Root numbers and rational points on elliptic curves

R. Sujatha

August 5, 2009

This article is broadly based on the talk that was given at the symposium 'Perspectives in the Mathematical Sciences', held at Indian Statistical Institute (ISI), Bangalore, to celebrate the Platinum Jubilee of the ISI. I would like to thank the organisers, especially Professor N.S.N. Sastry, for inviting me to lecture on this occasion. The article is intended for a general audience and does not contain any new results. We have aimed at highlighting several new results that have been proved on this topic by various authors, in the last few years. The proofs have been omitted and the interested reader is referred to the research papers, which we have tried to list rather extensively.

1 Elliptic curves and the Birch and Swinnerton-Dyer conjecture

Let F be a finite extension of $\mathbb{Q}$ and let E/F be an elliptic curve. Recall that E has an affine equation

$$E : y^2 = f(x),$$

where $f(x) \in F[x]$ is a cubic polynomial with distinct roots. A famous result of Mordell asserts that the group $E(F)$ of F-rational points of E is a finitely generated abelian group. Let $g_{E/F}$ denote the rank of $E(F)$. Associated with E is the complex L-function $L(E/F, s)$ of E, which is defined by an Euler product. This function converges only for $\mathrm{Re}(s) > 3/2$, but is conjectured to have an entire continuation (see [22]), and a functional equation relating its values at s and $2 - s$.

When $F = \mathbb{Q}$, thanks to deep results of Wiles [24] and [2], this conjecture is true, but it is only for elliptic curves with complex multiplication that it so far has been proven over all number fields F. Assuming the analytic continuation of $L(E/F, s)$, the analytic rank, which we denote by $r_{E/F}$, is defined to be the order of zero of $L(E/F, s)$ at $s = 1$, the centre of its critical strip. In the 1960's, based on rather compelling numerical evidence, Birch and Swinnerton-Dyer made the astonishing conjecture that

$$g_{E/F} = r_{E/F}. \tag{1}$$

A refined version of this conjecture even gives an exact formula for the leading Taylor coefficient of the L-function at $s = 1$. For more details, see [25]. An important part

of this exact formula is the order of the Tate-Shafarevich group of E/F. For a finite extension K of F, the *Tate Shafarevich group of E over K*, denoted by $Ш(E/K)$, is defined by

$$Ш(E/K) = \ker\left(H^1(K,E) \to \prod_v H^1(K_v,E)\right). \tag{2}$$

Here, v varies over all the places of K and K_v denotes the completion of F at v, while $E := E(\bar{F})$ denotes the group of points of E over a fixed algebraic closure $\bar{F}$ of F, considered as a module over the Galois group of K. Finally, for any field K and a module M over the Galois group $G_K := \mathrm{Gal}(\bar{K}/K)$, the first cohomology group is denoted by $H^1(K,M)$. The Tate-Shafarevich group is among the most mysterious groups occurring in the study of the arithmetic of elliptic curves and part of the full Birch and Swinnerton-Dyer conjecture is that it is always finite. However, it was only in the late 1980's that explicit examples of elliptic curves with finite Tate-Shafarevich group came to light. Kolyvagin, and independently Rubin, whose work was based on ideas of Thaine, gave these first examples. We remark here that we do not yet know the finiteness of the Tate-Shafarevich group for a single elliptic curve of rank at least 2.

2 Congruent Number Problem

Recall that a natural number $N \geq 1$ is said to be *congruent* if there exists a right angled triangle whose sides have rational length, and area N. In other words N is congruent if there exists rational numbers a, b, c in $\mathbb{Q}$ such that $a^2 + b^2 = c^2$ and $ab/2 = N$. One of the oldest problems in number theory is to explicitly give an algorithm which would determine whether a given number is congruent. While Arab manuscripts dating back to the tenth century A.D. give a long list of examples of congruent numbers, it is almost certain that the ancient Indians too grappled with congruent numbers and knew of many examples. For more on this subject, the reader is referred to the book by Koblitz [13] and the article by Coates [3]. A folklore conjecture in this subject is the following, which remains open despite overwhelming numerical evidence:

