



Contents lists available at ScienceDirect

## Journal of Number Theory

www.elsevier.com/locate/jnt

A note on the Mordell–Weil rank modulo  $n$ Tim Dokchitser<sup>a,\*</sup>, Vladimir Dokchitser<sup>b</sup><sup>a</sup> Robinson College, Cambridge CB3 9AN, United Kingdom<sup>b</sup> Emmanuel College, Cambridge CB2 3AP, United Kingdom

## ARTICLE INFO

## Article history:

Received 3 November 2009

Revised 11 March 2011

Accepted 11 March 2011

Available online xxxx

Communicated by D. Zagier

## MSC:

primary 11G05

secondary 11G40

## Keywords:

Mordell–Weil rank

Elliptic curves

## ABSTRACT

Conjecturally, the parity of the Mordell–Weil rank of an elliptic curve over a number field  $K$  is determined by its root number. The root number is a product of local root numbers, so the rank modulo 2 is (conjecturally) the sum over all places of  $K$  of a function of elliptic curves over local fields. This note shows that there can be no analogue for the rank modulo 3, 4 or 5, or for the rank itself. In fact, standard conjectures for elliptic curves imply that there is no analogue modulo  $n$  for any  $n > 2$ , so this is purely a parity phenomenon.

© 2011 Elsevier Inc. All rights reserved.

It is a consequence of the Birch–Swinnerton–Dyer conjecture that the parity of the Mordell–Weil rank of an elliptic curve  $E$  over a number field  $K$  is determined by its root number, the sign in the functional equation of the  $L$ -function. The root number is a product of local root numbers, which leads to a conjectural formula of the form

$$\mathrm{rk} E/K \equiv \sum_v \lambda(E/K_v) \pmod{2},$$

where  $\lambda$  is an invariant of elliptic curves over *local* fields, and  $v$  runs over the places of  $K$ . One might ask whether there is a local expression like this for the rank modulo 3 or modulo 4, or even for the rank itself. The purpose of this note is to show that, unsurprisingly, the answer is ‘no’.

The idea is simple: if the rank modulo  $n$  were a sum of local  $\mathbb{Z}/n\mathbb{Z}$ -valued invariants, then  $\mathrm{rk} E/K$  would be a multiple of  $n$  whenever  $E$  is defined over  $\mathbb{Q}$  and  $K/\mathbb{Q}$  is a Galois extension where every

\* Corresponding author.

E-mail addresses: t.dokchitser@dpmmms.cam.ac.uk (T. Dokchitser), v.dokchitser@dpmmms.cam.ac.uk (V. Dokchitser).

place of  $\mathbb{Q}$  splits into a multiple of  $n$  places. However, for small  $n > 2$  it is easy to find  $E$  and  $K$  for which this property fails (Theorem 2). In fact, if one believes the standard heuristics concerning ranks of elliptic curves in abelian extensions, it fails for every  $n > 2$  and every  $E/\mathbb{Q}$  (Theorems 9, 13).

This kind of argument can be used to test whether a global invariant has a chance of being a sum of local terms. We will apply it to other standard invariants of elliptic curves and show that the parity of the 2-Selmer rank, the parity of the rank of the  $p$ -torsion and the rank of the 2-torsion in the Tate–Shafarevich group  $\text{III}$  modulo 4 cannot be expressed as a sum of local terms (Theorem 6). Finally, we will also comment on  $L$ -functions all of whose local factors are  $n$ th powers and discuss the parity of the analytic rank for non-self-dual twists of elliptic curves (Remarks 4, 7).

Our results only prohibit an expression for the rank as a *sum* of local terms. Local data does determine the rank, see Remark 15.

## 1. Mordell–Weil rank is not a sum of local invariants

**Definition.** Suppose  $(K, E) \mapsto \Lambda(E/K)$  is some global invariant of elliptic curves over number fields.<sup>1</sup> We say it is a *sum of local invariants* if

$$\Lambda(E/K) = \sum_v \lambda(E/K_v),$$

where  $\lambda$  is some invariant of elliptic curves over local fields, and the sum is taken over all places of  $K$ .

Implicitly,  $\Lambda$  and  $\lambda$  take values in some abelian group  $A$ , usually  $\mathbb{Z}$  or  $\mathbb{Z}/n\mathbb{Z}$  for some  $n \geq 2$ . Moreover  $\lambda(E/K_v)$  should be 0 for all but finitely many  $v$ .

