The kernel of the Eisenstein ideal

by

János Csirik

B.A. (University of Cambridge) 1994

A dissertation submitted in partial satisfaction of the
requirements for the degree of
Doctor of Philosophy

in

Mathematics

in the

GRADUATE DIVISION
of the
UNIVERSITY of CALIFORNIA at BERKELEY

Committee in charge:

Professor Kenneth A. Ribet, Chair
Professor Robert F. Coleman
Professor Steven N. Evans

Spring 1999

The dissertation of János Csirik is approved:

Chair Date

Date

Date

University of California at Berkeley

Spring 1999

The kernel of the Eisenstein ideal

Abstract

The kernel of the Eisenstein ideal

by

János Csirik
Doctor of Philosophy in Mathematics

University of California at Berkeley

Professor Kenneth A. Ribet, Chair

Let N be a prime number, and let $J_0(N)$ be the Jacobian of the modular curve $X_0(N)$. Let $\mathbb{T}$ denote the endomorphism ring of $J_0(N)$. In a seminal 1977 article, B. Mazur introduced and studied an important ideal $I \subseteq \mathbb{T}$, the Eisenstein ideal. In this dissertation we give an explicit construction of the kernel $J_0(N)[I]$ of this ideal (the set of points in $J_0(N)$ that are annihilated by all elements of I). We use this construction to determine the action of the group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $J_0(N)[I]$. Then we apply our results to study the structure of the old subvariety of $J_0(NM)$, where M is a prime number distinct from N. Our results were previously known in the special case where $N - 1$ is not divisible by 16.

Professor Kenneth A. Ribet
Dissertation Committee Chair

This dissertation is dedicated to

my mother, Erzsébet Czachesz;
my father, János Csirik;
and my wife, Susan Harrington.

I thank them for their love and support.

Contents

Acknowledgements

First of all, I thank Ken Ribet for many helpful conversations and for suggesting this problem to me. I also thank Arthur Ogus for telling me some useful facts about étale cohomology.

I thank Matt Baker and Kevin Buzzard for the many fun conversations and seminars we participated in together. I also learned much from conversations with Hendrik W. Lenstra, Jr., and Bjorn Poonen.

I thank Donald Knuth for creating TEX, the typesetting system used for this dissertation, and for assigning it to the public domain. I also thank the creators of the computer program PARI–GP [1], which was used for some preliminary calculations for this dissertation.

Chapter 1

Introduction

Let N be a prime number and let $J_0(N)$ denote the Jacobian of the modular curve $X_0(N)$. The variety $J_0(N)$ possesses certain naturally defined endomorphisms T_ℓ (for all primes $\ell \neq N$) and w. These endomorphisms together with $\mathbb{Z}$ (the multiplications by integers) generate the Hecke ring $\mathbb{T}_N$ of endomorphisms of $J_0(N)$. In his celebrated article *Modular Curves and the Eisenstein Ideal* [11], Mazur defined the Eisenstein ideal I in $\mathbb{T}_N$ as the ideal generated by $1 + w$ and the $1 + \ell - T_\ell$ and used it to identify the possible rational torsion subgroups of elliptic curves defined over the rational numbers. The Galois module $J_0(N)(\overline{\mathbb{Q}})[I]$ plays an important role in [11] and later studies of the arithmetic geometry of the curve $X_0(N)$.

Mazur proved that

$$J_0(N)[I] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

as groups, for $n = (N-1)/\gcd(N-1, 12)$. In this dissertation we will study the action of the group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $J_0(N)[I]$. The group $J_0(N)[I]$ has two noteworthy Galois-invariant subgroups. The cuspidal subgroup C is generated by the divisor $c = 0 - \infty$ (the formal difference of the two cusps of $X_0(N)$). The group C is cyclic of order n and is pointwise fixed by $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. The Shimura subgroup Σ is a finite flat subgroup scheme of $J_0(N)$ such that

$$\Sigma(\overline{\mathbb{Q}}) = \ker(\beta^* : J_0(N) \to J_1(N)),$$

where β^* is induced by the usual degeneracy map $\beta : X_1(N) \to X_0(N)$. The group Σ is also cyclic of order n, but is isomorphic to μ_n as a group scheme.

In this dissertation we shall give an explicit construction of $J_0(N)[I]$, and apply the construction in various ways. Mazur's paper [11] contains an explicit construction of $J_0(N)[I]$ only in the case $N \not\equiv 1 \pmod{16}$, although he remarks in a few places that a general description would be desirable. Our construction identifies the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $J_0(N)[I]$.

If n is odd (equivalently $N \not\equiv 1 \pmod 8$) then $C \cap \Sigma = 0$, so $J_0(N)[I] \cong C \oplus \Sigma$ and therefore we know the Galois action on $J_0(N)[I]$.

If n is even then $C \cap \Sigma \neq 0$ and more is needed to find the Galois action. In this case $C + \Sigma$ has index 2 in $J_0(N)[I]$. Therefore it suffices to find an "extra" point P in $J_0(N)[I]$ that is not in $C + \Sigma$. The knowledge of the Galois action on P, Σ and C then gives a description of the $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-action of $J_0(N)[I]$. For the case $n \equiv 2 \pmod 4$ (or equivalently $N \equiv 9 \pmod{16}$), Mazur finds P by considering the Nebentypus covering $X_0^{\#}(N) \to X_0(N)$ of degree 2. Using a function constructed by Ogg and Ligozat, he obtains a divisor d on $X_0^{\#}(N)$ which turns out to be the pullback of a certain divisor on $X_0(N)$ that gives the extra point on $J_0(N)$.

This dissertation uses other coverings $X_0^{\#}(N) \to X_0(N)$ to generalize Mazur's construction and find extra points of $J_0(N)[I]$ for any $N \equiv 1 \pmod 8$. To find suitable divisors on our modular curves $X_0^{\#}(N)$, we use the theory of modular units: rational functions on a modular curve whose divisors are concentrated at the cusps. Our coverings $X_0^{\#}(N) \to X_0(N)$ are all intermediate to $X_1(N) \to X_0(N)$, enabling us to rely on the theory of modular units on $X_1(N)$. The units of $X(N)$ are treated in Kubert and Lang's [8]. We recall some of their results in Chapter 2. We then use the results of Chapter 2 to develop some results about the units of $X_1(N)$ in Chapter 3. (The references [6, 8] also treat this case but restrict their attention to units whose divisors are supported at the rational cusps, and don't explicitly give the data necessary for the descent to $X_0^{\#}(N)$.) In Chapter 4, we construct a divisor on $X_0^{\#}(N)$ and establish properties of the divisor that make our later arguments work. In Chapter 5, we prove that the extra point we obtain is in $J_0(N)[I]$ and use this fact to prove the following theorem, conjectured by Ribet. For any positive integer k, let χ_k denote the kth cyclotomic character $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to (\mathbb{Z}/k\mathbb{Z})^\times$ obtained via the identification $\mathrm{Gal}(\mathbb{Q}(\mu_k)/\mathbb{Q})) \cong (\mathbb{Z}/k\mathbb{Z})^\times$.

Theorem 1.1 $J_0(N)[I]$ *has a basis* e_1, e_2 *over* $\mathbb{Z}/n\mathbb{Z}$ *such that*

a) $c = e_1 + 2e_2$*;*

b) e_1 *generates* Σ*;*

c) $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *acts via left multiplication by*

$$\begin{pmatrix} \chi_n(\sigma) & (1-\chi_{2n}(\sigma))/2 \\ 0 & 1 \end{pmatrix}$$

with respect to the given basis $e_1 = \binom{1}{0}$, $e_2 = \binom{0}{1}$.

In Chapters 6 and 7, we give another application of our construction of $J_0(N)[I]$.

Let M be a prime number distinct from N. The old part of $J_0(NM)$ is the abelian subvariety of $J_0(NM)$ generated by

$$A = \mathrm{im}(\alpha : J_0(N)^2 \to J_0(NM)) \quad \text{and} \quad B = \mathrm{im}(\beta : J_0(M)^2 \to J_0(NM)),$$

where α and β are certain naturally defined degeneracy morphisms (to be specified precisely in Chapter 6). Each of A and B was determined by Ribet in [16]. Therefore, to complete the description of the old part of $J_0(NM)$, we need to determine $A \cap B$. This project was carried out partially by Ribet in [18], where he determined the odd part of $A \cap B$. In [9], Ling went on to obtain partial results about the even part of $A \cap B$ when neither N nor M is congruent to 1 modulo 16. In Chapter 6, we prove that $A \cap B$ is Eisenstein and we use Theorem 1.1 to completely determine $A \cap B$ to obtain

Theorem 1.2 *Let* N *and* M *be distinct primes. Let* $m = (M-1)/\gcd(M-1, 12)$*, and let* $D^{-,-} = P_1 - P_N - P_M + P_{NM} \in J_0(NM)$. *Then* $A \cap B$ *is the unique subgroup of order* $\gcd(n, m)$ *of the cyclic group generated by* $D^{-,-}$.

The symbols P_1, P_N, P_M and P_{NM} are the conventional names for the cusps of $X_0(NM)$. Their meaning will be explained in Chapter 6. Theorem 1.2 answers questions in [18], [16] and [12].

Chapter 7 contains some modular unit calculations that are used in Chapter 6.

Chapter 2

Notation and setup

For any non-zero rational number x, let $\mathrm{num}(x)$ denote the numerator of x, that is, the smallest positive integer n such that n/x is an integer.

We will now briefly summarize the relevant properties of the modular curves we will be using. The reader can find a thorough treatment of these in [3], as well as in the references cited below.

Let N be a positive integer. We shall consider the usual modular curves $X_0(N)$, $X_1(N)$ and $X(N)$, and their Jacobians $J_0(N)$, $J_1(N)$ and $J(N)$. These correspond to the moduli problems of classifying an elliptic curve with a cyclic subgroup of order N, an elliptic curve with a point of order N, and an elliptic curve with an embedding of $\mu_N \times \mathbb{Z}/N\mathbb{Z}$ compatible with the Weil pairing, respectively. These curves are all defined over $\mathbb{Q}$, as are the usual degeneracy maps (which are Galois coverings) $\alpha : X(N) \to X_1(N)$, $\beta : X_1(N) \to X_0(N)$ and $\gamma = \beta \circ \alpha$.

The curves $X_0(N)_{\mathbb{C}}$, $X_1(N)_{\mathbb{C}}$ and $X(N)_{\mathbb{C}}$ can also be regarded as compactified quotients of the complex upper half plane $\mathfrak{H}^*/\Gamma_0(N)$, $\mathfrak{H}^*/\Gamma_1(N)$ and $\mathfrak{H}^*/\Gamma(N)$, respectively, where

$$\begin{aligned}
\Gamma_0(N) &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2\mathbb{Z} : c \equiv 0 \pmod{N} \right\}, \\
\Gamma_1(N) &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2\mathbb{Z} : c \equiv 0, d \equiv 1 \pmod{N} \right\}, \\
\Gamma(N) &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2\mathbb{Z} : a \equiv 1, b \equiv 0, c \equiv 0, d \equiv 1 \pmod{N} \right\},
\end{aligned}$$

and these subgroups of $\mathrm{SL}_2\mathbb{Z}$ act on the complex upper half plane $\mathfrak{H}$ via fractional linear transformations. The points introduced during the compactification are called cusps.

Now let N be an odd prime number, and let

$$r = (N-1)/2.$$

The curve $X_0(N)$ has two cusps, denoted 0 and ∞. They are both defined over $\mathbb{Q}$ and are distinguished by the fact that under the natural map $X_0(N)_{\mathbb{C}} = \mathfrak{H}^*/\Gamma_0(N) \to X(1)_{\mathbb{C}} = \mathfrak{H}^*/SL_2\mathbb{Z}$, the cusp 0 is ramified with index N and the cusp ∞ is unramified.

The curve $X_1(N)$ has $N-1$ cusps that come in two groups. We shall use Klimek's notation in [6] for them. The cusps $P_1, P_2, \dots, P_r$ are defined over $\mathbb{Q}$ and are mapped to 0 under $\beta : X_1(N) \to X_0(N)$. The cusps $Q_1, Q_2, \dots, Q_r$ are defined over $\mathbb{Q}(\mu_N)^+$ (the maximal totally real subfield of the Nth cyclotomic field) and are mapped to ∞ under β. All the cusps of $X_1(N)$ are unramified with respect to β.

The curve $X(N)$ has $(N^2-1)/2$ cusps and we use Shimura's notation in [15] to regard them as pairs $\pm\binom{x}{y}$ with $x, y \in \mathbb{F}_N$, not both equal to 0. In this representation, $\mathrm{Gal}(X(N)_{\mathbb{C}}/X_0(N)_{\mathbb{C}}) \cong PSL_2\mathbb{F}_N$ acts naturally from the left. For $1 \le i \le r$, the cusps $\binom{*}{i}$ are all defined over $\mathbb{Q}(\mu_N)$ and map unramifiedly to P_i under $\alpha : X(N) \to X_1(N)$. For $1 \le i \le r$, the cusps $\binom{i}{0}$ are all defined over $\mathbb{Q}(\mu_N)^+$ and map to Q_i under α with ramification index N.

Shimura's notation can be used to label the cusps of any modular curve. We shall now provide the translations to Shimura's system of all the names we use. On the curve $X_0(N)$, the cusps 0 and ∞ (respectively) are called $\binom{0}{1}$ and $\binom{1}{0}$ (respectively). On the curve $X_1(N)$, for any $1 \le t \le r$, our notation P_t corresponds to $\binom{0}{t}$, while Q_t corresponds to $\binom{t}{0}$.

Recall that a *unit* of a modular curve is a rational function on the curve that has its divisor concentrated at the cusps. (It is a unit of the ring of rational maps from the noncuspidal points of the curve to the affine line.) In [8], Kubert and Lang determined all the units of $X(N)$. We briefly recall their results here, using $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ as the indexing group instead of their $\frac{1}{N}\mathbb{Z}/\mathbb{Z} \times \frac{1}{N}\mathbb{Z}/\mathbb{Z}$. Let $e = (e_1, e_2)$ be a pair of integers such that not both of e_1 and e_2 are divisible by N. One can use the classical Weierstrass σ and Dedekind η functions to define the Klein form $k_e(\tau)$ on $\mathfrak{H}$. This form enjoys the properties

$$\forall \alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2\mathbb{Z}, \qquad k_e(\alpha\tau) = (c\tau + d)^{-1} k_{e\alpha}(\tau) \tag{K1}$$

(where $e\alpha$ denotes usual matrix multiplication) and

$$\forall f = (f_1, f_2) \in N\mathbb{Z} \times N\mathbb{Z}, \qquad k_{e+f}(\tau) = \varepsilon(e, f) k_e(\tau), \tag{K2}$$

where

$$\varepsilon(e,f) = (-1)^{\frac{f_1 f_2}{N^2}+\frac{f_1}{N}+\frac{f_2}{N}} \exp\left(\frac{\pi i}{N^2}(e_1 f_2 - e_2 f_1)\right).$$

These Klein forms are then used to define for all $e = (e_1, e_2) \in (\mathbb{Z} \times \mathbb{Z}) \setminus (N\mathbb{Z} \times N\mathbb{Z})$ the *Siegel function*

$$g_e(\tau) = k_e(\tau)\eta^2(\tau).$$

Recall that

$$\forall \alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2\mathbb{Z}, \qquad \eta^2(\alpha\tau) = \psi(\alpha)(c\tau + d)\eta^2(\tau), \tag{N}$$

where ψ is defined by its values on the two standard generators of $SL_2\mathbb{Z}$ as

$$\psi\left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\right) = \exp(\frac{\pi i}{6}), \qquad \psi\left(\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\right) = \exp(\frac{\pi i}{2}) = i.$$

Now [8, Chapter 4, Theorem 1.3] says

Theorem 2.1 *The units of* $X(N)_{\mathbb{C}}$ *are exactly the functions of the form*

$$g = c \prod_{e \in E} g_e(\tau)^{m(e)},$$

for some constant c *and some finite set* $E \subseteq \mathbb{Z} \times \mathbb{Z}$*, where the* $m(e)$ *satisfy the conditions*

$$\sum_{e \in E} m(e) \equiv 0 \pmod{12}, \tag{U1}$$

$$\sum_{e=(e_1,e_2) \in E} e_1^2 m(e) \equiv 0 \pmod{N}, \tag{U2}$$

$$\sum_{e=(e_1,e_2) \in E} e_1 e_2 m(e) \equiv 0 \pmod{N}, \tag{U3}$$

$$\sum_{e=(e_1,e_2) \in E} e_2^2 m(e) \equiv 0 \pmod{N}. \tag{U4}$$

The order of such a g at a cusp $P = \binom{x}{y}$ of $X(N)$ is as follows. Pick some $\alpha \in PSL_2\mathbb{F}_N$ such that $\alpha\binom{1}{0} = P$, and let $\hat{\alpha}$ be some lift of α to $SL_2\mathbb{Z}$. Let $(c_1(e), c_2(e)) = e\hat{\alpha}$ be the components of the usual matrix product of e and $\hat{\alpha}$; thus, we may take $c_1(e) = xe_1 + ye_2$. Then

$$\mathrm{ord}_P(g) = \sum_{e \in E} m(e) \frac{N}{2} B_2\left(\frac{c_1(e) \bmod N}{N}\right), \tag{2.1}$$

where $B_2(X) = X^2 - X + 1/6$ is the second Bernoulli polynomial, and we used $x \bmod N$ to denote the smallest non-negative residue of x modulo N. For details and a derivation using the q-expansion of g, see [8, Chapter 2, §3].

