum_{k=1}^{N-1} k^2 \cdot \log(k)
\]

\[
= \frac{1}{6} \cdot \sum_{k=1}^{N-1} k \cdot \log(k)
\]
where the first equality follows from \( \sum_{k=1}^{N-1} \log(k) = \sum_{k=1}^{N-1} k \cdot \log(k) \equiv 0 \pmod{p} \) and the second equality is proved in Lemma 5.11. This gives a proof of Theorem 1.5 (i) by manipulations of \( q \)-expansion of modular forms. However this approach does not seem to yield a proof of Theorem 1.5 (ii), which instead follows from an intersection pairing computation in modular symbols (cf. 1.5).

We have seen that the first higher Eisenstein element \( f_1 \) at level \( \Gamma_0(N) \) can be obtained from Eisenstein series of weight 2 and level \( \Gamma_1(N) \). This suggests that a similar phenomenon is true in other Hecke modules than the space of modular forms, i.e. that the first higher Eisenstein element can be obtained from \textit{Eisenstein elements} of level \( \Gamma_1(N) \). This is the key idea underlying our work on odd and even modular symbols. As for the supersingular module, while our methods may seem \textit{a priori} unrelated to the modular curve \( X_1(N) \), Akshay Venkatesh has communicated to us a different approach relying on the Igusa curve, which is the special fiber modulo \( N \) of a model of \( X_1(N) \) over \( \mathbb{Z} \).

1.2 The supersingular module

Consider the free \( \mathbb{Z}_p \)-module \( M := \mathbb{Z}_p[S] \) on the set \( S \) of isomorphism classes of supersingular elliptic curves over \( \overline{\mathbb{F}}_N \). As we recall in Sect. 3.1, it is well-known that \( M \) carries an action of \( T \) such that \( M \otimes_T \mathbb{T}_p \) is free of rank one over \( \mathbb{T}_p \). We can thus consider a system of higher Eisenstein elements \( e_0, e_1, \ldots, e_{g_p} \) in \( M/pM \).

The element \( e_0 \) (unique up to \((\mathbb{Z}/p\mathbb{Z})^\times\)) is well-known:

\[
e_0 = \sum_{E \in S} \frac{1}{w_E} \cdot [E] \in M/pM
\]

where \( w_E \in \{1, 2, 3\} \) is half the number of automorphism of \( E \).

We determine completely the element \( e_1 \) (which is unique modulo \((\mathbb{Z}/p\mathbb{Z}) \cdot e_0 \)). Let

\[
H(X) = \sum_{i=0}^{N-1} \left( \frac{N-1}{2} \right)^2 \cdot X^i \in \mathbb{F}_N[X]
\]

be the classical Hasse polynomial and

\[
P(X) = \text{Res}_T(H'(T), 256 \cdot (1 - T + T^2)^3 - T^2 \cdot (1 - T)^2 \cdot X) \in \mathbb{F}_N[X]
\]

where \( \text{Res}_X \) means the resultant relative to the variable \( X \). Since \( p > 2 \), we can extend uniquely log to a morphism \( \mathbb{F}_{N^2}^X \to \mathbb{Z}/p\mathbb{Z} \), still denoted by log.
If \( E \in S \), let \( j(E) \in \mathbb{F}_{N^2} \) be the \( j \)-invariant of \( E \) and \([E] \in \mathbb{Z}_p[S]\) be the element corresponding to \( E \).

The following result is a consequence of Theorem 3.16 (i).

**Theorem 1.6** We have, modulo \((\mathbb{Z}/p\mathbb{Z}) \cdot e_0\):

\[
e_1 = \frac{1}{12} \sum_{E \in S} \frac{1}{w_E} \cdot \log(P(j(E))) \cdot [E].
\]

There is a \( \mathbb{T} \)-equivariant bilinear pairing (cf. Sect. 3.1)

\[
\bullet : M \times M \rightarrow \mathbb{Z}_p
\]

such that \([E][E'] = 0\) if \( E \neq E' \) and \([E]\bullet[E] = w_E\). This induces a perfect pairing:

\[
\bullet : M/pM \times M/pM \rightarrow \mathbb{Z}/p\mathbb{Z}.
\]

Corollary 2.5 shows that \(e_i \bullet e_j\) only depends on \(i + j\) and that

\[
e_i \bullet e_j \equiv 0 \pmod{p} \iff g_p \geq i + j + 1.
\]

Thus, to determine \(g_p\) it is enough to compute \(e_i \bullet e_j\) modulo \(p\). We now state two results about this pairing.

The following result is a consequence of Theorem 3.16 (ii) and (iii).

**Theorem 1.7** (i) We have

\[
e_1 \bullet e_0 = \frac{1}{12} \sum_{\lambda \in L} \log(H'(\lambda)).
\]

(ii) We have

\[
e_2 \bullet e_0 = e_1 \bullet e_1 = \sum_{\lambda \in L} \frac{1}{24} \cdot \log(H'(\lambda))^2 - \frac{1}{18} \cdot \log(\lambda)^2
\]

where \(L \subset \mathbb{F}_{N^2}^\times\) is the set of roots of \(H\) (these are simple roots).

This gives us criteria to determine whether \(g_p \geq 2\) and \(g_p \geq 3\) respectively.

One can in fact compute directly in an elementary way the discriminant of \(H\) modulo \(N\) (cf. Theorem 3.3), which gives us in particular the following...
formula:

\[ e_1 \cdot e_0 = \frac{1}{3} \cdot \sum_{k=1}^{N-1} k \cdot \log(k). \]

This gives another proof of Theorem 1.1.

The quantity \( e_i \cdot e_0 \) is the degree of \( e_i \). For \( i = 0 \), Eichler mass formula (in characteristic 0) tells us that

\[ e_0 \cdot e_0 \equiv \frac{N - 1}{12} \equiv 0 \pmod{p}. \]

We thus feel justified to call our formulas for \( e_0 \cdot e_i \) “higher Eichler’s formulas”. We can only state them for \( i \in \{1, 2\} \) (cf. Theorem 1.13).

### 1.3 Odd modular symbols

Consider \( M^- = H_1(Y_0(N), \mathbb{Z}_p)^- \), the largest quotient of \( H_1(Y_0(N), \mathbb{Z}_p) \) on which the complex conjugation acts by multiplication by \(-1\), where \( Y_0(N) \) is the open modular curve. Let \( M^+ = H_1(X_0(N), \text{cusps}, \mathbb{Z}_p)^+ \), the fixed subspace by the complex conjugation of the homology (relative to the cusps) of the classical modular curve \( X_0(N) \). Similar notation apply to other (co-)homology groups with various coefficient rings, eg. \( H_1(X_0(N), \mathbb{Z}_p)^- \), \( H^1(X_0(N), \mathbb{Z}/p\mathbb{Z})^+ \), the point being that a subscript symbol refers to a subspace and a superscript symbol refers to a quotient.

We recall a few basic facts about \( M^+ \) and \( M^- \) (cf. Sect. 4.2). The \( \mathbb{T}_\mathbb{Q} \)-modules \( M^+ \otimes \mathbb{T}_\mathbb{Q} \) and \( M^- \otimes \mathbb{T}_\mathbb{Q} \) are free of rank one. We can thus consider a system of higher Eisenstein elements \( m_0^- \), \( m_1^- \), \ldots, \( m_g^- \) in \( M^-/pM^- \). In this paper, we shall only need an explicit description of \( m_0^- \) (easy) and \( m_1^- \) (essentially due to Mazur). We refer to [16, Theorem 1.7] for a \( K \)-theoretic description of \( m_2^- \).

There is a perfect \( \mathbb{T} \)-equivariant bilinear pairing, called the intersection pairing, \( M^+ \times M^- \rightarrow \mathbb{Z}_p \). We denote this pairing by \( \cdot \).

Let

\[ \xi_{\Gamma_0(N)} : \mathbb{Z}_p[\Gamma_0(N)\backslash \text{SL}_2(\mathbb{Z})] \rightarrow H_1(X_0(N), \text{cusps}, \mathbb{Z}_p) \]

be the usual Manin surjection, given by

\[ \xi_{\Gamma_0(N)}(\Gamma_0(N) \cdot g) = \{ g(0), g(\infty) \} \]
where, if $\alpha, \beta \in P^1(\mathbb{Q})$, we denote by $\{\alpha, \beta\}$ the cohomology class of the image of the geodesic path between $\alpha$ and $\beta$ in the modular curve $X_0(N)$ (via the complex upper-half plane parametrization). There is a natural identification $\Gamma_0(N) \setminus \text{SL}_2(\mathbb{Z}) \sim \text{SL}_2(\mathbb{Z}/N\mathbb{Z})$ given by
\[
\Gamma_0(N) \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto [c : d].
\]

The element $m_0^−$ is easy to describe as a generator of the kernel of the map $H_1(Y_0(N), \mathbb{Z}/p\mathbb{Z})^− \rightarrow H_1(X_0(N), \mathbb{Z}/p\mathbb{Z})^−$. Since $X_0(N)$ has two cusps, this kernel is isomorphic to $\mathbb{Z}/p\mathbb{Z}$. We normalize $m_0^−$ so that $\{0, \infty\} \cdot \tilde{m}_0^− = −1$.

Since $m_1^−$ is uniquely determined modulo $m_0^−$, the image of $m_1^−$ in $H_1(X_0(N), \mathbb{Z}/p\mathbb{Z})^−$ is canonical. By intersection duality, we may describe $m_1^−$ as an element in $\text{Hom}(H_1(X_0(N), \mathbb{Z}/p\mathbb{Z})_+, \mathbb{Z}/p\mathbb{Z})$, or equivalently as an element in the cohomology group $H^1(X_0(N), \mathbb{Z}/p\mathbb{Z})^+$. A general procedure due to Merel (cf. Remark 4.1), allows us to give a formula for $m_1^−$ in terms of Manin symbols in $H^1_1(X_0(N), \mathbb{Z}/p\mathbb{Z})^+$.

The following result, proved in Theorem 4.2, essentially follows from the work of Mazur [19, Proposition 18.8]. For notational simplicity, if $x \in (\mathbb{Z}/N\mathbb{Z})^\times$ we denote the element $(1 + c) \cdot \xi_{\Gamma_0(N)}([x : 1])$ of $H_1(X_0(N), \mathbb{Z}_p)_+$ by $\langle x : 1 \rangle$.

**Theorem 1.8** For any $x \in (\mathbb{Z}/N\mathbb{Z})^\times$, we have in $\mathbb{Z}/p\mathbb{Z}$:
\[
\langle x : 1 \rangle \cdot m_1^− = \log(x),
\]
where $c$ is the complex conjugation.

### 1.4 Even modular symbols

We denote by $m_i^+, i = 0, 1, \ldots, gp$ a system of higher Eisenstein elements in $M_+/pM_+$ (where $M_+ = H_1(X_0(N), \text{cusps, } \mathbb{Z}_p)_+$). We denote by $\hat{m}_0^+$ a lift of $m_0^+$ in $M_+$ which is annihilated by $I$.

Merel determined the element $\hat{m}_0^+$ in terms of Manin symbols. We recall his result below, using a slightly different formula.

We will need to use the Bernoulli polynomial functions. Recall that $\overline{B}_1 : \mathbb{R} \rightarrow \mathbb{R}$ is the function defined by $\overline{B}_1(x) = x - [x] - \frac{1}{2}$ if $x \notin \mathbb{Z}$ and $\overline{B}_1(x) = 0$ if $x \in \mathbb{Z}$.
Consider the boundary map \( \partial : H_1(X_0(N), \text{cusps}, \mathbb{Z}_p) \to \mathbb{Z}_p[\text{cusps}]^0 \) given by \( \partial(\{\alpha, \beta\}) = (\Gamma_0(N) \cdot \beta - (\Gamma_0(N) \cdot \alpha). \)

**Theorem 1.9** (Merel) Let \( F_{0,p} : \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z}) \to \mathbb{Z}_p \) be such that if \( x = [c : d] \in \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z}) \), we have:

\[
6 \cdot F_{0,p}(x) = \sum_{(s_1,s_2) \in (\mathbb{Z}/2N\mathbb{Z})^2, \,(d-c)s_1 + (d+c)s_2 \equiv 0 \text{ (modulo N)}} (-1)^{s_1+s_2} \mathbb{B}_1 \left( \frac{s_1}{2N} \right) \mathbb{B}_1 \left( \frac{s_2}{2N} \right).
\]

This is independent of the choice of \( c \) and \( d \) such that \( x = [c : d] \). We have

\[
\tilde{m}_0^+ = \sum_{x \in \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})} F_{0,p}(x) \cdot \xi_{\Gamma_0(N)}(x) \in M_+.
\]

Furthermore, one has \( \partial \tilde{m}_0^+ = \frac{N-1}{12} \cdot \left( (\Gamma_0(N) \cdot 0) - (\Gamma_0(N) \cdot \infty) \right) \), i.e. \( \tilde{m}_0^+ \cdot \tilde{m}_0^- = \frac{N-1}{12} \).

We warn the reader that \( \tilde{m}_0^+ \) is \( \frac{1}{12} \cdot \mathcal{E} \) where \( \mathcal{E} \) is computed in [23, Corollaire 4].

Our main result about \( M_+ \) is a formula for \( m_1^+ \) (cf. Theorem 5.10).

**Theorem 1.10** Let \( F_{1,p} : \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z}) \to \mathbb{Z}/p\mathbb{Z} \) be such that

\[
12 \cdot F_{1,p}([c : d]) = \sum_{(s_1,s_2) \in (\mathbb{Z}/2N\mathbb{Z})^2, \,(d-c)s_1 + (d+c)s_2 \equiv 0 \text{ (modulo N)}} (-1)^{s_1+s_2} \mathbb{B}_1 \left( \frac{s_1}{2N} \right) \mathbb{B}_1 \left( \frac{s_2}{2N} \right) \cdot \log \left( \frac{s_2}{d-c} \right)
- \sum_{(s_1,s_2) \in (\mathbb{Z}/2N\mathbb{Z})^2, \,(d-c)s_1 + (d+c)s_2 \equiv 0 \text{ (modulo N)}} (-1)^{s_1+s_2} \mathbb{B}_1 \left( \frac{s_1}{2N} \right) \mathbb{B}_1 \left( \frac{s_2}{2N} \right) \cdot \log((d-c)s_1 + (d+c)s_2))
\]

if \([c : d] \neq [1 : 1]\) and \( F_{1,p}([1 : 1]) = 0. \)

We have the following equality in \( M_+ / pM_+ \) modulo \( \mathbb{Z}/p\mathbb{Z} \) \( m_1^+ \):

\[
m_1^+ = \sum_{x \in \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})} F_{1,p}(x) \cdot \xi_{\Gamma_0(N)}(x) .
\]
Furthermore, one has $\partial m_1^+ = \left(\frac{1}{3} \sum_{k=1}^{N-1} k \cdot \log(k)\right) \cdot ((\Gamma_0(N) \cdot 0) - (\Gamma_0(N) \cdot \infty))$, i.e.

$$m_1^+ \cdot m_0^- = \frac{1}{3} \sum_{k=1}^{N-1} k \cdot \log(k).$$

The last assertion gives another proof of Theorem 1.1. The proof of Theorem 1.10 follows the strategy outlined at the end of Sect. 1.1, i.e. we compute $m_1^+$ by relating it to Eisenstein elements in $H_1(X_1(N), \text{cusps}, \mathbb{Z}/p\mathbb{Z})^+$. These elements can be computed easily using the recent work of Banerjee–Merel [2].

1.5 Comparison

We have the following result relating the four Hecke modules (cf. Corollary 6.3).

**Theorem 1.11** Let $i$ and $j$ be integers such that $0 \leq i, j \leq g_p$ and $i + j \leq g_p$. We have:

$$m_i^+ \cdot m_j^- = e_i \cdot e_j = 2 \cdot a_0(f_{i+j}).$$

Furthermore, this quantity is $0$ if $i + j < g_p$ and it is non-zero if $i + j = g_p$.

Combining our results in the spaces of even and odd modular symbols, a computation gives us the following formulas (cf. Theorems 6.4 and 6.7).

**Theorem 1.12** (i) We have $m_0^+ \cdot m_1^- = m_1^+ \cdot m_0^- = \frac{1}{3} \cdot \sum_{k=1}^{N-1} k \cdot \log(k)$.

(ii) We have $m_1^+ \cdot m_2^- = m_2^+ \cdot m_0^- = m_0^+ \cdot m_2^- = \frac{1}{6} \cdot \sum_{k=1}^{N-1} k \cdot \log(k)^2$.

This proves Theorems 1.2 and 1.5. Note that all equalities but the last of each line follows formally from algebraic properties of pairing of Hecke modules.

In particular, the boundary of $m_2^+$ is $\left(\frac{1}{6} \cdot \sum_{k=1}^{N-1} k \cdot \log(k)^2\right) \cdot ((\Gamma_0(N) \cdot 0) - (\Gamma_0(N) \cdot \infty))$. However, we do not know an expression for $m_2^+$ in terms of Manin symbols similar to Theorems 1.9 and 1.10. It is unclear to us whether such an expression is to be expected as a quadratic expression of logarithms or as a formula in some algebraic number theoretic group such as the cyclotomic $\mathcal{K}$-group of [16].

The combination of Theorems 1.7, 1.12 and 1.11 allows us to deduce the following identity (cf. Corollary 6.8). We were not able to find an elementary proof of it.
Theorem 1.13 Assume that $\sum_{k=1}^{N-1} k \cdot \log(k) \equiv 0 \pmod{p}$. We then have

$$\sum_{\lambda \in L} \frac{1}{4} \cdot \log(H'(\lambda))^2 - \frac{1}{3} \cdot \log(\lambda)^2 \equiv \sum_{k=1}^{N-1} k \cdot \log(k)^2 \pmod{p}.\]$$

This is the most advanced instance (known to us) of what we call an higher Eichler mass formula. We do not know how to connect the algebraic objects of Sect. 1.3 with supersingular $j$ (or $\lambda$) invariants.

Obviously, there is a theory of higher Eisenstein elements for all levels and all weights. We finish this introduction by giving some reasons as to why we focus on the prime level and weight 2 cases.

(i) Mazur’s original question about the rank $g_p$ was in this setting.
(ii) It is known that in this case, the Hecke algebra has nice properties. For example it is a Gorenstein ring at the Eisenstein maximal ideals, and the Eisenstein ideal $I$ is locally principal, i.e. $I/I^2$ is cyclic.
(iii) We know, thanks to Mazur, some multiplicity one results for the homology of $X_0(N)$.
(iv) There is an explicit and simple description of $m_1^-$ coming from the Shimura covering $X_1(N) \to X_0(N)$. Mazur deduced from this a description of $I/I^2$ in terms of modular symbols.
(v) In this case, the supersingular module presents itself. Our methods in turn has applications to supersingular elliptic curves.

It is not clear to us in which settings we can obtain similar results. Mazur’s question makes sense in any weight and level (although there are possibly several maximal Eisenstein ideals). However, we do not know multiplicity one in general, and Eisenstein ideals are not locally principal in general neither. See the list of alternative settings already proposed by Mazur in [19, p. 39].

2 The formalism of higher Eisenstein elements

2.1 Algebraic setting

In this section, we develop the theory of higher Eisenstein elements in a tentative axiomatic setting. Let $\mathbb{T}$ be a $\mathbb{Z}_p$-algebra which is free of finite rank as a $\mathbb{Z}_p$-module. Let $I$ be an ideal of $\mathbb{T}$. We assume the following hypotheses.

(i) We have $\mathbb{T}/I \cong \mathbb{Z}_p$.
(ii) The group $I/I^2$ is cyclic of order $p^t$ for some integer $t \geq 1$. We fix a group isomorphism $e : I/I^2 \cong \mathbb{Z}/p^t\mathbb{Z}$. If $\eta \in I$, we denote by $e(\eta)$ the image by $e$ of the class of $\eta$ in $I/I^2$. 

\[ \text{Springer} \]
If \( m \in \text{Specmax}(\mathbb{T}) \) is a maximal ideal of \( \mathbb{T} \), we denote by \( \mathbb{T}_m \) the \( m \)-adic completion of \( \mathbb{T} \), and if \( M \) is a \( \mathbb{T} \)-module we let \( M_m = M \otimes_{\mathbb{T}} \mathbb{T}_m \). By hypothesis (i), the ideal \( \mathfrak{P} = I + (p) \) is maximal.

**Theorem 2.1** (Construction of higher Eisenstein elements) Let \( M \) be a \( \mathbb{T} \)-module such that \( M_{\mathfrak{P}} \) is free of rank one over \( \mathbb{T}_{\mathfrak{P}} \). Let \( r \) be an integer such that \( 1 \leq r \leq t \). We let \( \mathbb{T}_m = \mathbb{T} \otimes_{\mathbb{T}} \mathbb{T}_m \). By hypothesis (i), the ideal \( \mathbb{P} = I + (p) \) is maximal.

There exists a maximal positive integer \( n(r) \) and a sequence of elements \( e_0, e_1, \ldots, e_{n(r)} \) in \( \mathbb{M} \), called a system of higher Eisenstein elements of \( M \), such that the following properties hold.

(i) We have \( e_0 \notin p \cdot \mathbb{M} \)

(ii) For all \( \eta \in I \), we have

\[
\eta(e_i) \equiv e(\eta) \cdot e_{i-1} \mod (\mathbb{Z} \cdot e_0 + \cdots + \mathbb{Z} \cdot e_{i-2})
\]

(with the convention \( e_{-1} = 0 \)).

We have the following properties.

a) The element \( e_0 \) is unique up to \( (\mathbb{Z}/p^r \mathbb{Z})^x \). There exists \( \tilde{e}_0 \in M[I] \), unique up to \( \mathbb{Z}_p^x \), whose class in \( \mathbb{M} \) is \( e_0 \).

b) If we fix \( e_0 \) in \( \mathbb{M}[I] \), then for every integer \( i \) such that \( 1 \leq i \leq n(r) \) the image of \( e_i \) in \( \mathbb{M}/(\mathbb{Z} \cdot e_0 + \cdots + \mathbb{Z} \cdot e_{i-2}) \) is uniquely determined.

c) The integer \( n(r) \) is the largest integer \( n \geq 1 \) such that the group \( I^n \cdot \mathbb{T}/I^{n+1} \cdot \mathbb{T} \) is cyclic of order \( p^r \). Furthermore, we have \( n(r) \leq \text{rk}_{\mathbb{Z}_p}(\mathbb{T}_\mathfrak{P}) - 1 \) with equality if \( r = 1 \). In particular, the integer \( n(r) \) only depends on \( \mathbb{T} \) and \( r \), and not on the choice of \( M \).

**Remark 2.1** A typical example of situation where Theorem 2.1 applies is the following. We consider \( M = \mathbb{T} = \mathbb{Z}_p[X]/(X^4 + pX^3 + p^2X^2 + p^3X) \) and \( I = (X) \). In this case, we have \( t = 3 \) and \( (n(1), n(2), n(3)) = (3, 2, 1) \). We normalize the isomorphism \( e : I/I^2 \sim \mathbb{Z}/p^3 \mathbb{Z} \) by \( e(X) = 1 \). A system of higher Eisenstein elements is given in Table 1.

**Proof.**

**Lemma 2.2** We have a canonical isomorphism of \( \mathbb{Z}_p \)-algebras

\[
\mathbb{T} \sim \bigoplus_{m \in \text{Specmax}(\mathbb{T})} \mathbb{T}_m .
\]

**Proof** The ring \( \mathbb{T} \) has finitely many maximal ideals, i.e. is a semi-local ring since it is a finitely generated \( \mathbb{Z}_p \)-module. The ring \( \mathbb{T} \) is \( p \)-adically complete and semi-local, so is the direct sum of its completions at its maximal ideals [6, Chap. III, §2, no. 12].

\( \Box \)
By Lemma 2.2, we have

\[ M = \bigoplus_{m \in \text{Spec}_{\max}(T)} M_m. \] (7)

By hypothesis (i), \( \mathcal{P} \) is the unique maximal ideal of \( T \) containing \( I \). By (7) and the fact that \( M_{\mathcal{P}} \cong T_{\mathcal{P}} \), we get

\[ M[I] \cong T_{\mathcal{P}}[I] \] (8)

and

\[ \overline{M}[I^n] \cong T_{\mathcal{P}}[I^n] \] (9)

for any integer \( n \geq 1 \).

**Lemma 2.3** The ring \( T_{\mathcal{P}} \) is Gorenstein, i.e. the \( T_{\mathcal{P}} \)-module \( \text{Hom}_{\mathbb{Z}_p}(T_{\mathcal{P}}, \mathbb{Z}_p) \) is free of rank one.

**Proof** It follows from hypothesis (ii) that the ideal \( I \cdot T_{\mathcal{P}} \) is principal. If \( \eta \) is a generator of \( I \cdot T_{\mathcal{P}} \), then we have \( T_{\mathcal{P}} = \mathbb{Z}_p[\eta] \) since \( T_{\mathcal{P}} \) is \( I \)-adically complete and is a finitely generated \( \mathbb{Z}_p \)-module. Since \( T \) is a free \( \mathbb{Z}_p \)-module of finite rank, we can apply the criterion of [19, Proposition II.15.3] and conclude that \( T_{\mathcal{P}} \) is Gorenstein. \( \square \)

By Lemma 2.3, we get group isomorphisms

\[ T_{\mathcal{P}}[I] \cong \text{Hom}_{\mathbb{Z}_p}(T_{\mathcal{P}} / I \cdot T_{\mathcal{P}}, \mathbb{Z}_p) \cong \mathbb{Z}_p \] (10)

(where we have used hypothesis (i) in the last isomorphism) and

\[ \overline{T}_{\mathcal{P}}[I^n] \cong \text{Hom}(\overline{T}_{\mathcal{P}} / I^n \cdot \overline{T}_{\mathcal{P}}, \mathbb{Z}/p^r\mathbb{Z}). \] (11)

for any integer \( n \geq 0 \). By (8), (9), (10) and (11) with \( n = 1 \), we conclude the existence of \( e_0 \) and \( \tilde{e}_0 \) satisfying the properties of Theorem 2.1.

By (9) and (11), we get a group isomorphism

\[ \overline{M}[I^{n+1}] / \overline{M}[I^n] \cong \text{Hom}(I^n \cdot \overline{T}_{\mathcal{P}} / I^{n+1} \cdot \overline{T}_{\mathcal{P}}, \mathbb{Z}/p^r\mathbb{Z}). \] (12)

Since the ideal \( I \cdot T_{\mathcal{P}} \) is principal and \( \overline{T}_{\mathcal{P}} / I \cdot \overline{T}_{\mathcal{P}} = \mathbb{Z}/p^r\mathbb{Z} \) by hypothesis (i), the group \( I^n \cdot \overline{T}_{\mathcal{P}} / I^{n+1} \cdot \overline{T}_{\mathcal{P}} \) is cyclic of order dividing \( p^r \). By (12), the group \( \overline{M}[I^{n+1}] / \overline{M}[I^n] \) is cyclic of order dividing \( p^r \), with equality if and only if \( I^n \cdot \overline{T} / I^{n+1} \cdot \overline{T} \) is cyclic of order dividing \( p^r \). This proves the existence of a system of higher Eisenstein elements \( e_0, e_1, \ldots, e_{n(r)} \) satisfying the properties...
of Theorem 2.1, where \( n(r) \geq 0 \) is the largest integer \( n \geq 0 \) such that the group \( I^n \cdot \mathbb{T}/I^{n+1} \cdot \mathbb{T} \) is cyclic of order \( p^r \).

The map \( r \mapsto n(r) \) is obviously a decreasing function of \( r \). Thus, to conclude the proof of property \( d) \), we only need to prove that \( \text{rk}_{\mathbb{Z}_p}(\mathbb{T}_\mathfrak{P}) \geq 2 \) and that 
\[
\text{rk}_{\mathbb{Z}_p}(\mathbb{T}_\mathfrak{P}) = 1 \text{ then } \mathbb{T}_\mathfrak{P} = \mathbb{Z}_p \text{ and } I \cdot \mathbb{T}_\mathfrak{P} = 0,
\]
contradicting hypothesis \( \text{ (ii)} \). This proves \( \text{rk}_{\mathbb{Z}_p}(\mathbb{T}_\mathfrak{P}) \geq 2 \).

There is a surjective homomorphisms of \( \mathbb{Z}_p \)-algebras \( \mathbb{Z}_p[X] \to \mathbb{T}_\mathfrak{P} \) sending \( X \) to a generator \( \eta \) of \( I \cdot \mathbb{T}_\mathfrak{P} \). Its kernel does not contain any power of \( p \) since \( \mathbb{T}_\mathfrak{P}/I \cdot \mathbb{T}_\mathfrak{P} = \mathbb{Z}_p \), so this kernel equals \( (R(X)) \) for some \( R(X) \in \mathbb{Z}_p[X] \). We thus get an isomorphism of \( \mathbb{Z}_p \)-algebras

\[
\mathbb{T}_\mathfrak{P} \cong \mathbb{Z}_p[X]/(R(X)).
\]

By hypothesis \( (i) \), we have \( R(0) = 0 \). Since \( \mathbb{T}_\mathfrak{P} \) is a local ring, we have \( R(X) \equiv X^{\text{rk}_{\mathbb{Z}_p}(\mathbb{T}_\mathfrak{P})} \) (modulo \( p \)). Under the isomorphism \( \mathbb{T}_\mathfrak{P}/p \mathbb{T}_\mathfrak{P} \cong \mathbb{F}_p[X]/(X^{\text{rk}_{\mathbb{Z}_p}(\mathbb{T}_\mathfrak{P})}) \), the ideal \( I \cdot \mathbb{T}_\mathfrak{P}/p \mathbb{T}_\mathfrak{P} \) maps to \( (X) \). The fact that \( n(1) = \text{rk}_{\mathbb{Z}_p}(\mathbb{T}_\mathfrak{P}) - 1 \) then follows from the fact that the largest \( n \geq 1 \) such that 
\[
(X^n)/(X^{n+1}) \text{ is not zero in } \mathbb{F}_p[X]/(X^{\text{rk}_{\mathbb{Z}_p}(\mathbb{T}_\mathfrak{P})}) \text{ is } n = \text{rk}_{\mathbb{Z}_p}(\mathbb{T}_\mathfrak{P}) - 1.
\]
This concludes the proof of Theorem 2.1.

\[\Box\]

2.2 The Newton polygon of \( \mathbb{T}_\mathfrak{P} \)

This paragraph is not used in the rest of this paper, but we include it because Mazur asked more generally what can be said about the Newton polygon of \( \mathbb{T}_\mathfrak{P} \) [19, p. 140].

As in (13), there is a (non-canonical) isomorphism of \( \mathbb{Z}_p \)-algebras

\[
\mathbb{T}_\mathfrak{P} \cong \mathbb{Z}_p[X]/(R(X))
\]

for some monic polynomial \( R = \sum_{i=0}^{\text{rk}_{\mathbb{Z}_p}(\mathbb{T}_\mathfrak{P})} a_i \cdot X^i \in \mathbb{Z}_p[X] \). Recall that the Newton polygon of \( R \) is the lower convex hull of the points \( \{(i, v_p(a_i)), \; i \in \{0, \ldots, \text{rk}_{\mathbb{Z}_p}(\mathbb{T}_\mathfrak{P})\}\} \) (where \( v_p \) is the usual \( p \)-adic valuation and we omit the points with \( a_i = 0 \)). The Newton polygon of \( R \) only depends on \( \mathbb{T}_\mathfrak{P} \). The Newton polygon of \( \mathbb{T}_\mathfrak{P} \) is by definition the Newton polygon of \( R \), and we denote it by \( \text{NP}(\mathbb{T}_\mathfrak{P}) \).

We now recall a finer invariant of \( \mathbb{T}_\mathfrak{P} \) than \( \text{NP}(\mathbb{T}_\mathfrak{P}) \), introduced in by Wake–Wang-Erickson in [29, Section 8]. By convention, we let \( v_p(0) = \infty \). Define a sequence \( z_0, \ldots, z_{\text{rk}_{\mathbb{Z}_p}(\mathbb{T}_\mathfrak{P})} \) inductively by \( z_0 = v_p(a_0) \) and 
\[
z_i = \min(z_{i-1}, v_p(a_i)) \text{ (by convention, } \min(z, \infty) = z \text{ for any } z \in \mathbb{Z} \cup \{\infty\} \text{)}. One easily sees that \( \text{NP}(\mathbb{T}_\mathfrak{P}) \) is the lower convex hull of the points \( \{(i, z_i), \; i \in \{0, \ldots, \text{rk}_{\mathbb{Z}_p}(\mathbb{T}_\mathfrak{P})\}\} \) (we omit the points with \( z_i = \infty \)). Let

\[\because\] Springer
$i \in \{0, \ldots, \text{rk}_{\mathbb{Z}_p}(\mathbb{T}_q)\}$. Then $z_i$ is the supremum of the set of integers $r \geq 1$ such that there exists a surjective ring homomorphism

$$f : \mathbb{Z}_p[X]/(R(X)) \rightarrow (\mathbb{Z}/p^r\mathbb{Z})[x]/(x^{i+1})$$

such that $f(X) = x$ (this supremum can be $\infty$) [29, Lemma 8.1.2]. We choose $R$ so that $X$ corresponds to a generator of $I \cdot \mathbb{T}_q$ via (13). By Hypothesis (i) we have $a_0 = 0$. By hypothesis (ii) we have $v_p(a_1) = t$. Thus, we have $z_0 = \infty$ and $z_i \leq t$ for all $i \geq 1$.

By Theorem 2.1 c), one easily sees that for all integer $r$ such that $1 \leq r \leq t$, the integer $n(r)$ is the largest integer $i \geq 1$ such that there exists a surjective ring homomorphism

$$f' : \mathbb{Z}_p[X]/(R(X)) \rightarrow (\mathbb{Z}/p^r\mathbb{Z})[x]/(x^{i+1})$$

such that $f'(X) = x$. Thus, for all $r \in \{1, \ldots, t\}$ and $i \in \{1, \ldots, \text{rk}_{\mathbb{Z}_p}(\mathbb{T}_q)\}$, we have:

$$n(r) = \max\{j \in \{1, \ldots, \text{rk}_{\mathbb{Z}_p}(\mathbb{T}_q)\}, z_j \geq r\}$$

and

$$z_i = \max\{r' \in \{1, \ldots, t\}, n(r') \geq i\}.$$

Hence, knowing the sequence $(n(r))_{1 \leq r \leq t}$ amounts to knowing the sequence $(z_i)_{0 \leq i \leq \text{rk}_{\mathbb{Z}_p}(\mathbb{T}_q)}$. Thus, the sequence $(n(r))_{1 \leq r \leq t}$ is a finer invariant of $\mathbb{T}_q$ than NP$(\mathbb{T}_q)$ (cf. [29, 8.1.3] for an example where the Newton polygon does not determine the $(z_i)_{0 \leq i \leq \text{rk}_{\mathbb{Z}_p}(\mathbb{T}_q)}$).

### 2.3 Pairing between higher Eisenstein elements

The proof of the following is easy and left to the reader.

**Proposition 2.4** Let $M$ and $M'$ be two $\mathbb{T}$-modules satisfying the assumptions of Theorem 2.1. Let $1 \leq r \leq t$ be an integer. Let $e_0, \ldots, e_{n(r)}$ (resp. $e'_0, \ldots, e'_{n(r)}$) be the elements of $\overline{M}$ (resp. $\overline{M'}$) constructed in Theorem 2.1. Let

$$\bullet : M \times M' \rightarrow \mathbb{Z}/p^r\mathbb{Z}$$

be a perfect $\mathbb{T}$-equivariant bilinear pairing. Let $i \in \{0, \ldots, n(r)\}$. Then an element $m$ (resp. $m'$) of $I^i \cdot \overline{M}$ (resp. $I^i \cdot \overline{M'}$) is in $I^{i+1} \cdot \overline{M}$ (resp. $I^{i+1} \cdot \overline{M'}$) if and only if $m \bullet e'_i \equiv 0$ (modulo $p^r$) (resp. $e_i \bullet m' \equiv 0$ (modulo $p^r$)).
Corollary 2.5 Keep the notation of Proposition 2.4. The product $e_i \cdot e_j'$ only depends on $i + j$, is zero modulo $p^r$ if $i + j < n(r)$ and non-zero modulo $p^r$ if $i + j = n(r)$. (Note that if $i + j > n(r)$, the product is not well-defined since $e_i$ is only defined modulo $e_0, \ldots, e_{i-1}$ and the same for $e_j'$).

In particular, we have $n(r) \geq 2$ if and only if $e_1 \cdot e_0' \equiv 0 \pmod{p^r}$, and $n(r) \geq 3$ if and only if $e_1 \cdot e_0' \equiv e_1 \cdot e_1' \equiv 0 \pmod{p^r}$.

2.4 The special case of weight 2 and prime level

In this section, as well as in the rest of the article, let $T$ be the the Hecke algebra with $\mathbb{Z}_p$ coefficients acting faithfully on the space of modular forms of weight $2$ and level $\Gamma_0(N)$. The ideal $I$ is the Eisenstein ideal, generated by the Hecke operators $T_\ell - \ell - 1$ if $\ell \not= N$ and by $U_N - 1$. As in the introduction, let $T^0$ be the cuspidal quotient of $T$, $I^0$ be the image of $I$ in $T^0$ and $t \geq 1$ be the $p$-adic valuation of $\frac{N-1}{12}$.

We now check the hypotheses of Sect. 2. Hypothesis (i) is obvious. By [19, Proposition 18.9], there is a group isomorphism $e : I^0/(I^0)^2 \xrightarrow{\sim} \mathbb{Z}/p^t\mathbb{Z}$ such that for all prime $\ell$ not dividing $N$, we have:

$$e(T_\ell - \ell - 1) = \frac{\ell - 1}{2} \cdot \log(\ell)$$

where, if $p = \ell = 2$, this equality means

$$e(T_2 - 3) = \log(x)$$

where $x^2 \equiv 2 \pmod{N}$. Hypothesis (ii) thus follows from the following result.

Proposition 2.6 The map $I/I^2 \rightarrow I^0/(I^0)^2$ is a group isomorphism.

Proof We have a surjective group homomorphism $I/I^2 \rightarrow I^0/(I^0)^2 \simeq \mathbb{Z}/p^t\mathbb{Z}$. It remains to show that the kernel $K$ of this homomorphism is trivial.

