Explicit realization of elements of the Tate-Shafarevich group constructed from Kolyvagin classes

Lazar Radicevic

January 21, 2022

Hasse principle for genus one curves

The plane cubic C

$$3x^3 + 4y^3 + 5z^3 = 0$$

is a counterexample to the Hasse principle. A famous result of Selmer is that it has points over every completion of $\mathbb{Q}$, but no $\mathbb{Q}$-points.

Hasse principle for genus one curves

The plane cubic C

$$3x^3 + 4y^3 + 5z^3 = 0$$

is a counterexample to the Hasse principle. A famous result of Selmer is that it has points over every completion of $\mathbb{Q}$, but no $\mathbb{Q}$-points.
C is a smooth curve of genus one, with Jacobian elliptic curve E defined by the equation $x^3 + y^3 + 60z^3 = 0$. The failure of the Hasse principle for C can be interpreted as saying that C represents a non-trivial element of $\text{Ш}(E/\mathbb{Q})[3]$.

Hasse principle for genus one curves

The plane cubic C

$$3x^3 + 4y^3 + 5z^3 = 0$$

is a counterexample to the Hasse principle. A famous result of Selmer is that it has points over every completion of $\mathbb{Q}$, but no $\mathbb{Q}$-points.

C is a smooth curve of genus one, with Jacobian elliptic curve E defined by the equation $x^3 + y^3 + 60z^3 = 0$. The failure of the Hasse principle for C can be interpreted as saying that C represents a non-trivial element of $\text{Ш}(E/\mathbb{Q})[3]$.

In this talk we give a method to compute genus one curves that are counterexamples to the Hasse principle, and correspond to elements of $\text{Ш}(E/\mathbb{Q})[p]$, for various elliptic curves E and all odd prime $p \leq 11$.

n-diagrams and the n-Selmer group

Let k be a field, E/k an elliptic curve, $n \geq 2$ an integer. An n-diagram for E is a morphism $[C \to \mathbb{P}^{n-1}]$, where C is a genus one curve that is a torsor for E, and the morphism is induced by a complete linear system associated to a k-rational divisor D on E, of degree n.

n-diagrams and the n-Selmer group

Let k be a field, E/k an elliptic curve, $n \geq 2$ an integer. An n-diagram for E is a morphism $[C \to \mathbb{P}^{n-1}]$, where C is a genus one curve that is a torsor for E, and the morphism is induced by a complete linear system associated to a k-rational divisor D on E, of degree n.

We say diagrams $[C_1 \to \mathbb{P}^{n-1}]$ and $[C_2 \to \mathbb{P}^{n-2}]$ are isomorphic if we have a commutative diagram:

$$\begin{array}{ccc} C_1 & \longrightarrow & \mathbb{P}^{n-1} \\ \wr\downarrow & & \wr\downarrow \\ C_2 & \longrightarrow & \mathbb{P}^{n-1} \end{array}$$

Let k be a field, E/k an elliptic curve, $n \geq 2$ an integer. An n-diagram for E is a morphism $[C \to \mathbb{P}^{n-1}]$, where C is a genus one curve that is a torsor for E, and the morphism is induced by a complete linear system associated to a k-rational divisor D on E, of degree n.
We say diagrams $[C_1 \to \mathbb{P}^{n-1}]$ and $[C_2 \to \mathbb{P}^{n-2}]$ are isomorphic if we have a commutative diagram:

$$\begin{array}{ccc} C_1 & \longrightarrow & \mathbb{P}^{n-1} \\ \wr\downarrow & & \wr\downarrow \\ C_2 & \longrightarrow & \mathbb{P}^{n-1} \end{array}$$

To any rational point $P \in E(k)$ we associate (isomorphism class of) the n-diagram $[E \to \mathbb{P}^{n-1}]$, where the morphism is induced by the complete linear system $|(n-1) \cdot 0_E + P|$.

n-diagrams and the n-Selmer group

Proposition

Isomorphism classes of n-diagrams defined over k parametrize a certain subset of the group $H^1(k, E[n])$. Under this parametrization, if E is defined over $\mathbb{Q}$, the elements of $\mathrm{Sel}^{(n)}(E/\mathbb{Q})$ are represented by the n-diagrams $[C \to \mathbb{P}^{n-1}]$, where the curve C is everywhere locally soluble.

n-diagrams and the n-Selmer group

Proposition

Isomorphism classes of n-diagrams defined over k parametrize a certain subset of the group $H^1(k, E[n])$. Under this parametrization, if E is defined over $\mathbb{Q}$, the elements of $\mathrm{Sel}^{(n)}(E/\mathbb{Q})$ are represented by the n-diagrams $[C \to \mathbb{P}^{n-1}]$, where the curve C is everywhere locally soluble.

