Journal of Number Theory 182 (2018) 1–18

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Elliptic curves, L-functions, and Hilbert's tenth problem

M. Ram Murty [a], Hector Pasten [b,*]

[a] *Department of Mathematics and Statistics, Queen's University, Jeffery Hall, University ave., Kingston, ON K7L 3N6, Canada*
[b] *Department of Mathematics, Harvard University, 1 Oxford Street, Cambridge, MA 02138, USA*

ARTICLE INFO

Article history:
Received 7 March 2017
Accepted 7 July 2017
Available online 31 August 2017
Communicated by D. Thakur

To the memory of Anthony V. Geramita

MSC:
primary 11U05
secondary 11G05, 14G10

Keywords:
Hilbert's tenth problem
Rings of integers
Ranks of elliptic curves

ABSTRACT

Hilbert's tenth problem for rings of integers of number fields remains open in general, although a negative solution has been obtained by Mazur and Rubin conditional to a conjecture on Shafarevich–Tate groups. In this work we consider the problem from the point of view of analytic aspects of L-functions instead. We show that Hilbert's tenth problem for rings of integers of number fields is unsolvable, conditional to the following conjectures for L-functions of elliptic curves: the automorphy conjecture and the rank part of the Birch and Swinnerton–Dyer conjecture.

1. Introduction

In 1900, Hilbert asked for an algorithm to decide the Diophantine problem of $\mathbb{Z}$. Namely, he asked for an algorithm which takes as input a polynomial equation with integer coefficients (possibly in many variables) and after a finite amount of computation

* Corresponding author.
E-mail addresses: murty@mast.queensu.ca (M.R. Murty), hpasten@math.harvard.edu (H. Pasten).

http://dx.doi.org/10.1016/j.jnt.2017.07.008
0022-314X/

can determine if the equation has an integer solution or not. This problem is known as Hilbert's tenth problem.

Matijasevich proved in 1970 that the Diophantine problem of $\mathbb{Z}$ is undecidable [16], after the work of Davis, Putnam, and Robinson [4] thus showing that Hilbert's tenth problem is unsolvable. It is natural to address the analogous question in other rings with interesting arithmetic, such as number fields, meromorphic functions, function fields, their rings of integers, etc. (See Section 2 for a precise statement.) In this paper we consider the case of rings of integers of number fields.

Let K be a number field and let $\mathcal{O}_K$ be its ring of integers. The current approach to showing that the Diophantine problem for $\mathcal{O}_K$ is undecidable consists of trying to show that $\mathbb{Z}$ has a Diophantine definition in $\mathcal{O}_K$, thus reducing the problem to Matijasevich's theorem. This approach has been successful in the following cases:

- K is totally real, or a quadratic extension of a totally real number field [5,8,7],
- K has exactly one non-real archimedean place [23,28],
- subfields of the previous ones (e.g. all abelian extensions of $\mathbb{Q}$) [26].

By work of Poonen [24], Cornelissen–Pheidas–Zahidi [3], and Shlapentokh [30] the sought Diophantine definition of $\mathbb{Z}$ in $\mathcal{O}_K$ can be obtained from the existence of suitable elliptic curves over number fields retaining their rank in finite extensions. This important link with the theory of elliptic curves was used by Mazur and Rubin [18] to prove the following

Theorem 1.1 *(Mazur–Rubin). Assume the squareness conjecture for the* 2*-torsion part of Shafarevich–Tate groups of elliptic curves over number fields. Then for every number field* K*, the Diophantine problem of* $\mathcal{O}_K$ *is undecidable.*

The conjecture assumed in this result says that, if K is a number field and E is an elliptic curve over K, then the finite 2-group $Ш_E[2]$ has square order. This would follow from the folklore conjecture that $Ш_E$ is finite, which in turn is implied by the *special value formula* in the Birch and Swinnerton–Dyer conjecture.

In this paper we address the existence of the necessary elliptic curves from the point of view of L-functions. Our goal is to show that if L-functions of elliptic curves have the "expected good analytic properties" and if they satisfy the *rank part* of the Birch and Swinnerton–Dyer conjecture, then Hilbert's tenth problem for $\mathcal{O}_K$ is unsolvable for every number field K.

Our main results are presented in sections 6 and 7 below, in particular see Theorem 6.2 and Theorem 7.1. An immediate consequence which requires less preparation (although it is somewhat weaker) is the following

Theorem 1.2. *Suppose that elliptic curves over number fields are automorphic, that they satisfy the parity conjecture, and that they satisfy the analytic rank zero part of the twisted*

Birch and Swinnerton–Dyer conjecture. Then for every number field K, Hilbert's tenth problem for $\mathcal{O}_K$ is unsolvable (i.e. the Diophantine problem for $\mathcal{O}_K$ is undecidable).

Let us explain the conjectural hypotheses in this result. Let K be a number field. An elliptic curve E over K is *automorphic* if its L-function $L(s,E)$ agrees (up to some normalization) with the L-function of a cuspidal automorphic representation of GL_2, and it is conjectured that this is always the case [13]. This is a generalization to number fields of the Shimura–Taniyama conjecture (now the modularity theorem), see Section 3 for more details. By the Jacquet–Langlands converse theorem for GL_2 (see [14]), this is the same as requiring that the suitably defined L-functions $L(s,E,\eta)$ twisted by certain Hecke characters η, have "good analytic properties" including analytic continuation and functional equation.

The parity conjecture asserts that the global root number of E/K equals $(-1)^{\mathrm{rk}\, E(K)}$. For automorphic elliptic curves the root number of E equals the sign of the functional equation of $L(s,E)$, so the parity conjecture follows from the rank part of the Birch and Swinnerton–Dyer (BSD) conjecture, which asserts that

$$\mathrm{ord}_{s=1} L(s,E) = \mathrm{rk}\, E(K).$$

On the other hand, by the "twisted Birch and Swinnerton–Dyer conjecture" we mean the variation of the BSD conjecture involving twists by finite order Hecke characters, as proposed by Mazur [17]. Namely, if L/K is a finite abelian extension and η is a finite order Hecke character corresponding to it, then $\mathrm{ord}_{s=1} L(s,E,\eta)$ equals the dimension of the η-isotypical component of the $\mathrm{Gal}(L/K)$-representation $E(L)\otimes\mathbb{C}$. Note that when η is the trivial character one recovers the rank part of the BSD conjecture. The analytic rank zero part mentioned in Theorem 1.2 refers to the conjectural implication

$$\mathrm{ord}_{s=1} L(s,E,\eta) = 0 \Longrightarrow \dim(E(L)\otimes\mathbb{C})^{\eta} = 0.$$

Actually, Theorem 1.2 needs milder hypotheses (see Theorem 6.2), some of which are known to hold in certain degree of generality thanks to the current spectacular progress on the Langlands program and on the Birch and Swinnerton–Dyer conjecture made by several authors. This will be discussed in Section 7.

