F a number field, $E/_F$ an elliptic curve, p an odd prime ≥ 5.

Mordell-Weil: $E(F)$ is a finitely generated abelian group.
$r(E)$ = rank of $E(F)$.

B-SD Conjecture: (Weak form) $L(E,s)$: Hasse-Weil L-function of E
"arithmetic rank": Order of vanishing of $L(E,s)$ at $s=1$.

- Analogue of the classical Riemann Zeta function in context of elliptic curves.

B-SD Conjecture predicts that $r(E)$ = arithmetic rank of E.

Strong form of B-SD: An exact formula for L-value in terms of deep and mysterious arithmetic objects associated to E.

Iwasawa theory: "p-adic" in nature, provides a philosophical framework that explains this mysterious connection predicted by B-SD Conjecture.

Counter intuitive! This connection occurs by viewing objects associated to E over infinite Galois extensions associated to E of the base field F.

To such objects ("Selmer groups") one associates a "p-adic L-function" and a "characteristic element", both of these are elements in a common "Iwasawa algebra".

The p-adic L-function $\mathcal{L}_p(E,s)$ interpolates complex L-values, and the Characteristic power series can be related to $r(E)$.

The "main Conjecture" in Iwasawa theory predicts that these two elements generate the same ideal in the Iwasawa algebra. Thus the B-SD conjecture is to be viewed as two "descent manifestations" of invariants associated to a common object over an infinite extension of F!

$E/_F$ number field, $p \geq 5$ prime.

$F_\infty/_F$ a Galois extension, $G = Gal(F_\infty/_F)$.

<u>Assume:</u> G is pro-p, contains no elements of order p, G is a p-adic analytic group.

Eg. $G \simeq \mathbb{Z}_p$, $F_\infty = F_{cyc} \subseteq \bigcup_{n \geq 0} F(\mu_{p^n})$; μ_{p^n} : p^n-th roots of unity.

- K an imaginary quadratic field, F_∞ = Composite of all linearly independent $\mathbb{Z}_p$-extensions of K
  $$G = Gal(F_\infty/_K) \simeq \mathbb{Z}_p^2.$$

- $F \supseteq E[p]$, the p-torsion elements of $E(\bar{F})$; assume E has no complex multiplication i.e. $End(\bar{E}) \simeq \mathbb{Z}$.

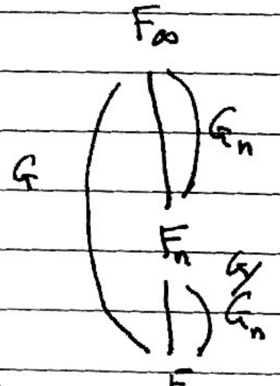
$$E[p^\infty] = \bigcup_{n \geq 0} E[p^n] ; \quad F_\infty = F(E_{p^\infty}).$$

$Gal(F_\infty/_F) = G \subseteq Gl_2(\mathbb{Z}_p)$, equal for almost all p (Serre).

<u>Iwasawa algebra:</u> G as above, Iwasawa algebra over G.

$$\Lambda(G) = \varprojlim_{G_n \trianglelefteq^{o} G} \mathbb{Z}_p \left[G/_{G_n} \right]$$

$F_\infty = \varinjlim F_n$, F_n finite layers of F in F_∞.



- S : finite set of primes of F containing the primes above p, the primes of bad reduction of E.

- F_S : Maximal unramified outside S extension of F, so F_{cyc} and $F(E_{p^\infty})$ are both contained in F_S.

Selmer group: $[L:F]<\infty$, Galois extension, $L \subseteq F_S$.

$$\begin{array}{c} F_S \\ | \\ L \\ | \\ F \end{array}$$

$$Sel_{p^\infty}(E/L) \subseteq H^1(F_{S}/L, E_{p^\infty}).$$

$$0 \to Sel_{p^\infty}(E/L) \to H^1(F_S/L, E_{p^\infty}) \to \bigoplus_{v\in S} J_v(E_{p^\infty}/L)$$

$$J_v(E_{p^\infty}/L) = \bigoplus_{w|v} H^1(F_w, E)(p).$$

The above sequence is an exact sequence of $Gal(L/F)$-modules.

If $\mathcal{L}/F$ is an infinite Galois extension with $\mathcal{G} = Gal(\mathcal{L}/F)$ then taking direct limits over finite extensions $F \subseteq L_n \subseteq \mathcal{L}$, we have

$$0 \to Sel_{p^\infty}(E/\mathcal{L}) \to H^1(F_S/\mathcal{L}, E_{p^\infty}) \to \bigoplus_{v\in S} J_v(E_{p^\infty}/\mathcal{L}) \to$$

This is an exact sequence of $\Lambda(\mathcal{G})$-modules; $\Lambda(\mathcal{G})$ is compact topological $\mathbb{Z}_p$-algebra, above modules are discrete $\Lambda(\mathcal{G})$-modules. Work with

$$X_{p^\infty}(E/\mathcal{L}) := Hom(Sel_{p^\infty}(E/\mathcal{L}), \mathbb{Q}_p/\mathbb{Z}_p), \text{ compact module.}$$

$$0 \to E(\mathcal{L}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to Sel_{p^\infty}(E/\mathcal{L}) \to Ш(E_{p^\infty}/\mathcal{L}) \to 0$$

Ш: Tate-Shafarevich gp; $Ker(H^1(\mathcal{L}, E)(p) \to \prod_w H^1(\mathcal{L}_w, E)(p))$.

