UNIVERSITY OF CALIFORNIA SAN DIEGO

p-adic Integration on Modular Curves and Code-Based Cryptography

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

in

Mathematics

by

Jun Bo Lau

Committee in charge:

Professor Kiran Kedlaya, Chair
Professor Russell Impagliazzo
Professor Jonathan Novak
Professor Cristian Popescu
Professor Claus Sorensen

2023

The dissertation of Jun Bo Lau is approved, and it is acceptable in quality and form for publication on microfilm and electronically:

Chair

University of California San Diego

2023

EPIGRAPH

A careful quotation

conveys brilliance.

—Smarty Pants

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

Thanks to whoever deserves credit for Blacks Beach, Porters Pub, and every coffee shop in San Diego.

Thanks also to hottubs.

VITA

2017	M.Math University of Warwick, U.K.
2017-2023	Graduate Teaching Assistant, University of California, San Diego
2023	Ph. D. in Mathematics, University of California, San Diego

ABSTRACT

In this dissertation, we study two problems arising from arithmetic geometry.

Falting's theorem states that there are only finitely many rational points on curves of genus greater than 1. However, an explicit determination of all such points on a curve remains a hard problem. There are various approaches to computing rational points on higher genus curves and we use Coleman's theory of p-adic line integrals to study a particular class of curves with rich arithmetic origins, namely, the modular curves. In join work with Chen and Kedlaya, we implement a new algorithm that does not use the models of the modular curves and illustrate this method through the computation of several examples.

On the other hand, in anticipation of the development of powerful quantum computers in the next few decades, we study cryptosystems that rely on the hardness of certain number theoretical problems. In particular, we investigate BIKE, a cryptosystem presented as one of the candidates for the National Institute of Standards and Technology Post-Quantum Cryptography Standardization Process. We identified several factors that affect the security of the code-based cryptosystem as a potential quantum-attack-resistant candidate for real world applications through extensive simulations.

Part I

Coleman Integration on Modular Curves

Chapter 1

Preliminaries

All curves in this paper are smooth, projective and geometrically irreducible with good reduction at a prime p.

1.1 Introduction

Some of the oldest questions in number theory can be reformulated in modern terms: given a finite list of polynomials, what are the integer or rational solutions to this set of equations? In fact, these solutions can be viewed as integer or rational solutions of geometric objects – curves, surfaces or higher dimensional objects.

In this project, we focus on the case of curves. A remarkable result, formulated by Mordell in 1922 and proved by Faltings in 1983, states that for curves of higher genus, there are only finitely many rational points on them.

Theorem 1.1.1. *(Mordell's conjecture/ Faltings's theorem) Let $X/\mathbb{Q}$ be a curve of genus $g \geq 2$, then the set of rational points $X(\mathbb{Q})$ is finite.*

However, Faltings's proofs are not effective, i.e., there is no way of explicitly determining the complete set of rational points on the curve. Before Faltings, Chabauty developed a method in this direction with the condition that if the rank of the Jacobian of the curve is strictly less than the genus, then one could compute this set of points. In [Col85b, Col85a] Coleman defined p-adic line integrals and re-interpreted Chabauty's method to explicitly compute the set of rational points. These Coleman integrals provide an effective method to problems in arithmetic geometry, including but not limited to, torsion points on Jacobians of curves (Manin-Mumford conjecture), p-adic heights on curves, p-adic polylogarithms, Mordell conjecture (rational points), etc. In [BD18, BD17], Balakrishnan and Dogra developed quadratic Chabauty as a computational tool to study the set of rational points as long as the curve satisfies a certain quadratic Chabauty bound, involving the rank of the Jacobian, genus and Néron-Severi rank of the Jacobian.

There are several approaches to numerically compute these Coleman integrals. Wetherell [Wet97] combined the certan properties of Coleman integrals and the arithmetic of the Jacobian to compute $\int_D \omega$, where D is a divisor in the Picard group and ω is a holomorphic differential on the curve. The next approach relies on computing the Frobenius action in p-adic cohomology following Dwork's principle of analytic continuation along the Frobenius [BBK10, Tui16, Tui17, BT20]. However, both of these approaches have their shortcomings – Wetherell's method requires an explicit divisor in order to reduce the computation to a power series integration ("tiny integrals") and the second method requires an explicit equation of the curves as input.

We turn our attention to computing Coleman integrals on modular curves. The set of rational points on modular curves has special arithmetic meaning. For instance, the set of rational points $X_0(N)(\mathbb{Q})$ correspond to the torsion points of elliptic curves (Mazur's theorem). Another motivation to study modular curves comes from Serre's Uniformity Conjecture. Let E be an elliptic curve defined over K. The group of p-torsion points $E[p](\bar{K})$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^2$ and is acted upon by the absolute Galois group $\mathrm{Gal}(\bar{K}/K)$, giving rise to a representation $\rho_{p,E} : \mathrm{Gal}(\bar{K}/K) \to \mathrm{GL}_2(\mathbb{F}_p)$. In [Ser72], Serre proved the following:

Theorem 1.1.2. *Suppose that E does not have complex multiplication. Then there exists a number $N(E)$ such that $\rho_{p,E}$ is surjective for all $p > N(E)$.*

In the same paper, he posed the following question:

Conjecture 1.1.3. (Serre's Uniformity Conjecture) Given a number field K, then there exist a constant $N_K > 0$ such that for any elliptic curve E defined over K without complex multiplication, the corresponding Galois representation $\rho_{p,E}$ is surjective for all primes $p > N_K$.

Since modular curves parametrise elliptic curves with torsion data, this can be formulated in terms of rational points on modular curves:

Conjecture 1.1.4. (Serre's Uniformity Conjecture) Let $H \leq \mathrm{GL}_2(\mathbb{F}_p)$ be a proper subgroup such that the determinant map $\det : H \to \mathbb{F}_p^\times$ is surjective, then there exist a constant $N_K > 0$ such that for any prime $p > N_K$, the associated modular curve $X_H(p)$ has K-rational points coming only from cusps and elliptic curves with complex multiplication.

If $\rho_{p,E}$ is not surjective, the image lies inside some maximal proper subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$. Therefore, one could prove the conjecture by showing that for p large enough, the image of $\rho_{p,E}$ does not lie in any maximal subgroup. The classification of maximal subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$ is known, originally due to [Dic]:

Theorem 1.1.5. *Let $H \leq \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ not containing $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$. Up to conjugacy, H is one of the following:*

- *(Borel) $H \subseteq B_0(p) = \{\left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right)\}$*
- *(Normaliser of split Cartan) $H \subseteq N_s^+(p) = \{\left(\begin{smallmatrix} \alpha & 0 \\ 0 & \beta \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & \alpha \\ \beta & 0 \end{smallmatrix}\right) : \alpha, \beta \in \mathbb{F}_p^\times\}$*
- *(Normaliser of non-split Cartan) $H \subseteq N_s^+(p) = \{\left(\begin{smallmatrix} \alpha & 0 \\ 0 & \alpha^p \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & \alpha \\ \alpha^p & 0 \end{smallmatrix}\right) : \alpha \in \mathbb{F}_{p^2}^\times\}$*
- *(Exceptional) The image of H in $\mathrm{PGL}_2(\mathbb{F}_p)$ is isomorphic to A_4, S_4 or A_5.*

Most of the cases have been resolved [Maz78, BPR13, BP11, Ser72], except for the normaliser of non-split Cartan. There has been some progress using quadratic Chabauty to find the rational points of the modular curve corresponding to the nonsplit Cartan of level 13 [BDM$^+$19] and level 17 [BDM$^+$21].

Since most modular curves satisfy the quadratic Chabauty bound [Sik17], we provide a model-free algorithm to compute Coleman integrals on modular curves arising arising from Serre's Uniformity Conjecture.

1.2 Background

1.2.1 Modular forms

In this section, we give a brief introduction of modular forms, following [DS05].

Let $\mathbb{H} := \{\tau \in \mathbb{C} : Im(\tau) > 0\}$ be the upper half complex plane. The special linear group $\mathrm{SL}_2(\mathbb{Z})$ acts on $\mathbb{H}$ via fractional linear transformations:

$$\gamma \cdot \tau = \frac{a\tau + b}{c\tau + d}$$

where $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right), \tau \in \mathbb{H}$.

Definition 1.2.1. Let $f : \mathbb{H} \to \mathbb{C}$ be a function and $k \in \mathbb{Z}$.

- The *automorphy factor* is a function

$$\begin{aligned} j : \mathrm{GL}_2^+(\mathbb{R}) \times \mathbb{H} &\to \mathbb{C} \\ (\gamma, z) &\mapsto cz + d \end{aligned}$$

  where $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$.

- The *weight-k slash operator* is defined as

$$\begin{aligned} (\,\cdot\,)|_k(\,\cdot\,) : \mathrm{Hom}(\mathbb{H}, \mathbb{C}) \times \mathrm{GL}_2^+(\mathbb{R}) &\to \mathrm{Hom}(\mathbb{H}, \mathbb{C}) \\ (f(z), \gamma) &\mapsto (f|_k\gamma)(z) := (\det \gamma)^{k-1} j(\gamma, z)^{-k} f(\gamma \cdot z). \end{aligned}$$

The automorphy factory satisfies a cocycle relation $j(\gamma_1\gamma 2, z) = j(\gamma_1, \gamma_2 z) j(\gamma_2, z)$ which implies that $\mathrm{GL}_2^+(\mathbb{R})$ acts on $\mathrm{Hom}(\mathbb{H}, \mathbb{C})$ via $f|_k\gamma_1\gamma_2 = (f|_k\gamma_1)|_k\gamma_2$.

Consider the projection map $\pi : \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. We define congruence subgroups in the following way.

Example 1.2.2. Here are some common examples of preimages of π:

- $\Gamma(N) = \pi^{-1}((\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix})) = \{(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}) \in \mathrm{SL}_2(\mathbb{Z}) : (\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}) \equiv (\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}) \pmod N\}$.
- $\Gamma_1(N) = \pi^{-1}(\{(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix})\}) = \{(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}) \in \mathrm{SL}_2(\mathbb{Z}) : (\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}) \equiv (\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}) \pmod N\}$.
- $\Gamma_0(N) = \pi^{-1}(\{(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix})\}) = \{(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}) \in \mathrm{SL}_2(\mathbb{Z}) : (\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}) \equiv (\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}) \pmod N\}$.

Definition 1.2.3. $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ is a *congruence subgroup* if there exists an integer $N \geq 1$ such that $\Gamma(N) \leq \Gamma$. The minimal such N is called the *level* of Γ.

It follows immediately that congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$ have finite index and correspond to subgroups of $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. The above examples are all congruence subgroups of level N.

Definition 1.2.4. Let $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ be a congruence subgroup of level N, $k \geq 0$ an integer. We say a function $f : \mathbb{H} \to \mathbb{C}$ is a *modular form of weight k with level* Γ if

1. f is holomorphic,
2. f is weight-k invariant under Γ, i.e., $f|_k\gamma = f$ for all $\gamma \in \Gamma$,
3. $f|_k\alpha$ is holomorphic at ∞ for all $\alpha \in \mathrm{SL}_2(\mathbb{Z})$, i.e., $(f|_k\alpha)(z)$ is bounded as $z \to i\infty$.

If, in addition, $f|_k\alpha$ vanishes at infinity for all $\alpha \in \mathrm{SL}_2(\mathbb{Z})$, we say that f is a *cusp form*. We denote the set of weight-k modular forms with respect to Γ (resp. cusp forms) as $\mathscr{M}_k(\Gamma)$ (resp. $\mathscr{S}_k(\Gamma)$).

Suppose f is a modular form of weight k with level Γ. Since Γ is a congruence subgroup, $\left(\begin{smallmatrix}1 & h\\ 0 & 1\end{smallmatrix}\right) \in \Gamma$ for some minimal integer $h \geq 1$, this integer is the *width* of the cusp ∞. Since a modular form satisfies $f|_k\gamma = f$ for $\gamma \in \Gamma$, we have $(f|_k\left(\begin{smallmatrix}1 & h\\ 0 & 1\end{smallmatrix}\right))(z) = f(z+h) = f(z)$, so $f(z)$ is $h\mathbb{Z}$-periodic and admits a Fourier expansion $f(\tau) = \sum_{n=0}^{\infty} a_n q_h^n$ where $q_h = \exp(2\pi i\tau/h)$. The third condition of modular forms implies that the Fourier expansion begins at index 0 and cusp forms satisfy $a_0 = 0$.

