(CM) Torsion on Elliptic Curves over Number Fields

Pete L. Clark

Department of Mathematics
The University of Georgia

June 22, 2021

$\mathcal{T}(d)$ and $T(d)$

For $E_{/F}$ an elliptic curve defined over a number field, the torsion subgroup $E(F)[\text{tors}]$ is **finite** (e.g. by Mordell-Weil) and **computable**. What are the possibilities?

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

$$\mathcal{T}(d) := \{\text{iso. classes of } E(F)[\text{tors}] \mid [F:\mathbb{Q}] = d\},$$

$$T(d) := \sup\{\#E(F)[\text{tors}] \mid [F:\mathbb{Q}] = d\}.$$

Is it obvious that $\mathcal{T}(d)$ and $T(d)$ are finite? Not at all, but...

Theorem (Merel, 1996)

$T(d) < \infty$ for all $d \in \mathbb{Z}^+$. Thus $\mathcal{T}(d)$ is a finite set for all d.

What is known about $\mathcal{T}(d)$

Theorem

a) *(Mazur, 1978) Computes $\mathcal{T}(1)$. Get: $T(1) = 16$.*
b) *(Kamienny, Kenku, Momose 1988, 1992) Compute $\mathcal{T}(2)$. Get $T(2) = 24$.*
c) *(Derickx-Etropolski-van Hoeij-Morrow-Zureick-Brown 2020) Compute $\mathcal{T}(3)$. Get $T(3) = 28$.*

So....maybe look for upper bounds on $T(d)$??

Merel's work is **effective**: gives an explicit upper bound on $T(d)$, improved by Oesterlé and Parent. But... These bounds are (worse than) exponential. This seems far from the truth.

Don't you know ANYTHING else about $T(d)$??

$T_{\mathbb{Q}}(d) :=$ like $T(d)$ but for $E_{/F}$ with $j(E) \in \mathbb{Q}$.

Theorem (C-Pollack 17)

For all $\epsilon > 0$, we have $T_{\mathbb{Q}}(d) = O_{\epsilon}(d^{5/2+\epsilon})$.

This result **suggests** (maybe) that $T(d)$ should grow at most **polynomially** in d. This is wide open.

What about lower bounds on $T(d)$?

Theorem (Breuer 2010)

We have $\limsup_d \frac{T(d)}{d \log \log d} > 0$.

We do not know whether $\limsup_d \frac{T(d)}{d \log \log d}$ is finite: i.e., it may be that $T(d)$ is **never** larger than a constant times $d \log \log d$.

Introducing CM

There are two kinds of elliptic curves $E_{/F}$, CM and not-CM. This depends only on $E_{/\mathbb{C}}$ (n'importe quelle $\iota : F \hookrightarrow \mathbb{C}$).

$$E(\mathbb{C}) \cong_{\mathbb{C}-\text{Lie group}} \mathbb{C}/\Lambda,$$

with Λ a full lattice in $\mathbb{C}$. Then

$$\mathrm{End}(E) = [\Lambda : \Lambda] := \{z \in \mathbb{C} \mid z\Lambda \subset \Lambda\}.$$

So $\mathbb{Z} \subset \mathrm{End}(E)$. Usually equality holds: not CM. Otherwise $\mathrm{End}(E) = \mathcal{O}$ is an order in an imaginary quadratic field K: CM.

(Since $[\mathcal{O} : \mathcal{O}] = \mathcal{O}$, every imaginary quadratic order $\mathcal{O}$ arises.)

Reorientation towards the CM case

Now we introduce

$T_{\mathrm{CM}}(d) :=$ like $T(d)$ but restricted to $E_{/F}$ *with* CM
$T_{\neg \mathrm{CM}}(d) :=$ like $T(d)$ but restricted to $E_{/F}$ *without* CM.

Clearly $T(d) = \max\left(T_{\mathrm{CM}}(d), T_{\neg \mathrm{CM}}(d)\right)$. Which is it??

$T_{\mathrm{CM}}(1) = 6 < 16 = T_{\neg \mathrm{CM}}(1)$
$T_{\mathrm{CM}}(2) = 12 < 24 = T_{\neg \mathrm{CM}}(2)$
$T_{\mathrm{CM}}(3) = 14 < 28 = T_{\neg \mathrm{CM}}(3)$

Not exactly definitive!

