Bounding Selmer Groups of Finite Galois Modules

Jacob Tsimerman

University of Toronto

July 25, 2019

Joint work with Arul Shankar

- K - Number field of degree n
- Cl_K - Class group of K
- D_K - Absolute value of the Discriminant of K

- K - Number field of degree n
- Cl_K - Class group of K
- D_K - Absolute value of the Discriminant of K

Class Number Formula:

$$w_K \cdot D_K^{\frac{1}{2}} \cdot \mathrm{Res}_{s=1}\zeta_K(s) = 2^{r_1} \cdot (2\pi)^{r_2} \cdot \mathrm{Reg}_K \cdot |\mathrm{Cl}_K|$$

- K - Number field of degree n
- Cl_K - Class group of K
- D_K - Absolute value of the Discriminant of K

Class Number Formula:

$$w_K \cdot D_K^{\frac{1}{2}} \cdot \mathrm{Res}_{s=1}\zeta_K(s) = 2^{r_1} \cdot (2\pi)^{r_2} \cdot \mathrm{Reg}_K \cdot |\mathrm{Cl}_K|$$

Corollary (Brauer-Siegel)

$|\mathrm{Cl}_K| \leqslant D_K^{\frac{1}{2}+o_n(1)}$

The exponent of $\frac{1}{2}$ is tight.

Question: How big is $\mathrm{Cl}_K[m]$ for fixed m?

Question: How big is $\mathrm{Cl}_K[m]$ for fixed m?
Applications to counting number fields, integral points on Elliptic Curves, lower bounds for Galois orbits(André-Oort), modular forms,. . .

Question: How big is $\mathrm{Cl}_K[m]$ for fixed m?
Applications to counting number fields, integral points on Elliptic Curves, lower bounds for Galois orbits(André-Oort), modular forms,...
Heuristic: Cl_K is a 'random' finite Abelian group, so should be 'close' to a cyclic group.

Question: How big is $\mathrm{Cl}_K[m]$ for fixed m?
Applications to counting number fields, integral points on Elliptic Curves, lower bounds for Galois orbits(André-Oort), modular forms,...

Heuristic: Cl_K is a 'random' finite Abelian group, so should be 'close' to a cyclic group.

Conjecture (Zhang, Brumer-Silverman)

Fix $n = [K : \mathbb{Q}]$ and $m > 1$. Then

$$|\mathrm{Cl}_K[m]| = D_K^{o(1)}$$

Question: How big is $\mathrm{Cl}_K[m]$ for fixed m?
Applications to counting number fields, integral points on Elliptic Curves, lower bounds for Galois orbits(André-Oort), modular forms,...
Heuristic: Cl_K is a 'random' finite Abelian group, so should be 'close' to a cyclic group.

Conjecture (Zhang, Brumer-Silverman)

Fix $n = [K : \mathbb{Q}]$ and $m > 1$. Then

$$|\mathrm{Cl}_K[m]| = D_K^{o(1)}$$

Trivial 'convexity bound': $|\mathrm{Cl}_K[m]| \leqslant D_K^{\frac{1}{2}+o(1)}$

Question: How big is $\mathrm{Cl}_K[m]$ for fixed m?
Applications to counting number fields, integral points on Elliptic Curves, lower bounds for Galois orbits(André-Oort), modular forms,...
Heuristic: Cl_K is a 'random' finite Abelian group, so should be 'close' to a cyclic group.

Conjecture (Zhang, Brumer-Silverman)

Fix $n = [K : \mathbb{Q}]$ and $m > 1$. Then

$$|\mathrm{Cl}_K[m]| = D_K^{o(1)}$$

Trivial 'convexity bound': $|\mathrm{Cl}_K[m]| \leqslant D_K^{\frac{1}{2}+o(1)}$

Subconvexity: $|\mathrm{Cl}_K[m]| \leqslant D_K^{\frac{1}{2}-\delta_{m,n}+o(1)}$

Previous Work:

Subconvexity: $|\mathrm{Cl}_K[m]| \leqslant D_K^{\frac{1}{2}-\delta_{m,n}+o(1)}$

- $\delta_{2^k,2} = \frac{1}{2}$ (Gauss)
- $\delta_{3,2} = \frac{1}{6}$ (Pierce, Helfgott-Venkatesh, Ellenberg Venkatesh).
- $\delta_{3,3} = \delta_{3,4} > 0$ (Ellenberg-Venkatesh)
- $\delta_{2,n} = \frac{1}{2n}$ (Bhargava-Shankar-Taniguchi-Thorne-T-Zhao)
- $\delta_{m,n} = \frac{1}{2m(n-1)}$ Conditional on GRH (Ellenberg-Venkatesh).