Let $e \in E$ and $\alpha \in SL_2\mathbb{Z}$. From (K1) and (N), we conclude that

$$g_e(\alpha\tau) = \psi(\alpha) g_{e\alpha}(\tau), \tag{2.2}$$

so using (U1) and the fact that $\psi(\alpha)^{12} = 1$ for any α, for $g(\tau) = c \prod_{e \in E} g_e(\tau)^{m(e)}$ we have

$$g(\alpha\tau) = c \prod_{e \in E} g_{e\alpha}(\tau)^{m(e)}. \tag{2.3}$$

By (K2), if $e \equiv e' \pmod N$, then $g_e/g_{e'}$ is a root of unity. By (K1) with $\alpha = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, if $e + e' = (0,0)$, then $g_e/g_{e'} = -1$ (here we also used the fact that with this α, the ψ and the $c\tau + d$ factors in (N) are both -1, and so they multiply to 1). Hence all units of $X(N)_{\mathbb{C}}$ can be put into the form $g = c' \prod_{e \in E'} g_e(\tau)^{m(e)}$, with

$$\begin{array}{rccccc} E' = & \{ & (0,1), & (0,2), & \ldots, & (0,r), & \\ (1,0), & (1,1), & (1,2), & & \ldots, & & (1,N-1), \\ (2,0), & (2,1), & (2,2), & & \ldots, & & (2,N-1), \\ \vdots & & & & & & \\ (r,0), & (r,1), & (r,2), & & \ldots, & & (r,N-1) \quad \}. \end{array}$$

Kubert and Lang [8, Chapter 5, Theorem 3.1] then prove that the degree zero divisors on $X(N)$ concentrated at the cusps span a finite subgroup of the divisor class group (this was also proved in general for all modular curves by Manin and Drinfeld, see [10, footnote to Corollary 3.6]). The number of cusps on $X(N)$ is $(N^2 - 1)/2$, which is also the cardinality of the set E'. Since the divisor of a rational function has degree 0, this implies that the functions g_e with $e \in E'$ are independent except for a single relation. A simple calculation using (2.1) shows that $\prod_{e \in E'} g_e(\tau)$ is a constant, providing the sought-after relation. To sum up, we have shown that

Fact 2.2 *The function $g = c \prod_{e \in E'} g_e(\tau)^{m(e)}$ is constant if and only if the $m(e)$ are the same for all $e \in E'$.*

Chapter 3

The Units of $X_1(N)$

We now determine units of $X_1(N)_{\mathbb{C}}$. They can be identified with the units of $X(N)_{\mathbb{C}}$ that are invariant under $\mathrm{Gal}(X(N)_{\mathbb{C}}/X_1(N)_{\mathbb{C}})$, which is generated by $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{Gal}(X(N)_{\mathbb{C}}/X(1)_{\mathbb{C}}) \cong \mathrm{PSL}_2\mathbb{F}_N$. Therefore the units of $X_1(N)$ can be determined from the knowledge of the units of $X(N)$ and their transformation properties under T.

Definition 3.1 *For all* $1 \leq i \leq r$, *let*

$$g_i(\tau) = g_{(0,i)}(\tau)$$

and

$$s_i(\tau) = \prod_{j=0}^{N-1} g_{(i,j)}(\tau).$$

Theorem 3.2 *The units of* $X_1(N)_{\mathbb{C}}$ *are exactly the functions of the form*

$$g(\tau) = c \prod_{i=1}^{r} g_i(\tau)^{c_i} s_i(\tau)^{d_i},$$

where c *is a constant and the* c_i *and* d_i *satisfy*

$$\sum_{i=1}^{r} c_i + N \sum_{i=1}^{r} d_i \equiv 0 \pmod{12}, \tag{V1}$$

$$\sum_{i=1}^{r} i^2 c_i \equiv 0 \pmod{N}, \tag{V2}$$

$$\sum_{i=1}^{r} i^2 d_i \equiv 0 \pmod{N}, \tag{V3}$$

PROOF. Let $g(\tau) = c\prod_{e\in E'} g_e(\tau)^{m(e)}$ be a unit of $X(N)$. By determining the conditions the $m(e)$ must satisfy to be invariant under T, we can find a criterion for g to be a unit of $X_1(N)$. Assume then that g is invariant under the action of T. By (2.3) and Fact 2.2, $m : E' \to \mathbb{Z}$ must be constant on the orbits of T (acting on E' from the right). Since $(e_1, e_2)T = (e_1, e_1 + e_2)$, this shows that g can be written as a product of g_i and s_i as above, with $c_i = m((0, i))$ and $d_i = m((i, 0)) = m((i, 1)) = \cdots = m((i, N-1))$.

Condition (U1) translates immediately to (V1).

The condition (U2) translates as

$$\sum_{e\in E'} e_1^2 m(e) = N\sum_{i=1}^{r} i^2 d_i \equiv 0 \pmod N,$$

so it is necessarily satisfied. The condition (U3) translates as

$$\sum_{e\in E'} e_1 e_2 m(e) = \sum_{i=1}^{r} i \sum_{j=0}^{N-1} j d_i = \sum_{i=1}^{r} iNr d_i \equiv 0 \pmod N,$$

so it is also necessarily satisfied. Lastly, (U4) in our case is

$$\sum_{e\in E'} e_2^2 m(e) = \sum_{i=0}^{r} i^2 c_i + \sum_{j=0}^{r}\sum_{i=0}^{N-1} i^2 d_j = \sum_{i=0}^{r} i^2 c_i + N\frac{(2N-1)r}{3}\sum_{j=0}^{r} d_j \equiv 0 \pmod N.$$

Since N is not divisible by 3, $r(2N-1)$ must be, so (U4) translates to (V2).

It remains to check that our function g is actually invariant under the action of T, as opposed to being just invariant up to multiplication by a constant. This is not automatic, despite the fact that (2.3) has no extra constant factors. Indeed, by restricting our indexing set to E' we sometimes have to convert some g_e (with $e \notin E'$) occurring in (2.3) to some $g_{e'}$ with $e' \in E'$, thereby introducing a factor of a root of 1.

Using (K2), we can see that when we are acting by T on our g, this factor will be

$$\begin{aligned}\prod_{j=1}^{r}\prod_{k=0}^{j-1} \varepsilon((j,k),(0,N))^{d_j} &= \prod_{j=1}^{r}\prod_{k=0}^{j-1}(-1)^{d_j}\exp\left(\frac{\pi i}{N} j d_j\right) \\ &= \prod_{j=1}^{r}(-1)^{j d_i}\exp\left(\frac{\pi i}{N} j^2 d_j\right).\end{aligned}$$

Hence to ensure invariance, we need

$$N\sum_{j=1}^{r} j d_j + \sum_{j=1}^{r} j^2 d_j \equiv 0 \pmod{2N}.$$

The condition mod 2 is automatic since N is odd and $j \equiv j^2 \pmod 2$. The condition mod N is just (V3).

It is also clear from the above calculations that any such g as given in the statement of the theorem satisfies (U1–4) and hence is actually a T-invariant unit of $X(N)$, so we have completed the proof. ■

REMARK. For any i, the Atkin–Lehner involution (associated to the matrix $\left(\begin{smallmatrix} 0 & 1 \\ -N & 0 \end{smallmatrix}\right)$) interchanges the functions g_i and s_i up to constants. (For more details, see the proof of Theorem 3.5.) Therefore, we expect the conditions (V1–3) to be invariant under exchanging the c_is and the d_is. This is clear for (V2) and (V3), but it is also true for (V1). Indeed, since $(N, 6) = 1$, we have $N^2 \equiv 1 \pmod{12}$, and hence

$$12 \mid C + ND \quad \Longleftrightarrow \quad 12 \mid N^2C + ND \quad \Longleftrightarrow \quad 12 \mid NC + D,$$

where we used the notation $C = \sum_{i=1}^{r} c_i$ and $D = \sum_{i=1}^{r} d_i$.

Theorem 3.3 *The order of such a function g (mentioned in Theorem 3.2) at the cusps is*

$$\begin{aligned} \mathrm{ord}_{P_t}(g) &= \sum_{i=1}^{r} \left(\frac{c_i N}{2} B_2 \left(\frac{it \bmod N}{N} \right) + \frac{d_i}{12} \right) \\ \mathrm{ord}_{Q_t}(g) &= \sum_{i=1}^{r} \left(\frac{c_i}{12} + \frac{d_i N}{2} B_2 \left(\frac{it \bmod N}{N} \right) \right). \end{aligned}$$

PROOF. A straightforward calculation using (2.1) and the fact that $\sum_{i=1}^{r} B_2(i/N) = -r/(6N)$ gives the order of g at the cusps of $X(N)$. Then, using the ramification indices of the cusps of $X(N)$ over the cusps of $X_1(N)$, we obtain our result. ■

Finally, we give the transformation properties of our functions under the Galois group of $X_1(N)_{\mathbb{C}}$ over $X_0(N)_{\mathbb{C}}$.

Definition 3.4 *As in [15, §2], for a odd positive integer u, let*

$$\{\cdot\}_u : \mathbb{Z} \to \{0, 1, \ldots, (u-1)/2\}$$

be the function defined by

$$\{a\}_u \equiv \pm a \pmod u.$$

For brevity, let $\{\cdot\}$ denote $\{\cdot\}_N$.

Theorem 3.5 *For any* $b \in \{1, \dots, r\}$ *and* $\alpha = \left(\begin{smallmatrix} s & f \\ Nh & t \end{smallmatrix}\right) \in \Gamma_0(N)$, *we have*

$$g_b(\alpha\tau) = \psi(\alpha)\kappa(\alpha; b)g_{\{bt\}}(\tau),$$

with

$$\kappa(\alpha; b) = (-1)^{bh} \exp\left(\pi i \left(-\frac{b^2ht}{N}\right)\right)(-1)^{\lfloor bt/N \rfloor}.$$

Although this fact will not be needed later, for reference we state that for any $a \in \{1, \dots, r\}$ *and* α *as above, we have*

$$s_a(\alpha\tau) = \psi(\alpha)^N \kappa'(\alpha; a)s_{\{as\}}(\tau),$$

with

$$\kappa'(\alpha; a) = (-1)^{af} \exp\left(\pi i \left(\frac{a^2sf}{N} + r\frac{a - \{as\}}{N}\right)\right)(-1)^{\lfloor as/N \rfloor}.$$

Proof. Using (2.2) we obtain

$$\begin{aligned} g_b(\alpha\tau) &= g_{(0,b)}(\alpha\tau) = \psi(\alpha)g_{(0,b)\alpha}(\tau) = \psi(\alpha)g_{(bhN,bt)}(\tau) \\ &= \psi(\alpha)\varepsilon((0, bt), (bhN, 0))g_{(0,bt)}(\tau) \\ &= \psi(\alpha)(-1)^{bh} \exp\left(\frac{\pi i}{N}(-b^2ht)\right) g_{(0,bt)}(\tau). \end{aligned}$$

If $bt \equiv \{bt\} \pmod N$ then

$$\begin{aligned} g_{(0,bt)}(\tau) &= \varepsilon((0, \{bt\}), (0, N\lfloor bt/N \rfloor))g_{(0,\{bt\})}(\tau) \\ &= (-1)^{\lfloor bt/N \rfloor} g_{\{bt\}}(\tau). \end{aligned}$$

If $bt \equiv -\{bt\} \pmod N$ then

$$\begin{aligned} g_{(0,bt)}(\tau) &= \varepsilon((0, -\{bt\}), (0, N(\lfloor bt/N \rfloor + 1)))g_{(0,-\{bt\})}(\tau) \\ &= (-1)^{\lfloor bt/N \rfloor} g_{\{bt\}}(\tau). \end{aligned}$$

In either case, this completes the proof of the formula for $g_b(\alpha\tau)$.

For $s_a(\alpha\tau)$, a similar but more involved calculation can be used. Alternatively, one might use the Atkin–Lehner involution $w_N = \left(\begin{smallmatrix} 0 & 1 \\ -N & 0 \end{smallmatrix}\right) \in SL_2\mathbb{Z}$ and the q-expansion of $g_{(e_1,e_2)}$ in [8, Chapter 2, §1, K4] via the identity $w_N(\tau) = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)(N\tau)$ to conclude that

$g_a(w\tau)/s_a(\tau) = c\exp(\pi i r a/N)$, for some constant c that does not depend on a, and thereby reduce the calculation to the one done above. ■

REMARK. Theorems 3.2 and 3.3 allow us to determine the group of divisors supported at the cusps for any particular N. For example, consider the conjecture by Klimek in [6, p. 3]. Let $J_1^\infty(N)$ denote the group of divisors on $X_1(N)$ supported at the set $\{P_1, P_2, \ldots, P_r\}$. Klimek proved that

$$\#J_1^\infty(N) = 4^{1-r} N \prod_{\chi \neq 1} B_{2,\chi},$$

(where χ runs over all non-trivial even characters of $(\mathbb{Z}/N\mathbb{Z})^\times$, and $B_{2,\chi}$ denotes the generalized Bernoulli numbers of Kubota-Leopoldt, see also [8, Chapter 6, Theorem 3.4] for another proof), and conjectured (presumably without the benefit of a computer) that the group $J_1^\infty(N)$ is always cyclic. He confirmed this conjecture for all $N \leq 23$. A simple (computer-aided) calculation using Theorems 3.2 and 3.3 shows that the conjecture is false for $N = 29$. We obtain

N	$J_1^\infty(N)$
$2,3,5,7$	0
11	$\mathbb{Z}/5\mathbb{Z}$
13	$\mathbb{Z}/19\mathbb{Z}$
17	$\mathbb{Z}/584\mathbb{Z}$
19	$\mathbb{Z}/4383\mathbb{Z}$
23	$\mathbb{Z}/37181\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}$
29	$\mathbb{Z}/64427244\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$
31	$\mathbb{Z}/1772833370\mathbb{Z} \times \mathbb{Z}/10$
$\vdots$	$\vdots$

Chapter 4

Some units on $X_0^{\#}(N)$

Assume from now on that

$$\boxed{N \equiv 1 \pmod 8,}$$

(in particular $N \geq 17$).

Definition 4.1 *Let* C_N *denote the group* $(\mathbb{Z}/N\mathbb{Z})^{\times}/\pm 1$.

Since $\beta : X_1(N)_{\mathbb{C}} \to X_0(N)_{\mathbb{C}}$ is a cyclic Galois covering of degree r, it has a unique intermediate covering of $X_0(N)_{\mathbb{C}}$ of any degree dividing r. Because of its uniqueness, any such curve is defined over $\mathbb{Q}$ (for a thorough treatment of these intermediate curves, see [2, IV, §3]). Letting $n = (N-1)/\gcd(N-1, 12)$, we know from [11, II, §2] that the intermediate curve $X_2(N)_{\mathbb{C}} \to X_0(N)_{\mathbb{C}}$ of degree n (the *Shimura covering*) is the largest étale covering of $X_0(N)_{\mathbb{C}}$ through which β factors. (As remarked before, the cusps of $X_0(N)$ are not branch points for β; it is the points with $j = 0$ and $j = 1728$ that ramify in β.)

