Bull. Aust. Math. Soc. **107** (2023), 440–450
doi:10.1017/S000497272200082X

REMARKS ON HILBERT'S TENTH PROBLEM AND THE IWASAWA THEORY OF ELLIPTIC CURVES

ANWESH RAY

(Received 13 June 2022; accepted 6 July 2022; first published online 30 August 2022)

Abstract

Let E be an elliptic curve with positive rank over a number field K and let p be an odd prime number. Let K_{cyc} be the cyclotomic $\mathbb{Z}_p$-extension of K and K_n its nth layer. The Mordell–Weil rank of E is said to be *constant* in the cyclotomic tower of K if for all n, the rank of $E(K_n)$ is equal to the rank of $E(K)$. We apply techniques in Iwasawa theory to obtain explicit conditions for the rank of an elliptic curve to be constant in this sense. We then indicate the potential applications to Hilbert's tenth problem for number rings.

2020 *Mathematics subject classification*: primary 11R23; secondary 11G05, 11U05.

Keywords and phrases: Hilbert's tenth problem, Iwasawa theory, elliptic curves, variation of Mordell–Weil ranks in towers of number fields.

1. Introduction

Hilbert's tenth problem for $\mathbb{Z}$ states that there is no Turing machine that takes as input polynomial equations over $\mathbb{Z}$ and decides whether they have nontrivial solutions. Matiyasevich [10] resolved Hilbert's tenth problem over $\mathbb{Z}$. It is well known that if $\mathbb{Z}$ is Diophantine as a subset of $\mathcal{O}_K$, then the analogue of Hilbert's tenth problem has a negative solution over $\mathcal{O}_K$. The following conjecture is due to Denef and Lipschitz [3].

CONJECTURE 1.1 (Denef–Lipshitz). For every number field K, $\mathbb{Z}$ is a Diophantine subset of $\mathcal{O}_K$.

There are various special cases in which the above conjecture has been resolved. Conjecture 1.1 is known to be true for all number fields K such that:

- K is either totally real or a quadratic extension of a totally real number field (see [2, 3]);
- K has exactly one complex place (see [14, 18, 21]);
- $K/\mathbb{Q}$ is abelian (see [17]).

It is natural to study the validity of Conjecture 1.1 for naturally occurring families of number fields K. For instance, Garcia-Fritz and Pasten [4] proved the conjecture for

number fields of the form $\mathbb{Q}(p^{1/3}, \sqrt{-q})$, where p and q range through certain explicit sets of primes of positive Dirichlet density. In this paper, we study Conjecture 1.1 for certain towers of number field extensions of a fixed number field K. More precisely, let K be a number field and p be an odd prime number. Let K_{cyc} denote the *cyclotomic* $\mathbb{Z}_p$*-extension* of K. The unique subfield of K_{cyc} that is of degree p^n over K is denoted by K_n and is called the nth *layer*.

Iwasawa studied the growth of the p-primary part of the class group of K_n as a function of n (see [7]). In Section 3, we prove that O_K is a Diophantine subset of O_{K_n} for all n, provided there exists an elliptic curve $E_{/K}$ satisfying certain specific additional conditions (see Theorem 3.6). It follows from this that if Conjecture 1.1 is satisfied for K, then it is satisfied for K_n for all n.

In Section 4, we fix an elliptic curve $E_{/\mathbb{Q}}$ of positive Mordell–Weil rank and also fix a number field K. We provide circumstantial evidence to show that there is a set of primes p of positive lower density for which the conditions of Theorem 3.6 are satisfied. This expectation (Conjecture 4.1) is based on computational evidence for the behaviour of the *p-adic regulator* of an elliptic curve.

2. Preliminaries and notation

The contents of this section are preliminary in nature. In Section 2.1, we introduce the notion of an *integrally Diophantine extension* of number rings and its applications to Hilbert's tenth problem for number fields. In Section 2.2, we recall basic concepts from the Iwasawa theory of elliptic curves.

2.1. Integrally Diophantine extensions. Let A be a commutative ring and $n > 0$ be an integer. Let A^n be a free A-module of rank n consisting of elements of the form $a = (a_1, \ldots, a_n)$, with entries $a_i \in A$. For $m \geq 0$, $a = (a_1, \ldots, a_n) \in A^n$, $b = (b_1, \ldots, b_m) \in A^m$, the element $(a, b) \in A^{n+m}$ is given by $(a_1, \ldots, a_n, b_1, \ldots, b_m)$. Given a set of polynomials $F_1, \ldots, F_k \in A[x_1, \ldots, x_n, y_1, \ldots, y_m]$ and $a \in A^n$, set

$$\mathcal{F}(a; F_1, \ldots, F_k) := \{b \in A^m \mid F_i(a, b) = 0 \text{ for } 1 \leq i \leq k\}.$$

Given a number field K, denote by O_K its ring of integers.

