Torsion Points on Elliptic Curves over Quartic Number Fields

Michael Stoll
Universität Bayreuth

ANTS IX
INRIA, Nancy
July 22, 2010

Torsion Points on Elliptic Curves

Let K be a number field and E/K an elliptic curve.

It is well-known that the torsion subgroup $E(K)_{\text{tors}}$ of $E(K)$ is finite.

This prompts the following

Questions.

1. Fixing K, is there a universal bound for $\#E(K)_{\text{tors}}$?
2. Is there even such a universal bound if we only fix the degree of K?
3. Can we explicitly determine the possible groups $E(K)_{\text{tors}}$ for given degree $d = [K : \mathbb{Q}]$?

Some Answers (1)

The third question was famously answered by Mazur for the case $d = 1$:

Theorem (Mazur 1978).

The following groups occur as $E(\mathbb{Q})_{\text{tors}}$ for elliptic curves $E/\mathbb{Q}$:

- $\mathbb{Z}/n\mathbb{Z}$ for $n \in \{1, 2, 3, \ldots, 9, 10, 12\}$
- $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$ for $n \in \{1, 2, 3, 4\}$

Each of these groups occurs for infinitely many distinct j-invariants.

Some Answers (2)

The second question was given a positive answer by Merel
(after previous results by Kamienny-Mazur ($d \le 8$)
and Abramovich ($d \le 14$)):

Theorem (Merel 1996).

Fix a positive integer d.
Then the groups $E(K)_{\text{tors}}$, where K is a number field of degree $\le d$
and E/K is an elliptic curve, belong to finitely many isomorphism classes.

The possible groups are known for $d = 2$
(Kenku, Momose, Kamienny, Mazur).

For $d = 3$ and $d = 4$, it is known which groups occur infinitely often
(Jeon, Kim, Schweizer 2004; Jeon, Kim, Park 2006).

The Main Step

The key step in proving a universal bound is to bound the set

$$S(d) = \{p \text{ prime} \mid \exists K, E/K, P \in E(K) : [K : \mathbb{Q}] \le d, \mathrm{ord}(P) = p\}$$

of possible prime orders of K-rational points on elliptic curves.

By results of Frey and Faltings,
finiteness of $S(d)$ implies a universal bound for fields of degree $\le d$.

- $S(1) = \{2, 3, 5, 7\}$
- $S(2) = \{2, 3, 5, 7, 11, 13\}$
- $S(3) = \{2, 3, 5, 7, 11, 13\}$ (Parent 2000, 2003)
- $S(4) = ?$

The Problem

We would like to determine $S(4)$.

From the result of Jeon, Kim and Park mentioned earlier, we know that

$$S(4) \supset \{2, 3, 5, 7, 11, 13, 17\}\,.$$

(These are the prime orders that occur for infinitely many curves.)

The situation for $d \leq 3$ suggests that we should have equality.

So we need good upper bounds.

Upper Bounds

Merel gave the first explicit upper bound:

$$\max S(d) \leq d^{3d^2}$$

This is not really helpful when $d = 4$.
Fortunately, there is a better bound due to Oesterlé:

$$\max S(d) \leq (3^{d/2} + 1)^2$$

For $d = 4$, this says that $\max S(4) \leq 97$.

Kamienny and Stein

Sheldon Kamienny and William Stein developed a computational test that can (with some luck) show that $p \notin S(d)$ for a given prime p.

Using this test, they were able to show that

$$S(4) \subset \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31\}.$$

William reported on this a few months ago
at the "Pacific Northwest Number Theory Conference".

Realizing that this is really a question about rational points
on symmetric powers of certain modular curves,
I offered my help in dealing with the remaining four primes.

The Theorem

Our joint efforts were successful, and we now have the following

Theorem (Kamienny, Stein, Stoll 2010).

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

In the remainder of this talk,
I will sketch how 19, 23, 29 and 31 can be excluded.

Rational Points on Symmetric Powers

Let $X_1(p)$ denote the usual modular curve
that parameterizes elliptic curves together with a point of order p.

Let $X_1(p)^{(d)}$ denote its dth symmetric power
(the points of $X_1(p)^{(d)}$ are effective divisors of degree d on $X_1(p)$).

$X_1(p)$ has $\frac{p-1}{2}$ rational cusps. Let P_0 be one of them.

If K is a number field of degree $d' \leq d$, E/K is an elliptic curve
and $P \in E(K)$ has order p, then we obtain a point $Q \in X_1(p)(K)$.

Adding the d' conjugates of Q and $d - d'$ times P_0,
we obtain a rational effective divisor of degree d on $X_1(p)$,
or equivalently, a rational point on $X_1(p)^{(d)}$.

A Lemma

We can deduce the following.

Lemma.