Let us briefly explain the connection between Hilbert's tenth problem and L-functions. By the work of Poonen and Shlapentokh, one only needs to show that for cyclic number field extensions L/K of prime degree, there is an elliptic curve E defined over K such that $\mathrm{rk}\, E(L) = \mathrm{rk}\, E(K) = 1$ (in fact, this is precisely what is obtained by Mazur and Rubin under the squareness conjecture for $Ш_E[2]$). A priori, if one assumes automorphy and BSD in order to address the problem in the analytic side, one ends up trying to control simultaneously the vanishing order of two L-functions for automorphic representations of GL_2, a problem which is currently out of reach (see [2] for a discussion on this problem in a general theoretical framework; the discussion in p. 169 is particularly relevant here). We can circumvent this difficulty thanks to a result of Shlapentokh which shows that

actually $\operatorname{rk} E(L) = \operatorname{rk} E(K) > 0$ suffices for the undecidability application. The analytic counterpart of this last condition can be translated into the problem of controlling just *one* L-function for an automorphic representation of GL_2 varying over quadratic twists, under some additional congruence restrictions for the admissible quadratic twists. The necessary non-vanishing results are provided by theorems of Friedberg–Hoffstein [12], see also Murty–Murty [19] and [20] for the case $K = \mathbb{Q}$. It is crucial that these non-vanishing results are also applicable to non-self-contragredient automorphic representations (in the case $K = \mathbb{Q}$, this corresponds to modular forms with non-trivial nebentypus).

We remark that the elliptic curves retaining their positive rank in number field extensions produced (conditionally) in our work as well as in [18], can also be used to obtain definability and decidability consequences in the context of Hilbert's tenth problem for *big sub-rings* of number fields (i.e. rings of S-integers of number fields with S a set of primes with positive natural density). We refer the reader to Theorem 1.9 in [30] for details.

We conclude this introduction with an outline of the paper. The necessary background on Hilbert's tenth problem, automorphic L-functions, and the BSD conjecture is given in sections 2, 3, and 4 respectively. Our results will only apply to elliptic curves satisfying certain conditions on their global root numbers, so in Section 5 we produce elliptic curves with the necessary properties. The main results in the context of Hilbert's tenth problem are given in Section 6. Finally, in Section 7 we discuss some arithmetic applications and *unconditional* results for L-functions, mainly related to elliptic curves retaining their positive rank in cyclic extensions of totally real number fields.

2. Hilbert's tenth problem

Let R be a (commutative, unitary) ring, and let R_0 be a recursive sub-ring of R. Then the polynomial ring in countably many variables $R_0[x_1, x_2, ...]$ is also recursive, and one can formulate the following analogue of Hilbert's tenth problem:

Problem 2.1 *($H10(R; R_0)$). Find an algorithm (in the sense of a Turing machine) that takes as input polynomial equations (possibly with many variables) with coefficients in R_0, and decides whether the equation has a solution over R or not.*

In other words, $H10(R; R_0)$ asks for an algorithm[1] to solve the Diophantine problem of R with coefficients in R_0. When the requested algorithm exists, we say that $H10(R; R_0)$ is decidable, otherwise we say that it is undecidable.

Let us stress the fact that $H10(R; R_0)$ is sensitive not only to R but also to R_0. For instance, $H10(\mathbb{C}[z]; \mathbb{Z})$ is decidable (the problem can be reduced to $H10(\mathbb{C}; \mathbb{Z})$) but $H10(\mathbb{C}[z]; \mathbb{Z}[z])$ is undecidable by [6].

[1] One can argue that a better question is to ask whether the Diophantine problem is decidable or not. We preferred to keep Hilbert's formulation for the sake of historical accuracy.

We will be interested in the case when K is a number field and $R = R_0 = \mathcal{O}_K$ is the ring of integers of K. So, instead of continuing with a general discussion, let us focus on this particular case and write $H10(\mathcal{O}_K)$ instead of $H10(\mathcal{O}_K; \mathcal{O}_K)$. Note that the case $K = \mathbb{Q}$ is precisely Hilbert's original problem and it is known to be undecidable by work of Davis, Putnam, Robinson and finally Matijasevich.

It is widely conjectured that $H10(\mathcal{O}_K)$ is undecidable for every number field K, and the general approach for showing results in this direction consists of showing that $\mathbb{Z}$ is *Diophantine* in $\mathcal{O}_K$, in the following sense: a set $S \subseteq \mathcal{O}_K^n$ is *Diophantine* if there is a polynomial $F \in \mathcal{O}_K[x_1, ...x_n, y_1, ..., y_m]$ such that

$$S = \{\mathbf{a} \in \mathcal{O}_K^n : \exists \mathbf{b} \in \mathcal{O}_K^m, F(\mathbf{a}, \mathbf{b}) = 0\}.$$

In fact, it is easy to see that if $\mathbb{Z}$ is Diophantine in $\mathcal{O}_K$ then an algorithm as the one requested in $H10(\mathcal{O}_K)$ can be modified to get an algorithm for $H10(\mathbb{Z})$, which is not possible by Matijasevich's theorem. We remark, however, that for the purpose of showing that $H10(\mathcal{O}_K)$ is undecidable, it would suffice to give a Diophantine interpretation of $\mathbb{Z}$ rather that an actual Diophantine definition.

The previous approach has had remarkable success, and now one knows that $\mathbb{Z}$ is Diophantine in $\mathcal{O}_K$ in the following cases (cf. the introduction):

- K is contained in a CM number field (imaginary quadratic extension of totally real);
- K is contained in a number field with exactly one non-real archimedean place.

More generally, we say that a number field extension L/K is *integrally Diophantine* if $\mathcal{O}_K$ is Diophantine in $\mathcal{O}_L$. This property of number field extensions enjoys some very useful "functorial" properties.

