Anatomy of torsion in the CM case

(joint work with Abbey Bourdon and Pete L. Clark)

The University of Georgia

Paul Pollack

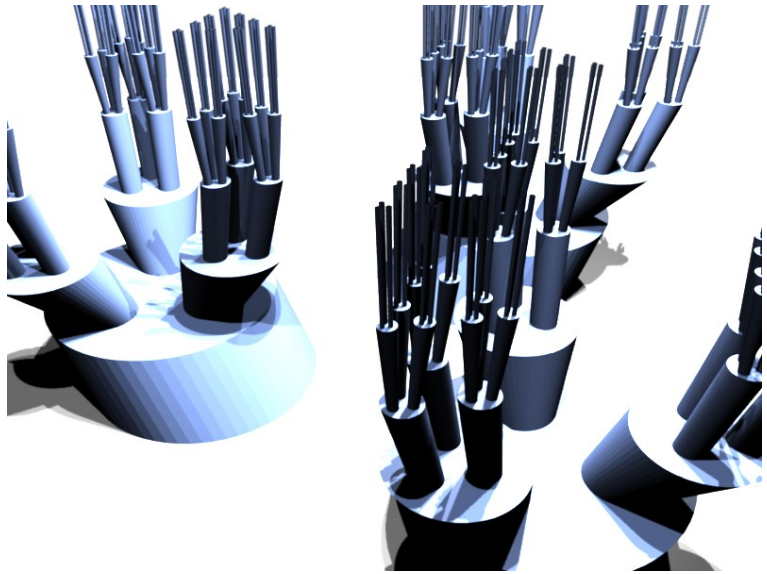
Illinois Number Theory Conference 2015

August 14, 2015

This talk is a report on some recent work in *arithmetic statistics*, specifically statistics about torsion subgroups of elliptic curves over number fields.

Everything I will discuss is joint work with two colleagues at the University of Georgia.

Abbey Bourdon



Pete L. Clark

This talk is a report on some recent work in *arithmetic statistics*, specifically statistics about torsion subgroups of elliptic curves over number fields.

Everything I will discuss is joint work with two colleagues at the University of Georgia.

Abbey Bourdon

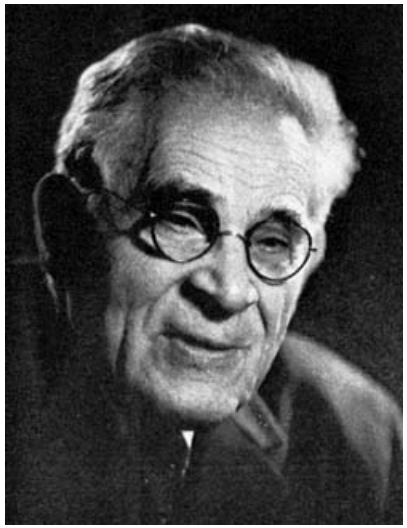
Pete L. Clark

Theorem (Mordell–Weil Theorem, 1920s)

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

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

for a certain integer $r \geq 0$.



Theorem (Mordell–Weil Theorem, 1920s)

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

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

for a certain integer $r \geq 0$.

Question

Given K, what are the possible values of the **rank** *r, as E varies over elliptic curves/K? Similarly, what are the possibilities for the torsion subgroup $E(K)[\mathrm{tors}]$?*

We do not have satisfactory answers to either question!

As far as the **rank**, even in the simplest case $K = \mathbb{Q}$, we do not know if r can be arbitrarily large. Elkies has produced an example of a curve $E/\mathbb{Q}$ with rank $r \geq 28$. Public opinion seems to be slowly shifting in the direction that ranks over $\mathbb{Q}$ are bounded.

We do not have satisfactory answers to either question!

As far as the **rank**, even in the simplest case $K = \mathbb{Q}$, we do not know if r can be arbitrarily large. Elkies has produced an example of a curve $E/\mathbb{Q}$ with rank $r \geq 28$. Public opinion seems to be slowly shifting in the direction that ranks over $\mathbb{Q}$ are bounded.

The situation is a little better for torsion.

