Math. Proc. Camb. Phil. Soc. (2013), **154**, 303–324 © *Cambridge Philosophical Society* 2012
doi:10.1017/S0305004112000564
First published online 29 October 2012

Non-commutative Iwasawa theory of elliptic curves at primes of multiplicative reduction

BY CHERN–YANG LEE
The School of Mathematical Sciences,
The University of Nottingham, Nottingham NG7 2RD.
e-mail: chern-yang.lee@nottingham.ac.uk

(*Received* 11 *April* 2011; *revised* 13 *August* 2012)

Abstract

This paper studies the compact p^{∞}-Selmer Iwasawa module $X(E/F_{\infty})$ of an elliptic curve E over a False Tate curve extension F_{∞}, where E is defined over $\mathbb{Q}$, having multiplicative reduction at the odd prime p. We investigate the p^{∞}-Selmer rank of E over intermediate fields and give the best lower bound of its growth under certain parity assumption on $X(E/F_{\infty})$, assuming this Iwasawa module satisfies the $\mathfrak{M}_H(G)$-Conjecture proposed by Coates–Fukaya–Kato–Sujatha–Venjakob.

Introduction

Throughout, p will denote an odd prime number and μ_{p^n} the group of all p^n-power roots of unity. Let $m > 1$ be an integer which is p-power free and consider the False Tate curve tower

$$\mathbb{Q} \subset F_1 \subset F_2 \subset \cdots \subset F_n \subset F_{n+1} \subset \cdots \subset F_{\infty}$$

where $F_n \overset{\text{def}}{=} \mathbb{Q}(\mu_{p^n}, \sqrt[p^n]{m})$ and $F_{\infty} \overset{\text{def}}{=} \bigcup_{n\geqslant 1} F_n$. Let E be an elliptic curve defined over $\mathbb{Q}$. We shall be concerned in this paper with proving parallel results to those given in [**1**], but with the hypothesis given there, that E has good ordinary reduction at p, replaced by the assumption that E has multiplicative reduction at p. This change of hypothesis leads to some interesting variants of the results of [**1**], for example see Theorem1·8 and Theorem1·11 in this paper. In the last section, we discuss a number of numerical examples to illustrate our general theorems.

1. *Notations and theorems*

p	a rational odd prime;
m	a positive integer greater than 1, with prime decomposition $m = \prod_i q_i^{r_i}$;
r	the positive integer $ord_p(m^{p-1} - 1) - 1$, for non-amenable pair (p, m);
K_n	$\mathbb{Q}(\mu_{p^n})$;
K	K_1;

L_n	$\mathbb{Q}(\sqrt[p^n]{m})$;
F_n	the composite of K_n and L_n;
χ_n	a character of $Gal(F_n/K_n)$ of exact order p^n;
ρ_{χ_n}	$Ind_{\mathbb{Q}}^{K_n}\chi_n$, the induced representation of χ_n to $Gal(F_n/\mathbb{Q})$;
$\mathfrak{P}_{(n)}$(or $\mathfrak{P}_{(n),i}$)	a prime of L_n above p;
$\mathcal{P}_{(n)}$(or $\mathcal{P}_{(n),i}$)	a prime of F_n above p;
K_∞	the union $\bigcup_{n\geqslant 1} K_n$;
L_∞	the union $\bigcup_{n\geqslant 1} L_n$;
F_∞	the union $\bigcup_{n\geqslant 1} F_n$;
G	the Galois group of F_∞ over $\mathbb{Q}$;
H	the closed subgroup of G which fixes $\mathbb{Q}^{cyc}$;
H_F	the closed subgroup of G which fixes F^{cyc}, for F a subfield of F_∞;
Γ_F	$Gal(F^{cyc}/F)$;
E	an elliptic curve defined over $\mathbb{Q}$;
S_p	the set $\{p\}$;
S_{ram}	the set $\{$prime divisors of $m\} = \{q_i^{\prime}s\}$;
S_{bad}	the set of primes at where E has bad reduction;
S_{good}	the set of primes at where E has good reduction;
S_{multi}	the set of primes at where E has multiplicative reduction;
S	the union $S_p \cup S_{ram} \cup S_{bad}$;
S_∞	the set consists of the Archimedean place of $\mathbb{Q}$;
S_s	the set of primes of K at where E has split multiplicative reduction;
S_{ns}	the set of primes of K at where E has non-split multiplicative reduction;
$S_*(F)$	the set of primes of F above S_* for any algebraic field F and $*$ being any subscript of S above, $K \subset F$ when $* = ns$ or s;
$\mathbb{Q}_S$	the maximal extension of $\mathbb{Q}$ which is unramified outside $S \cup S_\infty$;
$G_S(F)$	the Galois group $Gal(\mathbb{Q}_S/F)$ for any subfield $F \subset \mathbb{Q}_S$;
$X(E/F)$	the Pontryagin dual of $Sel_p(E/F)$, the classical p^∞-Selmer group of E over a subfield F of F_∞;
$s_{E/F}$	the $\mathbb{Z}_p$-rank of $X(E/F)$ for $[F:\mathbb{Q}]$ finite;
$M(p)$	the submodule of M consisting of all elements of p-power order;
$Y(E/F)$	$X(E/F)\big/X(E/F)(p)$;
$w(E)$	the root number of E;
$w(E,\rho)$	the twisted root number of E by an orthogonal Galois representation ρ.

Definition 1·1. For a p-adic Lie group $\mathcal{G}$, we denote the Iwasawa algebra of $\mathcal{G}$ by

$$\Lambda(\mathcal{G}) \overset{\text{def}}{=} \varprojlim \mathbb{Z}_p[\mathcal{G}/\mathcal{U}]$$

where the inverse limit is taken for $\mathcal{U}$ runs over all open normal subgroup of $\mathcal{G}$.

Assume from now on that the integer $m > 1$ is p-power free.

Definition 1·2 (Hypothesis A).
We say the triple (E, p, m) satisfies Hypothesis A if the elliptic curve E is defined over $\mathbb{Q}$, having multiplicative (split or non-split) reduction at p, and semi-stable reductions at all primes q_i dividing m.

Definition 1·3. Let

$$\delta_p \overset{\text{def}}{=} \begin{cases} 1, & \text{if } E \text{ has split multiplicative reduction at } p; \\ 0, & \text{if } E \text{ has non-split multiplicative reduction at } p. \end{cases} \tag{1·1}$$

Definition 1·4. Let ρ be an irreducible $\bar{\mathbb{Q}}_p$-Artin representation which factors through $Gal(F/\mathbb{Q})$ for F a finite Galois extension of $\mathbb{Q}$. Let $s_{E,\rho}$ denote the number of copies of ρ occurring in the representation $X(E/F) \otimes_{\mathbb{Z}_p} \bar{\mathbb{Q}}_p$.

CONJECTURE 1·5 (Parity Conjecture). *Let E be an elliptic curve defined over $\mathbb{Q}$. For any absolutely irreducible orthogonal Artin representation ρ of $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$, we have*

$$w(E,\rho) = (-1)^{s_{E,\rho}}. \tag{1·2}$$

Definition 1·6. Let $\mathfrak{M}_H(G)$ denote the category of all finitely generated $\Lambda(G)$-modules M, such that the quotient $M/M(p)$ is finitely generated over $\Lambda(H)$.

CONJECTURE 1·7 ($\mathfrak{M}_H(G)$-Conjecture [**2**]). *Under Hypothesis A, $X(E/F_\infty)$ belongs to the category $\mathfrak{M}_H(G)$.*

We can define the following invariants under the assumption that $\mathfrak{M}_H(G)$-Conjecture is valid:

τ	the $\Lambda(H_K)$-rank of $Y(E/F_\infty)$;
λ_F	the $\lambda_{\Lambda(\Gamma_F)}$-invariant of $X(E/F^{cyc})$, for F any subfield of F_∞ with $[F:\mathbb{Q}]$ finite;
λ_n	the value λ_{L_n}.

In this paper, I will prove the Parity Conjecture for an infinite number of ρ's under the Hypothesis A and the assumption of $\mathfrak{M}_H(G)$-Conjecture.

THEOREM 1·8. *Assume Hypothesis A and the $\mathfrak{M}_H(G)$-Conjecture. Then for all absolutely irreducible self-dual Artin representations ρ of $G = Gal(F_\infty/\mathbb{Q})$ with dimension greater than* 1, *we have*

$$w(E,\rho) = (-1)^{s_{E,\rho}}. \tag{1·3}$$

Remark 1·9. In fact, any such ρ as described in the statement of this theorem is isomorphic to the induction to $\mathbb{Q}$ of some cyclic character χ_n of $Gal(F_n/K_n)$ of exact order p^n for some $n \geqslant 1$. Namely,

$$\rho \cong \rho_{\chi_n}. \tag{1·4}$$

Moreover, these ρ_{χ_n} are all orthogonal.

Example. Let E be the elliptic curve with Cremona symbol 57b1, which has Weierstrass equation given by

$$y^2 + xy + y = x^3 - 7x + 5.$$

Since E has split multiplicative reduction at 3, non-split multiplicative reduction at 19 and good reductions elsewhere, the triple $(57b1, 3, m)$ satisfies Hypothesis A for every cubic free integer $m > 1$. We can compute the twisted root number $w(E,\rho_{\chi_n})$ using V. Dokchitser's formula (3·1) in Lemma 3·1. For instance, taking $m = 19$, we get $w(E,\rho_{\chi_1}) = 1$ and $w(E,\rho_{\chi_n}) = -1$ for all $n \geqslant 2$; taking $m = 3$, we get $w(E,\rho_{\chi_n}) = -1$ for all $n \geqslant 1$. One may deduce immediately from Theorem 1·8 that the non-negative integer $s_{E,\rho_{\chi_n}}$ is odd

https://doi.org/10.1017/S0305004112000564 Published online by Cambridge University Press

and hence positive for all $n \geqslant 2$ when $m = 19$, or for all $n \geqslant 1$ when $m = 3$. Assuming the finiteness of Tate-Shafarevich groups, the positivity of $s_{E,\rho_{\chi_n}}$ implies the existence of an extra rational point of E of infinite order, passing from over L_{n-1} to L_n. Indeed, for example when $m = 3$ and $n = 1$, we have

$$P = (-\sqrt[3]{3}^2 - \sqrt[3]{3} + 1, \sqrt[3]{3} + 2) \in E(\mathbb{Q}(\sqrt[3]{3}))$$

which is of infinite order. We will see a few more numerical examples in Section 7.

