KOLYVAGIN CLASSES ON ELLIPTIC CURVES: STRUCTURE, DISTRIBUTION, AND ALGORITHMS

WILLIAM STEIN AND JARED WEINSTEIN

Let E be an elliptic curve over $\mathbf{Q}$ of conductor N, and let $K/\mathbf{Q}$ be an imaginary quadratic field of discriminant $D \neq -4, -5$ for which all prime factors of N are split in K. Kolyvagin [Kol90] uses the system of Heegner points of conductor n for K to construct a family of cohomology classes $\tau_n \in H^1(K, E[p^a])$. Here p is an odd prime and n is a squarefree integer whose prime divisors obey a certain congruence condition relative to E, K and p^a. Once the existence of a *nonzero* Kolyvagin class τ_n is exhibited, there are strong consequences for the arithmetic of E. The most fundamental example is Kolyvagin's original theorem: if the extension $\mathbf{Q}(E[p])/\mathbf{Q}$ has Galois group $\mathrm{GL}_2(\mathbf{Z}/p\mathbf{Z})$, and τ_1 does not vanish, then the group $E(K)$ has rank 1, and the Tate-Shavarevich group $Ш(E/K)_p$ is trivial. Furthermore, in [Kol91] Kolyvagin conjectures that if p is given, then there will exist a power $q = p^a$ and an integer n for which the class $\tau_n \in H^1(K, E[p^a])$ is nonzero. Granting this conjecture, he gives a precise description of the structure of the Selmer group $\mathrm{Sel}(K, E[q])$.

In this paper, we calculate the density (in an appropriately defined sense) of the set of squarefree integers n for which τ_n is nonvanishing modulo p, under the assumption that there exists at least one such nonvanishing class. We also offer a means of calculating the classes τ_n under the further assumption that the p-torsion part of the Tate-Shafarevich group of E/K is trivial.

The elliptic curve E is modular: let $f = \sum_n a_n q^n$ be the associated newform and let the sign in the functional equation for $E/\mathbf{Q}$ be $-\varepsilon$. Whenever M is a $\mathrm{Gal}(K/\mathbf{Q})$-module over a ring in which 2 is invertible, let $M^{\pm}$ be the $\pm$-eigenspace under the action of the nontrivial action $c \in \mathrm{Gal}(K/\mathbf{Q})$.

We define a *Kolyvagin prime* to be a rational prime $\ell \nmid NDp$ satisfying the following pair of conditions:

(1) ℓ is inert in K
(2) $a_\ell \equiv \ell + 1 \equiv 0 \pmod{p}$.

These conditions imply that $(E(\mathcal{O}_K/\ell\mathcal{O}_K) \otimes \mathbf{Z}/p\mathbf{Z})^{\pm}$ is cyclic of order p. Let $\mathcal{L}_s$ be the collection of sqarefree products of s Kolyvagin primes, and let $\mathcal{L} = \cup_{s \geq 0} \mathcal{L}_s$. Given $n \in \mathcal{L}_s$, Kolyvagin constructs a class $\tau_n \in H^1(K, E_p)^{(-1)^s \varepsilon}$.

We define a notion of density for subsets of $\mathcal{L}_s$. For $N \geq 2$, let $\mathcal{L}_s(N)$ be the set of $n \in \mathcal{L}_s$ which are supported on primes $p \leq N$. Given a subset $S \subset \mathcal{L}_s$, define $S(N) = S \cap \mathcal{L}_s(N)$ and define

$$\delta(S) = \lim_{N \to \infty} \frac{\#S(N)}{\#\mathcal{L}_s(N)}$$

whenever this limit exists.

Let $r^{\pm} = \dim_{\mathbf{F}_p} \mathrm{Sel}(K, E[p])^{\pm}$, and let $r = r^+ + r^-$. By exchanging E with E^D we can and do assume that $r^+ \geq r^-$.

Hypothesis. We impose the following conditions on the data E, K, p:

(1) The representation $\rho_{E,p}\colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{Aut}\, E[p]$ is surjective.
(2) There exists $s_0 \geq 0$ and $n \in \mathcal{L}_{s_0}$ with $\tau_n \in H^1(K, E[p])$ nonzero.

Now let $s \geq 0$ with $(-1)^s = \varepsilon$. Under Hypothesis (1), the Kolyvagin class τ_n is a well-defined element of $H^1(K, E[p])^+/(\mathbf{Z}/p\mathbf{Z})^\times$. Under hypothesis (2), the parity of s matches the parity of $r^+ - 1$ (say more about this!). To state our density result, we need to introduce some notation. For integers $a, b \geq 0$ of the same parity with $b \geq a$, define

$$f^0(a,b) = \prod_{\substack{i=3 \\ i \text{ odd}}}^{b-a+2} \left(1 - \frac{1}{p^i}\right) \prod_{j=b-a+3}^{b} \left(1 - \frac{1}{p^j}\right).$$

For integers $a, b \geq 0$ of opposite parity with $b \geq a - 1$, define

$$f^1(a,b) = \prod_{\substack{i=1 \\ i \text{ odd}}}^{b-a+1} \left(1 - \frac{1}{p^i}\right) \prod_{j=b-a+2}^{b+1} \left(1 - \frac{1}{p^j}\right).$$

(These products are set to 1 if the lower limit exceeds the upper limit.)