Proposition 2.2. *The following holds for number field extensions:*

- *If L/K is integrally Diophantine and $H10(\mathcal{O}_K)$ is undecidable, then so is $H10(\mathcal{O}_L)$;*
- *If L/K and K/k are integrally Diophantine, then so is L/k;*
- *If L/k is integrally Diophantine and K is an intermediate field, then K/k is integrally Diophantine;*
- *If L/K_1 and L/K_2 are integrally Diophantine, then so is $L/K_1 \cap K_2$.*

See [8] and [26] for details, and see Chapter 2 of [29] for a general reference on this subject.

For instance, from the previous proposition it follows that $H10(\mathcal{O}_K)$ is undecidable whenever $K/\mathbb{Q}$ is abelian: in that case K is contained in a cyclotomic field by the Kronecker–Weber theorem, and cyclotomic fields are CM.

The following result is due to Poonen and Shlapentokh. It reduces the problem of verifying if an arbitrary Galois extension of number fields is integrally Diophantine to

a much simpler class of Galois extensions. The proof is the same as in Corollary 8.4 of [18]; we include a proof here for the convenience of the reader.

Proposition 2.3. *Let L/K be a Galois extension of number fields. Suppose that every cyclic extension of prime degree k'/k with $K \subseteq k \subseteq k' \subseteq L$ satisfies that k'/k is integrally Diophantine. Then L/K is integrally Diophantine.*

In particular, if every cyclic extension of prime degree of number fields is integrally Diophantine, then for every number field K one has that $\mathbb{Z}$ is Diophantine in $\mathcal{O}_K$ and $H10(\mathcal{O}_K)$ is undecidable.

Proof. Let k be any intermediate field of K/L such that L/k is cyclic, and consider a tower of fields $L = k_n \supseteq ... \supseteq k_1 \supseteq k_0 = k$ where each k_i/k_{i-1} is cyclic of prime degree. Then by hypothesis each k_i/k_{i-1} is integrally Diophantine, thus L/k is integrally Diophantine.

Let $G = \mathrm{Gal}(L/K)$. For each $g \in G$ we get that $L/L^{\langle g \rangle}$ is integrally Diophantine, therefore L/K is integrally Diophantine because $K = L^G = \cap_{g \in G} L^{\langle g \rangle}$. □

Let us now discuss the relation between integrally Diophantine number field extensions and elliptic curves retaining their rank in extensions. The observation that elliptic curves preserving their ranks in number field extensions K/k play a prominent role in Hilbert's tenth problem for rings of integers, can be traced back to the work of Denef [7]. At the end of that paper, and despite already having an unconditional result for totally real number fields, Denef notes that if L is a totally real number field and there is an elliptic curve $E/\mathbb{Q}$ with

$$\mathrm{rk}\, E(L) = \mathrm{rk}\, E(\mathbb{Q}) > 0$$

then one can show $\mathbb{Z}$ is Diophantine in $\mathcal{O}_L$ in a way simpler than in his unconditional proof.

In 2002, Poonen [24] gave related elliptic curve criterion (with a proof different to the argument of Denef) and applicable in more generality:

Theorem 2.4 *(Poonen). Let L/K be a number field extension and suppose that there is an elliptic curve E/K such that*

$$\mathrm{rk}\, E(L) = \mathrm{rk}\, E(K) = 1.$$

Then L/K is integrally Diophantine.

Specializing to the case $K = \mathbb{Q}$ and motivated by Hilbert's tenth problem, Poonen asked [24] whether it is true that for every L there is an elliptic curve $E/\mathbb{Q}$ with $\mathrm{rk}\, E(L) = \mathrm{rk}\, E(\mathbb{Q}) = 1$. It was later observed by Mazur and Rubin that this would contradict standard parity conjectures on elliptic curves. Nevertheless, in order to show that

$K/\mathbb{Q}$ is integrally Diophantine for every number field K it suffices to verify Poonen's elliptic curve criterion for cyclic extensions of prime degree, and this is precisely what Mazur and Rubin achieve in [18] assuming the squareness conjecture for the 2-torsion part of Shafarevich–Tate groups (which follows from the finiteness conjecture for Shafarevich–Tate groups).

Poonen's criterion was generalized by Cornelissen–Pheidas–Zahidi [3] and later by Shlapentokh (and independently by Poonen) [30] to relax the rank condition. Let us recall here Shlapentokh's version:

Theorem 2.5 *(Shlapentokh). Let L/K be a number field extension and suppose that there is an elliptic curve E/K such that*

$$\operatorname{rk} E(L) = \operatorname{rk} E(K) > 0.$$

Then L/K is integrally Diophantine.

It is this last elliptic curve criterion what we will verify in cyclic extensions of prime degree, under suitable conjectures regarding the L-functions of elliptic curves. In fact, it is very important for our approach that positivity of the rank suffices, rather than the more restrictive requirement that the rank be equal to 1.

3. Automorphic forms and L-functions

We will be interested in the study of L-functions of automorphic elliptic curves, for which we need the language of automorphic representations. The standard reference for the GL_2 theory (which is all we need) is [14]. The article of Gelbart [13] on automorphic elliptic curves is also relevant to our discussion. On the other hand, in this section we also recall the necessary non-vanishing results for quadratic twists of automorphic L-functions.

Let K be a number field and let π be an irreducible cuspidal automorphic representation of $GL_2(\mathbb{A}_K)$, where $\mathbb{A}_K$ denotes the adele ring of K. Let $L(s,\pi)$ be the (completed) L-function attached to π and the standard representation of GL_2. Then $L(s,\pi)$ is entire and satisfies a functional equation

$$L(s,\pi) = \epsilon(s,\pi)L(1-s,\tilde{\pi})$$

where $\tilde{\pi}$ is the contragredient representation of π and $\epsilon(s,\pi)$ is the corresponding global epsilon factor.

Let η be an irreducible automorphic representation of $GL_1(\mathbb{A}_K)$; it is 1-dimensional by Tate's theory. The representation η can be lifted to an automorphic representation of $GL_2(\mathbb{A}_K)$ by composition with the determinant map, so that one obtains an irreducible automorphic representation $\pi \otimes \eta := \pi \otimes (\eta \circ \det)$ of $GL_2(\mathbb{A}_K)$. Let us remark that the contragredient representation is then $(\pi \otimes \eta)^{\sim} = \tilde{\pi} \otimes \eta^{-1}$, and that the local

factors of $L(s, \pi \otimes \eta)$ at all but finitely many places agree with the local factors of the Rankin–Selberg L-function $L(s, \pi \times \eta)$.