DEFINITION 2.1. Let S be a subset of A^n. The set S is *Diophantine* in A^n if for some $m \geq 0$, there are polynomials $F_1, \ldots, F_k \in A[x_1, \ldots, x_n, y_1, \ldots, y_m]$ such that

$$S = \{a \in A^n \mid \mathcal{F}(a; F_1, \ldots, F_k) \text{ is not empty}\}.$$

An extension of number fields L/K is said to be integrally Diophantine if O_K is a Diophantine subset of O_L.

It follows from standard arguments that if $L/\mathbb{Q}$ is an integrally Diophantine extension of number fields, then Hilbert's tenth problem has a negative answer for O_L (see [3, page 385]). Moreover, if L/F and F/K are integrally Diophantine extensions of number fields, then so is L/K.

https://doi.org/10.1017/S000497272200082X Published online by Cambridge University Press

We recall Shlapentokh's criterion for an extension of number fields to be integrally Diophantine.

THEOREM 2.2 (Shlapentokh [19]). *Let L/K be an extension of number fields. Suppose there is an elliptic curve $E_{/K}$ such that* $\operatorname{rank} E(L) = \operatorname{rank} E(K) > 0$. *Then, L/K is an integrally Diophantine extension.*

2.2. Iwasawa theory of elliptic curves. Fix an algebraic closure $\bar{\mathbb{Q}}$ of $\mathbb{Q}$. Let p be an odd prime number and K be a number field. Throughout, $\mathbb{Z}_p$ is the ring of p-adic integers. Let E be an elliptic curve defined over K with good ordinary reduction at the primes above p. Denote by μ_{p^n} the group of p^nth roots of unity in $\bar{\mathbb{Q}}$, and set $\mu_{p^\infty} = \bigcup_n \mu_{p^n}$. We denote by $K(\mu_{p^n})$ (respectively $K(\mu_{p^\infty})$) the cyclotomic extension of K in $\bar{\mathbb{Q}}$ generated by μ_{p^n} (respectively μ_{p^∞}). The *cyclotomic $\mathbb{Z}_p$-extension* of K is the unique $\mathbb{Z}_p$-extension of K which is contained in $K(\mu_{p^\infty})$ and is denoted by K_{cyc}. Given a number field extension $\mathcal{F}$ of K, let $\mathrm{Sel}_{p^\infty}(E/\mathcal{F})$ denote the p-primary Selmer group of E over $\mathcal{F}$ (see [1, page 9] for the definition).

We let $Ш(E/K)$ denote the Tate–Shafarevich group of E over K and $Ш(E/K)[p^\infty]$ its p-primary part. The p-primary Selmer group fits into a short exact sequence:

$$0 \to E(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to \mathrm{Sel}_{p^\infty}(E/K) \to Ш(E/K)[p^\infty] \to 0. \tag{2.1}$$

Note that $\mathrm{Sel}_{p^\infty}(E/\mathcal{F})$ is a module over $\mathbb{Z}_p[G]$, when $\mathcal{F}$ is a finite Galois extension of K with Galois group $G = \mathrm{Gal}(\mathcal{F}/K)$. For $n \geq 0$, let K_n be the unique extension of K in K_{cyc} such that $\mathrm{Gal}(K_n/K) \simeq \mathbb{Z}/p^n\mathbb{Z}$. The Selmer group of E over K_{cyc} is taken to be the natural direct limit with respect to restriction maps

$$\mathrm{Sel}_{p^\infty}(E/K_{\mathrm{cyc}}) := \varinjlim_n \mathrm{Sel}_{p^\infty}(E/K_n).$$

Setting $\Gamma := \mathrm{Gal}(K_{\mathrm{cyc}}/K)$, note that $\Gamma^{p^n} = \mathrm{Gal}(K_{\mathrm{cyc}}/K_n)$. The Iwasawa algebra is the completed group ring

$$\Lambda(\Gamma) := \varprojlim_n \mathbb{Z}_p[\Gamma/\Gamma^{p^n}].$$

Let $\mathbb{Z}_p[\![T]\!]$ denote the formal power series ring over $\mathbb{Z}_p$ in the variable T. Fix a topological generator γ of Γ and consider the isomorphism $\Lambda(\Gamma) \simeq \mathbb{Z}_p[\![T]\!]$ sending $\gamma - 1$ to the formal variable T. The Selmer group $\mathrm{Sel}_{p^\infty}(E/K_{\mathrm{cyc}})$ is naturally a module over the Iwasawa algebra $\Lambda(\Gamma)$.

