Atti Accademia Nazionale Lincei Classe Scienze Fisiche Matematiche Naturali

Rendiconti Lincei Matematica e Applicazioni

Massimo Bertolini

An annihilator for the p-Selmer group by means of Heegner points

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti Lincei. Matematica e Applicazioni, Serie 9, Vol. **5** (1994), n.2, p. 129–140.

Accademia Nazionale dei Lincei

<http://www.bdim.eu/item?id=RLIN_1994_9_5_2_129_0>

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti Lincei. Matematica e Applicazioni, Accademia Nazionale dei Lincei, 1994.

Rend. Mat. Acc. Lincei
s. 9, v. 5:129-140 (1994)

Teoria dei numeri. — *An annihilator for the p-Selmer group by means of Heegner points.* Nota (*) di MASSIMO BERTOLINI, presentata dal Corrisp. C. Procesi.

ABSTRACT. — Let $E/\boldsymbol{Q}$ be a modular elliptic curve, and let K be an imaginary quadratic field. We show that the p-Selmer group of E over certain finite anticyclotomic extensions of K, modulo the universal norms, is annihilated by the «characteristic ideal» of the universal norms modulo the Heegner points. We also extend this result to the anticyclotomic $\boldsymbol{Z}_p$-extension of K. This refines in the current contest a result of [1].

KEY WORDS: Elliptic; Curve; Annihilator; Heegner; Selmer.

RIASSUNTO. — *Un annullatore per il p-gruppo di Selmer per mezzo dei punti di Heegner.* Sia $E/\boldsymbol{Q}$ una curva ellittica e K un campo quadratico immaginario. Si dimostra che il p-gruppo di Selmer di E sopra certe estensioni anticiclotomiche finite di K, modulo il gruppo delle norme universali, è annullato dall'«ideale caratteristico» delle norme universali modulo i punti di Heegner. Inoltre, questo risultato viene esteso al caso della $\boldsymbol{Z}_p$-estensione anticiclotomica di K. Esso costituisce, nella situazione considerata, un raffinamento di un risultato di [1].

1. CONVENTIONS AND ASSUMPTIONS

References: [1-3].

We assume that the reader is familiar with Kolyvagin's theory for elliptic curves. Here we content ourselves with recalling a few facts, and fixing notations.

ASSUMPTIONS.

1) $E/\boldsymbol{Q}$ is a modular elliptic curve of conductor N.

2) K is an imaginary quadratic field such that all primes dividing N split in K and $\mathcal{O}_K^X = \{\pm 1\}$.

3) $p \nmid 6N \operatorname{disc}(K) \# \operatorname{Pic}(\mathcal{O}_K) \# (E/E^0)$, where E/E^0 denotes the group of connected components of the Néron model of E.

4) The Galois representation $\rho_p : \operatorname{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q}) \to \operatorname{Aut}(E_{p^\infty})$ is surjective.

5) p is ordinary for E, *i.e.* $a_p \not\equiv 0 \pmod{p}$.

6) $p \nmid \# E(\boldsymbol{F}_{\mathcal{P}})$ for all primes $\mathcal{P}$ of K above p.

7) $a_p \not\equiv 2 \pmod{p}$ if p splits in K; $a_p \not\equiv -1 \pmod{p}$ if p is inert in K.

Let K_∞/K be the anticyclotomic $\boldsymbol{Z}_p$-extension of K, and let K_n be the subextension of degree p^n. Write $G_n := \operatorname{Gal}(K_n/K)$, $D_n := \operatorname{Gal}(K_n/\boldsymbol{Q})$, $R_n := \boldsymbol{Z}/p\boldsymbol{Z}[G_n]$, $\bar{R}_n := \boldsymbol{Z}/p\boldsymbol{Z}[D_n]$. Under our assumptions there is a family of Heegner points defined over K_∞. Write α_n for the standard Heegner point over K_n and $\mathcal{E}_n = R_n \alpha_n$ for the sub-module of $E(K_n)/pE(K_n)$ generated by α_n. $\mathcal{E}_n$ is an $\bar{R}_n$-module, as the p-Selmer group

(*) Pervenuta all'Accademia il 25 ottobre 1993.

$\mathrm{Sel}_p(E/K_n)$. Given a rational prime l we let

$$E((K_n)_l)/p := \oplus_{\lambda|l} E((K_n)_\lambda)/pE((K_n)_\lambda),$$

$$H^1((K_n)_l, A) := \oplus_{\lambda|l} H^1((K_n)_\lambda, A),$$

where the sum is taken over the primes of K_n dividing l and A denotes either E or E_p. We also write $\mathrm{res}_l := \oplus_{\lambda|l}\mathrm{res}_\lambda : H^1(K_n, A) \to H^1((K_n)_l, A)$ for the natural restriction map. We call *Kolyvagin primes* all rational primes $l \nmid 6pN$ such that $\mathrm{Frob}_l(K(E_p)/\boldsymbol{Q}) = [\tau]$, where τ is a fixed complex conjugation. Let $r = l_1 \dots l_h$ be a square-free product of Kolyvagin primes. We denote by $c(r, K_n) \in H^1(K_n, E_p)$ and $d(r, K_n) \in H^1(K_n, E)_p$ the *Kolyvagin cohomology classes*. Thus $c(r, K_n)$ corresponds to the point $-D_r\alpha_n(r)$, where D_r is the Kolyvagin derivative and $\alpha_n(r)$ is the Heegner point for K_n of level r. $d(r, K_n)$ is the image of $c(r, K_n)$ under the natural map. Under the above assumptions the following holds.

FACTS.

1) The norm mappings $N_{K_{n+1}/K_n} : \mathcal{E}_{n+1} \to \mathcal{E}_n$ are surjective.

2) (*i*) For any rational prime l not dividing r $\mathrm{res}_l d(r, K_n) = 0$.