Let S be a finite set of places of K and let $\Psi^{sp}(S)$ be the set of (isomorphism classes of) irreducible automorphic representations of $GL_1(\mathbb{A}_K)$ of order 2, unramified at every $v \in S$, with the property that their kernels contain the uniformizer at v for each non-archimedean $v \in S$. The set $\Psi^{sp}(S)$ is infinite and it corresponds, under class field theory, to the set of quadratic extensions of K that are unramified at every $v \in S$, and split at v if $v \in S$ is non-archimedean.

The following non-vanishing results are due to Friedberg and Hoffstein [12]. The case $K = \mathbb{Q}$ is also proved by completely different means by Murty and Murty [20] in the language of modular forms. (The results actually hold for more general choices of congruence conditions than our $\Psi^{sp}(S)$.)

Theorem 3.1. *Let S be a finite set of places of K and let π be a non-self-contragredient cuspidal automorphic representation of $GL_2(\mathbb{A}_K)$. There are infinitely many $\eta \in \Psi^{sp}(S)$ such that*

$$L(1/2, \pi \otimes \eta) \neq 0.$$

Theorem 3.2. *Let S be a finite set of places of K and let π be a self-contragredient cuspidal automorphic representation of $GL_2(\mathbb{A}_K)$. Suppose that there is some $\eta \in \Psi^{sp}(S)$ such that $\epsilon(1/2, \pi \otimes \chi) = 1$. Then there are infinitely many $\omega \in \Psi^{sp}(S)$ such that*

$$L(1/2, \pi \otimes \omega) \neq 0.$$

If E is an elliptic curve defined over K, we let $L(E, s)$ be the completed L-function of E. The automorphy conjecture for elliptic curves is the following (see Gelbart's article [13] for a detailed study of this conjecture):

Conjecture 3.3 *(Automorphy conjecture). If E is an elliptic curve over K, then there is a cuspidal automorphic representation π_E of $GL_2(\mathbb{A}_K)$ satisfying*

$$L(s, E) = L(s - 1/2, \pi_E).$$

Elliptic curves for which this conjecture holds are called *automorphic*. Remarkable progress on the above conjecture has been made for elliptic curves over totally real number fields. The literature on automorphy of elliptic curves in this last setting is constantly growing, but nevertheless, we refer the reader to [11] for some of the most recent developments and for further references.

Let L/K be an abelian extension with Galois group G and let χ vary over the irreducible characters of G. Then one can form the twisted L-functions $L(s, E, \chi)$ by modifying the local factors by $\chi(\mathrm{Frob}_p)$ at unramified places (a more subtle definition

is used at the remaining finitely many places). By comparing local factors, it can be verified that the L-function of the base change of E to L satisfies

$$L(s, E_L) = \prod_{\chi} L(s, E, \chi)$$

where for the trivial character 1, one has $L(s, E, 1) = L(s, E)$.

In the particular case when $[L : K] = 2$ (so that there is only one non-trivial character $\chi = \chi_L$) we have another factorization $L(s, E_L) = L(s, E)L(s, E^L)$ where E^L is the elliptic curve over K defined as the quadratic twist of E by L. Thus, in particular we find in this case that $L(s, E, \chi_L) = L(s, E^L)$.

Now we return to the general case when L/K is abelian. If η_χ denotes the finite order irreducible representation of $GL_1(\mathbb{A}_K)$ obtained from χ by class-field theory by composition with the Artin map, and if E is automorphic, then it follows by a local computation that

$$L(s, E, \chi) = L(s - 1/2, \pi_E \otimes \eta_\chi)$$

which implies that each $L(s, E, \chi)$ (hence, $L(s, E_L)$) extends to an entire function satisfying the appropriate functional equation relating s and $2 - s$.

4. The Birch and Swinnerton–Dyer conjecture

Let K be a number field and E an elliptic curve defined over K. The L-function $L(s, E)$, defined as an Euler product, converges for $\Re(s) > 3/2$. One expects that $L(s, E)$ can be extended to an entire function, in which case it makes sense to consider the vanishing order of it at $s = 1$.

Suppose that E is automorphic, so that analytic continuation holds. The rank part[2] of the Birch and Swinnerton–Dyer conjecture (BSD) asserts that

$$\operatorname{rk} E(K) = \operatorname{ord}_{s=1} L(s, E).$$

Moreover, the automorphic representation π_E is self-contragredient so that the functional equation takes the form

$$L(s, E) = \epsilon(s, E)L(2 - s, E)$$

with $\epsilon(1, E) = \epsilon(1/2, \pi_E) \in \{-1, 1\}$, which is often referred to as the *sign of the functional equation*. It is known that the sign of the functional equation is equal to $w(E)$, the *global root number* of E over K (which can be defined even when E is not automorphic).

[2] There is also a conjectural formula for the first non-zero term in the Taylor expansion – we will not need that part of the BSD conjecture.

Then, in the case of automorphic elliptic curves, the rank part of BSD implies the parity conjecture, which we now recall.

Conjecture 4.1 *(Parity conjecture). Let K be a number field and let E be an elliptic curve over K. Then the global root number satisfies $w(E) = (-1)^{\mathrm{rk}\, E(K)}$.*

(Note that the parity conjecture makes sense even for elliptic curves that are not known to be automorphic.)

Let L/K be a Galois extension of number fields with Galois group G, and let E be an elliptic curve over K. A generalization of the rank part of the BSD, called the *equivariant BSD conjecture*, predicts a relation between the dimensions of the isotypical components of the G-representation $V(E,L) := E(L) \otimes \mathbb{C}$ and the vanishing order at 1 of certain L-functions twisted by irreducible representations. Let us restrict our attention to the case when L/K is *abelian*, in which case the conjecture was proposed by Mazur [17] and we will refer to it as the *twisted BSD conjecture*.

In the abelian case we have a factorization (cf. previous section)

$$L(s, E_L) = \prod_{\chi} L(s, E, \chi)$$

where χ varies over the irreducible characters of G (a similar factorization holds without the abelian hypothesis). If E is automorphic, then each $L(s,E,\chi)$ is automorphic as explained in the previous section, and one can consider their vanishing orders at $s = 1$. On the other hand, we have an isotypical decomposition

$$V(E,L) = \bigoplus_{\chi} V(E,L)^{\chi}.$$

Conjecture 4.2 *(Twisted BSD conjecture). With the previous notation and assumptions, for each χ we have*

$$\dim V(E,L)^{\chi} = \mathrm{ord}_{s=1} L(s,E,\chi).$$

Note that for the trivial character $\chi = 1$ one has $V(E,L)^1 = E(K) \otimes \mathbb{C}$ and $L(s,E,1) = L(s,E)$, so that one recovers the original rank part of BSD. In general, however, it is not known if the rank part of BSD implies the general abelian case of the equivariant BSD.

