Uniform Boundedness in Terms of Ramification

Álvaro Lozano-Robledo

Department of Mathematics
University of Connecticut

2013 Maine-Québec Number Theory Conference
University of Maine, Orono, October 6th, 2013

Let F be a number field, and let E/F be an elliptic curve over F.

Theorem (Mordell-Weil)

$E(F)$ is a finitely generated abelian group.

In particular,

$$E(F) \cong E(F)_{\text{tors}} \oplus \mathbb{Z}^{R_{E/F}},$$

where the torsion subgroup, $E(F)_{\text{tors}}$, is finite and $R_{E/F} \geq 0$.

Question

For a fixed F, how large can $E(F)_{tors}$ be for an arbitrary curve E/F?

Theorem (Mazur, 1977)

Let $E/\mathbb{Q}$ be an elliptic curve. Then

$$E(\mathbb{Q})_{tors} \simeq \begin{cases} \mathbb{Z}/M\mathbb{Z} & \text{with } 1 \leq M \leq 10 \text{ or } M = 12, \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2M\mathbb{Z} & \text{with } 1 \leq M \leq 4. \end{cases}$$

Moreover, each group occurs for infinitely many $j(E) \in \mathbb{Q}$.

Theorem (Kenku and Momose, 1988; Kamienny, 1992)

Let $F/\mathbb{Q}$ be a quadratic field and let E/F be an elliptic curve. Then

$$E(F)_{tors} \simeq \begin{cases} \mathbb{Z}/M\mathbb{Z} & \text{with } 1 \leq M \leq 16 \text{ or } M = 18, \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2M\mathbb{Z} & \text{with } 1 \leq M \leq 6, \text{ or} \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3M\mathbb{Z} & \text{with } M = 1 \text{ or } 2, \text{ or} \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}. \end{cases}$$

Each group occurs for infinitely many $j(E)$, with $[\mathbb{Q}(j(E)) : \mathbb{Q}] \leq 2$.

The Uniform Boundedness Conjecture

The Uniform Boundedness ~~Conjecture~~ Theorem

Theorem (Merel, 1996)

Let F be a number field of degree $[F : \mathbb{Q}] = d > 1$. There is a number $B(d) > 0$ such that $|E(F)_{tors}| \leq B(d)$ **for all** *elliptic curves E/F.*

Definition

We define $T(d)$ as the supremum of $|E(F)_{\text{tors}}|$, over all number fields F of degree $[F : \mathbb{Q}] \leq d$, and elliptic curves E/F.

For instance, $T(1) = 16$, and $T(2) = 24$.

Folklore Conjecture (see Clark, Cook, Stankewicz, 2013)

There is a constant $C > 0$ such that

$$T(d) \leq C \cdot d \cdot \log\log d \quad \text{for all} \quad d \geq 3.$$

Folklore Conjecture (see Clark, Cook, Stankewicz, 2013)

There is a constant $C > 0$ such that

$$T(d) \leq C \cdot d \cdot \log\log d \quad \text{for all} \quad d \geq 3.$$

Highlights about $T(d)$:

- Flexor and Oesterlé:
  - If E/F has at least one place of additive reduction, then
    $$|E(F)_{\text{tors}}| \leq 48d.$$
  - If it has at least two places of additive reduction, then
    $$|E(F)_{\text{tors}}| \leq 12.$$
- Hindry and Silverman: If E/F has everywhere good reduction then
  $$|E(F)_{\text{tors}}| \leq 1977408 \cdot d \log d.$$

Related Question

What is the best bound for a prime power order that one can hope for?

Definition

For each $n \geq 1$, we define $S^n(d)$ as the set of primes p for which there exists a number field F of degree $\leq d$ and an elliptic curve E/F such that $E(F)_{\text{tors}}$ contains a point of order p^n.

Examples:

- $S^1(1) = \{2, 3, 5, 7\}$, $S^2(1) = \{2, 3\}$, $S^3(1) = 2$, and $S^n(1) = \emptyset$ for all $n \geq 4$.
- $S^1(2) = \{2, 3, 5, 7, 11, 13\}$, $S^2(2) = \{2, 3\}$, $S^3(2) = S^4(2) = \{2\}$, and $S^n(2) = \emptyset$ for all $n \geq 5$.