Definition 4.2 *Write* n *as*

$$n = 2^k \nu$$

where 2^k *is the largest power of 2 that divides* n *(and* $\nu = n/2^k$ *is an odd integer). Set* $z = 3$ *if* $N \equiv 1 \pmod 3$ *and* $z = 1$ *otherwise. For future use, we also set* $q = 3/z$ *here.*

Let

$$\phi : X_0^{\#}(N) \to X_0(N)$$

be the unique covering of degree 2^k *through which* β *factors. Let* $J_0^{\#}(N) = \mathrm{Jac}(X_0^{\#}(N))$.

Observe that the definitions of k, ν, z imply that

$$r = 2^{k+1} z\nu.$$

Since 2^k divides n, the Shimura covering factors through ϕ. This implies that ϕ is étale and that $\Sigma_0 = \ker(\phi^* : J_0(N) \to J_0^{\#}(N))$ is contained in $\Sigma = \ker(J_0(N) \to J_2(N))$.

The Galois group $X_1(N)_{\mathbb{C}}$ over $X_0(N)_{\mathbb{C}}$ is isomorphic to C_N, with $\left(\begin{smallmatrix} s & f \\ Nh & t \end{smallmatrix}\right)$ mapping to $\{t\}$. Let ξ be a generator of C_N. We will abuse notation to lighten it, and let the same ξ denote the generator of $\mathrm{Gal}(X_1(N)_{\mathbb{C}}/X_0(N)_{\mathbb{C}}) \cong C_N$ and the corresponding generator of the Galois group of the function field extension; so that $(\xi f)(\tau) = f(\xi\tau)$ for all functions f on $X_1(N)$. Let Ω denote the set of 2^kth powers in C_N. Then Ω is the Galois group of $X_1(N)$ over $X_0^{\#}(N)$ and

$$\#\Omega = 2z\nu.$$

By its uniqueness property, $X_0^{\#}(N)$ is Galois over $X_0(N)$.

The curve $X_0^{\#}(N)$ is the coarse moduli space for the problem of classifying elliptic curves with a point of order N, where (E, P) and (E', P') are to be considered equivalent if there is an isomorphism $\delta : E \to E'$ such that $\delta(P) = \pm b \cdot P'$ for some $b \in \Omega$.

We shall now construct some units of $X_0^{\#}(N)$. They will first be given as units of $X_1(N)$, and to check that they are actually units of $X_0^{\#}(N)$ we shall need the following lemmas. In these lemmas (and later), for any element $b \in C_N$ we let $\widetilde{b}$ denote the representative for b in the set $\{1, 2, \ldots, r\}$. For example, $\sum_{b \in C_N} \widetilde{b} = \sum_{i=1}^{r} i = r(r+1)/2$.

Lemma 4.3 *For any coset Ω' of Ω,*

$$\sum_{b \in \Omega'} \widetilde{b}^2 \equiv 0 \pmod{N}$$

Proof. Let μ be a primitive root modulo N. Then a set of representatives for C_N in $\mathbb{Z}$ are $1, \mu, \ldots, \mu^{(N-3)/2}$. The representatives of a coset Ω' of Ω are μ^j, μ^{j+2^k}, $\mu^{j+2 \cdot 2^k}$, $\ldots$, $\mu^{j+((N-1)/2^{k+1}-1)2^k}$ for some $0 \le j < 2^k$. If

$$\widetilde{b} \equiv \pm\mu^{j+t2^k} \pmod{N},$$

then

$$\widetilde{b}^2 \equiv \mu^{2j+t2^{k+1}} \pmod{N},$$

so

$$\sum_{b\in\Omega'} \widetilde{b}^2 \equiv \mu^{2j} \sum_{t=0}^{(N-1)/2^{k+1}-1} \mu^{2^{k+1}t} = \mu^{2j}\frac{\mu^{N-1}-1}{\mu^{2^{k+1}}-1} \equiv 0 \pmod N$$

by Fermat's Little Theorem. ■

In the proofs of the next two lemmas, we shall use the following convention.

Convention 4.4 *For* P *a statement, let* $[P]$ *be* 1 *if* P *is true,* 0 *if* P *is false.*

Lemma 4.5 *Let* t *be an integer relatively prime to* N. *Then*

$$S = \sum_{b\in C_N} \lfloor \widetilde{b}t/N \rfloor$$

is even if and only if t *is a square modulo* N.

PROOF. Note that $\sum_{b\in C_N} \widetilde{b} = r(r+1)/2$ is even (since r is divisible by 4), so

$$S = \sum_{b\in C_N} \lfloor \widetilde{b}t/N \rfloor \equiv \sum_{b\in C_N}^{r} \widetilde{b}t - \sum_{b\in C_N} N\lfloor \widetilde{b}t/N \rfloor = \sum_{b\in C_N} (\widetilde{b}t \bmod N) \pmod 2.$$

Now $\widetilde{b}t \bmod N$ is either $\{\widetilde{b}t\}$ or $N - \{\widetilde{b}t\}$ depending on whether $\widetilde{b}t \bmod N \le r$ or not, respectively. Therefore, we can write S as follows

$$\begin{aligned} S &\equiv \sum_{b\in C_N} \{\widetilde{b}t\} + \sum_{b\in C_N} [\widetilde{b}t \bmod N > r](-\{\widetilde{b}t\} + N - \{\widetilde{b}t\}) \\ &\equiv \sum_{b\in C_N} \widetilde{b} + \sum_{b\in C_N} [\widetilde{b}t \bmod N > r](-\{\widetilde{b}t\} + N - \{\widetilde{b}t\}) \\ &\equiv \sum_{b\in C_N} [\widetilde{b}t \bmod N > r](N - 2\{\widetilde{b}t\}) \equiv \sum_{b\in C_N} [\widetilde{b}t \bmod N > r] \pmod 2 \end{aligned}$$

Define m to equal $\sum_{b\in C_N} [\widetilde{b}t \bmod N > r]$. Then

$$(-1)^m r! = \prod_{b\in C_N} \{\widetilde{b}t\} \equiv \prod_{b\in C_N} (\widetilde{b}t) = t^r r! \pmod N$$

Since N does not divide $r!$, this implies that

$$(-1)^m \equiv t^r \pmod N.$$

Since $t^r \equiv 1 \pmod N$ exactly when t is a square modulo N, this proves our lemma. ■

Lemma 4.6 *Let Ω' be a coset of Ω and s, f, t, h integers with $st - Nfh = 1$ and $\{t\} \in \Omega$ and*

$$S = h(1-t)\sum_{b\in\Omega'} \widetilde{b} + \sum_{b\in\Omega'} \lfloor \widetilde{b}t/N \rfloor.$$

The parity of S does not depend on the choice of Ω'.

PROOF. First observe that $st - Nfh = 1$ implies that if t is even then h must be odd, so in any case $h(1-t) \equiv t+1 \pmod 2$. Therefore,

$$S \equiv (t+1)\sum_{b\in\Omega'} \widetilde{b} - N\sum_{b\in\Omega'} \lfloor \widetilde{b}t/N \rfloor = \sum_{b\in\Omega'} \widetilde{b} + \sum_{b\in\Omega'} (\widetilde{b}t \bmod N) \pmod 2.$$

Since $t \in \Omega$, for b ranging over Ω the reductions of $\{\widetilde{b}t\}$ to C_N just range over Ω', so we can once again use the method of the proof of Lemma 4.5. Accordingly,

$$\begin{aligned} S &\equiv 2\sum_{b\in\Omega'} \widetilde{b} + \sum_{b\in\Omega'} [\widetilde{b}t \bmod N > r](-\{\widetilde{b}t\} + N - \{\widetilde{b}t\}) \\ &\equiv \sum_{b\in\Omega'} [\widetilde{b}t \bmod N > r] \pmod 2. \end{aligned}$$

Let $m = \sum_{b\in\Omega'} [\widetilde{b}t \bmod N > r]$. Then

$$(-1)^m \prod_{b\in\Omega'} \widetilde{b} = \prod_{b\in\Omega'} \{\widetilde{b}t\} \equiv \prod_{b\in\Omega'} (\widetilde{b}t) = t^{\#\Omega} \prod_{b\in\Omega'} \widetilde{b} \pmod N$$

Since N does not divide $\prod_{b\in\Omega'} \widetilde{b}$,

$$(-1)^m \equiv t^{\#\Omega} \pmod N,$$

and it is plain that the parity of m (which is the same as the parity of S) depends only on the choice of t and not on the choice of Ω'. ■

Recall from Definition 4.2 that $q = 3/z$.

Theorem 4.7 *Define the following three functions on $X_1(N)$:*

$$\begin{aligned} f(\tau) &= \left(\prod_{b\in\Omega} g_{\widetilde{b}}(\tau)^{2^k q}\right)\left(\prod_{b\in C_N} g_{\widetilde{b}}(\tau)^{-q}\right), \\ g(\tau) &= \left(\prod_{b\in\Omega} g_{\widetilde{b}}(\tau)^{-q}\right)\left(\prod_{b\in\xi\Omega} g_{\widetilde{b}}(\tau)^{q}\right), \\ h(\tau) &= \left(\prod_{b\in\Omega} g_{\widetilde{b}}(\tau)^{2q}\right). \end{aligned}$$

Then the following are true:

(a) the group $\mathrm{Gal}(X_1(N)_{\mathbb{C}}/X_0^{\#}(N)_{\mathbb{C}})$ *is the subgroup of* $\mathrm{Gal}(X_1(N)_{\mathbb{C}}/X_0(N)_{\mathbb{C}})$ *that fixes the function* f*;*

(b) the functions g *and* h *are invariant under* $\mathrm{Gal}(X_1(N)_{\mathbb{C}}/X_0^{\#}(N)_{\mathbb{C}})$ *and can therefore be regarded as being defined on* $X_0^{\#}(N)_{\mathbb{C}}$*;*

(c) $\xi f = (-1)g^{2^k} f$*;*

(d) $g(\xi g)(\xi^2 g)\dots(\xi^{2^k-1}g) = -1$*;*

(e) the divisor $\mathrm{div}(f)$ *is divisible by* 2^k *in* $\mathrm{Div}^0(X_0^{\#}(N))$.

REMARK. Henceforth we will regard f, g and h as functions on $X_0^{\#}(N)$. By (a) above, f descends to no smaller cover of $X_0(N)$.

NOTE. The function f above is the analogue in our situation of the Ogg–Ligozat function f_{OL} that was used in [11, II, Proposition (12.2)]. (In that paper, f_{OL} is called f.) Note however that if we restrict to the case of $N \equiv 9 \pmod{16}$ (equivalently $n \equiv 2 \pmod 4$) considered in that paper, our function f does not equal the function f_{OL}. Instead, the "correct" function f (the one we are using above) is equal to f_{OL}^q. However, since q is always equal to 1 or 3, and Mazur was constructing a point in a group of exponent two, f and f_{OL} worked equally well.

PROOF. First we need to check (using Theorem 3.2) that f is actually a function on $X_1(N)$. Conditions (V1) and (V3) are clearly satisfied, since, in the notation of Theorem 3.2, each d_i is zero, and $\sum c_i$ is also zero. For (V2), note that we need that N divide

$$q\left(\sum_{b\in\Omega}\tilde{b}^2 2^k - \sum_{b\in C_N}\tilde{b}^2\right) = q\left(2^k\sum_{b\in\Omega}\tilde{b}^2 - \frac{r(r+1)}{6}N\right)$$

The first term is divisible by N by Lemma 4.3, the second is divisible by N since clearly $r(r+1)/6$ is an integer.

We have now confirmed that f is defined on $X_1(N)$. It remains to check that the largest subgroup Θ of C_N that fixes f is in fact Ω. Since the coefficients in f for those $g_{\tilde{b}}$ with $b \in \Omega$ are different from those for which $b \notin \Omega$, we must have $\Theta \subseteq \Omega$.

To check $\Theta = \Omega$ then, it remains to show that for any $\alpha = \left(\begin{smallmatrix} s & f \\ Nh & t\end{smallmatrix}\right) \in \Gamma_0(N)$ with $\{t\} \in \Omega$, we have $f(\alpha\tau) = f(\tau)$. Using Theorem 3.5 (and (V1) to get rid of the ψ factors), we need to confirm that

$$\begin{aligned} C &= q\left(\sum_{b\in\Omega} 2^k(N\widetilde{b}h - \widetilde{b}^2ht + N\lfloor \widetilde{b}t/N\rfloor)\right) - \\ & \quad q\left(\sum_{b\in C_N} (N\widetilde{b}h - \widetilde{b}^2ht + N\lfloor \widetilde{b}t/N\rfloor)\right) \equiv 0 \pmod{2N} \end{aligned}$$

The expression C can be thought of as six separate sums, and it turns out that each of them is divisible by $2N$. This is obvious for the first, third, fourth and fifth; follows by Lemma 4.3 for the second; and follows by Lemma 4.5 for the sixth. Hence we have proved (a).

Similarly, we can check that g is defined on $X_0^{\#}(N)$. Again using Theorem 3.5, we need to confirm that

$$\begin{aligned} & -q(\sum_{b\in\Omega} (N\widetilde{b}h - \widetilde{b}^2ht + N\lfloor \widetilde{b}t/N\rfloor)) \\ & +q(\sum_{b\in\xi\Omega} (N\widetilde{b}h - \widetilde{b}^2ht + N\lfloor \widetilde{b}t/N\rfloor)) \equiv 0 \pmod{2N} \end{aligned}$$

The divisibility by N is immediate by Lemma 4.3, and for divisibility by 2 observe that for any coset Ω' of Ω we have

$$\begin{aligned} S &= \sum_{b\in\Omega'} (N\widetilde{b}h - \widetilde{b}^2ht + N\lfloor \widetilde{b}t/N\rfloor) \\ &\equiv \sum_{b\in\Omega'} (\widetilde{b}h - \widetilde{b}ht + \lfloor \widetilde{b}t/N\rfloor) \equiv h(1-t)\sum_{b\in\Omega'} \widetilde{b} + \sum_{b\in\Omega'} \lfloor \widetilde{b}t/N\rfloor \pmod{2}. \end{aligned}$$

Now an application of Lemma 4.6 completes the proof.

For $h(\tau)$, we need $12|2q(\#\Omega)$ to verify (V1). But $2q(\#\Omega) = 2q \cdot 2z\nu = 12\nu$ so this is clear. The rest of the proof is analogous to the proof for $g(\tau)$. This completes the proof of (b).

To prove (c), we calculate

$$\begin{aligned} (\xi f)(\tau) = f(\xi\tau) &= \left(\prod_{b\in\Omega} g_{\widetilde{b}}(\xi\tau)^{2^k q}\right)\left(\prod_{b\in C_N} g_{\widetilde{b}}(\xi\tau)^{-q}\right) \\ &= \left(\prod_{b\in\Omega} g_{\widetilde{\xi b}}(\tau)^{2^k q}\kappa(\xi;\widetilde{b})^{2^k q}\right)\left(\prod_{b\in C_N} g_{\widetilde{\xi b}}(\tau)^{-q}\kappa(\xi;\widetilde{b})^{-q}\right), \end{aligned}$$

so (since $(-1)^q = -1$) it suffices to show that

$$\prod_{b\in\Omega} \kappa(\xi;\widetilde{b})^{2^k} \prod_{b\in C_N} \kappa(\xi;\widetilde{b})^{-1} = -1.$$

Pick some $\left(\begin{smallmatrix} s & f \\ Nh & t \end{smallmatrix}\right) \in \Gamma_0(N)$ that lifts ξ. Then t will necessarily generate $(\mathbb{Z}/N\mathbb{Z})^\times$, and in particular it will be a non-square modulo N. By Theorem 3.5, it suffices to show that

$$\begin{aligned} \exp\left(\frac{\pi i}{N}\left(2^k \sum_{b\in\Omega}(N\widetilde{b}h - \widetilde{b}^2 ht + N\lfloor \widetilde{b}t/N\rfloor)\right)\right) \times \\ \exp\left(\frac{\pi i}{N}\left(-\sum_{b\in C_N}(N\widetilde{b}h - \widetilde{b}^2 ht + N\lfloor \widetilde{b}t/N\rfloor)\right)\right) &= -1. \end{aligned}$$

The first exponential is clearly 1 by Lemma 4.3 and because 2^k is even. Clearly

$$\exp\left(\frac{\pi i}{N}\left(-\sum_{b\in C_N}(N\widetilde{b}h - \widetilde{b}^2 ht)\right)\right) = 1,$$

and we are done with (c) by Lemma 4.5.