Conjecture 4.3 *(Twisted analytic rank zero conjecture). Let K be a number field, let L/K be finite abelian with Galois group G, and let E be an automorphic elliptic curve over K. Let χ be an irreducible character of G. Then one has the following implication:*

$$L(1,E,\chi) \neq 0 \Longrightarrow \dim V(E,L)^{\chi} = 0.$$

The twisted analytic rank zero conjecture is certainly more accessible than the full equivariant BSD, and in fact, some important cases are known unconditionally. See for instance [25], [15], [21] and the references therein.

5. Root numbers

The results in the next section will apply to elliptic curves satisfying certain conditions on global root numbers. In this section we will give a supply of such elliptic curves.

First, let us recall the following from [9]:

Lemma 5.1. *Let K be a number field and let E be an elliptic curve defined over K. If K has some real place, or if E does not have potentially good reduction everywhere, then E has some quadratic twist with global root number -1.*

We will also need elliptic curves that acquire negative root number in a fixed quadratic extension.

Lemma 5.2. *Let L/K be a quadratic extension of number fields. There are infinitely many elliptic curves E defined over K such that $w(E \otimes L) = -1$ and having pairwise distinct j-invariants. Moreover, these curves can be taken semi-stable or quadratic twist of semi-stable.*

Proof. Let $\mathfrak{p} \nmid 2$ be a prime of K inert in L/K and let $\mathfrak{P}_L$ be the prime of L above it. Let E be a semi-stable elliptic curve defined over K with multiplicative reduction at $\mathfrak{p}$ and with $v_{\mathfrak{p}}(j_E) < 0$ (so that E does not have potentially good reduction at $\mathfrak{p}$). Such an E exists and can be taken of the form $y^2 + y = x^3 - x^2 + t$ for suitable $t \in \mathcal{O}_K$, see the proof of Lemma 5.4 in [18]; the requirement on j invariants can be achieved in this way. Let M/K be a quadratic extension which is ramified at $\mathfrak{p}$ (call $\mathfrak{P}_M$ the prime of M above $\mathfrak{p}$) and split at each of the following places: primes $\neq \mathfrak{p}$ where E has bad reduction, primes that ramify in L/K, and all places at infinity. (This initial setup for the proof is inspired by the initial choices in the proof of Proposition 6.1 [18].) Let $F = ML$ and note that it is a quadratic extension of M and of L due to the ramification conditions at $\mathfrak{p}$. Moreover, F/L ramifies at $\mathfrak{P}_L$ and we let $\mathfrak{P}_F$ be the only prime above $\mathfrak{P}_L$, so that $\mathfrak{P}_F$ is the only prime above $\mathfrak{p}$ in F/K.

We will show that either $w(E \otimes L) = -1$ or $w(E^M \otimes L) = -1$. This will prove the lemma after replacing E by E^M if necessary.

We have

$$w(E \otimes F) = w(E \otimes M)w((E \otimes M)^F) = w(E \otimes M)w(E^L \otimes M)$$

and by our splitting hypotheses on M/K, we see that local root numbers at primes not dividing $\mathfrak{p}$ cancel-out. Thus we get $w(E \otimes F) = w_{\mathfrak{P}_F}(E \otimes F)$, the local root number at $\mathfrak{P}_F$. Since E has multiplicative (non-potentially good) reduction at $\mathfrak{p}$ and since $\mathfrak{p}$ is inert

in L/K we see that $E\otimes L$ has split multiplicative reduction at $\mathfrak{P}_L$, hence $E\otimes F$ has split multiplicative reduction at $\mathfrak{P}_F$ and we deduce $w_{\mathfrak{P}_F}(E\otimes F)=-1$. Finally, we obtain

$$-1=w(E\otimes F)=w(E\otimes L)w((E\otimes L)^F)=w(E\otimes L)w(E^M\otimes L). \quad \square$$

We remark that the previous lemma does not hold for arbitrary number field extensions. In fact, there are number field extensions L/K of degree 4 for which *each* elliptic curve E/K satisfies $w(E\otimes L)=1$. For instance, $\mathbb{Q}(\sqrt{-1},\sqrt{17})/\mathbb{Q}$ is such an extension. See Remark 7.7 in [18] and see also [9].

6. Elliptic curves retaining their rank

The next lemma is a simple remark, which nevertheless is central to our approach. In fact, it is the technical reason for considering cyclic extensions of prime degree instead of more general abelian extensions.

Lemma 6.1. *Let V be a $\mathbb{Q}$-vector space of finite dimension and let $G\to \mathrm{Aut}_{\mathbb{Q}}(V)$ be a representation of a finite group G of prime order p. All non-trivial irreducible representations of G appear with the same multiplicity in $V_{\mathbb{C}}:=V\otimes\mathbb{C}$.*

Our main result is the following:

Theorem 6.2. *Let L/K be a cyclic extensions of number fields with prime degree p, and let G be the Galois group of L/K. Let E be an elliptic curve over K and suppose that it satisfies the following:*

(i) *If $p=2$ then $w(E\otimes L)=-1$, and if $p>2$ then E has some quadratic twist with global root number -1;*
(ii) *E is automorphic over K;*
(iii) *The quadratic twists of E satisfy the parity conjecture over K;*
(iv) *The quadratic twists of E satisfy the twisted analytic rank zero conjecture (over K) for the non-trivial characters of G.*

Then there are infinitely many quadratic extensions M/K for which the quadratic twist E^M/K satisfies that

$$\mathrm{rk}\, E^M(L)=\mathrm{rk}\, E^M(K)>0.$$

Proof. Let E/K satisfy (i)–(iv). By (i), possibly after replacing E by a suitable quadratic twist we can assume that $w(E)=-1$ (for $p=2$ either E or E^L works) while (i)–(iv) still hold for this new E. Let S be a finite set of places of K containing all archimedean places and all places of bad reduction of E. Let χ be a fixed non-trivial irreducible character

of G. We claim that there are infinitely many quadratic extensions M/K such that the quadratic twist E^M satisfies

(a) $\operatorname{ord}_{s=1} L(s, E^M)$ is odd, and
(b) $L(1, E^M, \chi) \neq 0$.

