Report on the CM Case

Pete L. Clark

Department of Mathematics
The University of Georgia

September 21, 2023

Scope

In this talk I will:

Scope

In this talk I will:

- Report on work on CM elliptic curves over number fields

Scope

In this talk I will:

- Report on work on CM elliptic curves over number fields (including almost two decades' work of collaborators and me)

Scope

In this talk I will:

• Report on work on CM elliptic curves over number fields (including almost two decades' work of collaborators and me)

• With emphasis on recent joint work with F. Saia that **solves** (stay tuned for fine print) the problem of computing torsion subgroups of CM elliptic curves in fixed number field degree

Scope

In this talk I will:

• Report on work on CM elliptic curves over number fields (including almost two decades' work of collaborators and me)

• With emphasis on recent joint work with F. Saia that **solves** (stay tuned for fine print) the problem of computing torsion subgroups of CM elliptic curves in fixed number field degree

• Discuss **open problems** you're encouraged to work on.

Analytic Study of CM Torsion

For $d \in \mathbb{Z}^+$, put

$$T_{\mathrm{CM}}(d) := \sup \{\#E(F)[\mathrm{tors}] \mid E/F \text{ is CM and } [F : \mathbb{Q}] = d\}.$$

(In a pre-Merel world, not obvious this is always finite, but....)

Analytic Study of CM Torsion

For $d \in \mathbb{Z}^+$, put

$$T_{\mathrm{CM}}(d) := \sup \{\#E(F)[\mathrm{tors}] \mid E/F \text{ is CM and } [F:\mathbb{Q}] = d\}.$$

(In a pre-Merel world, not obvious this is always finite, but....)

(Silverberg 1988) $T_{\mathrm{CM}}(d) = O((d \log\log d)^2)$.

Analytic Study of CM Torsion

For $d \in \mathbb{Z}^+$, put

$$T_{\mathrm{CM}}(d) := \sup \{\#E(F)[\mathrm{tors}] \mid E/F \text{ is CM and } [F:\mathbb{Q}] = d\}.$$

(In a pre-Merel world, not obvious this is always finite, but....)

(Silverberg 1988) $T_{\mathrm{CM}}(d) = O((d \log \log d)^2)$.
(Hindry-Silverman 1999) $\implies T_{\mathrm{CM}}(d) = O(d \log d)$.

Analytic Study of CM Torsion

For $d \in \mathbb{Z}^+$, put

$$T_{\mathrm{CM}}(d) := \sup \{\#E(F)[\mathrm{tors}] \mid E/F \text{ is CM and } [F:\mathbb{Q}] = d\}.$$

(In a pre-Merel world, not obvious this is always finite, but....)

(Silverberg 1988) $T_{\mathrm{CM}}(d) = O((d \log \log d)^2)$.
(Hindry-Silverman 1999) $\implies T_{\mathrm{CM}}(d) = O(d \log d)$.

(Actually, Silverberg showed $\exp E(F)[\mathrm{tors}] = O(d \log \log d)$.)

Analytic Study of CM Torsion

For $d \in \mathbb{Z}^+$, put

$$T_{\mathrm{CM}}(d) := \sup \{\#E(F)[\mathrm{tors}] \mid E/F \text{ is CM and } [F:\mathbb{Q}] = d\}.$$

(In a pre-Merel world, not obvious this is always finite, but....)

(Silverberg 1988) $T_{\mathrm{CM}}(d) = O((d \log \log d)^2)$.
(Hindry-Silverman 1999) $\implies T_{\mathrm{CM}}(d) = O(d \log d)$.

(Actually, Silverberg showed $\exp E(F)[\mathrm{tors}] = O(d \log \log d)$.)

(Breuer 2010) $T_{\mathrm{CM}}(d) \gg d \log \log d$ for infinitely many d.

Analytic Study of CM Torsion

For $d \in \mathbb{Z}^+$, put

$$T_{\mathrm{CM}}(d) := \sup \{\#E(F)[\mathrm{tors}] \mid E/F \text{ is CM and } [F : \mathbb{Q}] = d\}.$$

(In a pre-Merel world, not obvious this is always finite, but....)

(Silverberg 1988) $T_{\mathrm{CM}}(d) = O((d \log \log d)^2)$.
(Hindry-Silverman 1999) $\implies T_{\mathrm{CM}}(d) = O(d \log d)$.

(Actually, Silverberg showed $\exp E(F)[\mathrm{tors}] = O(d \log \log d)$.)

(Breuer 2010) $T_{\mathrm{CM}}(d) \gg d \log \log d$ for infinitely many d.