For (d), note that

$$\begin{aligned} g &= \left(\prod_{b\in\Omega} g_{\widetilde{b}}^{-q} \prod_{b\in\xi\Omega} g_{\widetilde{b}}^{q}\right) \\ \xi g &= \left(\prod_{b\in\xi\Omega} g_{\widetilde{b}}^{-q} \prod_{b\in\xi^2\Omega} g_{\widetilde{b}}^{q}\right)\left(\prod_{b\in\Omega}\kappa(\xi;\widetilde{b})^{-q}\right)\left(\prod_{b\in\xi\Omega}\kappa(\xi;\widetilde{b})^{q}\right) \\ \xi^2 g &= \left(\prod_{b\in\xi^2\Omega} g_{\widetilde{b}}^{-q} \prod_{b\in\xi^3\Omega} g_{\widetilde{b}}^{q}\right)\left(\prod_{b\in\Omega}\kappa(\xi;\widetilde{b})^{-q}\right)\left(\prod_{b\in\xi\Omega}\kappa(\xi;\widetilde{b})^{q}\right) \times \\ &\quad \times \left(\prod_{b\in\xi\Omega}\kappa(\xi;\widetilde{b})^{-q}\right)\left(\prod_{b\in\xi^2\Omega}\kappa(\xi;\widetilde{b})^{q}\right) \\ &= \left(\prod_{b\in\xi^2\Omega} g_{\widetilde{b}}^{-q} \prod_{b\in\xi^3\Omega} g_{\widetilde{b}}^{q}\right)\left(\prod_{b\in\Omega}\kappa(\xi;\widetilde{b})^{-q}\right)\left(\prod_{b\in\xi^2\Omega}\kappa(\xi;\widetilde{b})^{q}\right) \\ &\vdots \\ \xi^{2^k-1} g &= \left(\prod_{b\in\xi^{2^k-1}\Omega} g_{\widetilde{b}}^{-q} \prod_{b\in\Omega} g_{\widetilde{b}}^{q}\right)\left(\prod_{b\in\Omega}\kappa(\xi;\widetilde{b})^{-q}\right)\left(\prod_{b\in\xi^{2^k-1}\Omega}\kappa(\xi;\widetilde{b})^{q}\right). \end{aligned}$$

Therefore

$$g(\xi g)(\xi^2 g)\dots(\xi^{2^k-1}g) = \left(\prod_{b\in\Omega}\kappa(\xi;\widetilde{b})^{-q}\right)^{2^k}\left(\prod_{b\in C_N}\kappa(\xi;\widetilde{b})^{q}\right) = \frac{fg^{2^k}}{\xi f} = -1,$$

by (c). Thus the proof of (d) is complete.

We will use Theorem 3.3 to calculate $\mathrm{div}(f)$. It is immediately clear that $\mathrm{ord}_{Q_t}(f) = 0$ for all the cusps Q_t. On the other hand, letting Ω' denote the coset of Ω containing the reduction of $\widetilde{b}t$, and using the fact that $B_2(x) = B_2(1-x)$, we can calculate

$$\begin{aligned}
\mathrm{ord}_{P_t}(f) &= q\left(\sum_{b\in\Omega} 2^k \frac{N}{2} B_2\left(\frac{\widetilde{b}t \bmod N}{N}\right) - \sum_{b\in C_N} \frac{N}{2} B_2\left(\frac{\widetilde{b}t \bmod N}{N}\right)\right) \\
&= q\left(2^{k-1} N \sum_{b\in\Omega'}\left(\frac{\widetilde{b}^2}{N^2} - \frac{\widetilde{b}}{N} + \frac{1}{6}\right) - \frac{N}{2}\frac{(-r)}{6N}\right) \\
&= q 2^{k-1} \sum_{b\in\Omega'}\left(\frac{\widetilde{b}^2}{N} - \widetilde{b}\right) + q\left(2^{k-1} N \frac{\#\Omega}{6} + \frac{r}{12}\right).
\end{aligned}$$

By Lemma 4.3, the first term is an integer and clearly it is divisible by 2^k. Using the identities $\#\Omega = 2zv$, $r = 2^{k+1}zv$, $qz = 3$, the latter term in the above sum reduces to

$$2^{k-1}(N+1)v,$$

which is divisible by 2^k since $N+1$ is even. So we have completed the proof (e). ■

We will need the following lemma. For a curve X defined over $\mathbb{Q}$ and a field K containing $\mathbb{Q}$, denote the function field of X over K by $K(X)$. It is well known that a finite abelian group equipped with a continuous action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is the same as a finite étale commutative group scheme over $\mathbb{Q}$. We will use this identification throughout the rest of this dissertation.

Lemma 4.8 *Let $\phi : X \to Y$ be a finite étale map of projective curves, with X, Y and ϕ defined over $\mathbb{Q}$. Assume that ϕ is Galois after some finite base extension $F/\mathbb{Q}$. Let $\Gamma = \mathrm{Gal}(\overline{\mathbb{Q}}(X)/\overline{\mathbb{Q}}(Y)) \cong \mathrm{Gal}(F(X)/F(Y))$ and assume that Γ is commutative. By the Picard functoriality of the Jacobians, we have an exact sequence*

$$0 \longrightarrow K \longrightarrow \mathrm{Jac}(Y)(\overline{\mathbb{Q}}) \xrightarrow{\phi^*} \mathrm{Jac}(X)(\overline{\mathbb{Q}})^\Gamma,$$

where K denotes the finite $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module $\ker(\phi^*)$. Then

(a) the group scheme K is isomorphic to Γ^D, the Cartier dual of Γ;

(b) if Γ is cyclic, then ϕ^* surjects onto $\mathrm{Jac}(X)(\overline{\mathbb{Q}})^\Gamma$.

REMARK. To make sense of Γ^D, we need to consider Γ as an étale group scheme over $\mathbb{Q}$. The group Γ is naturally acted upon by $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ as follows: for any $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and $\tau \in \Gamma$, let $\sigma \cdot \tau = \widetilde{\sigma}\tau\widetilde{\sigma}^{-1}$ where $\widetilde{\sigma} \in \mathrm{Gal}(\overline{\mathbb{Q}}(X)/\mathbb{Q}(X)) \cong \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is any lift of σ.

PROOF. Taking the exact sequence of low degree terms for the Hochschild–Serre spectral sequence of the étale cohomology of $\mathbb{G}_m$ over the base $\overline{\mathbb{Q}}$ as in [14, III, Theorem 2.20], we obtain

$$\begin{array}{l} 0 \longrightarrow H^1(\Gamma, H^0(X_{et}, \mathbb{G}_m)) \longrightarrow H^1(Y_{et}, \mathbb{G}_m) \longrightarrow \\ \longrightarrow H^0(\Gamma, H^1(X_{et}, \mathbb{G}_m)) \longrightarrow H^2(\Gamma, H^0(X_{et}, \mathbb{G}_m)) \end{array}$$

which is

$$0 \longrightarrow H^1(\Gamma, \overline{\mathbb{Q}}^\times) \longrightarrow \mathrm{Pic}(Y) \xrightarrow{\phi^*} \mathrm{Pic}(X)^\Gamma \longrightarrow H^2(\Gamma, \overline{\mathbb{Q}}^\times).$$

Now since Γ acts trivially on $\overline{\mathbb{Q}}^\times$, $H^1(\Gamma, \overline{\mathbb{Q}}^\times) \cong \mathrm{Hom}(\Gamma, \overline{\mathbb{Q}}^\times) \cong \Gamma^D$. The kernel of $\phi^* : \mathrm{Pic}(Y) \to \mathrm{Pic}(X)$ is contained in $\mathrm{Jac}(Y)$, so we have proved (a).

If Γ is cyclic, then by [21, VIII §4], $H^2(\Gamma, \overline{\mathbb{Q}}^\times) \cong (\overline{\mathbb{Q}}^\times)^\Gamma/(\overline{\mathbb{Q}}^\times)^N = 0$. But if $\phi^* : \mathrm{Pic}(Y) \to \mathrm{Pic}(X)^\Gamma$ is surjective, then so is $\phi^* : \mathrm{Jac}(Y) \to \mathrm{Jac}(X)^\Gamma$, which proves (b). ■

Now we are almost ready to find extra points in $J_0(N)[I]$. Recall that c denotes the divisor $0 - \infty$ on $X_0(N)$.

Theorem 4.9 *Let* $d = \frac{1}{2^k}\,\mathrm{div}(f)$*, considered as a point on* $J_0^\#(N)$*. Then*

(a) the divisor d *is rational over* $\mathbb{Q}$*;*

(b) the divisor d *is in the image of* $\phi^* : J_0(N) \to J_0^\#(N)$*;*

(c) $2d = \phi^*(\nu \cdot c)$.

REMARK. In essence, we are trying to find "one half of c" in the group $J_0(N)[I]/\Sigma$. Assertion (c) in the above theorem shows that d is "one half of $\nu \cdot c$". Recall from Definition 4.2 that ν is the odd part of n, so this is as good as finding half of c, but some calculations work out simpler this way. Assertion (b) will be used to show that our point pulls back to $J_0(N)$, and assertion (a) will be used to show that we are actually finding points in $J_0(N)[I]$.

PROOF. As can be seen from the proof of Theorem 4.7(e), $\mathrm{div}(f)$ is concentrated at the cusps of $X_0^\#(N)$ that lie over the cusp 0 of $X_0(N)$. All of these cusps are rational over $\mathbb{Q}$, hence so is d, proving (a).

By Lemma 4.8(b), it suffices to check that d is fixed by ξ, the generator of the group $\mathrm{Gal}(X_0^\#(N)/X_0(N))$. By Theorem 4.7(c), $\mathrm{div}(f) - \mathrm{div}(\xi f) = -2^k \,\mathrm{div}(g)$, so

$$d - \xi d = \frac{1}{2^k}\,\mathrm{div}(f) - \frac{1}{2^k}\,\mathrm{div}(\xi f) = \mathrm{div}(1/g),$$

which is a principal divisor, so $d = \xi d$ in $J_0^\#(N)$, concluding our proof of (b).

Let $d' = \mathrm{div}(f)/2^{k-1} - \mathrm{div}(h)$ be a divisor on $X_0^\#(N)$. Using Theorem 3.3, for any $1 \le t \le r$,

$$\mathrm{ord}_{Q_t}(d') = \frac{1}{2^{k-1}}\left(\sum_{b\in\Omega}\frac{2^k q}{12} - \sum_{b\in C_N}\frac{q}{12}\right) - \sum_{b\in\Omega}\frac{2q}{12} = 0 - 2z\nu q/6 = -\nu,$$

and

$$\begin{aligned}\mathrm{ord}_{P_t}(d') &= \sum_{b\in\Omega}\frac{2^k qN}{2^k}B_2\left(\frac{\tilde{b}t \bmod N}{N}\right) - \sum_{b\in C_N}\frac{qN}{2^k}B_2\left(\frac{\tilde{b}t \bmod N}{N}\right)\\ &\quad - \sum_{b\in\Omega}\frac{2qN}{2}B_2\left(\frac{\tilde{b}t \bmod N}{N}\right) = -\frac{qN}{2^k}\frac{(-r)}{6N} = \nu.\end{aligned}$$

Hence $d' = \phi^*(\nu\cdot c)$, so

$$2d - \mathrm{div}(h) = \phi^*(\nu\cdot c)$$

as divisors. But h is a function defined on $X_0^\#(N)$ by Theorem 4.7(b), so this proves (c). ■

Chapter 5

The Galois structure of $J_0(N)[I]$

Theorem 5.1 *Let $\mathcal{D}$ denote the group generated by d in $J_0^{\#}(N)$. Let $A = (\phi^*)^{-1}\mathcal{D}$. Then*

(a) all the points of $\mathcal{D}$ are unramified at N;

(b) all the points of A are unramified at N;

(c) the group A is contained in $J_0(N)[I]$.

REMARK. Since $\#\ker(\phi) = \#\mathcal{D} = 2^k$, the group A has cardinality 2^{2k}. Therefore part (c) of the above theorem implies that A is the whole of the 2-primary component of $J_0(N)[I]$. Since the odd part of $J_0(N)[I]$ is the direct sum of the odd parts of C and Σ, we have now completed the concrete description of $J_0(N)[I]$ that we were aiming for.

PROOF. Assertion (a) is immediate from Theorem 4.9(a), since the points of $\mathcal{D}$ are rational. (Note that since the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the cusps of $X_0^{\#}(N)$ factors through the cyclotomic character χ_N, the only way for a divisor supported at the cusps to be unramified at N is to be rational.)

Assertion (b) follows from [11, II, Lemma (16.5)]. Note that since the lemma just cited applies only to points of prime power order, we have to apply it separately to each of the primary components of the point of A in question.

Multiplication by 2^k annihilates d. Therefore $2^kA \subseteq \ker(\phi^*) \subseteq \Sigma$, so certainly all points in A are torsion points. By [20, Prop. 3.3], all torsion points of $J_0(N)$ that are unramified at N are in $J_0(N)[I]$, so we have proved $A \subseteq J_0(N)[I]$. ∎

REMARK. For the reader's convenience we summarize another proof of part (c) of Theorem 5.1 that avoids invoking [20]. This proof also does not need the results of parts (a) and (b) of Theorem 5.1. We shall use the terminology and notation of [11]. Fix an embedding $\overline{\mathbb{Q}}_N \hookrightarrow \overline{\mathbb{Q}}$ and let J be the Néron model of $J_0(N)$ over $\mathbb{Z}_N$. Let $J_{/\mathbb{F}_N}$ denote the special fiber of J, and let $J^0_{/\mathbb{F}_N}$ denote the irreducible component of the identity in $J_{/\mathbb{F}_N}$. Let $\Sigma_{/\mathbb{F}_N}$ denote the reduction of Σ to $J_{/\mathbb{F}_N}$. Note that $\Sigma \cong \mu_n$, and so Σ is unramified at N. Therefore, by [22, Lemma 2], Σ reduces injectively to $\Sigma_{/\mathbb{F}_N}$. Then, by [11, II, Proposition (11.9)],

$$\Sigma_{/\mathbb{F}_N} \cap J^0_{/\mathbb{F}_N} = 0.$$

Thus, a point of Σ that reduces to a point in $J^0_{/\mathbb{F}_N}$ must be zero. We shall now use this observation to show that $A \subseteq J_0(N)[I]$.

It suffices to show that for arbitrary point x of A and any element T of I, we have $Tx = 0$. The group of irreducible components of $J_{/\mathbb{F}_N}$ is Eisenstein, as can be seen from the title (and contents) of [4] (see also [19]). Therefore, the operator T sends the reduction of x into the identity component. In other words, Tx reduces into $J^0_{/\mathbb{F}_N}$.

On the other hand, we can use the formulae in [24, Section 2] to define actions of T_l (for $l \neq N$) and w on ($J_1(N)$ and therefore on) $J_0^\#(N)$ that are compatible with the actions defined on $J_0(N)$ via the map ϕ^*, and calculate (in the spirit of the proof of Theorem 4.9(c)) that $\mathcal{D}$ is annihilated by each $1 + l - T_l$ and by $1 + w$. Let T' be a lift of T to the ring $\mathbb{Z}[\dots, T_l, \dots, w]$ and let T'' be the image of T' in $\mathrm{End}(J_0^\#(N))$. Then we have a commutative diagram

$$\begin{array}{ccc} J_0(N) & \xrightarrow{\phi^*} & J_0^\#(N) \\ \Big\downarrow T & & \Big\downarrow T'' \\ J_0(N) & \xrightarrow{\phi^*} & J_0^\#(N). \end{array}$$

Here x is mapped to $\phi^* x \in \mathcal{D}$ which is annihilated by T''. By the commutativity of the diagram we must have $Tx \in \ker(\phi^*) = \Sigma$. This completes our proof that $Tx = 0$. ■

Now that we established that $A \subseteq J_0(N)[I]$, we will determine the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on A and then assemble what we know to find the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the whole of $J_0(N)[I]$.

Definition 5.2 *Let* $\lambda : X_0^{\#\#}(N) \to X_0^\#(N)$ *be a minimal covering of* $X_0^\#(N)$ *on which* $f^{1/2^k}$ *is defined.*

By Theorem 4.7, parts (a) and (e), the degree of λ is 2^k and λ is étale. In fact, after base extension to $\mathbb{Q}(\mu_{2^{k+1}})$, λ becomes a Galois covering with Galois group Γ. The group Γ can be regarded as a finite étale group scheme over $\mathbb{Q}$, and by Lemma 4.8(a), A will be its Cartier dual. This allows us to determine the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on A.

