BULLETIN OF THE BRAZILIAN MATHEMATICAL SOCIETY

Bull Braz Math Soc, New Series 41(3), 399-407

A note on Iwasawa μ-invariants of elliptic curves

Rupam Barman and Anupam Saikia

Abstract. Suppose that E_1 and E_2 are elliptic curves defined over $\mathbb{Q}$ and p is an odd prime where E_1 and E_2 have good ordinary reduction. In this paper, we generalize a theorem of Greenberg and Vatsal [3] and prove that if $E_1[p^i]$ and $E_2[p^i]$ are isomorphic as Galois modules for $i = \mu(E_1)$, then $\mu(E_1) \leq \mu(E_2)$. If the isomorphism holds for $i = \mu(E_1) + 1$, then both the curves have same μ-invariants. We also discuss one numerical example.

Keywords: elliptic curves, Iwasawa μ-invariants, Selmer groups.

Mathematical subject classification: Primary: 11G05, 14H52.

1 Introduction

Let E be an elliptic curve defined over $\mathbb{Q}$ with good ordinary reduction at p. Let Σ denote any finite set of primes containing p, ∞, and the primes of bad reduction for E. Let $\mathbb{Q}_\infty$ be the cyclotomic-$\mathbb{Z}_p$ extension of $\mathbb{Q}$. Let η_p be the unique prime of $\mathbb{Q}_\infty$ lying over p, and I_{η_p} be the inertia subgroup of $G_{(\mathbb{Q}_\infty)_{\eta_p}}$. The Selmer group $S_{E[p^\infty]}(\mathbb{Q}_\infty)$ is defined as, following [3],

$$S_{E[p^\infty]}(\mathbb{Q}_\infty) := \ker\Big(H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, E[p^\infty]) \to \prod_{l\in\Sigma} \mathcal{H}_l(\mathbb{Q}_\infty, E[p^\infty])\Big), \quad (1.1)$$

where for $l \neq p$, $\mathcal{H}_l(\mathbb{Q}_\infty, E[p^\infty]) := \prod_{\eta|l} H^1((\mathbb{Q}_\infty)_\eta, E[p^\infty])$, with η running over the primes of $\mathbb{Q}_\infty$ lying over l, and

$$\mathcal{H}_p\big(\mathbb{Q}_\infty, E[p^\infty]\big) := H^1\big((\mathbb{Q}_\infty)_{\eta_p}, E[p^\infty]\big)/L_{\eta_p}$$

where $L_{\eta_p} = \ker\Big(H^1((\mathbb{Q}_\infty)_{\eta_p}, E[p^\infty]) \to H^1(I_{\eta_p}, \widetilde{E}[p^\infty])\Big)$. This is in fact the classical Selmer group of E over $\mathbb{Q}_\infty$. Since it is the object one usually works with, there is a lot of interest in gaining information about its mu-invariant.

Received 27 October 2009.

Let Σ_0 be any subset of Σ which does not contain p. We also consider a "non-primitive" Selmer group, following [3], defined by

$$S^{\Sigma_0}_{E[p^\infty]}(\mathbb{Q}_\infty) = \ker\Big(H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, E[p^\infty]) \to \prod_{l\in\Sigma-\Sigma_0} \mathcal{H}_l(\mathbb{Q}_\infty, E[p^\infty])\Big).$$

We now define a Selmer group for $E[p^i]$ where $i \geq 1$ in the following way. Let

$$S^{\Sigma_0}_{E[p^i]}(\mathbb{Q}_\infty) := \ker\Big(H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, E[p^i]) \to \prod_{l\in\Sigma-\Sigma_0} \mathcal{H}_l(\mathbb{Q}_\infty, E[p^i])\Big).$$

For

$$l \neq p,\ \mathcal{H}_l\big(\mathbb{Q}_\infty, E[p^i]\big) := \prod_{\eta|l} H^1\big(I_\eta, E[p^i]\big),$$

and for

$$l = p,\ \mathcal{H}_p\big(\mathbb{Q}_\infty, E[p^i]\big) := H^1\big(I_{\eta_p}, \widetilde{E}[p^i]\big).$$

Both $S_{E[p^\infty]}(\mathbb{Q}_\infty)$ and $S^{\Sigma_0}_{E[p^\infty]}(\mathbb{Q}_\infty)$ are modules over the Iwasawa algebra $\Lambda := \mathbb{Z}_p[[\Gamma]]$, where $\Gamma = G(\mathbb{Q}_\infty/\mathbb{Q})$. It is a deep theorem of Kato that $S_{E[p^\infty]}(\mathbb{Q}_\infty)$ is cotorsion over Λ. This allows us to define the μ-invariant which is the largest power of p dividing the characteristic polynomial.

