Prime Torsion Order on Elliptic Curves Over Number Fields of Small Degree

Michael Stoll

Universität Bayreuth

joint with Maarten Derickx, Sheldon Kamienny, William Stein

Oberseminar Arithmetic Geometry

November 19, 2020

The Problem

If E is an elliptic curve over a number field K,
then $E(K)$ is a finitely generated abelian group;
in particular, the torsion subgroup $E(K)_{\text{tors}}$ is finite.

Question.
Which (finite abelian) groups occur as $E(K)_{\text{tors}}$ for fields K of degree d?

A weaker version of this question is the following.

Question.
Which primes p can divide $\#E(K)_{\text{tors}}$ for fields K of degree d?

We write $S(d)$ for the set of these primes.

What is Known?

Mazur has shown that $E(\mathbb{Q})$ is isomorphic to one of the following groups:

$$\{0\},\ \mathbb{Z}/2\mathbb{Z},\ \mathbb{Z}/3\mathbb{Z},\ \ldots,\ \mathbb{Z}/9\mathbb{Z},\ \mathbb{Z}/10\mathbb{Z},\ \mathbb{Z}/12\mathbb{Z},$$
$$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z},\ \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z},\ \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z},\ \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z};$$

in particular, $\quad S(1)=\{2,3,5,7\}.$

Kamienny determined $\quad S(2)=\{2,3,5,7,11,13\},$
and Kenku and Momose had found all possible group structures for $d=2$ assuming this value of $S(2)$.

Parent showed $\quad S(3)=\{2,3,5,7,11,13\}$
(and the group structures have recently been determined).

Merel showed that $S(d)$ is finite for all d,
and **Oesterlé** gave the bound

$$p\in S(d) \quad\Longrightarrow\quad p\le\left(3^{d/2}+1\right)^2.$$

The Goal

We determine

$$S(4) = \{2, 3, 5, 7, 11, 13, 17\}$$
$$S(5) = \{2, 3, 5, 7, 11, 13, 17, 19\}$$
$$S(6) = \{2, 3, 5, 7, 11, 13, 17, 19, 37\}$$

and also give some results on $S(7)$.

The inclusions "$\supset$" are known,
so it suffices to show "$\subset$" in each case.

Relation With Rational Points

If $p \in S(d)$, then there is a number field K of degree d, an elliptic curve E over K and a point $P \in E(K)$ of order p.

To the pair (E, P) there corresponds a point $x \in X_1(p)(K)$ that is not a cusp.

Then $\mathrm{Tr}_{K/\mathbb{Q}}(x)$ is a $\mathbb{Q}$-rational effective divisor of degree d on $X_1(p)$. Such divisors correspond to points on the dth symmetric power $X_1(p)^{(d)}$.

So we obtain a rational point on $X_1(p)^{(d)}$ that is not in the image of the map $\mathrm{cusps}^d \to X_1(p)^{(d)}$.

Conclusion.

If all rational points on $X_1(p)^{(d)}$ are supported in cusps, then $p \notin S(d)$.

General Strategy

We fix a prime $\ell \neq p$; then $X_1(p)$ and its Jacobian have good reduction at ℓ.

If we can show the following two claims, then $p \notin S(d)$.

Let $x \in X_1(p)^{(d)}(\mathbb{F}_\ell)$.

The residue class of x is the set of points in $X_1(p)^{(d)}(\mathbb{Q})$ reducing to x.

❶ If x is a sum of cusps, then its residue class has exactly one element.

❷ Otherwise, the residue class of x is empty.

In case ❶, there is a rational point in the residue class: a sum of cusps.

We verify ❶ by exhibiting a morphism $t\colon X_1(p)^{(d)} \to A$
with an abelian variety A such that t is injective on the residue class of x
and $A(\mathbb{Q}) \to A(\mathbb{F}_\ell)$ is injective.

We have to show ❶ and ❷ for all primes $p \leq (3^{d/2}+1)^2$ that are not in $S(d)$.

Primes We Have To Deal With

We have to show ❶ and ❷ for all primes $p \le (3^{d/2}+1)^2$ that are not in $S(d)$.