By [11, Proposition 1.8], we have

$$\text{Ker}(T \rightarrow T^0) = \mathbb{Z}_p \cdot T_0$$

for some $T_0 \in T$ such that $T_0 - \frac{N-1}{v} \in I$ where $v = \gcd(N - 1, 12)$. Since $T/I = \mathbb{Z}_p$, we have $I \cap \mathbb{Z}_p T_0 = 0$. This concludes the proof of Proposition 2.6 since the group $K$ is the image of $I \cap \mathbb{Z}_p T_0$ in $I/I^2$. 

Using Proposition 2.6, we view $e$ as a group isomorphism $e : I/I^2 \xrightarrow{\sim} \mathbb{Z}/p^t\mathbb{Z}$. 

\[\square\] Springer
Remark 2.2 In order to study $g_p$, only higher Eisenstein elements modulo $p$ (and not modulo $p^r$ for $r > 1$) are important.

In practice, when we construct the elements $e_i$, we need only to check condition (ii) of Theorem 2.1 for Hecke operators $T_\ell - \ell - 1$ for primes $\ell$ outside a finite set.

**Proposition 2.7** We keep the notation of Theorem 2.1. Let $S$ be a finite set of rational primes containing $N$. Let $i$ be an integer such that $1 \leq i \leq n(r)$ and $m \in M / p^r M$ be such that for all $\ell \notin S$ prime, we have:

\[
(T_\ell - \ell - 1)(m) = \frac{\ell - 1}{2} \cdot \log(\ell) \cdot e_{i-1} \quad \text{(modulo the subgroup generated by $e_0, \ldots, e_{i-2}$)}.
\]

Then we have

\[
m \equiv e_i \quad \text{(modulo the subgroup generated by $e_0, \ldots, e_{i-1}$)}.
\]

**Proof** Let $m' = m - e_i \in M / p^r M$. There exists $\lambda \in (\mathbb{Z} / p^r \mathbb{Z})^\times$ and $j \in \{0, \ldots, i - 1\}$ such that for all $\ell \notin S$ we have

\[
(T_\ell - \ell - 1)(\lambda \cdot m') = \frac{\ell - 1}{2} \cdot \log(\ell) \cdot e_{j-1} \quad \text{(modulo the subgroup generated by $e_0, \ldots, e_{j-2}$)}.
\]

Thus, Proposition 2.7 follows by induction using the following result.

**Lemma 2.8** Let $W \subset M / p^r M$ be set of elements annihilated by $T_\ell - \ell - 1$ for $\ell$ prime not in $S$. Then $W = (\mathbb{Z} / p^r \mathbb{Z}) \cdot e_0$.

**Proof** We prove it by induction on $r$. Let $T$ be the $\mathbb{Z}_p$-subalgebra of $\mathbb{T}$ generated by the operators $T_\ell$ for $\ell \notin S$.

Assume first that $r = 1$. Let $w \in W$. By the Deligne–Serre lifting lemma [9, Lemme 6.11], there is a finite extension $\mathcal{O} \subset \overline{\mathbb{Q}}_p$ of $\mathbb{Z}_p$ ($\mathcal{O}$ is a discrete valuation ring) and an element $\tilde{w} \in M \otimes_{\mathbb{Z}_p} \mathcal{O}$ which is an eigenvector for the action of $T$ and such that the eigenvalue of $\tilde{w}$ for $T_\ell$ modulo $\pi$ (an uniformizer of $\mathcal{O}$) is the eigenvalue of $w$ for $T_\ell$ if $\ell \notin S$.

The strong multiplicity one theorem shows that $T \otimes_{\mathbb{Z}_p} \overline{\mathbb{Q}}_p = \mathbb{T} \otimes_{\mathbb{Z}_p} \overline{\mathbb{Q}}_p$. Thus, there is a ring homomorphism

\[
\varphi : \mathbb{T} \rightarrow \overline{\mathbb{Q}}_p
\]

such that for all $t \in T$, $\varphi(t)$ is the eigenvalue of $t$ on $\tilde{w}$. The morphism $\varphi$ takes values in $\overline{\mathbb{Z}}_p$ so we conclude that $w$ is an eigenvector for any $T \in \mathbb{T}$ with eigenvalue the reduction modulo $p$ of $\varphi(T)$.
There is a semi-simple Galois representation \( \rho_{\varphi} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{GL}_2(\overline{\mathbb{Q}}_p) \) attached to \( \varphi \). The associated semi-simple residual representation must be the direct sum of the trivial character and the Teichmüller character. One easily concludes that, in fact, \( w \) is annihilated by \( U_N - 1 \) and by \( T_\ell - \ell - 1 \) for all prime \( \ell \) not dividing \( N \). Thus the elements \( w \) and \( e_0 \) are proportional modulo \( p \), which concludes the case \( r = 1 \).

Now, let \( r \geq 1 \) be any integer. By the case \( r = 1 \), there exists \( \lambda \in \mathbb{Z} \) such that

\[
w - \lambda \cdot e_0 \in p \cdot M/p^r M.
\]

The element

\[
\frac{w - \lambda \cdot e_0}{p} \in M/p^{r-1} M
\]

is annihilated by \( T_\ell - \ell - 1 \) for all \( \ell \notin S \). By induction this concludes the proof of Lemma 2.8. \( \square \)

3 The supersingular module

We keep the notation of Sects. 1 and 2. In particular, \( p \geq 2 \) is a prime such that \( p^t \) divides exactly the numerator of \( \frac{N-1}{12} \). Let \( r \) be an integer such that \( 1 \leq r \leq t \).

3.1 Preliminary results and notation

Let \( S \) be the set of isomorphism classes of supersingular elliptic curves over \( \overline{\mathbb{F}}_N \), and \( M := \mathbb{Z}_p[S] \) be the free \( \mathbb{Z}_p \)-module with basis the elements of \( S \). If \( E \in S \), we denote by \( [E] \) the corresponding element in \( M \) and we let \( w_E = \frac{\text{Card}(\text{Aut}(E))}{2} \in \{1, 2, 3\} \). The ring \( \mathbb{T} \) acts on \( M \) in the following way. If \( n \geq 1 \), we have

\[
T_n([E]) = \sum C [E/C]
\]

where \( C \) goes through the cyclic subgroup schemes of order \( n \) in \( E \). If \( n \) and \( N \) are coprimes, these subgroup schemes correspond to the subgroups of \( E(\overline{\mathbb{F}}_N) \) isomorphic to \( \mathbb{Z}/n\mathbb{Z} \). We also have

\[
U_N([E]) = [E^{(N)}]
\]
where $U_N$ is the $N$th Hecke operator and $E^{(N)}$ is the Frobenius transform of $E$.

**Theorem 3.1** [11, Theorem 0.5] The $\mathbb{T}_\mathbb{Q}$-module $M \otimes_{\mathbb{T}} \mathbb{T}_\mathbb{Q}$ is free of rank one.

Thus, we can apply Theorem 2.1 to $M$. There is a $\mathbb{T}$-equivariant bilinear pairing

$$\cdot : M \times M \to \mathbb{Z}_p$$

given by $[E] \cdot [E'] = 0$ if $[E] \neq [E']$ and $[E] \cdot [E] = w_E$.

We let

$$\tilde{e}_0 = \sum_{E \in S} \frac{1}{w_E} \cdot [E] \in \mathbb{Q}_p[S].$$

The following result is well-known.

**Proposition 3.2** (i) We have $\tilde{e}_0 \in M[I]$.

(ii) We have:

$$\tilde{e}_0 \cdot \tilde{e}_0 = \frac{N - 1}{12}.$$  

**Proof** We first check that $\tilde{e}_0 \in M$. This is obvious if $p \geq 5$, so we need to check it when $p \in \{2, 3\}$. If $p = 2$ (resp. if $p = 3$), there is some $E$ in $S$ with $w_E = 2$ (resp. $w_E = 3$) if and only if 4 divides $N - 3$ (resp. 3 divides $N - 2$). Since $p$ divides the numerator of $\frac{N - 1}{12}$, we have $\tilde{e}_0 \in M$.

The fact that $\tilde{e}_0$ is annihilated by $I$ is an easy and well-known computation. The last assertion is equivalent to *Eichler mass formula*:

$$\sum_{E \in S} \frac{1}{w_E} = \frac{N - 1}{12}.$$  

(14)

We denote by $e_0, e_1, \ldots, e_n(r)$ a system of higher Eisenstein elements in $M/p^r M$, such that $e_0$ is the image of $\tilde{e}_0$ in $M/p^r M$. In this section, we give an explicit formula for $e_1$.

One idea would be to consider the element whose coefficient in $[E]$ is $\log(S'(j(E)))$, where $S(X) \in \mathbb{F}_N[X]$ is the monic polynomial whose roots are the $j$-invariants of elements in $S$. It turns out that this element is not $e_1$. For reasons we do not fully understand, this idea leads us to $e_1$ after adding an auxiliary $\Gamma(2)$-structure. In other words, we replace the $j$-invariants by the
Legendre $\lambda$-invariants. The analogue of the polynomial $S$ in this context is the well-known Hasse polynomial. In the next section, we mainly study the relation between the Hasse polynomial and the Hecke operators.

### 3.2 Overview of Sect. 3

We give a brief overview of the content of Sect. 3. In Sect. 3.3, we study the properties of the Hasse polynomial. We compute its discriminant in Theorem 3.3, which is crucial for the computation of $e_1 \bullet e_0$ (cf. Theorem 3.16 (ii)). We then study the relation between the Hasse polynomial and Hecke operators. The main result (and indeed of the whole section) is Theorem 3.5. Its proof relies crucially on Lemma 3.7, which really uses the $\Gamma(2)$-structure. Proposition 3.10 and Theorem 3.11 are related to the Hecke operator $U_2$ and are only secondary results. In Sects. 3.5, 3.6 and 3.7 we apply Theorem 3.5 to compute $e_1$ when $p = 5$, $p = 3$ and $p = 2$ respectively. Finally, Sects. 3.8 and 3.9 are not used elsewhere in the paper.

### 3.3 The Hasse polynomial

Recall the definition of the Hasse polynomial:

$$H(X) = \sum_{i=0}^{N-1} \left( \frac{N-1}{2i} \right)^2 X^i \in \mathbb{F}_N[X].$$

Let

$$P(Y) = \text{Res}_X (H'(X), 256 \cdot (1 - X + X^2)^3 - X^2 \cdot (1 - X)^2 \cdot Y) \in \mathbb{F}_N[Y].$$

#### 3.3.1 The discriminant of the Hasse polynomial

The computation of $e_1 \bullet e_0$ is related to the discriminant $\text{Disc}(H)$ of the Hasse polynomial.

**Theorem 3.3** Let $m = \frac{N-1}{2}$. We have, in $\mathbb{F}_N$:

$$\text{Disc}(H) = \frac{(-1)^{m(m-1)/2}}{m!} \cdot \prod_{k=1}^{m} k^{4k}.$$

*In particular, we have $\text{Disc}(H) \neq 0$, so the roots of $H$ are simples.*

**Proof** The following Picard–Fuchs differential equation is well-known (cf. the proof of [28, Theorem V.4.1]).
Lemma 3.4 Let $A = 4X(1 - X)$ and $B = 4(1 - 2X)$. Then for all $n \geq 0$, we have the following differential equation:

$$A \cdot H^{(n+2)} + (n + 1) \cdot B \cdot H^{(n+1)} - (2n + 1)^2 \cdot H^{(n)} = 0 \quad (15)$$

where $H^{(n)}$ is the $n$th derivative of $H$.

For all $n \geq 0$, let $r_n = \text{Res}(H^{(n)}, H^{(n+1)})$, where $\text{Res}$ is the resultant. Note that $r_0 = (-1)^{\frac{m(m-1)}{2}} \text{Disc}(H)$. We can rewrite the differential equation (15) as

$$A \cdot H^{(n+2)} + (n + 1) \cdot B \cdot H^{(n+1)} = (2n + 1)^2 \cdot H^{(n)}$$

and then take the resultant of both sides with $H^{(n+1)}$. Thus, for all $0 \leq n \leq m - 2$, we have:

$$r_n = (-4)^{m-n-1} \cdot (2n + 1)^{2n+2} \cdot H^{(n+1)}(0) \cdot H^{(n+1)}(1) \cdot r_{n+1}.$$ 

Note that $r_{m-1} = \text{Res}(H^{(m-1)}, m!) = m!$. We have to compute $a_n := H^{(n)}(0)$ and $b_n := H^{(n)}(1)$. We immediately see that $a_n = n! \cdot (\binom{m}{n})^2$. We can again use the differential equation (15) to compute $b_n$. For all $0 \leq n \leq m - 1$, we get:

$$b_n = -\frac{4(n + 1)}{(2n + 1)^2} \cdot b_{n+1}.$$ 

Furthermore, we have $b_m = m!$. We thus have, for all $0 \leq n \leq m$:

$$b_n = m! \cdot \prod_{i=n}^{m-1} \frac{-4 \cdot (i + 1)}{(2i + 1)^2}.$$ 

Thus, we have:

$$\prod_{i=1}^{m-1} H^{(i)}(0) \cdot H^{(i)}(1) = m!^{m-1} \cdot \prod_{i=1}^{m-1} i! \cdot \binom{m}{i}^2 \cdot \left(\frac{-4 \cdot (i + 1)}{(2i + 1)^2}\right)^i.$$ 

This gives us, after simplification:

$$\text{Res}(H, H') = r_0 = m!^{m} \cdot \prod_{i=1}^{m-1} (2i + 1)^2 \cdot (i + 1)^i \cdot i! \cdot \binom{m}{i}^2.$$
A direct computation finally shows that:
\[
\text{Res}(H, H') = m!^{-1} \cdot \prod_{k=1}^{m} k^{4k}.
\]

This concludes the proof of Theorem 3.3. \qed

3.3.2 Relation between the Hasse polynomial and the modular polynomials

We denote by \( L \) the set of roots of \( H \) in \( \overline{F}_N \). By Theorem 3.3, the roots of \( H \) are simples, so \( \text{Card}(L) = \frac{N-1}{2} \).

Let \( L' \) be the set of isomorphism classes of triples \((E, P_1, P_2)\) where \( E \) is a supersingular elliptic curve over \( \overline{F}_N \) and \((P_1, P_2)\) is a basis of the 2-torsion \( E[2](\overline{F}_N) \). Each such triple is isomorphic to a unique triple of the form \((E_\lambda : y^2 = x(x - 1)(x - \lambda), (0, 0), (1, 0))\) where \( \lambda \in \overline{F}_N \setminus \{0, 1\} \). We call \( \lambda \) the \textit{lambda-invariant} of \((E, P_1, P_2)\). The relation between the \( j \)-invariant and the lambda-invariant is:
\[
j = \frac{256 \cdot (1 - \lambda + \lambda^2)^3}{\lambda^2 \cdot (1 - \lambda)^2}.
\] (16)

We identify \( L' \) with the set of supersingular lambda-invariants. It is well-known that \( \lambda \in L' \) if and only if \( H(\lambda) = 0 \) [28, Theorem V.4.1(b)]. Thus, one can (and do) identify \( L' \) and \( L \). Since the supersingular Legendre elliptic curves in characteristic \( N \) are defined over \( F_{N^2} \), we have \( L \subset F_{N^2} \).

If \( \lambda \) and \( \lambda' \) are in \( \overline{F}_N \setminus \{0, 1\} \) (not necessarily in \( L \)) and \( \ell \geq 3 \) is a prime number different from \( N \), we say that \( \lambda \) and \( \lambda' \) are \( \ell \)-\textit{isogenous}, and we write \( \lambda \sim_\ell \lambda' \), if there is a rational isogeny \( \phi : E_\lambda \to E_{\lambda'} \) of degree \( \ell \) preserving the \( \Gamma(2) \)-structure, i.e. \( \phi(0, 0) = (0, 0) \) and \( \phi(1, 0) = (1, 0) \).

It is well-known (cf. for instance [3, Proposition 2.2]) that there exists a unique polynomial \( \varphi_\ell \in \mathbb{Z}[X, Y] \) which is monic in \( X \) and \( Y \), and such that we have \( \lambda \sim_\ell \lambda' \) if and only if \( \varphi_\ell(\lambda, \lambda') = 0 \). The polynomial \( \varphi_\ell(X, Y) \) is the “Legendre version” of the classical \( \ell \)th modular polynomial.

The following result is the key to compute \( e_1 \).

**Theorem 3.5** Let \( \ell \) be a prime number not dividing \( 2 \cdot N \) and let \( \lambda \in L \). We have, in \( F_{N^2} \):
\[
\prod_{\lambda' \sim_\ell \lambda} H'(\lambda') = \ell^{\ell-1} \cdot H'(\lambda)^{\ell+1}.
\] (17)
Remark 3.1 Equation (17) makes sense even if \( \lambda \in \overline{F}_N \setminus \{0, 1\} \cup L \), but it does not hold in general. The supersingularity of \( \lambda \) is used crucially in Lemma 3.9 below.

Proof The idea is to reinterpret \( H(\lambda) \) and \( H'(\lambda) \) as modular forms of level 1, and more precisely as Eisenstein series. If \( k \geq 2 \) is an integer, let

\[
E_k = 1 + \frac{(-1)^{k-1} \cdot 4k}{B_k} \cdot \sum_{n \geq 1} \sigma_{k-1}(n)q^n
\]

be the unique Eisenstein series of weight \( k \) and level \( SL_2(\mathbb{Z}) \) with constant coefficient 1.

Recall that a modular form of level \( SL_2(\mathbb{Z}) \) with coefficients in an \( F_N \)-algebra \( A \) can be considered, following Deligne and Katz [14, pp. 77–78], as a pair \( (E, \omega) \) were \( E \) is an elliptic curve over \( A \) and \( \omega \) is a differential form generating \( H^0(E, \Omega^1) \) over \( A \).

Recall that if \( \lambda \in \overline{F}_N \setminus \{0, 1\} \), we have denoted by \( E_{\lambda} \) the Legendre elliptic curve \( y^2 = x(x-1)(x-\lambda) \). We let \( \omega_{\lambda} = \frac{dx}{y} \). The following fact, essentially due du Katz, is crucial to interpret \( H'(\lambda) \).

Lemma 3.6 (Katz) Let \( m = \frac{N-1}{2} \). For all \( \lambda \in \overline{F}_N \setminus \{0, 1\} \), we have the following equality in \( \overline{F}_N \):

\[
E_{N+1}(E_{\lambda}, \omega_{\lambda}) = \frac{3}{m+1} \cdot (m \cdot H(\lambda) - (\lambda - 1) \cdot H'(\lambda)) + (\lambda + 1) \cdot H(\lambda).
\]

Proof Recall the following (unpublished) theorem of Katz [13, Theorem 3.1]. Let \( (E, \omega) \) be a pair of the form \( \left( y^2 = 4x^3 - g_2x - g_3, \frac{dx}{y} \right) \). Then, \( \frac{1}{12} \cdot E_{N+1}(E, \omega) \) is the coefficient of \( x^{N-2} \) in the polynomial \( (4x^3 - g_2x - g_3)^{\frac{N-1}{2}} \).

Let \( \lambda \in \overline{F}_N \setminus \{0, 1\} \), and \( f(x) = 4x(x-1)(x-\lambda) \). The pair \( \left( y^2 = f(x), \frac{dx}{y} \right) \) is isomorphic to the pair \( \left( y^2 = g(x), \frac{dx}{y} \right) \) with \( g(x) = f(x + c) = 4x^3 - g_2x - g_3 \) (for some \( g_2 \) and \( g_3 \)), where \( c = \frac{\lambda + 1}{3} \).

We have

\[
E_{N+1}(E_{\lambda}, \omega_{\lambda}) = E_{N+1}\left( y^2 = f(x), 2 \cdot \frac{dx}{y} \right) = 2^{-(N+1)} \cdot E_{N+1}\left( y^2 = g(x), \frac{dx}{y} \right),
\]
so \( \frac{2^{N+1}}{12} \cdot E_{N+1}^N(E_{\lambda}, \omega_{\lambda}) \) is the coefficient of \( x^{N-2} \) in \( g(x)^{\frac{N-1}{2}} = f(x + c)^{\frac{N-1}{2}}. \)

We have

\[
\left( \frac{f}{x^{\frac{N-1}{2}}} \right)^{(N-2)}(c) = \left( \frac{f}{x^{\frac{N-1}{2}}} \right)^{(N-2)}(0) + c \cdot \left( \frac{f}{x^{\frac{N-1}{2}}} \right)^{(N-1)}(0)
\]

where \( \left( \frac{f}{x^{\frac{N-1}{2}}} \right)^{(k)} \) is the \( k \)th derivative of \( f \), since \( \left( \frac{f}{x^{\frac{N-1}{2}}} \right)^{(k)} = 0 \) if \( k \geq N \).

A direct computation finally shows that

\[
\frac{2^{N+1}}{12} \cdot E_{N+1}(E_{\lambda}, \omega_{\lambda}) = \frac{2^{N-1}}{m + 1} \cdot \left( m \cdot H(\lambda) - (\lambda - 1) \cdot H'(\lambda) \right) \\
+ \frac{\lambda + 1}{3} \cdot 2^{N-1} \cdot H(\lambda).
\]

\( \square \)

Let \( \ell \) be a prime number not dividing \( 2 \cdot N \). If \( \varphi : E_{\lambda} \to E_{\lambda'} \) is an isogeny of degree \( \ell \) preserving the \( \Gamma(2) \)-structure then

\[
\varphi^*(\omega_{\lambda'}) = c_{\varphi} \cdot \omega_{\lambda}
\]

for some \( c_{\varphi} \in \overline{\mathbb{F}}_N^\times \). Note that there are only two \( \ell \)-isogenies \( E_{\lambda} \to E_{\lambda'} \). These are \( \varphi \) and \( -\varphi \). Consequently, \( c_{\varphi}^2 \) only depends on \( \lambda \) and \( \lambda' \) (satisfying \( \varphi_{\ell}(\lambda, \lambda') = 0 \)). In fact one can show that

\[
c_{\varphi}^2 =: c(\lambda, \lambda') \tag{18}
\]

is a rational function of \( \lambda \) and \( \lambda' \). More precisely, we have [17, Lemma 8]:

\[
c_{\varphi}^2 = -\ell \cdot \frac{\lambda(1 - \lambda)}{\lambda'(1 - \lambda')} \cdot \frac{\partial_Y \varphi_{\ell}(\lambda', \lambda)}{\partial_X \varphi_{\ell}(\lambda', \lambda)}. \tag{19}
\]

Note that this equality is true in \( \mathbb{Q}(\lambda, \lambda') \) and is deduced in \( \mathbb{F}_N(\lambda, \lambda') \) by reducing modulo \( N \) our objects (elliptic curves, isogenies...).

**Lemma 3.7** We have, over any field of characteristic \( \neq 2, \ell \), without assuming that \( E_{\lambda} \) is supersingular:

\[
\prod_{\varphi} c_{\varphi}^2 = \ell^2
\]

where the product is over a choice of non isomorphic degree \( \ell \) isogenies with origin \( E_{\lambda} \) and preserving the \( \Gamma(2) \)-structure. Equivalently, we have the fol-
lowing equality in $\mathbb{Q}(\lambda)$:

$$\frac{\text{Res}_X(\partial_Y \varphi_\ell(X, \lambda), \varphi_\ell(X, \lambda))}{\text{Res}_X(\partial_X \varphi_\ell(X, \lambda), \varphi_\ell(X, \lambda))} = \ell^{-(\ell-1)}.$$ 

Proof.

**Lemma 3.8** Let $F$ be a separably closed field of characteristic different from 2 and $\ell$. For all $\lambda \in F \setminus \{0, 1\}$, we have in $F$:

$$\prod_{\lambda' \sim \ell \lambda} \lambda' = \lambda^{\ell+1} \quad (20)$$

and

$$\prod_{\lambda' \sim \ell \lambda} (1 - \lambda') = (1 - \lambda)^{\ell+1}. \quad (21)$$

Proof This is well-known, cf. for instance [5, p. 122].

The equivalence between the two equalities comes from the relation

$$\prod_{\varphi} c_\varphi^2 = \ell^{\ell+1} \cdot \frac{\text{Res}_X(\partial_Y \varphi_\ell(X, \lambda), \varphi_\ell(X, \lambda))}{\text{Res}_X(\partial_X \varphi_\ell(X, \lambda), \varphi_\ell(X, \lambda))}$$

which is a direct consequence of (19) and Lemma 3.8. Let $F_\ell(\lambda) = \prod_{\varphi} c_\varphi^2$. This is a rational fraction in $\lambda$, which has no poles or zeros outside 0 and 1. Thus, we have $F_\ell(\lambda) = C_\ell \cdot \lambda^{n_\ell} \cdot (\lambda - 1)^{m_\ell}$ where $n_\ell, m_\ell \in \mathbb{Z}$ and $C_\ell \in \overline{F}_N^\times$.

The relations

$$\varphi_\ell(X, Y) = X^{\ell+1} Y^{\ell+1} \cdot \varphi_\ell(X^{-1}, Y^{-1})$$

and

$$\prod_{\lambda' \text{ s.t. } \varphi_\ell(\lambda', \lambda) = 0} \lambda' = \lambda^{\ell+1}$$

show that $F_\ell(\lambda) = F_\ell(\lambda^{-1})$. This last relation shows that $n_\ell = -(n_\ell + m_\ell)$. One can easily show that $\varphi_\ell(1-X, 1-Y) = \varphi_\ell(X, Y)$. This is deduced for example from the fact that $\lambda \left( \frac{-1}{z} \right) = 1 - \lambda(z)$ if $z$ is in the complex upper-half plane. The relation $\varphi_\ell(1-X, 1-Y) = \varphi_\ell(X, Y)$ shows that $F_\ell(1-\lambda) = F_\ell(\lambda)$, so $n_\ell = m_\ell$. Since $n_\ell = -(n_\ell + m_\ell)$, we have $n_\ell = m_\ell = 0$, so $F_\ell$ is a constant.
In order to show that $C_\ell = \ell^2$, it suffices to prove it over $\mathbb{C}$ using $q$-expansions, where $q = e^{i\pi z}$. More precisely, let $\lambda = \lambda(q)$ be fixed. The $\ell + 1$ roots of $\varphi_\ell(\lambda, X)$ are the $\lambda_i = \lambda \left( e^{\frac{i\pi (2i+1)}{\ell}} \right)$ where $i \in \{0, 1, \ldots, \ell - 1\}$ and $\lambda_\ell = \lambda(q^\ell)$. We thus have

$$C_\ell = c(\lambda, \lambda_\ell)^2 \cdot \prod_{i=0}^{\ell-1} c(\lambda, \lambda_i)^2$$

where $c$ was defined in (18).

This last factor is a constant function of $z$. Note that $c(\lambda, \lambda_i) = \frac{\ell}{c(\lambda_\ell, \lambda)}$. By [5, (4.6.1) p. 137], for all $i \in \{0, 1, \ldots, \ell - 1\}$ we have:

$$c(\lambda, \lambda_i) = \frac{\theta_3 \left( e^{\frac{i\pi (2i+1)}{\ell}} \right)^2}{\theta_3 \left( e^{i\pi z} \right)^2} ,$$

where $\theta_3(q) = \sum_{n \in \mathbb{Z}} q^{n^2}$. Thus, $c(\lambda, \lambda_i)$ goes to 1 when $z$ goes to $i \infty$. Similarly, $c(\lambda_\ell, \lambda)$ goes to 1 when $z$ goes to $i \infty$. This shows $C_\ell = \ell^2$. \qed

In order to conclude the proof of Theorem 3.5, we need one last result, which is only true in characteristic $N$ and uses the supersingularity in an essential way.

**Lemma 3.9** [27, Théorème B] Let $\lambda \in L$ and $\varphi : E_\lambda \to E_{\lambda'}$ be an isogeny of degree $\ell$. We have:

$$E_{N+1}(E_{\lambda'}, \omega_{\lambda'}) = \ell \cdot E_{N+1}(E_\lambda, \varphi^*(\omega_{\lambda'})) .$$

Using Lemma 3.6 and (21), we get

$$\prod_{\lambda' \sim \lambda} H'(\lambda') = \ell^{\ell+1} \prod_{\varphi} c_{\varphi}^{N+1} \cdot H(\lambda)^{\ell+1} .$$

Lemma 3.7 shows that $\prod_{\varphi} c_{\varphi}^{N+1} = (\ell^2)^{\frac{N+1}{2}} = \ell^2$, which concludes the proof of Theorem 3.5. \qed

We let

$$\varphi_2(X, Y) := Y^2 \cdot (1 - X)^2 + 16 \cdot X \cdot Y - 16 \cdot X \in \mathbb{Z}[X, Y] .$$

The following result motivates the definition of $\varphi_2$. 

\[ \square \] Springer
**Proposition 3.10** Let $z \in \mathbb{C}$ and $\lambda = \lambda(q)$ (where $q = e^{i\pi z}$). We have in $\mathbb{C}[Y]$:

$$
\left(Y - \lambda\left(e^{\frac{i\pi z}{2}}\right)\right) \cdot \left(Y - \lambda\left(e^{\frac{i\pi (z+2)}{2}}\right)\right) = \frac{1}{(1-\lambda)^2} \cdot \varphi_2(\lambda, Y).
$$

**Proof** We have:

$$
(Y - \lambda\left(e^{\frac{i\pi z}{2}}\right))(Y - \lambda\left(e^{\frac{i\pi (z+2)}{2}}\right))
= Y^2 - (\lambda(q^{\frac{1}{2}}) + \lambda(-q^{\frac{1}{2}})) \cdot Y + \lambda(q^{\frac{1}{2}})\lambda(-q^{\frac{1}{2}})
$$

where $q^{\frac{1}{2}} := e^{\frac{i\pi z}{2}}$. For clarity, let $\lambda_1 = \lambda(q^{\frac{1}{2}})$ et $\lambda_2 = \lambda(-q^{\frac{1}{2}})$. We have the following $q$-expansion identity:

$$
\lambda(q) = 16q \prod_{n=1}^{\infty} \left(\frac{1 + q^{2n}}{1 + q^{2n-1}}\right)^8.
$$

We follow [5, p. 63] by letting $Q_0 = \prod_{n=1}^{\infty}(1 - q^{2n})$, $Q_1 = \prod_{n=1}^{\infty}(1 + q^{2n})$, $Q_2 = \prod_{n=1}^{\infty}(1 + q^{2n-1})$ and $Q_3 = \prod_{n=1}^{\infty}(1 - q^{2n-1})$. We have:

$$
\lambda(q) = 16q \cdot \left(\frac{Q_1}{Q_2}\right)^8 \quad (23)
$$

and

$$
\lambda(q^{\frac{1}{2}}) \cdot \lambda(-q^{\frac{1}{2}}) = -16^2 q \prod_{n=1}^{\infty} \frac{(1 + q^n)^{16}}{(1 - q^{2n-1})^8} = -16^2 q \cdot \left(\frac{(Q_1 \cdot Q_2)^2}{Q_3}\right)^8 \quad (24)
$$

We have [5, p. 64,65]:

$$
Q_1 \cdot Q_2 \cdot Q_3 = 1 \quad (25)
$$

and

$$
Q_2^8 = Q_3^8 + 16q \cdot Q_1^8 \quad (26)
$$

By (24) and (25), we have:

$$
\lambda(q^{\frac{1}{2}}) \cdot \lambda(-q^{\frac{1}{2}}) = -16^2 q(Q_1 \cdot Q_2)^{3 \cdot 8} = -16^2 q \cdot \left(\frac{Q_1}{Q_2}\right)^{3 \cdot 8} \cdot Q_2^6 \cdot 8 \quad (27)
$$
By (25) and (26), we have:

\[ Q_2^{3:8} \cdot \left( \frac{Q_1}{Q_2} \right)^8 \cdot \left( 1 - 16q \cdot \left( \frac{Q_1}{Q_2} \right)^8 \right) = 1 \]

which gives

\[ Q_2^{6:8} = \frac{16^2 q^2}{\lambda^2 \cdot (1 - \lambda)^2} . \tag{28} \]

By (27) and (28), we have:

\[ \lambda \left( q^{\frac{1}{2}} \right) \cdot \lambda \left( -q^{\frac{1}{2}} \right) = \frac{-16 \cdot \lambda(q)}{(1 - \lambda(q))^2} \]

that is \( \lambda_1 \lambda_2 = \frac{-16\lambda}{(1 - \lambda)^2} \). By [5, p.115, (4.3.6)], we have \( \lambda(-q) = \frac{\lambda(q)}{1 - \lambda(q)} \), which gives

\[ (1 - \lambda_1) \cdot (1 - \lambda_2) = 1 , \]

that is

\[ \lambda_1 + \lambda_2 = \lambda_1 \cdot \lambda_2 = \frac{-16}{(1 - \lambda)^2} . \]

This concludes the proof of Proposition 3.10. \( \square \)

The following result is the analogue of Theorem 3.5 for \( \ell = 2 \).

**Theorem 3.11** Let \( \lambda \in L \) and let \( \lambda_1 \) and \( \lambda_2 \) be the roots of the polynomial \( \varphi_2(X, \lambda) \). We have:

\[ \lambda^{N-1} \cdot H'(\lambda_1) \cdot H'(\lambda_2) = \frac{\lambda^2 \cdot (\lambda - 1)}{4} \cdot H'(\lambda)^2 . \]

**Proof**

**Lemma 3.12** Keep the notation of Theorem 3.11, except that \( \lambda \in \bar{F}_N \backslash \{0, 1\} \) is now arbitrary. We have:

\[ \lambda^{N-1} \cdot H(\lambda_1) \cdot H(\lambda_2) = H(\lambda)^2 \tag{29} \]

**Proof** It suffices to prove the following identity, in \( \bar{F}_N[X] \):

\[ \text{Res}_X(H(X), \varphi_2(X, Y)) = H(Y)^2 . \tag{30} \]
We have
\[
\text{Res}_X(H(X), \varphi_2(X, Y)) = \prod_{\lambda' \in L} \varphi_2(\lambda', Y) = \prod_{\lambda' \in L} (1 - \lambda')^2 \cdot (\lambda'_1 - Y) \cdot (\lambda'_2 - Y),
\]
where \(\lambda'_1\) et \(\lambda'_2\) are the roots of \(\varphi_2(\lambda', Y) = 0\) (if \(\varphi_2(\lambda', Y)\) has double roots then we let \(\lambda'_1 = \lambda'_2\)). Since
\[
\prod_{\lambda' \in L} (1 - \lambda')^2 = 1,
\]
we get
\[
\text{Res}_X(H(X), \varphi_2(X, Y)) = \prod_{\lambda' \in L} (\lambda'_1 - Y) \cdot (\lambda'_2 - Y) = \prod_{\lambda' \in L} (\lambda' - Y)^2 = H(Y)^2. \tag{31}
\]

If \(\lambda' \in L\) then \(\lambda'_1\) and \(\lambda'_2\) are also in \(L\), since by Proposition 3.10 the elliptic curves \(E_{\lambda'_1}\) and \(E_{\lambda'_2}\) are 2-isogenous to \(E_\lambda\). If \(\lambda' \in \overline{\mathbb{F}}_N \setminus \{0, 1, -1\}\) (resp. \(\lambda' = -1\)) then the polynomial \(\varphi_2(\lambda', Y)\) has two distinct roots (resp. a double root \(Y = 2\)). Conversely, if \(\lambda_1 \in \overline{\mathbb{F}}_N \setminus \{0, 1, 2\}\) (resp. \(\lambda_1 = 2\)) then the polynomial \(\varphi_2(X, \lambda_1)\) has two distinct roots (resp. a double root \(X = -1\)). Thus, we have
\[
\prod_{\lambda' \in L} (\lambda'_1 - Y) \cdot (\lambda'_2 - Y) = \prod_{\lambda' \in L} (\lambda' - Y)^2 = H(Y)^2.
\]

We are going to differentiate (29) two times. Let \(K = \overline{\mathbb{F}}_N(\lambda)\) be the function field of \(\mathbb{P}^1(\lambda)\). We have a derivation \(\frac{d}{d\lambda}\) which sends \(\lambda\) to 1. Let \(F = K(\lambda_1)\) where \(\lambda_1\) has minimal polynomial \(X^2 + \frac{-2\lambda^2 + 16\lambda - 16}{\lambda^2} X + 1\) over \(K\).

**Lemma 3.13** The \(\overline{\mathbb{F}}_N\)-derivation \(\frac{d}{d\lambda}\) of \(K\) extends in an unique way to a \(\overline{\mathbb{F}}_N\)-derivation \(\frac{\partial}{\partial\lambda}\) of \(F\). More precisely, we have in \(F\):
\[
\frac{\partial \lambda_1}{\partial \lambda} = -\frac{\partial Y \varphi_2(\lambda_1, \lambda)}{\partial X \varphi_2(\lambda_1, \lambda)}.
\]

**Proof** This follows from the fact that \(\varphi_2\) is irreducible of degree 2 as a polynomial in \(X\) over \(\mathbb{F}_N(Y)\), and that \(N\) is prime to 2. \(\square\)

Let \(\lambda_2\) be the other root of \(X^2 + \frac{-2\lambda^2 + 16\lambda - 16}{\lambda^2} X + 1\) in \(F\).

**Lemma 3.14** We have:
\[
\frac{\partial \lambda_1}{\partial \lambda} \cdot \frac{\partial \lambda_2}{\partial \lambda} = \frac{4}{\lambda \cdot (\lambda - 1)}.
\]

**Proof** It is just a formal computation. \(\square\)
By differentiating (29) two times (λ is considered as a formal variable), we get:

$$\frac{4 \cdot \lambda^{N-1}}{\lambda \cdot (\lambda - 1)} \cdot H'(\lambda_1) \cdot H'(\lambda_2) = H'(\lambda)^2 + G(\lambda, \lambda_1, \lambda_2)$$

(32)

where $G(\lambda, \lambda_1, \lambda_2)$ is a sum of two terms of the form $H(\lambda)$, $H(\lambda_1)$ or $H(\lambda_2)$ times a polynomial in $\lambda, \lambda_1, \lambda_2, \frac{\partial H(\lambda_1)}{\partial \lambda}$ et $\frac{\partial H(\lambda_2)}{\partial \lambda}$. If $\lambda \in L$ then we have $H(\lambda) = H(\lambda_1) = H(\lambda_2) = 0$. By (32), we get

$$\frac{4 \cdot \lambda^{N-1}}{\lambda \cdot (\lambda - 1)} \cdot H'(\lambda_1) \cdot H'(\lambda_2) = H'(\lambda)^2 .$$

This concludes the proof of Theorem 3.11 (i).