We need to consider separately the cases when $p = 2$ and $p \geq 3$.

Case $p = 2$. By (i) we have $w(E^L) = 1$. The representation $\pi_E \otimes \eta_\chi = \pi_{E^L}$ is self-contragredient and the sign of the functional equation is $\epsilon(1/2, \pi_{E^L}) = w(E^L) = 1$. Let S be the set consisting of all archimedean places of K and all places of bad reduction of E and E^L. For any $\omega \in \Psi^{sp}(S)$ the corresponding quadratic extension K_ω/K is unramified at all places in S and split at the non-archimedean places of S, so that

$$\epsilon(1/2, \pi_E \otimes \omega) = w(E^{K_\omega}) = w(E) = -1$$

and similarly $\epsilon(1/2, \pi_{E^L} \otimes \omega) = w(E^L) = 1$. The former implies that the choice $M = K_\omega$ satisfies (a), while the latter along with Theorem 3.2 gives that for infinitely many such ω we have that $M = K_\omega$ also satisfies (b), because

$$L(1, E^{K_\omega}, \chi) = L(1/2, \pi_E \otimes \eta_\chi \otimes \omega) = L(1/2, \pi_{E^L} \otimes \omega).$$

Case $p \geq 3$. The representation $\pi_E \otimes \eta_\chi$ is not self-contragredient. In fact, the set of ordinary primes of E has density $1/2$ (CM case, by Deuring) or 1 (non-CM case, by Serre), while the set of primes $\mathfrak{p}$ of K with $\chi(\mathrm{Frob}_\mathfrak{p}) \neq 1$ has density $(p-1)/p \geq 2/3$ by Chebotarev's theorem. Hence there is some prime $\mathfrak{p}$ of K at which the local factors of $L(s, E, \chi)$ and $L(s, E, \chi^{-1})$ are distinct.

Let S be the set consisting of the archimedean places of K and the places of bad reduction for E. Then for each $\omega \in \Psi^{sp}(S)$ we have $\epsilon(1/2, \pi_E \otimes \omega) = w(E^{K_\omega}) = w(E) = -1$ as before, so that (a) is satisfied for any such $M = K_\omega$. By Theorem 3.1 there are infinitely many $\omega \in \Psi^{sp}(S)$ such that

$$L(1, E^{K_\omega}, \chi) = L(1/2, \pi_E \otimes \eta_\chi \otimes \omega) \neq 0.$$

Hence (b) is also satisfied if we let $M = K_\omega$ for any of these infinitely many ω. This proves the claim regarding the existence of infinitely many quadratic extensions M/K satisfying (a) and (b).

Take any of these extensions M/K. By (iii) and (a) we get that $\dim V(E^M, L)^1$ is odd, and by (iv) and (b) we get that $\dim V(E^M, L)^\chi = 0$. By Lemma 6.1 we see that for each non-trivial character ψ of G one has $\dim V(E^M, L)^\psi = 0$, and therefore

$$\operatorname{rk} E^M(L) = \dim V(E^M, L) = \dim V(E^M, L)^1 = \operatorname{rk} E^M(K),$$

which is an odd number. This proves the result. □

Now we deduce the theorem stated in the introduction.

Proof of Theorem 1.2. Let L/k be a cyclic extension of number fields of prime degree. By Lemmas 5.1 and 5.2, there is an elliptic curve E/k satisfying condition (i) in Theorem 6.2. Condition (ii) holds under the automorphy conjecture, and conditions (ii) and (iii) are part of our assumptions. Hence, under the assumptions of Theorem 1.2, from Theorem 6.2 we get a suitable quadratic twist E^M of E such that

$$\operatorname{rk} E^M(L) = \operatorname{rk} E^M(k) > 0.$$

By Theorem 2.5 this implies that L/k is integrally Diophantine. As this holds for every such an extension L/k, Proposition 2.3 gives that every Galois extension $F/\mathbb{Q}$ is integrally Diophantine. Given an arbitrary number field K, we apply this to F the normal closure of K, hence $K/\mathbb{Q}$ is integrally Diophantine by Proposition 2.2. In particular, $H10(\mathcal{O}_K)$ is undecidable. □

Actually, the previous argument gives a slightly stronger result which we record here for the convenience of the reader:

Theorem 6.3. *Let L/K be a Galois extension of number fields. Suppose that for every intermediate field $L \supseteq F \supseteq K$ properly contained in L, the following conjectures hold for all elliptic curves E defined over F:*

- *the automorphy conjecture,*
- *the parity conjecture, and*
- *the analytic rank zero twisted BSD conjecture, for prime order characters.*

Then L/K is integrally Diophantine. In particular, if $H10(K)$ is undecidable, then so is $H10(L)$.

7. Cyclic extensions of totally real number fields

In this section we consider cyclic extensions of prime degree of totally real fields. In this case, some conditions in our results can be relaxed and the resulting statements can be of arithmetic interest. However, no new consequence for Hilbert's tenth problem is deduced in this setting, because if K is totally real and L/K is cyclic of prime degree p, then either L is CM (this can only happen if $p = 2$) or totally real, and $H10(\mathcal{O}_L)$ is known to be undecidable in those cases (cf. Section 2).

Note that the part regarding vanishing order of L-functions (i.e. analytic ranks) in the following result is *unconditional*.

Theorem 7.1. *Let K be a totally real number field or $\mathbb{Q}$, and let L/K be a cyclic extension of prime degree p. There are infinitely many elliptic curves E/K, each having infinitely*

many quadratic twists E^M, such that $L(s, E^M)$ and $L(s, E^M \otimes L)$ are entire and such that

$$\mathrm{ord}_{s=1} L(s, E^M \otimes L) = \mathrm{ord}_{s=1} L(s, E^M)$$

is odd (hence, positive).

Furthermore, if $p > 2$ and $[K : \mathbb{Q}] \leq 2$ then every elliptic curve E/K has infinitely quadratic twists as before. Moreover, if $K = \mathbb{Q}$ and if we assume the parity conjecture for elliptic curves over $\mathbb{Q}$, then in the same cases we obtain $\mathrm{rk}\, E^M(L) = \mathrm{rk}\, E^M(\mathbb{Q}) > 0$.