Let p be a prime number, and let C be the set of rational cusps on $X_1(p)$.
If $d < \frac{p-1}{2}$, then

$$p \notin S(d) \iff X_1(p)^{(d)}(\mathbb{Q}) = C^{(d)}\,.$$

(The remaining cusps are defined over $\mathbb{Q}(\mu_p)^+$ of degree $\frac{p-1}{2}$.)

A Proposition

Proposition.

Let $X/\mathbb{Q}$ be a curve and use $P_0 \in X(\mathbb{Q})$ to embed X into its Jacobian J.
Let ℓ be a prime of good reduction, and let d be a positive integer.
Assume that

1. $J(\mathbb{Q})$ is finite.
2. If $\ell = 2$, then $J(\mathbb{Q})[2]$ injects into $J(\mathbb{F}_2)$.
3. There is no morphism $X \to \mathbb{P}^1$ of degree $\leq d$.
4. The reduction map $X(\mathbb{Q}) \to X(\mathbb{F}_\ell)$ is surjective.
5. The images of $X^{(d)}(\mathbb{F}_\ell)$ and $J(\mathbb{Q})$ in $J(\mathbb{F}_\ell)$ meet only in points coming from $X(\mathbb{F}_\ell)^{(d)}$.

Then $X^{(d)}(\mathbb{Q}) = X(\mathbb{Q})^{(d)}$:
Every point of degree $\leq d$ on X is already rational.

Proof

$$\begin{tikzcd}
X(\mathbb{Q})^{(d)} \arrow[r, hook] \arrow[d, two heads, "\mathbf{4}"] & X^{(d)}(\mathbb{Q}) \arrow[r, hook, "\mathbf{3}"] \arrow[d] & J(\mathbb{Q}) \arrow[d, hook, "\mathbf{1\ \&\ 2}"] \\
X(\mathbb{F}_\ell)^{(d)} \arrow[r] & X^{(d)}(\mathbb{F}_\ell) \arrow[r] & J(\mathbb{F}_\ell)
\end{tikzcd}$$

Let $P \in X^{(d)}(\mathbb{Q})$.
By Assumption 5, there is $Q \in X(\mathbb{F}_\ell)^{(d)}$ with the same image in $J(\mathbb{F}_\ell)$.
So (by Assumption 4) there is $P' \in X(\mathbb{Q})^{(d)}$ with the same image in $J(\mathbb{F}_\ell)$.
Since $X^{(d)}(\mathbb{Q}) \to J(\mathbb{F}_\ell)$ is injective (Assumptions 1–3),
it follows that $P = P'$.

Application

We apply the Proposition to $X = X_1(p)$ with $p \in \{19, 23, 29, 31\}$ and $d = 4$; we write $J_1(p)$ for the Jacobian of $X_1(p)$.

Note that by Mazur, for $p \geq 11$ we have $X_1(p)(\mathbb{Q}) = \{\text{rational cusps}\}$.

By work of Conrad, Edixhoven and Stein,
it is known that $J_1(p)(\mathbb{Q})$ is finite for $p \leq 31$ (and a few larger p).

By Jeon, Kim and Park, Assumption 3 is satisfied for $p \geq 19$.

Assumption 4 holds whenever $(\sqrt{\ell} + 1)^2 < p$.

The remaining Assumptions 2 and 5 need to be checked in each case.

19 and 23

For $p = 19$ and $p = 23$, it is known that $\#J_1(p)(\mathbb{Q})$ is odd.
So Assumption 2 is satisfied when we take $\ell = 2$.

To verify Assumption 5, it suffices to show that

$$X_1(p)^{(4)}(\mathbb{F}_2) = X_1(p)(\mathbb{F}_2)^{(4)}\,.$$

This means that there are no elliptic curves over $\mathbb{F}_{2^e}$, $e \le 4$, with a point of order p.

The Hasse-Weil bound forces $e = 4$ and $\#E(\mathbb{F}_{2^4}) = p$.

However, by results of Waterhouse (see Mestre's talk), such curves do not exist.

We conclude that

$$19 \notin S(4) \qquad \text{and} \qquad 23 \notin S(4)\,.$$

31

We want to take $\ell = 2$ again.

In this case, $\#J_1(31)(\mathbb{Q})$ is even, but it is known that $J_1(31)(\mathbb{Q})$ is generated by the images of the rational cusps.

This allows us to check by an explicit computation that Assumption 2 is satisfied.

Assumption 5 is trivially satisfied by the Hasse-Weil bound (note that $31 > (\sqrt{16} + 1)^2$).

We conclude that

$$31 \notin S(4)\,.$$

29

This is the hardest case:

It is not known (yet) what $J_1(29)(\mathbb{Q})$ is;
there are only upper and lower bounds (the ambiguity is in the 2-torsion).

We cannot use $\ell = 2$, because we cannot check Assumption 2.

So we use a larger prime ℓ and the upper bound for $J_1(29)(\mathbb{Q})$
and hope that we can verify that Assumption 5 holds.

After a lengthy computation, we are successful with $\ell = 11$.

We conclude that

$$29 \notin S(4)\,.$$