φ-nomenology and torsion subgroups of CM elliptic curves

Paul Pollack
(joint work w/ A. Bourdon
and P.L. Clark)

2016 Gainesville International
Number Theory Conference

March 20, 2016

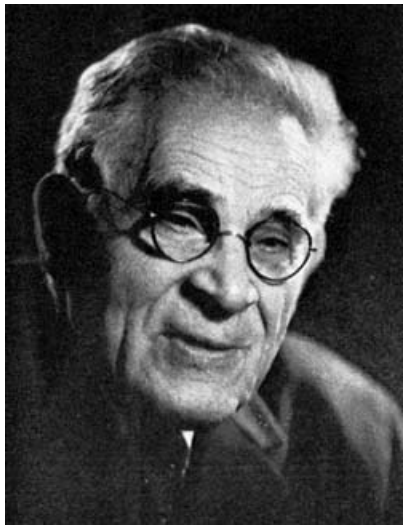
This is a talk about how certain questions in arithmetic statistics can be tackled using the theory of arithmetic functions, specifically the well-developed theory surrounding Euler's φ-function and its variants.

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 $r \geq 0$.

The question that brings us here today...

What are the possibilities for the torsion subgroup $E(K)[\mathrm{tors}]$?

- Mazur (1977) famously classified all possibilities for $E(\mathbb{Q})[\mathrm{tors}]$. There are 15 possibilities.

- Mazur (1977) famously classified all possibilities for $E(\mathbb{Q})[\mathrm{tors}]$. There are 15 possibilities.
- Kamienny and Kenku–Momose (in work completed in 1992) 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.

- Mazur (1977) famously classified all possibilities for $E(\mathbb{Q})[\mathrm{tors}]$. There are 15 possibilities.
- Kamienny and Kenku–Momose (in work completed in 1992) 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.
- In **late-breaking news** (announced in Athens on March 5, 2016), we now have a complete classification of possible torsion subgroups over cubic number fields — work of Dericx, Etropolski, Morrow, and Zureick-Brown. 26 possibilities (not the same 26 as before).

- Mazur (1977) famously classified all possibilities for $E(\mathbb{Q})[\mathrm{tors}]$. There are 15 possibilities.
- Kamienny and Kenku–Momose (in work completed in 1992) 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.
- In **late-breaking news** (announced in Athens on March 5, 2016), we now have a complete classification of possible torsion subgroups over cubic number fields — work of Dericx, Etropolski, Morrow, and Zureick-Brown. 26 possibilities (not the same 26 as before).

Q: What about in degree > 3?

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 $T(d)$

The best-known upper bounds on $T(d)$ (Oesterlé and Parent) are **doubly exponential** in d.

Conjecture

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

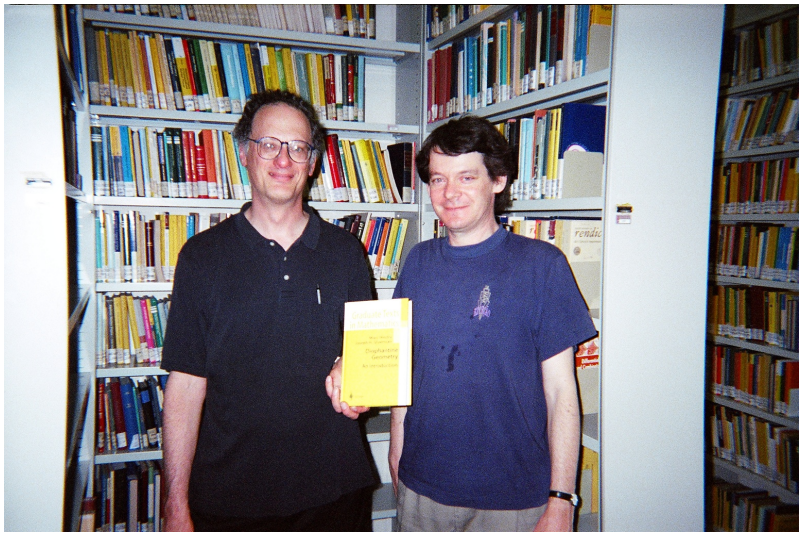
Explicit bounds for $T(d)$

The best-known upper bounds on $T(d)$ (Oesterlé and Parent) are **doubly exponential** in d.

Conjecture

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

It is a wide-open problem to prove this in general, but bounds of this kind are 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... by appreciating the relevant φ-nomena.