3.4 The supersingular module of Legendre elliptic curves

Keep the notation of Sects. 3.1 and 3.3. We denote by $v$ the $p$-adic valuation of $N^2 - 1$ (thus, $v = t$ if $p \geq 5$, $v = t + 1$ if $p = 3$ and $v = t + 3$ if $p = 2$). In view of the properties satisfied by the Hasse polynomial, the higher Eisenstein element $e_1$ is more easily determined after adding an auxiliary $\Gamma(2)$-structure.

Let $\mathbb{T}'$ be the $\mathbb{Z}_p$-Hecke algebra acting faithfully the space of modular forms of weight 2 and level $\Gamma_0(N) \cap \Gamma(2)$. If $n \geq 1$ is an integer, we denote by $T'_n$ the $n$th Hecke operator in $\mathbb{T}'$. The ring $\mathbb{T}'$ acts on the $\mathbb{Z}_p$-module $M' := \mathbb{Z}_p[L]$. If $\ell$ is a prime not dividing $2 \cdot N$ and $\lambda \in L$, we have in $M'$:

$$T'_\ell([\lambda]) = \sum_{\lambda' \in L, \phi(\lambda, \lambda') = 0} [\lambda'] .$$

Let

$$\tilde{e}'_0 = \sum_{\lambda \in L} [\lambda] \in M' .$$

Theorem 3.15 Let $\Lambda : \mathbb{F}_{N^2}^\times \to \mathbb{Z}/p^v\mathbb{Z}$ be a surjective group homomorphism. Let $e'_0$ be the image of $\tilde{e}'_0$ in $M' / p^v M'$ and let

$$e'_1 = \sum_{\lambda \in L} \Lambda(H'(\lambda)) \cdot [\lambda] \in M' / p^v M' .$$

For all prime $\ell$ not dividing $2 \cdot N$, we have in $M' / p^v M'$:

$$(T'_\ell - \ell - 1)(e'_0) = 0$$
and
\[(T_\ell' - \ell - 1)(e'_1) = (\ell - 1) \cdot \Lambda(\ell) \cdot e'_0.\]

**Proof** The first equality is obvious. The second equality is a direct consequence of Theorem 3.5.  

We let $\pi : M' \to M$ be the forgetful map. It is a $\mathbb{Z}_p$-linear map defined by $\pi([\lambda]) = [E_\lambda] \in S$ (recall that $E_\lambda$ is the Legendre elliptic curve $y^2 = x(x-1)(x-\lambda)$). For all prime $\ell$ not dividing $2 \cdot N$ and all $x \in M'$, we have in $M$:
\[
\pi \left( T_\ell'(x) \right) = T_\ell(\pi(\pi)).
\] (33)

We have, in $M$:
\[
\pi(\tilde{e}'_0) = 6 \cdot \tilde{e}_0. \quad \text{(34)}
\]

Theorem 3.15, (33) and (34) allow us to compute $e_1$. However, some complications arise when $p \in \{2, 3\}$, so we treat the cases $p \geq 5$, $p = 3$ and $p = 2$ separately.

**3.5 The case $p \geq 5$**

In this paragraph, we assume $p \geq 5$. Keep the notation of paragraphs 3.1, 3.3 and 3.4.

Theorems 1.6 and 1.7 are particular cases (when $r = 1$) of the following result.

**Theorem 3.16** Assume that $p \geq 5$. We extend $\log$ to a surjective group morphism $\log : F_{N^2}^x \to \mathbb{Z}/p^r\mathbb{Z}$.

(i) We have, in $M/p^r M$ modulo the subgroup generated by $e_0$:
\[
12 \cdot e_1 = \sum_{E \in S} \frac{1}{w_E} \cdot \log(P(j(E))) \cdot [E]
\]
where $j(E)$ is the $j$-invariant of $E$ (the fact that $P(j(E)) \neq 0$ is included in the statement).

(ii) We have, in $\mathbb{Z}/p^r\mathbb{Z}$:
\[
e_1 \cdot e_0 = \frac{1}{12} \cdot \sum_{\lambda \in L} \log(H'(\lambda))
\]
\[
= \frac{1}{3} \sum_{k=1}^{N-1} k \cdot \log(k).
\]
(iii) Assume $e_1 \cdot e_0 = 0$. We have, in $\mathbb{Z}/p^r\mathbb{Z}$:

$$72 \cdot e_1 \cdot e_1 = 3 \cdot \left( \sum_{\lambda \in L} \log(H'(\lambda))^2 \right) - 4 \cdot \left( \sum_{\lambda \in L} \log(\lambda)^2 \right).$$

Proof We prove (i). We choose $\Lambda : \mathbb{F}_{N^2}^\times \to \mathbb{Z}/p^v\mathbb{Z}$ so that for all $x \in \mathbb{F}_{N^2}^\times$, we have $\Lambda(x) \equiv \log(x)$ (modulo $p^r$). We abuse notation and still denote by $\pi : M' / p^r M' \to M / p^r M$ the forgetful map. Let $e_1''$ be the image of $e_1'$ in $M' / p^r M'$. Let $\ell$ be a prime not dividing $2 \cdot N$. By Theorem 3.15, (33) and (34) we have in $M / p^r M$:

$$(T_\ell - \ell - 1)(\pi(e_1'')) = 6 \cdot (\ell - 1) \cdot \log(\ell) \cdot e_0.$$

By Proposition 2.7, we have

$$\pi(e_1'') = 12 \cdot e_1 \pmod{\text{the subgroup generated by } e_0}.$$

Let $E \in S$. The coefficient of $\pi(e_1'')$ in $[E]$ is by definition

$$\sum_{\substack{\lambda \in L \\colon \ j(E_{\lambda}) = j(E)}} \log(H'(\lambda)).$$

By (16), we have

$$\sum_{\substack{\lambda \in L \\colon \ j(E_{\lambda}) = j(E)}} \log(H'(\lambda)) = \frac{1}{w_E} \cdot \log(P(j(E))).$$

This concludes the proof of Theorem 3.16 (i).

We prove (ii). We have:

$$12 \cdot e_1 \cdot e_0 = \sum_{E \in S} \frac{1}{w_E} \cdot \log(P(j(E)))$$

$$= \sum_{\lambda \in L} \log(H'(\lambda))$$

$$= \log(\text{Disc}(H))$$

$$= 4 \cdot \sum_{k=1}^{N-1} k \cdot \log(k).$$

The first equality follows from (i). The last equality follows from Theorem 3.3, using the fact that $\log\left(\left(\frac{N-1}{2}\right)\right) = 0$ (since $p > 2$ and $\left(\frac{N-1}{2}\right)!^4 = 1$ in $\mathbb{F}_N$).
We prove (iii). We identify an element of \( L \) with its \( \lambda \)-invariant. For \( E \in S \), let \( F_E \subset L \) be the fiber above \( E \), i.e. the set of \( \lambda \in L \) such that \( \pi(\lambda) = [E] \). There exists \( \lambda \in L \) such that

\[
F_E = \left\{ \lambda, \frac{1}{\lambda}, 1 - \lambda, \frac{\lambda - 1}{\lambda}, \frac{1}{\lambda - 1}, 1 - \frac{1}{\lambda} \right\}
\]

(we do not count multiplicity). Let \( c_E \in \{1, 2, 3, 6\} \) be the cardinality of \( F_E \). We have \( w_E = \frac{6}{c_E} \). We have, by definition of \( P \), for any \( E \in S \) and \( \lambda \in F_E \):

\[
P(j(E)) = H'(\lambda) \cdot H'(\frac{1}{\lambda}) \cdot H'(1 - \lambda) \cdot H'(\frac{\lambda - 1}{\lambda}) \cdot H'(1 - \frac{1}{\lambda}) \cdot H'(\frac{\lambda}{\lambda - 1}).
\]

We have \( H(X) = (-1)^m \cdot H(1 - X) \) and that \( H(\frac{1}{X}) = X^{-m} \cdot H(X) \) where \( m = \frac{N-1}{2} \). Indeed, \( H \) is monic and the roots of \( H \) are permuted by the transformation \( \lambda \mapsto 1 - \lambda \) and \( \lambda \mapsto \frac{1}{\lambda} \). By differentiating these two relations with respect to \( X \) and using (36), we get:

\[
P(j(E)) = H'(\lambda)^6 \cdot \lambda^4 \cdot (1 - \lambda)^4.
\]

Thus, we have, in \( \mathbb{Z}/p^r\mathbb{Z} \):

\[
12^2 \cdot e_1 \bullet e_1 = \sum_{E \in S} \frac{1}{w_E} \cdot \log(P(j(E)))^2
\]
\[
= \frac{1}{6} \cdot \left( \sum_{\lambda \in L} 6 \cdot \log(H'(\lambda)) + 4 \cdot \log(\lambda) + 4 \cdot \log(1 - \lambda) \right)^2
\]
\[
= 6 \cdot \left( \sum_{\lambda \in L} \log(H'(\lambda))^2 \right) - 8 \cdot \left( \sum_{\lambda \in L} \log(\lambda))^2 \right)
\]

This concludes the proof of Theorem 3.16.

\( \square \)

**Remarks 3.1**

(i) Theorem 3.16 (ii) will be proved independently using modular symbols in Sect. 6.3.

(ii) Theorem 3.16 (ii) is the first instance of what we call a higher Eichler mass formula, by analogy with the classical Eichler mass formula (14).

(iii) In Corollary 6.8, we will show (using modular symbols) that if \( e_1 \bullet e_0 = 0 \), then \( e_1 \bullet e_1 = 12 \cdot \sum_{k=1}^{N-1} k \cdot \log(k)^2 \). This is the second instance of a
higher Eichler mass formula. We have not been able to prove this identity directly. See Conjecture 3.21 (iii) for a generalization when \( e_1 \cdot e_0 \neq 0 \).

### 3.6 The case \( p = 3 \)

In this paragraph, we assume \( p = 3 \). Keep the notation of paragraphs 3.1, 3.3 and 3.4.

**Theorem 3.17** Extend and lift \( \log \) to a surjective group homomorphism \( \log : F_{\mathbf{N}_2} \rightarrow \mathbf{Z}/3^{r+1}\mathbf{Z} \). We have, in \( (M/3^{r+1}M) / (\mathbf{Z} \cdot (3 \cdot e_0)) \):

\[
12 \cdot e_1 \equiv 2 \cdot \log(2) \cdot \tilde{e}_0 + \sum_{E \in S} w_E \cdot \log(P(j(E))) \cdot [E].
\]

**Proof** It obviously suffices to prove Theorem 3.17 when \( r = t \), which we assume until the end of the proof. Note that \( v = t + 1 \), so we can let \( \Lambda = \log \).

We abuse notation and still denote by \( \pi : M'/3^{t+1}M' \rightarrow M/3^{t+1}M \) the forgetful map. Let \( \ell \) be a prime not dividing \( 2 \cdot N \). By Theorem 3.15, (33) and (34) we have in \( M/3^{t+1}M \):

\[
(T_{\ell} - \ell - 1)(\pi(e'_1)) = 6 \cdot (\ell - 1) \cdot \log(\ell) \cdot e_0.
\]

By Proposition 2.7, we have

\( \pi(e'_1) = 12 \cdot e_1 \) (modulo the subgroup generated by the image of \( \tilde{e}_0 \) in \( M/3^{t+1}M \)).

Let \( E \in S \). The coefficient of \( \pi(e'_1) \) in \( [E] \) is by definition

\[
\sum_{\lambda \in L} \log(H'(\lambda)) = \sum_{j(E_\lambda) = j(E)} \log(H'(\lambda)).
\]

By (16), we have

\[
\sum_{j(E_\lambda) = j(E)} \log(H'(\lambda)) = \frac{1}{w_E} \cdot \log(P(j(E))) .
\]

Thus, there exists \( C_3 \in \mathbf{Z}/3^{t+1}\mathbf{Z} \), uniquely defined modulo 3, such that we have in \( M/3^{t+1}M \):

\[
12 \cdot e_1 = C_3 \cdot \tilde{e}_0 + \sum_{E \in S} \frac{1}{w_E} \log(P(j(E))) \cdot [E]. \quad (38)
\]
By pairing (38) with \( \tilde{e}_0 \), we get in \( \mathbb{Z}/3^{t+1}\mathbb{Z} \):

\[
12 \cdot e_1 \cdot e_0 = C_3 \cdot \tilde{e}_0 \cdot \tilde{e}_0 + \log(\text{Disc}(H)).
\]

By Corollary 6.3, Theorem 6.4, Eichler mass formula (14), Theorem 3.3 and Lemma 5.11 (which are independent of the results of this section), we have in \( \mathbb{Z}/3^{t+1}\mathbb{Z} \):

\[
-3 \cdot \sum_{k=1}^{N-1} k^2 \cdot \log(k) = C_3 \cdot \frac{N - 1}{12} - 3 \cdot \sum_{k=1}^{N-1} k^2 \cdot \log(k) - \frac{N - 1}{6} \cdot \log(2).
\]

This concludes the proof of Theorem 3.17.

\( \square \)

Remark 3.2 One could use Theorem 3.17 to compute \( e_1 \cdot e_1 \) if \( t \geq 2 \) and \( r \leq t - 1 \).

### 3.7 The case \( p = 2 \)

In this paragraph, we assume \( p = 2 \). Keep the notation of paragraphs 3.1, 3.3 and 3.4.

**Theorem 3.18** Let \( \tilde{\Lambda} : F_{N_2}^\times \to \mathbb{Z}/2^{t+3}\mathbb{Z} \) be a surjective group homomorphism such that for all \( x \in F_{N}^\times \), we have \( \tilde{\Lambda}(x) \equiv 2 \cdot \log(x) \) (modulo \( 2^{r+1} \)). Let \( \epsilon_2 \in \{1, -1\} \) be defined by

\[
\tilde{\Lambda} \left( \left( \frac{N - 1}{2} \right)! \right) \equiv 2^{t+1} \cdot \epsilon_2 \pmod{2^{t+3}}.
\]

Let \( \Lambda \) be the reduction of \( \tilde{\Lambda} \) modulo \( 2^{r+3} \). We have, in \( M/2^{r+3}M \) modulo the subgroup generated by \( 8 \cdot e_0 \):

\[
24 \cdot e_1 = 2 \cdot C_2 \cdot \tilde{e}_0 + \sum_{E \in S} \frac{1}{w_E} \cdot \Lambda(P(j(E))) \cdot [E].
\]

where

\[
C_2 \equiv \frac{2^{t+2}}{N - 1} \cdot \epsilon_2 \pmod{4}.
\]

**Proof** It obviously suffices to prove Theorem 3.18 when \( r = t \) (so \( v = r + 3 \)), which we assume until the end of the proof. We abuse notation and still denote
by \( \pi : M'/2^{t+3}M' \to M/2^{t+3}M \) the forgetful map. Let \( \ell \) be a prime not dividing \( 2 \cdot N \). By Theorem 3.15, (33) and (34) we have in \( M/2^{t+3}M \):

\[
(T_\ell - \ell - 1)(\pi(e'_1)) = 12 \cdot (\ell - 1) \cdot \log(\ell) \cdot e_0.
\]

By Proposition 2.7, there exists \( C'_2 \in \mathbb{Z}/2^{t+3}\mathbb{Z} \) (uniquely defined modulo 8) such that we have, in \( M/2^{t+3}M \) modulo the subgroup generated by the image of \( \tilde{e}_0 \) in \( M/2^{t+3}M \):

\[
24 \cdot e_1 = C'_2 \cdot \tilde{e}_0 + \sum_{E \in S} \frac{1}{w_E} \cdot \tilde{\Lambda}(P(j(E))) \cdot [E]. \tag{39}
\]

By pairing (39) with \( \tilde{e}_0 \), we get in \( \mathbb{Z}/2^{t+3}\mathbb{Z} \):

\[
24 \cdot e_1 \cdot e_0 = C'_2 \cdot \tilde{e}_0 \cdot \tilde{e}_0 + \tilde{\Lambda}(\text{Disc}(H)) \pmod{2^{t+3}}.
\]

By Corollary 6.3, Theorem 6.4, Eichler mass formula (14) and Theorem 3.3 (which are independent of the results of this section), we have in \( \mathbb{Z}/2^{t+3}\mathbb{Z} \):

\[
-2^{t+2} + 8 \cdot \left( \sum_{k=1}^{N-1} k \cdot \log(k) \right) \equiv C'_2 \cdot \frac{N - 1}{12} + 8 \cdot \left( \sum_{k=1}^{N-1} k \cdot \log(k) \right) - \tilde{\Lambda} \left( \left( \frac{N - 1}{2} \right)! \right).
\]

Thus, we have in \( \mathbb{Z}/2^{t+3}\mathbb{Z} \):

\[
2^{t} \cdot \left( 4 + \frac{C'_2}{3} \cdot \frac{N - 1}{2^{t+2}} - 2 \cdot \epsilon_2 \right) = 0.
\]

Thus, we have

\[
C'_2 \equiv 6 \cdot \frac{2^{t+2}}{N - 1} \cdot (\epsilon_2 - 2) \equiv 2 \cdot C_2 \pmod{8}.
\]

This concludes the proof of Theorem 3.18.

The following result is an elementary consequence of Theorem 3.18, for which we have not found an elementary proof.

**Corollary 3.19** There exists \( \lambda \in L \) such that \( H'(\lambda) \) is not a square of \( \mathbf{F}_{N^2}^\times \).
Proof If $E \in S$, let $F_E$ be defined as in (35). By (37), for all $\lambda \in F_E$ we have:

$$P(j(E)) = H'(\lambda)^6 \cdot \lambda^4 \cdot (1 - \lambda)^4.$$ 

Thus exists $E \in S$ such that $P(j(E))$ is not a fourth power in $F_{N^2}^\times$ if and only if there is $\lambda \in L$ such that $H'(\lambda)$ is not a square of $F_{N^2}^\times$. Such a $E$ exists by Theorem 3.18 since we have $C_2 \in (\mathbb{Z}/4\mathbb{Z})^\times$. \hfill $\square$

The following conjecture was checked numerically for $N < 2000$ (without assuming $N \equiv 1$ (modulo 8) anymore). We do not know the significance of this empirical fact.

**Conjecture 3.20** Assume $N \equiv 1$ (modulo 4). For all $\lambda \in L$, $H'(\lambda)$ is not a square of $F_{N^2}^\times$.

**Remark 3.3** Conjecture 3.20 does not hold if $N \equiv 3$ (modulo 4), since in this case there exists $\lambda \in F_N \cap L$, so $H'(\lambda) \in F_N^\times$ is a square of $F_{N^2}^\times$ [3, Proposition 4.3].

### 3.8 Conjectural identities satisfied by the supersingular lambda invariants

In this section, we collect various (often conjectural) arithmetic properties satisfied by the elements of $L$. These identities are motivated by the theory of the Eisenstein ideal.

**Conjecture 3.21** Assume $p \geq 5$. Extend $\log$ to a surjective group homomorphism $\log : F_{N^2}^\times \rightarrow \mathbb{Z}/p^r\mathbb{Z}$.

1. We have $\sum_{\lambda \in L} \log(\lambda)^2 = -32 \cdot \log(2) \cdot \left( \sum_{k=1}^{N-1} k \cdot \log(k) \right)$.
2. There exists $\lambda \in L$ such that $\log(\lambda) \neq 0$.
3. We have $\sum_{\lambda \in L} \log(H'(\lambda))^2 = 4 \cdot \left( \sum_{k=1}^{N-1} k \cdot \log(k)^2 \right) - 3 \cdot 16 \cdot \log(2) \cdot \left( \sum_{k=1}^{N-1} k \cdot \log(k) \right)$.
4. Assume $\sum_{k=1}^{N-1} k \cdot \log(k) = 0$. For all $\lambda \in L$, we have

$$\sum_{\lambda' \in L \setminus \{\lambda\}} \log(\lambda' - \lambda) \cdot \log(H'(\lambda')) = \log(H'(\lambda))^2.$$
(v) Assume $\sum_{k=1}^{N-1} k \cdot \log(k) = 0$. For all $\lambda \in L$, we have
\[ \sum_{\lambda' \in L \setminus \{\lambda\}} \log(\lambda' - \lambda) \cdot \log(\lambda') = \log(\lambda)^2. \]

Remarks 3.2
(i) These conjectures have been numerically checked (using SAGE) for $N < 1000$.
(ii) Using (derivatives of) the relations $H(1 - X) = (-1)^m \cdot H(X)$ and $H(\frac{1}{X}) = X^{-m} \cdot H(X)$ (where $m = \frac{N-1}{2}$), we easily prove that
\[ \sum_{\lambda \in L} \log(H'(\lambda)) \cdot \log(\lambda) = \sum_{\lambda \in L} \log(H'(\lambda)) \cdot \log(1 - \lambda) = -\sum_{\lambda \in L} \log(\lambda)^2 \]
\[ = -2 \cdot \sum_{\lambda \in L} \log(\lambda) \cdot \log(1 - \lambda) \]

which allows us to reformulate Conjecture 3.21 (i).
(iii) The term $\log(2)$ in Conjecture 3.21 (i) comes from a criterion of Ribet concerning the existence of congruences between cuspidal newforms of weight 2 and level $\Gamma_0(2N)$, and Eisenstein series [31, Theorem 2.3].
(iv) It seems that Venkatesh found a proof of Conjecture 3.21 (i) using the Hecke operator $U_2$.
(v) We will show in Proposition 3.28 that (ii) holds if $\log(2) \not\equiv 0$ (modulo $p$).
(vi) If $\sum_{k=1}^{N-1} k \cdot \log(k) = 0$, Conjecture 3.21 (iii) is proved in Corollary 6.8, using modular symbols.
(vii) Conjecture 3.21 (iv) and (v) are suggested by the theory of the refined $\mathcal{L}$-invariant of de Shalit [8], Oesterlé, Mazur–Tate [20] and Mazur–Tate–Teitelbaum [21], and its generalization to level $\Gamma(2) \cap \Gamma_0(N)$ studied in [4].

We end this section with (conjectural) relations analogous to the ones of Conjecture 3.21 for $p = 3$ and $p = 2$.

**Conjecture 3.22** Assume $p = 3$. Extend and lift $\log$ to a surjective group homomorphism $\log : F_{N^2}^\times \to \mathbb{Z}/p^{r+1}\mathbb{Z}$.

(i) There exists $\lambda \in L$ such that $\log(\lambda) \not\equiv 0$ (modulo 3) (i.e. $\lambda$ is not a cube of $F_{N^2}$).
(ii) We have
\[ \sum_{\lambda \in L} \log(\lambda)^2 = 4 \cdot \log(2) \cdot \left( \sum_{k=1}^{N-1} k \cdot \log(k) \right) \pmod{9}. \]
Furthermore, both sides of the equality are congruent to 0 modulo 3.

(iii) For all \( \lambda \in L \), we have:
\[
\sum_{\lambda' \in L \setminus \{\lambda\}} \log(\lambda' - \lambda) \cdot \log(H'(\lambda')) = \log(H'(\lambda))^2 \pmod{3}
\]

(iv) For all \( \lambda \in L \), we have:
\[
\sum_{\lambda' \in L \setminus \{\lambda\}} \log(\lambda' - \lambda) \cdot \log(\lambda') = \log(\lambda)^2 \pmod{3}
\]

Remarks 3.3
(i) Conjecture 3.22 (i) should be true even if \( N \not\equiv 1 \pmod{9} \) (which is assumed since \( p = 3 \)).
(ii) Conjecture 3.22 (ii), (iii) and (iv), although similar to 3.21, is not true modulo \( 3^{r+1} \) in general.

The following result, in which \( N \) is an arbitrary odd prime, is kind of opposite to Conjecture 3.22 (i).

Proposition 3.23 For all \( \lambda \in L \), \( \frac{\lambda(1-\lambda)}{2} \) is a cube of \( F_{N^2}^\times \).

Proof Since \( j = \frac{256(\lambda^2-\lambda+1)^3}{\lambda^2(1-\lambda)^2} \), it suffices to show that supersingular \( j \)-invariants are cubes of \( F_{N^2}^\times \). This is well-known [24, Theorem 1.2 (b)]. \( \square \)

We conclude this section by stating a result which goes in the opposite direction of Conjecture 3.21 (ii).

Proposition 3.24 [1, Proposition 3.1] Every \( \lambda \in L \) is a fourth power modulo \( N \) (we do not assume anything on \( N \)). If \( N^2 \equiv 1 \pmod{8} \), then every \( \lambda \in L \) is a eighth power modulo \( N \).

3.9 Eisenstein ideals of level \( \Gamma_0(N) \cap \Gamma(2) \)

Assume \( p \geq 3 \). Keep the notation of paragraphs 3.1, 3.3 and 3.4. Extend log to a surjective group homomorphism \( \log : F_{N^2}^\times \to \mathbb{Z}/p^r\mathbb{Z} \).

In view of the role played by the Hasse polynomial, we reformulate the problem of Eisenstein elements in the context of the congruence subgroup \( \Gamma_0(N) \cap \Gamma(2) \). The modular curve \( X(\Gamma_0(N) \cap \Gamma(2)) \) has 6 cusps. Thus, the space of Eisenstein series of weight 2 and level \( \Gamma_0(N) \cap \Gamma(2) \) has dimension 5. It admits a basis of eigenforms for the Hecke operators \( T_\ell \) (\( \ell \) prime \( \neq 2, N \), \( U_2 \) and \( U_N \)). These Eisenstein series are characterized by the pair \( (a_N, a_2) \) of their Fourier coefficients (at the cusp \( \infty \)) at \( N \) and 2, which belongs
to \{(1, 1), (1, 2), (1, 0), (N, 1), (N, 0)\}. Since \(p^t\) divides \(N - 1\), these coefficients are in \{(1, 1), (1, 2), (1, 0)\} modulo \(p^t\). We define three Eisenstein ideals.

For \(\alpha \in \{0, 1, 2\}\), let \(I_\alpha\) be the ideal of the Hecke algebra acting on \(M_2(\Gamma(2) \cap \Gamma_0(N))\) generated by the \(T_\ell - \ell - 1\) (\(\ell\) prime number different from 2 and \(N\)), \(U_2 - \alpha\) and \(U_N - 1\). Recall that these Hecke operators generate a \(\mathbb{Z}_p\)-algebra \(T'\) acting on \(M' = \mathbb{Z}_p[L]\). We have described the action of \(T_\ell\) (given by the modular polynomial \(\phi_\ell\)) and \(U_N\) (given by \([\lambda] \mapsto [\lambda^N]\)). We are going do describe \(U_2\) (this might be well-known, be we could not find a reference).

**Proposition 3.25** For all \(\lambda \in L\), we have in \(M'\):

\[U_2([\lambda]) = [\lambda_1] + [\lambda_2]\]

where \(\lambda_1\) et \(\lambda_2\) are the roots of the polynomial \(\varphi_2(\lambda, Y)\).

**Proof** This follows from Proposition 3.10. \(\square\)

Define the following elements in \(M'/p^r M'\), if \(p \geq 5\):

- \(e^0_0 = \sum_{\lambda \in L} \log(\lambda) \cdot [\lambda]\)
- \(e^1_0 = \sum_{\lambda \in L} (\log(1 - \lambda) - 2 \cdot \log(\lambda) - 4 \cdot \log(2)) \cdot [\lambda]\)
- \(e^2_0 = \sum_{\lambda \in L} [\lambda]\)

If \(p = 3\), we define in the same way \(e^0_0\) and \(e^2_0\). To define \(e^1_0\), note that by Proposition 3.23, for all \(\lambda \in L\) there exists \(a_\lambda \in \mathbb{F}_{N^2}\) such that \(\frac{1 - \lambda}{\lambda^2 \cdot 2^t} = a_\lambda^3\). We then let

\[e^1_0 = \sum_{\lambda \in L} a_\lambda \cdot [\lambda] \in M'/3^r \cdot M'\]

(this does not depend on the choice of \(a_\lambda\) since \(r \leq t < v = v_3(N - 1) = t + 1\).

**Proposition 3.26** For all \(\alpha \in \{0, 1, 2\}\), \(e^\alpha_0\) is annihilated by the ideal \(I_\alpha\).

**Proof** The property for \(T_\ell - \ell - 1\) for a prime \(\ell \neq 2, N\) follows from Lemma 3.8. The fact that these elements are killed by \(U_N - 1\) is obvious. The property for \(U_2\) is a formal computation using Proposition 3.25. \(\square\)

**Conjecture 3.27** The elements \(e^1_0\) and \(e^0_0\) are non-zero modulo \(p\).

**Remarks 3.4** (i) The fact that \(e^0_0 \neq 0\) is equivalent to Conjecture 3.21 (ii) if \(p \geq 5\) and to Conjecture 3.22 (i) if \(p = 3\).

(ii) By [32, Theorems 1.3], the \(\mathbb{Z}/p^r \mathbb{Z}\)-module \((M'/p^r M')[I_\alpha]\) is free of rank one. Thus, if Conjecture 3.27 is true, we have \((M'/p^r M')[I_\alpha] = \mathbb{Z}/p^r \mathbb{Z} \cdot e^\alpha_0\).
**Proposition 3.28** Assume that 2 is not a $p$th power modulo $N$, i.e. $\log(2) \not\equiv 0$ (modulo $p$). Then Conjecture 3.27 holds.

**Proof** Assume that for all $\lambda \in L$, $\log(\lambda) \equiv 0$ (modulo $p$). We use the same notation as in Proposition 3.25. We have

$$\log(\lambda_1 \cdot \lambda_2) \equiv 0 \equiv \log \left( \frac{-16 \cdot \lambda}{(1 - \lambda)^2} \right) \equiv \log(-16) \pmod{p}.$$ 

This is a contradiction since $p \geq 3$ and $\log(2) \not\equiv 0$. Thus, we have $e_0^0$ is non-zero modulo $p$.

Assume that for all $\lambda \in L$,

$$\log(1 - \lambda) - 2 \cdot \log(\lambda) - 4 \cdot \log(2) \equiv 0 \pmod{p}.$$ 

We use the same notation as in Proposition 3.25. We then have

$$0 \equiv \log ((1 - \lambda_1)(1 - \lambda_2)) 
\equiv 2 \cdot \log(\lambda_1) + 2 \cdot \log(\lambda_2) + 8 \cdot \log(2) 
\equiv 2 \cdot \log \left( \frac{-16 \cdot \lambda}{(1 - \lambda)^2} \right) + 8 \cdot \log(2) \pmod{p}.$$ 

Thus, we have $\log(\lambda) - 2 \cdot \log(1 - \lambda) + 8 \cdot \log(2) \equiv 0$ (modulo $p$), so $-3 \cdot \log(\lambda) \equiv 0$ (modulo $p$). If $p > 3$, this is a contradiction by the previous case. If $p = 3$, we just work modulo 9 instead of working modulo 3. \qed

We now want to determine $(M'/p^r M')[I_2]$. The only result we got in this direction is the following.

**Theorem 3.29** Let

$$e_1^2 := e_0^0 + \frac{1}{2} \cdot e_0^1 + \frac{1}{2} \cdot \sum_{\lambda \in L} \log(H'(\lambda)) \cdot [\lambda].$$

(i) We have, for all prime number $\ell$ not dividing $2 \cdot N$:

$$(T - \ell - 1)(e_1^2) = \frac{\ell - 1}{2} \cdot \log(\ell) \cdot e_0^0.$$ 

(ii) We have:

$$(U_2 - 2)(e_1^2) = \log(2) \cdot e_0^0$$
(iii) We have
\[(U_N - 1)(e_1^2) = 0.\]

In particular, we have \(e_1^2 \in (M' / p^r M')[I_2^2].\)

**Proof** Point (i) follows from Proposition 3.26 and Theorem 3.5. Point (ii) follows from Proposition 3.25. Point (iii) is obvious. \(\square\)

**Remark 3.4** Although we will not need it, results of Yoo show that \((M' / p^r M')[I_2^2] = \mathbb{Z} / p^r \mathbb{Z} \cdot e_0^2 \oplus \mathbb{Z} / p^r \mathbb{Z} \cdot e_1^2.\)

We have not been able to conjecture any explicit formula for the higher Eisenstein elements corresponding to \(I_0\) and \(I_1\). We have no conjecture for the analogous element \(e_2^2\) annihilated by \(I_2^3\) (when it exists, i.e. when \(n(r) \geq 2\)).

The degree of \(e_2^2\) is \(e_1 \cdot e_1\), which is
\[
\frac{1}{24} \cdot \left( \sum_{\lambda \in L} \log(H'(\lambda))^2 \right) - \frac{1}{18} \cdot \left( \sum_{\lambda \in L} \log(\lambda)^2 \right)
\]
if \(p \geq 5\) by Theorem 3.16 (iii).

One idea would be to express \(e_2^2\) in terms of \(\log(H'(\lambda))^2, \log(\lambda)^2, \log(1-\lambda)^2\) or more general quadratic formula in the logarithms of differences of supersingular invariants. More precisely, define the following elements of \(M' / p^r M'\):

(i)
\[
\alpha_1 = \sum_{\lambda \in L} \left( \sum_{\lambda' \in L, \lambda' \neq \lambda} \log(\lambda' - \lambda)^2 \right) \cdot [\lambda]
\]

(ii)
\[
\alpha_2 = \sum_{\lambda \in L} \left( \sum_{\lambda' \neq \lambda, \lambda'' \neq \lambda, \lambda' \neq \lambda''} \log(\lambda' - \lambda) \cdot \log(\lambda'' - \lambda) \right) \cdot [\lambda]
\]

(iii)
\[
\alpha_3 = \sum_{\lambda \in L} \left( \sum_{\lambda' \neq \lambda, \lambda'' \neq \lambda', \lambda \neq \lambda''} \log(\lambda' - \lambda) \cdot \log(\lambda'' - \lambda') \right) \cdot [\lambda]
\]
Then we have checked numerically for $N = 181$ and $p = 5$ that $e_2^2$ modulo $p$ is not a linear combination of the elements $\alpha_i$.

4 Odd modular symbols

4.1 Some notation

We keep the notation of Sects. 1 and 2. Let $r$ be an integer such that $1 \leq r \leq t$. Thus, $p \geq 2$ is a prime such that $p^r$ divides the numerator of $\frac{N-1}{12}$.

If $\Gamma$ is a finite index subgroup of $\text{SL}_2(\mathbb{Z})$, Manin proved [18, Theorem 1.9] that we have a surjection

$$\xi_\Gamma : \mathbb{Z}_p[\Gamma \setminus \text{PSL}_2(\mathbb{Z})] \rightarrow H_1(X_\Gamma, C_\Gamma, \mathbb{Z}_p)$$

such that $\xi_\Gamma(\Gamma \cdot g)$ is the class of the geodesic path $\{g(0), g(\infty)\}$, where $X_\Gamma$ is the compact modular curve associated to $\Gamma$ and $C_\Gamma = \Gamma \setminus \mathbb{P}^1(\mathbb{Q})$ is the set of cusps of $X_\Gamma$. Furthermore, Manin proved that the kernel of $\xi_\Gamma$ is spanned by the sum of the (right) $\sigma$-invariants and $\tau$-invariants, where $\sigma = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $\tau = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \in \text{SL}_2(\mathbb{Z})$. We denote by

$$\partial : H_1(X_\Gamma, C_\Gamma, \mathbb{Z}_p) \rightarrow \mathbb{Z}_p[C_\Gamma]^0$$

the boundary map, sending the class of the geodesic path $\{\alpha, \beta\}$ to $[\Gamma \cdot \beta] - [\Gamma \cdot \alpha]$. 

Springer
If $\Gamma = \Gamma_0(N)$ then we have seen in Sect. 1.3 that there is a bijection $\Gamma_0(N) \backslash \text{PSL}_2(\mathbb{Z}) \sim \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$ given by

$$\Gamma_0(N) \cdot \left( \begin{array}{ll} a & b \\ c & d \end{array} \right) \mapsto [c : d].$$

Since $N$ is prime, we have $C_{\Gamma_0(N)} = \{ \Gamma_0(N) \cdot \infty, \Gamma_0(N) \cdot 0 \}$.

We now consider the case $\Gamma = \Gamma_1(N)$. There is a canonical bijection $\Gamma_1(N) \backslash \text{PSL}_2(\mathbb{Z}) \sim (\mathbb{Z}/N\mathbb{Z})^2 \backslash \{ (0, 0) \}/ \pm 1$ given by

$$\Gamma_1(N) \cdot \left( \begin{array}{ll} a & b \\ c & d \end{array} \right) \mapsto [c, d].$$

where we denote by $[c, d]$ the class of $(c, d)$ in $(\mathbb{Z}/N\mathbb{Z})^2 \backslash \{ (0, 0) \}/ \pm 1$. We sometimes abusively view $[c, d]$ as an element of $\Gamma_1(N) \backslash \text{PSL}_2(\mathbb{Z})$.

Let $C_{\Gamma_1(N)}^0$ (resp. $C_{\Gamma_1(N)}^\infty$) be the set of cusps of $X_1(N)$ above the cusp $\Gamma_0(N) \cdot 0$ (resp. $\Gamma_0(N) \cdot \infty$) of $X_0(N)$ via the quotient map $X_1(N) \rightarrow X_0(N)$.

We have $C_{\Gamma_1(N)} = C_{\Gamma_1(N)}^0 \cup C_{\Gamma_1(N)}^\infty$.

For all prime $\ell$ not dividing $N$, the Hecke operator $T_{\ell} - \ell - \langle \ell \rangle$ (resp. $T_{\ell} - \ell \langle \ell \rangle - 1$) annihilates $C_{\Gamma_1(N)}^\infty$ (resp. $C_{\Gamma_1(N)}^0$), where $\langle \ell \rangle$ is the $\ell$th diamond operator.

