Chabauty–Kim and the locally geometric section conjecture

Martin Lüdtke
joint with Alex Betts and Theresa Kumpitsch

Rijksuniversiteit Groningen

Intercity Number Theory Seminar
Amsterdam, 9th June 2023

1. The Selmer Section Conjecture

Grothendieck's letter to Faltings

In a letter to Faltings from 1983, Grothendieck lays out his vision of what he calls anabelian geometry.

Grothendieck -> Faltings 1

27.6.1983

Lieber Herr Falting,

Vielen Dank für Ihre rasche Antwort und Übersendung der Separate! Ih
Kommentar zur sog. "Theorie der Motive" ist von der üblichen Art, die woh
grossenteils der in der Mathematik stark eingewurzelten Tradition ent-
springt, nur denjenigen mathematischen Situationen und Zusammenhängen
einer (eventuell langatmiger) Untersuchung und Aufmerksamkeit zuzuwenden,
insofern sie die Hoffnung gewähren, nicht nur zu einem vorläufigen und
möglicherweise z.T. mutmasslichen Verständnis eines Bisher geheimnisvoll
Gebiets zu kommen, wie es in den Naturwissenschaften ja gang und gäbe is
– sondern auch zugleich Aussicht auf die Möglichkeit einer laufenden Abe
cherung der gewonnenen Einsichten durch stichhaltige Beweise. Diese Ein-
stellung scheint mir nun psychologisch ein ausserordentlich starkes Hinde

Idea: recover information about a scheme from its profinite étale fundamental group

Example: number fields are determined by their absolute Galois group (Neukirch–Uchida):

$$G_K \cong G_L \Rightarrow K \cong L.$$

Fundamental exact sequence

Let $X/\mathbb{Q}$ be a smooth projective curve of genus ≥ 2.

Grothendieck's section conjecture predicts that the set of rational points $X(\mathbb{Q})$ can be recovered from the étale fundamental group.

The maps

$$X_{\overline{\mathbb{Q}}} \to X \to \mathrm{Spec}(\mathbb{Q})$$

induce an exact sequence

$$1 \to \pi_1^{\text{ét}}(X_{\overline{\mathbb{Q}}}) \to \pi_1^{\text{ét}}(X) \to G_{\mathbb{Q}} \to 1 \tag{FES}$$

on profinite étale fundamental groups: the fundamental exact sequence.

If $x \in X(\mathbb{Q})$ is a rational point, it induces a section s_x of (FES), well-defined up to $\pi_1^{\text{ét}}(X_{\overline{\mathbb{Q}}})$-conjugation. So we have a section map

$$X(\mathbb{Q}) \to \mathrm{Sec}(X/\mathbb{Q}) := \{\text{sections of (FES)}\}/\sim\ . \tag{S}$$

The Section Conjecture

Section Conjecture (Grothendieck, 1983)

If $X/\mathbb{Q}$ is a smooth projective curve of genus ≥ 2, then (S) is bijection $X(\mathbb{Q}) \cong \mathrm{Sec}(X/\mathbb{Q})$.

- (S) is known to be injective. The question is whether it is surjective.
- Some examples of X have been constructed where one can show that $\mathrm{Sec}(X/\mathbb{Q}) = \emptyset$ (Stix, Li–Litt–Salter–Srinivasan). In these cases, (S) is bijective automatically.
- In general, $\mathrm{Sec}(X/\mathbb{Q})$ is very mysterious (we don't know $G_{\mathbb{Q}}$!).

Open Question

Can we find some X with $X(\mathbb{Q}) \neq \emptyset$ for which the Section Conjecture holds?

Selmer sections

If s is a section of the fundamental exact sequence and p is prime, then the restriction $s|_{G_p}$ is a section of the local fundamental exact sequence

$$1 \to \pi_1^{\text{ét}}(X_{\overline{\mathbb{Q}}_p}) \to \pi_1^{\text{ét}}(X_{\mathbb{Q}_p}) \to G_p \to 1\,.$$

Definition

We say that s is Selmer (or sometimes locally geometric or adelic) if $s|_{G_p}$ comes from a $\mathbb{Q}_p$-rational point $x_p \in X(\mathbb{Q}_p)$ for all primes p. We write $\mathrm{Sec}(X/\mathbb{Q})^{\mathrm{Sel}}$ for the set of Selmer sections.

