2020-06-11

Divisors of Modular Parameterizations of Elliptic Curves

Jonathan Reid Hales
Brigham Young University

Divisors of Modular Parameterizations of Elliptic Curves

Jonathan Reid Hales

A thesis submitted to the faculty of
Brigham Young University
in partial fulfillment of the requirements for the degree of

Master of Science

Michael Griffin, Chair
Paul Jenkins
Pace Nielsen

Department of Mathematics

Brigham Young University

ABSTRACT

Divisors of Modular Parameterizations of Elliptic Curves

Jonathan Reid Hales
Department of Mathematics, BYU
Master of Science

The modularity theorem implies that for every elliptic curve $E/\mathbb{Q}$ there exist rational maps from the modular curve $X_0(N)$ to E, where N is the conductor of E. These maps may be expressed in terms of pairs of modular functions $X(z)$ and $Y(z)$ that satisfy the Weierstrass equation for E as well as a certain differential equation. Using these two relations, a recursive algorithm can be constructed to calculate the q - expansions of these parameterizations at any cusp. These functions are algebraic over $\mathbb{Q}(j(z))$ and satisfy modular polynomials where each of the coefficient functions are rational functions in $j(z)$. Using these functions, we determine the divisor of the parameterization and the preimage of rational points on E. We give a sufficient condition for when these preimages correspond to CM points on $X_0(N)$. We also examine a connection between the algebras generated by these functions for related elliptic curves, and describe sufficient conditions to determine congruences in the q-expansions of these objects.

Keywords: number theory, elliptic curves, modular forms, complex-multiplication

Contents

List of Tables

List of Figures

Chapter 1. Motivation and Introduction

1.1 Introduction

The modularity theorem [3, 13] guarantees for every elliptic curve E of conductor N the existence of an element f_E of $S_2(\Gamma_0(N), \mathbb{Z})$, the space of modular forms of weight k, level N and Fourier coefficients in the ring $\mathbb{Z}$ (see section 1.3). The Eichler integral of f_E together with the Weierstrass $\wp$-function give a rational map from the modular curve $X_0(N)$ to E that parameterizes the coordinates of an integral model for the curve E for each element of the endomorphism group of E (see section 2.1). Kodgis [7] showed computationally that many of the zeros of modular parameterizations occur at CM points on $X_0(N)$. Peluse [9] later proved several general cases confirming many of these conjectured zeros using the theory of Hecke operators and Atkin–Lehner involutions.

In [2], the authors use the modular parametrization of an elliptic curve to give a harmonic Maass form of weight 3/2 whose Fourier coefficients encode the vanishing of central L-values and L-derivatives of quadratic twists of the curve. The Birch and Swinerton-Dyer conjecture asserts that the order of vanishing of the central L-value of an elliptic curve is the rank of the curve. Kolyvagin [8] confirmed this conjecture if the order of vanishing is less than 2. Unfortunately, the result of [2] is only fully constructive if the modular parametrization is holomorphic on the upper half plane. Otherwise we must remove the singularities, a task which is difficult without knowledge of their locations.

For a modular form $F \in M_k(\Gamma, \mathcal{O})$, where $\mathcal{O}$ is the ring of integers in some number field, we consider the modular polynomial of F

$$\Phi_F(x) := \prod_{\gamma \in \Gamma \backslash SL_2(\mathbb{Z})} \Big(x - F(\gamma z) \Big) = \sum A_i(z) x^i \tag{1.1}$$

where γz denotes $\frac{az+b}{cz+d}$ and $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ (see section 1.3). One of our goals is to calculate

the minimal divisor of (1.1) for rational functions in a given modular parameterization $(X(z), Y(z))$ of E. The zeros of this divisor are the poles of Φ_F, and in many cases they occur at CM points of $X_0(N)$. One way to calculate the divisor is to examine the coefficient functions $A_i(z)$ determined by symmetric polynomials in the factors $(x - F(\gamma z))$ and calculate their divisors until we have located all of the poles. In order to calculate the product in (1.1) we need the expansion of F at each of the cusps of Γ. Algorithms for calculating the coefficients at the cusp infinity are described by Cremona [4], and we include a variation of that method that allows for the computation of coefficients at any cusp, making the construction of the A_i's possible. Explicit code written for these computations is given in appendix A.

Example 1.1.1. For the elliptic curve

$$E : y^2 + y = x^3 - x^2 - 10x - 20 \tag{11a1}$$

one can calculate that E has $(5, 5)$ and $(5, -6)$ as points of order 5. If we set $F(z) = (X(z) - 5)^{-1}$, then $F(z)$ has zeros only when z is an element of the complex lattice associated to E, and poles only when z is mapped to one of these 5-torsion points. Computing the divisor of $\Phi_F(X)$, we find that

$$X(z) = 5 \quad \Longrightarrow \quad (j(z) + 24729001)(j(z) + 32768) = 0.$$

For $z = \frac{1+\sqrt{-11}}{2}$, $j(z) = -32768$. Since $j(z)$ is invariant under the action of $\mathrm{SL}_2(\mathbb{Z})$ while F is only $\Gamma_0(11)$ invariant, we look at the $\Gamma_0(11)\backslash \mathrm{SL}_2(\mathbb{Z})$ orbit of z to find

$$z_0 = \frac{-11 + \sqrt{-11}}{55} \quad \Longrightarrow \quad \big(X(z_0), Y(z_0)\big) = (5, 5).$$

Thus the point z_0 is a preimage of the rational point $(5, 5)$, and is a CM point on $X_0(11)$.

We give a sufficient condition for when a point $\mathcal{P}$ lying above a rational point P on E is a CM point. The proof is given in chapter 2.

Theorem 1.1.2. *Fix an elliptic curve $E/\mathbb{Q}$ of conductor N. Let P be a point on E and $\mathcal{P}$ a point on $X_0(N)$ that maps to P under some modular parameterization. The point $\mathcal{P}$ can be identified as the pair (e_1, c_1) where e_1 is an elliptic curve over a number field K and c_1 a cyclic subgroup of order N. For each m exactly dividing N, the Atkin-Lehner involution W_m imposes an m-isogeny defined over K or else e_1 has CM by an order of discriminant D with $0 \leq -D \leq 4m$ and D a square mod $4m$.*

In chapter 3 we consider the following question. Given an elliptic curve E, when are the coefficients of these parametrizations contained in some prime ideal $\mathfrak{p}$ of a number ring $\mathcal{O}$? Similarly, when are the Fourier expansions of two modular parameterizations for curves E_1 and E_2 congruent mod $\mathfrak{P}$? One sufficient condition we give is that the elliptic curves are isogenous and have congruent coefficients mod p for some prime p lying below $\mathfrak{p}$. Another sufficient condition we provide is a bound similar to Sturm's bound that implies that every coefficient of the parameterizations is in $\mathfrak{p}$ if the order of vanishing mod $\mathfrak{P}$ is large enough.

1.2 The Weierstrass $\wp$ Function

For any elliptic curve E with model $y^2 = 4x^3 - g_2x - g_3$ over $\mathbb{C}$, there are two $\mathbb{R}$-linear independent complex constants ω_1, ω_2 (calculated from certain definite integrals) known as the *periods* of E. We denote the period lattice that ω_1 and ω_2 generate by Λ_E. The Weierstrass $\wp$ function is defined in terms of Λ_E and a complex variable z as follows:

$$\wp(z, \Lambda_E) := \frac{1}{z^2} + \sum_{\substack{\lambda \in \Lambda_E \\ \lambda \neq 0}} \left(\frac{1}{(z+\lambda)^2} - \frac{1}{\lambda^2} \right).$$

Proposition 1.1. *$\wp(z, \Lambda_E)$ coverges absolutely and uniformly for z in any compact subset of $\mathbb{C} - \Lambda_E$.*

Proof. The proof follows from the following lemma.

Lemma 1.2. *The series $\sum_{\ell \in L} |\ell|^{-s}$ coverges absolutely in any lattice $L \subseteq \mathbb{C}$ if $s > 2$.*

Proof. This holds because the number of lattice points $\ell \in L$ satisfying $n-1 \leq |\ell| \leq n$ is at most a constant multiple of n (this constant depends on L but not n). Thus $\sum_{\ell \in L} |\ell|^{-s}$ is bounded above by $\sum_{n=1}^{\infty} n \cdot n^{-s}$ which converges for $s > 2$. □

The proposition now follows because for all $z \in \mathbb{C} - \Lambda_E$ and for $\lambda \in \Lambda_E$

$$\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} = \frac{2z - z^2/\lambda}{(z-\lambda)^2 \lambda}$$

which we can compare to a constant multiple of $|\lambda|^{-3}$ via the limit comparison test. □

Absolute convergence gives immediately that the function $\wp(z, \Lambda_E)$ is doubly periodic with periods ω_1 and ω_2. This also implies that $\wp(z, \Lambda_E)$ is an even function since

$$\wp(-z, \Lambda_E) = \sum_{\substack{\lambda \in \Lambda_E \\ \lambda \neq 0}} \left(\frac{1}{(-z+\lambda)^2} - \frac{1}{\lambda^2} \right) = \sum_{\substack{\lambda \in \Lambda_E \\ \lambda \neq 0}} \left(\frac{1}{(z-\lambda)^2} - \frac{1}{(-\lambda)^2} \right) = \wp(z, \Lambda_E).$$

Proposition 1.3. *Any even, meromorphic, doubly periodic function with periods ω_1 and ω_2 is a rational polynomial in $\wp(z, \Lambda)$ where Λ is the lattice generated by ω_1 and ω_2.*

Proof. See a very direct proof in chapter 1 section 5 of [6]. □

Since $\wp(z, \Lambda_E)$ is even, meromorphic, and doubly periodic, so is $(\wp'(z, \Lambda_E))^2$. Thus by the above proposition it can be written as a rational polynomial in $\wp(z, \Lambda_E)$. Comparing the coefficients of powers of z in the Laurent series expansion of $(\wp'(z, \Lambda_E))^2$ gives the equation

$$\wp'(z, \Lambda_E)^2 = 4\wp(z, \Lambda_E)^3 - g_2 \wp(z, \Lambda_E) - g_3, \tag{1.2}$$

where

$$g_2 = g_2(\Lambda_E) = 60 \sum_{\substack{\lambda \in \Lambda_E \\ \lambda \neq 0}} (\lambda)^{-4}$$

and

$$g_3 = g_3(\Lambda_3) = 140 \sum_{\substack{\lambda \in \Lambda_E \\ \lambda \neq 0}} (\lambda)^{-6}.$$

Thus the map $z \to (\wp(z, \Lambda_E), \wp'(z, \Lambda_E))$ gives an isomorphism from a fundamental parallelogram of Λ_E to E.

