On parameterizations of cyclic N-isogenies and strict K-curves lying above rational points of $Y_0^+(N)$

Christopher Joseph Decker Dowd

Advised by Professor Noam Elkies

Senior Thesis submitted in partial fulfillment for the honors requirements for the Bachelor of Arts degree in Mathematics

March 22, 2021

Contents

Acknowledgments

I thank my thesis advisor Professor Noam Elkies for our many conversations and correspondences, for his gracious willingness to give advice and feedback, and for introducing me to the topics of this thesis. I also thank Benjamin Peirce Fellow Fabian Gundlach for his work with me during Summer 2020; without the background on elliptic curves I gained during this time, this thesis would not have been possible. I thank Alec Sun for help with proofreading. Finally, I thank my parents and sister for their continued support of my mathematical pursuits.

1 Introduction

1.1 Cyclic isogenies

Modular curves are moduli spaces for elliptic curves: a point of a modular curve corresponds to an elliptic curve enhanced with certain torsion data. For example, the curve $X(1)$ corresponds to $\mathbb{C}$-isomorphism classes of curves, and the curves $X_0(N)$ correspond to such classes paired with additional data of a cyclic N-isogeny. Therefore, understanding the modular curves $X_0(N)$ is useful for understanding cyclic isogenies, which have many applications in elliptic curve computations. One of the most celebrated applications is the theory of descent, which often allows the computation of rank, conductor, and other invariants of interest for elliptic curves [Sil09]. The Schoof-Elkies-Atkin algorithm, which refines Schoof's algorithm for point-counting on elliptic curves over finite fields, relies on explicitly identifying cyclic isogenies and their kernels [Elk98]. Studying cyclic isogenies is a useful tool for finding elliptic curves with complex multiplication (CM), since any curve with a nontrivial cyclic self-isogeny is necessarily CM.

Since $X(1)$ is a rational curve, the correspondence between elliptic curves and $X(1)$ can be reinterpreted as a rational parametrization of elliptic curves—that is, we associate to every point of $\mathbb{C}$ a $\mathbb{C}$-isomorphism class of elliptic curves. This correspondence is given explicitly by the j-invariant. When $X_0(N)$ has genus 0, the same principle may be applied, and we obtain a correspondence between $\mathbb{C}$ and isomorphism classes of cyclic N-isogenies $E \to E'$. Analogously to the j-invariant, this correspondence may be explicitly given by a *Hauptmodul* h_N of $X_0(N)$. This Hauptmodul may be used to translate formulas involving q-expansions into rational functions involving h_N, clarifying data and providing a useful computational tool.

Elliptic K-curves are closely related to the subject of cyclic isogenies. These are curves E defined over some extension of a field K that are isogenous to all of their Galois conjugates E^σ. They arise as a natural generalization of curves defined over K. In particular, $\mathbb{Q}$-curves have been extensively studied. Which special properties of elliptic curves over $\mathbb{Q}$, such as modularity, extend to $\mathbb{Q}$-curves [Ell04]? The connection to cyclic isogenies comes from a theorem of Elkies, which states that all non-CM K-curves arise from K-rational points on the quotient $X^*(N)$ of $X_0(N)$ by the action of the Atkin-Lehner involutions.

1.2 This thesis

This thesis presents two original results. First, we tabulate explicit formulas for the coefficients of cyclic N-isogenous elliptic curves

$$E : y^2 = x^3 - \frac{A_4}{48}x + \frac{A_6}{864} \qquad\qquad E' : y^2 = x^3 - \frac{A'_4}{48}x + \frac{A'_6}{864}$$

in terms of a distinguished Hauptmodul on all modular curves $X_0(N)$ of genus 0. To this end, we provide an exposition on the derivation of these Hauptmoduln as products of the Dedekind eta function based on the approach of [Lig74]. We also include an abbreviated table of rational functions for the j-invariant in terms of Hauptmoduln, and we discuss an application of these expressions to finding special values of the j-invariant at CM points.

The second original result of this thesis is a new theorem on K-curves given by a K-rational orbit $\{\tau, -1/N\tau\}$ of the Fricke involution on $Y_0(N)$. Points on $Y_0(N)$ correspond to isomorphism classes of isogenies over $\mathbb{C}$, but these classes split into many twists when considered over a number field L. We prove the following theorem:

Theorem. Let L/K be a quadratic extension, and let $\{h, h'\} \subset Y_0(N)(L) \setminus Y_0(N)(K)$ be the fiber of a non-CM point in $Y_0^+(N)(K)$. Let E, E' be the corresponding isogenous curves. Then the following are equivalent:

(i) There exists a choice of twist of the cyclic N-isogeny $E \to E'$ defined over L such that E' is isomorphic over L to the conjugate curve $\overline{E}$ of E.

(ii) At least one of the integers N or $-N$ lies in the image of the Galois norm map $L^\times \to K^\times$.

Moreover, we give an explicit construction for all twists satisfying condition (i). In general, the isogenies between an elliptic K-curve and its conjugates might only be defined over some separable extension of $L = \mathbb{Q}(E)$. We lead into this theorem with background on elliptic K-curves.

Throughout, we assume basic familiarity with the theory of elliptic curves and modular forms. However, we provide background on the role of modular curves as moduli spaces, including the fundamental correspondence, the Atkin-Lehner involutions, the treatment of modular curves over number fields, and the Tate curve.

2 Modular curves

2.1 Modular curves as moduli spaces for complex elliptic curves

Let $\mathbb{H} \subset \mathbb{C}$ denote the complex upper half-plane and let $\mathrm{SL}_2(\mathbb{Z})$ act on $\mathbb{H}$ by fractional linear transformations. A modular curve Y is a Riemann surface given by a quotient space of $\mathbb{H}$ by the action of certain subgroups $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ known as congruence subgroups.

Definition 2.1.1. Let N be a positive integer. We define three classes of congruence subgroups:

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

More generally, a congruence subgroup is defined as a subgroup $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ containing $\Gamma(N)$ for some positive integer N.

Definition 2.1.2. We denote the modular curves corresponding to the three congruence groups above by

$$Y(N) = \mathbb{H}/\Gamma(N),$$
$$Y_1(N) = \mathbb{H}/\Gamma_1(N),$$
$$Y_0(N) = \mathbb{H}/\Gamma_0(N).$$

It is also useful to consider the compactifications of these curves. Let $\mathbb{H}^* = \mathbb{H} \cup \mathbb{Q} \cup \{\infty\}$ denote the extended upper half-plane. Since $\mathrm{SL}_2(\mathbb{Z})$ also acts on $\mathbb{P}^1_{\mathbb{Q}} = \mathbb{Q} \cup \{\infty\}$ by fractional linear transformations, its action on $\mathbb{H}$ extends to $\mathbb{H}^*$.

Definition 2.1.3. We define

$$X(N) = \mathbb{H}^*/\Gamma(N),$$
$$X_1(N) = \mathbb{H}^*/\Gamma_1(N),$$
$$X_0(N) = \mathbb{H}^*/\Gamma_0(N),$$

and we also call these modular curves. These are compact Riemann surfaces, and orbit classes of $\mathbb{P}^1_{\mathbb{Q}}$ are called *cusps*.

The inclusions $\Gamma(N) \subseteq \Gamma_1(N) \subseteq \Gamma_0(N)$ induce natural maps $Y(N) \to Y_1(N) \to Y_0(N)$, and likewise for their compactified versions. Furthermore, if $N' \mid N$, then the inclusion $\Gamma(N) \subseteq \Gamma(N')$ induces a map $Y(N) \to Y(N')$; likewise for Γ_0 and Γ_1.

These classes of modular curves can be interpreted as moduli spaces for *enhanced elliptic curves*—that is, each point of a modular curve corresponds to an isomorphism class of elliptic curves $\mathbb{C}/\Lambda$ together with a

certain type of torsion data, and this correspondence is natural in the sense that it commutes with the maps between the modular curves.

For $\tau \in \mathbb{H}$, let Λ_τ denote the lattice $\mathbb{Z} + \tau\mathbb{Z}$. We define three classes of enhanced elliptic curves corresponding to the above three classes of congruence subgroups.

Definition 2.1.4. An *enhanced elliptic curve for* $\Gamma_0(N)$ is a pair (E, C), where E is a complex elliptic curve and C is a cyclic subgroup of E of order N. We define $(E, C) \sim (E', C')$ if and only if there exists some isomorphism over $\mathbb{C}$ taking E to E' and C to C'. Then we define

$$S_0(N) = \{(E, C) \text{ enhanced elliptic curves for } \Gamma_0(N)\}/\sim .$$

Definition 2.1.5. The *degree* of an isogeny is the order of its kernel; if an isogeny has degree N, we call it an *N-isogeny*. We say that an isogeny is *cyclic* if it has cyclic kernel.

Instead of using the term "enhanced elliptic curve for $\Gamma_0(N)$" we will usually refer to (E, C) by its corresponding cyclic N-isogeny given by the quotient $E \to E/C$.

Definition 2.1.6. An *enhanced elliptic curve for* $\Gamma_1(N)$ is a pair (E, Q), where E is a complex elliptic curve and $Q \in E$ is a point of order N. We define $(E, Q) \sim (E', Q')$ if and only if there exists some isomorphism taking E to E' and Q to Q'. Then we define

$$S_1(N) = \{(E, Q) \text{ enhanced elliptic curves for } \Gamma_1(N)\}/\sim .$$

Definition 2.1.7. An *enhanced elliptic curve for* $\Gamma(N)$ is a pair $(E, (P, Q))$, where E is a complex elliptic curve and P, Q are a basis for the N-torsion subgroup $E[N]$ of E with Weil pairing $e_N(P, Q) = e^{2\pi i/N}$. We define $(E, (P, Q)) \sim (E', (P', Q'))$ if and only if there exists some isomorphism taking E to E' and both P to P' and Q to Q'. Then we define

$$S(N) = \{(E, (P, Q)) \text{ enhanced elliptic curves for } \Gamma(N)\}/\sim .$$

Theorem 2.1.8. *(a) The points of $Y_0(N)$ correspond bijectively to elements of $S_0(N)$ under the map*

$$\tau \leftrightarrow (\mathbb{C}/\Lambda_\tau, \langle 1/N \rangle).$$

(b) The points of $Y_1(N)$ correspond bijectively to elements of $S_1(N)$ under the map

$$\tau \leftrightarrow (\mathbb{C}/\Lambda_\tau, 1/N).$$

(c) The points of $Y_0(N)$ correspond bijectively to elements of $S_0(N)$ under the map

$$\tau \leftrightarrow (\mathbb{C}/\Lambda_\tau, (1/N, \tau/N)).$$

Proof. See [[DS05], Theorem 1.5.1]. ■

Corollary 2.1.9. *The points of $\Gamma(1) = \Gamma_1(1) = \Gamma_0(1)$ correspond bijectively to $\mathbb{C}$-isomorphism classes of elliptic curves (without additional torsion data) via the map*

$$\tau \leftrightarrow \mathbb{C}/\Lambda_\tau.$$

By part (a) of Theorem 2.1.8, we may interpret $Y_0(N)$ as parameterizing isomorphism classes of cyclic N-isogenies over $\mathbb{C}$.