(*ii*) For $l|r$, there is a G_n-equivariant and τ-antiequivariant isomorphism $\phi_l : H^1((K_n)_l, E)_p \to E((K_n)_l)/p$ such that $\phi_l(\mathrm{res}_l d(r, K_n)) = \mathrm{res}_l(D_{r/l}\alpha(r/l))$.

3) Let S be a finite set (possibly empty) of primes of K_n and let $\mathrm{Sel}_p^S(E, K_n)$ be the set of classes of $H^1(K_n, E_p)$ satisfying the local conditions outside S. Let S' be the extension of S to K_{n+1}. Then $\mathrm{Sel}_p^S(E/K_n) = \mathrm{Sel}_p^{S'}(E/K_{n+1})^{\mathrm{Gal}(K_{n+1}/K_n)}$ via the restriction map.

4) (*Local Tate duality*). For any l, the cup product induces a Galois-equivariant duality $\langle , \rangle_l : E((K_n)_l)/p \times H^1((K_n)_l, E)_p \to \boldsymbol{Z}/p\boldsymbol{Z}$.

5) (*Global duality*). Let $\partial : \oplus_l H^1((K_n)_l, E)_p \to \mathrm{Sel}_p(E/K_n)^{\mathrm{dual}}$ be the map induced by the local Tate pairing and let $\mathrm{res} = \oplus_l \mathrm{res}_l : H^1(K_n, E)_p \to \oplus_l H^1((K_n)_l, E)_p$ be the restriction map. Then for all $c \in H^1(K_n, E)_p$ we have $\partial\,\mathrm{res}(c) = 0$.

2. ALGEBRAIC PRELIMINARIES

In this section, let D denote a dihedral group of order $2p^n$ where $p \geq 3$ is a rational prime. (For instance, the Galois group $\mathrm{Gal}(K_n/\boldsymbol{Q})$ introduced in the previous section). D is the semidirect product of its cyclic subgroup G of order p^n and of any subgroup of order 2. Fix an involution τ of D and a generator γ for G. Then, for all $g \in G$ we have $g^\tau = g^{-1}$. We write R, resp. $\bar{R}$ for the group ring $\boldsymbol{Z}/p\boldsymbol{Z}[G]$, resp. $\boldsymbol{Z}/p\boldsymbol{Z}[D]$,

PROPOSITION 1. *Let M be a finitely generated $\bar{R}$-module. Then $M = V_1 \oplus \dots \oplus V_r$, where the V_i are $\bar{R}$-modules which are cyclic R-modules. Moreover, the decomposition is unique up to isomorphisms.*

Proposition 1 is a consequence of the following Lemmas.

LEMMA 2. *Let M be a f.g. R-module. Then $M = V_1 \oplus \ldots \oplus V_r$, where the V_i are cyclic R-modules. Moreover, the decomposition is unique up to isomorphisms.*

PROOF. We can identify (non-canonically) R with the quotient of the polynomial ring $\boldsymbol{F}_p[X]$ $\boldsymbol{F}_p[X]/(X^{p^n} - 1)$, by means of the assignement $\gamma \mapsto X$. The thesis follows from the structure theorem for a PID.

LEMMA 3. *If V is a cyclic R-module such that $\dim_{\boldsymbol{F}_p}(V) = t$, then $V \simeq R/(\gamma - 1)^t \simeq$ $\simeq (\gamma - 1)^{p^n - t}$.*

PROOF. It follows easily from the fact that the ideals of R are the powers of $\gamma - 1$ $(\gamma - 1)^s$, $0 \leqslant s \leqslant p^n$.

LEMMA 4. *Let V be a cyclic R-submodule of a f.g. $\bar{R}$-module M. Then there exists an $\bar{R}$-submodule $\bar{V}$ of M such that $\bar{V}$ is isomorphic to V as an R-module.*

PROOF. Let v be a generator of V. Define the $\bar{R}$-modules $V^{(\pm)} := Rv^{\pm}$, where $v^{\pm} :=$ $= (v \pm \tau v)/2$. Since $V \subset V^{(+)} + V^{(-)}$, either $V^{(+)}$ or $V^{(-)}$ must have the same dimension as V.

LEMMA 5. *Let M be a f.g. $\bar{R}$-module, and M_1 an $\bar{R}$-submodule. Assume there exists an R-decomposition $M = M_1 \oplus M_2$. Then there is an $\bar{R}$-decomposition $M = M_1 \oplus \bar{M}_2$.*

PROOF. Write $\pi\colon M \to M_1$ for the projection associated with the given decomposition. Define $\bar{\pi}\colon M \to M_1$, $m \mapsto (\pi(m) + \tau\pi(\tau m))/2$. One checks easily that $\bar{\pi}$ is a morphism of $\bar{R}$-modules, and that $\bar{\pi}(m_1) = m_1$ $\forall m_1 \in M_1$. Hence we have the $\bar{R}$-decomposition $M = M_1 \oplus \ker \bar{\pi}$.

PROOF OF PROP. 1. By Lemma 2 we may write $M = V_1 \oplus \ldots \oplus V_r$, where the V_i are cyclic R-modules. We perform an induction on the number $r = \dim_{\boldsymbol{F}_p}(M^G)$ of the cyclic summands of M, the case $r = 1$ being trivial. Assume that $\dim_{\boldsymbol{F}_p} V_1$ is maximal. By Lemma 4 combined with the theory of elementary divisors, we may assume in addition that V_1 is an $\bar{R}$-module. The thesis follows from Lemma 5 and the inductive hypothesis.

Given a non-zero cyclic R-module V, we have $V^G \simeq \boldsymbol{Z}/p\boldsymbol{Z}$. If, in addition, V is an $\bar{R}$-module, τ acts on V^G via $\varepsilon = \pm$. Note that ε does not depend on the choice of the involution τ. For, if τ' is another involution, we have $\tau' = \tau g$ for some $g \in G$.

