

Coranks of Selmer groups over p -division extensions of elliptic curves

Tibor Backhausz *

Supervisor: Gergely Zábrádi †

November 8, 2012

Abstract

For a prime $p \geq 5$ we investigate the p -Selmer group $\text{Sel}_{p^\infty}(E/K_\infty)$ of an elliptic curve E not having complex multiplication over the field $K_\infty = \mathbb{Q}(E[p^\infty])$ which is the smallest field containing all points of E with p -power order. The structure of $\text{Sel}_{p^\infty}(E/K_\infty)$ is not known in detail and is still the subject of conjectures in non-commutative Iwasawa theory. Under certain conditions it is known that $\text{Sel}_{p^\infty}(E/K_\infty)$ is a co-torsionfree module over the non-commutative Iwasawa algebra $\Lambda(H) = \Lambda(\text{Gal}(K_\infty/K))$ with finite nonzero corank τ . This τ has been proposed as the non-commutative analogue of the λ -invariant in the classical Iwasawa theory of elliptic curves. We show that odd τ is only possible for $p \in \{7, 11\}$. Furthermore, $\tau = 1$ is impossible for curves with non-integral j -invariants (finding such curves would have been useful in non-commutative Iwasawa theory). There are only finitely many integral j -invariants that a curve with odd τ can have. We also show that there are only finitely many curves with odd τ for each of these j -invariants. Hence our main result is that $\tau \geq 2$ holds with finitely many exceptions up to $\mathbb{Q}$ -isomorphism of elliptic curves. The exact set of exceptions can be determined computationally. These results do not use Iwasawa theory and have classical interpretations in terms of Selmer ranks and split multiplicative reductions over number fields.

Acknowledgements

I'd like to thank Gergely Zábrádi for his absolutely indispensable guidance that led to this work, and especially for his helpful and encouraging attitude.

1 Introduction

Elliptic curves

Many problems in number theory can be reduced to solving Diophantine equations of the form

$$E: \quad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

for constants a_i and $x, y \in F$ for a number field F . F is usually $\mathbb{Q}$, the field of rational numbers.

*2nd year Mathematics undergraduate, Eötvös Loránd University.

†Assistant professor, Eötvös Loránd University, Department of Algebra and Number Theory

If this equation defines a nonsingular curve in the projective plane over F , it is called an elliptic curve and denoted E/F . Basic arithmetic properties of elliptic curves are described in the book [18]. To keep this work short, we assume the reader is familiar with concepts such as the reduction types, Mordell–Weil group, torsion subgroup, isogenies, discriminant, j -invariant and conductor of an elliptic curve.

The F -rational points of E form an Abelian group, this is called the Mordell–Weil group of E/F . The group operation is given by a rational function which is easily computed, therefore to effectively find all F -rational points we only need the generators of the Mordell–Weil group. By the Mordell–Weil theorem, if F is a number field, this group is finitely generated, and therefore isomorphic to $\mathbb{Z}^r \oplus T$ where $r \geq 0$ and T is finite and called the torsion subgroup of E/F . The points in T can be determined relatively easily. The difficulty is now reduced to finding r , which is called the rank of E/F .

Selmer groups

The common method to find upper bounds for r is the following. It is the abstract variant of the classical descent process.

Any positive integer n defines a group homomorphism $[n]$ from E/F to itself: $[n]P = P + P + \dots + P$ with addition according to the Mordell–Weil group law. Let $E[n]$ denote the kernel, and nE denote the image of this map. Then the factor group E/nE contains $(\mathbb{Z}/n\mathbb{Z})^r$ as a subgroup. Now we need an upper bound for $|E/nE|$.

The Selmer group for a positive integer n , denoted $\text{Sel}_n(E/F)$ is a finite, effectively computable Abelian group that contains $E/E[n]$. Computing $\text{Sel}_n(E/F)$ is called an n -descent.

In particular, we have the following short exact sequence of Abelian groups:

$$0 \rightarrow E/E[n] \rightarrow \text{Sel}_n(E/F) \rightarrow \text{III}(E/F)[n] \rightarrow 0$$

$\text{III}(E/F)$ is called the Tate–Shafarevich group and $\text{III}(E/F)[n]$ is its n -torsion subgroup (the subgroup of elements whose order divides n). III is understood to measure the failure of the Hasse local-global principle that holds for quadratic forms. A common idea in the theory of elliptic curves is that the Hasse principle does fail sometimes, but not too severely. In particular, we have the Shafarevich–Tate conjecture: $\text{III}(E/F)$ is always finite when E/F is an elliptic curve over a number field. Hoping this is true, we set $n = p^k$ in the above exact sequence and take the direct limit as $k \rightarrow \infty$. Now we have an exact sequence

$$0 \rightarrow (\mathbb{Q}_p/\mathbb{Z}_p)^r \rightarrow \text{Sel}_{p^\infty}(E/F) \rightarrow \text{III}(E/F)[p^\infty] \rightarrow 0$$

Therefore the number of copies in the direct limit $\text{Sel}_{p^\infty}(E/F)$ is r plus the number of copies of $(\mathbb{Q}_p/\mathbb{Z}_p)$ in $\text{III}(E/F)$. But if $\text{III}(E/F)$ is finite, the latter is 0. Then we have found a way to express $(\mathbb{Q}_p/\mathbb{Z}_p)^r$ as the direct limit of effectively computable groups.

Algorithmically, we can give an upper bound for r after computing $\text{Sel}_{p^k}(E/F)$. Then the finiteness of $\text{III}(E/F)$ implies that this bound will eventually coincide with r .

Now we have a theoretical method to determine r . In Mazur’s words, we "do descents by day and search for points by night", and continue until the lower bound for r given by points we have found coincides with the upper bound given by descents. This process will end if the Shafarevich–Tate conjecture holds.

Iwasawa theory

Iwasawa theory is the idea that the behaviour of arithmetic objects can be studied in towers of number fields, and tied to certain p -adic L -functions. When applied to elliptic curves, this approach provides most of what we know about the Birch–Swinnerton-Dyer conjecture, a Millennium Prize problem that relates the rank of an elliptic curve to a *complex* L -function. Classically, Iwasawa theory considers extensions with Galois groups $\mathbb{Z}_p$ such as the field $\mathbb{Q}(\mu_{p^\infty}) = \bigcup_{n=1}^{\infty} \mathbb{Q}(\mu_{p^n})$ over the cyclotomic field $\mathbb{Q}(\mu_p)$. Here μ_{p^n} denotes the group of p^n -th roots of unity.

Fortunately, the Selmer group behaves well in these towers of fields, so Iwasawa theory is applicable to the arithmetic of elliptic curves.

To extend Iwasawa theory to a wider class of field extensions, John Coates has proposed non-commutative Iwasawa theory for elliptic curves, some parts of which are still conjectural. This involves a field extension with pro- p Galois group and some extra assumptions. Two interesting instances of non-commutative Iwasawa theory are:

- I. The "false Tate curve" extension $\mathbb{Q}(\sqrt[p^\infty]{m}, \mu_{p^\infty})$ over $\mathbb{Q}(\mu_p)$ for $m \in \mathbb{Z}$ a p th power-free integer.
- II. The GL_2 extension $\mathbb{Q}(E[p^\infty])$ over K where K is chosen so that the Galois group of the extension will be pro- p .