2.2 The Fricke and Atkin-Lehner involutions

Any isogeny $\varphi : E \to E'$ of degree N has a unique dual isogeny $\hat{\varphi} : E \to E'$ such that

$$\hat{\varphi} \circ \varphi = [N]_E$$
$$\varphi \circ \hat{\varphi} = [N]_{E'},$$

where $[N]_E$ denotes the multiplication-by-N map on E. When φ is cyclic, so is $\hat{\varphi}$. Since a point $\tau \in Y_0(N)$ corresponds to a cyclic N-isogeny φ, we conclude that there must be some other point in $Y_0(N)$ corresponding to the dual isogeny $\hat{\varphi}$.

Definition 2.2.1. The *Fricke involution* w_N on $Y_0(N)$ is the map that sends a cyclic N-isogeny to its dual. We sometimes write w in place of w_N when N is clear from context.

Proposition 2.2.2. *The Fricke involution is given by the map* $w_N : \tau \mapsto -\frac{1}{N\tau}$.

Proof. Let φ be a cyclic N-isogeny $(\mathbb{C}/\Lambda_\tau, \langle 1/N \rangle)$, with $\tau \in \mathbb{H}$. Its image is

$$\mathbb{C}\Big/\left(\frac{1}{N}\mathbb{Z} + \tau\mathbb{Z}\right) \cong \mathbb{C}/\left(\mathbb{Z} + N\tau\mathbb{Z}\right) \cong \mathbb{C}/(N\tau\mathbb{Z} - \mathbb{Z}) \cong \mathbb{C}\Big/\left(\mathbb{Z} - \frac{1}{N\tau}\mathbb{Z}\right) = \mathbb{C}/\Lambda_{-1/N\tau}$$

where the isomorphisms are given by scaling by N, applying the change of basis $S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, and then scaling by $\frac{1}{N\tau}$. A point $z \in \mathbb{C}/\Lambda_\tau$ is mapped to $-\frac{z}{\tau} \in \mathbb{C}/\Lambda_{-1/N\tau}$ under this isogeny. (Note that $-\frac{1}{N\tau} \in \mathbb{H}$, justifying the otherwise superfluous negative sign.)

In the other direction, the image of the isogeny $(\mathbb{C}/\Lambda_{-\frac{1}{N\tau}}, \langle 1/N \rangle)$ is

$$\mathbb{C}\Big/\left(-\frac{1}{N\tau}\mathbb{Z} + \frac{1}{N}\mathbb{Z}\right) \cong \Lambda_{-\frac{1}{\tau}} \cong \Lambda_\tau,$$

and $z \in \mathbb{C}/\Lambda_{-1/N\tau}$ gets mapped to $-N\tau z \in \mathbb{C}/\Lambda_\tau$. Thus, these two isogenies compose to the multiplication-by-N map, so they are dual isogenies. The isogeny $(\mathbb{C}/\Lambda_\tau, \langle 1/N \rangle)$ corresponds to $\tau \in Y_0(N)$, and the dual isogeny $(\mathbb{C}/\Lambda_{-\frac{1}{N\tau}}, \langle 1/N \rangle)$ corresponds to $w\tau = -\frac{1}{N\tau}$. ∎

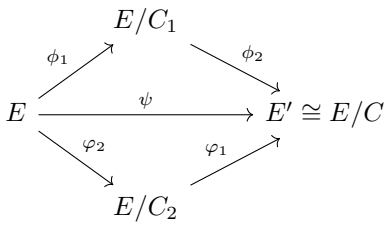
Definition 2.2.3. The curve $Y_0^+(N) = Y_0(N)/\{1, w\}$ is the quotient of $Y_0(N)$ by the action of the Fricke involution; we likewise define $X_0^+(N) = X_0(N)/\{1, w\}$.

We interpret points of $Y_0^+(N)$ as unordered pairs of curves E, E' related by cyclic N-isogenies. If a cyclic isogeny $E \to E$ of degree $N^2 > 1$ is self-dual, then it is not given by a multiplication-by-N map, since such a map has kernel

$$\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \ncong \mathbb{Z}/N^2\mathbb{Z}.$$

We therefore conclude that the ramified points of the quotient $Y_0(N) \to Y_0^+(N)$, i.e. the fixed points of the Fricke involution, give elliptic curves with complex multiplication, though not all CM curves arise in this way.

Let N_1N_2 be a coprime factorization of N, i.e. with N_1 and N_2 coprime. Let $P \in Y_0(N)$ correspond to a cyclic N-isogeny $\psi : E \to E'$ with cyclic kernel C, so that $E' \cong E/C$. We may factor this isogeny by first forming the quotient by the unique subgroup C_1 of order N_1 of C, and then forming the quotient by the image of C in E/C_1. Alternatively, we may first form the quotient by the unique subgroup C_2 of order N_2, and then form the quotient by the image of C in E/C_2. Both of these compositions yield ψ:



(1)

Here we have labeled isogenies so that ϕ_i and φ_i are cyclic N_i-isogenies. Using the dual isogeny, we obtain a new N-isogeny

$$\varphi_2 \circ \hat{\phi}_1 : E/C_1 \to E/C_2.$$

The kernel of this isogeny is isomorphic to $\mathbb{Z}/N_1\mathbb{Z} \times \mathbb{Z}/N_2\mathbb{Z}$, which is isomorphic to $\mathbb{Z}/N\mathbb{Z}$ since N_1 and N_2 are coprime. Therefore, $\varphi_2 \circ \hat{\phi}_1$ is itself a cyclic N-isogeny, so for each such factorization $N_1N_2 = N$ we may associate to P a unique point $P(N_1)$ corresponding to the isogeny $\varphi_2 \circ \hat{\phi}_1$. This association is an involution, since applying the construction a second time transforms $\varphi_2 \circ \hat{\phi}_1$ into $\phi_2 \circ \phi_1$. We have $P(1) = P$ and $P(N) = w(P)$, but we also obtain a larger class of involutions on $Y_0(N)$.

Definition 2.2.4. Let N_1N_2 be a coprime factorization of N. Then the *Atkin-Lehner involution* w_{N_1} associated to N_1 on $Y_0(N)$ is the map

$$Y_0(N) \to Y_0(N) : P \mapsto P(N_1)$$

as described above. We let $W(N)$ denote the group generated by the Atkin-Lehner involutions, and we let and $Y^*(N)$ denote the quotient of $Y_0(N)$ by the action of $W(N)$.

We cite some results about the Atkin-Lehner involutions from [LMFDB]. Generalizing the realization of the Fricke involution as the map $\tau \mapsto -1/N\tau$, we also have explicit representations of the Atkin-Lehner involutions as Möbius transformations.

Proposition 2.2.5. *The Atkin-Lehner involution w_{N_1} is given as a Möbius transformation by any matrix of form*

$$\begin{pmatrix} aN_1 & b \\ cN & dN_1 \end{pmatrix}$$

with determinant N_1.

This representation allows us to define an action of $W(N)$ on $X_0(N)$ as well, and thus allows us to define the quotient space $X^*(N) = X_0(N)/W(N)$.

Proposition 2.2.6. *If N_1, M_1 are coprime divisors of N, then*

$$w_{N_1} w_{M_1} = w_{N_1 M_1}.$$

In particular, the Atkin-Lehner involutions on $X_0(N)$ commute.

Corollary 2.2.7. *Let $\omega(N)$ denote the number of distinct prime divisors of N. Then $W(N) \cong (\mathbb{Z}/2\mathbb{Z})^{\omega(N)}$, with each element of this group corresponding to an ordered coprime factorization $N_1N_2 = N$.*

2.3 Modular functions and modular forms

In this section we cite several standard results on modular forms. For more details, see [DS05]. Throughout, we let $q(\tau) := e^{2\pi i \tau}$.

Definition 2.3.1. For even $k \geq 4$, the *normalized Eisenstein series of weight k* is

$$\mathsf{E}_k(\tau) := 1 - \frac{2k}{B_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n,$$

where $\sigma_k(n) = \sum_{d|n} d^k$ denotes the sum-of-divisors function and B_k denotes the k-th Bernoulli number:

$$B_0 = 1,\ B_1 = -\frac{1}{2},\ B_2 = \frac{1}{6},\ B_4 = -\frac{1}{30},\ B_6 = \frac{1}{42},\ B_8 = -\frac{1}{30},\ B_{10} = \frac{5}{66},\ B_{12} = -\frac{691}{2730}, \ldots$$

(The odd-indexed Bernoulli numbers B_{2n+1} vanish for $n > 0$.) We also define a second normalization G_k of the Eisenstein series given by

$$G_k(\tau) := 2\zeta(k)\mathsf{E}_k(\tau)$$

where ζ is the Riemann zeta function.

Both normalizations of the Eisenstein series are useful: the q-expansion of E_k has rational coefficients involving the arithmetic function σ_{k-1}, while the series G_k are involved in the correspondence between complex elliptic curves $\mathbb{C}/\Lambda$ and their affine models:

Theorem 2.3.2. (Uniformization.) *Let $\mathbb{C}/\Lambda_\tau$ be a complex elliptic curve. Then*

$$E : y^2 = 4x^3 - 60G_4(\tau)x - 140G_6(\tau)$$

is an affine elliptic curve, and the map $z \mapsto (\wp(z), \wp'(z))$ is an isomorphism of complex Lie groups. Moreover, for every affine elliptic curve $F/\mathbb{C}$ defined by a Weierstrass equation as above, there exists a unique lattice Λ_τ up to homothety such that the curve E given above is isomorphic to F.

Proof. See [[Sil09], Proposition VI.3.6 and Corollary VI.5.1.1]. ■

Proposition 2.3.3. *The normalized Eisenstein series E_k is a modular form of weight k on $X(1)$; that is,*

$$\mathsf{E}_k\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^k \mathsf{E}_k(\tau)$$

for any $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$.

Definition 2.3.4. The *Dedekind eta function* is

$$\eta(\tau) := q^{1/24} \prod_{n=1}^{\infty} (1 - q^n).$$

Here $q^{1/24}$ denotes $\exp(\pi i \tau/12)$.

Proposition 2.3.5. *The eta function satisfies the following functional equations:*

$$\eta(\tau + 1) = \exp(\pi i/12)\, \eta(\tau),$$
$$\eta(-1/\tau) = \sqrt{-i\tau}\, \eta(\tau),$$

where we take the branch of the square root that agrees with the square root on the positive real numbers.

Lemma 2.3.6. *Let $\nu(\tau) := \eta(N\tau)/\eta(\tau)$.*

(a) The function $\nu(\tau)$ transforms under the Fricke involution as

$$w_N^* \nu(\tau) = \nu(-1/N\tau) = \frac{1}{\sqrt{N}\nu(\tau)}.$$

(b) The derivative $\nu'(\tau)$ transforms under the Fricke involution as

$$w_N^* \nu(\tau) = \nu'(-1/N\tau) = -\sqrt{N}\tau^2 \cdot \frac{\nu'(\tau)}{\nu(\tau)^2}.$$

Proof. Part (a) follows immediately from the functional equation $\eta(-1/\tau) = \sqrt{-i\tau}\eta(\tau)$. For part (b), apply the chain rule to write

$$\nu'(-1/N\tau) \cdot \frac{1}{N\tau^2} = \frac{d}{d\tau}\nu(-1/N\tau).$$

Substituting using part (a), this gives

$$\begin{aligned}\nu'(-1/N\tau) &= N\tau^2 \frac{d}{d\tau}\left(\frac{1}{\sqrt{N}\nu(\tau)}\right) \\ &= -\sqrt{N}\tau^2 \cdot \frac{\nu'(\tau)}{\nu(\tau)^2}.\end{aligned}$$

■

Definition 2.3.7. The *j-invariant* is

$$j(\tau) := 1728 \cdot \frac{\mathsf{E}_2(\tau)^3}{\mathsf{E}_2(\tau)^3 - 27\mathsf{E}_3(\tau)^2}.$$

Definition 2.3.8. A *Hauptmodul* h (plural *Hauptmoduln*) of a modular curve X of genus 0 is a generator of the function field $\mathbb{C}(X) = \mathbb{C}(h)$ normalized to have q-expansion $\frac{1}{q} + O(1)$. In particular, h has its pole at the cusp at ∞.

