WATERLOO, 5 JULY 2024

L.COLÒ UWAT

SUPERSINGULAR ISOGENY GRAPHS & GALOIS REPRESENTATIONS

LEONARDO COLÒ

University of Waterloo

Tutte Colloquium

CONTENTS

- Supersingular isogeny graphs.
- Modular curves and level structures.
- Supersingular isogeny graphs with level structure.
- Methods of graphs.
- Galois Representations.

SUPERSINGULAR ISOGENY GRAPHS

ISOGENY GRAPHS

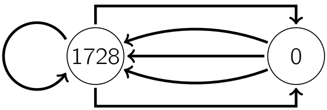
The study of supersingular isogeny graphs has come into vogue in cryptography for their local regularity and global mixing structure; the Ramanujan property.

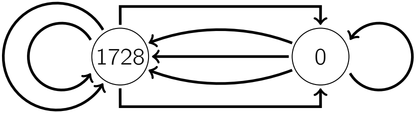
Definition

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 $\ell \in S$.

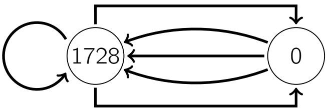
If $S = \{\ell\}$, then we write $G_\ell(E)$, the ℓ-isogeny graph.

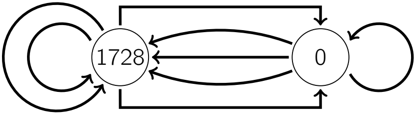




ISOGENY GRAPHS AND ADJACENCY MATRICES

The adjacency matrices of the ℓ-isogeny graphs:





form a system of commuting operators:

$$T_2 = \begin{pmatrix} 1 & 2 \\ 3 & 0 \end{pmatrix} \text{ and } T_3 = \begin{pmatrix} 2 & 2 \\ 3 & 1 \end{pmatrix}$$

whose characteristic polynomials are:

$$(x-3)(x+2) \text{ and } (x-4)(x+1).$$

One can guess that the eigenvalues -2 and -1 are traces of Frobenius on the elliptic curve:

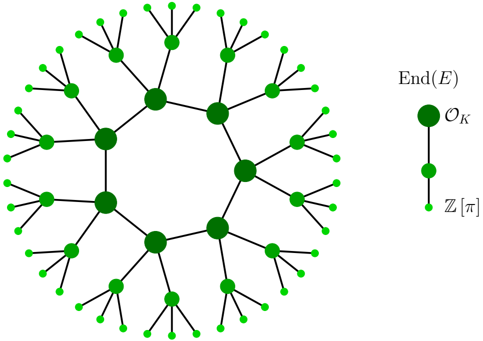
$$X_0(11) : y^2 + y = x^3 - x^2 - 10x - 20.$$

ORDINARY ISOGENY GRAPHS: VOLCANOES

Let $\mathrm{End}(E) = \mathcal{O} \subseteq K$, an imaginary quadratic field. The class group $\mathrm{Cl}(\mathcal{O})$ acts faithfully and transitively on the set of elliptic curves with endomorphism ring $\mathcal{O}$:

$$E \longrightarrow E/E[\mathfrak{a}] \qquad E[\mathfrak{a}] = \{P \in E \mid \alpha(P) = 0 \ \forall \alpha \in \mathfrak{a}\}$$

Thus, the CM isogeny graphs can be modelled by an equivalent category of fractional ideals of K.

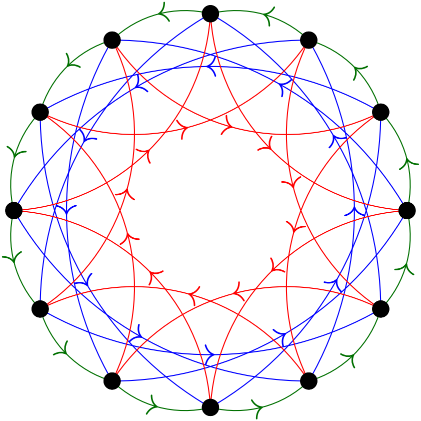


ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

Consider a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$

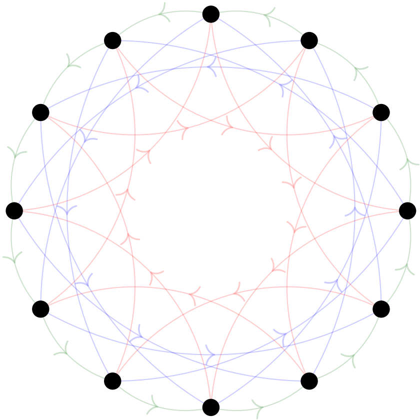


ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

Consider a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$

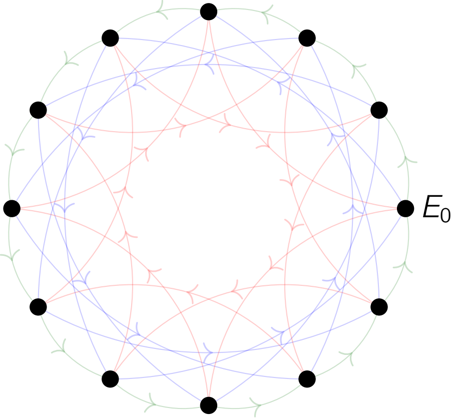


ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

Consider a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$



ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

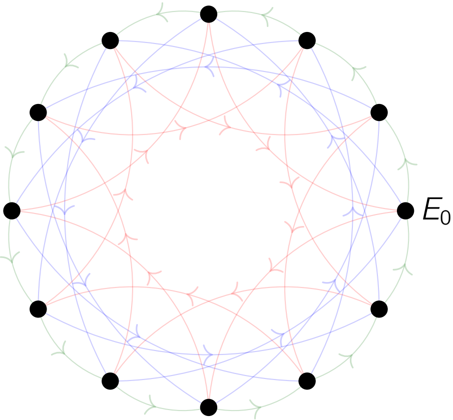
Consider a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$

Alice

$\rho_A = (2, 1, -1)$

$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$



ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

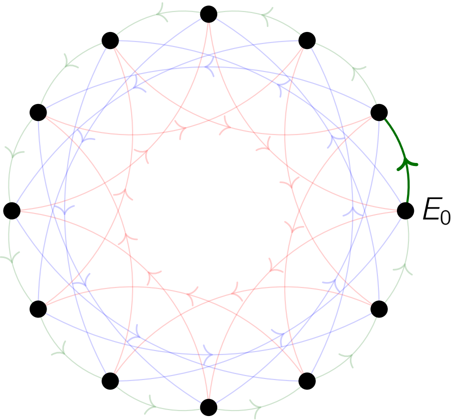
Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

Consider a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$$

Alice

$$\rho_A = (2, 1, -1)$$
$$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$$



ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

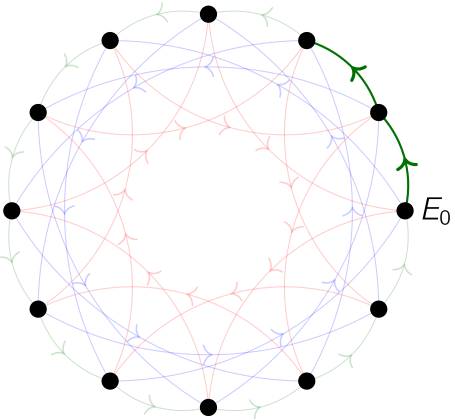
Consider a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$