So we have

$$X(\mathbb{Q}) \subseteq \mathrm{Sec}(X/\mathbb{Q})^{\mathrm{Sel}} \subseteq \mathrm{Sec}(X/\mathbb{Q})\,.$$

Selmer Section Conjecture

If $X/\mathbb{Q}$ is a smooth projective curve of genus ≥ 2, then

$$\mathrm{Sec}(X/\mathbb{Q})^{\mathrm{Sel}} = X(\mathbb{Q})\,.$$

Main point of this talk:

> *One can use the Chabauty–Kim method to prove instances of the Selmer Section Conjecture.*

Let p be some auxiliary prime and let U be a $G_{\mathbb{Q}}$-equivariant quotient of the $\mathbb{Q}_p$-pro-unipotent étale fundamental group of $X_{\overline{\mathbb{Q}}}$ (at some rational basepoint). We have the Chabauty–Kim diagram

$$\begin{array}{ccc} X(\mathbb{Q}) & \hookrightarrow & X(\mathbb{Q}_p) \\ \downarrow j & & \downarrow j_p \\ \mathrm{Sel}_U(X/\mathbb{Q})(\mathbb{Q}_p) & \xrightarrow{\mathrm{loc}_p} & \mathrm{H}^1_f(G_p, U(\mathbb{Q}_p)) \end{array}$$

where $\mathrm{Sel}_U(X/\mathbb{Q})$ is the global Selmer scheme of Balakrishnan–Dan-Cohen–Kim–Wewers[1].

[1] *A non-abelian conjecture of Tate–Shafarevich type*

The Chabauty–Kim method

$$\begin{array}{ccc} X(\mathbb{Q}) & \hookrightarrow & X(\mathbb{Q}_p) \\ \downarrow j & & \downarrow j_p \\ \mathrm{Sel}_U(X/\mathbb{Q})(\mathbb{Q}_p) & \xrightarrow{\mathrm{loc}_p} & \mathrm{H}^1_f(G_p, U(\mathbb{Q}_p)) \end{array}$$

Fact: loc_p is an algebraic map of affine $\mathbb{Q}_p$-schemes

Strategy:

- show that loc_p is not dominant (e.g., for dimension reasons)
- find $0 \neq f\colon \mathrm{H}^1_f(G_p, U) \to \mathbb{A}^1$ vanishing on $\mathrm{im}(\mathrm{loc}_p)$
- the pullback $f \circ j_p\colon X(\mathbb{Q}_p) \to \mathbb{Q}_p$ is a nonzero p-adic analytic function whose vanishing set is finite and contains $X(\mathbb{Q})$

Definition

The Chabauty–Kim locus associated to U is the set

$$X(\mathbb{Q}_p)_U \coloneqq \{x \in X(\mathbb{Q}_p) \ : \ j_p(x) \in \mathrm{im}(\mathrm{loc}_p)\} \subseteq X(\mathbb{Q}_p)\,.$$

Commutativity of the Chabauty–Kim diagram gives

$$X(\mathbb{Q}) \subseteq X(\mathbb{Q}_p)_U \subseteq X(\mathbb{Q}_p)\,.$$

In the particular case that U is the whole fundamental group, we write $X(\mathbb{Q}_p)_\infty$ for $X(\mathbb{Q}_p)_U$. This is contained in all other $X(\mathbb{Q}_p)_U$'s.

Kim's Conjecture

$$X(\mathbb{Q}_p)_\infty = X(\mathbb{Q}).$$

Kim's conjecture implies Selmer Section Conjecture

We make precise the relationship between Kim's Conjecture and the Selmer Section Conjecture.

Theorem A (Betts–Kumpitsch–L.), projective case

Let $X/\mathbb{Q}$ be a smooth projective curve of genus ≥ 2 with $X(\mathbb{Q}) \neq \emptyset$. Suppose that Kim's Conjecture holds for (X, p) for p in a set $\mathfrak{P}$ of primes of Dirichlet density 1. Then the Selmer Section Conjecture holds for X.