- Mazur (1977) famously classified all possibilities for $E(\mathbb{Q})[\mathrm{tors}]$. There are 15 possibilities.
- Kamienny and Kenku–Momose have given a complete list of the groups that can appear as $E(K)[\mathrm{tors}]$ for an elliptic curve over a quadratic field K. There are 26 possibilities.
- We still do not have a provably complete list of possible torsion structures over cubic number fields.

Merel's uniform boundedness theorem

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

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 $T(d)$

If N is the exponent of $E(F)[\mathrm{tors}]$, we can view $E(F)[\mathrm{tors}]$ as a subgroup of $E(\mathbb{C})[N] \cong \mathbb{Z}/N\mathbb{Z} \oplus \mathbb{Z}/N\mathbb{Z}$. So $E(F)[\mathrm{tors}]$ is a finite abelian group of rank ≤ 2, and so its order is bounded by the square of its exponent.

Oesterlé showed that every prime dividing the exponent is at most $(1 + 3^{d/2})^2$. And Parent showed that every prime power ℓ^α dividing the exponent is

$$\leq \begin{cases} 65(3^d - 1)(2d)^6 & \text{if } \ell > 3, \\ 65(5^d - 1)(2d)^6 & \text{if } \ell = 3, \\ 129(3^d - 1)(3d)^6 & \text{if } \ell = 2. \end{cases}$$

Piecing the prime power bounds together gives an upper bound on $\#E(F)[\mathrm{tors}]$ that is doubly exponential in d.

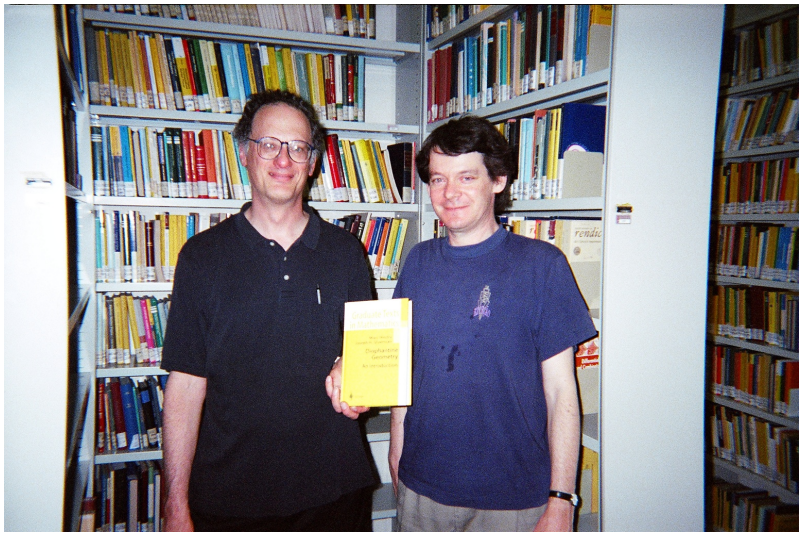
Piecing the prime power bounds together gives an upper bound on $\#E(F)[\mathrm{tors}]$ that is doubly exponential in d.

Conjecture

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

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

Our own small piece of Silvermania, here in Urbana



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 even more in the CM case. In fact, a truly surprising amount.

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.

Remark

In the case when the CM field is not contained in F, this can be deduced from results of Silverberg and (independently) Prasad–Yogananda concerning the exponent of $E(F)[\mathrm{tors}]$.

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.

Remark

In the case when the CM field is not contained in F, this can be deduced from results of Silverberg and (independently) Prasad–Yogananda concerning the exponent of $E(F)[\mathrm{tors}]$.

We improved $d \log d$ to $d \log\log d$. Is this exciting?
Or are we doing lumber theory instead of number theory?

Theorem (Breuer, 2010)

Let $E_{/F}$ be a CM elliptic curve over a number field F. There exists a constant $c(E,F) > 0$, integers $3 \leq d_1 < d_2 < \ldots < d_n < \ldots$ and number fields $F_n \supset F$ with $[F_n : F] = d_n$ such that for all positive integers n,

$$\#E(F_n)[\mathrm{tors}] \geq c(E,F) d_n \log\log d_n$$

So the $d \log\log d$ upper bound is *sharp*, up to a multiplicative constant.