The upper order of $T_{\mathrm{CM}}(d)$

Put $T_{\mathrm{CM}}(d)$ as the largest order of any torsion subgroup of a CM elliptic curve over a degree d number field.

Theorem (Clark and P., 2015)

We have

$$T_{\mathrm{CM}}(d) \ll d \log\log d.$$

The implied constant here is absolute and effectively computable.

The upper order of $T_{\mathrm{CM}}(d)$

Put $T_{\mathrm{CM}}(d)$ as the largest order of any torsion subgroup of a CM elliptic curve over a degree d number field.

Theorem (Clark and P., 2015)

We have

$$T_{\mathrm{CM}}(d) \ll d \log\log d.$$

The implied constant here is absolute and effectively computable.

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

The upper order of $T_{\mathrm{CM}}(d)$

Put $T_{\mathrm{CM}}(d)$ as the largest order of any torsion subgroup of a CM elliptic curve over a degree d number field.

Theorem (Clark and P., 2015)

We have

$$T_{\mathrm{CM}}(d) \ll d \log\log d.$$

The implied constant here is absolute and effectively computable.

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

A matching lower bound for infinitely many d had already been proved by Breuer in 2010. Hence, $d \log\log d$ is **the true upper order**.

The relevant φ-nomenon was already discovered by Landau in 1903. It is the **lower order** of φ. Landau's theorem is that as $n \to \infty$,

$$\varphi(n) \geq (1 + o(1))e^{-\gamma} \frac{n}{\log \log n}.$$

The relevant φ-nomenon was already discovered by Landau in 1903. It is the **lower order** of φ. Landau's theorem is that as $n \to \infty$,

$$\varphi(n) \geq (1 + o(1))e^{-\gamma} \frac{n}{\log \log n}.$$

Now suppose E is a CM elliptic curve over a degree d number field. Silverberg (1988) showed that with e the exponent of $E(F)[\mathrm{tors}]$,

$$\varphi(e) \leq 6d.$$

Now Landau's result, after "inversion", gives

$$e \ll d \log \log d.$$

This is almost what we want, except it is a bound on the exponent of $E(F)[\mathrm{tors}]$ and not on the size of the group!

Our theorem is proved by an argument very similar in spirit. The analytic glue that holds it all together is the following result:

Theorem

Let K be an imaginary quadratic field. Let $\mathfrak{a}$ be an ideal of $\mathcal{O}_K$. Then

$$\varphi_K(\mathfrak{a}) \gg \frac{1}{h_K} N(\mathfrak{a}) / \log\log N(\mathfrak{a}).$$

Here $\varphi_K(\mathfrak{a}) = \#(\mathcal{O}_K/\mathfrak{a})^\times$, h_K is the class number of K, and the implied constant is absolute and **effective**.

The chief difficulty here is getting the dependence on K to be as stated, with an effective constant. We use a result on Siegel zeros due to Goldfeld–Schinzel.

We know how large $T_{\mathrm{CM}}(d)$ sometimes gets.

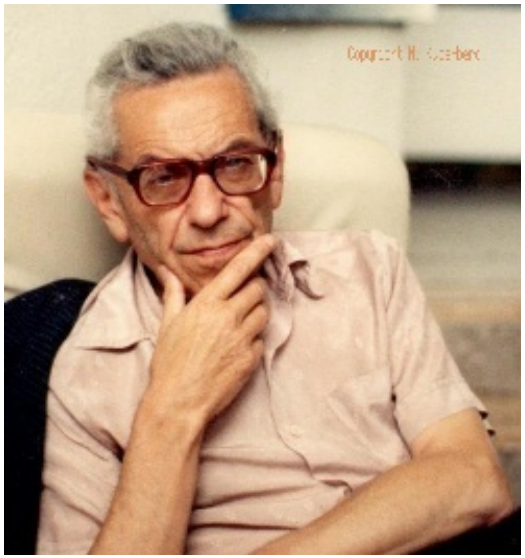
But how large is it typically?

One can show that having an element of $E(F)[\mathrm{tors}]$ of prime order ℓ forces a divisibility $\ell - 1 \mid 12d$.

If $T_{\mathrm{CM}}(d)$ is large, then $E(F)[\mathrm{tors}]$ is large for some E and some degree d number field F. This suggests that $\#E(F)[\mathrm{tors}]$ has a large prime factor ℓ. Then

$$\ell - 1 \mid 12d.$$

The frequency with which an integer is divisible by a large shifted prime has been investigated in connection with the study of the φ function and its close cousin, λ.