1.3 Introduction to Modular Forms:

Let $\mathrm{SL}_2(\mathbb{Z})$ denote the group of integer matrices with determinant 1. Then $\mathrm{SL}_2(\mathbb{Z})$ acts on the upper-half plane $\mathcal{H} := \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$ by $\gamma z = \frac{az+b}{cz+d}$ where $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Of particular interest to us is the congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ denoted by

$$\Gamma_0(N) := \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 \mod N\}.$$

Note that $\Gamma_0(1)$ is simply $\mathrm{SL}_2(\mathbb{Z})$. The action of $\Gamma_0(N)$ on $\mathbb{Q} \cup \{\infty\}$ gives an equivalence relation where $p \sim q$ if there exists some $\gamma \in \Gamma_0(N)$ such that $\gamma p = q$. We also define $\gamma\infty = a/c$. The equivalence classes are called the *cusps* of $\Gamma_0(N)$. By the *modular curve of level* N we mean $\mathcal{H} \cup \mathbb{Q} \cup \{\infty\}$ modulo the action of the elements of $\Gamma_0(N)$. We denote the modular curve by $X_0(N)$.

An analytic function $f : \mathcal{H} \to \mathcal{H}$ is a *modular form* of weight k for $\mathrm{SL}_2(\mathbb{Z})$ if $f(\gamma z) = (cz + d)^k f(z)$ for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ and f is analytic at infinity.

A natural operation to consider on these objects is the *weight k slash operator*, $f(z)|_k\gamma$

on a complex function defined to be

$$f(z)|_k\gamma := (cz+d)^{-k} f(\gamma z).$$

Thus a modular form of weight k is an analytic function that is invariant under the weight k slash operator. Since this operator is linear, modular forms of a given weight form a complex vector space. Given the congruence subgroup $\Gamma_0(N)$, a *modular form of weight k and level N* is a function f that is analytic on $\mathcal{H}$ such that $f|_k\gamma$ is analytic for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ and $f|_k\gamma_k = f$ for all $\gamma \in \Gamma_0(N)$. We denote the complex vector space of modular forms of weight k, and level N and by $M_k(\Gamma_0(N))$. We also denote the subset of $M_k(\Gamma_0(N))$ of modular forms whose Fourier coefficients are in a subring $\mathcal{O}$ of $\mathbb{C}$ by $M_k(\Gamma_0(N), \mathcal{O})$. If $\rho = a/c$ is a cusp of $\Gamma_0(N)$, and g_ρ is a matrix in $\mathrm{SL}_2(\mathbb{Z})$ such that $g_\rho(\infty) = \rho$, we say that the Fourier expansion of $f(g_\rho z)$ is the *expansion of f at the cusp ρ*. In general it is quite difficult to calculate the Fourier expansion of a modular form f at ρ even if the expansion at ∞ is known.

The first examples of modular forms typically given are the *weight k Eisenstein series* given by

$$G_k(z) = \sum_{\substack{m,n\in\mathbb{Z} \\ (m,n)\neq(0,0)}} \frac{1}{(mz+n)^k}$$

for $k \geq 3$. It is a routine check (following from Lemma 1.2) that $G_k(\gamma z) = (cz+d)^k G_k(z)$ for all $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$.

Modular forms often encode very interesting number theoretic properties in their Fourier coefficients.

Example 1.3.1. If we let q denote $e^{2\pi i z}$, then the above functions $G_k(z)$ satisfy

$$G_k(z) = 2\zeta(k) + 2\frac{(2\pi i)^k}{(k-1)!}\sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n$$

where $\zeta(k)$ is the Riemann ζ-function and $\sigma_k(n)$ is the typical $\sum_{d|n} d^k$. We define $E_k(z) = G_k(z)/2\zeta(k) = 1 - 2k/B_k \sum \sigma_{k-1}(n)q^n$ where B_k is the k^{th} Bernoulli number.

A modular form for $\Gamma_0(N)$ that vanishes at the cusps is called a *cusp form*. We denote the subspace of $M_k(\Gamma_0(N))$ of cusp forms by $S_k(\Gamma_0(N))$, and the subset of forms with Fourier coefficiets in $\mathcal{O}$ by $S_k(\Gamma_0(N), \mathcal{O})$. The first and most important example of a cusp form is

$$\Delta = \frac{E_4^3 - E_6^2}{1728} = q - 24q^2 + 252q^3 - 1472q^4 + 4830q^5 - 6048q^6 + \cdots .$$

The fact that Δ is a cusp form is immediate since the only cusp for $\Gamma_0(1)$ is at ∞ and Δ vanishes at that cusp because its Fourier expansion has no constant term.

1.4 Modular Functions

A consequence of Liouville's theorem is that any modular form of weight zero must be a constant. Thus, in order to say something interesting about the weight zero case we must weaken one of our hypotheses.

We define a *modular function* to be a meromorphic function on $\mathcal{H}$ that is invariant under the weight 0 slash operator for all $\gamma \in \Gamma_0(N)$.

Example 1.4.1. Consider $j(z)$, the Klein j-function, given by

$$j(z) := \frac{E_4^3}{\Delta} = q^{-1} + 744 + 196884q + 21493760q^2 + 864299970q^3 + 20245856256q^4 + \cdots$$

$j(z)$ has weight 0 since both Δ and E_4^3 have weight 12. Notice that since $j(z)$ is not a constant, we must have that $j(z)$ has a pole, which is evident by its Fourier expansion that starts with a q^{-1} term.

Clearly any rational polynomial in $j(z)$ will also be a modular function for all of $\mathrm{SL}_2(\mathbb{Z})$. The following proposition shows that these are all of the level 1 modular functions.

Proposition 1.4. *If f is a modular function for $\mathrm{SL}_2(\mathbb{Z})$, then there exist polynomials $P(x), Q(x) \in \mathbb{C}[x]$ so that $f(z) = P(j(z))/Q(j(z))$.*

Proof. First suppose that f is analytic everywhere in $\mathcal{H}$. In this case f is a polynomial in $j(z)$ of degree equal to the order of the pole of f at infinity. We prove this by induction on the order of this pole. If f has no pole at infinity, we have already seen that Liouville's theorem shows that f is constant, and thus a polynomial in $j(z)$.

If f has a pole of order n at infinity, with Fourier coefficient α of q^{-n}, then $f - \alpha j(z)^n$ has a pole of order $n-1$ at infinity and so by our inductive hypothesis is a polynomial of degree $n-1$ in $j(z)$.

If f has poles in $X_0(1)$, then since $X_0(1)$ is compact, there are only a finite number of such poles. Since $j(z)$ is a surjective map from $X_0(1)$ to $\mathbb{C} \cup \{\infty\}$ (the image of $j(z)$ is open because of analyticity and closed because $X_0(1)$ is compact and hence must be all of $\mathbb{C} \cup \infty$) we can pick complex numbers $\tau_1, \tau_2, \cdots, \tau_n$ in $\mathcal{H}$ so that $Q(j(z) = \prod_i j(z) - \tau_i$ has a zero at each of the poles of f (counted with multiplicity). Thus $fQ(j(z))$ has poles only at infinity and by the above case is some polynomial $P(j(z))$. Thus $f = P(j(z))/Q(j(z))$. □

Chapter 2. The Modular Parameterization

2.1 The Eichler Integral and Initial Definitions

The modularity theorem implies that for every elliptic curve $E/\mathbb{Q}$ there exists a weight 2 and level N cusp form f_E whose Fourier coefficients come from the number of

points on E in each of the finite fields $\mathbb{F}_q$. The smallest such N is the conductor of E.

Also associated to E is the canonical differential

$$\omega = m f_E(z) dz$$

where m is the Manin constant. The constant m is the unique rational number (up to sign) such that ω is a smooth nowhere-vanishing 1-form on the minimal Weierstrass model of E. It is known that m is an integer and it is conjectured (in close relation to the Birch and Swinnerton-Dyer conjecture) that $m = 1$ for the Strong Weil curve. For a more detailed discussion on the Manin constant see [1].

The Eichler integral is then defined as

$$\varepsilon(z) = 2\pi i \int_z^{i\infty} \omega = 2\pi i \int_z^{i\infty} m f_E(\tau) d\tau. \tag{2.1}$$

The function $\varepsilon(z)$ is not modular, but if $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$ acts as usual on the upper-half plane, then

$$\begin{aligned} \frac{d}{dz}\big(\varepsilon(\gamma z) - \varepsilon(z)\big) &= \frac{d}{dz} 2\pi i \int_{\gamma z}^{z} m f_E(\tau) d\tau \\ &= 2\pi i m\big(f_E(z) - (cz+d)^2 f_E(z)(cz+d)^{-2}\big) = 0 \end{aligned}$$

where the second to last equality follows from the fundamental theorem of calculus and the modularity of f_E. So $\varepsilon(z)$ is *almost* modular, in the sense that the difference $\varepsilon(\gamma z) - \varepsilon(z)$ depends only on γ, and not on z. Denote this difference by

$$C(\gamma) := \varepsilon(\gamma z) - \varepsilon(z).$$

One readily verifies that $C : \Gamma_0(N) \to m\Lambda_E$ is a group homomorphism. Eichler and Shimura [5, 10] showed that when the Manin constant is 1, then C is surjective.