The map $(\mathbb{Z}/N\mathbb{Z})^\times / \pm 1 \rightarrow C_{\Gamma_1(N)}^0$ (resp. $(\mathbb{Z}/N\mathbb{Z})^\times / \pm 1 \rightarrow C_{\Gamma_1(N)}^\infty$) given by $u \mapsto \langle u \rangle \cdot (\Gamma_1(N) \cdot 0)$ (resp. $u \mapsto \langle u \rangle \cdot (\Gamma_1(N) \cdot \infty)$) is a bijection. If $u \in (\mathbb{Z}/N\mathbb{Z})^\times / \pm 1$, we denote by $[u]_{\Gamma_1(N)}^0$ (resp. $[u]_{\Gamma_1(N)}^\infty$) the image of $u$ in $C_{\Gamma_1(N)}^0$ (resp. $C_{\Gamma_1(N)}^\infty$). In other words, we have $[u]_{\Gamma_1(N)}^0 = \Gamma \cdot \frac{c}{d}$ for some coprime integers $c$ and $d$ not divisible by $N$, and such that the image of $d$ in $(\mathbb{Z}/N\mathbb{Z})^\times / \pm 1$ is $u$. Similarly, $[u]_{\Gamma_1(N)}^\infty = \Gamma_1(N) \cdot \frac{a}{N \cdot \bar{b}}$ for some coprime integers $a$ and $b$ not divisible by $N$, and such that the image of $a$ in $(\mathbb{Z}/N\mathbb{Z})^\times / \pm 1$ is $u^{-1}$.

Let $\left( \begin{array}{ll} a & b \\ c & d \end{array} \right) \in \text{SL}_2(\mathbb{Z})$. We describe $\partial(\xi_{\Gamma_1(N)}([c, d]))$ in the various cases that can happen.

- If $c \equiv 0$ (modulo $N$) then $a \equiv d^{-1}$ (modulo $N$). Thus, we have $\partial(\xi_{\Gamma_1(N)}([c, d])) = [d]_{\Gamma_1(N)}^\infty - [d]_{\Gamma_1(N)}^0$.
- If $d \equiv 0$ (modulo $N$) then we have $b \equiv -c^{-1}$ (modulo $N$). Thus, we have $\partial(\xi_{\Gamma_1(N)}([c, d])) = [c]_{\Gamma_1(N)}^0 - [c]_{\Gamma_1(N)}^\infty$.
- If $c \cdot d \not\equiv 0$ (modulo $N$) then we have $\partial(\xi_{\Gamma_1(N)}([c, d])) = [c]_{\Gamma_1(N)}^0 - [d]_{\Gamma_1(N)}^0$. 

\( \odot \) Springer
4.2 Odd and even modular symbols

Let \( M^- = H_1(Y_0(N), \mathbb{Z}_p)^- \) (resp. \( H^- = H_1(X_0(N), \mathbb{Z}_p)^- \)) be the largest torsion-free quotient of \( H_1(Y_0(N), \mathbb{Z}_p) \) (resp. \( H_1(X_0(N), \mathbb{Z}_p) \)) anti-invariant by the complex conjugation. Let \( M^+ = H_1(X_0(N), \text{cusps}, \mathbb{Z}_p)^+ \) (resp. \( H^+ = H_1(X_0(N), \mathbb{Z}_p)^+ \)) be the subspace of \( H_1(X_0(N), \text{cusps}, \mathbb{Z}_p) \) (resp. \( H_1(X_0(N), \mathbb{Z}_p) \)) fixed by the complex conjugation.

The intersection product induces perfect \( \mathbb{T} \)-equivariant pairings:

\[
\bullet : M^+ \times M^- \to \mathbb{Z}_p
\]

and

\[
\bullet : H^+ \times H^- \to \mathbb{Z}_p.
\]

In order to apply the theory of higher Eisenstein elements as in Sect. 2, we need to check the hypotheses of Theorem 2.1 as a variant of Mazur’s well-known result [19, Proposition II.18.3].

**Proposition 4.1** The \( \mathbb{T}_\mathbb{Q}_p \)-modules \( M_+ \otimes_{\mathbb{T}} \mathbb{T}_\mathbb{Q}_p \) and \( M^- \otimes_{\mathbb{T}} \mathbb{T}_\mathbb{Q}_p \) are free of rank 1.

**Proof** Since \( M_+ \) and \( M^- \) are dual \( \mathbb{T} \)-modules, it suffices to prove that \( M_+ \otimes_{\mathbb{T}} \mathbb{T}_\mathbb{Q}_p \) is free of rank one over \( \mathbb{T}_\mathbb{Q}_p \) (dual and tensorization by \( \mathbb{T}_\mathbb{Q}_p \) commute by Lemma 2.2). By [19, Proposition II.18.3], \( H_+ \otimes_{\mathbb{T}_0} \mathbb{T}_\mathbb{Q}_p^0 \) is free of rank one over \( \mathbb{T}_\mathbb{Q}_p^0 \). We now prove that this implies that \( M_+ \otimes_{\mathbb{T}} \mathbb{T}_\mathbb{Q}_p \) is free of rank one over \( \mathbb{T}_\mathbb{Q}_p \). Consider the exact sequence of \( \mathbb{Z}_p \)-modules

\[
0 \to H_+ \to M_+ \xrightarrow{\pi} \mathbb{Z}_p \to 0, \tag{40}
\]

where the map \( \pi \) sends \( \{0, \infty\} \) to 1. It is a \( \mathbb{T} \)-equivariant exact sequence if we identify \( \mathbb{Z}_p \) with \( \mathbb{T}/I \) with its obvious \( \mathbb{T} \)-module structure. By Lemma 2.2, \( \mathbb{T}_\mathbb{Q}_p \) is flat over \( \mathbb{T} \). Thus, (40) gives an exact sequence of \( \mathbb{T}_\mathbb{Q}_p \)-modules

\[
0 \to H_+ \otimes_{\mathbb{T}_0} \mathbb{T}_\mathbb{Q}_p^0 \to M_+ \otimes_{\mathbb{T}} \mathbb{T}_\mathbb{Q}_p \xrightarrow{\pi'} \mathbb{T}_\mathbb{Q}_p/I \cdot \mathbb{T}_\mathbb{Q}_p \to 0. \tag{41}
\]

We claim that the map \( e : \mathbb{T}_\mathbb{Q}_p \to M_+ \otimes_{\mathbb{T}} \mathbb{T}_\mathbb{Q}_p \) given by \( T \mapsto \{0, \infty\} \otimes T \) is an isomorphism of \( \mathbb{T}_\mathbb{Q}_p \)-modules. This follows from (41), using the fact that \( \pi' (\{0, \infty\} \otimes T) \) is the image of \( T \) in \( \mathbb{T}_\mathbb{Q}_p/I \cdot \mathbb{T}_\mathbb{Q}_p \) and the fact that the restriction of \( e \) to \( I \cdot \mathbb{T}_\mathbb{Q}_p \) gives an isomorphism of \( \mathbb{T}_\mathbb{Q}_p^0 \)-modules \( I \cdot \mathbb{T}_\mathbb{Q}_p \to H_+ \otimes_{\mathbb{T}} \mathbb{T}_\mathbb{Q}_p \). The latter fact comes from [19, Theorem II.18.10] and the fact that the map \( I \to I^0 \) is an isomorphism of \( \mathbb{T} \)-modules (cf. the proof of Proposition 2.6). □
Thus, Theorem 2.1 holds for $M^-$ and $M_+$. Recall (cf. Sect. 1.3) that we have denoted by $m_0^\circ, m_1^\circ, \ldots, m_{n(r)}^\circ$ a system of higher Eisenstein elements in $M^- / p^r M^-$. Recall also that we have fixed an element $\tilde{m}_0^\circ \in M^-[I]$ reducing to $m_0^\circ$ modulo $p^r$, such that $\{0, \infty\} \cdot \tilde{m}_0^\circ = -1$. The kernel of the map $M^- \to H^-$ is $\mathbb{Z}_p \cdot \tilde{m}_0^\circ$. If $i \in \{1, \ldots, n(r)\}$, we denote by $\tilde{m}_i^\circ$ the image of $m_i^\circ$ in $H^-$. Since $m_1^\circ$ is uniquely defined modulo the subgroup generated by $m_0^\circ$, the element $\tilde{m}_1^\circ$ is uniquely defined and is annihilated by the Eisenstein ideal $I$.

As we explained in Sect. 1.3, our point of view in this section is cohomological i.e. we consider $\tilde{m}_1^\circ$ as an element of $\text{Hom}(H_+ / I \cdot H_+, \mathbb{Z} / p^r \mathbb{Z})$ by intersection duality. The element $\tilde{m}_1^\circ$ was essentially determined by Mazur [19, II.18.8] (although it was not formulated in this way). The $\mathbb{Z}_p$-module $H_1(X_0(N), \mathbb{Z}_p)$ is generated by the element $\xi_{\Gamma_0(N)}([x : 1])$ for $x \in (\mathbb{Z} / N \mathbb{Z})^\times$ [23, Proposition 3]. The group $H_1(X_0(N), \mathbb{Z}_p)$ is acyclic for the complex conjugation [23, Proposition 5]. In particular, we have $H_+ = (1 + c) \cdot H_1(X_0(N), \mathbb{Z}_p)$, where $c$ is the complex conjugation. Thus, the element $\tilde{m}_1^\circ$ is uniquely determined by its pairing with $(1 + c) \cdot \xi_{\Gamma_0(N)}([x : 1])$ (also denoted by $(x : 1)$) for $x \in (\mathbb{Z} / N \mathbb{Z})^\times$. This pairing was essentially computed by Mazur [19, II.18.8] (although Mazur does not take into account the complex conjugation).

**Theorem 4.2** For all $x \in (\mathbb{Z} / N \mathbb{Z})^\times$, we have in $\mathbb{Z} / p^r \mathbb{Z}$:

$$\langle x : 1 \rangle \cdot m_1^\circ = \log(x).$$

**Proof** We easily check that there is a unique group homomorphism $f : H_+ \to \mathbb{Z} / p^r \mathbb{Z}$ such that for all $x \in (\mathbb{Z} / N \mathbb{Z})^\times$, we have $f((x : 1)) = \log(x)$. We easily see (cf. [19, II.18.8]) that the map $f$ annihilates $I \cdot H_+$. Let $\ell$ be a prime not dividing $2 \cdot N$. A simple computation shows that we have, in $H_+$:

$$(T_\ell - \ell - 1)(\{0, \infty\}) = -(1 + c) \cdot \sum_{i=1}^{\ell-1} \{0, \frac{i}{\ell}\}.$$ 

Thus, we have in $\mathbb{Z} / p^r \mathbb{Z}$:

$$f((T_\ell - \ell - 1)(\{0, \infty\})) = \frac{\ell - 1}{2} \cdot \log(\ell) \cdot (\{0, \infty\} \cdot m_0^\circ)$$

$$= ((T_\ell - \ell - 1)(\{0, \infty\})) \cdot m_1^\circ.$$ 

The elements $(T_\ell - \ell - 1)(\{0, \infty\})$ generate $H_+ / I \cdot H_+$ when $\ell$ goes through the primes not dividing $2 \cdot N$ [19, II.18.10]. Thus, for all $x \in (\mathbb{Z} / N \mathbb{Z})^\times$ we have $f(x) = \langle x : 1 \rangle \cdot m_1^\circ$. This concludes the proof of Theorem 4.2. □
Remark 4.1 Let $f : H_+ \rightarrow A$ where $A$ is an abelian group. By intersection duality, $f$ corresponds to an element $\hat{f} \in H_1(X_0(N), A)$. Merel gave a formula for $\hat{f}$ in terms of Manin symbols (cf. Lemma 5.4 for the case where $3$ is invertible in $A$). This allows us to compute $\overline{m}_1$ in terms of Manin symbols.

If $p \neq 3$ the formula is given in Lemma 5.2 (i).

5 Even modular symbols

In this section, unless explicitly stated, we allow $p = 2$ and $p = 3$. We keep the notation of Sects. 1, 2 and 4. We assume as usual that $p$ divides the numerator of $N - 1$. We let $v$ be the $p$-adic valuation of $N - 1$. We extend log to a group homomorphism $((\mathbb{Z}/N\mathbb{Z})^{\times} \rightarrow \mathbb{Z}/\mathbb{Z})$ (still abusively denoted by log).

Recall that in Theorem 1.9, we defined an element $\tilde{m}_0^+ \in H_1(X_0(N), \text{cusps}, \mathbb{Q})$ (independent of the choice of $p$). We have, in fact, $\tilde{m}_0^+ \in H_1(X_0(N), \text{cusps}, \mathbb{Z}_p)$ even if when $p \in \{2, 3\}$ the formula defining $F_{0,p}$ is not $p$-integral. We fix this choice of $\tilde{m}_0^+$ for the rest of the paper.

Let $r$ be an integer such that $1 \leq r \leq t$. We denote by $m_{0}^+, \ldots, m_{n(r)}^+$ a system of higher Eisenstein elements in $M_+/p^r M_+$, where $m_{0}^+$ is the image of $\tilde{m}_0^+$ in $M_+/p^r M_+$.

In this section, we give an explicit formula for $m_{1}^+$ modulo $p^r$ if $p \geq 3$, and a formula for $m_{1}^+$ modulo $p^{t-1}$ if $t \geq 2$ and $p = 2$. In particular, we prove Theorem 1.10. The formula when $p = 5$ (resp. $p = 3$, resp. $p = 2$) is given in Theorem 5.10 (resp. Theorem 5.20, resp. Theorem 5.22).

5.1 Main idea

We briefly expose the main idea for computing $m_{1}^+$. Using a result of Banerjee and Merel (cf. Theorem 5.6), we compute explicitly two elements

$$\mathcal{E}_0, \mathcal{E}_\infty \in H_1(X_1(N), \text{cusps}, \mathbb{C}[((\mathbb{Z}/N\mathbb{Z})^{\times} \rightarrow \mathbb{Z})])$$

such that for all primes $\ell \neq N$, we have $T_\ell(\mathcal{E}_0) = (\ell[\ell] + 1)(\mathcal{E}_0)$ and $T_\ell(\mathcal{E}_\infty) = (\ell + [\ell])(\mathcal{E}_\infty)$ (cf. (46) and (47)). These are the analogues of (2) and (4) respectively. This allows us to compute $m_{1}^+$ using a similar idea as in Sect. 1.1. In Sect. 5.2, we develop tools to pass from diamond-invariant modular symbols for $\Gamma_1(N)$ to modular symbols for $\Gamma_0(N)$ (the main difficulties occur for the prime $p = 2$).
5.2 Some results about the homology of $X_0(N)$ and $X_1(N)$

In this paragraph, we gather some useful results about the homology of $X_0(N)$ and $X_1(N)$.

**Proposition 5.1** Let $n \geq 1$ be an integer.

(i) The inclusion $M_+ \hookrightarrow H_1(X_0(N), \text{cusps}, \mathbb{Z}_p)$ gives a $\mathbb{T}$-equivariant group isomorphism

$$M_+/p^nM_+ \cong H_1(X_0(N), \text{cusps}, \mathbb{Z}/p^n\mathbb{Z})_+ .$$

(ii) The surjection $H_1(Y_0(N), \mathbb{Z}_p) \twoheadrightarrow M^-$ gives a $\mathbb{T}$-equivariant group isomorphism

$$H_1(Y_0(N), \mathbb{Z}/p^n\mathbb{Z})^- \cong M^-/p^nM^- .$$

**Proof** Point (ii) follows from point (i) by intersection duality. Thus, we only need to prove (i). The multiplication by $p^n$ gives an exact sequence of $\mathbb{T}$-modules

$$0 \rightarrow H_1(X_0(N), \text{cusps}, \mathbb{Z}_p) \xrightarrow{p^n} H_1(X_0(N), \text{cusps}, \mathbb{Z}_p) \rightarrow 0 .$$

There is an action of $\mathbb{Z}/2\mathbb{Z}$ on each of the groups involved in (42), given by the complex conjugation. Furthermore, (42) is $\mathbb{Z}/2\mathbb{Z}$-equivariant. The long exact sequence of cohomology associated to $\mathbb{Z}/2\mathbb{Z}$ yields an exact sequence:

$$0 \rightarrow M_+ \xrightarrow{p^n} M_+ \rightarrow H_1(X_0(N), \text{cusps}, \mathbb{Z}/p^n\mathbb{Z})_+ \rightarrow H^1(\mathbb{Z}/2\mathbb{Z}, H_1(X_0(N), \text{cusps}, \mathbb{Z}_p)) [p^n] .$$

We have a $\mathbb{Z}/2\mathbb{Z}$-equivariant exact sequence

$$0 \rightarrow H_1(X_0(N), \mathbb{Z}_p) \rightarrow H_1(X_0(N), \text{cusps}, \mathbb{Z}_p) \rightarrow \mathbb{Z}_p \rightarrow 0 ,$$

where the action of $\mathbb{Z}/2\mathbb{Z}$ on $\mathbb{Z}_p$ is trivial. The long exact sequence in cohomology yields an exact sequence

$$H^1(\mathbb{Z}/2\mathbb{Z}, H_1(X_0(N), \mathbb{Z}_p)) \rightarrow H^1(\mathbb{Z}/2\mathbb{Z}, H_1(X_0(N), \text{cusps}, \mathbb{Z}_p)) \rightarrow H^1(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}_p) .$$

We have $H^1(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}_p) = 0$ and $H^1(\mathbb{Z}/2\mathbb{Z}, H_1(X_0(N), \mathbb{Z}_p)) = 0$ [23, Proposition 5]. Thus, we have $H^1(\mathbb{Z}/2\mathbb{Z}, H_1(X_0(N), \text{cusps}, \mathbb{Z}_p)) = 0$, which concludes the proof of Proposition 5.1 by (43).
Thus, we will abuse notation and write $H_1(X_0(N), \text{cusps}, \mathbb{Z}/p^n \mathbb{Z})_+$ (resp. $H_1(Y_0(N), \mathbb{Z}/p^n \mathbb{Z})^-$) for $M_+/p^n M_+$ (resp. $M^-/p^n M^-$).

Let $\pi : X_1(N) \to X_0(N)$ be the standard degeneracy map. This produces by pull-back and push-forward two maps

$$\pi^* : H_1(X_0(N), \text{cusps}, \mathbb{Z}) \to H_1(X_1(N), \text{cusps}, \mathbb{Z})$$

and

$$\pi_* : H_1(X_1(N), \text{cusps}, \mathbb{Z}) \to H_1(X_0(N), \text{cusps}, \mathbb{Z}).$$

We will freely abuse notation and still denote the pull-back and pushforward maps for different coefficient rings than $\mathbb{Z}$ by $\pi^*$ and $\pi_*$. 

**Proposition 5.2** (i) For any integer $n \geq 1$, the kernel of $\pi^* : H_1(X_0(N), \text{cusps}, \mathbb{Z}/p^n \mathbb{Z}) \to H_1(X_1(N), \text{cusps}, \mathbb{Z}/p^n \mathbb{Z})$ is cyclic of order $p \min(n, t)$, annihilated by the Eisenstein ideal $I$ and by $1 + c$ where $c$ is the complex conjugation. If $p \neq 3$, a generator of this kernel is $p \max(n-t, 0) \cdot \mathcal{E}_p^-$, where

$$\mathcal{E}_p^- := \frac{1}{3} \cdot \sum_{x \in \mathcal{R}, x \sim [1:1]} \log \left( \frac{x+1}{x-1} \right) \cdot \xi_{\Gamma_0(N)}(x) \in H_1(X_0(N), \mathbb{Z}/p^t \mathbb{Z}).$$

Here, $\mathcal{R}$ is the set of equivalences classes in $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$ for the equivalence relation $[c : d] \sim [-d : c]$.

(ii) If $p \geq 3$, then for any integer $n \geq 1$, the pull-back map

$$M_+/p^n M_+ \to H_1(X_1(N), \text{cusps}, \mathbb{Z}/p^n \mathbb{Z})$$

is injective.

(iii) For any integer $n \geq 1$, the kernel of the pull-back map

$$M_+/2^n M_+ \to H_1(X_1(N), \text{cusps}, \mathbb{Z}/2^n \mathbb{Z})$$

is spanned by the reduction of $2^{n-1} \cdot \tilde{m}_0^+ \mod 2^n$.

**Proof** We prove (i). Let $U = (\mathbb{Z}/N\mathbb{Z})^\times /\mu_{12}$, where $\mu_{12}$ is the 12-torsion subgroup of $(\mathbb{Z}/N\mathbb{Z})^\times$. We have a commutative diagram whose rows are exact
and whose vertical maps are surjective:

\[ \begin{align*}
\Gamma_1(N) & \rightarrow \Gamma_0(N) \rightarrow (\mathbb{Z}/N\mathbb{Z})^\times \rightarrow 0 \\
\gamma \mapsto \{z_1, \gamma(z_1)\} & \rightarrow \{z_0, \gamma(z_0)\}
\end{align*} \tag{44} \]

where \( z_1 \in Y_1(N) \) (resp. \( z_0 \in Y_0(N) \)) is any fixed point. The complex conjugation acts on \( \Gamma_0(N) \) via

\[ \left( \begin{array}{cc} a & b \\ c & d \end{array} \right) \mapsto \left( \begin{array}{cc} -1 & 0 \\ 0 & 1 \end{array} \right) \left( \begin{array}{cc} a & b \\ c & d \end{array} \right) \left( \begin{array}{cc} -1 & 0 \\ 0 & 1 \end{array} \right) = \left( \begin{array}{cc} -b & a \\ -c & d \end{array} \right). \]

Thus, the map \( \varphi \) is annihilated by \( 1 - c \). The map \( \varphi \) is also annihilated by \( I \) [19, II.18]. By intersection duality, we get an exact sequence

\[ 0 \rightarrow \text{Hom}(U, \mathbb{Z}/p^n\mathbb{Z}) \rightarrow H_1(X_0(N), \text{cusps}, \mathbb{Z}/p^n\mathbb{Z}) \rightarrow \pi^* H_1(X_1(N), \text{cusps}, \mathbb{Z}/p^n\mathbb{Z}). \]

The intersection duality is Hecke equivariant and changes the sign for the complex conjugation. This proves the first assertion of (i). The map \( \varphi : H_1(Y_0(N), \mathbb{Z}) \rightarrow U \) corresponds by intersection duality to an element \( \mathcal{E}^- \) of \( H_1(X_0(N), \text{cusps}, U) \), which is a generator of the kernel of \( \pi^* : H_1(X_0(N), \text{cusps}, U) \rightarrow H_1(X_1(N), \text{cusps}, U) \). The following general result, essentially due to Merel [22] and Rebolledo [26], allows us to compute \( \mathcal{E}^- \) in terms of Manin symbols.

**Lemma 5.3** Let \( \Gamma \) be any finite index subgroup of \( \text{SL}_2(\mathbb{Z}) \). Let \( A \) be an abelian group in which \( 3 \) is invertible. Let \( f : H_1(X_\Gamma, C_\Gamma, \mathbb{Z}) \rightarrow A \) be a group homomorphism and \( \hat{f} \in H_1(Y_\Gamma, A) \) be the element corresponding to \( f \) by intersection duality. Let \( R_\Gamma \) be the set of equivalence classes in \( \Gamma \backslash \text{PSL}_2(\mathbb{Z}) \) for the equivalence relation \( \Gamma \cdot g \sim \Gamma \cdot g \cdot \sigma \). The image of \( \hat{f} \) in \( H_1(X_\Gamma, A) \) is

\[
\sum_{\Gamma \cdot g \in R_\Gamma} f(\xi_\Gamma(\Gamma \cdot g)) \cdot \xi_\Gamma(\Gamma \cdot g) + \frac{1}{3} \sum_{\Gamma \cdot g \in \Gamma \backslash \text{PSL}_2(\mathbb{Z})} (2 \cdot f(\xi_\Gamma(\Gamma \cdot g \cdot \tau)) + f(\xi_\Gamma(\Gamma \cdot g \cdot \tau^2))) \cdot \xi_\Gamma(\Gamma \cdot g). 
\]

**Proof** We follow the notation of [22, Section 1]. Note that Merel assumes that \( \left( \begin{array}{cc} -1 & 0 \\ 0 & -1 \end{array} \right) \in \Gamma \), but he uses the coset \( \Gamma \backslash \text{SL}_2(\mathbb{Z}) \). Since we have \( \Gamma \backslash \text{SL}_2(\mathbb{Z}) = \Gamma \backslash \text{PSL}_2(\mathbb{Z}) \), this assumption of \( \Gamma \) is not important. Let \( \mathfrak{H} \) be the upper-half
plane and $\pi : \mathbb{H} \cup \mathbb{D}^1(\mathbb{Q}) \to X_\Gamma$ be the canonical surjection. Let $\rho = e^{\frac{2\pi i}{3}}$ and $\delta$ be the geodesic path between $i$ and $\rho$. Let $R = \pi(\text{SL}_2(\mathbb{Z}) \cdot \rho)$ and $I = \pi(\text{SL}_2(\mathbb{Z}) \cdot i)$. These sets are disjoints. If $\Gamma \cdot g \in \Gamma \setminus \text{PSL}_2(\mathbb{Z})$, let $\xi_1^\prime(\Gamma \cdot g)$ be the class of $\pi(g \cdot \delta)$ in $H_1(Y_\Gamma, R \cup I, \mathbb{Z})$. Let $f^\prime : H_1(X_\Gamma - (R \cup I), \text{cusp}, \mathbb{Z}) \to A$ be the composition $f$ with the canonical map $H_1(X_\Gamma - (R \cup I), \text{cusp}, \mathbb{Z}) \to H_1(X_\Gamma, \text{cusp}, \mathbb{Z})$. By intersection duality, $f^\prime$ corresponds to an element $\hat{f}^\prime \in H_1(Y_\Gamma, R \cup I, A)$. By [22, Proposition 1], we have
\[ \hat{f}^\prime = \sum_{g \cdot \Gamma \in \Gamma \setminus \text{PSL}_2(\mathbb{Z})} f(\xi_1^\prime(\Gamma \cdot g)-\xi_1^\prime(\Gamma \cdot g)) \cdot \xi_1^\prime(\Gamma \cdot g). \] (45)
We have $\hat{f}^\prime \in H_1(Y_\Gamma, A)$ since $f^\prime$ factors through $H_1(X_\Gamma, \text{cusp}, \mathbb{Z})$. Consider the image $\hat{f}''$ of $\hat{f}^\prime$ in $H_1(X_\Gamma, R \cup I, A)$. We have $\hat{f}'' \in H_1(X_\Gamma, A)$.

**Lemma 5.4** Let
\[ x = \sum_{\Gamma \cdot g \in \Gamma \setminus \text{PSL}_2(\mathbb{Z})} \lambda_{\Gamma \cdot g} \cdot \xi_1^\prime(\Gamma \cdot g) \in H_1(X_\Gamma, R \cup I, A). \]
Assume that $x \in H_1(X_\Gamma, A)$. We have, in $H_1(X_\Gamma, \text{cusp}, A)$:
\[ x = \sum_{\Gamma \cdot g \in \mathcal{R}_\Gamma} \lambda_{\Gamma \cdot g} \cdot \xi_1(\Gamma \cdot g) + \frac{1}{3} \sum_{\Gamma \cdot g \in \Gamma \setminus \text{PSL}_2(\mathbb{Z})} (2 \cdot \lambda_{\Gamma \cdot g} \cdot \tau + \lambda_{\Gamma \cdot g} \cdot \tau^2) \cdot \xi_1(\Gamma \cdot g). \]

**Proof** For simplicity, we write $\lambda_g$ for $\lambda_{\Gamma \cdot g}$. We have in $H_1(X_\Gamma, \text{cusp} \cup R \cup I, A)$:
\[
\begin{align*}
x &= \sum_{\Gamma \cdot g \in \Gamma \setminus \text{PSL}_2(\mathbb{Z})} \lambda_g \cdot \{g(i), g(\rho)\} \\
&= \sum_{\Gamma \cdot g \in \Gamma \setminus \text{PSL}_2(\mathbb{Z})} \lambda_g \cdot \{g(i), g(\infty)\} - \sum_{\Gamma \cdot g \in \Gamma \setminus \text{PSL}_2(\mathbb{Z})} \lambda_g \cdot \{g(\rho), g(\infty)\} \\
&= \sum_{\Gamma \cdot g \in \mathcal{R}_\Gamma} \left(\lambda_g \cdot \{g(i), g(\infty)\} + \lambda_{g \cdot \sigma} \cdot \{g \cdot \sigma(i), g \cdot \sigma(\infty)\}\right) \\
- \frac{1}{3} \sum_{\Gamma \cdot g \in \Gamma \setminus \text{PSL}_2(\mathbb{Z})} \left(\lambda_g \cdot \{g(\rho), g(\infty)\} + \lambda_{g \cdot \tau} \cdot \{g \cdot \tau(\rho), g \cdot \tau(\infty)\}\right) \\
+ \lambda_{g \cdot \tau^2} \cdot \{g \cdot \tau^2(\rho), g \cdot \tau^2(\infty)\} \\
&= \sum_{\Gamma \cdot g \in \mathcal{R}_\Gamma} \left(\lambda_g \cdot \{g(i), g(\infty)\} + \lambda_{g \cdot \sigma} \cdot \{g \cdot \sigma(i), g \cdot \sigma(\infty)\}\right).
\end{align*}
\]
\[ -\frac{1}{3} \sum_{\Gamma \cdot g \in \Gamma \backslash \text{PSL}_2(\mathbb{Z})} \left( \lambda_g \cdot \{g(\rho), g(\infty)\} \right) \]

\[ + \lambda_{g \cdot \tau} \cdot \{g \cdot \tau(\rho), g \cdot \tau(\infty)\} + \lambda_{g \cdot \tau^2} \cdot \{g \cdot \tau^2(\rho), g \cdot \tau^2(\infty)\} \].

Note that \(\sigma(i) = i, \sigma(\infty) = 0, \tau(\rho) = \rho\) and \(\tau(\infty) = 0\). Since the boundary of \(x\) is zero, we have \(\lambda_{g \cdot \sigma} = -\lambda_g\) and \(\lambda_g = -\lambda_{g \cdot \tau} - \lambda_{g \cdot \tau^2}\) [22, Théorème 3]. Thus, we have in \(H_1(X_\Gamma, \text{cusps} \cup R \cup I, A)\):

\[ x = \sum_{\Gamma \cdot g \in \mathcal{R}_\Gamma} \lambda_g \cdot \{g(0), g(\infty)\} \]

\[ - \frac{1}{3} \sum_{\Gamma \cdot g \in \Gamma \backslash \text{PSL}_2(\mathbb{Z})} \left( - (\lambda_{g \cdot \tau} + \lambda_{g \cdot \tau^2}) \cdot \{g(\rho), g(\infty)\} \right) \]

\[ + \lambda_{g \cdot \tau} \cdot \{g(\rho), g(0)\} + \lambda_{g \cdot \tau^2} \cdot \{g(\rho), g \cdot \tau(0)\} \]

\[ = \sum_{\Gamma \cdot g \in \mathcal{R}_\Gamma} \lambda_g \cdot \{g(0), g(\infty)\} \]

\[ - \frac{1}{3} \sum_{\Gamma \cdot g \in \Gamma \backslash \text{PSL}_2(\mathbb{Z})} \lambda_{g \cdot \tau} \cdot \{g(\infty), g(0)\} + \lambda_{g \cdot \tau^2} \cdot \{g(\infty), g \cdot \tau(0)\} .\]

We have:

\[ \{g(\infty), g \cdot \tau(0)\} = \{g(\infty), g \cdot \tau(\infty)\} + \{g \cdot \tau(\infty), g \cdot \tau(0)\} \]

\[ = -\{g(0), g(\infty)\} - \{g \cdot \tau(0), g \cdot \tau(\infty)\} .\]

Thus, we have:

\[ x = \sum_{\Gamma \cdot g \in \mathcal{R}_\Gamma} \lambda_g \cdot \{g(0), g(\infty)\} \]

\[ + \frac{1}{3} \sum_{\Gamma \cdot g \in \Gamma \backslash \text{PSL}_2(\mathbb{Z})} \lambda_{g \cdot \tau} \cdot \{g(0), g(\infty)\} \]

\[ + \frac{1}{3} \sum_{\Gamma \cdot g \in \Gamma \backslash \text{PSL}_2(\mathbb{Z})} \lambda_{g \cdot \tau^2} \cdot \{g(0), g(\infty)\} \]

\[ + \frac{1}{3} \sum_{\Gamma \cdot g \in \Gamma \backslash \text{PSL}_2(\mathbb{Z})} \lambda_{g \cdot \tau} \cdot \{g(0), g(\infty)\} .\]

This concludes the proof of Lemma 5.4. \(\square\)

This concludes the proof of Lemma 5.3. \(\square\)
We identify $H_1(X_0(N), \text{cusps}, U)$ with $H_1(X_0(N), \text{cusps}, \mathbb{Z}) \otimes \mathbb{Z} U$. The homomorphism $\varphi : H_1(Y_0(N), \mathbb{Z}) \to U$ induces a map $\varphi' : H_1(X_0(N), \mathbb{Z}) \to U$. It is given by

$$
\varphi' \left( \xi_{\Gamma_0(N)} \left( \Gamma_0(N) \cdot \left( \begin{array}{cc} a & b \\ c & d \end{array} \right) \right) \right) = \overline{c} \cdot \overline{d}^{-1},
$$

where $\gcd(c, N) = \gcd(d, N) = 1$ and if $x \in \mathbb{Z}$ is prime to $N$, then $\overline{x}$ is the image of $x$ in $U$. By Lemma 5.3, we have in $H_1(X_0(N), \text{cusps}, \mathbb{Z}) \otimes \mathbb{Z} U$:

$$
\mathcal{E}^- = \sum_{x \in \mathcal{E}, x \sim \infty} \xi_{\Gamma_0(N)}(x) \otimes \overline{x} + \frac{1}{3} \cdot \sum_{x \in \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z}), x \neq 0, \infty, 1, -1} \xi_{\Gamma_0(N)}(x) \otimes \frac{1}{x \cdot (x - 1)}
$$

$$
= \frac{1}{3} \cdot \sum_{x \in \mathcal{E}, x \sim \infty, 1} \xi_{\Gamma_0(N)}(x) \otimes \frac{x + 1}{x - 1}.
$$

This concludes the proof of point (i).

Point (ii) is an immediate consequence of point (i). We now prove point (iii). We have $\varphi((1 + c) \cdot H_1(Y_0(N), \mathbb{Z})) = U^2$, where $U^2$ is the subgroup of squares in $U$. We have an exact sequence:

$$
H_1(Y_1(N), \mathbb{Z}) \to H_1(Y_0(N), \mathbb{Z})/(1 + c) \cdot H_1(Y_0(N), \mathbb{Z}) \to U/U^2 \to 0.
$$

Let $H_1(Y_0(N), \mathbb{Z})^{-}$ (resp. $H_1(Y_1(N), \mathbb{Z})^{-}$) be the largest torsion-free quotient of $H_1(Y_0(N), \mathbb{Z})$ (resp. $H_1(Y_1(N), \mathbb{Z})$) annihilated by $1 + c$.

**Lemma 5.5** The kernel of the map $H_1(Y_0(N), \mathbb{Z}) \to H_1(Y_0(N), \mathbb{Z})^{-}$ is $(1 + c) \cdot H_1(Y_0(N), \mathbb{Z})$ where $c$ is the complex conjugation.

**Proof** The kernel of the map $H_1(X_0(N), \mathbb{Z}) \to H_1(X_0(N), \mathbb{Z})^{-}$ is $(1 + c) \cdot H_1(Y_0(N), \mathbb{Z})$ by [23, Proposition 5]. We have an exact sequence

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

Since the cusps are fixed by the complex conjugation, this gives on the plus subspaces an exact sequence:

$$
0 \to H_1(X_0(N), \mathbb{Z})_+ \to H_1(X_0(N), \text{cusps}, \mathbb{Z})_+ \to \mathbb{Z} \to 0.
$$
By intersection duality, we get a commutative diagram whose rows are exact:

\[
\begin{array}{ccccccccc}
0 & \longrightarrow & \mathbf{Z} & \longrightarrow & H_1(Y_0(N), \mathbf{Z}) & \longrightarrow & H_1(X_0(N), \mathbf{Z}) & \longrightarrow & 0 \\
0 & \longrightarrow & \mathbf{Z} & \longrightarrow & H_1(Y_0(N), \mathbf{Z}^-) & \longrightarrow & H_1(X_0(N), \mathbf{Z}^-) & \longrightarrow & 0 \\
\end{array}
\]

By the snake lemma, the kernel of the map \(H_1(Y_0(N), \mathbf{Z}) \to H_1(Y_0(N), \mathbf{Z}^-)\) is \((1 + c) \cdot H_1(Y_0(N), \mathbf{Z})\).

By Lemma 5.5, we have an exact sequence:

\[
H_1(Y_1(N), \mathbf{Z})^- \to H_1(Y_0(N), \mathbf{Z})^- \to U/U^2 \to 0.
\]

By intersection duality, we have an exact sequence

\[
0 \to \text{Hom}(U/U^2, \mathbf{Z}/2^n\mathbf{Z}) \to M_+/2^n M_+ \to H_1(X_1(N), \text{cusps}, \mathbf{Z}_2)_+ \otimes_{\mathbf{Z}_2} \mathbf{Z}/2^n\mathbf{Z}.
\]

Note that \(H_1(X_1(N), \text{cusps}, \mathbf{Z}_2)_+ \otimes_{\mathbf{Z}_2} \mathbf{Z}/2^n\mathbf{Z}\) is a subgroup of \(H_1(X_1(N), \text{cusps}, \mathbf{Z}_2) \otimes_{\mathbf{Z}_2} \mathbf{Z}/2^n\mathbf{Z}\), which we identify with \(H_1(X_1(N), \text{cusps}, \mathbf{Z}/2^n\mathbf{Z})\). The map \(\varphi: H_1(Y_0(N), \mathbf{Z}) \to U\) is annihilated by the Eisenstein ideal. The map \(H_1(Y_0(N), \mathbf{Z})^- \to U/U^2\) is also annihilated by the Eisenstein ideal. Thus, the image of \(\text{Hom}(U/U^2, \mathbf{Z}/2^n\mathbf{Z})\) in \(M_+/2^n M_+\) has order 2 and is Eisenstein, so is generated by \(2^{n-1} \cdot \tilde{m}_0^+\) modulo \(2^n\).

\(\Box\)

**Remark 5.1** Proposition 5.2 (iii) is another way to express that the Shimura subgroup and the cuspidal subgroup of \(J_0(N)\) intersect at a point of order 2 [19, Proposition II.11.11].