Conjecture 2.1. *If N is a positive integer congruent to 5, 6,or 7 modulo 8, then N is congruent.*

The connection between congruent numbers and elliptic curves is the following. For any integer $N \geq 1$, consider the elliptic curve E over $\mathbb{Q}$ defined by

$$E_N : y^2 = x^3 - N^2 x.$$

Then N is congruent if and only if E has a rational point (x,y), x, $y \in \mathbb{Q}$ with $y \neq 0$. Indeed, if (a,b,c) are the lengths of the corresponding right angled triangle, with area N and $a^2 + b^2 = c^2$, then (x,y) with

$$x = \frac{N(a+c)}{b},\ y = \frac{2N^2(a+c)}{b^2}$$

is a point on E_N with $y \neq 0$. Such a point is well-known to give a point of infinite order on E_N and the theory of L-functions shows that for $N \equiv 5, 6, 7 \mod 8$, $L(E_N, s)$ has a zero of odd order (and therefore a zero) at $s = 1$. Thus, Conjecture 2.1 is seen to be a special case of the Birch and Swinnerton-Dyer conjecture.

Iwasawa theory is a p-adic theory that provides a systematic method to attack the Birch and Swinnerton-Dyer conjecture and has led to important results in the study of the arithmetic of elliptic curves. The main object of study here is the investigation of the Galois action on the dual Selmer group, viewed over certain infinite extensions of F. We refer the reader to [21], [9] ,[3] for detailed accounts of the Iwasawa theory of elliptic curves. Hereafter, we fix an odd prime p. Recall that for an elliptic curve E/F and a finite extension K of F, the *p-Selmer group*, denoted $S_p(E/K)$, is defined as

$$S_p(E/K) \;=\; \mathrm{Ker}\left(H^1(K, E_{p^\infty}) \longrightarrow \bigoplus_v H^1(K_v, E)\right)$$

where $E_{p^\infty} := \bigcup_n E_{p^n}(\bar{F})$ denotes the group of all p-power division points of $E(\bar{F})$ considered as a module over G_K. It is well-known that $S_p(E/K)$ is a cofinitely generated $\mathbb{Z}_p$-module and we define

$$s_{p,E/K} := \mathbb{Z}_p - \text{corank of } S_p(E/K). \tag{3}$$

For an infinite Galois extension K_∞ of F with Galois group $G := \mathrm{Gal}(K_\infty/F)$ a p-adic Lie group, the Selmer group $S_p(E/K_\infty)$ is defined as the direct limit over the Selmer groups $S_p(E/L)$, as L varies over finite Galois extensions of F contained in K_∞. It is clear that $S_p(E/K_\infty)$ is a discrete G-module, and its Pontryagin dual denoted $X_p(E/K_\infty)$ is a compact G-module, and is the *dual Selmer group*. It is even a finitely generated, compact module over the Iwasawa algebra $\Lambda(G)$ defined as the inverse limit

$$\Lambda(G) \;:=\; \lim_{\leftarrow} \mathbb{Z}_p[G/G'],$$

the limit being taken over the group rings $\mathbb{Z}_p[G/G']$ as G' varies over open normal subgroups, with respect to the natural maps. The key idea in Iwasawa theory is to study the arithmetic of E over suitable infinite extensions via the dual Selmer groups considered as $\Lambda(G)$-modules. For a finite extension K of F, Kummer theory yields the well-known exact sequence of discrete G_K-modules

$$0 \to E(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p \;\to S_p(E/K) \;\to\; Ш(E/K)(p) \;\to 0, \tag{4}$$

where $Ш(E/K)(p)$ denotes the p-primary torsion subgroup of $Ш(E/K)$. For an infinite p-adic Lie extension K_∞ of F, with Galois group G, a direct limit argument gives the exact sequence of G-modules

$$0 \to E(K_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p \;\to S_p(E/K_\infty) \;\to\; Ш(E/K_\infty)(p) \to 0,$$

where $Ш(E/K_\infty)(p)$ denotes the p-primary part of the Tate-Shafarevich group of E over K_∞) and is defined as the direct limit of $Ш(E/K)(p)$ as K varies over finite Galois extensions of F in K_∞. Iwasawa theory can be used to prove the following result:

Theorem 2.2. *Let N be an integer ≥ 1 such that $L(E_N/\mathbb{Q}, 1) = 0$. If the p-primary part $Ш(E_N/\mathbb{Q})(p)$ is finite for some odd prime p, then N is congruent.*

The central idea here is to prove that $X_p(E_N/\mathbb{Q})$ has $\mathbb{Z}_p$-rank at least one. Then, using the hypothesis on $Ш(E_N)$, one deduces that the same is true of $E_N(\mathbb{Q})$. We shall return to this briefly in the next section.

3 Root numbers and the Parity Conjecture

Let G_F denote the absolute Galois group as before. An *Artin representation* of G_F is a finite dimensional complex representation ρ of G_F which is trivial on an open subgroup and thus factors through a finite Galois extension of F. Unless necessary, the base field will not be specified and the associated representation space will be denoted by V_ρ. In a similar vein, as most of the results we need or state below are independent of the finite extension of the base field through which the Artin representation factors, we shall omit reference to the associated finite Galois extension, except in cases where it might be necessary to specify the extension.

Given an elliptic curve E/F and an Artin representation ρ of G_F, there is an associated twisted L-function defined by an Euler product and denoted by $L(E, \rho, s)$ (see [23] for details). Again, this twisted L-function is conjectured to be entire with a functional equation. More precisely, let

$$\tilde{L}(E, \rho, s) := \left(\frac{N(E, \rho)}{\pi^{2d_\rho}}\right)^{s/2} \Gamma\left(\frac{s}{2}\right)^{d_\rho} \Gamma\left(\frac{s+1}{2}\right)^{d_\rho} L(E, \rho, s);$$

here d_ρ is the dimension of V_ρ and $N(E, \rho)$ is the global conductor of the Galois representation associated to that of E twisted by V_ρ (cf. [6, 2.4]). The conjectured functional equation is

$$\tilde{L}(E, \rho, s) \;=\; w(E, \rho)\, \tilde{L}(E, \hat{\rho}, 2 - s), \tag{5}$$

where $\hat{\rho}$ is the contragredient of ρ and $w(E, \rho)$ is the *root number*, which is an algebraic number of complex absolute value 1. We remark that even though the functional equation (5) is largely conjectural, the root number is nonetheless *well-defined*. Indeed, by the theorem of Deligne and Langlands, it can be written as a product of local root numbers, taken over all places v of F (see [23]). In particular, if ρ is self-dual (i.e. $\rho = \hat{\rho}$), then the root number is equal to ± 1 and is often referred to as the *sign in the functional equation*.

Definition 3.1. Assuming that $L(E, \rho, s)$ is entire, the ρ-analytic rank is defined as $r(E, \rho) = \mathrm{ord}_{s=1} L(E, \rho, s)$. Note that if ρ is self-dual and irreducible, then

$$w(E, \rho) = (-1)^{r(E,\rho)}. \tag{6}$$

Now let ρ be an irreducible Artin representation and K/F a finite Galois extension through which ρ factors, with $G_{K/F} = \mathrm{Gal}(K/F)$.

Definition 3.2. The multiplicity of the irreducible representation ρ occurring in the $G_{K/F}$-module $E(K) \otimes \bar{\mathbb{Q}}_p$ is the *ρ-algebraic rank* and is denoted by $g_{E,\rho}$.

The invariant $g_{E,\rho}$ is in fact independent of the prime p.