Alice

$\rho_A = (2, 1, -1)$

$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$



ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

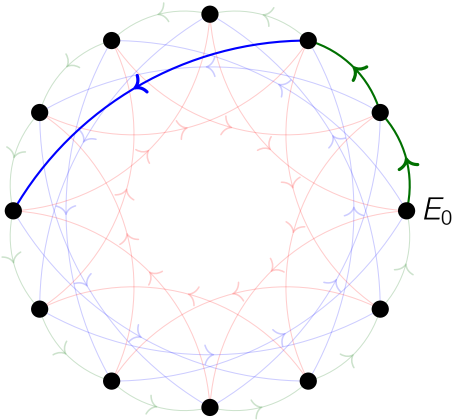
Consider a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$$

Alice

$$\rho_A = (2, 1, -1)$$

$$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$$



ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

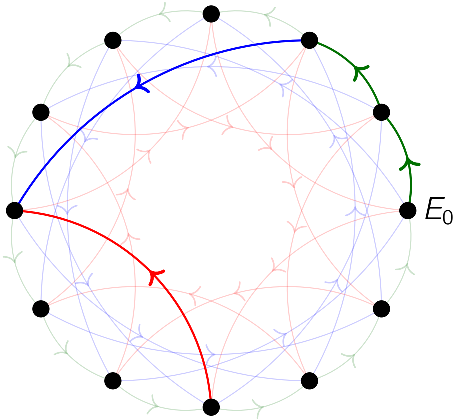
Consider a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$$

Alice

$$\rho_A = (2, 1, -1)$$

$$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$$



ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

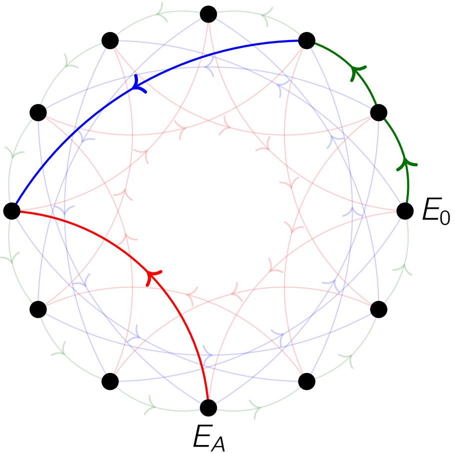
Consider a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$

Alice

$\rho_A = (2, 1, -1)$

$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$

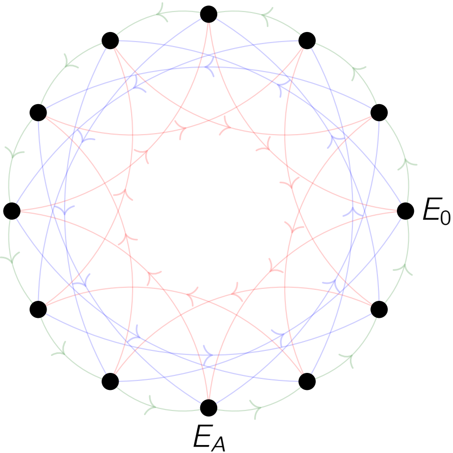


ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

Consider a set of primes $\mathcal{L} = \{\ell_1, \dots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$



Alice

$\rho_A = (2, 1, -1)$

$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$

Bob

$\rho_B = (-2, 0, 1)$

$\mathfrak{a} = \mathfrak{l}_1^{-2} \mathfrak{l}_3^1$

ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

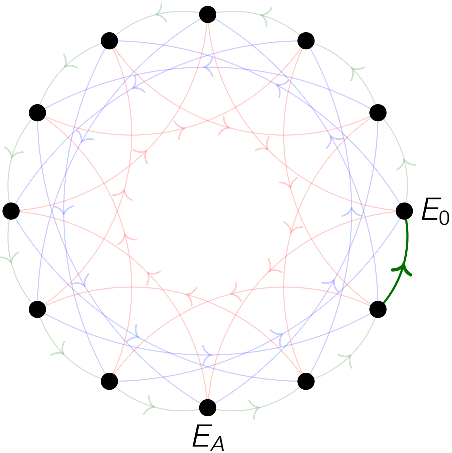
Consider a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$

Alice

$\rho_A = (2, 1, -1)$

$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$



Bob

$\rho_B = (-2, 0, 1)$

$\mathfrak{a} = \mathfrak{l}_1^{-2} \mathfrak{l}_3^1$

ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

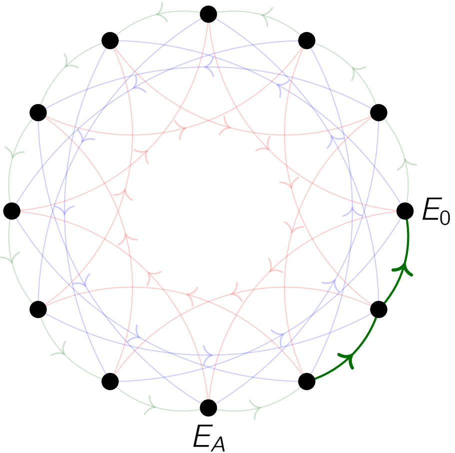
Consider a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$

Alice

$\rho_A = (2, 1, -1)$

$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$



Bob

$\rho_B = (-2, 0, 1)$

$\mathfrak{a} = \mathfrak{l}_1^{-2} \mathfrak{l}_3^1$

ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

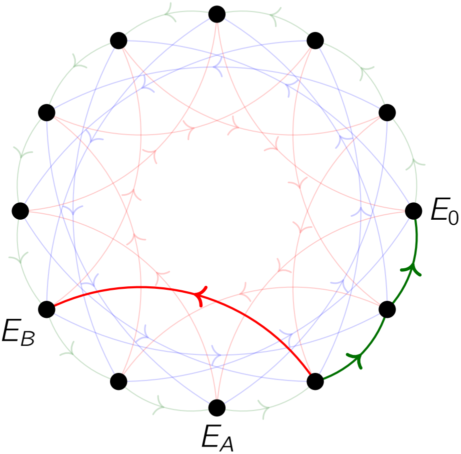
Consider a set of primes $\mathcal{L} = \{\ell_1, \dots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$

Alice

$\rho_A = (2, 1, -1)$

$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$



Bob

$\rho_B = (-2, 0, 1)$

$\mathfrak{a} = \mathfrak{l}_1^{-2} \mathfrak{l}_3^{1}$

ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

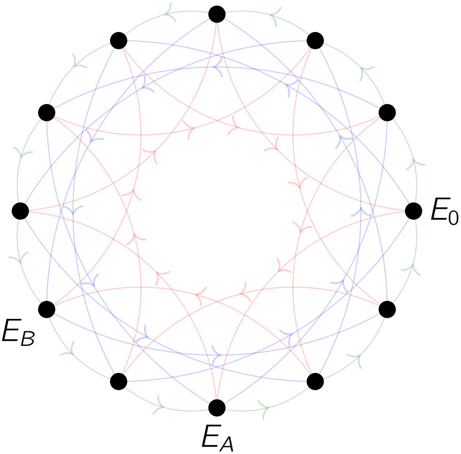
Consider a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$

Alice

$\rho_A = (2, 1, -1)$

$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$



Bob

$\rho_B = (-2, 0, 1)$

$\mathfrak{a} = \mathfrak{l}_1^{-2} \mathfrak{l}_3^1$

ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

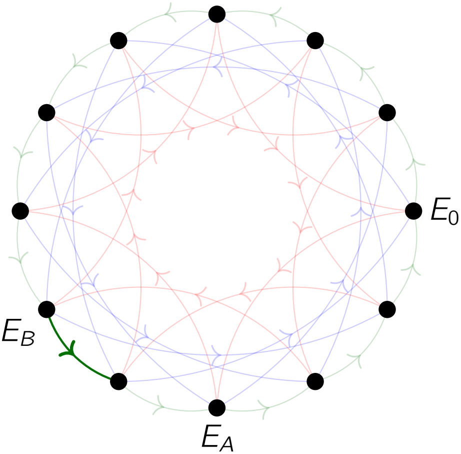
Consider a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$$