### 5.3 Eisenstein elements of level in \(H_1(X_1(N), \text{cusps}, \mathbf{C})\)

Recall the notation of Sect. 4.1. We denote by \(\Gamma(N)\) the principal congruence subgroup of level \(N\).

Recall that \(\overline{B}_1: \mathbf{R} \to \mathbf{R}\) is such that

\[
\overline{B}_1(x) = x - \lfloor x \rfloor - \frac{1}{2}
\]

if \(x \notin \mathbf{Z}\) and \(\overline{B}_1(x) = 0\) else, where \(\lfloor x \rfloor\) is the integer part of \(x\). Following [23, Sect. 2.2], let \(D_2: \mathbf{R} \to \mathbf{R}\) be given by \(D_2(x) = 2 \cdot (\overline{B}_1(x) - \overline{B}_1(x + \frac{1}{2}))\). It is a periodic function with period 1 such that \(D_2(0) = D_2\left(\frac{1}{2}\right) = 0, D_2(x) = -1\) if \(x \in ]0, \frac{1}{2}[\) and \(D_2(x) = 1\) if \(x \in ]\frac{1}{2}, 1[\).
For the convenience of the reader, we state the main result of [2]. Let $F : (\mathbb{Z}/N\mathbb{Z})^2 \to \mathbb{C}$ be defined by

$$F(x, y) = \sum_{(s_1, s_2) \in (\mathbb{Z}/2N\mathbb{Z})^2} e^{2\pi i (s_1 (x' + y') + s_2 (x' - y'))/2N} \cdot B_1 \left( \frac{s_1}{2N} \right) B_1 \left( \frac{s_2}{2N} \right)$$

where $(x', y') \in (\mathbb{Z}/2N\mathbb{Z})^2$ is a lift of $(x, y)$ such that $x' + y' \equiv 1$ (modulo 2).

We have $F(x, y) = F(-x, -y)$.

Since $N$ is odd, we have canonical identifications

$$\text{SL}_2(\mathbb{Z}/N\mathbb{Z})/\pm 1 \cong \Gamma(N) \setminus \text{PSL}_2(\mathbb{Z}) \cong \pm \Gamma(2N) \setminus \Gamma(2).$$

If $P \in (\mathbb{Z}/N\mathbb{Z})^2$, let

$$\tilde{E}_P = \sum_{\gamma \in \text{SL}_2(\mathbb{Z}/N\mathbb{Z})/\pm 1} F(\gamma^{-1} P) \cdot \xi_{\Gamma(N)}(\gamma) \in H_1(X(N), \text{cusps}, \mathbb{C}).$$

We have $\tilde{E}_P = \tilde{E}_{-P}$. Let $E_P$ be the image of $\tilde{E}_P$ to $H_1(X_1(N), \text{cusps}, \mathbb{C})$. The following result is an easy consequence of the work of Banerjee and Merel [2].

**Theorem 5.6** Let $\ell$ be a prime not dividing $N$. For all $x \in (\mathbb{Z}/N\mathbb{Z})^\times$, we have:

$$T_\ell(E_{(x,0)}) = \ell \cdot E_{(x,0)} + E_{(\ell^{-1}x,0)}$$

and

$$T_\ell(E_{(0,x)}) = \ell \cdot E_{(0,\ell x)} + E_{(0,x)}$$

where $T_\ell$ is the $\ell$th Hecke operator.

**Proof** Let $E_N$ be the $\mathbb{C}$-vector space generated by the elements $E_{(x,0)}$ and $E_{(0,x)}$ for all $x \in (\mathbb{Z}/N\mathbb{Z})^\times / \pm 1$. Recall that $\partial : H_1(X_1(N), \text{cusps}, \mathbb{C}) \to \mathbb{C}[C_{\Gamma_1(N)}]^0$ is the boundary map. Using [2, Corollary 4], we conclude that the restriction of $\partial$ to $E_N$ gives a Hecke-equivariant isomorphism $E_N \cong \mathbb{C}[C_{\Gamma_1(N)}]^0$. Using [2, Theorem 15], we have for all $x \in (\mathbb{Z}/N\mathbb{Z})^\times / \pm 1$:

$$\partial(E_{(x,0)}) = 2N \cdot \left( \sum_{\mu \in (\mathbb{Z}/N\mathbb{Z})^\times} (F(\mu \cdot (1, 0)) + \frac{1}{4} \cdot [((\mu \cdot x)^{-1})_\Gamma_1(N)]^\infty \right)$$

$$- \frac{N}{2} \cdot \left( \sum_{c \in C_{\Gamma_1(N)}^\infty} [c] + N \cdot \sum_{c \in C_{\Gamma_1(N)}^0} [c] \right)$$
Higher Eisenstein elements, higher Eichler formulas

and

\[
\partial(E_{0,x}) = 2N \cdot \left( \sum_{\mu \in (\mathbb{Z}/N\mathbb{Z})^\times} \left( F(\mu \cdot (1,0)) + \frac{1}{4} \cdot [\mu \cdot x]^0_{\Gamma_1(N)} \right) \right)
\]

\[
- \frac{N}{2} \cdot \left( \sum_{c \in C_{\Gamma_1(N)}^\infty} [c] + N \cdot \sum_{c \in C_{\Gamma_1(N)}^0} [c] \right).
\]

Thus, for all prime \( \ell \) not dividing \( N \) we have

\[
\partial(\langle \ell \rangle E_{x,0}) = \langle \ell \rangle \partial(E_{x,0}) = \partial(E_{\ell^{-1}x,0}).
\]

By injectivity of \( \partial \), we have \( \langle \ell \rangle E_{x,0} = E_{\ell^{-1}x,0} \). Similarly, we have \( (T_\ell - \ell - \langle \ell \rangle)(E_{x,0}) = 0 \) since it is true after applying \( \partial \). This proves the first relation of Theorem 5.6. The second relation is proved in a similar way.

The counterparts of the modular forms \( E_{x,1} \) and \( E_{1,\chi} \) of Sect. 1.1 are the following modular symbols

\[
\mathcal{E}_\infty = \sum_{x \in (\mathbb{Z}/N\mathbb{Z})^\times / \{ \pm 1 \}} [x] \cdot E_{x,0} \in H_1(X_1(N), \text{cusps}, \mathbb{C}[((\mathbb{Z}/N\mathbb{Z})^\times / \{ \pm 1 \})]
\]

and

\[
\mathcal{E}_0 = \sum_{x \in (\mathbb{Z}/N\mathbb{Z})^\times / \{ \pm 1 \}} [x]^{-1} \cdot E_{0,x} \in H_1(X_1(N), \text{cusps}, \mathbb{C}[((\mathbb{Z}/N\mathbb{Z})^\times / \{ \pm 1 \})]
\]

As an immediate application of Theorem 5.6, for all prime \( \ell \) not dividing \( N \) we have

\[
(T_\ell - \ell - [\ell])(\mathcal{E}_\infty) = 0 \quad (46)
\]

and

\[
(T_\ell - \ell \cdot [\ell] - 1)(\mathcal{E}_0) = 0 . \quad (47)
\]

Let

\[
\mathcal{E}' = \pi^*(\tilde{m}_0^+) \in H_1(X_1(N), \text{cusps, } \mathbb{Z}_p)
\]

Thus, for all prime \( \ell \) not dividing \( N \) we have

\[
\partial(\langle \ell \rangle E_{x,0}) = \langle \ell \rangle \partial(E_{x,0}) = \partial(E_{\ell^{-1}x,0}).
\]

By injectivity of \( \partial \), we have \( \langle \ell \rangle E_{x,0} = E_{\ell^{-1}x,0} \). Similarly, we have \( (T_\ell - \ell - \langle \ell \rangle)(E_{x,0}) = 0 \) since it is true after applying \( \partial \). This proves the first relation of Theorem 5.6. The second relation is proved in a similar way.

The counterparts of the modular forms \( E_{x,1} \) and \( E_{1,\chi} \) of Sect. 1.1 are the following modular symbols

\[
\mathcal{E}_\infty = \sum_{x \in (\mathbb{Z}/N\mathbb{Z})^\times / \{ \pm 1 \}} [x] \cdot E_{x,0} \in H_1(X_1(N), \text{cusps, } \mathbb{C}[((\mathbb{Z}/N\mathbb{Z})^\times / \{ \pm 1 \})]
\]

and

\[
\mathcal{E}_0 = \sum_{x \in (\mathbb{Z}/N\mathbb{Z})^\times / \{ \pm 1 \}} [x]^{-1} \cdot E_{0,x} \in H_1(X_1(N), \text{cusps, } \mathbb{C}[((\mathbb{Z}/N\mathbb{Z})^\times / \{ \pm 1 \})]
\]

As an immediate application of Theorem 5.6, for all prime \( \ell \) not dividing \( N \) we have

\[
(T_\ell - \ell - [\ell])(\mathcal{E}_\infty) = 0 \quad (46)
\]

and

\[
(T_\ell - \ell \cdot [\ell] - 1)(\mathcal{E}_0) = 0 . \quad (47)
\]

Let

\[
\mathcal{E}' = \pi^*(\tilde{m}_0^+) \in H_1(X_1(N), \text{cusps, } \mathbb{Z}_p)
\]

\[\text{Springer}\]
Lemma 5.7 We have

\[ 6 \cdot \mathcal{E}' = \sum_{[c,d] \in (\mathbb{Z}/N\mathbb{Z})^2 \setminus \{(0,0)\}/\pm 1} \sum_{(s_1,s_2) \in (\mathbb{Z}/2N\mathbb{Z})^2} (-1)^{s_1+s_2} \left( s_1(d-c)+s_2(d+c) \equiv 0 \pmod{N} \right) \]

\[
\bar{B}_1 \left( \frac{s_1}{2N} \right) \bar{B}_1 \left( \frac{s_2}{2N} \right) \cdot \xi \Gamma_1(N) ([c,d])
\]

\[ = \sum_{[c,d] \in (\mathbb{Z}/N\mathbb{Z})^2 \setminus \{(0,0)\}/\pm 1} \sum_{(s_1,s_2) \in (\mathbb{Z}/2N\mathbb{Z})^2} (-1)^{s_1+s_2} \left( s_1(d-c)+s_2(d+c) \not\equiv 0 \pmod{N} \right) \]

\[
\bar{B}_1 \left( \frac{s_1}{2N} \right) \bar{B}_1 \left( \frac{s_2}{2N} \right) \cdot \xi \Gamma_1(N) ([c,d]) .
\]

Proof The first equality follows from the fact that for all \([u : v] \in \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z}) = \Gamma_0(N) \setminus \text{SL}_2(\mathbb{Z}),\) we have

\[ \pi^\ast(\xi \Gamma_0(N) ([u : v])) = \sum_{[c,d] \in (\mathbb{Z}/N\mathbb{Z})^2 \setminus \{(0,0)\}/\pm 1} \xi \Gamma_1(N) ([c,d]) .\]

The second equality follows from the first equality and from the identity

\[ \sum_{(s_1,s_2) \in (\mathbb{Z}/2N\mathbb{Z})^2} (-1)^{s_1+s_2} \bar{B}_1 \left( \frac{s_1}{2N} \right) \bar{B}_1 \left( \frac{s_2}{2N} \right) = \left( \sum_{s \in (\mathbb{Z}/2N\mathbb{Z})^2} (-1)^s \cdot \bar{B}_1 \left( \frac{s}{2N} \right) \right)^2 = 0 . \]

\[ \square \]

Define two maps \(G_\infty, G_0 : \Gamma_1(N) \setminus \text{SL}_2(\mathbb{Z}) \to \mathbb{Z}[\frac{1}{2N}][(\mathbb{Z}/N\mathbb{Z})^\times / \pm 1]\) as follows.

\[ \wedge \text{ Springer} \]
Let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{PSL}_2(\mathbb{Z})$. We define

$$G_\infty(\Gamma_1(N) \cdot \gamma) = \sum_{(s_1, s_2) \in (\mathbb{Z}/2N\mathbb{Z})^2} \sum_{(d-c)s_1 + (d+c)s_2 \not\equiv 0 \pmod{N}} (-1)^{s_1+s_2} B_1 \left( \frac{s_1}{2N} \right) B_1 \left( \frac{s_2}{2N} \right) \cdot [(d - c)s_1 + (d + c)s_2]^{-1}$$

and

$$G_0(\Gamma_1(N) \cdot \gamma) = \sum_{(s_1, s_2) \in (\mathbb{Z}/2N\mathbb{Z})^2} \sum_{(d-c)s_1 + (d+c)s_2 \equiv 0 \pmod{N}} (-1)^{s_1+s_2} B_1 \left( \frac{s_1}{2N} \right) B_1 \left( \frac{s_2}{2N} \right) \cdot [(b - a)s_1 + (b + a)s_2].$$

Let

$$\mathcal{E}_\infty' = \sum_{\Gamma_1(N) \cdot \gamma \in \Gamma_1(N) \backslash \text{PSL}_2(\mathbb{Z})} G_\infty(\Gamma_1(N) \cdot \gamma) \cdot \xi_{\Gamma_1(N)}(\Gamma_1(N) \cdot \gamma) \in H_1(X_1(N), \text{cusps}, \mathbb{Z}[\frac{1}{2N}][\mathbb{Z}/N\mathbb{Z}^\times / \pm 1])$$

and

$$\mathcal{E}_0' = \sum_{\Gamma_1(N) \cdot \gamma \in \Gamma_1(N) \backslash \text{PSL}_2(\mathbb{Z})} G_0(\Gamma_1(N) \cdot \gamma) \cdot \xi_{\Gamma_1(N)}(\Gamma_1(N) \cdot \gamma) \in H_1(X_1(N), \text{cusps}, \mathbb{Z}[\frac{1}{2N}][\mathbb{Z}/N\mathbb{Z}^\times / \pm 1]).$$

The elements $\mathcal{E}_\infty'$ and $\mathcal{E}_0'$ satisfy similar Hecke relations as $\mathcal{E}_\infty$ and $\mathcal{E}_0$ but they have a much simpler description in terms of Manin symbols (there are no exponentials anymore, only Bernoulli polynomials).

**Lemma 5.8** For all prime $\ell$ not dividing $N$, we have

$$(T_\ell - \ell - [\ell])(\mathcal{E}_\infty') = 0$$

and

$$(T_\ell - \ell \cdot [\ell] - 1)(\mathcal{E}_0') = 0.$$
Proof Consider the following two elements of $\mathbf{C}[(\mathbb{Z}/N\mathbb{Z})^\times]/\pm 1$:

$$G = \sum_{x \in (\mathbb{Z}/N\mathbb{Z})^\times} e^{\frac{2i\pi x}{N}} \cdot [x]$$

and

$$\delta = \sum_{x \in (\mathbb{Z}/N\mathbb{Z})^\times} [x].$$

An easy computation shows that we have, in $H_1(X_1(N), \text{cusps}, \mathbf{C}[(\mathbb{Z}/N\mathbb{Z})^\times]/\pm 1)$:

$$\frac{2}{N} \cdot \mathcal{E}_\infty = \sum_{[c,d] \in (\mathbb{Z}/N\mathbb{Z})^2 \setminus [(0,0)]/\pm 1} \xi \Gamma_1(N)([c,d]) \cdot \sum_{x \in (\mathbb{Z}/N\mathbb{Z})^\times} (-1)^{s_1+s_2} \cdot \overline{B}_1 \left( \frac{s_1}{2N} \right) \overline{B}_1 \left( \frac{s_2}{2N} \right) \cdot [2x] \cdot e^{\frac{2i\pi x((d-c)s_1+(d+c)s_2)}{N}}$$

$$= 6 \cdot \delta \cdot \mathcal{E}' + [2] \cdot G \cdot \mathcal{E}'_\infty.$$

The last equality follows from Lemma 5.7. By (46), the operator $T_\ell - \ell - [\ell]$ annihilates $\mathcal{E}_\infty$. Furthermore, $T_\ell - \ell - 1$ annihilates $\mathcal{E}'$ and $[\ell] - 1$ annihilates $\delta$, so $T_\ell - \ell - [\ell]$ annihilates $\delta \cdot \mathcal{E}'$. Thus, $T_\ell - \ell - [\ell]$ annihilates $G \cdot \mathcal{E}'_\infty$.

Lemma 5.9 The element $G$ is not a zero divisor of $\mathbf{C}[(\mathbb{Z}/N\mathbb{Z})^\times]/\pm 1$.

Proof It suffices to prove that if $\alpha : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbf{C}^\times$ is any character such that $\alpha(-1) = 1$, then we have $\sum_{x \in (\mathbb{Z}/N\mathbb{Z})^\times} e^{\frac{2i\pi x}{N}} \cdot \alpha(x) \neq 0$. This is a well-known fact on Gauss sums. \qed

By Lemma 5.9, the operator $T_\ell - \ell - [\ell]$ annihilates $\mathcal{E}'_\infty$, as wanted. The proof that $T_\ell - \ell - [\ell] - 1$ annihilates $\mathcal{E}'_0$ is similar. \qed

Let $\mathcal{U} = \frac{\mathcal{E}'_0 + \mathcal{E}'_\infty}{2} \in H_1(X_1(N), \text{cusps}, \mathbf{Z}[\frac{1}{2N}][(\mathbb{Z}/N\mathbb{Z})^\times]/\pm 1)]$. This is the modular symbol counterpart of (6). Let $J \subset \mathbf{Z}[(\mathbb{Z}/N\mathbb{Z})^\times]/\pm 1]$ be the augmentation ideal. By Lemma 5.7, we have $\mathcal{U} \in J \cdot H_1(X_1(N), \text{cusps}, \mathbf{Z}[\frac{1}{2N}][(\mathbb{Z}/N\mathbb{Z})^\times]/\pm 1)]$. Lemma 5.8 shows that we have

$$(T_\ell - \ell - 1)(\mathcal{U}) = ([\ell] - 1) \cdot \frac{\mathcal{E}'_\infty + \ell \cdot \mathcal{E}'_0}{2}$$

(48)

This is the fundamental equality which allow us to compute $m_1^+$. We will study the cases $p \geq 5$, $p = 3$ and $p = 2$ separately.
5.4 The case \( p \geq 5 \)

The following theorem is a generalization of Theorem 1.10 modulo \( p' \).

**Theorem 5.10** Assume that \( p \geq 5 \). Let \( F_{1,p} : \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z}) \to \mathbb{Z}/p'\mathbb{Z} \) be defined as follows. Let \([c : d] \in \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})\). If \([c : d] \neq [1 : 1]\), let

\[
12 \cdot F_{1,p}([c : d]) = \sum_{(s_1, s_2) \in (\mathbb{Z}/2N\mathbb{Z})^2} \sum_{(d-c)s_1 + (d+c)s_2 \equiv 0 \ (\text{modulo} \ N)} (-1)^{s_1+s_2} B_1 \left( \frac{s_1}{2N} \right) B_1 \left( \frac{s_2}{2N} \right) \cdot \log \left( \frac{s_2}{d-c} \right)
\]

This is independent of the choice of \( c \) and \( d \). Let \( F_{1,p}([1 : 1]) = 0 \). We have:

\[
m_1^+ = \sum_{x \in \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})} F_{1,p}(x) \cdot \xi_{\Gamma_0(N)}(x) \text{ in } \left( \mathbb{M}_+ / p'M_+ \right) / \mathbb{Z} \cdot m_0^+
\]

**Proof** Let \( \beta : J / J^2 \to \mathbb{Z}/p'\mathbb{Z} \) be given by \([x] - 1 \mapsto \log(x)\) for \( x \in (\mathbb{Z}/N\mathbb{Z})^\times \). This induces a map \( \beta_* : J \cdot H_1(X_1(N), \text{cusps}, \mathbb{Z}[\frac{1}{2N}][(\mathbb{Z}/N\mathbb{Z})^\times / \pm 1]) \to H_1(X_1(N), \text{cusps}, \mathbb{Z}/p'\mathbb{Z}) \).

By (48) and Lemma 5.7, we have:

\[
(T_\ell - \ell - 1)(\beta_*(\mathcal{U})) \equiv 6 \cdot \frac{\ell - 1}{2} \cdot \log(\ell) \cdot \mathcal{E}' \ (\text{modulo} \ p^v) . \tag{49}
\]

Let \( F'_{1,p} : \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z}) \to \mathbb{Z}/p'\mathbb{Z} \) be defined by

\[
12 \cdot F'_{1,p}(x) = \sum_{(s_1, s_2) \in (\mathbb{Z}/2N\mathbb{Z})^2} \sum_{(d-c)s_1 + (d+c)s_2 \equiv 0 \ (\text{modulo} \ N)} (-1)^{s_1+s_2} B_1 \left( \frac{s_1}{2N} \right) B_1 \left( \frac{s_2}{2N} \right) \cdot \log((b-a)s_1 + (b+a)s_2)
\]

\[
- \sum_{(s_1, s_2) \in (\mathbb{Z}/2N\mathbb{Z})^2} \sum_{(d-c)s_1 + (d+c)s_2 \equiv 0 \ (\text{modulo} \ N)} (-1)^{s_1+s_2} B_1 \left( \frac{s_1}{2N} \right) B_1 \left( \frac{s_2}{2N} \right) \cdot \log((d-c)s_1 + (d+c)s_2))
\]
where as above \(a\) and \(b\) are such that \(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z}/N\mathbb{Z})\). This expression does not depend on the choice of \(c\) and \(d\) by Lemma 5.7. This also does not depend on the choice of \(a\) and \(b\).

For all \([c : d] \in \text{P}^1(\mathbb{Z}/N\mathbb{Z})\), we have \(F'_{1,p}([c : d]) = F'_{1,p}([-c : d])\). Thus, we have \(\sum_{x \in \text{P}^1(\mathbb{Z}/N\mathbb{Z})} F'_1, p(x) \cdot \xi \Gamma_0(N)(x) \in H_1(X_0(N), \text{cusps}, \mathbb{Z}/p^i\mathbb{Z})\). The element \(\frac{1}{6} \cdot \beta_*(\mathcal{U})\) is the image of \(\sum_{x \in \text{P}^1(\mathbb{Z}/N\mathbb{Z})} F'_1, p(x) \cdot \xi \Gamma_0(N)(x)\) via the pull-back map \(H_1(X_0(N), \text{cusps}, \mathbb{Z}/p^i\mathbb{Z}) \rightarrow H_1(X_1(N), \text{cusps}, \mathbb{Z}/p^i\mathbb{Z})\).

By (49) and Proposition 5.2 (ii), for any prime \(\ell\) not dividing \(N\) we have in \(H_1(X_0(N), \text{cusps}, \mathbb{Z}/p^i\mathbb{Z})\):

\[
(T_\ell - \ell - 1) \left( \sum_{x \in \text{P}^1(\mathbb{Z}/N\mathbb{Z})} F'_1, p(x) \cdot \xi \Gamma_0(N)(x) \right) = \frac{\ell - 1}{2} \cdot \log(\ell) \cdot m_0^+.
\] (50)

If \(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z})\) and \((s_1, s_2) \in (\mathbb{Z}/2N\mathbb{Z})^2\) are such that \((d - c)s_1 + (d + c)s_2 \equiv 0\) (modulo \(N\)) and \(d \not\equiv c\) (modulo \(N\)), then we have \((b - a)s_1 + (b + a)s_2 \equiv \frac{2}{d - c} \cdot s_2\) (modulo \(N\)). By Lemma 5.7, we have:

\[
12 \cdot \sum_{x \in \text{P}^1(\mathbb{Z}/N\mathbb{Z})} F'_1, p(x) \cdot \xi \Gamma_0(N)(x) = 12 \cdot \sum_{x \in \text{P}^1(\mathbb{Z}/N\mathbb{Z})} F'_1, p(x) \cdot \xi \Gamma_0(N)(x) - 6 \cdot \log(2) \cdot m_0^+.
\]

By (50), we have:

\[
(T_\ell - \ell - 1) \left( \sum_{x \in \text{P}^1(\mathbb{Z}/N\mathbb{Z})} F'_1, p(x) \cdot \xi \Gamma_0(N)(x) \right) = \frac{\ell - 1}{2} \cdot \log(\ell) \cdot m_0^+.
\]

This concludes the proof of Theorem 5.10. \(\Box\)

### 5.5 A few identities in \((\mathbb{Z}/N\mathbb{Z})^\times\) and in \(((\mathbb{Z}/N\mathbb{Z})^\times)^\otimes2\)

In this paragraph, we establish a few identities which will be useful to determine \(m_1^+\) when \(p \in \{2, 3\}\) and also in Sect. 6. We do not impose any restriction on \(p\). If \(i\) is a non-negative integer, we let

\(\odot\) Springer
\[ \mathcal{F}_i = \sum_{k=1}^{\frac{N-1}{2}} \log(k)^i \in \mathbb{Z}/p^v\mathbb{Z}. \]

We have \( \mathcal{F}_0 = \mathcal{F}_1 = 0 \) if \( p > 2 \) and \( 2 \cdot \mathcal{F}_0 = 4 \cdot \mathcal{F}_1 = 0 \) if \( p = 2 \). We have \( \mathcal{F}_2 = 0 \) if \( p > 3 \), \( 3 \cdot \mathcal{F}_2 = 0 \) if \( p = 3 \) and \( 4 \cdot \mathcal{F}_2 = 0 \) if \( p = 2 \). If \( 0 \leq i \leq 2 \), we easily check that \( \mathcal{F}_i = \sum_{k=\frac{N-1}{2}}^{\frac{N-1}{2}} \log(k)^i \) (we use the fact that \( \frac{N-1}{2} \) is even if \( p = 2 \)).

**Lemma 5.11** We have, in \( \mathbb{Z}/p^v\mathbb{Z} \):

\[
4 \cdot \sum_{k=1}^{\frac{N-1}{2}} k \cdot \log(k) = -3 \cdot \sum_{k=1}^{\frac{N-1}{2}} k^2 \cdot \log(k) - \log(2) \cdot \frac{N-1}{6} - \mathcal{F}_1.
\]

**Proof** Let \( f : \mathbb{R} \to \mathbb{R} \) be defined by \( f(x) = (x - \lfloor x \rfloor)^2 \) and let \( g : \mathbb{R} \to \mathbb{R} \) given by \( g(x) = f(2x) - 4f(x) \). If \( x \in [0, \frac{1}{2}] \), we have \( g(x) = 0 \) and if \( x \in [\frac{1}{2}, 1] \), we have \( g(x) = -4x + 1 \). We thus have, in \( \mathbb{Z}/p^v\mathbb{Z} \):

\[
\sum_{k \in (\mathbb{Z}/N\mathbb{Z})^\times} g \left( \frac{k}{N} \right) \cdot \log(k)
= -4 \cdot \sum_{k=\frac{N-1}{2}}^{\frac{N-1}{2}} k \cdot \log(k) + \log \left( (-1)^{\frac{N-1}{2}} \cdot \left( \frac{N-1}{2} \right)! \right)
= -4 \cdot \sum_{k=1}^{\frac{N-1}{2}} (N - k) \cdot \log(-k) + \log \left( (-1)^{\frac{N-1}{2}} \cdot \left( \frac{N-1}{2} \right)! \right)
= 4 \cdot \sum_{k=1}^{\frac{N-1}{2}} k \cdot \log(k) + \mathcal{F}_1.
\]

On the other hand, we have in \( \mathbb{Z}/p^v\mathbb{Z} \):

\[
\sum_{k \in (\mathbb{Z}/N\mathbb{Z})^\times} g \left( \frac{k}{N} \right) \cdot \log(k)
= \sum_{k \in (\mathbb{Z}/N\mathbb{Z})^\times} (f \left( \frac{2k}{N} \right) - 4 \cdot f \left( \frac{k}{N} \right)) \cdot \log(k)
\]
\[
\begin{align*}
&= -3 \cdot \sum_{k \in (\mathbb{Z}/N\mathbb{Z})^\times} f\left(\frac{k}{N}\right) \cdot \log(k) - \log(2) \cdot \sum_{k \in (\mathbb{Z}/N\mathbb{Z})^\times} f\left(\frac{k}{N}\right) \\
&= -3 \cdot \sum_{k=1}^{N-1} k \cdot \log(k) - \log(2) \cdot \frac{N - 1}{6}.
\end{align*}
\]

We have the following variant of Lemma 5.11.

**Lemma 5.12** We have, in \(\mathbb{Z}/p^v\mathbb{Z}\):

\[
4 \cdot \sum_{k=1}^{N-1} k \cdot \log(k)^2
\]

\[
= -3 \cdot \sum_{k=1}^{N-1} k^2 \cdot \log(k)^2 + \log(2)^2 \cdot \frac{N - 1}{6}
\]

\[
-2 \cdot \log(2) \cdot \sum_{k=1}^{N-1} k^2 \cdot \log(k) + 3 \cdot \mathcal{F}_2.
\]

**Proof** Let \(f, g : \mathbb{R} \to \mathbb{R}\) be as in the proof of Lemma 5.12. We have:

\[
\sum_{k \in (\mathbb{Z}/N\mathbb{Z})^\times} g\left(\frac{k}{N}\right) \cdot \log(k)^2 = -4 \cdot \sum_{k=\frac{N+1}{2}}^{N-1} k \cdot \log(k)^2 + \mathcal{F}_2
\]

\[
= -4 \cdot \sum_{k=1}^{N-1} (N - k) \cdot \log(-k)^2 + \mathcal{F}_2
\]

\[
= 4 \cdot \sum_{k=1}^{N-1} k \cdot \log(k)^2 - 3 \cdot \mathcal{F}_2.
\]

On the other hand, we have in \(\mathbb{Z}/p^v\mathbb{Z}\):

\[
\sum_{k \in (\mathbb{Z}/N\mathbb{Z})^\times} g\left(\frac{k}{N}\right) \cdot \log(k)^2
\]

\[
= \sum_{k \in (\mathbb{Z}/N\mathbb{Z})^\times} \left(f\left(\frac{2k}{N}\right) - 4 \cdot f\left(\frac{k}{N}\right)\right) \cdot \log(k)^2
\]
\[ \sum_{k \in (\mathbb{Z}/N\mathbb{Z})^\times} (-4) \cdot f \left( \frac{k}{N} \right) \cdot \log(k)^2 + f \left( \frac{2k}{N} \right) \cdot (\log(2k) - \log(2))^2 \]

\[ = -3 \sum_{k \in (\mathbb{Z}/N\mathbb{Z})^\times} f \left( \frac{k}{N} \right) \cdot \log(k)^2 + \log(2)^2 \cdot \sum_{k \in (\mathbb{Z}/N\mathbb{Z})^\times} f \left( \frac{2k}{N} \right) \cdot \log(2k) \]

\[ - 2 \cdot \log(2) \cdot \sum_{k \in (\mathbb{Z}/N\mathbb{Z})^\times} f \left( \frac{2k}{N} \right) \cdot \log(2k) \]

\[ = -3 \sum_{k=1}^{N-1} k^2 \cdot \log(k)^2 + \log(2)^2 \cdot \frac{N-1}{6} - 2 \cdot \log(2) \cdot \sum_{k=1}^{N-1} k^2 \cdot \log(k) . \]

\[ \square \]

**Lemma 5.13** We have, in \( \mathbb{Z}/p^v\mathbb{Z} \):

\[ \sum_{t_1, t_2=1 \atop t_1 \neq t_2}^{N-1 \over 2} \log(t_1 - t_2) = -2 \cdot \sum_{k=1}^{N-1 \over 2} k \cdot \log(k) \]

and

\[ \sum_{t_1, t_2=1}^{N-1} \log(t_1 + t_2) = 2 \cdot \sum_{k=1}^{N-1 \over 2} k \cdot \log(k) - F_1 . \]

**Proof** We first compute \( S_1 := \sum_{t_1, t_2=1 \atop t_1 \neq t_2}^{N-1 \over 2} \log(t_1 - t_2) \in \mathbb{Z}/p^v\mathbb{Z} \). When \( t_1 \) and \( t_2 \) vary in \( \{1, \ldots, N-1 \over 2\} \), the quantity \( t_1 - t_2 \) varies in \( X := \{-N-1 \over 2}+1, \ldots, N-1 \over 2 - 1\}. If \( k \neq 0 \in X \), then the number of such \( t_1 \) and \( t_2 \) such that \( k = t_1 - t_2 \) is \( \min(N-1 \over 2 - k, N-1 \over 2) - \max(1-k, 1) + 1 \). If \( 1 \leq k \leq N-1 \over 2 - 1 \), this number is \( N-1 \over 2 - k \). If \( -N-1 \over 2 + 1 \leq k \leq -1 \), this number is \( N-1 \over 2 + k \). Thus, we have

\[ S_1 = \sum_{k=-N-1 \over 2}^{-1} \left( k + \frac{N-1}{2} \right) \cdot \log(k) + \sum_{k=1}^{N-1 \over 2} \left( -k + \frac{N-1}{2} \right) \cdot \log(k) \]

\[ = 2 \cdot \sum_{k=1}^{N-1 \over 2} \left( -k + \frac{N-1}{2} \right) \cdot \log(k) \]

\[ = -2 \cdot \sum_{k=1}^{N-1 \over 2} k \cdot \log(k) . \]
The proof of the second equality is similar and is left to the reader. □

In a similar way, we have the following result (whose proof is left to the reader).

**Lemma 5.14** We have, in $\mathbb{Z}/p^v\mathbb{Z}$:

$$\sum_{\substack{t_1, t_2 = 1 \\ t_1 \neq t_2}}^{N-1} \log(t_1 - t_2)^2 = -2 \cdot \sum_{k=1}^{N-1} k \cdot \log(k)^2$$

and

$$\sum_{\substack{t_1, t_2 = 1}}^{N-1} \log(t_1 + t_2)^2 = 2 \cdot \sum_{k=1}^{N-1} k \cdot \log(k)^2 - F_2.$$

**Lemma 5.15** We have, in $\mathbb{Z}/p^v\mathbb{Z}$:

$$\sum_{(t_1, t_2) \in (\mathbb{Z}/N\mathbb{Z})^2 \atop t_1 \neq t_2} D_2 \left( \frac{t_1}{N} \right) \cdot D_2 \left( \frac{t_2}{N} \right) \cdot \log(t_1 - t_2)$$

$$= - \sum_{(t_1, t_2) \in (\mathbb{Z}/N\mathbb{Z})^2 \atop t_1 \neq -t_2} D_2 \left( \frac{t_1}{N} \right) \cdot D_2 \left( \frac{t_2}{N} \right) \cdot \log(t_1 + t_2)$$

$$= -8 \cdot \sum_{k=1}^{N-1} k \cdot \log(k) + 2 \cdot F_1$$

$$= 6 \cdot \sum_{k=1}^{N-1} k^2 \cdot \log(k) + \log(2) \cdot \frac{N - 1}{3}.$$

**Proof** The first equality of Lemma 5.15 follows from the change of variable $t_2 \mapsto -t_2$, using $D_2(-x) = -D_2(x)$ for all $x \in \mathbb{R}$. We have, in $\mathbb{Z}/p^v\mathbb{Z}$:

$$\sum_{(t_1, t_2) \in (\mathbb{Z}/N\mathbb{Z})^2 \atop t_1 \neq t_2} D_2 \left( \frac{t_1}{N} \right) \cdot D_2 \left( \frac{t_2}{N} \right) \log(t_1 - t_2)$$

$$= 2 \sum_{\substack{t_1, t_2 = 1 \\ t_1 \neq t_2}}^{N-1} \log(t_1 - t_2) - 2 \sum_{\substack{t_1, t_2 = 1 \\ t_1 \neq t_2}}^{N-1} \log(t_1 + t_2)$$
Higher Eisenstein elements, higher Eichler formulas

\[
\frac{N-1}{2} \sum_{k=1}^{\frac{N-1}{2}} k \cdot \log(k) + 2 \cdot \mathcal{F}_1.
\]

where in the last equality, we have used Lemma 5.13. This shows the second equality of Lemma 5.15. The third equality follows from Lemma 5.11 and \(4 \cdot \mathcal{F}_1 = 0\).

\[
\sum_{(t_1,t_2) \in \mathbb{Z}/N\mathbb{Z}^2} \frac{D_2}{N} \left( \frac{t_1}{N} \right) \cdot D_2 \left( \frac{t_2}{N} \right) \cdot \log(t_1 - t_2)^2
\]

Similarily, using Lemmas 5.12 and 5.14 we get the following result (which will be used in Sect. 6).

\textbf{Lemma 5.16} We have, in \(\mathbb{Z}/p^v\mathbb{Z}\):

\[
\sum_{(t_1,t_2) : t_1 \neq t_2} D_2 \left( \frac{t_1}{N} \right) \cdot D_2 \left( \frac{t_2}{N} \right) \cdot \log(t_1 - t_2)^2
\]

\[
= -8 \sum_{k=1}^{\frac{N-1}{2}} k \cdot \log(k)^2 + 2 \cdot \mathcal{F}_2
\]

\[
= 6 \sum_{k=1}^{\frac{N-1}{2}} k^2 \cdot \log(k)^2 - \log(2)^2 \cdot \frac{N-1}{3}
\]

\[
+ 4 \cdot \log(2) \cdot \sum_{k=1}^{\frac{N-1}{2}} k^2 \cdot \log(k) - 4 \cdot \mathcal{F}_2.
\]

The following identity will be useful in Sect. 6.