We have the short exact sequence

$$0 \to E(\mathbb{Q})/nE(\mathbb{Q}) \xrightarrow{\delta} \mathrm{Sel}^{(n)}(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})[n] \to 0$$

The Kummer map δ sends a class $[P] \in E(k)/nE(k)$ into the diagram $[E \to \mathbb{P}^{n-1}]$, determined by the complete linear system $|(n-1)\cdot 0_E + P|$, and the second map sends $[C \to \mathbb{P}^{n-1}]$ to (the class of) torsor C.

Let $[C \to \mathbb{P}^{n-1}]$ be an n-diagram. For $n \geq 3$, it is a closed embedding, and the image is a smooth genus one curve of degree n. For $n = 2$, it is a double cover of $\mathbb{P}^1$. It can be represented by a *genus one model* of degree n. For small n, this is the data of the equations that define C:

- $n = 2$: a binary quartic: $y^2 = f(x, z)$
- $n = 3$: a ternary cubic: $\{F(x, y, z) = 0\} \subset \mathbb{P}^2$
- $n = 4$: a pair of quaternary quadratic forms : $\{F(x_1, x_2, x_3, x_4) = G(x_1, x_2, x_3, x_4) = 0\} \subset \mathbb{P}^3$

For $n \geq 5$, the ideal defining C is generated by $n(n-3)/2$ quadrics, and C is no longer a complete intersection.

- A genus one model of a given n-diagram $[C \to \mathbb{P}^{n-1}]$ is far from unique. There are two reasons for this: we are free to make projective changes of coordinates on the ambient space $\mathbb{P}^{n-1}$, and the equations that define the curve C are not unique.
- For example, if F is a ternary cubic and $g \in \mathrm{GL}_n(\mathbb{Q})$, $F(x, y, z)$ and $F((x, y, z) \cdot g)$ represent the same diagram, as well as $\lambda \cdot F$ for any $\lambda \in \mathbb{Q}$.
- This is encoded in the action of a group $\mathcal{G}_n$, which is a product of several GL_n's, on the space X_n of genus one models of degree n. Every n-diagram $[C \to \mathbb{P}^{n-1}]$ gives rise to a well-defined equivalence class in $\mathcal{G}_n(\mathbb{Q})\backslash X_n(\mathbb{Q})$.

- Minimization theorem: n-diagrams $[C \to \mathbb{P}^{n-1}]$ that represent elements of the Selmer group, so that curve C is everywhere locally soluble, admit nice integral models.
- A minimal model $F \in X_n(\mathbb{Z})$ of $[C \to \mathbb{P}^{n-1}]$ will have small integral coefficients and nice properties. For example, if the curve E has good reduction at a prime p, then the reduction of C modulo p will be a smooth curve of genus one.

Heegner points and Kolyvagin classes

- $E/\mathbb{Q}$ an elliptic curve of conductor N, with a fixed modular parametrization $\phi : X_0(N) \to E$ that maps the cusp ∞ to 0_E.

Heegner points and Kolyvagin classes

- $E/\mathbb{Q}$ an elliptic curve of conductor N, with a fixed modular parametrization $\phi : X_0(N) \to E$ that maps the cusp ∞ to 0_E.
- $K = \mathbb{Q}(\sqrt{-D})$ an imaginary quadratic field, of discriminant $-D \neq 3, 4$ and with ring of integers $\mathcal{O}_K$.

Heegner points and Kolyvagin classes

- $E/\mathbb{Q}$ an elliptic curve of conductor N, with a fixed modular parametrization $\phi : X_0(N) \to E$ that maps the cusp ∞ to 0_E.
- $K = \mathbb{Q}(\sqrt{-D})$ an imaginary quadratic field, of discriminant $-D \neq 3, 4$ and with ring of integers $\mathcal{O}_K$.
- Assume the *Heegner hypothesis*: all prime factors of N split in K, and choose a factorization of the ideal $N\mathcal{O}_K = \mathcal{N}\bar{\mathcal{N}}$ with $\mathcal{O}_K/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$.

Heegner points and Kolyvagin classes

- $E/\mathbb{Q}$ an elliptic curve of conductor N, with a fixed modular parametrization $\phi : X_0(N) \to E$ that maps the cusp ∞ to 0_E.
- $K = \mathbb{Q}(\sqrt{-D})$ an imaginary quadratic field, of discriminant $-D \neq 3, 4$ and with ring of integers $\mathcal{O}_K$.
- Assume the *Heegner hypothesis*: all prime factors of N split in K, and choose a factorization of the ideal $N\mathcal{O}_K = \mathcal{N}\bar{\mathcal{N}}$ with $\mathcal{O}_K/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$.
- $\mathcal{O}_K$ and $\mathcal{N}^{-1}$ are lattices in $\mathbb{C}$, and the map $\mathbb{C}/\mathcal{O}_K \to \mathbb{C}/\mathcal{N}^{-1}$ is a cyclic isogeny of complex torii, of degree N, and hence corresponds to a point x of $X_0(N)(\mathbb{C})$.