Convention 5.3 *Choose once and for all a primitive 2^{k+1}st root of unity $\zeta \in \overline{\mathbb{Q}}$. Then ζ^2 is the primitive 2^kth root of unity that we will use in explicit Cartier duality calculations.*

Theorem 5.4 *Let K denote the function field of $X_0(N)$ over $\mathbb{Q}$ and L the function field of $X_0^{\#}(N)$ over $\mathbb{Q}$, so that $L(f^{1/2^k})$ is the function field of $X_0^{\#\#}(N)$ over $\mathbb{Q}$.*

(a) $L(f^{1/2^k}, \zeta)/K(\zeta)$ is a Galois extension with

$$\Gamma = \mathrm{Gal}(L(f^{1/2^k}, \zeta)/K(\zeta)) \cong \mathbb{Z}/2^k\mathbb{Z} \times \mathbb{Z}/2^k\mathbb{Z}.$$

In terms of the basis described in the proof, any element σ of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on Γ via the matrix

$$\begin{pmatrix} 1 & 0 \\ (\chi_{2^{k+1}}(\sigma) - 1)/2 & \chi_{2^k}(\sigma) \end{pmatrix}.$$

(b) The abelian group A is isomorphic to $\mathbb{Z}/2^k\mathbb{Z} \times \mathbb{Z}/2^k\mathbb{Z}$, with $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acting via

$$\begin{pmatrix} \chi_{2^k}(\sigma) & (1 - \chi_{2^{k+1}}(\sigma))/2 \\ 0 & 1 \end{pmatrix}.$$

Proof. We know that the field extension L/K is Galois of degree 2^k with cyclic Galois group generated by ξ, and this remains true for $L(\zeta)/K(\zeta)$. Clearly $L(f^{1/2^k}, \zeta)/L(\zeta)$ is also Galois (and cyclic) of degree 2^k. Since $K(\zeta)$ (and hence $L(\zeta)$) contains all 2^kth roots of unity, and by Theorem 4.7(c), $(\xi f)/f = (\zeta g)^{2^k}$, we can conclude that $L(f^{1/2^k}, \zeta) = L((\xi f)^{1/2^k}, \zeta)$. This way we obtain that $L(f^{1/2^k}, \zeta)$ contains all the 2^kth roots of f, ξf, ..., and therefore that $L(f^{1/2^k}, \zeta)/K(\zeta)$ is a Galois extension.

To determine the group $\Gamma = \mathrm{Gal}(L(f^{1/2^k}, \zeta)/K(\zeta))$, observe that the field extension $L(f^{1/2^k}, \zeta)/K(\zeta)$ contains all the conjugates of its generator $f^{1/2^k}$. Therefore it is obtained as a splitting field of the polynomial F whose roots are all the 2^kth roots of all conjugates of f. Since $\xi f = (-1)g^{2^k} f$, the 2^kth roots of ξf are $\zeta g f^{1/2^k}$, $\zeta^3 g f^{1/2^k}$, ..., $\zeta^{2^{k+1}-1} g f^{1/2^k}$. Then

$$\begin{aligned} \xi^2 f &= \xi((-1)g^{2^k} f) = (-1)(\xi g)^{2^k}(\xi f) \\ &= (-1)(\xi g)^{2^k}(-1)g^{2^k} f = (\xi g)^{2^k} g^{2^k} f, \end{aligned}$$

so the 2^kth roots of $\xi^2 f$ are $(\xi g)gf^{1/2^k}$,$\zeta^2(\xi g)gf^{1/2^k}$, ..., $\zeta^{2^{k+1}-2}(\xi g)gf^{1/2^k}$. Hence it is clear that the roots of F are exactly the

$$\delta_{i,j} = \zeta^{2i+j}\left(\prod_{k=0}^{j-1}(\xi^k g)\right) f^{1/2^k},$$

where i and j range over the interval $[0, 2^k - 1]$.

To determine Γ, observe that it must act simply transitively on the set of all roots of F. Let $\rho \in \Gamma$ be such that

$$\rho : \delta_{0,0} = f^{1/2^k} \mapsto \delta_{1,0} = \zeta^2 f^{1/2^k}.$$

Taking 2^kth powers, we see that ρ fixes f and hence all of $L(f^{1/2^k}, \zeta)$. So ρ sends $\delta_{i,j}$ to $\delta_{i+1,j}$ (with $\delta_{2^k,j}$ to be interpreted as $\delta_{0,j}$).

Now consider the element $\bar{\xi} \in \Gamma$ for which

$$\bar{\xi} : \delta_{0,0} = f^{1/2^k} \mapsto \delta_{0,1} = \zeta g f^{1/2^k}.$$

Taking 2^kth powers again, we see that $\bar{\xi}$ sends f to ξf, so it acts as ξ on $L(\zeta)$ (thereby justifying our choice of name for it). Note that

$$\bar{\xi}(\delta_{0,1}) = \bar{\xi}(\zeta g f^{1/2^k}) = \zeta(\bar{\xi} g)(\bar{\xi} f^{1/2^k}) = \zeta(\xi g)\zeta g f^{1/2^k} = \zeta^2(\xi g)gf^{1/2^k} = \delta_{0,2},$$

similarly

$$\bar{\xi}(\delta_{0,2}) = \bar{\xi}(\zeta^2(\xi g)gf^{1/2^k}) = \zeta^3(\xi^2 g)(\xi g)gf^{1/2^k} = \delta_{0,3},$$

and so on. Finally, using Theorem 4.7(d) we obtain

$$\begin{aligned}\bar{\xi}(\delta_{0,2^k-1}) &= \bar{\xi}(\zeta^{2^k-1}(\xi^{2^k-2}g)\ldots(\xi g)gf^{1/2^k}) = \zeta^{2^k}(\xi^{2^k-1}g)\ldots(\xi g)gf^{1/2^k} \\ &= (-1)(-1)f^{1/2^k} = f^{1/2^k} = \delta_{0,0}.\end{aligned}$$

Hence $\bar{\xi}$ sends $\delta_{i,j}$ to $\delta_{i,j+1}$ (with $\delta_{i,2^k}$ to be interpreted as $\delta_{i,0}$).

This shows that Γ is generated by two commuting elements of order 2^k. In other words, we have $\Gamma \cong \mathbb{Z}/2^k\mathbb{Z} \times \mathbb{Z}/2^k\mathbb{Z}$, and we can represent elements of Γ as column vectors over $\mathbb{Z}/2^k\mathbb{Z}$, with $\bar{\xi}$ corresponding to $\binom{1}{0}$ and ρ corresponding to $\binom{0}{1}$.

As for the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on Γ, take some $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and consider its natural action on $L(f^{1/2^k}, \zeta)$ that leaves $L(f^{1/2^k})$ fixed. Both $\sigma\bar{\xi}\sigma^{-1}$ and $\rho^{(\chi_{2^{k+1}}(\sigma)-1)/2}\bar{\xi}$ fix

ζ and

$$\begin{aligned}
\sigma\bar{\xi}\sigma^{-1} &: f^{1/2^k} \mapsto f^{1/2^k} \mapsto \zeta g f^{1/2^k} \mapsto \zeta^{\chi_{2^{k+1}}(\sigma)} g f^{1/2^k} \\
\rho^{(\chi_{2^{k+1}}(\sigma)-1)/2}\bar{\xi} &: f^{1/2^k} \mapsto \zeta g f^{1/2^k} \mapsto \zeta^{\chi_{2^{k+1}}(\sigma)} g f^{1/2^k}.
\end{aligned}$$

Therefore $\sigma\bar{\xi}\sigma^{-1} = \rho^{(\chi_{2^{k+1}}(\sigma)-1)/2}\bar{\xi}$. Similarly both $\sigma\rho\sigma^{-1}$ and $\rho^{\chi_{2^k}(\sigma)}$ fix ζ and

$$\begin{aligned}
\sigma\rho\sigma^{-1} &: f^{1/2^k} \mapsto f^{1/2^k} \mapsto \zeta^2 f^{1/2^k} \mapsto \zeta^{2\chi_{2^{k+1}}(\sigma)} f^{1/2^k} \\
\rho^{\chi_{2^k}(\sigma)} &: f^{1/2^k} \mapsto \zeta^{2\chi_{2^k}(\sigma)} f^{1/2^k} = \zeta^{2\chi_{2^{k+1}}(\sigma)} f^{1/2^k}.
\end{aligned}$$

Therefore $\sigma\rho\sigma^{-1} = \rho^{\chi_{2^k}(\sigma)}$. Hence $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ does act on the elements of Γ (represented by column vectors) as required. With this the proof of (a) is complete.

For (b), a simple calculation shows that if G is an étale group scheme over $\mathbb{Q}$ that is isomorphic to $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ with a Galois action described by

$$\begin{pmatrix} a(\sigma) & b(\sigma) \\ c(\sigma) & d(\sigma) \end{pmatrix} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}),$$

then its Cartier dual G^D is also isomorphic to $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, but with a Galois action described in terms of the usual dual basis by

$$\begin{pmatrix} \chi_m(\sigma)a(\sigma^{-1}) & \chi_m(\sigma)c(\sigma^{-1}) \\ \chi_m(\sigma)b(\sigma^{-1}) & \chi_m(\sigma)d(\sigma^{-1}) \end{pmatrix} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}).$$

In our case this means that $A \cong \Gamma^D$ is isomorphic to $\mathbb{Z}/2^k\mathbb{Z} \times \mathbb{Z}/2^k\mathbb{Z}$ with the action of $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ described by

$$\begin{pmatrix} \chi_{2^k}(\sigma) & \chi_{2^k}(\sigma)(\chi_{2^{k+1}}(\sigma^{-1})-1)/2 \\ 0 & 1 \end{pmatrix}$$

in terms of the basis $\bar{\xi}^D = \binom{1}{0}, \rho^D = \binom{0}{1}$. But $\chi_{2^k}(\sigma)(\chi_{2^{k+1}}(\sigma^{-1})-1)/2 \equiv (1-\chi_{2^{k+1}}(\sigma))/2 \pmod{2^k}$ so we have completed the proof of this theorem. ■

Proof of Theorem 1.1. Since the quotient group $\mathrm{Gal}(L(\zeta)/K(\zeta))$ of Γ is spanned by ξ, the dual subgroup $\Sigma_0 = \ker(J_0(N) \to J_0^{\#}(N))$ is spanned by $\bar{\xi}^D$ in A. One checks easily that $d \in \ker(J_0^{\#}(N) \to J_0^{\#\#}(N))$ corresponds to the image of ρ in A/Σ_0 under Cartier duality, so we can see by Theorem 4.9(c) that $\nu \cdot c \in A$ is represented by some vector $\binom{*}{2}$ in A. But since $\nu \cdot c \in A$ is $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-invariant, we can use Theorem 5.4(b) to conclude that $\nu \cdot c = \binom{1}{2}$.

The odd part of $J_0(N)[I]$ is a direct product $\mu_\nu \times \mathbb{Z}/\nu\mathbb{Z}$. The constant part is generated by $2^k c$, so we can choose a basis $g_1, 2^k c$ so that for any $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, $\sigma(g_1) = \chi_\nu(\sigma) g_1$

and $\sigma(2^k c) = 2^k c$. Taking the basis consisting of g_1 and $g_2 = (2^k c - g_1)(\nu + 1)/2$ instead, we have $2^k c = g_1 + 2g_2$ and σ acts via

$$\begin{pmatrix} \chi_\nu(\sigma) & (1-\chi_{2\nu}(\sigma))/2 \\ 0 & 1 \end{pmatrix}.$$

Now pick integers a, b such that $\nu a + 2^k b = 1$. Then

$$\begin{aligned} e_1 &= a\bar{\xi}^D + bg_1 \\ e_2 &= a\rho^D + bg_2 \end{aligned}$$

is a basis of $J_0(N)[I]$ that clearly has all properties required in Theorem 1.1.

Finally, observe that if $N \not\equiv 1 \pmod 8$, then $n = \nu$ and the 2-primary part of $J_0(N)[I]$ is 0. So formally setting $\bar{\xi}^D = \rho^D = 0$, we still have $\nu \cdot c = n \cdot c = 0 = \bar{\xi}^D + 2\rho^D$ and $\rho^D \in \Sigma$. The above argument about the prime-to-2 part works without a change, so we have proved Theorem 1.1 in this case too. ■

REMARK. As described in [20], H. W. Lenstra and K. Ribet proved a version of Theorem 1.1, where the expression $(1-\chi_{2n}(\sigma))/2$ in the statement of the theorem is replaced by a function

$$b : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{Z}/n\mathbb{Z},$$

satisfying the properties that for each $\sigma, \tau \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$,

$$\begin{aligned} b(\sigma\tau) &= b(\sigma) + \chi_n(\sigma)b(\tau), \\ 2b(\sigma) &= 1 - \chi_n(\sigma), \end{aligned}$$

and that the kernel of b cuts out the $2n$th cyclotomic field. We shall show here that his result is strictly weaker than Theorem 1.1.

Indeed, let $b_0(\sigma) = (1-\chi_{2n}(\sigma))/2$, and let

$$\epsilon : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{Z}/2\mathbb{Z}$$

be a *homomorphism* that factors through $\mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q})$. It is easy to check that for any such ϵ, the function

$$b(\sigma) = b_0(\sigma) + \frac{n}{2}\epsilon(\sigma)$$

satisfies all of the above conditions. Since there is more than one choice for such a function ϵ when n divisible by 4, we have shown that the above result is weaker than Theorem 1.1.

Chapter 6

The old subvariety of $J_0(NM)$

Let N and M be distinct primes. The modular curve $X_0(NM)$ classifies elliptic curves equipped with a subgroup of order NM. (Recall from elementary group theory that all abelian groups of order NM are cyclic.) Forgetting all but the N-primary part of such a subgroup yields a subgroup of order N, thereby giving rise to a degeneracy map

$$\pi_1 : X_0(NM) \to X_0(N),$$

which is defined over $\mathbb{Q}$.

The Atkin–Lehner involution

$$w_M : X_0(NM) \to X_0(NM)$$

is another morphism defined over $\mathbb{Q}$ that can be associated to a moduli-theoretic operation. The operation is as follows. Let (E, C) denote a pair of an elliptic curve E and a subgroup C of order NM. Let C_N (respectively, C_M) be the N-primary (respectively, M-primary) subgroup of C, so that $C = C_N \times C_M$. Let $\gamma : E \to E'$ be the degree M isogeny with kernel C_M. Then it is easy to see that the group $\gamma(E[M])$ is cyclic of order M, and that the group $\gamma(C_N)$ is cyclic of order N. Then the operation we are looking for sends the pair (E, C) to the pair $(E', \gamma(E[M]) \times \gamma(C_N))$.

On $X_0(NM)_{\mathbb{C}} = \mathfrak{H}^*/\Gamma_0(NM)$, the map w_M is induced by the action of the matrix $\left(\begin{smallmatrix} -aN & b \\ -NM & M \end{smallmatrix}\right)$ acting on $\mathfrak{H}^*$ via the corresponding Moebius transformation, where a and b are integers chosen so that $bN - aM = 1$.

The curve $X_0(NM)$ has four cusps, called P_1, P_N, P_M and P_{NM} in the notation of [18]. The morphism $\pi_1 : X_0(NM) \to X_0(N)$ sends P_1 and P_M to the cusp 0 on $X_0(N)$, with ramification indices M and 1, respectively. The map π_1 also sends P_N and P_{NM} to the cusp ∞ of $X_0(N)$, with ramification indices M and 1, respectively. The morphism w_M swaps the points P_1 and P_M, and it also swaps the points P_N and P_{NM}.

Now we can define the degeneracy map

$$\pi_M : X_0(NM) \to X_0(N)$$

by setting $\pi_M = \pi_1 \circ w_M$. This allows us to define the morphisms

$$\alpha = (\pi_1^*, \pi_M^*) \quad : \quad J_0(N) \times J_0(N) \to J_0(NM)$$

and

$$\beta = (\pi_1^*, \pi_N^*) \quad : \quad J_0(M) \times J_0(M) \to J_0(NM).$$

Since w_M^2 is the identity morphism on $X_0(NM)$, we can see that $w_M^* \alpha(R_1, R_2) = \alpha(R_2, R_1)$. (Note that we shall use w_M to denote w_M^* where it is not likely to cause confusion.)