This gives a new strategy for proving instances of the Selmer Section Conjecture.

We show that the strategy is viable by verifying the hypotheses in an example of an *affine* hyperbolic curve, the thrice-punctured line over $\mathbb{Z}[1/2]$.

Generalisation: S-integral points

Now fix a finite set S of primes. Let $Y/\mathbb{Q}$ be a hyperbolic curve, and let $\mathcal{Y}/\mathbb{Z}_S$ be an S-integral model of Y.

Definition

A section s of the fundamental exact sequence for Y is S-Selmer (with respect to the model $\mathcal{Y}$) if $s|_{G_p}$ comes from a

$$\begin{cases} \mathbb{Q}_p\text{-rational point } y_p \in Y(\mathbb{Q}_p) & \text{if } p \in S, \\ \mathbb{Z}_p\text{-integral point } y_p \in \mathcal{Y}(\mathbb{Z}_p) & \text{if } p \notin S, \end{cases}$$

for all primes p. We write $\mathrm{Sec}(\mathcal{Y}/\mathbb{Z}_S)^{\mathrm{Sel}}$ for the set of S-Selmer sections.

So we have

$$\mathcal{Y}(\mathbb{Z}_S) \subseteq \mathrm{Sec}(\mathcal{Y}/\mathbb{Z}_S)^{\mathrm{Sel}} \subseteq \mathrm{Sec}(Y/\mathbb{Q}).$$

Conjecture (S-Selmer Section Conjecture)

$$\mathrm{Sec}(\mathcal{Y}/\mathbb{Z}_S)^{\mathrm{Sel}} = \mathcal{Y}(\mathbb{Z}_S).$$

Chabauty–Kim for S-integral points

There is also a version of the Chabauty–Kim method which applies to S-integral points on $\mathcal{Y}$. For any $p \notin S$ and any $G_{\mathbb{Q}}$-equivariant quotient U of the $\mathbb{Q}_p$-pro-unipotent étale fundamental group of $Y_{\overline{\mathbb{Q}}}$, this method defines a locus

$$\mathcal{Y}(\mathbb{Z}_S) \subseteq \mathcal{Y}(\mathbb{Z}_p)_{S,U} \subseteq \mathcal{Y}(\mathbb{Z}_p)\,.$$

Kim's Conjecture

$$\mathcal{Y}(\mathbb{Z}_p)_{S,\infty} = \mathcal{Y}(\mathbb{Z}_S)\,.$$

Theorem A, general case

Theorem A (Betts–Kumpitsch–L.)

Let $\mathcal{Y}/\mathbb{Z}_S$ be a hyperbolic curve whose smooth completion has a $\mathbb{Q}$-rational point. Suppose that Kim's Conjecture holds for $(\mathcal{Y}, S, p)$ for p in a set $\mathfrak{P}$ of primes of Dirichlet density 1. Then the S-Selmer Section Conjecture holds for $(\mathcal{Y}, S)$.

Remark: If $Y = X$ is projective, then everything in sight is independent of the choice of set S and model $\mathcal{Y}$, and this specialises to the earlier projective statement.

Theorem B

We can verify the hypotheses of Theorem A in one example.

Theorem B (Betts–Kumpitsch–L.)

Let $\mathcal{Y} = \mathbb{P}^1_{\mathbb{Z}[1/2]} \smallsetminus \{0, 1, \infty\}$ be the thrice-punctured line over $\mathbb{Z}[1/2]$. Then Kim's Conjecture holds for $(\mathcal{Y}, \{2\}, p)$ for all odd primes p.

Consequence: The S-Selmer Section Conjecture holds for $\mathcal{Y} = \mathbb{P}^1_{\mathbb{Z}[1/2]} \smallsetminus \{0, 1, \infty\}$ and $S = \{2\}$.

2. Proof of Theorem A

Theorem A, projective case

Let $X/\mathbb{Q}$ be a smooth projective curve of genus ≥ 2 with $X(\mathbb{Q}) \neq \emptyset$. Suppose that Kim's Conjecture holds for (X, p) for p in a set $\mathfrak{P}$ of primes of Dirichlet density 1. Then the Selmer Section Conjecture holds for X.