For the false Tate curve extension, there is the paper [8] which describes $\text{Sel}_{p^\infty}(E/\mathbb{Q}(\sqrt[p^\infty]{m}, \mu_{p^\infty}))$ as a module over the group ring of $\text{Gal}(\mathbb{Q}(\sqrt[p^\infty]{m}, \mu_{p^\infty})/\mathbb{Q}(\mu_{p^\infty}))$.

This Selmer group is related to the growth of Selmer groups $\text{Sel}_{p^\infty}(E/\mathbb{Q}(\sqrt[p^n]{m}, \mu_{p^n}))$ as n increases, therefore we obtain concrete information over number fields, and if the Shafarevich–Tate conjecture holds, we also have would asymptotic information on the growth of the rank in the tower.

One hopes that analogous results are possible in the GL_2 extension case. While the relationship between $\text{Sel}_{p^\infty}(E/\mathbb{Q}(E[p^\infty]))$ and the growth in the tower is still conjectural, $\text{Sel}_{p^\infty}(E/\mathbb{Q}(E[p^\infty]))$ is worthy of study in light of these conjectures.

2 Assumptions and definitions

In this subsection we describe some of our assumptions for a field K , prime p and elliptic curve E . We assume that E does not have complex multiplication. For CM curves, the structure of torsion points of E is well understood, and entirely different from non-CM curves.

Let $K_\infty = \mathbb{Q}(E[p^\infty])$, and $K \subseteq \mathbb{Q}(E[p])$ be a Galois number field such that

- (I) $p \geq 5$
- (II) E/K has good ordinary reduction at all places above p
- (III) $\text{Gal}(K_\infty/K)$ is pro- p

For simplicity, assume that K is a minimal field satisfying these conditions. So K_∞/K is an *admissible extension*.

For our most critical assumption, we need definitions. For G , a pro- p group with p -adic Lie-group structure and no element of order p , we define its Iwasawa algebra as the inverse limit of p -adic group rings

$$\Lambda(G) = \varprojlim \mathbb{Z}_p[G/H]$$

where H varies over open normal subgroups of G .

Recall that by the Weil pairing, we have $\bigwedge^2 E[p^n] = \mu_{p^n}$, the group of p^n -th roots of unity as a Galois module. Therefore $\mathbb{Q}(E[p^n])$ contains $\mathbb{Q}(\mu_{p^n})$ so K_∞ contains $K^{\text{cyc}} = K(\mu_{p^\infty})$.

Now define $G = \text{Gal}(K_\infty/K)$ and $H = \text{Gal}(K_\infty/K^{\text{cyc}})$. By a Theorem of Serre [16] G can be viewed as an open subgroup of $GL_2(\mathbb{Z}_p)$. Then H is the kernel of the determinant on G . If $K = \mathbb{Q}(E[p])$, which is typical but not always the case, G is the subgroup of $GL_2(\mathbb{Z}_p)$ congruent to the identity modulo p . Assumption (I) guarantees that G and H have no p -torsion, and Assumption (III) guarantees they are pro- p , so we can form their Iwasawa algebras $\Lambda(G)$ and $\Lambda(H)$.

To study $\text{Sel}_{p^\infty}(E/\mathbb{Q}(E[p^\infty])) = \text{Sel}_{p^\infty}(E/K_\infty)$, we take its Pontryagin dual $X(E/K_\infty) = \text{Hom}(\text{Sel}_{p^\infty}(E/K_\infty), \mathbb{Q}_p/\mathbb{Z}_p)$. Similarly, let $X(E/K^{\text{cyc}})$ be the Pontryagin dual of $\text{Sel}_{p^\infty}(E/K^{\text{cyc}})$. Then $X(E/K_\infty)$ will be a $\Lambda(G)$ -module, and therefore also a $\Lambda(H)$ -module. A general goal in non-commutative Iwasawa theory is to describe the structure of $X(E/K_\infty)$ over $\Lambda(G)$, which could yield concrete, arithmetic information. An easier, intermediate step is to describe $X(E/K_\infty)$ over $\Lambda(H)$.

Define $\lambda = \text{rk}_{\mathbb{Z}_p} X(E/K^{\text{cyc}})$, which is a classical Iwasawa invariant. A proposed analogue (see e.g. [2]) is $\tau = \text{rk}_{\Lambda(H)} X(E/K_\infty)$. Under some technical assumptions that are always conjectured to be true given (I)-(III), Howson proved the following formula:

$$(1) \quad \tau = \lambda + s_{E/K^{\text{cyc}}}.$$

Here s denotes the number of primes with split multiplicative reduction for an elliptic curve over a field. This is the joint consequence of equation (47) and Theorem 2.8. in [10]. The conjecture required is her Conjecture 2.5 for K_∞ and K^{cyc} . Note that the finiteness of λ is known even when $X(E/K^{\text{cyc}})$ is not finitely generated. We will return to why $s_{E/K^{\text{cyc}}}$ is finite in Proposition 5.6.

Our fourth assumption is that

(IV) Howson's formula (1) holds for E and K_∞ .

One sufficient condition when we know (IV) is true is when $X(E/K^{\text{cyc}})$ is finitely generated over $\mathbb{Z}_p$. In this case, $X(E/K^{\text{cyc}})$ will also be torsion-free. Note that this is not always the case.

In this work, we study the right hand side of Howson's formula and thus try to give a lower bound for τ by non-Iwasawa theoretic methods. Our results are summarized in Theorem 7.5. (Although some more curves can be ruled out by computation, these results are not included in this work.)

3 Motivation

In this section we show how our work is connected to the general goal of describing the structure of $X(E/K_\infty)$ over $\Lambda(G)$.

Let Z be the center of G . If G is represented by a matrix group with entries in $\mathbb{Z}_p$ then Z is formed by the subgroup of diagonal matrices. Therefore Z is naturally isomorphic to the multiplicative group $1 + p\mathbb{Z}_p \leq \mathbb{Z}_p^\times$ which acts on $E[p^\infty]$ by multiplication. By a result of Howson [11], the center of $\Lambda(G)$ is $\Lambda(Z)$. Note that (disregarding

the identity element) Z has no element fixing K^{cyc} therefore it is disjoint from H so $G = Z \times H$.

Coates, Schneider and Sujatha in [3] have studied the case when $p \geq 5$, G is pro- p , E has good ordinary reduction everywhere above p in F and $X(E/F^{\text{cyc}})$ is finitely generated over $\mathbb{Z}_p$. They have asked whether the $\Lambda(G)$ module $X(E/F_\infty)$ is completely faithful (after disregarding pseudo-null submodules). In the $F_\infty = K_\infty$, $F^{\text{cyc}} = K^{\text{cyc}}$ case, complete faithfulness would be necessary for a well-behaved Iwasawa theory of elliptic curves over p -adic PGL_2 -extensions.

