KOLYVAGIN CLASSES FOR HIGHER RANK ELLIPTIC CURVES

Let E be an elliptic curve over $\mathbf{Q}$ of conductor N, and let $K/\mathbf{Q}$ be an imaginary quadratic field of discriminant $-D$ for which all prime factors of N are split in K. Kolyvagin [Kol90] uses the system of Heegner points of conductor m for K to construct a family of cohomology classes $c(m) \in H^1(K, E_p)$. Here p is an odd prime and m is a squarefree integer obeying a certain congruence condition relative to p. Once the existence of a *nonzero* Kolyvagin class $c(n)$ is exhibited, there are strong consequences for the arithmetic of E. The most fundamental example is Kolyvagin's original application of the Euler system of Heegner points: if the extension $\mathbf{Q}(E_p)/\mathbf{Q}$ has Galois group $\mathrm{GL}_2(\mathbf{Z}/p\mathbf{Z})$, and $c(1)$ 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 such a p is given, then there will exist a power $q = p^n$ and an integer m for which the class $c(m) \in H^1(K, E_q)$ is nonzero. Granting this conjecture, he gives a precise description of the structure of the Selmer group $\mathrm{Sel}(K, E_q)$.

The elliptic curve E is modular: let $f = \sum_n a_n q^n$ be the associated newform, let the sign in the functional equation for $E/\mathbf{Q}$ be $-\varepsilon$, and let $\phi\colon X_0(N) \to E$ be a modular parametrization. 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. Given $n \in \mathcal{L}_s$, Kolyvagin constructs a class $c(n) \in H^1(K, E_p)^{(-1)^s\varepsilon}$.

Let $r^+ = \mathrm{rk}_{\mathbf{Z}}\, E(\mathbf{Q})$, $r^- = \mathrm{rk}_{\mathbf{Z}}\, E^K(\mathbf{Q})$, so that $r = r^+ + r^- = \mathrm{rk}_{\mathbf{Z}}\, E(K)$. For simplicity we make the assumption that $r^- \leq 1$. (Given $E/\mathbf{Q}$, there is always a field $K/\mathbf{Q}$ satisfying the Heegner hypothesis for which $r^- \leq 1$.)

If ℓ is a rational prime inert in K, we will sometimes use the same symbol ℓ for the unique place of K lying above ℓ.

Let $\mathrm{loc}_\ell : E(K)/p(K) \to E(K_\ell)/pE(K_\ell)$ be the obvious map.

Lemma 0.1. *If $c(n) = \delta(P)$ for a rational point $P \in E(K)$, then $\mathrm{loc}_\ell P = 0$ for every $\ell | n$.*

Proof. Let Λ be a prime in $K[n]$ lying over $\ell\mathcal{O}_K$, and let F_Λ be the residue field. If σ_ℓ is a generator of $G_\ell = \mathrm{Gal}(K[n]/K[n/\ell])$, then the operator $D_\ell = \sum_{i=1}^{\ell} i\sigma_\ell^i$ annihilates $E(F_\Lambda) \otimes \mathbf{Z}/p\mathbf{Z}$, because σ_ℓ acts as the identity on the residue field of Λ and because $\ell(\ell+1)/2 \equiv 0 \pmod{p}$. Since the kernel of the reduction map $E(K[n]_\Lambda) \to E(F_\Lambda)$ is a pro-ℓ group, this implies that D_ℓ annihilates $E(K[n]_\Lambda) \otimes \mathbf{Z}/p\mathbf{Z}$ as well. Thus $P_n \in pE(K[n]_\Lambda)$.

If $P \in E(K)$ and $c(n) = \delta(P)$, it implies that $P \in pE(K[n]_\Lambda)$ and therefore the image of P in $E(F_\lambda)$ lies in $pE(F_\Lambda) = pE(\mathbf{F}_{\ell^2})$. Thus $\mathrm{loc}_\ell P = 0$. □

(Remark: Without the hypothesis that $c(n)$ lies in the image of δ, it would not follow that the localization $\mathrm{loc}_\lambda c(n)$ vanishes. The above argument shows that

$\mathrm{loc}_\Lambda \delta(P_n)$ vanishes as an element of $H^1(K[n]_\Lambda, E_p)$, but this says nothing about $\mathrm{loc}_\ell c(n)$ because $H^1(K, E_p) \to H^1(K[n]_\Lambda, E_p)^{G_n}$ is not an isomorphism.)

Assuming that the Kolyvagin system $\{c(n)\}$ does not vanish, and also assuming that $\text{Ш}(E/K)[p] = 0$, one can calculate the Kolyvagin classes $c(n)$ for $n \in \mathcal{L}_{r^+-1}$ by studying the localization behavior of the rational points in $E(K)$ at the primes dividing ℓ. We spell this out in a special case.