**Example.** If the Birch–Swinnerton–Dyer conjecture holds (or if  $\text{III}$  is finite, see [4]), then the Mordell–Weil rank modulo 2 is a sum of local invariants with values in  $\mathbb{Z}/2\mathbb{Z}$ . Specifically, for an elliptic curve  $E$  over a local field  $k$  write  $w(E/k) = \pm 1$  for its local root number, and define  $\lambda$  by  $(-1)^{\lambda(E/k)} = w(E/k)$ . Then

$$\text{rk } E/K \equiv \sum_v \lambda(E/K_v) \pmod{2}.$$

An explicit description of local root numbers can be found in [9] and [4].

**Theorem 1.** *The Mordell–Weil rank is not a sum of local invariants.*

This is a consequence of the following stronger statement:

**Theorem 2.** *For  $n \in \{3, 4, 5\}$  the Mordell–Weil rank modulo  $n$  is not a sum of local invariants (with values in  $\mathbb{Z}/n\mathbb{Z}$ ).*

**Lemma 3.** *Suppose  $\Lambda : (\text{number fields}) \rightarrow \mathbb{Z}/n\mathbb{Z}$  satisfies  $\Lambda(K) = \sum_v \lambda(K_v)$  for some invariant  $\lambda : (\text{local fields}) \rightarrow \mathbb{Z}/n\mathbb{Z}$ . Then  $\Lambda(F) = 0$  whenever  $F/K$  is a Galois extension of number fields in which the number of places above each place of  $K$  is a multiple of  $n$ .*

**Proof.** In the local expression for  $\Lambda(F)$  each local field occurs a multiple of  $n$  times.  $\square$

<sup>1</sup> Meaning that if  $K \cong K'$  and  $E/K$  and  $E'/K'$  are isomorphic elliptic curves (identifying  $K$  with  $K'$ ), then  $\Lambda(E/K) = \Lambda(E'/K')$ .

**Proof of Theorem 2.** Take  $E/\mathbb{Q} : y^2 = x(x+2)(x-3)$ , which is 480a1 in Cremona's notation. Writing  $\zeta_p$  for a primitive  $p$ th root of unity, let

$$F_n = \begin{cases} \text{the degree 9 subfield of } \mathbb{Q}(\zeta_{13}, \zeta_{103}) & \text{if } n = 3, \\ \text{the degree 25 subfield of } \mathbb{Q}(\zeta_{11}, \zeta_{241}) & \text{if } n = 5, \\ \mathbb{Q}(\sqrt{-1}, \sqrt{41}, \sqrt{73}) & \text{if } n = 4. \end{cases}$$

Because 13 and 103 are cubes modulo one another, and all other primes are unramified in  $F_3$ , every place of  $\mathbb{Q}$  splits into 3 or 9 places in  $F_3$ . Similarly  $F_4$  and  $F_5$  also satisfy the assumptions of Lemma 3 with  $n = 4, 5$ . Hence, if the Mordell–Weil rank modulo  $n$  were a sum of local invariants, it would be  $0 \in \mathbb{Z}/n\mathbb{Z}$  for  $E/F_n$ . However, 2-descent shows that  $\text{rk } E/F_3 = \text{rk } E/F_5 = 1$  and  $\text{rk } E/F_4 = 6$  (e.g. using Magma [1], over all minimal non-trivial subfields of  $F_n$ ).  $\square$

**Remark 4.** The  $L$ -series of the curve  $E = 480a1$  used in the proof over  $F = F_4 = \mathbb{Q}(\sqrt{-1}, \sqrt{41}, \sqrt{73})$  is formally a 4th power, in the sense that each Euler factor is:

$$L(E/F, s) = \left(\frac{1}{1}\right)^4 \left(\frac{1}{1-3^{-2s}}\right)^4 \left(\frac{1}{1-5^{-2s}}\right)^4 \left(\frac{1}{1+14\cdot 7^{-2s}+7^{2-4s}}\right)^4 \left(\frac{1}{1+6\cdot 11^{-2s}+11^{2-4s}}\right)^4 \cdots$$

However, it is not a 4th power of an entire function, as it vanishes to order 6 at  $s = 1$ . Actually, it is not even a square of an entire function: it has a simple zero at  $1 + 2.1565479\dots i$ .