Definition

For each $n \geq 1$, we define $S^n(d)$ as the set of primes p for which there exists a number field F of degree $\leq d$ and an elliptic curve E/F such that $E(F)_{\text{tors}}$ contains a point of order p^n.

Highlights about $S(d)$:

$S^1(1) = \{2,3,5,7\}$,	Mazur, 1977
$S^1(2) = \{2,3,5,7,11,13\}$,	Kamienny, Mazur, 1992
If $p \in S^1(d)$ and $d > 1$, then $p \leq d^{3d^2}$,	Merel, 1996
If $p \in S^1(d)$, then $p \leq (3^{d/2}+1)^2$,	Oesterlé, 1996
If $p \in S^n(d)$, then $p^n \leq 129(5^d - 1)(3d)^6$,	Parent, 1999
$S^1(3) = \{2,3,5,7,11,13\}$,	Parent, 2003
$S^1(4) = \{2,3,5,7,11,13,17\}$,	
$S^1(5) = \{2,3,5,7,11,13,17,19\}$,	Derickx, Kamienny,
$S^1(6) \subseteq \{2,3,5,7,11,13,17,19,37,73\}$.	Stein, Stoll, 2012

Theorem (Silverberg, 1988; Prasad-Yogananda, 2001)

Let F be a number field of degree d, and let E/F be an elliptic curve with CM by an order $\mathcal{O}$ in the imaginary quadratic field K. Let $w = w(\mathcal{O}) = |\mathcal{O}^\times|$ (so $w = 2, 4$ or 6) and let m be the maximal order of an element of $E(F)_{tors}$. Then:

1. $\varphi(m) \leq w \cdot d$.
2. *If* $K \subseteq F$, *then* $\varphi(m) \leq \frac{w}{2} \cdot d$.
3. *If* $K \not\subseteq F$, *then* $\varphi(|E(F)_{tors}|) \leq w \cdot d$.

Thus, if E/F has CM and $E(F)$ has a pt. of order p^n, then $\varphi(p^n) \leq 6d$.

Definition

We define $S^n_{\mathrm{CM}}(d)$ if we restrict our attention to elliptic curves E/F with CM, and F as above.

Silverberg, Prasad, Yogananda: if $p \in S^n_{\mathrm{CM}}(d)$, then $\varphi(p^n) \leq 6d$.

Folklore Conjecture

There is a constant $C > 0$ such that

$$T(d) \leq C \cdot d \cdot \log\log d \quad \text{for all} \quad d \geq 3.$$

We propose instead two conjectures:

Conjecture 1

There is a constant C_2 such that if $p \in S^n(d)$, then

$$\varphi(p^n) \leq C_2 \cdot d, \text{ for all } d \geq 1.$$

If $p \in S^n_{\mathrm{CM}}(d)$, then $\varphi(p^n) \leq 6d$, so the conjecture is true for CM curves, and $C_2 = 6$.

As advertised in the title, our results depend on ramification indices.

Definition

Let p be a prime, and let F/L be an extension of number fields. We define $e_{\min}(p, F/L)$ as the smallest ramification index $e(\mathfrak{P}|\wp)$ for a prime $\mathfrak{P}$ of $\mathcal{O}_F$ over a prime $\wp$ of $\mathcal{O}_L$ lying above the rational prime p. And similarly define $e_{\max}(p, F/L)$.

Conjecture 2

There is a constant C_3 such that if $p \in S^n(d)$ for a prime p and a curve E/F, with $F/\mathbb{Q}$ of degree $\leq d$, then

$$\varphi(p^n) \leq C_3 \cdot e_{\max}(p, F/\mathbb{Q}) \leq C_3 \cdot d.$$

Folklore Conjecture

There is $C > 0$ s.t. $T(d) \leq C \cdot d \cdot \log\log d$ for all $d \geq 3$.

Conjecture 1

There is $C_2 > 0$ s.t. if $p \in S^n(d)$, then $\varphi(p^n) \leq C_2 \cdot d$ for all $d \geq 1$.

Conjecture 2

There is $C_3 > 0$ s.t. if $p \in S^n(d)$ for some E/F with $[F : \mathbb{Q}] \leq d$, then

$$\varphi(p^n) \leq C_3 \cdot e_{\max}(p, F/\mathbb{Q}) \leq C_3 \cdot d.$$

Silverberg, Prasad and Yogananda $\Longrightarrow$ Conjecture 1 for CM curves.