Theorem 1.1 (See [3]). *We have* $\mu\Big(\widehat{S_{E[p^\infty]}(\mathbb{Q}_\infty)}\Big) = \mu\Big(\widehat{S^{\Sigma_0}_{E[p^\infty]}(\mathbb{Q}_\infty)}\Big)$.

Suppose that E_1 and E_2 are elliptic curves defined over $\mathbb{Q}$. Let p be an odd prime where E_1 and E_2 have good ordinary reduction. If $E_1[p] \cong E_2[p]$ as $G_{\mathbb{Q}}$-modules, then in [3], Greenberg and Vatsal proved that $S_{E_1[p^\infty]}(\mathbb{Q}_\infty)[p]$ is finite if and only if $S_{E_2[p^\infty]}(\mathbb{Q}_\infty)[p]$ is finite. Consequently, if $\mu(S_{E_1[p^\infty]}(\mathbb{Q}_\infty)) = 0$ then $\mu(S_{E_2[p^\infty]}(\mathbb{Q}_\infty)) = 0$. The aim of this paper is to prove the following main result and to discuss a numerical example. The proof of the main result is a simple generalization of the one given by Greenberg and Vatsal [3].

Theorem 1.2. *Suppose that E_1 and E_2 are elliptic curves defined over $\mathbb{Q}$. Let p be an odd prime where E_1 and E_2 have good ordinary reduction. Assume that $E_1[p^i] \cong E_2[p^i]$ as $G_{\mathbb{Q}}$-modules for $i = \mu(E_1)$. Also assume that both $E_1(\mathbb{Q})[p]$ and $E_2(\mathbb{Q})[p]$ are trivial. Then $\mu(E_1) \leq \mu(E_2)$. If $E_1[p^i] \cong E_2[p^i]$ as $G_{\mathbb{Q}}$-modules for $i = \mu(E_1) + 1$, then $\mu(E_1) = \mu(E_2)$.*

2 Proof of the Main Result

Before giving the proof of the Theorem 1.2, we first state a lemma.

Lemma 2.1. *Let $S = \mathrm{S}_{E[p^\infty]}(\mathbb{Q}_\infty)$ and $X_E(\mathbb{Q}_\infty)$ be the Pontryagin dual. Let p be a prime where E has good ordinary reduction. Then*

$$\mu(X_E(\mathbb{Q}_\infty)) = \sum_{i=1}^{\infty} \mathrm{corank}_{\mathbb{F}_p[[T]]} \frac{S[p^i]}{S[p^{i-1}]}.$$

Proof. The proof follows without difficulty from the following exact sequences and comparing $\mathbb{F}_p[[T]]$-coranks

$$0 \to \widehat{\left(\frac{S}{p^r S}\right)} \to \widehat{\left(\frac{S}{p^{r+1} S}\right)} \to \widehat{\left(\frac{p^r S}{p^{r+1} S}\right)} \to 0. \tag{2.1}$$

$$0 \to \left(p^{r-1} S\right)[p] \to \left(p^{r-1} S\right) \to (p^{r-1} S) \to \frac{p^{r-1} S}{p^r S} \to 0. \tag{2.2}$$

□

The following result is an easy generalization of Proposition 2.8 in [3] (also see [1]).

Theorem 2.2. *Let p be an odd prime. Assume that Σ_0 is a subset of $\Sigma - \{p, \infty\}$. Assume that $E(\mathbb{Q})[p] = 0$ and $i \geq 1$. Then*

$$S^{\Sigma_0}_{E[p^\infty]}(\mathbb{Q}_\infty)[p^i] \cong S^{\Sigma_0}_{E[p^i]}(\mathbb{Q}_\infty).$$