Given a module M over $\Lambda(\Gamma)$, let $M^\vee = \mathrm{Hom}_{\mathbb{Z}_p}(M, \mathbb{Q}_p/\mathbb{Z}_p)$ be its Pontryagin dual. It is conjectured by Mazur that the dual Selmer group $\mathrm{Sel}_{p^\infty}(E/K_{\mathrm{cyc}})^\vee$ is a finitely generated and torsion module over Λ. This is known to be true in the following special cases:

(1) the p-primary Selmer group $\mathrm{Sel}_{p^\infty}(E/K)$ (over K) is finite (see [1, Theorem 2.8]);
(2) K is an abelian extension of $\mathbb{Q}$. (This is a result of Kato [8] and [6, Theorem 2.2]. Rubin proved the result for CM elliptic curves.)

https://doi.org/10.1017/S000497272200082X Published online by Cambridge University Press

We say that a polynomial in $\mathbb{Z}_p[\![T]\!]$ is distinguished if it is monic and all its nonleading coefficients are divisible by p. A map of $\mathbb{Z}_p[\![T]\!]$-modules $M_1 \to M_2$ is said to be a *pseudo-isomorphism* if the kernel and cokernel have finite cardinality. One associates a characteristic element and Iwasawa invariants to a finitely generated and torsion module M over $\Lambda(\Gamma)$ as follows. By the structure theorem of finitely generated and torsion $\mathbb{Z}_p[\![T]\!]$-modules (see [22, Ch. 13]), there is a pseudo-isomorphism

$$M \longrightarrow \Big(\bigoplus_{j=1}^{t} \frac{\mathbb{Z}_p[\![T]\!]}{(f_j)} \Big),$$

where $f_1, \ldots, f_t$ are nonzero elements of $\mathbb{Z}_p[\![T]\!]$. The characteristic element is the product $\prod_j f_j$ and is denoted by $f_M(T)$. It is well defined up to multiplication by a unit in $\mathbb{Z}_p[\![T]\!]$. According to the Weierstrass preparation theorem, we may factor $f_M(T)$ as $p^{\mu}P(T)u(T)$, where $\mu \geq 0$, $P(T)$ is a distinguished polynomial and $u(T)$ is a unit in $\mathbb{Z}_p[\![T]\!]$. The Iwasawa μ invariant $\mu(M)$ is the quantity μ that appears in this factorisation. The λ-invariant $\lambda(M)$ is the degree of the polynomial $P(T)$.

Assume that Mazur's conjecture is satisfied for the Selmer group of E over K^{cyc}, that is, $\mathrm{Sel}_{p^\infty}(E/K^{\mathrm{cyc}})^\vee$ is finitely generated and torsion as a $\Lambda(\Gamma)$-module. Then, we denote by $\mu_p(E/K)$ and $\lambda_p(E/K)$ the associated μ and λ-invariants for the dual Selmer group $\mathrm{Sel}_{p^\infty}(E/K^{\mathrm{cyc}})^\vee$.

PROPOSITION 2.3. *Let E be an elliptic curve over a number field K and let p be an odd prime number. Assume that:*

(1) *E has good ordinary reduction at all primes $v \mid p$ of K;*
(2) *the dual Selmer group $\mathrm{Sel}_{p^\infty}(E/K^{\mathrm{cyc}})^\vee$ is a finitely generated and torsion module over $\Lambda(\Gamma)$.*

Then, $\operatorname{rank} E(K_n) \leq \lambda_p(E/K)$ *for all $n \geq 0$. In particular,* $\operatorname{rank} E(K_n)$ *is bounded as $n \to \infty$.*

PROOF. From (2.1), we arrive at

$$\operatorname{rank} E(K_n) \leq \operatorname{rank}_{\mathbb{Z}_p}(\mathrm{Sel}_{p^\infty}(E/K^n)^\vee).$$

According to [5, Theorem 1.9],

$$\operatorname{rank}_{\mathbb{Z}_p}(\mathrm{Sel}_{p^\infty}(E/K^n)^\vee) \leq \lambda_p(E/K),$$

provided $\mathrm{Sel}_{p^\infty}(E/K^{\mathrm{cyc}})^\vee$ is finitely generated and torsion as a module over $\Lambda(\Gamma)$. The result follows. □

3. Hilbert's tenth problem in the cyclotomic $\mathbb{Z}_p$-extension of a number field

3.1. Rank constancy in cyclotomic towers. We shall study the following property in the context of the cyclotomic $\mathbb{Z}_p$-extension of a number field K.

