The New York Math Times

04 OCT 2015

1208 images of 2-adic Galois representations

By PIERRE DE FERMAT

Jeremy Rouse - Wake Forest - and David Zureick-Brown - Emory - have stunned the number theory community with the announcement of a complete classication of all possible images of 2-adic Galois representations attached to the Tate module of an elliptic curve over Q without complex multiplication. In particular, they have shown that there are exactly 1208 possibilities, up to conjugation.

Reuters

International Moose Count Underway

By BOB O'BOBSTON

tion Council, worldwide moose numbers are expected to grow markedly on last year due to the traditional moose strongholds of Canada and the United States, with the larger developing moose ecologies also poised to make gains. The largest percentagege increase in moose will likely come from China", says McRobson, The Chinese government has invested heavily in moose infrastructure over the past decade, and their committment to macrofauna is beginning to pay dividends". Since 2004 China has expanded moose pasture from 1.5% of arable land to nearly 3.648% and moose numbers are expected to rise to 60,000 making China a net moose exporter for the first time. This is good news for neighbouring Mongolia, a barren moose-wasteland whose inhabitents nonetheless have an insatiable desire for the creatures. The increase in Beijing-Ulanbataar trade is anticipated to relieve pressure on the relatively strained Russian suppliers, but increase Mongolia's imbalance of trade with its larger neighbour.

Historically the only competitor to China in the far eastern moose markets has been Singapore but the tiny island nation is set to report a net loss, expecting a decrease of more than five percent on last year's 50,000 moose counted. The head of Singapore's Agency for Agriculture, Jing-Feng Lau, explained to an incredulous Singaporean parliament yesterday that bad weather had contributed

dred million billion.

Europe's rise as an international moose power will slow slightly this year as a response to the European Union's move towards standardising the European moose. Stringent quality controls are holding back the development of the eastern european populations compared to last year when they contributed significantly to europe's strong growth figures. Norway, which is not an EU member but has observer status, strengthed in numbers relative to the Euro area with numbers of Norweigian moose, known locally as elk" expected to rise for the tenth consecutive year, particularly thanks to a strong showing in the last quarter.

As moose season reaches its close, researchers world wide are turning to science in an attempt to boost next year's figures. NASA stunned the scientific community today with the announcment of their discovery that the moon is significantly smaller than previously believed. This conclusion, which is the conclusion of a ten-year collaborative project, will have profound implications for the moose community as the gravitational field is now known to be of the right strength to support moose in orbit.

According to John Johnson, head of the NASA Moon Sizing Experiment the first delivery of moose into low moon orbit could be achieved as early as the third quarter of next year. The technology to nurture moose in

Jeremy Rouse
(Wake Forest)

David Zureick-Brown
(Emory)

Jeremy Rouse
(Wake Forest)

David Zureick-Brown
(Emory)

Let $E/\mathbb{Q}$ be an elliptic curve, and let $T_2(E) = \varprojlim E[2^n]$ be the Tate module. The Galois action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $T_2(E)$ induces

$$\rho_{E,2} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(T_2(E)) \cong \mathrm{GL}(2, \mathbb{Z}_2).$$

Jeremy Rouse
(Wake Forest)

David Zureick-Brown
(Emory)

Theorem

Let $E/\mathbb{Q}$ be an elliptic curve with no CM. Then, there are precisely 1208 possibilities for the image $\rho_{E,2}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$, up to conjugation.

Jeremy Rouse
(Wake Forest)

David Zureick-Brown
(Emory)

Theorem

Let $E/\mathbb{Q}$ be an elliptic curve with no CM. Then, there are precisely 1208 possibilities for the image $\rho_{E,2}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$*, up to conjugation. Further:*

Jeremy Rouse
(Wake Forest)

David Zureick-Brown
(Emory)

Theorem

Let $E/\mathbb{Q}$ be an elliptic curve with no CM. Then, there are precisely 1208 possibilities for the image $\rho_{E,2}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$, up to conjugation. Further:

1. *The representation $\rho_{E,2}$ is defined (at most) modulo 32.*

Jeremy Rouse
(Wake Forest)

David Zureick-Brown
(Emory)

Theorem

Let $E/\mathbb{Q}$ be an elliptic curve with no CM. Then, there are precisely 1208 possibilities for the image $\rho_{E,2}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$, up to conjugation. Further:

1. *The representation $\rho_{E,2}$ is defined (at most) modulo 32.*
2. *The index of the image in $\mathrm{GL}(2, \mathbb{Z}_2)$ is a divisor of 64 or 96, and all such indices occur.*

Jeremy Rouse
(Wake Forest)

David Zureick-Brown
(Emory)

Theorem

Let $E/\mathbb{Q}$ be an elliptic curve with no CM. Then, there are precisely 1208 possibilities for the image $\rho_{E,2}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$, up to conjugation. Further:

1. *The representation $\rho_{E,2}$ is defined (at most) modulo 32.*
2. *The index of the image in $\mathrm{GL}(2, \mathbb{Z}_2)$ is a divisor of 64 or 96, and all such indices occur.*
3. *There exists a database that describes all possible images.*

Example

For instance, let

$$E : y^2 + xy = x^3 + 210x + 900.$$

Then, the 2-adic image is `X2351` in the notation of the RZB database, which is defined modulo 16, and is generated in $\mathrm{GL}(2, \mathbb{Z}/16\mathbb{Z})$ by

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 12 & 1 \end{pmatrix}, \begin{pmatrix} 9 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 14 & 1 \end{pmatrix}, \begin{pmatrix} 5 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 15 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 9 & 0 \\ 8 & 9 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 8 & 1 \end{pmatrix}$$

On the minimal degree of definition of p-primary torsion subgroups of elliptic curves

Álvaro Lozano-Robledo

Department of Mathematics
University of Connecticut

Maine-Québec Number Theory Conference
University of Maine, Orono, ME
October 3-4, 2015

This is joint work with

Enrique González-Jiménez
(Universidad Autónoma de Madrid)

Let $E/\mathbb{Q}$ be an elliptic curve, and let $n \geq 2$. Let $\mathbb{Q}(E[n])$ be the field of definition of all n-torsion points on E.