In fact, by construction of  $F$ , for any  $E/\mathbb{Q}$  the  $L$ -series  $L(E/F, s)$  is formally a 4th power and vanishes to even order at  $s = 1$  by the functional equation. Its square root has analytic continuation to a domain including  $\text{Re } s > \frac{3}{2}$ ,  $\text{Re } s < \frac{1}{2}$  and the real axis, and satisfies a functional equation  $s \leftrightarrow 2-s$ , but it is not clear whether it has an arithmetic meaning.

**Lemma 5.** Suppose an invariant  $\Lambda \in \mathbb{Z}/2^k\mathbb{Z}$  is a sum of local invariants. Let  $F = K(\sqrt{\alpha_1}, \dots, \sqrt{\alpha_m})$  be a multi-quadratic extension in which every prime of  $K$  splits into a multiple of  $2^k$  primes of  $F$ . Then for every elliptic curve  $E/K$ ,

$$\Lambda(E/K) + \sum_D \Lambda(E_D/K) = 0,$$

where the sum is taken over the quadratic subfields  $K(\sqrt{D})$  of  $F/K$ , and  $E_D$  denotes the quadratic twist of  $E$  by  $D$ .

**Proof.** In the local expression for the left-hand side of the formula each local term ( $\lambda$  of a given elliptic curve over a given local field) occurs a multiple of  $2^k$  times.  $\square$

**Theorem 6.** Each of the following is not a sum of local invariants:

- $\dim_{\mathbb{F}_2} \text{III}(E/K)[2] \bmod 4$ ,
- $\text{rk}(E/K) + \dim_{\mathbb{F}_2} \text{III}(E/K)[2] \bmod 4$ ,
- $\dim_{\mathbb{F}_2} \text{Sel}_2 E/K \bmod 2$ ,
- $\dim_{\mathbb{F}_p} E(K)[p] \bmod 2$  for any prime  $p$ .

Here  $\text{III}$  is the Tate–Shafarevich group and  $\text{Sel}_2$  is the 2-Selmer group.

**Proof.** The argument is similar to that of Theorem 2:

For the first two claims, apply Lemma 5 to  $E : y^2 + y = x^3 - x$  (37a1) with  $K = \mathbb{Q}$  and  $F = \mathbb{Q}(\sqrt{-1}, \sqrt{17}, \sqrt{89})$ . The quadratic twists of  $E$  by 1,  $-17$ ,  $-89$ ,  $17 \cdot 89$  have rank 1, and those by  $-1$ ,  $17$ ,  $89$ ,  $-17 \cdot 89$  have rank 0; the twist by  $-17 \cdot 89$  has  $|\text{III}[2]| = 4$  and the other seven have

trivial III[2]. The sum over all twists is therefore 2 mod 4 in both cases, so they are not sums of local invariants.

For the parity of the 2-Selmer rank and of  $\dim E[2]$  apply Lemma 3 to  $E: y^2 + xy + y = x^3 + 4x - 6$  (14a1) with  $K = \mathbb{Q}$ ,  $F = \mathbb{Q}(\sqrt{-1}, \sqrt{17})$  and  $n = 2$ . The 2-torsion subgroup of  $E/F$  is of order 2 and its 2-Selmer group over  $F$  is of order 8.

Finally, for  $\dim_{\mathbb{F}_p} E[p] \bmod 2$  for  $p > 2$  take any elliptic curve  $E/\mathbb{Q}$  with  $\text{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \cong \text{GL}_2(\mathbb{F}_p)$ , e.g.  $E: y^2 = x^3 - x^2 + x$  (24a4), see [10, 5.7.2]. Let  $K$  be the field obtained by adjoining to  $\mathbb{Q}$  the coordinates of one  $p$ -torsion point and  $F = K(\sqrt{-1}, \sqrt{17})$ . Because  $F$  does not contain the  $p$ th roots of unity,  $\dim_{\mathbb{F}_p} E(F)[p] = 1$ . So, by Lemma 3 the parity of this dimension is not a sum of local invariants.  $\square$

**Remark 7.** The functional equation expresses the parity of the analytic rank as a sum of local invariants not only for elliptic curves (or abelian varieties), but also for their twists by self-dual Artin representations. However, for the parity of the rank of non-self-dual twists there is presumably no such expression.