Complex multiplication: $x \in X_0(N)(L)$, where L is the Hilbert class field of K. We define the Heegner point to be $x_K = \phi(x) \in E(L)$. The trace $y_K = \mathrm{Tr}_{L/K}(x_K) \in E(K)$ is also sometimes called a Heegner point.

Complex multiplication: $x \in X_0(N)(L)$, where L is the Hilbert class field of K. We define the Heegner point to be $x_K = \phi(x) \in E(L)$. The trace $y_K = \mathrm{Tr}_{L/K}(x_K) \in E(K)$ is also sometimes called a Heegner point.

Theorem

(Kolyvagin) Assume that the point y_K has infinite order in $E(K)$. Then

- *The group $E(K)$ has rank 1, so the index $I_K = [E(K) : \mathbb{Z}y_K]$ is finite.*
- *The group $\text{Ш}(E/K)$ is finite, of order dividing $t_{E/K} I_K^2$. The number $t_{E/K}$ is a positive integer whose prime factors depend only on the curve E: they consist of 2 and the odd primes p where the Galois group of the extension of $\mathbb{Q}(E[p])/\mathbb{Q}$ is smaller than expected.*

Thus, if $p || \text{Ш}(E/\mathbb{Q})|$, it often follows that $p | I_K$, and hence y_K is divisible by p in $E(L)$.

- Let $p \geq 3$ be a prime, and assume that: K has class number p, p divides y_K in $E(L)$, $E(L)[p]$ is trivial, and that $E/\mathbb{Q}$ has rank 0.

- Let $p \geq 3$ be a prime, and assume that: K has class number p, p divides y_K in $E(L)$, $E(L)[p]$ is trivial, and that $E/\mathbb{Q}$ has rank 0.
- Then $L/\mathbb{Q}$ is a dihedral extension of degree $2p$, with the Galois group G generated by an element σ of order p and a lift of complex conjugation τ.

- Let $p \geq 3$ be a prime, and assume that: K has class number p, p divides y_K in $E(L)$, $E(L)[p]$ is trivial, and that $E/\mathbb{Q}$ has rank 0.
- Then $L/\mathbb{Q}$ is a dihedral extension of degree $2p$, with the Galois group G generated by an element σ of order p and a lift of complex conjugation τ.
- Define $D_\sigma = \sum_{i=1}^{p-1} i\sigma^i \in \mathbb{Z}[G]$ and $\mathrm{Tr} = \sum_{i=0}^{p-1} \sigma^i \in \mathbb{Z}[G]$. Then we have $(\sigma - 1)D_\sigma = p - \mathrm{Tr}$. The point $D_\sigma x_K$ is known as the derived Heegner point.

$$(\sigma - 1)D_\sigma x_K = (p - \mathrm{Tr})x_K = px_K - y_K \in pE(L)$$

and hence $[D_\sigma x_K] \in (E(L)/pE(L))^{\mathrm{Gal}(L/K)}$.

- $E(L)/pE(L)$ splits into $\pm$-eigenspaces for the action of τ, where $\pm$ is the sign of the functional equation of E. If E has rank 0, we have $[D_\sigma x_K] \in (E(L)/pE(L))^{\mathrm{Gal}(L/\mathbb{Q})}$.

- Let $\delta : E(L)/pE(L) \to H^1(L, E[p])$ be the Kummer map, and set $c_L = \delta[D_\sigma x_K]$. Kummer map is Galois equivariant, so $c_L \in H^1(L, E[p])^{\mathrm{Gal}(L/\mathbb{Q})}$.

- Let $\delta : E(L)/pE(L) \to H^1(L, E[p])$ be the Kummer map, and set $c_L = \delta[D_\sigma x_K]$. Kummer map is Galois equivariant, so $c_L \in H^1(L, E[p])^{\mathrm{Gal}(L/\mathbb{Q})}$.
- We have the inflation-restriction exact sequence

$$H^1(\mathrm{Gal}(L/\mathbb{Q}), E[p](L)) \xrightarrow{inf} H^1(\mathbb{Q}, E[p]) \xrightarrow{res} H^1(L, E[p])^{\mathrm{Gal}(L/\mathbb{Q})} \to$$
$$\to H^2(\mathrm{Gal}(L/\mathbb{Q}), E[p](L))$$