Theorem (L-R., 2013)

Let F be a number field with degree $[F : \mathbb{Q}] = d \geq 1$, and let p be a prime such that $p \in S^n_{CM}(d)$, for some E/F with CM. Then,

$$\varphi(p^n) \leq 12 \cdot e_{max}(p, F/\mathbb{Q}) \leq 12d.$$

Let us further "decorate" our notation... Let L be a number field.

Definition

- Let $S_L^n(d)$ be the set of primes p, where p is a prime for which there exists a finite extension F/L of number fields with $[F:\mathbb{Q}] \leq d$, and an elliptic curve E/L, such that $E(F)_{\text{tors}}$ contains a point of exact order p^n.
- If $\Sigma \subseteq L$, we define $S_L^n(d,\Sigma)$, as before, except that we only consider elliptic curves E/L with $j(E) \notin \Sigma$.

Examples:

- $S_{\mathbb{Q}}^1(1) = S^1(1) = \{2,3,5,7\}$.
- $S_{\mathbb{Q}}^1(2) = \{2,3,5,7\}$, $S_{\mathbb{Q}}^2(2) = \{2,3\}$, $S_{\mathbb{Q}}^3(2) = \{2\}$, $S_{\mathbb{Q}}^n(2) = \emptyset$ for all $n \geq 4$.
- $S_{\mathbb{Q}}^1(3) = \{2,3,5,7,13\}$, $S_{\mathbb{Q}}^2(3) = \{2,3\}$, $S_{\mathbb{Q}}^3(3) = \{2\}$, $S_{\mathbb{Q}}^n(3) = \emptyset$ for all $n \geq 4$.

Theorem (L-R., 2011)

Let $S^1_{\mathbb{Q}}(d)$ be the set of primes defined above. Then:

- $S^1_{\mathbb{Q}}(d) = \{2, 3, 5, 7\}$ *for* $d = 1$ *and* 2;
- $S^1_{\mathbb{Q}}(d) = \{2, 3, 5, 7, 13\}$ *for* $d = 3$ *and* 4;
- $S^1_{\mathbb{Q}}(d) = \{2, 3, 5, 7, 11, 13\}$ *for* $d = 5$, 6, *and* 7;
- $S^1_{\mathbb{Q}}(d) = \{2, 3, 5, 7, 11, 13, 17\}$ *for* $d = 8$;
- $S^1_{\mathbb{Q}}(d) = \{2, 3, 5, 7, 11, 13, 17, 19\}$ *for* $d = 9$, 10, *and* 11;
- $S^1_{\mathbb{Q}}(d) = \{2, 3, 5, 7, 11, 13, 17, 19, 37\}$ *for* $12 \leq d \leq 20$.
- $S^1_{\mathbb{Q}}(d) = \{2, 3, 5, 7, 11, 13, 17, 19, 37, 43\}$ *for* $d = 21$.

Moreover,

- *There is a conjectural formula for* $S^1_{\mathbb{Q}}(d)$ *for all* $d \geq 1$, *which is valid for all* $1 \leq d \leq 42$, *and would follow from a positive answer to Serre's uniformity question.*
- *If* $p \in S^1_{\mathbb{Q}}(d)$ *with* $p \geq 11$ *and* $p \neq 13$, *then* $\varphi(p) \leq 2d$.

Again, $S_L^n(d) = \{p :$ there is E/L and F/L such that $L \subseteq F, [F : \mathbb{Q}] \leq d,$ and there is a point $R \in E(F)$ of order $p^n\}$.

Theorem (L-R.,2013)

If $p > 2$ and $p \in S_{\mathbb{Q}}^n(d)$ for some E/F, then

$$\varphi(p^n) \leq 222 \cdot e_{max}(p, F/\mathbb{Q}) \leq 222 \cdot d.$$

Theorem (L-R.,2013)

