UNIVERSITY OF CALIFORNIA SAN DIEGO

The Title Of The Dissertation

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 crves. 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 [**?**, **?**] 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 [**?**, **?**], 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. **TODO: successful examples?**

There are several approaches to numerically compute these Coleman integrals. Wetherell [**?**] 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 [**?**, **?**, **?**, **?**]. 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 $Gal(\bar{K}/K)$, giving rise to a representation $\rho_{p,E} : Gal(\bar{K}/K) \to GL_2(\mathbb{F}_p)$. In [**?**], 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, does 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 $H \leq GL_2(\mathbb{F}_p)$ be a proper subgroup such that the determinant map $\mathrm{Det} : H \to \mathbb{F}_p^\times$ is surjective. Does 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 $GL_2(\mathbb{F}_p)$. 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 $GL_2(\mathbb{F}_p)$ is known, originally due to [**?**]:

Theorem 1.1.5. *Let $H \leq GL_2(\mathbb{Z}/p\mathbb{Z})$ not containing $SL_2(\mathbb{Z}/p\mathbb{Z})$. 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 $PGL_2(\mathbb{F}_p)$ is isomorphic to A_4, S_4 or A_5.*

Most of the cases have been resolved [**?**, **?**, **?**, **?**], 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 [**?**] and level 17 [**?**].

Since most modular curves satisfy the quadratic Chabauty bound [**?**], 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 [**?**].

Let $\mathbb{H} := \{\tau \in \mathbb{C} : Im(\tau) > 0\}$ be the upper half complex plane. The special linear group $SL_2(\mathbb{Z})$ 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 be function $f : \mathbb{H} \to \mathbb{C}$ and $k \in \mathbb{Z}$.

- The *automorphy factor* is a function

$$j : GL_2^+(\mathbb{R}) \times \mathbb{H} \to \mathbb{C}$$
$$(\gamma, z) \mapsto cz + d$$

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

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

$$(\,\cdot\,)|_k(\,\cdot\,) : \mathrm{Hom}(\mathbb{H}, \mathbb{C}) \times GL_2^+(\mathbb{R}) \to \mathrm{Hom}(\mathbb{H}, \mathbb{C})$$
$$(f(z), \gamma) \mapsto (f|_k\gamma)(z) := (\mathrm{Det}\,\gamma)^{k-1} j(\gamma, z)^{-k} f(\gamma \cdot z)$$

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 $GL_2^+(\mathbb{R})$ 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 $\pi : SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/N\mathbb{Z})$. We define congruence subgroups in the following way.

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

- $\Gamma(N) = \pi^{-1}(\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z}) : \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \pmod N\}$
- $\Gamma_1(N) = \pi^{-1}(\{\left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right)\}) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z}) : \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right) \pmod N\}$
- $\Gamma_0(N) = \pi^{-1}(\{\left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right)\}) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z}) : \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right) \pmod N\}$

Definition 1.2.3. $\Gamma \leq SL_2(\mathbb{Z})$ 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 $SL_2(\mathbb{Z})$ have finite index and correspond to subgroups of $SL_2(\mathbb{Z}/N\mathbb{Z})$. The above examples are allcongruence subgroups of level N.

Definition 1.2.4. Let $\Gamma \leq SL_2(\mathbb{Z})$ 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 $\alpha \in SL_2(\mathbb{Z})$, i.e., $(f|_k\alpha)(z)$ is bounded as $z \to i\infty$.

If, in addition, $f|_k\alpha$ vanishes at infinity for all $\alpha \in SL_2(\mathbb{Z})$, 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 $SL_2(\mathbb{Z})$ called *Eisenstein series*.

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

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

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 $X(\Gamma)$ (see next section).

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

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 $\Gamma \leq Sl_2(\mathbb{Z})$ 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 $\Gamma \leq SL_2(\mathbb{Z})$. The associated modular curve $X(\Gamma)$ has the structure of a compact Riemann surface. Compact Riemann surfaces and complex algebraic curves are equivalent notions [**?**]. Note that we are also considering modular curves where the determinant map on the subgroup $H \leq GL_2(\mathbb{Z}/N\mathbb{Z})$ is surjective. By Theorem 7.6.3 in [**?**], 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:*

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

$$C \mapsto k(C)$$

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 $\Gamma \leq SL_2(\mathbb{Z})$, 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 $\phi : E[N] \to (\mathbb{Z}/N\mathbb{Z})^2$. 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 $H \leq GL_2(\mathbb{Z}/N\mathbb{Z})$ 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 $\Gamma_H(N) = \{A \in SL_2(\mathbb{Z}) : A \pmod N \in H\}$, 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 [**?**] 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. ([**?**] Prop. 5.2.1) The theory of Hecke operators can be 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:

$$T_p f = \begin{cases} \sum_{i=0}^{p-1} f|_k\left(\begin{smallmatrix}1 & j\\ 0 & p\end{smallmatrix}\right), & \text{if } p|N, \\ \sum_{i=0}^{p-1} f|_k\left(\begin{smallmatrix}1 & j\\ 0 & p\end{smallmatrix}\right) + f|_k(\left(\begin{smallmatrix}m & n\\ N & p\end{smallmatrix}\right)\left(\begin{smallmatrix}p & 0\\ 0 & 1\end{smallmatrix}\right)), & \text{if } p \nmid N, \text{ where } mp - nN = 1. \end{cases}$$

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:

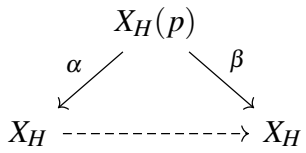
$$\begin{array}{ccccccc} \Gamma_2 & \hookleftarrow & \Gamma_3 & \xrightarrow{\cong} & \Gamma_3' & \hookrightarrow & \Gamma_1 \\ X_2 & \xleftarrow{\pi_2} & X_3 & \xrightarrow{\cong} & X_3' & \xrightarrow{\pi_1} & X_1 \end{array}$$

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.



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 [**?**, **?**] 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. *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, $\int_P^P \omega = 0$,*
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. *The integral is compatible with the action of $Gal(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$,*
5. *Let $P_0 \in X(\overline{\mathbb{Q}}_p)$ be fixed. 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,*
6. *We have additivity of endpoints:*

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

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. $\int_P^Q df = f(Q) - f(P)$,

9. *If $P, Q \in X(\mathbb{Q}_p)$ then $\int_P^Q \omega \in \mathbb{Q}_p$.*

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 [**?**], 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 [**?**] and this is generalized to arbitrary smooth curves [**?**, **?**, **?**]. 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, we have:

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

where A is the Hecke matrix 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-isogeneous to Q and R, therefore, the Eichler-Shimura relation ([**?**] 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 [**?**] and [**?**]. In [**?**], 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 [**?**]:

- 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. *([?] 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. *([?] 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 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* $j(Q)$ *and* $j(Q) - 1728$*.*
- *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:

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

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.*

Part II

Decoding Failures of BIKE

Chapter 3

Preliminaries

Appendix A

Final notes

Remove me in case of abdominal pain.