For any $\lambda \in \mathbb{C}$ such that $\lambda \in \mathrm{End}(E)$, we have that $\lambda\Lambda_E \subseteq \Lambda_E$. We define

$$\wp_\lambda(z, \Lambda_E) := \lambda^2 \wp(\lambda z, \Lambda_E) = \wp(z, \frac{1}{\lambda}\Lambda_E),$$

where the extra factor λ^2 normalizes $\wp_\lambda$ to have a leading coefficient of q^{-2} in its Fourier expansion. Similarly,

$$\wp'_\lambda(z, \Lambda_E) := \lambda^3 \wp'(\lambda z, \Lambda_E) = \wp'(z, \frac{1}{\lambda}\Lambda_E).$$

With this notation we define

$$X_\lambda(z) = m^2 \wp_\lambda(\varepsilon(z), \Lambda_E) - \frac{a_1^2 + 4a_2}{12},$$

$$Y_\lambda(z) = \frac{m^3}{2}\wp'_\lambda(\varepsilon(z), \Lambda_E) - \frac{a_1 m^2}{2}\wp_\lambda(\varepsilon(z), \Lambda_E) + \frac{a_1^3 + 4a_1a_2 - 12a_3}{24}$$

for E given in general Weierstrass form with the convention that if the subscript λ is omitted we take $\lambda = 1$. Note that if E is given in Wierstrass short form then we have a much simpler expression for $X_\lambda(z)$ and $Y_\lambda(z)$, namely

$$X_\lambda(z) := m^2 \wp_\lambda(\varepsilon(z), \Lambda_E) \quad Y_\lambda(z) := \frac{m^3}{2}\wp'_\lambda(\varepsilon(z), \Lambda_E).$$

By construction $X_\lambda(z), Y_\lambda(z)$ satisfy the Weierstrass equation for the elliptic curve and $X_\lambda(z)$ and $Y_\lambda(z)$ are modular over $\Gamma_0(N)$ since

$$\wp_\lambda(\varepsilon(\gamma z), \Lambda_E) = \wp_\lambda(\varepsilon(z) + C(\gamma), \Lambda_E) = \wp_\lambda(\varepsilon(z), \Lambda_E)$$

where the final equality holds because $\lambda C(\gamma) \in \Lambda_E$. A similar calculation holds for $Y_\lambda(z)$ as well as the parametrizations for the general form.

2.2 Expansions at Other Cusps

The first step in computing the coefficient functions A_i in (1.1) is to compute the q-expansions of each of the factors $(x - F(\gamma z))$ for x a formal variable and $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. Since we are interested specifically in F that are rational functions of $X_\lambda(z)$ and $Y_\lambda(z)$ it suffices to calculate the q-expansions for $X(\gamma z)$ and $Y(\gamma z)$. These coefficients are determined by two relations,

$$qX' = (2Y + a_1X + a_3)f_E \tag{2.2}$$

known as the invarient differential of E (see section III of [11]), and the rational model for the elliptic curve

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6. \tag{2.3}$$

A recursive algorithm was given by Cremona [4] using these two relations to calculate the expansions of $X(z)$ and $Y(z)$ at the cusp ∞. Acting on (2.2) and (2.3) by a matrix $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ gives relations that allow us to recursively calculate the coefficients of modular parametrizations around cusps other than infinity. There are, however, a few complications we examine below.

If we let $q_N(z) = e^{\frac{2\pi i}{N}z}$, we can write the expansions of the modular parametrizations at a cusp ρ with width w as $X_\lambda(\gamma z) = \sum_{n=-2}^{\infty} b_n q_w^n$ and $Y_\lambda(\gamma z) = \sum_{n=-3}^{\infty} d_n q_w^n$. Note that b_i, d_i might be zero for $i = -3, -2, -1$ if neither X nor Y have poles at ρ. By examining the first few terms if the Laurent series of $\wp_\lambda$ and $\wp'_\lambda$ and evaluating them at $\varepsilon(\gamma z)$ we can calculate b_{-2} and d_{-3}. So our inductive set up will be to assume that we know the

b_i coefficients for $-2 \leq i \leq n-1$ and the d_j coefficients for $-3 \leq j \leq n-2$ and use this information to calculate b_n and d_{n-1}. Letting c_n denote the coefficient of q_w^n of $f_E(\gamma z)$, relation (2.2) gives us that

$$\frac{1}{w}\sum_{n=-2}^{\infty} nb_n q_w^n = \Big(2\sum_{n=-3}^{\infty} d_n q_w^n + a_1 \sum_{n=-2}^{\infty} b_n q_w^n + a_3\Big)\sum_{n=1}^{\infty} c_n q_w^n.$$

Comparing the coefficients of q_w^n gives us the linear relation between b_n and d_{n-1}

$$nb_n = 2w\sum_{k=-3}^{n-1} c_{n-k}d_k + a_1 w\sum_{k=-2}^{n-1} c_{n-k}b_k + a_3 w c_n. \tag{2.4}$$

Comparing the q_w^{n-4} term in (2.3) gives us

$$\sum_{k=-3}^{n-1} d_{n-4-k}d_k + a_1\sum_{k=-3}^{n-2} b_{n-4-k}d_k + a_3 d_{n-4} = \sum_{k=-2}^{n}\sum_{j=-2}^{n-2-k} b_{n-4-k-j}b_j b_k + a_2\sum_{k=-2}^{n-2} b_{n-4-k}b_k + a_4 b_{n-4} + a_6^* \tag{2.5}$$

where a_6^* indicates that this term is present only if $n-4=0$. This gives a second linear relation between d_{n-1} and b_n, which allows us to solve for d_{n-1} and b_n uniquely whenever the determinant of the system is not 0, i.e. when $-2nd_{-3}^2 + 6wc_1 b_{-2}^2 \neq 0$. Supposing that $X_\lambda(z)$ has a pole at ρ, (so that neither d_{-3} nor b_{-2} are 0), then

$$-2n(d_{-3})^2 + 6wc_1(b_{-2})^2 = 0 \quad \Longrightarrow\ n = \frac{3wc_1(b_{-2})^2}{(d_{-3})^2}.$$

So this recursive process will not fail if we can find the first $\frac{3wc_1(b_{-2})^2}{(d_{-3}^2)}$ nontrivial terms of $X(z)$ and $Y(z)$ via the Laurent series expansions of $\wp_\lambda$ and $\wp_\lambda'$. Note that when $\rho=\infty$, we have that $w = c_1 = b_{-2} = d_{-3} = 1$ so that Cremona's algorithm doesn't fail with as few as 3 known terms of the Laurent expansion of $\wp_\lambda(\varepsilon(z))$.

However, if there are no poles at ρ, then $d_i = b_j = 0$ for $i, j < 0$, and the determinant

will be 0 for all n. So when calculating the q_w-expansions around cusps without poles, we need to compare other powers of q_w to get information about such systems. Comparing powers of q_w^n in both (2.2) and (2.3) gives

$$nb_n = 2w\sum_{k=0}^{n} c_{n-k}d_k + a_1 w\sum_{k=0}^{n} c_{n-k}b_k + a_3 w c_n.$$

$$\sum_{k=0}^{n} d_{n-k}d_k + a_1\sum_{k=0}^{n} b_{n-k}d_k + a_3 d_n = \sum_{k=0}^{n}\sum_{j=0}^{n-k} b_{n-k-j}b_j b_k + a_2\sum_{k=0}^{n} b_{n-k}b_k + a_4 b_n + a_6^*.$$

This gives two new linear relations between d_n and b_n whose determinant is $n(2d_0 + a_1b_0 + a_3)$. Interestingly, this determinant is zero when $2d_0 + a_1b_0 + a_3 = 0$, i.e. when the constant terms of the expansions of $X(z)$ and $Y(z)$ give a point of order 2 on E. This is seen most easily by looking at (2.2), and observing that $2d_0 + a_1b_0 + a_3 = 0$ corresponds to a vertical tangent line on E.

Thus the final case we consider is when $2d_0 + a_1b_0 + a_3 = 0$. In this case, we compare powers of q_w^n in (2.2) and powers of q_w^n in (2.3) exactly like the previous case. The main difference is that since $2d_0 + a_1b_0 + a_3 = 0$, this gives us a system in the unknowns b_n and d_{n-1} instead of in terms of b_n and d_n. Specifically, we get the linear equations

$$nb_n - 2wd_{n-1} = 2w\sum_{k=1}^{n-2} c_{n-k}d_k + a_1 w\sum_{k=1}^{n-1} c_{n-k}b_k$$

$$\begin{aligned}(2d_1)d_{n-1} - (3b_0^2 + 2a_2b_0 + a_4 - a_1d_0)b_n = &\sum_{k=1}^{n-1}\sum_{j=1}^{n-k} b_{n-k-j}b_j b_k + \sum_{j=1}^{n-1} b_{n-1-j}b_j b_1 \\ &+ a_2\sum_{k=1}^{n-1} b_{n-k}b_k - \left(\sum_{k=2}^{n-2} d_{n-k}d_k + a_1\sum_{k=2}^{n-1} d_{n-k}b_k\right).\end{aligned}$$

Thus, we calculate that this system is always uniquely solvable for b_n and d_{n-1} unless

$2nd_1 - 2w(3b_0^2 + 2a_2b_0 + a_4 - a_1d_0) = 0$. This would imply that

$$n = \frac{2w(3b_0^2 + 2a_2b_0 + a_4 - a_1d_0)}{d_1}.$$

Note that $d_1 \neq 0$ since $d_1 = 0$ would give $b_1 = b_2 = 0$, and in order to satisfy equations (2.4) and (2.5) $X(z)$ and $Y(z)$ would need to be b_0 and d_0, a contradiction. So this recursive process will not fail if we can find the first $2w(3b_0^2 + 2a_2b_0 + a_4 - a_1d_0)/d_1$ nontrivial terms of $X(z)$ and $Y(z)$ via the Laurent series expansions of $\wp_\lambda$ and $\wp'_\lambda$.

