Computing Kolyvagin Classes

Contents

§1. Kolyvagin Points
§2. Supersingular Points & Quaternions
§3. The Kolyvagin Divisor Mod p
§4. The Kolyvagin Point mod p.

§1. Kolyvagin Points:

$E/\mathbb{Q}$ elliptic curve, N = conductor, $\boxed{\begin{array}{c}\text{analytic}\\ \text{rank } 2\end{array}}$

$K = \mathbb{Q}(\sqrt{D})$ quad. imag. (primes dividing N split)

$\mathcal{O}_K/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$. q prime power

ℓ inert prime, $\ell \nmid N \cdot D$ s.t. $q \mid \gcd(a_\ell, \ell+1)$.

$\mathcal{O}_\ell = \mathbb{Z} + \ell\mathcal{O}_K$, $\mathcal{N}_\ell = \mathcal{N} \cap \mathcal{O}_\ell$, K_ℓ = ring class field conductor ℓ.

$$\begin{array}{ccc} (\mathbb{C}/\mathcal{O}_\ell,\ \mathcal{N}_\ell^{-1}/\mathcal{O}_\ell) = x_\ell & \in & X_0(N)(K_\ell) \\ \downarrow & & \downarrow \Phi_E \\ y_\ell & \in & E(K_\ell) \end{array}$$

Choice

$G_\ell = \mathrm{Gal}(K_\ell/K_1) = \langle\sigma\rangle$ order $\ell+1$

$$[P_\ell] = [P_{\ell,0}] = \mathrm{Tr}_{K_1/K}\left(\sum_{0\le i\le \ell} i\sigma^i([y_\ell])\right) \in \left(E(K_\ell)\otimes \mathbb{Z}/q\mathbb{Z}\right)^{\mathrm{Gal}(K_\ell/\mathbb{Q})} \overset{\text{hypo.}}{\hookrightarrow} \mathrm{Sel}^{(q)}(E/\mathbb{Q})$$

↑ well defined up to invertible scalar.

$$[P_\ell] \longleftrightarrow \tau_\ell.$$

Goal: Compute $[P_\ell]$. (Or at least prove $[P_\ell] \neq 0$ sometimes.)

Theorem (-) E: 389a, $q=3$, $K = \mathbb{Q}(\sqrt{-7})$. Basis for $\mathrm{Sel}^{(3)}(E/\mathbb{Q}) \cong \mathbb{F}_3^2$ such that:

$q=3$:

ℓ	5	17	41	59	83	173	227	269	479
τ_ℓ	$*(1,1)$	0	$*(1,2)$	$*(0,1)$	$*(1,2)$	0	0	0	6

Theorem: Some $\tau_\ell \neq 0$ $\Rightarrow$ way to compute all τ_ℓ up to nonzero scalar.

How? Fix auxiliary inert prime p and compute $[P_\ell \bmod p] \in E(\mathbb{F}_p) \otimes \mathbb{Z}/q\mathbb{Z}$ using quaternion algebras.

Assume q prime.

$$X_0(N)(K_\ell) \dashrightarrow X_0(N)(\mathbb{F}_{p^2})^{ss} \hookrightarrow \mathrm{Div}(X_0(N)^{ss}_{\mathbb{F}_{p^2}}) \xrightarrow[T]{} E(\mathbb{F}_p)\otimes \mathbb{Z}/q\mathbb{Z}.$$

$$x_\ell \longmapsto \bar{x}_\ell \rightsquigarrow \overline{\sum i\sigma^i(x_\ell)} \longmapsto \bar{P}_\ell$$

CM point

§2. Supersingular points and quaternions

$$X_0(N)(\mathbb{F}_{p^2})^{ss} \cong \left\{ \begin{array}{l} \text{right ideal classes } I \subseteq R \\ R = \text{Eichler order of level } N \\ \quad \text{in quat. alg. ramified at } p, \infty \\ \quad = \mathrm{End}(E_0) \end{array} \right\}.$$