Taking all this in...seems like Breuer's bound is the truth.

The Truth About Torsion

The Truth About Torsion

Theorem

a) *(C-Pollack 2015)* $T_{\mathrm{CM}}(d) = O(d \log \log d)$.

The Truth About Torsion

Theorem

a) *(C-Pollack 2015)* $T_{\mathrm{CM}}(d) = O(d \log \log d)$.

b) *(C-Pollack 2017)* $\limsup_{d \to \infty} \frac{T_{\mathrm{CM}}(d)}{d \log \log d} = \frac{e^{\gamma}\pi}{\sqrt{3}}$.

The Truth About Torsion

Theorem

a) *(C-Pollack 2015)* $T_{\mathrm{CM}}(d) = O(d \log \log d)$.

b) *(C-Pollack 2017)* $\limsup_{d \to \infty} \frac{T_{\mathrm{CM}}(d)}{d \log \log d} = \frac{e^{\gamma}\pi}{\sqrt{3}}$.

c) *(Bourdon-C-Stankewicz '17)* $\liminf_{d \to \infty} T_{\mathrm{CM}}(d) = 6 = T_{\mathrm{CM}}(1)$.

The Truth About Torsion

Theorem

a) *(C-Pollack 2015)* $T_{\mathrm{CM}}(d) = O(d \log \log d)$.

b) *(C-Pollack 2017)* $\limsup_{d \to \infty} \frac{T_{\mathrm{CM}}(d)}{d \log \log d} = \frac{e^{\gamma}\pi}{\sqrt{3}}$.

c) *(Bourdon-C-Stankewicz '17)*
$\liminf_{d \to \infty} T_{\mathrm{CM}}(d) = 6 = T_{\mathrm{CM}}(1)$.

The Truth About Torsion

Theorem

a) *(C-Pollack 2015)* $T_{\mathrm{CM}}(d) = O(d \log \log d)$.

b) *(C-Pollack 2017)* $\limsup_{d \to \infty} \frac{T_{\mathrm{CM}}(d)}{d \log \log d} = \frac{e^{\gamma}\pi}{\sqrt{3}}$.

c) *(Bourdon-C-Stankewicz '17)* $\liminf_{d \to \infty} T_{\mathrm{CM}}(d) = 6 = T_{\mathrm{CM}}(1)$.

(Cf: $T(d) \gg \sqrt{d}$ for *all* d! CM case is *very* different....)

Low Degree CM Points on Modular Curves

(C-Genao-Pollack-Saia 2022) Give – good but not quite optimal – upper and lower bounds on the **least degree** of a closed CM point on modular curves $X_0(N)$, $X_1(N)$, $X_1(M,N)$.

Low Degree CM Points on Modular Curves

(C-Genao-Pollack-Saia 2022) Give – good but not quite optimal – upper and lower bounds on the **least degree** of a closed CM point on modular curves $X_0(N)$, $X_1(N)$, $X_1(M, N)$.

Deduce: away from an **explicit** finite list of N or (M, N), these curves have sporadic CM points.

Galois Representations

- $\mathcal{O}$ be an order in an imaginary quadratic field K
- $F \supseteq K$ a number field.
- For $E_{/F}$ $\mathcal{O}$-CM elliptic curve, have $\hat{\rho} : \mathfrak{g}_F \to \widehat{\mathcal{O}}^\times \subsetneq \mathrm{GL}_2(\hat{\mathbb{Z}})$.

Galois Representations

- $\mathcal{O}$ be an order in an imaginary quadratic field K
- $F \supseteq K$ a number field.
- For $E_{/F}$ $\mathcal{O}$-CM elliptic curve, have $\hat{\rho} : \mathfrak{g}_F \to \widehat{\mathcal{O}}^\times \subsetneq \mathrm{GL}_2(\hat{\mathbb{Z}})$.

(Serre 1972) $[\widehat{\mathcal{O}}^\times : \mathrm{Im}\, \hat{\rho}] < \infty$

Galois Representations

- $\mathcal{O}$ be an order in an imaginary quadratic field K
- $F \supseteq K$ a number field.
- For $E_{/F}$ $\mathcal{O}$-CM elliptic curve, have $\hat{\rho} : \mathfrak{g}_F \to \widehat{\mathcal{O}}^\times \subsetneq \mathrm{GL}_2(\hat{\mathbb{Z}})$.

(Serre 1972) $[\widehat{\mathcal{O}}^\times : \mathrm{Im}\,\hat{\rho}] < \infty$

(Stevenhagen, Bourdon-C, Lozano-Robledo, Campagna-Pengo) The index is bounded in terms of $[F : \mathbb{Q}]$ alone!