\textbf{Lemma 5.17} For any \(a \in (\mathbb{Z}/N\mathbb{Z})^\times\), we have in \(\mathbb{Z}/p^v\mathbb{Z}\):

\[
\sum_{k \in (\mathbb{Z}/N\mathbb{Z})^\times : k \neq a} \log(k - a) \cdot \log(k) = -\log(a)^2 + \log(-1) \cdot \log(a) + \mathcal{F}_2.
\]

\textit{Proof} We make the change of variable \(k = a \cdot s\). We get, in \(\mathbb{Z}/p^v\mathbb{Z}\):
\[
\sum_{k \in (\mathbb{Z}/N\mathbb{Z})^\times \atop k \neq a} \log(k - a) \cdot \log(k) = \sum_{s \in (\mathbb{Z}/N\mathbb{Z})^\times \atop s \neq 1} \log(s - 1) \cdot \log(s)
- \log(a)^2 + \log(a) \cdot \sum_{s \in (\mathbb{Z}/N\mathbb{Z})^\times \atop s \neq 1} \log(s)
+ \log(a) \cdot \sum_{s \in (\mathbb{Z}/N\mathbb{Z})^\times \atop s \neq 1} \log(s - 1)
= \sum_{s \in (\mathbb{Z}/N\mathbb{Z})^\times \atop s \neq 1} \log(s - 1) \cdot \log(s)
- \log(a)^2 + 2 \cdot \log(a) \cdot \sum_{s \in (\mathbb{Z}/N\mathbb{Z})^\times \atop s \neq 1} \log(s)
- \log(-1) \cdot \log(a)
= - \log(a)^2 + \log(-1) \cdot \log(a)
+ \sum_{s \in (\mathbb{Z}/N\mathbb{Z})^\times \atop s \neq 1} \log(s - 1) \cdot \log(s) .
\]

Since \(2 \cdot \sum_{s \in (\mathbb{Z}/N\mathbb{Z})^\times} \log(s) = \log((N - 1)!^2) = 0\), we have in \(\mathbb{Z}/p^v\mathbb{Z}\):
\[
\sum_{k \in (\mathbb{Z}/N\mathbb{Z})^\times \atop k \neq a} \log(k - a) \cdot \log(k) = - \log(a)^2 + \log(-1) \cdot \log(a)
+ \sum_{s \in (\mathbb{Z}/N\mathbb{Z})^\times \atop s \neq 1} \log(s - 1) \cdot \log(s) .
\]

\textbf{Lemma 5.18} We have, in \(\mathbb{Z}/p^v\mathbb{Z}\):
\[
\sum_{s \in (\mathbb{Z}/N\mathbb{Z})^\times \atop s \neq 1} \log(s - 1) \cdot \log(s) = \mathcal{F}_2 .
\]

\textit{Proof} We treat the cases \(p = 2\) and \(p > 2\) separately. Assume first that \(p > 2\). In this case, we have \(\mathcal{F}_2 = 0\). On the other hand, the left-hand side is easily seen to be zero, using the change of variable \(s \mapsto \frac{1}{s}\). During the rest of the proof, we assume that \(p = 2\) (so \(N \equiv 1\) (modulo 8)). We define three equivalence relations \(\sim_1, \sim_2\) and \(\sim_3\) in \((\mathbb{Z}/N\mathbb{Z})^\times \setminus \{1, -1\}\), characterized by \(x \sim_1 -x\), \(x \sim_2 \frac{1}{x}\), \(x \sim_3 \frac{1}{x}\) and \(x \sim_3 -x\) for all \(x \in (\mathbb{Z}/N\mathbb{Z})^\times\). For \(i \in \{1, 2, 3\}\), let
$R_i \subset (\mathbb{Z}/N\mathbb{Z})^\times$ be a set of representative for $\sim_i$. We can and do choose $R_1$, $R_2$ and $R_3$ so that $R_3 \subset R_1 \cap R_2$. We denote by $\overline{R_i}$ the complement of $R_i$ in $(\mathbb{Z}/N\mathbb{Z})^\times \setminus \{1, -1\}$. Let $\zeta_4 \in R_2$ be the unique element of order 4. If $x \in R_3$ and $x \neq \zeta_4$, there is a unique element $[x]$ of $R_2$ such that $[x] \neq x$ and $[x] \sim_3 x$. We have $[x] = -x$ or $[x] = -\frac{1}{x}$. We get a partition

$$R_2 = \{\zeta_4\} \bigsqcup \{x, [x]\}.$$  

We have, in $\mathbb{Z}/p^\nu\mathbb{Z}$:

$$\sum_{s \in (\mathbb{Z}/N\mathbb{Z})^\times \setminus \{1, -1\}} \log(s - 1) \cdot \log(s) = \sum_{s \in (\mathbb{Z}/N\mathbb{Z})^\times} \log(s - 1) \cdot \log(s) = \sum_{s \in R_2} \log(s - 1) \cdot \log(s) + \sum_{s \in \overline{R}_2} \log(s - 1) \cdot \log(s) = \sum_{s \in R_2} \log(s - 1) \cdot \log(s) - \log \left(\frac{1}{s} - 1\right) \cdot \log(s).$$

In the first equality, we have used the fact that $\log(-1) \cdot \log(-2) = 0$ since $\log(2) \equiv 0 \pmod{2}$ by the quadratic reciprocity law (recall that $N \equiv 1 \pmod{8}$). Thus, we have:

$$\sum_{s \in (\mathbb{Z}/N\mathbb{Z})^\times \setminus \{1\}} \log(s - 1) \cdot \log(s) = \sum_{s \in R_2} \log(s)^2 - \log(-1) \cdot \log(s). \quad (52)$$

We have:

$$\sum_{s \in R_2} \log(s) \equiv \log(\zeta_4) + \sum_{s \in R_3 \setminus \{\zeta_4\}} \log(s) + \log([s]) \pmod{2}.$$  

We have $\log(s) + \log([s]) \equiv 0 \pmod{2}$, and $\log(\zeta_4) \equiv 0 \pmod{2}$. Thus, we have:

$$\sum_{s \in R_2} \log(-1) \cdot \log(s) = 0. \quad (53)$$
By (52) and (53), have:

\[
\sum_{s \in (\mathbb{Z}/N\mathbb{Z})^\times \atop s \neq 1} \log(s - 1) \cdot \log(s) = \sum_{s \in R_2} \log(s)^2 .
\] (54)

We have:

\[
\mathcal{F}_2 = \sum_{s \in R_1} \log(s)^2 \\
= \log(\zeta_4)^2 + 2 \cdot \sum_{s \in R_3 \atop s \neq \zeta_4} \log(s)^2 \\
= \log(\zeta_4)^2 + \sum_{s \in R_3 \atop s \neq \zeta_4} \log(s)^2 + \log([s])^2 = \sum_{s \in R_2} \log(s)^2 .
\]

Combining the latter equality with (54), this concludes the proof of Lemma 5.18.

Lemma 5.17 follows from (51) and Lemma 5.18.

The following identity will be useful to compute \( m_1^+ \) when \( p = 2 \) (Theorem 5.22).

**Lemma 5.19** Assume that \( p = 2 \), so that \( N \equiv 1 \pmod{8} \). For all \( x \in (\mathbb{Z}/N\mathbb{Z})^\times \setminus \{1, -1\} \), we have in \( \mathbb{Z}/2\mathbb{Z} \):

\[
\sum_{s_1, s_2 = 1 \atop (1-x)s_1 + (1+x)s_2 \equiv 0 \pmod{N}} \frac{N-1}{2} = \log \left( \frac{x + 1}{x - 1} \right) \\
= \sum_{s_1, s_2 = 1 \atop (1-x)s_1 + (1+x)s_2 \equiv 0 \pmod{N}} \log \left( \frac{2}{1 - x \cdot s_2} \right) \\
+ \sum_{s_1, s_2 = 1 \atop (1-x)s_1 + (1+x)s_2 \not\equiv 0 \pmod{N}} \log \left( (1 - x)s_1 + (1 + x)s_2 \right) .
\]
Proof The integer

\[
\sum_{s_1, s_2 = 1}^{\frac{N-1}{2}} 1 \quad \text{mod}_{(1-x)s_1 + (1+x)s_2 \equiv 0 \text{ (mod } N)}
\]

is the number of \( s_2 \in \{1, 2, \ldots, \frac{N-1}{2}\} \) such that the representative of \( \frac{x+1}{x-1} \cdot s_2 \in \mathbb{Z}/N\mathbb{Z} \) in \( \{1, 2, \ldots, N - 1\} \) is in \( \{1, 2, \ldots, \frac{N-1}{2}\} \). By Gauss’s Lemma [12, p. 52], this number is congruent to \( \frac{N-1}{2} - \log \left(\frac{x+1}{x-1}\right) \) modulo 2. Since \( \frac{N-1}{2} \) is even, we get in \( \mathbb{Z}/2\mathbb{Z} \):

\[
\sum_{s_1, s_2 = 1}^{\frac{N-1}{2}} 1 = \log \left(\frac{x + 1}{x - 1}\right).
\]

To conclude the proof of Lemma 5.19, it suffices to prove the following equality in \( \mathbb{Z}/2\mathbb{Z} \):

\[
\log \left(\frac{2}{1-x} \cdot s_2\right) + \sum_{s_1, s_2 = 1}^{\frac{N-1}{2}} \log ((1 - x)s_1 + (1 + x)s_2) \equiv 0 \text{ (mod } N)
\]

\[= \log \left(\frac{x + 1}{x - 1}\right). \quad (55)
\]

We denote by \( S \) the left hand side of (55). Since \( N \equiv 1 \) (modulus 8), the class of 2 in \( (\mathbb{Z}/N\mathbb{Z})^\times \) is a square i.e. \( \log(2) \equiv 0 \) (modulus 2), and we have \( \log(-1) \equiv 0 \) (modulus 4).

We have, in \( \mathbb{Z}/2\mathbb{Z} \) (using the first equality):
\[ S = \log \left( \frac{x + 1}{x - 1} \right) \cdot \log(x - 1) + \sum_{s_1, s_2 = 1}^{N-1} \log(s_2) \\
\quad + \sum_{s_1, s_2 = 1}^{N-1} \log ((1 - x)s_1 + (1 + x)s_2) \\
\quad \equiv \log \left( \frac{x + 1}{x - 1} \right) \cdot \log(x - 1) + \sum_{s_1, s_2 = 1}^{N-1} \log(s_2) \\
\quad + \sum_{s_1, s_2 = 1}^{N-1} \log \left( (1 - x) \cdot \frac{s_1}{s_2} + (1 + x) \right) \\
\quad \equiv \sum_{s_1, s_2 = 1}^{N-1} \log \left( \frac{s_1}{s_2} - \frac{x + 1}{x - 1} \right). \]

In the last equality, we have used:
\[ \sum_{s_1, s_2 = 1}^{N-1} 1 \equiv \sum_{s_1, s_2 = 1}^{N-1} 1 \]
\[ \equiv \log \left( \frac{x + 1}{x - 1} \right) \pmod{2}, \]
which follows from:
\[ \sum_{s_1, s_2 = 1}^{N-1} 1 = \left( \frac{N - 1}{2} \right)^2 \equiv 0 \pmod{2}. \]
Let $f : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{Z}$ be such that if $y \in (\mathbb{Z}/N\mathbb{Z})^\times$, $f(y)$ is the number of elements $(s_1, s_2) \in \{1, 2, \ldots, \frac{N-1}{2}\}^2$ such that $\frac{s_1}{s_2} \equiv y \pmod{N}$. We have shown that we have, in $\mathbb{Z}/2\mathbb{Z}$:

$$S = \sum_{y \in (\mathbb{Z}/N\mathbb{Z})^\times \atop y \neq \frac{x+1}{x-1}} \log \left( \frac{y - \frac{x+1}{x-1}}{y - \frac{x}{x-1}} \right) \cdot f(y). \quad (56)$$

As above, by Gauss’s lemma and the fact that $N \equiv 1 \pmod{4}$, we have $f(y) \equiv \log(y) \pmod{2}$. By (56), we have in $\mathbb{Z}/2\mathbb{Z}$:

$$S = \sum_{y \in (\mathbb{Z}/N\mathbb{Z})^\times \atop y \neq \frac{x+1}{x-1}} \log \left( \frac{y - \frac{x+1}{x-1}}{y - \frac{x}{x-1}} \right) \cdot \log(y).$$

By Lemma 5.17 and the fact that $N \equiv 1 \pmod{8}$, we have in $\mathbb{Z}/2\mathbb{Z}$:

$$S = -\log \left( \frac{x + 1}{x - 1} \right)^2 + \frac{N - 1}{12} = \log \left( \frac{x + 1}{x - 1} \right).$$

This concludes the proof of Lemma 5.19. \qed

5.6 The case $p = 3$

In this paragraph, we focus on the case $p = 3$. We determine the image of $m_1^+ \in \left(M_+/3^{i+1}M_+\right)/\mathbb{Z} \cdot m_0^+$. It suffices to determine the image of $6 \cdot m_1^+$ in $\left(M_+/3^{i+1}M_+\right)/\mathbb{Z} \cdot 3 \cdot m_0^+$. The formula given is a minor variation of Theorem 5.10. Recall that we lift log to a group homomorphism $(\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{Z}/3^{i+1}\mathbb{Z}$ (still denoted by log).

**Theorem 5.20** Assume that $p = 3$. We have, in $\left(M_+/3^{i+1}M_+\right)/\mathbb{Z} \cdot 3 \cdot m_0^+$:

$$6 \cdot m_1^+ \equiv \log(2) \cdot \tilde{m}_0^+ + \sum_{x \in \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})} F_{1,3}(x) \cdot \xi_{\Gamma_0(N)}(x),$$

where $F_{1,3} : \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z}) \to \mathbb{Z}/3^{i+1}\mathbb{Z}$ is defined by

$$F_{1,3}([c : d]) = \frac{1}{2} \sum_{(s_1, s_2) \in (\mathbb{Z}/2\mathbb{Z})^2 \atop (d-c)s_1 + (d+c)s_2 \equiv 0 \pmod{N}}$$

\[ \]
(-1)^{s_1+s_2} B_1 \left( \frac{s_1}{2N} \right) B_1 \left( \frac{s_2}{2N} \right) \cdot \log \left( \frac{s_2}{d-c} \right) \\
- \frac{1}{2} \sum_{(s_1,s_2) \in (\mathbb{Z}/2N\mathbb{Z})^2} \sum_{(d-c)s_1+(d+c)s_2 \equiv 0 \pmod{N}} (-1)^{s_1+s_2} B_1 \left( \frac{s_1}{2N} \right) B_1 \left( \frac{s_2}{2N} \right) \cdot \log((d-c)s_1 + (d+c)s_2))

if \([c : d] \neq [1 : 1] and F_{1,3}([1 : 1]) = 0.

**Proof** Let \( \beta : J/J^2 \to \mathbb{Z}/3^{t+1}\mathbb{Z} \) be given by \([x] - 1 \mapsto \log(x)\) for \(x \in (\mathbb{Z}/N\mathbb{Z})^\times\). This induces a map \( \beta_* : J \cdot H_1(X_1(N), \operatorname{cusps}, \mathbb{Z}[\frac{1}{2N}][\mathbb{Z}/N\mathbb{Z}^\times/\pm 1]) \to H_1(X_1(N), \operatorname{cusps}, \mathbb{Z}/3^{t+1}\mathbb{Z}).

Let \( F'_{1,3} : \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z}) \to \mathbb{Z}/3^{t+1}\mathbb{Z} \) be defined by:

\[
F'_{1,3}([c : d]) = \frac{1}{2} \sum_{(s_1,s_2) \in (\mathbb{Z}/2N\mathbb{Z})^2} \sum_{(d-c)s_1+(d+c)s_2 \equiv 0 \pmod{N}} (-1)^{s_1+s_2} B_1 \left( \frac{s_1}{2N} \right) B_1 \left( \frac{s_2}{2N} \right) \cdot \log((b-a)s_1 + (b+a)s_2)
\]

where \( \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z}). \) By Lemma 5.7, this does not depend on the choice of \( \begin{pmatrix} a & b \\ c & d \end{pmatrix}. \) We also have, for all \([c : d] \in \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z}):\)

\[
F'_{1,3}([c : d]) = \frac{1}{8} \sum_{(s_1,s_2) \in (\mathbb{Z}/N\mathbb{Z})^2} \sum_{(d-c)s_1+(d+c)s_2 \equiv 0 \pmod{N}} D_2 \left( \frac{s_1}{N} \right) D_2 \left( \frac{s_2}{N} \right) \cdot \log((b-a)s_1 + (b+a)s_2)
\]

- \frac{1}{8} \sum_{(s_1,s_2) \in (\mathbb{Z}/N\mathbb{Z})^2} \sum_{(d-c)s_1+(d+c)s_2 \equiv 0 \pmod{N}} D_2 \left( \frac{s_1}{N} \right) D_2 \left( \frac{s_2}{N} \right) \cdot \log((d-c)s_1 + (d+c)s_2)) .

\[\text{Springer}\]
For all \([c : d] \in \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})\), we have \(F'_{1,3}([-c : d]) = F'_{1,3}([c : d])\). Thus, we have

\[
\sum_{x \in \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})} F'_{1,3}(x) \cdot \xi_{\Gamma_0(N)}(x) \in H_1(X_0(N), \text{cusps}, \mathbb{Z}/3^{t+1}\mathbb{Z})_+.
\]

By construction, the pull-back of \(\sum_{x \in \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})} F'_{1,3}(x) \cdot \xi_{\Gamma_0(N)}(x)\) in \(H_1(X_1(N), \text{cusps}, \mathbb{Z}/3^{t+1}\mathbb{Z})_+\) is \(\beta_u(U)\).

By (49), Lemma 5.7 and Proposition 5.2 (ii), for all prime \(\ell\) not dividing \(N\) we have in \(M_+/3^{t+1}M_+\):

\[
(T_\ell - \ell - 1) \left( \sum_{x \in \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})} F'_{1,3}(x) \cdot \xi_{\Gamma_0(N)}(x) \right) = 6 \cdot \frac{\ell - 1}{2} \cdot \log(\ell) \cdot m_0^+.
\]

Thus, there exists \(K_3 \in \mathbb{Z}/3^{t+1}\mathbb{Z}\) such that we have:

\[
6 \cdot m_1^+ = K_3 \cdot m_0^+ + \sum_{x \in \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})} F'_{1,3}(x) \cdot \xi_{\Gamma_0(N)}(x) \text{ in } (M_+/3^{t+1}M_+) / \mathbb{Z} \cdot 3 \cdot m_0^+.
\]

Note that \(K_3\) is only uniquely defined modulo 3. We have, in \(\mathbb{Z}/3^{t+1}\mathbb{Z}\):

\[
6 \cdot m_1^+ \cdot m_0^- = K_3 \cdot (\tilde{m}_0^+ \cdot \tilde{m}_0^-) - F'_{1,3}([0 : 1]) + F'_{1,3}([1 : 0]).
\]

Recall that \(\tilde{m}_0^+ \cdot \tilde{m}_0^- = \frac{N-1}{12}\). We also have in \(\mathbb{Z}/3^t\mathbb{Z}\):

\[
m_1^+ \cdot m_0^- = m_0^+ \cdot m_1^- = -\frac{1}{4} \cdot \left( \frac{N - 1}{6} \cdot \log(2) + \sum_{k=1}^{N-1} k^2 \cdot \log(k) \right).
\]

The first equality follows from Corollary 6.3 and the second equality follows from Theorem 6.4 (these results essentially come from [23] and are thus independents of the results of this section).

We have, using Lemma 5.15:

\[
F'_{1,3}([0 : 1]) = -\frac{1}{8} \sum_{(s_1, s_2) \in (\mathbb{Z}/N\mathbb{Z})^2} D_2 \left( \frac{s_1}{N} \right) D_2 \left( \frac{s_2}{N} \right) \cdot \log(s_2 + s_1)
\]

\[
= \frac{3}{4} \sum_{k=1}^{N-1} k^2 \cdot \log(k) + \log(2) \cdot \frac{N - 1}{12}.
\]
Note also that we have $F_1^\prime([1 : 0]) = -F_1^\prime([0 : 1])$. We thus get, in $\mathbb{Z}/3^{i+1}\mathbb{Z}$:
\[
-\frac{1}{2} \cdot \left( \frac{N - 1}{2} \cdot \log(2) + 3 \sum_{k=1}^{N-1} k^2 \cdot \log(k) \right)
= (K_3 - \log(2)) \cdot \frac{N - 1}{12} - \frac{3}{2} \sum_{k=1}^{N-1} k^2 \cdot \log(k).
\]

We thus have $K_3 \equiv \log(2)$ (modulo 3).

If \( \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(2) \) and \((s_1, s_2) \in (\mathbb{Z}/2N\mathbb{Z})^2\) are such that \((d - c)s_1 + (d + c)s_2 \equiv 0 \pmod{N}\) and \(d \not\equiv c \pmod{N}\), then we have \((b - a)s_1 + (b + a)s_2 \equiv \frac{2}{d-c} \cdot s_2 \pmod{N}\). By Lemma 5.7, we have in $M_+/3^{i+1}M_+$:
\[
\sum_{x \in \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})} F_{1,3}(x) \cdot \xi_{\Gamma_0(N)}(x) = \sum_{x \in \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})} F_1^\prime(x) \cdot \xi_{\Gamma_0(N)}(x) - 3 \cdot \log(2) \cdot m_0^+.
\]
This concludes the proof of Theorem 5.20. \hfill \Box

### 5.7 The case $p = 2$

We now study the case $p = 2$ using a similar method, although our result is only partial. Recall that $\mathcal{R}$ is the set of equivalence classes in $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$ for the equivalence relation $[c : d] \sim [-d : c]$.

We first give a formula for $\tilde{m}_0^+$ in terms of Manin symbols.

**Theorem 5.21** Assume that $p = 2$. Let $F_{0,2} : \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z}) \to \mathbb{Z}_p$ be given by
\[
F_{0,2}([c : d]) = -\frac{N - 1}{12} + \frac{1}{3} \cdot \sum_{(d-c)s_1 + (d+c)s_2 \equiv 0 (\pmod{N})} \frac{1}{s_1, s_2 \geq 1}.
\]

If $[c : d] \in \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z}) \setminus \{[1 : 1], [-1 : 1]\}$, we have $F_{0,2}([-d : c]) = -F_{0,2}([c : d])$. Thus, for all $x \in \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$ the element $F_{0,2}(x) \cdot \xi_{\Gamma_0(N)}(x)$ of $M_+$ only depends on the class of $x$ in $\mathcal{R}$. We have in $M_+$:
\[
\tilde{m}_0^+ = \sum_{x \in \mathcal{R}} F_{0,2}(x) \cdot \xi_{\Gamma_0(N)}(x).
\]

**Proof** Recall [23, Lemme 3, Corollaire 4] that we have in $H_1(X_0(N), \text{cusps}, \mathbb{Q}_p)_+$:
Higher Eisenstein elements, higher Eichler formulas 563

\[ 12 \cdot \tilde{m}_0^+ = \mathcal{E} \quad (57) \]

where

\[ \mathcal{E} = \sum_{x \in \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})} F'_{0,2}(x) \cdot \xi \Gamma_0(N)(x) \]

and

\[ F'_{0,2}([c : d]) = \frac{1}{2} \cdot \sum_{(s_1, s_2) \in (\mathbb{Z}/N\mathbb{Z})^2} D_2 \left( \frac{s_1}{N} \right) \cdot D_2 \left( \frac{s_2}{N} \right) . \]

Assume that \( c \neq \pm d \). We have, in \( \mathbb{Z} \):

\[ F'_{0,2}([c : d]) = \sum_{s_1, s_2 = 1}^{N-1} \sum_{s_1 = 1}^{N-1} \sum_{s_2 = \frac{N+1}{2}}^{N-1} 1 \]

\[ (d-c)s_1 + (d+c)(s_2 \equiv 0 \pmod{N}) \]

\[ = 2 \cdot \sum_{s_1, s_2 = 1}^{N-1} \sum_{s_1 = 1}^{N-1} \sum_{s_2 = \frac{N+1}{2}}^{N-1} 1 \]

\[ (d-c)s_1 + (d+c)s_2 \equiv 0 \pmod{N} \]

\[ = -\frac{N-1}{2} + 2 \cdot \sum_{s_1, s_2 = 1}^{N-1} 1 \]

\[ (d-c)s_1 + (d+c)s_2 \equiv 0 \pmod{N} \]

Thus, for all \([c : d] \neq [1 : \pm 1] \in \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})\) we have

\[ F'_{0,2}([c : d]) = 6 \cdot F_{0,2}([c : d]) . \quad (58) \]

Thus, we have

\[ \mathcal{E} = 6 \cdot \sum_{x \in \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})} F_{0,2}(x) \cdot \xi \Gamma_0(N)(x) . \]

By (57), we get:

\[ \tilde{m}_0^+ = \frac{1}{2} \cdot \sum_{x \in \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})} F_{0,2}(x) \cdot \xi \Gamma_0(N)(x) . \quad (59) \]
For all \([c : d] \in \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})\), we have

\[
F'_{0,2}([-d : c]) = \frac{1}{2} \cdot \sum_{(s_1, s_2) \in (\mathbb{Z}/N\mathbb{Z})^2} D_2 \left( \frac{s_1}{N} \right) \cdot D_2 \left( \frac{s_2}{N} \right)
\]

\[
= \frac{1}{2} \cdot \sum_{(s_1, s_2) \in (\mathbb{Z}/N\mathbb{Z})^2} D_2 \left( \frac{s_1}{N} \right) \cdot D_2 \left( -\frac{s_2}{N} \right)
\]

\[
= -\frac{1}{2} \cdot \sum_{(s_1, s_2) \in (\mathbb{Z}/N\mathbb{Z})^2} D_2 \left( \frac{s_1}{N} \right) \cdot D_2 \left( \frac{s_2}{N} \right)
\]

\[
= -F'_{0,2}([c, d]).
\]

By (59) and (58), for all \([c : d] \neq [1 : \pm 1] \in \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})\), we have \(F_{0,2}([-d : c]) = -F_{0,2}([c : d])\). Since \(\xi_{\Gamma_0(N)}([-1 : 1]) = \xi_{\Gamma_0(N)}([1 : 1]) = 0\), we have in \(M_+\):

\[
\tilde{m}_0^+ = \sum_{x \in \mathcal{R}} F_{0,2}(x) \cdot \xi_{\Gamma_0(N)}(x).
\]

\(\square\)

**Remark 5.2** By combining Theorem 5.21, Lemma 5.19 and Proposition 5.2 (iii), we get a new proof of Proposition 5.2 (i) when \(p = 2\) and \(r = 1\).

**Theorem 5.22** Assume that \(p = 2\) and that \(t \geq 2\), i.e. \(N \equiv 1 (mod 16)\). We have:

\[
6 \cdot m_i^+ \equiv m_0^+ + \sum_{x \in \mathcal{R}} F_{1,2}(x) \cdot \xi_{\Gamma_0(N)}(x) \text{ in } (M_+/2^t M_+) / \mathbb{Z} \cdot 2 \cdot m_0^+
\]

where \(F_{1,2} : \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z}) \to \mathbb{Z}/2^{t+1}\mathbb{Z}\) is defined by

\[
F_{1,2}([c : d]) = \sum_{s_1, s_2 = 1 \atop (d-c)s_1 + (d+c)s_2 \equiv 0 (mod N)} \log \left( \frac{2}{d-c \cdot s_2} \right)
\]

\[-\sum_{s_1, s_2 = 1 \atop (d-c)s_1 + (d+c)s_2 \not\equiv 0 (mod N)} \log((d-c)s_1 + (d+c)s_2)\]
if \([c : d] \neq [1 : 1]\) and \(F_{1,2}([1 : 1]) = 0\) (this does not depend on the choice of \(c\) and \(d\)).

**Proof** Let \(\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{PSL}_2(\mathbb{Z})\) with \(c \neq \pm d\). We have

\[
G_\infty(\Gamma_1(N) : \gamma) = \frac{1}{4} \sum_{(s_1, s_2) \in (\mathbb{Z}/N\mathbb{Z})^2} \sum_{(d-c)s_1 + (d+c)s_2 \neq 0 \text{ (modulo } N)} D_2 \left( \frac{s_1}{N} \right) D_2 \left( \frac{s_2}{N} \right) \cdot [(d - c)s_1 + (d + c)s_2]^{-1}
\]

\[
= \frac{1}{2} \sum_{s_1, s_2 = 1}^{N - 1} [(d - c)s_1 + (d + c)s_2]^{-1}
\]

\[
- \frac{1}{2} \sum_{s_1 = 1}^{N - 1} \sum_{s_2 = 1}^{N - 1} [(d - c)s_1 + (d + c)s_2]^{-1}
\]

\[
= \sum_{s_1, s_2 = 1}^{N - 1} [(d - c)s_1 + (d + c)s_2]^{-1}
\]

\[
- \frac{1}{2} \sum_{s_1 = 1}^{N - 1} \sum_{s_2 = 1}^{N - 1} [(d - c)s_1 + (d + c)s_2]^{-1}
\]

\[
= -\frac{N - 1}{2} \cdot \delta + \frac{1}{2} \sum_{s_2 = 1}^{N - 1} [(d + c)s_2]^{-1}
\]

\[
+ \sum_{s_1, s_2 = 1}^{N - 1} [(d - c)s_1 + (d + c)s_2]^{-1}
\]

where \(\delta = \sum_{x \in (\mathbb{Z}/N\mathbb{Z})^* / \pm 1}[x]\). We thus get

\[
G_\infty(\Gamma_1(N) : \gamma) = \left( \frac{1}{2} - \frac{N - 1}{2} \right) \cdot \delta
\]

\[
+ \sum_{s_1, s_2 = 1}^{N - 1} [(d - c)s_1 + (d + c)s_2]^{-1}
\]

\(\square\) Springer
Similarly, noting \((d - c)s_1 + (d + c)s_2 \equiv 0 \pmod{N}\) implies \((b - a)s_1 + (b + a)s_2 \equiv \frac{2s_2}{d - c} \pmod{N}\), we get:

\[
G_0(\Gamma_1(N) \cdot \gamma') = -\frac{1}{2} \cdot \delta + \sum_{s_1, s_2=1}^{N-1} \frac{2}{(d - c)s_1 + (d + c)s_2} \cdot \left[ \frac{2}{d - c} \cdot s_2 \right].
\]

Note that for all \([c, d] \in (\mathbb{Z}/N\mathbb{Z})^2 \setminus \{(0, 0)\}/\pm 1\), we have \(G_\infty([-d, c]) = -G_\infty([-d, c])\) and \(G_0([-d, c]) = -G_0([c, d])\). Recall also that \(\xi_{\Gamma_1(N)}([-d, c]) = -\xi_{\Gamma_1(N)}([c, d])\) and that \(\xi_{\Gamma_1(N)}([1, 1]) = 0\). Let \(R_1\) be the set of equivalence classes in \((\mathbb{Z}/N\mathbb{Z})^2 \setminus \{(0, 0)\}/\pm 1\) under the equivalence relation \([c, d] \sim [-d, c]\). We thus have:

\[
\mathcal{U} = \sum_{[c, d] \in R_1} \xi_{\Gamma_1(N)}([c, d]) \cdot \left[ -\frac{N}{2} \cdot \delta + \sum_{s_1, s_2=1}^{N-1} \frac{(d - c)s_1 + (d + c)s_2}{(d - c)s_1 + (d + c)s_2} \right] \cdot \left[ \frac{2}{d - c} \cdot s_2 \right].
\]

By Lemma 5.7 and the definition of \(\mathcal{U}\), we have \(\mathcal{U} \in J \cdot H_1(X_1(N), \text{ cusps, } \mathbb{Z}[(\mathbb{Z}/N\mathbb{Z})^\times/\pm 1])\), where as above \(J\) is the augmentation ideal of \(\mathbb{Z}[(\mathbb{Z}/N\mathbb{Z})^\times/\pm 1]\). Let \(\beta : J/J^2 \to \mathbb{Z}/2^{t+1}\mathbb{Z}\) be the group homomorphism given by \([x] - [1] \mapsto \log(x)\). Let \(\beta_* : J \cdot H_1(X_1(N), \text{ cusps, } \mathbb{Z}[(\mathbb{Z}/N\mathbb{Z})^\times/\pm 1]) \to H_1(X_1(N), \text{ cusps, } \mathbb{Z}/2^{t+1}\mathbb{Z})\) be the map induced by \(\beta\). We have:

\[
\beta_*(\mathcal{U}) = \sum_{[c, d] \in R_1} F'_{1, 2}([c, d]) \cdot \xi_{\Gamma_1(N)}([c, d]), \quad (60)
\]
where $F'_{1,2} : (\mathbb{Z}/N\mathbb{Z})^2 \backslash \{(0, 0)\}/ \pm 1 \to \mathbb{Z}/2^{t+1}\mathbb{Z}$ is defined by

$$F'_{1,2}(c, d) = \sum_{s_1, s_2 = 1}^{N-1} \log \left( \frac{2}{d - c} \cdot s_2 \right) \log((d - c)s_1 + (d + c)s_2).$$

Formula (60) makes sense because

$$F'_{1,2}([-d, c]) = -F'_{1,2}(c, d),$$

so $F'_{1,2}([c, d]) \cdot \xi_{\Gamma_1(N)}([c, d])$ does not depend on the choice of $[c, d]$ in its equivalence class in $R_1$. By (48), for all prime $\ell$ not dividing $2 \cdot N$ we have in $H_1(X_1(N), \text{cusps}, \mathbb{Z}/2^{t+1}\mathbb{Z})$:

$$(T_\ell - \ell - 1)(\beta_\ast(U)) = 6 \cdot \frac{\ell - 1}{2} \cdot \log(\ell) \cdot \mathcal{E}'.$$

Note that for all $\lambda \in (\mathbb{Z}/N\mathbb{Z})^\times$ and $[c, d] \in (\mathbb{Z}/N\mathbb{Z})^2 \backslash \{(0, 0)\}/ \pm 1$, we have

$$F'_{1,2}([\lambda \cdot c, \lambda \cdot d]) = F'_{1,2}(c, d).$$

Thus $F'_{1,2}$ induces the map $F_{1,2} : \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z}) \to \mathbb{Z}/2^{t+1}\mathbb{Z}$ defined in the statement of Theorem 5.22. Let

$$V = \sum_{x \in \mathcal{R}} F_{1,2}(x) \cdot \xi_{\Gamma_0(N)}(x) \in H_1(X_0(N), \text{cusps}, \mathbb{Z}/2^{t+1}\mathbb{Z}).$$

One easily sees that for all $[c, d] \in (\mathbb{Z}/N\mathbb{Z})^2 \backslash \{(0, 0)\}/ \pm 1$, we have

$$F'_{1,2}([-c, d]) = F'_{1,2}(c, d).$$

Thus, we have $V \in H_1(X_0(N), \text{cusps}, \mathbb{Z}/2^{t+1}\mathbb{Z})_{\pm}$.

Let $\xi_4$ be a primitive fourth root in $(\mathbb{Z}/N\mathbb{Z})^\times$. For all $\lambda, x \in (\mathbb{Z}/N\mathbb{Z})^\times$, we have (using the Manin relations) in $H_1(X_1(N), \text{cusps}, \mathbb{Z})$:

$$\xi_{\Gamma_1(N)}([x, x \cdot \xi_4]) = -\xi_{\Gamma_1(N)}([x \cdot \xi_4, -x])$$

(65)
We also have, in $H_1(X_0(N), \text{cusps, } \mathbb{Z})$:

$$\xi_{\Gamma_0(N)}([\zeta_4]) = \xi_{\Gamma_0(N)}([-\zeta_4]) = 0.$$  \hfill (67)

By (65) and (66), the element

$$\alpha := \sum_{x \in (\mathbb{Z}/N\mathbb{Z})^\times / \langle \zeta_4 \rangle} \xi_{\Gamma_1(N)}([x, x \cdot \zeta_4]) + \xi_{\Gamma_1(N)}([x, -x \cdot \zeta_4])$$

is well-defined in $H_1(X_1(N), \text{cusps, } \mathbb{Z}/2\mathbb{Z})$, where $\langle \zeta_4 \rangle$ is the subgroup generated by $\zeta_4$. Thus, the element $2^t \cdot \alpha$ is well-defined in $H_1(X_1(N), \text{cusps, } \mathbb{Z}/2^{t+1}\mathbb{Z})$. We have

$$2^t \cdot \alpha \in (1 + c) \cdot H_1(X_1(N), \text{cusps, } \mathbb{Z}/2^{t+1}\mathbb{Z}),$$

where $c$ is the complex conjugation.

By (61), we have $F'_{1,2}([1, \zeta_4]) = -F'_{1,2}([\zeta_4, -1])$. Since $[\zeta_4, -1] = [\zeta_4 \cdot 1, \zeta_4 \cdot \zeta_4]$, by (63) we also have $F'_{1,2}([\zeta_4, -1]) = F'_{1,2}([1, \zeta_4])$. Thus, we have $2 \cdot F'_{1,2}([1, \zeta_4]) = 0$, i.e. $F'_{1,2}([1, \zeta_4]) \equiv 0$ (modulo $2^t$). Thus, there exists $K_2 \in \mathbb{Z}/2\mathbb{Z}$ such that for all $x \in (\mathbb{Z}/N\mathbb{Z})^\times$, we have

$$F'_{1,2}([x, x \cdot \zeta_4]) = K_2 \cdot 2^t.$$  \hfill (68)

By (64), for all $x \in (\mathbb{Z}/N\mathbb{Z})^\times$, we have

$$F'_{1,2}([x, -x \cdot \zeta_4]) = K_2 \cdot 2^t.$$  \hfill (69)

For any integer $r \geq 1$, let $\pi_r^* : H_1(X_0(N), \text{cusps, } \mathbb{Z}/2^r\mathbb{Z}) \to H_1(X_1(N), \text{cusps, } \mathbb{Z}/2^r\mathbb{Z})$ be the pull-back map. By construction and by (67), we have

$$\pi_{t+1}^*(\mathcal{V}) = \beta_* (\mathcal{U}) + K_2 \cdot 2^t \cdot \alpha.$$  \hfill (70)

Lemma 5.23 We have, in $H_1(X_1(N), \mathbb{Z}/2^{t+1}\mathbb{Z})$:

$$2^t \cdot \alpha = \pi_{t+1}^* \left( \sum_{x \in R} \log \left( \frac{x + 1}{x - 1} \right) \cdot \xi_{\Gamma_0(N)}(x) \right).$$
Proof Recall the notation of Lemma 5.3, applied to \( \Gamma = \Gamma_1(N) \). We identify as before \( \Gamma_1(N) \backslash \text{PSL}_2(\mathbb{Z}) \) with \((\mathbb{Z}/N\mathbb{Z})^2 \backslash \{(0,0)\}/\pm 1 \). We let \( \mathcal{R}_1 \subset \mathcal{R}_{\Gamma_1(N)} \) be the subset of equivalence classes of elements \([c, d]\) with \( c \not\equiv \pm d \) (modulo \( N \)). We have, in \( H_1(X_1(N), \text{cusps}, \mathbb{Z}/2^t+1\mathbb{Z}) \):

\[
\pi^*_{t+1} \left( \sum_{x \in \mathcal{R}, x \equiv \xi} \log \left( \frac{x+1}{x-1} \right) \cdot \bar{\xi}_{\Gamma_1(N)}(x) \right) = 2^t \cdot \alpha + \sum_{[c, d] \in \mathcal{R}_1} \log \left( \frac{d-c}{d+c} \right) \cdot \bar{\xi}_{\Gamma_1(N)}([c, d]) .
\] (71)

To conclude the proof of Lemma 5.23, it suffices to prove the following result.