For example, let  $\chi$  be a non-trivial Dirichlet character of  $(\mathbb{Z}/7\mathbb{Z})^\times$  of order 3. Then there is no function  $(k, E) \mapsto \lambda(E/k) \in \mathbb{Z}$  defined for elliptic curves over local fields  $k$ , such that for all elliptic curves  $E/\mathbb{Q}$ ,

$$\text{ord}_{s=1} L(E, \chi, s) \equiv \sum_v \lambda(E/\mathbb{Q}_v) \pmod{2}.$$

To see this, take

$$E/\mathbb{Q}: y^2 + y = x^3 + x^2 + x \text{ (19a3)}, \quad K = \mathbb{Q}, \quad F = \mathbb{Q}(\sqrt{-1}, \sqrt{17})$$

and apply Lemma 5. The twists of  $E, E_{-1}$  and  $E_{17}$  by  $\chi$  have analytic rank 0, and that of  $E_{-17}$  has analytic rank 1, adding up to an odd number.

## 2. Expectations

We expect the Mordell–Weil rank modulo  $n$  not to be a sum of local terms for any  $n > 2$  and any class of elliptic curves. Theorems 9 and 13 below show that this is a consequence of modularity of elliptic curves, the known cases of the Birch–Swinnerton-Dyer conjecture and standard conjectures for analytic ranks of elliptic curves.

**Notation.** For a prime  $p$  we write  $\Sigma_p$  for the set of all Dirichlet characters of order  $p$ . We say that  $S \subset \Sigma_p$  has density  $\alpha$  if

$$\lim_{x \rightarrow \infty} \frac{|\{\chi: \chi \in S \mid N(\chi) < x\}|}{|\{\chi: \chi \in \Sigma_p \mid N(\chi) < x\}|} = \alpha,$$

where  $N(\chi)$  denotes the conductor of  $\chi$ .

**Conjecture 8** (Weak form of [3, Conj. 1.2]). For  $p > 2$  and every elliptic curve  $E/\mathbb{Q}$ , those  $\chi \in \Sigma_p$  for which  $L(E, \chi, 1) = 0$  have density 0 in  $\Sigma_p$ .

**Theorem 9.** Let  $E/\mathbb{Q}$  be an elliptic curve and  $p$  an odd prime. Assuming Conjecture 8, there is no function  $k \mapsto \lambda(E/k) \in \mathbb{Z}/p\mathbb{Z}$  defined for local fields  $k$  of characteristic 0, such that for every number field  $K$ ,

$$\text{rk } E/K \equiv \sum_v \lambda(E/K_v) \pmod{p}.$$

**Lemma 10.** Let  $p$  be a prime number and  $S \subset \Sigma_p$  a set of characters of density 0 in  $\Sigma_p$ . For every  $d \geq 1$  there is an abelian extension  $F_d/\mathbb{Q}$  with Galois group  $G \cong \mathbb{F}_p^d$ , such that no characters of  $G$  are in  $S$ .

**Proof.** Without loss of generality, we may assume that if  $\chi \in S$  then  $\chi^n \in S$  for  $1 \leq n < p$ . When  $d = 1$ , take  $F_1$  to be the kernel of any  $\chi \in \Sigma_p \setminus S$ . Now proceed by induction, supposing that  $F_{d-1}$  is constructed. Writing  $\Psi$  for the set of characters of  $\text{Gal}(F_{d-1}/\mathbb{Q})$ , the set

$$S_d = \bigcup_{\psi \in \Psi} \{\phi\psi : \phi \in S\}$$

still has density 0. Pick any  $\chi \in \Sigma_p \setminus S_d$ , and set  $F_d$  to be the compositum of  $F_{d-1}$  and the degree  $p$  extension of  $\mathbb{Q}$  cut out by  $\chi$ . It is easy to check that no character of  $\text{Gal}(F_d/\mathbb{Q})$  lies in  $S$ .  $\square$

**Proof of Theorem 9.** Pick a quadratic field  $\mathbb{Q}(\sqrt{D})$  such that the quadratic twist  $E_D$  of  $E$  by  $D$  has analytic rank 1, which is possible by [2,8,11]. By Conjecture 8, the set  $S$  of Dirichlet characters  $\chi$  of order  $p$  such that  $L(E_D, \chi, 1) = 0$  has density 0. Apply Lemma 10 to  $S$  with  $d = 3$ . Every place of  $\mathbb{Q}$  splits in the resulting field  $F = F_3$  into a multiple of  $p$  places ( $\mathbb{Q}_l$  has no  $\mathbb{F}_p^3$ -extensions, so every prime has to split).