Thus, given any elliptic curve E, we can calculate $X(\gamma z), Y(\gamma z)$ for any $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ by considering one of the three cases, $X(z), Y(z)$ has a singularity at $\gamma\infty$, $X(z), Y(z)$ is analytic at $\gamma\infty$ and $(X(\gamma\infty), Y(\gamma\infty))$ is not a point of order 2 on E, and finally the case where $X(z), Y(z)$ is analytic at $\gamma\infty$ and $(X(\gamma\infty), Y(\gamma\infty))$ is a point of order 2 on E.

2.3 The Modular Polynomial

Now that we can efficiently calculate the q-expansions for $X(\gamma z), Y(\gamma z)$ it is possible to construct

$$\Phi_F(x) := \prod_{\gamma \in \Gamma_0(N) \backslash SL_2(\mathbb{Z})} \Big(x - F(\gamma z)\Big) = \sum A_i(z) x^i$$

where x is a formal variable and F is any rational function in $X_\lambda(z)$ and $Y_\lambda(z)$. Note that by construction, the coefficients of $\Phi_F(x)$ are modular functions which are invariant under the action of $\mathrm{SL}_2(\mathbb{Z})$, and so are rational functions in Klein's j-function.

In practice, in order to compute the minimal divisor of $\Phi_F(x)$ it is computationally advantageous to compute each of the functions $F(\gamma z)$ and then use symmetric polynomials to calculate the necessary coefficient functions until we locate all the poles of F.

Example 2.3.1. Consider the elliptic curve

$$E : y^2 + xy + y = x^3 - x^2 - 3x + 3. \tag{26b1}$$

The point $(1, 0)$ lies on E and has $(1, -2)$ as its inverse. Then looking at the function $F(z) = \frac{Y(z)+2}{X(z)-1}$, we see that F has a simple pole $z \in \mathcal{H}$ that map $(X(z), Y(z))$ to $(1, 0)$. Note that the conductor of E is 26, and $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(26)] = 42$. Calculating the trace of Φ_F (or the coefficient $A_{41}(z)$) we get

$$\sum_{\gamma \in \Gamma_0(26) \backslash \mathrm{SL}_2(\mathbb{Z})} F(\gamma z) = \frac{-j(z)^2 + 54688 j(z) - 37627200}{j(z) - 54000}.$$

Testing the 42 cosets of $\Gamma_0(26)$ in $\mathrm{SL}_2(\mathbb{Z})$ gives us that for $z_0 = \frac{-7+\sqrt{-3}}{52}$, $(X(z_0), Y(z_0)) = (1, 0)$. Thus a preimage of the rational point $(1, 0)$ is a CM point on $X_0(26)$.

Using this theory we are able to give a condition for when a point P on an elliptic curve E is the image of a CM point $\mathcal{P}$ on the modular curve and prove Theorem 1.2. *Proof of Theorem 1.2* Suppose that m exactly divides N and let $\mathcal{P}_2 = (e_2, c_2)$ be the image of $\mathcal{P}_1 = (e_1, c_1)$ under the Atkin-Lehner involution $W_m = \left(\begin{smallmatrix} am & b \\ cN & dm \end{smallmatrix}\right)$ for integers a, b, c, d. The matrix W_m imposes a rational map from $X_0(N)$ to itself, so if e_1 is not isomorphic to e_2, then W_m is a rational isogeny of the curves e_1 and e_2. If e_1 is isomorphic to e_2 and we write the periods for e_1, e_2 as ω_{11}, ω_{12} and ω_{21}, ω_{22} respectively, then W_m takes $\tau_1 = \frac{\omega_{12}}{\omega_{11}}$ to $\tau_2 = \frac{\omega_{22}}{\omega_{21}}$. However, since $e_1 \cong e_2$, there must be a matrix $A = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$ in $\mathrm{SL}_2(\mathbb{Z})$ such that $W_m \tau_1 = \tau_2 = A\tau_1$. This gives a quadratic relation that τ_1 satisfies, namely

$$(am\tau_1 + b)(\gamma\tau_1 + \delta) = (\alpha\tau_1 + \beta)(cN\tau_1 + dm).$$

Expanding and collecting like terms gives

$$(am\gamma - c\alpha N)\tau_1^2 + (b\gamma + am\delta - cN\beta - dm\alpha)\tau_1 + b\delta - dm\beta = 0.$$

The discriminant of this quadratic is

$$\begin{aligned} D &= (b\gamma + am\delta - cN\beta - dm\alpha)^2 - 4(am\gamma - c\alpha N)(b\delta - dm\beta) \\ &= b^2\gamma^2 + a^2m^2\delta^2 + c^2N^2\beta^2 + d^2m^2\alpha^2 \\ &+ 2b\gamma am\delta - 2b\gamma cN\beta - 2b\gamma dm\alpha - 2am\delta cN\beta - 2adm^2\alpha\delta + 2cN\beta dm\alpha \\ &- 4(am\gamma b\delta - am^2d\beta\gamma - cNb\alpha\delta + c\alpha Ndm\beta). \end{aligned}$$

We collect like terms and use the fact that $\det(W_m) = adm^2 - cNb = m$ to get

$$\begin{aligned} D &= b^2\gamma^2 + a^2m^2\delta^2 + c^2N^2\beta^2 + d^2m^2\alpha^2 \\ &- 2b\gamma am\delta + 2b\gamma cN\beta - 2b\gamma dm\alpha - 2am\delta cN\beta + 2adm^2\alpha\delta - 2cN\beta dm\alpha \\ &- 4(m\alpha\delta - m\beta\gamma). \end{aligned}$$

Factoring and using that $\det(A) = \alpha\delta - \beta\gamma = 1$ gives that

$$D = (b\gamma - am\delta + cN\beta - dm\alpha)^2 - 4m.$$

Thus D is a square mod $4m$. Since τ_1 is in the upper half plane, we must have that $D < 0$. However, since $(b\gamma - am\delta + cN\beta - dm\alpha)^2$ is non-negative, we have $-4m \leq D < 0$. $\square$

Example 2.3.2. We return to the curve

$$E : y^2 + xy + y = x^3 - x^2 - 3x + 3 \tag{26b1}$$

of conductor 26 and index 42. Consider the points $(1,-2)$ and $(3,2)$ with inverses $(1,0)$ and $(3,-6)$ on E. Then the functions F and G given by

$$F(z) = \frac{Y(z)-0}{X(z)-1}, \quad G(z) = \frac{Y(z)+6}{X(z)-3}$$

have simple poles for z such that $(X(z),Y(z)) = (1,-2)$ or $(3,2)$ respectively. We calculate specific coefficient functions of $\Phi_F = \sum A_i(z)x^i$ and $\Phi_G = \sum B_i(z)x^i$ to determine the location of these poles in the upper half plane:

$$A_{41}(z) = \frac{-j(z)^2 + 288156 \cdot j(z) - 199626768}{j(z) - 287496},$$
$$B_{40}(z) = \frac{j(z)^3 - 3214 \cdot j(z)^2 + 2726620 \cdot j - 274323456}{j(z) - 1728}.$$

Thus $\Phi_F(z)$ has poles only when $j(z) = 287496$, i.e. when z is in the $\mathrm{SL}_2(\mathbb{Z})$ orbit of $\sqrt{-4}$, and $G(z)$ has poles only when $j(z) = 1728$ i.e. when z is in the $\mathrm{SL}_2(\mathbb{Z})$ orbit of $\sqrt{-1}$. Comparing the actions of the coset representatives of $\Gamma_0(26)$, we find that $z_0 := \frac{-5+\sqrt{-1}}{52}$ satisfies $(X(z),Y(z)) = (1,-2)$, and $z_1 = \frac{5+\sqrt{-1}}{13}$ satisfies $(X(z),Y(z)) = (3,2)$.

Examining the action of the Atkin-Lehner involutions W_2 and W_{13}, we find that $F_2 = F(W_2 z)$, and $G_2 = G(W_2 z)$ have coefficient functions

$$A_{40}(z) = \frac{-j(z)^2 + 3235 \cdot j(z) - 2655936}{j(z) - 1728}, \qquad B_{41}(z) = \frac{-42 \cdot j(z) + 21954240}{j(z) - 287496},$$

while $F_{13} := F(W_{13}z)$ and $G_{13} := G(W_{13}z)$ have coefficient functions

$$A_{41}(z) = \frac{-j(z)^2 + 288156 \cdot j(z) - 199626768}{j(z) - 287496},$$
$$B_{40}(z) = \frac{j(z)^3 - 3214 \cdot j(z)^2 + 2726620 \cdot j - 274323456}{j(z) - 1728}.$$

Thus since W_2 exchanges the poles of F and G, Theorem 1.2 gives that the points z_0, z_1 correspond to isogenous elliptic curves on $X_0(26)$. Additionally, since W_{13} fixes z_0 and z_1, Theorem 1.2 also tells us they are both CM points on $X_0(26)$ whose orders have discriminants that must be squares mod 52. In fact, the minimal polynomial of z_0 is $104z^2 - 20z + 1$ which has discriminant $-16 \equiv 6^2 \mod 52$, and the minimal polynomial for z_1 is $13z^2 - 10z + 2$ which has discriminant $-4 \equiv 10^2 \mod 52$.

