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

Several variations of kamienny's criterion

Maarten Derickx

Mathematisch Instituut
Universiteit Leiden

UW Number Theory Seminar
18-03-2011

Outline

What is known

$$S(d) = \left\{ p \text{ prime} \mid \exists K \overset{d}{\supseteq} \mathbb{Q}\, \exists E/K : E(K)[p] \neq 0 \right\}$$

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

- $S(d)$ 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) to be published.

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. Consider the three cases:

- **Good reduction:** $p \leq \# \widetilde{E}(\mathbb{F}_q) \leq (q^{\frac{1}{2}} + 1)^2 \leq (l^{d/2} + 1)^2$
- **Additive reduction:** $0 \rightarrow G_{a,\mathbb{F}_q} \rightarrow \widetilde{E} \rightarrow \Phi \rightarrow 0$ hence $p \mid \#\Phi(F_q) \leq 4 < (l^{d/2} + 1)^2$
- **Multiplicative reduction:** $0 \rightarrow T \rightarrow \widetilde{E} \rightarrow \Phi \rightarrow 0$ 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 $x \in X_0(p)$ and $\sigma_1, \ldots, \sigma_d$ be all embeddings of K in $\mathbb{C}$. Then $x^{(d)} := [(\sigma_1(x), \ldots, \sigma_d(x))] \in X_0(p)^{(d)}(\mathbb{Q})$.
If $s' = (E, \langle P \rangle) \in X_0(p)(K)$ and E has multiplicative reduction at all primes over l and $\widetilde{P}$ has nonzero image in Φ then all specializations of s' to characteristic l are the cusp 0. Define $s = (E/\langle P \rangle, E[p]/\langle P \rangle)$ then all specializations of s to characteristic p are ∞. This proves:

Proposition

If $p \nmid l^k + 1$, $p \nmid l^k - 1$ for all $k \leq d$ then $s^{(d)}_{\mathbb{F}_l} = \infty^{(d)}_{\mathbb{F}_l}$.

In the rest of the talk we study $s \neq \infty \in X_0(p)$ 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 $A(\mathbb{Q})$ has rank 0, use the following lemma to satisfy **H**

Lemma

If $l > 2$ prime and A a $\mathbb{Z}_{(l)}$ group scheme with identity e. If also $P \in A$ is a $\mathbb{Z}_{(l)}$ valued torsion s.t. $P_{\mathbb{F}_l} = e_{\mathbb{F}_l}$ then $P = e$.

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

Winding quotient

The "largest" rank 0 quotient of $J_0(p)$

Definition (winding element)

The winding element $e \in H_1(X_0(p)(\mathbb{C}), \mathbb{Q})$ is the one corresponding to $\omega \mapsto \int_0^{i\infty} \omega \in H^0(X_0(p), \Omega)^\vee$

Definition (winding quotient)

Let $A_e \subseteq \mathbb{T}$ be the annihilator of e then $J_e(p) = J_0(p)/A_e J_0(p)$ is called the winding quotient.

This definition can also be made over $X_1(p)$, in both cases $J_e(\mathbb{Q})$ has rank zero as a result of Kato's theorem.

Kamienny's Criterion

The original case: $X_0(p)$ and $l \neq 2, p$

Theorem (Kamienny)

Let $l \neq 2, p$ be a prime and $f : X_0(p)^{(d)} \to J_e(p)$ be the canonical map normalized by $f(\infty^{(d)}) = 0$ then f is a formal immersion at $\infty_{\mathbb{F}_l}^{(d)}$ if and only if $\overline{T_1}, \ldots, \overline{T_d}$ are $\mathbb{F}_l$ linearly independent in $\mathbb{T}/(l\mathbb{T} + A_e)$.

Corollary

If $p > (l^{d/2} + 1)^2$ and $\overline{T_1}, \ldots, \overline{T_d}$ are $\mathbb{F}_l$ linearly independent in $\mathbb{T}/(l\mathbb{T} + A_e)$. Then $p \notin S(d)$.

What goes wrong at 2

Point orders don't always stay the same under reduction

Need again a lemma to satisfy (1)

Lemma

If $l = 2$ and A a $\mathbb{Z}_{(l)}$ group scheme with identity e. If also $P \in A$ is a $\mathbb{Z}_{(l)}$ valued torsion s.t. $P_{\mathbb{F}_l} = e_{\mathbb{F}_l}$ then $P = e$ or P generates a $\mu_{2,\mathbb{Z}_{(l)}}$ immersion.