From now on, we fix some $X/\mathbb{Q}$ and $\mathfrak{P}$ as above.

Let $s \in \mathrm{Sec}(X/\mathbb{Q})^{\mathrm{Sel}}$ be a Selmer section, so $s|_{G_p}$ is induced by some $x_p \in X(\mathbb{Q}_p)$ for all primes p.

Claim

$x_p \in X(\mathbb{Q}_p)_\infty$ for all primes p.

Proof: Let $\Pi = \pi_1^{\text{ét}}(X_{\overline{\mathbb{Q}}}, b)$ be the profinite étale fundamental group based at some $b \in X(\mathbb{Q})$. The section map

$$X(\mathbb{Q}) \to \mathrm{Sec}(X/\mathbb{Q})$$

can be identified with the map

$$X(\mathbb{Q}) \to \mathrm{H}^1(G_{\mathbb{Q}}, \Pi)$$

sending a point $x \in X(\mathbb{Q})$ to the cocycle $c\colon G_{\mathbb{Q}} \to \Pi$ measuring the difference between the two sections s_b and s_x:

$$c(\sigma) = s_x(\sigma) s_b(\sigma)^{-1}.$$

Have a similar local section map $X(\mathbb{Q}_\ell) \to \mathrm{H}^1(G_\ell, \Pi)$.

The $\mathbb{Q}_p$-pro-unipotent étale fundamental group U of $X_{\overline{\mathbb{Q}}}$ is the $\mathbb{Q}_p$-Malčev completion of Π, i.e., the universal pro-unipotent group over $\mathbb{Q}_p$ with a continuous homomorphism

$$\phi\colon \Pi \to U(\mathbb{Q}_p)\,.$$

For any prime ℓ, we then have a commuting diagram

$$\begin{array}{ccccc} & & \mathrm{H}^1(G_{\mathbb{Q}}, \Pi) & \xrightarrow{\phi_*} & \mathrm{H}^1(G_{\mathbb{Q}}, U(\mathbb{Q}_p)) \\ & & \downarrow{\scriptstyle \mathrm{loc}_\ell} & & \downarrow{\scriptstyle \mathrm{loc}_\ell} \\ X(\mathbb{Q}_\ell) & \longrightarrow & \mathrm{H}^1(G_\ell, \Pi) & \xrightarrow{\phi_*} & \mathrm{H}^1(G_\ell, U(\mathbb{Q}_p)) \end{array}$$

Selmer sections: elements of $\mathrm{H}^1(G_{\mathbb{Q}}, \Pi)$ locally coming from $X(\mathbb{Q}_\ell)$
Selmer scheme: elements of $\mathrm{H}^1(G_{\mathbb{Q}}, U(\mathbb{Q}_p))$ locally coming from $X(\mathbb{Q}_\ell)$

Since s is Selmer, $\phi_*(s) \in \mathrm{H}^1(G_{\mathbb{Q}}, U(\mathbb{Q}_p))$ lies in the Selmer scheme $\mathrm{Sel}_\infty(X/\mathbb{Q})$.

Take $\ell = p$ in the above diagram and restrict to Selmer elements:

$$\begin{array}{ccccc} & & s \in \mathrm{Sec}(X/\mathbb{Q})^{\mathrm{Sel}} & \xrightarrow{\phi_*} & \mathrm{Sel}_\infty(X/\mathbb{Q})(\mathbb{Q}_p) \\ & & \downarrow \mathrm{loc}_p & & \downarrow \mathrm{loc}_p \\ x_p \in X(\mathbb{Q}_p) & \longrightarrow & \mathrm{H}^1(G_p, \Pi) & \xrightarrow{\phi_*} & \mathrm{H}^1(G_p, U(\mathbb{Q}_p)) \end{array}$$

Hence

$$j_p(x_p) = \mathrm{loc}_p(\phi_*(s)) \in \mathrm{loc}_p(\mathrm{Sel}_\infty(X/\mathbb{Q})),$$

and so $x_p \in X(\mathbb{Q}_p)_\infty$ as claimed. □

If Kim's Conjecture holds for (X, p) for all $p \in \mathfrak{P}$, then the preceding claim shows that each

$$x_p \in X(\mathbb{Q}) \subseteq X(\mathbb{Q}_p)$$

is one of the finitely many rational points on X. Two questions:

1. Must the rational points x_p for $p \in \mathfrak{P}$ be the *same*?
2. Even if the rational points x_p are the same rational point x, must s be the section associated to x?