DEFINITION 3.1. Let K be a number field and p be a prime number. Let K_∞ be an infinite pro-p extension of K. We say that K is integrally Diophantine in K_∞ if for all

https://doi.org/10.1017/S000497272200082X Published online by Cambridge University Press

intermediate number fields L such that $K \subseteq L \subseteq K_\infty$, the extension L/K is integrally Diophantine.

We specialise the above notion to $K_\infty = K_{\mathrm{cyc}}$. Thus, K is integrally Diophantine in K_{cyc} precisely when K_n/K is an integrally Diophantine extension for all $n \geq 0$. Thus, if $K/\mathbb{Q}$ is integrally Diophantine and K_{cyc}/K is integrally Diophantine, then it will follow that $K_n/\mathbb{Q}$ is intergrally Diophantine for all n. In particular, this shall imply that Hilbert's tenth problem has a negative solution for the ring of integers of all number fields K_n in the infinite cyclotomic tower.

We shall use methods from the Iwasawa theory of elliptic curves to derive conditions for a number field K to be integrally Diophantine in K^{cyc}.

PROPOSITION 3.2. *Let E be an elliptic curve over a number field K and let p be an odd prime number. Assume that:*

(1) $\operatorname{rank} E(K) > 0$;
(2) *E has good ordinary reduction at all primes $v \mid p$ of K;*
(3) *the dual Selmer group $\mathrm{Sel}_{p^\infty}(E/K^{\mathrm{cyc}})^\vee$ is a finitely generated and torsion module over $\Lambda(\Gamma)$.*

Then, there is a value $n_0 \geq 0$ such that for all $n \geq n_0$, K_n/K_{n_0} is an integral Diophantine extension. Thus, the extension K_{cyc}/K_{n_0} is integrally Diophantine in the sense of Definition 3.1 and, if Conjecture 1.1 is satisfied for K_{n_0}, then it is satisfied for K_n for all $n \geq n_0$.

PROOF. According to Proposition 2.3, we find that $\operatorname{rank} E(K_n)$ is bounded as a function of n. Therefore, there exists $n_0 \geq 0$ such that $\operatorname{rank} E(K_n) = \operatorname{rank} E(K_{n_0})$ for all $n \geq n_0$. The result follows from Theorem 2.2. □

THEOREM 3.3. *Let p be an odd prime and E an elliptic curve over a number field K with good ordinary reduction at all primes $v \mid p$. Assume that $\mathrm{Sel}_{p^\infty}(E/K_{\mathrm{cyc}})^\vee$ is finitely generated and torsion as a module over $\Lambda(\Gamma)$ as conjectured by Mazur. Suppose that*

$$\lambda_p(E/K) = \operatorname{rank} E(K) > 0.$$

Then, for all $n \geq 0$, K_n/K is a Diophantine extension. Therefore, if Conjecture 1.1 is satisfied for K, then it is satisfied for K_n for all $n \geq 0$.

PROOF. Suppose K_n/K is an integral Diophantine extension and $K/\mathbb{Q}$ is an integral Diophantine extension. Then, $K_n/\mathbb{Q}$ is an integral Diophantine extension and thus Hilbert's tenth problem is negative for $\mathcal{O}_{K_n}$. We show that the above hypotheses imply that K_n/K is an integral Diophantine extension for all $n \geq 0$.

According to Proposition 2.3, $\operatorname{rank} E(K_n) \leq \lambda_p(E/K)$. Since it is assumed that $\operatorname{rank} E(K) = \lambda_p(E/K) > 0$, it follows that

$$\operatorname{rank} E(K_n) = \operatorname{rank} E(K) > 0.$$

Therefore, by Theorem 2.2, K_n/K is an integral Diophantine extension for all $n \geq 0$. □

https://doi.org/10.1017/S000497272200082X Published online by Cambridge University Press

3.2. An Euler characteristic formula. Let E be an elliptic curve over a number field K and let p be a prime number. Assume that E has good ordinary reduction at all primes of K that lie above p. Assume that the dual Selmer group $\mathrm{Sel}_{p^\infty}(E/K_{\mathrm{cyc}})^\vee$ is a finitely generated torsion $\Lambda(\Gamma)$-module and denote by $f_{E,p}(T)$ its characteristic element. Note that $f_{E,p}(T)$ is well defined up to multiplication by a unit in $\Lambda(\Gamma)$. We may express $f_{E,p}(T)$ as a formal power series in T:

$$f_{E,p}(T) = \sum_{i=r}^{\infty} a_i T^i,$$

where $a_r \neq 0$. The quantity $r \geq 0$ is the order of vanishing of $f_{E,p}(T)$ at zero, thus we may denote it by $\mathrm{ord}_{T=0} f_{E,p}(T)$. We call a_r the leading coefficient. Perrin-Riou [13] and Schneider [16] provide an explicit formula for the leading coefficient a_r. Note that a_r is well defined up to a unit in $\mathbb{Z}_p$. Given two elements $a, b \in \mathbb{Q}_p$, we write $a \sim b$ to mean that $a = ub$ for a unit $u \in \mathbb{Z}_p^\times$. The p-adic regulator $\mathcal{R}_p(E/K)$ is the determinant of the p-adic height pairing on the Mordell–Weil group of E (see [11, 15, 16] for further details). Schneider has conjectured that the p-adic regulator $\mathcal{R}_p(E/K)$ is always nonzero, that is, the p-adic height pairing is always nondegenerate. Let $R_p(E/K)$ be the normalised p-adic regulator, defined by $R_p(E/K) := p^{-\operatorname{rank} E(K)}\mathcal{R}_p(E/K)$. At each prime v of K, let $c_v(E/K)$ be the Tamagawa number of E at v (see [1, Ch. 3] for the definition). If v is a prime at which E has good reduction, then $c_v(E/K) = 1$. At any prime v of K, let $\mathbb{F}_v$ denote the residue field of $\mathcal{O}_v$ at v. For each prime $v \mid p$, let $\widetilde{E}$ be the reduction of E to an elliptic curve over $\mathbb{F}_v$.

THEOREM 3.4 (Perrin-Riou, Schneider). *Let E be an elliptic curve over a number field K and p an odd prime. Assume that the following conditions are satisfied:*

(1) *E has good ordinary reduction at all primes $v \mid p$ of K;*
(2) *$Ш(E/K)[p^\infty]$ is finite;*
(3) *$\mathcal{R}_p(E/K)$ is nonzero;*
(4) *$\mathrm{Sel}_{p^\infty}(E/K_{\mathrm{cyc}})^\vee$ is finitely generated and torsion as a $\Lambda(\Gamma)$-module.*

Then, the following assertions hold:

(1) *$r := \mathrm{ord}_{T=0} f_{E,p}(T) = \operatorname{rank} E(K)$;*
(2) *the leading coefficient is given up to a unit by*

$$a_r \sim \frac{R_p(E/K) \times \#Ш(E/K)[p^\infty] \times \prod c_v(E/K) \times (\prod_{v|p} \#\widetilde{E}(\mathbb{F}_v)[p^\infty])^2}{(\#E(K)[p^\infty])^2}.$$

PROOF. The above result is [16, Theorem 2′, page 342]. □

LEMMA 3.5. *Let E be an elliptic curve satisfying the conditions of Theorem 3.4 and set $r := \mathrm{ord}_{T=0} f_{E,p}(T) = \operatorname{rank} E(K)$. The following conditions are equivalent:*

(1) *a_r is a unit in $\mathbb{Z}_p$;*
(2) *$\mu_p(E/K) = 0$ and $\lambda_p(E/K) = \operatorname{rank} E(K)$.*

https://doi.org/10.1017/S000497272200082X Published online by Cambridge University Press

PROOF. We write $f_{E,p}(T)$ as $T^r g(T)$, where $g(0) = a_r \neq 0$. Suppose that a_r is a unit in $\mathbb{Z}_p$. Then, $g(T)$ is a unit in $\Lambda(\Gamma)$ and the Weierstrass factorisation of $f_{E,p}(T)$ is given by $P(T)u(T)$, where $P(T) = T^r$ is a distinguished polynomial and $u(T) = g(T)$ is a unit in $\Lambda(\Gamma)$. Thus, $\lambda_p(E/K) = \deg P(T) = \deg T^r = r$ and $\mu_p(E/K) = 0$.

However, suppose that $\mu_p(E/K) = 0$ and $\lambda_p(E/K) = r$. Then, we may write $f_{E,p}(T) = P(T)u(T)$, where $P(T)$ is a distinguished polynomial of degree r and $u(T)$ is a unit in $\Lambda(\Gamma)$. Since $P(T)$ is divisible by T^r, this forces $P(T) = T^r$ and $u(T) = g(T)$. Therefore, $g(T)$ is a unit in $\Lambda(\Gamma)$, and hence $a_r = g(0)$ is unit in $\mathbb{Z}_p$. □

THEOREM 3.6. *Let E be an elliptic curve over a number field K and p an odd prime. Assume that the following conditions are satisfied:*

(1) *E has good ordinary reduction at all primes $v \mid p$ of K;*
(2) *$\operatorname{rank} E(K) > 0$;*
(3) *$\mathrm{Sel}_{p^\infty}(E/K_{\mathrm{cyc}})^\vee$ is finitely generated and torsion as a $\Lambda(\Gamma)$-module;*
(4) *$R_p(E/K)$ is a p-adic unit (in particular, nonzero);*
(5) *$Ш(E/K)[p^\infty] = 0$;*
(6) *$p \nmid c_v(E/K)$ for all primes v at which E has bad reduction;*
(7) *$p \nmid \#\widetilde{E}(\mathbb{F}_v)$ for all primes $v \mid p$ of K.*

Then, for all $n \geq 0$, K_n/K is an integrally Diophantine extension. Therefore, if Conjecture 1.1 is satisfied for K, then it is satisfied for K_n for all $n \geq 0$.