Definition 6.1 *Let* $A = \mathrm{im}(\alpha)$ *and* $B = \mathrm{im}(\beta)$. *The old part of* $J_0(NM)$ *is the abelian subvariety of* $J_0(NM)$ *that is generated by* A *and* B.

Since $J_0(M)$ has good reduction everywhere away from M and β is defined over $\mathbb{Q}$, we can conclude that B has good reduction away from M. Similarly, A has good reduction away from N. Therefore, $A \cap B$ has good reduction everywhere and is finite (see [18, Theorem 3] and [5]).

It was proved in [16] that

$$\ker(\alpha) = \{(P, -P) \in J_0(N)^2 : P \in \Sigma\}.$$

We shall paraphrase this fact by saying that "the kernel of α is Σ, embedded anti-diagonally". The analogous result of course also holds for β.

This completes the description of A and B. To completely describe the old part of $J_0(NM)$, we need to find $A \cap B$. The odd part of $A \cap B$ was found in [18]. We shall complete that description by proving Theorem 1.2. We shall proceed through a sequence of lemmas.

Lemma 6.2 *The preimage of the group* $A \cap B$ *under the map* α *is contained in* $J_0(N)[I]^2$.

Proof. Let $x \in J_0(N)^2$ be such that $\alpha(x) \in A \cap B$. Then there is some $y \in J_0(M)^2$ such that $\beta(y) = \alpha(x)$. The point $\beta(y) = \alpha(x)$ has finite order, since it is contained in the finite group $A \cap B$. Since B has good reduction at N, the point $\beta(y)$ must be unramified at N unless its order is divisible by N. But that cannot happen, since, by [18, Corollary 1], the odd part of the order of $\beta(y)$ must divide the quantity

$$\gcd(\mathrm{num}((N-1)/24), \mathrm{num}((M-1)/24)),$$

which is not divisible by N. Therefore, $\beta(y) = \alpha(x)$ is unramified at N. Now, since $\ker(\alpha) = \Sigma$ (embedded anti-diagonally), this implies, as in [11, II, Lemma (16.5)], that x is unramified at N. This in turn implies by [20, Prop. 3.3] that $x \in J_0(N)[I]^2$ as required.

■

Lemma 6.3 *The image of the divisor* $c = 0 - \infty$ *on* $X_0(N)$ *under the map* $\pi_1^* - \pi_M^*$ *is the divisor* $(M-1)D^{-,-} = (M-1)(P_1 - P_N - P_M + P_{NM})$.

Proof. This is immediate using the action of w_M on $X_0(NM)$ and the ramification indices of the cusps of $X_0(NM)$ over the cusps of $X_0(N)$. Indeed,

$$\pi_1^*(c) \quad = \quad \pi_1^*(0-\infty) = MP_1 + P_M - MP_N - P_{NM}$$

and

$$\pi_M^*(c) \quad = \quad \overline{w}_M^*(\pi_1^*(c)) = MP_M + P_1 - MP_{NM} - P_N.$$

The difference of the two displayed lines yields the result. ■

If $M < 5$ then $B = 0$ and Theorem 1.2 is true. Therefore, we may assume from now on that $M \geq 5$.

Let P be a point that maps to the generator of $J_0(N)[I]/\Sigma$ that we constructed before. Thus, P can be chosen as the point e_2 in Theorem 1.1. If $N \equiv 1 \pmod 8$, let z be the non-trivial 2-torsion element in Σ.

If $N \equiv 1 \pmod 8$ then $\Sigma[2] = C[2]$. Thus, we can express z as

$$z = \frac{n}{2} \cdot c. \tag{6.1}$$

This relation, which usually plays the role of an obstacle to be circumvented, now will help us get a handle on the behavior of z instead.

Now that we have established that the image of $J_0(N)[I]^2$ is the only thing we need to consider when determining $A \cap B$, we prove a lemma that allows us to focus on an even smaller set.

Lemma 6.4 *Let* $R \in J_0(N)[I]^2$*. If* $\alpha(R) \in A \cap B$*, then*

- *if* $N \not\equiv 1 \pmod 8$ *then* R *lies in the* $\mathbb{Z}$*-linear span of* $\pi_1^*(P) - \pi_M^*(P)$*;*
- *if* $N \equiv 1 \pmod 8$ *then* R *lies in the* $\mathbb{Z}$*-linear span of* $\pi_1^*(P) - \pi_M^*(P)$ *and* $\pi_1^*(z)$.

PROOF. Assume that $R = (R_1, R_2)$ maps into $A \cap B$ under α. Note that w_M acts on $A \cap B$ as multiplication by -1. Indeed, it is well known that $\beta \circ w_M = w_M \circ \beta$ (see for example [18, "Formulaire"]), and by (the M-analog of) Lemma 6.2, we know that w_M acts as -1 on $\beta^{-1}(A \cap B)$. Therefore,

$$-\alpha(R_1, R_2) = w_M \alpha(R_1, R_2) = \alpha(R_2, R_1)$$

and hence

$$0 = \alpha(R_1 + R_2, R_1 + R_2).$$

Once again using the fact that $\ker(\alpha) = \Sigma$ (embedded anti-diagonally), we conclude that $R_1 + R_2$ is an element of $\Sigma[2]$. We now complete the proof by examining each of the possibilities that this allows for $R_1 + R_2$.

In case $R_1 + R_2 = 0$, we can write $R_1 = aP + \sigma$ for some integer a and some $\sigma \in \Sigma$. Then

$$\alpha(R_1, R_2) = \alpha(aP + \sigma, -aP - \sigma) = a\alpha(P, -P) = a(\pi_1^*(P) - \pi_M^*(P)).$$

If $N \equiv 1 \pmod 8$ then $\Sigma[2] \neq 0$, and therefore it can also happen that $R_1 + R_2 = z$. Then we can write $R_1 = z + aP + \sigma$ for some integer a and some $\sigma \in \Sigma$. Then $R_2 = -aP - \sigma$ and

$$\alpha(R_1, R_2) = \alpha(z, 0) + a\alpha(P, -P) = \pi_1^*(z) + a(\pi_1^*(P) - \pi_M^*(P)).$$

In either case, the lemma is proved. ∎

Let us assume from now on that

$$\boxed{N \equiv 1 \pmod 8.}$$

In the rest of this chapter, we shall frequently use the following argument to prove that various points on $J_0(NM)$ are not equal. Let J be an abelian variety defined over $\mathbb{Q}$ (for example, $J_0(NM)$). Given a prime number p, we can consider J to be defined over $\mathbb{Q}_p$ so that we can look at its Néron model $\mathcal{J}/\mathbb{Z}_p$.

Given a point Q in $J(\mathbb{Q})$, we can consider it an element of $J(\mathbb{Q}_p)$. By the Néron mapping property, Q even extends to an element of $\mathcal{J}(\mathbb{Z}_p)$. Reducing modulo p, we can then regard Q as an element of $\mathcal{J}_p(\mathbb{F}_p)$, where $\mathcal{J}_p$ denotes the special fiber of $\mathcal{J}$. The scheme $\mathcal{J}_p$ is a group scheme over $\mathbb{F}_p$, but it is not necessarily irreducible. Let $\Phi_p(J)$ denote its group of irreducible components. Given our point $Q \in \mathcal{J}_p(\mathbb{F}_p)$, we can check which element of $\Phi_p(J)$ it maps to. The argument we shall often use proceeds as follows. Consider the function

$$\varpi : J(\mathbb{Q}) \to \Phi_p(J)$$

described above. Let $P, Q \in J(\mathbb{Q})$. If $\varpi(P) \neq \varpi(Q)$ then we must also have $P \neq Q$. Usually we shall show that $\varpi(P) \neq \varpi(Q)$ by first showing that $\varpi(P) = 0$ (that is to say, P maps to the component of the identity under reduction modulo p), and then showing that $\varpi(Q) \neq 0$.

This method can work only if $\Phi_p(J)$ has more than one element, which in turn can happen only if J has bad reduction at p. Since $J_0(NM)$ has good reduction away from N and M, we will always choose $p = N$ or $p = M$.

Now we prepare the ground for this method by proving that various points are defined over $\mathbb{Q}$ and by studying the components they map to when reduced modulo N or modulo M.

Lemma 6.5 *The points $\pi_1^*(P) - \pi_M^*(P)$ and $\pi_1^*(z)$ are defined over $\mathbb{Q}$, and hence so is every point of $A \cap B$.*

Proof. By Lemma 6.4, (and the fact that $J_0(NM)$ is defined over $\mathbb{Q}$), $\pi_1^*(P)-\pi_M^*(P)$ and $\pi_1^*(z)$ being defined over $\mathbb{Q}$ does imply that every point of $A \cap B$ is defined over $\mathbb{Q}$.

The point c is defined over $\mathbb{Q}$, and hence so is $z = (n/2)c$. Since the degeneracy map π_1 is also defined over $\mathbb{Q}$, we conclude that $\pi_1^*(z)$ is defined over $\mathbb{Q}$.

By [16, Theorem 4.3], the map $\pi_1^* - \pi_M^* : J_0(N) \to J_0(NM)$ (which is defined over $\mathbb{Q}$) factors through $J_0(N)/\Sigma \to J_0(NM)$ (also defined over $\mathbb{Q}$). Since the image of P in $J_0(N)/\Sigma$ is also defined over $\mathbb{Q}$ by Theorem 1.1, it follows that $\pi_1^*(P) - \pi_M^*(P)$ is defined over $\mathbb{Q}$. ■

Lemma 6.6 *Every point of $A \cap B$ reduces to the identity component of $J_0(NM)$ modulo N (and modulo M).*

PROOF. By symmetry, it suffices to prove the claim for the reduction modulo N.

The variety B has good reduction modulo N, therefore any point in $A \cap B \subseteq B(\mathbb{Q})$ reduces to the identity component modulo N. ■

Lemma 6.7 *The point $\pi_1^*(z)$ does not reduce to the identity component of $J_0(NM)$ modulo N.*

PROOF. Recall from (6.1) that $z = (n/2)c$. This will enable us to use the results of [11, Appendix I] to determine exactly where in the component group of $J_0(N)$ modulo N the point $\pi_1^*(z)$ will map. We have

$$\begin{aligned}\pi_1^*(z) &= \pi_1^*(\frac{n}{2}(0-\infty)) = \frac{n}{2}(MP_1 + P_M - MP_N - P_{NM}) = \\ &= \frac{n}{2}(M+1)(\overline{0} - \overline{\infty}).\end{aligned}$$

Here $\overline{0}$ (respectively $\overline{\infty}$) means a cusp of $X_0(NM)$ that reduces to the same irreducible component as the cusp 0 (respectively ∞) modulo N.

Using the notation of [11, Appendix I], we have $u \in \{0, 1\}$ and $v \in \{0, 1\}$, with

$$\begin{aligned} u = 1 \quad &\Longleftrightarrow \quad N \equiv 7 \text{ or } 11 \pmod{12} \quad \text{and} \quad M \equiv 1 \pmod 4 \\ v = 1 \quad &\Longleftrightarrow \quad N \equiv 5 \text{ or } 11 \pmod{12} \quad \text{and} \quad M \equiv 1 \pmod 3. \end{aligned}$$

We have assumed that $N \equiv 1 \pmod 8$, which excludes the possibilities $N \equiv 7, 11 \pmod{12}$. Therefore we must have $u = 0$, and

$$v = 1 \quad \Longleftrightarrow \quad N \equiv 2 \pmod 3 \quad \text{and} \quad M \equiv 1 \pmod 3.$$

Now that we have a good grip on the pair (u, v), we can look up in the table of [11, Appendix I] the order of the divisor $\overline{0} - \overline{\infty}$ in the component group of $J_0(NM)$ modulo N. The table below summarizes the possibilities (for brevity, we use the notation $x = (N-1)(M+1)$).

$N \pmod 3$	$M \pmod 3$	n	$\mathrm{ord}(\overline{0} - \overline{\infty})$	$\pi_1^*(z)$
1	1, 2	$(N-1)/12$	$x/12$	$x(\overline{0} - \overline{\infty})/24$
2	1	$(N-1)/4$	$x/4$	$x(\overline{0} - \overline{\infty})/8$
2	2	$(N-1)/4$	$x/12$	$x(\overline{0} - \overline{\infty})/8$

In each case, we can see that $\pi_1^*(z)$ does not reduce to the identity. This completes the proof. ■

Lemma 6.8 *The point* $D^{-,-}$ *reduces to the identity component of* $J_0(NM)$ *modulo* N *and modulo* M.

PROOF. Considering $D^{-,-}$ in the group of components modulo N, we have

$$D^{-,-} = P_1 - P_N - P_M + P_{NM} = \overline{0} - \overline{\infty} - \overline{0} + \overline{\infty} = 0.$$

The same proof works modulo M. ■

Lemma 6.9 *The point* $(\pi_1^* - \pi_M^*)P$ *reduces to the identity component of* $J_0(NM)$ *modulo* N.

PROOF. This is a direct consequence of the fact that $\pi_1^* - \pi_M^*$ annihilates the component group of $J_0(N)$. (See [17, Theorem 2] and [4, proof of Théorème 1].) ■

In view of Lemma 6.4, the following Theorem shall bring us closer to our goal of proving Theorem 1.2.

Theorem 6.10 *The divisor class of* $(\pi_1^* - \pi_M^*)(\nu P)$ *on* $X_0(NM)$ *is equal to the divisor class of* $\frac{\nu(M-1)}{2}D^{-,-}$.

REMARK. Note that since $\pi_1^* - \pi_M^*$ annihilates $\Sigma \subset J_0(N)$ and P is "half of c modulo Σ", the Theorem 6.10 is consistent with the statement of the Lemma 6.3. Unfortunately, the Theorem does not follow yet, since there are a lot of ways in which we could take half of $\nu(M-1)D^{-,-}$, only one of which is consistent with the Theorem.

Since the definition of P involved the cover $X_0^{\#}(N)$ of $X_0(N)$, we must pause here to define a cover of $X_0(NM)$ that will allow us to determine $(\pi_1^* - \pi_M^*)P$.

Let $X_{1,0}(N, M)$ denote the modular curve corresponding to the congruence subgroup $\Gamma_1(N) \cap \Gamma_0(M)$. The curve $X_{1,0}(N, M)$ is defined over $\mathbb{Q}$ and corresponds to the moduli problem of classifying elliptic curves equipped with a point of order N *and* a subgroup of order M. The natural degeneracy map

$$X_{1,0}(N, M) \to X_0(NM)$$

will be denoted by β, by an abuse of notation that is intended to remind the reader to the similarity of this map to the previously defined $\beta : X_1(N) \to X_0(N)$. Specifically, both maps β have the moduli-theoretic interpretation of taking a point of order N and replacing it by the subgroup of order N that it generates.

There is also a degeneracy map

$$\pi_1 : X_{1,0}(N, M) \to X_1(N),$$

corresponding to the natural transformation "forget the level M structure" between the corresponding moduli functors. Then we have a commutative diagram of curves and maps defined over $\mathbb{Q}$ as follows:

$$\begin{array}{ccc} X_{1,0}(N, M) & \xrightarrow{\beta} & X_0(NM) \\ \downarrow{\scriptstyle \pi_1} & & \downarrow{\scriptstyle \pi_1} \\ X_1(N) & \xrightarrow{\beta} & X_0(N). \end{array}$$

The curve $X_{1,0}(N, M)$ has $2N - 2$ cusps, which shall be denoted P_i^0, P_i^∞, Q_i^0, Q_i^∞, where the index i is allowed to range over 1, 2, ..., r. The map $\pi_1 : X_{1,0}(N, M) \to X_1(N)$ sends the points P_i^0 and P_i^∞ to the point P_i, with ramification indices M and 1, respectively. Similarly, the same map π_1 sends the points Q_i^0 and Q_i^∞ to the point Q_i, with ramification indices M and 1, respectively.

The map $\beta : X_{1,0}(N, M) \to X_0(NM)$ takes the cusps P_1^0, P_2^0, ..., P_r^0 to the cusp P_1 of $X_0(NM)$; P_1^∞, P_2^∞, ..., P_r^∞ are sent to P_M; Q_1^0, Q_2^0, ..., Q_r^0 go to the cusp P_N; Q_1^∞, Q_2^∞, ..., Q_r^∞ all map to P_{NM}. None of the four cusps of $X_0(NM)$ is a branch point of β.

