CM Points on $X_0(N)$: Volcanoes and Reality, Extended Edition

Pete L. Clark

Department of Mathematics
The University of Georgia

June 14, 2020

This is the Extended Edition

When preparing for my talk, I had to cut a certain amount of material. Those are the breaks, and I'm sure my talk went better for fitting in the allotted time. On the other hand, some of what got cut is closely related to material that other speakers have discussed. So taking advantage of the online format, I am providing this version of the slides with some of this relevant material put back in IN PURPLE.

Torsion Subgoups of Elliptic Curves

Let $E_{/F}$ be an elliptic curve over a number field F.

Torsion Subgoups of Elliptic Curves

Let $E_{/F}$ be an elliptic curve over a number field F.

$E(F)[\mathrm{tors}]$ is finite. By Merel (1996), only finitely many groups arise for each $d = [F : \mathbb{Q}]$.

Torsion Subgoups of Elliptic Curves

Let $E_{/F}$ be an elliptic curve over a number field F.

$E(F)[\mathrm{tors}]$ is finite. By Merel (1996), only finitely many groups arise for each $d = [F : \mathbb{Q}]$.

Can we find all possibilities, for each d??

Torsion Subgoups of Elliptic Curves

Let $E_{/F}$ be an elliptic curve over a number field F.

$E(F)[\mathrm{tors}]$ is finite. By Merel (1996), only finitely many groups arise for each $d = [F : \mathbb{Q}]$.

Can we find all possibilities, for each d??

Yes, for...

Torsion Subgoups of Elliptic Curves

Let $E_{/F}$ be an elliptic curve over a number field F.

$E(F)[\mathrm{tors}]$ is finite. By Merel (1996), only finitely many groups arise for each $d = [F : \mathbb{Q}]$.

Can we find all possibilities, for each d??

Yes, for... $d = 1$ (Mazur, 1970s)

Torsion Subgoups of Elliptic Curves

Let $E_{/F}$ be an elliptic curve over a number field F.

$E(F)[\mathrm{tors}]$ is finite. By Merel (1996), only finitely many groups arise for each $d = [F : \mathbb{Q}]$.

Can we find all possibilities, for each d??

Yes, for... $d = 1$ (Mazur, 1970s) $d = 2$ (Kamienny, Kenku, Momose, 1990s)

Torsion Subgoups of Elliptic Curves

Let $E_{/F}$ be an elliptic curve over a number field F.

$E(F)[\mathrm{tors}]$ is finite. By Merel (1996), only finitely many groups arise for each $d = [F : \mathbb{Q}]$.

Can we find all possibilities, for each d??

Yes, for... $d = 1$ (Mazur, 1970s) $d = 2$ (Kamienny, Kenku, Momose, 1990s) $d = 3$ (Derickx, Etropolski, Morrow, van Hoeij, Zureick-Brown, 20??)

Torsion Subgoups of Elliptic Curves

Let $E_{/F}$ be an elliptic curve over a number field F.

$E(F)[\mathrm{tors}]$ is finite. By Merel (1996), only finitely many groups arise for each $d = [F : \mathbb{Q}]$.

Can we find all possibilities, for each d??

Yes, for... $d = 1$ (Mazur, 1970s) $d = 2$ (Kamienny, Kenku, Momose, 1990s) $d = 3$ (Derickx, Etropolski, Morrow, van Hoeij, Zureick-Brown, 20??)

Here I want to discuss work which should lead to a complete solution in the **CM case**.

Motivating Problem: Fibers Over J

Let $X_{/\mathbb{Q}}$ be a modular curve: say $X_0(N)$, $X_1(N)$, $X(N)$ or $X(M,N)$. Let $\pi : X \to X(1)$ be the map to the j-line. Given a closed point $J \in X(1)$, understand the fiber of π over X.

Motivating Problem: Fibers Over J

Let $X_{/\mathbb{Q}}$ be a modular curve: say $X_0(N)$, $X_1(N)$, $X(N)$ or $X(M,N)$. Let $\pi : X \to X(1)$ be the map to the j-line. Given a closed point $J \in X(1)$, understand the fiber of π over X.

It's a case of the classic ANT problem: how do prime ideals split in finite extensions of Dedekind domains?

Motivating Problem: Fibers Over J

Let $X_{/\mathbb{Q}}$ be a modular curve: say $X_0(N)$, $X_1(N)$, $X(N)$ or $X(M,N)$. Let $\pi : X \to X(1)$ be the map to the j-line. Given a closed point $J \in X(1)$, understand the fiber of π over X.

It's a case of the classic ANT problem: how do prime ideals split in finite extensions of Dedekind domains?

Away from $J = 0, 1728, \infty$, no ramification. Want to count upstairs primes – **closed points** P lying over J – and residual degrees $\frac{d_P}{d_J} = [\mathbb{Q}(P) : \mathbb{Q}(J)]$.

Motivating Problem: Fibers Over J

Let $X_{/\mathbb{Q}}$ be a modular curve: say $X_0(N)$, $X_1(N)$, $X(N)$ or $X(M,N)$. Let $\pi : X \rightarrow X(1)$ be the map to the j-line. Given a closed point $J \in X(1)$, understand the fiber of π over X.

It's a case of the classic ANT problem: how do prime ideals split in finite extensions of Dedekind domains?

Away from $J = 0, 1728, \infty$, no ramification. Want to count upstairs primes – **closed points** P lying over J – and residual degrees $\frac{d_P}{d_J} = [\mathbb{Q}(P) : \mathbb{Q}(J)]$. Determine $\mathbb{Q}(P)$ if possible.

Motivating Problem: Fibers Over J

Let $X_{/\mathbb{Q}}$ be a modular curve: say $X_0(N)$, $X_1(N)$, $X(N)$ or $X(M, N)$. Let $\pi : X \to X(1)$ be the map to the j-line. Given a closed point $J \in X(1)$, understand the fiber of π over X.

