Torsion points on elliptic curves over number fields of small degree.

An application of sage in number theoretic research.

Maarten Derickx

Mathematisch Instituut
Universiteit Leiden

Sage Flint Days (sd35)

Outline

Mazurs Torsion Theorem

Theorem

If $E/\mathbb{Q}$ is an elliptic curve then $E(\mathbb{Q})_{tors}$ is isomorphic to one of the following groups:

- $\mathbb{Z}/n\mathbb{Z}$ *for* $1 \leq n \leq 10$ *or* $n = 12$
- $\mathbb{Z}/2n\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ *for* $1 \leq n \leq 4$

Question Does a similar finite list also exist for other numberfields.
Answer Yes, in fact something much stronger is true.

Uniform Boundednes Conjecture

Definition

A group G is an elliptic torsion group of degree d if $G \cong E(K)_{tors}$ for some elliptic curve E/K with $\mathbb{Q} \overset{\leq d}{\subseteq} K$. $\phi(d)$ is the set of all isomorphism classes of such groups.

Theorem (Uniform Boundednes Conjecture)

$\phi(d)$ is finite.

Definition

A prime p is a torsion prime of degree d if $p | \# E(K)_{tors}$ for some elliptic curve E/K with $\mathbb{Q} \overset{\leq d}{\subseteq} K$. $S(d)$ is the set of all torsion primes of degree d.

What is known

Definition

$Primes(n) := \{p \text{ prime} \mid p \leq n\}$

- $\phi(d)$ is finite $\Leftrightarrow$ $S(d)$ is finite (Kamienny, Mazur)
- $S(d)$ is finite (Merel)
- $S(d) \subseteq Primes((3^{d/2} + 1)^2)$ (Oesterlé)
- $S(1) = Primes(7)$ (Mazur)
- $S(2) = Primes(13)$ (Kamienny,Kenku,Momose)
- $S(3) = Primes(13)$ (Parent)
- $S(4) = Primes(17)$ (Kamienny, Stein, Stoll)
- $S(5) = Primes(19)$ (Stein, Stoll, me)

Reduce to Multiplicative Reduction

Let $\mathbb{Q} \overset{d}{\subset} K$ be a field extension, E/K an elliptic curve, l a prime $m \subseteq O_K$ a max. ideal lying over l with res. field $\mathbb{F}_q$,$P \in E(K)$ of order p and $\widetilde{E}$ the fiber over $\mathbb{F}_q$ of the Néron model . If $p \nmid q$ then $\widetilde{P} \in \widetilde{E}(\mathbb{F}_q)$ has order p.

- **Good reduction:** $p \leq \# \widetilde{E}(\mathbb{F}_q) \leq (q^{\frac{1}{2}} + 1)^2 \leq (l^{d/2} + 1)^2$
- **Additive reduction:** $0 \to G_{a,\mathbb{F}_q} \to \widetilde{E} \to \Phi \to 0$ hence $p \mid \#\Phi(F_q) \leq 4 < (l^{d/2} + 1)^2$
- **Multiplicative reduction:** $0 \to T \to \widetilde{E} \to \Phi \to 0$ with $T = G_{m,\mathbb{F}_q}$ or $T = \widetilde{G}_{m,\mathbb{F}_q}$. Hence $p \mid q - 1$, $p \mid q + 1$ or $p \mid \#\Phi(F_q)$

Conclusion: $(l^{d/2} + 1)^2$ is a bound for the torsion order in the good and the additive case.

What happens in the multiplicative case

Let $x \in X_0(p)(O_K)$ and $\sigma_1, \ldots, \sigma_d$ be all embeddings of K in $\mathbb{C}$. Then $x^{(d)} := [(\sigma_1(x), \ldots, \sigma_d(x))] \in X_0(p)^{(d)}(\mathbb{Z})$.
In the rest of this talk:

- E has mult. red. at all primes over l and $\tilde{P}$ has nonzero image in Φ (i.e. P reduces to the singular point)
- $s' = (E, \langle P \rangle) \in X_0(p)(K)$
- $s = w_p(s')$ (doesn't work for $X_1(p)(K)$, but there is a workaround)

So we have:

- $s'^{(d)}_{\mathbb{F}_l} = 0^{(d)}_{\mathbb{F}_l}$
- $s^{(d)}_{\mathbb{F}_l} = \infty^{(d)}_{\mathbb{F}_l}$ (because $w_p(0) = \infty$)

Hence we study $s \neq \infty \in X_0(p)(O_K)$ such that $s^{(d)}_{\mathbb{F}_l} = \infty^{(d)}_{\mathbb{F}_l}$. (and try to prove that no such s exist for certain p).