Example 1.2.5. Let $G_k(\tau) = \sum_{(c,d)\neq(0,0)} 1/(c\tau+d)^k$. This is a modular form of weight k for $\mathrm{SL}_2(\mathbb{Z})$ called *Eisenstein series*.

The *j-invariant* is a modular form of weight 0, i.e., a modular function and an element of $\mathbb{C}(X(\mathrm{SL}_2(\mathbb{Z})))$, with q-expansion:

$$j : \mathbb{H} \to \mathbb{C}, j(\tau) = 1728\frac{(60G_4(\tau))^3}{(60G_4(\tau))^3 - 27(140G_6(\tau))^2} = \frac{1}{q} + 744 + 196884q + \dots.$$

It is a standard result that $\mathscr{M}_k(\Gamma) \supseteq \mathscr{S}_k(\Gamma)$ are finite dimensional complex vector spaces. Modular forms and modular curves are related by the fact that there is an isomorphism between the space of weight 2 cusp forms and the space of holomorphic differentials on the modular curve $X(\Gamma)$.

$$\mathscr{S}_2(\Gamma) \xrightarrow{\cong} H^0(X(\Gamma), \Omega^1)$$
$$f(\tau) \mapsto f(\tau)d\tau.$$

1.2.2 Modular curves

In this section, we define our object of study. Modular curves have rich structures as Riemann surfaces, algebraic curves and moduli spaces of elliptic curves (with some torsion information). We frequently use properties from various perspectives interchangeably.

As Riemann surfaces

Let $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ be a subgroup of finite index. $\mathbb{H}$ inherits the Euclidean topology from $\mathbb{C}$ and so $Y(\Gamma) := \Gamma\backslash\mathbb{H}$ carries the quotient topology that is Hausdorff. $Y(\Gamma)$ can be compactified by adjoining cusps, which are orbits of $\mathbb{P}^1(\mathbb{Q})$ under the action of Γ. The resulting quotient space $X(\Gamma) := \Gamma\backslash\mathbb{H}^*$ where $\mathbb{H}^* := \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$ is called the modular curve associated to Γ. One could further show that by considering elliptic points and cusps, one can choose suitable charts, therefore giving $Y(\Gamma)$ and $X(\Gamma)$ the structure of Riemann surface.

This approach allows us to use techniques from Riemann surfaces, e.g., genus/ramification theory, Riemann-Hurwitz formula, Riemann-Roch, etc. to study modular curves.

As algebraic curves

For a finite index subgroup $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$. The associated modular curve $X(\Gamma)$ has the structure of a compact Riemann surface. Compact Riemann surfaces and complex algebraic curves are equivalent notions [For81]. Note that we are also considering modular curves where the determinant map on the subgroup $H \leq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ is surjective. By Theorem 7.6.3 in [DS05], these algebraic curves are in fact defined over $\mathbb{Q}$. We have a Galois-theoretic correspondence between curves and their function fields:

Theorem 1.2.6. *(Curves-Fields Correspondence) For any field k, there is a bijection:*

$$\{C/k \textit{ smooth projective algebraic curves}\}/\cong \leftrightarrow \{K/k \textit{ function field extensions over } k\}/\sim$$

$$C \mapsto k(C)$$

Furthermore, this is contravariant: a nonconstant morphism from algebraic curves C to C' over k corresponds to a field morphism from $k(C')$ to $k(C)$.

The above theorem allows us to work with simpler objects, i.e., we can replace curves and their morphisms by fields and field injections. In particular, the function field of the modular curve $X(\Gamma)$ consists of modular functions of weight 0 and level Γ.

As moduli spaces of elliptic curves

For each $\tau \in \mathbb{H}$, one could associate it with a lattice $\Lambda_\tau := \mathbb{Z} + \tau \cdot \mathbb{Z} \subseteq \mathbb{C}$. The resulting quotient space $\mathbb{C}/\Lambda_\tau$ is a compact Riemann surface of genus 1, an elliptic curve. Conversely, for any elliptic curve, as a genus 1 compact Riemann surface, the homology group of the elliptic curve $H_1(E, \mathbb{Z})$ is generated by two loops, γ_1, γ_2. For an invariant differential ω of the elliptic curve, we can construct the lattice generated by the periods $\Lambda_E = (\int_{\gamma_1} \omega) \cdot \mathbb{Z} + (\int_{\gamma_2} \omega) \cdot \mathbb{Z}$. This can be renormalised so that $\Lambda_E = \mathbb{Z} + \tau \cdot \mathbb{Z}$ with $\tau = (\int_{\gamma_1} \omega)/(\int_{\gamma_2} \omega) \in \mathbb{H}$. In particular the points on $\mathbb{H}$ correspond to elliptic curves.

For $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$, the modular curve $X(\Gamma)(\bar{\mathbb{Q}})$ parametrise elliptic curves with some torsion data, i.e., a pair (E, ϕ) where E is an elliptic curve defined over $\bar{\mathbb{Q}}$ and ϕ is an isomorphism of its N-torsion points $\phi : E[N] \to (\mathbb{Z}/N\mathbb{Z})^2$. Two points $(E_1, \phi_1), (E_2, \phi_2)$ are isomorphic if there is an isomorphism of elliptic curves $\psi : E_1 \to E_2$ and some matrix $M \in \Gamma$ such that the diagram commutes:

$$
\begin{array}{ccc}
E_1[N] & \xrightarrow{\phi_1} & (\mathbb{Z}/N\mathbb{Z})^2 \\
\Big\downarrow \psi & & \Big\downarrow M \\
E_2[N] & \xrightarrow{\phi_2} & (\mathbb{Z}/N\mathbb{Z})^2.
\end{array}
$$

Furthermore, there is an action of the absolute Galois group $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ on (E,ϕ) and we say that (E,ϕ) is a $\mathbb{Q}$-rational point if it is invariant under the action. We can view points on modular curves as elliptic curves with certain torsion structures which allows us to apply properties of elliptic curves to study the rational points on $X(\Gamma)$.

Example 1.2.7. Let $H \leq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ be a subgroup such that

- $-I \in H$,
- the determinant map $\det : H \to (\mathbb{Z}/N\mathbb{Z})^\times$ is surjective.

Then for an integer $N \geq 1$, we have the congruence subgroup $\Gamma_H(N) = \{A \in \mathrm{SL}_2(\mathbb{Z}) : A \pmod{N} \in H\}$, which gives rise to the modular curves $X_H := X(\Gamma_H(N))$.

Following Example 1.2.2, the corresponding modular curves parametrise:

- $X(N) := X(\Gamma(N))$ consists of $(E,(P,Q))$ an elliptic curve and a pair of points generating the N-torsion subgroup of E.
- $X_1(N) := X(\Gamma_1(N))$ consists of (E,Q) an elliptic curve and a point of order N.
- $X_0(N) := X(\Gamma_0(N))$ consists of (E,C) an elliptic curve and a cyclic subgroup of order N.

1.2.3 Hecke operators

We begin with the definition of Hecke operators as operators on spaces of modular forms. These are used in conjunction with spectral theory to show that the inner product space of modular forms contains a basis of modular forms that are eigenvectors under the Hecke operators $\{T_p\}_p$. Hecke operators are defined on modular forms and modular curves. We use both the transcendental and algebraic/geometric definitions of Hecke operators in our algorithm.

Definition 1.2.8. Let Γ_1, Γ_2 be congruence subgroups of $SL_2(\mathbb{Z})$ and $\alpha \in GL_2^+(\mathbb{Q})$.

- We define the *double coset* $\Gamma_1 \alpha \Gamma_2$ as the set

$$\Gamma_1 \alpha \Gamma_2 := \{\gamma_1 \alpha \gamma_2 : \gamma_1 \in \Gamma_1, \gamma_2 \in \Gamma_2\}$$

- This gives rise to the *double coset operators*:

$$\begin{aligned}(\,\cdot\,)|_k[\Gamma_1 \alpha \Gamma_2] : \mathscr{M}_k(\Gamma_1) &\to \mathscr{M}_k(\Gamma_2) \\ f(\tau) &\mapsto f|_k \Gamma_1 \alpha \Gamma_2 := \sum_i f|_k \beta_i\end{aligned}$$

  where $\Gamma_1 \alpha \Gamma_2 = \bigcup_i \Gamma_1 \beta_i$ is a (finite) disjoint coset decomposition that does not depend on the choice of decomposition. This map restricts to an operator on the space of cusp forms $(\,\cdot\,)|_k[\Gamma_1 \alpha \Gamma_2] : \mathscr{S}_k(\Gamma_1) \to \mathscr{S}_k(\Gamma_2)$.

We follow the approach [Ass20] to define Hecke operators.

Definition 1.2.9. Fix a congruence subgroup Γ with $\bar{\Gamma} \leq SL_2(\mathbb{Z}/N\mathbb{Z})$. Let $\alpha \in M_2(\mathbb{Z})$ such that $\det(\alpha) \in \det(\bar{\Gamma})$ and $\alpha \pmod N \in \bar{\Gamma}$. We define the Hecke operator as

$$T_p = T_\alpha = (\,\cdot\,)|_k[\Gamma\alpha\Gamma]$$

Example 1.2.10. ([DS05] Prop. 5.2.1) The theory of Hecke operators can be made explicit for certain congruence subgroups. The Hecke operator $T_p = [\Gamma_1(N)\left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right)\Gamma_1(N)]_k$ on $\mathscr{M}_k(\Gamma_1(N))$ has the following formulae:

$$T_pf = \begin{cases} \sum_{i=0}^{p-1} f|_k\begin{pmatrix}1&j\\0&p\end{pmatrix}, & \text{if } p|N, \\ \sum_{i=0}^{p-1} f|_k\begin{pmatrix}1&j\\0&p\end{pmatrix} + f|_k(\left(\begin{smallmatrix}m&n\\N&p\end{smallmatrix}\right)\left(\begin{smallmatrix}p&0\\0&1\end{smallmatrix}\right)), & \text{if } p \not| N, \text{ where } mp-nN=1. \end{cases}$$

There is also an algebraic/geometric interpretation of the double coset operator as a morphism of divisor groups. For Γ_1, Γ_2 congruence subgroups, $\alpha \in GL_2^+(\mathbb{Q})$, $\Gamma_3 := \alpha^{-1}\Gamma_1\alpha \cap \Gamma_2$ and $\Gamma_3' := \alpha\Gamma_3\alpha^{-1}$. Since points on the modular curve $X(\Gamma)$ have the form $\Gamma\tau$, we have a diagram at the level of groups which induces a diagram on modular curves:

$$\Gamma_2 \hookleftarrow \Gamma_3 \xrightarrow{\cong} \Gamma_3' \hookrightarrow \Gamma_1$$
$$X_2 \xleftarrow{\pi_2} X_3 \xrightarrow{\cong} X_3' \xrightarrow{\pi_1} X_1$$

Suppose $\Gamma_3/\Gamma_2 = \bigcup_j \Gamma_3\gamma_{2,j}$ and $\beta_j = \alpha\gamma_{2,j}$. Then the double coset operator induces a map on the divisor groups after $\mathbb{Z}$-linear extension:

$$\begin{aligned} \mathrm{Div}(X_2) &\to \mathrm{Div}(X_1) \\ \Gamma_2\tau &\mapsto \sum_j \Gamma_1\beta_j\tau \end{aligned}$$

Specialising to the case of Hecke operator, we obtain a similar diagram.

