Two analytic problems about CM elliptic curves

The University of Georgia

Paul Pollack

Stanford University Number Theory Seminar

January 16, 2015

Two problems

1. Fix an elliptic curve $E/\mathbb{Q}$. How do the groups $E(\mathbb{F}_p)$ vary as p runs over primes of good reduction?
2. Let d be a positive integer. What are the possible torsion subgroups $E(F)[\mathrm{tors}]$ if E is an elliptic curve defined over a number field F of degree d?

We will find it convenient later to restrict to curves with complex multiplication (CM), but we keep the discussion general for as long as possible.

Part I: Statistics for reductions mod p

Fix an elliptic curve $E/\mathbb{Q}$. We know that for each prime p of good reduction,

$$\#E(\mathbb{F}_p) = p + 1 - a_p,$$

where $|a_p| \leq 2\sqrt{p}$. Moreover,

$$E(\mathbb{F}_p) \cong \mathbb{Z}/d_p\mathbb{Z} \oplus \mathbb{Z}/e_p\mathbb{Z},$$

for uniquely determined positive integers d_p and e_p where $d_p \mid e_p$. The integers d_p and e_p are the **invariant factors** of the group.

We would like to understand how the d_p and e_p behave as p varies over primes of good reduction.

A prototypical result

Question: How often is $d_p = 1$?

Theorem (Serre, 1977)

Assume GRH. Let $E/\mathbb{Q}$ be a fixed elliptic curve with an irrational 2-torsion point. Then $E(\mathbb{F}_p)$ is cyclic for a well–defined positive proportion of primes p.

If E has CM, the GRH assumption can be omitted (Murty, 1979 and Cojocaru, 2003).

How many primes divide $\#E(\mathbb{F}_p)$?

In 1935, Erdős proved that almost all primes $p \leq x$ are such that $p - 1$ has about $\log\log p$ prime factors; this was a shifted-prime analogue of a theorem proved by Hardy and Ramanujan (1917).

How many primes divide $\#E(\mathbb{F}_p)$?

In 1935, Erdős proved that almost all primes $p \le x$ are such that $p-1$ has about $\log\log p$ prime factors; this was a shifted-prime analogue of a theorem proved by Hardy and Ramanujan (1917).

The Hardy–Ramanujan theorem was famously sharpened to a normal law by Erdős and Kac.

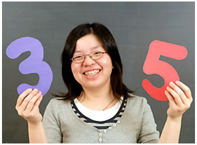
The analogue for shifted primes was worked out by Halberstam:

Theorem (Halberstam, 1967)

Fix a real number u. As $x \to \infty$,

$$\frac{1}{\pi(x)}\#\{p \le x : \omega(p-1) - \log_2 p \le u\sqrt{\log_2 x}\} \to \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{u} e^{-t^2/2}\,dt.$$

The normal behavior of the number of prime factors



In her 2003 PhD thesis, Yu-Ru Liu proved the analogue of Erdős–Kac with the numbers $\#E(\mathbb{F}_p) = p + 1 - a_p$ replacing $p - 1$.

Her result is unconditional if E has complex multiplication and conditional on GRH otherwise.

Titchmarsh's divisor problem

The Titchmarsh divisor problem asks one to estimate

$$\sum_{p \le x} \tau(p-1).$$

Under GRH, Titchmarsh (1931) showed that as $x \to \infty$,

$$\sum_{p \le x} \tau(p-1) \sim \frac{\zeta(2)\zeta(3)}{\zeta(6)} x.$$

The assumption of GRH was eventually removed by Linnik (1963). Today, the result can be thought of as a fairly simple corollary of the Brun–Titchmarsh and Bombieri–Vinogradov results.

Titchmarsh's divisor problem

What would an analogue for elliptic curves look like?