Previous Work:

Subconvexity: $|\mathrm{Cl}_K[m]| \leqslant D_K^{\frac{1}{2}-\delta_{m,n}+o(1)}$

- $\delta_{2^k,2} = \frac{1}{2}$ (Gauss)
- $\delta_{3,2} = \frac{1}{6}$ (Pierce, Helfgott-Venkatesh, Ellenberg Venkatesh).
- $\delta_{3,3} = \delta_{3,4} > 0$ (Ellenberg-Venkatesh)
- $\delta_{2,n} = \frac{1}{2n}$ (Bhargava-Shankar-Taniguchi-Thorne-T-Zhao)
- $\delta_{m,n} = \frac{1}{2m(n-1)}$ Conditional on GRH (Ellenberg-Venkatesh).

Theorem (Shankar-T)

Assume the Refined BSD Conjecture. Then $\delta_{5,2} = \frac{1}{16}$.
Further Assuming GRH, $\delta_{5,2} = \delta_{3,2} = \frac{1}{4}$.

Heuristic Method: Embedding into Global Motives

Heuristic Method: Embedding into Global Motives

WARNING: I KNOW NOTHING ABOUT MOTIVES!

Heuristic Method: Embedding into Global Motives

WARNING: I KNOW NOTHING ABOUT MOTIVES!

- Step 1: Reframe $\mathrm{Cl}_K[n]$ as the Selmer group of a finite $\mathrm{G}_{\mathbb{Q}}$-module, 'separating it from K'.

Heuristic Method: Embedding into Global Motives

WARNING: I KNOW NOTHING ABOUT MOTIVES!

- Step 1: Reframe $\mathrm{Cl}_K[n]$ as the Selmer group of a finite $\mathrm{G}_{\mathbb{Q}}$-module, 'separating it from K'.
- On the one hand, we have finite $\mathrm{G}_{\mathbb{Q}}$-modules A, and we want to bound $\mathrm{Sel}(A)$.

Heuristic Method: Embedding into Global Motives

WARNING: I KNOW NOTHING ABOUT MOTIVES!

- Step 1: Reframe $\mathrm{Cl}_K[n]$ as the Selmer group of a finite $\mathrm{G}_{\mathbb{Q}}$-module, 'separating it from K'.
- On the one hand, we have finite $\mathrm{G}_{\mathbb{Q}}$-modules A, and we want to bound $\mathrm{Sel}(A)$.
- On the other hand, we have motives M, and these have 'Class groups' $\mathrm{Cl}(M)$, which satisfy a *Class Number Formula*, giving analytic control over $|\mathrm{Cl}(M)|$.

Heuristic Method: Embedding into Global Motives

WARNING: I KNOW NOTHING ABOUT MOTIVES!

- Step 1: Reframe $\mathrm{Cl}_K[n]$ as the Selmer group of a finite $\mathrm{G}_{\mathbb{Q}}$-module, 'separating it from K'.
- On the one hand, we have finite $\mathrm{G}_{\mathbb{Q}}$-modules A, and we want to bound $\mathrm{Sel}(A)$.
- On the other hand, we have motives M, and these have 'Class groups' $\mathrm{Cl}(M)$, which satisfy a *Class Number Formula*, giving analytic control over $|\mathrm{Cl}(M)|$.
- Occasionally, we may 'embed' $A \hookrightarrow M$, giving an 'embedding' $\mathrm{Sel}(A) \hookrightarrow \mathrm{Cl}(M)$, yielding a 'trivial' upper bound.

Heuristic Method: Embedding into Global Motives

WARNING: I KNOW NOTHING ABOUT MOTIVES!

- Step 1: Reframe $\mathrm{Cl}_K[n]$ as the Selmer group of a finite $\mathrm{G}_{\mathbb{Q}}$-module, 'separating it from K'.
- On the one hand, we have finite $\mathrm{G}_{\mathbb{Q}}$-modules A, and we want to bound $\mathrm{Sel}(A)$.
- On the other hand, we have motives M, and these have 'Class groups' $\mathrm{Cl}(M)$, which satisfy a *Class Number Formula*, giving analytic control over $|\mathrm{Cl}(M)|$.
- Occasionally, we may 'embed' $A \hookrightarrow M$, giving an 'embedding' $\mathrm{Sel}(A) \hookrightarrow \mathrm{Cl}(M)$, yielding a 'trivial' upper bound.
- The game is to find the best M for a given A. In other words, perhaps $D_K^{\frac{1}{2}}$ is not the best possible trivial bound for $|\mathrm{Cl}_K[m]|$

Finite Selmer Groups

A - Finite $\mathrm{G}_{\mathbb{Q}}$ module.

$$\begin{tikzcd}
\mathrm{Sel}(A) \arrow[r, hook] \arrow[d] & H^1(\mathrm{G}_{\mathbb{Q}}, A) \arrow[d] \\
\prod_v H^1(\mathrm{G}_{\mathbb{F}_v}, A^{I_v}) \arrow[r, hook] & \prod_v H^1(\mathrm{G}_{\mathbb{Q}_v}, A)
\end{tikzcd}$$

Finite Selmer Groups

A - Finite $\mathrm{G}_{\mathbb{Q}}$ module.

$$\begin{tikzcd}
\mathrm{Sel}(A) \arrow[r, hook] \arrow[d] & H^1(\mathrm{G}_{\mathbb{Q}}, A) \arrow[d] \\
\prod_v H^1(\mathrm{G}_{\mathbb{F}_v}, A^{I_v}) \arrow[r, hook] & \prod_v H^1(\mathrm{G}_{\mathbb{Q}_v}, A)
\end{tikzcd}$$

$D_A := D_L$ where G_L is the kernel of the action of $\mathrm{G}_{\mathbb{Q}}$ on A.
Analytic convention: We will write $>, <, \approx$ *to mean up to factors of* $D_A^{o(1)}$.