We could benefit from the moduli interpretation of modular curves for the case of Hecke operators by defining it as a correspondence. For $H \leq GL_2(\mathbb{Z}/N\mathbb{Z})$ and p coprime to N, we obtain the modular curve X_H and its fiber product $X_H(p) := X_0(p) \times_{X(1)} X_H$. There are two degeneracy maps $\alpha, \beta : X_H(p) \to X_H$ defining the Hecke operator at p where one forgets the cyclic group of order p and the other quotients out by the cyclic group of order p.

$$\begin{tikzcd} & X_H(p) \arrow[dl, "\alpha"'] \arrow[dr, "\beta"] & \\ X_H \arrow[rr, dashed] & & X_H \end{tikzcd}$$

By Picard functoriality, for a point $(E, \mathfrak{n}) \in X_H$ where the level structure $\mathfrak{n}$ is determined by H, we have an algebraic description of the Hecke operator at p:

$$T_p(E, \mathfrak{n}) := \alpha^* \beta_* (E, \mathfrak{n}) = \sum_{f: E \to E', deg(f) = p} (E', f(\mathfrak{n})).$$

1.2.4 Coleman integrals

Coleman's construction of p-adic line integrals share many similar properties as their complex-analytic analogue. Below we record some properties of Coleman integrals from [CdS88, Col85c] that will be used in our calculations.

Theorem 1.2.11. *Let $X/\mathbb{Q}_p$ be a smooth, projective, and geometrically irreducible curve with good reduction at p, let J be the Jacobian of X.Then there is a p-adic integral*

$$\int_P^Q \omega \in \overline{\mathbb{Q}}_p$$

with $P, Q \in X(\overline{\mathbb{Q}}_p), \omega \in H^0(X, \Omega^1)$ satisfying:

1. *The integral is $\overline{\mathbb{Q}}_p$ linear in ω,*
2. *We have additivity of endpoints:*

$$\int_P^Q \omega = \int_P^R \omega + \int_R^Q \omega,$$

3. $$\int_P^Q \omega + \int_{P'}^{Q'} \omega = \int_P^{Q'} \omega + \int_{P'}^Q \omega$$

   Thus, we can define $\int_D \omega$, where $D \in Div_X^0(\overline{\mathbb{Q}}_p)$. Also, if D is principal, $\int_D \omega = 0$,

4. *There is an open subgroup of $J(\mathbb{Q}_p)$ such that $\int_P^Q \omega$ can be computed in terms of power series in some uniformiser by formal term-by-term integration. In particular, $\int_P^P \omega = 0$,*
5. *The integral is compatible with the action of $Gal(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$. In particular, if $P, Q \in X(\mathbb{Q}_p)$ then $\int_P^Q \omega \in \mathbb{Q}_p$.*

6. *Let* $P_0 \in X(\overline{\mathbb{Q}}_p)$ *be fixed and* $\omega \neq 0$*. Then the set of* $P \in X(\overline{\mathbb{Q}}_p)$ *reducing to* $X(\overline{\mathbb{F}}_p)$ *such that* $\int_{P_0}^{P} \omega = 0$ *is finite,*

7. *If* $U \subseteq X, V \subseteq Y$ *are wide open subspaces of the rigid analytic spaces* X, Y*,* ω *a 1-form on* V*, and* $\phi : U \to V$ *a rigid analytic map, then we have the change of variables formula:*

$$\int_P^Q \phi^* \omega = \int_{\phi(P)}^{\phi(Q)} \omega,$$

8. *We have an analogue of the Fundamental Theorem of Calculus:* $\int_P^Q df = f(Q) - f(P)$*,*

Definition 1.2.12. The Coleman integral $\int_P^Q \omega$ is called a *tiny integral* if P and Q reduce to the same point in $X_{\mathbb{F}_p}(\overline{\mathbb{F}}_p)$, i.e., they lie in the same residue disc.

Explicitly, if P and Q are in the same residue disc, then the differential form can be expressed as a power series in terms of a uniformiser at P. The tiny integral can be computed by formally integrating the power series and evaluated at the endpoints:

$$\int_P^Q \omega = \int_{t(P)}^{t(Q)} \omega(t) = \int_{t(P)}^{t(Q)} \sum a_i t^i dt = \sum \frac{a_i}{i+1} (t(Q) - t(P))^{i+1}.$$

Coleman's construction is suitable for computations. In [BBK10], the authors demonstrated an algorithm to compute single Coleman integrals for hyperelliptic curves. Their method is based on Kedlaya's algorithm for computing the Frobenius action on the de Rham cohomology of hyperelliptic curves [Ked01] and this is generalized to arbitrary smooth curves [BT22, Tui16, Tui17]. Despite recent developments in this direction, the current implementations require nice affine plane models for the curves as inputs. Since modular curves tend to have large gonality, such models are not readily available and are often bottlenecks in existing algorithms.

Chapter 2

Coleman Integration on Modular Curves

In this section, we introduce an algorithm that computes single Coleman integrals on modular curves. The modular curves in consideration have congruence subgroups $\Gamma_H \leq SL_2(\mathbb{Z})$ where $H \leq GL_2(\mathbb{Z}/N\mathbb{Z})$ and

- $-I \in H$,
- $\det : H \to \mathbb{Z}/N\mathbb{Z}$ is surjective.

Furthermore, our method extends to the Atkin-Lehner quotients of modular curves with a slight modification, i.e., by choosing a different uniformiser.

Another innovation is that the algorithm does not make use of the affine models of the modular curves, which are often required as inputs in previous algorithms. Furthermore, we can compute Coleman integrals between any two points that are not necessarily on the same residue disc.

TODO: review this part

The general strategy works as follows:

1. Reduce the problem of computing arbitrary Coleman integrals into a sum of tiny integrals,

2. Find a basis of holomorphic 1-forms and a suitable uniformiser,
3. Formally integrate and evaluate at the end points.

2.1 Breaking the Coleman integrals into tiny integrals

Let $X/\mathbb{Q}$ be a modular curve associated to a congruence subgroup Γ, two points $Q, R \in X(\bar{\mathbb{Q}})$, $\{\omega_1, \ldots, \omega_g\}$ a $\mathbb{Q}$-basis of $H^0(X, \Omega^1)$ where g is the genus of the curve and p a prime of good reduction on X.

The Hecke operator at p, T_p acts on the weight 2 cusp forms, which corresponds to the holomorphic 1-forms:

$$T_p^* \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_g \end{pmatrix} = A \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_g \end{pmatrix}.$$

where A is the Hecke matrix acting on the basis of cusp forms. Integrating between the points Q and R gives:

$$\begin{pmatrix} \int_R^Q T_p^* \omega_1 \\ \vdots \\ \int_R^Q T_p^* \omega_g \end{pmatrix} = A \begin{pmatrix} \int_R^Q \omega_1 \\ \vdots \\ \int_R^Q \omega_g \end{pmatrix}.$$

For any $\omega \in H^0(X, \Omega^1)$, using the definition of Hecke operator as a correspondence and the functoriality of Coleman integrals, we obtain the following equality:

$$\int_R^Q T_p^*(\omega) = \int_{T_p(R)}^{T_p(Q)} \omega = \sum_{i=0}^{p} \int_{R_i}^{Q_i} \omega,$$

where $T_p(Q) = \sum_{i=0}^{p} Q_i$ and $T_p(R) = \sum_{i=0}^{p} R_i$.

By considering $((p+1)\int_Q^R \omega - \int_Q^R T_p^* \omega)$, we have the following fundamental equation:

$$((p+1)I - A)\begin{pmatrix} \int_R^Q \omega_1 \\ \vdots \\ \int_R^Q \omega_g \end{pmatrix} = \begin{pmatrix} \sum_{i=0}^p \int_{Q_i}^Q \omega_1 - \sum_{i=0}^p \int_{R_i}^R \omega_1 \\ \vdots \\ \sum_{i=0}^p \int_{Q_i}^Q \omega_g - \sum_{i=0}^p \int_{R_i}^R \omega_g \end{pmatrix}. \tag{2.1}$$

The Q_i's and R_i's are by definition p-isogenous to Q and R, therefore, the Eichler-Shimura relation ([DS05] Theorem 8.7.2) implies that they are in the same residue discs respectively. So the vector on the right hand side consists of sums of tiny integrals. On the left hand side, the matrix $((p+1)I - A)$ is invertible by the Ramanujan bound – the Hecke matrix A has eigenvalues $\{a_p\}$ which satisfy $|a_p| \leq 2\sqrt{p}$.

From the above discussion, since any ω is a linear combination of the ω_j's, we can simultaneously compute the Coleman integrals $\int_Q^R \omega$ once we have evaluated the tiny integrals $\sum_{i=0}^p \int_{Q_i}^Q \omega$ and $\sum_{i=0}^p \int_{R_i}^R \omega$.

2.2 Computing a basis of cusp forms

The spaces of cusp forms for the congruence subgroups $\Gamma(N), \Gamma_1(N)$ and $\Gamma_0(N)$ are available in software packages [The22b] and [BCP97]. In [Zyw20], the author gave a method to compute the action of $SL_2(\mathbb{Z})$ and $GL_2(\mathbb{Z}/N\mathbb{Z})$ on $\mathscr{S}_k(\Gamma(N))$, which uses the properties that [BN20]:

- There is an action of $SL_2(\mathbb{Z}/N\mathbb{Z})$ induced from $SL_2(\mathbb{Z})$ on the cusp forms,
- $\left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right)$ acts on the coefficients of the q-expansion by $\zeta_N \mapsto \zeta_N^d$, where ζ_N is a N-th root of unity.

Furthermore, for $H \leq GL_2(\mathbb{Z}/N\mathbb{Z})$ satisfying the conditions above, $\mathscr{S}_2(\Gamma(N))^H$, the space of weight 2 cusp forms invariant under H is isomorphic to $H^0(X_H, \Omega^1)$.

For congruence subgroups $\Gamma_0^+(N) := \Gamma_0(N)/w_N$ with an Atkin-Lehner involution, we modify Zywina's Magma implementation to compute our examples.

2.3 Hecke operators as double coset operators

Hecke operators act on both cusp forms and the divisor group of the modular curve. To compute them as a double coset operator, we need to compute the coset representatives $\Gamma_H \backslash \Gamma_H \alpha \Gamma_H$ for congruence subgroups Γ_H. A few key lemmas will give us a procedure to compute the coset representatives.

Lemma 2.3.1. *([DS05] Lemmata 5.1.1, 5.1.2) Let $\Gamma, \Gamma_1, \Gamma_2$ be congruence subgroups and $\alpha \in GL_2^+(\mathbb{Q})$. Then,*

1. *$\alpha^{-1}\Gamma\alpha \cap SL_2(\mathbb{Z}) \leq SL_2(\mathbb{Z})$ is a congruence subgroup.*
2. *There is a bijection:*

$$(\alpha^{-1}\Gamma_1\alpha \cap \Gamma_2)\backslash\Gamma_2 \leftrightarrow \Gamma_1\backslash\Gamma_1\alpha\Gamma_2$$
$$(\alpha^{-1}\Gamma_1\alpha \cap \Gamma_2)\gamma_2 \mapsto \Gamma_1\alpha\gamma_2$$

More concretely, $\{\gamma_{2,i}\}$ is a set of coset representatives for $(\alpha^{-1}\Gamma_1\alpha \cap \Gamma_2)\backslash\Gamma_2$ if and only if $\{\alpha\gamma_{2,i}\}$ is a set of coset representatives of $\Gamma_1\backslash\Gamma_1\alpha\Gamma_2$.

Lemma 2.3.2. *([Shi94] Lemma 3.29(5)) Let $\alpha \in M_2(\mathbb{Z})$ be such that $\det(\alpha) = p$ and $\alpha \pmod N \in H$. If $\Gamma_H\alpha\Gamma_H = \bigcup_i \Gamma_H\alpha_i$ is a disjoint union, then $SL_2(\mathbb{Z})\alpha SL_2(\mathbb{Z}) = \bigcup_i SL_2(\mathbb{Z})\alpha_i$ is a disjoint union.*

The procedure for computing the Hecke operator as a double coset operator is as follows:

1. Find $\alpha \in M_2(\mathbb{Z})$ satisfying $\det(\alpha) = p$, $\alpha \pmod N \in H$,

2. Find the coset representatives $\{\alpha_i\}$ in $(\alpha^{-1}SL_2(\mathbb{Z})\alpha \cap SL_2(\mathbb{Z}))\backslash SL_2(\mathbb{Z})$. Usually, α will be chosen such that $(\alpha^{-1}SL_2(\mathbb{Z})\alpha \cap SL_2(\mathbb{Z}))$ has a clear description. By Lemma 2.3.1, $SL_2(\mathbb{Z})\backslash SL_2(\mathbb{Z})\alpha SL_2(\mathbb{Z})$ has coset representatives $\{\alpha\alpha_i\}$,

3. By Lemma 2.3.2, for each $\alpha\alpha_i$, find $\beta_i \in SL_2(\mathbb{Z})$ such that $\beta_i\alpha\alpha_i \in \Gamma_H$. Then $\{\beta_i\alpha\alpha_i\}$ will be the desired coset representatives for $\Gamma_H\backslash\Gamma_H\alpha\Gamma_H$.