The previous example describes a process that is quite general. Given a curve E, with a rational point (x, y) and modular parameterization $X(z), Y(z)$, then the function $F(z) = (Y(z) - y^*) / (X(z) - x^*)$ where (x^*, y^*) is the inverse of the point (x, y) as a point on E has a pole of order 1 at any complex number $w \in \Lambda_E$ such that $(X(w), Y(w)) = (x, y)$. This is because $Y(z) - y^*$ and $X(z) - x^*$ have poles of order 3 and 2 respectively at such a point w. Using the algorithm described in section 2.2, we calculate $F(\gamma z)$ for coset representitives of $\Gamma_0(N) \backslash \mathrm{SL}_2(\mathbb{Z})$. This allows us to use symmetric polynomials to calculate the coefficients $A_i(z)$ of $\Phi_F(z)$ whose poles are precisily the complex numbers w we desire. This process was previously known, but was limited to the cases where N was a prime so that the functions $F(\gamma z)$ could be feasably computed.

Example 2.3.3. Theorem 1.2 can also be visualized in the following way. Consider again the elliptic curve $E : y^2 + y = x^3 - x^2 - 10x - 20$ of conductor 11, and the fundamental domain F_{11} in figure 2.1 for the congruence subgroup $\Gamma_0(11)$.

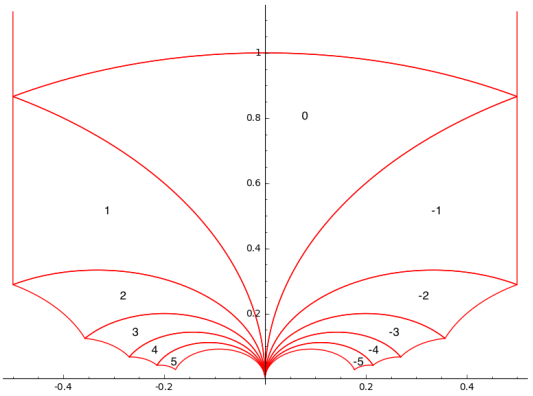

Figure 2.1: Fundamental domain F_{11} for $\Gamma_0(11)$

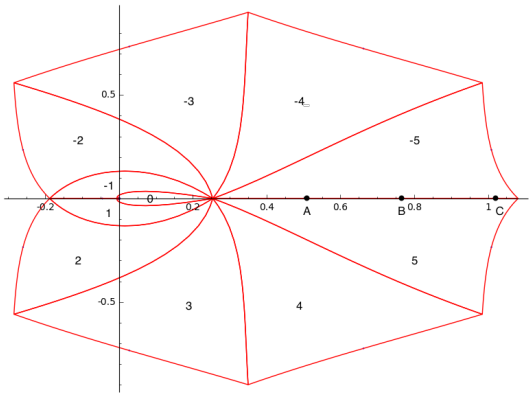

Figure 2.2: Eichler integral over the boundary of F_{11}

This fundamental domain has been constructed by taking $\mathrm{SL}_2(\mathbb{Z})$ coset representatives of the form $\left(\begin{smallmatrix} 0 & -1 \\ 1 & j \end{smallmatrix}\right)$ for $-5 \leq j \leq 5$, with each j labeled in the corresponding hypertriangle. The associated newform of E is $f_E = q - 2q^2 - q^3 + 2q^4 \ldots$. Taking complex values z on the boundary of F_{11} and calculating $\varepsilon(z) = \int_z^{i\infty} m f_E(\tau) d\tau$ gives the image in Figure 2.2. The resulting image tiles the plane in a parallelogram-type pattern, with the same periods as E. The points A, B and C have been labeled at $2/5$, $3/5$ and $4/5$ times the real period of E respectively. They correspond to the points $(5, -6), (5, 5)$ and $(16, 60)$ on E respectively. The action of W_{11} interchanges the two cusps in Figure 2 (∞ located at the origin, and 0 located at the value $.2538\ldots$ on the real line which is $1/5$ the real period of E). Up to translation by the real period, we see that W_{11} interchanges the points A and C but fixes point B. By Theorem 1.2 we conclude that the preimages of the points $(5, -6)$ and $(16, 60)$ on $X_0(11)$ give isogenous elliptic curves, while the preimage of $(5, 5)$ on $X_0(11)$ must be a CM point as we saw in Example 1.1.

Chapter 3. Congruences Between Modular Parametrizations

3.1 Motivating Examples

Consider the elliptic curves E_1, E_2 given by

$$E_1 : y^2 + xy + y = x^3 + 4x - 6, \tag{14a1}$$

$$E_2 : y^2 + xy + y = x^3 - 36x - 70. \tag{14a2}$$

Looking at the q-expansions of the row reduced basis elements of $\mathbb{Q}[X(z), Y(z)]$, we see

Basis over E_1, $X = X_{E_1}(z)$, $Y = Y_{E_1}(z)$	q-expansion					
1	1					
$X(z) - 2$	q^{-2}	$+q^{-1}$	$+2q$	$+2q^2$	$+3q^3$	$+\cdots$
$-Y(z) - 2X(z) - 2$	q^{-3}	$+2q^{-1}$	$+5q$	$+4q^2$	$+2q^3$	$+\cdots$
$X(z)^2 + 2Y(z) - X(z) + 2$	q^{-4}	$-q^{-1}$	$-2q$	$+8q^2$	$+5q^3$	$+\cdots$
$-Y(z)X(z) - 3X(z)^2 + 2Y(z) + 3X(z) - 2$	q^{-5}		$-2q$	$-4q^2$	$+18q^3$	$+\cdots$
$X(z)^3 + 3X(z)Y(z) - 5Y(z) + 2X(z) - 6$	q^{-6}	$-2q^{-1}$	$+4q$	$-7q^2$	$-6q^3$	$+\cdots$

Basis over E_2, $X = X_{E_2}(z)$, $Y = Y_{E_2}(z)$	q-expansion					
1	1					
$X(z) - 2$	q^{-2}	$+q^{-1}$	$+2q$	$10q^2$	$-5q^3$	$+\cdots$
$-Y(z) - 2X(z) - 2$	q^{-3}	$+2q^{-1}$	$-3q$	$-4q^2$	$+2q^3$	$+\cdots$
$X(z)^2 + 2Y(z) - X(z) - 14$	q^{-4}	$-q^{-1}$	$+14q$		$+29q^3$	$+\cdots$
$-Y(z)X(z) - 3X(z)^2 + 2Y(z) + 3X(z) + 38$	q^{-5}		$+6q$	$-28q^2$	$-14q^3$	$+\cdots$
$X(z)^3 + 3X(z)Y(z) - 5Y(z) - 22X(z) - 6$	q^{-6}	$-2q^{-1}$	$-12q$	$+25q^2$	$+138q^3$	$+\cdots$

Table 3.1: Congruences for basis of $\mathbb{Q}[X(z), Y(z)]$ for related elliptic curves.

the coefficients of the q-expansions are congruent mod 8 (see the above table).

The coefficients of the integral models for E_1 and E_2 are also congruent mod 8. However, the congruence in the basis elements of the algebras $\mathbb{Q}[X_{E_i}(z), Y_{E_i}(z)]$ for $i = 1, 2$ is not a simple consequence of the congruence of the equations of E_1 and E_2. For example, the curves

$$E_3 : y^2 + xy + y = x^3 + x^2 - 5x + 2, \tag{15a3}$$

$$E_4 : y^2 + xy + y = x^3 + x^2 + 35x - 28. \tag{15a4}$$

are congruent mod 10, but the q-expansions of the X term of their optimal modular parametrizations are

$$X_{E_3}(z) = q^{-2} + q^{-1} + 1 + 2q + 3q^2 + \ q^3 + \cdots - 6q^{11} + \cdots,$$
$$X_{E_4}(z) = q^{-2} + q^{-1} + 1 + 2q - 5q^2 + 9q^3 + \cdots + 7q^{11} + \cdots.$$

Comparing the q^2 terms shows that any congruence between these two parametrizations must divide 8, and comparing the q^{11} terms shows that any such congruence must divide 13. Thus we conclude that there are *no* nontrivial congruences between the parametrizations. So when do congruences in the elliptic curve equation give rise to congruences in the generated algebras?

If we assume that the two elliptic curves E_1 and E_2 given by

$$E_1 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$
$$E_2 : y^2 + \alpha_1xy + \alpha_3y = x^3 + \alpha_2x^2 + \alpha_4x + \alpha_6,$$

are isogenous, then their period lattices will intersect nontrivially in a lattice Λ_3, corre-

sponding to an elliptic curve E_3 with integral model

$$y^2 + \beta_1 xy + \beta_3 y = x^3 + \beta_2 x^2 + \beta_4 x + \beta_6.$$

Thus the difference

$$g(z) := \wp(z, \Lambda_1) - \wp(z, \Lambda_2)$$

is an even, elliptic function with period lattice Λ_3. If we let $\{r_i\}$ represent the complex numbers such that $\wp(r_i, \Lambda_3)$ is a zero of $g(z)$ in a fundamental parallelogram of Λ_3 and let $\{t_j\}$ be the values in Λ_3 such that $\wp(t_j, \Lambda_3)$ is a pole of $g(z)$ (repeated according to multiplicities) except possibly at the origin (even if the origin is a zero or pole of g), then the function

$$\frac{\prod_i (\wp(z, \Lambda_3) - \wp(r_i, \Lambda_3))}{\prod_j (\wp(z, \Lambda_3) - \wp(t_j, \Lambda_3))}$$

is monic, and has the same zeros and poles as $g(z)$ except possibly at 0. However, a classical argument shows that the product must have the same zero or pole as $g(z)$ at 0 as well (see [6] for example). Thus

$$g(z) = \wp(z, \Lambda_1) - \wp(z, \Lambda_2) = C \frac{\prod_i (\wp(z, \Lambda_3) - \wp(r_i, \Lambda_3))}{\prod_j (\wp(z, \Lambda_3) - \wp(t_j, \Lambda_3))} \tag{3.1}$$

for some constant C. Since

$$\wp(z, \Lambda_1) - \wp(z, \Lambda_2) = \frac{g_2(\Lambda_1) - g_2(\Lambda_2)}{20} z^2 + \frac{g_3(\Lambda_1) - g_3(\Lambda_2)}{28} z^4 + \cdots$$

we see that

$$C = C(\Lambda_1, \Lambda_2) = \begin{cases} \frac{g_2(\Lambda_1) - g_2(\Lambda_2)}{20} & \text{if } g_2(\Lambda_1) \neq g_2(\Lambda_2) \\ \frac{g_3(\Lambda_1) - g_3(\Lambda_2)}{28} & \text{if } g_2(\Lambda_1) = g_2(\Lambda_2). \end{cases}$$

3.2 A Sufficient Condition for Congruent Algebras

With this notation we have the following theorem.