Akbary and Ghioca (2012): Observed that $d \mid p-1 \iff p$ splits completely in $\mathbb{Q}(\zeta_d)$. Since $\mathbb{Q}(E[d])$ is analogous to $\mathbb{Q}(\zeta_d)$, an analogue of $\tau(p-1)$ would be

$$\underbrace{\sum_{d:\ p \text{ splits completely in } \mathbb{Q}(E[d])} 1}_{\text{in fact, this is } \tau(d_p)} .$$

Theorem

Fix an elliptic curve $E/\mathbb{Q}$. As $x \to \infty$, we have $\sum_{p \le x} \tau(d_p) \sim c_E \pi(x)$. Here GRH is assumed unless E has CM.

Of course, one could be more naive about the analogue one considers.

What about just $\sum_{p\le x}\tau(\#E(\mathbb{F}_p))$?

Theorem (P.)

Fix $E/\mathbb{Q}$. If E has CM, then $\sum_{p\le x}\tau(d_pe_p)\sim c_Ex$, as $x\to\infty$, where c_E is a positive constant depending on E.

Of course, one could be more naive about the analogue one considers.

What about just $\sum_{p\leq x} \tau(\# E(\mathbb{F}_p))$?

Theorem (P.)

Fix $E/\mathbb{Q}$. If E has CM, then $\sum_{p\leq x} \tau(d_p e_p) \sim c_E x$, as $x \to \infty$, where c_E is a positive constant depending on E.

If we do not assume E has CM, but do assume GRH, $\sum_{p\leq x} \tau(d_p e_p) \asymp x$.

The Akbary–Ghioca result has been extended by Felix and Murty (2013) to estimate other sums of the form

$$\sum_{p \le x} f(d_p).$$

They assume one can write $f(n) = \sum_{d|n} g(d)$ where $\sum_{d \le x} |g(d)|$ is appropriately bounded.

Example

Assume $E/\mathbb{Q}$ is an elliptic curve with CM. Fix $0 < \alpha < 1$. As $x \to \infty$,

$$\sum_{p \le x} d_p^{\alpha} \sim c_{E,\alpha} \cdot \pi(x),$$

where $c_{E,\alpha} > 0$.

The last example suggests studying the mean value of d_p, and also of e_p.

Information about these mean values should encode how near to cyclic $E(\mathbb{F}_p)$ is, on average.

The last example suggests studying the mean value of d_p, and also of e_p.

Information about these mean values should encode how near to cyclic $E(\mathbb{F}_p)$ is, on average.

Theorem (Freiberg–Kurlberg, 2014)

Fix $E/\mathbb{Q}$. Then as $x \to \infty$, $\sum_{p \le x} e_p \sim c_E \frac{x^2}{\log x}$, for some $c_E > 0$. GRH is assumed if E does not have CM.

Theorem (Freiberg–Kurlberg, 2014)

Fix $E/\mathbb{Q}$. As $x \to \infty$, $\sum_{p \le x} e_p \sim c_E \frac{x^2}{\log x}$, for some $c_E > 0$. GRH is assumed if E does not have CM.

Since also $\sum_{p \le x} p \asymp \frac{x^2}{\log x}$, we see that e_p is of average order const $\cdot\, p$.

Theorem (Freiberg–Kurlberg, 2014)

Fix $E/\mathbb{Q}$. As $x \to \infty$, $\sum_{p \le x} e_p \sim c_E \frac{x^2}{\log x}$, for some $c_E > 0$. GRH is assumed if E does not have CM.

Since also $\sum_{p \le x} p \asymp \frac{x^2}{\log x}$, we see that e_p is of average order $\mathrm{const} \cdot p$.

Since $d_p e_p = p + 1 - a_p \sim p$, this suggests that d_p is usually bounded.

Theorem (Duke, 2003)

Let $\psi(p)$ be any function that tends to ∞. Then $d_p < \psi(p)$ for almost all primes p. GRH is assumed if E does not have CM.

Duke's result tells us about the normal order of d_p. What about the average order?