Let L be a number field, and let $p > 2$ be a prime with $p \in S_L^n(d)$ for some E/F. Then, there is a constant C_L such that

$$\varphi(p^n) \leq C_L \cdot e_{max}(p, F/\mathbb{Q}) \leq C_L \cdot d.$$

Moreover, there is a computable finite set Σ_L such that if $p \in S_L^n(d, \Sigma_L)$, then

$$\varphi(p^n) \leq 588 \cdot e_{max}(p, F/\mathbb{Q}) \leq 588 \cdot d.$$

Example

Let $E/\mathbb{Q}$ be '121B1', defined by:

$$y^2 + y = x^3 - x^2 - 7x + 10.$$

Let $\zeta = \zeta_{11}$ be a primitive 11th root of unity. Then:

$$R = (\zeta^8 + \zeta^7 - \zeta^6 - \zeta^5 + \zeta^4 + \zeta^3 + 2,\ 2\zeta^9 - \zeta^8 - 2\zeta^7 - 2\zeta^4 - \zeta^3 + 2\zeta^2 - 4)$$

is a point of $E(\mathbb{Q}(\zeta_{11}))$ of order 11. Notice that the coordinates $x = x(R)$ and $y = y(R)$ are real! So R is defined over $\mathbb{Q}(\zeta_{11})^+$. Hence

$$\varphi(11) = 2e(\Omega_R|(11)),$$

for the prime Ω_R above 11.

Example

The elliptic curve $E/\mathbb{Q}$, with $j = 23^3/(2 \cdot 13)$, defined by

$$y^2 + xy + y = x^3$$

admits a $\mathbb{Q}$-rational isogeny of degree 9. The curve E has a point of order 9 defined over a Galois extension $F/\mathbb{Q}$ of degree 3, which ramifies at 13 but not at 3.

Example

The elliptic curve $E/\mathbb{Q}$, with $j = 2^6 \cdot 1439^3/71$, defined by

$$y^2 = x^3 - x^2 - 959x - 11117$$

admits a $\mathbb{Q}$-rational isogeny of degree 25. The curve E has a point of order 25 defined over a Galois extension $F/\mathbb{Q}$ of degree 20, which ramifies at 2 and 71 but not at 5.

Results on L-rational isogenies.

Theorem (Momose; Larson, Vaintrob)

Let L be a number field, and let $\mathcal{S}_L$ be the set of rational primes such that there is an E/L with a L-rational isogeny of degree p.

1. *(Momose, 1995) Suppose that $L/\mathbb{Q}$ is quadratic, but not imaginary of class number 1. Then, $\mathcal{S}_L$ is finite.*
2. *(Larson, Vaintrob, 2012) Assume GRH. The set $\mathcal{S}_L$ is finite if and only if L does not contain the Hilbert class field of an imaginary quadratic field F (i.e., if and only if there are no elliptic curves with CM defined over L). Moreover, if $\mathcal{S}_L$ is finite, then there is an effective computable constant P_L such that if $p \in \mathcal{S}_L$, then $p \leq P_L$.*

Uniform Boundedness in terms of Ramification

- Suppose L doesn't contain any H.c.f. of a quad. imag. field.
- Let $\mathcal{S}_L$ be the set of primes given by Momose, or Larson-Vaintrob.
- Let $a(L,p) \geq 1$ be the smallest integer such that $X_0(p^a)$ is of genus ≥ 2, or $X_0(p^a)$ is of genus 1 but $X_0(p^a)(L)$ is finite.
- Let $\Sigma(L,p) \subset L$ be the finite set of j-invariants corresponding to the non-cuspidal L-rational points on $X_0(p^{a(L,p)})$.
- For each $j_0 \in \Sigma(L,p)$ let $a = a(p,j_0)$ be the least positive integer a such that any curve E/L with $j(E) = j_0$ does not admit L-rational isogenies of degree p^a.
- Let $A(L,p) = \max\{a(L,p), a(p,j_0) : j_0 \in \Sigma(L,p)\}$.
- Define $C_L = 12 \cdot \max\{p^{A(L,p)-1} : p \in \mathcal{S}_L\}$.

Then, there is a constant $1 \leq C(E/L,\wp) \leq 12e(\wp|p)$ such that:

$$\begin{aligned}\varphi(p^n) &\leq \gcd(\varphi(p^n), c(E/L,\wp)\cdot p^{A(L,p)-1}) \cdot e(\Omega_R|\wp)\\ &\leq C_L \cdot e(\wp|p)e(\Omega_R|\wp)\\ &\leq C_L \cdot e_{\max}(p, F/\mathbb{Q}) \leq C_L \cdot [F:\mathbb{Q}].\end{aligned}$$

alozano@math.uconn.edu

http://homepage.uconn.edu/alozano