Theorem 3.2.1. *Suppose that E_1, E_2 are two isogenous elliptic curves over $\mathbb{Q}$. Also assume that the coordinates of the torsion points of order dividing N in $\overline{\mathbb{Q}}$ are algebraic integers. Then there is an explicit natural number $D(\Lambda_1, \Lambda_2)$ so that the q-expansion of $X_{E_1} - X_{E_2}$ is congruent to a constant mod $C(\Lambda_1, \Lambda_2)/D(\Lambda_1, \Lambda_2)$.*

Proof. Evaluating equation (3.1) at $\varepsilon(z)$ and adding the appropriate constant to both sides of the equality gives

$$\begin{aligned} X_{E_1}(z) - X_{E_2}(z) &= \wp(\varepsilon(z), \Lambda_1) + \frac{a_1^2 - 4a_2}{12} - \wp(\varepsilon(z), \Lambda_2) - \frac{\alpha_1^2 - 4\alpha_2}{12} \\ &= C\frac{\prod_i (\wp(\varepsilon(z), \Lambda_3) - \wp(r_i, \Lambda_3))}{\prod_j (\wp(\varepsilon(z), \Lambda_3) - \wp(t_j, \Lambda_3))} + \frac{a_1^2 - \alpha_1^2 + 4\alpha_2 - 4a_2}{12} \\ &= C\frac{\prod_i X_{E_3} - R_i}{\prod_j X_{E_3} - T_j} + \frac{a_1^2 - \alpha_1^2 + 4\alpha_2 - 4a_2}{12} \end{aligned}$$

where $R_i = \wp(r_i, \Lambda_3) - \frac{\beta_1^2 - 4\beta_2}{12}$ and $T_j = \wp(t_j, \Lambda_3) - \frac{\beta_1^2 - 4\beta_2}{12}$. The final equality follows from $X_{E_3} = \wp(z, \Lambda_3) + \frac{\beta_1^2 - 4\beta_4}{12}$ so that the fraction cancels out of the X_{E_3} term and the R_i or T_j term.

The T_j's are x-coordinates of torsion points of order dividing N because the poles of $g(z)$ occur at lattice points of either Λ_1 or Λ_2. By hypothesis, these coordinates are algebraic integers. Since the q-expansions of both X_{E_1} and X_{E_2} are both integers, we also have that each of $\wp(r_i, \Lambda_3)$ must be algebraic. So we define $D = D(\Lambda_1, \Lambda_2) = \prod_i D_i$ where D_i is the minimal natural number so that $D_i R_i$ is an algebraic integer. Thus

$$X_{E_1}(z) - X_{E_2}(z) = \frac{C}{D}\frac{\prod_i D_i X_{E_3} - D_i R_i}{\prod_j X_{E_3} - T_j}.$$

Since the formal product $(\prod_j X_{E_3} - T_j)^{-1}$ has algebraic integer coefficients, and since $D_i R_i$ is an algebraic integer for all i, the above shows that all but the constant term of the q-expansion of $X_{E_1}(z) - X_{E_2}(z)$ are congruent to zero mod C/D. $\square$

Example 3.2.2. Let's return to the curves E_1, E_2 (Cremona labels 14a1 and 14a2) where we found a congruence mod 8 between the q-expansions for their modular parametrizations. The period lattices for E_1, E_2 are given by the generators

$$(z_{11}, z_{12}) \approx (1.981341, .990670 + 1.325491i), \quad (z_{21}, z_{22}) \approx (.990670, 1.325491i),$$

and so we see that $\Lambda_{E_1} \subseteq \Lambda_{E_2}$. So we can write $\wp(z, \Lambda_2)$ as a rational function in $\wp(z, \Lambda_1)$. A quick calculation shows that in fact,

$$\wp(z, \Lambda_1) - \wp(z, \Lambda_2) = \frac{8}{13/12 - \wp(z, \Lambda_1)}.$$

Since $X_{E_1}(z) = \wp(\varepsilon(z), \Lambda_1) - 1/12$, we conclude that

$$X_{E_1}(z) - X_{E_2}(z) = \frac{8}{1 - X_{E_1}}.$$

Since X_{E_1} has integer coefficients, this makes the congruence mod 8 between X_{E_1} and X_{E_2} now apparent.

Example 3.2.3. Using Theorem 3.2.1 we can now see why the curves

$$E_3 : y^2 + xy + y = x^3 + x^2 - 5x + 2, \tag{15a3}$$

$$E_4 : y^2 + xy + y = x^3 + x^2 + 35x - 28., \tag{15a4}$$

had only the trivial congruence mod 1 even though their expressions share a congruence mod 10. These curves are isogenous and $\Lambda_3 \subseteq \Lambda_4$, so we can write the difference $X_{E_4} -$

X_{E_3} as a rational funtion in terms of X_{E_3}. Since $g_2(\Lambda_{E_3})/20 = 241/240$ and $g_2(\Lambda_{E_4})/20 = -1679/240$, we see that $C = (241 + 1679)/240 = 8$. Also, we compute that

$$X_{E_4} - X_{E_3} = C\frac{-(X_{E_3} - \frac{3}{4})(X_{E_3} - \frac{3}{2})}{(X_{E_3} - 1)(X_{E_3})^2}.$$

So we see that $D = 8$ as well. Thus $C/D = 1$.

3.3 A Sturm-like Bound for Meromorphic Modular Forms

While Theorem 3.2.1 describes many congruent algebras, it does not describe all congruences that we noticed computationally on curves of conductor less than 100. For example, the curves

$$E_1 : y^2 = x^3 + x^2 - 32x + 60 \tag{96a3}$$

$$E_2 : y^2 = x^3 + x^2 - 384x + 2772. \tag{48a5}$$

are not isogenous over $\mathbb{Q}$, so Theorem 3.2.1 doesn't tell us of any congruences between the two algebras. However, looking at the difference of the q-expansions of the modular parametrizations of the x coordinates of these two curves gives

$$-68q + 780q^3 - 5020q^5 + 24140q^7 - 96712q^9 + 340500q^{11} - 1086568q^{13} + \mathrm{O}(q^{15}).$$

We see that this form appears to be 0 mod 4. In fact, computationally we can confirm that a large number of coefficients are divisible by 4. We would like to be able to tell whether all of the coefficients are congruent to 0 mod 4 by looking at some finite number of terms in the q-expansion. To this end, we give a generalization of Sturm's bound that applies to meromorphic modular forms. The arguement is essentially the same, but we

give a proof for completeness. For a modular form with q-expansion $f = \sum a_n q^n$ we denote

$$\mathrm{ord}_{\mathfrak{p}} f := \mathrm{ord}_{\infty}(f \bmod \mathfrak{p}) = \min\{n : a_n \notin \mathfrak{p}\}$$

and observe that since $\mathfrak{p}$ is a prime ideal, $\mathrm{ord}_{\mathfrak{p}}(fg) = \mathrm{ord}_{\mathfrak{p}}(f) + \mathrm{ord}_{\mathfrak{p}}(g)$. We also denote by $M_k^{!!}(\Gamma, \mathcal{O})$ the collection of meromorphic modular forms of weight k over Γ with Fourier coefficients in $\mathcal{O}$. With this notation we prove the following.

Lemma 3.3.1. *Let $\mathfrak{p}$ be a prime ideal in the ring of integers $\mathcal{O}$ of a number field K. Further suppose that $f \in M_k^{!!}(\Gamma, \mathcal{O})$ and $|\Gamma \backslash \mathrm{SL}_2(\mathbb{Z})| = m$. Finally, let Ω be the set of points on $X_0(N)$ where f has poles. Then*

$$\mathrm{ord}_{\mathfrak{p}}(f) + \sum_{\tau \in \Omega} \mathrm{ord}_{\tau}(f) > \frac{km}{12}$$

implies that $f \equiv 0 \pmod{\mathfrak{p}}$.