It's a case of the classic ANT problem: how do prime ideals split in finite extensions of Dedekind domains?

Away from $J = 0, 1728, \infty$, no ramification. Want to count upstairs primes – **closed points** P lying over J – and residual degrees $\frac{d_P}{d_J} = [\mathbb{Q}(P) : \mathbb{Q}(J)]$. Determine $\mathbb{Q}(P)$ if possible.

For fixed J, it's **in principle** equivalent to understanding adelic Galois representations on E with $j(E) = J$.

Motivating Problem: Fibers Over J

Let $X_{/\mathbb{Q}}$ be a modular curve: say $X_0(N)$, $X_1(N)$, $X(N)$ or $X(M, N)$. Let $\pi : X \to X(1)$ be the map to the j-line. Given a closed point $J \in X(1)$, understand the fiber of π over X.

It's a case of the classic ANT problem: how do prime ideals split in finite extensions of Dedekind domains?

Away from $J = 0, 1728, \infty$, no ramification. Want to count upstairs primes – **closed points** P lying over J – and residual degrees $\frac{d_P}{d_J} = [\mathbb{Q}(P) : \mathbb{Q}(J)]$. Determine $\mathbb{Q}(P)$ if possible.

For fixed J, it's **in principle** equivalent to understanding adelic Galois representations on E with $j(E) = J$. It's more interesting to work uniformly across sets of J.

Motivating Problem: Fibers Over J

Let $X_{/\mathbb{Q}}$ be a modular curve: say $X_0(N)$, $X_1(N)$, $X(N)$ or $X(M,N)$. Let $\pi : X \rightarrow X(1)$ be the map to the j-line. Given a closed point $J \in X(1)$, understand the fiber of π over X.

It's a case of the classic ANT problem: how do prime ideals split in finite extensions of Dedekind domains?

Away from $J = 0, 1728, \infty$, no ramification. Want to count upstairs primes – **closed points** P lying over J – and residual degrees $\frac{d_P}{d_J} = [\mathbb{Q}(P) : \mathbb{Q}(J)]$. Determine $\mathbb{Q}(P)$ if possible.

For fixed J, it's **in principle** equivalent to understanding adelic Galois representations on E with $j(E) = J$. It's more interesting to work uniformly across sets of J. (Over $J \in \mathbb{Q}$, this is "Serre's Uniformity Problem.")

Motivating Problem: Fibers Over J

Let $X_{/\mathbb{Q}}$ be a modular curve: say $X_0(N)$, $X_1(N)$, $X(N)$ or $X(M, N)$. Let $\pi : X \to X(1)$ be the map to the j-line. Given a closed point $J \in X(1)$, understand the fiber of π over X.

It's a case of the classic ANT problem: how do prime ideals split in finite extensions of Dedekind domains?

Away from $J = 0, 1728, \infty$, no ramification. Want to count upstairs primes – **closed points** P lying over J – and residual degrees $\frac{d_P}{d_J} = [\mathbb{Q}(P) : \mathbb{Q}(J)]$. Determine $\mathbb{Q}(P)$ if possible.

For fixed J, it's **in principle** equivalent to understanding adelic Galois representations on E with $j(E) = J$. It's more interesting to work uniformly across sets of J. (Over $J \in \mathbb{Q}$, this is "Serre's Uniformity Problem.")

All hail the triumvirate: torsion subgroups $\iff$ points on modular curves $\iff$ Galois representations.

The CM Case

We will work in the **CM case**. Here much more is known. After pioneering work of Silverberg (1988, 1992) and recent work of Lozano-Robledo, Bourdon, Clark, Pollack, Stankewicz, we are getting close to **complete answers**.

The CM Case

We will work in the **CM case**. Here much more is known. After pioneering work of Silverberg (1988, 1992) and recent work of Lozano-Robledo, Bourdon, Clark, Pollack, Stankewicz, we are getting close to **complete answers**.

So let's try to get even closer!

The CM Case

We will work in the **CM case**. Here much more is known. After pioneering work of Silverberg (1988, 1992) and recent work of Lozano-Robledo, Bourdon, Clark, Pollack, Stankewicz, we are getting close to **complete answers**.

So let's try to get even closer!

2019 work of Lozano-Robledo gives lots of information on the mod N and ℓ-adic Galois reps on a CM elliptic curve over $\mathbb{Q}(J)$. His work in progress should do even more.

Imaginary Quadratic Orders

CM setup: an elliptic curve $E_{/\mathbb{C}} \cong \mathbb{C}/\Lambda$ has **complex multiplication** if $\operatorname{End} E = \{\alpha \in \mathbb{C} \mid \alpha\Lambda \subset \Lambda\} \supsetneq \mathbb{Z}$, in which case $\operatorname{End} E$ is an order $\mathcal{O}$ in an imaginary quadratic field K.

Imaginary Quadratic Orders

CM setup: an elliptic curve $E_{/\mathbb{C}} \cong \mathbb{C}/\Lambda$ has **complex multiplication** if $\operatorname{End} E = \{\alpha \in \mathbb{C} \mid \alpha\Lambda \subset \Lambda\} \supsetneq \mathbb{Z}$, in which case $\operatorname{End} E$ is an order $\mathcal{O}$ in an imaginary quadratic field K.

$K = \mathbb{Q}(\Delta_K)$ an imaginary quadratic field. For $\mathfrak{f} \in \mathbb{Z}^+$, unique order $\mathcal{O} = \mathcal{O}(\Delta)$ in K with $[\mathbb{Z}_K : \mathcal{O}] = \mathfrak{f}$, of discriminant $\Delta = \mathfrak{f}^2\Delta_K$. $E_{/\mathbb{C}}$ has **Δ-CM** if $\operatorname{End} E \cong \mathcal{O}(\Delta)$.

