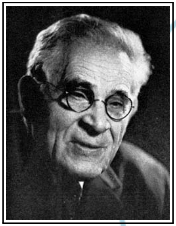
Progress in the Classification of Torsion Subgroups of Elliptic Curves

Caleb McWhorter
Syracuse University

44th Annual New York State Regional Graduate Mathematics Conference

March 23, 2019



1888–1972

"Mathematicians have been familiar with very few questions for so long a period with so little accomplished in the way of general results, as that of finding the rational [points on elliptic curves]."

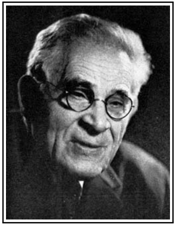
– L.J. Mordell, 1922

Theorem (Mordell, 1922)

Let $E/\mathbb{Q}$ be an elliptic curve. Then the group of rational points on E, denoted $E(Q)$ is a finitely generated abelian group. In particular,

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})_{tors},$$

where $r \geq 0$ is the rank and $E(\mathbb{Q})_{tors}$ is the set of points with finite order.

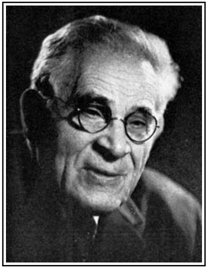


Louis J. Mordell
1888–1972

Theorem (Mordell-Weil-Néron, 1952)

Let K be a field that is finitely generated over its prime field and A/K be an abelian variety. Then the group of K-rational points on A, denoted $A(K)$, is a finitely generated abelian group. In particular,

$$A(K) \cong \mathbb{Z}^{r_{A/K}} \oplus A(K)_{tors}$$



Louis J. Mordell
1888–1972

André Weil
1906–1998

André Néron
1922–1985

Structure of the Torsion Subgroup

$$E(K)_{\text{tors}} \cong \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/mn\mathbb{Z}$$

$$E[n] \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$$

Theorem (Levi-Ogg Conjecture; Mazur, 1977)

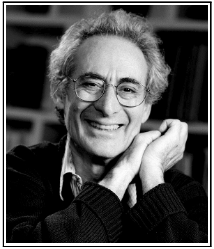
If $E/\mathbb{Q}$ is a rational elliptic curve, then $E(\mathbb{Q})_{tors}$ is isomorphic to precisely one of the following:

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & n = 1, 2, \ldots, 10, 12 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & n = 1, \ldots, 4 \end{cases}$$

Moreover, each possibility occurs infinitely often.

Beppo Levi
1875–1961

Andrew Ogg
1934 –



Barry Mazur
1937 –

Question

What finitely generated abelian groups arise from abelian varieties over global fields?

Question

What torsion subgroups arise for elliptic curves E/K, where K is a number field of degree d?

With massive loss of generality, let $d = 2$*.*

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

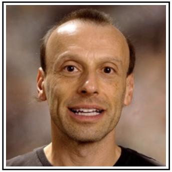
Let $K/\mathbb{Q}$ be a quadratic number field and E/K be an elliptic curve. Then $E(K)_{tors}$ is isomorphic to precisely one of the following:

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & n = 1, 2, \ldots, 16, 18 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & n = 1, \ldots, 6 \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3n\mathbb{Z}, & n = 1, 2 \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \end{cases}$$

Moreover, each possibility occurs infinitely often.

Monsur Kenku

Fumiyuki Momose



Sheldon Kamienny

Theorem (Jeon,Kim,Schweizer, 2004; Etropolski-Morrow-Zureick Brown; Derickx, 2016)

Let $K/\mathbb{Q}$ be a cubic number field and E/K be an elliptic curve. Then $E(K)_{tors}$ is isomorphic to precisely one of the following:

$$\begin{cases} \mathbb{Z}/n\mathbb{Z} & n = 1, 2, \ldots, 16, 18, 20, 21 \\ \mathbb{Z}/2n\mathbb{Z} & n = 1, \ldots, 7 \end{cases}$$

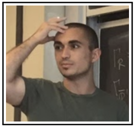
Each of these possibilities occurs infinitely many times except $\mathbb{Z}/21\mathbb{Z}$.


Jeon


Kim


Schweizer


Etropolski


Morrow


Z-B.