Structure Theorem for f.g. compact modules over $\Lambda(G)$ due to Serre-Iwasawa.

$$G \simeq \mathbb{Z}_p,\ \Lambda(G) \simeq \mathbb{Z}_p[[T]],\quad G \simeq \mathbb{Z}_p^d,\ \Lambda(G) \simeq \mathbb{Z}_p[[T_1, \ldots, T_d]].$$

M a f.g. $\Lambda(G)$-module, $M \sim N$, N a f.g. $\Lambda(G)$-module means "M is pseudoisomorphic to N" $\rightsquigarrow$ $\exists$ a $\Lambda(G)$-hom φ

$$M \xrightarrow{\varphi} N$$

such that $\ker\varphi$ and $\operatorname{coker}\varphi$ have Krull dimension at most ~~eq~~ $\dim(\Lambda(G)) - 2$.

Structure Theorem: M a f.g. $\Lambda(G)$-module, $G \simeq \mathbb{Z}_p$, so $\Lambda(G) \simeq \mathbb{Z}_p[[T]]$.
Then

$$M \sim \Lambda(G)^{m} \oplus \bigoplus_{i=1}^{k} \Lambda/_{p^{n_i}} \oplus \bigoplus_{j=1}^{r} \Lambda/_{f_j^{m_j}},$$

where $f_j \in \mathbb{Z}_p[T]$ is a distinguished polynomial.

Invariants: m = rank of M, $\mu(M) = \sum_{i=1}^{k} n_i$, $\lambda(M) = \sum_{j=1}^{r} m_j \deg f_j$.

When $M = X_\infty$ = Dual Selmer group of E over F_∞/F, these invariants encode information on the M–W ranks of E/F_n.

Our results below are framed in the following context, joint with Sören Kleine and Ahmed Ali Matar.

E/K elliptic curve, K imaginary quadratic field
K_∞/K composite of all $\mathbb{Z}_p$-extensions of K, $G = \mathrm{Gal}(K_\infty/K) \simeq \mathbb{Z}_p^2$.

$K \subseteq H_\infty \subseteq K_\infty$ an intermediary $\mathbb{Z}_p$-extension.

$$H = \mathrm{Gal}(K_\infty/H_\infty) \simeq \mathbb{Z}_p, \quad \Gamma_H \simeq \mathrm{Gal}(H_\infty/K) \simeq \mathbb{Z}_p. \qquad G$$

$$\begin{array}{c} K_\infty \\ \Big| \; H \\ H_\infty \\ \Big| \; \Gamma_H \\ K \end{array}$$

$X(E/H_\infty)$: Dual Selmer group of E over H_∞.

$\mu_{H_\infty}, \lambda_{H_\infty}$ associated invariants. Note $\Lambda_H \subseteq \Lambda_G$.

Greenberg: $\mathcal{E}$:= Set of all $\mathbb{Z}_p$-extensions of K contained in K_∞

$$\updownarrow$$

$$\mathbb{P}^1(\mathbb{Z}_p)$$

$G = \langle \sigma, \tau \rangle \qquad (a,b) \in \mathbb{P}^1(\mathbb{Z}_p) \longmapsto \overline{\langle \sigma^a \tau^b \rangle}$

Camlin

Topology on $\mathcal{E}$: $L \in \mathcal{E}$, $n \in \mathbb{Z}^{+}$, $\mathcal{E}(L,n) := \{L' \in \mathcal{E} \mid [L' \cap L] : K \geq p^n\}$ base.

A neighbourhood consists of all $\mathbb{Z}_p$-extensions of K contained in K_∞ that coincide with L at least up to the n^{th}-layer.

- $X(E/K_\infty)$ is a compact, f.g. $\Lambda(G)$-module.

$$\begin{tikzcd} K_\infty \arrow[d, dash, "H"'] \\ K_\infty^H = H_\infty \arrow[d, dash, "\Gamma_H"'] \\ F \end{tikzcd}$$

$\mathfrak{M}_H(G)$-Conjecture: $\dfrac{X(E/K_\infty)}{X(E/K_\infty)(p)} =: X_f(E/K_\infty)$ is a finitely generated $\Lambda(H)$-module.

Easy to see that $\mu_{E,H_\infty} = 0 \iff X(E/K_\infty)$ is f.g. over $\Lambda(H)$.

$\mathfrak{M}_H(G)$ Conjecture asserts that $X_f(E/K_\infty)$ is f.g. over $\Lambda(H)$.