Proof. Since $H^0(\mathbb{Q}, E[p]) = E(\mathbb{Q})[p] = 0$ and $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$ is a pro-p group, we have $H^0(\mathbb{Q}_\infty, E[p^\infty]) = 0$. Consider the exact sequence

$$0 \to E[p^i] \to E[p^\infty] \xrightarrow{p^i} E[p^\infty] \to 0$$

of $\mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty)$-modules. Taking $\mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty)$ cohomology and using the fact that $H^0(\mathbb{Q}_\infty, E[p^\infty]) = 0$, we find the following isomorphism

$$H^1\big(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, E[p^i]\big) \cong H^1\big(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, E[p^\infty]\big)[p^i].$$

Comparing the local conditions defining $S^{\Sigma_0}_{E[p^\infty]}(\mathbb{Q}_\infty)[p^i]$ and $S^{\Sigma_0}_{E[p^i]}(\mathbb{Q}_\infty)$, we complete the proof of the result. □

Let Σ be a finite set of primes containing p, ∞, and all primes where either E_1 or E_2 has bad reduction. Let $\Sigma_0 = \Sigma - \{p, \infty\}$.

Proof of the Theorem 1.2. From Theorem 2.1 and Theorem 1.1, we have

$$\begin{aligned}
\mu(E_1) &= \sum_{i=1}^{\mu(E_1)} \operatorname{corank}_{\mathbb{F}_p[[T]]} \frac{S^{\Sigma_0}_{E_1[p^\infty]}(\mathbb{Q}_\infty)[p^i]}{S^{\Sigma_0}_{E_1[p^\infty]}(\mathbb{Q}_\infty)[p^{i-1}]} \\
&= \sum_{i=1}^{\mu(E_1)} \operatorname{corank}_{\mathbb{F}_p[[T]]} \frac{S^{\Sigma_0}_{E_1[p^i]}(\mathbb{Q}_\infty)}{S^{\Sigma_0}_{E_1[p^{i-1}]}(\mathbb{Q}_\infty)} \\
&= \sum_{i=1}^{\mu(E_1)} \operatorname{corank}_{\mathbb{F}_p[[T]]} \frac{S^{\Sigma_0}_{E_2[p^i]}(\mathbb{Q}_\infty)}{S^{\Sigma_0}_{E_2[p^{i-1}]}(\mathbb{Q}_\infty)} \\
&= \sum_{i=1}^{\mu(E_1)} \operatorname{corank}_{\mathbb{F}_p[[T]]} \frac{\mathrm{S}^{\Sigma_0}_{E_2[p^\infty]}(\mathbb{Q}_\infty)[p^i]}{\mathrm{S}^{\Sigma_0}_{E_2[p^\infty]}(\mathbb{Q}_\infty)[p^{i-1}]} \\
&\leq \mu(E_2).
\end{aligned}$$

The equalities follow directly from Theorem 2 and the isomorphisms $E_1[p^i] \cong E_2[p^i]$ as $G_{\mathbb{Q}}$-modules for $i = \mu(E_1)$. Indeed, since $E_1[p^i] \cong E_2[p^i]$ as $G_{\mathbb{Q}}$-modules for $i = \mu(E_1) + 1$, so

$$\operatorname{corank}_{\mathbb{F}_p[[T]]} \frac{\mathrm{S}^{\Sigma_0}_{E_1[p^i]}(\mathbb{Q}_\infty)}{\mathrm{S}^{\Sigma_0}_{E_1[p^{i-1}]}(\mathbb{Q}_\infty)} = 0$$

implies

$$\operatorname{corank}_{\mathbb{F}_p[[T]]} \frac{\mathrm{S}^{\Sigma_0}_{E_2[p^i]}(\mathbb{Q}_\infty)}{\mathrm{S}^{\Sigma_0}_{E_2[p^{i-1}]}(\mathbb{Q}_\infty)} = 0$$

for $i = \mu(E_1) + 1$. Hence if $E_1[p^i] \cong E_2[p^i]$ as $G_{\mathbb{Q}}$-modules for $i = \mu(E_1) + 1$, then $\mu(E_1) = \mu(E_2)$. □