Philosophy of the CM case

• The CM case is (apparently or provably) **extremal** in some ways and **exceptional** in others. If you are in interested in the general case, you may need to **sieve out** the CM case to study it properly.

Theorem (C-Genao-Pollack-Saia 2020)

All but finitely many of the modular curves $X_0(N)$, $X_1(N)$, $X_1(M,N)$ have sporadic CM points.

Upper order of $T_{\mathrm{CM}}(d)$

Theorem (C-Pollack 2016)

$$\limsup_{d} \frac{T_{\mathrm{CM}}(d)}{d \log \log d} = \frac{e^{\gamma}\pi}{\sqrt{3}}.$$

So the "upper order" of $T_{\mathrm{CM}}(d)$ is $d \log \log d$.

Comparing Upper and Lower Orders

Theorem (Better Breuer 2010)

$$\limsup_d \frac{T_{\mathrm{CM}}(d)}{d \log \log d} > 0, \ \limsup_d \frac{T_{\neg \mathrm{CM}}(d)}{\sqrt{d \log \log d}} > 0.$$

Whether the latter lim sup is finite is **wide open**: if so, then for infinitely many d we have $T(d) = T_{\mathrm{CM}}(d) > T_{\neg \mathrm{CM}}(d)$.

The lower order works a bit differently: can show that

$$\liminf_d \frac{T_{\neg \mathrm{CM}}(d)}{\sqrt{d}} > 0$$

and combining with Bourdon-C-Pollack 2017, it follows that

$$\{d \in \mathbb{Z}^+ \mid T(d) = T_{\neg \mathrm{CM}}(d) > T_{\mathrm{CM}}(d)\}$$

has density 1 in $\mathbb{Z}^+$.

Computing $\mathcal{T}_{\mathrm{CM}}(d)$ for all d

Next up: want to compute $\mathcal{T}_{\mathrm{CM}}(d)$ for any given d. This is now *almost* solved. It is essentially the same problem as computing degrees of Δ-CM points on $X_1(M,N)$, the modular curve that (roughly) parameterizes $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \hookrightarrow E(F)[\text{tors}]$.

An imaginary quadratic order $\mathcal{O}$ is uniquely determined by its **discriminant** $\Delta = [\mathcal{O}_K : \mathcal{O}]^2 \Delta_K$, which can be any negative integer that is 0 or 1 modulo 4.

Let $P_\Delta(t) \in \mathbb{Z}[t]$ the **Hilbert class polynomial**: the monic poly whose roots in $\mathbb{C}$ are j-invariants of Δ-CM elliptic curves. This is irreducible over $\mathbb{Q}$ (and over K) of degree

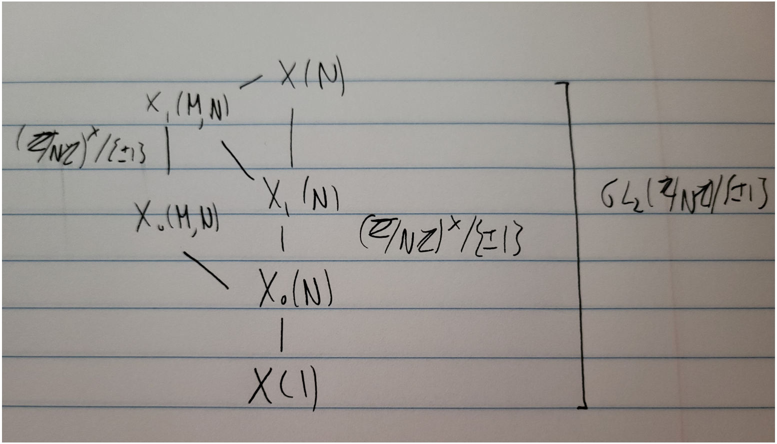
$$h_\Delta := \# \operatorname{Pic} \mathcal{O}.$$

Arithmetic Geometry Ensues

Since $Y(1)_{/\mathbb{Q}} = \mathbb{A}^1_{/\mathbb{Q}}$,

$$P_\Delta \in \mathbb{Q}[t] \leftrightarrow J_\Delta \in Y(1) \subset X(1),$$

a closed point of degree h_Δ. Have towers of modular curves



The Splitting Problem

Q: How does J_{Δ} split in $X_0(N)$, $X_1(N)$ and so forth? This is (literally!) the ANT1 problem of how prime ideals split in extensions of Dedekind domains. We want to know:
(i) ramification "e_i's",
(ii) number of places "g",
(iii) degree of each place "f_i's",
(iv) residue field $\mathbb{Q}(P)$ of the place P.