Finite Selmer Groups

A - Finite $\mathrm{G}_{\mathbb{Q}}$ module.

$$\begin{tikzcd} \mathrm{Sel}(A) \arrow[r, hook] \arrow[d] & H^1(\mathrm{G}_{\mathbb{Q}}, A) \arrow[d] \\ \prod_v H^1(\mathrm{G}_{\mathbb{F}_v}, A^{I_v}) \arrow[r, hook] & \prod_v H^1(\mathrm{G}_{\mathbb{Q}_v}, A) \end{tikzcd}$$

$D_A := D_L$ where G_L is the kernel of the action of $\mathrm{G}_{\mathbb{Q}}$ on A.
Analytic convention: We will write $\succ, \prec, \approx$ to mean up to factors of $D_A^{o(1)}$.

- For exact $0 \to A \to B \to C \to 0$, we have

$$\max(|\mathrm{Sel}(A)|, |\mathrm{Sel}(C)|) \preceq |\mathrm{Sel}(B)| \preceq |\mathrm{Sel}(A)| \cdot |\mathrm{Sel}(C)|.$$

- (Poitou-Tate) For $A^D := \mathrm{Hom}(A, \mathbb{G}_m)$,

$$|\mathrm{Sel}(A)| \approx |\mathrm{Sel}(A^D)|$$

Example: Algebraic Tori

- T- Algebraic Torus over $\mathbb{Q}$, dimension d.
- $X(T)$ - cocharacter Group of T over $\overline{\mathbb{Q}}$.
- $\rho_T : \mathrm{G}_{\mathbb{Q}} \circlearrowright X(T)$, of Artin conductor f_T.
- $\mathrm{Cl}_T := T(\mathbb{Q}) \backslash T(\mathbb{A}_f) / T(\hat{\mathbb{Z}})$.

Example: Algebraic Tori

- T- Algebraic Torus over $\mathbb{Q}$, dimension d.
- $X(T)$ - cocharacter Group of T over $\overline{\mathbb{Q}}$.
- $\rho_T : \mathrm{G}_{\mathbb{Q}} \circlearrowright X(T)$, of Artin conductor f_T.
- $\mathrm{Cl}_T := T(\mathbb{Q})\backslash T(\mathbb{A}_f)/T(\hat{\mathbb{Z}})$.
- (Shyr, Ono, T, Ullmo-Yafaev) $|\mathrm{Cl}_T| \cdot \mathrm{Reg}_T = f_T^{\frac{1}{2}+o_d(1)}$.

Example: Algebraic Tori

- T- Algebraic Torus over $\mathbb{Q}$, dimension d.
- $X(T)$ - cocharacter Group of T over $\overline{\mathbb{Q}}$.
- $\rho_T : \mathrm{G}_{\mathbb{Q}} \circlearrowright X(T)$, of Artin conductor f_T.
- $\mathrm{Cl}_T := T(\mathbb{Q})\backslash T(\mathbb{A}_f)/T(\hat{\mathbb{Z}})$.
- (Shyr, Ono, T, Ullmo-Yafaev) $|\mathrm{Cl}_T| \cdot \mathrm{Reg}_T = f_T^{\frac{1}{2}+o_d(1)}$.

Analytic Warning: we will write $\approx$ to mean equal up to factors of $f_T^{o(1)}$.

Example: Algebraic Tori

- T- Algebraic Torus over $\mathbb{Q}$, dimension d.
- $X(T)$ - cocharacter Group of T over $\overline{\mathbb{Q}}$.
- $\rho_T : \mathrm{G}_{\mathbb{Q}} \circlearrowright X(T)$, of Artin conductor f_T.
- $\mathrm{Cl}_T := T(\mathbb{Q})\backslash T(\mathbb{A}_f)/T(\hat{\mathbb{Z}})$.
- (Shyr, Ono, T, Ullmo-Yafaev) $|\mathrm{Cl}_T| \cdot \mathrm{Reg}_T = f_T^{\frac{1}{2}+o_d(1)}$.

Analytic Warning: we will write $\approx$ to mean equal up to factors of $f_T^{o(1)}$.

Let $\phi : T \to S$ be an Isogeny, $M_\phi : \mathrm{Coker}(X(\phi) : X(T) \to X(S))$.