These are both resolved using a theorem of Stoll.

Theorem (Harari–Stix, 2012)

$(x_p)_p \in X(\mathbb{A}_{\mathbb{Q}}^f)$ is the adelic point associated to a Selmer section s if and only if $(x_p)_p \in X(\mathbb{A}_{\mathbb{Q}}^f)^{\mathrm{fcov}}$ lies in the finite descent locus.

Theorem of the Diagonal (Stoll, 2007)

Let $Z \subset X$ be a finite subscheme, and let $(x_p)_p \in X(\mathbb{A}_{\mathbb{Q}}^f)^{\mathrm{fcov}}$ be an adelic point in the finite descent locus. If $x_p \in Z(\mathbb{Q}_p)$ for a density 1 set of primes p, then $(x_p)_p \in Z(\mathbb{Q})$ is a rational point of Z.

Now return to the setting that $(x_p)_p$ is the adelic point associated to a Selmer section s, so $(x_p)_p \in X(\mathbb{A}_{\mathbb{Q}}^f)^{\mathrm{fcov}}$, and assume that $x_p \in X(\mathbb{Q})$ for all $p \in \mathfrak{P}$.

Claim

There is a rational point $x \in X(\mathbb{Q})$ such that $x_p = x$ for all p.

Proof: Apply the Theorem of the Diagonal to the finite subscheme Z consisting of the rational points of X. □

Claim

s is the section attached to x.

Proof (sketch): It suffices to prove that s is the section attached to some rational point. According to a theorem of Tamagawa, it is equivalent to show that for every finite étale covering $\pi \colon X' \to X$ such that s lifts to a section $s' \in \mathrm{Sec}(X'/\mathbb{Q})$, we have $X'(\mathbb{Q}) \neq \emptyset$. The section s' is automatically Selmer, and its associated adelic point $(x'_p)_p$ satisfies $x'_p \in \pi^{-1}(x)(\mathbb{Q}_p)$ for all p. Applying the Theorem of the Diagonal to $\pi^{-1}(x)$ shows that $X'(\mathbb{Q}) \neq \emptyset$. □

3. Proof of Theorem B

Theorem B, recap

Theorem B

Let $\mathcal{Y} = \mathbb{P}^1_{\mathbb{Z}[1/2]} \setminus \{0, 1, \infty\}$ be the thrice-punctured line over $\mathbb{Z}[1/2]$. Then Kim's Conjecture holds for $(\mathcal{Y}, \{2\}, p)$ for all odd primes p.

From now on, we fix $\mathcal{Y} = \mathbb{P}^1_{\mathbb{Z}[1/2]} \setminus \{0, 1, \infty\}$, $S = \{2\}$ and p an odd prime. We write $Y = \mathcal{Y}_{\mathbb{Q}}$.

Recall that Kim's conjecture says that the inclusion

$$\mathcal{Y}(\mathbb{Z}[1/2]) \subseteq \mathcal{Y}(\mathbb{Z}_p)_{\{2\},\infty}$$

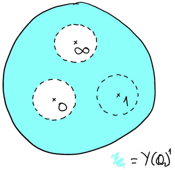
is an equality.