Since $\beta : X_{1,0}(N, M) \to X_0(NM)$ is a cyclic Galois covering of degree r, it has a unique intermediate covering of $X_0(NM)$ of any degree dividing r (and this intermediate covering is also defined over $\mathbb{Q}$). As in the definition of $X_0^\#(N)$, we can use this fact to define the curve $X_0^\#(N, M)$.

Definition 6.11 *Let*

$$\phi : X_0^\#(N, M) \to X_0(NM)$$

be the unique covering of degree 2^k that factors through $\beta : X_{1,0}(N, M) \to X_0(NM)$. Let $J_0^\#(N, M) = \mathrm{Jac}(X_0^\#(N, M))$.

The curve $X_0^\#(N, M)$ has a moduli interpretation similar to that of $X_0^\#(N)$, with an extra subgroup of order M thrown in.

We have again a degeneracy map $\pi_1 : X_0^{\#}(N,M) \to X_0^{\#}(N)$ (corresponding to forgetting the level M structure) that makes the following diagram commute

$$\begin{tikzcd} X_0^{\#}(N,M) \arrow[r, "\phi"] \arrow[d, "\pi_1"] & X_0(NM) \arrow[d, "\pi_1"] \\ X_0^{\#}(N) \arrow[r, "\phi"] & X_0(N). \end{tikzcd} \tag{6.2}$$

The curve $X_0^{\#}(N,M)$ has 2^{k+2} cusps. Every cusp of $X_0(NM)$ has 2^k cusps of $X_0^{\#}(N,M)$ lying over it. To simplify the notation, we shall refer to a cusp of $X_0^{\#}(N,M)$ by the name of any cusp of $X_{1,0}(N,M)$ that lies over it.

We can now use $X_0^{\#}(N,M)$ to deal with π_1^*P, but in order to study $\pi_M^*P = w_M^*\pi_1^*P$, we shall need an analog of w_M on the curve $X_0^{\#}(N,M)$. Let

$$\lambda : X_0^{\#}(N,M) \to X_0^{\#}(N,M)$$

be the morphism induced by the action of the matrix $\begin{pmatrix} Mb & 1 \\ aNM & M \end{pmatrix}$ on the complex upper half plane (here again, a and b are integers chosen so that $bM - aN = 1$). The morphism λ has the following moduli interpretation: if (E, P_N, C_M) is a triplet of an elliptic curve E, a point $P \in E$ of order N, and a cyclic subgroup $C_M \subset E[M]$ of order M corresponding to a point Q of $X_0^{\#}(N,M)$, then λQ corresponds to the triplet $(E/C_M, P_N/C_M, E[M]/C_M)$.

We now let $\overline{w}_M = \lambda^{-1}$. The morphism $\overline{w}_M$ covers w_M in the sense that the following diagram is commutative:

$$\begin{tikzcd} X_0^{\#}(N,M) \arrow[r, "\overline{w}_M"] \arrow[d, "\pi_1"] & X_0^{\#}(N,M) \arrow[d, "\pi_1"] \\ X_0(NM) \arrow[r, "w_M"] & X_0(NM). \end{tikzcd}$$

(One might notice that λ also covers w_M and wonder why we set $\overline{w}_M = \lambda^{-1}$ instead of $\overline{w}_M = \lambda$. The reason is that although $\overline{w}_M = \lambda$ would also work, the function we would have to consider to prove Theorem 6.13 would be much more complicated.)

The morphism $\overline{w}_M$ sends the cusps P_i^0, P_i^∞, Q_i^0, Q_i^∞ (respectively) to the cusps P_i^∞, $P_{i/M}^0$, Q_{Mi}^∞, Q_i^0 (respectively), where i/M is understood to mean division modulo N and where all indices are to be taken in C_N.

We now have the tools to deal with $(\pi_1^* - \pi_M^*)P$. Before we move on to the proof of Theorem 6.10, we shall need the following lemma.

Lemma 6.12 *The unique non-trivial 2-torsion element in the kernel of*

$$\phi^* : J_0(NM) \to J_0^{\#}(N, M)$$

is the point $\pi_1^*(z)$.

PROOF. We can use the fact that z is a 2-torsion element of the kernel $\phi^* : J_0(N) \to J_0^{\#}(N)$ and the commutativity of the diagram (6.2) to conclude that $\pi_1^*(z)$ is a 2-torsion element of the kernel of $\phi^* : J_0(NM) \to J_0^{\#}(N, M)$.

The fact that $\pi_1^*(z)$ is not trivial follows from Lemma 6.7.

Since the map $\phi : X_0^{\#}(N, M) \to X_0(NM)$ is Galois with cyclic Galois group, there are no other non-trivial 2-torsion points in its kernel. ■

Let us now take for granted the following theorem, the proof of which shall be the subject of Chapter 7.

Theorem 6.13 *The divisors*

$$(1 - \overline{w}_M^*)\pi_1^*(d) \qquad \textit{and} \qquad \phi^*\left(\frac{\nu(M-1)}{2} D^{-,-}\right)$$

on $X_0^{\#}(N, M)$ *are linearly equivalent.*

This theorem allows us to conclude our proof as follows.

PROOF OF THEOREM 6.10. Consider the following commutative diagram.

$$\begin{tikzcd}
J_0(NM) \arrow[r, "\phi^*"] & J_0^{\#}(N, M) \\
J_0(NM) \arrow[u, "1-w_M^*"] \arrow[r, "\phi^*"] & J_0^{\#}(N, M) \arrow[u, "1-\overline{w}_M^*"'] \\
J_0(N) \arrow[u, "\pi_1^*"] \arrow[r, "\phi^*"] & J_0^{\#}(N). \arrow[u, "\pi_1^*"']
\end{tikzcd}$$

By definition, the point νP maps to $d \in J_0^{\#}(N)$. The left hand vertical map $(1 - w_M^*) \circ \pi_1^* = \pi_1^* - \pi_M^*$ sends the point νP to $(\pi_1^* - \pi_M^*)(\nu P)$. By the commutativity of the diagram and Theorem 6.13, we may therefore deduce that $(\pi_1^* - \pi_M^*)(\nu P) - \left(\frac{\nu(M-1)}{2} D^{-,-}\right)$ lies in the kernel of the top map ϕ^*. Furthermore, by Lemma 6.3 and the remark after it, we can see that

$$2\left((\pi_1^* - \pi_M^*)(\nu P) - \left(\frac{\nu(M-1)}{2} D^{-,-}\right)\right) = 0.$$

By Lemma 6.12, $(\pi_1^* - \pi_M^*)(\nu P) - \left(\frac{\nu(M-1)}{2} D^{-,-}\right)$ is equal to either 0 or $\pi_1^*(z)$. However, reduction modulo N lands in the identity component of $J_0(NM)$ for $(\pi_1^* - \pi_M^*)(\nu P)$ (by Lemma 6.9), and for $D^{-,-}$ (by Lemma 6.8), and away from the identity component for $\pi_1^*(z)$ (by Lemma 6.7). Therefore

$$(\pi_1^* - \pi_M^*)(\nu P) = \left(\frac{\nu(M-1)}{2} D^{-,-}\right)$$

and we have now completed the proof of Theorem 6.10. ■

PROOF OF THEOREM 1.2. In this proof, allow N and M to be any pair of distinct primes. Observe that if $N < 11$ then $A = 0$ and Theorem 1.2 is true. Similarly, we may assume that $M \geq 11$.

If $N \not\equiv 1 \pmod 8$ (equivalently, n is odd), then by Lemmas 6.2 and 6.4, the group $A \cap B$ is spanned by a multiple of $(\pi_1^* - \pi_M^*)(P)$.

On the other hand, if $N \equiv 1 \pmod 8$ (equivalently, n is even), then by Lemmas 6.2 and 6.4, the group $A \cap B$ is spanned by a multiple of $(\pi_1^* - \pi_M^*)(P)$ and $\pi^*(z)$. However, by Lemmas 6.6 and 6.7, in fact the group $A \cap B$ is spanned by multiples of $(\pi_1^* - \pi_M^*)(P)$ alone.

The multiples of $(\pi_1^* - \pi_M^*)(P)$ are exactly the image of the group $J_0(N)[I]/\Sigma$ under the map $\pi_1^* - \pi_M^*$. Since $\pi_1^* - \pi_M^*$ is injective on $J_0(N)[I]/\Sigma$, we can see that the image X_N has order n. We will now show that this image lies entirely in the cyclic group spanned by $D^{-,-}$.

We shall consider separately the image of the 2-primary part and the odd part of $J_0(N)[I]/\Sigma$. The odd part is generated by $2^k P = 2^{k-1} c$, and its image does lie among the multiples of $D^{-,-}$ by Lemma 6.3. The 2-primary part of $J_0(N)[I]/\Sigma$ (which is non-trivial only if n is even) is generated by νP. An application of Theorem 6.13 completes our argument.

Running the same argument again, but exchanging the roles of N and M, we find that $A \cap B$ can also be found in the subgroup X_M of order m of the multiples of $D^{-,-}$. Therefore, $A \cap B$ must be the intersection of our groups X_N and X_M. This completes the proof. ■

Chapter 7

A unit calculation on $X_0^{\#}(N, M)$

We now proceed to give a proof of Theorem 6.13.

Let us use the notation of Chapter 2 to identify our Siegel units. Note that (K1) and (K2) are still valid (with N replaced by NM), as are (2.2) and (2.3). At the appropriate points, we shall still massage the indices of our Siegel units into the array E' (with N, r replaced by NM, $(NM-1)/2$, respectively). Note that [8, Chapter 4, Theorem 1.3] does not apply to a level that is not a prime power; thus our Theorem 2.1 does not apply in this case. However, we shall use the half of Theorem 2.1 which remains valid by [8, Chapter 3, Theorem 5.2]—namely, a function satisfying conditions (U1–4) is a unit on $X(NM)$. (Note that (U2–4) are now congruences modulo NM.)

Definition 7.1 *Recall from Chapter 4 that Ω denotes the set of 2^kth powers in C_N. For any integer y that is not divisible by N,*

- *let Ω_y denote the representatives in the interval $[1, r]$ of the elements of the coset $y\Omega$ of Ω;*
- *let J_y denote the set of integers x in the interval $[1, (NM-1)/2]$ such that*
  - *M does not divide x, and*
  - *x maps to Ω_y under the natural surjection $\mathbb{Z} \to C_N$;*
- *let*

$$e(x) = \prod_{j \in J_M} g_{(0,j)}^{q}.$$

We shall need a definition and some lemmas before we can show that $\mathrm{div}(e)$ is the divisor mentioned in Theorem 6.13.

Definition 7.2 *For any integer $x \in [1, r]$, let $\phi(x)$ be the element of $[1, r]$ that satisfies the congruence*

$$M\phi(x) \equiv \pm x \pmod{N}.$$

(In other words, $\phi(x)$ is the representative for x/M in C_N.)

The following two lemmas will be useful later. Their proofs are very easy and will not be given here.

Lemma 7.3 *For any integer y that is not divisible by N,*

(a)

$$\sum_{j \in J_y} 1 = 2z\nu(M-1),$$

(b)

$$\sum_{j \in J_y} j = \frac{1}{2} z\nu N(M-1)(M+1) + \sum_{b \in \Omega_y} (\widetilde{b} - M\phi(\widetilde{b})),$$

(c)

$$\sum_{j \in J_y} j^2 = \frac{1}{6} z\nu N^2(M-1)(M+1)M + \sum_{b \in \Omega_y} (M\widetilde{b}^2 - M^2\phi(\widetilde{b})^2).$$

Lemma 7.4 *Let y be a real number. Then*

$$M\left(\sum_{i=0}^{M-1} B_2\left(\frac{y+iN}{NM}\right)\right) - B_2\left(\frac{y}{N}\right) = 0.$$

We shall need one last lemma.

Lemma 7.5 *Let c and d be relatively prime integers. Assume that c is divisible by NM and that d maps into Ω under the map $\mathbb{Z} \to C_N$. If y is any integer that is not divisible by N, we have*

$$\sum_{j \in J_y} \left\lfloor \frac{dj}{NM} \right\rfloor \equiv (1+d) \sum_{j \in J_y} j \pmod{2}.$$

PROOF. In this proof only, let $\{\cdot\}$ denote $\{\cdot\}_{NM}$, as given in Definition 3.4. All the congruences below are modulo 2. Proceeding as in the proof of Lemma 4.6, we obtain

$$\begin{aligned}
\sum_{j\in J_y}\left\lfloor\frac{dj}{NM}\right\rfloor &\equiv -d\sum_{j\in J_y} j + d\sum_{j\in J_y} j - NM\sum_{j\in J_y}\left\lfloor\frac{dj}{NM}\right\rfloor \\
&= -d\sum_{j\in J_y} j + \sum_{j\in J_y}(dj \bmod NM) \\
&= -d\sum_{j\in J_y} j + d\sum_{j\in J_y}\{dj\} + \sum_{j\in J_y}[dj \bmod NM > NM/2](-\{dj\} + NM - \{dj\}) \\
&\equiv (1+d)\sum_{j\in J_y} j + m,
\end{aligned}$$

where $m = \sum_{j\in J_y}[dj \bmod NM > NM/2]$. Then

$$(-1)^m \prod_{j\in J_y} j \equiv \prod_{j\in J_y}\{dj\} \equiv \prod_{j\in J_y}(dj) \pmod{NM},$$

which we can divide through by $\prod_{j\in J_y} j$, since no element of J_y is divisible by either N or M, to obtain

$$(-1)^m \equiv d^{\#J_y} \pmod{NM}.$$

Since $M-1$ divides $\#J_y$, we get that

$$d^{\#J_y} \equiv 1 \pmod{M}$$

by Fermat's Little Theorem. On the other hand, since $2(\#\Omega)$ divides $\#J_y$, we obtain

$$d^{\#J_y} \equiv 1 \pmod{N}.$$

(Already raising to the $(\#\Omega)$th power will send $d \in \Omega$ to $1 \in C_N$, which corresponds to $d \equiv \pm 1 \pmod{N}$.) Therefore, m must be even and the proof of the lemma is complete. ■

Claim 7.6 *The function $e(\tau)$ is a unit on $X_0^{\#}(N, M)$.*

PROOF. We just need to check conditions (U1–4) of Theorem 2.1, and that $e(\tau)$ remains invariant under the action of any matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2\mathbb{Z}$ with $c \equiv 0 \pmod{NM}$ and d mapping to Ω under the map $\mathbb{Z} \to C_N$.

By the definition of the function e and Lemma 7.3(a), (U1) is equivalent to

$$2z\nu q(M-1) \equiv 0 \pmod{12}.$$

This is always satisfied since $2zq = 6$ and $M-1$ is even.

It is clear from the definition of e that conditions (U2) and (U3) are satisfied, because 0 is divisible by NM.

Lemma 7.3(c) shows us that condition (U4) is equivalent to

$$\frac{1}{6}z\nu qN^2(M-1)(M+1)M + q\sum_{b\in\Omega_y}(M\widetilde{b}^2 - M^2\phi(\widetilde{b})^2) \equiv 0 \pmod{NM}.$$

The condition modulo M is obviously satisfied. For the condition modulo N, observe that the first term is clearly divisible by N, whereas the second term is divisible by N since for any $b\in\Omega_y$,

$$\widetilde{b}^2 \equiv M^2\phi(\widetilde{b})^2 \pmod{N},$$

and hence

$$\sum_{b\in\Omega_y}(M\widetilde{b}^2 - M^2\phi(\widetilde{b})^2) \equiv \sum_{b\in\Omega_y}(M\widetilde{b}^2 - \widetilde{b}^2) \equiv (M-1)\sum_{b\in\Omega_y}\widetilde{b}^2 \equiv 0 \pmod{N},$$

where the last congruence used Lemma 4.3.