Arguing by contradiction, suppose the rank of  $E \bmod p$  is a sum of local invariants. Because in  $F/\mathbb{Q}$  and therefore also in  $F(\sqrt{D})/\mathbb{Q}$  every place splits into a multiple of  $p$  places,

$$\text{rk } E/F \equiv 0 \pmod{p} \quad \text{and} \quad \text{rk } E/F(\sqrt{D}) \equiv 0 \pmod{p}$$

by Lemma 3. Therefore  $\text{rk } E_D/F = \text{rk } E/F(\sqrt{D}) - \text{rk } E/F$  is a multiple of  $p$ . On the other hand,

$$L(E_D/F, s) = \prod_{\chi} L(E_D, \chi, s),$$

the product taken over the characters of  $\text{Gal}(F/\mathbb{Q})$ . By construction, it has a simple zero at  $s = 1$ . Because  $F$  is totally real of odd degree over  $\mathbb{Q}$ , by Zhang's theorem [12, Thm. A],  $E_D/F$  has Mordell–Weil rank  $1 \not\equiv 0 \pmod{p}$ , a contradiction.  $\square$

**Conjecture 11.** (See Goldfeld [6].) For every elliptic curve  $E/\mathbb{Q}$ , those  $\chi \in \Sigma_2$  for which  $\text{ord}_{s=1} L(E, \chi, s) > 1$  have density 0 in  $\Sigma_2$ .

**Conjecture 12.** Every elliptic curve  $E/\mathbb{Q}$  has a quadratic twist of Mordell–Weil rank 2.

**Theorem 13.** Let  $E/\mathbb{Q}$  be an elliptic curve. Assuming Conjectures 11 and 12, there is no function  $k \mapsto \lambda(E/k) \in \mathbb{Z}/4\mathbb{Z}$  defined for local fields  $k$  of characteristic 0, such that for every number field  $K$ ,

$$\text{rk } E/K \equiv \sum_v \lambda(E/K_v) \pmod{4}.$$

**Proof.** Let  $\mathbb{Q}(\sqrt{D})$  be a quadratic field such that the quadratic twist  $E' = E_D$  of  $E$  by  $D$  has Mordell–Weil rank 2 (Conjecture 12). The set  $S$  of those  $\chi \in \Sigma_2$  for which  $\text{ord}_{s=1} L(E', \chi, s) > 1$  has density 0 (Conjecture 11). Let  $P$  be the set of primes where  $E'$  has bad reduction union  $\{\infty\}$ , and apply Lemma 10 to  $S$  with  $d = 5 + 3|P|$ . The resulting field  $F_d$  has a subfield  $F$  of degree  $2^5$  over  $\mathbb{Q}$ , where all places in  $P$  split completely:  $\mathbb{Q}_l$  has no  $\mathbb{F}_2^4$ -extensions, so the condition that a given place in  $P$  splits completely drops the dimension by at most 3. By the same argument, every place of  $\mathbb{Q}$  splits in  $F$  into a multiple of 4 places.

Arguing by contradiction, suppose the rank of  $E \bmod 4$  is a sum of local invariants. Because in  $F/\mathbb{Q}$  and therefore also in  $F(\sqrt{D})/\mathbb{Q}$  every place splits into a multiple of 4 places,

$$\mathrm{rk} E/F \equiv 0 \pmod{4} \quad \text{and} \quad \mathrm{rk} E/F(\sqrt{D}) \equiv 0 \pmod{4}$$

by Lemma 3. Therefore  $\mathrm{rk} E'/F = \mathrm{rk} E/F(\sqrt{D}) - \mathrm{rk} E/F$  is a multiple of 4. Now we claim that  $E'/F$  has rank 2 or 33, yielding a contradiction.

Let  $\mathbb{Q}(\sqrt{m}) \subset F$  be a quadratic subfield. The root number of  $E'$  over  $\mathbb{Q}(\sqrt{m})$  is 1, because the root number is a product of local root numbers and the places in  $P$  split in  $\mathbb{Q}(\sqrt{m})$ . (The local root number is +1 at primes of good reduction.) So

$$L(E'/\mathbb{Q}(\sqrt{m}), s) = L(E'/\mathbb{Q}, s)L(E'_m/\mathbb{Q}, s)$$

vanishes to even order at  $s = 1$ . Hence the 31 twists of  $E'$  by the non-trivial characters of  $\mathrm{Gal}(F/\mathbb{Q})$  have the same analytic rank 0 or 1, by the choice of  $F$ . By Kolyvagin's theorem [7], their Mordell–Weil ranks are the same as their analytic ranks, and so  $\mathrm{rk} E'/F$  is either  $2 + 0$  or  $2 + 31$ .  $\square$