Lemma 5.24 We have, in \( H_1(X_1(N), \mathbb{Z}/2^t+1\mathbb{Z}) \):

\[
\sum_{[c, d] \in \mathcal{R}_1} \log \left( \frac{d-c}{d+c} \right) \cdot \bar{\xi}_{\Gamma_1(N)}([c, d]) = 0 .
\]

Proof Consider the morphism \( h : \mathbb{Z}[\Gamma_1(N) \backslash \text{PSL}_2(\mathbb{Z})] \rightarrow \mathbb{Z}/2^t+1\mathbb{Z} \) given by \([c, d] \mapsto \log \left( \frac{d}{c} \right) \) if \( c \cdot d \not\equiv 0 \) (modulo \( N \)) and \([c, d] \mapsto 0 \) else. This factors through \( \bar{\xi}_{\Gamma_1(N)} \), and we let \( g : H_1(X_1(N), \text{cusps}, \mathbb{Z}) \rightarrow \mathbb{Z}/2^t+1\mathbb{Z} \) be the induced map. Let \( f : H_1(X_1(N), \mathbb{Z}) \rightarrow \mathbb{Z}/2^t+1\mathbb{Z} \) be the restriction of \( g \) to \( H_1(X_1(N), \mathbb{Z}) \), and \( \hat{f} \in H_1(X_1(N), \mathbb{Z}/2^t+1\mathbb{Z}) \) be the element corresponding to \( f \) by intersection duality. By Lemma 5.3, we have:

\[
\hat{f} = \sum_{[c, d] \in \mathcal{R}_1} \left( \log \left( \frac{c}{d} \right) + \frac{2}{3} \cdot \log \left( \frac{d}{d-c} \right) + \frac{1}{3} \cdot \log \left( \frac{d-c}{-c} \right) \right.
- \frac{2}{3} \cdot \log \left( \frac{c}{c+d} \right) - \frac{1}{3} \cdot \log \left( \frac{c+d}{d} \right) \big) \cdot \bar{\xi}_{\Gamma_1(N)}([c, d])
= \frac{1}{3} \sum_{[c, d] \in \mathcal{R}_1} \log \left( \frac{d+c}{d-c} \right) \cdot \bar{\xi}_{\Gamma_1(N)}([c, d]) .
\]

To prove that \( \hat{f} = 0 \), it suffices to prove that \( f = 0 \). Let

\[
\sum_{[c, d] \in (\mathbb{Z}/N\mathbb{Z})^2 \backslash \{(0,0)\}/\pm 1 \ c \cdot d \not\equiv 0 \ (\text{modulo} \ N)} \lambda_{[c, d]} \cdot \bar{\xi}_{\Gamma_1(N)}([c, d]) \in H_1(X_1(N), \mathbb{Z}) .
\]
A boundary consideration (cf. Sect. 4.1) shows that we have, in \( \mathbb{Z}[(\mathbb{Z}/N\mathbb{Z})^\times/\pm 1] \):

\[
\sum_{[c,d] \in (\mathbb{Z}/N\mathbb{Z})^2\setminus\{(0,0)\}/\pm 1} \lambda_{[c,d]} \cdot ([c] - [d]) = 0 .
\]

Thus, we have

\[
f \left( \sum_{[c,d] \in (\mathbb{Z}/N\mathbb{Z})^2\setminus\{(0,0)\}/\pm 1} \lambda_{[c,d]} \cdot \xi_1(N) ([c, d]) \right)
= \sum_{[c,d] \in (\mathbb{Z}/N\mathbb{Z})^2\setminus\{(0,0)\}/\pm 1} \lambda_{[c,d]} \cdot (\log(c) - \log(d)) = 0 .
\]

This concludes the proof of Lemma 5.24. \( \Box \)

This concludes the proof of Lemma 5.23. \( \Box \)

By (70), Lemma 5.23 and (62), for all prime \( \ell \) not dividing \( 2 \cdot N \), we have in \( H_1(X_1(N), \text{cusps}, \mathbb{Z}/2^{l+1}\mathbb{Z}) \):

\[
\pi_{l+1}^* \left( (T_\ell - \ell - 1) \left( \mathcal{V} - K_2 \cdot \sum_{x \in \mathcal{R} \atop x \neq 1} \log \left( \frac{x + 1}{x - 1} \right) \cdot \xi_0(N) (x) \right) \left( -6 \cdot \frac{\ell - 1}{2} \cdot \log(\ell) \cdot m_0^+ \right) \right) = 0 .
\]

Thus, we have in \( H_1(X_1(N), \text{cusps}, \mathbb{Z}/2^{l+1}\mathbb{Z}) \):

\[
\pi_{l+1}^* \left( (T_\ell - \ell - 1) \left( \mathcal{V} - 6 \cdot m_1^+ - K_2 \cdot \sum_{x \in \mathcal{R} \atop x \neq 1} \log \left( \frac{x + 1}{x - 1} \right) \cdot \xi_0(N) (x) \right) \right) = 0 .
\]

(72)

By (72) and Proposition 5.2 (i), for all prime \( \ell \) not dividing \( 2 \cdot N \), we have in \( H_1(X_0(N), \text{cusps}, \mathbb{Z}/2^{l+1}\mathbb{Z}) \):

\[
(1 + c) \cdot (T_\ell - \ell - 1) \left( \mathcal{V} - 6 \cdot m_1^+ \right) = 0 ,
\]
where \( c \) is the complex conjugation. By (64), we have \((1 - c) \cdot (T_\ell - \ell - 1) (V - 6 \cdot m_1^+) = 0\). Thus, for all prime \( \ell \) not dividing \( 2 \cdot N \), we have in \( H_1(X_0(N), \text{cusps}, \mathbb{Z}/2^t\mathbb{Z}) \):

\[
(T_\ell - \ell - 1) (V - 6 \cdot m_1^+) = 0.
\]

Thus, there exists a constant \( C_2 \), uniquely defined modulo 2, such that we have:

\[
6 \cdot m_1^+ \equiv C_2 \cdot m_0^+ + V \mod (M_+/2^t \cdot M_+) / \mathbb{Z} \cdot 2 \cdot m_0^+.
\]

To conclude the proof of Theorem 5.22, it suffices to prove that \( m_0^+ \equiv V \mod 2 \). This follows from Theorem 5.22 and Lemma 5.19.

\[\square\]

6 Modular forms and interplay between higher Eisenstein elements

In this section, we relate the various Hecke modules (and their higher Eisenstein elements) that were considered before. This is done by relating them to the space of modular forms.

We assume as usual that \( p \) divides the numerator of \( N-1 \) (we allow \( p = 2 \) and \( p = 3 \)). We keep the notation of the previous sections. In particular \( M = \mathbb{Z}_p[S] \) is the supersingular module, \( M_+ = H_1(X_0(N), \text{cusps}, \mathbb{Z}_p)_+ \) and \( M^- = H_1(Y_0(N), \mathbb{Z}_p)^- \). As before, we fix an integer \( r \) such that \( 1 \leq r \leq t \).

We let \( v = \gcd(N - 1, 12) \).

6.1 Modular forms

Following [11], let \( \mathcal{N} \) be the \( \mathbb{Z} \)-module of weight 2 modular forms \( f \) of level \( \Gamma_0(N) \) and weight 2 for which \( a_n(f) \in \mathbb{Z} \) if \( n \geq 1 \) and \( a_0(f) \in \mathbb{Q} \), where \( \sum_{n \geq 0} a_n(f) \cdot q^n \) is the \( q \)-expansion of \( f \) at the cusp \( \infty \). We let \( \mathcal{M} = \mathcal{N} \otimes_{\mathbb{Z}} \mathbb{Z}_p \).

By [19, Corollary II.16.3] and [11, Theorem 0.5 and Proposition 1.9], the \( \mathbb{T}_2 \)-module \( \mathcal{M} \otimes_{\mathbb{T}} \mathbb{T}_2 \) is free of rank one. We can thus apply Theorem 2.1 and consider a system of higher Eisenstein elements \( f_0, \ldots, f_{n(r)} \) in \( \mathcal{M}/p' \mathcal{M} \). As in Sect. 1.1, we let \( \tilde{f}_0 \in \mathcal{M} \) be a lift of \( f_0 \), normalized such that its \( q \)-expansion at the cusp \( \infty \) is:

\[
\frac{N - 1}{24} + \sum_{n \geq 1} \left( \sum_{d|n} d \right) \cdot q^n.
\]
By [11, Proposition 1.3 (i)], the pairing \( \mathcal{M} \times \mathbb{T} \to \mathbb{Q}_p \) given by \( (f, T) \mapsto a_1(T(f)) \) takes values in \( \mathbb{Z}_p \) and induces a canonical \( \mathbb{T} \)-equivariant isomorphism \( \mathcal{M} \cong \text{Hom}_{\mathbb{Z}_p}(\mathbb{T}, \mathbb{Z}_p) \). Let \( T_0 \in \mathbb{T} \) be such that

\[
a_1(T_0(f)) = \frac{24}{v} \cdot a_0(f) \tag{73}\]

for all \( f \in \mathcal{N} \). We have \( \text{Ker}(\mathbb{T} \to \mathbb{T}^0) = \mathbb{Z}_p \cdot T_0 \). By [11, Proposition 1.8 (ii)], we have

\[
T_0 - \frac{N - 1}{v} \in I . \tag{74}\]

### 6.2 Comparison between the various pairings

**Proposition 6.1**  
(i) We have, for all \( m \in M \):

\[
T_0(m) = \frac{12}{v} \cdot (m \bullet \tilde{e}_0) \cdot \tilde{e}_0 .
\]

(ii) We have, for all \( m_+ \in M_+ \):

\[
T_0(m_+) = \frac{12}{v} \cdot (m_+ \bullet \tilde{m}_0^-) \cdot \tilde{m}_0^+ .
\]

(iii) We have, for all \( m^- \in M^- \):

\[
T_0(m^-) = \frac{12}{v} \cdot (\tilde{m}_0^+ \bullet m^-) \cdot \tilde{m}_0^- .
\]

**Proof** We have

\[
I \cdot T_0 = 0 \tag{75}
\]

since the Hecke operators of \( I \cdot T_0 \) annihilate all the modular forms of weight 2 and level \( \Gamma_0(N) \).

We first prove (i). By (75), for all \( m \in M \) the element \( T_0(m) \) is annihilated by \( I \), so is proportional to \( \tilde{e}_0 \). Thus, for all \( m \in M \) there exists \( C_m \in \mathbb{Z}_p \) such that

\[
T_0(m) = C_m \cdot \tilde{e}_0 .
\]

We thus have, in \( \mathbb{Z}_p \):

\[
C_m \cdot (\tilde{e}_0 \bullet \tilde{e}_0) = T_0(m) \cdot \tilde{e}_0 = m \bullet T_0(\tilde{e}_0) . \tag{76}
\]
By (74), we have \( T_0(\tilde{e}_0) = \frac{N-1}{\nu} \cdot \tilde{e}_0 \). Recall that by Eichler mass formula, we have \( \tilde{e}_0 \cdot \tilde{e}_0 = \frac{N-1}{12} \). By (76), we get:

\[
C_m = \frac{12}{\nu} \cdot (m \cdot \tilde{e}_0).
\]

We now prove (ii). As above, for all \( m_+ \in M_+ \) there exists \( C_{m_+} \in \mathbb{Z}_p \) such that

\[
T_0(m_+) = C_{m_+} \cdot \tilde{m}_0^+.
\]

We thus have, in \( \mathbb{Z}_p \):

\[
C_{m_+} \cdot (\tilde{m}_0^+ \cdot \tilde{m}_0^-) = T_0(m_+) \cdot \tilde{m}_0^- = m_+ \cdot T_0(\tilde{m}_0^-). \tag{77}
\]

By (74), we have \( T_0(\tilde{m}_0^-) = \frac{N-1}{\nu} \cdot \tilde{m}_0^- \). Recall that we have \( \tilde{m}_0^+ \cdot \tilde{m}_0^- = \frac{N-1}{12} \). By (77), we get:

\[
C_{m_+} = \frac{12}{\nu} \cdot (m_+ \cdot \tilde{m}_0^-).
\]

The proof of (iii) is similar. \( \square \)

Let \( M_1 \) and \( M_2 \) be \( \mathbb{T} \)-modules equipped with a \( \mathbb{T} \)-equivariant bilinear pairing \( \bullet : M_1 \times M_2 \to \mathbb{Z}_p \). By (73), for any \( m_1 \in M_1 \) and \( m_2 \in M_2 \) we have an element of \( \mathcal{M} \) whose \( q \)-expansion at the cusp \( \infty \) is

\[
\frac{\nu}{24} \cdot (m_1 \cdot T_0(m_2)) + \sum_{n \geq 1} (m_1 \cdot T_n(m_2)) \cdot q^n. \tag{78}
\]

We apply this remark to the cases \((M_1, M_2) = (M, M)\) and \((M_1, M_2) = (M_+, M^-)\). We choose the pairing \( \bullet \) already described in the previous sections for these couples.

**Proposition 6.2** Let \( x \in M \) (resp. \( x_+ \in M_+, \text{ resp. } x^- \in M^- \)) be such that \( \tilde{e}_0 \cdot x = 1 \) (resp. \( x_+ \cdot \tilde{m}_0^- = 1 \), resp. \( \tilde{m}_0^+ \cdot x^- = 1 \)). For all integers \( i \) such that \( 0 \leq i \leq n(r) \), let

\[
E_i = \frac{e_i \cdot e_0}{2} + \sum_{n \geq 1} (e_i \cdot T_n(x)) \cdot q^n,
\]

\[
E_i^+ = \frac{m_i^+ \cdot m_0^-}{2} + \sum_{n \geq 1} (m_i^+ \cdot T_n(x^-)) \cdot q^n.
\]
and

\[ E_i^- = \frac{m_0^+ \bullet m_i^-}{2} + \sum_{n \geq 1} (T_n(x_+) \bullet m_i^-) \cdot q^n \]

in \( \left( \frac{1}{2} \mathbb{Z} \oplus q \cdot \mathbb{Z}[[q]] \right) \otimes_Z \mathbb{Z}/p^r\mathbb{Z} \). Note that the image of \( E_i \) in

\[ \left( \left( \frac{1}{2} \mathbb{Z} \oplus q \cdot \mathbb{Z}[[q]] \right) \otimes_Z \mathbb{Z}/p^r\mathbb{Z} \right)/ (\mathbb{Z} \cdot E_1 + \cdots + \mathbb{Z} \cdot E_{i-1}) \]

is uniquely determined, and similarly for \( E_i^+ \) and \( E_i^- \).

For all integers \( i \) such that \( 0 \leq i \leq n(r) \), we have:

\[ \sum_{n \geq 0} a_n(f_i) \cdot q^n \equiv E_i \equiv E_i^+ \equiv E_i^- \text{ in } \left( \left( \frac{1}{2} \mathbb{Z} \oplus q \cdot \mathbb{Z}[[q]] \right) \otimes_Z \mathbb{Z}/p^r\mathbb{Z} \right)/ (\mathbb{Z} \cdot E_1 + \cdots + \mathbb{Z} \cdot E_{i-1}) . \]

**Proof** By (73), the image of the group homomorphism \( M \to \mathbb{Q}_p \) given by \( f \mapsto a_0(f) \) is contained in \( \frac{1}{24} \cdot \mathbb{Z} \). Thus, the \( q \)-expansion at the cusp \( \infty \) gives an injective group homomorphism \( \iota : M/p^rM \to \left( \frac{1}{2} \mathbb{Z} \oplus q \cdot \mathbb{Z}[[q]] \right) \otimes_Z \mathbb{Z}/p^r\mathbb{Z} \). The fact that \( E_i, E_i^+ \) and \( E_i^- \) lie in \( \iota(M/p^rM) \) follows from Proposition 6.1 and (78). We abuse notation and consider \( E_i, E_i^+ \) and \( E_i^- \) as elements of \( M/p^rM \).

One easily sees that we have \( E_0 = E_0^+ = E_0^- = f_0 \). Furthermore, for all prime \( \ell \) not dividing \( 2 \cdot N \) and all \( 1 \leq i \leq n(r) \), we have

\[ (T_\ell - \ell - 1)(E_i) \equiv \frac{\ell - 1}{2} \cdot \log(\ell) \cdot E_{i-1} \text{ in } (M/p^rM) / (\mathbb{Z} \cdot E_0 + \cdots + \mathbb{Z} \cdot E_{i-1}) . \]

Proposition 6.2 follows immediately by induction on \( i \).

By comparing the constant coefficients of the various modular forms of Proposition 6.2, we get the following comparison result, which is Theorem 1.11 if \( r = 1 \).

**Corollary 6.3** For all \( 0 \leq i, j \leq n(r) \) such that \( i + j \leq n(r) \), we have in \( \mathbb{Z}/p^r\mathbb{Z} \):

\[ e_i \bullet e_j = m_i^+ \bullet m_j^- = 2 \cdot a_0(f_{i+j}) . \]

By Corollary 2.5, this common quantity is 0 if and only if \( i + j < n(r) \).

**Remark 6.1** If \( p = 2 \) and \( f \in M/p^rM \), then \( a_0(f) \) is an element of \( \frac{1}{2} \mathbb{Z}/p^{r-1}\mathbb{Z} \), so \( 2 \cdot a_0(f) \) is a well-defined element of \( \mathbb{Z}/p^r\mathbb{Z} \).
6.3 Computation of \( m_i^+ \cdot m_j^- \) when \( i + j = 1 \)

By Corollary 6.3, we have in \( \mathbb{Z}/p^r\mathbb{Z} \):

\[
e_0 \cdot e_1 = e_1 \cdot e_0 = m_1^+ \cdot m_0^- = m_0^+ \cdot m_1^- = 2 \cdot a_0(f_1) .
\] (79)

Theorem 3.16 shows that if \( p \geq 5 \) then \( e_1 \cdot e_0 = \frac{1}{3} \cdot \sum_{k=1}^{N-1} k \cdot \log(k) \). In fact, one can compute \( m_0^+ \cdot m_1^- \) directly even for \( p \leq 3 \), using Merel’s work.

**Theorem 6.4** We have

\[
m_0^+ \cdot m_1^- = -\frac{1}{12} \cdot \log \left( \epsilon \cdot \zeta \cdot \prod_{k=1}^{N-1} k^{-4k} \right) \in \mathbb{Z}/p^r\mathbb{Z}
\]

where \( \epsilon = 1 \) if \( N \notin 1 + 8\mathbb{Z} \), \( \epsilon = -1 \) if \( N \in 1 + 8\mathbb{Z} \), \( \zeta = 1 \) if \( N \notin 1 + 3\mathbb{Z} \) and \( \zeta = 2^{-\frac{N-1}{3}} \) if \( N \in 1 + 3\mathbb{Z} \).

If \( p = 2 \), \( \epsilon \cdot \zeta \cdot \prod_{k=1}^{N-1} k^{-4k} \equiv x^4 \) (modulo \( N \)) is a 4th power of \( (\mathbb{Z}/N\mathbb{Z})^\times \), and the meaning of the right-hand side is \(-\frac{1}{3} \cdot \log(x)\), which is

\[-\frac{1}{3} \cdot (2^{t-1} - \sum_{k=1}^{N-1} k \cdot \log(k)) .
\]

If \( p = 3 \), \( \epsilon \cdot \zeta \cdot \prod_{k=1}^{N-1} k^{-4k} \equiv x^3 \) (modulo \( N \)) is a 3rd power of \( (\mathbb{Z}/N\mathbb{Z})^\times \), and the meaning of the right-hand side is \(-\frac{1}{4} \cdot \log(x)\), which is

\[-\frac{1}{4} \sum_{k=1}^{N-1} k^2 \cdot \log(k) .
\]

**Proof** This follows from [23, Théorème 1]. The last assertion in the case \( p = 3 \) follows from Lemma 5.11. \( \square \)

**Remark 6.2** Theorem 1.12 (i) is a particular case of Theorem 6.4 (when \( r = 1 \)).

**Corollary 6.5** Assume \( p = 3 \). We have \( n(r) \geq 2 \) if and only if \( \sum_{k=1}^{N-1} k^2 \cdot \log(k) \equiv 0 \) (modulo \( 3^r \)).

**Corollary 6.6** Assume \( p = 2 \). We have \( n(r) \geq 2 \) if and only if \( \sum_{k=1}^{N-1} k \cdot \log(k) \equiv 2^{t-1} \) (modulo \( 2^r \)).
**Remark 6.3** In the case \( r = 1, g_2 = n(1) \) was determined completely in terms of the class group of \( \mathbb{Q}(\sqrt{-N}) \) in [7, Theorem 1.1 and p.133]; we have \( g_2 = 2^{m-1} - 1 \) where \( m \) is the 2-adic valuation of the order of this class group.

**Remark 6.4** Theorem 1.5 (i) is an immediate consequence of (79) and Theorem 6.4.

### 6.4 Computation of \( m_i^+ \cdot m_j^- \) when \( i + j = 2 \) and \( p \geq 5 \)

In all this section, we assume \( p \geq 5 \). Theorems 1.2 and 1.12 (ii) are consequences of the following result.

**Theorem 6.7** Assume that we have \( 1 \leq r \leq t \) and \( n(r) \geq 2 \) (i.e. \( \sum_{k=1}^{N-1} k \cdot \log(k) \equiv 0 \pmod{p^r} \)). We have:

\[
m_i^+ \cdot m_j^- \equiv \frac{1}{6} \sum_{k=1}^{N-1} k \cdot \log(k)^2 \pmod{p^r}.
\]

**Proof** By Theorems 5.10 and 4.2, we have in \( \mathbb{Z}/p^r\mathbb{Z} \):

\[
24 \cdot m_i^+ \cdot m_j^- = \sum_{x \in (\mathbb{Z}/N\mathbb{Z})^\times \atop x \neq 1} \log(x) \cdot \left( \sum_{(s_1, s_2) \in (\mathbb{Z}/2N\mathbb{Z})^2 \atop (1-x)s_1 + (1+x)s_2 \equiv 0 \pmod{N}} \right.
\]

\[
(-1)^{s_1+s_2} B_1 \left( \frac{s_1}{2N} \right) B_1 \left( \frac{s_2}{2N} \right) \cdot \log \left( \frac{s_2}{1-x} \right)
\]

\[
- \log(x) \cdot \left( \sum_{(s_1, s_2) \in (\mathbb{Z}/2N\mathbb{Z})^2 \atop (1-x)s_1 + (1+x)s_2 \not\equiv 0 \pmod{N}} \right.
\]

\[
(-1)^{s_1+s_2} B_1 \left( \frac{s_1}{2N} \right) B_1 \left( \frac{s_2}{2N} \right) \cdot \log((1-x)s_1 + (1+x)s_2)
\]
\[
\begin{align*}
= \frac{1}{4} \sum_{x \in \mathbb{Z}/N\mathbb{Z}^\times \atop x \neq 1} \log(x) \cdot \\
& \quad \left( \sum_{(s_1, s_2) \in (\mathbb{Z}/N\mathbb{Z})^2 \atop (1-x)s_1 + (1+x)s_2 \neq 0} \log \left( \frac{s_2}{1-x} \right) \right) \\
& \quad - \log(x) \cdot \\
& \quad \left( \sum_{(s_1, s_2) \in (\mathbb{Z}/N\mathbb{Z})^2 \atop (1-x)s_1 + (1+x)s_2 \neq 0} D_2 \left( \frac{s_1}{N} \right) D_2 \left( \frac{s_2}{N} \right) \cdot \right) \\
& \quad - \sum_{x \neq 0, s_1 \neq -s_2} \log(x) \cdot \log((x-1)s_1 + (x+1)s_2) \\
\end{align*}
\]

Since \( n(r) \geq 2 \), we have \( \sum_{k=1}^{N-1} k \cdot \log(k) \equiv 0 \) (modulo \( p^r \)). By Lemma 5.15, we have:

\[
\sum_{(s_1, s_2) \in (\mathbb{Z}/N\mathbb{Z})^2 \atop s_1 \neq \pm s_2} D_2 \left( \frac{s_1}{N} \right) D_2 \left( \frac{s_2}{N} \right) \cdot \log \left( \frac{s_1 + s_2}{s_1 - s_2} \right) \equiv 0 \pmod{p^r}.
\]
Thus, we have:

\[ 96 \cdot m_1^+ \cdot m_1^- = \sum_{(s_1, s_2) \in (\mathbb{Z}/N\mathbb{Z})^2, s_1 \neq \pm s_2} D_2 \left( \frac{s_1}{N} \right) D_2 \left( \frac{s_2}{N} \right) \cdot \left( \log \left( \frac{s_1 + s_2}{s_1 - s_2} \right) \cdot \log(s_2 - s_1) \right) \]

\[ - \sum_{x \neq 0, \frac{s_1 + s_2}{s_1 - s_2}} \log(x) \cdot \log((1 - x)s_1 + (1 + x)s_2). \]

Lemma 5.17 shows that

\[ \sum_{x \neq 0, \frac{s_1 + s_2}{s_1 - s_2}} \log(x) \cdot \log((1 - x)s_1 + (1 + x)s_2) \]

\[ = - \log(s_2 - s_1) \cdot \log \left( \frac{s_1 + s_2}{s_1 - s_2} \right) - \log \left( \frac{s_1 + s_2}{s_1 - s_2} \right)^2. \]

We conclude that

\[ 96 \cdot m_1^+ \cdot m_1^- = \sum_{(s_1, s_2) \in (\mathbb{Z}/N\mathbb{Z})^2, s_1 \neq \pm s_2} D_2 \left( \frac{s_1}{N} \right) D_2 \left( \frac{s_2}{N} \right) \cdot \left( \log \left( \frac{s_1 + s_2}{s_1 - s_2} \right) \cdot \log(s_2 - s_1) \right) \]

\[ = \sum_{(s_1, s_2) \in (\mathbb{Z}/N\mathbb{Z})^2, s_1 \neq \pm s_2} D_2 \left( \frac{s_1}{N} \right) D_2 \left( \frac{s_2}{N} \right) \cdot \left( \log(s_1 + s_2)^2 - \log(s_1 - s_2)^2 \right) \]

\[ = 16 \cdot \sum_{k=1}^{N-1} k \cdot \log(k)^2 \]

where the last equality follows from Lemma 5.16.

Combining Corollary 6.3, Theorems 3.16 (iii) and 6.7, we get the following identity (which is Theorem 1.13 if \( r = 1 \)).

**Corollary 6.8** Assume \( n(r) \geq 2 \), i.e. \( \sum_{k=1}^{N-1} k \cdot \log(k) \equiv 0 \) (modulo \( p^r \)). We have, in \( \mathbb{Z}/p^r\mathbb{Z} \):

\[ \sum_{\lambda \in L} 3 \cdot \log(H'(\lambda))^2 - 4 \cdot \log(\lambda)^2 = 12 \cdot \sum_{k=1}^{N-1} k \cdot \log(k)^2. \]

**Remark 6.5** Theorem 1.5 (ii) is an immediate consequence of Corollary 6.3 and Theorem 6.7.
6.5 Computation of \( m_1^+ \cdot m_1^- \) when \( p = 3 \)

In this section, we assume \( p = 3 \).

We give a formula for \( m_1^+ \cdot m_1^- \) modulo \( 3^t \). We are only able to simplify the formula for this intersection product modulo \( 3^{t-1} \). Note that we do not have an explicit formula for \( m_2^- \), but nevertheless it is possible to compute \( m_0^+ \cdot m_2^- = m_1^+ \cdot m_1^- \).

For \( \bar{a} \) and \( \bar{b} \) in \( (\mathbb{Z}/N\mathbb{Z})^\times \), we let \([\bar{a}, \bar{b}]\) be the reduction modulo \( N \) of the interval \([a, b]\), where \( a \) and \( b \) are representatives of \( a \) and \( b \) in \([-N, \ldots, -1]\) and \( \{1, 2, \ldots, N\} \) respectively.

Let \( \mu_3' \) the set of cubic primitive roots of unity in \( (\mathbb{Z}/N\mathbb{Z})^\times \). Let \( \sigma = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \) and \( \tau = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \in \text{SL}_2(\mathbb{Z}) \). There is a right action of \( \text{SL}_2(\mathbb{Z}) \) on \( \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z}) \) given by \( x \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \frac{ax + c}{bx + d} \) if \( x \in \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z}) \). The set \( (\mathbb{Z}/N\mathbb{Z})^\times \setminus \{\bar{1}, \bar{-1}\} \subset \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z}) \) is stable under \( \sigma \).

Let \( \log_3 : \mathbb{Z}[(\mathbb{Z}/N\mathbb{Z})^\times \setminus \{\bar{1}, \bar{-1}\}] \to \mathbb{Z}/3^{t+1}\mathbb{Z} \) be given by

\[
\log_3 \left( \sum_{x \in (\mathbb{Z}/N\mathbb{Z})^\times \setminus \{\bar{1}, \bar{-1}\}} \lambda_x \cdot [x] \right) = \sum_{x_3 \in \mu_3'} \sum_{y \in [-x_3, x_3]} (\lambda_{y\sigma} - \lambda_y) \cdot \log(x_3).
\]

The following lemma summarizes the properties \( \log_3 \) we will need.

**Lemma 6.9 (Merel)**

(i) If \( a \in (\mathbb{Z}/N\mathbb{Z})^\times \setminus \{\bar{1}, \bar{-1}\} \) is fixed by \( \tau \), then \( \log_3([a]) \equiv \log(a) \) (modulo \( 3^{t+1} \)).

(ii) If \( a \in (\mathbb{Z}/N\mathbb{Z})^\times \setminus \{\bar{1}, \bar{-1}\} \) is fixed by \( \sigma \), then \( \log_3(a) \equiv 0 \) (modulo \( 3^{t+1} \)).

**Proof** Point (i) (resp. point (ii)) follows from [23, Lemme 6] (resp. [23, Lemme 7]).

By Lemma 6.9, the group homomorphism \( \mathbb{Z}[(\mathbb{Z}/N\mathbb{Z})^\times \setminus \{\bar{1}, \bar{-1}\}] \to \mathbb{Z}/3^{t+1}\mathbb{Z} \) given by \([x] \mapsto \log(x) - \log_3(x)\) annihilates the Manin relations, and thus induces a group homomorphism

\[
\varphi_3 : H_1(X_0(N), \mathbb{Z}/3^{t+1}\mathbb{Z}) \to \mathbb{Z}/3^{t+1}\mathbb{Z}.
\]

**Theorem 6.10** Assume \( p = 3 \). Assume \( n(r) \geq 2 \), i.e. \( \sum_{k=1}^{N-1} k^2 \cdot \log(k) \equiv 0 \) (modulo \( 3^r \)). Then we have in \( \mathbb{Z}/3^{t+1}\mathbb{Z} \):

\[
12 \cdot m_1^+ \cdot m_1^- = \log(2) \cdot \varphi_3(m_0^+).
\]
where $F_{1,3} : P^1(\mathbb{Z}/N\mathbb{Z}) \to \mathbb{Z}/3^{r+1}\mathbb{Z}$ is defined in Theorem 5.20.

**Proof** By Theorem 5.20, we have $H_1(X_0(N))$, cusps, $\mathbb{Z}/3^{r+1}\mathbb{Z}$:

$$6 \cdot m_1^+ = \log(2) \cdot m_0^+ + \sum_{x \in (\mathbb{Z}/N\mathbb{Z})^* \setminus \{1, -1\}} F_{1,3}(x) \cdot \xi \Gamma_0(N)([x : 1]).$$

Let $G_0 : (\mathbb{Z}/N\mathbb{Z})^* \setminus \{1, -1\} \to \mathbb{Z}/3^{r}\mathbb{Z}$ be such that

$$m_0^+ = \sum_{x \in (\mathbb{Z}/N\mathbb{Z})^* \setminus \{1, -1\}} G_0(x) \cdot \xi \Gamma_0(N)([x : 1]).$$

Let $G_1 : (\mathbb{Z}/N\mathbb{Z})^* \setminus \{1, -1\} \to \mathbb{Z}/3^{r}\mathbb{Z}$ be such that

$$m_1^+ = \sum_{x \in (\mathbb{Z}/N\mathbb{Z})^* \setminus \{1, -1\}} G_1(x) \cdot \xi \Gamma_0(N)([x : 1]).$$

By Theorem 5.20 and [23, Proposition 3], we have the following equality in $(\mathbb{Z}/3^{r+1}\mathbb{Z})[(\mathbb{Z}/N\mathbb{Z})^* \setminus \{1, -1\}]$:

$$6 \cdot \sum_{x \in (\mathbb{Z}/N\mathbb{Z})^* \setminus \{1, -1\}} G_1(x) \cdot [x] = \log(2) \cdot \sum_{x \in (\mathbb{Z}/N\mathbb{Z})^* \setminus \{1, -1\}} G_0(x) \cdot [x]$$

$$+ \sum_{x \in (\mathbb{Z}/N\mathbb{Z})^* \setminus \{1, -1\}} F_{1,3}(x) \cdot [x] + a_\sigma + a_\tau$$

where $a_\sigma$ (resp. $a_\tau$) is an element of $(\mathbb{Z}/3^{r+1}\mathbb{Z})[(\mathbb{Z}/N\mathbb{Z})^* \setminus \{1, -1\}]$ fixed by $\sigma$ (resp. by $\tau$). By definition, we have in $\mathbb{Z}/3^{r}\mathbb{Z}$:

$$m_1^+ \cdot m_1^- = \frac{1}{2} \cdot \sum_{x \in (\mathbb{Z}/N\mathbb{Z})^* \setminus \{1, -1\}} G_1(x) \cdot \log(x).$$

By Lemma 6.9 (i), we get in $\mathbb{Z}/3^{r+1}\mathbb{Z}$:

$$12 \cdot m_1^+ \cdot m_1^- = \log(2) \cdot \varphi_3(m_0^+)$$

$$+ \varphi_3 \left( \sum_{x \in (\mathbb{Z}/N\mathbb{Z})^* \setminus \{1, -1\}} F_{1,3}(x) \cdot \xi \Gamma_0(N)([x : 1]) \right).$$
which concludes the proof of Theorem 6.10.

\begin{flushright}
\qed
\end{flushright}

**Corollary 6.11** Assume \( t \geq 2 \), i.e. \( N \equiv 1 \) (modulo 27). Assume \( 1 \leq r \leq t - 1 \). If \( n(r) \geq 2 \), i.e. if \( \sum_{k=1}^{N-1} k^2 \cdot \log(k) \equiv 0 \) (modulo \( 3^r \)), then we have in \( \mathbb{Z}/3^r \mathbb{Z} \):

\[
m_1^+ \cdot m_1^- = -\frac{1}{4} \cdot \sum_{k=1}^{N-1} k^2 \cdot \log(k)^2.
\]

**Proof** Since \( r \leq t - 1 \), the map \( \log_3 \) is zero modulo \( 3^{r+1} \). Thus, for all \( x \in (\mathbb{Z}/N\mathbb{Z}) \times \{1, -1\} \) we have \( \varphi_3(\xi_{\Gamma_0(N)}(x)) \equiv \log(x) \) (modulo \( 3^{r+1} \)). In particular, we have

\[
\varphi_3(m_0^+) \equiv 2 \cdot m_0^+ \cdot m_1^- \pmod{3^{r+1}}.
\]

We get, by Theorem 6.4:

\[
\varphi_3(m_0^+) \equiv -\frac{1}{2} \cdot \sum_{k=1}^{N-1} k^2 \cdot \log(k) \pmod{3^{r+1}}.
\]

Thus, we have in \( \mathbb{Z}/3^{r+1} \mathbb{Z} \):

\[
6 \cdot m_1^+ \cdot m_1^- = -\frac{1}{2} \cdot \log(2) \cdot \sum_{k=1}^{N-1} k^2 \cdot \log(k)
+ \sum_{x \in (\mathbb{Z}/N\mathbb{Z}) \times \{1, -1\}} F_{1,3}(x) \cdot \log(x) \quad (80)
\]

Recall that \( F_{1,3} : P^1(\mathbb{Z}/N\mathbb{Z}) \to \mathbb{Z}/3^{r+1} \mathbb{Z} \) is defined by

\[
F_{1,3}([c : d]) = \frac{1}{2} \sum_{(s_1, s_2) \in (\mathbb{Z}/2N\mathbb{Z})^2} \sum_{(d-c)s_1 + (d+c)s_2 \equiv 0 \pmod{N}} \left((-1)^{s_1+s_2} \mathbb{B}_1 \left( \frac{s_1}{2N} \right) \mathbb{B}_1 \left( \frac{s_2}{2N} \right) \cdot \log \left( \frac{s_2}{d-c} \right) - \frac{1}{2} \sum_{(s_1, s_2) \in (\mathbb{Z}/2N\mathbb{Z})^2} \sum_{(d-c)s_1 + (d+c)s_2 \not\equiv 0 \pmod{N}} \left((-1)^{s_1+s_2} \mathbb{B}_1 \left( \frac{s_1}{2N} \right) \mathbb{B}_1 \left( \frac{s_2}{2N} \right) \cdot \log((d-c)s_1 + (d+c)s_2)) \right)
\]

\[\square\] Springer
if $[c : d] \neq [1 : 1]$ and $F_{1,3}([1 : 1]) = 0$. We have, in $\mathbb{Z}/3^{r+1}\mathbb{Z}$:

$$2 \cdot \sum_{x \in (\mathbb{Z}/N\mathbb{Z})^* \setminus [1, -1]} F_{1,3}(x) \cdot \log(x)$$

$$= \sum_{x \in (\mathbb{Z}/N\mathbb{Z})^*} \log(x) \cdot \left( \sum_{(s_1, s_2) \in (\mathbb{Z}/2N\mathbb{Z})^2} (-1)^{s_1+s_2} B_1 \left( \frac{s_1}{2N} \right) B_1 \left( \frac{s_2}{2N} \right) \cdot \log \left( \frac{s_2}{1-x} \right) \right)$$

$$- \log(x) \cdot \left( \sum_{(s_1, s_2) \in (\mathbb{Z}/2N\mathbb{Z})^2} (-1)^{s_1+s_2} B_1 \left( \frac{s_1}{2N} \right) B_1 \left( \frac{s_2}{2N} \right) \cdot \log((1-x)s_1 + (1+x)s_2) \right)$$

$$= \frac{1}{4} \sum_{x \in (\mathbb{Z}/N\mathbb{Z})^*} \log(x) \cdot \left( \sum_{(s_1, s_2) \in (\mathbb{Z}/N\mathbb{Z})^2} D_2 \left( \frac{s_1}{N} \right) D_2 \left( \frac{s_2}{N} \right) \cdot \log \left( \frac{s_2}{1-x} \right) \right)$$

$$- \log(x) \cdot \left( \sum_{(s_1, s_2) \in (\mathbb{Z}/N\mathbb{Z})^2} D_2 \left( \frac{s_1}{N} \right) D_2 \left( \frac{s_2}{N} \right) \cdot \log \left( \frac{s_2}{1-x} \right) \right)$$
\[
D_2 \left( \frac{s_1}{N} \right) D_2 \left( \frac{s_2}{N} \right) \cdot \log((1 - x)s_1 + (1 + x)s_2)
\]

\[
= \frac{1}{4} \sum_{(s_1, s_2) \in (\mathbb{Z}/N\mathbb{Z})^2 \atop s_1 \neq \pm s_2} D_2 \left( \frac{s_1}{N} \right) D_2 \left( \frac{s_2}{N} \right) \cdot \\
\left( \log \left( \frac{s_1 + s_2}{s_1 - s_2} \right) \cdot \log \left( \frac{s_2 - s_1}{2} \right) \right) \\
- \sum_{x \neq \frac{s_1 + s_2}{s_1 - s_2}} \log(x) \log((1 - x)s_1 + (1 + x)s_2)).
\]

Since \( r + 1 \leq t \), Lemma 5.17 shows that we have, in \( \mathbb{Z}/3^{r+1}\mathbb{Z} \):

\[
\sum_{x \neq \frac{s_1 + s_2}{s_1 - s_2}} \log(x) \log((1 - x)s_1 + (1 + x)s_2) \\
= - \log(s_2 - s_1) \log \left( \frac{s_1 + s_2}{s_1 - s_2} \right) - \log \left( \frac{s_1 + s_2}{s_1 - s_2} \right)^2 .
\]

Thus we have, in \( \mathbb{Z}/3^{r+1}\mathbb{Z} \):

\[
2 \sum_{x \in (\mathbb{Z}/N\mathbb{Z})^2 \setminus \{T, -T\}} F_{1,3}(x) \cdot \log(x) \\
= \frac{1}{4} \sum_{(s_1, s_2) \in (\mathbb{Z}/N\mathbb{Z})^2 \atop s_1 \neq \pm s_2} D_2 \left( \frac{s_1}{N} \right) D_2 \left( \frac{s_2}{N} \right) \cdot \\
\left( \log(s_1 + s_2)^2 - \log(s_1 - s_2)^2 - \log(2) \cdot \log \left( \frac{s_1 + s_2}{s_1 - s_2} \right) \right)
\]

Using Lemmas 5.15 and 5.16 and the assumption \( r + 1 \leq t \), we get in \( \mathbb{Z}/3^{r+1}\mathbb{Z} \):

\[
\sum_{x \in (\mathbb{Z}/N\mathbb{Z})^2 \setminus \{T, -T\}} F_{1,3}(x) \cdot \log(x) \\
= - \frac{3}{2} \cdot \sum_{k=1}^{N-1} k^2 \cdot \log(k)^2 + \frac{1}{2} \cdot \log(2) \cdot \sum_{k=1}^{N-1} k^2 \cdot \log(k) .
\]
By (80), we have in \( \mathbb{Z}/3^{t+1}\mathbb{Z} \):

\[
6 \cdot m_1^+ \cdot m_1^- = -\frac{3}{2} \sum_{k=1}^{N-1} k^2 \cdot \log(k)^2.
\]

This concludes the proof of Corollary 6.11.

\[\square\]

**Corollary 6.12** Assume that \( t \geq 2 \), i.e. that \( N \equiv 1 \) (modulo 27). Assume that \( 1 \leq r \leq t - 1 \). The following assertions are equivalent:

(i) \( n(r) \geq 3 \)

(ii) \( \sum_{k=1}^{N-1} k^2 \cdot \log(k) \equiv \sum_{k=1}^{N-1} k^2 \cdot \log(k)^2 \equiv 0 \) (modulo 3').