Definition 3.3. The multiplicity of the contragredient representation $\hat{\rho}$ in $X(E/K) \otimes_{\mathbb{Z}_p} \bar{\mathbb{Q}}_p$ is denoted by $s_{p,E,\rho}$.

The refined form of Birch and Swinnerton-Dyer conjecture in this context is the conjecture that

$$g_{E,\rho} = r_{E,\rho} \text{ and } g_{E,\rho} = s_{p,E,\rho} \text{ for all } p. \tag{7}$$

Note that when ρ is the trivial representation these invariants coincide with the invariants g_E, r_E and $s_{p,E}$ defined earlier.

The *ρ-parity conjecture* is the assertion that for self-dual, irreducible Artin representations ρ, we have

$$w(E,\rho) = (-1)^{s_{p,E,\rho}}, \text{ or equivalently that } s_{p,E,\rho} \equiv r_{E,\rho} \mod 2. \tag{8}$$

We stress that it is completely unknown whether $s_{p,E,\rho}$ has the same parity as $g_{E,\rho}$, or even whether the parity of $s_{p.E,\rho}$ is independent of p. When ρ is the trivial representation, we clearly recover (1) as a special case of (7). Finally, note that if the root number is -1 for some self-dual Artin representation, then the parity conjecture implies that the dual Selmer group $X_p(E/K)$ has positive $\mathbb{Z}_p$-rank for a finite extension K of F. Further, the Birch and Swinnerton-Dyer conjecture predicts that $E(K)$ is infinite. However, to deduce that the elliptic curve has a point of infinite order over K, by (4), one needs to know the finiteness of the p-primary part of the Tate-Shafarevich group of E. We refer the reader to the beautiful paper of Rohrlich [19] which elaborates on the interplay between Artin representations, root numbers and elliptic curves.

Suppose that E/F is an elliptic curve and we are given a p-adic Lie extension K_∞ of F (with p and odd prime), with Galois group G. Let ρ be an irreducible, self-dual, Artin representation which factors through a finite quotient of G. Then there is the notion of the *twisted dual Selmer group*, which we denote by $X_p(E/K_\infty, \rho)$ (see [4, §3]). The basic idea is to study the invariants $g_{E,\rho}$, $r_{E,\rho}$ and $s_{p,E,\rho}$ for E as ρ ranges over all self-dual representations of G. We remark that the study of the dual Selmer group twisted by an Artin representation ρ of G, [4, §3], considered as a $\Lambda(G)$-module (see §3), is an important ingredient in the determination of the invariant $s_{p,E,\rho}$. We refer the reader to the papers of Greenberg, Guo [10], [11] and [4] for more details.

4 Recent results

In this section, we list some of the comparitively recent results towards the ρ-parity conjecture. Earlier affirmative results in this direction (when the representation ρ is

trivial), have been proved by many authors, notably Birch and Stephens [1], Greenberg and Guo [11], Monsky [16] and Nekovář [17]. More recently, interesting work has been done by T. and V. Dokchitser [6], [7], Greenberg [10], Kim [12] and Mazur-Rubin [14], [15] and Nekovàř [18].

In the next section, we shall illustrate some of these results with numerical examples and also consider some interesting applications. Here is a striking result due to Tim and Vladimir Dokchitser [8]:

Theorem 4.1. *Let E be any elliptic curve over $\mathbb{Q}$ and p any prime number. Then $s_{p,E/\mathbb{Q}} \equiv r_{E/\mathbb{Q}} \bmod 2$.*

A completely different perspective is adopted in [4], where the results proved give some fragmentary evidence that a close connection exists between root numbers and the dual Selmer group of an elliptic curve over certain non-commutative Galois extensions of the base field F. In fact, the Galois extensions being non-commutative, provide us with a rich source of examples of infinite families of irreducible self-dual Artin representations of the corresponding Galois groups. We consider two such extensions below where the base field is assumed to be $\mathbb{Q}$ for simplicity.