Galois Representations

- $\mathcal{O}$ be an order in an imaginary quadratic field K
- $F \supseteq K$ a number field.
- For $E_{/F}$ $\mathcal{O}$-CM elliptic curve, have $\hat{\rho} : \mathfrak{g}_F \to \widehat{\mathcal{O}}^\times \subsetneq \mathrm{GL}_2(\hat{\mathbb{Z}})$.

(Serre 1972) $[\widehat{\mathcal{O}}^\times : \mathrm{Im}\,\hat{\rho}] < \infty$

(Stevenhagen, Bourdon-C, Lozano-Robledo, Campagna-Pengo) The index is bounded in terms of $[F : \mathbb{Q}]$ alone!

In fact: $[\widehat{\mathcal{O}}^\times : \mathrm{Im}\,\hat{\rho}] \mid \#\mathcal{O}^\times [F : K(j(E))] \leq 3[F : \mathbb{Q}]$.

Recent work of Alvaro, Campagna-Pengo, York goes farther.

Algebraic Torsion

Problem: For $d \in \mathbb{Z}^+$, compute the complete (finite!) list of torsion subgroups $E(F)[\mathrm{tors}]$ for $[F : \mathbb{Q}] = d$ and E/F CM.

Algebraic Torsion

Problem: For $d \in \mathbb{Z}^+$, compute the complete (finite!) list of torsion subgroups $E(F)[\mathrm{tors}]$ for $[F : \mathbb{Q}] = d$ and E/F CM.

Better: give the list separately for each CM j-invariant (up to Galois conjugacy); equivalently for each order $\mathcal{O}$; equivalently, for each imaginary quadratic discriminant $\Delta = \Delta(\mathcal{O})$.

Algebraic Torsion

Problem: For $d \in \mathbb{Z}^+$, compute the complete (finite!) list of torsion subgroups $E(F)[\mathrm{tors}]$ for $[F : \mathbb{Q}] = d$ and E/F CM.

Better: give the list separately for each CM j-invariant (up to Galois conjugacy); equivalently for each order $\mathcal{O}$; equivalently, for each imaginary quadratic discriminant $\Delta = \Delta(\mathcal{O})$.

Theorem (Prior Work)

a) $d \leq 13$ *(Olson 1976, Clark-Corn-Rice-Stankewicz 2014)*

Algebraic Torsion

Problem: For $d \in \mathbb{Z}^+$, compute the complete (finite!) list of torsion subgroups $E(F)[\text{tors}]$ for $[F:\mathbb{Q}] = d$ and E/F CM.

Better: give the list separately for each CM j-invariant (up to Galois conjugacy); equivalently for each order $\mathcal{O}$; equivalently, for each imaginary quadratic discriminant $\Delta = \Delta(\mathcal{O})$.

Theorem (Prior Work)

a) $d \leq 13$ *(Olson 1976, Clark-Corn-Rice-Stankewicz 2014)*

b) $d = p$ *prime (Bourdon-Clark-Stankewicz 2017)*

Algebraic Torsion

Problem: For $d \in \mathbb{Z}^+$, compute the complete (finite!) list of torsion subgroups $E(F)[\mathrm{tors}]$ for $[F:\mathbb{Q}] = d$ and E/F CM.

Better: give the list separately for each CM j-invariant (up to Galois conjugacy); equivalently for each order $\mathcal{O}$; equivalently, for each imaginary quadratic discriminant $\Delta = \Delta(\mathcal{O})$.

Theorem (Prior Work)

a) $d \leq 13$ *(Olson 1976, Clark-Corn-Rice-Stankewicz 2014)*

b) $d = p$ *prime (Bourdon-Clark-Stankewicz 2017)*

c) d *odd (Bourdon-Pollack 2018)*

Algebraic Torsion

Problem: For $d \in \mathbb{Z}^+$, compute the complete (finite!) list of torsion subgroups $E(F)[\mathrm{tors}]$ for $[F:\mathbb{Q}] = d$ and E/F CM.

Better: give the list separately for each CM j-invariant (up to Galois conjugacy); equivalently for each order $\mathcal{O}$; equivalently, for each imaginary quadratic discriminant $\Delta = \Delta(\mathcal{O})$.