Derickx

Theorem (Jeon, Kim, Park, 2006)

Let $K/\mathbb{Q}$ be a quartic number field and E/K be an elliptic curve. Then the possible torsion subgroups $E(K)_{tors}$ appearing infinitely often are precisely:

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & n = 1, 2, \ldots, 18, 20, 21, 22 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & n = 1, \ldots, 9 \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3n\mathbb{Z}, & n = 1, 2, 3 \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4n\mathbb{Z}, & n = 1, 2 \\ \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z} \\ \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \end{cases}$$

Daeyeol Jeon

Chang Kim

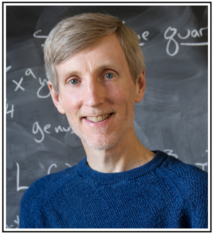
Eui-Sung Park

Theorem (Derickx, Sutherland, 2016)

Let $K/\mathbb{Q}$ be a quintic number field and E/K be an elliptic curve. Then the possible torsion subgroups $E(K)_{tors}$ appearing infinitely often are precisely:

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & n = 1, \ldots, 22, 24, 25 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & n = 1, \ldots, 8 \end{cases}$$

Maarten Derickx



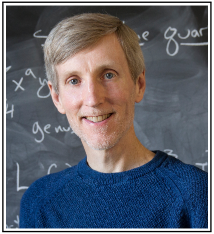
Drew Sutherland

Theorem (Derickx, Sutherland, 2016)

Let $K/\mathbb{Q}$ be a sextic number field and E/K be an elliptic curve. Then the possible torsion subgroups $E(K)_{tors}$ appearing infinitely often are precisely:

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & n = 1, \ldots, 30; n \neq 23, 25, 29 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & n = 1, \ldots, 10 \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3n\mathbb{Z}, & n = 1, \ldots, 4 \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4n\mathbb{Z}, & n = 1, 2 \\ \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \end{cases}$$

Maarten Derickx



Drew Sutherland

Theorem (Clark, Corn, Rice, Stankewicz; 2013)

Let K be a number field of degree $d = 1, 2, \ldots, 13$ and E/K be an elliptic curve with CM. Then all possible torsion subgroups are given, and an algorithm to compute the list.

Pete Clark

Patrick Corn

Alex Rice

James Stankewicz

What if you restrict to rational elliptic curves?

Definition (Isogeny)

Let E_1, E_2 be elliptic curves. An isogeny from E_1 to E_2 is a morphism $\phi : E_1 \to E_2$ with $\phi(\mathcal{O}) = \mathcal{O}$. If $|\ker \phi| = n$, we say ϕ is an n-isogeny.

Definition (Isogeny)

Let E_1, E_2 be elliptic curves. An isogeny from E_1 to E_2 is a morphism $\phi : E_1 \to E_2$ with $\phi(\mathcal{O}) = \mathcal{O}$. If $|\ker \phi| = n$, we say ϕ is an n-isogeny.

Theorem (Fricke, Kenku, Klein, Kubert, Ligozat, Mazur, Ogg, et al.)

If $E/\mathbb{Q}$ has an n-isogeny over $\mathbb{Q}$, then

$$n \in \{1, 2, \ldots, 19, 21, 25, 27, 37, 43, 67, 163\}.$$

If E does not have CM, then $n \leq 18$ or $n \in \{21, 25, 37\}$.

Theorem (Rouse,Zureick-Brown, 2015)

Let $E/\mathbb{Q}$ be a rational elliptic curve without CM. Then the index of $\rho_{E,2^\infty}(\mathrm{Gal}(\overline{\mathbb{Q}}/Q))$ divides 64 or 96, and all such indices occur. Furthermore, the image of $\rho_{E,2^\infty}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ is the inverse image in $\mathrm{GL}_2(\mathbb{Z}_2)$ of the image of $\rho_{E,32}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$.

Jeremy Rouse

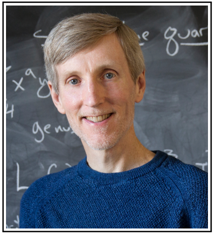
David Zureick-Brown

Remark

They also enumerate all 1,208 possibilities and find their rational points.

Theorem (Sutherland, Zywina, 2016)

Up to conjugacy, there are 248 open subgroups of $\mathrm{GL}_2(\hat{\mathbb{Z}})$ of prime power level satisfying $-I \in G$ and $\det G = \hat{\mathbb{Z}}^\times$ for which X_G has infinitely many rational points. Of these 248 groups, there are 220 of genus 0 and 28 of genus 1.