This is the GL_2 -extension analogue of the question [8] answers in the false Tate curve case. By a result of Ardakov ([1], section 1.4), under our assumptions (I)-(IV) $X(E/K^{\text{cyc}})$ must be completely faithful over $\Lambda(G)$ if it is torsion-free over both $\Lambda(H)$ and $\Lambda(Z)$. There are many curves where $X(E/K_\infty)$ is known to be $\Lambda(H)$ -torsionfree but *none* where $X(E/K_\infty)$ is $\Lambda(Z)$ -torsionfree.

One could hope the following argument could provide a curve whose $X(E/K_\infty)$ is known to be torsion-free over $\Lambda(Z)$. If $X(E/K_\infty)$ is small in the sense of having rank 1 over $\Lambda(H)$, then the $\Lambda(Z)$ -torsion also implies annihilation by some element of $\Lambda(Z)$. But annihilation, being much stronger than torsion, can be ruled out more easily. Indeed, [19] states that, given assumptions equivalent to (I)-(IV), and that the j -invariant of E is non-integral (a rather mild assumption satisfied by most curves), $X(E/K_\infty)$ is not annihilated by any element of $\Lambda(Z)$.

Then we only have to find a curve with $\tau = 1$ and $j \notin \mathbb{Z}$ to give the first example where the complete faithfulness conjecture holds. Despite this incentive, no such curves were found and some, including the supervisor of this work, began to doubt their existence. This work confirms that there are indeed no such curves. For the sake of completeness, we also consider the $j \in \mathbb{Z}$ case.

4 Determining τ

We restate Howson's formula from the introduction.

Theorem 4.1. *Suppose that Conditions (I)-(IV) hold. Then*

$$\tau = \text{rk}_{\Lambda(H)} X(E/K_\infty) = \lambda + s_{E/K^{\text{cyc}}}$$

Corollary 4.2. $\tau \geq \text{rk}_{\mathbb{Z}} E/K + s_{E/K}$

Proof. This follows from $\lambda \geq \text{rk}_{\mathbb{Z}} E/K$ and $s_{E/K^{\text{cyc}}} \geq s_{E/K}$. □

Example

Let E be the modular curve $X_1(11)$, which is an elliptic curve with Cremona label 11a3 and Weierstrass minimal equation

$$y^2 + y = x^3 - x$$

This curve has no complex multiplication. It has split multiplicative reduction at 11 and good reduction everywhere else. It also has rank 0 and a 5-torsion subgroup over $\mathbb{Q}$.

Let $p = 5$ and $K = \mathbb{Q}(\mu_5)$. Conditions (I) and (II) hold. The torsion subgroup means that $\text{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$ is isomorphic to the $(\text{mod } p)$ matrix group $\begin{pmatrix} 1 & \mathbb{F}_p \\ 0 & \mathbb{F}_p^\times \end{pmatrix}$ of order 20. $\mathbb{Q}(E[p^\infty])$ is pro- p Galois extension of $\mathbb{Q}(E[p])$ which has degree p over K therefore condition (III) holds. Conditions (I) and (II) are easy to see.

It is well known that $\text{Sel}_{p^\infty}(E/K^{\text{cyc}}) = \text{Sel}_{p^\infty}(E/\mathbb{Q}(\mu_{p^\infty}))$ is finite for this curve therefore condition (IV) must hold with $\lambda = 0$. This leaves $\tau = s_{E/K^{\text{cyc}}}$. 11 has order 4 mod 25 so it decomposes into 4 primes over K^{cyc} therefore $\tau = s_{E/K^{\text{cyc}}} = 4$.

Heuristically, curves such as E with prime conductor, having rank 0 and p -torsion in $\mathbb{Q}$, should have a relatively small τ . However, we will see later that they cannot have $\tau = 1$ by the strict conditions imposed on elliptic curves with p -torsion.

Another example for $p = 7$, also having 7-torsion is the one given in ([2], equation (89)). Here, $\tau = 3$, which coincides with our lower bound for 7-torsion curves.

5 The parity of τ

Theorem 5.1. *Suppose that Conditions (I)-(IV) hold for some Galois number field $K \subseteq K_\infty$. Then we have*

$$\text{rk}_{\Lambda(H)} X(E/K_\infty) \equiv \frac{[K : \mathbb{Q}]}{2} \pmod{2}$$

This is not a new result because this can be obtained as a consequence of Corollary 5.7. in [2].

We give a proof nonetheless because the technical machinery of [2], notably crystalline cohomology, is overkill in our case. Also, some lemmas in the following proof will be used throughout.

Proof. Let $K_n = K(\mu_{p^n})$.

Proposition 5.2. (a) $\text{Gal}(\mathbb{Q}(E[p])/K)$ has order dividing p .

(b) E/K has a nontrivial p -torsion subgroup.

Proof. $\text{Gal}(\mathbb{Q}(E[p])/K)$ is a factor group of $\text{Gal}(K_\infty/K)$ which is pro- p by our assumptions. On the other hand, $\text{Gal}(\mathbb{Q}(E[p])/K)$ is also a subgroup of $\text{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$ which has order $|\text{GL}_2(\mathbb{F}_p)| = p(p^2 - 1)(p - 1)$. This means $\text{Gal}(\mathbb{Q}(E[p])/K)$ has p -power order dividing $p(p^2 - 1)(p - 1)$, which proves part (a).

If $\text{Gal}(\mathbb{Q}(E[p])/K)$ is trivial, claim (b) is also trivial. Otherwise it has order p and so it is a p -Sylow subgroup in $\text{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$. Since all p -Sylow subgroups are related by conjugation, $\text{Gal}(\mathbb{Q}(E[p])/K)$ is conjugate to $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$ when written in a suitable basis of $E[p]$. Hence it fixes a one-dimensional $\mathbb{F}_p$ -subspace of $E[p]$. This means the coordinates of a p -torsion consisting of p elements lie in K . $\square$

Proposition 5.3. *For all $n \geq 0$, the bad reductions of E/K_n are split multiplicative.*

Proof. It is well known that good and split multiplicative reductions remain that way through field extensions so it is enough to prove the claim for K .

When K contains $\mathbb{Q}(E[p])$, this is a classical result from [17]. Otherwise we have by Proposition 5.2, part (a) that $\text{Gal}(\mathbb{Q}(E[p])/K)$ has order p .

For places lying above p our assumptions assure good reduction. Suppose for contradiction that E/K has additive reduction at some v not lying above p . Then we invoke Theorem 1.13. from [12] for $l = p$ which tells us that

$$(p - 1)b(p) \leq 2$$

where the p -primary subgroup of E/K has order $p^{b(p)}$. From Proposition 5.2 part (b) we have $b(p) \geq 1$ and since $p \geq 5$, the inequality cannot hold.

Therefore we have either good or multiplicative reduction everywhere. Since splitting of a multiplicative reduction depends on solvability of $x^2 + c_6$ in the local residue field (where c_6 is computed from coefficients of E), and solvability of quadratic equations remains unchanged by the degree p extension $\mathbb{Q}(E[p])_v/K_v$, we conclude from the results of [17] above that bad reductions are already split in K . $\square$

Proposition 5.4. (a) *The local root number for a place v is $w_v(E/K_n) = -1$ if v is Archimedean or E/K_n has split multiplicative reduction at v . Otherwise, $w_v(E/K_n) = 1$.*

(b)

$$w(E/K_n) = (-1)^{a_{K_n}} (-1)^{s_{E/K_n}}$$

where a_{K_n} is the number of Archimedean valuations of K_n , and s_{E/K_n} is the number of split multiplicative reductions of E over K_n .