DEFINITION 6. *The* sign *of V* $\operatorname{sign}(V)$ *is the* sign $\varepsilon = \pm$ *defined above.*

LEMMA 7. *Let V be a non-zero R-cyclic $\bar{R}$-module, having dimension over $\boldsymbol{F}_p$ equal to $t \geqslant 1$. Then, the sign of V is equal to ε if and only if we may find an R-module generator v of V such that $\tau v = (-1)^{t-1} \varepsilon v$.*

PROOF. Given an R-module generator v of V, write as before $v^{\pm} = (v \pm \tau v)/2$. Then v^{δ}, $\delta = +$ or $-$ is also a generator. Let $\omega := (\gamma - 1) - (\gamma - 1)^{\tau}$. Then ω is a generator for the augmentation ideal $(\gamma - 1)R$ and $\tau\omega = -\omega\tau$. Thus $\omega^{t-1} v^{\delta}$ is a generator for V^G and $\tau(\omega^{t-1} v^{\delta}) = (-1)^{t-1}\, \delta(\omega^{t-1} v^{\delta})$. Hence $\varepsilon = (-1)^{t-1} \delta$.

Later we shall need the following technical result.

PROPOSITION 8. *Let V_1 and V_2 be R-cyclic $\bar{R}$-submodules of an $\bar{R}$-module M, neither of which contained in the other. Assume that $d := \dim_{F_p}(V_1 \cap V_2) \geq 1$. Then we may write $V_1 + V_2 = V_1 \oplus W$, where W is a non-zero R-cyclic $\bar{R}$-submodule of M such that* $\operatorname{sign}(W) = (-1)^d \operatorname{sign}(V_1)$.

PROOF. By the theory of elementary divisors, we may write $V_1 + V_2 = V_1 \oplus W$, where W is a non-zero R-module. By Lemma 5, we may assume that W is an $\bar{R}$-module. Notice that W is R-cyclic, since V_2 projects onto $(V_1 + V_2)/V_1 \simeq W$. Thus, we are reduced to prove that the sign of W is equal to $(-1)^d \operatorname{sign}(V_1)$. Write ε for the sign of V_1 and δ for the sign of W. Let w denote a generator for W^G. Then $w = v_1 + v_2$, with $v_i \in V_i - (V_1 \cap V_2)$ and $(\gamma - 1)v_i \in V_1 \cap V_2$, $i = 1, 2$. By Lemma 7, we may assume that $\tau v_1 = (-1)^d \varepsilon v_1$. We deduce $\tau w = \delta v_1 + \delta v_2 = (-1)^d \varepsilon v_1 + \tau v_2$. This is possible only if $\delta = (-1)^d \varepsilon$.

3. THE MAIN THEOREM

We work with a fixed layer $H := K_n$. To ease notations we let $G := \operatorname{Gal}(H/K)$, $D := \operatorname{Gal}(H/\mathbf{Q})$, $R := \mathbf{Z}/p\mathbf{Z}[G]$, $\bar{R} := \mathbf{Z}/p\mathbf{Z}[D]$, $\alpha := \alpha_n$ and $\mathcal{E} := \mathcal{E}_n$. We may apply to $\bar{R}$-modules the results of the previous section.

LEMMA 9. *Assume that $\mathcal{E}$ is non-zero. Then there exists an $\bar{R}$-submodule U of* $\operatorname{Sel}_p(E/H)$ *containing $\mathcal{E}$ such that U is a free R-module of* rank 1.

PROOF. Let H' be the sub-extension of K_∞/K having degree p over H. Let $\mathcal{E}'$ denote the module of Heegner points defined over H'. Let γ, resp. γ' be a generator for G, resp. $G' := \operatorname{Gal}(H'/K)$. Let $\omega := (\gamma - 1)$ and $\omega' := (\gamma' - 1)$. By facts 1 and 3, §1 and Lemma 3 we have $\mathcal{E} \subset \mathcal{E}'$ and $\mathcal{E} \simeq (\omega)^{t_0}$, $\mathcal{E}' \simeq (\omega')^{t_0}$, where $\dim_{F_p} \mathcal{E} = p^n - t_0 \geq 1$. It follows that $U := (\omega')^{p^{n+1} - p^n - t_0}\mathcal{E}' \simeq (\omega')^{p^{n+1} - p^n} \simeq R$ satisfies our requirements.

Note that the module U is a kind of mod p universal norm sub-module of $\operatorname{Sel}_p(E/H)$. Clearly we have $\omega^{t_0} U = \mathcal{E}$.

LEMMA 10. *Assume that $\mathcal{E} \neq 0$. Then there exists an $\bar{R}$-decomposition* $\operatorname{Sel}_p(E/H) = U \oplus V_1 \oplus \ldots \oplus V_s$ *where the V_i are R-cyclic.*

PROOF. By the theory of elementary divisors, we may find an R-module decomposition $\operatorname{Sel}_p(E/H) = U \oplus V$. We conclude by applying Lemma 5 and Prop. 1.

Let $\mathfrak{L} = \omega^{t_0}$, with t_0 as above. By analogy with the terminology of Iwasawa theory we give

DEFINITION 11. *We call $\mathfrak{L}R$ the characteristic ideal of $U/\mathcal{E}$.*

THEOREM 12 (MAIN RESULT). *Assume $\mathcal{E} \neq 0$. Then $\mathfrak{L}R$ annihilates* $\operatorname{Sel}_p(E/H)/U$.

REMARKS. 1) The ideal $\mathfrak{L}R$ depends only on $\mathrm{Sel}_p(E/H)$.

2) $\mathfrak{L}^2$ is related, in view of a theorem of Gross-Zagier, to the Galois L-function interpolating special values of the first derivatives of the complex L-functions corresponding to the characters of the extension H/K.

3) The analogue of Th. 12 when $\delta = 0$ is trivial.

PROOF. Let $\mathrm{sign}(\delta) := \varepsilon$. Reorder, if necessary, the V_i in the decomposition of Lemma 10 in order to have

$$\mathrm{sign}(V_i) = -\varepsilon\,, \qquad 1 \leqslant i \leqslant s_1\,,$$
$$\mathrm{sign}(V_i) = \varepsilon\,, \qquad s_1 + 1 \leqslant i \leqslant s\,,$$

where we do not exclude $s_1 = 0$ or $s_1 = s$.