$d = 4$:	19, 23, 29, 31, 37, 41, 43, …, 97
$d = 5$:	23, 29, 31, 37, 41, 43, ……, 271
$d = 6$:	23, 29, 31, 41, 43, ………, 773

We work with $\ell = 2$. Then ❷ is automatic when $p > (2^{d/2}+1)^2$,
or when $p \nmid 2^{d'} \pm 1$ and there are no E over $\mathbb{F}_{2^{d'}}$ with $p \mid \#E(\mathbb{F}_{2^{d'}})$ for $d' \le d$.
This leaves for ❷:

$d = 4$:	(none)
$d = 5$:	31, 41
$d = 6$:	29, 31, 41, 73

The primes 19, 23, 29, 31, 41, 47, 59, 71

For all these primes p, $J_1(p)(\mathbb{Q})$ is finite, and $J_1(p)(\mathbb{Q}) \to J_1(p)(\mathbb{F}_2)$ is injective.

This verifies ❶ for these primes, since $X_1(p)^{(d)}$ injects into $J_1(p)$.

In addition, $J_1(p)(\mathbb{Q})$ is generated by differences of rational cusps,
which allows us to verify ❷
by checking that the points x are not reductions of rational points.

This leaves only $(d, p) = (6, 73)$ for ❷. $\rightsquigarrow$ later

For ❶, the following primes remain:

$d = 4$:	37, 43, 53, 61, 67, 73, 79, 83, 89, 97
$d = 5$:	37, 43, 53, 61, 67, 73, 79, 83, 89, 97, ..., 271
$d = 6$:	43, 53, 61, 67, 73, 79, 83, 89, 97, ..., 773

Strategy for ❶

We deal with the remaining pairs (d, p) for ❶ in the following way.

① Find an endomorphism t of $J_1(p)$ (t is a Hecke operator) such that $t\big(J_1(p)(\mathbb{Q})\big)$ is finite and of odd order.
This implies that $t\big(J_1(p)(\mathbb{Q})\big) \to J_1(p)(\mathbb{F}_2)$ is injective.

② Verify that $X_1(p)^{(d)} \xrightarrow{\iota} J_1(p) \xrightarrow{t} J_1(p)$ is a formal immersion at each point $x \in X_1(p)^{(d)}(\mathbb{F}_2)$ supported in cusps.
This implies that $t \circ \iota$ is injective on the residue class of x.

Given any t_0 in the Hecke algebra,
we can construct $t = t_1(t_0)t_2$ satisfying ①.
($t_1(t_0)$ is a projection into the winding quotient,
which has rank 0 by BSD, Kolyvagin-Logachëv, Kato;
t_2 kills the rational torsion if necessary.)

Formal Immersions

There is a criterion due to Kamienny and Parent
that reduces ② to a finite computation in the Hecke algebra $\mathbb{T}$.

Essentially, one has to show that there is no $\mathbb{F}_2$-linear dependence in $\mathbb{T}/2\mathbb{T}$
of a certain form between $\leq d$ elements of a certain explicit set $T(t)$
that depends on t as in ①.
Our Magma code uses functionality for binary linear codes to do that.

We try a number of choices of t_0 and t_2,
compute t and $T(t)$, and check if ② is satisfied.

This is successful for all the pairs (d, p) we had to consider.
So ❶ is done.

❷ for $d = 6$ and $p = 73$

It remains to verify ❷ for $(d, p) = (6, 73)$.

There are four non-cuspidal points $x \in X_1(73)^{(6)}(\mathbb{F}_2)$.
There is an intermediate curve

$$X_1(73) \xrightarrow{4} X_H \xrightarrow{9} X_0(73)$$

such that all four points map to the same point $x_H \in X_H^{(6)}(\mathbb{F}_2)$.
There is a rational point P_H in the residue class of x_H
(coming from an elliptic curve with complex multiplication by $\mathbb{Q}(\sqrt{-3})$).

We find $t \in \mathrm{End}(J_H)$ such that $t(J_H(\mathbb{Q}))$ is finite of odd order
and verify that $t \circ \iota \colon X_H^{(6)} \to J_H$ is a formal immersion at x_H.

It follows that P_H is the only rational point reducing to x_H,
but P_H does not lift to a rational point on $X_1(73)^{(6)}$.

Remarks on $d = 7$

With the methods explained so far, we can show that

$\{2, 3, 5, 7, 11, 13, 17, 19, 23\} \subset S(7) \subset \{2, 3, 5, 7, 11, 13, 17, 19, 23, 37, 59, 61, 67, 71, 73, 113\}$.

The expectation is that the left inclusion is an equality.

The problem is with ❷:
there are non-cuspidal points in $X_1(p)^{(6)}(\mathbb{F}_2)$ that we need to exclude.

Maarten Derickx has a refined method that appears to work for

$$p = 59,\ 61,\ 67,\ 71,\ 73,\ 113\,,$$

and there is some hope that $p = 37$ can be dealt with, too.

Thank You!