Question

When is $\mathbb{Q}(E[n]) = \mathbb{Q}(\zeta_n)$*?*

Let $E/\mathbb{Q}$ be an elliptic curve, and let $n \geq 2$. Let $\mathbb{Q}(E[n])$ be the field of definition of all n-torsion points on E.

Question

When is $\mathbb{Q}(E[n]) = \mathbb{Q}(\zeta_n)$? When is $\mathbb{Q}(E[n])/\mathbb{Q}$ an abelian extension?

Let $E/\mathbb{Q}$ be an elliptic curve, and let $n \geq 2$. Let $\mathbb{Q}(E[n])$ be the field of definition of all n-torsion points on E.

Question

When is $\mathbb{Q}(E[n]) = \mathbb{Q}(\zeta_n)$? When is $\mathbb{Q}(E[n])/\mathbb{Q}$ an abelian extension?

Theorem (GJLR, 2015)

- *If $\mathbb{Q}(E[n]) = \mathbb{Q}(\zeta_n)$, then $n = 2, 3, 4, 5$.*
- *If $\mathbb{Q}(E[n])/\mathbb{Q}$ is an abelian extension, then $n = 2, 3, 4, 5, 6, 8$.*

Let $E/\mathbb{Q}$ be an elliptic curve, and let $n \geq 2$. Let $\mathbb{Q}(E[n])$ be the field of definition of all n-torsion points on E.

Question

When is $\mathbb{Q}(E[n]) = \mathbb{Q}(\zeta_n)$? When is $\mathbb{Q}(E[n])/\mathbb{Q}$ an abelian extension?

Theorem (GJLR, 2015)

- *If $\mathbb{Q}(E[n]) = \mathbb{Q}(\zeta_n)$, then $n = 2, 3, 4, 5$.*
- *If $\mathbb{Q}(E[n])/\mathbb{Q}$ is an abelian extension, then $n = 2, 3, 4, 5, 6, 8$.*

- $E_{15a2} : y^2 + xy + y = x^3 + x^2 - 135x - 660$ has $\mathbb{Q}(E[2]) = \mathbb{Q}$,
- $E_{19a1} : y^2 + y = x^3 + x^2 - 9x - 15$ has $\mathbb{Q}(E[3]) = \mathbb{Q}(\zeta_3)$,
- $E_{15a1} : y^2 + xy + y = x^3 + x^2 - 10x - 10$ has $\mathbb{Q}(E[4]) = \mathbb{Q}(\zeta_4)$,
- $E_{11a1} : y^2 + y = x^3 - x^2 - 10x - 20$ has $\mathbb{Q}(E[5]) = \mathbb{Q}(\zeta_5)$,
- $E_{14a1} : y^2 + xy + y = x^3 + 4x - 6$ has $\mathbb{Q}(E[6]) = \mathbb{Q}(\zeta_6, \sqrt{-7})$,
- $E_{15a1} : y^2 + xy + y = x^3 + x^2 - 10x - 10$ has $\mathbb{Q}(E[8]) = \mathbb{Q}(\zeta_8, \sqrt{3}, \sqrt{7})$.

Let $E/\mathbb{Q}$ be an elliptic curve, and let $P \in E(\overline{\mathbb{Q}})_{\text{tors}}$ be a torsion point.

Let $E/\mathbb{Q}$ be an elliptic curve, and let $P \in E(\overline{\mathbb{Q}})_{\text{tors}}$ be a torsion point.

Question

What is the degree of $\mathbb{Q}(P)/\mathbb{Q}$?

Let $E/\mathbb{Q}$ be an elliptic curve, and let $P \in E(\overline{\mathbb{Q}})_{\text{tors}}$ be a torsion point.

Question

What is the degree of $\mathbb{Q}(P)/\mathbb{Q}$?

- Mazur's proof of the Ogg/Levi's conjecture implies that if $[\mathbb{Q}(P) : \mathbb{Q}] = 1$, then

$$\operatorname{ord}(P) \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12\}.$$

Let $E/\mathbb{Q}$ be an elliptic curve, and let $P \in E(\overline{\mathbb{Q}})_{\text{tors}}$ be a torsion point.

Question

What is the degree of $\mathbb{Q}(P)/\mathbb{Q}$?

- Mazur's proof of the Ogg/Levi's conjecture implies that if $[\mathbb{Q}(P) : \mathbb{Q}] = 1$, then

$$\text{ord}(P) \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12\}.$$

- Work of Kenku, Momose, Kamienny, Najman implies that if $[\mathbb{Q}(P) : \mathbb{Q}] = 2$, then

$$\text{ord}(P) \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 15, 16\}.$$

Let $E/\mathbb{Q}$ be an elliptic curve, and let $P \in E(\overline{\mathbb{Q}})_{\text{tors}}$ be a torsion point.