LEMMA 13. *There exist infinitely many Kolyvagin primes l_1 satisfying the simultaneous conditions*

$$\mathrm{res}_{l_1}(U \oplus V_i) \simeq U \oplus V_i\,, \qquad 1 \leqslant i \leqslant s_1\,,$$
$$\mathrm{res}_{l_1} V_1 = 0\,, \qquad s_1 + 1 \leqslant i \leqslant s\,,$$

where $\mathrm{res}_{l_1}\colon \mathrm{Sel}_p(E/H) \to E(H_{l_1})/p$ *is the restriction map.*

PROOF.

Step 1. We may identify the elements of the Selmer group with homomorphisms in $\mathrm{Hom}_{\mathcal{G}}(\mathrm{Gal}(\bar{K}/H(E_p)), E_p)$, with $\mathcal{G} := \mathrm{Gal}(H(E_p)/H)$. For, under our assumptions $\mathcal{G} \simeq \simeq GL_2(\boldsymbol{F}_p)$. Then, the kernel $H^1(\mathcal{G}, E_p)$ of the restriction map $H^1(H, E_p) \to \to H^1(H(E_p), E_p)$ is zero. Given an $\bar{R}$-submodule T of $\mathrm{Sel}_p(E/H)$, let M_T denote the extension of $H(E_p)$ cut out by T. In our setting, Kummer theory gives $\mathrm{Gal}(M_T/H(E_p)) = \mathrm{Hom}(T, E_p)$ as $\bar{R}$-modules (see [1, §I.3] for more details). Let

$$T := U^G \oplus V_1^G \oplus \ldots \oplus V_{s_1}^G \oplus V_{s_1+1} \oplus \ldots \oplus V_s\,.$$

Then

$$\mathrm{Gal}(M_T/H(E_p)) = \mathrm{Hom}(U^G, E_p) \oplus \left(\oplus_{i=1}^{s_1} \mathrm{Hom}(V_i^G, E_p)\right) \oplus \left(\oplus_{j=s_1+1}^{s} \mathrm{Hom}(V_j, E_p)\right).$$

Note that $U^G \simeq V_i^G \simeq \boldsymbol{Z}/p\boldsymbol{Z}$, and that the complex conjugation τ acts via ε, resp. $-\varepsilon$ on U^G, resp. V_i^G, $1 \leqslant i \leqslant s_1$. Choose generators $u, v_1, \ldots, v_{s_1}$. Write $E_p^{\pm}$ for the $\pm$-part of E_p under the action of τ. Let $e \in E_p^{\varepsilon} - \{0\}$, $e_i \in E_p^{-\varepsilon} - \{0\}$ for $1 \leqslant i \leqslant s_1$. Define the homomorphisms

$$\phi\colon U^G \to E_p\,, \qquad u \mapsto e\,,$$
$$\phi_i\colon V_i^G \to E_p\,, \qquad v_i \mapsto e_i\,, \qquad 1 \leqslant i \leqslant s_1\,,$$
$$\phi_j\colon V_j \to E_p\,, \qquad \phi_j \equiv 0\,, \qquad s_i + 1 \leqslant j \leqslant s\,.$$

Identify $(\phi, \phi_1, \ldots \phi_{s_1}, \phi_{s_1+1}, \ldots, \phi_s)$ with an element g of $\mathrm{Gal}(M_T/H(E_p))$.

Step 2. By the Chebotarev density theorem there exist infinitely many Kolyvagin primes l_1 such that

$$\mathrm{Frob}_{l_1}(M_T/\boldsymbol{Q}) = [\tau g].$$

Then

$$\mathrm{Frob}_{l_1}(M_T/K) = [(\tau g)^2] = [g^\tau g] =$$
$$= [(\varepsilon\tau\phi + \phi, -\varepsilon\tau\phi_1 + \phi_1, \ldots, -\varepsilon\tau\phi_{s_1} + \phi_{s_1}, 0, \ldots, 0)].$$

It follows

$$\mathrm{res}_{l_1}(U^G \oplus V_i^G) \simeq U^G \oplus V_i^G, \qquad 1 \leqslant i \leqslant s_1,$$
$$\mathrm{res}_{l_1} V_{i=0}, \qquad s_1 + 1 \leqslant i \leqslant s.$$

Step 3. We claim that with the above choice of l_1 we have in fact

$$\mathrm{res}_{l_1}(U \oplus V_i) \simeq U \oplus V_i, \qquad 1 \leqslant i \leqslant s_1.$$

For, if for some i there is a non-zero $v \in U \oplus V_i$ such that $\mathrm{res}_{l_1} v = 0$, then the module $(Rv)^G$ is mapped to 0 by res_{l_1}. But $(Rv)^G$ is non-zero, in contradiction with step 2. This concludes the proof of the Lemma.

PROPOSITION 14. *For* $1 \leqslant i \leqslant s_1$, *we have* $\mathcal{L}V_i = 0$.

PROOF. With the above choice of l_1 we have, by fact 2, §1,

$$\mathrm{res}_{l_1}(Rd(l_1)) \simeq \mathrm{res}_{l_1} \delta \simeq R\omega^{t_0}, \qquad \text{with sign } (\mathrm{res}_{l_1} Rd(l_1)) = -\varepsilon.$$