Proposition 2.3.9. *The j-invariant is a modular function on $X(1)$. Moreover, it is a Hauptmodul for $X(1)$, so that it parameterizes $\mathbb{C}$-isomorphism classes of elliptic curves.*

Proof. The j-invariant is a modular function on $X(1)$ since it is the quotient of two weight 12 modular forms and thus has trivial transformation law under $\mathrm{SL}_2(\mathbb{Z})$. The fact that it is a Hauptmodul follows from computing its q-expansion

$$j(q) = q^{-1} + 744 + 196884q + \dots$$

and from the fact that j parameterizes $\mathbb{C}$-isomorphism classes of elliptic curves; see [[Sil09], Proposition III.1.4]. ■

Definition 2.3.10. The *Eisenstein series of weight 2 and level N* is

$$\mathsf{E}_2^{(N)}(\tau) := q \cdot \frac{d}{dq}\log\left(\frac{\eta(q^N)}{\eta(q)}\right) = \frac{N-1}{24} + \sum_{n=1}^{\infty}\sigma_1(n)(q^n - Nq^{Nn}).$$

Proposition 2.3.11. *The Eisenstein series $\mathsf{E}_2^{(N)}(\tau)$ is a modular form of weight 2 on $X_0(N)$.*

Proposition 2.3.12. *The modular form $\mathsf{E}_2^{(N)}(\tau)$ is anti-invariant under the Fricke involution. That is, it transforms under the Fricke involution by the functional equation*

$$\mathsf{E}_2^{(N)}(-1/N\tau) = -N\tau^2 E_2^{(N)}(\tau).$$

Proof. Write $\tau = \frac{\log q}{2\pi i}$. Then by the chain rule $\frac{d}{dq} = \frac{1}{2\pi i q}\frac{d}{d\tau}$ as differential operators. We use this to define $\mathsf{E}_2^{(N)}(\tau)$ entirely in terms of τ, eliminating the variable q:

$$\mathsf{E}_2^{(N)}(\tau) = \frac{1}{2\pi i}\frac{d}{d\tau}\log\left(\frac{\eta(N\tau)}{\eta(\tau)}\right).$$

Write $\nu(\tau) = \frac{\eta(N\tau)}{\eta(\tau)}$. Taking logarithmic derivatives, this is

$$\mathsf{E}_2^{(N)}(\tau) = \frac{1}{2\pi i}\frac{\nu'(\tau)}{\nu(\tau)}.$$

Apply Lemma 2.3.6 to get

$$w_N^* \frac{\nu'(\tau)}{\nu(\tau)} = -\frac{\sqrt{N}\tau^2 \frac{\nu'(\tau)}{\nu(\tau)^2}}{\frac{1}{\sqrt{N}\nu(\tau)}}$$
$$= -N\tau^2 \cdot \frac{\nu'(\tau)}{\nu(\tau)},$$

and we conclude

$$w_N^* \mathsf{E}_2^{(N)}(\tau) = -N\tau^2 \mathsf{E}_2^{(N)}.$$

■

2.4 K-rational points on modular curves

When defining elliptic curves and isogenies algebraically, we have a notion of a field of definition K. Since modular curves parameterize elliptic curves, we would like to similarly have a notion of K-rational functions and K-rational points that correspond to enhanced elliptic curves defined over K. We focus only on the modular curves $X_0(N)$, since these are our primary interest.

Definition 2.4.1. The set of *K-rational functions* $K(X_0(N))$ on $X_0(N)$ consists of the modular functions on $X_0(N)$ having q-expansions with coefficients in K.

Definition 2.4.2. The set of *K-rational points* $X_0(N)(K)$ on $X_0(N)$ are those corresponding to cyclic N-isogenies defined over K.

It is not obvious that these two definitions are compatible; we would rather treat $X_0(N)$ as a projective curve in order to translate the transcendental language of q-expansions to the rational language of function fields in algebraic geometry. Fortunately, this is always possible.

Theorem 2.4.3. [[Ste99], Theorem 8.10]. *There exists an irreducible integer polynomial $\Phi_N(x, y)$, known as the modular polynomial, with vanishing set parameterized by $x = j(\tau), y = j(N\tau)$ over $\tau \in X_0(N)$.*

This is similar to the map between a complex elliptic curve $\mathbb{C}/\Lambda$ to an algebraic elliptic curve in the sense that it translates between a Riemann surface and an affine model. The affine version of the modular curve $X_0(N)$ is sometimes called the "classical modular curve." Every point $\tau \in Y_0(N)$ corresponding to a K-rational cyclic N-isogeny $E \to E'$ maps to a K-rational point on the classical modular curve, since $j(\tau) = j(E) \in K$ and $j(N\tau) = j(-1/N\tau) = j(E') \in K$.

Note that the Fricke involution w_N^* swaps the coordinates x and y, so that it is always a rational automorphism of order 2 on the classical modular curve over any field of definition. It can be shown that the other Atkin-Lehner involutions are also rational automorphisms of order 2. Thus, when forming the spaces $X_0^+(N) = X_0(N)/\{1, w_N\}$ and $X^*(N) = X_0(N)/W(N)$, we may treat these quotient spaces algebraically. This verifies that the natural maps $X_0(N) \to X_0^+$ and $X_0(N) \to X^*(N)$ are K-rational for any field K, since the automorphisms defining the quotient are K-rational. A K-rational point on $X_0^+(N)$ must have fiber $\mathcal{P} \subset X_0(N)$ stable under $\mathrm{Gal}(\overline{K}/K)$. Since the map $X_0(N) \to X_0^+$ has degree 2, we conclude that either $\mathcal{P}$ consists of one or two points defined over K, or it consists of two points P, P' defined over some quadratic extension L/K with P, P' related by Galois conjugation. Similarly, the fiber in $X_0(N)$ of a K-rational point on $X^*(N)$ consists of points lying in some multi-quadratic extension of K since $W(N) \cong (\mathbb{Z}/2\mathbb{Z})^{\omega(N)}$, and this fiber is stable under the Galois action $\mathrm{Gal}(\overline{K}/K)$; we will return to this idea in our discussion of K-curves.

One issue with treating $X_0(N)$ as a curve over K is that points of $X_0(N)$ correspond to cyclic N-isogenies up to $\mathbb{C}$-isomorphism, *not* up to K-isomorphism. In general, a $\mathbb{C}$-isomorphism class of isogenies will split into infinitely many K-isomorphism classes of isogenies related by twists; as long as we avoid $j \in \{0, 1728\}$, these will be quadratic twists. Therefore, to a given K-rational point $\tau \in X_0(N)$, there is no canonical association with a particular K-isomorphism class of affine elliptic curves $E \to E'$ related by a cyclic N-isogeny in the sense of Theorem 2.1.8. However, once a choice of twist for E is fixed, this determines the twist of E' and the isogeny.

2.5 The Tate curve

Some computations involving modular curves and modular forms can be reduced to linear algebra on q-expansions. For example, this is one way to prove the Uniformization Theorem 2.3.2. It is therefore useful when considering the model of an affine elliptic curve to treat it as a curve with coefficients given by q-series; the Tate curve does precisely this.

Let K be a number field. Instead of treating an elliptic curve E/K as a projective plane curve with coefficients in K, we may instead apply the Uniformization Theorem to treat all elliptic curves over number fields as specializations of a plane curve defined over $\mathbb{C}((q))$, known as the *Tate curve*:

$$\mathbb{G}/q^{\mathbb{Z}} : y^2 = 4x^3 - 60G_4(q)x - 140G_6(q).$$

We may apply a change of variables to transform the Eisenstein series $G_4(q), G_6(q)$ into their normalized versions $\mathsf{E}_4(q), \mathsf{E}_6(q)$ to show that $\mathbb{G}/q^{\mathbb{Z}}$ is actually defined over $\mathbb{Q}((q))$, with model

$$\mathbb{G}/q^{\mathbb{Z}} : y^2 = x^3 - \frac{\mathsf{E}_4}{48}x + \frac{\mathsf{E}_6}{864}.$$

See [[Elk98], Equation (32)].

One benefit of viewing elliptic curves from the perspective of the Tate curve is that the Weierstrass coefficients can be treated as modular functions. For any modular curve X, the coefficients $-\frac{\mathsf{E}_4}{48}$ and $\frac{\mathsf{E}_6}{864}$ are modular forms on X of weight 4 and 6 respectively. However, if λ is a modular form of weight 2 on X, then the change of variables $(x, y) \mapsto (\lambda x, \lambda^{3/2} y)$ twists the Tate curve into the curve

$$\mathbb{G}/q^{\mathbb{Z}} : y^2 = x^3 - \frac{\mathsf{E}_4}{48\lambda^2}x + \frac{\mathsf{E}_6}{864\lambda^3}. \tag{2}$$

Now the coefficients

$$a_4 = -\frac{\mathsf{E}_4}{48\lambda^2}, \qquad a_6 = \frac{\mathsf{E}_6}{864\lambda^3}$$

may be treated as modular *functions* on X. In this model, the coordinate functions x, y may be given as functions of τ and $z \in \mathbb{C}/\Lambda_\tau$ based on the Weierstrass $\wp$-function, and indeed as functions of $q = \exp(2\pi i\tau)$ and $q_z = \exp(2\pi i z)$. More precisely, we have

$$x = \lambda^{-1}\left[\frac{1}{2} - 2\sum_{n=1}^{\infty}\frac{q^n}{(1-q^n)^2} + \sum_{n=-\infty}^{\infty}\frac{q^n q_z}{(1-q^n q_z)^2}\right], \tag{3}$$

$$y = \frac{1}{2}\lambda^{-3/2}\sum_{n=-\infty}^{\infty}\frac{(q^n q_z)^2 + q^n q_z}{(1-q^n q_z)^3}. \tag{4}$$

Again, see [[Elk98], Equation (31)].

We will discuss explicit parameterizations of the function field $K(X_0(N))$ in Section 3 when the modular curve $X_0(N)$ has genus 0, and so we will be able to explicitly identify the coefficients a_4, a_6 in the model (2) in terms of this parameterization. Taking $\lambda = \mathsf{E}_2^{(N)}$ will be a useful choice of weight 2 modular form on $X_0(N)$ since $\mathsf{E}_2^{(N)}$ is anti-invariant under the Fricke involution by Proposition 2.3.12. This model will play a critical role in the proof of the Main Theorem 4.3.3 on strict K-curves over fibers of $X_0^+(N)$.

3 Rational parameterizations of genus 0 modular curves

3.1 A Hauptmodul of $X_0(N)$ as an eta product

Modular curves have parameterizations that give rational expressions for various quantities of interest, such as the j-invariant or the coefficients of the corresponding elliptic curve. This is especially true for modular curves of genus 0: rational functions involving Hauptmoduln are effective computational tools.