Theorem 0.1. *Let $\mathcal{L}_s^{\tau \neq 0}$ be the set of $n \in \mathcal{L}_s$ for which $\tau_n \neq 0$. Assume hypotheses (1) and (2) above. Then $\mathcal{L}_s^{\tau \neq 0}$ is nonempty if and only if $s \geq r^+ - 1$. If this inequality holds then*

$$\delta\left(\mathcal{L}_s^{\tau \neq 0}\right) = f^1(r^+, s) f^0(r^-, s).$$

1. The Kolyvagin system of Heegner points

1.1. **Heegner points and Kolyvagin classes: basic definitions.** If ℓ is a rational prime inert in K, we will often use the same symbol ℓ for the unique place of K lying above ℓ. As all prime divisors of N are split in K, there exists an ideal $\mathcal{N} \subset \mathcal{O}_K$ for which $\mathcal{O}_K/\mathcal{N} = \mathbf{Z}/N\mathbf{Z}$. For any $s \geq 0$ and $n \in \mathcal{L}_s$ let $\mathcal{O}_n$ be the order of conductor n in $\mathcal{O}_K$. Let y_n be the image under $X_0(N) \to E$ of the point represented by the cyclic isogeny $\mathbf{C}/\mathcal{O}_n \to \mathbf{C}/(\mathcal{O}_n \cap \mathcal{N})^{-1}$. Then y_n belongs to $E(K[n])$, where $K[n]/K$ is the ray class field corresponding to $\mathcal{O}_n$.

Let $G(n) = \mathrm{Gal}(K[n]/K[1])$. Then $G(n) \cong \prod_{\ell | n} G(\ell)$, where ℓ runs over the prime divisors of n. For each Kolyvagin prime ℓ we have $G(\ell) \cong \mathbf{F}_{\ell^2}^\times/\mathbf{F}_\ell^\times$. Fix a generator σ_ℓ of $G(\ell)$ and define the derivative operators

$$D_\ell = \sum_{i=1}^{\ell} i\sigma_\ell^i \in \mathbf{Z}[G(\ell)]$$

$$D_n = \prod_{\ell | n} D_\ell \in \mathbf{Z}[G(\ell)]$$

Let S be a set of coset representatives for $G(n)$ in $\mathrm{Gal}(K[n]/K)$, and define

$$P_n = \sum_{\sigma \in S} \sigma(D_n y_n) \in E(K[n]).$$

Then the image of the point P_n in $E(K_n)/pE(K_n)$ is fixed by $\mathrm{Gal}(K[n]/K)$ ([Gro91], §4.)

We now adopt Hypothesis (1): assume that $\rho_{E,p}\colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{Aut}\, E[p]$ is surjective. The *Kolyvagin class* $\tau_n \in H^1(K, E[p])$ is the unique class whose restriction to $K[n]$ equals the image of $[P_n] \in E(K[n])/pE(K[n])$ under the Kummer map. (Hypothesis (1) ensures that the restriction map $H^1(K, E[p]) \to H^1(K[n], E[p])$ is

an isomorphism, see [Gro91], Lemma 4.3.) The cohomology classes τ_n as n runs through $\mathcal{L}$ form a *Kolyvagin system* in the sense of [How04], §1.2, although it should be stressed that the Kolyvagin classes appearing in that paper have coefficients in $\mathbf{Z}_p$-modules of higher length, not simply $E[p]$.

1.2. **Local Selmer conditions.** For a place v we write $\mathrm{loc}_v : H^1(K, E[p]) \to H^1(K_v, E[p])$ for the localization map. We write $H^1_f(K_v, E[p])$ for the finite part of $H^1(K_v, E[p])$, this is

$$H^1_f(K_v, E[p]) = \begin{cases} \ker H^1(K_v, E[p]) \to H^1(K_v^{\mathrm{nr}}, E[p]), & v \nmid p, \\ \text{image of } E(K_v) \otimes \mathbf{Z}/p\mathbf{Z} \to H^1(K_v, E[p]), & v \mid p \end{cases}$$

For a Kolyvagin prime ℓ we also define the "transverse" part of $H^1(K_\ell, E[p])$ by

$$H^1_t(K_\ell, E[p]) = \ker(H^1(K_\ell, E[p]) \to H^1(L, E[p])),$$

where L/K_ℓ is a maximal totally ramified elementary abelian p-extension; *e.g.* L is the subextension of degree p in the localization of the ring class field $K[\ell]$ at a prime above ℓ. Recall that we have chosen a generator σ_ℓ of $\mathrm{Gal}(K[\ell]/K)$ for each Kolyvagin prime ℓ; this choice also gives us a generator of $\mathrm{Gal}(L/K_\ell)$, which we also call σ_ℓ.