I shall prove Theorem 1·8 separately in the case where p is a prime of non-split multiplicative reduction and in the case where p is a prime of split multiplicative reduction. In the non-split multiplicative case, the proof is very similar to the case where p is a prime of good ordinary reduction, which has been proved in [**1**]. It is slightly complicated in the split multiplicative case. I shall give the proof separately in the cases defined below.

Definition 1·10. We say the pair (p, m) is amenable if either $p \mid m$ or $p \parallel m^{p-1} - 1$. We call the pair non-amenable otherwise, and denote by $r > 0$ the positive integer such that $p^{r+1} \parallel m^{p-1} - 1$.

THEOREM 1·11. *Assume Hypothesis A and the $\mathfrak{M}_H(G)$-Conjecture. Then when τ is odd,*

(i) *when E has non-split multiplicative reduction at p, we have*

$$s_{E/L_n} \geqslant n + s_{E/\mathbb{Q}} \qquad \textit{for all } n \geqslant 1; \tag{1·5}$$

$$s_{E/F_n} \geqslant p^n - 1 + s_{E/K} \qquad \textit{for all } n \geqslant 1; \tag{1·6}$$

(ii) *when E has split multiplicative reduction at p,*

(a) *for amenable pair (p, m), we have*

$$s_{E/L_n} \geqslant n + s_{E/\mathbb{Q}} \qquad \textit{for all } n \geqslant 1; \tag{1·7}$$

$$s_{E/F_n} \geqslant p^n - 1 + s_{E/K} \qquad \textit{for all } n \geqslant 1; \tag{1·8}$$

(b) *for non-amenable pair (p, m), we have*

$$s_{E/L_{r+k}} \geqslant k + s_{E/L_r} \qquad \textit{for all } k \geqslant 1; \tag{1·9}$$

$$s_{E/F_{r+k}} \geqslant p^r(p^k - 1) + s_{E/L_r K_{r+1}} \qquad \textit{for all } k \geqslant 1. \tag{1·10}$$

Moreover, when $\tau = 1$, then all the equalities in these six inequalities hold.

2. *Decompositions of p in the subfields of F_∞*

This section is irrelevant to elliptic curves. Throughout this section, we fix an odd prime p and always assume $m > 1$ being a p-power free integer.

LEMMA 2·1. *For each $n \geqslant 1$, there exists an positive integer m'_n, with either $p \nmid m'_n$ or $p \parallel m'_n$ such that*

$$\mathbb{Q}(\sqrt[p^n]{m}) = \mathbb{Q}(\sqrt[p^n]{m'_n}).$$

Proof. This is trivial except for the case where $ord_p(m) \geqslant 2$. Since $ord_p(m)$ is coprime to p by assumption, there exist integers t_n and s_n such that $ord_p(m)t_n + p^n s_n = 1$. Let $m'_n = m^{t_n} \cdot p^{p^n s_n}$. It is easy to verify the following two relations

$$\sqrt[p^n]{m'_n} = p^{s_n} \cdot (\sqrt[p^n]{m})^{t_n} \in \mathbb{Q}(\sqrt[p^n]{m})$$

https://doi.org/10.1017/S0305004112000564 Published online by Cambridge University Press

$$\sqrt[p^n]{m} = m^{s_n} p^{-s_n \cdot ord_p(m)} (\sqrt[p^n]{m'_n})^{ord_p(m)} \in \mathbb{Q}(\sqrt[p^n]{m'_n})$$

and obviously $ord_p(m'_n) = ord_p(m)t_n + p^n s_n = 1$.

2·1. *Over L_n.*

LEMMA 2·2. *We have*:

(i) *if the pair (p, m) is amenable, then for all $n \geqslant 1$*

$$p\mathcal{O}_{L_n} = \mathfrak{P}_{(n)}^{p^n}; \qquad f(\mathfrak{P}_{(n)}/p) = 1; \tag{2·1}$$

(ii) *if the pair (p, m) is non-amenable and $p^{r+1} \parallel m^{p-1} - 1$, then*:

(a) *for $1 \leqslant n \leqslant r$,*

$$p\mathcal{O}_{L_n} = \mathfrak{P}_{(n),0}\mathfrak{P}_{(n),1}^{p-1}\mathfrak{P}_{(n),2}^{p(p-1)} \cdots \mathfrak{P}_{(n),n}^{p^{n-1}(p-1)}; \qquad f(\mathfrak{P}_{(n),i}/p) = 1, \tag{2·2}$$

for $0 \leqslant i \leqslant n$;

(b) *for $n > r$,*

$$p\mathcal{O}_{L_n} = \left(\mathfrak{P}_{(n),0}\mathfrak{P}_{(n),1}^{p-1}\mathfrak{P}_{(n),2}^{p(p-1)} \cdots \mathfrak{P}_{(n),r}^{p^{r-1}(p-1)}\right)^{p^{n-r}}; \qquad f(\mathfrak{P}_{(n),i}/p) = 1, \tag{2·3}$$

for $0 \leqslant i \leqslant r$.

Proof.

(i) When $p \mid m$, we have seen that $L_n = \mathbb{Q}(\sqrt[p^n]{m'})$ for some m' such that $p \parallel m'$ by Lemma 2·1. Hence this statement is precisely [**14**, theorem 2 (a)].
It is proven in [**15**, theorem 5·4] that for any integer $r \geqslant 0$,

$$m \in \mathbb{Q}_p^{p^r} \Leftrightarrow p^{r+1} \mid m^{p-1} - 1. \tag{2·4}$$

When $p \parallel m^{p-1} - 1$, $r = 0$ and the statement is proven in [**14**, theorem 5].

(ii) (a) This is proven in [**14**, theorem 2 (b)].
(b) This is proven in [**14**, theorem 5].

PROPOSITION 2·3. *Suppose the pair (p, m) is non-amenable. Then, we have*:

$$\mathfrak{P}_{(n),0}\mathcal{O}_{L_{n+1}} = \begin{cases} \mathfrak{P}_{(n+1),0}^{p}, & r \leqslant n, \qquad (2·5a) \\ \mathfrak{P}_{(n+1),0}\mathfrak{P}_{(n+1),1}^{p-1}, & 0 \leqslant n < r; \qquad (2·5b) \end{cases}$$

and

$$\mathfrak{P}_{(n),i}\mathcal{O}_{L_{n+1}} = \begin{cases} \mathfrak{P}_{(n+1),i}^{p}, & 1 \leqslant i \leqslant r \leqslant n, \qquad (2·6a) \\ \mathfrak{P}_{(n+1),i+1}^{p}, & 1 \leqslant i \leqslant n < r. \qquad (2·6b) \end{cases}$$

Proof. This is immediate by tower law and multiplicative law on the ramification degrees.

https://doi.org/10.1017/S0305004112000564 Published online by Cambridge University Press

2·2. *Over F_n.*

PROPOSITION 2·4. *We have*:

(i) *when (p,m) is amenable, then*

$$p\mathcal{O}_{F_n} = \mathcal{P}_{(n)}^{p^{2n-1}(p-1)}; \tag{2·7}$$

(ii) *when (p,m) is non-amenable, then*

$$p\mathcal{O}_{F_n} = \begin{cases} \prod_{i=1}^{p^r} \mathcal{P}_{(n),i}^{p^{2n-r-1}(p-1)}, & r < n, \quad (2·8a) \\ \prod_{i=1}^{p^n} \mathcal{P}_{(n),i}^{p^{n-1}(p-1)}, & 0 \leqslant n \leqslant r. \quad (2·8b) \end{cases}$$

Proof. See the proof in [**15**, theorem 5·2 and lemma 6·1]

2·3. *Over F_n^{cyc}.*

Definition 2·5. For any subfield F of F_∞, denote by $S_p(F)$ the set of primes of F lying over prime p.

LEMMA 2·6. *When (p,m) is non-amenable, for $r < n < N$, we have*

$$\#S_p(K_N L_n) = p^r. \tag{2·9}$$

Proof. The completion of K_N at its only prime above p is $\mathbb{Q}_p(\zeta_{p^N})$. The minimal polynomial of $\sqrt[p^n]{m}$ over K_N is $X^{p^n} - m$, which has factorization in $\mathbb{Q}_p(\zeta_{p^N})$ as follows:

$$X^{p^n} - m = (X^{p^{n-r}})^{p^r} - b^{p^r} = \prod_{i=1}^{p^r} \left(X^{p^{n-r}} - \zeta_{p^r}^i b\right), \tag{2·10}$$

for some $b \in \mathbb{Q}_p \setminus \mathbb{Q}_p^p$ such that $b^{p^r} = m$. Applying [**11**, theorem 9·1], I claim the irreducibility of $(X^{p^{n-r}} - \zeta_{p^r}^i b)$ in $\mathbb{Q}_p(\zeta_{p^N})[X]$ by showing that $\zeta_{p^r}^i b \notin \mathbb{Q}_p(\zeta_{p^N})^p$ for all $1 \leqslant i \leqslant p^r$. Since $\zeta_{p^r}^i \in \mathbb{Q}_p(\zeta_{p^N})^p$, it is sufficient to show that $b \notin \mathbb{Q}_p(\zeta_{p^N})^p$. Suppose, on the contrary, that $b \in \mathbb{Q}_p(\zeta_{p^N})^p$, then we have $\mathbb{Q}_p(\sqrt[p]{b}) \subset \mathbb{Q}_p(\zeta_{p^N})$ which implies $\mathbb{Q}_p(\zeta_p, \sqrt[p]{b}) \subset \mathbb{Q}_p(\zeta_{p^N})$ and hence $\mathbb{Q}_p(\zeta_p, \sqrt[p]{b})$ is an abelian extension over $\mathbb{Q}_p$. By [**13**, theorem 2], $b \in \mathbb{Q}_p^p$ which contradicts the value of r.