<u>Known</u>: If $X(E/H_\infty)$ is a f.g. torsion $\Lambda(\Gamma_H)$-module, then $X(E/H'_\infty)$ is also f.g. torsion $\Lambda(\Gamma_{H'})$-module for H' in a neighbourhood of H in $\mathcal{E}$.

<u>Def</u>: $\mathcal{H} \subseteq \mathcal{E}$; $H \in \mathcal{H}$, $H = \overline{\langle \sigma^a, \tau^b \rangle}$, $(a,b) \in \mathbb{P}^1(\mathbb{Z}_p)$ such that:

(a) No prime of S splits completely in K_∞^H/K

(b) Every prime of K above p ramifies in K_∞^H/K

(c) $X(E/K_\infty^H)$ is a torsion $\Lambda(\Gamma_H) = \Lambda(G/H)$-module.

<u>Prop</u>: $\mathcal{H}$ is non-empty for all but finitely many $(a,b) \in \mathbb{P}^1(\mathbb{Z}_p)$.

<u>Conjecture</u> (Mazur): The Mordell-Weil rank of E stays bounded along any $\mathbb{Z}_p$-extension of the imaginary quadratic field K, unless the extension is the anticyclotomic extension and the root number of E/K is -1.

Our results seem to manifest some surprising connections between $\mathfrak{M}_H(G)$-Conjecture and Mazur's conjecture.

$\mathcal{H}$ as above, $\mathcal{H} \neq \phi$; $\Lambda(G) \simeq \mathbb{Z}_p[[T_1, T_2]]$. Assume E has good ordinary reduction at the primes above p in K. Then it is known that $X(E/K_\infty)$ is a f.g. torsion Λ_G-module.

Theorem 1: Assume $\mathcal{H} \neq \phi$. Then $X(E/K_\infty)$ is a torsion $\Lambda(G)$-module. For any $H = \langle \sigma^a \tau^b \rangle \in \mathcal{H}$, the TFAE:

$$\begin{tikzcd} K_\infty \arrow[d, dash, "H"'] \\ H_\infty = K_\infty^H \arrow[d, dash, "\Gamma_H"'] \\ K \end{tikzcd}$$

(a) $X(E/K_\infty)_f$ is f.g. over $\Lambda(H)$ (i.e. the $\mathfrak{M}_H(G)$-conjecture holds for E).

(b) $\mu_G(X(E/K_\infty)) = \mu_{\Gamma_H}(X(E/H_\infty))$.

(c) $\lambda(X(E/\mathcal{L}))$ is bounded as $\mathcal{L}$ varies through the elements in a neighbourhood of $H \in \mathcal{H}$.

(d) If $E_{p^\infty}(K_\infty)$ is finite, then the above are equivalent to

$$X(E/K_\infty)_f \hookrightarrow (\Lambda_H)^{\lambda_H}, \text{ with } \lambda_H \geq \lambda\text{-invariant of } X(E/H_\infty).$$

Theorem 2: Let t be the numbers of $\mathbb{Z}_p$-extensions of K where the rank of E does not stay bounded. Then

$$t \leq \min\{\lambda_H \mid H \in \Sigma\}, \text{ where } \Sigma = \left\{ H \in \mathcal{H} \text{ s.t. } X(E/K_\infty)_f \text{ is f.g as a } \Lambda_H\text{-module} \right.$$

In other words, suppose $\mathfrak{M}_H(G)$-conjecture holds for a $H \in \mathcal{E}$. Then can bound the number of $\mathbb{Z}_p$-extensions where $rk(E)$ is unbounded.

Rem: $K/\mathbb{Q}$ abelian, $K_{cyc} \in \mathcal{H}$.

Theorem: Assume that p is odd. If rank $E(K)=0$, and $Ш(E/K)(p^\infty)$ is finite then Mazur's Conjecture is true.

In the rank one case, use results of Kundu-Ray to obtain cases where Mazur's conjecture holds.

Theorem: Assume p odd and unramified in $K/\mathbb{Q}$. Suppose rank $E(K)=1$, $Ш(E/K)(p^\infty)=0$, the p-adic valuation of the p-adic regulator of E and its quadratic twist are at most 1. Also assume:

- primes dividing N (Conductor of E) split in $K/\mathbb{Q}$.
- $p \nmid \prod_\ell c_\ell(E) \cdot c_\ell(E^K)$ (c_ℓ: Tamagawa number)
- $p \nmid \# \tilde{E}(\mathbb{F}_p) \cdot \# \tilde{E}^{(K)}(\mathbb{F}_p)$.

Then Mazur's conjecture is true.

Eg: $E = 43a1$, $K = \mathbb{Q}(\sqrt{-3})$, $p = 11, 13, 17, 19$

$E = 58a1$, $K = \mathbb{Q}(\sqrt{-7})$, $p = 5, 11, 13, 17$

$E = 61a1$, $K = \mathbb{Q}(i)$, $p = 5, 11, 17, 19$.

- Results in the supersingular setting.
- Proofs are technical and delicate, analyse the cyclotomic case $H_\infty = K_{cyc}$ and see how these can be carried over to $H \in \mathcal{H}$.