Note that $\mathbb{Z}[1/2]^\times = \{\pm 2^n : n \in \mathbb{Z}\}$ and

$$\mathcal{Y}(\mathbb{Z}[1/2]) = \{z \in \mathbb{Z}[1/2]^\times \text{ s.t. } 1 - z \in \mathbb{Z}[1/2]^\times\} = \{2, -1, \tfrac{1}{2}\}.$$

Components of the Selmer scheme

Consider the mod 2 reduction map



$$\mathrm{red}_2\colon\ Y(\mathbb{Q}_2) \subseteq \mathbb{P}^1(\mathbb{Q}_2) = \mathbb{P}^1(\mathbb{Z}_2) \twoheadrightarrow \mathbb{P}^1(\mathbb{F}_2).$$

For each cusp $\Sigma \in \{0, 1, \infty\}$ define

$$\mathcal{Y}(\mathbb{Z}[1/2])^{\Sigma} := \{z \in \mathcal{Y}(\mathbb{Z}[1/2]) : \mathrm{red}_2(z) \in \mathcal{Y} \cup \{\Sigma\}\}.$$

This partitions the $\mathbb{Z}[1/2]$-integral points into

$$\mathcal{Y}(\mathbb{Z}[1/2]) = \mathcal{Y}(\mathbb{Z}[1/2])^0 \cup \mathcal{Y}(\mathbb{Z}[1/2])^1 \cup \mathcal{Y}(\mathbb{Z}[1/2])^{\infty}.$$

This corresponds to the irreducible components of the Selmer scheme:

$$\mathrm{Sel}_{\infty}(\mathcal{Y}/\mathbb{Z}[1/2]) = \mathrm{Sel}_{\infty}(\mathcal{Y}/\mathbb{Z}[1/2])^0 \cup \mathrm{Sel}_{\infty}(\mathcal{Y}/\mathbb{Z}[1/2])^1 \cup \mathrm{Sel}_{\infty}(\mathcal{Y}/\mathbb{Z}[1/2])^{\infty}.$$

Reduction to the 1-component

Accordingly, the Chabauty–Kim locus is a union of three subsets

$$\mathcal{Y}(\mathbb{Z}_p)_{\{2\},\infty} = \mathcal{Y}(\mathbb{Z}_p)^0_{\{2\},\infty} \cup \mathcal{Y}(\mathbb{Z}_p)^1_{\{2\},\infty} \cup \mathcal{Y}(\mathbb{Z}_p)^\infty_{\{2\},\infty}.$$

We have $\mathcal{Y}(\mathbb{Z}[1/2])^\Sigma \subseteq \mathcal{Y}(\mathbb{Z}_p)^\Sigma_{\{2\},\infty}$, conjecturally an equality.

The automorphisms of $\mathbb{P}^1_{\mathbb{Z}[1/2]} \setminus \{0,1,\infty\}$,

$$z, \quad \frac{1}{z}, \quad 1-z, \quad \frac{1}{1-z}, \quad \frac{z-1}{z}, \quad \frac{z}{z-1},$$

permute the three cusps transitively. By exploiting this, it suffices to take $\Sigma = 1$ and prove that

$$\{-1\} = \mathcal{Y}(\mathbb{Z}[1/2])^1 \subseteq \mathcal{Y}(\mathbb{Z}_p)^1_{\{2\},\infty}$$

is an equality.

The localisation map

It suffices to replace the full fundamental group U with its polylogarithmic quotient U_{PL}. Prior work by Corwin–Dan-Cohen implies that the localisation map

$$\mathrm{loc}_p\colon \mathrm{Sel}_{\mathrm{PL}}(\mathcal{Y}/\mathbb{Z}[1/2])^1 \to \mathrm{H}^1_f(G_p, U_{\mathrm{PL}})$$

is given by

$$\mathrm{loc}_p\colon \operatorname{Spec} \mathbb{Q}_p[y, z_3, z_5, z_7, \ldots] \to \operatorname{Spec} \mathbb{Q}_p[\log, \mathrm{Li}_1, \mathrm{Li}_2, \mathrm{Li}_3, \ldots],$$

$$\begin{aligned}
\mathrm{loc}_p^\sharp \log &= 0, \\
\mathrm{loc}_p^\sharp \mathrm{Li}_1 &= \log(2) y, \\
\mathrm{loc}_p^\sharp \mathrm{Li}_2 &= 0, \\
\mathrm{loc}_p^\sharp \mathrm{Li}_3 &= \zeta(3) z_3, \\
\mathrm{loc}_p^\sharp \mathrm{Li}_4 &= 0, \\
\mathrm{loc}_p^\sharp \mathrm{Li}_5 &= \zeta(5) z_5, \\
&\vdots
\end{aligned}$$

