Functiones et Approximatio
52.2 (2015), 283–298
doi: 10.7169/facm/2015.52.2.7

RANKS OF GL_2 IWASAWA MODULES OF ELLIPTIC CURVES

Tibor Backhausz

Abstract: Let $p \geqslant 5$ be a prime and E an elliptic curve without complex multiplication and let $K_\infty = \mathbb{Q}(E[p^\infty])$ be a pro-p Galois extension over a number field K. We consider $X(E/K_\infty)$, the Pontryagin dual of the p-Selmer group $\mathrm{Sel}_{p^\infty}(E/K_\infty)$. The size of this module is roughly measured by its rank τ over a p-adic Galois group algebra $\Lambda(H)$, which has been studied in the past decade. We prove $\tau \geqslant 2$ for almost every elliptic curve under standard assumptions. We find that $\tau = 1$ and $j \notin \mathbb{Z}$ is impossible, while $\tau = 1$ and $j \in \mathbb{Z}$ can occur in at most 8 explicitly known elliptic curves. The rarity of $\tau = 1$ was expected from Iwasawa theory, but the proof is essentially elementary.

It follows from a result of Coates et al. that τ is odd if and only if $[\mathbb{Q}(E[p]) : \mathbb{Q}]/2$ is odd. We show that this is equivalent to $p = 7$, E having a 7-isogeny, a simple condition on the discriminant and local conditions at 2 and 3. Up to isogeny, these curves are parametrised by two rational variables using recent work of Greenberg, Rubin, Silverberg and Stoll.

Keywords: elliptic curve, division field.

1. Introduction

Let E be an elliptic curve defined over $\mathbb{Q}$ with good ordinary reduction at the prime $p \geqslant 5$ and without complex multiplication. We denote by $X(E/K_\infty)$ the dual Selmer group of E over its associated p-division extension $K_\infty := \mathbb{Q}(E[p^\infty])$. The aim of this paper is to investigate the $\Lambda(H)$-rank of $X(E/K_\infty)$ under certain usual technical conditions that are conjectured to be always satisfied. Here $\Lambda(H)$ denotes the Iwasawa algebra of $H = \mathrm{Gal}(K_\infty/K^{\mathrm{cyc}})$ where $K/\mathbb{Q}$ is a finite extension so that $\mathrm{Gal}(K_\infty/K)$ is pro-p, and K^{cyc} is the cyclotomic $\mathbb{Z}_p$-extension of K. Our main result is that this $\Lambda(H)$-rank τ can never be 1 except possibly for finitely many, explicitly known curves. It was previously proven using Iwasawa theoretic techniques that $\tau \neq 0$, and that $\tau = \lambda + s_{E/K^{\mathrm{cyc}}}$. Here $s_{E/K^{\mathrm{cyc}}}$ denotes the number of primes in K^{cyc} at which the curve E has split multiplicative reduction and λ is the usual λ-invariant of E over K^{cyc}, ie. the $\mathbb{Z}_p$-rank of the dual Selmer group $X(E/K^{\mathrm{cyc}})$. We do not use further Iwasawa theory. Instead, the main ingredients are:

2010 Mathematics Subject Classification: primary: 11G05; secondary: 11R23

(i) refinements of Serre's [19] study of division points on E;
(ii) Mazur's [16] result on possible isogenies over $\mathbb{Q}$; and
(iii) elementary calculations on the moduli curve $X_0(7)$.

In fact, τ is very rarely odd as one could expect from the formula $\tau \equiv [K : \mathbb{Q}]/2 \equiv [\mathbb{Q}(E[p]) : \mathbb{Q}] \pmod 2$ (this follows from [3], we give a simplified proof).

This decides the parity of $[\mathbb{Q}(E[p]) : \mathbb{Q}]/2$ for a given curve in a computationally easy way (Theorem 5.10), and combining this result with parametrisation from [10] gives all curves with odd $[\mathbb{Q}(E[p]) : \mathbb{Q}]/2$ (Theorem 5.12). This determines all the curves with odd τ.

Moreover, by the formula $\tau = \lambda + s_{E/K^{cyc}}$ there are two possibilities for $\tau = 1$: either $\lambda = 0$ and $s_{E/K^{cyc}} = 1$, or $\lambda = 1$ and $s_{E/K^{cyc}} = 0$. We prove that the former never occurs — all the possible exceptions are in the latter case.