Proof. (a) For Archimedean and good or split multiplicative non-Archimedean places, this is a special case of Rohrlich's Theorem 2 in [14]. (In his notation, τ should be the trivial character, and χ will also be trivial in the split case.) Other possibilities are ruled out by Proposition 5.3

(b) This follows by multiplying the local root numbers given by (a). $\square$

Proposition 5.5. *For all n , $s_{E/K_n} \equiv s_{E/K} \pmod{2}$*

Proof. We proceed by induction. The claim is trivial for $n = 1$ where $K_n = K$ by the Weil pairing. The proof of the induction step $s_{E/K_{n+1}} \equiv s_{E/K_n}$. Due to Proposition 5.3 bad reduction is equivalent to split multiplicative in these fields. Primes in K_n with bad (i.e. split multiplicative) reduction correspond one-to-one with conjugacy classes of bad primes (under the action of $\text{Gal}(K_{n+1}/K_n)$). Since the extension has odd degree p , these classes have an odd number of elements. Thus cardinality $\pmod{2}$ is unchanged. $\square$

Corollary 5.6. *There are finitely many primes in K^{cyc} over any prime of K . We also have $s_{E/K^{\text{cyc}}} \equiv s_{E/K} \pmod{2}$*

Proof. The first claim is well known. Let q be a prime in K . It has a decomposition subgroup $D_q < \text{Gal}(K^{\text{cyc}}/K)$ which is closed in the profinite topology. q splits into $[\text{Gal}(K^{\text{cyc}}/K) : D_q]$ primes. But $\text{Gal}(K^{\text{cyc}}/K) \cong \mathbb{Z}_p$ and the only closed subgroup with infinite index is trivial. Suppose that D_q is trivial. Then the completion of K at q , denoted K_q , would contain μ_{p^∞} . This is impossible since there can only be finitely many roots of unity in the residue field of K_q . Therefore D_q must have finite index.

A finite number of places with bad reduction each decomposes into a finite number of places in K^{cyc} . There is a K_n in the extension tower after which none of them decomposes further. Apply Proposition 5.5 to this n . $\square$

Proposition 5.7. $a_{K_n} = \frac{1}{2}[K_n : \mathbb{Q}] = \frac{1}{2}p^{n-1}[K : \mathbb{Q}]$

Proof. K_n contains $\mathbb{Q}(\mu_p)$ and is therefore a totally imaginary number field. It is well known that totally imaginary number fields have Archimedean valuations equal to half their degree. $\square$

Proposition 5.8. *The p -parity conjecture applies for E/K_n i.e. $(-1)^{\lambda_{E/K_n}} = w(E/K_n)$*

Proof. From Proposition 5.2 we have a p -torsion subgroup in E/K . Hence can construct a K -rational isogeny having this subgroup as kernel from E/K to some curve E'/K . This means we can apply Theorem 2 from [6]. $\square$

Substitute part (b) from Proposition 5.4 for the right side of Proposition 5.8 to obtain

$$\begin{aligned} (-1)^{\lambda_{E/K_n}} &= w(E/K_n) = (-1)^{a_{K_n}} (-1)^{s_{E/K_n}} \\ \lambda_{E/K_n} + s_{E/K_n} &\equiv a_{K_n} \pmod{2} \end{aligned}$$

Since λ is finite and increasing in n , there is an n so that $\lambda_{E/K_n} = \lambda$. Continue with this n .

$$\lambda + s_{E/K_n} \equiv a_{K_n} \pmod{2}$$

Now apply Propositions 5.6 and 5.7.

$$\lambda + s_{E/K_{\text{cyc}}} \equiv \frac{[K : \mathbb{Q}]}{2} \pmod{2}$$

$\square$

Consequences

With the above result, we can prove that $\tau \equiv 0 \pmod{2}$ in many cases, we only need to show that $4 \mid [K : \mathbb{Q}]$. It turns out that this is almost always the case.

Recall that $\text{Gal}(\mathbb{Q}(E[p^\infty])/\mathbb{Q})$ acts on the Tate module $E[p^\infty]$. Since $\text{Aut}(E[p^\infty]) \cong \text{GL}_2(\mathbb{Z}_p)$, this provides a representation $\rho : \text{Gal}(\mathbb{Q}(E[p^\infty])/\mathbb{Q}) \rightarrow \text{GL}_2(\mathbb{Z}_p)$. Taking its $(\text{mod } p)$ reduction we obtain a representation $\varphi : \text{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \rightarrow \text{GL}_2(\mathbb{F}_p)$. Note that these are injective.

Serre's celebrated paper [16] studies this representation and concludes that for a non-CM curve, the image of ρ is always a subgroup of finite index (equivalently, an open subgroup) of $\text{GL}_2(\mathbb{Z}_p)$.

In addition, he proves the following:

Theorem 5.9. *Let $E/\mathbb{Q}$ be a non-CM elliptic curve. Then ρ (and, consequently, φ) is surjective for all but finitely many primes p .*

This means that, statistically, the most significant case is when $\text{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \cong \text{GL}_2(\mathbb{F}_p)$.

Proposition 5.10. *Assuming Conditions (I)-(IV) and $\text{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \cong \text{GL}_2(\mathbb{F}_p)$ we have*

$$\text{rk}_{\Lambda(H)} X(E/K_\infty) \equiv 0 \pmod{2}$$

Proof. By Proposition 5.2, $\mathbb{Q}(E[p])/K$ has degree 1 or p . Since $[\mathbb{Q}(E[p]) : \mathbb{Q}] = |\text{GL}_2(\mathbb{F}_p)| = p(p-1)(p^2-1)$, we have the sequence of divisibility relations $4 \mid p^2-1 \mid [K : \mathbb{Q}]$ which yields the claim by Theorem 5.1. $\square$

We also have another immediate consequence depending chiefly on p .

Proposition 5.11. *Assume in addition to conditions (I)-(IV) that $p \equiv 1 \pmod{4}$. Then*

$$\mathrm{rk}_{\Lambda(H)} X(E/K_\infty) \equiv 0 \pmod{2}$$

Proof. Using Theorem 5.1 we only have to show that $4 \mid [K : \mathbb{Q}]$.

By the Weil pairing we know that $\det \rho : \mathrm{Gal}(K/\mathbb{Q}) \rightarrow \mathbb{F}_p^\times$ is surjective, therefore the order of $\mathrm{Gal}(K/\mathbb{Q})$ is divisible by $p - 1$ which we assumed is divisible by 4. $\square$

This rules out $\tau = 1$ for primes $p \equiv 1 \pmod{4}$.

6 A lower bound for τ

Using Theorem 4.1, our goal is to give a lower bound for $\lambda_{E/K} + s_{E/K}$ under certain conditions. This will not involve Iwasawa theory and is mostly based on classical results of Mazur and Serre ([13] and [16], respectively). Recall that E is still assumed to be a non-CM curve defined over $\mathbb{Q}$.