If ℓ is a Kolyvagin prime, then the action of $\mathrm{Gal}(\overline{K}_\ell/K_\ell)$ on $E[p]$ is trivial, so that there is an isomorphism

$$H^1_f(K_v, E[p]) \tilde{\to} E[p] \tag{1}$$

given by evaluation of classes on Frobenius. The transverse subspace $H^1_t(K_\ell, E[p])$ is linearly disjoint from $H^1_f(K_v, E[p])$, so that the composition

$$H^1_t(K_\ell, E[p]) \hookrightarrow H^1(K_\ell, E[p]) \to H^1_s(K_\ell, E[p]) \tag{2}$$

is an isomorphism.

There is an isomorphism

$$H^1_t(K_\ell, E[p]) \to E[p] \tag{3}$$

given by $c \mapsto c(\sigma_\ell)$ (see [How04], Prop. 1.1.7).

By combining the isomorphisms of (1), (2) and (3) we arrive at the *finite-singular comparison map*

$$\psi_{\mathrm{fs}} \colon H^1_f(K_\ell, E[p]) \tilde{\to} H^1_s(K_\ell, E[p])$$

1.3. **Global Selmer structures.** For $n \in \mathcal{L}$, we write $H^1_{\mathcal{F}(n)}(K, E[p])$ for the $\mathbf{F}_p$-vector space of classes $\xi \in H^1(K, E[p])$ for which

$$\mathrm{loc}_v\, \xi \in \begin{cases} H^1_f(K_v, E[p]), & v \nmid n \\ H^1_t(K_v, E[p]), & v \mid n \end{cases}$$

for all places v.

Lemma 1.1. *For $n \in \mathcal{L}$ we have $\tau_n \in H^1_{\mathcal{F}(n)}(K, E[p])$. If $n = \ell n'$ for a prime ℓ, then $\mathrm{loc}_\ell\, \tau_n$ lies in $H^1_f(K_\ell, E[p])$ if and only if $P_{n'} \in pE(K[n'])_\lambda)$ for any (hence all) places $\lambda | \ell$ in $K[n']$.*

Proof. The statement that τ_n belongs to $H^1_{\mathcal{F}(n)}(K, E[p])$ is Lemma 1.7.2 of [How04]. The criterion for $\mathrm{loc}_\ell\, \tau_n$ to lie in $H^1_f(K_\ell, E[p])$ is Prop. 6.2 of [Gro91]. □

The following property of Kolyvagin classes τ_n accounts for their remarkable rigidity as n runs through $\mathcal{L}$.

Lemma 1.2. *Up to a nonzero scalar in* $\mathbf{F}_p$ *we have* $\phi_{fs}(\mathrm{loc}_\ell\,\tau_n) = \mathrm{loc}_\ell(\tau_{n\ell})$.

(In the lemma, $\mathrm{loc}_\ell(\tau_{n\ell})$ must be interpreted as the image of $\tau_{n\ell}$ in $H^1_s(K_\ell, E[p])$.)

Proof. This is the content of [How04], Prop. 1.7.4. □

1.4. **A vanishing criterion for Kolyvagin classes.** We give a criterion for the vanishing behavior of the Kolyvagin classes τ_n. For $n \in \mathcal{L}$ we abbreviate $\mathcal{H}(n) = H^1_{\mathcal{F}(n)}(K, E[p])$ and $\mathcal{H}(n)^\pm = H^1_{\mathcal{F}(n)}(K, E[p])^\pm$. The proof of the following theorem will occupy the remainder of this section.

Theorem 1.3. *Assume Hypothesis (1) and (2), and let* $s \geq 0$. *Then for* $n \in \mathcal{L}_s$, $\tau_n \neq 0$ *if and only if* $\dim \mathcal{H}(n) = 1$.

First we review a result from [How04], an application of the Poitou-Tate sequence in class field theory, which will be used in nearly every argument that follows.

Lemma 1.4 ([How04], Lemma 1.5.3)**.** *For* $n\ell \in \mathcal{L}$*:*

1. *If* $\mathrm{loc}_\ell(\mathcal{H}(n)^\pm) \neq 0$, *then* $\dim \mathcal{H}(n\ell)^\pm = \dim \mathcal{H}(n)^\pm - 1$, *and* $\mathrm{loc}_\ell(\mathcal{H}(n\ell)^\pm) = 0$.
2. *if* $\mathrm{loc}_\ell(\mathcal{H}(n)^\pm) = 0$, *then* $\dim \mathcal{H}(n\ell)^\pm = \dim \mathcal{H}(n)^\pm + 1$.