Our results are in some sense negative, as Selmer groups with low $\Lambda(H)$-corank would be easier to test conjectures on. Moreover, using the results in [23] it can be shown that whenever the j-invariant of E is non-integral (or, equivalently, if $s_{E/K^{cyc}} \neq 0$) then $X(E/K_\infty)$ is not annihilated by any central element in $\Lambda(G)$ where $G = \mathrm{Gal}(K_\infty/K)$. Combining this with results in [1] would give the first example of a completely faithful Selmer group over the GL_2-extension if $\tau = 1$. However, as we show, this does not exist in nature even though it is expected that Selmer groups are *all* completely faithful. The possible exceptions are still good candidates to test this and other conjectures. On the other hand, the $\Lambda(H)$-rank encodes important information on the growth of the λ-invariant inside K_∞ and is therefore interesting on its own (see Proposition 3.5).

Acknowledgements. The author would like to thank Gergely Zábrádi for his absolutely indispensable guidance that led to this work, and especially for his helpful and encouraging attitude.

2. Assumptions and definitions

In this section 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 theory is different and better understood.

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.

For a $\Lambda(G)$-module M, the standard definition of rank is

$$\mathrm{rk}_{\Lambda(G)}(M) = \dim_{K(G)} K(G) \otimes_{\Lambda(G)} M$$

where $K(G)$ is the skew field of fractions of $\Lambda(G)$. Let $K_\infty = \mathbb{Q}(E[p^\infty])$, and K be a Galois number field such that K_∞/K is pro-p. 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 $K(E[p^n])$ contains $K(\mu_{p^n})$ so K_∞ contains $K^{\mathrm{cyc}} = K(\mu_{p^\infty})$.

Define $G = \mathrm{Gal}(K_\infty/K)$, $H = \mathrm{Gal}(K_\infty/K^{\mathrm{cyc}})$ and $\Gamma = \mathrm{Gal}(K^{\mathrm{cyc}}/K)$.

Let $M(p)$ denote the p-primary torsion subgroup of a module M. Let $\mathfrak{M}_H(G)$ denote the category of finitely generated $\Lambda(G)$ modules M such that $M/M(p)$ is finitely generated over $\Lambda(H)$. We make the following assumptions, which are traditional in non-commutative Iwasawa theory.

(I) $p \geqslant 5$;
(II) E/K has good ordinary reduction at all places above p;
(III) $\mathrm{Gal}(K_\infty/K)$ is pro-p;
(IV) $X(E/K_\infty) \in \mathfrak{M}_H(G)$.

It is always conjectured that Assumptions (I)-(II) imply Assumption (IV) [4, Conjecture 5.1]. Equivalently, define $Y(E/K_\infty) = X(E/K_\infty)/X(E/K_\infty)(p)$, then $Y(E/K_\infty)$ should be finitely generated over $\Lambda(H)$. This assumption also implies that $X(E/K^{\mathrm{cyc}})$ is torsion over $\Lambda(\Gamma)$ see [4, Lemma 5.3].

In the usual case when $X(E/K^{\mathrm{cyc}})$ is finitely generated over $\mathbb{Z}_p$, $X(E/K_\infty)$ is torsion-free and finitely generated over $\Lambda(H)$, in particular $Y(E/K_\infty) = X(E/K_\infty)$.

3. The τ rank

A proposed analogue to λ in the non-commutative case is

$$\tau = \mathrm{rk}_{\Lambda(H)} Y(E/K_\infty)$$

(see, e.g. [3], whose notation τ we follow). We state some earlier results on τ, originally stated with stronger assumptions, and show they are applicable assuming (I)-(IV).

Theorem 3.1 (Howson). *Suppose that Assumptions* (I)-(IV) *hold. Then*

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

Proof. As stated above, (IV) is stronger than [13, Conjecture 2.6] which implies [13, Conjecture 2.5] therefore [13, Theorem 2.8] is applicable. This states that $\lambda + s_{E/K^{\mathrm{cyc}}}$ is the homological rank of $X(E/K_\infty)$. This equals τ using [13, eqn. 47]. ■

Let $\mathrm{rk}_p^{Sel} E/F = \mathrm{rk}_{\mathbb{Z}_p} X(E/F)$ be the p-Selmer rank of E/F.

Corollary 3.2. $\tau \geqslant \mathrm{rk}_p^{Sel} E/K + s_{E/K}$

Proof. This follows from $\lambda \geqslant \mathrm{rk}_p^{Sel} E/K$ [9, Theorem 1.9] and $s_{E/K^{\mathrm{cyc}}} \geqslant s_{E/K}$. ■

Theorem 3.3 ([5]). *Assuming* (I)-(IV), $\tau > 0$.