Let p be an odd prime. Fix an integer $m \geq 1$ which is p-power free, and not divisible by any prime of additive reduction for E.

Definition 4.2. The *False Tate extension* of $\mathbb{Q}$ corresponding to m is defined as

$$F_\infty = \bigcup_{n\geq 1} \mathbb{Q}(\mu_{p^n}, m^{1/p^n}). \tag{9}$$

For $n \geq 1$, put

$$F_n \,=\, \mathbb{Q}(\mu_{p^n}, m^{1/p^n}),\ K_n \,=\, \mathbb{Q}(\mu_{p^n}),\ L_n \,=\, \mathbb{Q}(m^{1/p^n}), \tag{10}$$

and let K^{cyc} denote the field obtained by adjoining all the p-power roots of unity to $K := \mathbb{Q}(\mu_p)$. Put

$$G = \mathrm{Gal}(F_\infty/\mathbb{Q}), \qquad H = \mathrm{Gal}(F_\infty/K^{\mathrm{cyc}}) \simeq \mathbb{Z}_p. \tag{11}$$

Our hypotheses above on m imply that the degree $[L_n : \mathbb{Q}] = p^n$ for all $n \geq 0$. The extension F_∞ is a p-adic Lie extension of $\mathbb{Q}$ with Galois group isomorphic to the semi-direct product of H and $\mathbb{Z}_p^\times$. As the group H is isomorphic to $\mathbb{Z}_p$, the Iwasawa algebra $\Lambda(H)$ is isomorphic to the power series ring in one variable over $\mathbb{Z}_p$.

We fix an odd prime p such that $E/\mathbb{Q}$ has good ordinary reduction at p. Further, we shall also assume that the quotient of the dual Selmer group by its p-primary torsion subgroup,

$$Y_p(E/F_\infty) \,=\, X_p(E/F_\infty)/X_p(E/F_\infty)(p) \tag{12}$$

is finitely generated as a $\Lambda(H)$-module. Indeed, as we shall discuss in the next section, there are interesting numerical examples where these assumptions are satisfied, and it is conjectured in [5] that this latter hypothesis always holds. The self-dual irreducible Artin representations of G are well-known in this case. Further, the twisted L-functions are all known to be entire, and satisfy the standard functional equation, thanks to deep results in automorphic forms (Langlands-Tunnell, Arthur-Clozel, Wiles, Breuil-Conrad-Diamond-Taylor). Also, the root numbers exhibit a surprisingly uniform behaviour as was shown by T. Dokchitser. Further, it can be shown that the parity of the root numbers is equal to that of the $\Lambda(H)$-rank of $Y_p(E/F_\infty)$. We also have [4, §4]

Theorem 4.3. *Let $E/\mathbb{Q}$ be an elliptic curve such that E has good ordinary reduction at p. Assume that $Y_p(E/F_\infty)$ (see (12)), is a finitely generated $\Lambda(H)$-module. Then for all self-dual, irreducible Artin representations ρ of G with dimension > 1, the ρ-parity conjecture holds, i.e.*

$$w(E,\rho) \;=\; (-1)^{s_{p,E,\rho}}.$$

The second infinite extension is obtained as follows. Let $E/\mathbb{Q}$ be an elliptic curve with potential good ordinary reduction at p, where $p \geq 5$. Assume also that E does not have complex multiplication. Define

$$F_\infty := \mathbb{Q}(E_{p^\infty}) \tag{13}$$

where

$$E_{p^\infty} := \bigcup_{n\geq 0} E_{p^n}$$

is the Galois module of all p-power division points of E. Let $G := \mathrm{Gal}(F_\infty/\mathbb{Q})$, which by a theorem of Serre is an open subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$. By the Weil pairing, $K^{\mathrm{cyc}} = \mathbb{Q}(\mu_{p^\infty})$ is a subfield of F_∞, and we put $H := \mathrm{Gal}(F_\infty/K^{\mathrm{cyc}})$. The module $Y_p(E/F_\infty)$ is again defined as in (12). Recall that an Artin representation is said to be *orthogonal* if the underlying vector space carries a G-invariant, non-degenerate, symmetric bilinear form. The following theorem is a particular case of a more general result proved in [4, §6].