Lemma 1.4 implies that the parity of the dimension of $\mathcal{H}(n)$ does not depend on n. We have $r = \dim \mathcal{H}(1)$ is odd.

We are ready to prove one direction of Thm. 1.3.

Proposition 1.5. *Let* $n \in \mathcal{L}$. *If* $\tau_n \neq 0$ *then* $\dim \mathcal{H}(n) = 1$.

Proof. This is a corollary of [How04], Lemma 1.6.4, but we give a self-contained proof. Let $\varepsilon(n) = \pm 1$ be the unique sign for which τ_n belongs to $\mathcal{H}(n)^{\varepsilon(n)}$.

We claim $\mathcal{H}(n)^{-\varepsilon(n)} = 0$. Assume otherwise. Choose a Kolyvagin prime ℓ at which both τ_n and $\mathcal{H}(n)^{-\varepsilon(n)}$ have nontrivial localization. Then by Lemma 1.4, $\dim \mathcal{H}(n\ell) = \dim \mathcal{H}(n) - 2$ and $\mathrm{loc}_\ell \mathcal{H}(n\ell) = 0$. But consider $\tau_{n\ell}$: its localization at ℓ is $\mathrm{loc}_\ell \tau_{n\ell} = \phi_{\mathrm{fs}} \mathrm{loc}_\ell \tau_n$, which is nonzero by our choice of ℓ, contradiction.

Therefore $\mathcal{H}(n)^{-\varepsilon(n)} = 0$. It remains to show that $\dim \mathcal{H}(n)^{\varepsilon(n)} = 1$. Choose a Kolyvagin prime ℓ at which τ_n has nontrivial localization. Then $\dim \mathcal{H}(n\ell)^{\varepsilon(n)} = \dim \mathcal{H}(n) - 1$ and $\dim \mathcal{H}(n\ell)^{-\varepsilon(n)} = 1$. Once again we have $\mathrm{loc}_\ell \tau_{n\ell} \neq 0$, so in particular $\tau_{n\ell} \neq 0$. The case of the previous paragraph now applies with $n\ell$ in place of ℓ: we must have $\mathcal{H}(n\ell)^{\varepsilon(n)} = 0$. Therefore $\dim \mathcal{H}(n) = \dim \mathcal{H}(n)^{\varepsilon(n)} = 1$. □

1.5. **Kolyvagin systems: an overview.** For the "if" direction of Thm. 1.3, we apply the theory of Kolyvagin systems developed in [MR04], §4. We give a brief synopsis of this theory as it is presented there before adapting it to our situation. Let T be a $R[\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})]$-module of finite R-length, where R is a principal local Artinian ring with maximal ideal $\mathfrak{m}$. One considers the family of spaces $\mathcal{H}(n) = H^1_{\mathcal{F}(n)}(\mathbf{Q}, T)$ for an arbitrary Selmer structure $\mathcal{F}$, and one defines the quantities $\lambda(n, T) = \mathrm{length}(\mathcal{H}(n))$. Here n ranges through a set of admissible squarefree integers, akin to our $\mathcal{L}$. These integers constitute the vertices of a graph $\mathcal{X}$ in a natural way, see Definition 3.1.2. A vertex n is called a *core vertex* if $\lambda(n, T)$ or $\lambda(n, T^*)$ equals 0. If n is a core vertex then $H^1_{\mathcal{F}(n)}(\mathbf{Q}, T)$ is a free R-module of rank

independent of n (Thm 4.1.10); this rank is the *core rank* $\chi(T)$. Finally one defines the stub Selmer sheaf $\mathcal{H}'(n) = \mathfrak{m}^{\lambda(n,T^*)}(n,T)$ for any vertex n of $\mathcal{X}$.

When T is a Galois module of core rank $\chi(T) = 1$, one has results on the existence of nontrivial Kolyvagin systems. We state the theorem in the case that $R = \mathbf{Z}/p\mathbf{Z}$.

Theorem 1.6. *Assume $R = \mathbf{Z}/p\mathbf{Z}$ and $\chi(T) = 1$. Suppose κ is a Kolyvagin system for T for which κ_m generates $\mathcal{H}'(m)$ for some vertex m. Then κ_n generates $\mathcal{H}'(n)$ for every vertex n.*

Proof. This is Cor. 4.5.2(ii) of [MR04], with $j = 0$. □

In the present situation, $\mathbf{Q}$ is replaced with imaginary quadratic field K. We take $T = E[p]$ as our $\mathbf{Z}/p\mathbf{Z}[\mathrm{Gal}(\overline{K}/K)]$-module. Then T is self-dual. The role of $\lambda(n,T)$ are played by the $\lambda^{(k)}(n)$ of [How04], §1.6. The classes τ_n constitute a Kolyvagin system $\tau \in \mathbf{KS}(T)$ up to a nonzero scalar, cf. [How04], 1.7.5.