Proof. Let E/K be an elliptic curve satisfying condition (i) in Theorem 6.2; when $p > 2$ any E/K works, and in general we know that there are infinitely many such E with distinct j-invariants. Then (ii) holds for $K = \mathbb{Q}$ by the modularity theorem of Wiles [32], Taylor–Wiles [31], and Breuil–Conrad–Diamond–Taylor [1]; in the case of K real quadratic (ii) holds by work of Freitas, Le Hung and Siksek [11]. In the general case of K totally real, (ii) can only fail for finitely many j-invariants, see [11].

Moreover, when $K = \mathbb{Q}$ we also have that (iv) holds by a result of Kato [15].

Fix χ an irreducible non-trivial character of $G = \mathrm{Gal}(L/\mathbb{Q})$. The arguments of the previous section give infinitely many quadratic twists E^M for which $\mathrm{ord}_{s=1} L(s, E^M)$ is odd and $L(s, E^M, \chi) \neq 0$. The L-functions of automorphic elliptic curves over totally real fields correspond to L-functions of Hilbert modular forms, so by general results of Shimura [27] one sees that actually $L(s, E^M, \psi) \neq 0$ for each ψ irreducible non-trivial character of G (because they are Galois conjugate to χ). Hence

$$\mathrm{ord}_{s=1} L(s, E^M \otimes L) = \mathrm{ord}_{s=1} L(s, E^M),$$

which is an odd positive integer. Furthermore, since (iv) holds for $K = \mathbb{Q}$, one obtains that in this case $\dim V(E^M, L)^\psi = 0$ for each irreducible non-trivial ψ, hence $\mathrm{rk}\, E^M(L) = \mathrm{rk}\, E^M(\mathbb{Q})$, and the claim regarding the parity conjecture follows. □

Note that it follows that for K real quadratic or $\mathbb{Q}$ and for cyclic extensions L/K of odd prime degree, *every* elliptic curve over K is expected to have infinitely many quadratic twists with positive rank preserved under base change to L. We believe this to be the case whenever K is replaced by a number field having some real place; observe that this is supported (conditionally) by Theorem 6.2 and Lemma 5.1.

For the sake of completeness of our discussion on cyclic extensions of totally real number fields, let us record here a result of Mazur and Rubin which is implicit in their work [18]. First, one can see that in [18], the assumption of squareness of $Ш_E[2]$ can be replaced by the assumption of both the 2-parity conjecture and the parity conjecture; this was explained to us by Karl Rubin. Using the available results on the 2-parity conjecture, this gives:

Theorem 7.2 *(Mazur–Rubin). Let K be a totally real number field, and let L/K be a cyclic extension of prime degree p. Assume that the parity conjecture holds. Then there exist elliptic curves E/K such that* $\operatorname{rk} E(L) = \operatorname{rk} E(K) = 1$.

Proof. In [18] it is proved (unconditionally) that there are elliptic curves E/K with the property that $\dim_{\mathbb{F}_2} \mathrm{Sel}_2(E) = 1$ and $\operatorname{rk} E(L) = \operatorname{rk} E(K)$ (cf. Theorem 6.2 and Corollary 7.6 in [18]). The elliptic curves produced in the proof have trivial K-rational 2-torsion and non-integral j-invariant, hence one has (cf. (2) in [18])

$$r_2(E) := \operatorname{corank}_{\mathbb{Z}_2} \mathrm{Sel}_{2^\infty}(E) \equiv \dim_{\mathbb{F}_2} \mathrm{Sel}_2(E) \mod 2.$$

Since the p-parity conjecture is proved for elliptic curves over totally real fields with non-integral j-invariant [22], we deduce $w(E) = (-1)^{r_2(E)} = -1$. Under the assumption of the parity conjecture, we obtain that $\operatorname{rk} E(K)$ is odd. From the injectivity of the map $E(K)/2E(K) \to \mathrm{Sel}_2(E)$ and the fact that the 2-torsion of $E(K)$ is trivial, we get the result. □

8. Final comments

Assuming the relevant conjectures required in our work and in [18], let us briefly give a more detailed discussion on the *conditional* arithmetic consequences for elliptic curves. For this, let K be a number field, L/K a cyclic extension of prime degree p and let E be an elliptic curve defined over K.

First, we are concerned with the existence of a suitable quadratic extension F/K such that the twist E^F of E satisfies

$$\operatorname{rk} E^F(K) = \operatorname{rk} E^F(L) > 0 \tag{1}$$

while in [18] the more precise condition

$$\operatorname{rk} E^F(K) = \operatorname{rk} E^F(L) = 1 \tag{2}$$

is considered. Our results apply to a larger class of elliptic curves than those in [18], since our approach does not require $E(K)[2] = 0$ (unlike [18]); in fact, when K has some real place our approach predicts that *every* E defined over K has infinitely many quadratic twists satisfying (1), as explained in the previous section. On the other hand, our approach only shows the existence of infinitely many twists satisfying (1), while in [18] they give a lower bound for the number of twists satisfying (2) (with conductor up to a given bound) for the elliptic curves E/K to which their results apply.

Finally, we would like to make some remarks in the direction of unconditional arithmetic results. From the discussion in the previous section, one can see that the main obstruction to obtaining unconditional results where (1) or (2) are satisfied (using our approach or the results of [18]), is the *parity conjecture*. The current state-of-the-art on

the parity conjecture is the work of Dokchitser–Dokchitser [10], which is conditional to the finiteness of the 2-primary and 3-primary parts of the Shafarevich–Tate group of elliptic curves. Following a different path, we would like to suggest a possible analytic approach to relax the assumption of the parity conjecture in our work. The question seems to be closely related to the problem of estimating averages of central values of L-functions for automorphic representations of GL_4 (which is admittedly hard). In fact, a better understanding of the latter subject should lead to non-vanishing theorems for simultaneous twists of two L-functions for automorphic representations of GL_2, cf. p. 169 in [2]. This technical tool would give a version of our results where the analytic counterpart of (1) is replaced by the analytic counterpart of (2). Thus, it would suffice to assume the rank part of the BSD conjecture for analytic rank 1 instead of the parity conjecture. This is relevant because the rank part of BSD for analytic rank ≤ 1 has been proved unconditionally in several important cases, see for instance [33].

