Washington, 6 January, 2026

JMM 2026

UNIVERSITY OF WATERLOO

ORIENTATIONS, MODULAR SYMBOLS & p-ADIC PERIODS FOR CRYPTOGRAPHY

LEONARDO COLÒ

CONTENTS

- Supersingular isogeny graphs.
- Bruhat-Tits trees.
- Modular curves and level structures.
- Attaching modular symbols to orientations.
- p-adic integrals.
- Cryptographic constructions.

ISOGENY GRAPHS, ORIENTATIONS & BRUHAT-TITS TREES

ISOGENY GRAPHS

Definition

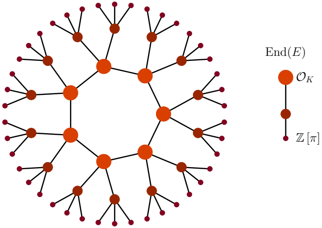
Given an elliptic curve E over k, and a finite set of primes S, we can associate an isogeny graph $G_S(E)$

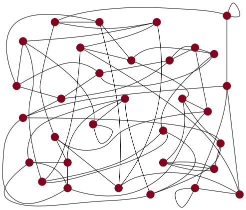
- whose vertices are elliptic curves isogenous to E over $\bar{k}$, and
- whose edges are isogenies of degree $\ell \in S$.

If $S = \{\ell\}$, then we write $G_\ell(E)$, the ℓ-isogeny graph.

The vertices are defined up to $\bar{k}$-isomorphism and the edges from a given vertex are defined up to a $\bar{k}$-isomorphism of the codomain.

The ℓ-isogeny graph of E is $(\ell + 1)$-regular (as a directed multigraph).

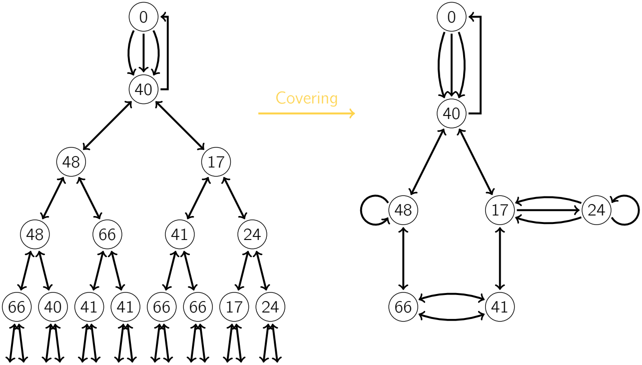




IDEAL CLASSES AND ORIENTED SUPERSINGULAR CURVES

Theorem

The category of K-oriented supersingular elliptic curves (E, ι), whose morphisms are isogenies commuting with the K-orientations, is equivalent to the category of elliptic curves with CM by K.



THE BRUHAT-TITS TREE

Definition

The Bruhat-Tits tree associated to $\mathrm{PGL}_2(\mathbb{Q}_\ell)$ is the graph $\mathcal{B}_\ell$ such that

- homothety classes of lattices of $\mathbb{Q}_\ell^2$.
- edges represent set of pairs of adjacent homothety classes.

- A lattice L of $\mathbb{Q}_\ell^2$ is a free $\mathbb{Z}_\ell$-module of rank 2 in $\mathbb{Q}_\ell^2$
- We say that two lattices L_1 and L_2 are homothetic if there exists $\lambda \in \mathbb{Q}_\ell^\times$ such that $L_1 = \lambda L_2$.
- Two homothety classes $[L_1]$ and $[L_2]$ are adjacent if their representatives L_1 and L_2 can be chosen so that $\ell L_1 \subset L_2 \subset L_1$.

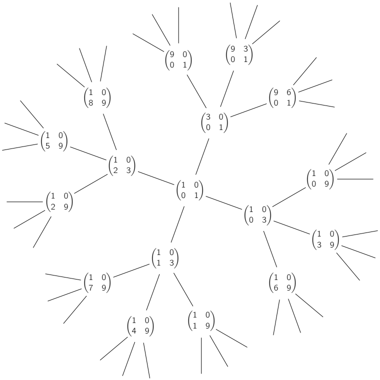
$\mathcal{B}_\ell$ is an Infinite $(\ell + 1)$-regular tree encoding lattices in $\mathbb{Q}_\ell^2$.