To check invariance under $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, we proceed as in the proof of Theorem 3.2. First observe that $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ indeed permutes the indices of functions in $e(\tau)$ (after reducing the indices to E'). The only thing we need to show is that the transformation factor arising from reducing the indices to E' is 1. Using (K2), this reduces to showing that

$$c\sum_{j\in J_M} j - d\frac{c}{NM}\sum_{j\in J_M} j^2 + NM\sum_{j\in J_M}\left\lfloor\frac{dj}{NM}\right\rfloor \equiv 0 \pmod{2NM}.$$

(The floor function in $\lfloor dj/NM\rfloor$ arises in a fashion entirely analogous to how it came up in the proof of Theorem 3.5.) Since NM divides each of c, $\sum j^2$ (see above in our proof that (U4) is satisfied) and NM (respectively), it must divide the first, second and third term (respectively) of the above expression. Therefore, we need only check that

$$c\sum_{j\in J_M} j - d\frac{c}{NM}\sum_{j\in J_M} j^2 + NM\sum_{j\in J_M}\left\lfloor\frac{dj}{NM}\right\rfloor \equiv 0 \pmod{2}.$$

We have, using Lemma 7.5 and Lemma 7.3 parts (b) and (c),

$$\begin{aligned}
& c\sum_{j\in J_M} j - d\frac{c}{NM}\sum_{j\in J_M} j^2 + NM\sum_{j\in J_M}\left\lfloor\frac{dj}{NM}\right\rfloor \\
\equiv\ & c\sum_{b\in\Omega_M}(\widetilde{b} - \phi(\widetilde{b})) - dc\sum_{b\in\Omega_M}(\widetilde{b} - \phi(\widetilde{b})) + (1+d)\sum_{b\in\Omega_M}(\widetilde{b} - \phi(\widetilde{b})) \\
\equiv\ & (d+1)(c+1)\sum_{b\in\Omega_M}(\widetilde{b} - \phi(\widetilde{b})) \pmod{2}.
\end{aligned}$$

Since c and d are relatively prime integers, at least one of them is odd, and therefore the number $(d+1)(c+1)$ must be even. This concludes our proof of the claim. ■

Claim 7.7 *The divisor of* $e(\tau)$ *is*

$$(1-\overline{w}_M^*)\pi_1^*(d) - \phi^*\left(\frac{\nu(M-1)}{2}D^{-,-}\right).$$

PROOF. As was mentioned before, we shall prove here that the divisor above is equal to the divisor of the function $e(\tau)$.

The proof of this claim is going to be similar to that of Theorem 4.9(c), but more complex since there are more kinds of cusps and the objects we are considering are more complicated.

First, we shall identify the divisors $\pi_1^*(d) \in J_0^{\#}(N,M)$ and $\overline{w}_M^*\pi_1^*(d) \in J_0^{\#}(N,M)$. We do this by first recalling what the divisor $d \in J_0^{\#}(N)$ is. For any $1 \le t \le r$, let

$$A_t = \frac{q}{2^k}\left(\sum_{b\in\Omega}\frac{2^kN}{2}B_2\left(\frac{\{\widetilde{bt}\}}{N}\right) + \sum_{b\in C_N}\frac{-N}{2}B_2\left(\frac{\{\widetilde{bt}\}}{N}\right)\right).$$

Then, by the definition of d, for any $1 \le t \le r$ we have

$$\mathrm{ord}_{P_t}(d) = A_t, \qquad \mathrm{ord}_{Q_t}(d) = 0,$$

and therefore

$$\mathrm{ord}_{P_t^0}(\pi_1^*(d)) = MA_t, \qquad \mathrm{ord}_{Q_t^0}(\pi_1^*(d)) = 0$$
$$\mathrm{ord}_{P_t^\infty}(\pi_1^*(d)) = A_t, \qquad \mathrm{ord}_{Q_t^\infty}(\pi_1^*(d)) = 0.$$

By considering the action of $\overline{w}_M^*$ on the cusps, we also obtain that

$$\mathrm{ord}_{P_t^0}(\overline{w}_M^*\pi_1^*(d)) = A_{Mt}, \qquad \mathrm{ord}_{Q_t^0}(\overline{w}_M^*\pi_1^*(d)) = 0$$
$$\mathrm{ord}_{P_t^\infty}(\overline{w}_M^*\pi_1^*(d)) = MA_t, \qquad \mathrm{ord}_{Q_t^\infty}(\overline{w}_M^*\pi_1^*(d)) = 0.$$

Before we turn our attention to $\mathrm{div}(e)$, we note that

$$\mathrm{ord}_{P_t^0}(D^{-,-}) = 1, \qquad \mathrm{ord}_{Q_t^0}(D^{-,-}) = -1$$
$$\mathrm{ord}_{P_t^\infty}(D^{-,-}) = -1, \qquad \mathrm{ord}_{Q_t^\infty}(D^{-,-}) = 1.$$

We shall now show for each cusp of $J_0^{\#}(N,M)$ that the divisor mentioned in the statement of the claim and $\mathrm{div}(e)$ have the same order.

For a cusp labeled Q_t^∞ for some $1 \le t \le r$ (having ramification index 1 over the cusp of $X(1)$), we observe that it can be represented by $\binom{t}{NM}$ in Shimura's notation and therefore

$$\mathrm{ord}_{Q_t^\infty}(\mathrm{div}(e)) = q(\#J_M)\frac{1}{2}B_2(0) = \frac{2z\nu q(M-1)}{12} = \frac{\nu(M-1)}{2}.$$

Since $\pi_1^*(d)$ and $\overline{w}_M^*\pi_1^*(d)$ have order 0 at this cusp, this proves our claim for the cusps Q_t^∞.

For a cusp labeled Q_t^0 for some $1 \le t \le r$ (having ramification index M over the cusp of $X(1)$), we observe that it can be represented by $\binom{t}{N}$ in Shimura's notation and therefore

$$\begin{aligned}\mathrm{ord}_{Q_t^0}(\mathrm{div}(e)) &= q\sum_{j\in J_M}\frac{M}{2}B_2\left(\frac{Nj \bmod NM}{NM}\right) = q\sum_{j\in J_M}\frac{M}{2}B_2\left(\frac{j \bmod M}{M}\right)\\ &= qM(\#\Omega_M)\frac{1}{2}\sum_{i=1}^{M-1}B_2\left(\frac{i}{M}\right) = \frac{-\nu(M-1)}{2},\end{aligned}$$

where we used the fact that $\sum_{i=1}^{M-1}B_2(i/M)$ is equal to $(1-M)/(6M)$. Since $\pi_1^*(d)$ and $\overline{w}_M^*\pi_1^*(d)$ have order 0 at this cusp, this proves our claim for the cusps Q_t^0.

For a cusp labeled P_t^∞ for some $1 \le t \le r$ (having ramification index N over the cusp of $X(1)$), we observe that it can be represented by $\binom{1}{M\phi(t)}$ in Shimura's notation. Therefore, as above,

$$\mathrm{ord}_{P_t^\infty}(\mathrm{div}(e)) = q\sum_{j\in J_M}\frac{N}{2}B_2\left(\frac{\phi(t)j \bmod N}{N}\right).$$

Therefore,

$$\begin{aligned}&\mathrm{ord}_{P_t^\infty}(\mathrm{div}(e) - \pi_1^*(d) + \overline{w}_M^*\pi_1^*(d))\\ &= \frac{qN}{2}\sum_{j\in J_M}B_2\left(\frac{\phi(t)j \bmod N}{N}\right) + (1-M)\left(q\sum_{b\in\Omega}\frac{N}{2}B_2\left(\frac{\{\widetilde{bt}\}}{N}\right) + \frac{qr}{12\cdot 2^k}\right)\\ &= \frac{qN}{2}(1-M)\left(\sum_{b\in\Omega_{M\phi(t)}}B_2\left(\frac{\widetilde{b}}{N}\right) - \sum_{b\in\Omega_t}B_2\left(\frac{\widetilde{b}}{N}\right)\right) + \frac{qr(1-M)}{12\cdot 2^k}\\ &= \frac{qN}{2}(1-M)\cdot 0 + \frac{-2qz\nu(M-1)}{12} = \frac{-\nu(M-1)}{2},\end{aligned}$$

where the above argument used the fact that modulo N, the set J_M can be considered as $M-1$ copies of the set Ω_M. Then we used the fact that $M\phi(t)$ and t map to the same element in C_N to cancel out the last two nasty-looking sums. Thereby we completed the proof for the cusps P_t^∞.

It remains for us to consider the cusps labeled P^0_t for some $1 \le t \le r$ (having ramification index NM over the cusp of $X(1)$). We observe that such a cusp can be represented by $\binom{0}{t}$ in Shimura's notation (where we add N to t if it is otherwise divisible by M). Then

$$\mathrm{ord}_{P^0_t}(\mathrm{div}(e)) = q \sum_{j \in J_M} \frac{NM}{2} B_2\left(\frac{tjM \bmod NM}{NM}\right).$$

Therefore

$$\begin{aligned}\mathrm{ord}_{P^0_t}(\mathrm{div}(e) - \pi_1^*(d) + \overline{w}^*_M \pi_1^*(d)) &= \frac{qNM}{2} \sum_{j \in J_M} B_2\left(\frac{tjM \bmod NM}{NM}\right) \\ + \frac{qNM}{2} \sum_{b \in \Omega} B_2\left(\frac{\{\widetilde{b}t\}}{N}\right) &- \frac{qNM}{2^{k+1}} \sum_{b \in C_N} B_2\left(\frac{\widetilde{b}}{N}\right) \\ - \frac{qN}{2} \sum_{b \in \Omega} B_2\left(\frac{\{\widetilde{b}tM\}}{N}\right) &+ \frac{qN}{2^{k+1}} \sum_{b \in C_N} B_2\left(\frac{\widetilde{b}}{N}\right).\end{aligned}$$

We shall separate the above sum of five terms into groups. First of all, note that the sum of the third and the fifth terms is equal to

$$\frac{qN}{2}(1-M)\frac{1}{2^k} \sum_{b \in C_N} B_2\left(\frac{\widetilde{b}}{N}\right) = \frac{qN}{2}(1-M)\frac{1}{2^k}\frac{-r}{6N} = \frac{\nu(M-1)}{2}.$$

Therefore, to complete the proof of our claim, it suffices to show that the sum of the first, second and fourth terms is zero. This boils down (after division by $qN/2$) to showing that

$$M \sum_{j \in J_{Mt}} B_2\left(\frac{j}{NM}\right) + M \sum_{b \in \Omega_t} B_2\left(\frac{\widetilde{b}}{N}\right) - \sum_{b \in \Omega_{Mt}} B_2\left(\frac{\widetilde{b}}{N}\right) = 0.$$

However, the above equation is just the sum of the conclusions of Lemma 7.4 when we allow the y of the Lemma to run over all elements of Ω_M. ∎

Proof of Theorem 6.13. This theorem follows from Claims 7.6 and 7.7. ∎

We shall now make some general comments about studying the cuspidal divisor group on $X_0^{\#}(N, M)$ in the style of our Chapter 3. We find a number of differences from the case of prime level considered in Chapter 3.

First of all, it is still the case (as can be seen from [8, Chapter 3, Theorem 5.2]) that the functions of the form specified by Theorem 2.1 are units (they are the so-called *Siegel units*), but they do not exhaust all the units of $X(NM)$ any more. Instead, the Siegel units form a subgroup of the group of all units, in such a way that the quotient group is an elementary 2-abelian group. Therefore, the divisor mentioned in Theorem 6.13 might have been principal without this fact being revealed by an analysis of Siegel units on $X_0^{\#}(N, M)$.

Secondly, we cannot expect the analog of our Fact 2.2 to hold in the present case, since $X(NM)$ has $(N^2 - 1)(M^2 - 1)/2$ cusps, whereas there are $(N^2M^2 - 1)/2$ essentially different Siegel units. Therefore, there will be a lot of extra relations between the divisors of Siegel units that will make it significantly harder to emulate the proof of our Theorem 3.2 to establish the group of Siegel units on $X_1(NM)$.

Fortunately, both of the above difficulties can probably be overcome, and we shall outline a suggested solution now.

Firstly, the non-Siegel units of $X(NM)$ have also been studied extensively. An analysis of [7] and [23] should probably allow a sufficiently explicit description of all units and their divisors.

Secondly, although we have too many Siegel units, the relations among them are well-understood. They are discussed in [8] under the name "distribution relations". These relations generally take the form of an "old" unit (i.e., one coming from a lower level) giving a divisor that is linear combination of divisors of various other Siegel units (some of which might also be old). It turns out that by the time we descend all the way to $X_{1,0}(N, M)$, we have $2N - 2$ cusps and $2N + 1$ Siegel units. Instead of having just two kinds of functions as in Definition 3.1, we now have eight different kinds of functions. (There are two types each coming from levels N and M, as well as four kinds of new functions.) Nevertheless, the relations each work out to be in the form where the product of a subset of the Siegel units is a constant. Since the three subsets arising form a partition of the set of Siegel units, it turns out that the arguments of Theorem 3.2 still go through.

Bibliography

[1] C. Batut, D. Bernardi, H. Cohen, M. Olivier, *PARI–GP*, computer software, 1995–1999

[2] P. Deligne and M. Rapoport, *Les schémas de modules de courbes elliptiques*, pages 143–316 in P. Deligne and W. Kuyk (eds.), *Modular Functions of One Variable II*, Lecture Notes in Mathematics, 349, Springer, 1973

[3] F. Diamond and J. Im, *Modular forms and modular curves*, pages 39–133 in *Seminar on Fermat's Last Theorem (Toronto, ON 1993–1994)*, Canadian Mathematical Society Conference Proceedings, Vol. 17, 1995

[4] B. Edixhoven, *L'action de l'algèbre de Hecke sur les groupes de composantes des jacobiennes des courbes modulaires est "Eisenstein"*, Astérisque, No. 196–197 (1992), 159–170

[5] J.-M. Fontaine, *Il n'y a pas de variété abélienne sur* $\mathbb{Z}$, Invent. math. **81** (1985), 515–538

[6] P. E. Klimek, *Modular functions for* $\Gamma_1(N)$, Ph.D. dissertation, Berkeley, 1975

[7] D. S. Kubert, *The square root of the Siegel group*, Proc. London Math. Soc., (3) **43** (1981), 193–226

[8] D. S. Kubert and S. Lang, *Modular Units*, Grundlehren der mathematischen Wissenschaften 244, Springer, 1981

[9] S. Ling, *The old subvariety of* $J_0(pq)$ *and the Eisenstein kernel in Jacobians*, Israel Journal of Mathematics, **84** (1993), 365–384

[10] Ju. I. Manin, *Parabolic points and zeta functions of modular curves*, (Russian), Izv. Akad. Nauk SSSR Ser. Math., **36** (1972), 19–66

[11] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. **47**, 1977, 33–186. See also the Errata on pages 187–188 of [13] for an important correction for line 18 of page 105. Also note that some typos in Appendix I are corrected in [4, Section 4.4.1]

[12] B. Mazur, *Rational isogenies of prime degree*, Invent. math. **44** (1978), 129–162

[13] B. Mazur and A. Wiles, *Class fields of abelian extensions of* $\mathbb{Q}$, Invent. math. **76** (1984), 179–330

[14] J. S. Milne, *Étale Cohomology*, Princeton University Press, 1980

[15] A. P. Ogg, *Rational points on certain elliptic modular curves*, pages 221–231 in *Analytic number theory*, Proc. Sympos. Pure Math., Vol. XXIV, AMS, 1973

[16] K. A. Ribet, *Congruence relations between modular forms*, in *Proceedings of the ICM 1983*, 503–514

[17] K. A. Ribet, *On the component groups and the Shimura subgroup of* $J_0(N)$, Exp. No. 6, 10, in *Séminaire de Théorie des Nombres, 1987–1988 (Talence, 1987–1988)*, Univ. Bordeaux I, Talence.

[18] Kenneth A. Ribet, *The old subvariety of* $J_0(pq)$, in G. van der Geer, F. Oort, J. Steenbrink (eds.), *Arithmetic Algebraic Geometry*, Progress in Mathematics **89** (1990), 293–307

[19] Kenneth A. Ribet, *Irreducible Galois representations arising from component groups of Jacobians*, pages 131–147 in *Elliptic curves, modular forms, and Fermat's last theorem (Hong Kong, 1993),* Ser. Number Theory, I, Internat. Press, Cambridge, MA, 1995

[20] Kenneth A. Ribet, *Torsion points on* $J_0(N)$ *and Galois representations*, 1998

[21] J.-P. Serre, *Local Fields*, Graduate Texts in Mathematics 67, Springer, 1979

[22] Jean-Pierre Serre and John Tate, *Good reduction of abelian varieties*, Ann. of Math. (2) **88** (1968), 492–517

[23] Jing Yu, *A cuspidal class number formula for the modular curves* $X_1(N)$, Math. Ann. **252** (1980), 197–216

[24] A. Wiles, *Modular curves and the class group of* $\mathbb{Q}(\mu_p)$, Invent. math. **58** (1980), 1–35