Imaginary Quadratic Orders

CM setup: an elliptic curve $E_{/\mathbb{C}} \cong \mathbb{C}/\Lambda$ has **complex multiplication** if $\operatorname{End} E = \{\alpha \in \mathbb{C} \mid \alpha\Lambda \subset \Lambda\} \supsetneq \mathbb{Z}$, in which case $\operatorname{End} E$ is an order $\mathcal{O}$ in an imaginary quadratic field K.

$K = \mathbb{Q}(\Delta_K)$ an imaginary quadratic field. For $\mathfrak{f} \in \mathbb{Z}^+$, unique order $\mathcal{O} = \mathcal{O}(\Delta)$ in K with $[\mathbb{Z}_K : \mathcal{O}] = \mathfrak{f}$, of discriminant $\Delta = \mathfrak{f}^2\Delta_K$. $E_{/\mathbb{C}}$ has **Δ-CM** if $\operatorname{End} E \cong \mathcal{O}(\Delta)$.

The Δ-CM j-invariants form a **single closed point** J_Δ on $X(1)_{/\mathbb{Q}}$, of degree $h_\Delta = \# \operatorname{Pic} \mathcal{O}(\Delta)$.

Imaginary Quadratic Orders

CM setup: an elliptic curve $E_{/\mathbb{C}} \cong \mathbb{C}/\Lambda$ has **complex multiplication** if $\operatorname{End} E = \{\alpha \in \mathbb{C} \mid \alpha\Lambda \subset \Lambda\} \supsetneq \mathbb{Z}$, in which case $\operatorname{End} E$ is an order $\mathcal{O}$ in an imaginary quadratic field K.

$K = \mathbb{Q}(\Delta_K)$ an imaginary quadratic field. For $\mathfrak{f} \in \mathbb{Z}^+$, unique order $\mathcal{O} = \mathcal{O}(\Delta)$ in K with $[\mathbb{Z}_K : \mathcal{O}] = \mathfrak{f}$, of discriminant $\Delta = \mathfrak{f}^2\Delta_K$. $E_{/\mathbb{C}}$ has **Δ-CM** if $\operatorname{End} E \cong \mathcal{O}(\Delta)$.

The Δ-CM j-invariants form a **single closed point** J_Δ on $X(1)_{/\mathbb{Q}}$, of degree $h_\Delta = \# \operatorname{Pic} \mathcal{O}(\Delta)$.

In other words, the j-invariants of Δ-CM elliptic curves form a complete, single Galois orbit. Our favorite j-invariant in this orbit is $j_\Delta := j(\mathbb{C}/\mathcal{O}) \in \mathbb{R}$. More on this later.

Extended Slide: The Main Theorem of CM

In the case $X = X(N)$, which is a $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$-Galois covering of $X(1)$ (and cofinal in all modular curves), work of Stevenhagen (and later, Bourdon-Clark and Lozano-Robledo) determines the splitting field of the fiber over $J_\Delta \in X(1)_{/K}$ as an explicit class field. In principle this reduces all the fiber computations on $X \to X(1)_{/K}$ to class field theory.

Extended Slide: The Main Theorem of CM

In the case $X = X(N)$, which is a $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$-Galois covering of $X(1)$ (and cofinal in all modular curves), work of Stevenhagen (and later, Bourdon-Clark and Lozano-Robledo) determines the splitting field of the fiber over $J_\Delta \in X(1)_{/K}$ as an explicit class field. In principle this reduces all the fiber computations on $X \to X(1)_{/K}$ to class field theory.

Reminder: Reducing a problem to CFT (or group theory, or Galois theory) is not the same as solving it! Retaining some arithmetic geometry can be helpful.

Extended Slide: The Main Theorem of CM

In the case $X = X(N)$, which is a $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$-Galois covering of $X(1)$ (and cofinal in all modular curves), work of Stevenhagen (and later, Bourdon-Clark and Lozano-Robledo) determines the splitting field of the fiber over $J_\Delta \in X(1)_{/K}$ as an explicit class field. In principle this reduces all the fiber computations on $X \to X(1)_{/K}$ to class field theory.

Reminder: Reducing a problem to CFT (or group theory, or Galois theory) is not the same as solving it! Retaining some arithmetic geometry can be helpful.

Also: want to compute fibers on $X(1)_{/\mathbb{Q}}$. Nailing down difference between $/K$ and $/\mathbb{Q}$ is the hardest part.

Bourdon-Clark

Let $M \mid N$. Recent work of Bourdon-Clark computes the **least degree** of a point in the fiber of $X(M, N) \to X(1)$ over J_Δ (for all Δ), first as curves over K and later as curves over $\mathbb{Q}$.

Bourdon-Clark

Let $M \mid N$. Recent work of Bourdon-Clark computes the **least degree** of a point in the fiber of $X(M,N) \to X(1)$ over J_Δ (for all Δ), first as curves over K and later as curves over $\mathbb{Q}$. When $M \geq 3$, residue fields of closed points must contain K.

Bourdon-Clark

Let $M \mid N$. Recent work of Bourdon-Clark computes the **least degree** of a point in the fiber of $X(M,N) \rightarrow X(1)$ over J_Δ (for all Δ), first as curves over K and later as curves over $\mathbb{Q}$. When $M \geq 3$, residue fields of closed points must contain K.

Over K, degree of every closed point is a multiple of the least degree. Need **not be the case** over $\mathbb{Q}$ (when $M \leq 2$).

Bourdon-Clark

Let $M \mid N$. Recent work of Bourdon-Clark computes the **least degree** of a point in the fiber of $X(M,N) \rightarrow X(1)$ over J_Δ (for all Δ), first as curves over K and later as curves over $\mathbb{Q}$. When $M \geq 3$, residue fields of closed points must contain K.