Question

What is the degree of $\mathbb{Q}(P)/\mathbb{Q}$?

- Mazur's proof of the Ogg/Levi's conjecture implies that if $[\mathbb{Q}(P):\mathbb{Q}] = 1$, then

$$\operatorname{ord}(P) \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12\}.$$

- Work of Kenku, Momose, Kamienny, Najman implies that if $[\mathbb{Q}(P):\mathbb{Q}] = 2$, then

$$\operatorname{ord}(P) \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 15, 16\}.$$

- Work of Najman implies that if $[\mathbb{Q}(P):\mathbb{Q}] = 3$, then

$$\operatorname{ord}(P) \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 13, 14, 18, 21\}.$$

Definition

Let $d > 0$. We define:
$S_{\mathbb{Q}}(d) = \{p :$ primes such that $p | E(K)_{\text{tors}}$ for some elliptic curve E defined over $\mathbb{Q}$, and a number field K of degree $\leq d\}$.

Definition

Let $d > 0$. We define:
$S_{\mathbb{Q}}(d) = \{p$: primes such that $p|E(K)_{\text{tors}}$ for some elliptic curve E defined over $\mathbb{Q}$, and a number field K of degree $\leq d\}$.

Theorem (L-R., 2011)

Let $p \geq 11$ with $p \neq 13$ or 37. If $p \in S_{\mathbb{Q}}(d)$, then $p \leq 2d + 1$.

Definition

Let $d > 0$. We define:
$S_{\mathbb{Q}}(d) = \{p : \text{primes such that } p | E(K)_{\text{tors}} \text{ for some elliptic curve } E$ defined over $\mathbb{Q}$, and a number field K of degree $\leq d\}$.

Theorem (L-R., 2011)

Let $p \geq 11$ with $p \neq 13$ or 37. If $p \in S_{\mathbb{Q}}(d)$, then $p \leq 2d + 1$.

Theorem

Let $S_{\mathbb{Q}}(d)$ be the set of primes defined above.

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

Question

If $E/\mathbb{Q}$ and $P \in E[2^n]$, what is $[\mathbb{Q}(P) : \mathbb{Q}]$?

$$
\begin{tikzcd}
\mathbb{Q}(E[2^\infty]) \arrow[d, dash] \arrow[ddr, dash] & \\
\mathbb{Q}(E[2^n]) \arrow[dd, dash] \arrow[dr, dash, "H_P"'] & \\
 & \mathbb{Q}(P) \\
\mathbb{Q} \arrow[ur, dash] &
\end{tikzcd}
$$

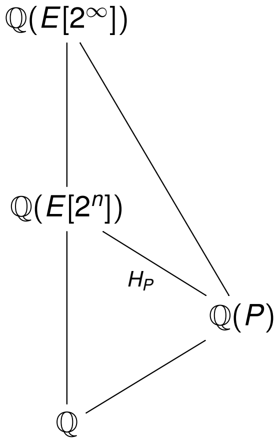
Question

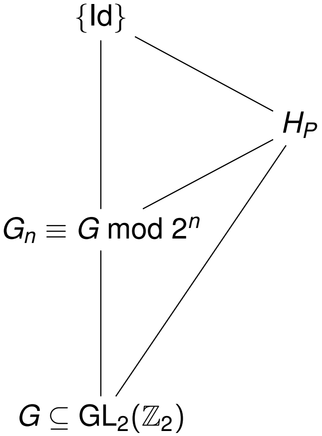
If $E/\mathbb{Q}$ and $P \in E[2^n]$, what is $[\mathbb{Q}(P) : \mathbb{Q}]$?

$$\begin{tikzcd}
\mathbb{Q}(E[2^\infty]) \arrow[d, dash] \arrow[ddr, dash] & \\
\mathbb{Q}(E[2^n]) \arrow[dr, dash, "H_P"'] \arrow[dd, dash] & \\
& \mathbb{Q}(P) \arrow[dl, dash] \\
\mathbb{Q} &
\end{tikzcd}
\qquad
\begin{tikzcd}
\{\mathrm{Id}\} \arrow[dr, dash] \arrow[dd, dash] & \\
& H_P \arrow[dl, dash] \arrow[ddl, dash] \\
G_n \equiv G \bmod 2^n \arrow[d, dash] & \\
G \subseteq \mathrm{GL}_2(\mathbb{Z}_2) &
\end{tikzcd}$$

Question

If $E/\mathbb{Q}$ and $P \in E[2^n]$, what is $[\mathbb{Q}(P) : \mathbb{Q}]$?





Note: if H_P is the stabilizer of P in G_n, then $[\mathbb{Q}(P) : \mathbb{Q}] = |G_n|/|H_P|$.

Question

If $E/\mathbb{Q}$ and $P \in E[2^n]$, what is $[\mathbb{Q}(P) : \mathbb{Q}]$ (if $\rho_{E,2}$ is defined mod 2^d)?