Mazur's approach

Derive a contradiction with formal immersions in the multiplicative case

A morphism $f : X \to Y$ of noetherian schemes is a formal immersion at $x \in X$ if $\widehat{f} : \widehat{O_{Y,f(x)}} \to \widehat{O_{X,x}}$ is surjective. Or equivalently $k(x) = k(f(x))$ and $f^* : \mathrm{Cot}_{f(x)} Y \to Cot_x X$ is surjective.

Lemma (Mazur)

Let A be the Néron model over $\mathbb{Z}_{(l)}$ of an abelian variety over $\mathbb{Q}$. Suppose there is a morphism $f : X_0(p)^{(d)} \to A$ normalized by $f(\infty^{(d)}) = 0$. If $s \neq \infty \in X_0(p)$, $s^{(d)}_{\mathbb{F}_l} = \infty^{(d)}_{\mathbb{F}_l}$ and

$$f(s^{(d)}) = 0 \qquad \textbf{(H)}$$

then f is not a formal immersion at $\infty^{(d)}_{\mathbb{F}_l}$

If im f is torsion and doesn't contain $\mu_{2,\mathbb{Z}_{(l)}}$ immersions if $l = 2$ then we can use the following to satisfy **H** (i.e. $f(s^{(d)}) = 0$)

Lemma

Let A be a $\mathbb{Z}_{(l)}$ group scheme with identity e. If also $P \in A(\mathbb{Z}_{(l)})$ torsion s.t. $P_{\mathbb{F}_l} = e_{\mathbb{F}_l}$. And $l = 2$ then P does not generate a $\mu_{2,\mathbb{Z}_{(l)}}$ immersion then $P = e$.

This is enough since $\infty_{\mathbb{F}_l}^{(d)} = s_{\mathbb{F}_l}^{(d)}$ implies $0_{\mathbb{F}_l} = f(\infty^{(d)})_{\mathbb{F}_l} = f(s^{(d)})_{\mathbb{F}_l} \in A_{\mathbb{F}_l}$.

How to construct an f satisfying **H**

There are several ways to garantee im f is torsion and doesn't contain $\mu_{2,\mathbb{Z}_{(l)}}$ immersions if $l = 2$

- Mazur, Kammienny and Oesterle all take $l \neq 2$ and f a composition $X_0^{(d)} \to J_0(p) \to A$ where A is a rank zero quotient of $J_0(p)$.
- Parent takes $l = 2$, $A = J_1(p)$ and $f = t_1 \circ t_2 \circ g$ where $g : X_1^{(d)}(p) \to J_1(p)$, t_1 kills the free part and t_2 all the 2 torsion.
- I do the same as Parent but with $A = J_0(p)$ and $g : X_1^{(d)}(p) \to J_0(p)$.

How to construct t_1 and t_2

We can take t_1 a hecke operator such that $t_1 : J_0(p)(\mathbb{Q}) \to J_0(p)(\mathbb{Q})$ factors trough a rank zero quotient of $J_0(p)$ (for example the eisenstein or the winding quotient). There is an algorithm for finding such t_1.

Proposition

If $q \neq p$ prime. Then $T_q - q - 1$ kills all the $\mathbb{Q}$-rational torsion of $J_0(p)$ of order co prime to pq.

Hence we can take $t_2 = T_q - q - 1$ with $p \neq q \neq 2$.

Putting it all together

Proposition

Let $p > (2^{d/2} + 1)^2$ be prime, t_1 and t_2 be as above and $g : X_0^{(d)}(p) \to J_0(p)$ the cannonical map normalized by $g(\infty^{(d)}) = 0$. And suppose that $f = t_1 \circ t_2 \circ g : X_1^{(d)}(p) \to J_0(p)$ is a formal immersion at $\infty_{\mathbb{F}_l}^{(d)}$ then $p \notin S(d)$.