PROPOSITION 2·7. *We have*:

(i) *when (p,m) is amenable, then,*

$$\#S_p(F_n^{cyc}) = 1, \qquad n \geqslant 0; \tag{2·11}$$

(ii) *when (p,m) is non-amenable, then,*

(a) *for $0 \leqslant n \leqslant r$, there are p^n many primes of F_n^{cyc} lying above p, we denote this fact by*

$$\#S_p(F_n^{cyc}) = p^n, \tag{2·12}$$

moreover, they all have inertia degree equal to 1;

https://doi.org/10.1017/S0305004112000564 Published online by Cambridge University Press

(b) *for $n > r$, there are p^r many primes of F_n^{cyc} lying above p, they all have inertia degree equal to* 1.

Proof.

(i) This is trivial from Proposition 2·4, which implies that

$$\#S_p(F_\infty) = 1. \tag{2·13}$$

(ii) (a) The statement is well known when $n = 0$.
Assume that the statement is true for all n with $0 \leqslant n \leqslant k < r$, by (2·8$b$),

$$p^{k+1} = \#S_p(F_{k+1}) \leqslant \#S_p\big(F_{k+1}^{cyc}\big). \tag{2·14}$$

On the other hand, since F_{k+1}^{cyc}/F_k^{cyc} is an extension of degree p, we have

$$\#S_p\big(F_{k+1}^{cyc}\big) \leqslant p \cdot S_p\big(F_k^{cyc}\big) = p^{k+1} \tag{2·15}$$

by inductive assumption. Therefore, we have

$$\#S_p\big(F_{k+1}^{cyc}\big) = p^{k+1} \tag{2·16}$$

and every prime in $S_p(F_k^{cyc})$ splits completely over F_{k+1}^{cyc} and by inductive assumption and tower law on the inertia degree, every prime in $S_p(F_{k+1}^{cyc})$ has inertia degree equals to 1. Hence we proved the statement by induction on n.

(b) For $r < n$, this statement is immediate from Lemma 2·6. Indeed, suppose $\#S_p(F_n^{cyc}) > \#S_p(F_n)$, then $\#S_p(K_{n+1}L_n) > \#S_p(F_n)$, since $K_{n+1}L_n$ is the fixed field of the maximal non-trivial open subgroup of $Gal(F_n^{cyc}/F_n)$.

2·4. *Over L_n^{cyc}.*

Definition 2·8. For Galois extensions $J_0 \subset J_1 \subset J_2$ and a prime $\mathfrak{P}_0$ of J_0, let $e(J_i/J_j, \mathfrak{P}_0)$ denote the relative ramification degree $e(\mathfrak{P}_i/J_j)$, where $\mathfrak{P}_i$ is any prime of J_i above $\mathfrak{P}_0$ over J_j. These values $e(\mathfrak{P}_i/J_j)$ are defined without the Galois assumption, but are equal when the extensions are Galois.

PROPOSITION 2·9. *We have*:

(i) *when (p, m) is amenable, then*

$$\#S_p\big(L_n^{cyc}\big) = 1, \qquad n \geqslant 0; \tag{2·17}$$

(ii) *when (p, m) is non-amenable, then*

$$\#S_p\big(L_n^{cyc}\big) = \begin{cases} 1 + \sum_{i=0}^{r-1} p^i, & r < n, \qquad (2·18a) \\ 1 + \sum_{i=0}^{n-1} p^i, & 1 \leqslant n \leqslant r, \qquad (2·18b) \\ 1, & n = 0. \qquad (2·18c) \end{cases}$$

Proof.

(i) Trivial as above.

https://doi.org/10.1017/S0305004112000564 Published online by Cambridge University Press

(ii) The case when $n = 0$ is well known.

For $1 \leqslant n \leqslant r$ and all $0 \leqslant i \leqslant n$, we have, by tower law,

$$\begin{aligned} e(F_n/L_n, \mathfrak{P}_{(n),i}) &= \frac{e(F_n/\mathbb{Q}, p)}{e(\mathfrak{P}_{(n),i}/\mathbb{Q})} = \frac{p^{n-1}(p-1)}{e(\mathfrak{P}_{(n),i}/\mathbb{Q})} \\ &= \begin{cases} p^{n-1}(p-1), & \text{for } i = 0, \\ p^{n-i}, & \text{for } 1 \leqslant i \leqslant n. \end{cases} \end{aligned} \tag{2·19}$$

On the other hand, with

$$e(F_n/L_n, \mathfrak{P}_{(n),i}) = e(F_n/K_1L_n, \mathfrak{P}_{(n),i}) \cdot e(K_1L_n/L_n, \mathfrak{P}_{(n),i}), \tag{2·20}$$

$$e(F_n/K_1L_n, \mathfrak{P}_{(n),i}) \mid [F_n : K_1L_n] = p^{n-1}, \tag{2·21}$$

$$e(K_1L_n/L_n, \mathfrak{P}_{(n),i}) \mid [K_1L_n : L_n] = p-1, \tag{2·22}$$

since $(p, p-1) = 1$, we have:

$$e(K_1L_n/L_n, \mathfrak{P}_{(n),i}) = \begin{cases} p-1, & \text{for } i = 0, & (2·23\,a) \\ 1, & \text{for } 1 \leqslant i \leqslant n; & (2·23\,b) \end{cases}$$

$$e(F_n/K_1L_n, \mathfrak{P}_{(n),i}) = \begin{cases} p^{n-1}, & \text{for } i = 0, & (2·24\,a) \\ p^{n-i}, & \text{for } 1 \leqslant i \leqslant n. & (2·24\,b) \end{cases}$$

With F_n^{cyc} being Galois over L_n, we may assume that there are d_i many primes above each prime of L_n^{cyc} above $\mathfrak{P}_{(n),i}$ for all $0 \leqslant i \leqslant n$. From the above, as $F_n^{cyc} = L_n^{cyc} \cdot K_1L_n$ we have,

$$d_i = p-1 \qquad 1 \leqslant i \leqslant n. \tag{2·25}$$

Since $Gal(L_n^{cyc}/L_n) \cong \mathbb{Z}_p$, suppose that there are p^{a_i} many primes of L_n^{cyc} lying above $\mathfrak{P}_{(n),i}$ for all $0 \leqslant i \leqslant n$. We have

$$\#S_p\big(F_n^{cyc}\big) = p^n = \sum_{i=0}^{n} d_i p^{a_i} = d_0 p^{a_0} + (p-1)\sum_{i=1}^{n} p^{a_i}. \tag{2·26}$$

As F_n^{cyc}/L_n^{cyc} is Galois of degree $p-1$, clearly $d_0 \mid p-1$ and hence we deduce $d_0 \mid p^n$ from (2·26). Conclusively, $d_0 = 1$. Alternatively, since $\mathfrak{P}_{(n),0}$ is totally ramified over F_n and $\#S_p(F_n^{cyc}) = \#S_p(F_n)$, there is a unique prime of F_n^{cyc} lying above $\mathfrak{P}_{(n),0}$, that is $d_0 \cdot p^{a_0} = 1$. This implies that $d_0 = 1$ and $p^{a_0} = 1$

$$\begin{aligned} \#S_p\big(L_n^{cyc}\big) = p^{a_0} + \sum_{i=1}^{n} p^{a_i} &= p^{a_0} + \frac{\#S_p\big(F_n^{cyc}\big) - p^{a_0}}{p-1} \\ &= p^{a_0} \cdot \left(1 + \sum_{i=0}^{n-a_0-1} p^i\right) \\ &= 1 + \sum_{i=0}^{n-1} p^i. \end{aligned} \tag{2·27}$$

For $r < n$, the proof is similar except that there are $r+1$ many primes of L_n above p, labeled as $\mathfrak{P}_{(n),i}$ for $0 \leqslant i \leqslant r$. The equations (2·19) till (2·25) still hold, with

$1 \leqslant i \leqslant n$ replaced by $1 \leqslant i \leqslant r$. With $\#S_p(F_n^{cyc}) = \#S_p(F_n) = p^r$ still holds for $r < n$, again we get $d_0 = 1$ and $p^{a_0} = 1$, where p^{a_0} denotes the number of primes of L_n^{cyc} above $\mathfrak{P}_{(n),0}$ and d_0 denotes the number of primes of F_n^{cyc} above each of the primes of L_n^{cyc} above $\mathfrak{P}_{(n),0}$. Hence we get

$$\begin{aligned}\#S_p\big(L_n^{cyc}\big) = p^{a_0} + \sum_{i=1}^{n} p^{a_i} &= p^{a_0} + \frac{\#S_p(F_n^{cyc}) - d_0 p^{a_0}}{p-1}\\ &= p^{a_0} \cdot \left(1 + \sum_{i=0}^{r-a_0-1} p^i\right) \qquad (2{\cdot}28)\\ &= 1 + \sum_{i=0}^{r-1} p^i.\end{aligned}$$

3. *Root numbers computations*

We use a slightly simplified formula of the following result of V. Dokchitser:

LEMMA 3·1 (V. Dokchitser Formula [**5**]). *Let E be an elliptic curve defined over $\mathbb{Q}$, and ρ an Artin representation which is self-dual. Let S_{add} and S_{multi} be the set of rational primes at where E has additive reduction and multiplicative reduction respectively. If ρ is unramified at all places of S_{add}, then*

$$\begin{aligned}w(E,\rho) = w(E)^{dim\rho} \cdot (-1)^{dim\rho^-} \cdot &\prod_{p\in S_{multi}} s_p^{dim\rho - dim\rho^{I_p}} \cdot det(\Phi_p|\rho^{I_p})\\ &\cdot \prod_{p\in S_{add}} det(\Phi_p|\rho)^{N_p(E)} \qquad (3{\cdot}1)\end{aligned}$$

where ρ^- denotes the eigenspace of $\rho(\tau)$ of eigenvalue -1, where τ is the complex conjugation, and the conductor of E has prime factorization $\prod_p p^{N_p(E)}$. Here Φ_p is an geometric Frobenius element, I_p is the corresponding inertia subgroup and

$$s_p = \begin{cases} -1 & \text{if } E \text{ has split multiplicative reduction at } p,\\ 1 & \text{if } E \text{ has non-split multiplicative reduction at } p.\end{cases}$$

This enables us to prove:

PROPOSITION 3·2. *Under Hypothesis A,*

(i) *when E has non-split multiplicative reduction at p, we have*

$$\frac{w(E,\rho_{\chi_n})}{w(E,\rho_K)} = \prod_{q_i \neq p \in S_{multi}} \left(\frac{q_i}{p}\right); \qquad (3{\cdot}2)$$