Over K, degree of every closed point is a multiple of the least degree. Need **not be the case** over $\mathbb{Q}$ (when $M \leq 2$).

Why this matters: If F is a number field such that there is a Δ-CM $E_{/F}$ and $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \hookrightarrow E(F)$, then there is a closed Δ-CM point $P \in X(M,N)$ and a field embedding $\mathbb{Q}(P) \hookrightarrow F$.

Bourdon-Clark

Let $M \mid N$. Recent work of Bourdon-Clark computes the **least degree** of a point in the fiber of $X(M,N) \to X(1)$ over J_Δ (for all Δ), first as curves over K and later as curves over $\mathbb{Q}$. When $M \geq 3$, residue fields of closed points must contain K.

Over K, degree of every closed point is a multiple of the least degree. Need **not be the case** over $\mathbb{Q}$ (when $M \leq 2$).

Why this matters: If F is a number field such that there is a Δ-CM $E_{/F}$ and $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \hookrightarrow E(F)$, then there is a closed Δ-CM point $P \in X(M,N)$ and a field embedding $\mathbb{Q}(P) \hookrightarrow F$. So knowing all "primitive" degrees of Δ-CM closed points on $X(M,N) \iff$ knowing all degrees of number fields over which there is a Δ-CM elliptic curve with torsion subgroup containing $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$.

Transitioning to $X_0(N)$

To classify CM torsion subgroups in degree d, after Bourdon-Clark we still to determine all primitive degrees of closed CM points on $X_1(N)$ and $X(2, 2N)$. (Today: $X_1(N)$.)

Transitioning to $X_0(N)$

To classify CM torsion subgroups in degree d, after Bourdon-Clark we still to determine all primitive degrees of closed CM points on $X_1(N)$ and $X(2, 2N)$. (Today: $X_1(N)$.)

Fix K. **From now on we assume** $K \neq \mathbb{Q}(\sqrt{-3}), \mathbb{Q}(\sqrt{-4})$

Transitioning to $X_0(N)$

To classify CM torsion subgroups in degree d, after Bourdon-Clark we still to determine all primitive degrees of closed CM points on $X_1(N)$ and $X(2, 2N)$. (Today: $X_1(N)$.)

Fix K. **From now on we assume** $K \neq \mathbb{Q}(\sqrt{-3}), \mathbb{Q}(\sqrt{-4})$

Work of Bourdon-Clark implies, for all $N \geq 3$, that the fiber of $X_1(N) \to X_0(N)$ over every closed CM point is INERT: consists of one closed point and the residual degree is multiplied by $\deg(X_1(N) \to X_0(N)) = \frac{\varphi(N)}{2}$. So:

Transitioning to $X_0(N)$

To classify CM torsion subgroups in degree d, after Bourdon-Clark we still to determine all primitive degrees of closed CM points on $X_1(N)$ and $X(2, 2N)$. (Today: $X_1(N)$.)

Fix K. **From now on we assume** $K \neq \mathbb{Q}(\sqrt{-3}), \mathbb{Q}(\sqrt{-4})$

Work of Bourdon-Clark implies, for all $N \geq 3$, that the fiber of $X_1(N) \rightarrow X_0(N)$ over every closed CM point is INERT: consists of one closed point and the residual degree is multiplied by $\deg(X_1(N) \rightarrow X_0(N)) = \frac{\varphi(N)}{2}$. So:

Knowing degrees of all Δ-CM closed points on $X_0(N) \iff$ knowing all degrees of Δ-CM closed points on $X_1(N)$.

Main Result on $X_0(N)$

MAIN RESULT: for all Δ (with $\Delta_K < -4$) and all $N \in \mathbb{Z}^+$, we determine the fiber of the $\mathbb{Q}$-morphism $X_0(N) \to X(1)$ over J_Δ

Main Result on $X_0(N)$

MAIN RESULT: for all Δ (with $\Delta_K < -4$) and all $N \in \mathbb{Z}^+$, we determine the fiber of the $\mathbb{Q}$-morphism $X_0(N) \to X(1)$ over J_Δ and identify the fields $\mathbb{Q}(P)$.

The rational ring class field I

The field of moduli $\mathbb{Q}(\varphi)$ of an isogeny $\varphi : E \to E'$ satisfies

$$\mathbb{Q}(\varphi) \supset \mathbb{Q}(j(E), j(E')).$$

The rational ring class field I

The field of moduli $\mathbb{Q}(\varphi)$ of an isogeny $\varphi : E \to E'$ satisfies

$$\mathbb{Q}(\varphi) \supset \mathbb{Q}(j(E), j(E')).$$

FACT: If E has no CM, then $\mathbb{Q}(\varphi) = \mathbb{Q}(j(E), j(E'))$. Not true in CM case, but not far off!

The rational ring class field I

The field of moduli $\mathbb{Q}(\varphi)$ of an isogeny $\varphi : E \rightarrow E'$ satisfies

$$\mathbb{Q}(\varphi) \supset \mathbb{Q}(j(E), j(E')).$$

FACT: If E has no CM, then $\mathbb{Q}(\varphi) = \mathbb{Q}(j(E), j(E'))$. Not true in CM case, but not far off!

(It turns out that $\mathbb{Q}(\varphi) = \mathbb{Q}(j(E), j(E'))$ or $K(j(E), j(E'))$.)

The rational ring class field I

The field of moduli $\mathbb{Q}(\varphi)$ of an isogeny $\varphi : E \to E'$ satisfies

$$\mathbb{Q}(\varphi) \supset \mathbb{Q}(j(E), j(E')).$$

FACT: If E has no CM, then $\mathbb{Q}(\varphi) = \mathbb{Q}(j(E), j(E'))$. Not true in CM case, but not far off!