Theorem (Prior Work)

a) *$d \leq 13$ (Olson 1976, Clark-Corn-Rice-Stankewicz 2014)*
b) *$d = p$ prime (Bourdon-Clark-Stankewicz 2017)*
c) *d odd (Bourdon-Pollack 2018)*
d) *$d = 2p$ twice a prime (Bourdon-Chaos 2023)*

Introducing Clark-Saia

Recent work of C-Saia, building on work of Bourdon-C, gives a **complete classification** of torsion subgroups of CM elliptic curves in *any* number field d. More precisely:

Introducing Clark-Saia

Recent work of C-Saia, building on work of Bourdon-C, gives a **complete classification** of torsion subgroups of CM elliptic curves in *any* number field d. More precisely:

• INPUT List of all imaginary quadratic orders Δ such that h_Δ properly divides d.

Introducing Clark-Saia

Recent work of C-Saia, building on work of Bourdon-C, gives a **complete classification** of torsion subgroups of CM elliptic curves in *any* number field d. More precisely:

• INPUT List of all imaginary quadratic orders Δ such that h_Δ properly divides d.

• OUTPUT For every CM j-invariant j with $[\mathbb{Q}(j) : \mathbb{Q}]$ properly dividing d, list of all possible subgroups $E(F)[\mathrm{tors}]$ with $j(E)$ Galois conjugate to j, $[F : \mathbb{Q}] = d$.

Introducing Clark-Saia

Recent work of C-Saia, building on work of Bourdon-C, gives a **complete classification** of torsion subgroups of CM elliptic curves in *any* number field d. More precisely:

• INPUT List of all imaginary quadratic orders Δ such that h_Δ properly divides d.

• OUTPUT For every CM j-invariant j with $[\mathbb{Q}(j) : \mathbb{Q}]$ properly dividing d, list of all possible subgroups $E(F)[\mathrm{tors}]$ with $j(E)$ Galois conjugate to j, $[F : \mathbb{Q}] = d$.

(Why **properly** divides? Because otherwise $F = \mathbb{Q}(j(E))$, and then $\varphi(\#E(F)[\mathrm{tors}]) \leq 2$ (Parish 1989). All six such groups occur over $\mathbb{Q}$ (Olson 1976) and thus occur in every degree.)

Details on Clark-Saia, Part 1

Fix $M \mid N$. Torsion problem is equivalent to understanding degrees of closed CM points on modular curves $X_1(M, N)$.

Details on Clark-Saia, Part 1

Fix $M \mid N$. Torsion problem is equivalent to understanding degrees of closed CM points on modular curves $X_1(M,N)$.

Details on Clark-Saia, Part 1

Fix $M \mid N$. Torsion problem is equivalent to understanding degrees of closed CM points on modular curves $X_1(M, N)$.

We approach this via the corresponding problem on the "isogeny version" $X_0(M, N)$, defined by the subgroup $H_0(M, N) =$

$$\left\{ \left[\begin{array}{cc} a & b \\ 0 & d \end{array} \right] \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \middle| \, b \equiv 0 \mod M, \, a \equiv d \mod M \right\}.$$

Details on Clark-Saia, Part 1

Fix $M \mid N$. Torsion problem is equivalent to understanding degrees of closed CM points on modular curves $X_1(M,N)$.

We approach this via the corresponding problem on the "isogeny version" $X_0(M,N)$, defined by the subgroup $H_0(M,N) =$

$$\left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \middle| b \equiv 0 \mod M,\ a \equiv d \mod M \right\}.$$

TASK: for each Δ and $M \mid N$, compute fiber of $X_0(M,N) \to X(1)$ over the closed point J_Δ (of degree h_Δ). When $\Delta < -4$, these fibers are reduced, so are products of number fields. Each number field is $\mathbb{Q}(J_{n^2\Delta})$ or $K(J_{n^2\Delta})$ for some $n \mid N$.

Details on Clark-Saia, Part 2

Broad sketch of how we accomplish the main task:

Details on Clark-Saia, Part 2

Broad sketch of how we accomplish the main task:

1: Reduce to $N = \ell^a$. (*Mostly* straightforward.)

Details on Clark-Saia, Part 2

Broad sketch of how we accomplish the main task:

1: Reduce to $N = \ell^a$. (*Mostly* straightforward.)

2: For ℓ-primary case, use **isogeny volcanoes**. With extant theory, this would solve the problem working with K-schemes. To work with $\mathbb{Q}$-schemes, need to explicitly determine the action of complex conjugation on isogeny volcanoes.

Details on Clark-Saia, Part 2

Broad sketch of how we accomplish the main task:

1: Reduce to $N = \ell^a$. (*Mostly* straightforward.)

2: For ℓ-primary case, use **isogeny volcanoes**. With extant theory, this would solve the problem working with K-schemes. To work with $\mathbb{Q}$-schemes, need to explicitly determine the action of complex conjugation on isogeny volcanoes.