3 Numerical examples

Consider the following elliptic curves:

$$E_1 : y^2 = x^3 - x^2 - 2858x - 10163, \qquad [4900a1] \qquad (3.1)$$

$$E_2 : y^2 = x^3 - x^2 - 174358x - 27964663, \qquad [4900a2] \qquad (3.2)$$

$$E_3 : y^2 = x^3 - x^2 - 24908x + 1522312, \qquad [4900b1] \qquad (3.3)$$

$$E_4 : y^2 = x^3 - x^2 + 24092x + 6422312. \qquad [4900b2] \qquad (3.4)$$

Here the labels in the square brackets denote the Cremona numbers of the curves. We begin with some facts about these curves. There is a single 3-isogeny $\phi \colon E_1 \longrightarrow E_2$ and $\psi \colon E_3 \longrightarrow E_4$, defined over $\mathbb{Q}$. All the curves have good ordinary reduction at 3. A computation using 3-division polynomials shows that there is no non-trivial 3-torsion point over $\mathbb{Q}$ on these curves. Recall that for an elliptic curve $E \colon y^2 = x^3 + ax + b$ over $\mathbb{Q}$, its 3-division polynomial is given by $\psi(x) = 3x^4 + 6ax^2 + 12bx - a^2$. Let x_0, x_1 be two different roots of ψ, so that

$$\psi(x) = 3(x - x_0)\big(x^3 + x_0x^2 + \big(2a + x_0^2\big)x + 4b + 2ax_0 + x_0^3\big).$$

Let $y_1^2 = x_1^3 + ax_1 + b$. Then $-4y_1^2x_0 = (x_0^2 + a + 2x_0x_1)^2$. Hence

$$y_1 = \pm\sqrt{-x_0}\left(x_1 + \frac{x_0^2 + a}{2x_0}\right).$$

Similarly,

$$y_0 = \pm\sqrt{-x_1}\left(x_0 + \frac{x_1^2 + a}{2x_1}\right).$$

Therefore, $\mathbb{Q}(E[3]) = \mathbb{Q}(\sqrt{-x_0}, \sqrt{-x_1}, \sqrt{-x_2}, \sqrt{-x_3})$, which is nothing but the splitting field of $\psi(-X^2) = 3X^8 + 6aX^4 - 12bX^2 - a^2$.

Lemma 3.1. *Suppose that for an elliptic curve $E/\mathbb{Q}$, $\mathbb{Q}(E[3])$ denotes the field of 3-torsion points. Then $\mathbb{Q}(E_1[3]) = \mathbb{Q}(E_3[3])$ and $\mathbb{Q}(E_2[3]) = \mathbb{Q}(E_4[3])$. Moreover, these fields are of degree 12 over $\mathbb{Q}$. There is a 3-torsion point of E_1 and E_3 defined over $\mathbb{Q}(\sqrt{5})$, while E_2 and E_4 have a 3-torsion point defined over $\mathbb{Q}(i\sqrt{15})$.*

Proof. Let $\psi_i(X)$ denote the 3-division polynomial for the Weierstrass equation of $E_i : i = 1, \ldots, 4$. Using MAGMA the splitting fields of $\psi_1(-X^2)$ and $\psi_3(-X^2)$ as well as $\psi_2(-X^2)$ and $\psi_4(-X^2)$ are found to be equal. Further, the degree of the extensions $\mathbb{Q}(E_i[3])$ over $\mathbb{Q}$ is also found to be 12 for each i. Along with this, we also find 3-torsion points

$$P_1 = (2940, 2^3 3^3 7^2 5\sqrt{5}), \qquad P_2 = (-8820, 2^3 3.5.7^2\sqrt{15}i),$$
$$P_3 = (2940, 2^4 3^3.5.7\sqrt{5}), \qquad P_4 = (-8820, 2^4.3.5^4.7\sqrt{15}i)$$

on E_1, E_2, E_3, E_4 respectively. Therefore E_1 and E_3 have a 3-torsion point over $L = \mathbb{Q}(\sqrt{5})$, while E_2 and E_4 have a 3-torsion point over $K = \mathbb{Q}(\sqrt{15}i)$. □

Our next goal is to show that $E_1[3] \cong E_3[3]$ and $E_2[3] \cong E_4[3]$ as $G_{\mathbb{Q}}$-modules.

We would like to acknowledge the suggestions and help of Aribam C. Sharma in finding a proof of the following theorem.