Let $X \subset H^1(H_{l_1}, E)_p$ be an $\bar{R}$-module free of rank 1 over R and containing $\mathrm{res}_{l_1}(Rd(l_i))$. The existence of X follows from the results of §2. More precisely, note that $H^1(H_{l_1}, E)_p$ is isomorphic to $E(H_{l_1})/p$ by local Tate duality (fact 4, §1); moreover, $E(H_{l_1})/p \simeq R \oplus R$ since, by definition of Kolyvagin prime, $E(H_{\lambda_1})/p \simeq \boldsymbol{Z}/p\boldsymbol{Z} \oplus \boldsymbol{Z}/p\boldsymbol{Z}$ for all primes λ_1 dividing l_1. Then the theory of elementary divisors guarantees the existence of a free rank 1 R-module X containing $\mathrm{res}_{l_1}(Rd(l_1))$. Since $\mathrm{res}_{l_1}(Rd(l_1))$ is τ-invariant, by Lemma 4 we may assume that X is an $\bar{R}$-module. Clearly, $\mathrm{sign}(X) = -\varepsilon$. Let Y be any $\bar{R}$-submodule of $E(H_{l_1})/p$ free of rank 1 over R and such that $\mathrm{sign}(Y) = -\varepsilon$. Y exist because, if ℓ_1 denotes the unique prime of K above l_1, we have $\mathrm{Frob}_{\ell_1}(K/\boldsymbol{Q}) = \tau$, and $(E(K_{\ell_1})/p)^{\pm} \simeq \boldsymbol{Z}/p\boldsymbol{Z}$; then we may let, for instance, $Y := R(E(K_{\ell_1})/p)^{-\varepsilon}$. We claim that X and Y as above are dual of each other with respect to the local Tate duality

$$\langle , \rangle_l : E(H_l)/p \times H^1(H_l, E)_p \to \boldsymbol{Z}/p\boldsymbol{Z},$$

i.e. X maps onto the dual of Y, which is a rank 1 quotient of $E(H_{l_1})/p$. This follows from the Galois-equivariance of the local Tate pairing. More precisely, the τ-equivariance implies that $(E(K_{\ell_1})/p)^{\pm}$ is dual of $(H^1(K_{\ell_1}, E)_p)^{\pm}$. The thesis follows from the G-equivariance. Recall the map

$$\delta_l : H^1(H_l, E)_p \to \mathrm{Sel}_p(E/L)^{\mathrm{dual}}$$

induced by the local Tate duality. Since for $1 \leqslant i \leqslant s_1$ $\operatorname{sign}(V_i) = \operatorname{sign}(X) = -\varepsilon$, the above considerations imply that $\partial_{l_1}(X)$ projects onto V_i^{dual}. By the global duality theorem (fact 5, §1) combined with the local behaviour of the Kolyvagin cohomology classes (fact 2, §1) we find $\partial_{l_1}(\operatorname{res}_{l_1} Rd(l_1)) = 0$. Hence $\omega^{t_0}(V_i)^{\mathrm{dual}} = 0$ and $\omega^{t_0} V_i = 0$, $1 \leqslant i \leqslant s_1$.

Choose a Kolyvagin prime l_1 as in Lemma 13. Let

$$\mathcal{E}_1 := Rc(l_1) \simeq (\omega)^{t_1} .$$

Note that $t_1 \leqslant t_0$, since the natural map $H^1(H, E_p) \to H^1(H_{l_1}, E)_p$ induces a projection

$$\mathcal{E}_1 \twoheadrightarrow \operatorname{res}_{l_1}(Rd(l_1)) \simeq (\omega)^{t_0} .$$

Case 1: $\operatorname{sign}(\mathcal{E}_1) = -\varepsilon$.

Note that in this case

$$\mathcal{E}_1 \cap (V_{s_1+1} \oplus \ldots \oplus V_s) = 0 .$$

Otherwise, there would be a non-zero element in $\mathcal{E}_1^G \cap (V_{s_1+1} \oplus \ldots \oplus V_s)^G$. This is impossible, since $\operatorname{sign}(V_i) = \varepsilon$ for $s_1 + 1 \leqslant i \leqslant s$.

PROPOSITION 15. *In the «case 1», we have* $\omega^{t_1} V_i = 0$ *for* $s_1 + 1 \leqslant i \leqslant s$.

PROOF. Choose a Kolyvagin prime l_2 satisfying the conditions

$$\operatorname{res}_{l_2}(\mathcal{E}_1 \oplus V_i) \simeq \mathcal{E}_1 \oplus V_i , \qquad s_1 + 1 \leqslant i \leqslant s .$$

The existence of l_2 follows from an argument similar to the proof of Lemma 13. By fact 2, §1 we have

$$\operatorname{res}_{l_2}(Rd(l_1 l_2)) \simeq \operatorname{res}_{l_2} \mathcal{E}_1 \simeq (\omega)^{t_1} , \qquad \text{with } \operatorname{sign}(\operatorname{res}_{l_1} Rd(l_1)) = \varepsilon .$$

Since $\operatorname{res}_{l_1} V_i = 0$, an argument similar to the proof of Prop. 14 shows

$$\omega^{t_1} V_i = 0 , \qquad s_1 + 1 \leqslant i \leqslant s .$$

This concludes the proof of Th. 12 if there exists a Kolyvagin prime l_1 satisfying the conditions of Lemma 13 and such that $\operatorname{sign}(\mathcal{E}_1) = -\varepsilon$.

Case 2: $\operatorname{sign}(\mathcal{E}_1) = \varepsilon$.

Recall that $\mathcal{E}_1 \simeq (\omega)^{t_1}$, with $t_1 \leqslant t_0$.

LEMMA 16. *In the «case 2», we have* $t_1 \not\equiv t_0 \pmod 2$. *In particular,* $t_1 < t_0$.

PROOF. Recall that the class $c(l_1)$ is the image of the point $-D_{l_1}\alpha(l_1)$ (§1). We may choose the Heegner points α and $D_{l_1}\alpha(l_1)$ so that τ acts on α, resp. $c(l_1)$ via σ, resp. $-\sigma$, where σ denotes the negative of the sign of the functional equation for $L(E/\boldsymbol{Q}, s)$. Since $\operatorname{sign}(\mathcal{E}) = \operatorname{sign}(\mathcal{E}_1)$, Lemma 7 implies that $\dim_{\boldsymbol{F}_p}(\mathcal{E}) \not\equiv \dim_{\boldsymbol{F}_p}(\mathcal{E}_1) \pmod 2$. Hence by Lemma 3 $t_0 \not\equiv t_1 \pmod 2$.