(ii) *when E has split multiplicative reduction at p,*

(a) *when (p, m) is amenable, we have*

$$\frac{w(E,\rho_{\chi_n})}{w(E,\rho_K)} = (-1) \cdot \prod_{q_i \neq p \in S_{multi}} \left(\frac{q_i}{p}\right); \qquad (3{\cdot}3)$$

https://doi.org/10.1017/S0305004112000564 Published online by Cambridge University Press

(b) *when* (p, m) *is non-amenable, we have*

$$\frac{w(E,\rho_{\chi_n})}{w(E,\rho_K)} = \prod_{q_i \neq p \in S_{multi}} \left(\frac{q_i}{p}\right) \times \begin{cases} -1, & \textit{for } r < n; \quad (3{\cdot}4a) \\ 1, & \textit{for } 1 \leqslant n \leqslant r. \quad (3{\cdot}4b) \end{cases}$$

Proof. By Hypothesis A, both ρ_{χ_n} and ρ_K are unramified at all places of S_{add}, so the Proposition follows from computing the quotient $w(E,\rho_{\chi_n})/w(E,\rho_K)$ using the Dokchitser formula. Elementary computations shows

$$dim\rho_K \overset{mod2}{\equiv} dim\rho_{\chi_n} \overset{mod2}{\equiv} 0,$$

$$dim\rho_K^- \overset{mod2}{\equiv} dim\rho_{\chi_n}^- \overset{mod2}{\equiv} \frac{1}{2}(p-1),$$

$$det\big(\Phi_q|\rho_K^{I_q}\big) = \begin{cases} \left(\frac{q}{p}\right), & \text{when } q \neq p, \quad (3{\cdot}5a) \\ 1, & \text{when } q = p, \quad (3{\cdot}5b) \end{cases}$$

$$det\big(\Phi_q|\rho_{\chi_n}^{I_q}\big) = \begin{cases} \left(\frac{q}{p}\right), & \text{when } q \neq p, q \nmid m, \quad (3{\cdot}6a) \\ 1, & \text{when } q \neq p, q \mid m, \quad (3{\cdot}6b) \\ 1, & \text{when } q = p. \quad (3{\cdot}6c) \end{cases}$$

For $q \in S_{add}$, $q \neq p, q_i$ by Hypothesis A. From the above, we have

$$det(\Phi_q|\rho_K) = det(\Phi_q|\rho_{\chi_n}) = \left(\frac{q}{p}\right),$$

and hence, we have simplified the quotient as

$$\begin{aligned} \frac{w(E,\rho_{\chi_n})}{w(E,\rho_K)} &= \prod_{q \in S_{multi}} \frac{s_q^{dim\rho_{\chi_n}^{I_q}} \cdot det\big(\Phi_q|\rho_{\chi_n}^{I_q}\big)}{s_q^{dim\rho_K^{I_q}} \cdot det\big(\Phi_q|\rho_K^{I_q}\big)} \\ &= \prod_{q \in S_{multi}} \frac{s_q^{dim\rho_{\chi_n}^{I_q}}}{s_q^{dim\rho_K^{I_q}}} \cdot \prod_{q_i \neq p \in S_{multi}} \left(\frac{q_i}{p}\right) \qquad (3{\cdot}7) \\ &= s_p^{\beta_n} \cdot \prod_{q_i \neq p \in S_{multi}} \left(\frac{q_i}{p}\right), \end{aligned}$$

where

$$\beta_n \overset{\text{def}}{=} \begin{cases} 0 \bmod 2, & \text{for } 1 \leqslant n \leqslant r \text{ when } (p,m) \text{ is non-amenable;} \\ 1 \bmod 2, & \text{otherwise.} \end{cases} \qquad (3{\cdot}8)$$

The final equality in (3·7) is due to the following computations:

$$dim\rho_K^{I_q} \overset{mod2}{\equiv} \begin{cases} 1, & \text{when } q = p, \quad (3{\cdot}9a) \\ 0, & \text{otherwise;} \quad (3{\cdot}9b) \end{cases}$$

$$dim\rho_{\chi_n}^{I_q} \overset{mod2}{\equiv} \begin{cases} 1, & \text{when } q = p, (p,m) \text{ is non-amenable, } 1 \leqslant n \leqslant r, \quad (3{\cdot}10a) \\ 0, & \text{otherwise.} \quad (3{\cdot}10b) \end{cases}$$

The statement of this Proposition is immediate from (3·7) and (3·8).

https://doi.org/10.1017/S0305004112000564 Published online by Cambridge University Press

4. *Homological ranks of $Y(E/F_\infty)$*

Recall that $H \overset{\text{def}}{=} Gal(F_\infty/\mathbb{Q}^{cyc}) \cong \mathbb{Z}_p^\times$, is a p-adic Lie group without p-torsion, hence $\Lambda(H)$ has finite global homological dimension.

Definition 4·1. For a finitely generated $\Lambda(H)$-module M, let

$$\cdots \longrightarrow P_{j+1} \longrightarrow P_j \longrightarrow P_{j-1} \longrightarrow \cdots \longrightarrow P_0 \longrightarrow M \longrightarrow 0 \tag{4·1}$$

be a finite projective resolution of M. We denote by

$$[M] \overset{\text{def}}{=} \sum_{i \geqslant 0} (-1)^i [P_i] \tag{4·2}$$

a well-defined element in $K_0(\Lambda(H))$, which is independent of the choice of projective resolution.

Definition 4·2. For any number field $L \subset F_\infty$ with $[L : \mathbb{Q}] < \infty$. Let h_L be the group homomorphism

$$h_L : K_0\big(\Lambda(H)\big) \longrightarrow \mathbb{Z} \tag{4·3}$$

defined by

$$[M] \mapsto \sum_{i \geqslant 0} (-1)^i rank_{\mathbb{Z}_p} H_i(H_L, M) \tag{4·4}$$

for M any finitely generated $\Lambda(H)$-module, and being extended to the Grothendieck group linearly.

Remark 4·3. Under $\mathfrak{M}_H(G)$-Conjecture, Definition 4·1 well-defines for $Y(E/F_\infty) \overset{\text{def}}{=} X(E/F_\infty)/X(E/F_\infty)(p)$ an element $[Y(E/F_\infty)] \in K_0\big(\Lambda(H)\big)$. The value $h_L([M])$ is called the homological rank of M in [**9**], and the author proves $h_K([M]) = rank_{\Lambda(H_K)} M$ for any finitely generated $\Lambda(H_K)$-module M. In particular, $\tau = h_K([Y(E/F_\infty)])$.

LEMMA 4·4. *Under Hypothesis A, assuming the validity of $\mathfrak{M}_H(G)$-Conjecture, then for $n \geqslant 0$, we have*

$$h_{L_n}([Y(E/F_\infty)]) = \sum_{i \geqslant 0} (-1)^i rank_{\mathbb{Z}_p} (H_i(H_K, Y(E/F_\infty))^{(\mathbf{1})}) + \tau \cdot \frac{p^n - 1}{p - 1}. \tag{4·5}$$

Proof. See the proof of [**1**, proposition 4·1].

5. *Fundamental diagram*

Using the notations introduced in Section 1, before assuming any hypothesis, we have the following:

Definition 5·1. Fix a subfield $L \subset F_\infty$ with $[L : \mathbb{Q}] < \infty$. By fundamental diagram for

https://doi.org/10.1017/S0305004112000564 Published online by Cambridge University Press

L, we mean the following commutative diagram with exact rows:

$$\begin{tikzcd}
 & & H^2(H_L, E_{p^\infty}(F_\infty)) & \\
0 \arrow[r] & Sel_p(E/F_\infty)^{H_L} \arrow[r] & H^1(G_S(F_\infty), E_{p^\infty})^{H_L} \arrow[u] \arrow[r, "\lambda^{H_L}_{F_\infty}"] & \oplus_{u_L \in S(L^{cyc})} J_{u_L}(F_\infty)^{H_L} \\
0 \arrow[r] & Sel_p(E/L^{cyc}) \arrow[u, "r_{L^{cyc}}"'] \arrow[r] & H^1(G_S(L^{cyc}), E_{p^\infty}) \arrow[u, "res_{L^{cyc}}"'] \arrow[r, "\lambda_{L^{cyc}}"] & \oplus_{u_L \in S(L^{cyc})} J_{u_L}(L^{cyc}) \arrow[u, "\oplus_{u_L \in S(L^{cyc})} h_{u_L}"] \\
 & & H^1(H_L, E_{p^\infty}(F_\infty)). \arrow[u] &
\end{tikzcd}$$

(5·1)

The vertical upward sequence is the inflation-restriction exact sequence. Here u_L denotes a place of L^{cyc}, h_{u_L} is the corresponding restriction map from

$$J_{u_L}(L^{cyc}) \overset{\text{def}}{=} H^1\big(L^{cyc}_{u_L}, E(\overline{L^{cyc}_{u_L}})\big)_{p^\infty} \tag{5·2}$$

to

$$J_{u_L}(F_\infty) \overset{\text{def}}{=} \varinjlim_{\substack{[L':L^{cyc}]<\infty \\ L'\subset F_\infty}} \bigoplus_{w'|u_L} H^1\big(L'_{w'}, E(\overline{L'_{w'}})\big)_{p^\infty}, \tag{5·3}$$

where the limit is taken via restriction map.

From now on, we assume $\mathfrak{M}_H(G)$-Conjecture under Hypothesis A and work on the fundamental diagram.

LEMMA 5·2. *The validity of $\mathfrak{M}_H(G)$-Conjecture implies that for all subfield $L \subset F_\infty$ with $[L:\mathbb{Q}] < \infty$, the homomorphism $\lambda_{L^{cyc}}$ is surjective, and*

$$H^2(G_S(L^{cyc}), E_{p^\infty}) = 0. \tag{5·4}$$

Proof. Firstly, $\mathfrak{M}_H(G)$-Conjecture implies that $X(E/L^{cyc})$ is $\Lambda(\Gamma_L)$-torsion. Secondly, $E_{p^\infty}(L^{cyc})$ is finite due to Ribet [**12**, theorem 1·1]. This lemma follows from [**8**, theorem 7·2].