**Remark 14.** In some cases, it may seem reasonable to try and write some global invariant in  $\mathbb{Z}/n\mathbb{Z}$  as a sum of local invariants in  $\frac{1}{m}\mathbb{Z}/n\mathbb{Z}$ , i.e. to allow denominators in the local terms. For instance, one could ask whether the parity of the rank of a cubic twist (as in Remark 7) can be written as a sum of local invariants of the form  $\frac{a}{3} \bmod 2\mathbb{Z}$ .

However, introducing a denominator does not appear to help. First, the prime-to- $n$  part  $m'$  of  $m$  adds no flexibility, as can be seen by multiplying the formula by  $m'$ . (For instance, if there were a formula for the parity of the rank of a cubic twist as a sum of local terms in  $\frac{a}{3} \bmod 2\mathbb{Z}$ , then multiplying it by 3 would yield a formula for the same parity with local terms in  $\mathbb{Z}/2\mathbb{Z}$ .) As for the non-prime-to- $n$  part, e.g. the proofs of Theorems 9 and 13 immediately adapt to local invariants in  $\frac{1}{p^k}\mathbb{Z}/p\mathbb{Z}$  and  $\frac{1}{2^k}\mathbb{Z}/4\mathbb{Z}$ , by increasing  $d$  by  $k$ .

**Remark 15.** The negative results in this paper rely essentially on the fact that we allow only additive formulae for global invariants in terms of local invariants. Although Theorem 1 shows that there is no formula of the form

$$\mathrm{rk} E/K = \sum_v \lambda(E/K_v),$$

the Mordell–Weil rank is determined by the set  $\{E/K_v\}_v$  of curves over local fields. In other words,

$$\mathrm{rk} E/K = \text{function}(\{E/K_v\}_v).$$

In fact, for any abelian variety  $A/K$  the set  $\{A/K_v\}_v$  determines the  $L$ -function  $L(A/K, s)$  which is the same as  $L(W/\mathbb{Q}, s)$  where  $W$  is the Weil restriction of  $A$  to  $\mathbb{Q}$ . By Faltings' theorem [5] the  $L$ -function recovers  $W$  up to isogeny, and hence also recovers the rank  $\mathrm{rk} A/K (= \mathrm{rk} W/\mathbb{Q})$ .

## Acknowledgments

The first author is supported by a Royal Society University Research Fellowship. The second author would like to thank Gonville & Caius College, Cambridge.

## References

- [1] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system. I: The user language, *J. Symbolic Comput.* 24 (3–4) (1997) 235–265.
- [2] D. Bump, S. Friedberg, J. Hoffstein, Nonvanishing theorems for  $L$ -functions of modular forms and their derivatives, *Invent. Math.* 102 (1990) 543–618.
- [3] C. David, J. Fearnley, H. Kisilevsky, Vanishing of  $L$ -functions of elliptic curves over number fields, in: *Ranks of Elliptic Curves and Random Matrix Theory*, in: London Math. Soc. Lecture Note Ser., vol. 341, Cambridge University Press, 2007, pp. 247–259.
- [4] T. Dokchitser, V. Dokchitser, Root numbers and parity of ranks of elliptic curves, arXiv:0906.1815, 2009.
- [5] G. Faltings, Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, *Invent. Math.* 73 (3) (1983) 349–366.
- [6] D. Goldfeld, Conjectures on elliptic curves over quadratic fields, *Springer Lect. Notes* 751 (1979) 108–118.
- [7] V.A. Kolyvagin, Euler systems, in: *The Grothendieck Festschrift*, in: *Progr. Math.*, Birkhäuser, Boston, 1990.
- [8] M.R. Murty, V.K. Murty, Mean values of derivatives of modular  $L$ -series, *Ann. of Math.* 133 (1991) 447–475.
- [9] D. Rohrlich, Galois theory, elliptic curves, and root numbers, *Compos. Math.* 100 (1996) 311–349.
- [10] J.-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.* 15 (4) (1972) 259–331.
- [11] J.-L. Waldspurger, Correspondences de Shimura et quaternions, *Forum Math.* 3 (1991) 219–307.
- [12] S. Zhang, Heights of Heegner points on Shimura curves, *Ann. of Math.* 153 (2001) 27–147.