Acknowledgments

We would like to express our gratitude to Bjorn Poonen for asking a question that led us to initiate this research project. We thank Barry Mazur and Karl Rubin for explaining us the relation of their work with the parity conjecture and the 2-parity conjecture, and for allowing us to include here Theorem 7.2 (see above). We also thank Shou-Wu Zhang for helpful discussions regarding the existing results on the BSD conjecture, and Alexandra Shlapentokh for valuable feedback on a previous version of this manuscript.

M.R.M. was partially supported by an NSERC Discovery grant. H.P. was partially supported by a Benjamin Peirce Fellowship at Harvard, and by a Schmidt Fellowship and the National Science Foundation agreement No. DMS-1128155 at the Institute for Advanced Study. Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

References

[1] C. Breuil, B. Conrad, F. Diamond, R. Taylor, On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises, J. Amer. Math. Soc. 14 (4) (2001) 843–939.
[2] D. Bump, S. Friedberg, J. Hoffstein, On some applications of automorphic forms to number theory, Bull. Amer. Math. Soc. (N.S.) 33 (2) (1996) 157–175.
[3] G. Cornelissen, T. Pheidas, K. Zahidi, Division-ample sets and the Diophantine problem for rings of integers, J. Théor. Nombres Bordeaux 17 (3) (2005) 727–735.
[4] M. Davis, H. Putnam, J. Robinson, The decision problem for exponential Diophantine equations, Ann. of Math. (2) 74 (1961) 425–436.
[5] J. Denef, Hilbert's tenth problem for quadratic rings, Proc. Amer. Math. Soc. 48 (1975) 214–220.
[6] J. Denef, The Diophantine problem for polynomial rings and fields of rational functions, Trans. Amer. Math. Soc. 242 (1978) 391–399.
[7] J. Denef, Diophantine sets over algebraic integer rings. II, Trans. Amer. Math. Soc. 257 (1) (1980) 227–236.
[8] J. Denef, L. Lipshitz, Diophantine sets over some rings of algebraic integers, J. Lond. Math. Soc. (2) 18 (3) (1978) 385–391.

[9] T. Dokchitser, V. Dokchitser, Elliptic curves with all quadratic twists of positive rank, Acta Arith. 137 (2) (2009) 193–197.
[10] T. Dokchitser, V. Dokchitser, Root numbers and parity of ranks of elliptic curves, J. Reine Angew. Math. 658 (2011) 39–64 (English summary).
[11] N. Freitas, B. Le Hung, S. Siksek, Elliptic curves over real quadratic fields are modular, Invent. Math. 201 (1) (2015) 159–206 (English summary).
[12] S. Friedberg, J. Hoffstein, Nonvanishing theorems for automorphic L-functions on $GL(2)$, Ann. of Math. (2) 142 (2) (1995) 385–423.
[13] S. Gelbart, Elliptic curves and automorphic representations, Adv. Math. 21 (3) (1976) 235–292.
[14] H. Jacquet, R. Langlands, Automorphic Forms on $GL(2)$, Lecture Notes in Math., vol. 114, Springer-Verlag, Berlin–New York, 1970, vii+548 pp.
[15] K. Kato, p-adic Hodge theory and values of zeta functions of modular forms, in: Cohomologies p-Adiques et Applications Arithmétiques. III, Astérisque 295 (2004) 117–290 (English, French summary).
[16] J. Matijasevich, The Diophantineness of enumerable sets, Dokl. Akad. Nauk SSSR 191 (1970) 279–282 (in Russian).
[17] B. Mazur, Modular curves and arithmetic, in: Proceedings of the International Congress of Mathematicians, vols. 1, 2, Warsaw, 1983, PWN, Warsaw, 1984, pp. 185–211.
[18] B. Mazur, K. Rubin, Ranks of twists of elliptic curves and Hilbert's tenth problem, Invent. Math. 181 (3) (2010) 541–575.
[19] K. Murty, R. Murty, Mean values of derivatives of modular L-series, Ann. of Math. (2) 133 (3) (1991) 447–475.
[20] K. Murty, R. Murty, Non-vanishing of L-Functions and Applications, Progr. Math., vol. 157, Birkhäuser Verlag, Basel, ISBN 3-7643-5801-7, 1997, xii+196 pp. (English summary).
[21] J. Nekovar, Level raising and anticyclotomic Selmer groups for Hilbert modular forms of weight two, Canad. J. Math. 64 (3) (2012) 588–668.
[22] J. Nekovar, Some consequences of a formula of Mazur and Rubin for arithmetic local constants, Algebra Number Theory 7 (5) (2013) 1101–1120 (English summary).
[23] T. Pheidas, Hilbert's tenth problem for a class of rings of algebraic integers, Proc. Amer. Math. Soc. 104 (2) (1988) 611–620.
[24] B. Poonen, Using elliptic curves of rank one towards the undecidability of Hilbert's tenth problem over rings of algebraic integers, in: Algorithmic Number Theory, Sydney, 2002, in: Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, pp. 33–42.
[25] K. Rubin, Elliptic curves with complex multiplication and the conjecture of Birch and Swinnerton–Dyer, Invent. Math. 64 (3) (1981) 455–470.
[26] H. Shapiro, A. Shlapentokh, Diophantine relationships between algebraic number fields, Comm. Pure Appl. Math. 42 (8) (1989) 1113–1122.
[27] G. Shimura, The special values of the zeta functions associated with Hilbert modular forms, Duke Math. J. 45 (3) (1978) 637–679.
[28] A. Shlapentokh, Extension of Hilbert's tenth problem to some algebraic number fields, Comm. Pure Appl. Math. 42 (7) (1989) 939–962.
[29] A. Shlapentokh, Hilbert's Tenth Problem. Diophantine Classes and Extensions to Global Fields, New Math. Monogr., vol. 7, Cambridge University Press, Cambridge, 2007, xiv+320 pp. ISBN: 978-0-521-83360-8; 0-521-83360-4.
[30] A. Shlapentokh, Elliptic curves retaining their rank in finite extensions and Hilbert's tenth problem for rings of algebraic numbers, Trans. Amer. Math. Soc. 360 (7) (2008) 3541–3555.
[31] R. Taylor, A. Wiles, Ring-theoretic properties of certain Hecke algebras, Ann. of Math. (2) 141 (3) (1995) 553–572.
[32] A. Wiles, Modular elliptic curves and Fermat's last theorem, Ann. of Math. (2) 141 (3) (1995) 443–551.
[33] S. Zhang, Heights of Heegner points on Shimura curves, Ann. of Math. (2) 153 (1) (2001) 27–147.