- Let $\delta : E(L)/pE(L) \to H^1(L, E[p])$ be the Kummer map, and set $c_L = \delta[D_\sigma x_K]$. Kummer map is Galois equivariant, so $c_L \in H^1(L, E[p])^{\mathrm{Gal}(L/\mathbb{Q})}$.
- We have the inflation-restriction exact sequence

$$H^1(\mathrm{Gal}(L/\mathbb{Q}), E[p](L)) \xrightarrow{inf} H^1(\mathbb{Q}, E[p]) \xrightarrow{res} H^1(L, E[p])^{\mathrm{Gal}(L/\mathbb{Q})} \to$$
$$\to H^2(\mathrm{Gal}(L/\mathbb{Q}), E[p](L))$$

- By assumption, the outermost groups are trivial, so the restriction map is an isomorphism. We define the Kolyvagin class $c_\mathbb{Q} \in H^1(\mathbb{Q}, E[p])$ as $c_\mathbb{Q} = res^{-1}(c_L)$. In fact, we have $c_\mathbb{Q} \in \mathrm{Sel}^{(p)}(E/\mathbb{Q})$.

- Let $\delta : E(L)/pE(L) \to H^1(L, E[p])$ be the Kummer map, and set $c_L = \delta[D_\sigma x_K]$. Kummer map is Galois equivariant, so $c_L \in H^1(L, E[p])^{\mathrm{Gal}(L/\mathbb{Q})}$.
- We have the inflation-restriction exact sequence

$$H^1(\mathrm{Gal}(L/\mathbb{Q}), E[p](L)) \xrightarrow{inf} H^1(\mathbb{Q}, E[p]) \xrightarrow{res} H^1(L, E[p])^{\mathrm{Gal}(L/\mathbb{Q})} \to$$
$$\to H^2(\mathrm{Gal}(L/\mathbb{Q}), E[p](L))$$

- By assumption, the outermost groups are trivial, so the restriction map is an isomorphism. We define the Kolyvagin class $c_{\mathbb{Q}} \in H^1(\mathbb{Q}, E[p])$ as $c_{\mathbb{Q}} = res^{-1}(c_L)$. In fact, we have $c_{\mathbb{Q}} \in \mathrm{Sel}^{(p)}(E/\mathbb{Q})$.
- Our aim will be to compute a minimal model of the diagram $[C \to \mathbb{P}^{p-1}]$ representing the class $c_{\mathbb{Q}}$.

Computing the diagram representing $c_{\mathbb{Q}}$

- Fix a degree p divisor D with $\mathrm{sum}_E D = D_\sigma x_K$. For example, $D = (p-1)0_E + D_\sigma x_K$. Next, fix a basis of the Riemann-Roch space $\mathcal{L}(D)$ - space of rational functions on E which have poles at bounded by D. These choices determine a morphism $E \to \mathbb{P}^{p-1}$.

Computing the diagram representing $c_{\mathbb{Q}}$

- Fix a degree p divisor D with $\mathrm{sum}_E D = D_\sigma x_K$. For example, $D = (p-1)0_E + D_\sigma x_K$. Next, fix a basis of the Riemann-Roch space $\mathcal{L}(D)$ - space of rational functions on E which have poles at bounded by D. These choices determine a morphism $E \to \mathbb{P}^{p-1}$.
- The class c_L is Galois invariant. In terms of p-diagrams, this means, for any $g \in G$:

$$\begin{array}{ccc} E & \xrightarrow{|D|} & \mathbb{P}^{p-1} \\ \downarrow{\scriptstyle \tau_{R_g}} & & \downarrow{\scriptstyle M_g} \\ E & \xrightarrow{|g(D)|} & \mathbb{P}^{p-1} \end{array}$$

- The map $g \mapsto M_g$ is a 1-cocycle of G valued in $\mathrm{PGL}_p(L)$: we have $M_{gh} = M_g g(M_h)$.

- First step: compute the cocycle M_g. This is done by an explicit calculation: for a certain choice of D and a basis of $\mathcal{L}(D)$, we have formulas for the matrices M_g in terms of the coordinates of the Heegner point.
- In fact, these formulas provide matrices with $M_g \in \mathrm{GL}_p(L)$. In other words, we have a lift of the cocycle $g \mapsto M_g$ to GL_p, so the map $g \mapsto M_g$ is an element of $Z^1(G, GL_p(L))$.

- First step: compute the cocycle M_g. This is done by an explicit calculation: for a certain choice of D and a basis of $\mathcal{L}(D)$, we have formulas for the matrices M_g in terms of the coordinates of the Heegner point.
- In fact, these formulas provide matrices with $M_g \in \mathrm{GL}_p(L)$. In other words, we have a lift of the cocycle $g \mapsto M_g$ to GL_p, so the map $g \mapsto M_g$ is an element of $Z^1(G, GL_p(L))$.
- By standard facts about Galois descent, the data of this cocycle is equivalent to the data of a semilinear action of $G = \mathrm{Gal}(L/\mathbb{Q})$ on the L-vector space $\mathcal{L}(D)$:

$$g(\alpha \cdot v) = g(\alpha)g(v)$$

  for all $g \in G$, $\alpha \in L$, $v \in \mathcal{L}(D)$.
- Formulas for the matrices M_g translate into formulas for a matrix representation of this action.