Proposition 0.2. *Let $r^+ = 2$, $r^- = 1$, and assume that $\text{Ш}(E/K)[p] = 0$. Assume the Kolyvagin system $\{c(n)\}$ does not vanish. For a prime ℓ satisfying the Kolyvagin condition, we have $c(\ell) \neq 0$ if and only if the linear map $\mathrm{loc}_\ell : E(K)/pE(K) \to E(K_\lambda)/pE(K_\lambda)$ has maximal rank. If loc_ℓ does have maximal rank, let $P \in E(\mathbf{Q})$ span the kernel; then up to a scalar we have $c(\ell) = \delta(P)$.*

Proof. First suppose that $\mathrm{loc}_\ell : E(K)/pE(K) \to E(K_\lambda)/pE(K_\lambda)$ does have maximal rank, with kernel spanned by P. Since $\mathrm{rk}\, E(K) > 1$, $c(1) = 0$. Therefore $c(\ell) \in \mathrm{Sel}(K, E_p)^+$. Since $\text{Ш}(E/K)[p] = 0$ there exists $P' \in E(Q)$ with $c(\ell) = \delta(P')$. We have $P' \neq 0$ because....? Then Lemma 0.1 shows that $\mathrm{loc}_\ell P' = 0$, so that up to a scalar $P' = P$ as desired.

Now suppose loc_ℓ does not have maximal rank. Write $c(\ell) = \delta(P)$. We claim $P = 0$. Assume otherwise: Let $\{P, Q\}$ be a basis for $E(\mathbf{Q})/pE(\mathbf{Q})$, and let $\{R\}$ be a basis for $E^D(\mathbf{Q})/pE^D(\mathbf{Q})$. Choose a prime ℓ' for which $\mathrm{loc}_{\ell'} : E(K)/pE(K) \to E(K_{\ell'})/pE(K_{\ell'})$ has kernel exactly $\langle Q \rangle$. Thus up to a scalar we have $c(\ell') = \delta(Q)$. Consider the two classes $c(\ell\ell'), \delta(R) \in H^1(K, E_p)^-$. For each place v of K away from $\ell\ell'$ we have $\langle \mathrm{loc}_v c(\ell\ell'), \mathrm{loc}_v \delta(R) \rangle = 0$ because both classes are finite at v.

We claim $\langle \mathrm{loc}_\ell c(\ell\ell'), \mathrm{loc}_\ell \delta(R) \rangle = 0$. By hypothesis, the kernel of the localization map $\mathrm{loc}_\ell : E(K)/pE(K) \to E(K_\ell)/pE(K_\ell)$ is strictly larger than $\langle P \rangle$. Thus $\mathrm{loc}_\ell(Q) = 0$ or $\mathrm{loc}_\ell(R) = 0$ (or possibly both). If $\mathrm{loc}_\ell(R) = 0$ the claim is obvious. If $\mathrm{loc}_\ell(Q) = 0$, then since $c(\ell') = \delta(Q)$ we have that $\mathrm{loc}_\ell c(\ell\ell')$ is finite and therefore that it is orthogonal to $\delta(R)$ in $H^1(K_\ell, E_p)^-$.

By the global reciprocity law, we have $\langle \mathrm{loc}_{\ell'} c(\ell\ell'), \mathrm{loc}_{\ell'} \delta(R) \rangle = 0$. Since $\mathrm{loc}_{\ell'} R$ is nonzero by our choice of ℓ', it follows that $\mathrm{loc}_{\ell'} c(\ell\ell')$ lies in the finite part of $H^1(K_{\lambda'}, E_p)^-$. This implies that $\mathrm{loc}_{\ell'} c(\ell) = \mathrm{loc}_{\ell'} P = 0$, again contrary to our choice of ℓ'. □

Keep the assumption that $r^+ = 2$ and $r^- = 1$. We calculate the density of Kolyvagin primes ℓ for which $c(\ell) = 0$. This can be computed using the Chebotarev Density Theorem as follows. Let $L = \mathbf{Q}(E_p)$, so that $\mathrm{Gal}(L/\mathbf{Q}) \cong \mathrm{GL}_2(\mathbf{Z}/p\mathbf{Z})$. The image of complex conjugation τ in $\mathrm{Gal}(L/\mathbf{Q})$ is conjugate to $\begin{pmatrix} 1 & \\ & -1 \end{pmatrix}$, and the size of the normalizer $N_{\mathrm{Gal}(L/\mathbf{Q})}(\tau)$ in $\mathrm{Gal}(L/\mathbf{Q})$ is the order of the split torus in $\mathrm{GL}_2(\mathbf{Z}/p\mathbf{Z})$, namely $(q-1)^2$. Since $L \cap K = \mathbf{Q}$, we have $\mathrm{Gal}(KL/\mathbf{Q}) \cong \mathrm{GL}_2(\mathbf{Z}/p\mathbf{Z}) \times \mathrm{Gal}(K/\mathbf{Q})$. let $\tau_{KL} \in \mathrm{Gal}(KL/\mathbf{Q})$ be the image of τ. The Kolyvagin condition on ℓ is equivalent to the requirement that for any prime $\lambda|\ell$ in KL, a Frobenius element $\left(\frac{\lambda}{KL/\mathbf{Q}}\right) \in \mathrm{Gal}(KL/\mathbf{Q})$ be conjugate to τ_{KL}. The density of such primes is $1/(2(q-1)^2)$.