2.4 Tiny integrals via complex number approximation

We present a method to compute tiny integrals by comparing Taylor coefficients of a system of equations and recovering them as algebraic number approximations from complex solutions.

Algorithm 2.4.1. *Computing* $\sum_{i=0}^{p}\int_{Q_i}^{Q}\omega$

Input:

- $\tau_0 \in \mathbb{H}$ *such that* $\Gamma\tau_0$ *corresponds to a rational point* Q *on* X*, and* $q_0 := e^{2\pi i\tau_0/h}$ *where* h *is the width of the cusp.*
- *A good prime* p *which does not divide* $j(Q)$ *or* $j(Q)-1728$.
- *A cusp form* $f \in \mathscr{S}_2(\Gamma)$ *given by its* q*-expansion where* $q = e^{2\pi i\tau/h}$*. We denote the corresponding* $1-$*form by* ω.

Output:

- *The sum of tiny Coleman integrals* $\sum_{i=0}^{p}\int_{Q_i}^{Q}\omega \in \mathbb{Q}_p$*, where* $T_p(Q)=\sum_{i=0}^{p}Q_i$.

Steps:

1. *(Writing* ω *as a power series in terms of an uniformiser* u*) Fix a precision* n*. Find* $x_i \in \mathbb{Q}$ *such that*

$$\omega = (\sum_{i=0}^{n} x_i(u)^n + \mathscr{O}(u^{n+1}))d(u). \tag{2.2}$$

These x_i*'s can be found using the following steps:*

a. *Write* u *and* ω_i *as power series expansions of* $q-q_0$ *by differentiating their* q*-expansions* *and evaluating at q_0:*

$$
\begin{aligned}
u &= \sum_{i=1}^{C_1} a_i (q-q_0)^i + O((q-q_0)^{C_1+1}),\\
\omega &= \sum_{i=0}^{C_2} b_i (q-q_0)^i + O((q-q_0)^{C_2+1}) dq,\\
d(u) &= (\sum_{i=1}^{C_1} i a_i (q-q_0)^{i-1} + O((q-q_0)^{C_1})) dq,
\end{aligned}
$$

where C_1, C_2 are some fixed precision determined by n and the norm of q_0. The coefficients a_i, b_i's are in $\mathbb{C}$.

b. *Replace ω, u and $d(u)$ by their power series expansions in $q-q_0$ as in equation (2.2). Comparing the coefficients of $(q-q_0)^k$ on both sides gives us the following linear system:*

$$
\begin{pmatrix}
a_1 & 0 & 0 & \dots & 0\\
2a_2 & a_1^2 & 0 & \dots & 0\\
3a_3 & 3a_1a_2 & a_1^3 & \dots & 0\\
\vdots & \vdots & \vdots & \ddots & \vdots\\
(n+1)a_{n+1} & \sum_{i=1}^{n} a_i(n+1-i)a_{n+1-i} & * & \dots & a_1^{n+1}
\end{pmatrix}
\cdot
\begin{pmatrix} x_0\\ x_1\\ x_2\\ \vdots\\ x_n \end{pmatrix}
=
\begin{pmatrix} b_0\\ b_1\\ b_2\\ \vdots\\ b_n \end{pmatrix}
$$

c. *Solve this system of equations and get complex approximations of x_i's. These x_i's can be recovered as elements in $\mathbb{Q}$ using `algdep` from `PARI/GP`. This is likely to succeed given sufficient complex precision.*

2. *Calculate $u(Q_i)$ as algebraic numbers. In practice, we use the j-invariant function as an uniformiser. We calculate $j(Q_i)$ transcendentally by evaluating the q-expansion of the j-function on $\beta_i(\tau_0)$ and then obtain the algebraic approximation. On the other hand, the roots of the modular polynomial $\Phi_p(x, j(Q)) = 0$ are the j-invariants of elliptic curves that are*

p-isogeneous to Q. This gives another (algebraic) method to compute $j(Q_i)$.

3. *Compute the sum of tiny integrals* $\sum_{i=0}^{p} \int_{Q}^{Q_i} \omega \approx \sum_{i=0}^{p} \int_{0}^{u(Q_i)} (\sum_{j=0}^{n} x_j u^j du)$ *with its p-adic expansion.*

Chapter 3

Computations and examples

In the previous chapter, we outlined an algorithm to compute single Coleman integrals on modular curves between any two known points. The modular curves in consideration come from Serre's Uniformity Conjecture, i.e., they are of the form $X = X_H(N) := \mathbb{H}^+/\Gamma_H(N)$ and they satisfy:

- $\Gamma_H(N) \leq \mathrm{SL}_2(\mathbb{Z})$ where $H \leq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$,
- $-I \in H$,
- $\det : H \to \mathbb{Z}/N\mathbb{Z}$ is surjective.

Moreover, we also consider quotients of modular curves by the action of Atkin-Lehner involutions. We will demonstrate three classes of examples, namely, $X_0(N)$, $X_0^+(N)$, and $X_{ns}^+(N)$, while gathering the necessary ingredients such as known rational points, basis of differentials and the action of the Hecke operators to perform Coleman integration.

3.1 $X_0(N)$

Let N be positive integer. The modular curve $X = X_0(N)$ is defined to be the quotient of the upper half plane by the congruence subgroup $\Gamma_0(N) = \{\left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right) \pmod{N}\} \leq \mathrm{SL}_2(\mathbb{Z})$. As a moduli space, the $\mathbb{Q}$-rational points of X correspond elliptic curves E defined over $\mathbb{Q}$ such that E admits a $\mathbb{Q}$-rational isogeny of degree N to another elliptic curve E'. Given a point Q on X, to find the coset representative on the upper half plane, one first finds the ratio of periods $\tau' \in \mathbb{H}$ of the elliptic curve Q, which corresponds to $\mathrm{SL}_2(\mathbb{Z})\tau' \in \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ satisfying $j(\tau') = j(E)$. This can be done by finding an elliptic curve $E_\tau/\mathbb{C}$ with j-invariant j_E via the universal elliptic curve:

$$y^2 + xy = x^3 - \frac{36}{j_E - 1728}x - \frac{1}{j_E - 1728}$$

Then, one iterates through the cosets of $\mathrm{SL}_2(\mathbb{Z})/\Gamma_0(N)$ to find γ such that its j-invariant satisfies:

$$j(\gamma\tau') = j(N\gamma\tau') = j(E)$$

As a result, the point Q corresponds to $\Gamma_0(N)\gamma\tau' \in \Gamma_0(N)\backslash\mathbb{H}^+$. One could find a basis of weight 2 cusp forms $\mathscr{S}_2(\Gamma_0(N))$ and the action of Hecke operators on the basis of cusp forms using well known methods that are implemented in SAGEMATH[Ste07, The22b]. Let $\omega \in H^0(X, \Omega^1)$, $Q \in X(\mathbb{Q})$. We follow Algorithm 2.4.1 for computing $\sum_{i=0}^{p} \int_{Q_i}^{Q} \omega$. We choose $j(\tau) - j(Q)$ as our uniformiser.

3.1.1 Example: $X_0(37)$

- **Curve data:** We consider the modular curve $X = X_0(37)$. X is a hyperelliptic curve. Comparing relations between q-expansions of rational functions $x, y \in \mathbb{C}(X)$, we obtain a plane model $y^2 = -x^6 - 9x^4 - 11x^2 + 37$ [MSD74]. There are four $\mathbb{Q}$-rational points $Q = (1,-4), R = (-1,-4), S = (1,4), T = (-1,4)$, where Q,R are noncuspidal rational points and S,T are cuspidal rational points.

- **Rational points:** Since the j-function is a modular function on $X_0(37)$ and that $X_0(37)$ is hyperelliptic, we could express j-function as a rational function of x and y to compute that

$$
\begin{aligned}
j(Q) &= -9317 = -7 \cdot 11^3, \\
j(R) &= -162677523113838677 = -7 \cdot 137^3 \cdot 2083^3.
\end{aligned}
$$

  The points Q,R corresponds to the elliptic curve E_Q, E_R with j-invariants $j(Q), j(R)$ containing a cyclic subgroup of order 37 (or equivalently, with a degree 37-isogeny). This information could be verified in LMFDB [LMF22]. Following the method in Section 3.1, we obtain the upper half plane representatives of Q,R as follows:

$$
\begin{aligned}
\tau_Q &\approx 0.5 + 0.17047019819380 \cdot i \in \mathbb{H}, \\
\tau_R &\approx 0.5 + 0.39635999889406 \cdot i \in \mathbb{H}.
\end{aligned}
$$

- **Basis of differential forms:** One could compute that $\mathscr{S}_2(\Gamma_0(N))$ has $\mathbb{C}$-dimension 2 and a basis of the space of weight 2 cusp forms using SAGEMATH. Furthermore, the action of Hecke operators on the basis of cusp forms is available on SAGEMATH. Linear algebra leads to an eigenbasis $\{f_0, f_1\}$ of the $\mathbb{C}$-vector space $\mathscr{S}_2(\Gamma_0(37))$ with the following q-expansions:

$$f_0 = q + q^3 - 2q^4 + O(q^6),$$
$$f_1 = q - 2q^2 - 3q^3 + 2q^4 - 2q^5 + O(q^6).$$

- **Hecke action:** We choose $p = 3$, and $T_3(f_0) = f_0, T_3(f_1) = -3f_1$. Therefore the Hecke operator matrix T_3 is $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -3 \end{smallmatrix}\right)$.

- **Algorithm 2.4.1 and results:** Let ω_0, ω_1 be 1-forms that corresponds to cusp forms $-\frac{1}{2}f_0$, $-\frac{1}{2}f_1$ respectively in order to obtain $\omega_0 = \frac{dx}{y}$ and $\omega_1 = \frac{xdx}{y}$. This way, we can get a direct comparison with MAGMA's hyperelliptic curve implementation. Now, we proceed with computing the Coleman integrals on ω_0, ω_1.

  We explain how to calculate $\sum_{i=0}^{p} \int_{Q_i}^{Q} \omega_1$ using Algorithm 2.4.1. By comparing complex coefficients and using `algdep` to algebraically approximate complex numbers, we first obtain rational coefficients x_i in the expansion of ω_1 about $j = j(Q)$:

$$\begin{aligned}\omega_1 =&(-9317) + \frac{717409}{2 \cdot 37 \cdot 47}(j - j(Q)) + \frac{253086749261192}{37^2 \cdot 47^3}(j - j(Q))^2 \\ &+ \frac{176804544077038351043955}{37^3 \cdot 47^5}(j - j(Q))^3 + O((j - j(Q))^4) \ \ d(j - j(Q)).\end{aligned}$$

  After that, the j-invariants $j(Q_i)$ of Q_i's for $i = 0, \ldots, 3$ can be realised as the roots of the modular polynomial $\Phi_3(j(Q), X) = 0$. In the last step, we substitute the roots into a sum of local power series:

$$\begin{aligned}\sum_{i=0}^{3} \int_{Q_i}^{Q} \omega_1 = \sum_{i=0}^{3} \int_{j(Q_i)-j(Q)}^{0} &(-9317) + \frac{717409}{2 \cdot 37 \cdot 47}t + \frac{253086749261192}{37^2 \cdot 47^3}t^2 \\ &+ \frac{176804544077038351043955}{37^3 \cdot 47^5}t^3 + \cdots dt\end{aligned}$$

Our results are listed in the table below. One can verify the results by comparing with the hyperelliptic model of this curve or with the MAGMA's hyperelliptic curves implementation of [BT22].