Question

What is the asymptotic behavior of $\sum_{p \leq x} d_p$?

Duke's result tells us about the normal order of d_p. What about the average order?

Question

What is the asymptotic behavior of $\sum_{p \leq x} d_p$?

This question was proposed by Kowalski (2001), who conjectured that

$$\begin{aligned} \sum_{p \leq x} d_p &\sim c_E \pi(x) && \text{if } E \text{ does not have CM} \\ &\sim c_E x && \text{if } E \text{ has CM.} \end{aligned}$$

If E does not have CM, there has been very little progress towards the upper bound; e.g., even on GRH, $x^{1+o(1)}$ is unknown (to me).

Suppose $E/\mathbb{Q}$ is a fixed elliptic curve with CM. Then

$$x\frac{\log\log x}{\log x} \ll \sum_{p\leq x} d_p \ll x\sqrt{\log x} \qquad \text{(Kowalski, 2001)}$$

$$\sum_{p\leq x} d_p \ll x\log\log x \qquad \text{(Kim, 2014).}$$

Kowalski's argument was fleshed out by Felix and Murty (2013), who noted a small improvement:

$$\frac{\sum_{p\leq x} d_p}{x\log\log x/\log x} \to \infty.$$

Suppose $E/\mathbb{Q}$ is a fixed elliptic curve with CM. Then

$$x\frac{\log\log x}{\log x} \ll \sum_{p\le x} d_p \ll x\sqrt{\log x} \qquad \text{(Kowalski, 2001)}$$

$$\sum_{p\le x} d_p \ll x\log\log x \qquad \text{(Kim, 2014).}$$

Kowalski's argument was fleshed out by Felix and Murty (2013), who noted a small improvement:

$$\frac{\sum_{p\le x} d_p}{x\log\log x/\log x} \to \infty.$$

Theorem (Freiberg and P., 2014)

For large x, we have $\sum_{p\le x} d_p \asymp x$.

Sketch of the proof

Recall our claim that for CM curves,

$$\sum_{p \leq x} d_p \asymp x.$$

For simplicity, **the** CM curve is

$$E\colon\ y^2 = x^3 - x,$$

which has CM by the ring of Gaussian integers $\mathbb{Z}[i]$.

For the primes $p \equiv 3 \pmod 4$,

$$\#E(\mathbb{F}_p) = p + 1.$$

These are the **supersingular primes.** For these $d_p \leq 2$, and so these can be ignored.

Suppose instead that $p \equiv 1 \pmod 4$. These are our **ordinary primes.** Then p factors in $\mathbb{Z}[i]$ as

$$p = \pi\bar{\pi},$$

where $\pi \equiv 1 \pmod{(1+i)^3}$. (In other words, π is **primary.**)

Then

$$\#E(\mathbb{F}_p) = p + 1 - (\pi + \bar{\pi}) = N(\pi - 1),$$

and d_p is the largest rational integer dividing $\pi - 1$.

Using the identity $d_p = \sum_{d \mid d_p} \phi(d)$, and remembering that $d_p^2 \mid d_p e_p = \#E(\mathbb{F}_p) \le (\sqrt{x}+1)^2$, we have

$$\begin{aligned}
\sum_{\substack{p \le x \\ p \equiv 1 \pmod 4}} d_p &= \sum_{\substack{p \le x \\ p \equiv 1 \pmod 4}} \sum_{d \mid d_p} \phi(d) \\
&= \sum_{d \le \sqrt{x}+1} \phi(d) \sum_{\substack{p \le x \\ p \equiv 1 \pmod 4 \\ d \mid d_p}} 1 \\
&= \frac{1}{2} \sum_{d \le \sqrt{x}+1} \phi(d) \sum_{\substack{N(\pi) \le x \\ N(\pi) \text{ prime}, \equiv 1 \pmod 4 \\ \pi \equiv 1 \pmod{[d, (1+i)^3]}}} 1.
\end{aligned}$$