All of these maps ramify only over $j = 0, 1728, \infty$.
$j = 0 \leftrightarrow \Delta = -3$, $j = 1728 \leftrightarrow \Delta = -4$; exclude them.

The $X(N)$ Case

Theorem (Bourdon-C 2020)

Let $P \in X(N)$ lie over $J_\Delta \in X(1)$.

a) *Suppose $N \geq 3$ or Δ is odd. Then*

$$\mathbb{Q}(P) = K(J_{N^2\Delta})K^{(N)},$$

so $\mathbb{Q}(P) \supset K$. Also $[\mathbb{Q}(P):\mathbb{Q}] = 2h_\Delta \#(\mathcal{O}/N\mathcal{O})^\times$.

b) *If $N = 2$ and $\Delta < -4$ is even, then $\mathbb{Q}(P) \cong \mathbb{Q}(J_{4\Delta})$, so $\mathbb{Q}(P)$ does not contain K.*

So the answer to the splitting problem in the (easiest!) case of $X(N)$ is a generalization of the **First Main Theorem of CM**.

Invisible Volcanoes

In recent work on **isogeny volcanoes** I've solved the splitting problem for $X_0(N)$ and $X_0(2, 2N)$ when $\Delta_K \neq -3, -4$.

Every field $\mathbb{Q}(P)$ for $P \in X_0(N)$ or $X_0(2, 2N)$ lying over J_Δ is of the form $\mathbb{Q}(J_{n^2\Delta})$ or $K(J_{n^2\Delta})$ for some $n \mid N$.

The same methods can treat $X_0(M, N)$ in any case of interest. But the answers get intricate: complete information for $X_0(p^a)$ is recorded in **95 tables**.

For $M \geq 3$, prior work of Bourdon-Clark applies to give slightly less precise results...these are sufficient to compute $\mathcal{T}_{\mathrm{CM}}(d)$.

From $X_0(M, N)$ to $X_1(M, N)$

Classifying rational points on $X_0(N)$ is much harder than classifying rational points on $X_1(N)$. "Isogeny Mordell" is wide open.

In this respect the CM case is like Bizarroworld:

Theorem (C-, building on Bourdon-C 2020)

Let $\Delta < -4$. Then $\pi : X_1(M, N) \rightarrow X_0(M, N)$ is inert over every Δ-CM point $P \in X_0(M, N)$.

Thus on $X_0(M, N)$ we can determine the number of Δ-CM points and their residue *fields*, which yields on $X_1(M, N)$ the number of Δ-CM points and their *degrees*, which is enough to compute $\mathcal{T}_{\mathrm{CM}}(d)$.

What Remains To be Done

I. Solve splitting problem for $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-3})$-CM points.
II. Actually apply this work to compute $\mathcal{T}_{\mathrm{CM}}(d)$ for various d's.
III. Find **infinite** families of d on which $\mathcal{T}_{\mathrm{CM}}(d)$ can be computed uniformly. Examples of uniformity:

Theorem (Bourdon-C-Stankewicz 2017)

For all **primes** $p \geq 7$*, we have* $\mathcal{T}_{\mathrm{CM}}(p) =$

$$\mathcal{T}_{\mathrm{CM}}(1) = \{\bullet,\ \mathbb{Z}/2\mathbb{Z},\ \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\}.$$

Theorem (Bourdon-Pollack 2017)

Determination of $\mathcal{T}_{\mathrm{CM}}(d)$ *for all* **odd** d*.*

Theorem (Chaos 2020 Masters Thesis)

Determines $\mathcal{T}_{\mathrm{CM}}(2p)$ *for all odd primes* p*. Depends on whether* $2p+1$, $4p+1$, $6p+1$ *are prime.*