Proposition 3.1.1. *The modular curve $X_0(N)$ has genus 0 if and only if N is one of the following 15 integers:*

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18, 25.$$

Proof. One can prove this by using the formula [[DS05], Theorem 3.1.1] for the genus of a modular curve $X(\Gamma)$

$$g = 1 + \frac{d}{12} - \frac{\varepsilon_2}{4} - \frac{\varepsilon_3}{3} - \frac{\varepsilon_\infty}{2},$$

where d is the degree of the map $X(\Gamma) \to X(1)$, the quantities ε_2 and ε_3 are the number of elliptic points of period 2 and 3 on $X(\Gamma)$, and ε_∞ is the number of cusps on $X(\Gamma)$. In the case $X(\Gamma) = X_0(N)$, we have

$$\begin{aligned}
d &= N \prod_{p|N} \left(1 + \frac{1}{p}\right), \\
\varepsilon_2 &= \begin{cases} \prod_{p|N} \left(1 + \left(\frac{-1}{p}\right)\right) : & 4 \nmid N \\ 0 : & 4 \mid N, \end{cases} \\
\varepsilon_3 &= \begin{cases} \prod_{p|N} \left(1 + \left(\frac{-3}{p}\right)\right) : & 9 \nmid N \\ 0 : & 9 \mid N, \end{cases} \\
\varepsilon_\infty &= \sum_{\delta|N} \varphi(\gcd(\delta, N/\delta)),
\end{aligned}$$

where

- p denotes a prime divisor of N;
- δ denotes an arbitrary positive divisor of N;
- $\left(\frac{-1}{p}\right)$ and $\left(\frac{-3}{p}\right)$ are Legendre symbols, with $\left(\frac{-3}{3}\right)$ defined to be 0; and
- φ is the Euler totient function.

See [[DS05], Figure 3.3]. ∎

The curve $X_0(1) = X(1)$ has the j-invariant as a Hauptmodul. We would like to explicitly compute a Hauptmodul for the other 14 values of N. Eta products provide a convenient method of doing so; these are products of the form

$$\prod_{\delta|N} \eta(\delta\tau)^{r_\delta}$$

with each r_δ an integer. In order for an eta product to be a Hauptmodul, we recall the normalization conditions from Definition 2.3.8 and require that

1. The Hauptmodul h_N has a simple zero at the cusp $\tau = 0$ and a simple pole at the cusp $\tau = \infty$; and
2. The q-expansion of h_N is of the form
$$1 \cdot q^{-1} + O(1).$$

Note that the first condition is possible because 0 is always inequivalent to ∞ under $\Gamma_0(N)$ as long as $N > 1$. Some authors, such as [Mai09], swap our h_N with $w_N^* h_N$; under our definitions, the function $w_N^* h_N$ is not a Hauptmodul since it does not have its pole at ∞, but it is an alternative rational coordinate on $X_0(N)$. Some authors also refer to "eta products" as "eta quotients."

We regard the eta function as vanishing to order $1/24$ at ∞ since η^{24} is a constant multiple of the modular discriminant Δ, which has a simple zero at ∞. Additionally, since Δ has no zeros or poles on $\mathbb{H}$, neither does the eta function. This leads us to the *Ligozat conditions*, which give number-theoretic conditions on the exponents r_δ to ensure that the eta product is a modular function:

Proposition 3.1.2. [[Lig74], Proposition 3.2.1]. *The function $\prod_{\delta|N} \eta(\delta\tau)^{r_\delta}$ defines a modular function on $X_0(N)$ if and only if the following four conditions hold:*

(a) $\sum_{\delta|N} r_\delta \cdot \delta \equiv 0 \mod 24$,

(b) $\sum_{\delta|N} r_\delta \cdot (N/\delta) \equiv 0 \mod 24$,

(c) $\sum_{\delta|N} r_\delta = 0$,

(d) $\prod_{\delta|N} (N/\delta)^{r_\delta} \in (\mathbb{Q}^\times)^2$.

Condition (a) corresponds to integrality of the order of vanishing at ∞, and condition (b) corresponds to integrality at 0. However, we require more than integrality: we need the order at ∞ to be exactly -1 and the order at 0 to be exactly $+1$. We also require that the eta product have zero order of vanishing at all other cusps. Let $\frac{a}{d} \in \mathbb{Q}$ be in lowest form. To find the order of vanishing of $\eta(\delta\tau)$ at $\frac{a}{d}$, we apply some "cusp-normalizing map" $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ that sends $\infty \mapsto \frac{a}{d}$, and we may use the functional equation of η to verify that $\eta(\delta\tau)$ has order $\frac{1}{24}(\delta, d)^2/\delta$ at $\frac{a}{d}$. Here $(\cdot, \cdot)$ denotes the greatest common divisor.

To compute the order at the cusp $\left[\frac{a}{d}\right] \in X_0(N)$, we must multiply by the width $(N/d) \cdot (d, N/d)$ of this cusp. All cusps of $X_0(N)$ have a representative $\frac{a}{d}$ with d a divisor of N, so this means that it suffices to impose the conditions

$$(N/d)(d, N/d) \cdot \sum_{\delta|N} r_\delta \cdot (\delta, d)^2/\delta = 0$$

for each divisor $d \mid N$ other than $d = 1, N$. We include the factor of $(N/d)(d, N/d)$ so that the coefficient of each r_δ is an integer, but omitting it does not affect the condition. The divisors 1 and N correspond to the cusps at $0 \in \left[\frac{1}{1}\right]$ and $\infty \in \left[\frac{1}{N}\right]$ respectively, for which we have the conditions

$$\sum_{\delta|N} r_\delta \cdot (N/\delta) = 24,$$

$$\sum_{\delta|N} r_\delta \cdot \delta = -24.$$

for order of vanishing 1 and -1 respectively. We summarize this discussion as a proposition:

Proposition 3.1.3. *An eta product $\prod_{\delta|N} \eta(\delta\tau)^{r_\delta}$ defines a Hauptmodul on the modular curve $X_0(N)$ if and only if the following conditions hold on the integer exponents r_δ:*

(a) $\sum_{\delta|N} r_\delta \cdot \delta = -24$,

(b) $\sum_{\delta|N} r_\delta \cdot (N/\delta) = 24$,

(c) $\sum_{\delta|N} r_\delta = 0$,

(d) $\prod_{\delta|N} (N/\delta)^{r_\delta} \in (\mathbb{Q}^\times)^2$,

and for all divisors $d \mid N$ besides $d = 1, N$, we have

(e) $(N/d)(d, N/d) \sum_{\delta|N} r_\delta \cdot (\delta, d)^2/\delta = 0$.

The linear conditions (a), (b), (c), and (e) in Proposition 3.1.3 are enough to uniquely specify the exponents r_δ when $N > 1$ is in the list given in Proposition 3.1.1, and we may check that these solutions also satisfy condition (d). We denote the corresponding eta product by h_N, or by h when the value of N is clear. These eta products are listed in Table 1. In this table, we also describe the image of these Hauptmoduln under the Fricke involution. We always have $w_N^* h_N = \kappa_N / h_N$ for some constant κ_N, which can be readily verified using the functional equation for η.

N	2	3	4	5	6	7	8	9
h_N	$\left(\frac{\eta(\tau)}{\eta(2\tau)}\right)^{24}$	$\left(\frac{\eta(\tau)}{\eta(3\tau)}\right)^{12}$	$\left(\frac{\eta(\tau)}{\eta(4\tau)}\right)^{8}$	$\left(\frac{\eta(\tau)}{\eta(5\tau)}\right)^{6}$	$\frac{\eta^5(\tau)\eta(3\tau)}{\eta(2\tau)\eta^5(6\tau)}$	$\left(\frac{\eta(\tau)}{\eta(7\tau)}\right)^{4}$	$\frac{\eta^4(\tau)\eta^2(4\tau)}{\eta^2(2\tau)\eta^4(8\tau)}$	$\left(\frac{\eta(\tau)}{\eta(9\tau)}\right)^{3}$
$w_N^* h_N$	$2^{12}/h_2$	$3^6/h_3$	$2^8/h_4$	$5^3/h_5$	$2^3 \cdot 3^2/h_6$	$7^2/h_7$	$2^5/h_8$	$3^3/h_9$

N	10	12	13	16	18	25
h_N	$\frac{\eta^3(\tau)\eta(5\tau)}{\eta(2\tau)\eta^3(10\tau)}$	$\frac{\eta^3(\tau)\eta(4\tau)\eta^2(6\tau)}{\eta^2(2\tau)\eta(3\tau)\eta^3(12\tau)}$	$\left(\frac{\eta(\tau)}{\eta(13\tau)}\right)^{2}$	$\frac{\eta^2(\tau)\eta(8\tau)}{\eta(2\tau)\eta^2(16\tau)}$	$\frac{\eta^2(\tau)\eta(6\tau)\eta(9\tau)}{\eta(2\tau)\eta(3\tau)\eta^2(18\tau)}$	$\frac{\eta(\tau)}{\eta(25\tau)}$
$w_N^* h_N$	$20/h_{10}$	$12/h_{12}$	$13/h_{13}$	$8/h_{16}$	$6/h_{18}$	$5/h_{25}$

Table 1: The Hauptmodul h_N of $X_0(N)$ as an eta product and its image $w_N^* h_N$ under the Fricke involution.

3.2 The j-invariant as a rational function of each Hauptmodul

The degree of the map $X_0(N) \to X(1)$ is equal to the index of $\Gamma_0(N)/\{\pm I\}$ in $\mathrm{SL}_2(\mathbb{Z})/\{\pm I\}$, which is

$$\psi(N) := N \prod_{p \mid N} \left(1 + \frac{1}{p}\right).$$

Therefore, when $X_0(N)$ has genus 0, there exists a degree $\psi(N)$ rational function giving the j-invariant in terms of the Hauptmodul for $X_0(N)$. Since the degree of the rational function is known, this expression may be found by using linear algebra to compare q-expansions. Explicitly, we have the following algorithm:

1. Let $n = \psi(N)$, let $h = q^{-1} + O(1)$ be the Hauptmodul of $X_0(N)$, and let $H = 1/h$. Compute the inverse
$$Q(H) + O(H^{2n+3}) = q(H)$$
of the q-expansion of H to at least $2n + 2$ terms.

2. Compute
$$J(H) + O(H^{2n+2}) := j(Q(H))$$
to express j as a Laurent series $J(H) = H^{-1} + O(1)$ in H correct to a precision of $2n + 1$ terms. Let the coefficient of H^i in $J(H)$ be a_i.

3. Find a generator $(b_n, b_{n-1}, \ldots, b_0)$ of the 1-dimensional kernel of the $(n+2) \times (n+2)$ matrix

$$\begin{pmatrix} 1 & a_0 & a_1 & \ldots & a_n \\ a_0 & a_1 & a_2 & \ldots & a_{n+1} \\ a_1 & a_2 & a_3 & \ldots & a_{n+2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_n & a_{n+1} & a_{n+2} & \ldots & a_{2n+1} \end{pmatrix}$$

4. Compute

$$P(H) = J(H) \cdot (b_n H^n + b_{n-1} H^{n+1} + \cdots + b_0).$$

Then

$$j = \frac{P(H)}{b_n H^n + b_{n-1} H^{n+1} + \cdots + b_0}.$$

Substitute $1/h = H$ to obtain j as a rational function of h.

As a "sanity check," in practice we compute the series in the algorithm to a few more terms than required. We list in Table 2 the results up to $N = 5$; see [[Mai09], §3.2] for a full table.