OK, so

$$\sum_{\substack{p\le x\\ p\equiv 1\pmod 4}} d_p = \frac{1}{2}\sum_{d\le\sqrt{x}+1}\phi(d)\sum_{\substack{N(\pi)\le x\\ N(\pi)\text{ prime},\equiv 1\pmod 4\\ \pi\equiv 1\pmod{[d,(1+i)^3]}}} 1.$$

Let's look at the **upper bound**.
If we use Brun–Titchmarsh for $\mathbb{Z}[i]$, the inner sum is

$$\ll \frac{x}{\Phi(d)\log\frac{4x}{d^2}},$$

where Φ is the Euler function for $\mathbb{Z}[i]$.

Using this above and summing, we are led to Kim's bound

$$\ll x\log\log x.$$

To avoid losing a $\log\log$ factor, we need to treat the d close to $\sqrt{x}$ more efficiently.

The part of the sum corresponding to $d \leq x^{1/3}$ is OK, by the above argument, since then $\log \frac{4x}{d^2} \asymp \log x$. So suppose $d > x^{1/3}$.

We now have to estimate

$$\sum_{x^{1/3} < d \leq \sqrt{x}+1} \phi(d) \sum_{\substack{N(\pi) \leq x \\ N(\pi) \text{ prime}, \equiv 1 \pmod 4 \\ \pi \equiv 1 \pmod{[d, (1+i)^3]}}} 1.$$

In the inner sum, write $\pi = \omega d + 1$. If $N(\pi) \leq x$, then $N(\omega) \leq 4x/d^2$. If $N(\omega d + 1)$ is prime, clearly $\mathrm{Im}(\omega) \neq 0$.

We invert the order of summation and after some simplifications, we are left with the problem of bounding

$$\sum_{\substack{N(\omega)\leq 4x \\ \mathrm{Im}(\omega)\neq 0}} \sum_{\substack{x^{1/3}<d\leq\sqrt{\frac{4x}{N(\omega)}} \\ N(\omega d+1)\text{ prime}}} \phi(d).$$

Replace $\phi(d)$ with $\sqrt{4x/N(\omega)}$.
The problem comes down to counting $d \in (x^{1/3}, \sqrt{4x/N(\omega)}]$ for which the quadratic polynomial

$$N(\omega d + 1) = N(\omega)d^2 + Tr(\omega)d + 1$$

is prime.

The upper bound sieve gives that this is

$$\ll \mathfrak{S}\frac{\sqrt{x/N(\omega)}}{\log x},$$

where $\mathfrak{S}$ is a certain singular series depending on the particular quadratic polynomial.

(We can assume $\sqrt{4x/N(\omega)} > x^{1/3}$. This is why we get a denominator proportional to $\log x$.)

If $\mathfrak{S}$ were 1, we could sum with no problems. To complete the proof, one shows $\mathfrak{S}$ averages to $\ll 1$ in a suitable sense. Here mean value theorems for nonnegative multiplicative functions are used.

What about the lower bound?

Remember, we need to bound from below

$$\frac{1}{2}\sum_{d\leq\sqrt{x}+1}\phi(d)\sum_{\substack{N(\pi)\leq x\\ N(\pi)\text{ prime},\equiv 1 \pmod 4\\ \pi\equiv 1 \pmod{[d,(1+i)^3]}}} 1.$$

One's first inclination is to truncate the sum on d use Bombieri–Vinogradov; but the weights $\phi(d)$ complicate matters.

One can carry this out with a **severe** truncation, going only up to $(\log x)^A$, and use B–V to get $\gg x\log\log x/\log x$ (Felix and Murty), with an arbitrarily large implied constant.

Rather than try to bound

$$\frac{1}{2}\sum_{d\le\sqrt{x}+1}\phi(d)\sum_{\substack{N(\pi)\le x\\ N(\pi)\text{ prime},\equiv 1 \pmod 4\\ \pi\equiv 1 \pmod{[d,(1+i)^3]}}} 1$$

from below using an average result, we use a result about **most** individual progressions.