In the following sections we will adapt the proof of Thm. 1.6 to the context of the Kolyvagin system of Heegner points. The proof is nearly identical in its details to that given in [MR04], but the adaptation required enough modifications to merit a self-contained proof here.

1.6. **Connectedness of the core graph $\mathcal{X}^0$.** Define a graph $\mathcal{X}$ by taking the integers $n \in \mathcal{L}$ as vertices and by drawing an edge between each pair $n, n\ell \in \mathcal{L}$. We define the *core subgraph* $\mathcal{X}^0$ of $\mathcal{X}$ by including only those vertices n with $\dim \mathcal{H}(n) = 1$. An edge of $\mathcal{X}^0$ joins n and $n\ell$ if and only if the localization map

$$\mathrm{loc}_\ell : H^1_{\mathcal{F}(n)}(K, E[p]) \to H^1_f(K_\ell, E[p])$$

is nonzero.

The action of complex conjugation preserves each $\mathcal{H}(n)$. Therefore if n is a vertex of $\mathcal{X}^0$ there is a unique sign $\varepsilon(n) = \pm 1$ for which $\mathcal{H}(n) = \mathcal{H}(n)^{\varepsilon(n)}$. We have

$$\varepsilon(n) = (-1)^{r^+ + \nu(n) + 1} \tag{4}$$

Lemma 1.7. *Suppose n and $n\ell$ are vertices of $\mathcal{X}^0$. Then n and $n\ell$ are adjacent in $\mathcal{X}^0$, and $\varepsilon(n\ell) = -\varepsilon(n)$.*

Proof. We have $\mathcal{H}(n)^{-\varepsilon(n)} = 0$, so by Lemma 1.4, $\dim \mathcal{H}(n\ell)^{-\varepsilon(n)} = 1$. Since $n\ell$ is also a vertex of $\mathcal{X}^0$, $\dim \mathcal{H}(n\ell) = 1$ and therefore $\varepsilon(n\ell) = -\varepsilon(n)$. Once again by Lemma 1.4, we must have $\mathrm{loc}_\ell \mathcal{H}(n) = \mathrm{loc}_\ell \mathcal{H}(n)^{\varepsilon(n)} \neq 0$; thus n and $n\ell$ are adjacent in $\mathcal{X}^0$. □

Lemma 1.8. *Every connected component of $\mathcal{X}^0$ contains a vertex m with $\nu(m) = r^+ - 1$.*

Proof. Let n be an arbitrary vertex of $\mathcal{X}^0$; we claim there exists a path in $\mathcal{X}^0$ from n to a vertex m with $\nu(m) = r^+ - 1$. If $\nu(n) = r^+ - 1$ we are done; therefore assume $\nu(n) \geq r^+$. It is enough to show that there exists a path in $\mathcal{X}^0$ from n to a vertex m with $\nu(m) < \nu(n)$, whence we can proceed inductively. There are two cases to consider.

Case (i): There exists $r|n$ for which $\mathrm{loc}_r(\mathcal{H}(n)) \neq 0$. This is equivalent to $\mathrm{loc}_r \mathcal{H}(n)^{\varepsilon(n)} \neq 0$. By Lemma 1.4 we have $\mathrm{loc}_r(\mathcal{H}(n/r))^{\varepsilon(n)} = 0$. It follows that $\dim \mathcal{H}(n/r)^{\varepsilon(n)} = 0$. On the other hand, since $\mathcal{H}(n)^{-\varepsilon(n)} = 0$, Lemma 1.4 forces

$\dim \mathcal{H}(n/r)^{-\varepsilon(n)} = 1$ and $\mathrm{loc}_r(\mathcal{H}(n)^{-\varepsilon(n)}) \neq 0$. Thus $m = n/r$ is a vertex of $\mathcal{X}^0$ adjacent to n as required.

Case (ii): $\mathrm{loc}_r(\mathcal{H}(n)) = 0$ for all $r|n$. This implies that $\mathcal{H}(n) \subset \mathcal{H}(1)^{\varepsilon(n)}$. For each r, let $\mathcal{H}(1)_r^{\varepsilon(n)} \subset \mathcal{H}(1)^{\varepsilon(n)}$ denote the subspace of classes with trivial localization at r. Then

$$\mathcal{H}(n) = \bigcap_{r|n} \mathcal{H}(1)_r^{\varepsilon(n)}$$

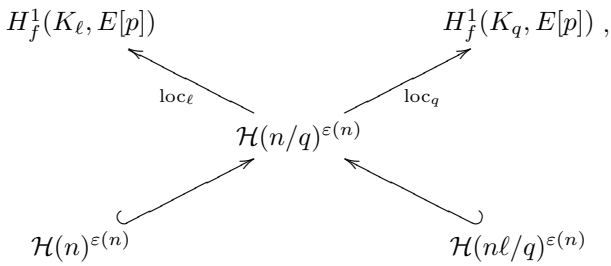
is a nonzero intersection of $\nu(n) \geq r^+ \geq r^{\varepsilon(n)}$ subspaces of an $r^{\varepsilon(n)}$-dimensional vector space. Therefore at least one of the spaces in the above intersection is redundant: there is a prime q dividing n so that

$$\mathcal{H}(n) = \bigcap_{r|\frac{n}{q}} \mathcal{H}(1)_\ell^{\varepsilon(n)}. \tag{5}$$