Proof. We start with the case $\Gamma = \mathrm{SL}_2(\mathbb{Z})$. We first note that since f is meromorphic, $\mathrm{ord}_{\tau} f < \infty$ for all $\tau \in \Omega$. Also, since the coefficients of f are elements of $\mathcal{O}$, for each of the finite complex numbers $\tau_i \in \Omega \cap \Gamma \backslash \mathcal{H}$, we can pick relatively prime algebraic integers α_i, β_i so that $\beta_i j(z) - \alpha_i$ has a zero of order at least 1 at τ_i. So

$$g(z) := f(z) \prod_i (\beta_i j(z) - \alpha_i)^{-\mathrm{ord}_{\tau_i} f}$$

has poles only at infinity, and is modular over $\mathrm{SL}_2(\mathbb{Z})$. Thus Sturm's theorem applies giving $g(z) \equiv 0 \mod \mathfrak{p}$ since

$$\begin{aligned} \mathrm{ord}_{\mathfrak{p}}(g) &= \mathrm{ord}_{\mathfrak{p}}(f) - \sum_{\tau_i \in \Omega} \mathrm{ord}_{\tau_i}(f_i) \mathrm{ord}_{\mathfrak{p}}(\beta_i j + \alpha_i) \\ &\geq \mathrm{ord}_{\mathfrak{p}}(f) + \sum_{\tau_i \in \Omega} \mathrm{ord}_{\tau_i}(f) > \frac{k}{12}. \end{aligned}$$

The first inequality holds since α_i and β_i are relatively prime algebraic integers in $\mathcal{O}$, implying that each of the terms $(\beta_i j + \alpha_i)$ has order 0 or -1 mod $\mathfrak{p}$ corresponding to $\beta_i \in \mathfrak{p}$ or not. Thus $g \equiv 0 \pmod{\mathfrak{p}}$ which implies that $f \equiv 0 \pmod{\mathfrak{p}}$. This concludes the proof in the case that $\Gamma = \mathrm{SL}_2(\mathbb{Z})$.

If Γ is an arbitrary congruence subgroup, we first pick N so that $\Gamma(N) \subseteq \Gamma$ with m coset representatives γ_ℓ for $\Gamma(N)$ and we set $L = K(\zeta_N)$. Since $f \in M_k^{!!}(\Gamma(N), L)$ and $\Gamma(N)$ is a normal subgroup of $\mathrm{SL}_2(\mathbb{Z})$, the functions $f|_k\gamma_\ell$ are elements of $M_k^{!!}(\Gamma(N), L)$. Furthermore, the denominators of the Fourier coefficients of $f|_k\gamma_\ell$ are bounded because each is a finite L-linear combination of some integral basis of a finite dimensional subspace of $M_k^{!!}(\Gamma(N), L)$. Note that in general $M_k^{!!}(\Gamma(N), L)$ is not finite dimensional; however, if we restrict ourselves to the subspace that has poles of the same order and at the same locations as those of f and $f|_k\gamma_\ell$, then this subspace is finite dimensional. Thus we can pick constants $A_\ell \in L^\times$ so that each of the functions $\mathrm{ord}_{\mathfrak{P}}(A_\ell f^{[\gamma_\ell]_k}) = 0$ for some prime ideal $\mathfrak{P}$ lying over $\mathfrak{p}$. Reordering if necessary, let γ_1 be the identity matrix. The function

$$G(z) := f(z) \prod_{\ell=2}^{m} A_\ell f|_k\gamma_\ell$$

is a meromorphic modular form of weight km over $\mathrm{SL}_2(\mathbb{Z})$ with coefficients in $\mathcal{O}_L$. Then

$$\mathrm{ord}_{\mathfrak{P}}(G) \geq \mathrm{ord}_{\mathfrak{p}}(G) \geq \mathrm{ord}_{\mathfrak{p}}(f) + \sum_{\tau \in \Omega} \mathrm{ord}_\tau(f) > \frac{km}{12},$$

where the first equality follows because $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$. We conclude that $G \equiv 0 \pmod{\mathfrak{P}}$ from the $\mathrm{SL}_2(\mathbb{Z})$ case. Since each of the functions $A_{\gamma_\ell} f|_k\gamma_\ell$ were chosen such that $\mathrm{ord}_{\mathfrak{P}}(A_\ell f|_k\gamma_\ell) = 0$, this gives $G \equiv 0 \pmod{\mathfrak{p}}$ and so $f \equiv 0 \pmod{\mathfrak{p}}$. See theorem 9.18 in [12] to compare the above to the proof of Sturm's theorem for elements of $M_k(\Gamma, \mathcal{O})$. □

Corollary 3.3.2. *If X_{E_1} and X_{E_2} are modular parametrizations for the x coordinates*

of elliptic curves E_1 and E_2 of conductor N_1 and N_2 with modular degrees d_1 and d_2 respectively, then if $\mathrm{ord}_p(X_{E_1} - X_{E_2}) > 2(d_1 + d_2)$, *then* $X_{E_1} \equiv X_{E_2} \mod p$.

Proof: The number of poles of X_{E_i} is at most $2d_i$ counting multiplicities. Thus the corollary follows immediately from Theorem 4.4 applied to the difference $X_{E_1} - X_{E_2}$ which is modular over $\Gamma_0(\mathrm{lcm}\,(N_1, N_2))$ since

$$\mathrm{ord}_p(X_{E_1} - X_{E_2}) + \sum_{\tau \in \omega} \mathrm{ord}_\tau(X_{E_1} - X_{E_2}) > 2(d_1 + d_2) - 2(d_1 + d_2) = 0 = \frac{km}{12}. \qquad \square$$

Note that this bound is independent of both N_1 and N_2 since the weight k of the modular parametrizations is zero. We obtain a better estimate if we know a priori the locations of the poles of X_{E_i} and if they cancel in the difference $X_{E_1} - X_{E_2}$.

Corollary 3.3.2 gives us an easy way of determining if two related parametrizations are congruent mod $\mathfrak{p}$. Returning to our earlier example with the curves

$$E_1 : y^2 = x^3 + x^2 - 32x + 60, \tag{96a3}$$

$$E_2 : y^2 = x^3 + x^2 - 384x + 2772, \tag{48a5}$$

since the modular degree of both E_1 and E_2 is 8, computing $2(8 + 8) = 32$ coefficients of the difference function and observing that they are congruent to 0 mod 4 is sufficient to prove that all of the coefficients are congruent mod 4.

Appendix A. Code for Expansions at Cusps

The following is the code used to calculate the examples found in chapters 1-3. It is written for the CAS PARI/GP. Throughout the code, $\wp$ is usully refered to as "wp" and the derivative $\wp'$ is usually denoted as "wpp" (the extra "p" for prime).

```
MatAction(Gamma, z) =
```

```
{
return((Gamma[1,1]*z+Gamma[1,2])/(Gamma[2,1]*z+Gamma[2,2])); };
```

The following function takes an elliptic curve E and a matrix γ as an input, and calculates the value of the constant term of the expansion of X_E and Y_E at the image of infinity under the matrix Gamma.

```
get_point(E,Gamma) = {
mf = mffromell(E)[1];
nf = mffromell(E)[2];
FS1 = mfsymbol(mf,nf);
N = mf[1][1]; \\level
if(Gamma[2,1]/N+Gamma[2,2]!=0,
z = 2*Pi*I*mfsymboleval(FS1,[MatAction(Gamma,1/N),oo]);
z = -polcoef(z,0);
 \\mfsymboleval returns a polynomial instead of a float
,return([0]));
\\if the cusp is 1/N, then the constant term is zero (i.e. a pole in \wp).
if (z!=0 ,
return([ellztopoint(E,z),z]),
return([[0],0]));
};
```

The following uses the two recurrence relations to calculate the expansion of X_E and Y_E at a cusp if there is no pole there. The variable "Point" is a list $[[x, y], z]$ where $(x, y) = (\wp(z), \wp'(z))$ is a point on E.

```
expansion_at_cusp_no_pole(E,num_of_terms,Gamma,point) = {
X = vector(num_of_terms,i,0);
```

```
Y = vector(num_of_terms,i,0);
\\empty vectors where we will put the coefficients of the q-expansion
X[1] = point[1][1]; Y[1] = point[1][2];
mf = mffromell(E)[1];
\\modular forms space of weight 2 and level N (the conductor of E)
nf = mffromell(E)[2];
 \\ the associated newform
C = mfslashexpansion(mf,nf,Gamma,num_of_terms,0,&P);
\\the coefficients of f | [Gamma]_2
\\P is a parameter that holds the width of the cusp
\\among other things (see the pari documentation). for when the form
\\the form we're slashing isn't as nice as the weight 2 cusp form.

w = P[2]; \\ the width
\\The following are the coefficients for the model of E.
A1 = E.a1; A2 = E.a2; A3 = E.a3;  A4 = E.a4; A6 = E.a6;

\\This is the main recurrence that solves for b_n and d_n
\\the coefficients X and Y at the cusp rho.
\\Note that whenever I call Y[i+1] or X[i+1] that this corresponds
\\to the coefficient of q^i since PARI indexes starting at 1 and not 0.
for(n=1,num_of_terms-1,
RHS = w*(2*sum(i=1,n,Y[n-i+1]*C[i+1]) + A1*sum(i=1,n,X[n-i+1]*C[i+1])
                                                    +A3*C[n+1]);
X[n+1] = RHS/n;
RHS = sum(i=0,n,sum(j=0,n-i,X[n-i-j+1]*X[i+1]*X[j+1])) +
```

```
                                A2*sum(i=0,n,X[n-i+1]*X[i+1])+A4*X[n+1];
Y[n+1]=(RHS-sum(i=1,n-1,Y[n-i+1]*Y[i+1])
            -A1*sum(i=1,n,Y[n-i+1]*X[i+1]))/(2*Y[0+1]+A1*X[0+1]+A3);
); \\ This ends the for loop
return([X,Y]);}; \\ This ends the function.
```

The following solves the system $ax + by = c, dx + ey = f$ if the system is consistent.

```
solver(a,b,c,d,e,f) = {
return([(e*c-b*f)/(a*e-b*d),(f*a-c*d)/(a*e-b*d)])};
```