The next Lemma adapts an idea of H. Darmon to our situation.

LEMMA 17. *Let* $c \in \mathcal{S}_1 \cap \mathrm{Sel}_p(E/H)$ *be given. Then the image of* c *under the restriction map* $\mathrm{res}_{l_1}\colon \mathrm{Sel}_p(E/H) \to E(H_{l_1})/p$ *is* 0.

PROOF. Let $H[l_1]$ denote the maximal p-extension of H contained in the compositum of H and the ring class field of conductor l_1. Let $\tilde{\lambda}_1$ be a prime of $H[l_1]$ above l_1, and let λ_1 be the prime of H below $\tilde{\lambda}_1$. The image of c in $H^1(H[l_1]_{\tilde{\lambda}_1}, E_p)$ is zero, because $D_{l_1}\alpha(l_1)$ is locally divisible at $\tilde{\lambda}_1$ by p, as it follows from the congruence axiom for the Euler system of Heegner points [2]. Moreover, c maps to an unramified cocycle in $H^1(H_{\lambda_1}, E_p)$, since it belongs to $\mathrm{Sel}_p(E/H)$. Finally, the map $H^1_{unr}(H_{\lambda_1}, E_p) \to$ $\to H^1(H[l_1]_{\tilde{\lambda}_1}, E_p)$ is injective, since $H[l_1]/H$ has trivial residue field extension at λ_1. We deduce that c maps to zero in $H^1(H_{\lambda_1}, E_p)$, and this concludes the proof.

Let $\mathcal{C}$ denote the module $\mathcal{S}_1 \cap (V_{s_1+1} \oplus \ldots \oplus V_s)$.

PROPOSITION 18. *In the «case 2», the dimension of* $\mathcal{C}$ *is odd.*

PROOF. Let $\tilde{\mathcal{C}} := \mathcal{S}_1 \cap \mathrm{Sel}_p(E/H)$. Clearly $\tilde{\mathcal{C}} \supset \mathcal{C}$. $\tilde{\mathcal{C}}$ is the kernel of the surjection

$$\mathcal{S}_1 \twoheadrightarrow \mathrm{res}_{l_1}(Rd(l_1)),$$

induced by the natural map $H^1(H, E_p) \to H^1(H_{l_1}, E)_p$. Hence Lemma 3 gives

$$\tilde{\mathcal{C}} \simeq R/(\omega)^{t_0 - t_1}$$

and $\dim_{\mathbf{F}_p}(\tilde{\mathcal{C}}) = t_0 - t_1$. By Lemma 16 $t_0 - t_1$ is odd. Since $\tilde{\mathcal{C}}$ is cyclic, we have $\mathcal{C} = \omega^{\rho}\tilde{\mathcal{C}}$. In view of Lemma 3, we are reduced to show that ρ is even. Let $\tilde{\mathcal{C}} := R\tilde{c}$, where τ acts on $\tilde{c}$ by $+$ or $-$. Given our fixed decomposition of $\mathrm{Sel}_p(E/H)$, write

$$\tilde{c} = (u, v_1, \ldots, v_s),$$

with $u \in U$, $v_i \in V_i$. Since $\mathrm{res}_{l_1}\tilde{c} = 0$ by Lemma 17 and $\mathrm{res}_{l_1} U \simeq U$ by our choice of l_1, we get $u = 0$. Consider the projection

$$\tilde{C} \twoheadrightarrow Rv_i, \qquad \tilde{c} \mapsto v_i.$$

We claim that for $1 \leq i \leq s_1$ we have $\dim_{\mathbf{F}_p}(Rv_i) = 2\mu_i$, $\mu_i \geq 0$. Equivalently,

$$\mathrm{Ann}_R(Rv_i) = (\omega)^{2\mu_i}.$$

This follows from Lemma 7, since either $Rv_i = 0$ or $\mathrm{sign}(Rv_i) = -\mathrm{sign}(\tilde{\mathcal{C}})$ and τ acts on $\tilde{c}$ and v_i in the same way. If we let $\mu := \max_{1 \leq i \leq s_1}\{\mu_i\}$, we find $\rho = 2\mu$. This concludes the proof of Prop. 18.

It is possible to assume that the R-decomposition of the module $V_{s_1+1} \oplus \ldots \oplus V_s$ is such that

$$\mathcal{C} \subset V_{s_1+1} \quad \text{and} \quad \dim(V_{s_1+1}) \leq p^n - t_1.$$

For, it is possible to treat the other cases with similar techniques, this being the most difficult. Let $V_{s_1+1} \supset \mathcal{C}$ be an R-module. By Lemma 4 and the τ-in-

variance of $\mathcal{C}$, we may assume that V_{s_1+1} is an $\bar{R}$-module. In view of the theory of elementary divisors, we conclude by applying Lemma 5 and Prop. 1.

Case 2.1: Assume that $V_{s_1+1} \not\subset \mathcal{E}_1$.

I.e., $\mathcal{C} \neq V_{s_1+1}$. Clearly $\mathcal{E}_1 \not\subset V_{s_1+1}$, because $\mathrm{res}_{l_1}(Rd(l_1)) \simeq (\omega)^{t_0} \neq 0$, hence $\mathcal{E}_1$ cannot be contained in the Selmer group. Then, by Prop. 8 and Prop. 18, we may write

$$\mathcal{E}_1 + V_{s_1+1} = \mathcal{E}_1 \oplus W,$$

with $\mathrm{sign}(W) = (-1)^{\dim_{\mathbf{F}_p}(\mathcal{C})} \mathrm{sign}(\mathcal{E}_1) = -\varepsilon$.