Alice

$$\rho_A = (2, 1, -1)$$

$$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$$



Bob

$$\rho_B = (-2, 0, 1)$$

$$\mathfrak{a} = \mathfrak{l}_1^{-2} \mathfrak{l}_3^1$$

ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

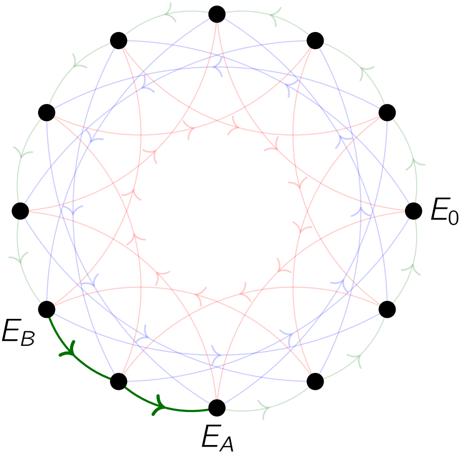
Consider a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$

Alice

$\rho_A = (2, 1, -1)$

$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$



Bob

$\rho_B = (-2, 0, 1)$

$\mathfrak{a} = \mathfrak{l}_1^{-2} \mathfrak{l}_3^1$

Ordinary protocol - Couveignes & Rostovtsev-Stolbunov, 2006

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

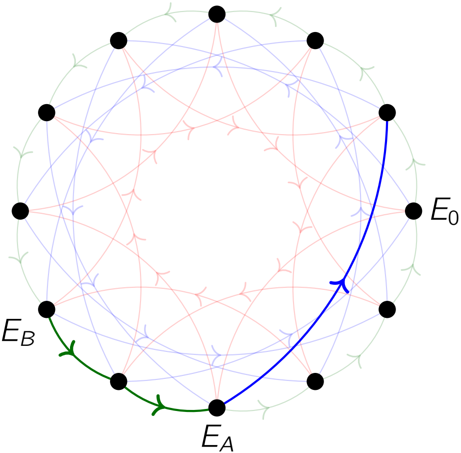
Consider a set of primes $\mathcal{L} = \{\ell_1, \dots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$

Alice

$\rho_A = (2, 1, -1)$

$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$



Bob

$\rho_B = (-2, 0, 1)$

$\mathfrak{a} = \mathfrak{l}_1^{-2} \mathfrak{l}_3^1$

ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

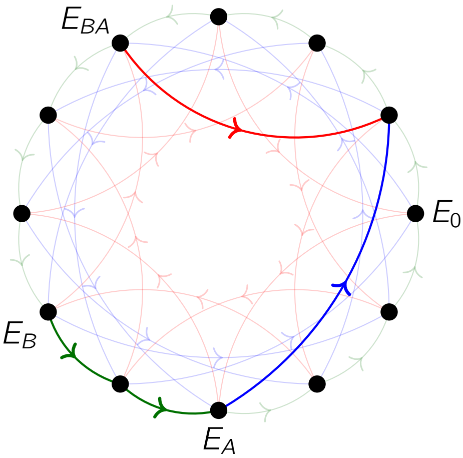
Consider a set of primes $\mathcal{L} = \{\ell_1, \dots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$

Alice

$\rho_A = (2, 1, -1)$

$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$



Bob

$\rho_B = (-2, 0, 1)$

$\mathfrak{a} = \mathfrak{l}_1^{-2} \mathfrak{l}_3^1$

ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

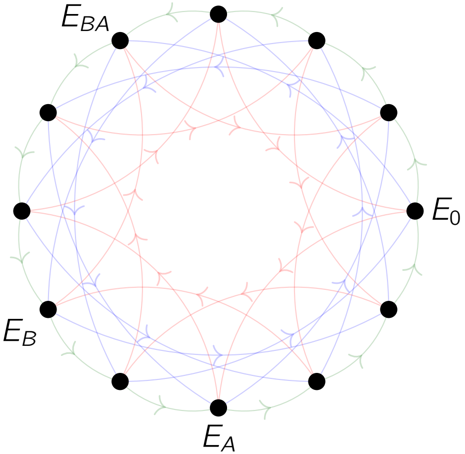
Consider a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$

Alice

$\rho_A = (2, 1, -1)$

$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$



Bob

$\rho_B = (-2, 0, 1)$

$\mathfrak{a} = \mathfrak{l}_1^{-2} \mathfrak{l}_3^1$

ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

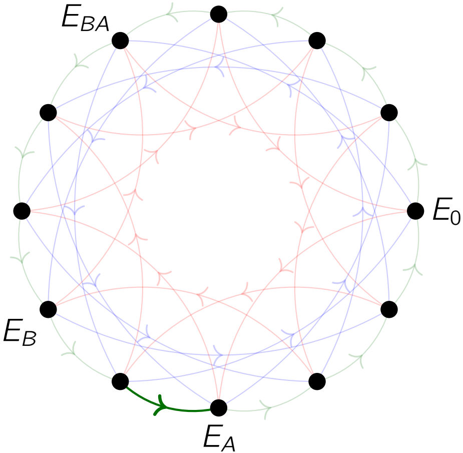
Consider a set of primes $\mathcal{L} = \{\ell_1, \dots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$

Alice

$\rho_A = (2, 1, -1)$

$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$



Bob

$\rho_B = (-2, 0, 1)$

$\mathfrak{a} = \mathfrak{l}_1^{-2} \mathfrak{l}_3^1$

ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

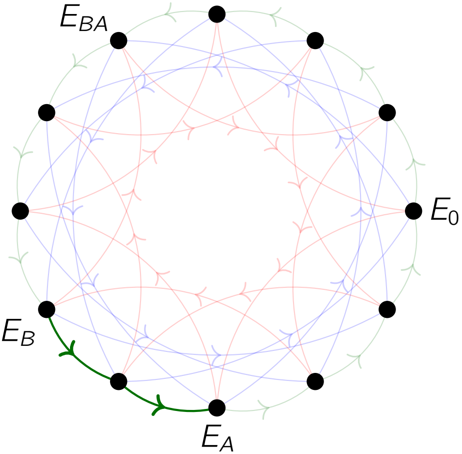
Consider a set of primes $\mathcal{L} = \{\ell_1, \dots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$

Alice

$\rho_A = (2, 1, -1)$

$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$



Bob

$\rho_B = (-2, 0, 1)$

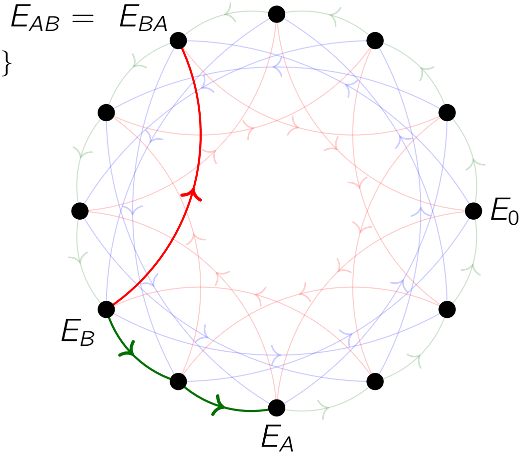
$\mathfrak{a} = \mathfrak{l}_1^{-2} \mathfrak{l}_3^1$

ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

Consider a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$



Alice

$\rho_A = (2, 1, -1)$

$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$

Bob

$\rho_B = (-2, 0, 1)$

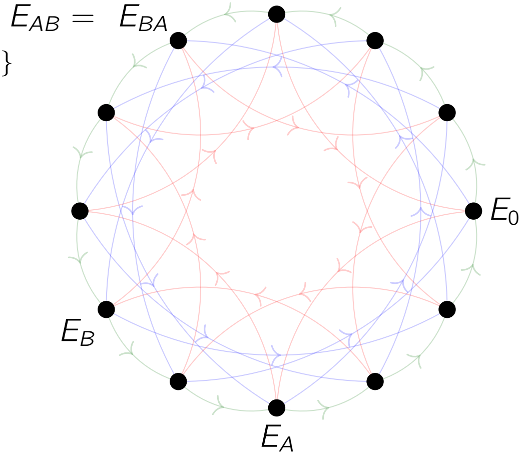
$\mathfrak{a} = \mathfrak{l}_1^{-2} \mathfrak{l}_3^1$

Ordinary Protocol - Couveignes & Rostovtsev-Stolbunov, 2006

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

Consider a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$



Alice

$\rho_A = (2, 1, -1)$

$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$

Bob

$\rho_B = (-2, 0, 1)$

$\mathfrak{a} = \mathfrak{l}_1^{-2} \mathfrak{l}_3^1$

SUPERSINGULAR ISOGENY GRAPHS - ORIGINS

The study of these isogeny graphs, in the guise of the theory of left ideal of a maximal quaternion order, goes back to Brandt (1943).

Eichler (1955) extended the theory to so-called Eichler orders, corresponding to a $\Gamma_0(N)$-structure on the underlying elliptic curves.

In this Brandt–Eichler framework, the objective is to have explicit models for modular forms and their Hecke action, with the view to studying the associated Galois representations.

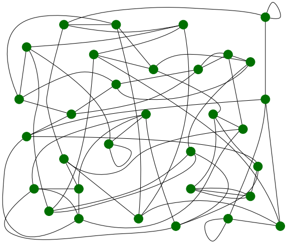
The same computational tools and explicit algorithms for isogeny graphs in cryptography apply equally to the study of Galois representations.

SUPERSINGULAR ISOGENY GRAPHS

The supersingular isogeny graphs are remarkable because the vertex sets are finite : there are $(p+1)/12+\epsilon_p$ curves. Moreover

- every supersingular elliptic curve can be defined over $\mathbb{F}_{p^2}$;
- all ℓ-isogenies are defined over $\mathbb{F}_{p^2}$;
- every endomorphism of E is defined over $\mathbb{F}_{p^2}$.

The lack of a commutative group acting on the set of supersingular elliptic curves/$\mathbb{F}_{p^2}$ makes the isogeny graph more complicated.



SIDH - L. De Feo & D. Jao, 2011

Supersingular isogeny Diffie-Hellman

- Fix two small primes ℓ_A and ℓ_B;
- Choose a prime p such that $p+1 = \ell_A^a \ell_B^b f$ for a small correction term f;
- Pick a supersingular elliptic curve $E/\mathbb{F}_{p^2}$: $E\left(\mathbb{F}_{p^2}\right) \simeq \left(\frac{\mathbb{Z}}{(p+1)\mathbb{Z}}\right)^2$
- Alice consider $E\left[\ell_A^a\right] = \langle P_A, Q_A\rangle$ while Bob takes $E\left[\ell_B^b\right] = \langle P_B, Q_B\rangle$.
- **Secret Data:** $R_A = m_A P_A + n_A Q_A$ and $R_B = m_B P_B + n_B Q_B$.
- **Private Key:** isogenies $\phi_A : E \to E_A = E/\langle R_A\rangle$ and $\phi_B : E \to E_B = E/\langle R_B\rangle$.
- **Shared Data:** $E_A, \phi_A(P_B), \phi_A(Q_B)$ and $E_B, \phi_B(P_A), \phi_B(Q_A)$.
- **Shared Key:** $E/\langle R_A, R_B\rangle = E_B/\langle \phi_B(R_A)\rangle = E_A/\langle \phi_A(R_B)\rangle$.

$$\begin{tikzcd}
 & E/\langle R_A\rangle\ ,\ \begin{matrix}\phi_A(P_B)\\ \phi_A(Q_B)\end{matrix} \arrow[dr, dash, "\phi'_B"] & \\
E \arrow[ur, dash, "\phi_A"] \arrow[dr, dash, "\phi_B"'] \arrow[rr, dashed, shift left=3, "\phi_A(R_B)"'] \arrow[rr, dashed, shift right=3, "\phi_B(R_A)"] & & E/\langle R_A, R_B\rangle \\
 & E/\langle R_B\rangle\ ,\ \begin{matrix}\phi_B(P_A)\\ \phi_B(Q_A)\end{matrix} \arrow[ur, dash, "\phi'_A"'] &
\end{tikzcd}$$

CSIDH - Castryck, Lange, Martindale, Panny & Renes, 2018

It is an adaptation of the CouveignesâRostovtsevâStolbunov scheme to supersingular elliptic curves.

Commutative Supersingular isogeny Diffie-Hellman

- Fix a prime $p = 4 \cdot \ell_1 \cdot \ldots \cdot \ell_t - 1$ for small distinct odd primes ℓ_i.
- The elliptic curve $E_0 : y^2 = x^3 + x/\mathbb{F}_p$ is supersingular and its endomorphism ring over $\mathbb{F}_p$ is $\mathcal{O} = \mathbb{Z}[\pi]$ (commutative).
- A supersingular Montgomery curve $E_A : y^2 = x^3 + Ax^2 + x/\mathbb{F}_p$ appear in the $\mathcal{C}\ell(\mathcal{O})$-orbit of E_0.
- **Private Key:** it is an n-tuple of integers $(e_1, \ldots, e_t)$ sampled in a range $\{-m, \ldots, m\}$ representing an ideal class $[\mathfrak{a}] = [\mathfrak{l}_1^{e_1} \cdot \ldots \cdot \mathfrak{l}_t^{e_t}] \in \mathcal{C}\ell(\mathcal{O})$ where $\mathfrak{l}_i = (\ell_i, \pi - 1)$.
- **Public Key:** The Montgomery coefficients A of the elliptic curve $E_A = [\mathfrak{a}] \cdot E_0 : y^2 = x^3 + Ax^2 + x$.
- **Shared Key:** If Alice and Bob have private key $(\mathfrak{a}, A)$ and $(\mathfrak{b}, B)$ then they can compute the shared key $E_{AB} = [\mathfrak{a}][\mathfrak{b}] \cdot E_0 = [\mathfrak{b}][\mathfrak{a}] \cdot E_0$.

ORIENTATIONS

Let E/k be a supersingular elliptic curve over $k = \mathbb{F}_{p^2}$, let K be an imaginary quadratic field with maximal order $\mathcal{O}_K$, and define

$$\mathrm{End}(E)^0 = \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

Then $\mathrm{End}(E)^0$ is a quaternion algebra over $\mathbb{Q}$, ramified at p, which admits an embedding of K if and only if p is ramified or inert in K.