Theorem 3.2. *As $G_{\mathbb{Q}}$-modules, $E_1[3] \cong E_3[3]$ and $E_2[3] \cong E_4[3]$.*

Proof. Let ρ_i denote the $G_{\mathbb{Q}}$-representation associated to $E_i[3]$, for $i = 1, \ldots, 4$ and $L = \mathbb{Q}(\sqrt{5})$ and $K = \mathbb{Q}(i\sqrt{15})$. Since each of these curves admit a 3-isogeny, we get

$$\rho_1(g) \sim \begin{pmatrix} \epsilon(g) & b(g) \\ 0 & \eta(g) \end{pmatrix} \quad \text{and} \quad \rho_3(g) \sim \begin{pmatrix} \epsilon'(g) & b'(g) \\ 0 & \eta'(g) \end{pmatrix} \; \forall g \in G_{\mathbb{Q}},$$

where $\epsilon, \epsilon', \eta, \eta'$ are all characters of $G_{\mathbb{Q}}$. Since there is 3-torsion point in L, we have

$$\rho_1|_{G_L} \sim \begin{pmatrix} 1 & * \\ 0 & \chi \end{pmatrix} \quad \text{and} \quad \rho_3|_{G_L} \sim \begin{pmatrix} 1 & * \\ 0 & \chi \end{pmatrix}.$$

where $\chi = \chi_3 \pmod 3$ is the mod 3 cyclotomic character. Suppose that $\Delta := G_{\mathbb{Q}}/G_L =< \tau >$, then $\epsilon(\tau) = -1$ as there is no non-trivial rational 3-torsion. Therefore, $\eta(\tau) = -\chi(\tau)$.

Comparing the traces of $\rho_1(g) \mid_{G_L}$, we get $\epsilon(g) + \eta(g) = 1 + \chi(g)$, for $g \in G_L$. Therefore, by Artin's theorem on linear independence of characters, either $\epsilon(g) = \chi(g)$ or 1 for $g \in G_L$. Suppose that $\epsilon(g) = \chi(g)$. Then

$$\rho_1 \mid_{G_L} (g) \sim \begin{pmatrix} \chi(g) & b(g) \\ 0 & \eta(g) \end{pmatrix},$$

which means that there is a point in $E_1[3]$, say P' such that $gP' = \chi(g)P'$. There is also a point P_1 in $E_1[3]$ such that $gP_1 = P_1$. It is easy to see that P_1 is not in the span of P'. Hence with respect to these points as basis, we have

$$\rho_1 \mid_{G_L} (g) \sim \begin{pmatrix} \chi(g) & 0 \\ 0 & \eta(g) \end{pmatrix}.$$

Therefore the kernel of $\rho_1 \mid_{G_L}$ cuts out a field whose extension degree over L is 2 or 4. This is not possible as the extension degree over L is computed to be 6 in the previous lemma. Hence, $\epsilon(g) = 1$ and $\eta(g) = \chi(g)$ for $g \in G_L$.

Similarly, for the $G_{\mathbb{Q}}$-representation ρ_3, we have $\epsilon'(\tau) = -1$ and $\eta'(\tau) = -\chi(\tau)$. As above, $\epsilon' \mid_{G_L} (g) = 1$ and $\eta' \mid_{G_L} (g) = \chi(g)$. Now, for any

$\gamma = h\tau \in G_{\mathbb{Q}}$ with $h \in G_L$, we have $\epsilon'(h\tau) = -1 = \epsilon(h\tau)$ and $\eta'(h\tau) = \chi(h\tau) = \eta(h\tau)$. This implies that

$$\rho_1 \sim \begin{pmatrix} \epsilon & b \\ 0 & \eta \end{pmatrix} \quad \text{and} \quad \rho_3 \sim \begin{pmatrix} \epsilon & b' \\ 0 & \eta \end{pmatrix}.$$

Let $\mathbf{F} = \mathbb{Z}/3\mathbb{Z}$ as a vector space over itself. For $g, h \in G_{\mathbb{Q}}$, using $\rho_1(gh) = \rho_1(g)\rho_2(h)$, it is easy to see that $u := \eta^{-1}b$, and $v := \eta^{-1}b'$ are 1-cocycles in $Z^1(G_{\mathbb{Q}}, \mathbf{F}(\epsilon\eta^{-1}))$. If u, v differ by a 1-coboundary in $B^1(G_{\mathbb{Q}}, \mathbf{F}(\epsilon\eta^{-1}))$, then it is easy to see that $\rho_1 \sim \rho_3$. Using the inflation-restriction sequence with respect to $G_L \subset G_{\mathbb{Q}}$, we get

$$\begin{aligned} 0 &\to H^1\big(\Delta, \mathbf{F}(\epsilon\eta^{-1})^{G_L}\big) \to H^1\big(G_{\mathbb{Q}}, \mathbf{F}(\epsilon\eta^{-1})\big) \\ &\to H^1\big(G_L, \mathbf{F}(\epsilon\eta^{-1})\big)^{\Delta} \to H^2\big(\Delta, \mathbf{F}(\epsilon\eta^{-1})^{G_L}\big). \end{aligned}$$