Theorem (Breuer, 2010)

Let $E_{/F}$ be a CM elliptic curve over a number field F. There exists a constant $c(E,F) > 0$, integers $3 \leq d_1 < d_2 < \ldots < d_n < \ldots$ and number fields $F_n \supset F$ with $[F_n : F] = d_n$ such that for all positive integers n,

$$\#E(F_n)[\mathrm{tors}] \geq c(E,F) d_n \log\log d_n$$

So the $d \log\log d$ upper bound is *sharp*, up to a multiplicative constant.

To set some notation, define $T_{\mathrm{CM}}(d)$ as the largest size of a torsion subgroup of a CM elliptic curve over a degree d number field. We obtained an optimal bound on the upper order of $T_{\mathrm{CM}}(d)$.

What about its lower order? average order? normal order?

Lower order

Say that a group is realizable in degree d if it appears as $E(F)[\mathrm{tors}]$ for some CM elliptic curve over some degree d number field F. There are six possible groups realizable in degree $d = 1$ (i.e., over $F = \mathbb{Q}$): $\mathbb{Z}/n\mathbb{Z}$ for $n = 1, 2, 3, 4, 6$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

This list was obtained by Olson shortly before Mazur's theorem.

Since we can base change a curve over $\mathbb{Q}$ to a curve over any number field F, it is immediate that $T_{\mathrm{CM}}(d) \geq 6$ for all d.

Theorem (Bourdon, Clark, Stankewicz)

$T_{\mathrm{CM}}(d) = 6$ for all primes $d \geq 7$. In fact, the groups realizable in these degrees d are exactly the groups realizable over $\mathbb{Q}$.

Thus, $\liminf_{d \to \infty} T_{\mathrm{CM}}(d) = 6$.

Theorem (Bourdon, Clark, Stankewicz)

$T_{\mathrm{CM}}(d) = 6$ for all primes $d \geq 7$. In fact, the groups realizable in these degrees d are exactly the groups realizable over $\mathbb{Q}$.

Thus, $\liminf_{d \to \infty} T_{\mathrm{CM}}(d) = 6$.

One can still ask how often this lim inf is attained. We call a d with $T_{\mathrm{CM}}(d) = 6$ an **Olson degree**. (This turns out to be equivalent to saying that the groups realizable in degree d are the same as those realizable over $\mathbb{Q}$.)

Theorem (Bourdon, Clark, P.)

The set of Olson degrees has a well-defined, effectively computable asymptotic density, lying strictly between 0 *and* 1*.*

Computations suggest that the density is just above 26%.

N	# Olson degrees in $[1, N]$
1000	265
10 000	2649
100 000	26 474
1 000 000	264 633
10 000 000	2 646 355
100 000 000	26 462 845
1 000 000 000	264 625 698
10 000 000 000	2 646 246 218
100 000 000 000	26 462 418 808

Counts of Olson degrees to 10^{11}.

Average order

Theorem (Bourdon, Clark, P.)

As $x \to \infty$,

$$\frac{1}{x} \sum_{d \le x} T_{\mathrm{CM}}(d) = \frac{x}{(\log x)^{1+o(1)}}.$$

The average over odd d is much smaller:

Theorem (Bourdon, Clark, P.)

As $x \to \infty$,

$$\frac{1}{x} \sum_{d \le x,\ 2 \nmid d} T_{\mathrm{CM}}(d) = x^{\frac{1}{3}+o(1)}.$$

Typical boundedness

It turns out that while $T_{\mathrm{CM}}(d)$ is far from bounded on average, it is bounded "typically".

Theorem (Bourdon, Clark, P.)

As $B \to \infty$, the proportion of d with $T_{\mathrm{CM}}(d) > B$ tends to 0. Here "proportion" means upper density.

So, for example, there is a B for which the following holds: All but 0.0001% of the natural numbers d have $T_{\mathrm{CM}}(d) \leq B$. (One might call this uniform uniform boundedness!)

In fact, we can be even more precise about the decay of this proportion as $B \to \infty$.

Theorem

As $B \to \infty$, the upper density of d with $T_{\mathrm{CM}}(d) > B$ has the shape

$$(\log B)^{-\eta+o(1)},$$

where

$$\eta = 1 - \frac{1 + \log\log 2}{\log 2}.$$

The same estimate holds for the lower density of this set of n.