N	j	$j - 1728$
2	$\frac{(h+256)^3}{h^2}$	$\frac{(h+64)(h-512)^2}{h^2}$
3	$\frac{(h+27)(h+243)^3}{h^3}$	$\frac{(h^2-486h-19683)^2}{h^3}$
4	$\frac{(h^2+256h+4096)^3}{h^4(h+16)}$	$\frac{(h+32)^2(h^2-512-8192)^2}{h^4(h+16)}$
5	$\frac{(h^2+250h+3125)^3}{h^5}$	$\frac{(h^2+22h+125)(h^2-500h-15625)^2}{h^5}$
$\vdots$	$\vdots$	$\vdots$

Table 2: Expressions of j and $j - 1728$ in terms of the Hauptmodul $h = h_N$ up to $N = 5$.

The group $\mathrm{SL}_2(\mathbb{Z})/\{\pm I\}$ acts freely on $\mathbb{H}^*$ except on the cusps and the *elliptic points* given by the orbits of $e^{2\pi i/3}$ and i corresponding to $j = 0$ and $j = 1728$ respectively. This implies that the only ramified values of the map $X_0(N) \to X(1)$ are given by $j = 0, 1728$, and ∞. One benefit of computing the rational functions giving j in terms of h_N is that we may view the ramification behavior at $j = 0$ and ∞ at a glance. Similarly, we may view the ramification behavior at $j = 1728$ and ∞ from the rational function expressing $j - 1728$ in terms of h_N. For example, the expressions for j and $j - 1728$ in terms of h_2 show that the ramification divisor of $X_0(2) \to X(1)$ is

$$2[-256] + [512] + [0].$$

with coordinates given by h_2. This agrees with the Riemann-Hurwitz formula for a degree 3 map between genus 0 Riemann surfaces.

As noted in Section 2.4, the fixed points of the Fricke involution yield elliptic curves with complex multiplication. For each of the curves $X_0(N)$ of genus 0, we found that $w_N^* h_N = \kappa_N / h_N$ for some constant

κ_N coming from the functional equation of the eta function, so we may immediately find the values of the Hauptmodul at the two fixed points. However, if we can independently determine these fixed points as elements $\tau \in \mathbb{H}$, we obtain the value of $h_N(\tau)$ explicitly at such τ. In conjunction with the rational expression for the j-invariant, this allows us to find many special values of j at certain CM points.

The point $\tau = i/\sqrt{N}$ is always a fixed point of the Fricke involution w_N. We also know that $h_N \cdot w_N^* h_N = \kappa_N$ for some constant κ_N, so the fixed points in h-coordinates are given by $\pm\sqrt{\kappa_N}$. When τ lies on the positive imaginary axis, the variable $q = \exp(2\pi i\tau)$ lies in the interval $(0, 1)$. Therefore the product $\prod_{n=1}^{\infty}(1-q^n)$ used in the definition of the eta function must be positive for τ on the positive imaginary axis. When writing a Hauptmodul as an eta product, the factors of $q^{1/24}$ from the eta function must cancel, so we conclude that h_N is also positive when τ lies on the positive imaginary axis. Combining this with the expressions for the j-invariant from Table 2 (and its completion in [[Mai09], §3.2]), we obtain 14 special values of $j(\tau)$, which we list in Table 3 in Appendix A.

3.3 Coefficients of elliptic curves as rational functions of Hauptmoduln

Recall from our discussion of the Tate curve in Section 2.5 that we may explicitly find an affine model of the elliptic curve E corresponding to $\tau \in X_0(N)$:

$$E : y^2 = x^3 - \frac{\mathsf{E}_4(\tau)}{48\lambda^2} + \frac{\mathsf{E}_6(\tau)}{864\lambda^2}. \tag{5}$$

Here λ is an arbitrary weight 2 modular form on $X_0(N)$. However, if we want to find the isogenous curve E' associated to τ, we must exercise caution. If E is defined over K, then we would like the isogenous curve E' to be isogenous to E *over* K rather than merely over $\mathbb{C}$. Since $w_N(\tau) = -1/N\tau$, and $j(-1/N\tau) = j(N\tau)$, the isogenous curve E' will have some model isomorphic to

$$E' : y^2 = x^3 - \frac{\mathsf{E}_4(N\tau)}{48\lambda^2} + \frac{\mathsf{E}_6(N\tau)}{864\lambda^3} \tag{6}$$

where we replace τ with $N\tau$ in the arguments of the normalized Eisenstein series, but not in the modular form λ. To prove that this is the correct twist corresponding to the chosen model (5) of E, we note that by Theorem 2.1.8, the isogeny of complex curves corresponding to $\tau \in Y_0(N)$ is given explicitly by

$$\begin{aligned} \mathbb{C}/\Lambda_\tau &\to \mathbb{C}/\Lambda_{N\tau} \\ z &\mapsto Nz. \end{aligned}$$

Therefore, on the Tate curve, the isogeny given on the coordinates x, y by replacing q with q^N and q_z with q_z^N in formulas (3) and (4), and indeed these new coordinates lie on the model of E' given by (6).

Taking $\lambda = \mathsf{E}_2^{(N)}(\tau)$, we can find an expression for the modular functions

$$a_4 := -\frac{\mathsf{E}_4(\tau)}{48\mathsf{E}_2^{(N)}(\tau)^2}, \qquad a_6 := \frac{\mathsf{E}_3(\tau)}{864\mathsf{E}_2^{(N)}(\tau)^3},$$
$$a_4' := -\frac{\mathsf{E}_4(N\tau)}{48\mathsf{E}_2^{(N)}(\tau)^2}, \qquad a_6' := \frac{\mathsf{E}_3(N\tau)}{864\mathsf{E}_2^{(N)}(\tau)^3}$$

in terms of the Hauptmodul h_N when $X_0(N)$ has genus zero by comparing q-expansions, similar to how we found the rational functions giving j in terms of each h_N. These give explicit expressions for the coefficients of the isogenous curves

$$\begin{aligned} E &: y^2 = x^3 + a_4 x + a_6 \\ E' &: y^2 = x^3 + a_4' x + a_6' \end{aligned}$$

in terms of the coordinate h_N. We give a complete set of results for all

$$N \in \{2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18, 25\}$$

in Tables 4 to 14 in the appendix.

Finally, we include here some additional formulas for curves in special Weierstrass forms familiar from 2- and 3-isogeny descent. The curves

$$E_2 : y^2 = x^3 + a_2x^2 + a_4x, \qquad E_2' : y^2 = x^3 - 2a_2x^2 + (a_2^2 - 4a_4)x$$

are always 2-isogenous, and the curves

$$E_3 : y^2 = x^3 + d(ax + b)^2 \qquad E_3' : y^2 = x^3 - 3d(ax + (27b - 4a^3d)/9)^2$$

are always 3-isogenous in characteristic 0; see [[Sil09], Chapter X.1], and [CP09] for more details on the role of these models in 2- and 3-isogeny descent, respectively. We have

$$j(E_2) = \frac{256(a_2^2 - 3a_4)^3}{(a_2^2a_4^2 - 4a_4^3)},$$
$$j(E_3) = \frac{256(d^2a^4 - 6dab)^3}{4d^3a^3b^3 - 27d^2b^4}.$$

Equating these j-invariants with the formula for the j-invariant in terms of Hauptmoduln from Table 2

$$j = \frac{(h_2 + 256)^3}{h_2^2},$$
$$j = \frac{(h_3 + 27)(h_3 + 243)^3}{h_3^3},$$

we search for rational solutions for h. In both cases, we find only one rational solution given by

$$h_2 = \frac{256a_4}{a_2^2 - 4a_4}, \tag{7}$$
$$h_3 = \frac{729b}{4a^3d - 27b}. \tag{8}$$

so in these models we explicitly find the points in $Y_0(2)$ and $Y_0(3)$ corresponding to the isogenies $E_2 \to E_2'$ and $E_3 \to E_3'$ respectively. Finally, we may invert expressions (7) and (8) to find that E_2 and E_3 correspond to the same points on $Y_0(2)$ and $Y_0(3)$ as

$$\tilde{E}_2 : y^2 = x^3 + (4h_2 + 256)x^2 + h_2(4h_2 + 256)x,$$
$$\tilde{E}_3 : y^2 = x^3 + \frac{1}{4}((27h_3 + 729)x + h_3(27h_3 + 729)^2)^2,$$

respectively, though $\tilde{E}_2$ might be a twist of E_2 and $\tilde{E}_3$ might be a twist of E_3.

4 Elliptic K-curves

4.1 Introduction to K-curves

Elliptic curves defined over $\mathbb{Q}$ have been extensively studied, and results such as Mazur's Theorem and the Modularity Theorem are some of the most celebrated in modern number theory. Therefore, one reasonable direction of study would be to find some generalization of elliptic curves over $\mathbb{Q}$ that would allow the extension of such known results. This has led to the study of elliptic $\mathbb{Q}$-curves, or more generally elliptic K-curves for any field K.

Definition 4.1.1. Let K be a field with separable closure M, and let $G = \mathrm{Gal}(M/K)$. An elliptic curve E defined over M is said to be a an *elliptic K-curve*, or K-curve, if all G-conjugates of E are isogenous to E over M. We let L denote the field of definition of the K-curve E, so that $K \subseteq L \subseteq M$.

Example 4.1.2. Let E be the curve

$$E : y^2 = x^3 - 2\sqrt{-2} \cdot x^2 + (-1 + 2\sqrt{-2})x.$$

defined over $\mathbb{Q}(\sqrt{-2})$. The curve E is 2-isogenous over $\mathbb{Q}(\sqrt{-2})$ to

$$E' : y^2 = x^3 + 4\sqrt{-2} \cdot x^2 - (4 + 8\sqrt{-2})x$$

Scale x by 2 and y by $2\sqrt{2}$ to find that E' is isomorphic over $\mathbb{Q}(i, \sqrt{2})$ to

$$\overline{E} : y^2 = x^3 + 2\sqrt{-2} \cdot x^2 - (1 + \sqrt{-2})x.$$

Since $\overline{E}$ is the only conjugate of E under $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ other than itself, we conclude that E is a $\mathbb{Q}$-curve via the isogeny $E \to E' \to \overline{E}$.

Notice that in this example the isomorphism between E' and $\overline{E}$ had to be taken over an extension $\mathbb{Q}(i, \sqrt{2})$ of the field of definition $\mathbb{Q}(\sqrt{-2})$ of E. In the absence of complex multiplication, isogenies are unique up to composition with $[-1]$, so we cannot force this isogeny $E \to \overline{E}$ to be defined over the field of definition. Therefore, one natural question is:

Question 4.1.3. When can the isogeny $E \to E^\sigma$ between a K-curve E and its conjugate be defined over the field of definition L of E?

We will examine this question shortly as one of the main results of this thesis.

Galois representations coming from the Tate module $T_\ell E$ illustrate one reason why elliptic $\mathbb{Q}$-curves can be considered to generalize curves defined over $\mathbb{Q}$. We have a representation

$$\rho_{C,\ell} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{End}(T_\ell C)$$

for any elliptic curve C defined over $\mathbb{Q}$, and the isomorphism class of this representation depends only on the isogeny class of C. Similarly, letting E be a K-curve, we may derive a Galois representation

$$\rho_{E,\ell} : \mathrm{Gal}(\mathbb{Q}/\mathbb{Q}) \to \overline{\mathbb{Q}}_\ell^* \mathrm{GL}_2(\mathbb{Q}_\ell).$$

We omit further motivational discussion, since it would involve introducing Galois cohomology and would take us too far afield; see [Ell04] for further details.

4.2 Constructing and classifying K-curves

Elliptic curves with complex multiplication provide the first examples of K-curves. Indeed, some authors, such as [BG85], originally restricted the definition only to CM curves. We prove that CM curves are K-curves in the case that K is a number field.