Example: Algebraic Tori

- T- Algebraic Torus over $\mathbb{Q}$, dimension d.
- $X(T)$ - cocharacter Group of T over $\overline{\mathbb{Q}}$.
- $\rho_T : \mathrm{G}_{\mathbb{Q}} \circlearrowright X(T)$, of Artin conductor f_T.
- $\mathrm{Cl}_T := T(\mathbb{Q})\backslash T(\mathbb{A}_f)/T(\hat{\mathbb{Z}})$.
- (Shyr, Ono, T, Ullmo-Yafaev) $|\mathrm{Cl}_T| \cdot \mathrm{Reg}_T = f_T^{\frac{1}{2}+o_d(1)}$.

Analytic Warning: we will write $\approx$ to mean equal up to factors of $f_T^{o(1)}$.

Let $\phi : T \to S$ be an Isogeny, $M_\phi : \mathrm{Coker}(X(\phi) : X(T) \to X(S))$.

For $\mathrm{Cl}(\phi) : \mathrm{Cl}_T \to \mathrm{Cl}_S$, $|\mathrm{Sel}(M_\phi)| \approx |\mathrm{KerCl}(\phi)| \approx |\mathrm{Coker}(\mathrm{Cl}(\phi))|$.

Example: Algebraic Tori

- T- Algebraic Torus over $\mathbb{Q}$, dimension d.
- $X(T)$ - cocharacter Group of T over $\overline{\mathbb{Q}}$.
- $\rho_T : \mathrm{G}_{\mathbb{Q}} \circlearrowright X(T)$, of Artin conductor f_T.
- $\mathrm{Cl}_T := T(\mathbb{Q})\backslash T(\mathbb{A}_f)/T(\hat{\mathbb{Z}})$.
- (Shyr, Ono, T, Ullmo-Yafaev) $|\mathrm{Cl}_T| \cdot \mathrm{Reg}_T = f_T^{\frac{1}{2}+o_d(1)}$.

Analytic Warning: we will write $\approx$ to mean equal up to factors of $f_T^{o(1)}$.

Let $\phi : T \to S$ be an Isogeny, $M_\phi : \mathrm{Coker}(X(\phi) : X(T) \to X(S))$.

For $\mathrm{Cl}(\phi) : \mathrm{Cl}_T \to \mathrm{Cl}_S$, $|\mathrm{Sel}(M_\phi)| \approx |\mathrm{KerCl}(\phi)| \approx |\mathrm{Coker}(\mathrm{Cl}(\phi))|$.

Example: 3-torsion of cubic fields

.

- K - S_3 cubic field
- L - quadratic resolvent field of K ($L = (K^{\mathrm{nor}})^{A_3}$).

Example: 3-torsion of cubic fields

.

- K - S_3 cubic field
- L - quadratic resolvent field of K ($L = (K^{\mathrm{nor}})^{A_3}$).
- $T_K := \mathrm{Res}_{K/\mathbb{Q}}\mathrm{G}_m$
- $\rho_{K,n} := \rho_{T_K} \otimes \mathbb{Z}/n\mathbb{Z}$.
- $\mathrm{Cl}_K[3] \approx \mathrm{Sel}(\rho_{K,3})$.

Example: 3-torsion of cubic fields

.

- K - S_3 cubic field
- L - quadratic resolvent field of K ($L = (K^{\mathrm{nor}})^{A_3}$).
- $T_K := \mathrm{Res}_{K/\mathbb{Q}}\mathrm{G}_m$
- $\rho_{K,n} := \rho_{T_K} \otimes \mathbb{Z}/n\mathbb{Z}$.
- $\mathrm{Cl}_K[3] \approx \mathrm{Sel}(\rho_{K,3})$.
- Now, we have an exact sequence of $\mathrm{G}_{\mathbb{Q}}$ modules $0 \to \rho_{L,3} \to \rho_{K,3} \to \mathbb{F}_3 \to 0$.

Example: 3-torsion of cubic fields

.

- K - S_3 cubic field
- L - quadratic resolvent field of K ($L = (K^{\mathrm{nor}})^{A_3}$).
- $T_K := \mathrm{Res}_{K/\mathbb{Q}} \mathrm{G}_m$
- $\rho_{K,n} := \rho_{T_K} \otimes \mathbb{Z}/n\mathbb{Z}$.
- $\mathrm{Cl}_K[3] \approx \mathrm{Sel}(\rho_{K,3})$.
- Now, we have an exact sequence of $\mathrm{G}_{\mathbb{Q}}$ modules $0 \to \rho_{L,3} \to \rho_{K,3} \to \mathbb{F}_3 \to 0$.
- Since $|\mathrm{Sel}(\mathbb{F}_3)| \approx |\mathrm{Cl}_{\mathbb{Q}}[3]| \approx 1$, we see that

Transfer Principle for 3-torsion in cubic fields (Gerth)

$$|\mathrm{Cl}_K[3]| \approx |\mathrm{Cl}_L[3]|$$

Example: 2-torsion of quartic fields

- K - S_4 or A_4 quartic field
- L - cubic resolvent field of K ($L = (K^{\mathrm{nor}})^{D_4}$).
- $\mathrm{Cl}_K[2] \approx \mathrm{Sel}(\rho_{K,2})$.
- $\rho_{K,2}$ and $\rho_{L,2}$ are extensions of the same 2-dimensional irreducible component by trivial modules, so

Transfer Principle for 2-torsion in quartic fields (T)

$$|\mathrm{Cl}_K[2]| \approx |\mathrm{Cl}_L[2]|$$

More refined comparisons

One can get precise comparisons of torsion ‘up to the ramified primes’.

