Torsion subgroups of CM elliptic curves

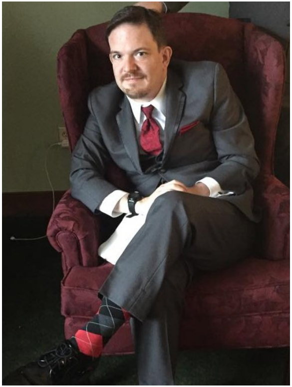
Paul Pollack

The University of Georgia

JMM 2017: Special session on discrete structures in number theory

January 5, 2017

Everything I will discuss is joint work with two colleagues at the University of Georgia, Abbey Bourdon and Pete L. Clark.

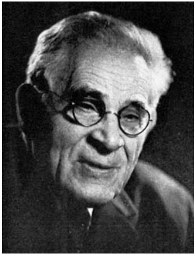


Theorem (Mordell–Weil Theorem, 1920s)

Let E be an elliptic curve over a number field F. The group $E(F)$ is finitely generated. Thus, letting $E(F)[\mathrm{tors}]$ denote the K-rational points of finite order on E, the group $E(F)[\mathrm{tors}]$ is a finite abelian group, and

$$E(F) \cong \mathbb{Z}^r \oplus E(F)[\mathrm{tors}]$$

for a certain integer $r \geq 0$.



Merel's uniform boundedness theorem

In particular, $\#E(F)[\mathrm{tors}] < \infty$ for any elliptic curve over any degree d number field F. It is a deep and remarkable fact that $\#E(F)[\mathrm{tors}]$ can be bounded entirely in terms of $[F : \mathbb{Q}]$.

Theorem (Merel, 1994)

For all positive integers d, there is a bound $T(d)$ such that for any elliptic curve E over any degree d number field F,

$$\#E(F)[\mathrm{tors}] \leq T(d).$$

Merel's uniform boundedness theorem

In particular, $\#E(F)[\mathrm{tors}] < \infty$ for any elliptic curve over any degree d number field F. It is a deep and remarkable fact that $\#E(F)[\mathrm{tors}]$ can be bounded entirely in terms of $[F : \mathbb{Q}]$.

Theorem (Merel, 1994)

For all positive integers d, there is a bound $T(d)$ such that for any elliptic curve E over any degree d number field F,

$$\#E(F)[\mathrm{tors}] \leq T(d).$$

Question

Great! But what is $T(d)$?

Explicit bounds for $T(d)$

Piecing together results of Oesterlé and Parent, one can write down an admissible value of $T(d)$ that is doubly exponential in d.

PARENTAL CONTENT EXPLICIT ADVISORY

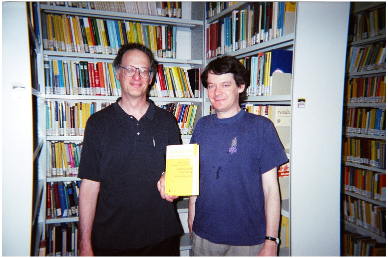
Explicit bounds for $T(d)$

Piecing together results of Oesterlé and Parent, one can write down an admissible value of $T(d)$ that is doubly exponential in d.

Conjecture

$\#E(F)[\mathrm{tors}] \ll d^{\mathrm{constant}}$.

This much improved bound is known for certain special classes of curves.



Theorem (Hindry–Silverman, 1998)

If E is an elliptic curve over a number field F of degree $d \geq 2$, and the j-invariant of E is an algebraic integer, then

$$\#E(F)[\mathrm{tors}] \leq 1977408 d \log d.$$

As a very special case, this bound holds if we assume E has complex multiplication.

Moral of this talk: We can say much more in the CM case!

Now you CM, now you don't?

Theorem (Clark and P., 2015)

If E is a CM elliptic curve over a degree d number field F, with $d \geq 3$, then

$$\#E(F)[\mathrm{tors}] \ll d \log \log d.$$

The implied constant here is absolute and effectively computable.

So we improved $d \log d$ to $d \log \log d$.

Theorem (Clark and P., 2015)

If E is a CM elliptic curve over a degree d number field F, with $d \geq 3$, then

$$\#E(F)[\mathrm{tors}] \ll d \log \log d.$$

The implied constant here is absolute and effectively computable.

So we improved $d \log d$ to $d \log \log d$. Who cares? Is this number theory or lumber theory?

Remark

Prior work of Breuer shows that this result is best possible, up to the value of the implied constant.

Now you CM, now you don't? II

Let $T_{\mathrm{CM}}(d)$ be the largest order of the torsion subgroup of a CM elliptic curve over a degree d number field. From Breuer + the theorem on the last slide,

$$0 < \limsup_{d \to \infty} \frac{T_{\mathrm{CM}}(d)}{d \log \log d} < \infty.$$

Now you CM, now you don't? II

Let $T_{\mathrm{CM}}(d)$ be the largest order of the torsion subgroup of a CM elliptic curve over a degree d number field. From Breuer + the theorem on the last slide,

$$0 < \limsup_{d\to\infty} \frac{T_{\mathrm{CM}}(d)}{d \log\log d} < \infty.$$

Theorem (Clark and P., 2016)

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

The lower bound

The lower bound is an elaboration on Breuer's method. Start with

$$E : y^2 = x^3 - 1,$$

which has CM by the full ring of integers of $K = \mathbb{Q}(\sqrt{-3})$.