- The set of invariant vectors $\mathcal{L}(D)^G$ is a p-dimensional $\mathbb{Q}$-vector space, and a $\mathbb{Q}$-basis $l_1, \ldots, l_p$ of $\mathcal{L}(D)^G$ will also be an L-basis of $\mathcal{L}(D)$.
- The image of E in $\mathbb{P}^{p-1}$ under the embedding determined by $l_1, \ldots, l_p$ will be a curve C that admits a model defined over $\mathbb{Q}$, and the inclusion $C \subset \mathbb{P}^{p-1}$ is the n-diagram we are looking to construct.

- Heegner points that we consider often have very large height. Thus we need to be careful in choosing a basis of $\mathcal{L}(D)^G$, for otherwise we end up with models with enormous coefficients.

- Heegner points that we consider often have very large height. Thus we need to be careful in choosing a basis of $\mathcal{L}(D)^G$, for otherwise we end up with models with enormous coefficients.
- The idea, roughly, is to choose a $\mathbb{Q}$-basis $l_1, \ldots, l_p$ of $\mathcal{L}(D)^G$ that reduces, modulo any prime $\mathfrak{p}$ of good reduction of E, to a basis of $\mathcal{L}(\bar{D})$.
- Do this by carefully doing linear algebra over $\mathbb{Z}$, instead of over $\mathbb{Q}$.

- Toy example: $E/\mathbb{Q}$ an elliptic curve, with an equation $y^2 = x^3 + Ax + B$, $P = (x_P, y_P) \in E(\mathbb{Q})$.
- Let $p = 3$. The class $[P] \in E(\mathbb{Q})/3E(\mathbb{Q})$ determines a 3-diagram $[E \to \mathbb{P}^2]$, where the map is determined by the divisor $2 \cdot 2 \cdot 0_E + P$.

- Toy example: $E/\mathbb{Q}$ an elliptic curve, with an equation $y^2 = x^3 + Ax + B$, $P = (x_P, y_P) \in E(\mathbb{Q})$.
- Let $p = 3$. The class $[P] \in E(\mathbb{Q})/3E(\mathbb{Q})$ determines a 3-diagram $[E \to \mathbb{P}^2]$, where the map is determined by the divisor $2 \cdot 2 \cdot 0_E + P$.
- First attempt: We start by choosing a basis of $\mathcal{L}(2 \cdot 0_E + P)$. Simplest way to proceed: we take $1, x$, a basis of $\mathcal{L}(2 \cdot 0_E)$, together with $\frac{y+y_p}{x-x_P}$, which has a simple pole at at 0_E and at P.
- C is the image of the map $E \to \mathbb{P}^2$: $Q = (x, y) \mapsto (1 : x : \frac{y+y_P}{x-x_P})$. The image C is a plane cubic.

- If P has large height, the cubic form $F(X, Y, Z)$ cutting out C in $\mathbb{P}^2$ will have very large coefficients.
- Reason: Write $x_Q = r/t^2, y_Q = s/t^3$, where $r, s, t \in \mathbb{Z}$, then $\frac{y+y_P}{x-x_P} = \frac{t^3y+s}{t^3x-tr}$. Then $E \to \mathbb{P}^2$ is given by

$$(x, y) \mapsto (t : tx : \frac{t^3y + s}{t^2x - r})$$

- This does not reduce to an embedding for any prime q that divides t, i.e. exactly for those q for which P reduces to zero, and C will reduce to a singular curve modulo these primes.

- If P has large height, the cubic form $F(X, Y, Z)$ cutting out C in $\mathbb{P}^2$ will have very large coefficients.
- Reason: Write $x_Q = r/t^2, y_Q = s/t^3$, where $r, s, t \in \mathbb{Z}$, then $\frac{y+y_p}{x-x_P} = \frac{t^3y+s}{t^3x-tr}$. Then $E \to \mathbb{P}^2$ is given by

$$(x, y) \mapsto (t : tx : \frac{t^3y + s}{t^2x - r})$$

- This does not reduce to an embedding for any prime q that divides t, i.e. exactly for those q for which P reduces to zero, and C will reduce to a singular curve modulo these primes.
- To fix this, we want to instead use a basis of $\mathcal{L}(D)$ which reduces to a basis of $\mathcal{L}(\widetilde{D})$ for all q.

- Idea: replace D by the linearly equivalent divisor $4 \cdot 0_E - (-P)$.

- Idea: replace D by the linearly equivalent divisor $4 \cdot 0_E - (-P)$.
- $\mathcal{L}(D) \subset \mathcal{L}(4 \cdot 0_E)$.
- $1, x, y, x^2$ is a nice basis of $\mathcal{L}(4 \cdot 0_E)$, in the sense that the morphism $E \xrightarrow{(1:x:y:x^2)} \mathbb{P}^3$ reduces to an embedding modulo any prime q.