Proof. [6, Theorem 1.5] means that $Y(E/K_\infty) \neq 0$. The kernel of the projection $X(E/K_\infty) \to Y(E/K_\infty)$ is finitely generated over $\Lambda(G)$ therefore annullated by some p^h. Let N be a pseudo-null submodule of $Y(E/K_\infty)$ with preimage M in$X(E/K_\infty)$. Then $p^h M$ isomorphic to N, hence pseudo-null. Under assumptions weaker than Howson's, [17, Theorem 5.1] states that all nontrivial pseudo-null submodules of $X(E/K_\infty)$ are zero, hence $N = p^h M = 0$.

Then [5, Corollary 7.4] holds for $Y(E/K_\infty)$ instead of $X(E/K_\infty)$. ■

Proposition 3.4 ([13]). *Assumptions* (I)-(IV) *for K imply the same for K', and*

$$\tau(E/K') = [K'^{cyc} : K^{\mathrm{cyc}}]\tau(E/K).$$

Proof. (I) and (II) are obviously unchanged. (III) holds because G' is pro-p as a subgroup of G. Define G', H' analogously for K'. $\Lambda(H)$ is finitely generated of $\Lambda(H')$ rank $[H : H'] = [K^{cyc'} : K^{\mathrm{cyc}}]$. ■

This means that we only need to determine $\tau(E/K)$ when K is minimal among fields satisfying $(I)-(IV)$, and then we can use the above formula. Therefore from now on we assume that K is minimal in this sense.

Remark. Our minimal K will turn out to be same as the field K in [10] if there is a p-isogeny and $\mathbb{Q}(E[p])$ otherwise.

The quantitative meaning of τ is given by the following,

Proposition 3.5 (Coates, Howson). *Assume* (I)-(IV). *Let $K_n = \mathbb{Q}(E[p^n])$. By Serre's theorem [19] there exists m such that*

$$\mathrm{Gal}(K_\infty/K_n) \cong \ker\left(GL_2(\mathbb{Z}_p) \to GL_2(\mathbb{Z} \bmod p^m)\right).$$

Then

$$\lambda(E/K_n) = \tau(E/K_m)p^{3(n-m)} + O(p^{2n}).$$

Proof. Take the sequence of subgroups $H_n = \mathrm{Gal}(K_\infty/K_n^{cyc})$. These are p-adic Lie groups of dimension 3, and $|H_m\colon H_n| = p^{3(n-m)}$. Then [13, Corollary 2.12] means that $\lambda(E/K_n) = \tau(E/K_m)p^{3(n-m)} - s_{E/K_n}$.

The decomposition subgroup D_q of a prime q with multiplicative reduction of E has dimension 2 as a p-adic Lie subgroup of G [2, Lemma 2.8], therefore these primes each decompose into $O(p^{2n})$ primes over K_n. Hence $s_{E/K_n} = O(p^{2n})$. ■

Therefore giving a lower bound to τ implies a lower bound for the growth of λ in the tower of division fields of E.

4. The parity of τ

Theorem 4.1. *Suppose that Conditions (I)-(IV) hold for some Galois number field $K \subseteq K_\infty$. Then we have*

$$\tau(E/K) \equiv \frac{[K\colon \mathbb{Q}]}{2} \pmod 2$$

Remark. Theorem 4.1 can be obtained as a consequence of Corollary 5.7. in [3] for $F = \mathbb{Q}$, $F' = K$. Using its notation,

$$\tau \equiv \sum_{\alpha \in \hat{\Omega},\ \alpha^2=1} [\mathcal{L}\colon \mathbb{Q}]/2 = |\hat{\Omega}[2]| \cdot [\mathcal{L}\colon \mathbb{Q}]/2 \equiv |\Omega| \cdot [\mathcal{L}\colon \mathbb{Q}]/2 = [K\colon \mathbb{Q}]/2 \pmod 2$$

We give a direct, somewhat simpler proof using Theorem 3.1, a case of the p-parity conjecture and some lemmas about the field K. We will use these lemmas in subsequent sections as well.

Proposition 4.2.

(a) $\mathrm{Gal}(K(E[p])/K)$ *has order dividing* p.
(b) E/K *has a nontrivial* p*-torsion subgroup.*

Proof. $\mathrm{Gal}(K(E[p])/K)$ is a factor group of $\mathrm{Gal}(K_\infty/K)$ which is pro-p by our assumptions. $\mathrm{Gal}(K(E[p])/K)$ acts on $E[p]$ $\mathbb{F}_p$-linearly so it has order dividing $|GL_2(\mathbb{F}_p)| = p(p^2-1)(p-1)$. This means $\mathrm{Gal}(K(E[p]/K))$ has p-power order dividing $p(p^2-1)(p-1)$, which proves part (a).