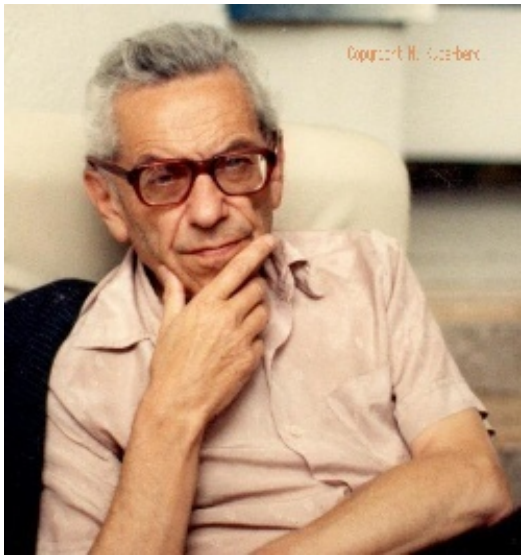


Paul Erdős

S. S. Wagstaff

Theorem (Erdős and Wagstaff, 1980)

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



Paul Erdős

S. S. Wagstaff

Theorem (Erdős and Wagstaff, 1980)

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

A toy model (and a slide where I steal a quote from a talk of John Voight)

> *The goal of mathematics is to convert rigorous proofs into heuristics. The latter are, in turn, used to produce new rigorous proofs. – Michael Harris, mathematics without apologies*

The preceding examples are suggestive enough that they motivated us to find an adequate toy model of $T_{\mathrm{CM}}(d)$.

It turns out that a reasonable such model is to pretend $T_{\mathrm{CM}}(d)$ is equal to

$$T_{\mathsf{fake}}(d) = \text{largest } m \text{ with } \varphi(m) \mid d.$$

A little motivation

To justify one direction of the analogy, one can show that if $T_{\mathrm{CM}}(d) = m$,

$$\Phi \mid 12d,$$

for some integer $\Phi = \prod_{\ell^\alpha \| m} \Phi(\ell^\alpha)$, where each

$$\Phi(\ell^\alpha) \in \begin{cases} \{(\ell^2-1)\ell^{\alpha-2}, \ell^{\alpha-2}(\ell-1)^2, \ell^{\alpha-1}(\ell-1)\} & \text{if } \alpha \geq 2, \\ \{\ell - 1\} & \text{if } \alpha = 1. \end{cases}$$

Conversely, divisibility of d by certain φ-like numbers allows one to construct examples of CM elliptic curves achieving desired torsion structures.

On average?

One one has this model, one can resume proving theorems.

Theorem (Bourdon, Clark, P.)

As $x \to \infty$,

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

How do we prove this?

We adapt a 1935 argument of Erdős that the number of elements in $[1, x]$ in the range of the φ-function is $x/(\log x)^{1+o(1)}$. (This result of Erdős has seen many improvements, culminating in work of Ford.)

How many groups?

Define $G_{\mathrm{CM}}(d)$ as the number of distinct groups that appear as the torsion subgroup of a CM elliptic curve over a degree d number field.

Say $d \leq x$. Any group that appears is of size $O(x \log\log x)$. The total number of finite abelian groups obeying this restriction is $O(x \log\log x)$. So, crudely,

$$\max_{d \leq x} G_{\mathrm{CM}}(d) = O(x \log\log x).$$

Is this a good upper bound?

Theorem (Bourdon and P.)

As $x \to \infty$,

$$\max_{d \le x} G_{\mathrm{CM}}(d) \le x/L(x)^{1+o(1)},$$

where $L(x) = \exp(\log x \frac{\log\log\log x}{\log\log x})$.

Theorem (Bourdon and P.)

As $x \to \infty$,

$$\max_{d \le x} G_{\mathrm{CM}}(d) \le x/L(x)^{1+o(1)},$$

where $L(x) = \exp(\log x \frac{\log\log\log x}{\log\log x})$. *Equality holds if the distribution of smooth numbers extends in the expected way to shifted primes* $p-1$.

Theorem (Pomerance, 1980)

As $x \to \infty$, *the maximum number of preimages of an element of* $[1, x]$ *under* φ *is at most* $x/L(x)^{1+o(1)}$. *Equality holds if the distribution of smooth numbers extends in the expected way to shifted primes* $p-1$.

(One wants that $\#\{p \le T : p-1 \text{ is } \exp(\sqrt{\log T}) - \text{smooth}\}$ is $\gg \frac{1}{\log T}\Psi(T, \exp(\sqrt{\log T}))$, or something not too much weaker.)

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

Thank you for listening ...

and

Happy Birthday Krishna!