Drew Sutherland

David Zywina

A bit of notation

$$\Phi_{\mathbb{Q}}(d) := \{\text{Set of Iso. Classes of } E(K)_{\text{tors}} \colon E_{\mathbb{Q}}(K), [K \colon \mathbb{Q}] = d\}$$

$$\Phi_{\mathbb{Q}}(d) := \{\text{Set of Iso. Classes of } E(K)_{\text{tors}} \colon E_{\mathbb{Q}}(K), [K \colon \mathbb{Q}] = d\}$$

$$S_{\mathbb{Q}}(d) := \{p \text{ prime} \colon \exists\, E_{\mathbb{Q}}(K), p \text{ divides } |E_{\mathbb{Q}}(K)|_{\text{tors}}, [K \colon \mathbb{Q}] \leq d\}$$

What happens to torsion under base extension?

Theorem (Chou,Daniels,González-Jimenez,Lozano-Robledo,Najman,Tornero,et al.)

Let $\mathcal{C}_n$ denote the cyclic subgroup of order n. Then

$$\begin{aligned}
\Phi_{\mathbb{Q}}(2) = &\{\mathcal{C}_n \colon n = 1, 2, \ldots, 10, 12, 15, 16\} \\
&\cup \{\mathcal{C}_2 \oplus \mathcal{C}_{2n} \colon 1, 2, \ldots, 6\} \cup \{\mathcal{C}_3 \oplus \mathcal{C}_3, \mathcal{C}_3 \oplus \mathcal{C}_6, \mathcal{C}_4 \oplus \mathcal{C}_4\} \\
\Phi_{\mathbb{Q}}(3) = &\{\mathcal{C}_n \colon n = 1, 2, \ldots, 10, 12, 13, 14, 18, 21\} \\
&\cup \{\mathcal{C}_2 \oplus \mathcal{C}_{2n} \colon n = 1, 2, 3, 4, 7\} \\
\Phi_{\mathbb{Q}}(4) = &\{\mathcal{C}_n \colon n = 12, \ldots, 10, 12, 13, 15, 16, 20, 24\} \\
&\cup \{\mathcal{C}_2 \oplus \mathcal{C}_{2n} \colon n = 1, 2, \ldots, 6, 8\} \cup \{\mathcal{C}_3 \oplus \mathcal{C}_{3n} \colon n = 1, 2\} \\
&\quad \cup \{\mathcal{C}_4 \oplus \mathcal{C}_{4n} \colon n = 1, 2\} \cup \{\mathcal{C}_5 \oplus \mathcal{C}_5\} \cup \{\mathcal{C}_6 \oplus \mathcal{C}_6\} \\
\Phi_{\mathbb{Q}}(5) = &\{\mathcal{C}_n \colon n = 1, 2, \ldots, 12, 25\} \cup \{\mathcal{C}_2 \oplus \mathcal{C}_{2n} \colon n = 1, 2, 3, 4\} \\
\Phi_{\mathbb{Q}}(6) \supseteq &\{\mathcal{C}_n \colon n = 1, 2, \ldots, 21, 30 \colon n \neq 11, 17, 19, 20\} \\
&\cup \{\mathcal{C}_2 \oplus \mathcal{C}_{2n} \colon n = 1, 2, \ldots, 7, 9\} \\
&\quad \cup \{\mathcal{C}_3 \oplus \mathcal{C}_{3n} \colon n = 1, 2, 3, 4\} \cup \{\mathcal{C}_4 \oplus \mathcal{C}_4, \mathcal{C}_6 \oplus \mathcal{C}_6\}
\end{aligned}$$

$$\Phi_{\mathbb{Q}}(d^*) = \Phi_{\mathbb{Q}}(1)$$

Michael Chou

Harris Daniels

Enrique González-Jiménez

Álvaro Lozano-Robledo

Filip Najman

José Tornero

Theorem (Najman, 2012)

Let $K/\mathbb{Q}$ be a cubic number field and $E/\mathbb{Q}$ be a rational elliptic curve. Then

$$E(F)_{tors} \cong \begin{cases} \mathbb{Z}/n\mathbb{Z}, & n = 1, \ldots, 10, 12, 13, 14, 18, 21 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & n = 1, \ldots, 4, 7 \end{cases}$$

Moreover, the elliptic curve 162B1 over $\mathbb{Q}(\zeta_9)^+$ is the unique rational elliptic curve over a cubic number field with torsion subgroup $\mathbb{Z}/21\mathbb{Z}$.

Filip Najman

Theorem (Chou, 2015)

Let $K/\mathbb{Q}$ be a quartic Galois field and $E/\mathbb{Q}$ be an elliptic curve. Then $E(K)_{tors}$ is isomorphic to one of the following:

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & n = 1, \dots, 10, 12, 13, 15, 16 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & n = 1, \dots, 6, 8 \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3n\mathbb{Z}, & n = 1, 2 \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4n\mathbb{Z}, & n = 1, 2 \\ \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z} & \\ \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} & \end{cases}$$

Michael Chou

Theorem (M.)