- Idea: replace D by the linearly equivalent divisor $4 \cdot 0_E - (-P)$.
- $\mathcal{L}(D) \subset \mathcal{L}(4 \cdot 0_E)$.
- $1, x, y, x^2$ is a nice basis of $\mathcal{L}(4 \cdot 0_E)$, in the sense that the morphism $E \xrightarrow{(1:x:y:x^2)} \mathbb{P}^3$ reduces to an embedding modulo any prime q.
- $\mathcal{L}(D)$ is the $\mathbb{Q}$-space of $\mathbb{Q}$-linear combinations of $1, x, y, x^2$ that vanish at $-P$.
- The basis of $\mathcal{L}(D)$ that we choose is one that is also a basis for the $\mathbb{Z}$-module of $\mathbb{Z}$-linear combinations of $1, x, y, x^2$ that vanish at $-P$.

- Idea: replace D by the linearly equivalent divisor $4 \cdot 0_E - (-P)$.
- $\mathcal{L}(D) \subset \mathcal{L}(4 \cdot 0_E)$.
- $1, x, y, x^2$ is a nice basis of $\mathcal{L}(4 \cdot 0_E)$, in the sense that the morphism $E \xrightarrow{(1:x:y:x^2)} \mathbb{P}^3$ reduces to an embedding modulo any prime q.
- $\mathcal{L}(D)$ is the $\mathbb{Q}$-space of $\mathbb{Q}$-linear combinations of $1, x, y, x^2$ that vanish at $-P$.
- The basis of $\mathcal{L}(D)$ that we choose is one that is also a basis for the $\mathbb{Z}$-module of $\mathbb{Z}$-linear combinations of $1, x, y, x^2$ that vanish at $-P$.
- Generalizes to $p > 3$, and to Kolyvagin classes, where we need to also keep track of the semilinear action of $\mathrm{Gal}(L/\mathbb{Q})$.

Computing the Heegner point itself

- The Galois conjugates of the point x_K are represented by the cyclic isogenies $\mathbb{C}/\mathfrak{a}_i \to \mathbb{C}/\mathfrak{a}_i\mathcal{N}^{-1}$, where $\mathfrak{a}$ ranges over a set of representatives of $\mathrm{Cl}K$.

Computing the Heegner point itself

- The Galois conjugates of the point x_K are represented by the cyclic isogenies $\mathbb{C}/\mathfrak{a}_i \to \mathbb{C}/\mathfrak{a}_i\mathcal{N}^{-1}$, where $\mathfrak{a}$ ranges over a set of representatives of $\mathrm{Cl}K$.
- Identify $Y_0(N)(\mathbb{C})$ with $H/\Gamma_0(N)$, and compute a τ_i in the upper half-plane for each conjugate of x_K.

Computing the Heegner point itself

- The Galois conjugates of the point x_K are represented by the cyclic isogenies $\mathbb{C}/\mathfrak{a}_i \to \mathbb{C}/\mathfrak{a}_i\mathcal{N}^{-1}$, where $\mathfrak{a}$ ranges over a set of representatives of $\mathrm{Cl}K$.
- Identify $Y_0(N)(\mathbb{C})$ with $H/\Gamma_0(N)$, and compute a τ_i in the upper half-plane for each conjugate of x_K.
- Let $f \in S_2(\Gamma_0(N))$ be the newform corresponding to E, and Λ a complex lattice such that $E \cong \mathbb{C}/\Lambda$. The modular parametrization $\phi : Y_0(N)(\mathbb{C}) \to \mathbb{C}/\Lambda$ is given by

$$\phi(\tau) = \int_\tau^\infty f(z)dz = \sum_{n\geq 1} \frac{a_n}{n} e^{2\pi i n\tau},$$

- Compute $\phi(\tau_i)$ to a high precision, and thus obtain approximations to the image of x_K in $E(\mathbb{C})$ for each embedding $\sigma : L \to \mathbb{C}$. Use lattice reduction to recover $x_K \in E(L)$.

- The standard method to recognize an algebraic number x from archimedean approximations of its Galois conjugates $x_1, \ldots, x_n$ is to compute an approximation to its minimal polynomial $f(T) = (T - x_1)(T - x_2) \cdots (T - x_n)$. Coefficients of f are rational numbers, so one can recognize them from floating point approximations using continued fractions or the LLL algorithm.

- The standard method to recognize an algebraic number x from archimedean approximations of its Galois conjugates $x_1, \ldots, x_n$ is to compute an approximation to its minimal polynomial $f(T) = (T - x_1)(T - x_2) \cdots (T - x_n)$. Coefficients of f are rational numbers, so one can recognize them from floating point approximations using continued fractions or the LLL algorithm.
- In our case, when p is large, this is very slow. When x has large height, the coefficients of f are symmetric polynomials in x_i, so they have even larger height.