So we reduced the problem of showing $p \notin S(d)$ to showing $g^* : \mathrm{Cot}_{0_{\mathbb{F}_l}} J_0(p) \to Cot_{\infty_{\mathbb{F}_l}^{(d)}} X_0^{(d)}(p)$ is surjective. But this is linear algebra and Sage is good at this!

Kamienny's criterion

Parent's version translated to $X_0(p)$

Theorem

Let $l \neq p$ be a prime and $g : X_0(p)^{(d)} \to J_0(p)$ be the canonical map normalized by $f(\infty^{(d)}) = 0$ and $t \in \mathbb{T}$ then $t \circ f$ is a formal immersion at $\infty_{\mathbb{F}_l}^{(d)}$ if and only if $\overline{T_1 t}, \ldots, \overline{T_d t}$ are $\mathbb{F}_l$ linearly independent in $\mathbb{T}/(l\mathbb{T})$.

Corollary

Take $l = 2$ prime, if the independence holds for $p > (2^{d/2} + 1)^2$ and $t = t_1 \cdot t_2$ with t_1, t_2 as defined previously then $p \notin S(d)$.

Some notation to formulate Kamienny for $X_1(p)$

This is why I explained everything for $X_0(p)$ first

Let $\pi : X_1(p) \to X_0(p)$ the canonical map. And $S := \pi^{(-1)}(\infty)$ then as in the $X_0(p)$ case the $s' \in X_1(p)(K)$ which reduce multiplicative give rise to an s s.t. $\pi(s_{\mathbb{F}_q}) = \infty_{\mathbb{F}_q}$ for all char l residue fields.
Now take $\sigma_i \in S$ and $n_i \in \mathbb{N}$ s.t.

- $s^{(d)}_{\mathbb{F}_l} = \sum_{i=0}^m n_i \sigma_{i,\mathbb{F}_l}$
- σ_i pairwise distinct
- $n_m \geq n_{m-1} \geq \ldots \geq n_0 \geq 1$
- $\sum n_i = d$.

Write $\sigma = \sum_{i=0}^m n_i \sigma_i$ and $\sigma_0 = \langle d \rangle_j \sigma_j$ (ok since $\langle d \rangle$ act transitively on S).

Kamienny's Criterion
Parent's original version

Theorem

Let $l \neq p$ be a prime and $f_\sigma : X_1(p)^{(d)} \to J_q(p)$ be the canonical map normalized by $f(\sigma) = 0$ and $t \in \mathbb{T}$ then $t \circ f$ is a formal immersion at $\sigma_{\mathbb{F}_l}$ if and only if

$$\overline{T_1\langle d_0\rangle t}, \overline{T_2\langle d_0\rangle t}, \ldots, \overline{T_{n_0}\langle d_0\rangle t}, \overline{T_1\langle d_1\rangle t}, \ldots, \overline{T_{n_1}\langle d_1\rangle t}, \ldots,$$

$$\overline{T_1\langle d_m\rangle t}, \ldots, \overline{T_{n_m}\langle d_m\rangle t}$$

are $\mathbb{F}_l$ linearly independent in $\mathbb{T}/(l\mathbb{T})$.

Kamienny's Criterion

Parent's original version

Corollary

Take $l = 2$ and $p > (2^{d/2} + 1)^2$ prime. Take $t = t_1 \cdot t_2$ with t_1 suppose that for all partitions $\sum_{i=0}^{m} n_i = d$ and all $1 < d_1, \ldots, d_m \leq \frac{p-1}{2}$ pairwise distinct that

$$\overline{T_1\langle 1\rangle t}, \ldots, \overline{T_{n_0}\langle 1\rangle t}, \overline{T_1\langle d_1\rangle t}, \ldots, \overline{T_{n_1}\langle d_1\rangle t}, \ldots,$$

$$\overline{T_1\langle d_m\rangle t}, \ldots, \overline{T_{n_m}\langle d_m\rangle t}$$

are linearly independent then $p \notin S(d)$.