(It turns out that $\mathbb{Q}(\varphi) = \mathbb{Q}(j(E), j(E'))$ or $K(j(E), j(E'))$.)

For $\Delta = \mathfrak{f}^2 \Delta_K$, we define the **rational ring class field**

$$\mathbb{Q}(\mathfrak{f}) := \mathbb{Q}(j_\Delta) = \mathbb{Q}(j(\mathbb{C}/\mathcal{O}(\Delta)))$$

and the **ring class field**

$$K(\mathfrak{f}) := K(j_\Delta).$$

We have $\mathbb{Q}(\mathfrak{f}_1)\mathbb{Q}(\mathfrak{f}_2) = \mathbb{Q}(\mathrm{lcm}(\mathfrak{f}_1, \mathfrak{f}_2))$.

The rational ring class field I

The field of moduli $\mathbb{Q}(\varphi)$ of an isogeny $\varphi : E \to E'$ satisfies

$$\mathbb{Q}(\varphi) \supset \mathbb{Q}(j(E), j(E')).$$

FACT: If E has no CM, then $\mathbb{Q}(\varphi) = \mathbb{Q}(j(E), j(E'))$. Not true in CM case, but not far off!

(It turns out that $\mathbb{Q}(\varphi) = \mathbb{Q}(j(E), j(E'))$ or $K(j(E), j(E'))$.)

For $\Delta = \mathfrak{f}^2 \Delta_K$, we define the **rational ring class field**

$$\mathbb{Q}(\mathfrak{f}) := \mathbb{Q}(j_\Delta) = \mathbb{Q}(j(\mathbb{C}/\mathcal{O}(\Delta)))$$

and the **ring class field**

$$K(\mathfrak{f}) := K(j_\Delta).$$

We have $\mathbb{Q}(\mathfrak{f}_1)\mathbb{Q}(\mathfrak{f}_2) = \mathbb{Q}(\mathrm{lcm}(\mathfrak{f}_1, \mathfrak{f}_2))$.

This would compute $\mathbb{Q}(j(E), j(E'))$ except...

The rational ring class field II

...the field $\mathbb{Q}(\mathfrak{f})/\mathbb{Q}$ is not [except in finitely many cases] Galois.

The rational ring class field II

...the field $\mathbb{Q}(\mathfrak{f})/\mathbb{Q}$ is not [except in finitely many cases] Galois.

But it's close. $K(\mathfrak{f})/\mathbb{Q}$ is Galois, so if $\mathbb{Q}(\mathfrak{f})/\mathbb{Q}$ is not Galois, its Galois closure is $K(\mathfrak{f})$.

The rational ring class field II

...the field $\mathbb{Q}(\mathfrak{f})/\mathbb{Q}$ is not [except in finitely many cases] Galois.

But it's close. $K(\mathfrak{f})/\mathbb{Q}$ is Galois, so if $\mathbb{Q}(\mathfrak{f})/\mathbb{Q}$ is not Galois, its Galois closure is $K(\mathfrak{f})$.

The number of real Δ-CM j-invariants is

$$h_2(\Delta) := \#(\operatorname{Pic}\mathcal{O}(\Delta))[2].$$

Gauss's genus theory gives a formula for this in terms of Δ.

The rational ring class field II

...the field $\mathbb{Q}(\mathfrak{f})/\mathbb{Q}$ is not [except in finitely many cases] Galois.

But it's close. $K(\mathfrak{f})/\mathbb{Q}$ is Galois, so if $\mathbb{Q}(\mathfrak{f})/\mathbb{Q}$ is not Galois, its Galois closure is $K(\mathfrak{f})$.

The number of real Δ-CM j-invariants is

$$h_2(\Delta) := \#(\operatorname{Pic} \mathcal{O}(\Delta))[2].$$

Gauss's genus theory gives a formula for this in terms of Δ.

$\mathbb{Q}(\mathfrak{f})/\mathbb{Q}$ is Galois iff $h(\Delta) = h_2(\Delta)$, and if j is a Δ-CM j-invariant, then $j \in \mathbb{Q}(\mathfrak{f})$ iff $j \in \mathbb{R}$, since $\mathbb{Q}(\mathfrak{f}) = K(\mathfrak{f})^c$.

A Crude Form of the Answer

A useful upper bound on $\mathbb{Q}(\varphi)$:

Theorem (Parish, 1989)

For any cyclic N-isogeny $\varphi : E \to E'$ such that E has $\Delta (= \mathfrak{f}^2 \Delta_K)$-CM, we have $K(\varphi) \subset K(\mathfrak{f}N)$.

A Crude Form of the Answer

A useful upper bound on $\mathbb{Q}(\varphi)$:

Theorem (Parish, 1989)

For any cyclic N-isogeny $\varphi : E \to E'$ such that E has $\Delta(= \mathfrak{f}^2\Delta_K)$-CM, we have $K(\varphi) \subset K(\mathfrak{f}N)$.

Our main result will give, in particular, that for any cyclic N-isogeny $\varphi : E \to E'$ with E Δ-CM, then $\mathbb{Q}(\varphi)$ is (up to field isomorphism) either $\mathbb{Q}(M\mathfrak{f})$ or $K(M\mathfrak{f})$ for some $M \mid N$.

A Crude Form of the Answer

A useful upper bound on $\mathbb{Q}(\varphi)$:

Theorem (Parish, 1989)

For any cyclic N-isogeny $\varphi : E \to E'$ such that E has $\Delta(= \mathfrak{f}^2\Delta_K)$-CM, we have $K(\varphi) \subset K(\mathfrak{f}N)$.