More refined comparisons

One can get precise comparisons of torsion 'up to the ramified primes'.

Theorem (Gras,Gerth)

Let L be a cubic field, and K its quadratic resolvent. If LK/K is unramified, then

$$\mathrm{rk}_2 \mathrm{Cl}_L = \mathrm{rk}_2 \mathrm{Cl}_K + 1.$$

More refined comparisons

One can get precise comparisons of torsion 'up to the ramified primes'.

Theorem (Gras,Gerth)

Let L be a cubic field, and K its quadratic resolvent. If LK/K is unramified, then

$$\mathrm{rk}_2 \mathrm{Cl}_L = \mathrm{rk}_2 \mathrm{Cl}_K + 1.$$

Conjecture (Lemmermeyer)

Let K be an A_4 quartic field, and L its cubic resolvent. Then

$$0 \leqslant \mathrm{rk}_2 \mathrm{Cl}_K - \mathrm{rk}_2 \mathrm{Cl}_L \leqslant 2.$$

More refined comparisons

One can get precise comparisons of torsion 'up to the ramified primes'.

Theorem (Gras,Gerth)

Let L be a cubic field, and K its quadratic resolvent. If LK/K is unramified, then

$$\mathrm{rk}_2\mathrm{Cl}_L = \mathrm{rk}_2\mathrm{Cl}_K + 1.$$

Conjecture (Lemmermeyer)

Let K be an A_4 quartic field, and L its cubic resolvent. Then

$$0 \leqslant \mathrm{rk}_2\mathrm{Cl}_K - \mathrm{rk}_2\mathrm{Cl}_L \leqslant 2.$$

(Klys, 2018) $\quad -10 \leqslant \mathrm{rk}_2\mathrm{Cl}_K - \mathrm{rk}_2\mathrm{Cl}_L \leqslant 12.$

Elliptic Curves

- $E : y^2 = x^3 + Ax + B$ - Elliptic curve over $\mathbb{Q}$
- $H_E := \max(A^3, B^2)$
- r - rank of $E(\mathbb{Q})$
- Ω_E - minimal period of E.

Elliptic Curves

- $E : y^2 = x^3 + Ax + B$ - Elliptic curve over $\mathbb{Q}$
- $H_E := \max(A^3, B^2)$
- r - rank of $E(\mathbb{Q})$
- Ω_E - minimal period of E.

Refined BSD Conjecture

$$\frac{L^{(r)}(E,1)}{r!} = \frac{\#\text{Ш}(E/\mathbb{Q})}{\#E(\mathbb{Q})^2_{tor}} \cdot \mathrm{Reg}_E \cdot \Omega_E \cdot \prod_{p|N} c_p$$

Elliptic Curves

- $E : y^2 = x^3 + Ax + B$ - Elliptic curve over $\mathbb{Q}$
- $H_E := \max(A^3, B^2)$
- r - rank of $E(\mathbb{Q})$
- Ω_E - minimal period of E.

Refined BSD Conjecture

$$\frac{L^{(r)}(E,1)}{r!} = \frac{\#\text{Ш}(E/\mathbb{Q})}{\#E(\mathbb{Q})_{tor}^2} \cdot \mathrm{Reg}_E \cdot \Omega_E \cdot \prod_{p|N} c_p$$

We think of Ш$(E/\mathbb{Q})$ as the 'Class Group' of the motive given by E, and the Refined BSD Conjecture as the 'Class number Formula'.

Elliptic Curves

- $E : y^2 = x^3 + Ax + B$ - Elliptic curve over $\mathbb{Q}$
- $H_E := \max(A^3, B^2)$
- r - rank of $E(\mathbb{Q})$
- Ω_E - minimal period of E.

Refined BSD Conjecture

$$\frac{L^{(r)}(E,1)}{r!} = \frac{\#\text{Ш}(E/\mathbb{Q})}{\#E(\mathbb{Q})_{tor}^2} \cdot \mathrm{Reg}_E \cdot \Omega_E \cdot \prod_{p|N} c_p$$

We think of $\text{Ш}(E/\mathbb{Q})$ as the 'Class Group' of the motive given by E, and the Refined BSD Conjecture as the 'Class number Formula'.