LEMMA 19. *In the «case 2.1», there exist infinitely many Kolyvagin primes l_2 satisfying the simultaneous conditions*

$$\mathrm{res}_{l_2}(\mathcal{E}_1 + V_{s_1+1}) \simeq (\mathcal{E}_1 + V_{s_1+1}),$$
$$\mathrm{res}_{l_2}(V_i) \simeq V_i, \qquad s_1 + 2 \leqslant i \leqslant s,$$
$$\mathrm{res}_{l_2}(\mathcal{E}_1) \cap \mathrm{res}_{l_2}(V_i) = (\mathrm{res}_{l_2}\mathcal{E}_1)^G, \qquad s_1 + 2 \leqslant i \leqslant s.$$

PROOF. Since $\mathrm{sign}(\mathcal{E}_1) = -\mathrm{sign}(W)$, the argument in the proof of Lemma 13 shows that the first condition is equivalent to

$$\mathrm{res}_{l_2}\mathcal{E}_1^G \simeq \mathcal{E}_1^G, \qquad \mathrm{res}_{l_2}W^G \simeq W^G,$$

and it is satisfied by infinitely many Kolyvagin primes. At any rate, consider the module

$$T := \mathcal{E}_1 \oplus W \oplus V_{s_1+2} \oplus \ldots \oplus V_s.$$

If M_T denotes the extension of $H(E_p)$ cut out by T, we have

$$\mathrm{Gal}(M_T/H(E_p)) = \mathrm{Hom}(\mathcal{E}_1, E_p) \oplus \mathrm{Hom}(W, E_p) \oplus \oplus \mathrm{Hom}(V_{s_1+2}, E_p) \oplus \ldots \oplus \mathrm{Hom}(V_s, E_p).$$

Choose embeddings of $\bar{R}$-modules

$$\mathcal{E}_1 \hookrightarrow R^{(1)},$$
$$W \hookrightarrow R^{(2)},$$
$$V_i \hookrightarrow R^{(i-s_1+1)}, \qquad s_1 + 2 \leqslant i \leqslant s,$$

where the $R^{(j)}$ are free of rank one over R. This is possible by Lemmas 3 and 7. Note that $\mathrm{sign}(R^{(2)}) = -\varepsilon$, and $\mathrm{sign}(R^{(j)}) = \varepsilon$ for $j \neq 2$. We get an embedding

$$T \hookrightarrow \oplus_{j=1}^{s-s_1+1} R^{(j)}.$$

By applying $\mathrm{Hom}(\ , E_p)$ we obtain a projection of $\bar{R}$-modules

$$\pi\colon \oplus_{j=1}^{s-s_1+1} \mathrm{Hom}(R^{(j)}, E_p) \twoheadrightarrow \mathrm{Gal}(M_T/H(E_p)).$$

By Lemma 7, we may choose R-module generators ξ_j for $R^{(j)}$ such that $\xi_2^\tau = -\varepsilon\xi_2$, $\xi_j^\tau = \varepsilon\xi_j$, $j \neq 2$. Fix $e \in E_p^\varepsilon - \{0\}$, $e' \in E_p^{-\varepsilon} - \{0\}$. Write γ for a fixed generator of G.

We define homomorphisms ϕ_j: $\mathrm{Hom}(R^{(j)}, E_p)$ by letting

$$\phi_1(\xi_1) := e\,, \quad \phi_1(\gamma\xi_1) := e'\,, \quad \phi_1(\xi_1^g) := 0\,, \quad g \in G\,, \quad g \neq 1_G, \gamma\,;$$
$$\phi_2(\xi_2) := e'\,, \quad \phi_2(\xi^g) := 0\,, \quad g \in G\,, \quad g \neq 1_G\,;$$
$$\phi_j(\xi_j) := e\,, \quad \phi_j(\xi_j^g) = 0\,, \quad g \in G\,, \quad g \neq 1_G\,, \quad 3 \leqslant j \leqslant s - s_1 + 1\,.$$

By the Chebotarev density theorem there exist infinitely many primes l_2 such that

$$\mathrm{Frob}_{l_2}(M_T/\boldsymbol{Q}) = [\tau\pi(\phi_1, \phi_2, \ldots, \phi_{s-s_1+2})]\,.$$

We leave to the reader the task of checking, also keeping in mind the proof of Lemma 13, that these primes satisfy the above conditions.

PROPOSITION 20. *In the «case 2.1», we have* $\omega^{t_0} V_{s_1+1} = 0$.

PROOF. We have $\mathrm{res}_{l_2}(Rd(l_1 l_2)) \simeq \mathrm{res}_{l_2} \mathcal{E}_1 \simeq (\omega)^{t_1}$, with sign $(\mathrm{res}_{l_2}(Rd(l_1 l_2))) = -\varepsilon$. Note that $V_{s_1+1}/\mathcal{C} = \mathcal{E}_1 + V_{s_1+1}/\mathcal{E}_1 = W$. Since $\mathrm{res}_{l_1} V_{s_1+1} = 0$, global duality and the Galois-equivariance of the local Tate pairing give $\omega^{t_1}(V_{s_1+1}/C) = 0$ (cf. the proof of Prop. 14). Moreover, $\omega^{t_0 - t_1}\mathcal{C} = 0$, since this holds for $\widetilde{\mathcal{C}}$. The thesis follows.

PROPOSITION 21. *In the «case 2.1»,* $\omega^{t_0} V_j = 0$ *for* $s_1 + 2 \leqslant j \leqslant s$.

PROOF. Our choice of l_2 and the fact that $\mathrm{res}_{l_1} V_j = 0$, combined with a global duality argument similar to the one above, gives $\omega^{t_1+1} V_j = 0$. Since $t_1 < t_0$ by Lemma 16, we obtain $\omega^{t_0} V_j = 0$.

Case 2.2: Assume that $\mathcal{C} = V_{s_1+1}$.

We already observed that $\omega^{t_0 - t_1}\mathcal{C} = 0$. Thus the following concludes the Proof of Th. 12.

PROPOSITION 22. *In the «case 2.2»,* $\omega^{t_0} V_j = 0$ *for* $s_1 + 2 \leqslant j \leqslant s$.