(The constant η, which is ≈ 0.086, is known in the literature as the **Erdős–Ford–Tenenbaum constant**.)

Upper order and average order

Ask me later!

Had I but time,
I could a tale unfold whose lightest word
Would harrow up thy soul, freeze thy young blood,
Make thy two eyes like stars start from their spheres,
Thy knotted and combined locks to part,
And each particular hair to stand on end.

Hamlet, Act 1, Scene 5

Lower order

Theorem (Bourdon, Clark, P.)

The set of Olson degrees has a well-defined, effectively computable asymptotic density, lying strictly between 0 *and* 1.

Since we can always base change a curve over one number field to any extension, if

$$T_{\mathrm{CM}}(d) > 6 \Longrightarrow T_{\mathrm{CM}}(D) > 6 \quad \text{whenever } d \mid D.$$

Thus, the complement of the Olson degrees is closed under taking multiples; it is a **set of multiples**.

Sets of multiples 101

Any set of multiples $\mathcal{S}$ can be written in the form $M(\mathcal{G})$ for a certain set $\mathcal{G}$, where

$M(\mathcal{G}) = \{\text{all integers that are multiples of at least one element of } \mathcal{G}\}$.

We call $\mathcal{G}$ a **set of generators**.

For example, one can always take $\mathcal{G} = \mathcal{S}$ (boring!). Would prefer to choose $\mathcal{G}$ more economically.

Theorem (Erdős)

If $\sum_{g \in \mathcal{G}} \frac{1}{g} < \infty$, *then* $M(\mathcal{G})$ *possesses an asymptotic density. If* $\mathcal{G} \neq \emptyset$, *this density is* > 0. *If* $1 \notin \mathcal{G}$, *this density is* < 1.

Proposition

For the complement of the set of Olson degrees, we can take

$$\mathcal{G} = \{2\} \cup \{\frac{\ell - 1}{2} \cdot h_{\mathbb{Q}(\sqrt{-\ell})} : \text{ primes } \ell \equiv 3 \pmod 4, \ell > 3\}.$$

The sum of the reciprocals of the elements of $\mathcal{G}$ diverges, either because

- $h_{\mathbb{Q}(\sqrt{-\ell})} \gg \ell^{1/2-\epsilon}$ (Siegel, ineffective), *or*
- $h_{\mathbb{Q}(\sqrt{-\ell})} \gg (\log \ell)^{1-\epsilon}$ (Goldfeld–Gross–Zagier, effective).

[Since $2, 3, 5 \in \mathcal{G}$, the density of non-Olsons is $\geq 11/15$, and the density of Olsons is $\leq 4/15 = 26.66\ldots\%$.]

What is behind this determation of $\mathcal{G}$?

The bulk of the algebraic work with Bourdon and Clark goes into proving certain divisibility relations.

For example, if ℓ^α divides $E(F)[\mathrm{tors}]$, where E/F is a CM elliptic curve and F contains the CM field K, we show that $d = [F : \mathbb{Q}]$ is divisible by one of

$$h_K \ell^{\alpha-2}(\ell^2 - 1), \quad h_K \ell^{\alpha-2}(\ell - 1)^2, \quad \text{or} \quad h_K \ell^{\alpha-1}(\ell - 1).$$

Here $\ell^{\alpha-2}$ should be replaced with 1 in the case $\alpha = 1$, and h_K is the class number of K.

What is behind this determation of $\mathcal{G}$?

The bulk of the algebraic work with Bourdon and Clark goes into proving certain divisibility relations.