Specifically, using work of Weiss — who proved a generalization of Linnik's theorem for algebraic number fields — we show that if d is not divisible by a certain exceptional modulus, then we get a lower bound on the inner sum of the correct order for d up to some small power of x. This is enough.

PART II: TORSION OF ELLIPTIC CURVES OVER NUMBER FIELDS

According to the Mordell–Weil theorem, if E is an elliptic curve over a number field F, then

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

where $E(F)[\mathrm{tors}]$ is a finite abelian group.

Question

Let E be an elliptic curve over a number field F. What can we say about $E(F)[\mathrm{tors}]$?

From Mazur to Merel

Theorem (Mazur's torsion theorem, 1977)

For an elliptic curve $E_{/\mathbb{Q}}$, there are only finitely many possibilities for $E(\mathbb{Q})[\mathrm{tors}]$: It is either $\mathbb{Z}/n\mathbb{Z}$ for some $n = 1, 2, \ldots, 10, 12$, or it is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$ for $n = 1, 2, 3$, or 4.

From Mazur to Merel

Theorem (Mazur's torsion theorem, 1977)

For an elliptic curve $E_{/\mathbb{Q}}$, there are only finitely many possibilities for $E(\mathbb{Q})[\mathrm{tors}]$: It is either $\mathbb{Z}/n\mathbb{Z}$ for some $n = 1, 2, \ldots, 10, 12$, or it is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$ for $n = 1, 2, 3$, or 4.

If E is an elliptic curve over a quadratic number field, then $E(F)[\mathrm{tors}]$ is isomorphic to one of 26 possible groups. This follows from work of Kamienny, Kenku, and Momose, completed in 1992.

From Mazur to Merel

We do not have a provably complete list of all possible groups of the form $E(F)[\mathrm{tors}]$, for elliptic curves E over cubic number fields.

But we do know that only finitely many groups appear. The following **uniform boundedness theorem** is due to Merel.

Theorem (Merel, 1994)

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

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

How bounded is uniform boundedness?

One can in bound $B(d)$ explicitly. Since $E(F)[\mathrm{tors}]$ is a finite abelian group of rank two, 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

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

How bounded is uniform boundedness?

One can in bound $B(d)$ explicitly. Since $E(F)[\mathrm{tors}]$ is a finite abelian group of rank two, 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

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

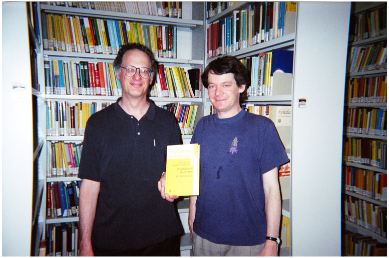
Conjecture

$B(d)$ is bounded by a polynomial in d.

Conjecture

$B(d)$ is bounded by a polynomial in d.

This is quite a ways from the known results! However, for certain classes of curves, this conjecture is a theorem.



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

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

Now you CM, now you don't (or vice versa)

A subclass of elliptic curves with integral *j*-invariant is the class of elliptic curves with complex multiplication. For CM curves, it is conjectured that one can do better.

Conjecture (Clark, Cook, Stankiewicz)

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

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

for an absolute constant C.

Number theory or lumber 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,

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

Thus, the conjecture — if true — is best possible, up to the value of the implied constant.

When F does not contain the CM field, the conjecture follows from work of Silverberg and Prasad–Yogananda.

Theorem (Clark, P.)

The conjecture holds if E has CM by the maximal order of an imaginary quadratic field.

We are optimistic that we will soon have a proof of the full conjecture.

[**Added after this talk was given**: We now have a proof of the full conjecture!]