**Remark 6.6** Corollary 6.12 does not hold in general if \( N \not\equiv 1 \) (modulo 27). For instance, if \( N = 1279 \) and \( r = 1 \) then \( g_3 = 2 \) and \( \sum_{k=1}^{N-1} k^2 \cdot \log(k) \equiv \sum_{k=1}^{N-1} k^2 \cdot \log(k)^2 \equiv 0 \) (modulo 3). If \( N = 1747 \) and \( r = 1 \) then \( g_3 = 3 \) and \( \sum_{k=1}^{N-1} k^2 \cdot \log(k)^2 \not\equiv 0 \) (modulo 3).

### 6.6 Computation of \( m_1^+ \cdot m_1^- \) when \( p = 2 \)

In this section, we assume that \( p = 2 \). We give a formula for \( m_1^+ \cdot m_1^- \) modulo \( 2^{t-1} \). Note that we do not have an explicit formula for \( m_2^- \) modulo \( 2^{t-1} \), but nevertheless it is possible to compute \( m_0^+ \cdot m_2^- = m_1^+ \cdot m_1^- \) modulo \( 2^{t-1} \).

**Theorem 6.13** Assume that \( t \geq 2 \), i.e. that \( N \equiv 1 \) (modulo 16). Let \( r \) be an integer such that \( 1 \leq r \leq t - 1 \) and \( n(r) \geq 2 \) (i.e. \( \sum_{k=1}^{N-1} k \cdot \log(k) \equiv 0 \) (modulo 2^r) by Corollary 6.6). We have, in \( \mathbb{Z}/2^{t+1}\mathbb{Z} \):

\[
6 \cdot m_1^+ \cdot m_1^- = \sum_{k=1}^{N-1} k \cdot \log(k) + \sum_{k=1}^{N-1} k \cdot \log(k)^2.
\]

**Proof** Recall that we have normalized \( \tilde{m}_0^- \), and thus \( m_1^- \), so that for all \( x \in \mathbb{P}(\mathbb{Z}/N\mathbb{Z}) \setminus \{0, \infty\} \) we have, in \( \mathbb{Z}/2^t\mathbb{Z} \):

\[
(1 + c) \cdot \xi_{\Gamma_0(N)}(x) \cdot m_1^- = \log(x).
\]

For all \( x \in (\mathbb{Z}/N\mathbb{Z})^\times \), we have in \( \mathbb{Z}/2^{t+1}\mathbb{Z} \):

\[
F_{1,2}(x) = F_{1,2}(-x). \quad (81)
\]
By Theorems 5.22, 6.4 and (81), we have in $\mathbb{Z}/2^{t+2}\mathbb{Z}$:

$$12 \cdot m^{+}_{1} \cdot m^{-}_{1} = -\frac{2}{3} \cdot \left( 2^{t-1} - \sum_{k=1}^{N-1} k \cdot \log(k) \right)$$

$$+ \sum_{x \in R'} F_{1,2}(x) \cdot \log(x) ,$$

where $R'$ is any set of representative in $(\mathbb{Z}/N\mathbb{Z})^{\times} \setminus \{1, -1\}$ for the equivalence relation $x \sim \frac{-1}{x}$.

Let $\tilde{F}_{1,2} : (\mathbb{Z}/N\mathbb{Z})^{\times} \to \mathbb{Z}/2^{t+2}\mathbb{Z}$ be defined by

$$\tilde{F}_{1,2}(x) = \sum_{s_{1}, s_{2}=1}^{N-1} \log \left( \frac{2}{1-x} \cdot s_{2} \right)$$

$$(1-x)s_{1} + (1+x)s_{2} \equiv 0 \pmod{N}$$

$$- \sum_{s_{1}, s_{2}=1}^{N-1} \log ((1-x)s_{1} + (1+x)s_{2}) ,$$

$$(1-x)s_{1} + (1+x)s_{2} \not\equiv 0 \pmod{N}$$

By definition, for all $x \in (\mathbb{Z}/N\mathbb{Z})^{\times}$ we have

$$F_{1,2}(x) \equiv \tilde{F}_{1,2}(x) \pmod{2^{t+1}} .$$

Lemma 6.14 For all $x \in (\mathbb{Z}/N\mathbb{Z})^{\times}$, we have in $\mathbb{Z}/2^{t+2}\mathbb{Z}$:

$$\tilde{F}_{1,2} \left( \frac{-1}{x} \right) = -\tilde{F}_{1,2}(x) + \frac{N-1}{2} + \frac{N-1}{2} \cdot \log \left( \frac{x-1}{x+1} \right) .$$

Proof Let $x \in (\mathbb{Z}/N\mathbb{Z})^{\times}$. We have, in $\mathbb{Z}/2^{t+1}\mathbb{Z}$:

$$\tilde{F}_{1,2}(x) + \tilde{F}_{1,2} \left( \frac{-1}{x} \right)$$

$$= \sum_{s_{2}=1}^{N-1} \sum_{s_{1}=1}^{N-1} \log \left( \frac{2}{1-x} \cdot s_{2} \right)$$

$$(1-x)s_{1} + (1+x)s_{2} \equiv 0 \pmod{N}$$

$$+ \sum_{s_{2}=1}^{N-1} \sum_{s_{1}=N+1}^{N-1} \log \left( \frac{2 \cdot x}{1-x} \cdot s_{2} \right)$$

$$(1-x)s_{1} + (1+x)s_{2} \equiv 0 \pmod{N}$$
\[
- \sum_{s_2=1}^{N-1} \sum_{s_1=1}^{N-1} \frac{\log ((1-x)s_1 + (1+x)s_2)}{(1-x)s_1 + (1+x)s_2 \not\equiv 0 \pmod{N}}
\]

\[
- \sum_{s_2=1}^{N-1} \sum_{s_1=\frac{N+1}{2}}^{N-1} \frac{\log \left( \frac{1}{x} \cdot ((1-x)s_1 + (1+x)s_2) \right)}{(1-x)s_1 + (1+x)s_2 \not\equiv 0 \pmod{N}}
\]

\[
eq \sum_{s_2=1}^{N-1} \sum_{s_1=1}^{N-1} \frac{\log \left( \frac{2}{1-x} \cdot s_2 \right) + \log(x) \cdot \mathcal{N}(x)}{(1-x)s_1 + (1+x)s_2 \equiv 0 \pmod{N}}
\]

\[
- \sum_{s_2=1}^{N-1} \sum_{s_1=1}^{N-1} \frac{\log ((1-x)s_1 + (1+x)s_2)}{(1-x)s_1 + (1+x)s_2 \not\equiv 0 \pmod{N}}
\]

\[
+ \log(x) \cdot \left( \left( \frac{N-1}{2} \right)^2 - \mathcal{N}(x) \right),
\]

where \(\mathcal{N}(x)\) is the number of \(s \in \{1, 2, \ldots, \frac{N-1}{2}\}\) such that the representative of \(s \cdot \frac{x-1}{x+1}\) in \(\{1, \ldots, N-1\}\) is in \(\{\frac{N+1}{2}, \ldots, N-1\}\). Thus, we have in \(\mathbb{Z}/2^{t+2}\mathbb{Z}\):

\[
\tilde{F}_{1,2}(x) + \tilde{F}_{1,2} \left( -\frac{1}{x} \right) = \sum_{s_2=1}^{N-1} \sum_{s_1=1}^{N-1} \frac{\log \left( \frac{2}{1-x} \cdot s_2 \right)}{(1-x)s_1 + (1+x)s_2 \equiv 0 \pmod{N}}
\]

\[
- \sum_{s_2=1}^{N-1} \sum_{s_1=1}^{N-1} \frac{\log ((1-x)s_1 + (1+x)s_2)}{(1-x)s_1 + (1+x)s_2 \not\equiv 0 \pmod{N}}
\]

\[
= \frac{N-1}{2} \cdot \log \left( \frac{2}{1-x} \right) + \log \left( \left( \frac{N-1}{2} \right)! \right)
\]

\[
- \frac{N-1}{2} \cdot (N-2) \cdot \log(1+x)
\]

\[
- \sum_{s_2=1}^{N-1} \sum_{s_1=1}^{N-1} \frac{\log \left( s_2 - \frac{x-1}{x+1} \cdot s_1 \right)}{(1-x)s_1 + (1+x)s_2 \not\equiv 0 \pmod{N}}
\]

Since \(N \equiv 1 \pmod{8}\), we have \(\log(2) \equiv 0 \pmod{2}\) by the quadratic reciprocity law. Thus we have in \(\mathbb{Z}/2^{t+2}\mathbb{Z}\):
\[
\tilde{F}_{1,2}(x) + \tilde{F}_{1,2}\left(-\frac{1}{x}\right) = \frac{N-1}{2} \cdot \log \left(\frac{x+1}{x-1}\right) + \log \left(\left(\frac{N-1}{2}\right)!\right) - \sum_{s_2=1}^{\frac{N-1}{2}} (\log((N-1)!)-\log(s_2))
\]
\[
= \frac{N-1}{2} \cdot \log \left(\frac{x+1}{x-1}\right) + 2 \cdot \log \left(\left(\frac{N-1}{2}\right)!\right)
\]
\[
= \frac{N-1}{2} + \frac{N-1}{2} \cdot \log \left(\frac{x+1}{x-1}\right).
\]

This concludes the proof of Lemma 6.14. \hfill \Box

Let \(\zeta_4\) be an element of order 4 in \((\mathbb{Z}/N\mathbb{Z})^\times\). Since \(t \geq 2\), we have \(2^t \cdot \log(\zeta_4) = 0\) in \(\mathbb{Z}/2^{t+2}\mathbb{Z}\). Since \(F_{1,2}(\zeta_4) \equiv 0\) (modulo \(2^t\)), we have in \(\mathbb{Z}/2^{t+2}\mathbb{Z}\):

\[
\tilde{F}_{1,2}(\zeta_4) \cdot \log(\zeta_4) = 0 \tag{84}
\]

Similarly, we have in \(\mathbb{Z}/2^{t+2}\mathbb{Z}\):

\[
\tilde{F}_{1,2}(-1) \cdot \log(-1) = 0 \tag{85}
\]

By Lemma 6.14, (84) and (85), we have in \(\mathbb{Z}/2^{t+2}\mathbb{Z}\):

\[
\sum_{x \in (\mathbb{Z}/N\mathbb{Z})^\times} \tilde{F}_{1,2}(x) \cdot \log(x) = \sum_{x \in R'} \tilde{F}_{1,2}(x) \cdot \log(x) + \tilde{F}_{1,2}\left(-\frac{1}{x}\right) \cdot \log \left(-\frac{1}{x}\right)
\]
\[
= 2 \cdot \sum_{x \in R'} \tilde{F}_{1,2}(x) \cdot \log(x) + \sum_{x \in R'} \frac{N-1}{2} \cdot \log(x)
\]
\[
+ \frac{N-1}{2} \cdot \log(x) \cdot \log \left(\frac{x-1}{x+1}\right)
\]
\[
+ \log(-1) \cdot \sum_{x \in R'} \tilde{F}_{1,2}(x).
\]

By (81), we have \(\sum_{x \in R'} F_{1,2}(x) \equiv 0\) (modulo 2). By Lemma 5.17 and the fact that \(\log(-1) \cdot \log(-2) \equiv 0\) (modulo 4), we have

\[
2 \cdot \sum_{x \in R'} \log(x) \cdot \log \left(\frac{x-1}{x+1}\right)
\]
\[
\equiv \sum_{x \in (\mathbb{Z}/N\mathbb{Z})^\times \setminus \{1,-1\}} \log(x) \cdot \log \left(\frac{x-1}{x+1}\right) \equiv 0\) (modulo 4).
Thus, we have in \( \mathbb{Z}/2^{t+2}\mathbb{Z} \):

\[
\sum_{x \in (\mathbb{Z}/N\mathbb{Z})^\times} \tilde{F}_{1,2}(x) \cdot \log(x) = 2 \cdot \sum_{x \in R'} \tilde{F}_{1,2}(x) \cdot \log(x) . \tag{86}
\]

By (82) and (86), we have in \( \mathbb{Z}/2^{t+2}\mathbb{Z} \):

\[
24 \cdot m_1^+ \cdot m_1^- = -\frac{4}{3} \left( 2^{t-1} - \sum_{k=1}^{N-1} k \cdot \log(k) \right) + \sum_{x \in (\mathbb{Z}/N\mathbb{Z})^\times} \tilde{F}_{1,2}(x) \cdot \log(x) . \tag{87}
\]

We have, in \( \mathbb{Z}/2^{t+2}\mathbb{Z} \):

\[
\sum_{x \in (\mathbb{Z}/N\mathbb{Z})^\times} \tilde{F}_{1,2}(x) \cdot \log(x)
\]

\[
= \sum_{x \in (\mathbb{Z}/N\mathbb{Z})^\times} \sum_{s_1, s_2=1 \atop (1-x)s_1+(1+x)s_2 \equiv 0 \text{ (modulo } N)}^{N-1} \log \left( \frac{2}{1-x} \cdot s_2 \right) \cdot \log(x)
\]

\[
- \sum_{x \in (\mathbb{Z}/N\mathbb{Z})^\times} \sum_{s_1, s_2=1 \atop (1-x)s_1+(1+x)s_2 \not\equiv 0 \text{ (modulo } N)}^{N-1} \log ((1-x)s_1 + (1+x)s_2) \cdot \log(x)
\]

\[
= \sum_{s_1, s_2=1 \atop s_1 \neq s_2}^{N-1} \log (s_2 - s_1) \cdot \log \left( \frac{s_1 + s_2}{s_1 - s_2} \right)
\]

\[
- \sum_{s_1, s_2=1 \atop x \not\equiv \frac{s_1+s_2}{s_1-s_2} \text{ (modulo } N)}^{N-1} \log ((1-x)s_1 + (1+x)s_2) \cdot \log(x)
\]

\[
= \sum_{s_1, s_2=1 \atop s_1 \neq s_2}^{N-1} \log (s_2 - s_1) \cdot \log \left( \frac{s_1 + s_2}{s_1 - s_2} \right)
\]

\[
- \sum_{s_1, s_2=1 \atop s_1 \neq s_2}^{N-1} \log(s_2 - s_1) \cdot \left( \log((N-1)! - \log \left( \frac{s_1 + s_2}{s_1 - s_2} \right) \right)
\]
\[ \sum_{s_1, s_2=1 \atop s_1 \neq s_2}^{N-1} \sum_{x \in \mathbb{Z}/N\mathbb{Z}} \log \left( x - \frac{s_1 + s_2}{s_1 - s_2} \right) \cdot \log(x) \]

\[ = 2 \cdot \sum_{s_1, s_2=1 \atop s_1 \neq s_2}^{N-1} \log (s_2 - s_1) \cdot \log \left( \frac{s_1 + s_2}{s_2 - s_1} \right) + \log(-1) \cdot \sum_{s_1, s_2=1 \atop s_1 \neq s_2}^{N-1} \log(s_2 - s_1) \]

\[ + \sum_{s_1, s_2=1 \atop s_1 \neq s_2}^{N-1} \sum_{x \in \mathbb{Z}/N\mathbb{Z}} \log \left( x - \frac{s_1 + s_2}{s_1 - s_2} \right) \cdot \log(x) \cdot \log \left( \frac{s_1 + s_2}{s_1 - s_2} \right) - \log \left( \frac{s_1 + s_2}{s_1 - s_2} \right)^2 + \mathcal{F}_2 \]

By Lemmas 5.13 and 5.17, we have in \( \mathbb{Z}/2^{l+2}\mathbb{Z} \):

\[ \sum_{x \in \mathbb{Z}/N\mathbb{Z}} \tilde{F}_{1,2}(x) \cdot \log(x) = 2 \cdot \sum_{s_1, s_2=1 \atop s_1 \neq s_2}^{N-1} \log (s_1 - s_2) \cdot \log \left( \frac{s_1 + s_2}{s_1 - s_2} \right) \]

\[ + \sum_{s_1, s_2=1 \atop s_1 \neq s_1}^{N-1} \left( \log(-1) \cdot \log \left( \frac{s_1 + s_2}{s_1 - s_2} \right) - \log \left( \frac{s_1 + s_2}{s_1 - s_2} \right)^2 + \mathcal{F}_2 \right) \]

Since \( N \equiv 1 \pmod{8} \), \( 4 \cdot \mathcal{F}_2 = 4 \cdot \mathcal{F}_1 = 0 \) and \( \log(-1) \equiv 0 \pmod{4} \), we have in \( \mathbb{Z}/2^{l+2}\mathbb{Z} \):

\[ \sum_{x \in \mathbb{Z}/N\mathbb{Z}} \tilde{F}_{1,2}(x) \cdot \log(x) = 2 \cdot \sum_{s_1, s_2=1 \atop s_1 \neq s_2}^{N-1} \log (s_1 - s_2) \cdot \log \left( \frac{s_1 + s_2}{s_1 - s_2} \right) \]

\[ - \sum_{s_1, s_2=1 \atop s_1 \neq s_1}^{N-1} \log \left( \frac{s_1 + s_2}{s_1 - s_2} \right)^2 \cdot \log \left( x - \frac{s_1 + s_2}{s_1 - s_2} \right) \cdot \log(x)^2 \]

We have in \( \mathbb{Z}/2^{l+2}\mathbb{Z} \):

\[ \sum_{s_1, s_2=1 \atop s_1 \neq s_2}^{N-1} \log(s_1 + s_2)^2 = \sum_{s_1, s_2=1}^{N-1} \log(s_1 + s_2)^2 - \sum_{s=1}^{N-1} \log(2 \cdot s)^2 \]
\[
\sum_{s_1, s_2 = 1}^{N - 1 \over 2} \log(s_1 + s_2)^2 = \frac{N - 1}{2} + 2 \cdot \sum_{k=1}^{N - 1 \over 2} k \cdot \log(k)^2
\] (89)

and

\[
\sum_{s_1, s_2 = 1}^{N - 1 \over 2} \log(s_1 - s_2)^2 = -2 \cdot \sum_{k=1}^{N - 1 \over 2} k \cdot \log(k)^2
\] (90)

By (88), (89) and (90), we have in \(\mathbb{Z}/2^{t+2}\mathbb{Z}\):

\[
\sum_{x \in (\mathbb{Z}/N \mathbb{Z})^\times} \tilde{F}_{1,2}(x) \cdot \log(x) = \frac{N - 1}{2} + 4 \cdot \sum_{k=1}^{N - 1 \over 2} k \cdot \log(k)^2 + 4 \cdot \sum_{s_1, s_2 = 1}^{N - 1 \over 2} \log(s_1 + s_2) \cdot \log(s_1 - s_2)
\] (91)

We have, in \(\mathbb{Z}/2^{t+2}\mathbb{Z}\):

\[
2 \cdot \sum_{s_1, s_2 = 1}^{N - 1 \over 2} \log(s_1 + s_2) \cdot \log(s_1 - s_2)
= \sum_{s_1 = 1}^{N - 1 \over 2} \sum_{s_2 = 1}^{N - 1 \over 2} \log(s_1 + s_2) \cdot \log(s_1 - s_2)
= \sum_{s_1 = 1}^{N - 1 \over 2} \sum_{s_2 \in (\mathbb{Z}/N \mathbb{Z})^\times} \log(s_1 + s_2) \cdot \log(s_1 - s_2)
\]
\[
\begin{align*}
&= \frac{N-1}{2} \sum_{s_1=1}^{N-1} \sum_{s_2 \in \mathbb{Z}/N\mathbb{Z}^\times \atop s_2 \neq 2s_1, s_1} \log(s_2) \cdot \log(2 \cdot s_1 - s_2) \\
&= \frac{N-1}{2} \sum_{s_1=1}^{N-1} \sum_{s_2 \in \mathbb{Z}/N\mathbb{Z}^\times \atop s_2 \neq 2s_1} \log(s_2) \cdot \log(s_2 - 2 \cdot s_1) \\
&\quad + \log(-1) \cdot \frac{N-1}{2} \sum_{s_1=1}^{N-1} \log(2 \cdot s_1) - \frac{N-1}{2} \sum_{s_1=1}^{N-1} \log(s_1)^2 \\
&= -F_2 + \frac{N-1}{2} \sum_{s_1=1}^{N-1} \sum_{s_2 \in \mathbb{Z}/N\mathbb{Z}^\times \atop s_2 \neq 2s_1} \log(s_2) \cdot \log(s_2 - 2 \cdot s_1) \cdot.
\end{align*}
\]

In the last equality, we have used the fact that \(\log(2) \equiv 0 \pmod{2}\) by the quadratic reciprocity law, since \(N \equiv 1 \pmod{8}\).

\[
2 \cdot \sum_{s_1, s_2 = 1 \atop s_1 \neq s_2}^{N-1} \log(s_1 + s_2) \cdot \log(s_1 - s_2) = -F_2 + \sum_{s_1=1}^{N-1} \left( \log(-1) \cdot \log(2 \cdot s_1) - \log(2 \cdot s_1)^2 + F_2 \right) \\
= -F_2 - \sum_{s_1=1}^{N-1} \log(2 \cdot s_1)^2 \\
= -2 \cdot F_2.
\]

By (91), we have in \(\mathbb{Z}/2^{t+2}\mathbb{Z}\):

\[
\sum_{x \in \mathbb{Z}/N\mathbb{Z}^\times} F_{1,2}(x) \cdot \log(x) = \frac{N-1}{2} + 4 \cdot \sum_{k=1}^{N-1} k \cdot \log(k)^2.
\]

By (87), we have in \(\mathbb{Z}/2^{r+3}\mathbb{Z}\):

\[
24 \cdot m_1^+ \bullet m_1^- = \frac{4}{3} \sum_{k=1}^{N-1} k \cdot \log(k) + 4 \cdot \sum_{k=1}^{N-1} k \cdot \log(k)^2
\]

\(\odot\) Springer
Table 1 Higher Eisenstein elements modulo $p^r$ for $1 \leq r \leq 3$

| $r$ | $e_0$    | $e_1$    | $e_2$ | $e_3$ |
|-----|---------|---------|-------|-------|
| 1   | $X^3$   | $X^2$   | $X$   | 1     |
| 2   | $X^3 + pX^2$ | $X^2 + pX$ | $X + p$ | Not defined |
| 3   | $X^3 + pX^2 + p^2X$ | $X^2 + pX + p^2$ | Not defined | Not defined |

$$= 4 \cdot \sum_{k=1}^{\frac{N-1}{2}} k \cdot \log(k) + 4 \cdot \sum_{k=1}^{\frac{N-1}{2}} k \cdot \log(k)^2.$$ 

In the last equality, we have used the fact that $\sum_{k=1}^{\frac{N-1}{2}} k \cdot \log(k) \equiv 0 \pmod{2^r}$.

This concludes the proof of Theorem 6.13. \qed

**Corollary 6.15** Assume that $t \geq 2$, i.e. that $N \equiv 1 \pmod{16}$. Let $r$ be an integer such that $1 \leq r \leq t - 1$. Assume that $n(r) \geq 2$, (i.e. $\sum_{k=1}^{\frac{N-1}{2}} k \cdot \log(k) \equiv 0 \pmod{2^r}$) by Corollary 6.6. The following assertions are equivalent:

(i) We have $n(r) \geq 3$.

(ii) We have

$$\sum_{k=1}^{\frac{N-1}{2}} k \cdot \log(k) + \sum_{k=1}^{\frac{N-1}{2}} k \cdot \log(k)^2 \equiv 0 \pmod{2^{r+1}}$$

**Remark 6.7** By Remark (6.3), the integer $n(1)$ is odd when $p = 2$. In particular, if $n(1) \geq 2$ then $n(1) \geq 3$. If $N \equiv 1 \pmod{16}$, this means by Corollary 6.15 that $\sum_{k=1}^{\frac{N-1}{2}} k \cdot \log(k) \equiv 0 \pmod{2}$ implies $\sum_{k=1}^{\frac{N-1}{2}} k \cdot \log(k) + \sum_{k=1}^{\frac{N-1}{2}} k \cdot \log(k)^2 \equiv 0 \pmod{4}$. We have not found an elementary proof of this fact.

7 Tables and summary of our results

The following Table 2 for $g_p$ was extracted from the data of [25] (Naskrecki extended his computations to $N < 13,000$, and kindly sent the result to us). We give the 5-uples $(N, p, t, g_p, m)$, where $N$, $p$, $t$ and $g_p$ were defined in the article, and $m$ is the number of conjugacy class of newforms which are congruent to the Eisenstein series modulo $p$. The range is $N < 13,000$, and we only display the data where $p \geq 5$ and $g_p \geq 3$. 

\[\text{Springer}\]
Let \( r \) be an integer such that \( 1 \leq r \leq t = v_p \left( \frac{N-1}{12} \right) \). The following Tables 3, 4 and 5 summarize our results about the integer \( n(r) \) using the three \( \mathbb{T} \)-modules \( M, M^- \) and \( M^+ \) studied in this paper (the equalities below take place in \( \mathbb{Z}/p^n\mathbb{Z} \) unless explicitly stated otherwise).

| Table 2 | Numerical data for \( g_p \) |
|---------|-----------------------------|
| \( N \) | \( p \) | \( t \) | \( g_p \) | \( m \) | \( N \) | \( p \) | \( t \) | \( g_p \) | \( m \) |
| 181     | 5   | 1   | 3   | 1   | 12,101 | 5   | 2   | 4   | 2   |
| 1571    | 5   | 1   | 3   | 1   | 12,301 | 5   | 2   | 3   | 2   |
| 2621    | 5   | 1   | 3   | 1   | 12,541 | 5   | 1   | 3   | 1   |
| 3001    | 5   | 3   | 6   | 3   | 12,641 | 5   | 1   | 4   | 1   |
| 3671    | 5   | 1   | 5   | 1   | 12,791 | 5   | 1   | 3   | 1   |
| 4931    | 5   | 1   | 3   | 1   | 4159  | 7   | 1   | 4   | 1   |
| 5381    | 5   | 1   | 3   | 1   | 4229  | 7   | 1   | 3   | 1   |
| 5651    | 5   | 2   | 4   | 2   | 4957  | 7   | 1   | 3   | 1   |
| 5861    | 5   | 1   | 4   | 1   | 7673  | 7   | 1   | 3   | 1   |
| 6451    | 5   | 2   | 3   | 2   | 10,627 | 7   | 1   | 3   | 1   |
| 9001    | 5   | 3   | 4   | 2   | 11,159 | 7   | 1   | 3   | 1   |
| 9521    | 5   | 1   | 3   | 1   | 1321  | 11  | 1   | 3   | 1   |
| 10,061  | 5   | 1   | 3   | 1   | 6761  | 13  | 2   | 3   | 2   |
| 11,321  | 5   | 1   | 3   | 1   | 1381  | 23  | 1   | 3   | 1   |

Table 3 | The case \( p \geq 5 \)

\[
\begin{align*}
\text{Table 3} \quad & n(r) \geq 2 & n(r) \geq 3 \\
M & \sum_{\lambda \in L} \log(H'(\lambda)) = 0 & \sum_{\lambda \in L} 3 \cdot \log(H'(\lambda))^2 - 4 \cdot \log(\lambda)^2 = 0 \\
M^- & \sum_{k=1}^{N-1} k \cdot \log(k) = 0 & \sum_{k=1}^{N-1} k \cdot \log(k)^2 = 0 \\
M^+ & \sum_{k=1}^{N-1} k^2 \cdot \log(k) = 0 & \sum_{k=1}^{N-1} k^2 \cdot \log(k)^2 = 0
\end{align*}
\]

Table 4 | The case \( p = 3 \)

\[
\begin{align*}
\text{Table 4} \quad & n(r) \geq 2 & n(r) \geq 3, t \geq 2 \text{ and } r \leq t - 1 \\
M^- & \sum_{k=1}^{N-1} k^2 \cdot \log(k) = 0 & \sum_{k=1}^{N-1} k^2 \cdot \log(k)^2 = 0
\end{align*}
\]
Table 5  The case \( p = 2 \)

\[
\begin{array}{|c|c|}
\hline
n(r) \geq 2 & n(r) \geq 3, \ t \geq 2 \text{ and } r \leq t - 1 \\
\hline
M_+ & 2^{t-1} - \sum_{k=1}^{N-1} k \cdot \log(k) = 0 \\
& \sum_{k=1}^{N-1} k \cdot \left( \log(k) + \log(k)^2 \right) \equiv 0 \pmod{2^{r+1}} \\
\hline
\end{array}
\]

Acknowledgements  This article is a part of my Ph.D. thesis, done under the supervision of Prof. Loïc Merel at the Université Paris-Diderot. I would like to express my sincere gratitude to Prof. Merel for his generous help. He suggested that I work on this question of Mazur and he introduced the notion of higher Eisenstein elements. His constant support has been very important for me. I would like to thank Akshay Venkatesh for his comments on my paper, and in particular for sharing his new inspiring proof of Theorem 1.6. I would like to thank various colleagues for interesting discussions related to this work: Tony Feng, Preston Wake, Jun Wang and Carl Wang-Erickson. I would like to thank the anonymous referee for his or her helpful comments, which significantly improved the exposition of this paper. This work was supported by Université Paris-Diderot (now Université de Paris), the Yau Mathematical Sciences Center and Tsinghua University.

References

1. Auer, R., Top, J.: Legendre elliptic curves over finite fields. J. Number Theory 95(2), 303–312 (2002)
2. Banerjee, D., Merel, L.: The Eisenstein cycles as modular symbols. J. Lond. Math. Soc. (2) 98(2), 329–348 (2018)
3. Betina, A., Lecouturier, E.: Congruence formulas for Legendre modular polynomials. J. Number Theory 188, 71–87 (2018)
4. Betina, A., Lecouturier, E.: On the \( p \)-adic periods of the modular curve \( X(\Gamma_0(p) \cap \Gamma(2)) \). Trans. Am. Math. Soc. 371(1), 413–429 (2019)
5. Borwein, J.M., Borwein, P.B.: \( p \)-adic periods and modular symbols of elliptic curves of prime conductor. Invent. Math. 121(2), 225–255 (1995)
6. Deligne, P., Serre, J.-P.: Formes modulaires de poids 1. Ann. Sci. École Norm. Sup. (4) 7(507–530), 1974 (1975)
7. Diamond, F., Shurman, J.: A First Course in Modular Forms. Graduate Texts in Mathematics, vol. 228. Springer, New York (2005)
8. Ireland, K., Rosen, M.: A Classical Introduction to Modern Number Theory, Volume 84 of Graduate Texts in Mathematics, 2nd edn. Springer, New York (1990)
9. Katz, N.: On a Question of Zannier. http://www.math.princeton.edu/~nmk/zannier22.pdf
14. Katz, N.M.: $p$-adic properties of modular schemes and modular forms. Lect. Notes Math. 350, 69–190 (1973)
15. Lecouturier, E.: On the Galois structure of the class group of certain Kummer extensions. J. Lond. Math. Soc. (2) 98(1), 35–58 (2018)
16. Lecouturier, E., Wang, J.: On a conjecture of Sharifi and Mazur’s Eisenstein ideal. To appear in IMRN. https://doi.org/10.1093/imrn/rnaa115
17. Madsen, M.S.: A $p$-adic point counting algorithm for elliptic curves on Legendre form. Finite Fields Appl. 11(1), 71–88 (2005)
18. Manin, Y.: Parabolic points and zeta functions of modular curves. Izv. Akad. Nauk SSSR Ser. Mat. 36, 19–66 (1972)
19. Mazur, B.: Modular curves and the Eisenstein ideal. Inst. Hautes Études Sci. Publ. Math. 47, 33–186 (1978)
20. Mazur, B., Tate, J.: Refined conjectures of the “Birch and Swinnerton-Dyer type”. Duke Math. J. 54(2), 711–750 (1987)
21. Mazur, B., Tate, J., Teitelbaum, J.: On $p$-adic analogues of the conjectures of Birch and Swinnerton-Dyer. Invent. Math. 84(1), 1–48 (1986)
22. Merel, L.: Homologie des courbes modulaires affines et paramétrisations modulaires. Elliptic curves, modular forms, & Fermat’s last theorem (Hong Kong, 1993), Ser. Number Theory, I, pp. 110–130. International Press, Cambridge, MA (1995)
23. Merel, L.: L’accouplement de Weil entre le sous-groupe de Shimura et le sous-groupe cuspidal de $J_0(p)$. J. Reine Angew. Math. 477, 71–115 (1996)
24. Morton, P.: The cubic Fermat equation and complex multiplication on the Deuring normal form. Ramanujan J. 25(2), 247–275 (2011)
25. Naskrecki, B.: On higher congruences between cusp forms and Eisenstein series. In: Computations with Modular Forms, Volume 6 of Contributions in Mathematical and Computational Sciences, pp. 257–277. Springer, Cham (2014)
26. Rebolledo, M.: Module supersingulier et homologie des courbes modulaires. J. Number Theory 121(2), 234–264 (2006)
27. Robert, G.: Congruences entre séries d’Eisenstein, dans le cas supersingulier. Invent. Math. 61(2), 103–158 (1980)
28. Silverman, J.H.: The Arithmetic of Elliptic Curves, Volume 106 of Graduate Texts in Mathematics, 2nd edn. Springer, Dordrecht (2009)
29. Wake, P., Wang-Erickson, C.: The rank of Mazur’s Eisenstein ideal. Duke Math. J. 169(1), 31–115 (2020)
30. Washington, L.C.: Introduction to Cyclotomic Fields, Volume 83 of Graduate Texts in Mathematics, 2nd edn. Springer, New York (1997)
31. Yoo, H.: Non-optimal levels of a reducible mod $\ell$ modular representation. Trans. Am. Math. Soc. 371(6), 3805–3830 (2019)
32. Ribet, K., Yoo, H.: The kernel of an Eisenstein prime at square-free level. Preprint. https://arxiv.org/abs/1712.01717v1

Publisher’s Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.