Definition

A *K-orientation* on an elliptic curve E/k is a homomorphism

$$\iota : K \hookrightarrow \mathrm{End}^0(E).$$

An *$\mathcal{O}$-orientation* on E is a K-orientation such that $\iota(\mathcal{O})$ is contained in $\mathrm{End}(E)$. An $\mathcal{O}$-orientation is *primitive* if

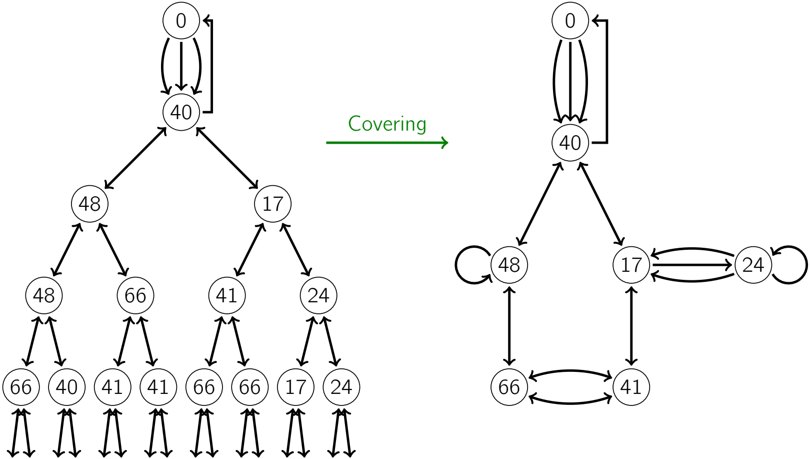
$$\iota : \mathcal{O} \to \iota(K) \cap \mathrm{End}(E)$$

is an isomorphism.

ORIENTED ISOGENY GRAPHS - AN EXAMPLE

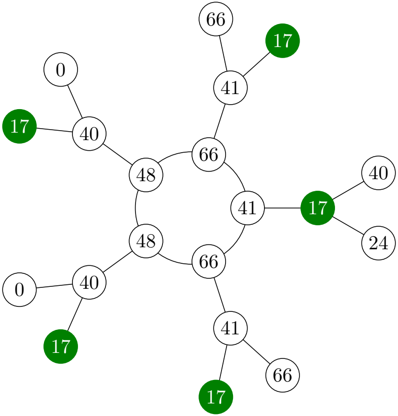
Let $p = 71$ and $E_0/\mathbb{F}_{71}$ be the supersingular elliptic curve with $j(E) = 0$ oriented by the $\mathcal{O}_K = \mathbb{Z}[\omega]$, where $\omega^2 + \omega + 1 = 0$.

The orientation by $K = \mathbb{Q}[\omega]$ differentiates vertices in the descending paths from E_0, determining an infinite graph shown here to depth 4:



Oriented isogeny graphs - yet another example

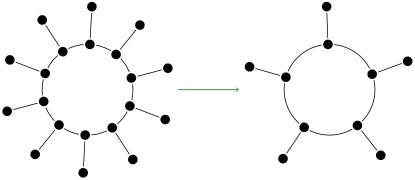
We let again $p = 71$ and we consider the isogeny graph oriented by $\mathbb{Z}[\omega_{79}]$ where ω_{79} generates the ring of integers of $\mathbb{Q}(\sqrt{-79})$.



ORIENTATIONS AND MODULI

The moduli of elliptic curves j-invariant don't suffice to classify isomorphism of oriented curves. In the OSIDH protocol we focused on orientations by the system of orders $\mathcal{O}_n = \mathbb{Z} + \ell^n O_K$, linked via a chain of ℓ-isogenies: the *path* traversed is more important.

To resolve the local ambiguities, we can add more level structure:



such that an ambiguous chain of moduli $(j_0, \dots, j_{n-1}, j_n, \dots)$ can be resolved to

$$(t_0, \dots, t_{n-1}, t_n, \dots) \text{ or } (t_0, \dots, t_{n-1}, t_n', \dots).$$

ADDING LEVEL STRUCTURE

ADDING LEVEL STRUCTURE

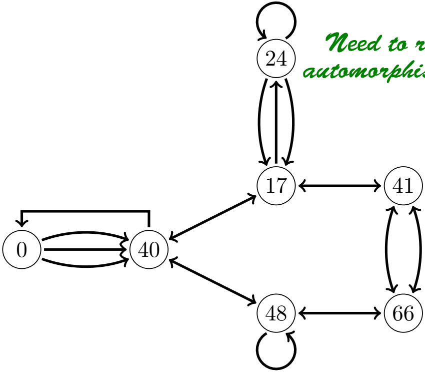
There are multiple reasons to add level structure to our construction:

- With an ℓ-level structure, the extension of ℓ-isogenies by modular correspondences allows one to automatically remove the dual isogeny (backtracking): there are ℓ rather than $\ell + 1$ extensions.

ADDING LEVEL STRUCTURE

There are multiple reasons to add level structure to our construction:

- With an ℓ-level structure, the extension of ℓ-isogenies by modular correspondences allows one to automatically remove the dual isogeny (backtracking): there are ℓ rather than $\ell + 1$ extensions.
- The modular isogeny chain is a potentially-non injective image of the isogeny chain.



Need to rigidify automorphism group

Need to distinguish 2-isogenies

ADDING LEVEL STRUCTURE

There are multiple reasons to add level structure to our construction:

- With an ℓ-level structure, the extension of ℓ-isogenies by modular correspondences allows one to automatically remove the dual isogeny (backtracking): there are ℓ rather than $\ell+1$ extensions.
- The modular isogeny chain is a potentially-non injective image of the isogeny chain.
- Rigidifying automorphisms should also shorten the distance to which we need to go in order to differentiate 2 points (two torsion of $\mathcal{C}\ell(\mathcal{O})$ may lift to non 2-torsion point in $\mathcal{C}\ell(\mathcal{O},\Gamma)$).

ADDING LEVEL STRUCTURE

There are multiple reasons to add level structure to our construction:

- With an ℓ-level structure, the extension of ℓ-isogenies by modular correspondences allows one to automatically remove the dual isogeny (backtracking): there are ℓ rather than $\ell + 1$ extensions.
- The modular isogeny chain is a potentially-non injective image of the isogeny chain.
- Rigidifying automorphisms should also shorten the distance to which we need to go in order to differentiate 2 points (two torsion of $\mathcal{C}\ell(\mathcal{O})$ may lift to non 2-torsion point in $\mathcal{C}\ell(\mathcal{O}, \Gamma)$).
- q-modular polynomial of higher level are smaller.

MODULAR GROUP

The group

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \, ad - bc = 1 \right\}$$

acts by fractional linear Mobius transformations

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \tau = \frac{a\tau + b}{c\tau + d}$$

on the upper half plane

$$\mathbb{H} = \{z \in \mathbb{C} \,|\, \mathrm{Im}(z) > 0\}$$

equipped with its standard complex analytic structure.

We define the modular group as the quotient group

$$\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})/\{\pm I\}$$

CONGRUENCE SUBGROUPS

We define the principal congruence subgroup as the kernel of the reduction map $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. This is

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

A subgroup Γ of $\mathrm{SL}_2(N)$ is called a congruence subgroup if it contains $\Gamma(N)$ for some N. Some important examples of congruence subgroups are

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

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

MODULAR CURVES

The modular group acts on the upper half plane and its quotient classifies homothety classes of lattices or, equivalently, isomorphism classes of elliptic curves. As a geometric object it is a sphere with one point missing.