LEMMA 5·3. (Hachimori–Venjakob [**8**, lemma 3·3]).
For all subfield $L \subset F_\infty$ with $[L:\mathbb{Q}] < \infty$, we have

$$corank_{\mathbb{Z}_p} H^1(H_L, E_{p^\infty}(F_\infty)) = 0. \tag{5·5}$$

LEMMA 5·4. *The validity of $\mathfrak{M}_H(G)$-Conjecture implies that for all subfield $L \subset F_\infty$ with $[L:\mathbb{Q}] < \infty$, we have:*

$$H_1\big(H_L, X(E/F_\infty)\big) = 0; \tag{5·6}$$

$$H_i\big(H_L, Y(E/F_\infty)\big) = 0, \qquad for \;\; i \geqslant 1; \tag{5·7}$$

$$rank_{\mathbb{Z}_p} H_0\big(H_L, Y(E/F_\infty)\big) = \lambda_{\Lambda(\Gamma_L)} H_0\big(H_L, X(E/F_\infty)\big). \tag{5·8}$$

Proof. From the first row of the fundamental diagram (5·1), we obtain an exact sequence

$$0 \longrightarrow Sel_p(E/F_\infty)^{H_L} \longrightarrow H^1(G_S(F_\infty), E_{p^\infty})^{H_L} \longrightarrow (Im\lambda_{F_\infty})^{H_L} \\ \longrightarrow H^1(H_L, Sel_p(E/F_\infty)) \longrightarrow H^1(H_L, H^1(G_S(F_\infty), E_{p^\infty})). \quad (5\cdot9)$$

Hence, (5·6) holds if

$$H^1(H_L, H^1(G_S(F_\infty), E_{p^\infty})) = 0, \quad (5\cdot10)$$

and $H^1(G_S(F_\infty), E_{p^\infty})^{H_L} \longrightarrow (Im\lambda_{F_\infty})^{H_L}$ is surjective. Since H_L has p-cohomological dimension 1, we have

$$H^3(H_L, E_{p^\infty}(F_\infty)) = 0 \quad (5\cdot11)$$

and

$$coker\left(\bigoplus_{u_L\in S(L^{cyc})} h_{u_L}\right) = 0. \quad (5\cdot12)$$

By Lemma 5·2, we deduce (5·10) by the exactness of the Hochschild–Serre spectral sequence

$$H^2(G_S(L^{cyc}), E_{p^\infty}) \longrightarrow H^1(H_L, H^1(G_S(F_\infty), E_{p^\infty})) \longrightarrow H^3(H_L, E_{p^\infty}(F_\infty)) \quad (5\cdot13)$$

and the surjectivity of $\lambda_{F_\infty}^{H_L}$ by the commutativity of the fundamental diagram (5·1). The latter implies that $H^1(G_S(F_\infty), E_{p^\infty})^{H_L} \longrightarrow (Im\lambda_{F_\infty})^{H_L}$ coincides with $\lambda_{F_\infty}^{H_L}$, which is a surjection, hence proved (5·6).

Trivially, $H_i(H_L, Y(E/F_\infty)) = 0$ for $i \geqslant 2$. To observe the case when $i = 1$, take the H_L-homology of the canonical short exact sequence of $\Lambda(H_L)$-modules

$$0 \longrightarrow X(E/F_\infty)(p) \longrightarrow X(E/F_\infty) \longrightarrow Y(E/F_\infty) \longrightarrow 0. \quad (5\cdot14)$$

It yields an exact sequence of $\Lambda(\Gamma_L)$-modules

$$0 = H_1(H_L, X(E/F_\infty)) \longrightarrow H_1(H_L, Y(E/F_\infty)) \longrightarrow H_0(H_L, X(E/F_\infty)(p)) \\ \longrightarrow H_0(H_L, X(E/F_\infty)) \longrightarrow H_0(H_L, Y(E/F_\infty)) \longrightarrow 0. \quad (5\cdot15)$$

In fact, each term in this exact sequence is $\Lambda(\Gamma_L)$-torsion. Indeed, the validity of $\mathfrak{M}_H(G)$-Conjecture implies that $Sel_p(E/L^{cyc})$ is a finitely generated $\Lambda(\Gamma_L)$-cotorsion module, which implies that $H_0(H_L, X(E/F_\infty))$ is $\Lambda(\Gamma_L)$-torsion, hence so is $H_0(H_L, Y(E/F_\infty))$. On the other hand, $X(E/F_\infty)(p)$ is annihilated by some power of p, and hence the homological group $H_i(H_L, X(E/F_\infty)(p))$ will be annihilated by this power of p, for each $i \geqslant 0$. In particular, they are $\Lambda(\Gamma_L)$-torsion, with trivial $\lambda_{\Lambda(\Gamma_L)}$-invariants and so is the submodule $H_1(H_L, Y(E/F_\infty))$. Moreover, since multiplying by p, (and hence by any power of p) is injective in $Y(E/F_\infty)$, the induced multiplying by p in $H_1(H_L, Y(E/F_\infty))$ is again injective, (so is the multiplying by a power of p map). Hence, $H_1(H_L, Y(E/F_\infty)) = 0$ since it injects into a module which is annihilated by some power of p, hence proved (5·7).

Since the $\lambda_{\Lambda(\Gamma_L)}$-invariant is additive in exact sequences and it coincides the $\mathbb{Z}_p$-rank upon finitely generated $\mathbb{Z}_p$-modules, (5·8) follows from taking $\lambda_{\Lambda(\Gamma_L)}$-invariant along the long exact sequence (5·15) above.

LEMMA 5·5. *For $u_L \notin S_{ram}(L^{cyc}) \cup S_p(L^{cyc})$, we have*

$$ker(h_{u_L}) = 0. \quad (5\cdot16)$$

https://doi.org/10.1017/S0305004112000564 Published online by Cambridge University Press

For $u_L \in S_p(L^{cyc})$, we have

$$corank_{\mathbb{Z}_p} ker(u_L) = \delta_p. \tag{5·17}$$

Proof. The first statement is trivial as the kernel of h_{u_L} is a cohomology group of the relevant decomposition subgroup of u_L over F_∞, but this decomposition subgroup is trivial since u_L is unramified over F_∞. The second statement is a consequence of [**3**, proposition 4·3] and Greenberg [**6**, section 3].

LEMMA 5·6. *Under Hypothesis A, assuming the validity of $\mathfrak{M}_H(G)$-Conjecture, then for any number field $L \subset F_\infty$ with $[L : \mathbb{Q}] < \infty$, we have*

$$h_L([Y(E/F_\infty)]) = \lambda_L + \sum_{u_L} corank_{\mathbb{Z}_p}\big(ker(h_{u_L})\big) + \delta_p \cdot \#S_p(L^{cyc}) \tag{5·18}$$

where the u_L runs over all places of $S_{ram}(L^{cyc}) - S_p(L^{cyc})$ in the sum.

Proof. By Lemma 5·4, $h_L([Y(E/F_\infty)]) = \lambda_{\Lambda(\Gamma_L)} H_0\big(H_L, X(E/F_\infty)\big)$. By Lemma 5·2 and Snake Lemma, Lemma 5·3 implies that

$$corank_{\mathbb{Z}_p} ker(r_{L^{cyc}}) = 0, \tag{5·19}$$

$$corank_{\mathbb{Z}_p} coker(r_{L^{cyc}}) = corank_{\mathbb{Z}_p} ker\left(\bigoplus_{u_L \in S(L^{cyc})} h_{u_L}\right). \tag{5·20}$$

Therefore, (5·18) follows plainly from Lemma 5·5.

Specifying Lemma 5·6 with $L = K$, $L = L_n$, and $L = F_n$, we have the following three propositions.

PROPOSITION 5·7. *Under Hypothesis A, assuming the validity of $\mathfrak{M}_H(G)$-Conjecture, then we have*

$$\tau = \lambda_K + \sum_{u_K} corank_{\mathbb{Z}_p}(ker(h_{u_K})) + \delta_p \tag{5·21}$$

where u_K runs over all places of $S_{ram}(K^{cyc}) - S_p(K^{cyc})$ in the sum.

LEMMA 5·8. *Assuming Hypothesis* A, *we have*:

$$corank_{\mathbb{Z}_p}(ker(h_{u_K})) = \begin{cases} 0, & when\ u_K \notin S_{ram}(K^{cyc}) \bigcup S_p(K^{cyc}); \\ 0, & when\ u_K \in S_{ram}(K^{cyc}) \bigcap S_{good}(K^{cyc}) - S_p(K^{cyc}) \\ & with\ E(K^{cyc}_{u_K})_{p^\infty} = 0; \\ 2, & when\ u_K \in S_{ram}(K^{cyc}) \bigcap S_{good}(K^{cyc}) - S_p(K^{cyc}) \\ & with\ E(K^{cyc}_{u_K})_{p^\infty} \neq 0; \\ 0, & when\ u_K \in S_{ram}(K^{cyc}) \bigcap S_{ns}(K^{cyc}) - S_p(K^{cyc}); \\ 1, & when\ u_K \in S_{ram}(K^{cyc}) \bigcap S_s(K^{cyc}) - S_p(K^{cyc}); \\ \delta_p, & when\ u_K \in S_p(K^{cyc}). \end{cases}$$

Proof. The first and last line are repeated statements from Lemma 5·5. The proof of the rest of the statements can be found in the proof of [**8**, lemma 3·4], in the case when $p \geqslant 5$. The same proof carries over to our case under Hypothesis A without failure as even when

https://doi.org/10.1017/S0305004112000564 Published online by Cambridge University Press

$p = 3$, the only primes that can possibly ramify in F_∞/K^{cyc} are those lying above S_{ram} and S_p, which are all of semistable reduction type for E. Therefore, the reduction types of these primes do not change from over K to over F_∞.

PROPOSITION 5·9. *Under Hypothesis A, assuming the validity of $\mathfrak{M}_H(G)$-Conjecture, then for $n \geqslant 0$, we have*

$$h_{L_n}([Y_p(E/F_\infty)]) = \lambda_n + \sum_{u_n} rank_{\mathbb{Z}_p}\big(T_p(E)^{J_{u_n}}\big) + \delta_p \cdot \#S_p(L_n^{cyc}) \tag{5·22}$$

where u_n runs over all places of $S_{ram}(L_n^{cyc}) - S_p(L_n^{cyc})$ in the sum, J_{u_n} denotes the absolute Galois group of L^{cyc}_{n,u_n}. Moreover, for each $u_n \in S_{ram}(L_n^{cyc}) - S_p(L_n^{cyc})$, the value

$$rank_{\mathbb{Z}_p}\big(T_p(E)^{J_{u_n}}\big)$$

is dependent only on the rational prime q_i lying below u_n, and independent on n.