$\sum_{i=0}^{3}\int_{Q_i}^{Q}\omega_0$	$O(3^{14})$
$\sum_{i=0}^{3}\int_{Q_i}^{Q}\omega_1$	$3^2+3^3+3^9+3^{10}+2\cdot 3^{11}+3^{12}+2\cdot 3^{13}+O(3^{14})$
$\sum_{i=0}^{3}\int_{R_i}^{R}\omega_0$	$O(3^{14})$
$\sum_{i=0}^{3}\int_{R_i}^{R}\omega_1$	$3^2+3^3+3^9+3^{10}+2\cdot 3^{11}+3^{12}+2\cdot 3^{13}+O(3^{14})$

Table 3.1: Coleman Integrations on $X_0(37)$

3.2 $X_0^+(N)$

Consider the modular curve $X_0(N)$ from the previous example. There is an involution acting on the points of $X_0(N)$, called the Atkin-Lehner involution $w_N := \frac{1}{\sqrt{N}}\left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right)$. One could verify that w_N^2 acts as the identity on the $\Gamma_0(N)$-orbits of $\mathbb{H}$. Let $\Gamma_0^+(N) := \Gamma_0(N) \cup w_N\Gamma_0(N)$. The compactification of the quotient of the upper half plane by $\Gamma_0^+(N)$ gives rise to the modular curve $X := X_0^+(N)$.

Proposition 3.2.1. Suppose $\Gamma_0(N)\tau \in X_0(N)$ corresponds to the elliptic curve with torsion data $(E_1, \phi : E_1 \to E_2)$, then $w_N(\Gamma_0(N)\tau)$ corresponds to $(E_2, \hat{\phi} : E_2 \to E_1)$, where $\hat{\phi}$ is the dual isogeny.

Proof. $\Gamma_0(N)\tau$ corresponds $(E_\tau, \langle \frac{1}{N}, \tau \rangle)$ up to isomorphism. As $w_N \cdot \tau = \frac{-1}{N\tau}$, $w_N \cdot \Gamma_0(N)\tau$ corresponds to $[E_{\frac{1}{N\tau}}, \langle \frac{1}{N}, \frac{1}{N\tau} \rangle]$. Note that the relation between complex tori over $\Gamma_0(N)$ and elliptic curves with a cyclic subgroup of order N are captured by the following isomorphism $E_\tau / \langle \frac{1}{N}, \tau \rangle \cong \mathbb{C} / \langle \frac{1}{N}, \tau \rangle$. It is clear that $\langle \frac{1}{N}, \tau \rangle = \tau \langle 1, \frac{1}{N\tau} \rangle$, hence $E_{\frac{1}{N\tau}}$ is isomorphic to $E_\tau / \langle \frac{1}{N}, \tau \rangle$. It remains to check that the dual isogeny of $\phi : E \to E_\tau / \langle \frac{1}{N}, \tau \rangle$ is indeed the isogeny induced by $E_{\frac{1}{N\tau}}$. This can be checked by first computing the dual isogeny and comparing kernels. $\square$

The above proposition provides a moduli interpretation for $X_0^+(N)$, i.e., the $\mathbb{Q}$-points correspond to unordered pairs of elliptic curves $(\phi_1 : E_1 \to E_2, \phi_2 : E_2 \to E_1)$ such that ϕ_1 is an isogeny of degree N, and ϕ_2 is the dual isogeny, with the additional requirement that they are $\mathrm{Gal}(\bar{\mathbb{Q}} \backslash \mathbb{Q})$-invariant. Note that by complex multiplication theory, it is possible that the elliptic curves E_1, E_2 or the isogenies ϕ_1, ϕ_2 may not be defined over $\mathbb{Q}$ but over a quadratic extension of $\mathbb{Q}$, and in that case the elliptic curves or isogenies are fixed by nontrivial Galois element of the quadratic extension.

The expected rational points on X correspond to elliptic curves with complex multiplication. Following [Mer18, Sta75], we have a list of discriminants of imaginary quadratic number fields with class number one:

$$\mathscr{D} = \{-3, -4, -7, -8, -11, -12, -16, -19, -27, -28, -43, -67, -163\}.$$

Let E be a CM elliptic curve such that its endomorphism ring $\mathscr{O}_E$ has discriminant $\Delta_E \in \mathscr{D}$. Elliptic curves E such that N splits or ramifies in $\mathscr{O}_E$ give rise to rational points on X [Gal99]. Iterating through the class number one discriminants, we have list of candidates of expected rational points coming from CM elliptic curves. We denote the one of the rational points by Q and find the upper half plane representative via the following steps.

The endomorphism ring $\mathscr{O}_E$ is an order in an imaginary quadratic field and therefore has a generator τ_E and we factor the ideal (N) into a product of principal ideals $\mathfrak{m}\bar{\mathfrak{m}}$ in $\mathscr{O}_E$. Write $\mathfrak{m} = (\alpha)$. Since $\alpha \in \mathscr{O}_E$, there exists integers such that $\alpha = c\tau_E + d$. Euclidean algoritm gives two integers a, b such that $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. In this case, the upper half representative is $\tau_Q = \gamma \cdot \tau_E$.

To compute the basis of cusp forms $\mathscr{S}_2(\Gamma_0^+(N))$, one observes that by the definition of $X_0^+(N)$, $\mathscr{S}_2(\Gamma_0^+(N)) = \{f \in \mathscr{S}_2(\Gamma_0(N)) : f|_2 w_N = f\}$.

The Hecke operator action can be understood through its definition as a double coset operator:

Lemma 3.2.2. *Let $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$. The coset representatives of $(\alpha^{-1}\Gamma_0^+(N)\alpha \cap \Gamma_0^+(N))\backslash\Gamma_0^+(N)$ is the same as that of $(\alpha^{-1}\Gamma_0(N)\alpha \cap \Gamma_0(N))\backslash\Gamma_0(N)$.*

Proof. Observe that

$$\begin{aligned}\alpha^{-1}\Gamma_0^+(N)\alpha \cap \Gamma_0^+(N) &= \alpha^{-1}(\Gamma_0(N) \cup w_N\Gamma_0(N))\alpha \cap (\Gamma_0(N) \cup w_N\Gamma_0(N)) \\ &= (\alpha^{-1}\Gamma_0(N)\alpha \cap \Gamma_0(N)) \cup (\alpha^{-1}(w_N\Gamma_0(N))\alpha \cap w_N\Gamma_0(N))\end{aligned}$$

Now, by Lemma 2.3.1, one has an explicit description of the double coset representatives of $\Gamma_0(N)\alpha\Gamma_(N)$ and one could show that the two sets of coset representatives above are equal. $\square$

In particular, the above Lemma implies that, for a prime p, the Hecke operator T_p on $X_0^+(N)$ and $X_0(N)$, as a double coset operator, has the same coset representatives:

$$(\,\cdot\,)|_k[\Gamma_0^+(N)\alpha\Gamma_0^+(N)] = (\,\cdot\,)|_k[\Gamma_0(N)\alpha\Gamma_0(N)] : f \mapsto \sum_i f|_k\beta_i = \sum_{i=0}^{p-1} f|_k\left(\begin{smallmatrix} 1 & i \\ 0 & p \end{smallmatrix}\right) + f|_k\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)$$

For the uniformiser, we require a combination of modular functions that is invariant under the Atkin-Lehner involution w_N. Since $j(w_N\cdot\tau) = j(-1/N\tau) = j(N\tau)$, we can choose $j + j_N$ as our uniformiser, where $j_N(\tau) := j(N\tau)$. For a given point $Q = (E_1 \leftrightarrow E_2)$ and the points Q_i in the same residue disc, the endpoints of the sum of tiny integrals are $j(Q_i) + j(NQ_i)$ where $j(Q_i)$ and $j(NQ_i)$ can be computed as roots of the modular polynomials $\Phi_p(x, j(E_1)) = 0$ and $\Phi_p(x, j(E_2)) = 0$.

3.2.1 Example: $X_0^+(67)$

- **Curve data:** We consider the modular curve $X = X_0^+(67)$. X is a hyperelliptic curve. Again, by comparing relations between q-expansions of rational functions $x, y \in \mathbb{C}(X)$, we obtain a plane model $y^2 = x^6 + 2x^5 + x^4 - 2x^3 + 2x^2 - 4x + 1$. A quick box search yields two rational points $R = (0, -1), S = (1, 1)$ on X.

- **Uniformisers:** We use $j + j_N$ as the uniformiser since it is a modular function invariant under the Atkin-Lehner involution.

  TODO: messy!check this part

- **Rational points:** For the rational points R, S, their upper half plane representatives can be found as follows. R is the pair $\{\phi_1 : E_1 \to E_1, \hat{\phi}_1 : E_1 \to E_1\}$, with $j(E_1) = -2^{18}3^3 5^3$. $E_1/\mathbb{Q}$

has CM by the ring of integers $\mathscr{O}_{K_1}$ where $K_1 = \mathbb{Q}(\sqrt{-43})$. 67 splits in $\mathscr{O}_{K_1}$ implies that such pair of isogenies exists. Similarly, S is the pair $\{\phi_2 : E_2 \to E_2, \hat{\phi}_2 : E_2 \to E_2\}$, with $j(E_2) = 2^6 5^3$. $E_2/\mathbb{Q}$ has CM by the ring of integers $\mathscr{O}_{K_2}$ with $K_2 (= \mathbb{Q}(\sqrt{-2}))$, 67 splits in $\mathscr{O}_{K_2}$ as well. Note that both R and S are not fixed by the Atkin-Lehner involution, since that corresponds to the case when 67 is ramified.

We have $j(R) = 2^6 5^3, D(R) = -8$, hence $\tau_R = \sqrt{-2}$. Following the steps described in the previous section, we have $(67) = (7+3\sqrt{-2})(7-3\sqrt{-2})$ and the Euclidean algorithm gives

$$7+3\sqrt{-2} = 7+3\cdot\sqrt{-2} \implies \hat{\gamma} = \left(\begin{smallmatrix} 1 & 2 \\ 3 & 7 \end{smallmatrix}\right)$$

Therefore,

$$\begin{aligned} \hat{\tau}_R = \hat{\gamma}\tau_R = \frac{\sqrt{-2}+2}{3\sqrt{-2}+7} \\ \approx 0.298507462686567 + 0.0211076651100462 \cdot i. \end{aligned}$$

Similarly, we have $j(S) = 2^4 3^3 5^3, D(S) = -12, \tau_S = \sqrt{-3}$. $(67) = (8+\sqrt{-3})(8-\sqrt{-3})$ and the Euclidean algorithm gives

$$8+\sqrt{-3} = 8+1\cdot\sqrt{-3} \implies \hat{\gamma} = \left(\begin{smallmatrix} -1 & -9 \\ 1 & 8 \end{smallmatrix}\right)$$

Therefore,

$$\hat{\tau}_S = \hat{\gamma}\tau_S = -\frac{\sqrt{-3}+9}{\sqrt{-3}+8}$$
$$\approx 1.11940298507463 - 0.0258515045905802 \cdot i.$$

- **Basis of differential forms:** $\mathscr{S}_2(\Gamma_0(67))$ has dimension 5. One could compute the action of w_{67} on the space and find a 2-dimensional subspace spanned by cusp forms invariant under the Atkin-Lehner involution using SAGEMATH, to get a basis of $H^0(X,\Omega^1)$:

$$\omega_0 = f_0\ dq/q\ = 2q - 3q^2 - 3q^3 + 3q^4 - 6q^5 + O(q^6)\ \ dq/q$$
$$\omega_1 = f_1\ dq/q\ = -q^2 + q^3 + 3q^4 + O(q^6)\ \ dq/q$$

- **Hecke action:** Let $p = 13$ be a good prime. The Hecke matrix on this subspace is $T_{13} = \left(\begin{smallmatrix} -7/2 & 15/2 \\ 3/2 & -7/2 \end{smallmatrix}\right)$.
- **Algorithm 2.4.1 and results:** Step 1 of Algorithm 2.4.1 gives a power series expansion of the differential forms for the uniformiser $j := j + j_N$ (for simplicity, we use this notation). For example, ω_0 at $j = j(R)$ has the following power series expansion:

$$\begin{aligned}\omega_0 = &\frac{-1}{2^7\cdot 5^2\cdot 7^2} + \frac{3047}{2^{15}\cdot 5^5\cdot 7^6}(j-j(R)) + \frac{-38946227}{2^{24}\cdot 5^8\cdot 7^{10}}(j-j(R))^2 \\ &+ \frac{33888900627}{2^{32}\cdot 5^{10}\cdot 7^{14}} + \frac{-110823337943341}{2^{42}\cdot 5^{13}\cdot 7^{17}}(j-j(R))^3 + O((j-j(R))^4)\ \ d(j-j(R)).\end{aligned}$$

The endpoints $j(Q_i) + j(NQ_i)$ appearing in the sum of tiny integrals can be computed as mentioned in the previous section. Finally, we compute the Coleman integrals and our results can be verified with the MAGMA implementation by [BT22] since X is hyperelliptic.