$\underline{E}_0 = [(E_0, C_0)] \in$

Fix arb. choice

$$\underline{E} = (E, C) \longmapsto I = \mathrm{Hom}(\underline{E}_0, \underline{E})$$

Remark: Distribution Relation

$$T_\ell(x_1) = \sum_{0 \leq i \leq \ell} \sigma^i(x_\ell) \qquad \text{(a calculation)}$$

Also,
$$T_\ell(\bar{x}_1) = \sum \overline{\sigma^i(x_\ell)} \in \mathrm{Div}\left(X_0(N)_{\mathbb{F}_{p^2}}^{ss}\right)$$

Computing T_ℓ on $\mathrm{Div}\left(X_0(N)_{\mathbb{F}_{p^2}}^{ss}\right)$ is "standard":

$$T_\ell([I]) = \sum_{\substack{J \subseteq I \\ \text{right ideal s.t.} \\ I/J \cong (\mathbb{F}_\ell)^2}} [J] \in \bigoplus_I \mathbb{Z}[I]$$

$$\boxed{\begin{array}{l} \text{Strategy:} \\ \quad (1) \text{ Figure out } \bar{x}_1 \text{, somehow} \\ \quad (2) \text{ "Sort out" } \overline{\sigma^i(x_\ell)} \text{, somehow.} \end{array}}$$

(1) Finding $\bar{x}_1$: $\bar{x}_1 = \underline{E}_1 = \overline{(\mathbb{C}/\mathcal{O}_K, \mathcal{N}^{-1}/\mathcal{O}_K)}$ so $\mathcal{O}_K \hookrightarrow \mathrm{End}(\underline{E}_1) \subseteq B$

I right ideal $\rightsquigarrow R_I = \{x \in B : xI \subseteq I\}$ left order $\cong \mathrm{End}(\underline{E}_I)$

Ternary quadratic form:

$$(2R_I + \mathbb{Z}) \cap \ker(B \xrightarrow{\mathrm{Tr}} \mathbb{Q}) \xrightarrow[\text{Norm}]{q_I} \mathbb{Q}$$

3d - picture?

Lemma (Gross; 1987; also Jetchev-Kane §4.1):

$$\mathcal{O}_K \hookrightarrow \mathrm{End}(E_I) \iff q_I \text{ represents } |D|.$$

$\Rightarrow$ Algorithm to compute $\bar{x}_1$! (up to conjugation)

(proof is elementary number theory)

§3. The Kolyvagin Divisor Mod p

Background: ~~How to~~ compute

$$T_\ell(\bar{x}_1) = \sum_i \overline{\sigma^i(x_\ell)}$$

$\bar{x}_1 \leftrightarrow [I]$

Assume $I \otimes \mathbb{F}_\ell = R \otimes \mathbb{F}_\ell \overset{\varphi}{\cong} M_2(\mathbb{F}_\ell)$. [can always rescale I]

For $(u,v) \in \mathbb{P}^1(\mathbb{F}_\ell)$ let $\bar{J}_{(u,v)} = \{A \in M_2(\mathbb{F}_\ell) : (u,v)A = 0\}$

let $J_{(u,v)} = \varphi^{-1}(\bar{J}_{(u,v)})$.

Then $T_\ell([I]) = \sum_{x \in \mathbb{P}^1(\mathbb{F}_\ell)} [J_x] \in \mathrm{Div}(X_0(N)^{ss}_{\mathbb{F}_{p^2}})$.

Recall:

$$\langle \sigma \rangle = \mathrm{Gal}(K_\ell / K_1) \underset{\text{CFT}}{=} (\mathcal{O}_K / \ell \mathcal{O}_K)^* / (\mathbb{Z}/\ell\mathbb{Z})^* = \langle \alpha \rangle$$

since ℓ inert.