Define the extended upper-half plane

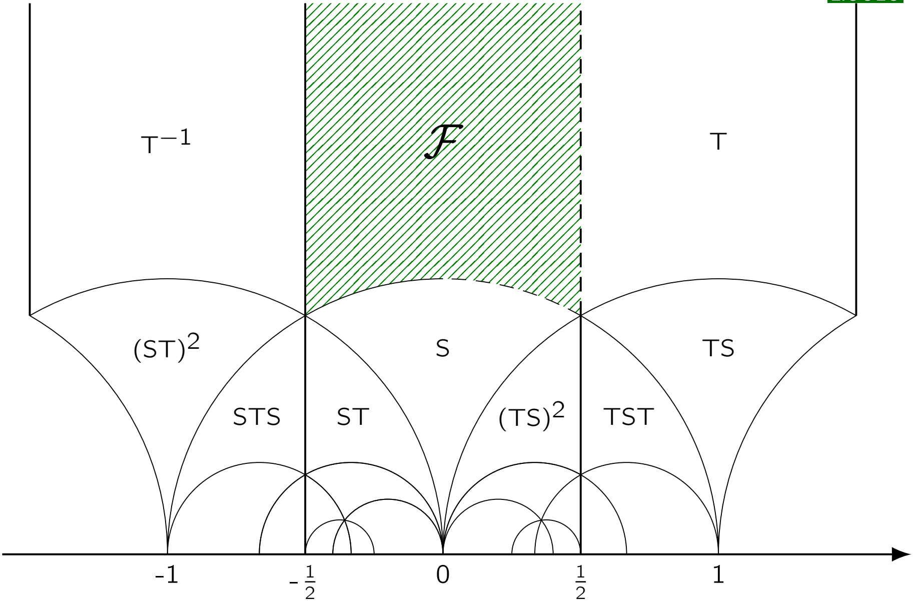
$$\mathbb{H}^* = \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$$

Definition

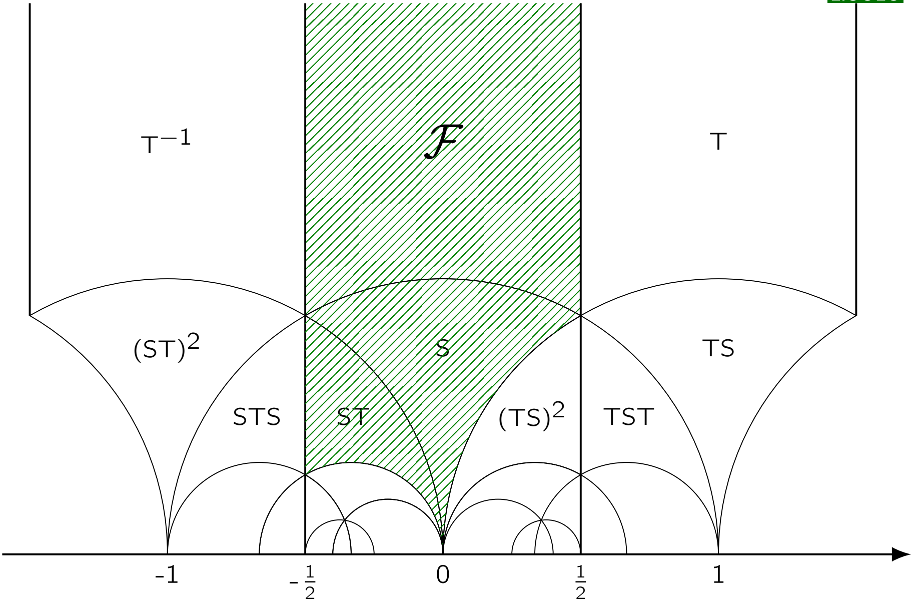
The affine modular curve over $\mathbb{C}$ attached to Γ is an algebraic curve $Y(\Gamma)$ whose complex points are identified with $\Gamma\backslash\mathbb{H}$ with its natural Riemann surface structure.

The complete modular curve over $\mathbb{C}$ attached to Γ is an algebraic curve $X(\Gamma)$ whose complex points are identified with $\Gamma\backslash\mathbb{H}^*$ equipped with some Riemann surface structure.

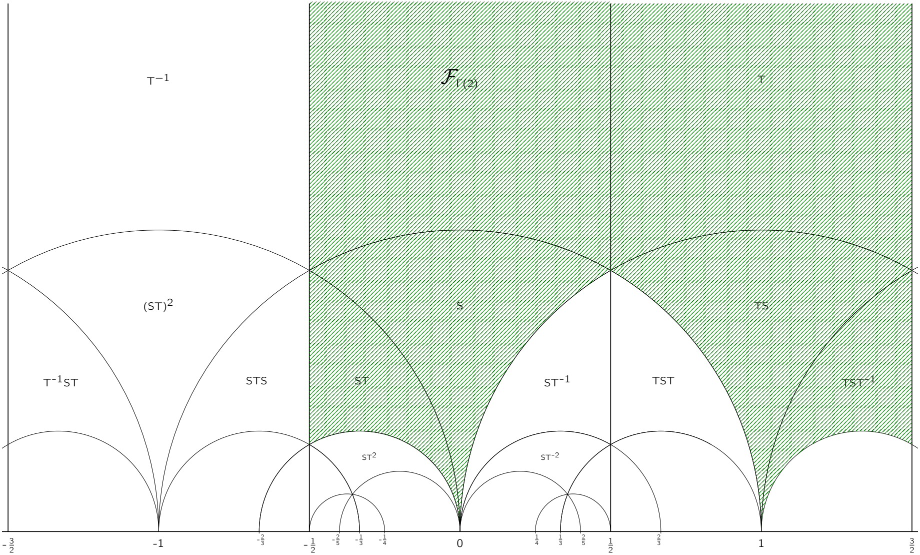
MODULAR CURVES - AN EXAMPLE



MODULAR CURVES - AN EXAMPLE



MODULAR CURVES - AN EXAMPLE



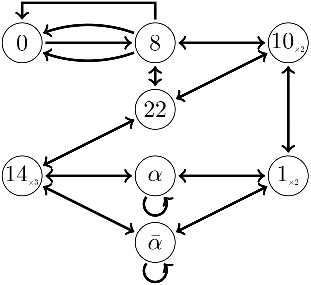
MODULAR INTERPRETATION

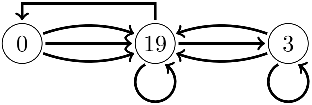
The points in $Y(\Gamma) = \mathbb{H}/\Gamma$ can be interpreted as elliptic curves over $\mathbb{C}$ with some extra ”level N” structure. More precisely,

- If $\Gamma = \Gamma_0(N)$, then the Γ-orbit of $\tau \in \mathbb{H}$ corresponds to the complex torus $E = \mathbb{C}/\langle, \tau\rangle$ with the distinguished cyclic subgroup of order N generated by $1/N$. Thus, points on $Y_0(N)$ parametrize isomorphism classes of pairs (E, C) where E is an elliptic curve over $\mathbb{C}$ and C is a cyclic subgroup of E of order N.
- $\Gamma = \Gamma_1(N)$, then the Γ-orbit of $\tau \in \mathbb{H}$ corresponds to the complex torus $E = \mathbb{C}/\langle, \tau\rangle$ with the distinguished point of order N given by $1/N$. Hence, points on $Y_1(N)$ parametrize isomorphism classes of pairs (E, P) where now P is a point on E of exact order N.

ISOGENY GRAPHS WITH LEVEL STRUCTURE

For any congruence subgroup Γ of level coprime to the characteristic, we have a covering $G_S(E, \Gamma) \to G_S(E)$ whose vertices are pairs $(E, \Gamma(P, Q))$ of supersingular elliptic curves/$\mathbb{F}_{p^2}$ and a Γ-level structure, and edges are isogenies $\psi : (E, \Gamma(P, Q)) \to (E', \Gamma(P', Q'))$ such that $\psi(\Gamma(P, Q)) = \Gamma(P', Q')$.





Eg. $\Gamma_0(N)$-structures.
Vertices (E, G) with $G \leq E[N]$ of order N
$\mathrm{End}(E, G) = \{\alpha \in \mathrm{End}(E) \,|\, \alpha(G) \subseteq G\}$
isomorphic to Eichler order.

On the left the $\Gamma_0(3)$ supersingular 2-isogeny graph.