PROPOSITION 5·10. *Under Hypothesis A, assuming the validity of $\mathfrak{M}_H(G)$-Conjecture, then for $n \geqslant 1$, we have*

$$\tau \cdot p^n = \lambda_{F_n} + \sum_{u_{F_n}} corank_{\mathbb{Z}_p}\big(ker(h_{u_{F_n}})\big) + \delta_p \cdot \#S_p(F_n^{cyc}) \tag{5·23}$$

where u_{F_n} runs over all places of $S_{ram}(F_n^{cyc}) - S_p(F_n^{cyc})$ in the sum.

Proof. The only extra statement here is $h_{F_n}([Y_p(E/F_\infty)]) = h_K([Y_p(E/F_\infty)]) \cdot p^n$, which is due to the fact that $[\Lambda(H_K) : \Lambda(H_{F_n})] = p^n$.

LEMMA 5·11. *Assuming Hypothesis A. For each $n \geqslant 1$, we have:*

$$corank_{\mathbb{Z}_p}(ker(h_{u_{F_n}})) = \begin{cases} 0, & when\ u_{F_n} \notin S_{ram}(F_n{}^{cyc}) \cup S_p(F_n{}^{cyc}); \\ 0, & when\ u_{F_n} \in S_{ram}(F_n{}^{cyc}) \cap S_{good}(F_n{}^{cyc}) - S_p(F_n{}^{cyc}) \\ & with\ E(F^{cyc}_{n\,u_{F_n}})_{p^\infty} = 0; \\ 2, & when\ u_{F_n} \in S_{ram}(F_n{}^{cyc}) \cap S_{good}(F_n{}^{cyc}) - S_p(F_n{}^{cyc}) \\ & with\ E(F^{cyc}_{n\,u_{F_n}})_{p^\infty} \neq 0; \\ 0, & when\ u_{F_n} \in S_{ram}(F_n{}^{cyc}) \cap S_{ns}(F_n{}^{cyc}) - S_p(F_n{}^{cyc}); \\ 1, & when\ u_{F_n} \in S_{ram}(F_n{}^{cyc}) \cap S_s(F_n{}^{cyc}) - S_p(F_n{}^{cyc}); \\ \delta_p, & when\ u_{F_n} \in S_p(F_n{}^{cyc}). \end{cases}$$

Proof. This is essentially the same proof as in Lemma 5·8, since $K \subset F_n$.

PROPOSITION 5·12. *Under Hypothesis A, assuming $\mathfrak{M}_H(G)$-Conjecture is valid:*

(i) *when E has non-split multiplicative reduction at p, we have*

$$\lambda_n - \lambda_{n-1} = \tau p^{n-1}, \qquad for\ all\ n \geqslant 1; \tag{5·24}$$

(ii) *when E has split multiplicative reduction at p,*

(a) *if (p, m) is amenable, we have*

$$\lambda_n - \lambda_{n-1} = \tau p^{n-1}, \qquad for\ all\ n \geqslant 1, \tag{5·25}$$

(b) *if (p, m) is non-amenable, we have:*

$$\lambda_n - \lambda_{n-1} = \begin{cases} \tau p^{n-1}, & r < n; \qquad (5·26a) \\ (\tau - 1)p^{n-1}, & 1 \leqslant n \leqslant r. \qquad (5·26b) \end{cases}$$

https://doi.org/10.1017/S0305004112000564 Published online by Cambridge University Press

Proof. For $n \geqslant 1$, from Proposition 5·9, we have

$$h_{L_n}([Y_p(E/F_\infty)]) - h_{L_{n-1}}([Y_p(E/F_\infty)]) = \lambda_n - \lambda_{n-1} + \delta_p \cdot (\#S_p\big(L_n^{cyc}\big) - \#S_p(L_{n-1}^{cyc})), \quad (5·27)$$

from Lemma 4·4, we get

$$h_{L_n}([Y_p(E/F_\infty)]) - h_{L_{n-1}}([Y_p(E/F_\infty)]) = \tau \cdot \frac{p^n - p^{n-1}}{p-1} = \tau \cdot p^{n-1}. \qquad (5·28)$$

Therefore,

$$\lambda_n - \lambda_{n-1} = \tau \cdot p^{n-1} - \delta_p \cdot \big(\#S_p\big(L_n^{cyc}\big) - \#S_p(L_{n-1}^{cyc})\big). \qquad (5·29)$$

From Proposition 2·9, we conclude that:

$$\#S_p(L_n^{cyc}) - \#S_p(L_{n-1}^{cyc}) = \begin{cases} p^{n-1}, & \text{non-amenable } (p, m),\ 1 \leqslant n \leqslant r; \\ 0, & \text{otherwise,} \end{cases} \qquad (5·30)$$

and thus the Proposition follows.

6. *Proof of the Theorems*

We still need several lemmas before we can prove Theorem 1·8 and Theorem 1·11.

LEMMA 6·1 (T,V. Dokchitser [**4**, theorem 1·2]).
Let E be an elliptic curve defined over $\mathbb{Q}$, and p be any odd prime. For F any finite abelian extension of $\mathbb{Q}$, we have

$$w(E/F) = (-1)^{s_{E/F}}. \qquad (6·1)$$

LEMMA 6·2 (Greenberg–Guo [**6**, proposition 3·10], [**7**, section 5]).
Let E be an elliptic curve defined over a number field F, and fix an odd prime p. If $X(E/F^{cyc})$ is $\Lambda(\Gamma_F)$-torsion, then we have

$$s_{E/F} \overset{mod\ 2}{\equiv} \lambda_F. \qquad (6·2)$$

Remark 6·3. Under Hypothesis A, for any subfield F of F_∞ with $[F : \mathbb{Q}]$ finite, the validity of $\mathfrak{M}_H(G)$-Conjecture implies that $X(E/F^{cyc})$ is $\Lambda(\Gamma_F)$-torsion, hence the hypothesis in Greenberg-Guo is satisfied for these subfields F.

LEMMA 6·4. *Assume the notations declared in Section* 1. *For $n \geqslant 1$, we have*

$$s_{E/L_n} = s_{E/L_{n-1}} + s_{E,\rho_{\chi_n}}. \qquad (6·3)$$

Proof. By definition, ρ_{χ_n} factors through $Gal(F_n/\mathbb{Q})$ and up to isomorphism, it is the only irreducible representation of $Gal(F_n/\mathbb{Q})$ which does not factor through the Galois group $Gal(K_nL_{n-1}/\mathbb{Q})$. So we have

$$X(E/F_n) \otimes_{\mathbb{Z}_p} \bar{\mathbb{Q}}_p = X(E/K_nL_{n-1}) \otimes_{\mathbb{Z}_p} \bar{\mathbb{Q}}_p \oplus (\rho_{\chi_n})^{s_{E,\rho_{\chi_n}}}. \qquad (6·4)$$

The statement is immediate from this by counting the dimensions of the $Gal(F_n/L_n)$-invariants and the fact that $(\rho_{\chi_n})^{Gal(F_n/L_n)}$ is one dimensional.

https://doi.org/10.1017/S0305004112000564 Published online by Cambridge University Press

Proof of Theorem 1·8. For any $n \geqslant 1$, we have

$$\begin{aligned} s_{E,\rho_{\chi_n}} &= s_{E/L_n} - s_{E/L_{n-1}} && \text{by Lemma 6·4} \\ &\overset{mod2}{\equiv} \lambda_n - \lambda_{n-1} && \text{by Lemma 6·2} \\ &\overset{mod2}{\equiv} \tau - \delta_p \cdot (\#S_p(L_n^{cyc}) - \#S_p(L_{n-1}^{cyc})) && \text{by (5·29).} \end{aligned}$$

On the other hand, we compute the parity of τ via (5·21), we have

$$\lambda_K \overset{mod2}{\equiv} s_{E/K} \tag{6·5}$$

by Lemma 6·2, and

$$\sum_{u_K \in S_{ram}(K_\infty) - S_p(K_\infty)} corank_{\mathbb{Z}_p}\big(ker(h_{u_K})\big) \overset{mod2}{\equiv} \#\big(S_{ram}(K_\infty) \cap S_s(K_\infty) - S_p(K_\infty)\big)$$

by Lemma 5·8. Conclusively, we have

$$\begin{aligned} (-1)^{s_{E,\rho_{\chi_n}}} &= (-1)^{s_{E/K}} (-1)^{\#\left(S_{ram}(K_\infty) \cap S_s(K_\infty) - S_p(K_\infty)\right)} (-1)^{\delta_p \cdot (\#S_p(L_n^{cyc}) - \#S_p(L_{n-1}^{cyc}) - 1)} \\ &= w(E/K) \cdot \prod_{q_i \ddagger p \in S_{multi}} \left(\frac{q_i}{p}\right) \cdot s_p^{(\#S_p(L_n^{cyc}) - \#S_p(L_{n-1}^{cyc}) - 1)} \\ &= w(E, \rho_{\chi_n}) \cdot s_p^{\beta_n} \cdot s_p^{(\#S_p(L_n^{cyc}) - \#S_p(L_{n-1}^{cyc}) - 1)} && \text{by (3·7)} \\ &= w(E, \rho_{\chi_n}), \end{aligned}$$

because

$$\beta_n + \#S_p\big(L_n^{cyc}\big) - \#S_p(L_{n-1}^{cyc})) \overset{mod2}{\equiv} 1 \tag{6·6}$$

by (5·30) and (3·8).

COROLLARY 6·5. *Under Hypothesis A, assuming $\mathfrak{M}_H(G)$-Conjecture is valid*:

(i) *when E has non-split multiplicative reduction at p, we have*

$$s_{E,\rho_{\chi_n}} \overset{mod2}{\equiv} \tau, \qquad \textit{for all } n \geqslant 1; \tag{6·7}$$

(ii) *when E has split multiplicative reduction at p*;

(a) *if (p, m) is amenable, we have*

$$s_{E,\rho_{\chi_n}} \overset{mod2}{\equiv} \tau, \qquad \textit{for all } n \geqslant 1; \tag{6·8}$$

(b) *if (p, m) is non-amenable, we have*

$$s_{E,\rho_{\chi_n}} \overset{mod2}{\equiv} \begin{cases} \tau, & r < n, \qquad\qquad (6·9a) \\ (\tau - 1), & 1 \leqslant n \leqslant r. \qquad (6·9b) \end{cases}$$

Proof. This is immediate from Lemma 6·1, 6·2, 6·4 and Proposition 5·12, since p is odd.