If $\dim \mathcal{H}(n/q) = 1$, then n/q is a vertex of $\mathcal{X}^0$, so that by Lemma 1.7, n and n/q are adjacent vertices in $\mathcal{X}^0$ and we are done. Assume otherwise, so that $\dim \mathcal{H}(n/q)^{\varepsilon(n)} = 2$ and $\dim \mathcal{H}(n/q)^{-\varepsilon(n)} = 1$. Our strategy is to find a prime $r|(n/q)$ and an auxiliary prime ℓ for which $n\ell$, $n\ell/q$, and $m = n\ell/qr$ are vertices of $\mathcal{X}^0$, thereby linking n to a vertex m for which $\nu(m) = \nu(n) - 1$.

Let $c \in \mathcal{H}(n)^{\varepsilon(n)}$ and $d^\pm \in \mathcal{H}(n/q)^{\pm\varepsilon(n)}$ be nonzero elements, and choose $\ell \in \mathcal{L}_1$ be such that $\mathrm{loc}_\ell(c)$ and $\mathrm{loc}_\ell(d^\pm)$ are all nonzero. Then by Lemma 1.4, $\dim \mathcal{H}(n\ell/q) = 1$ and $n\ell/q$ is a vertex of $\mathcal{X}^0$. By the same lemma, $\mathrm{loc}_\ell(\mathcal{H}(n\ell/q)^{\varepsilon(n)})$ is zero, so that $\mathcal{H}(n\ell/q)^{\varepsilon(n)} \subset \mathcal{H}(n/q)^{\varepsilon(n)}$. By the assumption of Case (ii), $\mathrm{loc}_q \mathcal{H}(n)$ is also zero, so that $\mathcal{H}(n)^{\varepsilon(n)} \subset \mathcal{H}(n/q)^{\varepsilon(n)}$ as well.

The situation can be summarized as follows. In the diagram



the space $\mathcal{H}(n/q)^{\varepsilon(n)}$ two-dimensional, while the spaces $\mathcal{H}(n)^{\varepsilon(n)}$ and $\mathcal{H}(n\ell/q)^{\varepsilon(n)}$ are each one-dimensional. Applying Lemma 1.4 once again shows that each diagonal is exact. The lower spaces are disjoint because the element $c \in \mathcal{H}(n)^{\varepsilon(n)}$ has $\mathrm{loc}_\ell c \in H^1_f(K_\ell, E[p])$ nonzero, so that $c \notin \mathcal{H}(n\ell/q)^{\varepsilon(n)}$. It follows that $\mathrm{loc}_\ell(\mathcal{H}(n)^{\varepsilon(n)}) \neq 0$, for otherwise we would have $\mathcal{H}(n)^{\varepsilon(n)} = \mathcal{H}(n\ell/q)^{\varepsilon(n)}$, contradiction. Therefore $\dim \mathcal{H}(n\ell)^{\varepsilon(n)} = \dim \mathcal{H}(n\ell/q)^{\varepsilon(n)} - 1 = 0$. Meanwhile, $\dim \mathcal{H}(n\ell)^{-\varepsilon(n)} = 0$ is automatic because $\mathcal{H}(n)^{-\varepsilon} = 0$. We find that $n\ell$ is a vertex of $\mathcal{X}^0$, necessarily adjacent to n by Lemma 1.7.

We claim there exists a prime $r|(n/q)$ for which $\mathrm{loc}_r(\mathcal{H}(n\ell/q)) \neq 0$. Assume not: then $\mathrm{loc}_r(\mathcal{H}(n\ell/q) = 0$ for all primes r dividing $n\ell/q$ (including ℓ, by the above diagram). Therefore

$$\mathcal{H}(n\ell/q) \subset \bigcap_{r|\frac{n}{q}} \mathcal{H}(1)_r^{\varepsilon(n)},$$

but by Eq. 5 this intersection is $\mathcal{H}(n)$, contradiction.

Therefore let $r|(n/q)$ be such that $\mathrm{loc}_r(\mathcal{H}(n\ell/q)) \neq 0$. It follows immediately that $n\ell/qr$ is a vertex of $\mathcal{X}^0$. Since $\nu(n\ell/qr) = \nu(n) - 1$, the proof is complete. □

Theorem 1.9. *The graph $\mathcal{X}^0$ is connected.*

Proof. By Lemma 1.8 it is enough to show that if m and n are two vertices of $\mathcal{X}^0$ with $\nu(m) = \nu(n) = r^+ - 1$, then m and n are connected by a path in $\mathcal{X}^0$. We will prove this by induction on $\mu(m,n) = r^+ - \nu(\gcd(m,n)) \geq 1$. If $\mu(m,n) = 1$ then $m = n$ and there is nothing to prove.