$14 \leftrightarrow \{(E_0, G_1), (E_0, G_2), (E_0, G_3)\}$ where G_1, G_2, G_3 maps to each other under the automorphism of E_0; they define 3 isogenies to E_3.

SOME MODULAR CURVES OF INTEREST

Weber modular function $\mathfrak{f} = f$

such that $j = \frac{(\mathfrak{f}^{24}-16)^3}{\mathfrak{f}^{24}}$

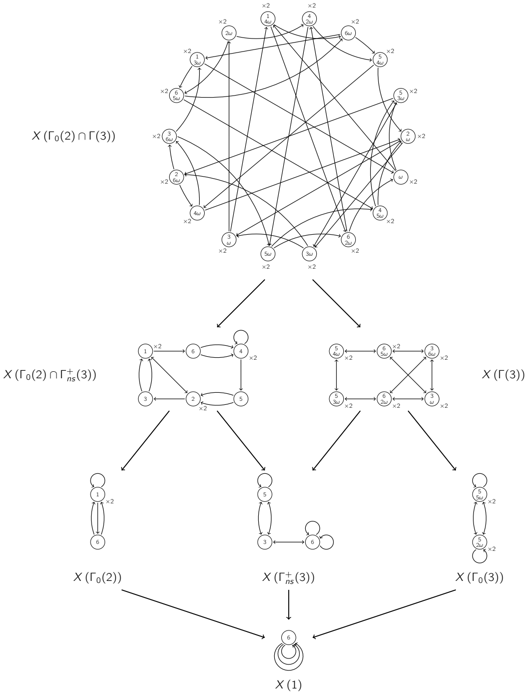
$$\begin{tikzcd}
 & & W \arrow[d, "u = f^8"', "8"] & & \underset{v}{X} \arrow[dll, "u = \frac{(t^3+8)v}{(v^3-1)}"', "4"] \arrow[dr, "3"', "t = \frac{v^3+2}{v}"] & & \\
 & & X\left(\Gamma_0(2) \cap \Gamma_{ns}^+(3)\right) = \underset{u}{Y} \arrow[dl, "s = -u^3"', "3"] \arrow[dr, "3"', "r = \frac{u^3-16}{u}"] & & & X(3) \arrow[dll, "4"', "r = \frac{(t^3+216)t}{t^3-27}"] \arrow[dr, "3"', "t_3 = t^3"] & \\
 & X_0(2) \arrow[dr, "j = \frac{(s+16)^3}{s}"', "3"] & & \underset{r}{X_{ns}^+(3)} \arrow[dl, "3"', "j = r^3"] & & & X_0(3) \arrow[dllll, bend left, "4"', "j = \frac{t_3(t_3+216)^3}{(t_3-27)^3}"] \\
 & & \underset{j}{X(1)} & & & &
\end{tikzcd}$$

t = Hesse invariant

$2^{12}\left(\frac{\eta_2(\tau)}{\eta_1(\tau)}\right)^{24} = s$

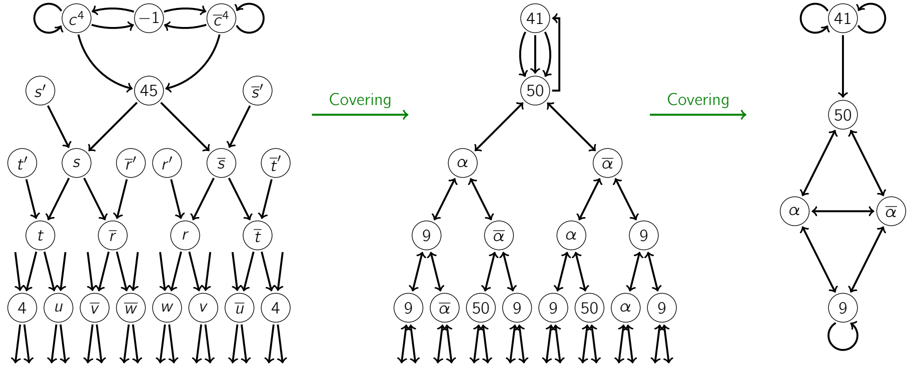
$t_3 = 27 + \left(\frac{\eta_1(\tau)}{\eta_3(\tau)}\right)^{12}$

j-invariant


$X\,(\Gamma_0(2) \cap \Gamma(3))$
$X\,(\Gamma_0(2) \cap \Gamma^+_{ns}(3))$
$X\,(\Gamma(3))$
$X\,(\Gamma_0(2))$
$X\,(\Gamma^+_{ns}(3))$
$X\,(\Gamma_0(3))$
$X\,(1)$
1
2
3
4
5
6
4ω
2ω
6ω
3ω
5ω
ω
×2

WEBER INITIALIZATIONS - AN EXAMPLE OF GRAPHS

We orient the supersingular 2-isogeny graph in characteristic 61 by $\mathbb{Q}(\sqrt{-7})$ and we then climb the Weber modular tower.



Weber Modular Polynomials

$$\Psi_2(x,y) = (x^2 - y)y + 16x \qquad \Psi_3(x,y) = x^4 - x^3y^3 + 8xy + y^4$$

THE METHOD OF GRAPHS

SUPERSINGULAR CURVES AND MODULAR FORMS - ORIGINS

The relations between supersingular elliptic curves and the ideal theory in a quaternion algebra appears in a classical work of Deuring (1941).

The basis problem of Eichler (1973) provides the means to relate the ideal theory to modular forms.

Using this theory, Pizer (1980) describes an algorithm for computing modular forms.

The method of graphs of Oesterlé and Mestre (1986) rephrases the theory of Quaternion ideals in terms of supersingular elliptic curves.

BRANDT MATRICES

Let p be a prime number and $\mathfrak{A}_{p,\infty}$ the quaternion algebra ramified at p and infinity. Let R be a fixed maximal order in $\mathfrak{A}_{p,\infty}$.

For $\{J_1, \ldots, J_h\}$ a list of representatives for the isomorphism classes of left R-ideals and $n \geq 1$, we can construct the $h \times h$ matrix $B(n) = (b_{i,j}(n))$ by

$$\begin{aligned} b_{i,j}(n) &= \#\{I \subset J_i \,|\, \mathrm{Nr}(I) = n\mathrm{Nr}(J_i) \text{ and } [I] = [J_i]\} = \\ &= \#\{I \subset J_i \,\big|\, [J_i : I] = n^2 \text{ and } [I] = [J_i]\} = \\ &= \frac{1}{2\omega_i}\#\{\alpha \in J_j J_i^{-1} \mid \mathrm{Nr}(\alpha) q_i/q_j = n\} \end{aligned}$$

We can construct the $h \times h$ matrix valued function

$$\Theta(z) = \sum_{n \geq 0} B(n) q^n$$

whose i, j component is

$$\theta_{i,j}(z) = \sum_{n \geq 0} b_{i,j}(n) q^n \in \mathrm{M}_2(\Gamma_0(p))$$

BRANDT MATRICES - AN EXAMPLE

Let $p = 23$. The quaternion algebra $\mathfrak{A}_{p,\infty}$ has maximal order

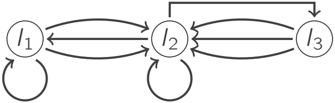
$$R = \mathbb{Z} + \mathbb{Z}\, i + \mathbb{Z}\, \frac{1+j}{2} + \mathbb{Z}\, i\, \frac{1+j}{2}$$

with three ideal classes$\{[J_1], [J_2], [J_3]\}$. We find

$$B(2) = \begin{pmatrix} 1 & 1 & 0 \\ 2 & 1 & 3 \\ 0 & 1 & 0 \end{pmatrix} \qquad B(3) = \begin{pmatrix} 0 & 1 & 3 \\ 2 & 3 & 0 \\ 2 & 0 & 1 \end{pmatrix} \qquad B(101) = \begin{pmatrix} 30 & 28 & 24 \\ 56 & 54 & 60 \\ 16 & 20 & 18 \end{pmatrix}$$