PROOF. Choose a Kolyvagin prime l_2 such that

$$\mathrm{res}_{l_2}(\mathcal{E}_1) \simeq (\mathcal{E}_1)\,,$$
$$\mathrm{res}_{l_2}(V_i) \simeq V_i\,, \quad s_1 + 2 \leqslant i \leqslant s\,,$$
$$\mathrm{res}_{l_2}(\mathcal{E}_1) \cap \mathrm{res}_{l_2}(V_i) = (\mathrm{res}_{l_2}\mathcal{E}_1)^G\,.$$

It is clear that the choice we made in the proof of Lemma 19 will work, since these conditions are weaker than those of Lemma 19. As in the proof of Prop. 21, we deduce $\omega^{t_1+1} V_j = 0$, hence the thesis.

3. IWASAWA THEORY

Let γ be a topological generator of $\mathrm{Gal}(K_\infty/K)$, and let $\omega := \gamma - 1$. The mod p Iwasawa algebra $\Lambda := \boldsymbol{Z}/p\boldsymbol{Z}[\![\mathrm{Gal}(K_\infty/K)]\!]$ is a DVR. Under our assumptions, $\mathcal{E}_n$ embeds in $\mathcal{E}_{n+1}$ under the restriction map. Let $\mathcal{E}_\infty := \varprojlim_n \mathcal{E}_n$, where the limit is taken with respect to the norm mappings. Write χ_∞ for the Pontryagin dual of $\mathrm{Sel}_p(E/K_\infty)$.

LEMMA 23. *Assume that* $\mathcal{E}_\infty \neq 0$. *Then there is an isomorphism of* Λ*-modules*

$$\chi_\infty \simeq \Lambda \oplus \Lambda/(\omega)^{\alpha_1} \oplus \ldots \oplus \Lambda/(\omega)^{\alpha_s},$$

where the $\alpha_i \geq 1$. *In particular, the* Λ-rank *of* χ_∞ *is* 1.

PROOF. By assumption, there exists n such that $\mathcal{E}_n \neq 0$. Let $\mathcal{E}_n \simeq R_n \omega^{t_0}$. By fact 1, §1 we get $\mathcal{E}_m \simeq R_m \omega^{t_0} \neq 0$ for all $m \geq n$. Then, for all $m \geq n$ Th. 12 gives

$$\mathrm{Sel}_p(E/K_m) \simeq R_m \oplus R_m/(\omega)^{\alpha_1} \oplus \ldots \oplus R_m/(\omega)^{\alpha_s},$$

with the $\alpha_i \geq 1$. Lemma 3 implies that $\mathrm{Sel}_p(E/K_m)^{\mathrm{dual}}$ is isomorphic to $\mathrm{Sel}_p(E/K_m)$ as an R_m-module. The thesis follows from the isomorphism

$$\chi_\infty/(\gamma^{p^m} - 1)\chi_\infty \simeq (\mathrm{Sel}_p(E/K_m))^{\mathrm{dual}},$$

consequence of fact 3, §1.

Given a decomposition as in Lemma 22 we let

$$(\chi_\infty)_{\mathrm{tors}} := \Lambda/(\omega)^{\alpha_1} \oplus \ldots \oplus \Lambda/(\omega)^{\alpha_s}.$$

$(\chi_\infty)_{\mathrm{tors}}$ is well defined up to isomorphisms. It is the analogue of the torsion over the Iwasawa algebra of the dual of $\mathrm{Sel}_{p^\infty}(E/K_\infty)$, which one considers in characteristic zero. Moreover, if U_n denotes the sub-module of $\mathrm{Sel}_p(E/K_n)$ defined in Lemma 9, let $U_\infty := \varprojlim_n U_n$, where the limit is with respect to the norm mappings. Then $U_\infty \simeq \Lambda$. We call

$$\mathrm{char}(U_\infty/\mathcal{E}_\infty) := \mathrm{Ann}_\Lambda(U_\infty/\mathcal{E}_\infty)$$

the *characteristic ideal* of $U_\infty/\mathcal{E}_\infty$. Thus $\mathrm{char}(U_\infty/\mathcal{E}_\infty) = \Lambda\omega^{t_0}$ if $\mathcal{E}_n \simeq R_n \omega^{t_0} \neq 0$ for some n.

We reformulate in the present situation Th. 12.

THEOREM 24. $\mathrm{char}(U_\infty/\mathcal{E}_\infty)$ *annihilates* $(\chi_\infty)_{\mathrm{tors}}$.

REMARKS.

1) Th. 24 provides evidence (mod p) for a conjecture of B. Perrin-Riou [4], which is the analogue in the current setting of the Main Conjecture of Iwasawa theory for cyclotomic fields.

2) Th. 24 can be viewed as a refinement in the mod p case of the main result of [1], relative to the characteristic zero situation, where a similar statement is proved with an extra-factor appearing in the annihilator. Can the methods of this paper be extended to the characteristic zero case in order to improve the result of [1]?

3) The same techniques of this paper can be used inductively to show that the characteristic ideal of $(\chi_\infty)_{\mathrm{tors}}$ $\mathrm{char}((\chi_\infty)_{\mathrm{tors}}) := \left(\prod_{i=1}^{s} \omega^{\alpha_i}\right)\Lambda$ divides a certain power of $\mathrm{char}(U_\infty/\mathcal{E}_\infty)$.

References

[1] M. Bertolini, *Selmer groups and Heegner points in anticyclotomic $\mathbf{Z}_p$-extensions.* Preprint.

[2] M. Bertolini - H. Darmon, *Kolyvagin's descent and Mordell-Weil groups over ring class fields.* Journal für die Reine und Angewandte Mathematik, 412, 1990, 63-74.

[3] B. H. Gross, *Kolyvagin's work on modular elliptic curves*. In: Proceedings of the Durham Symposium on *L-functions and Arithmetic.* Cambridge Univ. Press, 1991.

[4] B. Perrin-Riou, *Fonctions L p-adiques Théorie d'Iwasawa et points de Heegner.* Bull. Soc. Math. de France, 115, 1987, 399-456.

Dipartimento di Matematica
Università degli Studi di Pavia
Via Abbiategrasso, 209 - 27100 Pavia