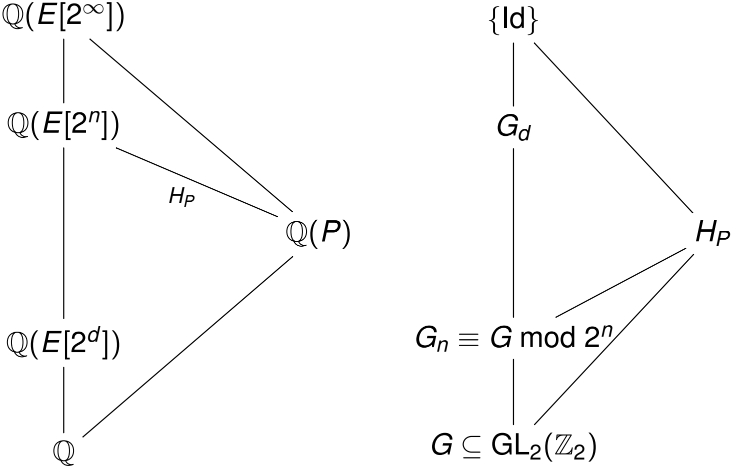
Question

If $E/\mathbb{Q}$ and $P \in E[2^n]$, what is $[\mathbb{Q}(P):\mathbb{Q}]$ (if $\rho_{E,2}$ is defined mod 2^d)?

$$\begin{tikzcd}
\mathbb{Q}(E[2^\infty]) \arrow[d, dash] \arrow[dddr, dash] & \\
\mathbb{Q}(E[2^d]) \arrow[d, dash] & \\
\mathbb{Q}(E[2^n]) \arrow[dd, dash] \arrow[dr, dash, "H_P"'] & \\
 & \mathbb{Q}(P) \\
\mathbb{Q} \arrow[ur, dash] &
\end{tikzcd}
\qquad
\begin{tikzcd}
\{\mathrm{Id}\} \arrow[dd, dash] \arrow[dr, dash] & \\
 & H_P \arrow[dl, dash] \arrow[dddl, dash] \\
G_n \equiv G \bmod 2^n \arrow[d, dash] & \\
G_d \arrow[d, dash] & \\
G \subseteq \mathrm{GL}_2(\mathbb{Z}_2) &
\end{tikzcd}$$

Question

If $E/\mathbb{Q}$ and $P \in E[2^n]$, what is $[\mathbb{Q}(P) : \mathbb{Q}]$ (if $\rho_{E,2}$ is defined mod 2^d)?



Theorem

Let $E/\mathbb{Q}$ be an elliptic curve defined over $\mathbb{Q}$ without CM, and let $P \in E[2^N]$ be a point of exact order 2^N, with $N \geq 4$.

Theorem

Let $E/\mathbb{Q}$ be an elliptic curve defined over $\mathbb{Q}$ without CM, and let $P \in E[2^N]$ be a point of exact order 2^N, with $N \geq 4$. Then, the degree $[\mathbb{Q}(P) : \mathbb{Q}]$ is divisible by 2^{2N-7}.

Theorem

Let $E/\mathbb{Q}$ be an elliptic curve defined over $\mathbb{Q}$ without CM, and let $P \in E[2^N]$ be a point of exact order 2^N, with $N \geq 4$. Then, the degree $[\mathbb{Q}(P) : \mathbb{Q}]$ is divisible by 2^{2N-7}. Moreover, this bound is best possible, in the sense that there is a one-parameter family $E_t/\mathbb{Q}$, one for each $t \in \mathbb{Q}$, and there is a point $P_{t,N} \in E_t(\overline{\mathbb{Q}})$ of exact order 2^N, such that

$$[\mathbb{Q}(P_{t,N}) : \mathbb{Q}] = 2^{2N-7}.$$

Theorem

Let $E/\mathbb{Q}$ be an elliptic curve defined over $\mathbb{Q}$ without CM, and let $P \in E[2^N]$ be a point of exact order 2^N, with $N \geq 4$. Then, the degree $[\mathbb{Q}(P) : \mathbb{Q}]$ is divisible by 2^{2N-7}. Moreover, this bound is best possible, in the sense that there is a one-parameter family $E_t/\mathbb{Q}$, one for each $t \in \mathbb{Q}$, and there is a point $P_{t,N} \in E_t(\overline{\mathbb{Q}})$ of exact order 2^N, such that

$$[\mathbb{Q}(P_{t,N}) : \mathbb{Q}] = 2^{2N-7}.$$

The family mentioned in the statement of the theorem is

$$\mathcal{X}_{235l} : y^2 = x^3 + (t^8 - 4t^6 - 2t^4 - 4t^2 + 1)x^2 + 16t^8 x.$$

One concrete member of the family is the curve with Cremona label `210e1`, given in Weierstrass form by

$$E : y^2 + xy = x^3 + 210x + 900.$$

Corollary

Let $E/\mathbb{Q}$ be an elliptic curve without CM, and let $F/\mathbb{Q}$ be an extension of degree $d \geq 1$. Then $E(F)$ can only contain points of order 2^N with

$$N \leq (\log_2(d) + 7)/2.$$

Corollary

Let $E/\mathbb{Q}$ be an elliptic curve without CM, and let $F/\mathbb{Q}$ be an extension of degree $d \geq 1$. Then $E(F)$ can only contain points of order 2^N with

$$N \leq (\log_2(d) + 7)/2.$$

More precisely, if ν_2 is the usual 2-adic valuation, then $E(F)$ can only contain points of order 2^N with

$$N \leq \lfloor \frac{\nu_2(d) + 7}{2} \rfloor.$$

More generally, let $E/\mathbb{Q}$ be an elliptic curve, and let

$$T = \langle P_s, Q_N \rangle \cong \mathbb{Z}/2^s\mathbb{Z} \oplus \mathbb{Z}/2^N\mathbb{Z} \subseteq E[2^N].$$

More generally, let $E/\mathbb{Q}$ be an elliptic curve, and let

$$T = \langle P_s, Q_N \rangle \cong \mathbb{Z}/2^s\mathbb{Z} \oplus \mathbb{Z}/2^N\mathbb{Z} \subseteq E[2^N].$$