$\sum_{i=0}^{3} \int_{R_i}^{R} \omega_0$	$2 \cdot 13 + 13^2 + 3 \cdot 13^3 + 7 \cdot 13^4 + 11 \cdot 13^5 + 8 \cdot 13^6 + 8 \cdot 13^7 + 7 \cdot 13^8 + 13^9 + O(13^{10})$
$\sum_{i=0}^{3} \int_{R_i}^{R} \omega_1$	$11 \cdot 13 + 8 \cdot 13^2 + 6 \cdot 13^3 + 8 \cdot 13^4 + 3 \cdot 13^5 + 6 \cdot 13^6 + 6 \cdot 13^7 + 7 \cdot 13^8 + 11 \cdot 13^9 + O(13^{10})$
$\sum_{i=0}^{3} \int_{S_i}^{S} \omega_0$	$10 \cdot 13 + 8 \cdot 13^2 + 2 \cdot 13^5 + 5 \cdot 13^6 + 10 \cdot 13^7 + 2 \cdot 13^8 + 2 \cdot 13^9 + O(13^{10})$
$\sum_{i=0}^{3} \int_{S_i}^{S} \omega_1$	$3 \cdot 13 + 7 \cdot 13^2 + 2 \cdot 13^3 + 10 \cdot 13^4 + 8 \cdot 13^5 + 5 \cdot 13^6 + 8 \cdot 13^8 + 10 \cdot 13^9 + O(13^{10})$

Table 3.2: Coleman Integrations on $X_0^+(67))$

3.3 $X_{ns}^{+}(p)$

For a prime p, we start with the definitions of the nonsplit Cartan subgroup C_{ns} and its normaliser C_{ns}^{+}. Let $\{1,\alpha\}$ be a $\mathbb{F}_p$- basis of $\mathbb{F}_{p^2}$. Suppose that α satisfies a minimal polynomial $X^2 - tX + n \in \mathbb{F}_p[X]$. For any $\beta = x + y\alpha \in \mathbb{F}_{p^2}^{\times}$, there is a multiplication-by-β map with respect to the basis $\{1,\alpha\}$:

$$i_\alpha : \mathbb{F}_{p^2}^{\times} \to \mathrm{GL}_2(\mathbb{F}_p)$$
$$\beta \mapsto \left(\begin{smallmatrix} x & -ny \\ y & x+ty \end{smallmatrix}\right)$$

Given this choice of basis, we define the nonsplit Cartan subgroup $C_{ns}(p) \leq GL_2(\mathbb{F}_p)$ as the image of i_α. The normaliser of the nonsplit Cartan subgroup $C_{ns}^{+}(p)$ is the subgroup generated by $C_{ns}(p)$ and the conjugation map (under i_α) coming from $\mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$. If we have the freedom to choose the basis, then α can be picked to be the squareroot of a quadratic nonresidue ε in $\mathbb{F}_{p^2}$ satisfying $X^2 - \varepsilon^2 = 0$. Then, we have:

$$C_{ns}^{+}(p) = \langle \left(\begin{smallmatrix} x & \varepsilon^2 y \\ y & x \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) : (x,y) \in \mathbb{F}_p^2 \backslash (0,0) \rangle.$$

If $\langle \beta \rangle = \mathbb{F}_{p^2}^{\times}$, then we can write down the generators of $C_{ns}^{+}(p)$

Example 3.3.1. Let $p = 13, \varepsilon = \sqrt{7}, \mathbb{F}_{p^2}^{\times} = \langle 1+\varepsilon \rangle$. Then

$$C_{ns}^{+}(13) = \langle \left(\begin{smallmatrix} 1 & 7\cdot 1 \\ 1 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \rangle.$$

The modular curve corresponding to the normaliser of nonsplit Cartan subgroup $C_{ns}^{+}(p)$ is defined as the compactification of the quotient of the upper half plane by the lift of $C_{ns}^{+}(p)$ to a subgroup $\Gamma_{ns}^{+}(p) \leq \mathrm{SL}_2(\mathbb{Z})$.

Finding a basis of $\mathscr{S}_2(\Gamma_{ns}^+(p))$ can be done following Zywina's MAGMA implementation as in Section 2.2. For the purpose of exposition, suppose $\mathscr{S}_2(\Gamma_{ns}^+(p)) = \{f_1, \ldots, f_g\}$.

To find the upper half plane representatives of the expected rational points, we follow a similar procedure for $X_0(N)$. First, in the list of class number one discriminants $\mathscr{D}$, the expected points correspond to the discriminants Δ such that p is inert in the corresponding order $\mathscr{O}_\Delta$ [Maz77]. Once we have the list of expected points $\{P_1, \ldots P_r\}$, one could use the same method of inverting the j-invariant function to find $\mathrm{SL}_2(\mathbb{Z})$-orbits $\{\tau_1, \ldots, \tau_r\}$. The cosets of $\Gamma_{ns}^+(p) \backslash \mathrm{SL}_2(\mathbb{Z})$ allow us to find the correct upper half plane representatives corresponding to $\{P_1, \ldots P_r\}$. The problem now reduces to computing $\Gamma_{ns}^+(p) \backslash \mathrm{SL}_2(\mathbb{Z})$. There is bijection:

$$\mathrm{SL}_2(\mathbb{Z})/\Gamma_{ns}^+(p) \to \mathrm{SL}_2((\mathbb{Z}/p\mathbb{Z})/C_{ns}^+(p) \cap \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$$
$$\Gamma_{ns}^+(p)\gamma \mapsto (C_{ns}^+(p) \cap \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}))\bar{\gamma}.$$

Therefore, once we obtained coset representatives $\{\gamma_i\}$ of $\mathrm{SL}_2((\mathbb{Z}/p\mathbb{Z})/C_{ns}^+(p) \cap \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$, we can verify if $\gamma_i\tau$ is a $\mathbb{Q}$-rational point on X for $\tau \in \{\tau_1, \ldots, \tau_r\}$ by considering the canonical embedding, i.e., we can check if $(f_1(\gamma_i \cdot \tau) : \ldots : f_g(\gamma_i \cdot \tau)) \in \mathbb{P}^{g-1}$ has rational coordinates.

For the Hecke operators, recall that they act on the cusp forms and on the divisor group of points and we need to distinguish both cases.

On the cusp forms, there are two major steps: find the double coset representatives and then decompose these representatives into products on simpler matrices, for which there are algorithms to compute the slash-k operators [Zyw20, DS05]. The Hecke operator at the prime ℓ acts as a double coset operator:

$$[\Gamma_{ns}^{+}(p)\alpha\Gamma_{ns}^{+}(p)]_2 f = \sum f|_2\alpha_i,$$

where $\{\alpha_i\}_{i=0,\ldots,p}$ are the double coset representatives of $\Gamma_{ns}^{+}(N)\backslash\Gamma_{ns}^{+}(p)\alpha\Gamma_{ns}^{+}(p)$. It turns out that the representatives have the form $\alpha_i = \varepsilon\varepsilon'\left(\begin{smallmatrix}1 & 0\\ 0 & p\end{smallmatrix}\right)\beta$ or $\varepsilon\varepsilon'\beta\left(\begin{smallmatrix}p & 0\\ 0 & 1\end{smallmatrix}\right)$, where $\varepsilon,\varepsilon' \in \mathrm{SL}_2(\mathbb{Z})$ depends on α and β comes from the standard cosets of $\Gamma^0(p)\backslash\mathrm{SL}_2(\mathbb{Z})$. The motivation for this decomposition is that Zywina's algorithm [Zyw20] can compute the slash-k operator on determinant 1 matrices and the two matrices on the right can be resolved using techniques from [DS05]

In the first case, $f|_2\alpha_i = f|_2\varepsilon\varepsilon'\left(\begin{smallmatrix}1 & 0\\ 0 & p\end{smallmatrix}\right)\beta$ is given by Zywina's algorithm and explicit formulas found in Chapter 5, Section 2 of [DS05]. For the second case, one uses the fact that $\left(\begin{smallmatrix}1 & 0\\ 0 & p\end{smallmatrix}\right)\left(\begin{smallmatrix}mp & n\\ N & 1\end{smallmatrix}\right) = \left(\begin{smallmatrix}m & n\\ N & p\end{smallmatrix}\right)\left(\begin{smallmatrix}p & 0\\ 0 & 1\end{smallmatrix}\right)$ where $mp - nN = 1$. So the last coset α_p is of the form $\varepsilon\varepsilon\beta\left(\begin{smallmatrix}p & 0\\ 0 & 1\end{smallmatrix}\right)$. Again, Zywina's algorithm allows us to compute the slask-k operator for the first three matrices of determinant 1 while $\left(\begin{smallmatrix}p & 0\\ 0 & 1\end{smallmatrix}\right)$ acts by shifting the indices by multiples of p via the slask-k operator.

Since we already have a basis $\{f_1,\ldots,f_g\}$ of weight 2 cusp forms on $\Gamma_{ns}^{+}(p)$ by Zywina's algorithm, writing $[\Gamma_{ns}^{+}(p)\alpha\Gamma_{ns}^{+}(p)]_2 f_i$ as a linear combination of the basis elements of $\mathscr{S}_2(\Gamma(N),\mathbb{Q}(\zeta_N))$ would give us the Hecke matrix.

The Hecke operator on points can be computed in two ways as before. Firstly, if we have the double coset representatives, we can evaluate the points. Secondly, we could find the roots of the modular polynomial. Each approach has its (dis)advantages: we can evaluate cusp forms on explicit representatives but this will require a closer analysis of the group structure of $C_{ns}^{+}(N)$ and high enough complex precision; the modular polynomials give us the j-invariants of p-isogeneous points but they have large coefficients.

3.3.1 Example: $X_{ns}^+(13)$

We consider the cursed curve $X = X_{ns}^+(13)$ [BDM+19]. Let $C_{ns}^+(13)$ be defined by choosing the quadratic non-residue to be 7 as in the previous example, and let $\Gamma_{ns}^+(13)$ be the lift of $C_{ns}^+(13)$ in $\mathrm{SL}_2(\mathbb{Z})$.

- **Basis of differential forms:** Using Zywina's Magma implementation [Zyw20] , we obtain a basis of cusp forms as follows:

$$\begin{aligned}
f_0 =&(3\zeta_{13}^{11}+\zeta_{13}^{9}+3\zeta_{13}^{8}+\zeta_{13}^{7}+\zeta_{13}^{6}+3\zeta_{13}^{5}+\zeta_{13}^{4}+3\zeta_{13}^{2}+1)q\\
&+(-\zeta_{13}^{10}-2\zeta_{13}^{9}-\zeta_{13}^{7}-\zeta_{13}^{6}-2\zeta_{13}^{4}-\zeta_{13}^{3}-2)q^2+O(q^3)\\
f_1 =&(4\zeta_{13}^{11}+2\zeta_{13}^{9}+5\zeta_{13}^{8}+5\zeta_{13}^{5}+2\zeta_{13}^{4}+4\zeta_{13}^{2})q\\
&+(-3\zeta_{13}^{11}-5\zeta_{13}^{10}-4\zeta_{13}^{9}-4\zeta_{13}^{8}-4\zeta_{13}^{7}-4\zeta_{13}^{6}-4\zeta_{13}^{5}-4\zeta_{13}^{4}-5\zeta_{13}^{3}-3\zeta_{13}^{2}-2)q^2+O(q^3)\\
f_2 =&(\zeta_{13}^{10}-2\zeta_{13}^{7}-2\zeta_{13}^{6}+\zeta_{13}^{3})q\\
&+(-\zeta_{13}^{11}-2\zeta_{13}^{10}-2\zeta_{13}^{8}-2\zeta_{13}^{5}-2\zeta_{13}^{3}-\zeta_{13}^{2}+2)q^2+O(q^3),
\end{aligned}$$

  where ζ_{13} is a 13-th primitive root of unity and $q = e^{\frac{2\pi i\tau}{13}}$.