Let N run through the sequence of 'primorials'

$$2, \quad 2 \cdot 3, \quad 2 \cdot 3 \cdot 5, \quad 2 \cdot 3 \cdot 5 \cdot 7, \dots,$$

and let d run through the corresponding degrees of the N-torsion fields $\mathbb{Q}(E[N])$. One argues that, as $d \to \infty$,

$$T_{\mathrm{CM}}(d) \geq (e^{\gamma}\pi/\sqrt{3} + o(1)) d \log\log d.$$

The upper bound: Some ingredients

To bound $T_{\mathrm{CM}}(d)$ from above is to bound from above

$$\#E(F)[\mathrm{tors}]$$

for all CM elliptic curves E over all degree d number fields F.

We distinguish two cases:

- F contains the imaginary quadratic field K by which E has CM,
- F doesn't contain K.

We will begin by assuming we are in the first case, i.e., that $F \supset K$.

The upper bound: Some ingredients

To bound $T_{\mathrm{CM}}(d)$ from above is to bound from above

$$\#E(F)[\mathrm{tors}]$$

for all CM elliptic curves E over all degree d number fields F.

We distinguish two cases:

- F contains the imaginary quadratic field K by which E has CM,
- F doesn't contain K.

We will begin by assuming we are in the first case, i.e., that $F \supset K$.

If we restrict to the first case, we can in fact that the CM order is the full ring of integers of K.

If we restrict to the first case, we can assume the CM order $\mathcal{O}$ is all of $\mathcal{O}_K$. This is a consequence of the following **torsion isogeny theorem**.

Theorem (Bourdon–Clark, 2016)

Let E be a CM elliptic curve of a number field F having CM by a nonmaximal order in the imaginary quadratic field K, where $F \supset K$. There is a way of canonically associating E with an elliptic curve $E'/_F$ having CM by the maximal order $\mathcal{O}_K$; moreover,

$$\#E(F)[\mathrm{tors}] \mid \#E'(F)[\mathrm{tors}].$$

Thus, if we have an upper bound on $\#E'(F)[\mathrm{tors}]$, we get the same bound on $\#E(F)[\mathrm{tors}]$.

Key fact: If we view $E(F)[\mathrm{tors}]$ as an $\mathcal{O}_K$ module and let $\mathfrak{a}$ be its annihilator, then

$$\#E(F)[\mathrm{tors}] = N(\mathfrak{a});$$

moreover, the ray class field $K^{(\mathfrak{a})}$ sits inside F.

Key fact: If we view $E(F)[\mathrm{tors}]$ as an $\mathcal{O}_K$ module and let $\mathfrak{a}$ be its annihilator, then

$$\#E(F)[\mathrm{tors}] = N(\mathfrak{a});$$

moreover, the ray class field $K^{(\mathfrak{a})}$ sits inside F.

Using this ray class field containment and the formula for the degree of a ray class field, one gets (using that $[K^{(\mathfrak{a})} : \mathbb{Q}] \leq [F : \mathbb{Q}]$)

$$\Phi(\mathfrak{a}) \leq \frac{w_K d}{h_K},$$

where w_K is the number of roots of unity in K (always at most 6) and Φ is the analogue of Euler's phi-function for ideals of $\mathcal{O}_K$.

Question

Given an upper bound on $\Phi(\mathfrak{a})$, how large can $N(\mathfrak{a})$ be?

We have:

$$\Phi(\mathfrak{a}) \leq \frac{w_K d}{h_K},$$

Question

Given an upper bound on $\Phi(\mathfrak{a})$, how large can $N(\mathfrak{a})$ be?

For the classical Euler function, the answer is well-known. If $\phi(a) \leq z$, then $a \leq (1 + o(1)) \cdot e^{\gamma} z \log\log z$, as $z \to \infty$.

If K is a fixed imaginary quadratic field, something similar is true: $\Phi(\mathfrak{a}) \leq z$ implies that

$$N(\mathfrak{a}) \leq (1 + o(1)) \cdot e^{\gamma} \frac{2\pi h_K}{w_K \sqrt{|\Delta_K|}} z \log\log z.$$

All this is enough to prove that, if we consider elliptic curves with CM by a *fixed* imaginary quadratic field K (and $F \supset K$), then

$$\#E(F)[\mathrm{tors}] \leq (1 + o(1)) \frac{e^{\gamma}\pi}{\sqrt{|\Delta_K|}} d \log\log d,$$

as $d \to \infty$.

The factor in front of $d \log\log d$ is largest when $|\Delta_K|$ is smallest, i.e., when $K = \mathbb{Q}(\sqrt{-3})$, and this gives the upper bound appearing in our theorem.

There are two debts outstanding before we call this a proof.

To bound $N(\mathfrak{a})$ given a bound on $\Phi(\mathfrak{a})$ depended on K being fixed. Since we aim for a totally uniform result, we cannot make this assumption. We reduce to the case of fixed K by proving a weaker, totally uniform bound on $N(\mathfrak{a})$ — this needs Siegel's theorem on the growth of quadratic class numbers.

We only treated the case when the field of definition F of the elliptic curve contains the CM field K. It turns out that in the opposite case, $E(F)[\mathrm{tors}]$ is much smaller !

Using recent results of Bourdon–Clark, we show that

$$\#E(F)[\mathrm{tors}] = o(d \log\log d)$$

as $d \to \infty$ in this case. In fact, one can prove a bound of the shape $O(d^{1-\delta})$ for a certain positive δ.

Hence, for the lim sup question, these cases are irrelevant.

THANK YOU!