Question

What is $[\mathbb{Q}(T) : \mathbb{Q}]$*?*

More generally, let $E/\mathbb{Q}$ be an elliptic curve, and let

$$T = \langle P_s, Q_N \rangle \cong \mathbb{Z}/2^s\mathbb{Z} \oplus \mathbb{Z}/2^N\mathbb{Z} \subseteq E[2^N].$$

Question

What is $[\mathbb{Q}(T) : \mathbb{Q}]$?

$$[\mathbb{Q}(T):\mathbb{Q}] = 1 \Longrightarrow \begin{cases} \mathbb{Z}/M\mathbb{Z} & \text{with } 1 \leq M \leq 10 \text{ or } M = 12, \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2M\mathbb{Z} & \text{with } 1 \leq M \leq 4. \end{cases}$$

$$[\mathbb{Q}(T):\mathbb{Q}] = 2 \Longrightarrow \begin{cases} \mathbb{Z}/M\mathbb{Z} & \text{with } 1 \leq M \leq 10 \text{ or } M = 12, 15, 16, \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2M\mathbb{Z} & \text{with } 1 \leq M \leq 6, \text{ or} \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3M\mathbb{Z} & \text{with } 1 \leq M \leq 2 \text{ and } F = \mathbb{Q}(\sqrt{-3}), \text{ or} \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} & \text{with } F = \mathbb{Q}(\sqrt{-1}). \end{cases}$$

$$[\mathbb{Q}(T):\mathbb{Q}] = 3 \Longrightarrow \begin{cases} \mathbb{Z}/M\mathbb{Z} & \text{with } 1 \leq M \leq 10 \\ & \text{ or } M = 12, 13, 14, 18, 21, \text{ or} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2M\mathbb{Z} & \text{with } 1 \leq M \leq 4 \text{ or } M = 7. \end{cases}$$

Theorem

Let $E/\mathbb{Q}$ be an elliptic curve without CM. Let $1 \leq s \leq N$ be fixed integers, and let $T \cong \mathbb{Z}/2^s\mathbb{Z} \oplus \mathbb{Z}/2^N\mathbb{Z} \subseteq E[2^N]$.

Theorem

Let $E/\mathbb{Q}$ be an elliptic curve without CM. Let $1 \leq s \leq N$ be fixed integers, and let $T \cong \mathbb{Z}/2^s\mathbb{Z} \oplus \mathbb{Z}/2^N\mathbb{Z} \subseteq E[2^N]$. Then, $[\mathbb{Q}(T) : \mathbb{Q}]$ is divisible by 2 if $s = N = 2$, and otherwise by $2^{2N+2s-8}$ if $N \geq 3$

Theorem

Let $E/\mathbb{Q}$ be an elliptic curve without CM. Let $1 \leq s \leq N$ be fixed integers, and let $T \cong \mathbb{Z}/2^s\mathbb{Z} \oplus \mathbb{Z}/2^N\mathbb{Z} \subseteq E[2^N]$. Then, $[\mathbb{Q}(T) : \mathbb{Q}]$ 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

$$-\frac{18234932071051198464000}{48661191875666868481} \text{ or}$$

$$-\frac{35817550197738955933474532061609984000}{2301619141096101839813550846721}$$

in which case $[\mathbb{Q}(T) : \mathbb{Q}]$ is divisible by $3 \cdot 2^{2N+2s-9}$.

Theorem

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

$$-\frac{18234932071051198464000}{48661191875666868481} \text{ or }$$

$$-\frac{35817550197738955933474532061609984000}{2301619141096101839813550846721}$$

in which case $[\mathbb{Q}(T):\mathbb{Q}]$ is divisible by $3 \cdot 2^{2N+2s-9}$. Moreover, this bound is best possible, i.e., there is $E_{s,N}(t)/\mathbb{Q}$ 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 $[\mathbb{Q}(T_{s,N}):\mathbb{Q}]$ is equal to the bound given above.

d				
1	2	4	8	16
$\mathbb{Z}/2$ $\mathbb{Z}/4$ $\mathbb{Z}/8$ $\mathbb{Z}/2 \oplus \mathbb{Z}/2$ $\mathbb{Z}/2 \oplus \mathbb{Z}/4$ $\mathbb{Z}/2 \oplus \mathbb{Z}/8$	$\mathbb{Z}/16$ $\mathbb{Z}/4 \oplus \mathbb{Z}/4$	$\mathbb{Z}/2 \oplus \mathbb{Z}/16$ $\mathbb{Z}/4 \oplus \mathbb{Z}/8$	$\mathbb{Z}/32$	$\mathbb{Z}/2 \oplus \mathbb{Z}/32$ $\mathbb{Z}/4 \oplus \mathbb{Z}/16$ $\mathbb{Z}/8 \oplus \mathbb{Z}/8$

Table : 2-primary torsion subgroups that appear in degree d for the first time.

Theorem

Let K be a number field, and let p be a prime.

Theorem

Let K be a number field, and let p be a prime. Then, there is only a finite number $a(K,p) \geq 1$ of possibilities (up to conjugation) for the image of $\rho_{E,p} : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}(2,\mathbb{Z}_p)$, for any elliptic curve E/K without CM.

Theorem

Let K be a number field, and let p be prime.

Theorem

Let K be a number field, and let p be prime. Then, there is only a finite number $a(K,p) \geq 1$ of possibilities (up to conjugation) for the image of $\rho_{E,p} : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}(2,\mathbb{Z}_p)$, for any elliptic curve E/K without CM.