- **Curve data:** The method of canonical embedding [Gal96] gives us the following model:

$$\begin{aligned}
&X^4-\frac{7}{12}X^3Y-\frac{37}{30}X^2Y^2+\frac{37}{30}XY^3-\frac{3}{10}Y^4-\frac{61}{60}X^3Z+\frac{41}{15}X^2YZ\\
&-\frac{103}{60}XY^2Z+\frac{19}{60}Y^3Z-\frac{23}{6}X^2Z^2+\frac{87}{20}XYZ^2-\frac{14}{15}Y^2Z^2-\frac{199}{60}XZ^3\\
&+\frac{97}{60}YZ^3-\frac{11}{15}Z^4=0,
\end{aligned}$$

  where X, Y and Z corresponds to f_0, f_1 and f_2 respectively. The rational points can be found by a box search:

$$\{(\frac{3}{5}:2:1),(-2:2:1),(-2:\frac{-9}{2}:1),(-2:\frac{-7}{3}:1),(\frac{7}{3}:2:1),(\frac{5}{4}:2:1),(11:\frac{43}{2}:1)\}$$

.

- **Uniformisers:** $\mathscr{S}_2(\Gamma^+_{ns}(13)) \subseteq \mathscr{S}_2(\Gamma(N),\mathbb{Q}(\zeta_N))$ so the j-function is still a modular function for the normaliser of nonsplit Cartan and therefore can be used as an uniformiser.

- **Rational points:** Among the class number one discriminants Δ in $\mathscr{D}$, we find Δ such that 13 is inert in the corresponding order $\mathscr{O}_\Delta$. The set $\{-7,-8,-11,-19,-28,-67,-163\}$ contains discriminants that give rise to 7 expected rational points on X. We pick Q to be the point that corresponds to discriminant -7, and R to be the point that corresponds to discriminant -11. Following the notations in previous section, we have $\tau_7 = \frac{1}{2}+\frac{1}{2}\sqrt{-7}$ and $\tau_{11} = \frac{1}{2}+\frac{1}{2}\sqrt{-11}$. We then compute the coset representatives of $\mathrm{SL}_2(\mathbb{Z})/\Gamma^+_{ns}(13)$,

$$\{g_0,\ldots,g_{77}\} = \{T^i,\, (T^2)ST^i,\, (T^3)ST^i,\, (T^4)ST^i,\, (T^5)ST^i,\, (T^{12})ST^i \text{ for } i=0,\ldots,12\},$$

where $T = \left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$, $S = \left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right)$ are the two generators of $\mathrm{SL}_2(\mathbb{Z})$. By evaluating f_0, f_1, f_2 at $g_i(\tau_7)$ and $g_i(\tau_{11})$ for $i=0,\ldots,77$, we obtain the correct $\Gamma^+_{ns}(13)$-orbit representatives for Q and R, $\tau_Q = \frac{4+2\sqrt{-7}}{3+\sqrt{-7}}$, $\tau_R = \frac{13+\sqrt{-11}}{2}$. As in the previous section, the correct representative for Q can be found by evaluating $\frac{f_0(g_i(\tau_7))}{f_2(g_i(\tau_7))}$ and $\frac{f_1(g_i(\tau_7))}{f_2(g_i(\tau_7))}$ for different coset representatives g_i so that the ratios are rational numbers. Applying the same method to all the 7 discriminants, we get their corresponding rational points as computed from the model above.

- **Hecke action on forms:** We choose p to be 11. Let $\alpha = \left(\begin{smallmatrix}-13&44\\42&-143\end{smallmatrix}\right)\left(\begin{smallmatrix}1&0\\0&11\end{smallmatrix}\right)$ be the element $\alpha \in M_2(\mathbb{Z})$ with $\det(\alpha)=11$, $\alpha \pmod{13} \in C^+_{ns}(13)$. To find the double coset representatives we start with finding the coset representatives for $\mathscr{S} := (\alpha^{-1}\,\mathrm{SL}_2(\mathbb{Z})\alpha \cap \mathrm{SL}_2(\mathbb{Z}))\backslash \mathrm{SL}_2(\mathbb{Z}) =$

$\Gamma^0(11)\backslash \mathrm{SL}_2(\mathbb{Z})$. For each $\beta \in \mathscr{S}$, we found a corresponding $\gamma \in \Gamma^0(11)$ such that the representative $\beta' = \gamma\beta \in \Gamma_{ns}^+(13)$. We define the set of coset representatives to be $\mathscr{S}' := (\alpha^{-1}\Gamma_{ns}^+(13)\alpha \cap \Gamma_{ns}^+(13))\backslash\Gamma_{ns}^+(13)$ and the set of corresponding γ's to be Γ:

$$\begin{aligned}
\mathscr{S} &= \{\left(\begin{smallmatrix}1 & i\\ 0 & 1\end{smallmatrix}\right), i = 0,1,\ldots,10\} \cup \{\left(\begin{smallmatrix}66 & 5\\ 13 & 1\end{smallmatrix}\right)\},\\
\Gamma &= \{\left(\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right), \left(\begin{smallmatrix}1 & 0\\ -2 & 1\end{smallmatrix}\right), \left(\begin{smallmatrix}1 & 11\\ 0 & 1\end{smallmatrix}\right), \left(\begin{smallmatrix}1 & -55\\ 0 & 1\end{smallmatrix}\right), \left(\begin{smallmatrix}1 & 22\\ 0 & 1\end{smallmatrix}\right), \left(\begin{smallmatrix}1 & -44\\ 0 & 1\end{smallmatrix}\right), \left(\begin{smallmatrix}1 & 33\\ 0 & 1\end{smallmatrix}\right), \left(\begin{smallmatrix}1 & -33\\ 0 & 1\end{smallmatrix}\right), \left(\begin{smallmatrix}1 & 44\\ 0 & 1\end{smallmatrix}\right),\\
&\quad \left(\begin{smallmatrix}1 & -22\\ 0 & 1\end{smallmatrix}\right), \left(\begin{smallmatrix}-1 & -55\\ 0 & -1\end{smallmatrix}\right), \left(\begin{smallmatrix}1 & -44\\ 0 & 1\end{smallmatrix}\right)\},\\
\mathscr{S}' &= \{\left(\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right), \left(\begin{smallmatrix}1 & 1\\ -2 & 1\end{smallmatrix}\right), \left(\begin{smallmatrix}1 & 13\\ 0 & 1\end{smallmatrix}\right), \left(\begin{smallmatrix}1 & -52\\ 0 & 1\end{smallmatrix}\right), \left(\begin{smallmatrix}1 & 26\\ 0 & 1\end{smallmatrix}\right), \left(\begin{smallmatrix}1 & -39\\ 0 & 1\end{smallmatrix}\right), \left(\begin{smallmatrix}1 & 39\\ 0 & 1\end{smallmatrix}\right), \left(\begin{smallmatrix}1 & -26\\ 0 & 1\end{smallmatrix}\right), \left(\begin{smallmatrix}1 & 52\\ 0 & 1\end{smallmatrix}\right),\\
&\quad \left(\begin{smallmatrix}1 & -13\\ 0 & 1\end{smallmatrix}\right), \left(\begin{smallmatrix}-1 & -65\\ 0 & -1\end{smallmatrix}\right), \left(\begin{smallmatrix}-506 & -39\\ 13 & 1\end{smallmatrix}\right)\}.
\end{aligned}$$

From the bijection

$$\begin{aligned}
\Gamma_{ns}^+(13)\backslash\Gamma_{ns}^+(13)\alpha\Gamma_{ns}^+(13) &\to (\alpha^{-1}\Gamma_{ns}^+(13)\alpha \cap \Gamma_{ns}^+(13))\backslash\Gamma_{ns}^+(13)\\
\Gamma_{ns}^+(13)\delta &\mapsto (\alpha^{-1}\Gamma_{ns}^+(13)\alpha \cap \Gamma_{ns}^+(13))\alpha^{-1}\delta
\end{aligned}$$

we can get the double coset representatives of $\Gamma_{ns}^+(13)\backslash\Gamma_{ns}^+(13)\alpha\Gamma_{ns}^+(13)$:

$$\begin{aligned}
\mathscr{S}_\alpha = \{&\left(\begin{smallmatrix}-13 & 4\\ 42 & -13\end{smallmatrix}\right)\left(\begin{smallmatrix}1 & 0\\ 0 & 11\end{smallmatrix}\right)\left(\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right)\left(\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right), \left(\begin{smallmatrix}-13 & 4\\ 42 & -13\end{smallmatrix}\right)\left(\begin{smallmatrix}1 & 0\\ 0 & 11\end{smallmatrix}\right)\left(\begin{smallmatrix}1 & 0\\ -2 & 1\end{smallmatrix}\right)\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right), \ldots,\\
&\left(\begin{smallmatrix}-13 & 4\\ 42 & -13\end{smallmatrix}\right)\left(\begin{smallmatrix}1 & 0\\ 0 & 11\end{smallmatrix}\right)\left(\begin{smallmatrix}-1 & -55\\ 0 & -1\end{smallmatrix}\right)\left(\begin{smallmatrix}1 & 10\\ 0 & 1\end{smallmatrix}\right), \left(\begin{smallmatrix}-13 & 4\\ 42 & -13\end{smallmatrix}\right)\left(\begin{smallmatrix}1 & 0\\ 0 & 11\end{smallmatrix}\right)\left(\begin{smallmatrix}1 & -44\\ 0 & 1\end{smallmatrix}\right)\left(\begin{smallmatrix}66 & 5\\ 13 & 1\end{smallmatrix}\right)\}\\
= \{&\left(\begin{smallmatrix}-13 & 4\\ 42 & -13\end{smallmatrix}\right)\left(\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right)\left(\begin{smallmatrix}1 & 0\\ 0 & 11\end{smallmatrix}\right)\left(\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right), \left(\begin{smallmatrix}-13 & 4\\ 42 & -13\end{smallmatrix}\right)\left(\begin{smallmatrix}1 & 0\\ -22 & 1\end{smallmatrix}\right)\left(\begin{smallmatrix}1 & 0\\ 0 & 11\end{smallmatrix}\right)\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right), \ldots,\\
&\left(\begin{smallmatrix}-13 & 4\\ 42 & -13\end{smallmatrix}\right)\left(\begin{smallmatrix}-1 & -5\\ 0 & -1\end{smallmatrix}\right)\left(\begin{smallmatrix}1 & 0\\ 0 & 11\end{smallmatrix}\right)\left(\begin{smallmatrix}1 & 10\\ 0 & 1\end{smallmatrix}\right),\\
&\left(\begin{smallmatrix}-13 & 4\\ 42 & -13\end{smallmatrix}\right)\left(\begin{smallmatrix}1 & -4\\ 0 & 1\end{smallmatrix}\right)\left(\begin{smallmatrix}1 & 0\\ 0 & 11\end{smallmatrix}\right)\left(\begin{smallmatrix}66 & 5\\ 13 & 1\end{smallmatrix}\right) = \left(\begin{smallmatrix}-13 & 4\\ 42 & -13\end{smallmatrix}\right)\left(\begin{smallmatrix}1 & -4\\ 0 & 1\end{smallmatrix}\right)\left(\begin{smallmatrix}6 & 5\\ 13 & 11\end{smallmatrix}\right)\left(\begin{smallmatrix}11 & 0\\ 0 & 1\end{smallmatrix}\right)\}.
\end{aligned}$$

Following the discussion in the previous section, the Hecke matrix is $A = \left(\begin{smallmatrix}0 & -1 & 2\\ 4 & -4 & 3\\ -1 & 1 & 4\end{smallmatrix}\right)$ in our fundamental equation

$$((p+1)I-A)(\int_Q^R \omega_i) = (\sum_j \int_Q^{Q_j} \omega_i - \sum_j \int_R^{R_j} \omega_i).$$

- **Algorithm 2.4.1 and results:** In Step 1 of Algorithm 2.4.1, linear algebra over $\mathbb{C}$ gives a power series expansion of the differential form ω_0 at $j = j(Q)$:

$$\omega_0 = \frac{1}{3^4\cdot 5^2\cdot 13} + \frac{23}{3^{10}\cdot 5^5\cdot 13}(j-j(Q)) + \frac{4}{3^{13}\cdot 5^7\cdot 13}(j-j(Q))^2 + \frac{437174}{3^{22}\cdot 5^{10}\cdot 13^3}(j-j(Q))^3 + \frac{138504533}{3^{28}\cdot 5^{13}\cdot 13^4}(j-j(Q))^4 + O((j-j(Q))^5)\ \ d(j-j(Q)).$$

The Hecke images can be found by computing the roots of the modular polynomial equation $\Phi_{11}(j(Q),x)=0$. Next, we compute the integrals as in Step 3. We record our results in the following table.