Theorem 4.4. *Assume that E admits an isogeny of degree p over $\mathbb{Q}$, where p is a prime of potential good ordinary reduction. Assume further that $Y_p(E/F_\infty)$ is a finitely generated $\Lambda(H)$-module. Further, assume that the image of G in $PGL_2(\mathbb{F}_p)$ has even order. Then the ρ-parity conjecture holds for any self-dual, irreducible, orthogonal Artin representation ρ of G of dimension greater than 1.*

It is intriguing to note that the proof of this theorem given in [4] is uncannily parallel to Rohrlich's computation of the root numbers $w(E,\rho)$ in this case [20], perhaps suggesting an as yet undiscovered deeper connection between Iwasawa theory and local root numbers.

Finally T. and V. Dokchitser [8] have proven the following more general result by completely different methods, which do not involve Iwasawa theory.

Theorem 4.5. *Let $E/\mathbb{Q}$ be an elliptic curve with semi-stable reduction at 2 and 3, and let p be any prime. Let K be a finite Galois extension of $\mathbb{Q}$ such that the p-Sylow subgroup of $\mathrm{Gal}(K/\mathbb{Q})$ is normal and has abelian quotient. Then the ρ-parity conjecture holds for the prime p, and all orthogonal representations of $\mathrm{Gal}(K/\mathbb{Q})$.*

5 Examples and Applications

In this final section, we give some applications of the ρ-parity conjecture to obtain lower bounds on the $\mathbb{Z}_p$-ranks of dual Selmer groups, and discuss several numerical examples. It is also worth noting that Iwasawa theory can be used to give upper bounds for the $\mathbb{Z}_p$-coranks of the ρ-components of the Selmer group, as ρ varies over the irreducible Artin characters of a p-adic Lie extension. In this spirit, we end by stating a joint conjecture with J. Coates that proposes strong upper bounds for the multiplicities of Artin representations which can occur in the dual Selmer group of an elliptic curve, considered over finite extensions within a p-adic Lie extension.

Let $E/\mathbb{Q}$ be an elliptic curve and write N_E for the conductor of E. Let p be an odd prime. For each integer $n \geq 1$, let F_n be the fixed field of the centre of $\mathrm{Gal}(\mathbb{Q}(E_{p^n})/\mathbb{Q}))$. The following result is a special case of a more general result of Mazur and Rubin [15, Corollary 2.5]:-

Theorem 5.1. *Assume that E has good ordinary reduction at p and a rational prime of order p. Suppose further that every prime of bad reduction of E has odd order in $\mathbb{F}_p^\times$, and that $-N_E$ is not a square mod p. Then there exists a positive rational number c independent of n such that for every $n \geq 1$, we have*

$$s_{p,E/F_n} \geq c\, p^{2n}.$$

As stated above, Iwasawa theory provides lower bounds for the coranks of the Selmer groups. Particularly striking is the case of the False Tate extension (see Definition 4.2), when the module $Y_p(E/F_\infty)$ (see (12)) has $\Lambda(H)$-rank 1 where H is as in (11). We remark that there are many numerical examples where this is the case. We then have the following theorem [4, Theorem 4.8], where we recall that $K = \mathbb{Q}(\mu_p)$.

Theorem 5.2. *Assume $Y(E/F_\infty)$ is a finitely generated $\Lambda(H)$-module of $\Lambda(H)$-rank 1. Then for all $n \geq 1$, we have*

$$s_{p,E/L_n} \,=\, n + s_{p,E/\mathbb{Q}}, \quad s_{p,E/F_n} \,=\, p^n - 1 + s_{p,E/K},$$

where the fields F_n and L_n are as in (10).