Assume $m \neq n$. Since $\nu(m) = \nu(n)$, there must exist distinct primes $q|n$ and $r|m$. By Eq. (4) we have $\varepsilon(m) = \varepsilon(n) = 1$. We have $\dim \mathcal{H}(n/q)^+ = \dim \mathcal{H}(m/r)^+ = 2$ and $\dim \mathcal{H}(n/q)^- = \dim \mathcal{H}(m/r)^- = 1$. Choose nonzero elements c_1, c_2, c_3, c_4 from each of these four spaces and find a prime $\ell \in \mathcal{L}_1$ with $\mathrm{loc}_\ell(c_i) \neq 0$ for $i = 1, \ldots, 4$. Then by Lemma 1.4 we have $\dim \mathcal{H}(n\ell/q) = \dim \mathcal{H}(m\ell/r) = 1$, so that $n\ell/q$ and $m\ell/r$ are vertices of $\mathcal{X}^0$. In fact $n\ell$ and $m\ell$ are also vertices of $\mathcal{X}^0$: the argument is identical to that given in the proof of Lemma 1.8.

There are paths in $\mathcal{X}^0$ connecting n and m to $n\ell/q$ and $m\ell/r$, respectively, and $\mu(m\ell/r, n\ell/q) = \mu(m,n) - 1$, so by the inductive hypothesis, m and n are joined by a path in $\mathcal{X}^0$ as well. □

1.7. **Conclusion of the proof of Thm. 1.3.** Suppose there exists $m \in \mathcal{L}$ with $\tau_m \neq 0$. Let n be a vertex of $\mathcal{X}^0$. To complete the proof of Thm. 1.3, we need to prove that $\tau_n \neq 0$.

By Thm. 1.9 there is a path $m = k_0, k_1, \ldots, k_t = n$ joining m to n in $\mathcal{X}^0$. We can show that $\tau_{k_i} \neq 0$ by induction on i. Suppose $\tau_{k_i} \neq 0$. Since k_i and k_{i+1} are adjacent in $\mathcal{X}^0$, we have either $k_{i+1} = k_i\ell$ or $k_i = k_{i+1}\ell$.

Case (i): $k_{i+1} = k_i\ell$. By definition of adjacency in $\mathcal{X}^0$ we have $\mathrm{loc}_\ell \mathcal{H}(k_i)^{\varepsilon(k_i)} \neq 0$. In particular $\mathrm{loc}_\ell \tau_{k_i} \neq 0$. But then $\mathrm{loc}_\ell \tau_{k_{i+1}}$ must also be nonzero, since by Lemma 1.2 the image of this class under ϕ_{fs} agrees with $\mathrm{loc}_\ell \tau_{k_i}$ up to a nonzero constant.

Case (ii): $k_i = k_{i+1}\ell$. We have $\dim \mathcal{H}(k_i)^{\varepsilon(k_i)} = 1$ and $\dim \mathcal{H}(k_{i+1})^{\varepsilon(k_i)} = 0$. Therefore $\mathrm{loc}_\ell \mathcal{H}(k_i)^{\varepsilon(k_i)} \neq 0$, for otherwise we would have $\mathcal{H}(k_i)^{\varepsilon(k_i)} \subset \mathcal{H}(k_{i+1})^{\varepsilon(k_i)}$. Since $\tau_{k_i} \neq 0$ it spans $\mathcal{H}(k_i)^{\varepsilon(k_i)}$ and therefore $\mathrm{loc}_\ell \tau_{k_i} \neq 0$. Applying Lemma 1.2 we have $\tau_{k_{i+1}} \neq 0$.

2. A density calculation

Lemma 2.1. *Let $n \in \mathcal{L}$, and let $\rho(n)^\pm = \dim \mathcal{H}(n)^\pm$. For a choice of sign $d \in \{1, -1\}$, let*

$$\mathcal{P}_{n,d}^\pm = \left\{ \ell \in \mathcal{P} \;\middle|\; \ell \nmid n,\ \rho(n\ell)^\pm = \rho(n)^\pm + d \right\}.$$

Then

$$\delta\left(\mathcal{P}_{n,d}^\pm\right) = \begin{cases} p^{-\rho(n)^\pm}, & d = 1 \\ 1 - p^{-\rho(n)^\pm}, & d = 1. \end{cases}$$