Note: $\Omega_E = H_E^{\frac{1}{12}+o(1)}$,

Optimistic Conjecture(Refined BSD+GRH+Bounds on Ranks)

$$\#\text{Ш}(E/\mathbb{Q}) \cdot \mathrm{Reg}_E = H_E^{\frac{1}{12}+o(1)}$$

Elliptic curves: Comparing Selmer Groups

$$\begin{tikzcd}
\mathrm{Sel}_n(E) \arrow[r, hook] \arrow[d] & H^1(\mathrm{G}_{\mathbb{Q}}, E[n]) \arrow[d] \\
\prod_v \kappa_v : \prod_v E[5](\mathbb{Q}_v) \otimes \mathbb{Z}/n\mathbb{Z} \arrow[r, hook] & \prod_v H^1(\mathrm{G}_{\mathbb{Q}_v}, E[n])
\end{tikzcd}$$

Elliptic curves: Comparing Selmer Groups

$$\begin{tikzcd} & \mathrm{Sel}_n(E) \arrow[r, hook] \arrow[d] & H^1(\mathrm{G}_{\mathbb{Q}}, E[n]) \arrow[d] \\ \prod_v \kappa_v : & \prod_v E[5](\mathbb{Q}_v) \otimes \mathbb{Z}/n\mathbb{Z} \arrow[r, hook] & \prod_v H^1(\mathrm{G}_{\mathbb{Q}_v}, E[n]) \end{tikzcd}$$

For all v at which E has good reduction and $E[n]$ is unramified, the image of κ_v consists exactly of the unramified classes, i.e. the image of $H^1(G_{\mathbb{F}_v}, E[n])$.

Elliptic curves: Comparing Selmer Groups

$$\begin{tikzcd} \mathrm{Sel}_n(E) \arrow[r, hook] \arrow[d] & H^1(\mathrm{G}_{\mathbb{Q}}, E[n]) \arrow[d] \\ \prod_v \kappa_v : \prod_v E[5](\mathbb{Q}_v) \otimes \mathbb{Z}/n\mathbb{Z} \arrow[r, hook] & \prod_v H^1(\mathrm{G}_{\mathbb{Q}_v}, E[n]) \end{tikzcd}$$

For all v at which E has good reduction and $E[n]$ is unramified, the image of κ_v consists exactly of the unramified classes, i.e. the image of $H^1(G_{\mathbb{F}_v}, E[n])$.

It follows that $|\mathrm{Sel}_n(E)| \approx |\mathrm{Sel}(E[n])|$.

Proof of 5-Torsion Bound

- Assume $E[5] = \mathbb{Z}/5\mathbb{Z} \oplus \mu_5$. *This is the only part of the proof which uses 5 and not a higher prime.*

Proof of 5-Torsion Bound

- Assume $E[5] = \mathbb{Z}/5\mathbb{Z} \oplus \mu_5$. *This is the only part of the proof which uses 5 and not a higher prime.*
- $E_D : y^2 = x^3 + AD^3X + BD^2$.

Proof of 5-Torsion Bound

- Assume $E[5] = \mathbb{Z}/5\mathbb{Z} \oplus \mu_5$. *This is the only part of the proof which uses 5 and not a higher prime.*
- $E_D : y^2 = x^3 + AD^3X + BD^2$.
- $E_D[5] = \chi_{D,5} \oplus \chi_{D,5}(1)$, where $\chi_{D,5} : \mathrm{G}_{\mathbb{Q}} \circlearrowright \mathbb{Z}/5\mathbb{Z}$ - quadratic character associated to $\mathbb{Q}(\sqrt{D})$.

Proof of 5-Torsion Bound

- Assume $E[5] = \mathbb{Z}/5\mathbb{Z} \oplus \mu_5$. *This is the only part of the proof which uses 5 and not a higher prime.*
- $E_D : y^2 = x^3 + AD^3X + BD^2$.
- $E_D[5] = \chi_{D,5} \oplus \chi_{D,5}(1)$, where $\chi_{D,5} : \mathrm{G}_{\mathbb{Q}} \circlearrowright \mathbb{Z}/5\mathbb{Z}$ - quadratic character associated to $\mathbb{Q}(\sqrt{D})$.
- $\mathrm{Sel}(E_D[5]) = \mathrm{Sel}(\chi_{D,5}) \oplus \mathrm{Sel}(\chi_{D,5}(1))$.

Proof of 5-Torsion Bound

- Assume $E[5] = \mathbb{Z}/5\mathbb{Z} \oplus \mu_5$. *This is the only part of the proof which uses 5 and not a higher prime.*
- $E_D : y^2 = x^3 + AD^3X + BD^2$.
- $E_D[5] = \chi_{D,5} \oplus \chi_{D,5}(1)$, where $\chi_{D,5} : \mathrm{G}_{\mathbb{Q}} \circlearrowright \mathbb{Z}/5\mathbb{Z}$ - quadratic character associated to $\mathbb{Q}(\sqrt{D})$.
- $\mathrm{Sel}(E_D[5]) = \mathrm{Sel}(\chi_{D,5}) \oplus \mathrm{Sel}(\chi_{D,5}(1))$.
- Since $\chi_{D,5}, \chi_{D,5}(1)$ are Cartier Dual, $|\mathrm{Sel}(\chi_{D,5})(1)| \approx |\mathrm{Sel}(\chi_{D,5}| \approx |\mathrm{Cl}_{\mathbb{Q}(\sqrt{D})}[5]|$.