So we need to kill all the 2 torsion:

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.

What goes wrong at 2

Kamienny's criterion doesn't work.

The criterion is proved by calculating when the composition

$$\operatorname{Cot}_0 J_e(p)_{\mathbb{F}_l} \to \operatorname{Cot}_0 J_0(p)_{\mathbb{F}_l} \to \operatorname{Cot}_{\infty_{\mathbb{F}_l}^{(d)}} X_0(p)_{\mathbb{F}_l}^{(d)}$$

is surjective and then translate this to the dual condition in $\operatorname{Tan} J_e(p)_{\mathbb{F}_l} \cong \mathbb{T}/(l\mathbb{T} + A_e)$. The problems at $l = 2$ arise in proving the isomorphism:

$$\operatorname{Cot} J_e(p)_{\mathbb{Z}_{(l)}} \cong \operatorname{Cot} J_0(p)_{\mathbb{Z}_{(l)}} [A_e] \subseteq \operatorname{Cot} J_0(p)_{\mathbb{Z}_{(l)}} \cong S_2(\Gamma_0(p), \mathbb{Z}_{(l)})$$

Approach by Parent: Instead of looking at $f : X_0(p)^{(d)} \to J_e(p)$ construct an $f : X_0(p)^{(d)} \to J_0(p)$ which factors through $J_e(p)$.

Kamienny's criterion

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

Theorem

Let $l \neq p$ be a prime and $f : X_0(p)^{(d)} \to J_0(p)$ 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 $l = 2$ and $q > 2$ prime, if the independence holds for $p > (2^{d/2} + 1)^2$ and $t = a_q \cdot t_1$ with $t_1 \in A_e^{\perp}$ then $p \notin S(d)$.

Proof of the corollary

Proof.

Need to show that for $s \in X_0(p)(K)$ with multiplicative reduction at 2 that $t \circ f(s^{(d)}) = 0$. Now $t_1 \circ f$ factors through $J_e(p)$ since $t_1 \in A_e^{\perp}$ hence $t_1 \circ f(s^{(d)})$ is torsion. $s_{\mathbb{F}_2}^{(d)} = \infty_{\mathbb{F}_2}^{(d)}$ so $t_1 \circ f(s^{(d)})$ is 2 torsion hence killed by a_q. □

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 $s' \in X_1(p)(K)$ which reduce multiplicative give rise to an s s.t. $s_{\mathbb{F}_q} = \infty_{s,\mathbb{F}_q}$.
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
- $n_m \geq n_{m-1} \geq \ldots \geq n_0 \geq 1$
- $\sum n_i = d$.

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

Kamienny's Criterion
Parent's original version

Theorem

Let $l \neq p$ be a prime and $f_\sigma : X_1(p)^{(d)} \to J_0(p)$ 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 $\mathbb{T}/(l\mathbb{T})$.

Corollary

Take $l = 2$ and $q > 2$, $p > (2^{d/2} + 1)^2$ both prime. Take $t = a_q \cdot t_1$ with $t_1 \in A_e^\perp$, 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^2 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 some $p < (2^{d/2}+1)^2$ 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 j is a twist of $y^2 + y = x^3$.

In case (1) we see that $\frac{1}{2}(2^{d/2} + 1)^2$ bounds the torsion of prime order.
In case (2) count points on $y^2 + y = x^3$ over an extension of $\mathbb{F}_{2^d}$ for which all twists are isomorphic.
This approach is still work in progress, I already ruled out $p = 23, 37, 43$ for $d = 5$ and $p > 37$ except $p = 71$ for $d = 6$.

Summary

- The existence of torsion points on can be studied by looking what happens at reduction.
- Use kamienny's criterion to control multiplicative reduction. Hasse's bound and other smart things for good reduction. Additive reduction is never a problem.
- $S(5) \subseteq Primes(19) \cup \{29, 31, 41\}$ v.s. $Primes(271)$
  $S(6) \subseteq Primes(41) \cup \{71\}$ v.s. $Primes(773)$
  $S(7) \subseteq Primes(151)$ v.s. $Primes(2281)$
- Possible future work:
  - Construct elliptic curves for $d = 5, 6, 7$
  - Do more smart things for $p < (l^{d/2} + 1)^2$ for $d = 5, 6, 7$
  - Use the computer to test $d = 8, 9, 10, \ldots$
  - Look if Oesterlé's proof can be translated to $l = 2$.