Proof of Theorem 1·11. When τ is odd, in the case when E has non-split multiplicative reduction at p, by Proposition 5·12 and Lemma 6·2,

$$s_{E/L_n} - s_{E/L_{n-1}} \overset{mod2}{\equiv} 1 \tag{6·10}$$

holds for all $n \geqslant 1$, since p is an odd prime. Thus,

$$s_{E/\mathbb{Q}} < s_{E/L_1} < s_{E/L_2} < \cdots \tag{6·11}$$

https://doi.org/10.1017/S0305004112000564 Published online by Cambridge University Press

which implies the inequality (1·5). When E has split multiplicative reduction at p, the same argument leads to inequality (1·7) in the case when (p, m) is amenable; while in the non-amenable case, (6·10) holds for $n > r$ due to Proposition 5·12, hence we have strict growth from the r-th level

$$s_{E/L_r} < s_{E/L_{r+1}} < s_{E/L_{r+2}} \cdots \tag{6·12}$$

which implies the inequality (1·9).

When E has non-split multiplicative reduction at p, from (6·11) and (6·3) of Lemma 6·4, we conclude that

$$s_{E,\rho_{\chi n}} \geqslant 1 \tag{6·13}$$

holds for all $n \geqslant 1$. Therefore, we deduce from (6·4) of Lemma 6·4 that

$$\begin{aligned} s_{E/F_n} &= s_{E/K_nL_{n-1}} + p^{n-1}(p-1) \cdot s_{E,\rho_{\chi n}} \\ &\geqslant s_{E/K_nL_{n-1}} + p^{n-1}(p-1) \\ &\geqslant s_{E/F_{n-1}} + p^{n-1}(p-1) \end{aligned} \tag{6·14}$$

for all $n \geqslant 1$. Applying the inequality (6·14) recursively for all $n \geqslant 1$, we obtain

$$\begin{aligned} s_{E/F_n} &\geqslant p^{n-1}(p-1) + p^{n-2}(p-1) + \cdots + p^1(p-1) + s_{E/F_1} \\ &\geqslant p^n - 1 + s_{E/K}, \end{aligned} \tag{6·15}$$

and hence have proved inequality (1·6). When E has split multiplicative reduction at p, the same argument leads to the same inequality (1·8) in the case when (p, m) is amenable; while in the non-amenable case, inequalities (6·13) and (6·14) hold for $n > r$. Let $n = r + k$ and applying inequality (6·14) recursively for all $k \geqslant 1$, we obtain

$$\begin{aligned} s_{E/F_{r+k}} &\geqslant p^r[p^{k-1}(p-1) + p^{k-2}(p-1) + \cdots + p^1(p-1)] + s_{E/F_{r+1}} \\ &\geqslant p^r(p^k - 1) + s_{E/K_{r+1}L_r}, \end{aligned} \tag{6·16}$$

and hence have proved inequality (1·10).

We now show that these lower bounds are upper bounds too when $\tau = 1$. From (5·23) of Proposition 5·10, we have

$$s_{E/F_n} \leqslant \lambda_{F_n} = p^n \cdot \tau - \left(\sum_{u_{Fn}} corank_{\mathbb{Z}_p}(ker(h_{u_{F_n}})) + \delta_p \cdot \#S_p\left(F_n^{cyc}\right) \right) \tag{6·17}$$

where u_{F_n} runs over all places of $S_{ram}(F_n^{cyc}) - S_p(F_n^{cyc})$ in the sum. It is obvious from $K \subset F_1 \subset F_2 \subset \cdots$, Lemma 5·8 and Lemma 5·11 that

$$\sum_{u_K} corank_{\mathbb{Z}_p}\left(ker(h_{u_K})\right) \leqslant \sum_{u_{F_1}} corank_{\mathbb{Z}_p}\left(ker(h_{u_{F_1}})\right) \leqslant \sum_{u_{F_2}} corank_{\mathbb{Z}_p}\left(ker(h_{u_{F_2}})\right) \leqslant \cdots \tag{6·18}$$

hence, when E has non-split multiplicative reduction at p, $\delta_p = 0$, the right-hand side of (6·17) is further upper-bounded by

$$p^n - \sum_{u_K} corank_{\mathbb{Z}_p}\left(ker(h_{u_K})\right) = p^n - 1 + \lambda_K = p^n - 1 + s_{E/K} \tag{6·19}$$

where the first equality is due to Proposition 5·7; the second equality $\lambda_K = s_{E/K}$ is due to the fact that $\tau = 1$ implies $\lambda_K = 0$ or 1, and by Lemma 6·2, $\lambda_K \overset{mod2}{\equiv} s_{E/K}$. When E has split multiplicative reduction at p, $\delta_p = 1$. In the case when (p, m) is amenable, by Proposition 2·7, we have

$$\#S_p\big(F_n^{cyc}\big) = 1 = \#S_p(K^{cyc}) \tag{6·20}$$

for all $n \geqslant 1$. Hence the right-hand side of (6·17) is further upper-bounded by

$$p^n - \sum_{u_K} corank_{\mathbb{Z}_p}\big(ker(h_{u_K})\big) - \delta_p = p^n - 1 + \lambda_K = p^n - 1 + s_{E/K} \tag{6·21}$$

by the same reasons. In fact, in this case, we can deduce further from Proposition 5·7 that

$$\sum_{u_K} corank_{\mathbb{Z}_p}\big(ker(h_{u_K})\big) = \lambda_K = s_{E/K} = 0. \tag{6·22}$$

In the case when (p, m) is non-amenable, by Proposition 2·7, we have

$$\#S_p\big(F_{r+k}^{cyc}\big) = \#S_p\big(F_r^{cyc}\big) = p^r \tag{6·23}$$

for all $k \geqslant 1$. Let $n = r + k$, the right-hand side of (6·17) is further upper-bounded by

$$\begin{aligned} p^{r+k} - \sum_{u_{F_r}} corank_{\mathbb{Z}_p}\big(ker(h_{u_{F_r}})\big) - \delta_p \cdot \#S_p\big(F_r^{cyc}\big) &= p^{r+k} - p^r \cdot \tau + \lambda_{F_r} \\ &= p^r(p^k - 1) \end{aligned}$$

The first equation is due to Proposition 5·10 when $n = r$. In fact, in this case, we can deduce from the same proposition that

$$\sum_{u_{F_r}} corank_{\mathbb{Z}_p}\big(ker(h_{u_{F_r}})\big) = \lambda_{F_r} = 0. \tag{6·24}$$

So in particular $s_{E/K_{r+1}L_r} = 0$, and hence proved the statement.

Lastly, since the equalities of (1·6), (1·8) and (1·10) hold, all the equalities in (6·14), (6·15) and (6·16) must hold in the respective cases, and in particular:

(i) when E has non-split multiplicative reduction at p, we have

$$s_{E,\rho_{\chi n}} = 1, \qquad \text{for all } n \geqslant 1; \tag{6·25}$$

(ii) when E has split multiplicative reduction at p:

(a) if (p, m) is amenable, we have

$$s_{E,\rho_{\chi n}} = 1, \qquad \text{for all } n \geqslant 1; \tag{6·26}$$

(b) if (p, m) is non-amenable, we have

$$s_{E,\rho_{\chi n}} = 1, \qquad \text{for all } n > r. \tag{6·27}$$

Hence, the equalities of (1·5), (1·7) and (1·9) hold, by Lemma 6·4.

7. *Numerical examples*

By Theorem 1·11 in the case of $\tau = 1$, assuming the finiteness of the Shafarevich group over number field $\mathbb{Q}(\theta)$, where $\theta \overset{\text{def}}{=} \sqrt[p]{m}$, we should obtain an extra Mordell–Weil rank over $\mathbb{Q}(\theta)$ than over $\mathbb{Q}$. Table 1 below provides several examples of triples (E, p, m) satisfying Hypothesis A with $rank_{\mathbb{Z}}E(\mathbb{Q}) = 0$. Computations by Magma predicts (this computation involves the formula given in [**10**, theorem 1] and conjectural order of the Shafarevich group of E over K via BSD Conjecture by computing the Hasse-Weil L-function over K at 1)

https://doi.org/10.1017/S0305004112000564 Published online by Cambridge University Press

Table 1. *Examples (E, p, m) with $\tau = 1$, $rank_{\mathbb{Z}} E(\mathbb{Q}) = 0$ and $rank_{\mathbb{Z}}(E(\mathbb{Q}(\theta))) = 1$, with p is a non-split multiplicative prime for E, or (p, m) is amenable (abbreviated by AM) when p is a split multiplicative prime for E.*