Proof of 5-Torsion Bound

- Assume $E[5] = \mathbb{Z}/5\mathbb{Z} \oplus \mu_5$. *This is the only part of the proof which uses 5 and not a higher prime.*
- $E_D : y^2 = x^3 + AD^3X + BD^2$.
- $E_D[5] = \chi_{D,5} \oplus \chi_{D,5}(1)$, where $\chi_{D,5} : \mathrm{G}_{\mathbb{Q}} \circlearrowright \mathbb{Z}/5\mathbb{Z}$ - quadratic character associated to $\mathbb{Q}(\sqrt{D})$.
- $\mathrm{Sel}(E_D[5]) = \mathrm{Sel}(\chi_{D,5}) \oplus \mathrm{Sel}(\chi_{D,5}(1))$.
- Since $\chi_{D,5}, \chi_{D,5}(1)$ are Cartier Dual, $|\mathrm{Sel}(\chi_{D,5})(1)| \approx |\mathrm{Sel}(\chi_{D,5}| \approx |\mathrm{Cl}_{\mathbb{Q}(\sqrt{D})}[5]|$.

Key Relation

$$|\mathrm{Sel}(E_D[5])| = |\mathrm{Cl}_{\mathbb{Q}(\sqrt{D})}[5]|^2.$$

Proof: Analytic Details

- $0 \to E_D(\mathbb{Q}) \otimes \mathbb{F}_5 \to \mathrm{Sel}_5(E_D) \to Ш(E_D/\mathbb{Q})[5] \to 0$

Proof: Analytic Details

- $0 \to E_D(\mathbb{Q}) \otimes \mathbb{F}_5 \to \mathrm{Sel}_5(E_D) \to Ш(E_D/\mathbb{Q})[5] \to 0$
  So

$$|Ш(E_D/\mathbb{Q})| \geqslant |\mathrm{Sel}_5(E_D)| \cdot 5^{r_{E_D}+2} \succ |\mathrm{Sel}(E_D[5])| \cdot 5^{r_{E_D}+2}$$

Proof: Analytic Details

- $0 \to E_D(\mathbb{Q}) \otimes \mathbb{F}_5 \to \mathrm{Sel}_5(E_D) \to Ш(E_D/\mathbb{Q})[5] \to 0$
  So
  $$|Ш(E_D/\mathbb{Q})| \geqslant |\mathrm{Sel}_5(E_D)| \cdot 5^{r_{E_D}+2} \succ |\mathrm{Sel}(E_D[5])| \cdot 5^{r_{E_D}+2}$$
- $\mathrm{Sel}_2(E_D) \ll \omega(D) \Rightarrow r_{E_d} \ll \omega(D) = o(\ln(D))$

Proof: Analytic Details

- $0 \to E_D(\mathbb{Q}) \otimes \mathbb{F}_5 \to \mathrm{Sel}_5(E_D) \to Ш(E_D/\mathbb{Q})[5] \to 0$
  So
  $$|Ш(E_D/\mathbb{Q})| \geqslant |\mathrm{Sel}_5(E_D)| \cdot 5^{r_{E_D}+2} \succ |\mathrm{Sel}(E_D[5])| \cdot 5^{r_{E_D}+2}$$

- $\mathrm{Sel}_2(E_D) \ll \omega(D) \Rightarrow r_{E_d} \ll \omega(D) = o(\ln(D))$
- $\mathrm{Reg}_E \geqslant |D|^{o(1)}$ since $E_D(\mathbb{Q}) \otimes \mathbb{Q}$ has dimension $o(\ln(D))$, and Neron-Tate height is bounded below.

Proof: Analytic Details

- $0 \to E_D(\mathbb{Q}) \otimes \mathbb{F}_5 \to \mathrm{Sel}_5(E_D) \to Ш(E_D/\mathbb{Q})[5] \to 0$
  So
  $$|Ш(E_D/\mathbb{Q})| \geqslant |\mathrm{Sel}_5(E_D)| \cdot 5^{r_{E_D}+2} \succ |\mathrm{Sel}(E_D[5])| \cdot 5^{r_{E_D}+2}$$

- $\mathrm{Sel}_2(E_D) \ll \omega(D) \Rightarrow r_{E_d} \ll \omega(D) = o(\ln(D))$
- $\mathrm{Reg}_E \geqslant |D|^{o(1)}$ since $E_D(\mathbb{Q}) \otimes \mathbb{Q}$ has dimension $o(\ln(D))$, and Neron-Tate height is bounded below.
- $\frac{L^{(r_E)}(E_D,1)}{r_E!} \ll D^{\frac{1}{2}-\frac{1}{8}+o(1)}$ - Subconvexity estimate+Cauchy integral formula (Harcos)