Proposition 4.2.1. *Let K be a number field, and let $E/\overline{\mathbb{Q}}$ have complex multiplication. Then E is a K-curve.*

Proof. Since E is CM, the endomorphism ring $\mathrm{End}_{\mathbb{C}}(E)$ must be an imaginary quadratic order A [[Sil09], Corollary III.9.4]. For any $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/K)$, the rings $\mathrm{End}_{\mathbb{C}}(E)$ and $\mathrm{End}_{\mathbb{C}}(E^\sigma)$ are isomorphic, since an endomorphism φ of E corresponds to the endomorphism φ^σ of E^σ.

Now treat E and E^σ as complex elliptic curves $\mathbb{C}/\Lambda$ and $\mathbb{C}/\Lambda'$. Since endomorphisms of E are in correspondence with homotheties of Λ [[Sil09], Corollary 4.1.1], we conclude that $\mathrm{End}_{\mathbb{C}}(\Lambda) \cong \mathrm{End}_{\mathbb{C}}(\Lambda') \cong A$. But the only complex lattices equipped with an endomorphism ring isomorphic to the imaginary quadratic

order A are those of the form cI for some ideal I of A and $c \in \mathbb{C}$. Here, we are embedding $A \subset \mathbb{C}$ as a lattice itself.

We may therefore write $\Lambda = cI$ and $\Lambda = c'I$ for some ideals $I, I' \subseteq A \subset \mathbb{C}$ and $c, c' \in \mathbb{C}$. The ideal I' has finite index N', so it contains $N'A$. Therefore, $\Lambda' = c'I'$ contains the scalar multiple $\frac{c'N'}{c}I$ of Λ with finite index, yielding a map $\mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ of finite degree, which corresponds to an isogeny $E \to E'$. ■

The set of K-curves is closed under isogeny, so that we may speak of isogeny classes of K-curves rather than isomorphism classes.

Proposition 4.2.2. *If E is a K-curve, then so is any curve E' isogenous to E over M.*

Proof. Let $\sigma \in \mathrm{Gal}(M/K)$, and let $\varphi : E \to E^\sigma$ and $\psi : E \to E'$ be isogenies. Then we obtain an isogeny $\psi^\sigma : E^\sigma \to (E')^\sigma$, and so we can construct an isogeny $\psi^\sigma \circ \varphi \circ \hat{\psi} : E' \to (E')^\sigma$:

$$\begin{array}{ccc} E & \xrightarrow{\varphi} & E^\sigma \\ {\scriptstyle\hat{\psi}}\uparrow & & \downarrow{\scriptstyle\psi^\sigma} \\ E' & \longrightarrow & (E')^\sigma \end{array}$$

■

We may obtain K-curves from K-rational points on a modular curve $Y^*(N)$—recall that this modular curve is the the quotient of $Y_0(N)$ by the action of the group of Atkin-Lehner involutions $W(N)$. We may also obtain them similarly from K-rational points on $Y_0^+(N)$, the quotient of $Y_0(N)$ by the action of the Fricke involution.

Proposition 4.2.3. *Let P be a K-rational point on $Y^*(N)$. Then every point in the fiber $\mathcal{P}$ of P in $Y_0(N)$ corresponds to a K-curve. Similarly, the fibers of K-rational points on $Y_0^+(N)$ correspond to K-curves.*

Proof. The set $\mathcal{P}$ is stable under $\mathrm{Gal}(M/K)$ because it is the fiber of a K-rational point under a K-rational map. However, since the points of $\mathcal{P}$ are all related by Atkin-Lehner involutions, their corresponding elliptic curves are all isogenous. The same reasoning applies for the K-rational fibers of $Y_0^+(N)$. ■

The previous proposition classifies all non-CM K-curves by a theorem of Elkies:

Theorem 4.2.4. [Elk04]. *Let K be any field with separable closure M, and let E be a K-curve without complex multiplication. Then there exists a squarefree integer N, depending only on the M-isogeny class of E, such that:*

1. *E is isogenous over M with a K-curve arising from a K-rational point on $Y^*(N)$ in the sense of Proposition 4.2.3; and*
2. *If for some N' there is a K-rational point on $Y^*(N')$ that parameterizes K-curves isogenous with E, then $N \mid N'$.*

Corollary 4.2.5. *Any non-CM K-curve E is isogenous to a curve defined over a finite multi-quadratic extension L/K. That is, L is of the form $K(\sqrt{a_1}, \sqrt{a_2}, \ldots, \sqrt{a_n})$ with $a_i \in K$.*

Proof. This follows from the fact that the group $W(N)$ of Atkin-Lehner involutions is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{\omega(N)}$. ■

4.3 Main theorem on strict K-curves given by fibers over $Y_0^+(N)$

We now revisit Question 4.1.3. If E is a K-curve defined over L, when may we define the isogeny $E \to E^\sigma$ over L? As discussed in Section 2.4, the points on the modular curve $Y_0(N)$ correspond to $\mathbb{C}$-isomorphism classes of elliptic curves, but these split into many K-isomorphism classes related by quadratic twists as long as we avoid $j \in \{0, 1728\}$. We may ignore these two cases in our discussion because they correspond to CM curves. There is no canonical way to associate a K-isomorphism class of elliptic curves to a point $P \in Y_0(N)(K)$, yet this ambiguity also allows some freedom that we may leverage to our advantage. To illustrate, we reconsider Example 4.1.2.

Example 4.1.2 revisited. We found that the curve

$$E : y^2 = x^3 - 2\sqrt{-2} \cdot x^2 + (-1 + 2\sqrt{-2})x$$

is isomorphic to its conjugate only over $\mathbb{Q}(i, \sqrt{2})$. However, let us instead consider the twist

$$F : y^2 = x^3 + 4x^2 + (2 - 4\sqrt{-2})x,$$

which is isomorphic to E over $\mathbb{C}$ via the change of variables $(x, y) \mapsto \left(\sqrt{-2} \cdot x, \sqrt{-2\sqrt{-2}} \cdot y\right)$. Then F is 2-isogenous over $\mathbb{Q}(\sqrt{-2})$ to

$$F' : y^2 = x^3 - 8x^2 + 8(1 + 2\sqrt{-2})x.$$

But F' is isomorphic to

$$\overline{F} : y^2 = x^3 + 4x^2 + (2 + 4\sqrt{-2})x$$

via the change of variables $(x, y) \mapsto (-2x, -2\sqrt{-2} \cdot y)$. Thus, we obtain an isogeny $F \to \overline{F}$ that is defined *over the field of definition* $L = \mathbb{Q}(\sqrt{-2})$ of F, which was impossible for the twist E.

This example illustrates that by taking an appropriate twist of a K-curve, it may be possible to find a K-curve for which the isogeny between Galois conjugates is defined over the field of definition L/K rather than requiring some extension of L.

Definition 4.3.1. Let E be a K-curve defined over the extension L/K. We say that E is a *strict* K-curve if E is isogenous to its $\mathrm{Gal}(L/K)$ conjugates over L rather than some larger extension.

Thus, we refine our main question to:

Question 4.3.2. Let K be a number field, and let P be an L-rational point on $Y_0(N)$ corresponding to a $\mathbb{C}$-isomorphism class of K-curves. When can we *choose* a twist giving a strict K-curve E/L corresponding to P? When this is possible, can we determine exactly which twists of E are strict K-curves?

Let h, h' denote L-rational coordinates on $X_0(N)$, even when $X_0(N)$ does not have genus 0. We use bar notation, e.g. $\overline{h}$, to denote Galois conjugation over the quadratic extension L/K, which is not to be confused with complex conjugation. The fiber of any unramified point H on $X^+(N)$ contains two curves E, E'; the ramified points correspond to CM curves, we which we ignore in our discussion. If H is K-rational, then its two preimages h, h' are either K-rational themselves and thus are automatically strict K-curves, else they are L-rational for some quadratic extension of K. In the latter case, the points h and h' must be conjugates in L/K. That is, we must have

$$w^* h = \overline{h} = h',$$

where $\overline{h}$ denotes the unique Galois conjugate of h in L/K.

With this setup, we present the main theorem of this thesis, which gives a precise constructive description of strict K-curves that arise from K-rational points on $X_0^+(N)$. This description involves a Diophantine condition on a pair of conics that is independent of the coordinate h, only depending on the field extension L.

Theorem 4.3.3. *Let L/K be a quadratic extension, and let $\{h, h'\} \subset Y_0(N)(L) \setminus Y_0(N)(K)$ be the fiber of a non-CM point in $Y_0^+(N)(K)$. Let $\tau, \tau' \in \mathbb{H}$ correspond to h, h', and likewise let E, E' be the isogenous elliptic curves corresponding to h, h'.*

(a) The following are equivalent:

(i) There exists a choice of twist of cyclic N-isogeny $E \to E'$ defined over L such that E' is isomorphic over L to the conjugate curve $\overline{E}$ of E.

(ii) At least one of the integers N or $-N$ lies in the image of the Galois norm map $L^\times \to K^\times$.

(b) The twists described by (a) are precisely those isomorphic to the models

$$E : y^2 = x^3 - \frac{\alpha^2 A_4}{48}x + \frac{\alpha^3 A_6}{864}, \qquad E' : y^2 = x^3 - \frac{\alpha^2 A_4'}{48}x + \frac{\alpha^3 A_6'}{864},$$

such that $\alpha \in L^\times$ has Galois norm $\alpha\overline{\alpha}$ lying in $-N \cdot (L^\times)^2$. Here, the coefficients A_4, A_6, A_4', A_6' are given by

$$A_4 := \frac{\mathsf{E}_4(\tau)}{\left(\mathsf{E}_2^{(N)}(\tau)\right)^2}, \qquad A_6 := \frac{\mathsf{E}_6(\tau)}{\left(\mathsf{E}_2^{(N)}(\tau)\right)^3},$$
$$A_4' := \frac{\mathsf{E}_4(N\tau)}{\left(\mathsf{E}_2^{(N)}(\tau)\right)^2}, \qquad A_6' := \frac{\mathsf{E}_6(N\tau)}{\left(\mathsf{E}_2^{(N)}(\tau)\right)^3}$$

as in Section 3.3.

Proof. As discussed in Section 3.3, the points h, h' correspond to the pair of isogenous curves

$$E : y^2 = x^3 + a_4 x + a_6$$
$$E' : y^2 = x^3 + a_4' x + a_6'$$

where

$$a_4 = -\frac{E_4(\tau)}{48\lambda^2}, \qquad a_6 = \frac{\mathsf{E}_6(\tau)}{864\lambda^3},$$
$$a_4' = \frac{\mathsf{E}_4(N\tau)}{48\lambda^2}, \qquad a_6' = \frac{\mathsf{E}_6(N\tau)}{864\lambda^3}$$

for an arbitrary modular form λ of weight 2 on $X_0(N)$; this pair is equipped with the cyclic N-isogeny $E \to E'$ defined over L given by h.