Compute $\alpha \in \mathcal{O}_K$ by computing order$([\sqrt{D} + a] \in \mathbb{F}_{\ell^2})$ for $a = 1, 2, \ldots$

But $\mathcal{O}_K \hookrightarrow I$ by lemma!

So $\alpha \mapsto 0 \neq \bar{\alpha} \in M_2(\mathbb{F}_\ell)$.

Prop (–): $\sum i \, \overline{\sigma^i(x_\ell)} = \sum_{0 \le i \le \ell} i \, [J_{(1,0)\alpha^i}]$ for some <u>choice</u> of σ.

(<u>Proof</u> involves unwinding all definitions and using CM theory.)

$\Downarrow$

Algorithm to compute Kolyvagin divisor

$$Z_\ell = \sum i \, \overline{\sigma^i(x_\ell)} \in \mathrm{Div}(X_0(N)^{ss}_{\mathbb{F}_{p^2}})$$

W. Stein

§4. The Kolyvagin Point Mod p

$$\mathrm{Div}(X_0(N)^{ss}_{\mathbb{F}_{p^2}}) \xrightarrow{\bar{\Phi}_E^{ss}} E(\mathbb{F}_{p^2}) \otimes \mathbb{Z}/q\mathbb{Z}$$

$J_0(N)(\mathbb{F}_{p^2})^{ss}$

$$Z_\ell \longmapsto [\bar{P}_\ell]. \quad ?$$

Prop (−) E optimal and $E[q]$ irreducible $\Longrightarrow$ $\bar{\Phi}_E$ surjective.

Proof: Lang's theorem + Ihara's Theorem + Snake lemma.

Let $k = \mathbb{F}_{p^2}$. Exact sequence of abelian varieties over k: $J_k = J_0(N)_k$

$$0 \to A_k \to J_k \to E_k \to 0$$

Galois cohomology: $0 \to A(k) \to J(k) \to E(k) \to H^1(k, A) = 0$

by Lang's theorem.

(Hasse bound when $\dim(A) = 1$.)

Ihara's Theorem:

Exact sequence $0 \to J(k)^{ss} \to J(k) \to Sh \to 0$

Sh "Shimura subgroup"

Snake Lemma:

$$\begin{array}{ccccccc} 0 \to & J(k)^{ss} & \to & J(k) & \to & Sh & \to 0 \\ & \downarrow \Phi & & \downarrow & & \downarrow & \\ & E(k) & \xrightarrow{\cong} & E(k) & \to & 0 & \to 0 \\ & \downarrow & & \downarrow \text{see above} & & & \\ & Y & \to & 0 & & & \end{array}$$

So as a $\mathbb{T}$=Hecke module, $Y = \mathrm{coker}(\bar{\Phi}_E^{ss}) \otimes \mathbb{Z}/q\mathbb{Z}$ is a quotient of Sh, so Y is Eisenstein. But

$$\mathfrak{m} = (q,\ T_n - a_n \text{ all } n) \subseteq \mathrm{Ann}_{\mathbb{T}}(Y)$$

is not Eisenstein by hypo. ∎

$\Downarrow$

Algorithm: We compute $\bar{\Phi}_E^{ss}$ up to a fixed scalar using linear algebra over $\mathbb{F}_p$ and $\mathbb{T}$-action.

Bonus:

A_f: 1061b   dim 2 abelian surface

$\operatorname{ord}_{s=1} L(f,s) = 2$

$K = \mathbb{Q}(\sqrt{-7})$

Use $X_0(1061)_{\mathbb{F}_5}$: G [illegible]

Get $0 \neq [P_{59}] \pmod{\lambda} \in A_f(\mathbb{F}_5) \otimes (\mathbb{Z}/3\mathbb{Z})$.

$\Longrightarrow$ Analogue of Kolyvan's conjecture for this abvar is <u>true</u>.

First ever Heegner point calculation on abvar.?