Our main result will give, in particular, that for any cyclic N-isogeny $\varphi : E \to E'$ with E Δ-CM, then $\mathbb{Q}(\varphi)$ is (up to field isomorphism) either $\mathbb{Q}(M\mathfrak{f})$ or $K(M\mathfrak{f})$ for some $M \mid N$.

This explains the tensor products of such fields in the next slide.

Reduction to the Prime Power Case

Reduction to $X_0(\ell^a)$ is straightforward, though a bit technical.

Reduction to the Prime Power Case

Reduction to $X_0(\ell^a)$ is straightforward, though a bit technical.

Underlying Principle: If $\gcd(N_1, N_2) = 1$, then $X_0(N_1 N_2) \rightarrow X(1)$ is the fiber product of $X_0(N_1) \rightarrow X(1)$ and $X_0(N_2) \rightarrow X(1)$.

Reduction to the Prime Power Case

Reduction to $X_0(\ell^a)$ is straightforward, though a bit technical.

Underlying Principle: If $\gcd(N_1, N_2) = 1$, then $X_0(N_1N_2) \to X(1)$ is the fiber product of $X_0(N_1) \to X(1)$ and $X_0(N_2) \to X(1)$.

(NOT true for $X_1(N)$....isogenies are better.)

Reduction to the Prime Power Case

Reduction to $X_0(\ell^a)$ is straightforward, though a bit technical.

Underlying Principle: If $\gcd(N_1, N_2) = 1$, then $X_0(N_1 N_2) \rightarrow X(1)$ is the fiber product of $X_0(N_1) \rightarrow X(1)$ and $X_0(N_2) \rightarrow X(1)$.

(NOT true for $X_1(N)$....isogenies are better.)

Using this and the fact that if $\gcd(\mathfrak{f}_1, \mathfrak{f}_2) = \mathfrak{f}$, then

$$\mathbb{Q}(\mathfrak{f}_1) \otimes_{\mathbb{Q}(\mathfrak{f})} \mathbb{Q}(\mathfrak{f}_2) \cong \mathbb{Q}(\operatorname{lcm}(\mathfrak{f}_1, \mathfrak{f}_2)),$$

$$\mathbb{Q}(\mathfrak{f}_1) \otimes_{\mathbb{Q}(\mathfrak{f})} K(\mathfrak{f}_2) \cong K(\operatorname{lcm}(\mathfrak{f}_1, \mathfrak{f}_2)),$$

$$K(\mathfrak{f}_1) \otimes_{\mathbb{Q}(\mathfrak{f})} K(\mathfrak{f}_2) \cong K(\operatorname{lcm}(\mathfrak{f}_1, \mathfrak{f}_2)) \times K(\operatorname{lcm}(\mathfrak{f}_1, \mathfrak{f}_2)),$$

we reduce to the prime power case.

Um, I was told there would be volcanoes

Fix a prime ℓ. The (K, ℓ)-**isogeny volcano** is a directed multigraph with vertices the j-invariants of K-CM elliptic curves $E_{/\mathbb{C}}$ and with edges $E \to E'$ corresponding to ℓ-isogenies $\varphi : E \to E'$ up to isomorphism on E'. Every edge has an inverse edge, the dual isogeny. The **level** of a vertex is $\mathrm{ord}_\ell(\mathfrak{f})$.

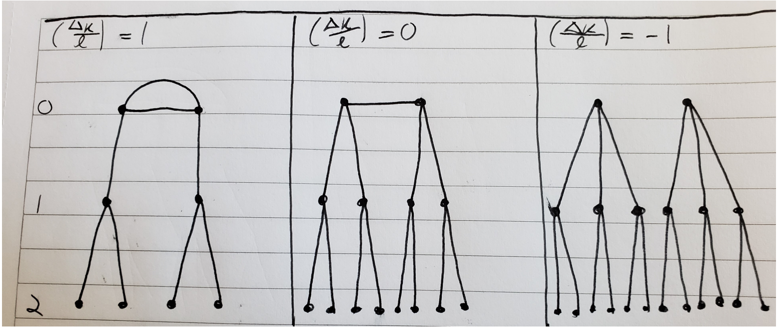
Um, I was told there would be volcanoes

Fix a prime ℓ. The (K, ℓ)-**isogeny volcano** is a directed multigraph with vertices the j-invariants of K-CM elliptic curves $E_{/\mathbb{C}}$ and with edges $E \to E'$ corresponding to ℓ-isogenies $\varphi : E \to E'$ up to isomorphism on E'. Every edge has an inverse edge, the dual isogeny. The **level** of a vertex is $\mathrm{ord}_\ell(\mathfrak{f})$.

Since ℓ-power isogenies can only change the ℓ-part of $\mathfrak{f}$, the graph breaks up into pieces parameterized by $\mathfrak{f}_0$, the prime-to-ℓ part of $\mathfrak{f}$. Let's also fix $\mathfrak{f}_0$.

Isogeny Volcanoes

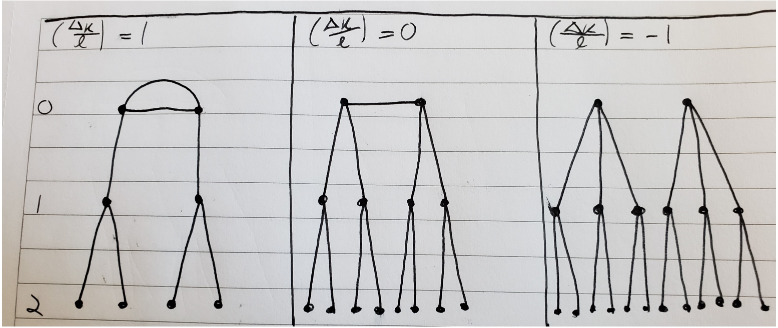
The graph has a very simple structure:



- Every vertex has outward degree $\ell + 1$.