THE BRUHAT-TITS TREE - EXAMPLE

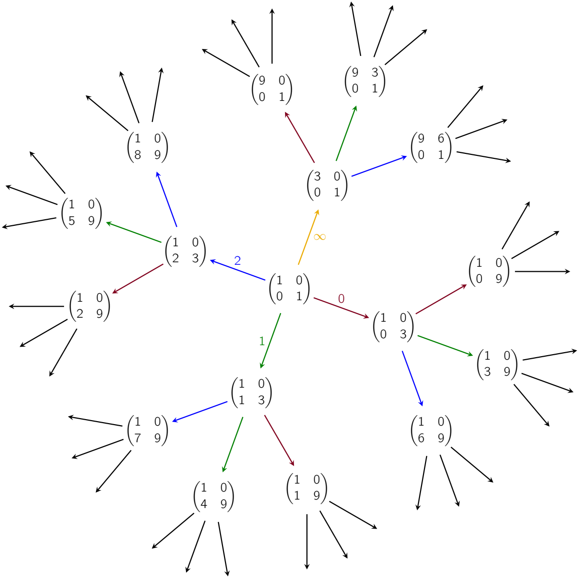
L.COLÒ UWAT

There are several equivalent ways to define $\mathcal{B}_\ell$

- homothety classes of lattices of $\mathbb{Q}_\ell^2$.
- classes of matrices in $\mathrm{PGL}_2(\mathbb{Q}_\ell)/\mathrm{PGL}_2(\mathbb{Z}_\ell)$.
- maximal orders in the quaternion algebra $M_2(\mathbb{Q}_\ell)$.



NAVIGATING THE BRUHAT-TITS TREE - EXAMPLE



MODULAR SYMBOLS AND RELATIVE HOMOLOGY

THE MODULAR CURVE $X_0(N)$ AND ITS CUSPS

Let $\Gamma_0(N) \subset \mathrm{SL}_2(\mathbb{Z})$ be the congruence subgroup of level N defined by

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

The modular curve $X_0(N)$ is the compact Riemann surface (and smooth projective algebraic curve over $\mathbb{Q}$) obtained by compactifying the quotient

$$Y_0(N) = \Gamma_0(N) \backslash \mathbb{H}$$

by adding finitely many cusps C, corresponding to the $\Gamma_0(N)$-orbits in $\mathbb{P}^1(\mathbb{Q})$. We denote by $g = g(X_0(N))$ the genus of $X_0(N)$ and by

$$C = \{c_1, \ldots, c_c\}$$

the finite set of cusps, where $c = \#C$.

RELATIVE HOMOLOGY & MANIN SYMBOLS

We let H denote the relative homology group

$$H := H_1(X_0(N), C; \mathbb{Z}).$$

In practice, one often chooses a set of representatives for $\Gamma_0(N)\backslash \mathrm{SL}_2(\mathbb{Z})$ and works with *Manin symbols* indexed by cosets.

roposition

Let $g = g(X_0(N))$ be the genus of $X_0(N)$ and let $c = \#C$ be the number of cusps. Then

$$\mathrm{rank}_{\mathbb{Z}} H_1(X_0(N), C; \mathbb{Z}) = 2g + (c - 1).$$

ATTACH MODULAR SYMBOL TO AN ORIENTATION

BRANDT HOMOLOGY

Input: An $\mathcal{O}$–oriented supersingular elliptic curve (E_0, ι_0) and an ideal class $[\mathfrak{a}] \in \mathrm{Pic}(\mathcal{O})$.

- Supersingular curves with orientation correspond to left ideal classes in a definite quaternion algebra:

$$(E, \iota) \leftrightarrow [I] \in \mathcal{C}\ell(\mathcal{O}_B).$$

- The Brandt module

$$\mathbb{B} = \mathbb{Z}[\mathcal{C}\ell(\mathcal{O}_B)]$$

  carries a Hecke action.
- Via Jacquet–Langlands + Eichler–Shimura:

$$\iota_{\mathrm{JL}} : \mathbb{B} \hookrightarrow H_1(X_0(N), C; \mathbb{Z}) \otimes \mathbb{Q}.$$

- $\mathrm{Pic}(\mathcal{O})$ acts by permuting ideal classes; transporting a fixed base cycle gives:

$$\gamma^{(1)}([\mathfrak{a}]) := \rho([\mathfrak{a}])(\gamma_0) \in H_1(X_0(N), C; \mathbb{Z}).$$

GEOMETRIC GEODESIC CYCLES ON $X_0(N)$

Input: The same ideal class $[\mathfrak{a}]$.

- CM theory yields a Heegner point:

$$[\mathfrak{a}] \longmapsto x_{\mathfrak{a}} \in X_0(N)(\mathbb{C}),$$

  compatible with the class group action.