A numerical example of this theorem is given by the elliptic curve

$$E \,:\, y^2 + y = x^3 - x^2,$$

and for the prime $p = 3$ with $m = 11$. We deduce from the theorem that

$$s_{3,E/L_n} = n, \quad \text{and } s_{3,E/F_n} = 3^n - 1, \quad \text{for } n \geq 1.$$

Similarly, the assertions of the theorem hold for $p = 7$ and $m = 2$, showing that

$$s_{7,E/L_n} = n, \quad \text{and } s_{7,E/F_n} = 7^n, \quad \text{for } n \geq 1.$$

Here we have used the fact that $s_{p,E/K} = 1$.

There is also a lower bound in the case of the GL_2 extension F_∞ as defined in (13).

Theorem 5.3. *Let E be an elliptic curve without complex multiplication and p a prime of potential good ordinary reduction. Let*

$$F_\infty = F(E_{p^\infty}), \quad F_n = \mathbb{Q}(E_{p^n}).$$

In addition to the hypotheses of Theorem 4.4, assume that $p \equiv 3 \bmod 4$. Then there exists $c > 0$ independent of n, such that

$$s_{p,E/F_n} \geq c.p^{2n} \quad (n \geq 1).$$

As a numerical example of both Theorem 4.4 and Theorem 5.3, take E to be the elliptic curve

$$y^2 + xy = x^3 - x - 1,$$

of conductor $N_E = 2.3.7^2$, with $p = 7$, and $F_\infty = \mathbb{Q}(E_{7^\infty})$. Then E achieves good ordinary reduction at the unique prime of $\mathbb{Q}(\mu_7)$ above 7. Moreover, μ_7 is a Galois submodule of E_7, and so E has an isogeny of degree 7 defined over $\mathbb{Q}$. It can be shown that $X_7(E/F_\infty)$ is a finitely generated $\Lambda(H)$-module where $H = \mathrm{Gal}(F_\infty/\mathbb{Q}(\mu_{7^\infty}))$. Further, the image in this case of G in $PGL_2(\mathbb{F}_p)$ has order 42. Hence all the hypotheses of Theorems 4.4 and 5.3 hold in this example. We remark that Rohrlich has shown that the cases $w(E, \rho) = +1$ and $w(E, \rho) = -1$ both occur for infinitely many self-dual irreducible Artin representations ρ of G.

We end with a conjecture proposed jointly with John Coates, which was suggested by Theorem 4.12 of [4]. Let F_∞ be a Galois extension of $\mathbb{Q}$ which is unramified outside a finite set of primes, and whose Galois group G is p-adic Lie group. We assume that F_∞ contains the cyclotomic $\mathbb{Z}_p$-extension $\mathbb{Q}^{\mathrm{cyc}}$ of $\mathbb{Q}$. Let $\mathfrak{X}$ denote the set of all one dimensional characters of $\mathrm{Gal}(\mathbb{Q}^{\mathrm{cyc}}/\mathbb{Q})$, and E be any elliptic curve defined over $\mathbb{Q}$.

Conjecture 5.4. *Assume E has potential good ordinary reduction at p. Then there exists an integer C, depending only on E and F_∞, such that, for all irreducible Artin representations ρ of G, we have*

$$\sum_{\chi \in \mathfrak{X}} s_{p,E,\rho\chi} \leq C. \tag{14}$$

Naturally, there is another version of the above conjecture in which we replace $s_{p,E.\rho\chi}$ in (14) by $r_{E,\rho\chi}$. Of course, the generalised Birch and Swinnerton-Dyer conjecture (7), would imply the equivalence of the two versions. We note finally that Theorem 4.12 of [4] shows that the first version of the above conjecture holds for the False Tate extension. Both forms are true for the cyclotomic $\mathbb{Z}_p$ extension of $\mathbb{Q}$ by virtue of well-known theorems of Kato and Rohrlich. At present, it is completely unknown for the extension $F_\infty = F(E_{p^\infty})$ when E does not admit complex multiplication.