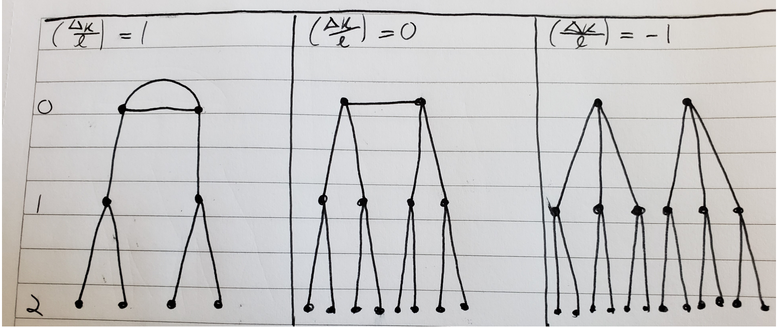
Isogeny Volcanoes

The graph has a very simple structure:



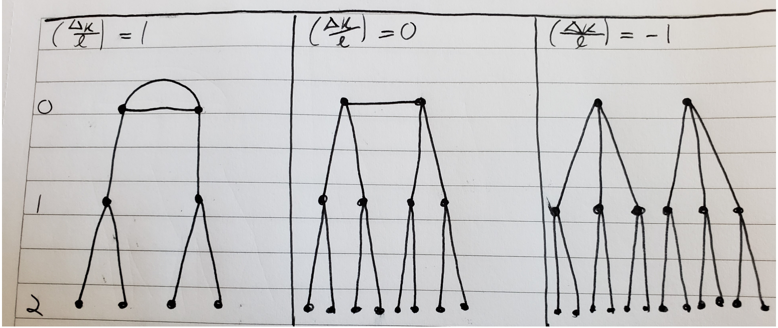
- Every vertex has outward degree $\ell + 1$.
- The set of level 0 vertices is the **surface**. Edges lying within the surface are **horizontal**. Each surface vertex has $1 + \left(\frac{\Delta_K}{\ell}\right)$ horizontal outward edges.

Isogeny Volcanoes II



- The other edges are **ascending**, going from level $L \geq 1$ to level $L - 1$, or **descending**, the inverses of ascending edges.

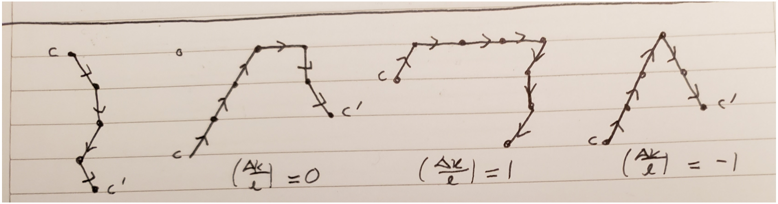
Isogeny Volcanoes II



• The other edges are **ascending**, going from level $L \geq 1$ to level $L-1$, or **descending**, the inverses of ascending edges.

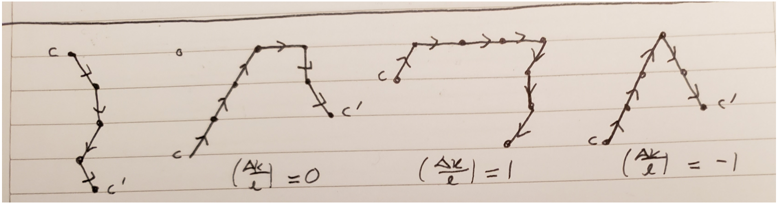
• Every vertex not on the surface has a unique ascending outward edge. From this one deduces the number of descending outward edges every vertex has (it's ℓ away from the surface, and always at least 1).

Paths in Isogeny Volcanoes



Key Fact: Cyclic ℓ^a-isogenies $\varphi : E \rightarrow E' \iff$ length a nonbacktracking paths from $j(E)$ to $j(E')$. Such paths are restricted: they must, ascend, then be horizontal, then descend. (Some parts may have length zero.) So you can count them without real trouble.

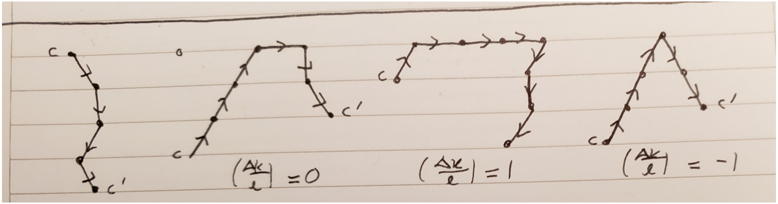
Fields of moduli on $X_1(\ell^a)_{/K}$



We can now compute $K(\varphi)$ for any cyclic ℓ^a-isogeny $\varphi : E \to E'$. If E has level c, E' has level c' and $C := \max(c, c')$, then

$$K(\varphi) \supset K(j(E), j(E')) = K(\ell^C \mathfrak{f}_0).$$

Fields of moduli on $X_1(\ell^a)_{/K}$



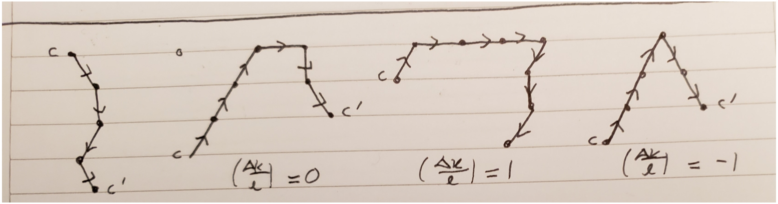
We can now compute $K(\varphi)$ for any cyclic ℓ^a-isogeny $\varphi : E \to E'$. If E has level c, E' has level c' and $C := \max(c, c')$, then

$$K(\varphi) \supset K(j(E), j(E')) = K(\ell^C \mathfrak{f}_0).$$

Using Parish's Theorem one sees that $K(\varphi) \subset K(\ell^C \mathfrak{f}_0)$, so

$$K(\varphi) = K(\ell^C \mathfrak{f}_0).$$

Fields of moduli on $X_1(\ell^a)_{/K}$



We can now compute $K(\varphi)$ for any cyclic ℓ^a-isogeny $\varphi : E \to E'$. If E has level c, E' has level c' and $C := \max(c, c')$, then

$$K(\varphi) \supset K(j(E), j(E')) = K(\ell^C \mathfrak{f}_0).$$

Using Parish's Theorem one sees that $K(\varphi) \subset K(\ell^C \mathfrak{f}_0)$, so

$$K(\varphi) = K(\ell^C \mathfrak{f}_0).$$

There is still a nontrivial **counting problem**.