Proof: Analytic Details

- $0 \to E_D(\mathbb{Q}) \otimes \mathbb{F}_5 \to \mathrm{Sel}_5(E_D) \to Ш(E_D/\mathbb{Q})[5] \to 0$
  So
  $$|Ш(E_D/\mathbb{Q})| \geqslant |\mathrm{Sel}_5(E_D)| \cdot 5^{r_{E_D}+2} \succ |\mathrm{Sel}(E_D[5])| \cdot 5^{r_{E_D}+2}$$
- $\mathrm{Sel}_2(E_D) \ll \omega(D) \Rightarrow r_{E_d} \ll \omega(D) = o(\ln(D))$
- $\mathrm{Reg}_E \geqslant |D|^{o(1)}$ since $E_D(\mathbb{Q}) \otimes \mathbb{Q}$ has dimension $o(\ln(D))$, and Neron-Tate height is bounded below.
- $\frac{L^{(r_E)}(E_D,1)}{r_E!} \ll D^{\frac{1}{2}-\frac{1}{8}+o(1)}$ - Subconvexity estimate+Cauchy integral formula (Harcos)
- $H_{E_D} \sim |D|^6$

Proof: Analytic Details

- $0 \to E_D(\mathbb{Q}) \otimes \mathbb{F}_5 \to \mathrm{Sel}_5(E_D) \to Ш(E_D/\mathbb{Q})[5] \to 0$
  So
  $$|Ш(E_D/\mathbb{Q})| \geqslant |\mathrm{Sel}_5(E_D)| \cdot 5^{r_{E_D}+2} \succ |\mathrm{Sel}(E_D[5])| \cdot 5^{r_{E_D}+2}$$

- $\mathrm{Sel}_2(E_D) \ll \omega(D) \Rightarrow r_{E_d} \ll \omega(D) = o(\ln(D))$
- $\mathrm{Reg}_E \geqslant |D|^{o(1)}$ since $E_D(\mathbb{Q}) \otimes \mathbb{Q}$ has dimension $o(\ln(D))$, and Neron-Tate height is bounded below.
- $\frac{L^{(r_E)}(E_D,1)}{r_E!} \ll D^{\frac{1}{2}-\frac{1}{8}+o(1)}$ - Subconvexity estimate+Cauchy integral formula (Harcos)
- $H_{E_D} \sim |D|^6$
- Refined BSD$\Rightarrow |\mathrm{Cl}_{\mathbb{Q}(\sqrt{D})}[5]|^2 \approx |\mathrm{Sel}(E_D[5])| \leqslant |D|^{\frac{1}{2}+\frac{1}{2}-\frac{1}{8}+o(1)}$

Primes $p > 5$

- There is no $E/\mathbb{Q}$ with $E[p] = \mathbb{Z}/p\mathbb{Z} \oplus \mu_p$. Note that having a p-torsion point is not enough!

Primes $p > 5$

- There is no $E/\mathbb{Q}$ with $E[p] = \mathbb{Z}/p\mathbb{Z} \oplus \mu_p$. Note that having a p-torsion point is not enough!
- We win with BSD+subconvexity if we can find Abelian Variety over $\mathbb{Q}$ with full level p-structure.

Primes $p > 5$

- There is no $E/\mathbb{Q}$ with $E[p] = \mathbb{Z}/p\mathbb{Z} \oplus \mu_p$. Note that having a p-torsion point is not enough!
- We win with BSD+subconvexity if we can find Abelian Variety over $\mathbb{Q}$ with full level p-structure.
- For motives M, have Bloch Kato + (Equivariant) Tamagawa number conjecture. Highly conjectural, not so clear (to me!) how to systematically find embeddings $\mathrm{Sel}(A) \hookrightarrow H^1(M)$.

Primes $p > 5$

- There is no $E/\mathbb{Q}$ with $E[p] = \mathbb{Z}/p\mathbb{Z} \oplus \mu_p$. Note that having a p-torsion point is not enough!
- We win with BSD+subconvexity if we can find Abelian Variety over $\mathbb{Q}$ with full level p-structure.
- For motives M, have Bloch Kato + (Equivariant) Tamagawa number conjecture. Highly conjectural, not so clear (to me!) how to systematically find embeddings $\mathrm{Sel}(A) \hookrightarrow H^1(M)$.
- Concretely, for $X/\mathbb{Q}$ smooth projective, $M = H^i(X)(j)$. Want

$$H^i(X_{\overline{\mathbb{Q}}}, \mathbb{F}_\ell(j)) = (\mathbb{Z}/p\mathbb{Z})^a \oplus (\mu_p)^b.$$

Do these exist?

Thank you!