In this section, we prove the following.

Theorem 6.1. *Assume (I)-(IV) for an elliptic curve E/K defined over $\mathbb{Q}$ with non-integral j -invariant. Then*

$$\tau \geq \mathrm{rk}_{\mathbb{Z}_p} X(E/K^{\mathrm{cyc}}) + s_{E/K} \geq 2.$$

Note that curves with non-integral j -invariant never have CM. The following lemma justifies why we can restrict to cases when $K \subseteq \mathbb{Q}(E[p])$ when studying small τ .

Lemma 6.2. *For an elliptic curve $E/\mathbb{Q}$ let $F \subseteq F'$ be number fields that satisfy (I)-(IV). Then we have $\tau_F \leq \tau_{F'}$.*

Proof. This is immediate from Theorem 4.1, where the summands cannot decrease in field extensions. We can also deduce this directly from the original definition of τ since $\Lambda(H_F)$ contains $\Lambda(H_{F'})$ as a subring. $\square$

Therefore it is enough to prove Theorem 6.1 for $K \subseteq \mathbb{Q}(E[p])$, taking $K \cap \mathbb{Q}(E[p])$ if necessary. We also reduce K as much as possible to keep assumption (III) true. If $\mathrm{Gal}(K/\mathbb{Q})$ has normal p -Sylow subgroup, we pass to the field fixed by this subgroup. This way we assume $\mathrm{Gal}(K/\mathbb{Q})$ has no normal p -Sylow subgroup.

Nontriviality

Non-commutative Iwasawa theory [3] tells us that $\tau > 0$. We also note that the non-integral j -invariant guarantees $\tau \geq s_{E/K} \geq 1$. Therefore from Theorem 5.1 we have

Proposition 6.3. *If $4 \mid [K : \mathbb{Q}]$ then $\tau \geq 2$.*

Inertia

In this section, denote $\text{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$ by G and $\text{Gal}(K/\mathbb{Q})$ by G_0 . G is identified with a subgroup of $GL_2(\mathbb{F}_p)$ as before. For a prime $q \in \mathbb{Q}$, let D_q denote its decomposition subgroup within G_0 , and let I_q denote its subgroup of inertia within D_q . (Note that D_q and I_q are, in general, defined only up to conjugacy in $\text{Gal}(K/\mathbb{Q})$. However, they are unique if the extension is Abelian, which turns out to be the most interesting case.)

Recall that q splits into $[G_0 : D_q]$ distinct prime ideals, and has ramification degree $|I_q|$. I_q is also a normal subgroup of D_q with a cyclic quotient (isomorphic to the Galois group of an extension of finite fields).

Serre ([16], section 1.11) has shown the following:

Proposition 6.4. *I_p is either*

- a) *conjugate to a subgroup of the form $\begin{pmatrix} 1 & 0 \\ 0 & \mathbb{F}_p^\times \end{pmatrix}$ of order $p - 1$. We will call these semi-Cartan subgroups.*
- b) *a non-split Cartan subgroup (isomorphic to a cyclic group of order $p^2 - 1$, corresponding to the action of a primitive root in $\mathbb{F}_{p^2}$ by multiplication)*

Image in GL_2 and PGL_2

Further, Serre gives the following classification for: $\text{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$, based on the following definitions:

Borel subgroups are those conjugate to

$$\begin{pmatrix} \mathbb{F}_p^\times & \mathbb{F}_p \\ 0 & \mathbb{F}_p^\times \end{pmatrix}$$

Split Cartan subgroups are those conjugate to

$$\begin{pmatrix} \mathbb{F}_p^\times & 0 \\ 0 & \mathbb{F}_p^\times \end{pmatrix}$$

Non-split Cartan subgroups are as defined in Proposition 6.4.

Proposition 6.5. *G satisfies at least one of these:*

- a) $G = GL_2(\mathbb{F}_p)$
- b) G is contained in a Borel subgroup
- c) G is contained in the normaliser of a split Cartan subgroup
- d) G is contained in the normaliser of non-split Cartan subgroup

Note that it can be easily computed (and Serre does so) that in cases c) and d), p does not divide $|G|$. Therefore

Proposition 6.6. *If $p \mid |G|$ but $4 \nmid p$ then G is contained in a Borel subgroup.*

Then we have another classification by Serre ([16], section 2.6.):

Proposition 6.7. *Suppose that $p \nmid |G|$ for a group $G < GL_2(\mathbb{F}_p)$. Let H be the quotient of G by the center of $GL_2(\mathbb{F}_p)$. Then H , lying in $PGL_2(\mathbb{F}_p)$, satisfies at least one of these:*

- i) H is cyclic. Then G is in a Cartan subgroup of $GL_2(\mathbb{F}_p)$.
- ii) H is dihedral. Then G is in the normaliser of a Cartan subgroup.
- iii) H is isomorphic to A_4 , S_4 or A_5 .

Apply this to our G . In case i), the Cartan subgroup containing G is either split or non-split. If it is split, then it is contained in a Borel subgroup. When it is non-split, then I_p must have been a nonsplit Cartan subgroup, which leads to $4 \mid |G|$.

In case ii), G must be the group extension of a Cartan or semi-Cartan subgroup by a cyclic group of order two. $|G|$ is again divisible by 4.

In case iii), it is obvious that $4 \mid |H| \mid |G|$.

Summing up these observations, we have

Proposition 6.8. *Suppose that $p \nmid |G|$ and $4 \nmid |G|$. Then G lies in a Borel subgroup.*

This, together with the similar proposition above, implies

Theorem 6.9. *Suppose that $4 \nmid |G|$. Then G lies in a Borel subgroup.*

Restrictions on p

Whether G is contained in a Borel subgroup is equivalent to whether $E/\mathbb{Q}$ has an isogeny of degree p to some elliptic curve E' . There are plenty of examples for such isogenies, but not for all primes.

Mazur's results [13] show that a non-CM curve $E/\mathbb{Q}$ can only have isogenies with prime degree for

$$p \in \{2, 3, 5, 7, 11, 13, 17, 37\}$$

Recalling (I) and using Theorem 5.11, we can exclude all of these but 7 and 11.

Inertia in the Borel case

In this subsection, we examine Serre's results [16] in the Borel case, paying attention to the parity of $[K : \mathbb{Q}]$.

Whether G is contained in a Borel subgroup is equivalent to whether $E/\mathbb{Q}$ has an isogeny of degree p . Borel subgroups can be written over a suitable basis in the form

$$\begin{pmatrix} \mathbb{F}_p^\times & \mathbb{F}_p \\ 0 & \mathbb{F}_p^\times \end{pmatrix}$$

We work in this basis from now on. Note that the Borel subgroup contains the unipotent subgroup (with 1s in the diagonal) as a normal subgroup of order p . In fact, the Borel subgroup is the semidirect product of the unipotent subgroup and the subgroup of diagonal matrices. Since, G_0 is the factor group of G by this unipotent subgroup, G is also the semidirect product of G_0 and the unipotent subgroup. G_0 is then canonically isomorphic to the diagonal elements of G , denoted G^0 .