References

[1] Birch, B., Stephens, N., *The parity of the rank of the Mordell-Weil group*, Topology **5** (1966), 295–299.

[2] Breuil. C., Conrad, B., Diamond, F., Taylor, R., *On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises*, Jour. AMS **14** (2001), 843–931.

[3] Coates, J., *Fragments of the GL_2 Iwasawa theory of elliptic curves without complex multiplication*, in Arithmetic theory of elliptic curves, Lecture Notes in Math. **1716** Springer (1999), 1–50.

[4] Coates, J., Fukaya, T., Kato,K., Sujatha, R., *Root numbers, Selmer groups and noncommutative Iwasawa theory*, Jour. Alg. Geometry, (To appear).

[5] Coates, J., Fukaya, T., Kato,K., Sujatha, R., Venjakob, O., *The GL_2 main conjecture for elliptic curves without complex multiplication*, Publ. Math. IHES **101** (2005), 163-208.

[6] Dokchitser, T., Dokchitser, V., *Numerical computations in non-commutative Iwasawa theory*, with Appendix by Coates, J., and Sujatha, R., Proc. London Math. Soc. **94** (2006), 211-272

[7] Dokchitser, T., Dokchitser, V., Regulator constants and the parity conjecture, (To appear).

[8] Dokchitser, T., Dokchitser, V., *On the Birch-Swinnerton-Dyer quotients modulo squares*, (To appear).

[9] Greenberg, R., *Iwasawa theory for elliptic curves*, in Arithmetic theory of elliptic curves, Lecture Notes in Math. **1716** Springer (1999), 51–144.

[10] Greenberg, R., *Iwasawa theory, projective modules, and modular representations*, Preprint (2007).

[11] Guo, L., *General Selmer groups and critical values of Hecke L-functions*, Math. Ann. **297** (1993), 221-233.

[12] Kim, B.D., *The parity conjecture and algebraic functional equations for elliptic curves at supersingular reduction primes*, Ph.D Thesis, Stanford University (2005).

[13] Koblitz, N., Introduction to elliptic curves and modular forms. Graduate Texts in Math. Springer (1984).

[14] Mazur, B., Rubin, K., *Finding large Selmer ranks via an arithmetic theory of local constants*, Ann. of Math., (To appear).

[15] Mazur, B., Rubin, K.,, *Growth of Selmer ranks in nonabelian extensions of number fields*, Duke Math. Journal, (To appear).

[16] Monsky, P., *Generalizing the Birch-Stephens theorem*, Math. Z., 221 (1996), 415–420.

[17] Nekovář, J., *Selmer complexes*, Astérisque **310** (2006).

[18] Nekovář, J., *On the parity of ranks of Selmer groups III*, Documenta Math. **12** (2007), 243 - 274.

[19] Rohrlich, D. E., *Galois theory, elliptic curves, and root numbers*, Compositio Math. **100** (1996), 311-349.

[20] Rohrlich, D. E., *Scarcity and abundance of trivial zeros in division towers*, Jour. Alg. Geometry, (To appear).

[21] Rubin, K., *Elliptic curves with complex multiplication and the conjecture of Birch and Swinnerton-Dyer*, in Arithmetic theory of elliptic curves, Lecture Notes in Math. **1716** Springer (1999), 167–234.

[22] Silverman, J., The Arithmetic of Elliptic Curves, Springer-Verlag, GTM **106**, 1986.

[23] Tate, J., *Number Theoretic Background,* Proc. of Symp. in Pure Math. **33** 1979, 3–26.

[24] Wiles, A., *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. **141** (1995), 443-551.

[25] Wiles, A., *The Birch and Swinnerton-Dyer conjecture*, in The Millennium Prize Problems, ed. J. Carlson, A. Jaffe and A. Wiles, Clay Math. Inst. and AMS, (2006), 31–44.