We take the choice $\lambda = \alpha^{-1}\mathsf{E}_2^{(N)}(\tau)$ for some $\alpha \in L^\times$. As α ranges over $L^\times$, the models for E and E' range over all their quadratic twists. Then $\frac{\mathsf{E}_4(\tau)}{\mathsf{E}_2^{(N)}(\tau)^2}$ and $\frac{\mathsf{E}_6(\tau)}{\mathsf{E}_2^{(N)}(\tau)^3}$ are modular functions on $X_0(N)$. These functions are defined over $\mathbb{Q}$, and we have $h' = \overline{h} = w^* h$, so this implies that

$$\overline{A_4} = \overline{\left(\frac{\mathsf{E}_4(\tau)}{\left(\mathsf{E}_2^{(N)}(\tau)\right)^2}\right)} = \frac{\mathsf{E}_4(-1/N\tau)}{\left(\mathsf{E}_2^{(N)}(-1/N\tau)\right)^2}, \tag{9}$$

$$\overline{A_6} = \overline{\left(\frac{\mathsf{E}_6(\tau)}{\left(\mathsf{E}_2^{(N)}(\tau)\right)^3}\right)} = \frac{\mathsf{E}_6(-1/N\tau)}{\left(\mathsf{E}_2^{(N)}(-1/N\tau)\right)^3}, \tag{10}$$

since $\frac{\mathsf{E}_4(\tau)}{\mathsf{E}_2^{(N)}(\tau)^2}$ and $\frac{\mathsf{E}_6(\tau)}{\mathsf{E}_2^{(N)}(\tau)^3}$ are given by some rational expression in terms of the coordinate h.

The Eisenstein series E_4 and E_6 satisfy

$$\mathsf{E}_4(-1/N\tau) = (N\tau)^4\mathsf{E}_4(N\tau),$$
$$\mathsf{E}_6(-1/N\tau) = (N\tau)^6\mathsf{E}_6(N\tau),$$

and by Proposition 2.3.12, the modular form $\mathsf{E}_2^{(N)}$ is anti-invariant under the Fricke involution, so that

$$\mathsf{E}_2^{(N)}(-1/N\tau) = -N\tau^2\mathsf{E}_2^{(N)}(\tau).$$

Combining these functional equations gives

$$\frac{\mathsf{E}_4(-1/N\tau)}{\left(\mathsf{E}_2^{(N)}(-1/N\tau)\right)^2} = N^2\frac{\mathsf{E}_4(N\tau)}{\left(\mathsf{E}_2^{(N)}(\tau)\right)^2} = N^2A_4',$$
$$\frac{\mathsf{E}_6(-1/N\tau)}{\left(\mathsf{E}_2^{(N)}(-1/N\tau)\right)^3} = -N^3\frac{\mathsf{E}_6(N\tau)}{\left(\mathsf{E}_2^{(N)}(\tau)\right)^3} = -N^3A_6',$$

so that substituting equations (9) and (10) yields

$$\overline{A_4} = (\alpha/\overline{\alpha})^2N^2A_4', \qquad \overline{A_6} = -(\alpha/\overline{\alpha})^3N^3A_6'. \tag{11}$$

The only isomorphisms that preserve Weierstrass equations of the form $y^2 = x^3 + a_4x + a_6$ come from changes of variables of the form

$$(x, y) \mapsto (u^2x, u^3y).$$

We need such a change of variables from

$$E' : y^2 = x^3 + a_4'x + a_6'$$

to

$$\overline{E} : y^2 = x^3 + \overline{a}_4x + \overline{a}_6,$$

which necessitates

$$u^4\overline{a_4} = a_4',$$
$$u^6\overline{a_6} = a_6',$$

or equivalently

$$u^4\overline{A_4} = A_4',$$
$$u^6\overline{A_6} = A_6'.$$

The relations (11) show that these conditions are equivalent to

$$u^2 = -(\alpha/\overline{\alpha})N.$$

We need $u^3 \in L^\times$ in order for the change of variables to occur over L. Therefore the isomorphism occurs over L if and only if $-(\alpha/\overline{\alpha})N$ is a square in $L^\times$. Multiplying by the square $\overline{\alpha}^2/N^2$ gives the equivalent condition

$$\alpha\overline{\alpha} \in -N \cdot (L^\times)^2, \tag{12}$$

yielding conclusion (b).

To reach conclusion (a) from (b), we must determine when (12) has a solution over $L^\times$, which is equivalent to asking whether $-N$ is the product of a norm and a square. We state and prove the desired equivalent condition as a separate lemma:

Lemma 4.3.4. *Let L/K be a quadratic extension of characteristic not equal to 2, and let $\mathbf{N}$ denote the image of the norm map $L^\times \to K^\times$. Then an element $N \in K$ lies in $\mathbf{N} \cdot (L^\times)^2$ if and only if either $\pm N$ lies in $\mathbf{N}$.*

Proof. We may write $L = K(\sqrt{D})$ for some $D \in K$, so -1 always lies in $\mathbf{N} \cdot (L^\times)^2$ as the product of the norm $-D$ of $\sqrt{D}$ and the square D^{-1}. Therefore, if either N or $-N$ is a norm, then $N \in \mathbf{N} \cdot (L^\times)^2$.

Conversely, suppose that N lies in $\mathbf{N} \cdot (L^\times)^2$, so that we may write

$$N = \gamma^2(a^2 - b^2 D)$$

for some $\gamma \in L^\times$ and $a, b \in K$. Over characteristic not equal to 2, if $c, d \in K$ then an element of the form $(c + d\sqrt{D})^2$ lies in K if and only $c = 0$ or $d = 0$. Since N lies in K, we conclude that γ must either lie in K or in $\sqrt{D} \cdot K$.

If $\gamma \in K$, then we may absorb the factor of γ into a and b to conclude that N lies in the image of the norm. Else $\gamma = d\sqrt{D}$ for some $d \in K$, so that

$$-N = (bD)^2 - (ad)^2 D$$

and thus $-N$ lies in the image of the norm map. ∎

Since $-N$ is an integer and therefore lies in the base field K, conclusion (a) follows from (b) by the lemma. ∎

If we write $L = K(\sqrt{D})$, then part (a) states that the existence of a strict K curve defined over L corresponding to a K-rational point on $X_0^+(N)$ is equivalent to a solution to the pair of conics

$$x^2 - Dy^2 = \pm N$$

over K.

We conclude by illustrating the construction from part (b) of the theorem more explicitly in the case $N = 2$. Let $L = K(\sqrt{D})$. The values of $h = a + b\sqrt{D}$ satisfying the hypothesis of the theorem are those such that $\overline{h} = w_2^* h = 4096/h$, so that these values of h are given precisely by the solutions to the conic

$$a^2 - Db^2 = 4096$$

with $a, b \in K$. We may parameterize this conic over $t \in K$ as

$$a = 64 \cdot \frac{1 + Dt^2}{1 - Dt^2},$$
$$b = 128 \cdot \frac{t}{1 - Dt^2},$$

and thus

$$h = 64 \cdot \frac{(t\sqrt{D} + 1)^2}{1 - Dt^2}.$$

Substitute this parameterization of h into the formulas in Table 4 to find the coefficients of E, E':

$$E : y^2 = x^3 - \alpha^2 \frac{(5 - 3t\sqrt{D})}{96} x + \alpha^3 \frac{(-7 + 9t\sqrt{D})}{1728},$$
$$E' : y^2 = x^3 - \alpha^2 \frac{(5 + 3t\sqrt{D})}{384} x + \alpha^3 \frac{(7 + 9t\sqrt{D})}{13824}.$$

Therefore, as t ranges over K and $\alpha \in L$ ranges over all solutions to $\alpha\overline{\alpha} \in -2 \cdot (L^\times)^2$, the two models above range over all twists of strict K-curves defined over L corresponding to a K-rational fiber of $X_0^+(N)$. A

similar construction may be given for other N with $X_0(N)$ of genus 0 as long as a rational parameterization of the conic

$$a^2 - b^2 D = \kappa_N$$

is known, where $\kappa_N = h_N \cdot w_N^* h_N$. This is easier to do when κ_N is a rational square, which only happens for $N = 2, 3, 4$, and 7 (see Table 1).

A natural way to extend Theorem 4.3.3 would be to prove a version for fibers of K-rational points on $X^*(N)$ rather than $X_0^+(N)$, working over multi-quadratic extensions L/K rather than quadratic extensions. Then the result would account for *all* non-CM K-curves by Elkies' Theorem 4.2.4. One way to approach this problem would be to find suitable models for E corresponding to $h \in Y_0(N)$ that transform nicely under the Atkin-Lehner involutions, since doing this for the Fricke involution was the key step in the proof of Theorem 4.3.3.

A Special values of the j-invariant at CM points

N	$-1/\tau = i\sqrt{N}$	$h_N(\tau) = +\sqrt{\kappa_N}$	$j(\tau) = j(-1/\tau)$
2	$i\sqrt{2}$	64	8000
3	$i\sqrt{3}$	81	54000
4	$2i$	16	287496
5	$i\sqrt{5}$	$5\sqrt{5}$	$632000 + 282880\sqrt{5}$
6	$i\sqrt{6}$	$6\sqrt{2}$	$2417472 + 1707264\sqrt{2}$
7	$i\sqrt{7}$	7	16581375
8	$2i\sqrt{2}$	$4\sqrt{2}$	$26125000 + 18473000\sqrt{2}$
9	$3i$	$3\sqrt{3}$	$76771008 + 44330496\sqrt{3}$
10	$i\sqrt{10}$	$2\sqrt{5}$	$212846400 + 95178240\sqrt{5}$
12	$2i\sqrt{3}$	$2\sqrt{3}$	$1417905000 + 818626500\sqrt{3}$
13	$i\sqrt{13}$	$\sqrt{13}$	$3448440000 + 956448000\sqrt{13}$
16	$4i$	$2\sqrt{2}$	$41113158120 + 29071392966\sqrt{2}$
18	$3i\sqrt{2}$	$\sqrt{6}$	$188837384000 + 77092288000\sqrt{6}$
25	$5i$	$\sqrt{5}$	$22015749611520 + 9845745509376\sqrt{5}$

Table 3: Special values of the j-invariant at CM points given by fixed points of the Fricke involution.

B Tables of coefficients of cyclic N-isogenies in terms of Hauptmoduln

These tables express the coefficients of an elliptic curve E and its isogenous curve E' corresponding to a point in $Y_0(N)$ given in terms of the Hauptmodul h_N (see Table 1):

$$E : y^2 = x^3 - \frac{A_4}{48} + \frac{A_6}{864},$$
$$E : y^2 = x^3 - \frac{A'_4}{48} + \frac{A'_6}{864},$$

where

$$A_4 := \mathsf{E}_4(\tau)/\mathsf{E}_2(\tau)^2, \qquad A_6 := \mathsf{E}_6(\tau)/\mathsf{E}_2(\tau)^3,$$
$$A'_4 := \mathsf{E}_4(N\tau)/\mathsf{E}_2(\tau)^2, \qquad A'_6 := \mathsf{E}_6(N\tau)/\mathsf{E}_2(\tau)^3.$$

We omit the factors of $-1/48$ and $1/864$ in the tables. Additionally, the denominators of A_4, A_6, A'_4, A'_6 often involve common factors that can be twisted away. When this applies, we label these factors as D and instead give expressions for $D^2A_4, D^3A_6, D^2A'_4, D^3A'_6$ in order to save space.

N	A_4	A_6	A'_4	A'_6
2	$\frac{h+256}{h+64}$	$\frac{h-512}{h+64}$	$\frac{h+16}{h+64}$	$\frac{h-8}{h+64}$
3	$\frac{h+243}{h+27}$	$\frac{h^2-486h-19683}{(h+27)^2}$	$\frac{h+3}{h+27}$	$\frac{h^2+18h-27}{(h+27)^2}$
4	$\frac{h^2+256h+4096}{(h+16)^2}$	$\frac{(h+32)(h^2-512h-8192)}{(h+16)^3}$	$\frac{h^2+16h+16}{(h+16)^2}$	$\frac{(h+8)(h^2+16h-8)}{(h+16)^3}$
5	$\frac{h^2+250h+3125}{h^2+22h+125}$	$\frac{h^2-500h-15625}{h^2+22h+125}$	$\frac{h^2+10h+5}{h^2+22h+125}$	$\frac{h^2+4h-1}{h^2+22h+125}$

Table 4: Coefficients of E, E' corresponding to $h = h_N$ for $N = 2, 3, 4, 5$.