Now let $M = KL\left(\frac{1}{p}E(K)\right)$. We have an isomorphism

$$\mathrm{Gal}(M/KL) \cong \mathrm{Hom}\left(E(K) \otimes \mathbf{Z}/p\mathbf{Z}, E_p\right),$$

wherein the image of $\sigma \in \mathrm{Gal}(M/KL)$ is the map $P \mapsto Q^\sigma - Q$, where $Q \in E(M)$ satisfies $pQ = P$. Let $V = \mathrm{Hom}\,(E(K) \otimes \mathbf{Z}/p\mathbf{Z}, E_p)$; then V admits a natural action by the group $\mathrm{Gal}(KL/\mathbf{Q}) \cong \mathrm{GL}_2(\mathbf{Z}/p\mathbf{Z}) \times \mathrm{Gal}(K/\mathbf{Q})$. We have the exact sequence

$$0 \to V \to \mathrm{Gal}(M/\mathbf{Q}) \to \mathrm{GL}_2(\mathbf{F}_q) \times \mathrm{Gal}(K/\mathbf{Q}) \to 1$$

which can be split once p-division points of elements of a basis for $E(K) \otimes \mathbf{Z}/p\mathbf{Z}$ are chosen. Thus $\mathrm{Gal}(M/\mathbf{Q})$ is isomorphic to the semidirect product $V \rtimes \mathrm{Gal}(KL/\mathbf{Q})$, with group law $(v, g)(v', g') = (v + g(v'), gg')$. Suppose ℓ is a prime satisfying the Kolyvagin hypothesis, so that $\left(\frac{\lambda}{KL/\mathbf{Q}}\right)$ is conjugate to the image of τ for any prime λ of KL above ℓ. Let Λ be a prime in M above λ. Since the residue degree of λ/ℓ is 2, we have that $\left(\frac{\Lambda}{M/\mathbf{Q}}\right)^2 = \left(\frac{\Lambda}{M/KL}\right) \in V$. Furthermore, let $\phi_\lambda \colon E(K) \otimes \mathbf{Z}/p\mathbf{Z} \to E_p$ be the homomorphism represented by the automorphism $\left(\frac{\Lambda}{M/KL}\right)$. (Since M/KL is abelian, ϕ_λ does not depend on the choice of Λ.) For $P \in E(K)$ we have that $\phi_\lambda(P) = 0$ if and only if $\mathrm{loc}_\ell(P) = 0$. Therefore loc_ℓ has maximal rank if and only if ϕ_λ does.

Let $V^{\max} \subset V$ denote the set of linear maps $E(K)/pE(K) \to E_p$ which have maximal rank. Write $\left(\frac{\Lambda}{M/\mathbf{Q}}\right) = (v, g)$ for $v \in V$, $g \in \mathrm{GL}_2(\mathbf{Z}/p\mathbf{Z})$. Since g is conjugate to the image of τ we have $g^2 = 1$ and $(v, g)^2 = (v + g(v), 1)$. Thus

$$\begin{aligned} c(\ell) \neq 0 \quad &\iff \quad \left(\frac{\Lambda}{M/KL}\right) \in V^{\max} \\ &\iff \quad = v + g(v) \in V^{\max} \end{aligned}$$

The subset $H \subset \mathrm{Gal}(M/\mathbf{Q})$ consisting of all pairs (v, g) having the properties that g is conjugate to τ_{KL} and $v + g(v) \in V^{\max}$ has cardinality

$$\#H = \#\left<\tau_{KL}\right> \#\left\{v \in V | v + \tau(v) \in V^{\max}\right\}$$

The order of $\langle \tau_{KL} \rangle$ is $\frac{\#\,\mathrm{GL}_2(\mathbf{Z}/p\mathbf{Z})}{(p-1)^2}$. Now consider the set S of $v \in V$ for which $v + \tau(v)$ has maximal rank. We have the direct sum decomposition $V = V^{\tau=1} \oplus V^{\tau=-1}$: therefore $\#S = \#(V^{\tau=1} \cap V^{\max}) \# V^{\tau=-1} = (p-1)^2 \times (p-1)p^3$. Therefore the density of Kolyvagin primes ℓ for which $c(\ell) \neq 0$ is $\#H/\#\,\mathrm{Gal}(M/\mathbf{Q}) = (p+1)/(2p^3)$. The relative density of such primes from the set of Kolyvagin primes is $(p+1)(p-1)^2/p^3$. Interestingly, it is roughly p times as likely for a Kolyvagin prime ℓ to have $c(\ell) = 0$ as it is for $c(\ell)$ to be any particular class in the image of $E(\mathbf{Q})/pE(\mathbf{Q})$.

References

[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)