- Fix:

$$x_0 := x_{\mathcal{O}_f}, \qquad c_\infty \in \text{cusps}.$$

  Choose analytic paths:

$$\delta_{\mathfrak{a}} : x_{\mathfrak{a}} \to c_\infty, \qquad \delta_0 : x_0 \to c_\infty.$$

- Relative homology:

$$\gamma^{(2)}([\mathfrak{a}]) := \delta_{\mathfrak{a}} - \delta_0 \in H_1(X_0(N), C; \mathbb{Z}).$$

  This is well-defined modulo absolute cycles and depends only on $[\mathfrak{a}]$.

BRUHAT-TITS GRAPH AND HARMONIC COCYCLES

L.COLÒ UWAT

Input: Same ideal class $[\mathfrak{a}]$.

- By Cerednik–Drinfeld uniformization, $X_0(N)$ admits a p-adic model whose skeleton is:

$$\Gamma\backslash\mathcal{T}_p,$$

where $\mathcal{T}_p$ is the Bruhat–Tits tree of $\mathrm{PGL}_2(\mathbb{Q}_p)$.

- Vertices correspond to oriented supersingular curves (or their p-adic lifts).
- The class-group action induces an *oriented path*:

$$v_0 \rightsquigarrow v_{\mathfrak{a}} \quad \text{in } \Gamma\backslash\mathcal{T}_p.$$

- Closing this path to a fixed base reference edge yields a graph cycle

$$c_{\mathfrak{a}} \in H_1(\Gamma\backslash\mathcal{T}_p; \mathbb{Z}).$$

- Via the harmonic cocycle isomorphism:

$$\gamma^{(3)}([\mathfrak{a}]) := \Phi(c_{\mathfrak{a}}) \in H_1(X_0(N), C; \mathbb{Z}).$$

p-ADIC PERIOD VECTORS AND COLEMAN INTEGRALS

WEIGHT-2 CUSP FORMS AND THE PERIOD PAIRING

$S_2(\Gamma_0(N))$ is the space of weight-2 cusp forms of level $\Gamma_0(N)$.

Definition

Let f be a weight-2 cusp form for $\Gamma_0(N)$. We define *period pairing* as

$$\langle f, \gamma \rangle = \int_\gamma f(z)\, dz,$$

Let $f_1, \ldots, f_d$ be a fixed collection of weight-2 cusp forms For $\gamma \in H$, we define the (infinite precision) p-adic period vector

$$\Pi(\gamma) := \left(\langle f_1, \gamma \rangle_p, \ldots, \langle f_d, \gamma \rangle_p\right) \in \mathbb{Q}_p^d.$$

Definition

Let q be a prime distinct from p and not dividing N. For $m \geq 1$ and $\gamma \in H$, the *truncated p-adic period vector* of γ is

$$\Pi_m(\gamma) := \left(\langle f_1, \gamma \rangle_p, \ldots, \langle f_d, \gamma \rangle_p\right) \bmod p^m \in (\mathbb{Z}/p^m\mathbb{Z})^d.$$

p-ADIC INTEGRATION - THE PROBLEM

L.COLÒ UWAT

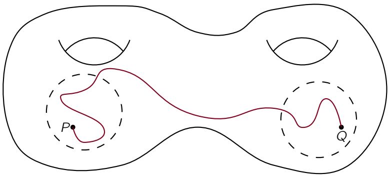
Is there a Theory of p-adic integration?

We cannot use the same methods that we have in $\mathbb{R}$ or in $\mathbb{C}$ because of the totally disconnected topology of rigid analytic spaces.

Theorem (Coleman)

- Additivity at points: $\int_P^Q \omega + \int_Q^R \omega = \int_P^R \omega$
- Linearity on forms: $\lambda_1 \int_P^Q \omega_1 + \lambda_2 \int_P^Q \omega_2 = \int_P^Q (\lambda_1\omega_1 + \lambda_2\omega_2)$
- Change of variables: if X' is another rigid space and $\Psi : X \to X'$ is a rigid analytic map, then $\int_P^Q \Psi^*\omega' = \int_{\Psi(P)}^{\Psi(Q)} \omega'$.
- Fundamental Theorem of Calculus: $\int_P^Q df = f(Q) - f(P)$.

There is no obvious way of integrating over affinoids.

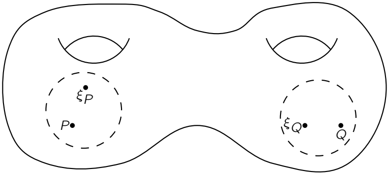


Coleman's Solution

- Cover the Affinoid space by residue disks.
- Integrate on each residue disk.
- **Problem:** Residue disks have no intersection.
- Connect integrals on different residue disks using Frobenius.