This function gives the isomorphism from the Weierstrass short form to the general Weierstrass equation.

```
get_iso(E) =
{
s = -E.a1/2;
r = (s^2-E.a2+s*E.a1)/3;
t = (-E.a3 - r*E.a1)/2;
a2p = E.a2 + 1/4*E.a1^2;
a4p = E.a4 + 1/2*E.a1*E.a3;
a6p = E.a6 + 1/4*E.a3^2;
a4pp = a4p-1/3*a2p^2;
a6pp = a6p + 2/27*a2p^3 - 1/3*a2p*a4p;
E_short = ellinit([a4pp,a6pp]);
u = bestappr((E_short.disc/E.disc)^(1/12));
return([u,r,s,t]);
};
```

This function is the analog of the function `expansion_at_cusp_no_pole` if there is a pole at the cusp ρ.

```
expansion_at_cusp_pole(E,num_of_terms,Gamma) =
{
\\initial setup stuff
\\elliptic curve coefficients
A1 = E.a1; A2 = E.a2; A3 = E.a3; A4 = E.a4;A6 = E.a6;
X= vector(num_of_terms+4,i,0);
Y= vector(num_of_terms + 3,i,0);
mf = mffromell(E)[1];
nf = mffromell(E)[2];
N = mf[1][1]; \\this is the conductor of the curve E
width = N/(gcd(N,Gamma[2,1]^2)); \\this is the standard formula
C = mfslashexpansion(mf,nf,Gamma,num_of_terms+10,0,&P);
C = width*C;
\\this next part is getting the initial seed values to start the
\\iterative process
C_integrated = C;
for(i=2,#C_integrated, C_integrated[i] = C_integrated[i]/(i-1));
\\the minus one is because PARI starts indexing its lists at 1 and not 0.
\\That's also why we start at i = 2, (nf is a newform)

q_expansion_E = Ser(C_integrated,q)+O(q^10);
\\ the O(q^10) is so that evaluating wp at this series is fast.
[X_series,Y_series] = ellwp(E,q_expansion_E,1);
\\stuffing the integrated q_series into the weierstrass p function

\\isomorphism to the normal form of E and not the weierstrass short form
```

```
[u,r,s,t] = get_iso(E);
Y_series = Y_series/2;
Y_series  = u^3*Y_series + s*u^2*X_series+t;
X_series = u^2*X_series+r;
for(i=-3,5, X[i+4] = polcoef(X_series,i); Y[i+4] = polcoef(Y_series,i););

\\this for loop will fill the rest of X and Y via the recurrence relation.
\\We will calculate values of a,b,c,d,e,f,g,h
\\so that the solutions to ax+b = cy + d and ex+f = gy+h for
\\x and y are the q^k X coefficient and the q^{k-1} Y coefficient

for(k=5,num_of_terms,
\\ first linear relation from differential equation, qX' = (2Y+a1X+a3)f*w
[a,c] = [k,2*C[1+1]];
b = 0;
d = 2*sum(i=-3,k-2,C[k-i+1]*Y[i+4]) + A1*sum(i=-3,k-1,C[k-i+1]*X[i+4])
                                                    + A3*C[k+1];

\\ second linear relation from elliptic curve
\\Y^2 + a1XY + a3Y = X^3 + a2X^2 + a4X + A6.
[e,g] = [3*X[-2+4]^2,2*Y[-3+4]];
h = sum(i=-2,k-2,Y[k-4-i+4]*Y[i+4]) + A1*sum(i=-3,k-2,X[k-4-i+4]*Y[i+4])

                                                    +A3*Y[k-4+4];
```

```
f = X[-2+4]*sum(j=-1,k-1,X[k-2-j+4]*X[j+4]) +
    sum(i=-1,k-1,sum(j=-2,k-2-i,X[k-4-i-j+4]*X[j+4]*X[i+4]))+
                        A2*sum(i=-2,k-2,X[k-4-i+4]*X[i+4])+A4*X[k-4+4];
[new_x,new_y] = solve_2_system(a,b,c,d,e,f,g,h);
X[k+4] = new_x;
Y[k-1+4] = new_y;
); \\ end of the for loop
return([X,Y]);
};
```

The following is the sum formula for $\wp(z+y)$. This is mostly used when z is a complex number and y is a power series centered at the origin. If the indicator is 1 then this returns both $\wp$ and the derivative $\wp$' evaluated at $z+y$. Note that we can't have $z=y$ or else the formula we use is invalid.

```
wp_addition(E,z,y,indicator) =
{
[wpz,wppz] = ellwp(E,z,1);
[wpy,wppy] = ellwp(E,y,1);
lambda = (wppz-wppy)/(wpz-wpy);
wpzy = 1/4*lambda^2 - wpz-wpy;
if(indicator != 1, return(wpzy),
wppzy = -1*lambda*wpzy + (wpy*wppz-wpz*wppy)/(wpz-wpy);
return([wpzy,wppzy]););
}
```

This is the "point of order 2" case described in section 2.2. The only difference between this function and `expansion_at_cusp_no_pole` is that the recurrence relation ischanged

to reflect that we need to take `(2Y[1]+A1*X[1]+A3) == 0` as a hypothesis. Here `const` is the preimage in Λ_E of the point of order 2 given as the constant terms in $X(z)$ and $Y(z)$. This is something that's going to be calculated already and so it saves time to just pass this in as a variable.

```
expansion_at_cusp_order_2(E,num_of_terms,Gamma,const) =
{
A1 = E.a1;A2 = E.a2;A3 = E.a3;A4 = E.a4;A6 = E.a6;
X= vector(num_of_terms+1,i,0);
Y = vector(num_of_terms,i,0);
mf = mffromell(E)[1];
nf = mffromell(E)[2];
C = mfslashexpansion(mf,nf,Gamma,num_of_terms+5,0,&P);
N = mf[1][1]; \\conductor of E
width = N/(gcd(N,Gamma[2,1]^2)); \\ this is the standard formula
C = width*C; C_integrated = C; for(i=2, #C, C_integrated[i]
                                          = C_integrated[i]/(i-1));

\\using the wp function and wp_addition formulas to get initial values
\\so we can start the iteration. PARI currently doesn't allow you to
\\evaluate wp at a series expansion away from zero.
[wp,wpp] = wp_addition(E,Ser(C_integrated,q)+O(q^(10)),const,1);
\\this changes the curve to elliptic form
[u,r,s,t] = get_iso(E);
wpp = wpp/(2);
wpp = u^3*wpp + s*u^2*wp + t; \\isomorphism formulas for general form
wp = u^2*wp+r;
```

```
for(i=0,5, X[i+1] = polcoef(wp,i); Y[i+1] = polcoef(wpp,i););
\\this will now be the recursive step that solves a 2x2 system for
\\the kth coefficient of X and the k-1th coefficient of Y.
for(k=6,num_of_terms,
\\ differential equation relation
[a,c] = [k,2*C[1+1]];
b=0;
d = 2*sum(n=1,k-2,C[k-n+1]*Y[n+1])+A1*sum(n=1,k-1,C[k-n+1]*X[n+1]);
\\elliptic curve relation
[e,g] = [3*X[0+1]^2+2*A2*X[0+1]+A4-A1*Y[0+1],2*Y[1+1]+A1*X[1+1]];
h = sum(n=2,k-2,Y[k-n+1]*Y[n+1]) + A1*sum(n=1,k-2,X[k-n+1]*Y[n+1]);
f = X[0+1]*sum(m=1,k-1,X[k-m+1]*X[m+1])
              +sum(n=1,k-1,sum(m=0,k-n,X[k-m-n+1]*X[m+1]*X[n+1]))
                                  +A2*sum(n=1,k-1,X[k-n+1]*X[n+1]);
[new_x,new_y] =  solve_2_system(a,b,c,d,e,f,g,h);
X[k+1] = new_x;
Y[k-1+1] = new_y; ); \\end for loop
return([X,Y]);
};
```

Bibliography

[1] Amod Agashe, Kenneth Ribet, and William A. Stein. The manin constant. *Pure and Applied Mathematics Quarterly*, 2(2):617, 2006.

[2] Claudia Alfes, Michael Griffin, Ken Ono, and Larry Rolen. Weierstrass mock modular forms and elliptic curves. *Res. Number Theory*, 1:Art. 24, 31, 2015.

[3] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor. On the modularity of elliptic curves over $\mathbf{q}$: wild 3-adic exercises. *Journal of the American Mathematical Society*, 14(4):843, 2001.

[4] J. E. Cremona. *Algorithms for modular elliptic curves.* Cambridge University Press, Cambridge, 1992.

[5] Martin Eichler. Quaternäre quadratische formen und die riemannsche vermutung für die kongruenzzetafunktion. *Archiv der Mathematik*, 5:355, 1954.

[6] Neal Koblitz. *Introduction to elliptic curves and modular forms.* Graduate Texts in Mathematics, 97. Springer-Verlag, New York, 1993.

[7] Lisa Kodgis. Zeros of the modular parameterization of rational elliptic curves. *Thesis submitted to the University of Hawai'i*, 2011.

[8] V. A. Kolyvagin. Finiteness of $E(\mathbf{Q})$ and $\mathrm{Sha}(E, \mathbf{Q})$ for a subclass of Weil curves. *Izv. Akad. Nauk SSSR Ser. Mat.*, 52(3):522–540, 670–671, 1988.

[9] Sarah Peluse. On zeros of eichler integrals. *Archiv der Mathematik*, 102(1):71, 2014.

[10] Goro Shimura. Correspondances modulaires et les fonctions ζ de courbes algébriques. *Journal of the Mathematical Society of Japan*, 10:1, 1958.

[11] Joseph H. Silverman. *The arithmetic of elliptic curves.* Graduate Texts in Mathematics, 106. Springer, Dordrecht, 2009.

[12] William Stein. *Modular forms, a computational approach.* Graduate Studies in Mathematics, 79. American Mathematical Society, Providence, RI, 2007.

[13] Andrew Wiles. Modular elliptic curves and fermat's last theorem. *Annals of Mathematics. Second Series*, 141(3):443, 1995.