Since Δ acts non-trivially on the one dimensional space $\mathbf{F}(\epsilon\eta^{-1})$ and Δ is cyclic, therefore the first term of this sequence vanishes. Hence we have an inclusion

$$H^1\big(G_{\mathbb{Q}}, \mathbf{F}(\epsilon\eta^{-1})\big) \hookrightarrow H^1\big(G_L, \mathbf{F}(\chi^{-1})\big)^{\Delta} \hookrightarrow H^1\big(G_L, \mathbf{F}(\chi^{-1})\big), \tag{3.5}$$

where we have used the fact that $\epsilon \mid_{G_L} = 1$ and $\eta \mid_{G_L} = \chi$. Let M be the extension over L cut out by χ, $H = G_M$ and $D = G(M/L)$. Then $M = K(\mu_3)$ so that D has order 2. Using the inflation restriction sequence again, but with respect to $H \subset G_L$, we get

$$\begin{aligned} 0 &\longrightarrow H^1\big(D, \mathbf{F}(\chi^{-1})^H\big) \longrightarrow H^1\big(G_L, \mathbf{F}(\chi^{-1})\big) \\ &\longrightarrow H^1\big(H, \mathbf{F}(\chi^{-1})\big)^D \longrightarrow H^2\big(D, \mathbf{F}(\chi^{-1})^H\big). \end{aligned}$$

As D is cyclic and H acts trivially on $\mathbf{F}$, the first term is trivial.

Combining this injection with the injection in (3.5), we get

$$H^1\big(G_{\mathbb{Q}}, \mathbf{F}(\epsilon\eta^{-1})\big) \hookrightarrow H^1\big(G_L, \mathbf{F}(\chi^{-1})\big) \hookrightarrow H^1\big(H, \mathbf{F}(\chi^{-1})\big)^D.$$

Let $b \mid_{G_L} = a, b' \mid_{G_L} = a'$. By the first injectivity, to show that b, b' are co-homologous it is enough to show that a, a' differ by a co-boundary. We give a proof of this below.

Since H acts trivially on $\mathbf{F}(\chi^{-1})$ therefore $H^1(H, \mathbf{F}(\chi^{-1}))^D = \mathrm{Hom}(H, \mathbf{F})^D$. Hence the image of a, which is $a|_H$, gives a homomorphism $H \longrightarrow \mathbf{F}$.

Since $\mathbb{Q}(E_1[3]) = \mathbb{Q}(E_3[3])$, therefore the field cut out by $a|_H$ and $a'|_H$ are the same. Hence $J := ker(a|_H) = ker(a'|_H) =: J'$. Further, as $a|_H$, and $a'|_H$

are non-trivial, they are surjective. Hence $a|_H$, and $a'|_H$ are isomorphisms from H/J onto $\mathbf{F}$. Finally, since $|H/J| = |\mathbf{F}| = 3$, therefore $|\mathrm{Isom}(H/J, \mathbf{F})| = 2$, and hence either $a|_H = a'|_H$ or $a|_H = -a'|_H$.

If $a|_H = a'|_H$, then by injectivity of the above exact sequence, it follows that $[a] = [a']$ and we are done.

Let $a|_H = -a'|_H = 2a'|_H$, then $[a] = [2a']$. Therefore $[b] = [2b']$. As $[2b'] = 2[b']$, so

$$\begin{pmatrix} \epsilon & b \\ 0 & \eta \end{pmatrix} \sim \begin{pmatrix} \epsilon & 2b' \\ 0 & \eta \end{pmatrix}.$$

Now,

$$\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} \epsilon & b' \\ 0 & \eta \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}^{-1} = \begin{pmatrix} \epsilon & 2b' \\ 0 & \eta \end{pmatrix}.$$

Therefore

$$\begin{pmatrix} \epsilon & b \\ 0 & \eta \end{pmatrix} \sim \begin{pmatrix} \epsilon & b' \\ 0 & \eta \end{pmatrix}.$$

Hence $\rho_1 \sim \rho_3$. This proves that $E_1[3]$ and $E_3[3]$ are isomorphic as $G_{\mathbb{Q}}$-modules.