PROOF. Since it is assumed that $Ш(E/K)[p^\infty] = 0$, in particular, $Ш(E/K)[p^\infty]$ is finite, the conditions of Theorem 3.4 are satisfied. It follows from Theorem 3.4 that a_r is a unit, where $r = \operatorname{rank} E(K)$. Lemma 3.5 then asserts that $\lambda_p(E/K) = \operatorname{rank} E(K)$. Since $\operatorname{rank} E(K) > 0$, the result follows from Theorem 3.3. □

The above result shows that given a number field K, if there exists an elliptic curve $E_{/K}$ satisfying the conditions of Theorem 3.6, then, K_n/K is integrally Diophantine for all n. In the next section, we shall explain the conditions of Theorem 3.6.

4. Conditions for rank constancy in cyclotomic $\mathbb{Z}_p$-towers

Let E be an elliptic curve defined over $\mathbb{Q}$ such that $\operatorname{rank} E(\mathbb{Q}) > 0$, and let $K/\mathbb{Q}$ be a number field extension. We consider the base change of E to K. Note that $\operatorname{rank} E(K) > 0$. The data (E, K) is fixed throughout and the results are of most interest in the case when K is neither totally real nor abelian. Assume that E does not have complex multiplication. Given any set of prime numbers $\mathcal{P}$, the upper (respectively lower) density of $\mathcal{P}$ refers to its upper (respectively lower) Dirichlet density. When we say that $\mathcal{P}$ has density $\delta \in [0, 1]$, we mean that the Dirichlet density of $\mathcal{P}$ exists and equals δ. Note that the upper and lower densities always exist. Let Ω be the set of odd prime numbers p such that E has good ordinary reduction at p, and the conditions of Theorem 3.6 are satisfied for $E_{/K}$ and the cyclotomic

https://doi.org/10.1017/S000497272200082X Published online by Cambridge University Press

$\mathbb{Z}_p$-extension of K. In this section, we provide circumstantial evidence for the following conjecture.

CONJECTURE 4.1. The set of primes Ω has positive lower density.

In this section, the prime p is allowed to vary over the prime numbers at which E has good ordinary reduction. A classical result of Serre shows that for a non-CM elliptic curve, the set of primes of good ordinary (respectively supersingular) reduction has density 1 (respectively 0). Since the prime p is not fixed in this section, it is pertinent that we do not suppress the role of p in the notation for cyclotomic extensions. Thus, $K_{\mathrm{cyc}}^{(p)}$ denotes the cyclotomic $\mathbb{Z}_p$-extension of K and $K_n^{(p)}$ denotes the subfield of $K_{\mathrm{cyc}}^{(p)}$ with $[K_n : K] = p^n$.

THEOREM 4.2. *Let K be a number field and E a non-CM elliptic curve over $\mathbb{Q}$ such that:*

(1) $\operatorname{rank} E(\mathbb{Q}) > 0$*;*
(2) $Ш(E/K)$ *is finite.*

Then there exists a set of odd prime numbers Σ of positive density satisfying the following conditions:

(1) *E has good ordinary reduction at all prime numbers $p \in \Sigma$;*
(2) *if for a prime $p \in \Sigma$,*

   (a) *$R_p(E/K)$ is a p-adic unit,*
   (b) *$\mathrm{Sel}_{p^\infty}(E/K_{\mathrm{cyc}})^\vee$ is a finitely generated and torsion module over $\Lambda(\Gamma)$,*

   then, $\operatorname{rank} E(K_n^{(p)}) = \operatorname{rank} E(K)$ *for all n and the conclusion of Theorem 3.6 holds.*

PROOF. By the aforementioned result of Serre, the set of primes p at which E has good ordinary reduction has density 1. Let $\widetilde{K} \subset \bar{\mathbb{Q}}$ be the Galois closure of K. By a standard application of the Chebotarev density theorem, the set of prime numbers p that split completely in $\widetilde{K}$ has density $[\widetilde{K} : \mathbb{Q}]^{-1}$. Let Σ_0 be the set of primes p at which E has good ordinary reduction and that split completely in K. Then Σ_0 has density $[\widetilde{K} : \mathbb{Q}]^{-1}$.