Some fragments of the proof

I can say a few words about the proof, with special attention paid to the analytic number theory bits. Let's say E is an elliptic curve over a degree d number field F with CM by the maximal order $\mathcal{O}_K$ of the imaginary quadratic field K.

Some fragments of the proof

I can say a few words about the proof, with special attention paid to the analytic number theory bits. Let's say E is an elliptic curve over a degree d number field F with CM by the maximal order $\mathcal{O}_K$ of the imaginary quadratic field K.

From the results already mentioned, we can assume $F \supset K$.

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

$$\Phi(\mathfrak{a}) \leq \frac{6d}{h_K},$$

where 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:

$$\Phi(\mathfrak{a}) \leq \frac{6d}{h_K},$$

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. We have $\phi(a) \gg a/\log\log a$, for $a \geq 3$. Inverting, $a \ll \phi(a)\log\log\phi(a)$ for large a.

We have:

$$\Phi(\mathfrak{a}) \leq \frac{6d}{h_K},$$

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. We have $\phi(a) \gg a/\log\log a$, for $a \geq 3$. Inverting, $a \ll \phi(a)\log\log\phi(a)$ for large a.

For any *fixed* quadratic field K, there is no difficulty generalizing this argument. We have $\Phi(\mathfrak{a}) \gg_K N(\mathfrak{a})/\log\log N(\mathfrak{a})$ for each integral ideal $\mathfrak{a}$ of norm ≥ 3.

This is encouraging. If we had

$$\Phi(\mathfrak{a}) \gg_K N(\mathfrak{a}) / \log\log N(\mathfrak{a})$$

without the K-dependence, then we could invert our upper bound and get that

$$N(\mathfrak{a}) \ll \frac{d}{h_K} \log\log \frac{d}{h_K}.$$

The left-hand side is $\#E(F)[\mathrm{tors}]$ and the right-hand side is $O(d \log\log d)$.

This is encouraging. If we had

$$\Phi(\mathfrak{a}) \gg_K N(\mathfrak{a})/\log\log N(\mathfrak{a})$$

without the K-dependence, then we could invert our upper bound and get that

$$N(\mathfrak{a}) \ll \frac{d}{h_K}\log\log\frac{d}{h_K}.$$

The left-hand side is $\#E(F)[\mathrm{tors}]$ and the right-hand side is $O(d\log\log d)$.

Unfortunately, the above estimate doesn't hold uniformly in K! All is not lost, however. To get $O(d\log\log d)$ at the end, we only need

$$\Phi(\mathfrak{a}) \gg \frac{N(\mathfrak{a})}{h_K\log\log N(\mathfrak{a})}.$$

We only need

$$\Phi(\mathfrak{a}) \gg \frac{N(\mathfrak{a})}{h_K \log\log N(\mathfrak{a})}.$$

By an elementary argument, this reduces to showing the following.

Proposition

Let K be an imaginary quadratic field with discriminant Δ. Let $\chi(\cdot) = (\Delta|\cdot)$ be the associated quadratic character. Then

$$\prod_{p \le z} \left(1 - \frac{\chi(p)}{p}\right) \ge \frac{C}{h_K},$$

for some positive absolute constant C, and all $z \ge 2$.

Proposition

Let K be an imaginary quadratic field with discriminant Δ. Let $\chi(\cdot) = (\Delta|\cdot)$ be the associated quadratic character. Then

$$\prod_{p \le z} \left(1 - \frac{\chi(p)}{p}\right) \ge \frac{C}{h_K},$$

for some positive absolute constant C, and all $z \ge 2$.

When working on the paper, we came up with two proofs of the proposition. The first is extremely short and elementary, and gives

$$\ge \frac{C'}{\log|\Delta|}.$$

Since $h_K \approx |\Delta|^{1/2}$ (by Siegel), we win by a lot with this proof.

However, this argument does not lead to an effective constant, since we do not know **effectively** that

$$h_K \gg \log|\Delta|.$$

(Goldfeld–Gross–Zagier gets tantalizingly close, but doesn't quite reach this.)