Theorem

Let p be a prime, let K be a number field, and let E/K be an elliptic curve defined over K without CM. Let $0 \leq s \leq N$ be integers, and let $T_{s,N} \subseteq E(\overline{K})_{tors}$ with $T_{s,N} \cong \mathbb{Z}/p^s\mathbb{Z} \oplus \mathbb{Z}/p^N\mathbb{Z}$.

Theorem

Let K be a number field, and let p be prime. Then, there is only a finite number $a(K,p) \geq 1$ of possibilities (up to conjugation) for the image of $\rho_{E,p} : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}(2,\mathbb{Z}_p)$, for any elliptic curve E/K without CM.

Theorem

Let p be a prime, let K be a number field, and let E/K be an elliptic curve defined over K without CM. Let $0 \leq s \leq N$ be integers, and let $T_{s,N} \subseteq E(\overline{K})_{tors}$ with $T_{s,N} \cong \mathbb{Z}/p^s\mathbb{Z} \oplus \mathbb{Z}/p^N\mathbb{Z}$. Then:

1. *There are positive integers $n = n(K,p)$, and $g_{s,M}(K,p)$, for $0 \leq s \leq n$ and $M = \min\{n, N\}$, that depend on K and p but not on the choice of E/K or $T_{s,N}$, such that*

Theorem

Let K be a number field, and let p be prime. Then, there is only a finite number $a(K,p) \geq 1$ of possibilities (up to conjugation) for the image of $\rho_{E,p} : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}(2,\mathbb{Z}_p)$, for any elliptic curve E/K without CM.

Theorem

Let p be a prime, let K be a number field, and let E/K be an elliptic curve defined over K without CM. Let $0 \leq s \leq N$ be integers, and let $T_{s,N} \subseteq E(\overline{K})_{tors}$ with $T_{s,N} \cong \mathbb{Z}/p^s\mathbb{Z} \oplus \mathbb{Z}/p^N\mathbb{Z}$. Then:

1. *There are positive integers $n = n(K,p)$, and $g_{s,M}(K,p)$, for $0 \leq s \leq n$ and $M = \min\{n, N\}$, that depend on K and p but not on the choice of E/K or $T_{s,N}$, such that*
    - *$[K(T_{s,N}) : K]$ is divisible by $g_{s,M}(K,p) \cdot \max\{1, p^{2N-2n}\}$ if $s < n$, and*

Theorem

Let K be a number field, and let p be prime. Then, there is only a finite number $a(K,p) \geq 1$ of possibilities (up to conjugation) for the image of $\rho_{E,p} : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}(2,\mathbb{Z}_p)$, for any elliptic curve E/K without CM.

Theorem

Let p be a prime, let K be a number field, and let E/K be an elliptic curve defined over K without CM. Let $0 \leq s \leq N$ be integers, and let $T_{s,N} \subseteq E(\overline{K})_{tors}$ with $T_{s,N} \cong \mathbb{Z}/p^s\mathbb{Z} \oplus \mathbb{Z}/p^N\mathbb{Z}$. Then:

1. *There are positive integers $n = n(K,p)$, and $g_{s,M}(K,p)$, for $0 \leq s \leq n$ and $M = \min\{n, N\}$, that depend on K and p but not on the choice of E/K or $T_{s,N}$, such that*
   - $[K(T_{s,N}) : K]$ *is divisible by* $g_{s,M}(K,p) \cdot \max\{1, p^{2N-2n}\}$ *if* $s < n$, *and*
   - $[K(T_{s,N}) : K]$ *divisible by* $g_{n,n}(K,p) \cdot p^{2N+2s-4n}$ *if* $n \leq s \leq N$.

Theorem

Let K be a number field, and let p be prime. Then, there is only a finite number $a(K,p) \geq 1$ of possibilities (up to conjugation) for the image of $\rho_{E,p} : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}(2,\mathbb{Z}_p)$, for any elliptic curve E/K without CM.

Theorem

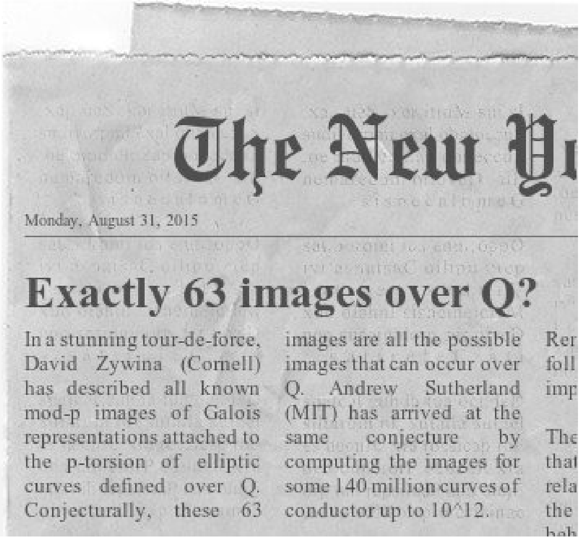
Let p be a prime, let K be a number field, and let E/K be an elliptic curve defined over K without CM. Let $0 \leq s \leq N$ be integers, and let $T_{s,N} \subseteq E(\overline{K})_{tors}$ with $T_{s,N} \cong \mathbb{Z}/p^s\mathbb{Z} \oplus \mathbb{Z}/p^N\mathbb{Z}$. Then:

1. *There are positive integers $n = n(K,p)$, and $g_{s,M}(K,p)$, for $0 \leq s \leq n$ and $M = \min\{n, N\}$, that depend on K and p but not on the choice of E/K or $T_{s,N}$, such that*
    - *$[K(T_{s,N}) : K]$ is divisible by $g_{s,M}(K,p) \cdot \max\{1, p^{2N-2n}\}$ if $s < n$, and*
    - *$[K(T_{s,N}) : K]$ divisible by $g_{n,n}(K,p) \cdot p^{2N+2s-4n}$ if $n \leq s \leq N$.*
2. *For a fixed E/K, and for all but finitely many primes p, we have*

$$[K(T_{s,N}) : K] = \begin{cases} (p^2-1)p^{2N-2} & , \text{ if } s = 0, \\ (p-1)(p^2-1)p^{2N+2s-3} & , \text{ if } s \geq 1. \end{cases}$$


DAILY NEWS
EXTRA!
EXTRA!
EXTRA!

News ... for $p \geq 2$!


The New Y

Monday, August 31, 2015

Exactly 63 images over Q?

In a stunning tour-de-force, David Zywina (Cornell) has described all known mod-p images of Galois representations attached to the p-torsion of elliptic curves defined over Q. Conjecturally, these 63 images are all the possible images that can occur over Q. Andrew Sutherland (MIT) has arrived at the same conjecture by computing the images for some 140 million curves of conductor up to 10^12.

News ... for $p \geq 2$!

Drew Sutherland
(MIT)

David Zywina
(Cornell)

Conjecture

Let $E/\mathbb{Q}$ be an elliptic curve, and let p be an arbitrary prime. Then, there are precisely 63 possibilities for the image $\rho_{E,p}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$, up to conjugation.

Theorem

Let $E/\mathbb{Q}$ be an elliptic curve without CM, and let p be a prime such that

Theorem

Let $E/\mathbb{Q}$ be an elliptic curve without CM, and let p be a prime such that

(A) *the image G_1 of $\rho_{E,p} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(2, \mathbb{Z}/p\mathbb{Z})$ is not contained in the normalizer of a non-split Cartan subgroup.*

Theorem

Let $E/\mathbb{Q}$ be an elliptic curve without CM, and let p be a prime such that

(A) *the image G_1 of $\rho_{E,p} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(2, \mathbb{Z}/p\mathbb{Z})$ is not contained in the normalizer of a non-split Cartan subgroup.*

In addition, let us assume that either (B) or (C) occurs, where

(B) *p is not in the set $S = \{2, 3, 5, 7, 11, 13, 17, 37\}$, or*

Theorem

Let $E/\mathbb{Q}$ be an elliptic curve without CM, and let p be a prime such that

(A) *the image G_1 of $\rho_{E,p} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(2, \mathbb{Z}/p\mathbb{Z})$ is not contained in the normalizer of a non-split Cartan subgroup.*

In addition, let us assume that either (B) or (C) occurs, where

(B) *p is not in the set $S = \{2, 3, 5, 7, 11, 13, 17, 37\}$, or*

(C) *if $p \in S$, we suppose that the p-adic image G of ρ_{E,p^∞} is defined modulo p, i.e., the image G of ρ_{E,p^∞} is the full inverse image of $G_1 = \rho_{E,p}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ under mod-p reduction.*

Theorem

Let $E/\mathbb{Q}$ be an elliptic curve without CM, and let p be a prime such that

(A) *the image G_1 of $\rho_{E,p} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(2, \mathbb{Z}/p\mathbb{Z})$ is not contained in the normalizer of a non-split Cartan subgroup.*

In addition, let us assume that either (B) or (C) occurs, where

(B) *p is not in the set $S = \{2, 3, 5, 7, 11, 13, 17, 37\}$, or*

(C) *if $p \in S$, we suppose that the p-adic image G of ρ_{E,p^∞} is defined modulo p, i.e., the image G of ρ_{E,p^∞} is the full inverse image of $G_1 = \rho_{E,p}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ under mod-p reduction.*

Let $T = T_{s,N} \cong \mathbb{Z}/p^s\mathbb{Z} \oplus \mathbb{Z}/p^N\mathbb{Z} \subseteq E[p^N]$ be a subgroup. Then,

Theorem

Let $E/\mathbb{Q}$ be an elliptic curve without CM, and let p be a prime such that

(A) *the image G_1 of $\rho_{E,p} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(2, \mathbb{Z}/p\mathbb{Z})$ is not contained in the normalizer of a non-split Cartan subgroup.*

In addition, let us assume that either (B) or (C) occurs, where

(B) *p is not in the set $S = \{2, 3, 5, 7, 11, 13, 17, 37\}$, or*

(C) *if $p \in S$, we suppose that the p-adic image G of ρ_{E,p^∞} is defined modulo p, i.e., the image G of ρ_{E,p^∞} is the full inverse image of $G_1 = \rho_{E,p}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ under mod-p reduction.*

Let $T = T_{s,N} \cong \mathbb{Z}/p^s\mathbb{Z} \oplus \mathbb{Z}/p^N\mathbb{Z} \subseteq E[p^N]$ be a subgroup. Then,

1. *For a fixed $G_1 = \rho_{E,p}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$, the degree $[\mathbb{Q}(T) : \mathbb{Q}]$ is divisible by $g_{0,1}(G_1) \cdot p^{2N-2}$ if $s = 0$, and $[\mathbb{Q}(T) : \mathbb{Q}]$ is divisible by $g_{1,1}(G_1) \cdot p^{2N+2s-4}$ if $s \geq 1$, where the constants are explicit.*