- The standard method to recognize an algebraic number x from archimedean approximations of its Galois conjugates $x_1, \ldots, x_n$ is to compute an approximation to its minimal polynomial $f(T) = (T - x_1)(T - x_2) \cdots (T - x_n)$. Coefficients of f are rational numbers, so one can recognize them from floating point approximations using continued fractions or the LLL algorithm.
- In our case, when p is large, this is very slow. When x has large height, the coefficients of f are symmetric polynomials in x_i, so they have even larger height.
- Instead, we make use of the fact that L is a Hilbert class field. Before computing the Heegner point $x_K = (x, y)$, we compute L and its ring of integers $\mathcal{O}_L$.

- The idea is to try to guess u and v such that we $u + v \cdot x = 0$, with $u, v \in \mathcal{O}_L$, and recover x as $-u/v$.
- View $\mathcal{O}_L$ as a lattice in $\mathbb{R}^{2p}$ via the Minkowski embedding i. Let $\alpha_1, \ldots, \alpha_{2p}$ be a basis of $\mathcal{O}_L$, $x_1, \ldots, x_n$ conjugates of x.
- Write $u = u_1\alpha_1 + \ldots + u_{2p}\alpha_{2p}$, $v = v_1\alpha_1 + \ldots + v_{2p}\alpha_{2p}$. A relation $u + vx = 0$ is specified by a $\mathbb{Z}$-linear relation between $2p$ vectors in $\mathbb{R}^{2p}$: $i(\alpha_1), \ldots, i(\alpha_{2p}), i(\alpha_1 x), \ldots, i(\alpha_{2p} x)$.
- We then use a standard method to try to guess such a relation, using the LLL algorithm.

Examples

- Warmup: case $p = 3$, $E = 681b3$ in Cremona's tables. Smallest example of a curve with no 3-isogeny, and with $\text{Ш}(E/\mathbb{Q})[3] \cong (\mathbb{Z}/3\mathbb{Z})^2$.

$$E : y^2 + xy = x^3 + x^2 - 1154x - 15345$$

Take $K = \mathbb{Q}(\sqrt{-107})$, and find $L = \mathbb{Q}[\alpha]$, minimal polynomial of α is $x^6 - 2x^5 - 2x^3 + 30x^2 - 52x + 29$.

Examples

- Warmup: case $p = 3$, $E = 681b3$ in Cremona's tables. Smallest example of a curve with no 3-isogeny, and with $Ш(E/\mathbb{Q})[3] \cong (\mathbb{Z}/3\mathbb{Z})^2$.

$$E : y^2 + xy = x^3 + x^2 - 1154x - 15345$$

Take $K = \mathbb{Q}(\sqrt{-107})$, and find $L = \mathbb{Q}[\alpha]$, minimal polynomial of α is $x^6 - 2x^5 - 2x^3 + 30x^2 - 52x + 29$. The Kolyvagin class is $[D_\sigma R] \in E(L)/pE(L)$, where the x-coordinate of R is

$$1/74977794136(-10484343883\alpha^5 + 105552865682\alpha^4 - 221944788673\alpha^3 - 53131146267\alpha^2 + 678092277032\alpha - 2010522031643)$$

We then compute a G-invariant basis l_1, l_2 and l_3.