G^0 is contained in

$$\begin{pmatrix} \mathbb{F}_p^\times & 0 \\ 0 & \mathbb{F}_p^\times \end{pmatrix}$$

This means G^0 , G_0 , and therefore K , are Abelian. Then, by the Kronecker–Weber theorem, K is contained in $\mathbb{Q}(\mu_N)$ where N is the conductor of K . Using the Fundamental Theorem of Galois theory, we obtain a map

$$\kappa : \text{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q}) \rightarrow \text{Gal}(K/\mathbb{Q})$$

$\text{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q})$ can be naturally regarded as $(\mathbb{Z}/N\mathbb{Z})^\times$ and through G^0 we have an embedding

$$\kappa' : (\mathbb{Z}/N\mathbb{Z})^\times \rightarrow \begin{pmatrix} \mathbb{F}_p^\times & 0 \\ 0 & \mathbb{F}_p^\times \end{pmatrix}$$

The two components of this function are two characters to $\mathbb{F}_p^\times$ times. Serre states his theorems in terms of these two characters χ' and χ'' . For example, part a) of Serre's Proposition 23 in [16] can be formulated as

Proposition 6.10. *Let $q \neq p$ be a rational prime where $E/\mathbb{Q}$ has good reduction. Let t_q denote the trace of the Frobenius morphism at q . Then*

$$t_q \equiv \text{tr } \kappa'(q) \pmod{p}$$

$$q \equiv \det \kappa'(q) \pmod{p}$$

As a consequence, $|E/\mathbb{F}_q| \equiv q + 1 - \text{tr } \kappa'(q) \pmod{p}$.

Using the Weil pairing, we know that the determinant

$$\det : \text{Gal}(K/\mathbb{Q}) \rightarrow \text{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$$

from the above matrix group is surjective to $\mathbb{F}_p^\times$ i.e. $\text{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$.

Proposition 6.11. *For a rational prime $q \neq p$, let I_q be the inertia subgroup of $\text{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q})$ at q . The image of $\det(\kappa(I_q))$ is trivial.*

Proof. Note that $\mathbb{Q}(\mu_N) \supseteq K \supseteq \mathbb{Q}(\mu_p)$ and the maps involved are exactly the restriction maps of Galois groups therefore $\det \circ \kappa(\sigma)$ has the same action on $\text{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ as $\sigma \in \text{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q})$. On the other hand the only ramified prime in $\text{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ is p so q is unramified there i.e. the projection of I_q is trivial. $\square$

The case for I_p is quite the opposite.

Proposition 6.12. *Let I_p be the inertia subgroup of $\text{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q})$ at p , and $\kappa(I_p)$ its image. Then $\det$ maps $\kappa(I_p)$ bijectively to $\mathbb{F}_p^\times$.*

Proof. $\kappa(I_p)$ is exactly the inertia subgroup determined in Proposition 6.4. We have already ruled out case b) therefore $\kappa(I_p)$ is a semi-Cartan subgroup of order $p-1$. The claim follows from its matrix form. $\square$

Proposition 6.13. *For any rational prime $q \neq p$, $\kappa(I_q) \cap \kappa(I_p) = \{1\}$.*

Proof. By Proposition 6.11, any element $\sigma \in \kappa(I_q) \cap \kappa(I_p)$ must have determinant 1. Using Proposition 6.12, $\det$ is injective on I_p so σ must coincide with the identity element. $\square$

Corollary 6.14. G_0 contains the subgroup $\kappa(I_q)\kappa(I_p) \cong \kappa(I_q) \times \kappa(I_p)$.

Proposition 6.15. If $[K : \mathbb{Q}]/2$ is odd, then $p \equiv 3 \pmod{4}$ and $|\kappa(I_q)|$ is odd for all rational primes $q \neq p$.

Proof. $[K : \mathbb{Q}] = |G_0|$ is divisible by $(p-1)|I_q|$ as shown by the above corollary. $\square$

Section 5.6, part a) of [16] states that

Proposition 6.16. Let $\mathbb{Q}_p^{\text{unr}}$ be a maximal unramified extension of $\mathbb{Q}_p$. Then $|\kappa(I_p)|$ is the degree of the minimal extension over $\mathbb{Q}_p^{\text{unr}}$ where E obtains good reduction.

Proposition 6.17. If $E/\mathbb{Q}$ has additive, potentially multiplicative reduction at q , $|\kappa(I_q)| = 2$.

Proof. E becomes semistable at q at the degree 2 extension $\mathbb{Q}_q(\sqrt{-c_6})$ where c_6 is a fixed polynomial of the a_i s (see [18]). $\square$

Serre states that since E obtains good reduction at q (hence, discriminant Δ with q -valuation $0 \pmod{12}$) at a field extension with Galois group $\kappa(I_q)$,

$$|\kappa(I_q)|v_q(\Delta) \equiv 0 \pmod{12}$$

and if $\gcd(q, 12) = 1$ then

$$\kappa(I_q) = \frac{12}{\gcd(12, v_q(\Delta))}$$

Summarizing the above, we have the following.

Theorem 6.18. Suppose that $\text{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$ is in a Borel subgroup. If it has order not divisible by 4, the following conditions hold necessarily.

- 1) $p \equiv 3 \pmod{4}$
- 2) For all primes q where $E/\mathbb{Q}$ has additive reduction, it has potentially good reduction and $4 \mid v_q(\Delta)$.

These conditions are sufficient provided $E/\mathbb{Q}$ is semistable at 2 and 3, or it is otherwise known that $|I_2|$ and $|I_3|$ are odd.

Remaining cases

In this subsection we use ad hoc arguments to complete the proof of Theorem 6.1 in the case when the above conditions for the parity of $[K : \mathbb{Q}]/2$ hold.

Let $\ell \in \mathbb{Q}$ be a rational prime dividing the denominator of the j -invariant of E i.e. having potentially multiplicative reduction. By Theorem 6.18 this is semistable multiplicative reduction and $|\kappa(I_\ell)| = 1$.

Non-semistable case

When there is some $q \neq p$ with $|\kappa(I_q)| \neq 1$, it must decompose in K . Suppose for contradiction that ℓ does not decompose i.e. its decomposition subgroup is all of G_0 . Note that $1 < |\kappa(I_q)|$, which must divide $|\mathbb{F}_p^\times|$, has a nontrivial common factor with $p - 1$. This means that the product in Corollary 6.14 cannot be cyclic therefore G_0 cannot be cyclic.

The factor group of the decomposition subgroup by the inertia subgroup is known to be a Galois group of Galois fields. But we have established on the contrary that $G_0/\kappa(I_\ell) = G_0$ cannot be cyclic.

This means there will be at least 3 primes in K lying over ℓ . These will all have split multiplicative reduction by Proposition 5.3, hence $3 \leq s_{E/K}$ and our claim follows.

Semistable case

Establishing torsion

When the above case does not apply, K is unramified apart from p . Therefore $\text{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q}) = I_p$, whence $n = p$ and $G_0 = \kappa(I_p) \cong \mathbb{F}_p^\times$. Also, since additive reductions at a prime q can only become multiplicative in an extension if q ramifies, we obtain from Proposition 5.3 that $E/\mathbb{Q}$ is semistable at all primes, except possibly p .