N = 6

D^2A_4	$25 \cdot (h+12)(h^3+252h^2+3888h+15552)$
D^3A_6	$125 \cdot (h^2+36h+216)(h^4-504h^3-13824h^2-124416h-373248)$
D^2A_4'	$25 \cdot (h+6)(h^3+18h^2+84h+24)$
D^3A_6'	$125 \cdot (h^2+12h+24)(h^4+24h^3+192h^2+504h-72)$
D	$5h^2+84h+360$

Table 5: Coefficients of E, E' corresponding to $h = h_6$.

N = 7

A_4	$\frac{h^2+245h+2401}{h^2+13h+49}$
A_6	$\frac{h^4-490h^3-21609h^2-235298h-823543}{(h^2+13h+49)^2}$
A_4'	$\frac{h^2+5h+1}{h^2+13h+49}$
A_6'	$\frac{h^4+14h^3+63h^2+70h-7}{(h^2+13h+49)^2}$

Table 6: Coefficients of E, E' corresponding to $h = h_7$.

N = 8

D^2A_4	$49 \cdot (h^4+256h^3+5120h^2+32768h+65536)$
D^3A_6	$343 \cdot (h^2+32h+128)(h^4-512h^3-10240h^2-65536h-131072)$
D^2A_4'	$49 \cdot (h^4+16h^3+80h^2+128h+16)$
D^3A_6'	$343 \cdot (h^2+8h+8)(h^4+16h^3+80h+128h-8)$
D	$7h^2+80h+224$

Table 7: Coefficients of E, E' corresponding to $h = h_8$.

N = 9

D^2A_4	$(h+1)(h^3+243h^2+2187h+6561)$
D^3A_6	$h^6-486h^5-24057h^4-367416h^3-2657205h^2-9565938h-14348907$
D^2A_4'	$(h+27)(h^3+9h^2+27h+3)$
D^3A_6'	$h^6+18h^5+135h^4+504h^3+891h^2+486h-27$
D	$h^2+9h+27$

Table 8: Coefficients of E, E' corresponding to $h = h_9$.

N = 10

D^2A_4	$9 \cdot \frac{h^6+260h^5+6400h^4+64000h^3+320000h^2+800000h+800000}{h^2+8h+20}$
D^3A_6	$27 \cdot \frac{(h^2+12h+40)(h^2+30h+100)(h^4-520h^3-6600h^2-28000h-40000)}{h^2+8h+20}$
D^2A_4'	$9 \cdot \frac{h^6+20h^5+160h^4+640h^3+1280h^2+1040h+80}{h^2+8h+20}$
D^3A_6'	$27 \cdot \frac{\left(h^2+6h+4\right)\left(h^2+6h+10\right)\left(h^4+14h^3+66h^2+104h-4\right)}{h^2+8h+20}$
D	$3h^2+26h+60$

Table 9: Coefficients of E, E' corresponding to $h = h_{10}$.

N = 12

D^2A_4	$121 \cdot (h^2+12h+24)(h^6+252h^5+4392h^4+31104h^3+108864h^2+186624h+124416)$
D^3A_6	$1331 \cdot (h^4+36h^3+288h^2+864h+864)$ $\cdot (h^8-504h^7-14832h^6-179712h^5-1175040h^4-4478976h^3-9953280h^2-11943936h-5971968)$
D^2A_4'	$121 \cdot \left(h^2+6h+6\right)\left(h^6+18h^5+126h^4+432h^3+732h^2+504h+24\right)$
D^3A_6'	$1331 \cdot \left(h^4+12h^3+48h^2+72h+24\right)\left(h^8+24h^7+240h^6+1296h^5+4080h^4+7488h^3+7416h^2+3024h-72\right)$
D	$11h^4+156h^3+816h^2+1872h+1584$

Table 10: Coefficients of E, E' corresponding to $h = h_{12}$.

N = 13

A_4	$\frac{h^4+247h^3+3380h^2+15379h+28561}{(h^2+5h+13)(h^2+6h+13)}$
A_6	$\frac{h^6-494h^5-20618h^4-237276h^3-1313806h^2-3712930h-4826809}{(h^2+5h+13)^2(h^2+6h+13)}$
A_4'	$\frac{h^4+7h^3+20h^2+19h+1}{(h^2+5h+13)(h^2+6h+13)}$
A_6'	$\frac{h^6+10h^5+46h^4+108h^3+122h^2+38h-1}{(h^2+5h+13)^2(h^2+6h+13)}$

Table 11: Coefficients of E, E' corresponding to $h = h_{13}$.

N = 16

D^2A_4	$25 \cdot (h^8 + 256h^7 + 5632h^6 + 53248h^5 + 282624h^4 + 917504h^3 + 1835008h^2 + 2097152h + 1048576)$
D^3A_6	$125 \cdot (h^4 + 32h^3 + 192h^2 + 512h + 512)$ $\cdot (h^8 - 512h^7 - 11264h^6 - 106496h^5 - 565248h^4 - 1835008h^3 - 3670016h^2 - 4194304h - 2097152)$
D^2A_4'	$25 \cdot \left(h^8 + 16h^7 + 112h^6 + 448h^5 + 1104h^4 + 1664h^3 + 1408h^2 + 512h + 16\right)$
D^3A_6'	$125 \cdot \left(h^4 + 8h^3 + 24h^2 + 32h + 8\right)\left(h^8 + 16h^7 + 112h^6 + 448h^5 + 1104h^4 + 1664h^3 + 1408h^2 + 512h - 8\right)$
D	$\left(h^2 + 4h + 8\right)\left(5h^2 + 28h + 40\right)$

Table 12: Coefficients of E, E' corresponding to $h = h_{16}$.

N = 18

D^2A_4	$289 \cdot (h^3 + 12h^2 + 36h + 36)$ $\cdot (h^9 + 252h^8 + 4644h^7 + 39636h^6 + 198288h^5 + 629856h^4 + 1294704h^3 + 1679616h^2 + 1259712h + 419904)$
D^3A_6	$4913 \cdot (h^6 + 36h^5 + 324h^4 + 1404h^3 + 3240h^2 + 3888h + 1944)$ $\cdot (h^{12} - 504h^{11} - 15336h^{10} - 208872h^9 - 1700352h^8 - 9206784h^7 - 34836480h^6$ $- 94058496h^5 + 181398528h^4 - 245223936h^3 + 221709312h^2 - 120932352h - 30233088)$
D^2A_4'	$289 \cdot \left(h^3 + 6h^2 + 12h + 6\right)\left(h^9 + 18h^8 + 144h^7 + 666h^6 + 1944h^5 + 3672h^4 + 4404h^3 + 3096h^2 + 1008h + 24\right)$
D^3A_6'	$4913 \cdot \left(h^6 + 12h^5 + 60h^4 + 156h^3 + 216h^2 + 144h + 24\right)$ $\cdot (h^{12} + 24h^{11} + 264h^{10} + 1752h^9 + 7776h^8 + 24192h^7 + 53760h^6$ $+ 85248h^5 + 94464h^4 + 69624h^3 + 30672h^2 + 6048h - 72)$
D	$17h^6 + 228h^5 + 1332h^4 + 4284h^3 + 7992h^2 + 8208h + 3672$

Table 13: Coefficients of E, E' corresponding to $h = h_{18}$.

N = 25

D^2A_4	$(h^{10}+250h^9+4375h^8+35000h^7+178125h^6+631250h^5+1640625h^4$ $+3125000h^3+4296875h^2+3906250h+1953125)/(h^2+2h+5)$
D^3A_6	$(h^4+10h^3+45h^2+100h+125)$ $\cdot(h^{10}-500h^9-18125h^8-163750h^7-871875h^6-3137500h^5-8203125h^4$ $-15625000h^3-21484375h^2-19531250h-9765625)/(h^2+2h+5)$
D^2A_4'	$(h^{10}+10h^9+55h^8+200h^7+525h^6+1010h^5+1425h^4+1400h^3+875h^2+250h+5)/(h^2+2h+5)$
D^3A_6'	$\left(h_{25}^4+4h^3+9h^2+10h+5\right)$ $\cdot\left(h^{10}+10h^9+55h^8+200h^7+525h^6+1004h^5+1395h^4+1310h^3+725h^2+100h-1\right)/(h^2+2h+5)$
D	$h^4+5h^3+15h^2+25h+25$

Table 14: Coefficients of E, E' corresponding to $h = h_{25}$.

References

[BG85] Joe P. Buhler and Benedict H. Gross. "Arithmetic on elliptic curves with complex multiplication. II". In: *Invent. Math.* 79.1 (1985), pp. 11–29. ISSN: 0020-9910. DOI: 10.1007/BF01388654.

[CP09] Henri Cohen and Fabien Pazuki. "Elementary 3-descent with a 3-isogeny". In: *Acta Arith.* 140.4 (2009), pp. 369–404. ISSN: 0065-1036. DOI: 10.4064/aa140-4-6.

[DS05] Fred Diamond and Jerry Shurman. *A First Course in Modular Forms*. Vol. 228. Graduate Texts in Mathematics. Springer-Verlag, New York, 2005, pp. xvi+436. ISBN: 0-387-23229-X.

[Elk04] Noam D. Elkies. "On elliptic K-curves". In: *Modular Curves and Abelian Varieties*. Vol. 224. Progr. Math. Birkhäuser, Basel, 2004, pp. 81–91.

[Elk98] Noam D. Elkies. "Elliptic and modular curves over finite fields and related computational issues". In: *Computational Perspectives on Number Theory (Chicago, IL, 1995)*. Vol. 7. AMS/IP Stud. Adv. Math. Amer. Math. Soc., Providence, RI, 1998, pp. 21–76. DOI: 10.1090/amsip/007/03.

[Ell04] Jordan S. Ellenberg. "$\mathbb{Q}$-curves and Galois representations". In: *Modular curves and abelian varieties*. Vol. 224. Progr. Math. Birkhäuser, Basel, 2004, pp. 93–103.

[Lig74] G. Ligozat. *Courbes modulaires de genre* 1. Publication Mathématique d'Orsay, No. 75 7411. U.E.R. Mathématique, Université Paris XI, Orsay, 1974, p. 102.

[LMFDB] The LMFDB Collaboration. *The L-functions and Modular Forms Database*. [Online; accessed 20 March 2021]. 2021. URL: https://www.lmfdb.org/knowledge/show/cmf.atkin-lehner.

[Mai09] Robert S. Maier. "On rationally parametrized modular equations". In: *J. Ramanujan Math. Soc.* 24.1 (2009), pp. 1–73. ISSN: 0970-1249.

[Sil09] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. 2nd edition. Vol. 106. Graduate Texts in Mathematics. Springer, Dordrecht, 2009, pp. xx+513. ISBN: 978-0-387-09493-9. DOI: 10.1007/978-0-387-09494-6.

[Ste99] Serguei A. Stepanov. *Codes on algebraic curves*. Kluwer Academic/Plenum Publishers, New York, 1999, pp. xiv+350. ISBN: 0-306-46144-7. DOI: 10.1007/978-1-4615-4785-3.