(E, p, m)	δ_p	Weierstrass equation of E	$E(\mathbb{Q})$	$E(\mathbb{Q}(\theta))$	$P = (x, y) \in E(\mathbb{Q}(\theta))$	H(P)
$(15a1, 3, 5)$	0	$y^2+xy+y = x^3+x^2-10x-10$	$C_2 \oplus C_4$	$C_2 \oplus C_4 \oplus \mathbb{Z}$	$\left(-\frac{30}{121}\theta^2 - \frac{200}{121}\theta + \frac{38}{121}, -\frac{1325}{1331}\theta^2 + \frac{4275}{1331}\theta - \frac{1387}{1331}\right)$	1.5723
$(33a1, 3, 11)$	0	$y^2 + xy = x^3 + x^2 - 11x$	$C_2 \oplus C_2$	$C_2 \oplus C_2 \oplus \mathbb{Z}$	$\left(-\frac{27}{25}\theta^2 + \frac{108}{25}\theta + \frac{143}{25}, -\frac{216}{125}\theta^2 + \frac{2214}{125}\theta - \frac{506}{125}\right)$	1.3937
$(42a1, 3, 2)$	0	$y^2+xy+y = x^3+x^2-4x+5$	C_8	$C_8 \oplus \mathbb{Z}$	$(-\theta^2 - 1, \theta^2 + 2\theta - 1)$	0.8162
$(150c1, 3, 2)$	0	$y^2+xy+y = x^3+x^2+37x+281$	C_4	$C_4 \oplus \mathbb{Z}$	$(2\theta^2-4\theta-1, 6\theta^2+8\theta-6)$	1.0902
$(21a1, 3, 3)$	1, AM	$y^2 + xy = x^3 - 4x - 1$	$C_2 \oplus C_4$	$C_2 \oplus C_4 \oplus \mathbb{Z}$	$\left(-\frac{3}{4}\theta^2 - \frac{1}{4}, -\frac{3}{8}\theta^2 + \frac{9}{8}\theta - 1\right)$	0.8934
$(21a1, 3, 7)$	1, AM	$y^2 + xy = x^3 - 4x - 1$	$C_2 \oplus C_4$	$C_2 \oplus C_4 \oplus \mathbb{Z}$	$\left(-\theta^2 + \frac{3}{4}\theta + \frac{3}{4}, -\frac{7}{8}\theta^2 + \frac{29}{8}\theta - \frac{3}{2}\right)$	2.0767
$(30a1, 3, 3)$	1, AM	$y^2+xy+y = x^3+x+2$	C_6	$C_6 \oplus \mathbb{Z}$	$(2\theta^2 - 3, -6\theta + 10)$	0.4708
$(57b1, 3, 3)$	1, AM	$y^2+xy+y = x^3-7x+5$	$C_2 \oplus C_2$	$C_2 \oplus C_2 \oplus \mathbb{Z}$	$(-\theta^2 - \theta + 1, \theta + 2)$	0.9280
$(30a1, 5, 3)$	0	$y^2+xy+y = x^3+x+2$	C_6	$C_6 \oplus \mathbb{Z}$	$(2\theta^4-2\theta^3+2\theta^2-3, 4\theta^4-6\theta^2+12\theta-14)$	0.5750
$(70a1, 5, 2)$	0	$y^2+xy+y = x^3-x^2+2x-3$	C_4	$C_4 \oplus \mathbb{Z}$	$(4\theta^4 - 2\theta^3 + \theta^2 + 2\theta - 5, -3\theta^4 - 6\theta^3 + 17\theta^2 - 20\theta + 17)$	1.5505

the finiteness of $X(E/K^{cyc})$ and hence $\tau = 1$ by (5·21) in all these examples. We conclude the structure of $E(\mathbb{Q}(\theta))$, by finding a rational point of infinite order $P \in E(\mathbb{Q}(\theta))$ (computations by Pari/gp), with $H(P)$ denotes the height of the point P. We indeed see $rank_{\mathbb{Z}}(E(\mathbb{Q}(\theta))) = 1$ as predicted in these examples.

Example 1. Here is an example of an elliptic curve with split multiplicative reduction at p with non-amenable pair (p, m), and with $\tau = 1$. Let E be the elliptic curve with Cremona symbol 57b1, which has Weierstrass equation given by

$$y^2 + xy + y = x^3 - 7x + 5. \qquad (7{\cdot}1)$$

We see in Table 1 that E has split multiplicative reduction at $p = 3$, furthermore it has non-split multiplicative reduction at prime 19. Let $m = 19$, then the pair (3, 19) is non-amenable with $r = 1$. Since 19 splits in $\mathbb{Q}(\mu_3)$, E has non-split multiplicative reduction at the primes of $\mathbb{Q}(\mu_3)$ above 19. From the table above, we have seen that $X(E/K^{cyc})$ is finite. Hence, we conclude from (5·21) again that $\tau = \delta_3 = 1$. According to the statement of Theorem 1·11, one cannot ensure any growth of the $\mathbb{Z}_3$-Selmer rank from over $\mathbb{Q}$ to over $\mathbb{Q}(\sqrt[3]{19})$, but can ensure the growth of this rank from over $\mathbb{Q}(\sqrt[3]{19})$ to $\mathbb{Q}(\sqrt[9]{19})$ to be exactly 1. The *RankBound* command in Magma gives

$$rank_{\mathbb{Z}} E(\mathbb{Q}(\sqrt[3]{19})) \leqslant 0 \tag{7·2}$$

$$rank_{\mathbb{Z}} E(\mathbb{Q}(\sqrt[3^2]{19})) \leqslant 3. \tag{7·3}$$

Assuming the finiteness of the 3-primary part of the Shafarevich group of an elliptic curve over a number field, then the Mordell–Weil rank of this elliptic curve over this number field coincides with the $\mathbb{Z}_3$-Selmer rank over this number field. These two upperbounds of the Mordell–Weil ranks given by Magma simply justify the fact that when the elliptic curve has split multiplicative reduction at p and (p, m) is non-amenable, even if $\tau = 1$, one can wait until $n > r$ to possibly gain an extra Mordell–Weil rank along the non-Galois tower $\{L_n\}$.

Example 2. Here is another example of split multiplicative reduction at p with non-amenable pair (p, m), but with even τ. Let E be the elliptic curve with Cremona symbol 210a1, which has Weierstrass equation given by

$$y^2 + xy = x^3 - 41x - 39. \tag{7·4}$$

The elliptic curve E has split multiplicative reduction at primes 2, 3, 7 and non-split multiplicative reduction at 5. Let $p = 3$ and $m = 35$. The pair (3, 35) is non-amenable with $r = 1$. Since 5 is inert and 7 splits over $\mathbb{Q}(\mu_3)$, there are three primes of $\mathbb{Q}(\mu_3)$ dividing $m = 35$, and E has split multiplicative reduction over all these primes. Computations by Magma again predicts the finiteness of $X(E/K^{cyc})$. Hence, we conclude from (5·21) again that $\tau = 0 + 3 + \delta_3 = 4$. By Magma, we obtain that

$$E(\mathbb{Q}) = E(\mathbb{Q})_{tors} = E(\mathbb{Q}(\sqrt[3]{35}))_{tors} \cong C_6. \tag{7·5}$$

Assuming the finiteness of the 3-primary part of the Shafarevich group of E over number fields, Corollary 6·5 and Lemma 6·4 suggest an odd growth of Mordell–Weil rank of E from over $\mathbb{Q}$ to over $\mathbb{Q}(\sqrt[3]{35})$. Indeed, the Magma command *RankBound* gives an upperbound

$$rank_{\mathbb{Z}} E(\mathbb{Q}(\sqrt[3]{35})) \leqslant 1. \tag{7·6}$$

On the other hand, computations by Pari/gp provides

$$P = (2\sqrt[3]{35} - 12, 4(\sqrt[3]{35})^2 - 6\sqrt[3]{35} - 15) \in E(\mathbb{Q}(\sqrt[3]{35})) \tag{7·7}$$

which is a point of infinite order of height ≈ 0.6153. Hence, we have

$$E(\mathbb{Q}(\sqrt[3]{35})) \cong C_6 \oplus \mathbb{Z}. \tag{7·8}$$

Acknowledgements. This paper is based on the author's Ph.D. thesis, at the University of Cambridge, with the same title. The author would like to thank his Ph.D. advisor Professor John Coates for his guidance and encouragement and his examiner Dr. Tim Dokchitser whose suggestions lead to the improvements in this paper from the thesis. The author is grateful to EPSRC for supporting this research.

REFERENCES

[**1**] J. COATES, T. FUKAYA, K. KATO and R. SUJATHA. Root numbers, Selmer groups and non-commutative Iwasawa theory. *J. Algebraic Geom.* **19** (2010), no. 1, 19–97.

[**2**] J. COATES, T. FUKAYA, K. KATO, R. SUJATHA and O. VENJAKOB. The GL_2 main conjecture for elliptic curves without complex multiplication. *Publ. Math. Inst. Hautes Études Sci.* (2005), no. 101, 163–208.

[**3**] J. COATES and R. GREENBERG. Kummer theory for abelian varieties over local fields. *Invent. Math.* **124** (1996), no. 1-3, 129–174.

[**4**] T. DOKCHITSER and V. DOKCHITSER. Self-duality of Selmer groups. *Math. Proc. Camb. Phils. Soc.* **146** (2009), no. 2, 257–267.

[**5**] V. DOKCHITSER. Root numbers of non-abelian twists of elliptic curves. *Proc. London Math. Soc.* **3** (2005), no. 91, 300–324.

[**6**] R. GREENBERG. *Iwasawa theory for elliptic curves*, Arithmetic theory of elliptic curves (Cetraro, 1997). *Lecture Notes in Math.* vol. 1716. (Springer, Berlin, 1999), pp. 51–144.

[**7**] L. GUO. On a generalization of Tate dualities with application to Iwasawa theory. *Compositio Math.* **85** (1993), no. 2, 125–161.

[**8**] Y. HACHIMORI and O.VENJAKOB. Completely faithful selmer groups over kummer extensions. *Doc. Math. Extra Volume: Kazuya Kato's Fiftieth Birthday* (2003), 443–478.

[**9**] S. HOWSON. Euler characteristics as invariants of Iwasawa modules. *Proc. London Math. Soc.* (3) **85** (2002), no. 3, 634–658.

[**10**] J. JONES. Iwasawa L-functions and the mysterious $\mathcal{L}$-invariant, p-adic monodromy and the Birch and Swinnerton-Dyer conjecture (Boston, MA, 1991). *Contemp. Math.* vol. 165, (Amer. Math. Soc., Providence, RI, 1994), pp. 63–70.

[**11**] S. LANG. *Algebra*, third ed., Graduate Texts in Mathematics, vol. 211 (Springer-Verlag, New York, 2002).

[**12**] K. RIBET. Torsion points of abelian varieties in cyclotomic extensions. *Lenseignement Mathematique* **27** (1981), 315–319.

[**13**] A. SCHINZEL. Abelian binomials, power residues and exponential congruences. *Acta Arith.* **32** (1977), no. 3, 245–274.

[**14**] W. Y. VÉLEZ. The factorization of p in $\mathbf{Q}(a^{1/p^k})$ and the genus field of $\mathbf{Q}(a^{1/n})$. *Tokyo J. Math.* **11** (1988), no. 1, 1–19.

[**15**] F. VIVIANI. Ramification groups and Artin conductors of radical extensions of $\mathbb{Q}$. *J. Théor. Nombres Bordeaux* **16** (2004), no. 3, 779–816.

https://doi.org/10.1017/S0305004112000564 Published online by Cambridge University Press