We recall some easy results implicit in ([16], $n^\circ 5.4$).

In our basis for $E[p]$,

$$G^0 \in \left\{ \begin{pmatrix} \mathbb{F}_p^\times & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & \mathbb{F}_p^\times \end{pmatrix} \right\}$$

$\text{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$ is a degree 1 or p extension of G^0 therefore

$$\text{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \in \left\{ G^0, \begin{pmatrix} 1 & \mathbb{F}_p \\ 0 & \mathbb{F}_p^\times \end{pmatrix}, \begin{pmatrix} \mathbb{F}_p^\times & \mathbb{F}_p \\ 0 & 1 \end{pmatrix} \right\}$$

Write $T = E[p]/K$ for the p -torsion subgroup of E over K , and T' for the quotient Galois module $E[p]/T$. Then $\text{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$ acts on both T and T' , and one of the actions must be trivial. There is a $\mathbb{Q}$ -rational degree p isogeny from E to an elliptic curve E' with kernel T and a dual isogeny from E' to E with kernel isomorphic to T' as a Galois module of $\text{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$.

Galois action on either T or T' is trivial therefore one of them lies in $\mathbb{Q}$. Hence either $E/\mathbb{Q}$ or $E'/\mathbb{Q}$ has p -torsion. Recall that $p \equiv -1 \pmod{4}$ and $p \geq 5$. From the work of Mazur we know that this is only possible for $p = 7$.

7-torsion

Let $A \in \{E, E'\}$ be the curve with rational 7-torsion. Suppose that it has good reduction at 2. Then its rational 7-torsion points map injectively to its reduction $\tilde{A}$ over $\mathbb{F}_2$. Hence $\tilde{A}$ is an elliptic curve with at least 7 points over $\mathbb{F}_2$. But by the Hasse bound, an elliptic curve over a finite field $\mathbb{F}_q$ of order q can have at most $(\sqrt{q} + 1)^2$ points and $(\sqrt{2} + 1)^2 \approx 5.82842712 < 7$ which is a contradiction.

Therefore A must have semistable bad (i.e. multiplicative) reduction at 2. Since the conductor of an elliptic curve is isogeny invariant, E also has multiplicative reduction at 2.

Over $K = \mathbb{Q}(\mu_7)$, the prime 2 decomposes into 2 primes, and by Proposition 5.3 the reductions at these primes are all split multiplicative, which gives $2 \leq s_{E/K} \leq \tau$. Note that from parity, we have in fact $3 \leq \tau$. This closes the last remaining case.

7 Integral j -invariant

We consider the same problem for elliptic curves with integral j -invariant using other methods. This solution will not be complete, but will rule out all but finitely many curves up to $\mathbb{Q}$ -isomorphism.

The hardest part is showing $\tau > 0$. This requires Iwasawa theory, see [3] for a proof. Therefore it is still the case that $2|\tau$ implies $\tau \geq 2$.

We apply Theorem 6.9 so we can restrict to curves with a p -isogeny. Using Mazur's results, we can restrict to $p \in \{7, 11\}$.

Our main tool is the following well known theorem:

Theorem 7.1. *There is a p -isogeny between two elliptic curves E and E' if and only if $(j(E), j(E'))$ is a point on the modular curve $X_0(p)$.*

Therefore we are looking for integral points on $X_0(7)$ and $X_0(11)$.

Integral points on $X_0(11)$

$X_0(11)$ has genus 1: it is isomorphic to the elliptic curve

$$11A1 : y^2 + y = x^3 - x^2 - 10x - 20$$

In Cremona's tables [4] we find that this curve has rank 0 and torsion subgroup of order 5. Integral points on this curve correspond to the following pairs of j -invariants (see [7]):

$$(-11 \cdot 131^3, -11^2), (-11^2, -11 \cdot 131^3), (-2^{15}, -2^{15})$$

This last one means that the elliptic curve with $j = -2^{15}$ has a 11-isogeny to itself i.e. it is CM so we do not consider it. Now the possible j -invariants for $p = 11$ are -11^2 and $-11 \cdot 132^3$.

Integral points on $X_0(7)$

On the other hand, $X_0(7)$ has genus 0. It has a rational parametrisation (see e.g. [9])

$$((t^2 + 13t + 49)(t^2 + 245t + 2401)^3/t^7, (t^2 + 13t + 49)(t^2 + 5t + 1)^3/t) \quad t \in \mathbb{Q}$$

We need both coordinates to be integral. Let $t = a/b$ in reduced form. The first coordinate is then

$$\frac{(a^2 + 13ab + 49b^2)(a^2 + 245ab + 2401b^2)^3}{a^7b}$$

Modulo a , the numerator is 7^6b^8 . Using $(a, b) = 1$, this is divisible by a if and only if $a \mid 7^6$. Modulo b , the numerator is a^8 . This is divisible by b if and only if $b \mid 1$.

The second coordinate is

$$\frac{(a^2 + 13ab + 49b^2)(a^2 + tab + b^2)^3}{ab^7}$$

Modulo a , the numerator is 7^2b^8 . Using $(a, b) = 1$, this is divisible by a if and only if $a \mid 7^2$. Modulo b , the numerator is a^8 . This is divisible by b if and only if $b \mid 1$.

Therefore the possibilities are $t \in \{1, 7, 49, -1, -7, -49\}$. Note that if t parametrizes the pair (j_1, j_2) then $49/t$ gives (j_2, j_1) .

Now $t = 1$ and $t = 49$ give $j \in \{3^2 \cdot 7 \cdot 2647^3, 3^2 \cdot 7^4\}$. $t = -1$ and $t = -49$ give $j \in \{-3^3 \cdot 37 \cdot 719^3, 3^3 \cdot 37\}$. The rest are symmetric i.e. CM points: $t = 7$ gives $j = 3^3 \cdot 5^3 \cdot 17^3$ and $t = -7$ gives $j = -3^3 \cdot 5^3$.

Therefore the possible j -invariants for $p = 7$ are $j \in \{3^2 \cdot 7 \cdot 2647^3, 3^2 \cdot 7^4, -3^3 \cdot 37 \cdot 719^3, 3^3 \cdot 37\}$.

Twisting

If two elliptic curves are isomorphic over $\bar{\mathbb{Q}}$, they are said to be *twists* of each other. Possible twists of an elliptic curve $E/\mathbb{Q}$ are classified by $H^1(\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}), \text{Aut}(E))$. As suggested by its name, j is invariant in $\mathbb{C}$ -isomorphisms, therefore twists have the same j -invariant.

Let E_d denote the twist of an elliptic curve E by the character $(\frac{\cdot}{d})$ for a square-free integer d .

Explicitly, for an equation

$$E: y^2 = x^3 + a_2x^2 + a_4x + a_6$$

$$E_d: dy^2 = x^3 + a_2x^2 + a_4x + a_6$$

E and E_d are not isomorphic over $\mathbb{Q}$ if $d \neq 1$, but they are isomorphic over $\mathbb{Q}(\sqrt{d})$.