Let $K/\mathbb{Q}$ be a nonic Galois field and $E/\mathbb{Q}$ be an elliptic curve. Then $E(K)_{tors}$ is isomorphic to one of the following groups:

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & n = 1, 2, \ldots, 10, 12, 13, \ldots, 16, 18, 19, 21, 25, 27 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & n = 1, \ldots, 7, 9 \end{cases}$$

Caleb McWhorter

Theorem (Mazur, Parent, Derickx, Kammienny, Stein, Stoll, Lozano-Robledo, et al.)

$$\begin{aligned}
S_{\mathbb{Q}}(\{1,2\}) &= \{2,3,5,7\} \\
S_{\mathbb{Q}}(\{3,4\}) &= \{2,3,5,7,13\} \\
S_{\mathbb{Q}}(\{5,6,7\}) &= \{2,3,5,7,11,13\} \\
S_{\mathbb{Q}}(8) &= \{2,3,5,7,11,13\} \\
S_{\mathbb{Q}}(\{9,10,11\}) &= \{2,3,5,7,11,13,17,19\} \\
S_{\mathbb{Q}}(\{12,\ldots,20\}) &= \{2,3,5,7,11,13,17,19,37\} \\
S_{\mathbb{Q}}(21) &= \{2,3,5,7,11,13,17,19,37,43\}
\end{aligned}$$

Remark

Lozano-Robledo computes $S_{\mathbb{Q}}(d)$ for $1 \leq d \leq 21$, and gives a conjecturally formula valid for all $1 \leq d \leq 42$, following from a positive answer to Serre's uniformity question.

Álvaro Lozano-Robledo

Remark

Furthermore, Enrique González-Jiménez and Filip Najman determine all possible prime orders of a point $P \in E(K)_{\text{tors}}$, where $[K : \mathbb{Q}] = d$ for all $d \leq 3\,342\,296$.

Theorem (González-Jiménez, Lozano-Robledo, 2015)

Let $E/\mathbb{Q}$ be an elliptic curve without CM. Let $1 \leq s \leq N$ be fixed integers, and let $T \subseteq E[2^N]$ be a subgroup isomorphic to $\mathbb{Z}/2^s/Z \oplus \mathbb{Z}/2^N\mathbb{Z}$. Then $[\mathbb{Q}(T) \colon \mathbb{Q}]$ is divisible by 2 if $s = N = 2$, and otherwise by $2^{2N+2s-8}$ if $N \geq 3$, unless $s \geq 4$ and $j(E)$ is one of the two values:

$$-\frac{3 \cdot 18249920^3}{17^{16}} \quad or \quad -\frac{7 \cdot 1723187806080^3}{79^{16}}$$

in which case $[\mathbb{Q}(T) \colon \mathbb{Q}]$ is divisible by $3 \cdot 2^{2N+2s-9}$. Moreover, this is best possible in that there are one-parameter families $E_{s,N}(t)$ of elliptic curves over $\mathbb{Q}$ such that for each $s, N \geq 0$ and each $t \in \mathbb{Q}$, and subgroups $T_{s,N} \in E_{s,N}(t)(\overline{\mathbb{Q}})$ isomorphic to $\mathbb{Z}/2^s\mathbb{Z} \oplus \mathbb{Z}/2^N\mathbb{Z}$ such that $[\mathbb{Q}(T_{s,N}) \colon \mathbb{Q}]$ is equal to the bound given above.

What about infinite extensions?

Theorem (Laska, Lorenz, 1985; Fujita, 2005)

Let $E/\mathbb{Q}$ be an elliptic curve. The torsion subgroup $E(\mathbb{Q}(2^\infty))_{tors}$ is finite and is isomorphic to precisely one of the following:

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & n = 1, 3, 5, 7, 9, 15 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & n = 1, \ldots, 6, 8 \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} & \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4n\mathbb{Z}, & n = 1, \ldots, 4 \\ \mathbb{Z}/2n\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & n = 3, 4 \end{cases}$$

Michael Laska

Martin Lorenz

Yasutsugu Fujita

Theorem (Daniels, Lozano-Robledo, Najman, Sutherland, 2017)

Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q}(3^\infty))_{tors}$ is finite and is isomorphic to precisely one of the following:

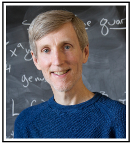
$$\begin{cases} \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & n = 1,2,4,5,7,8,13 \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4n\mathbb{Z}, & n = 1,2,4,7 \\ \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6n\mathbb{Z}, & n = 1,2,3,5,7 \\ \mathbb{Z}/2n\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, & n = 4,6,7,9 \end{cases}$$

All but four of the possibilities occur infinitely often: $(4,28)$, $(6,30)$, $(6,42)$, $(14,14)$, *which occur for only 2, 2, 4, and 1 elliptic curves, respectively.*

Harris Daniels

Álvaro Lozano-Robledo

Filip Najman



Drew Sutherland

What about other types of fields?