3: When $\Delta_K < -4$, this all goes **very smoothly**...and I rederived some prior results to showcase the method.

Details on Clark-Saia, Part 2

Broad sketch of how we accomplish the main task:

1: Reduce to $N = \ell^a$. (*Mostly* straightforward.)

2: For ℓ-primary case, use **isogeny volcanoes**. With extant theory, this would solve the problem working with K-schemes. To work with $\mathbb{Q}$-schemes, need to explicitly determine the action of complex conjugation on isogeny volcanoes.

3: When $\Delta_K < -4$, this all goes **very smoothly**...and I rederived some prior results to showcase the method.

4: When $\Delta_K \in \{-3, -4\}$, extra technical complications **everywhere**. E.g. Step 1 is *not* straightforward. In some cases **there isn't a well-defined action of complex conjugation on isogeny volcano**. Much less clean, but we got it.

Details on Clark-Saia, Part 3

But why does the torsion problem $X_1(M,N)$ reduce to the isogeny problem $X_0(M,N)$? Because:

Details on Clark-Saia, Part 3

But why does the torsion problem $X_1(M,N)$ reduce to the isogeny problem $X_0(M,N)$? Because:

Theorem

All fibers of $\pi : X_1(M,N) \to X_0(M,N)$ over closed CM points are connected – i.e., π is a bijection on the CM-locus.

This is deduced from the largeness of the adelic Galois rep!

Details on Clark-Saia, Part 3

But why does the torsion problem $X_1(M, N)$ reduce to the isogeny problem $X_0(M, N)$? Because:

Theorem

All fibers of $\pi : X_1(M, N) \to X_0(M, N)$ over closed CM points are connected – i.e., π is a bijection on the CM-locus.

This is deduced from the largeness of the adelic Galois rep!

So: away from $\Delta = -3, -4$ the degree of every upstairs closed point is $\deg \pi = \max(\frac{\varphi(N)}{2}, 1)$ times the degree of the corresponding downstairs closed point.

Details on Clark-Saia, Part 3

But why does the torsion problem $X_1(M, N)$ reduce to the isogeny problem $X_0(M, N)$? Because:

Theorem

All fibers of $\pi : X_1(M, N) \to X_0(M, N)$ over closed CM points are connected – i.e., π is a bijection on the CM-locus.

This is deduced from the largeness of the adelic Galois rep!

So: away from $\Delta = -3, -4$ the degree of every upstairs closed point is $\deg \pi = \max(\frac{\varphi(N)}{2}, 1)$ times the degree of the corresponding downstairs closed point.

Thus in passage from $X_0(M, N)$ to $X_1(M, N)$ we lose information about what the residue fields are, but we retain the number of such points and their degrees...which is (more than) enough info to solve the torsion problem.

What Remains

Problem

Record classification of CM torsion in degree d, for:

a) $d \leq 203$ *unconditionally.*

b) $d \leq 18,105$ *on GRH.*

What Remains

Problem

Record classification of CM torsion in degree d, for:

a) $d \leq 203$ *unconditionally.*

b) $d \leq 18,105$ *on GRH.*

Problem

Complete the classification of sporadic CM points on $X_0(N)$, $X_1(M,N)$.

What Remains

Problem

Record classification of CM torsion in degree d, for:

a) $d \leq 203$ *unconditionally.*

b) $d \leq 18,105$ *on GRH.*

Problem

Complete the classification of sporadic CM points on $X_0(N)$, $X_1(M, N)$. N.B.: What remains is not about CM points!

What Remains

Problem

Record classification of CM torsion in degree d, for:

a) $d \leq 203$ *unconditionally.*

b) $d \leq 18,105$ *on GRH.*

Problem

Complete the classification of sporadic CM points on $X_0(N)$, $X_1(M,N)$. N.B.: What remains is not about CM points!

More that Remains

Problem

Define an equivalence relation on $\mathbb{Z}^+$: $d_1 \sim_{\mathrm{CM}} d_2$ *if the classification of CM torsion in degrees* d_1 *and* d_2 *is the same (same groups arise). E.g for all* $p \geq 7$, $p \sim_{\mathrm{CM}} 1$. *Conjecture:*

- (i) *For all* $d \in \mathbb{Z}^+$, $\mathrm{density}([d]) > 0$; *and*
- (ii) *Summing over all equivalence classes, we get density* 1.

Bourdon-Pollack (2017) showed this for odd degrees. Showing that $[2]$ *has positive density is open, though Bourdon-Chaos (2023) show that it contains* $2p$ *for a density* 1 *set of primes* p *conditionally on Schinzel's Hypothesis H.*