Theorem

Let $E/\mathbb{Q}$ be an elliptic curve without CM, and let p be a prime such that

(A) *the image G_1 of $\rho_{E,p} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(2, \mathbb{Z}/p\mathbb{Z})$ is not contained in the normalizer of a non-split Cartan subgroup.*

In addition, let us assume that either (B) or (C) occurs, where

(B) *p is not in the set $S = \{2, 3, 5, 7, 11, 13, 17, 37\}$, or*

(C) *if $p \in S$, we suppose that the p-adic image G of ρ_{E,p^∞} is defined modulo p, i.e., the image G of ρ_{E,p^∞} is the full inverse image of $G_1 = \rho_{E,p}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ under mod-p reduction.*

Let $T = T_{s,N} \cong \mathbb{Z}/p^s\mathbb{Z} \oplus \mathbb{Z}/p^N\mathbb{Z} \subseteq E[p^N]$ be a subgroup. Then,

1. *For a fixed $G_1 = \rho_{E,p}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$, the degree $[\mathbb{Q}(T) : \mathbb{Q}]$ is divisible by $g_{0,1}(G_1) \cdot p^{2N-2}$ if $s = 0$, and $[\mathbb{Q}(T) : \mathbb{Q}]$ is divisible by $g_{1,1}(G_1) \cdot p^{2N+2s-4}$ if $s \geq 1$, where the constants are explicit.*
2. *In general, $[\mathbb{Q}(T) : \mathbb{Q}]$ is divisible by $g_{0,1}(\mathbb{Q}, p) \cdot p^{2N-2}$ if $s = 0$, and divisible by $g_{1,1}(\mathbb{Q}, p) \cdot p^{2N+2s-4}$ if $s \geq 1$, where the constants $g_{k,1}(\mathbb{Q}, p)$ are explicit.*

In general, if $\rho_{E,p}$ is defined modulo p (and image is not in a normalizer of non-split Cartan), and $T_{s,N} \cong \mathbb{Z}/2^s\mathbb{Z} \oplus \mathbb{Z}/2^N\mathbb{Z} \subseteq E[2^N]$, then

- $[\mathbb{Q}(T_{s,N}) : \mathbb{Q}]$ is divisible by $g_{0,1}(\mathbb{Q}, p) \cdot p^{2N-2}$ if $s = 0$, and
- $[\mathbb{Q}(T_{s,N}) : \mathbb{Q}]$ is divisible by $g_{1,1}(\mathbb{Q}, p) \cdot p^{2N+2s-4}$ if $s \geq 1$,

where the constants $g_{k,1}(\mathbb{Q}, p)$ are

p	$g_{0,1}(\mathbb{Q}, p)$	$m_{0,1}(\mathbb{Q}, p)$	$g_{1,1}(\mathbb{Q}, p)$	$m_{1,1}(\mathbb{Q}, p)$
2	1	1	1	1
3	1	1	2	2
5	1	1	4	4
7	1	1	6	18
11	5	5	10	110
13	1	3	12	288
17	8	8	1088	1088
37	12	12	15984	15984
else	$p^2 - 1$	$p^2 - 1$	$(p-1)p(p^2-1)$	$(p-1)p(p^2-1)$

Table : $g_{k,1}(\mathbb{Q}, p)$ and $m_{k,1}(\mathbb{Q}, p)$, for $k = 0, 1$.

p	G	$g_{0,1}(G)$	$m_{0,1}(G)$	$g_{1,1}(G) = m_{1,1}(G)$	Example $E/\mathbb{Q}$
11	11B.1.4	5	5	110	121a2
11	11B.1.5	5	5	110	121c2
11	11B.1.6	5	10	110	121a1
11	11B.1.7	5	10	110	121c1
11	11B.10.4	10	10	220	1089f2
11	11B.10.5	10	10	220	1089f1
11	11Nn	120	120	240	232544f1
11	$\mathrm{GL}(2,\mathbb{F}_{11})$	120	120	13200	11a1
13	13S4	24	72	288	152100g1
13	13B.3.1	3	3	468	147b1
13	13B.3.2	3	12	468	147b2
13	13B.3.4	6	6	468	24843o1
13	13B.3.7	6	12	468	24843o2
13	13B.5.1	4	4	624	2890d1
13	13B.5.2	4	12	624	2890d2
13	13B.5.4	12	12	624	216320i1
13	13B.4.1	6	6	936	147c1
13	13B.4.2	6	12	936	147c2
13	13B	12	12	1872	2450l1
13	$\mathrm{GL}(2,\mathbb{F}_{13})$	168	168	26208	11a1
17	17B.4.2	8	8	1088	14450n1
17	17B.4.6	8	16	1088	14450n2
17	$\mathrm{GL}(2,\mathbb{F}_{17})$	288	288	78336	11a1
37	37B.8.1	12	12	15984	1225e1
37	37B.8.2	12	36	15984	1225e2
37	$\mathrm{GL}(2,\mathbb{F}_{37})$	1368	1368	1822176	11a1
else	$\mathrm{GL}(2,\mathbb{F}_p)$	p^2-1	p^2-1	$(p-1)p(p^2-1)$	11a1

TABLE 6. $g_{k,1}(G)$ and $m_{k,1}(G)$, for $k=0,1$, and example curves.

alvaro@uconn.edu

http://alozano.clas.uconn.edu