Theorem (McDonald, 2017)

Let $K = \mathbb{F}_q(T)$, where $q = p^n$. Let E/K be non-isotrivial. If $p \nmid E(K)_{tors}$, then $E(K)_{tors}$ is one of the following:
$0, \mathbb{Z}/2\mathbb{Z}, \ldots, \mathbb{Z}/10\mathbb{Z}, \mathbb{Z}/12\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}, \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$.
If $p \mid \#E(K)_{tors}$, then $p \leq 11$, and $E(K)_{tors}$ is one of

$$\begin{cases} \mathbb{Z}/p\mathbb{Z}, & p = 2, 3, 5, 7, 11 \\ \mathbb{Z}/2p\mathbb{Z}, & p = 2, 3, 5, 7 \\ \mathbb{Z}/3p\mathbb{Z}, & p = 2, 3, 5 \\ \mathbb{Z}/4p\mathbb{Z}, & p = 2, 3 \\ \mathbb{Z}/5p\mathbb{Z}, & p = 2, 3 \\ \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}, & p = 2 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}, & p = 3 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}, & p = 5 \end{cases}$$

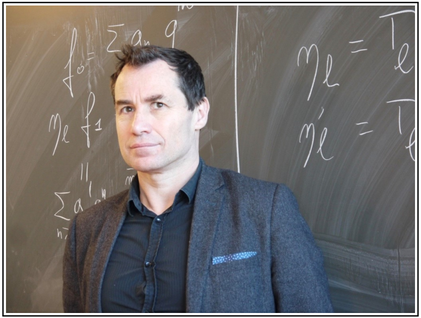
Robert McDonald

What are other questions one might ask?

How large can the torsion be?

Theorem (Merel,1996)

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

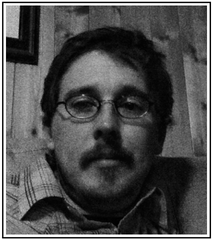


Loïc Merel

Conjecture (Clark, Cook, Stakewicz)

There is a constant C such that $B(d) \leq C\, d \log \log d$ for all $d \geq 3$.

Pete Clark



Brian Cook

James Stankewicz

Theorem (Hindry, Silverman, 1999)

Let K be a field of degree $d \geq 2$ and E/K be an elliptic curve such that $j(E)$ is an algebraic integer. Then we have

$$|E(K)_{tors}| \leq 1\,977\,404 \cdot d \log d$$

Marc Hindry

Joseph Silverman

Theorem (Clark, Pollack, 2015)

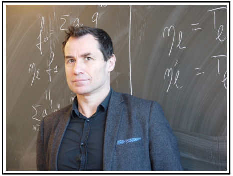
There is an absolute, effective constant C such that for all number fields K of degree $d \geq 3$ and all elliptic curves E/K with CM, we have $|E(K)_{tors}| \leq C\, d \log \log d$.

Pete Clark

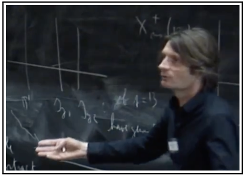
Paul Pollack

Theorem (Merel, 1996)

Let $F/\mathbb{Q}$ be a number field of degree d. If $P \in E(F)$ is a point of exact prime power p^n, then $p \leq 3^{3d^2}$.



Loïc Merel



Pierre Parent

Remark

In 1999, Parent improved this to $p^n \leq 129(5^d - 1)(3d)^6$.

Theorem (Lozano-Robledo, 2013)

Let $K/\mathbb{Q}$ be a number field of degree d and suppose there is an elliptic curve E/K with CM by a full order with a point of order p^n, then

$$\varphi(p^n) \leq 24\, e_{\max}(p, K/\mathbb{Q}) \leq 24\, d$$

Álvaro Lozano-Robledo

What are even more questions one can consider?

Over what fields do torsion subgroups occur?

What happens over other intermediate extensions?

What about other fields?

How 'common' are given torsion subgroups?

What all this means is the number of interesting questions about torsion subgroups of elliptic curves is unbounded…unlike the rank…probably.

Questions?