Proof. This is an application of the Cebotarev density theorem to Lemma 1.4. For any class $\zeta \in \mathcal{H}(n)^\pm$, the restriction $\mathrm{res}_{K(E[p])}\zeta \in \mathrm{Hom}(\mathrm{Gal}(\overline{Q}/K(E[p]), E[p])$ cuts out an extension $M_\zeta/K(E[p])$ of exponent p; let $M(n)^\pm$ be the compositum of the M_ζ for $\zeta \in \mathcal{H}(n)^\pm$. Then there is a perfect pairing of $\mathbf{F}_p$-vector spaces

$$\mathcal{H}(n)^\pm \times \mathrm{Gal}(M(n)^\pm/K(E[p])) \to E[p]^\pm$$

whereby $(\zeta, \sigma) \mapsto \zeta(\sigma)$; in particular $\mathrm{Gal}(M(n)^{\pm}/K(E[p])) \approx (\mathbf{Z}/p\mathbf{Z})^{\rho(n)^{\pm}}$. Now let $\ell \nmid n$ be a Kolyvagin prime. In light of Lemma 1.4, we have $p \in \mathcal{P}_{n,1}^{\pm}$ if and only if $\mathrm{loc}_\ell \mathcal{H}(n)^{\pm} = 0$. Let $\lambda|\ell$ be a place of $K(E[p])$; the Kolyvagin condition implies that $K(E[p])_\lambda \approx K_\lambda$. Thus $\mathrm{loc}_\ell \mathcal{H}(n)^{\pm} = 0$ if and only if $\mathrm{loc}_\lambda \mathrm{res}_{K(E[p])} \mathcal{H}(n)^{\pm} = 0$, which means precisely that λ splits completely in $M(n)^{\pm}$. The relative density of such ℓ relative to the Kolyvagin primes is $1/[M(n)^{\pm} : K(E[p])] = p^{-\rho(n)^{\pm}}$. □

Recall that $r^{\pm} = \dim \mathrm{Sel}(K, E[p])^{\pm}$.

Proposition 2.2. *Let $s \geq r^{\pm} - \nu$, and let $\nu \in \{0, 1\}$. Let*

$$\mathcal{L}_{s,\nu}^{\pm} = \left\{ n \in \mathcal{L}_s \;\middle|\; \dim \mathcal{H}(n)^{\pm} = \nu \right\}.$$

Then

$$\delta\left(\mathcal{L}_{s,\nu}^{\pm}\right) = f^{\nu}(r^{\pm}, s).$$

Proof. The proof is by inductive application of Lemma 2.1. Let $r_1, r_2 \geq 0$, and let $m \in \mathcal{L}_{s'}$ be such that $\rho(m)^{\pm} = r_1$.

$$D(r_1, r_2, s) = \delta\left(\left\{ n \in \mathcal{L}_s \;\middle|\; \rho(mn) = r_2 \right\}\right)$$

Define $D(r_1, r_2, s) = 0$ if any of the arguments r_1, r_2, s are negative. It will become clear momentarily that $D(r_1, r_2, s)$ does not depend on the choice of s' or $m \in \mathcal{L}_{s'}$. Clearly we have

$$D(r_1, r_2, 0) = \begin{cases} 1, & r_1 = r_2 \geq 0 \\ 0, & \text{otherwise} \end{cases}$$

Lemma 2.1 implies that $d(r_1, r_2, s)$ satisfies the recursion relation

$$D(r_1, r_2, s) = \frac{p^{r_1} - 1}{p^{r_1}} D(r_1 - 1, r_2, s - 1) + \frac{1}{p^{r_1}} D(r_1 + 1, r_2, s - 1),$$

which together with the initial condition above is enough to determine $D(r_1, r_2, s)$ for all values of r_1, r_2, s. For $\nu \in \{0, 1\}$ we have $D(r_1, \nu, s) = f^{\nu}(r_1, s)$ (proof by induction – haven't actually checked it yet). □

3. An algorithm for the computation of Kolyvagin classes

[Whereby given $n \in \mathcal{L}$ we determine whether $\dim \mathcal{H}(n) = 1$ through a devilishly clever procedure.]

References

[Gro91] Benedict H. Gross, *Kolyvagin's work on modular elliptic curves*, L-functions and arithmetic (Durham, 1989), London Math. Soc. Lecture Note Ser., vol. 153, Cambridge Univ. Press, Cambridge, 1991, pp. 235–256. MR MR1110395 (93c:11039)

[How04] Benjamin Howard, *The Heegner point Kolyvagin system*, Compos. Math. **140** (2004), no. 6, 1439–1472. MR MR2098397 (2006a:11070)

[Kol90] V. A. Kolyvagin, *Euler systems*, The Grothendieck Festschrift, Vol. II, Progr. Math., vol. 87, Birkhäuser Boston, Boston, MA, 1990, pp. 435–483. MR MR1106906 (92g:11109)

[Kol91] ———, *On the structure of Selmer groups*, Math. Ann. **291** (1991), no. 2, 253–259. MR MR1129365 (93e:11073)

[MR04] Barry Mazur and Karl Rubin, *Kolyvagin systems*, Mem. Amer. Math. Soc. **168** (2004), no. 799, viii+96. MR MR2031496 (2005b:11179)