Let the set of primes $p \in \Sigma_0$ such that p divides $\#\widetilde{E}(\mathbb{F}_p)$ be denoted by Σ_1. Primes p at which E has good reduction such that p divides $\#\widetilde{E}(\mathbb{F}_p)$ are known as *anomalous* primes. If p is large enough, then a prime p is anomalous precisely when $a_p(E) := p + 1 - \#\widetilde{E}(\mathbb{F}_p)$ is equal to 1. As is well known, the set of anomalous primes has density 0 (see [12]). It follows that Σ_1 has density 0. Note that since any prime $p \in \Sigma_0 \backslash \Sigma_1$ is completely split in $\widetilde{K}$, for each prime v of K that lies above p, we find that $\mathbb{F}_v = \mathbb{F}_p$. Therefore, since p is not anomalous, p does not divide the product $\prod_{v|p} \#\widetilde{E}(\mathbb{F}_v)$ for all primes $p \in \Sigma_0 \backslash \Sigma_1$. The set of primes that divide any given natural number is clearly finite. Therefore, the set of primes $p \in \Sigma_0$ such that $p \mid \prod_v c_v(E/K)$ is finite. Denote this set by Σ_2. Finally, note that since it is assumed that $Ш(E/K)$ is finite, the set of primes p such that $Ш(E/K)[p^\infty] \neq 0$ is finite as well. Let Σ_3 denote this set. Set Σ

https://doi.org/10.1017/S000497272200082X Published online by Cambridge University Press

TABLE 1. Elliptic curves of rank 2.

	Cremona Label	$\Pi^{\leq 1000}$		Cremona Label	$\Pi^{\leq 1000}$
1.	$389a$	$\emptyset$	6.	$643a$	$\emptyset$
2.	$433a$	$\{13\}$	7.	$655a$	$\{7, 31\}$
3.	$446d$	$\{7\}$	8.	$664a$	$\{59\}$
4.	$563a$	$\emptyset$	9.	$681c$	$\emptyset$
5.	$571b$	$\emptyset$	10.	$707a$	$\{29\}$

to be the set of primes $\Sigma_0 \backslash (\bigcup_{i=1}^{3} \Sigma_i)$. For $p \in \Sigma$, if $R_p(E/K)$ is a unit in $\mathbb{Z}_p$, then the conditions of Theorem 3.6 are satisfied and the result follows. □

REMARK 4.3. One would like to understand how often $R_p(E/K)$ is *not* a p-adic unit. Unfortunately, the p-adic regulator is a fairly complex invariant and computations involving the p-adic regulator over a number field K are challenging. There are built-in packages on the Sage computational system [20] to compute p-adic regulators over $\mathbb{Q}$; however, the author is not aware of any such packages written for number fields $K \neq \mathbb{Q}$ that are readily usable.

Computations over $\mathbb{Q}$ suggest the following conjecture over other number fields.

CONJECTURE 4.4. Let E be an elliptic curve over $\mathbb{Q}$ and K be a number field. The set of primes p such that $R_p(E/K)$ is divisible by p has density 0.

Given an elliptic curve $E_{/\mathbb{Q}}$ and $N > 0$, let $\Pi^{\leq N}$ be the set of primes $p \leq N$ of good ordinary reduction such that $p \mid R_p(E/\mathbb{Q})$. We compute $\Pi^{\leq 1000}$ for the first ten elliptic curves of rank 2 ordered by conductor. The calculations in Table 1 are from [9, page 7955] and were done on Sage. The data indicate that the $p \mid R_p(E/K)$ should be a rare occurrence.

We give one concrete example of an elliptic curve E over $\mathbb{Q}$ for which Theorem 3.6 can be expected to apply. We do not obtain any new result by working over $\mathbb{Q}$, and the calculation below is only included to illustrate our technique.

Consider the elliptic curve E with Weierstrass equation $y^2 + y = x^3 - x$, Cremona label 37a1, and set $p = 5$. Referring to the conditions of Theorem 3.6:

(1) E has good ordinary reduction at 5;
(2) $\operatorname{rank} E(\mathbb{Q}) = 1$, in particular, $\operatorname{rank} E(\mathbb{Q}) > 0$;
(3) we assume that the dual Selmer group $\mathrm{Sel}_{5^\infty}(E/\mathbb{Q}_{\mathrm{cyc}})^\vee$ is torsion over the Iwasawa algebra (recall that Mazur's conjecture predicts this condition to hold for all elliptic curves with good ordinary reduction at p);
(4) the normalised 5-adic regulator is a 5-adic unit;
(5) the analytic order of $Ш(E/\mathbb{Q})$ is exactly 1;

https://doi.org/10.1017/S000497272200082X Published online by Cambridge University Press

(6) all Tamagawa numbers $c_v(E/\mathbb{Q})$ are equal to 1;
(7) $\widetilde{E}(\mathbb{F}_5) = 8$, and hence $\widetilde{E}(\mathbb{F}_5)$ is not divisible by 5.