Giving normic forms

$$\mathrm{nr}_1(X_1, X_2, X_3, X_4) = X_1^2 + X_2^2 + 6X_3^2 + 6X_4^2 + X_1X_3 + X_2X_4$$
$$\mathrm{nr}_2(X_1, X_2, X_3, X_4) = X_1^2 + X_2^2 + 8X_3^2 + 8X_4^2 + X_1X_2 + X_1X_3 + X_2X_3 + X_2X_4 + 4X_3X_4$$
$$\mathrm{nr}_3(X_1, X_2, X_3, X_4) = X_1^2 + 2X_2^2 + 3X_3^2 + 6X_4^2 + X_1X_4 + X_2X_3$$



Eichlers Basis Problem - Brandt Modules

We define the Brandt Module $\mathbb{M}_{\mathbb{C}}(R)$ as the $\mathbb{C}$-vector space with basis $\mathcal{Cl}(R)$ equipped with the right action of Brandt matrices.

Define the Brandt morphism as

$$\begin{aligned} \mathbb{M}_{\mathbb{C}}(R) \times \mathbb{M}_{\mathbb{C}}(R) &\longrightarrow \mathrm{M}_2(\Gamma_0(p), \mathbb{Q}) \\ (J_i, J_j) &\longmapsto \sum b_{i,j}(n) q \\ &= \frac{1}{\omega_i} \sum_{\gamma} q^{Q_{i,j(\gamma)}} \\ &= \sum \langle B(n)E, F \rangle q^n \end{aligned}$$

Theorem

As part of the basis problem Eichler proved that the morphism above is surjective, equivalently that $\mathrm{M}_2(\Gamma_0(p), \mathbb{Q})$ is spanned by theta series.

SUPERSINGULAR HECKE MODULE

Let $E_1, \dots, E_h$ be a complete set of isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}}_p$. We define the supersingular module as the free abelian group

$$\mathcal{X}(p) = \bigoplus_{i=1}^{h} \mathbb{Z}[E_i],$$

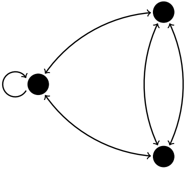
equipped with Hecke operators T_ℓ, the adjacency operators of the ℓ-isogeny supersingular graphs.

The supersingular points $j(E_i)$ are the singular points of $X_0(p)/\mathbb{F}_p$, which has two irreducible components, isomorphic to $X(1)/\mathbb{F}_p$, crossing at the supersingular points.

The singular module can be identified with the monodromy group of the Neron model of its Jacobian $J_0(p)$.

METHOD OF GRAPH - AN EXAMPLE

Let $p = 37$. There are 3 supersingular elliptic curves over the algebraic closure of $\mathbb{F}_{37}$. Since non of these curves has automorphism group larger than $\{\pm 1\}$ we can view the graph as undirected. For $p = 2$ we have



$$T(2) = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 2 \\ 1 & 2 & 0 \end{pmatrix}$$

The matrix $T(2)$ has characteristic polynomial $X(X-3)(X+2)$ and can be interpreted as a Hecke operator on the space $\mathbb{M}_2(\Gamma_0(37), \mathbb{Q})$ of modular forms of weight 2 for $\Gamma_0(37)$.

The rational roots of this polynomial imply that the Jacobian of the modular curve $X_0(37)$ splits as the product of two elliptic curves over $\mathbb{Q}$.

LEVEL STRUCTURE

Let G be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. For a choice $\mathcal{B} = (P, Q)$ of basis for $E[N]$, let $\mathcal{B}G$ be the orbit under the action:

$$(P, Q) \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = (aP + cQ, bP + dQ).$$

The pair $(E, \mathcal{B}G)$ corresponds to a point on a modular curve $\mathcal{X}_G$.

Example. An upper triangular Borel subgroup $G = B_0(N)$ stabilizes the subgroup $\langle P \rangle$, and $\mathcal{X}_G$ is the modular curve $X_0(N)$.

For a complete set $(E_i, \mathcal{B}_{ij}G)$ of representative moduli points, we can define a supersingular module:

$$\mathcal{X}(p, G) = \bigoplus_{i,j} \mathbb{Z}[(E_i, \mathcal{B}_{ij}G)],$$

on the modular curve $\mathcal{X}_G$, equipped with the action of Hecke operators.

GALOIS REPRESENTATIONS

The addition of level structure allows us to compute objects of more general reduction type. In particular, 1-dimensional factors of $\mathcal{X}(p)$ correspond to semistable elliptic curves of prime conductor p.

The supersingular module $\mathcal{X}(p, G)$ covering $\mathcal{X}(p)$ gives rise to Galois representations of elliptic curves and modular abelian varieties which need not be semistable at the primes dividing N.

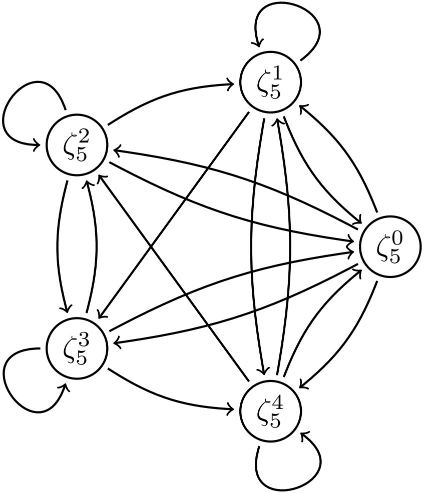
Example. The modular cover $X(5) \to X(1)$ is defined by the map:

$$u \longmapsto j(u) = \frac{(u^{20} + 228u^{15} + 494u^{10} - 228u^5 + 1)^3}{u^5(u^{10} - 11u^5 - 1)^5}.$$

The supersingular point $j = 0 = 12^3$ on $X(1)/\mathbb{F}_2$ splits into the five supersingular points $\{1, \zeta_5, \zeta_5^2, \zeta_5^3, \zeta_5^4\}$ on $X(5)$ over $\mathbb{F}_2[\zeta_5] = \mathbb{F}_{2^4}$.

A LEVEL 50 EXAMPLE

The supersingular 3-isogeny graph on $X(5)/\mathbb{F}_2$ takes the form:



A LEVEL 50 EXAMPLE

This gives the adjacency matrix

$$T_3 = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 \end{pmatrix}$$

with characteristic polynomial $(x-4)(x-1)(x+1)(x-i)(x+i)$, whose linear factors correspond to twists of an elliptic curve of conductor 50.

SIEVING FOR ELLIPTIC CURVES

The rank of the supersingular modules $\mathcal{X}(p, G)$ grows linearly with p, but the Hecke operators (Brandt matrices) on $\mathcal{X}(p, G)$ are sparse.

In order to study existence of elliptic factors in $\mathcal{X}(p, G)$, it suffices to look in the kernels:

$$\ker(T_\ell - c), \ker(T_\ell - c + 1), \ldots \ker(T_\ell + c - 1), \ker(T_\ell + c),$$

where $c = \lfloor 2\sqrt{\ell} \rfloor$ is the Hasse-Weil bound. This allows one to study existence of elliptic curves with semistable reduction at p and reduction type dictated by G at N.

Further work is in progress to be able to capture Hecke modules and their Galois representations with additive reduction at p, using partial p-adic lifts of supersingular points.

THANK YOU FOR YOUR ATTENTION