It is well known (see e.g. [18]) that

Theorem 7.2. *If $E/\mathbb{Q}$ is an elliptic curve with $j(E) \neq 0, 1728$ then the elliptic curves with j -invariant $j(E)$ are exactly the curves E_d .*

In this section, we prove the following consequence:

Proposition 7.3. *For any given j -invariant j_0 , there are only finitely many curves $E/\mathbb{Q}$ having $j(E) = j_0$ and also satisfying conditions (I)-(IV) $4 \nmid [\mathbb{Q}(E[p]) : \mathbb{Q}]$. These curves have the same conductor apart from a possible factor of p^2 .*

Lemma 7.4. *Let $E/\mathbb{Q}$ be an elliptic curve with a p -isogeny, having good reduction at a prime $q \neq p$. Let $(\frac{\cdot}{d})$ be a quadratic character with conductor divisible by q . Then the inertia subgroup of q in $\text{Gal}(\mathbb{Q}(E_d[p])/\mathbb{Q})$ is 2.*

Proof. Since the existence of a p -isogeny only depends on the j -invariant, E_d also has a p -isogeny. $E/\mathbb{Q}$ and $E_d/\mathbb{Q}$ are isomorphic over $\mathbb{Q}(\sqrt{d})$. $E/\mathbb{Q}(\sqrt{d})$ has good reduction at q , therefore so does $E_d/\mathbb{Q}(\sqrt{d})$.

Hence the minimal extension where E_d obtains good reduction at q is a quadratic extension with ramification degree 2 at q . The claim follows from ([16], p. 312). $\square$

Now we prove Proposition 7.3.

Proof. Let $E/\mathbb{Q}$ be a curve with minimal conductor N_E in the family of elliptic curves with j -invariant j_0 . Then by our previous results, E has a rational p -isogeny.

Let Δ be the minimal discriminant of $E/\mathbb{Q}$. If d is a square-free integer not dividing $p\Delta$, then there is prime $q \neq p$ dividing d where E has good reduction. Then by the above lemma and 6.14, $4 \mid [\mathbb{Q}(E_d[p]) : \mathbb{Q}]$.

Therefore all exceptional curves with j -invariant j_0 are twists of E by some square-free divisor of $p\Delta$, of which there are finitely many.

Similarly, twists that change the conductor result in a larger conductor because we chose N_E to be minimal. The twisted conductor is either $p^2 N_E$ (since an additive bad reduction appeared at p) or has a prime divisor $q \neq p$ where E has good reduction. This implies a good reduction becomes potentially good additive after the twist, and we can invoke the lemma. Note that since $p \geq 5$ the exponent of p in the conductor of any elliptic curve with integral j -invariant is 0 or 2.

□

This is effective: together with the list of possible j -invariants, provides a list of all curves that could have $\tau = 1$. Using SAGE [15], especially the function `EllipticCurve_from_j`, we obtain the minimal conductor for each j -invariant involved. To get an explicit list of potentially exceptional elliptic curves, we can look up the conductors given below in [4].

Theorem 7.5. *Assume assumptions (I)-(IV) for an elliptic curve E/K having rational coefficients. Then*

$$\tau := \mathrm{rk}_{\Lambda(H)} X(E/K_\infty) \geq 2$$

holds with the finitely many exceptions up to $\mathbb{Q}$ -isomorphism of elliptic curves. The exceptions are classified by the following table.

p	j -invariant	Conductor
7	$3^3 \cdot 37$	$1369 = 37^2$
7	$-3^3 \cdot 37 \cdot 719^3$	$1369 = 37^2$
7	$3^3 \cdot 37$	$67071 = 7^2 \cdot 37^2$
7	$-3^3 \cdot 37 \cdot 719^3$	$67071 = 7^2 \cdot 37^2$
7	$3^2 \cdot 7^4$	$3969 = 3^4 \cdot 7^2$
7	$3^2 \cdot 7 \cdot 2647^3$	$3969 = 3^4 \cdot 7^2$
11	-11^2	$121 = 11^2$
11	$-11 \cdot 131^3$	$121 = 11^2$

References

- [1] Konstantin Ardakov, *Centres of skewfields and completely faithful Iwasawa modules*, J. Inst. Math. Jussieu 7 (2008) 457–468.
- [2] J. Coates, T. Fukaya, K. Kato, R. Sujatha, *Root numbers, Selmer groups, and non-commutative Iwasawa theory*. J. Algebraic Geom. 19 (2010), no. 1, 19–97.
- [3] J. Coates, P. Schneider, R. Sujatha, *Modules over Iwasawa algebras*. J. Inst. Math. Jussieu 2 (2003), 73–108.
- [4] John Cremona. *The Elliptic Curve Database for Conductors to 130000*. In Florian Hess, Sebastian Pauli, and Michael Pohst (ed.). ANTS VII: Proceedings of the 7th International Symposium on Algorithmic Number Theory. Springer, Lecture Notes in Computer Science, volume 4076, pages 11–29, 2006.
- [5] T. Dokchitser, V. Dokchitser (appendix by J. Coates and R. Sujatha) *Computations in noncommutative Iwasawa theory*. Proc. London Math. Soc. (3) 94 (2006), 211–272.

- [6] T. Dokchitser, V. Dokchitser, *Parity of ranks for elliptic curves with a cyclic isogeny*. J. Number Theory 128 (2008), 662-679
- [7] Noam D. Elkies, *Elliptic Curves in Nature*, <http://www.math.harvard.edu/~elkies/nature.html>
- [8] Y. Hachimori, O. Venjakob, *Completely faithful Selmer groups over Kummer extensions*. Documenta Mathematica, Extra Volume: Kazuya Kato's Fiftieth Birthday (2003), 478.
- [9] Mark van Hoeij, *Parametrization of the modular curve $X_0(N)$ for N from 2 to 37* <http://www.math.fsu.edu/~hoeij/files/X0N/Parametrization>
- [10] Susan Howson, *Euler Characteristics as Invariants of Iwasawa Modules* Proc. London Math. Soc. (2002) 85 (3): 634-658.
- [11] Susan Howson, *Structure of central torsion Iwasawa modules*, Bull. Soc. Math. France 130 (2002), no. 4, 507-535.
- [12] H. W. Lenstra, F. Oort *Abelian varieties having purely additive reduction*. Journal of Pure and Applied Algebra vol. 36, pp. 281-298, 1985
- [13] Barry Mazur, *Rational isogenies of prime degree*, Inventiones Math. 44, 2 (June 1978), pp 129-162.
- [14] David E. Rohrlich, *Galois theory, elliptic curves, and root numbers*. Compositio Mathematica, 100 no. 3 (1996), p. 311-349
- [15] William A. Stein et al. Sage Mathematics Software (Version 5.1), The Sage Development Team, 2012, <http://www.sagemath.org>.
- [16] Jean-Pierre Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*. Inventiones mathematicae 15 (1971/72): 259-331.
- [17] J-P. Serre, J. Tate *Good Reduction of Abelian Varieties*. The Annals of Mathematics Second Series, Vol. 88, No. 3 (Nov., 1968), pp. 492-517
- [18] Joseph H. Silverman, *The Arithmetic of Elliptic Curves*. Springer-Verlag, GTM 106, 1986.
- [19] Gergely Zábrádi, *A note on central torsion Iwasawa-modules*, preprint