For example, if ℓ^α divides $E(F)[\mathrm{tors}]$, where E/F is a CM elliptic curve and F contains the CM field K, we show that $d = [F : \mathbb{Q}]$ is divisible by one of

$$h_K \ell^{\alpha-2}(\ell^2 - 1), \quad h_K \ell^{\alpha-2}(\ell - 1)^2, \quad \text{or} \quad h_K \ell^{\alpha-1}(\ell - 1).$$

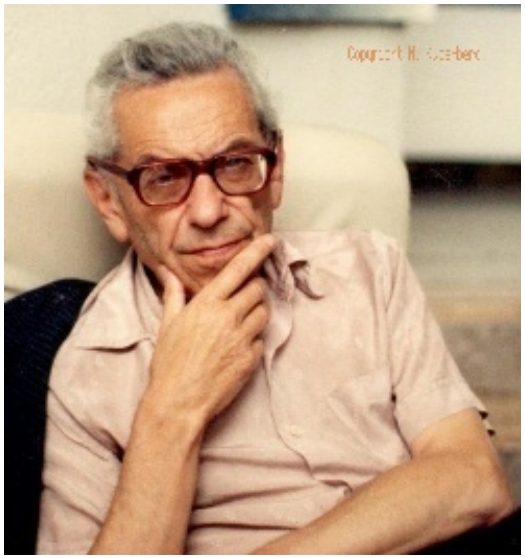
Here $\ell^{\alpha-2}$ should be replaced with 1 in the case $\alpha = 1$, and h_K is the class number of K.

We also have partial converse relations. For example, if $\ell \equiv 3 \pmod 4$ is prime, there is an elliptic curve E over a degree $\frac{\ell-1}{2} h_{\mathbb{Q}(\sqrt{-\ell})}$ number field L with $E(L)$ having a point of order ℓ.

These results forge a connection between integers for wich $T_{\mathrm{CM}}(d)$ is large, and integers which have a divisor of the form $\ell - 1$ (a shifted prime).

How rare is it for a number to be divisible by a large $\ell - 1$?
One might guess it is fairly common. After all, most numbers are divisible by a large ℓ.

Actually, it is surprisingly rare!

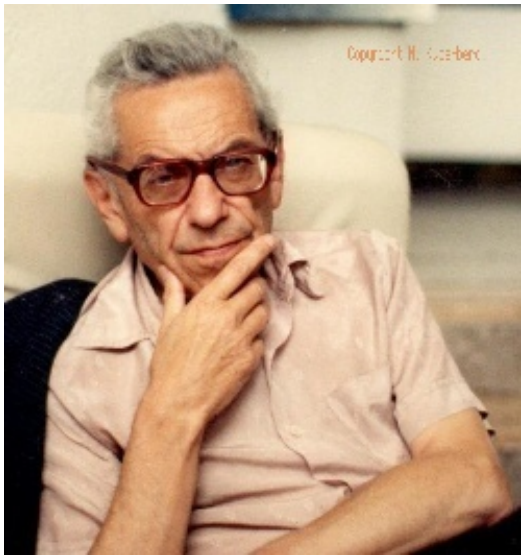


Paul Erdős

S. S. Wagstaff

Theorem (Erdős and Wagstaff, 1980)

As $B \to \infty$, the density of natural numbers divisible by $\ell - 1$ for some prime $\ell > B$ tends to 0.



Paul Erdős

S. S. Wagstaff

Theorem (Erdős and Wagstaff, 1980)

As $B \to \infty$, the density of natural numbers divisible by $\ell - 1$ for some prime $\ell > B$ tends to 0.

Theorem (Bourdon, Clark, P.)

As $B \to \infty$, the upper density of natural numbers d with $T_{\mathrm{CM}}(d) > B$ tends to 0.

Theorem

As $B \to \infty$, the upper density of n with $T_{\mathrm{CM}}(d) > B$ has the shape

$$(\log B)^{-\eta+o(1)},$$

where

$$\eta = 1 - \frac{1 + \log\log 2}{\log 2}.$$

The same estimate holds for the lower density of this set of n.

Where does η come from? We use a quantitative sharpening of the Erdős–Wagstaff theorem.

Theorem (McNew, Pomerance, and P.)

As $B \to \infty$ *with* $B \le x/\exp((\log x)^{1+o(1)}$,

$$\#\{d \le x : (\ell - 1) \mid d \text{ for some prime } \ell > B\} = \frac{x}{(\log B)^{\eta+o(1)}}. \quad (1)$$

OK, where does **that** η come from?

The theorem is proved by adapting recent work of Ford–Luca–Pomerance. They show that the counting function of the range of Carmichael's λ-function is $x/(\log x)^{\eta+o(1)}$.

Thank you!