Coleman functions vanishing on the Chabauty–Kim locus

We find infinitely many functions on $\mathrm{H}^1_f(G_p, U_{\mathrm{PL}})$ which vanish on the image of the Selmer scheme. Pulling back the functions along j_p shows:

Proposition

The following functions vanish on the Chabauty–Kim locus $\mathcal{Y}(\mathbb{Z}_p)^1_{\{2\},\infty}$:

$$\log(z) \quad \textit{and} \quad \mathrm{Li}_k(z) \textit{ for } k \geq 2 \textit{ even.}$$

Here, log and Li_k are p-adic analytic functions on $\mathcal{Y}(\mathbb{Z}_p)$ defined as iterated Coleman integrals:

$$\log(z) = \int_0^z \frac{\mathrm{d}z}{z}, \quad \mathrm{Li}_k(z) = \int_0^z \underbrace{\frac{\mathrm{d}z}{z} \cdots \frac{\mathrm{d}z}{z} \frac{\mathrm{d}z}{1-z}}_{k}.$$

Proof of Kim's conjecture

We are reduced to proving:

Proposition

The only common zero in $\mathcal{Y}(\mathbb{Z}_p)$ of the functions $\log(z)$ and $\mathrm{Li}_k(z)$ for $k \geq 2$ even is $z = -1$.

$\log(z) = 0$ implies that z is a $(p-1)$-st root of unity in $\mathbb{Z}_p$.

Li_k has a mod-p variant $\mathrm{li}_k \colon \mathbb{F}_p \to \mathbb{F}_p$ given by

$$\mathrm{li}_k(z) = \sum_{i=1}^{p-1} \frac{z^i}{i^k}.$$

$\mathrm{Li}_k(z) = 0$ implies $\mathrm{li}_k(\overline{z}) = 0$. Take $k = p-3$ and use little Fermat:

$$\mathrm{li}_{p-3}(z) = \sum_{i=1}^{p-1} i^{-(p-3)} z^i = \sum_{i=1}^{p-1} i^2 z^i = z(z+1)(z-1)^{p-3}.$$

Proof of Kim's conjecture

At this point we have:

(1) $z \in \mathcal{Y}(\mathbb{Z}_p)$

(2) z is a $(p-1)$-st root of unity

(3) $\bar{z} := z \bmod p$ is a zero of $\mathrm{li}_{p-3}(z) = z(z+1)(z-1)^{p-3}$

(3) implies $\bar{z} \in \{0, -1, 1\}$.

But by (1), $\bar{z}$ is in $\mathcal{Y}(\mathbb{F}_p) = \mathbb{F}_p \smallsetminus \{0, 1\}$, so $\bar{z} = -1$.

Finally, (2) implies $z = -1$.

This shows that

$$\{-1\} = \mathcal{Y}(\mathbb{Z}[1/2])^1 \subseteq \mathcal{Y}(\mathbb{Z}_p)^1_{\{2\},\infty}$$

is an equality, hence Kim's conjecture holds.

4. Summary

Summary of main results

Theorem A

Let $\mathcal{Y}/\mathbb{Z}_S$ be a hyperbolic curve whose smooth completion has a $\mathbb{Q}$-rational point. Suppose that Kim's Conjecture holds for $(\mathcal{Y}, S, p)$ for p in a set $\mathfrak{P}$ of primes of Dirichlet density 1. Then the S-Selmer Section Conjecture holds for $(\mathcal{Y}, S)$.

Theorem B

Let $\mathcal{Y} = \mathbb{P}^1_{\mathbb{Z}[1/2]} \smallsetminus \{0, 1, \infty\}$ be the thrice-punctured line over $\mathbb{Z}[1/2]$. Then Kim's Conjecture holds for $(\mathcal{Y}, \{2\}, p)$ for all odd primes p.

Further reading: *Chabauty–Kim and the Section Conjecture for locally geometric sections* (arXiv:2305.09462)

Thank you for listening