The calculations above were performed via Sage (see [20]).

Acknowledgement

The author would like to thank the anonymous referee for helpful suggestions.

References

[1] J. Coates and R. Sujatha, *Galois Cohomology of Elliptic Curves*, Tata Institute of Fundamental Research, Lectures on Mathematics, 91 (Narosa Publishing House, New Delhi, 2010).
[2] J. Denef, 'Diophantine sets over algebraic integer rings. II', *Trans. Amer. Math. Soc.* **257**(1) (1980), 227–236.
[3] J. Denef and L. Lipshitz, 'Diophantine sets over some rings of algebraic integers', *J. Lond. Math. Soc. (2)* **18**(3) (1978), 385–391.
[4] N. Garcia-Fritz and H. Pasten, 'Towards Hilbert's tenth problem for rings of integers through Iwasawa theory and Heegner points', *Math. Ann.* **377**(3) (2020), 989–1013.
[5] R. Greenberg, 'Iwasawa theory for elliptic curves', in: *Arithmetic Theory of Elliptic Curves*, Lecture Notes in Mathematics, 1716 (ed. C. Viola) (Springer, Berlin–Heidelberg, 1999), 51–144.
[6] Y. Hachimori and K. Matsuno, 'An analogue of Kida's formula for the Selmer groups of elliptic curves', *J. Algebraic Geom.* **8**(3) (1999), 581–601.
[7] K. Iwasawa, 'On $\mathbb{Z}$-extensions of algebraic number fields', *Ann. of Math. (2)* **98**(2) (1973), 246–326.
[8] K. Kato, 'p-adic Hodge theory and values of zeta functions of modular forms', *Astérisque* **295** (2004), 174 pages.
[9] D. Kundu and A. Ray, 'Statistics for Iwasawa invariants of elliptic curves', *Trans. Amer. Math. Soc.* **374**(11) (2021), 7945–7965.
[10] Y. V. Matiyasevich, 'The Diophantineness of enumerable sets', *Dokl. Akad. Nauk* **191** (1970), 279–282.
[11] B. Mazur, J. Tate and J. Teitelbaum, 'On p-adic analogues of the conjectures of Birch and Swinnerton–Dyer', *Invent. Math.* **84**(1) (1986), 1–48.
[12] V. K. Murty, 'Modular forms and the Chebotarev density theorem II', in: *Analytic Number Theory*, London Mathematical Society Lecture Note Series, 247 (ed. Y. Motohashi) (Cambridge University Press, Cambridge, 1997), 287–308.
[13] B. Perrin-Riou, 'Théorie d'Iwasawa des représentations p-adiques sur un corps local', *Invent. Math.* **115**(1) (1994), 81–149.
[14] T. Pheidas, 'Hilbert's tenth problem for a class of rings of algebraic integers', *Proc. Amer. Math. Soc.* **104**(2) (1988), 611–620.
[15] P. Schneider, 'p-adic height pairings. I', *Invent. Math.* **69**(3) (1982), 401–409.
[16] P. Schneider, 'p-adic height pairings. II', *Invent. Math.* **79**(2) (1985), 329–374.
[17] H. N Shapiro and A. Shlapentokh, 'Diophantine relationships between algebraic number fields', *Comm. Pure Appl. Math.* **42**(8) (1989), 1113–1122.
[18] A. Shlapentokh, 'Extension of Hilbert's tenth problem to some algebraic number fields', *Comm. Pure Appl. Math.* **42**(7) (1989), 939–962.
[19] 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.
[20] W. Stein, *Sage: Open Source Mathematical Software*, 2010. Available online at https://www.sagemath.org.

[21] C. Videla, 'Sobre el dècimo problema de Hilbert', *Atas da Xa Escola de Algebra, Vitoria, ES, Brasil. Colecao Atas* **16** (1989), 95–108.
[22] L. C. Washington, *Introduction to Cyclotomic Fields*, Graduate Texts in Mathematics, 83 (Springer, New York, 1997).

ANWESH RAY, Department of Mathematics,
University of British Columbia, Vancouver, BC V6T 1Z2, Canada
e-mail: anweshray@math.ubc.ca

https://doi.org/10.1017/S000497272200082X Published online by Cambridge University Press