93e:11073 11G05 11G40

Kolyvagin, V. A. (RS-AOS)

On the structure of Selmer groups.

Math. Ann. **291** (1991), *no.* 2, 253–259.

Let $E/\mathbf{Q}$ denote a modular elliptic curve. Fix an auxiliary complex quadratic field K such that all primes dividing the conductor of E split. Let p be a rational prime not dividing the discriminant of the ring of endomorphisms of E and such that the natural Galois representation $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{Aut}(T_p(E))$ is surjective. Consider the set of rational primes $\mathcal{L}^{(n)} = \{l\colon l \text{ is inert in } K \text{ and } p^n \mid l+1, a_l\}$. The author associates to every square-free product $m = l_1 \cdots l_k$ of primes of $\mathcal{L}^{(n)}$ a cohomology class $c(m,n) \in H^1(K, E_{p^n})$, defined by means of the Heegner points. When $m = 1$ so that the product is empty, $c(1,n)$ is the image of the Heegner point over K in $\mathrm{Sel}_{p^n}(E/K)$.

In the fundamental paper "Euler systems" [92g:11109in The Grothendieck Festschrift, Vol. II, 435–483, Progr. Math., 87, Birkhauser Boston, Boston, MA, 1990; MR 92g:11109], the author proved that under the hypothesis $c(1,n) \neq 0$ the rank of $E(K)$ is equal to 1 and $\mathrm{Sh}(E/K)$ is finite. Moreover, he determined in another paper [in Algebraic geometry (Chicago, IL, 1989), 94–121, Lecture Notes in Math., 1479, Springer, Berlin, 1991] the invariants of $\mathrm{Sh}(E/K)_{p^\infty}$ under the same hypothesis. In the paper under review, the author generalizes his methods to study the structure of the Selmer group of higher rank elliptic curves. He conjectures that the Heegner cohomology classes $c(m,n)$ are not all zero. This is a natural generalization of the condition $c(1,n) \neq 0$, which holds for curves of analytic rank 1. Here is one of the results of this paper. Let ε denote the opposite of the sign of the functional equation of $E/\mathbf{Q}$, and let $\mathrm{Sel}_{p^n}(E/K)^\sigma$, $\sigma = \pm 1$, denote the subgroup of $\mathrm{Sel}_{p^n}(E/K)$ on which a fixed complex conjugation acts as multiplication by σ. Let $P_m \in E(K[m])$ be the point defined over the ring class field of conductor m corresponding to $c(m,n)$ in the construction of the Heegner cohomology classes. Write $p^{\alpha(m,n)}$ for the p-divisibility index of P_m in $E(K[m]) \otimes \mathbf{Z}/p^n\mathbf{Z}$ (put $\alpha(m,n) = \infty$ if P_m is zero in $E(K[m]) \otimes \mathbf{Z}/p^n\mathbf{Z}$), and write α_k for the minimum of the $\alpha(m,n)$ when n runs over the positive integers and m varies among the square-free products of k primes of $\mathcal{L}^{(n)}$. Assume that the above conjecture is true, i.e. that $\min_{k\geq 0}\{\alpha_k\} < \infty$. Let k_0 be the smallest integer for which $\alpha_k < \infty$.

Theorem. Let $\nu = 0, 1$. After the first $k_0 + \nu$ terms, the nonincreasing sequence of the invariants of $\mathrm{Sel}_{p^n}(E/K)^{\varepsilon(-1)^{k_0+\nu+1}}$ is equal to $(\alpha_{k_0+\nu+2i} - \alpha_{k_0+\nu+2i+1}, \alpha_{k_0+\nu+2i} - \alpha_{k_0+\nu+2i+1})$, $i = 0, 1, \cdots$. Moreover, if

$\nu = 1$ the first $k_0 + 1$ invariants are all equal to n.

We refer to the paper for the formulation of other results along these lines, and generalizations. *Massimo Bertolini* (I-PAVI)