COLEMAN INTEGRATION

There is no obvious way of integrating over affinoids.



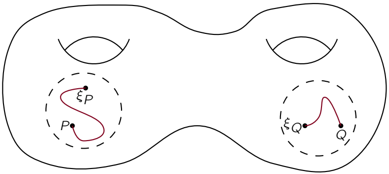
Coleman's Solution

- Find Teichmüller points

$$\int_P^Q \omega = \int_P^{\xi_P} \omega + \int_{\xi_P}^{\xi_Q} \omega + \int_{\xi_Q}^{Q} \omega$$

COLEMAN INTEGRATION

There is no obvious way of integrating over affinoids.



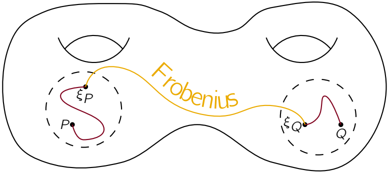
Coleman's Solution

- Find Teichmüller points
- Compute tiny integrals

$$\int_P^Q \omega = \int_P^{\xi_P} \omega + \int_{\xi_P}^{\xi_Q} \omega + \int_{\xi_Q}^{Q} \omega$$

COLEMAN INTEGRATION

There is no obvious way of integrating over affinoids.



Coleman's Solution

- Find Teichmüller points
- Compute tiny integrals
- Connect integrals using Frobenius

$$\int_P^Q \omega = \int_P^{\xi_P} \omega + \int_{\xi_P}^{\xi_Q} \omega + \int_{\xi_Q}^{Q} \omega$$

COMPUTING INTEGRALS ON $X_0(N)$

L.COLÒ UWAT

Computing $\int_Q^R \omega$ for $Q, R \in X = X_0(N)$ and $\omega \in H^0(X, \Omega^1)$

We can leverage the existence of Hecke operators.

Algorithm (Chen, Kedlaya, Lau)

- Write $\int_Q^R \omega$ as a sum of tiny integrals.
- Find a basis of holomorphic 1-forms and a suitable uniformizer.
- Compute the action of Hecke operators on cusp forms and points
- Write 1-forms as a power series in the uniformizer. This involves algebraic approximation after solving a system of equations over $\mathbb{C}$.
- Formally integrate and evaluate at the end points.

THE MODULAR SYMBOL INVERSION PROBLEM MSI

DEFINITION OF MSI

Let $\Pi_m : H \to (\mathbb{Z}/p^m\mathbb{Z})^d$ be the truncated p-adic period map. Fix parameters L, p, m, d, and consider the following relation.

MSI relation

The *Modular Symbol Inversion relation* R_{MSI} is the subset of $(\mathbb{Z}/p^m\mathbb{Z})^d \times \mathcal{W}_L$ given by

$$R_{\mathrm{MSI}} := \{(y, \gamma) : \gamma \in \mathcal{W}_L,\ y = \Pi_m(\gamma)\}.$$

We will write $(y, \gamma) \in R_{\mathrm{MSI}}$ to mean that γ is a valid "short" homology preimage of y under Π_m.

MSI problem

Given a value $y \in (\mathbb{Z}/p^m\mathbb{Z})^d$ known (or promised) to satisfy $y = \Pi_m(\gamma^\star)$ for some unknown $\gamma^\star \in \mathcal{W}_L$, the *Modular Symbol Inversion (MSI) problem* is to find a $\gamma \in \mathcal{W}_L$ such that $(y, \gamma) \in R_{\mathrm{MSI}}$.

A FIAT-SHAMIR SIGNATURE BASED ON MSI

Public parameters:

$$(p, m, N, q), \quad \Pi_m : H_1(X_0(N), C; \mathbb{Z}) \to (\mathbb{Z}/p^m\mathbb{Z})^d.$$

Public key: $\mathbf{v} = \Pi_m(\gamma)$.
Secret key: short representative γ.

- **Commitment:** Pick random short $r \in H_1(X_0(N), C; \mathbb{Z})$, send

$$c = \Pi_m(r + \gamma).$$

- **Challenge:** Verifier samples

$$b \xleftarrow{\$} \{0, 1, \ldots, q - 1\}.$$

- **Response:** Send

$$z = r + b\gamma.$$

  Apply rejection sampling to ensure $\|z\|$ stays within bounds.

Verification:

$$\Pi_m(z) \stackrel{?}{\equiv} c - b \cdot \mathbf{v} \quad \text{in } (\mathbb{Z}/p^m\mathbb{Z})^d.$$

(Security relies on hardness of MSI: recovering γ from $v = \Pi_m(\gamma)$.)

THANK YOU FOR THE ATTENTION