Volcanoes and Reality

We want to work over $\mathbb{Q}$. If $\varphi : E \to E'$ is a cyclic ℓ^a-isogeny with E Δ-CM, WLOG we may assume $j(E) = j_\Delta$. If E has level c and E' has level c', we may assume $c \geq c'$: otherwise switch to $\varphi^\vee$, which has the same field of moduli.

Volcanoes and Reality

We want to work over $\mathbb{Q}$. If $\varphi : E \rightarrow E'$ is a cyclic ℓ^a-isogeny with E Δ-CM, WLOG we may assume $j(E) = j_\Delta$. If E has level c and E' has level c', we may assume $c \geq c'$: otherwise switch to $\varphi^\vee$, which has the same field of moduli. Then:

$$\mathbb{Q}(j(E)) = \mathbb{Q}(\ell^c \mathfrak{f}_0) \subset \mathbb{Q}(\varphi) \subset K(\varphi) = K(\ell^c \mathfrak{f}_0),$$

so the only question is whether $\mathbb{Q}(\varphi)$ contains K.

Volcanoes and Reality

We want to work over $\mathbb{Q}$. If $\varphi : E \to E'$ is a cyclic ℓ^a-isogeny with E Δ-CM, WLOG we may assume $j(E) = j_\Delta$. If E has level c and E' has level c', we may assume $c \geq c'$: otherwise switch to $\varphi^\vee$, which has the same field of moduli. Then:

$$\mathbb{Q}(j(E)) = \mathbb{Q}(\ell^c \mathfrak{f}_0) \subset \mathbb{Q}(\varphi) \subset K(\varphi) = K(\ell^c \mathfrak{f}_0),$$

so the only question is whether $\mathbb{Q}(\varphi)$ contains K.

There is an action of complex conjugation c on the volcano. Call a path **real** if all its edges are c-fixed.

Reality of the Path Determines the Field of Moduli

If the path is not real then either
(i) It contains a non-real surface edge, or
(ii) The terminal vertex is not real.

Reality of the Path Determines the Field of Moduli

If the path is not real then either
(i) It contains a non-real surface edge, or
(ii) The terminal vertex is not real.

Case (i) is less interesting: trust me that $\mathbb{Q}(\varphi)$ contains K.

Reality of the Path Determines the Field of Moduli

If the path is not real then either
(i) It contains a non-real surface edge, or
(ii) The terminal vertex is not real.

Case (i) is less interesting: trust me that $\mathbb{Q}(\varphi)$ contains K.

In Case (ii) $\mathbb{Q}(\varphi)$ contains $\mathbb{Q}(\ell^c \mathfrak{f}_0)$ and a field that is conjugate but not equal to $\mathbb{Q}(\ell^{c'} \mathfrak{f}_0)$. By what we saw above, that means it contains K.

Reality of the Path Determines the Field of Moduli

If the path is not real then either
(i) It contains a non-real surface edge, or
(ii) The terminal vertex is not real.

Case (i) is less interesting: trust me that $\mathbb{Q}(\varphi)$ contains K.

In Case (ii) $\mathbb{Q}(\varphi)$ contains $\mathbb{Q}(\ell^c \mathfrak{f}_0)$ and a field that is conjugate but not equal to $\mathbb{Q}(\ell^{c'} \mathfrak{f}_0)$. By what we saw above, that means it contains K.

In order to implement this, we have to determine the action of complex conjugation on the isogeny volcano.

Reality of the Path Determines the Field of Moduli

If the path is not real then either
(i) It contains a non-real surface edge, or
(ii) The terminal vertex is not real.

Case (i) is less interesting: trust me that $\mathbb{Q}(\varphi)$ contains K.

In Case (ii) $\mathbb{Q}(\varphi)$ contains $\mathbb{Q}(\ell^c \mathfrak{f}_0)$ and a field that is conjugate but not equal to $\mathbb{Q}(\ell^{c'} \mathfrak{f}_0)$. By what we saw above, that means it contains K.

In order to implement this, we have to determine the action of complex conjugation on the isogeny volcano.

I did so. (Tell you about it some other time!)

Reality of the Path Determines the Field of Moduli

If the path is not real then either
(i) It contains a non-real surface edge, or
(ii) The terminal vertex is not real.

Case (i) is less interesting: trust me that $\mathbb{Q}(\varphi)$ contains K.

In Case (ii) $\mathbb{Q}(\varphi)$ contains $\mathbb{Q}(\ell^c \mathfrak{f}_0)$ and a field that is conjugate but not equal to $\mathbb{Q}(\ell^{c'} \mathfrak{f}_0)$. By what we saw above, that means it contains K.

In order to implement this, we have to determine the action of complex conjugation on the isogeny volcano.

I did so. (Tell you about it some other time!)

Finally, one is left with a refined version of the above combinatorial problem: count real / complex paths, up to closed points. It takes some work...Hope to have a preprint

Thanks!

Thanks for listening, and thanks to the organizers.