In a similar manner, since the elliptic curves E_2 and E_4 have a 3-torsion point over $K = \mathbb{Q}(i\sqrt{15})$ and $\mathbb{Q}(E_2[3]) = \mathbb{Q}(E_4[3])$, along with the fact that $\mathbb{Q}(E_2[3])$ has degree 12 over $\mathbb{Q}$, we see that $\rho_2 \sim \rho_4$, thereby completing the proof. □

Theorem 3.3. *As $G_{\mathbb{Q}}$-modules, $E_1[9] \cong E_3[9]$ and $E_2[9] \ncong E_4[9]$.*

Proof. Using Sage, William Stein has checked that $E_1[9]$ and $E_3[9]$ are isomorphic, in fact "equal", as subvarieties of $J_0(4900)$. The 9-division polynomials of E_2 and E_4 have factors of degree $1 + 3 + 9 + 27$. Using Sage it can be checked that the two degree 27 polynomials (the largest factors of the two 9-division polynomials) do not define isomorphic fields. Let $f\colon E_2[9] \longrightarrow E_4[9]$ be an isomorphism of Galois modules. Then for each $P \in E_2[9]$ its field of definition $\mathbb{Q}(P)$ is equal to $\mathbb{Q}(f(P))$. Clearly subgroup of $G_{\mathbb{Q}}$ fixing $\{P, -P\}$ is the same subgroup for P as for $f(P)$. The fixed field of this subgroup is $\mathbb{Q}(x(P))$, hence $\mathbb{Q}(x(P)) = \mathbb{Q}(x(f(P)))$. Since the last fact holds for every (nonzero) $P \in E_2[9]$, it follows that the two 9-division polynomials (whose roots are all the $x(P)$ for nonzero P) match up, in the sense that there is a bijection from the irreducible factors of the first to those of the second such that for each irreducible factor h_2 of the first which matches the factor h_4 of the second, the fields $\mathbb{Q}[x]/(h_2)$ and $\mathbb{Q}[x]/(h_4)$ are isomorphic. But $E_2[9]$ and $E_4[9]$ have a single irreducible factor of degree 27 in its 9-division polynomial, but these do not define isomorphic number fields. This proves that $E_2[9] \ncong E_4[9]$ as Galois modules. □

Using MAGMA, we find that the first coefficients of the p-adic L-functions of E_1 and E_3 are not divisible by 3. Therefore, assuming the *main conjecture*, the μ-invariant of E_1 and E_3 are 0. Moreover, since the ratio of the periods is 3 in each isogeny class, so the μ-invariant of E_2 and E_4 are 1. This numerically verifies our Main theorem.

Acknowledgment. We are very grateful to William Stein for writing a SAGE code for us to check that $E_1[9]$ and $E_3[9]$ are the same as subvarieties of $J_0(4900)$. We are also very grateful to John H. Coates for careful reading of the initial draft of the manuscript. We also thank Aribam C. Sharma, Christian Wuthrich, and John Cremona for many helpful suggestions during the preparation of the article. The first author is partially supported by a grant "Teacher Fellowship" from National Board for Higher Mathematics, India.

References

[1] A. Nichifor. *Iwasawa Theory for Elliptic Curves with Cyclic Isogenies.* PhD Thesis, submitted at the Department of Mathematics, University of Washington (2004).

[2] R. Greenberg. *Introduction to Iwasawa Theory for Elliptic Curves.* IAS/Park City Mathematicas Series, **9** (2001).

[3] R. Greenberg and V. Vatsal. *On the Iwasawa Invariants of Elliptic Curves.* Invent. Math., **142** (2000), 17–63.

Rupam Barman
Department of Mathematical Sciences
Tezpur University
Napaam-784028
Sonitpur, Assam
INDIA

E-mail: rupamb@tezu.ernet.in

Anupam Saikia
Department of Mathematics
Indian Institute of Technology
Guwahati-781039
INDIA

E-mail: a.saikia@iitg.ernet.in