$\sum_{i=0}^{11}\int_{Q_i}^{Q}\omega_0$	$10\cdot 11^{-1}+9+9\cdot 11+6\cdot 11^2+7\cdot 11^3+9\cdot 11^4+O(11^5)$
$\sum_{i=0}^{11}\int_{Q_i}^{Q}\omega_1$	$8\cdot 11^{-1}+7+7\cdot 11+2\cdot 11^2+6\cdot 11^3+6\cdot 11^4+O(11^5)$
$\sum_{i=0}^{11}\int_{Q_i}^{Q}\omega_2$	$10\cdot 11^{-1}+8+8\cdot 11+11^2+9\cdot 11^4+O(11^5)$
$\sum_{i=0}^{11}\int_{R_i}^{R}\omega_0$	$7\cdot 11^{-1}+2+3\cdot 11+9\cdot 11^2+3\cdot 11^3+5\cdot 11^4+O(11^5)$
$\sum_{i=0}^{11}\int_{R_i}^{R}\omega_1$	$6+6\cdot 11+11^3+5\cdot 11^4+O(11^5)$
$\sum_{i=0}^{11}\int_{R_i}^{R}\omega_2$	$7\cdot 11^{-1}+4+11+10\cdot 11^2+10\cdot 11^3+5\cdot 11^4+O(11^5)$

Table 3.3: Coleman Integrations on $X_{ns}^{+}(13))$

Part II

Decoding Failures of BIKE

Chapter 4

Preliminaries

4.1 Introduction

Most cryptosystems implemented today rely on certain hard problems in number theory, such as factorisation or the discrete log problem. These problems fall into the general category of Hidden Subgroup Problems. Recently, there has been significant research on quantum computers and quantum algorithms which make use of quantum phenomena to solve some of these problems that are deemed difficult on classical computers([Sho99, Joz01]).

While building a large-scale quantum computer is an engineering challenge, some scientists predict that within the twenty to fifty years, sufficiently powerful quantum computers will be built to break most if not all current public key cryptography infrastructure. Taking into account the amount of time to implement quantum resistant cryptosystems in public, the National Institute of Standards and Technology (NIST) initiated a process in 2016 to standardise post-quantum digital signature algorithms (DSA), public-key encryption (PKE), and key-encapsulation mechanisms (KEM). Initially, there were 82 submissions. As of April 2023, there 4 algorithms are selected for standardisation while there are three code-based candidates that are still going through evaluation.

	PKE/KEM	DSA
Selected		
Lattice	1	2
Hash	0	1
Candidates		
Code	0	3

Table 4.1: NIST Post-Quantum Standardisation Process - Round 4

There is also an on-ramp call for new DSA's in order to diversify the signature portfolio to include signature schemes that are not based on lattices.

In this document, we focus on code-based cryptography, more specifically, one of the 4th round candidates in NIST's standardisation process, BIt-flipping Key Encapsulation (BIKE) [The22a]. In 1978, McEliece introduced the use of error-correcting codes in cryptography [McE78]. Originally, error-correcting codes are used in telecommunications in which one party transmits a message through a noisy channel and the recipient recovers the original message from a noisy codeword. In McEliece's proposal, one would use a structured code and hide a message by adding as many errors as the decoder can remove so that the codewords are indistinguishable from random codes. So far, there are no major classical or quantum attacks on the McEliece system but the downside is that it suffers from having large key sizes which make implementations costly.

BIKE is an instance of a more general scheme, called Quasi-Circulant Moderate Density Parity Check (QC-MDPC) codes [MTSB13]. QC-MDPC codes have much smaller key sizes compared to the McEliece cryptosystem and have not suffered from major attacks. One difference between QC-MDPC codes and McEliece's variants is that QC-MDPC codes use decoders which depend on probabilitistic properties, not algebraic ones. Therefore, one expects decoding failures to occur. Furthermore, decoding failures also reveal information about the secret key. An attack by [GJS16] exploits these failures by collecting a set of failure-causing inputs and recover the secret key. With this in mind, one needs to consider the use of ephemeral versus statis keys in applications and also verify certain security conditions, called indistinguishability under chosen cipher attack

(IND-CCA).

NIST has considered BIKE as one of the promising candidates and has expressed concerns about its IND-CCA security and decoding failure analysis. Our approach to this problem is to study a scaled-down version of BIKE, and identify various properties of QC-MDPC codes and their decoding failures through extensive experiements.

4.2 Preliminaries on coding theory

test

Appendix A

Final notes

Remove me in case of abdominal pain.

Bibliography

[Ass20] Eran Assaf. Computing classical modular forms for arbitrary congruence subgroups. *arXiv: Number Theory*, 2020.

[BBK10] Jennifer S. Balakrishnan, Robert W. Bradshaw, and Kiran S. Kedlaya. Explicit coleman integration for hyperelliptic curves. In Guillaume Hanrot, François Morain, and Emmanuel Thomé, editors, *Algorithmic Number Theory*, pages 16–31, Berlin, Heidelberg, 2010. Springer Berlin Heidelberg.

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[BD17] Jennifer Balakrishnan and Netan Dogra. Quadratic chabauty and rational points ii: Generalised height functions on selmer varieties. *International Mathematics Research Notices*, 04 2017.

[BD18] Jennifer S. Balakrishnan and Netan Dogra. Quadratic Chabauty and rational points, I: p-adic heights. *Duke Math. J.*, 167(11):1981–2038, 2018. With an appendix by J. Steffen Müller.

[BDM$^+$19] Jennifer Balakrishnan, Netan Dogra, J. Steffen Müller, Jan Tuitman, and Jan Vonk. Explicit Chabauty–Kim for the split Cartan modular curve of level 13. *Annals of Mathematics*, 189(3):885 – 944, 2019.

[BDM$^+$21] Jennifer Balakrishnan, Netan Dogra, Jan Müller, Jan Tuitman, and Jan Vonk. Quadratic chabauty for modular curves: Algorithms and examples. *Preprint, 2101.01862*, 01 2021.

[BN20] François Brunault and Michael Neururer. Fourier expansions at cusps. *The Ramanujan Journal*, 53(2):423–437, Nov 2020.

[BP11] Yuri Bilu and Pierre Parent. Serre's uniformity problem in the split Cartan case. *Ann. of Math. (2)*, 173(1):569–584, 2011.

[BPR13] Yuri Bilu, Pierre Parent, and Marusia Rebolledo. Rational points on $X_0^+(p^r)$. *Ann. Inst. Fourier (Grenoble)*, 63(3):957–984, 2013.

[BT20] Jennifer S. Balakrishnan and Jan Tuitman. Explicit coleman integration for curves. *Mathematics of Computation*, 89:2965–2984, 2020.

[BT22] Jennifer Balakrishnan and Jan Tuitman. Magma code. `https://github.com/jtuitman/Coleman`, 2022.

[CdS88] Robert Coleman and Ehud de Shalit. p-adic regulators on curves and special values of p-adic L-functions. *Invent. Math.*, 93(2):239–266, 1988.

[Col85a] Robert F. Coleman. Effective Chabauty. *Duke Mathematical Journal*, 52(3):765 – 770, 1985.

[Col85b] Robert F. Coleman. Torsion points on curves and p-adic abelian integrals. *Ann. of Math. (2)*, 121(1):111–168, 1985.

[Col85c] Robert F. Coleman. Torsion points on curves and p-adic abelian integrals. *Ann. of Math. (2)*, 121(1):111–168, 1985.

[Dic] Leonard E. Dickson. *Linear groups with an exposition of the Galois field theory*. Leipzig, B.G. Teubner, 1901.

[DS05] Fred Diamond and Jerry Shurman. *A first course in modular forms*, volume 228 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2005.

[For81] Otto Forster. *Lectures on Riemann Surfaces*. Springer New York, NY, 1981.

[Gal96] Steven D. Galbraith. Equations for modular curves. *DPhil thesis, University of Oxford*, 1996.

[Gal99] Steven D. Galbraith. Rational points on $X_0^+(p)$. *Experiment. Math.*, 8(4):311–318, 1 1999.

[GJS16] Qian Guo, Thomas Johansson, and Paul Stankovski. A key recovery attack on mdpc with cca security using decoding errors. pages 789–815, 12 2016.

[Joz01] R. Jozsa. Quantum factoring, discrete logarithms, and the hidden subgroup problem. *Computing in Science & Engineering*, 3(2):34–43, 2001.

[Ked01] Kiran S. Kedlaya. Counting Points on Hyperelliptic Curves using Monsky-Washnitzer Cohomology. *arXiv Mathematics e-prints*, page math/0105031, May 2001.

[LMF22] The LMFDB Collaboration. The L-functions and modular forms database. `http://www.lmfdb.org`, 2022.

[Maz77] B. Mazur. Rational points on modular curves. In Jean-Pierre Serre and Don Bernard Zagier, editors, *Modular Functions of one Variable V*, pages 107–148, Berlin, Heidelberg, 1977. Springer Berlin Heidelberg.

[Maz78] B. Mazur. Rational isogenies of prime degree (with an appendix by D. Goldfeld). *Invent. Math.*, 44(2):129–162, 1978.

[McE78] R. J. McEliece. A Public-Key Cryptosystem Based On Algebraic Coding Theory. *Deep Space Network Progress Report*, 44:114–116, January 1978.

[Mer18] Pietro Mercuri. Equations and rational points of the modular curves $X_0^+(p)$. *Ramanujan J.*, 47(2):291–308, 2018.

[MSD74] B. Mazur and P. Swinnerton-Dyer. Arithmetic of weil curves. *Invent Math*, 25:1–61, 1974.

[MTSB13] Rafael Misoczki, Jean-Pierre Tillich, Nicolas Sendrier, and Paulo S. L. M. Barreto. Mdpc-mceliece: New mceliece variants from moderate density parity-check codes. In *2013 IEEE International Symposium on Information Theory*, pages 2069–2073, 2013.

[Ser72] J.-P. Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Inv. Math.*, 15:259–3319, 1972.

[Shi94] Goro Shimura. *Introduction to the arithmetic theory of automorphic functions*, volume 11 of *Publications of the Mathematical Society of Japan*. Princeton University Press, Princeton, NJ, 1994. Reprint of the 1971 original, Kanô Memorial Lectures, 1.

[Sho99] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Review*, 41(2):303–332, 1999.

[Sik17] Samir Siksek. Quadratic chabauty for modular curves. *Preprint, 1704.00473*, 04 2017.

[Sta75] H. M. Stark. On complex quadratic fields with class-number two. *Mathematics of Computation*, 29(129):289–302, 1975.

[Ste07] William Stein. *Modular forms, a computational approach*, volume 79 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2007. With an appendix by Paul E. Gunnells.

[The22a] The BIKE Developers. *BIKE: Bit-Flipping Key Encapsulation*, 2022. `https://bikesuite.org/`.

[The22b] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.6.1)*, 2022. `https://www.sagemath.org`.

[Tui16] Jan Tuitman. Counting points on curves using a map to $\mathbf{P}^1$, i. *Math. Comput.*, 85:961–981, 2016.

[Tui17] Jan Tuitman. Counting points on curves using a map to $\mathbf{P}^1$, II. *Finite Fields and Their Applications*, 45:301–322, 05 2017.

[Wet97] Joseph L. Wetherell. *Bounding the number of rational points on certain curves of high rank*. PhD thesis, 1997.

[Zyw20] David Zywina. Computing actions on cusp forms. *arXiv: Number Theory*, 2020.