Comparison

Criterion for $X_1(p)$ is more powerful but is expensive to verify

- Advantage $X_1(p)$ over $X_0(p)$: Higher chance on success
- Disadvantage $X_1(p)$ over $X_0(p)$: Way slower
    1. hecke matrices of size $(p-5)(p-7)/24$ vs. $\frac{p}{12}$
    2. partition $d = 1 + \ldots + 1$ already gives $\binom{(p-3)/2}{d-1}$ dependency's to check instead of 1.

Luckily 2 can be worked around since t.f.a.e:

- $\langle 1 \rangle t, \langle d_1 \rangle t, \ldots \langle d_d \rangle t$ are linearly independent for all $1 < d_1, \ldots, d_m \leq \frac{p-1}{2}$ pairwise distinct.
- The smallest dependency in $\langle 1 \rangle t, \langle 2 \rangle t, \ldots \langle \frac{p-1}{2} \rangle t$ is of weight $> d$

Similar things can be done for other partitions.

Result of testing the criterion

d	5	6	7
$(2^{d/2}+1)^2$	$44.3\ldots$	81	$151.6\ldots$
$(3^{d/2}+1)^2$	$275.1\ldots$	784	$2281.5\ldots$

$p = 271$ using $X_1(p)$ in sage takes about 12h and 21GB.
I used $X_0(p)$ to show $S(d) \subseteq Primes(193)$ for $d = 5, 6, 7$
After that I used $X_1(p)$ to show $S(d) \subseteq Primes((2^{d/2}+1)^2)$
The criterion is also satisfied for a lot $p < (2^{d/2}+1)^2$ so in these cases we only need to rule out good reduction.

Elliptic curves over $\mathbb{F}_{2^d}$

Let $E/\mathbb{F}_{2^d}$ be an elliptic curve. Consider the two cases:

1. $j(E) \neq 0$ then it can be shown that E has a point of order 2
2. $j(E) = 0$ Then E is a twist of $y^2 + y = x^3$.

In case (1): $\frac{1}{2}(2^{d/2} + 1)^2$ bounds the torsion of prime order.
In case (2) there are only very few curves, and the number of their rational points are well known.
This gives:

d	$S(d)$	$(2^{d/2} + 1)^2$
5	$Primes(19) \cup \{29, 31, 41\}$	$44.3\ldots$
6	$Primes(41) \cup \{73\}$	$81.0\ldots$
7	$Primes(73) \cup \{113, 127\}$	$151.6\ldots$

Overview

There is already a lot of literature on the subject. The idea of the proof is often the same, details are different.

- Mazur gave initial strategy (using $X_0(p)$).
- Kamienny showed how to apply it to numberfields.
- Merel managed to do it for all number fields
- Oesterle improved on Merel's upperbound, (needs $l \neq 2$).
- Parent used $X_1(p)$ to get better bounds for $d = 3$
- Parent gave workarounds for $l = 2$ (and aplied it to $d = 3$)
- William Stein applied Parents work to $d = 4$.
- I translated parents workarounds back to $X_0(p)$ again for faster computations and applied it to $d = 5, 6, 7$
- Michael Stoll has an entirely different strategy, to help William and me with remaining cases.

Summary

- The existence of torsion points on Elliptic curves can be studied by looking what happens at reduction.
- Use Kamienny's criterion to control multiplicative reduction. Hasse's bound and a more precise study for good reduction. Additive reduction is never a problem.
- $S(5) = \mathit{Primes}(19)$ (was $\subseteq \mathit{Primes}(271)$)
  $S(6) \subseteq \mathit{Primes}(41) \cup \{73\}$ (was $\subseteq \mathit{Primes}(773)$)
  $S(7) \subseteq \mathit{Primes}(73) \cup \{113, 127\}$ (was $\subseteq \mathit{Primes}(2281)$)
- Possible future work:
  - Construct elliptic curves for $d = 6, 7$
  - Think of more strategies to rule out primes for $d = 6, 7$
  - Use Johns faster modular symbols code for $d = 8, 9, 10, \ldots$
  - Improve function fields in Sage so Micheal Stolls part doesn't need Magma.