Our second proof gets exactly the claimed estimate, without any "extra winnings". But the constant is effective!

The second proof uses the class number formula for h_K, which involves a factor of $L(1, \chi)$. Replacing $L(1, \chi)$ with its Euler product, proving the previous proposiiton amounts to showing that

$$\prod_{p>z}\left(1 - \frac{\chi(p)}{p}\right) \leq C''\sqrt{|\Delta|},$$

for some absolute constant C'' and all $z \geq 2$.

The second proof uses the class number formula for h_K, which involves a factor of $L(1,\chi)$. Replacing $L(1,\chi)$ with its Euler product, proving the previous proposiiton amounts to showing that

$$\prod_{p>z}\left(1-\frac{\chi(p)}{p}\right)\leq C''\sqrt{|\Delta|},$$

for some absolute constant C'' and all $z\geq 2$.

The primes up to $\exp(\sqrt{|\Delta|})$ make a contribution of $\ll \sqrt{|\Delta|}$, by Mertens' theorem.

Once $p>\exp(\sqrt{|\Delta|})$, we use that $\sum \chi(p)$ displays enough cancelation to make this part of the product $\ll 1$. Here we need that any Siegel zero, if it exists, is at least $c/\sqrt{|\Delta|}$ away from 1. (This is slightly more than what follows immediately from the class number formula, and is due to Goldfeld–Schinzel.)

Max to min

I want to close by mentioning a theorem with Abbey Bourdon and Pete L. Clark describing when we see the minimal number of possibilities for torsion.

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.

Each of these six **Olson groups** is realizable in *every degree d*. (In fact, if a group is realizable in degree d, one can show it is realizable in every degree that is a multiple of d.)

So the "least that can happen" in degree d is if the Olson groups are the only possible torsion subgroups of CM curves.

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.

Each of these six **Olson groups** is realizable in *every degree d*. (In fact, if a group is realizable in degree d, one can show it is realizable in every degree that is a multiple of d.)

So the "least that can happen" in degree d is if the Olson groups are the only possible torsion subgroups of CM curves.

Theorem (Bourdon, Clark, P.)

This "minimal behavior" occurs for a well-defined, positive proportion of all degrees d.

A classification of Olson degrees

Proposition

If d does not have this "minimal behavior" – i.e., there is a number field F of degree d and a CM elliptic curve $E_{/F}$ with $E(F)[\mathrm{tors}]$ not an Olson group – then either d is even or d is a multiple of

$$\frac{\ell - 1}{2} h_{\mathbb{Q}(\sqrt{-\ell})} \qquad (*)$$

for some prime $\ell \equiv 3 \pmod 4$ with $\ell > 3$. The converse holds as well.

The proposition follows from general facts about "sets of multiples", using that the sum on ℓ of the reciprocals of the numbers in (*) converges.

Of course, one sometimes gets more than the Olson groups. But usually not ‘much’ more.

Theorem (Bourdon, Clark, P.)

Let $\epsilon > 0$. Then there is a constant T_ϵ such that for all d outside of a certain set of upper density at most ϵ, every possible torsion subroup one sees has size at most T_ϵ.

Of course, one sometimes gets more than the Olson groups. But usually not ‘much’ more.

Theorem (Bourdon, Clark, P.)

Let $\epsilon > 0$*. Then there is a constant* T_ϵ *such that for all d outside of a certain set of upper density at most* ϵ*, every possible torsion subroup one sees has size at most* T_ϵ*.*

How is this proved? Very roughly speaking (and lying slightly), one shows that if *E* has a large torsion subgroup, then probably *d* is divisible by a large shifted prime $\ell - 1$. (This follows from the ray class field containment that came up a few slides before.)

Now we use a beautiful 1980 result of Erdős and Wagstaff: Very few positive integers have a large divisor of the form $\ell - 1$.

THANK YOU!