$$l_1 = (1/47(-649929\alpha^5 + 4887174\alpha^4 + 4393374\alpha^3 - 1637529\alpha^2 - 25060386\alpha + 26031148)x$$
$$+ 1/47(-12471488\alpha^5 + 94234104\alpha^4 + 84531516\alpha^3 - 31876664\alpha^2 - 482246120\alpha + 485403708))y$$
$$+ 1/94(62028175\alpha^5 + 3524414\alpha^4 - 184322318\alpha^3 - 313665289\alpha^2 + 981877558\alpha - 586773344)x^2$$
$$+ 1/94(1253471703\alpha^5 - 79436262\alpha^4 - 3800133240\alpha^3 - 6187922253\alpha^2$$
$$+ 20293856034\alpha - 12015089758)x + 1/47(339305237\alpha^5 + 3975834\alpha^4$$
$$- 1015927794\alpha^3 - 1700502019\alpha^2 + 5416956290\alpha + 989547264)$$
$$l_2 = (1/47(889658\alpha^5 - 5962716\alpha^4 - 5650332\alpha^3 + 1514426\alpha^2 + 32122676\alpha - 32405332)x$$
$$+ 1/94(70372977\alpha^5 - 230419010\alpha^4 - 326328436\alpha^3 - 121445875\alpha^2 + 1817224662\alpha - 1574470158))y$$
$$+ 1/47(-37512305\alpha^5 - 346372\alpha^4 + 112363729\alpha^3 + 187907897\alpha^2 - 599157764\alpha + 360922221)x^2$$
$$+ 1/94(-1364138531\alpha^5 + 234361318\alpha^4 + 4209596252\alpha^3$$
$$+ 6586331337\alpha^2 - 22529300450\alpha + 13482027010)x + 1/94(1126129237\alpha^5 + 1173434218\alpha^4$$
$$- 2791670602\alpha^3 - 6804080403\alpha^2 + 14497765138\alpha - 17913336552)$$
$$l_3 = (1/47(-1241268\alpha^5 + 2560152\alpha^4 + 5003880\alpha^3 + 3646188\alpha^2 - 27540744\alpha + 19648804)x$$
$$+ 1/94(-385145467\alpha^5 + 103142838\alpha^4 + 1207007820\alpha^3 + 1822584497\alpha^2$$
$$- 6471755986\alpha + 4141836330))y + 1/47(17035756\alpha^5 - 16327814\alpha^4 - 59271175\alpha^3$$
$$- 68850966\alpha^2 + 321555538\alpha - 228627841)x^2 + 1/47(98448242\alpha^5 - 698052044\alpha^4 - 644370748\alpha^3$$
$$+ 205810834\alpha^2 + 3669328004\alpha - 3498574700)x + 1/2(10400285\alpha^5 - 298652262\alpha^4$$
$$- 180526986\alpha^3 + 246650837\alpha^2 + 1062361346\alpha - 1192042808)$$

- The image of $E \to \mathbb{P}^2$ under the map $P \mapsto (l_1(P) : l_2(P) : l_3(P))$ is defined by

$$F = 3258x^3 + 8367x^2y + 909x^2z + 7157xy^2 +$$
$$1557xyz + 89xz^2 + 2039y^3 + 666y^2z + 76yz^2 + 3z^3$$

- The image of $E \to \mathbb{P}^2$ under the map $P \mapsto (l_1(P) : l_2(P) : l_3(P))$ is defined by

$$F = 3258x^3 + 8367x^2y + 909x^2z + 7157xy^2 + 1557xyz + 89xz^2 + 2039y^3 + 666y^2z + 76yz^2 + 3z^3$$

- Get a nicer equation using *reduction*. The $\mathrm{SL}_3(\mathbb{Z})$-change of variables corresponding to the matrix

$$\begin{pmatrix} 1 & -1 & -2 \\ -1 & 1 & 1 \\ -3 & 4 & -4 \end{pmatrix}$$

takes F to the cubic

$$G = x^3 - 5x^2y - 5x^2z + 2xy^2 + xyz + xz^2 - y^3 + 5y^2z - 2yz^2 - 6z^3$$

- An example of a 7-torsion element of Ш.
- $E = 3364c1$, defined by a minimal Weierstrass equation $y^2 = x^3 - 4062871x - 3152083138$
- We take $K = \mathbb{Q}(\sqrt{-71})$. The Kolyvagin class is $[D_\sigma R]$, where R is a point of height 194.99. We obtain a curve in $\mathbb{P}^6$, cut out by the 14 quadrics:

$$f_1 = 5x_1x_6 + 2x_1x_7 + x_2x_3 + 3x_2x_4 - 4x_2x_6 - x_2x_7 + x_3^2 - 3x_3x_4 -$$
$$3x_3x_5 + 3x_3x_6 + x_3x_7 + 2x_4^2 + 3x_4x_5 - 5x_4x_6 - 5x_4x_7 + x_5^2 + 2x_5x_6 - 3x_6^2 - 2x_7^2$$
$$f_2 = 3x_1^2 - x_1x_3 - x_1x_4 + 2x_1x_5 - 3x_1x_6 + 3x_1x_7 - 2x_2^2 + 2x_2x_5 -$$
$$2x_2x_6 - 4x_2x_7 + x_3^2 - x_3x_4 - 2x_3x_5 - x_3x_6 - 3x_3x_7 + x_4^2 + 2x_4x_5 - 7x_4x_7 + 5x_5x_6 - 3x_6^2 + 2x_6x_7 + 3x_7^2$$
$$\ldots$$
$$f_{14} = 2x_1^2 + 2x_1x_4 - x_1x_5 - x_1x_6 + 4x_1x_7 - 4x_2^2 - 3x_2x_3 - 3x_2x_4 +$$
$$x_2x_5 - x_2x_7 - 8x_3^2 - 4x_3x_4 - 3x_3x_6 - 4x_3x_7 - 2x_4^2 + x_4x_6 + 6x_4x_7 + 8x_5^2 + x_5x_6 + 6x_5x_7 - x_6^2 + 3x_6x_7 + x_7^2$$

Thanks for listening!