If $\mathrm{Gal}(K(E[p])/K))$ is trivial, claim (b) is also trivial. Otherwise it has order p and so it is a p-Sylow subgroup in $\mathrm{Gal}(K(E[p])/K)$. As such, it is conjugate to $\left(\begin{smallmatrix} 1 & \mathbb{F}_p \\ 0 & 1 \end{smallmatrix}\right)$ when written in a suitable basis of $E[p]$. Hence it fixes a one-dimensional $\mathbb{F}_p$-subspace of $E[p]$. ∎

Proposition 4.3. *All bad reductions of* E/K *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 [20]. Otherwise we have by Proposition 4.2 part (a) that $\mathrm{Gal}(K(E[p])/K)$ 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 [15, Theorem 1.13.] applies and rules out p-torsion for $p > 3$. This contradicts Proposition 4.2, so E/K is semistable.

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). This is unchanged in the degree p extension $K(E[p])/K$, so by [20], bad reductions are already split in K. ∎

Proposition 4.4.

(a) *The local root number for a place* v *is* $w_v(E/K) = -1$ *if* v *is Archimedean or* E/K *has split multiplicative reduction at* v*. Otherwise,* $w_v(E/K) = 1$.
(b) *Let* $s_{E/K}$ *be the number of split multiplicative reductions of* E *in* K.

$$w(E/K) = (-1)^{[K\colon \mathbb{Q}]/2}(-1)^{s_{E/K}}$$

Proof.

(a) For Archimedean and good or split multiplicative non-Archimedean places, this is a special case of Rohrlich's Theorem 2 in [18]. (In his notation, τ should be the trivial character, and χ will also be trivial in the split case.) Other possibilites are ruled out by Proposition 4.3

(b) This follows by multiplying the local root numbers given by (a). The number of Archimedean valuations of K is $[K\colon \mathbb{Q}]/2$ since $\mu_p \subset K$ so K is totally imaginary. ■

Proposition 4.5. *There are finitely many primes in K^{cyc} over any prime of K. Furthermore, $s_{E/K^{\mathrm{cyc}}} \equiv s_{E/K} \pmod 2$*

Proof. $\mathrm{Gal}(K^{\mathrm{cyc}}/K) \cong \mathbb{Z}_p$ since $\mu_p \subset K$. Then the decomposition subgroup of each prime has finite index, which must be a power of p. Since p is odd, each primes in K corresponds to an odd number of primes in K^{cyc}. ■

Proposition 4.6. *The p-parity conjecture applies for E/K i.e. $(-1)^{\mathrm{rk}_p^{Sel} E/K} = w(E/K)$*

Proof. From Proposition 4.2 we have a p-torsion subgroup in E/K. There is a K-rational isogeny having this subgroup as kernel. Then we can apply Theorem 2 from [8]. ■

Substituting part (b) from Proposition 4.4 for the right side of Proposition 4.6, then using Propositions 4.5, we have

$$\begin{aligned} (-1)^{\mathrm{rk}_p^{Sel} E/K} &= w(E/K) = (-1)^{[K\colon \mathbb{Q}]/2}(-1)^{s_{E/K}}, \\ \mathrm{rk}_p^{Sel} E/K + s_{E/K} &\equiv [K\colon \mathbb{Q}]/2 \pmod 2, \\ \mathrm{rk}_p^{Sel} E/K + s_{E/K^{\mathrm{cyc}}} &\equiv [K\colon \mathbb{Q}]/2 \pmod 2. \end{aligned}$$

[9, Proposition 3.10] states that $\mathrm{rk}_p^{Sel} E/K \equiv \lambda \pmod 2$. This proves Theorem 4.1.

5. The parity of $[K\colon \mathbb{Q}]/2$

Our goal in this section is to classify the elliptic curves E where $[K\colon \mathbb{Q}]/2$ is odd. This is mostly based on classical results of Mazur and Serre [16, 19]. In fact, we roughly follow Serre's argument while also paying attention to parity of various subgroups. We retain Assumptions (I)-(III). Recall also that E is still assumed to be a non-CM curve defined over $\mathbb{Q}$.

Note that we assumed in the beginning that K is minimal among fields satisfying Assumption (III). The parity of τ for other fields in the tower is the same (Proposition 3.4).

5.1. Inertia

In this section, denote $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$ by G and $\mathrm{Gal}(K/\mathbb{Q})$ by G_0. Since it acts faithfully on $E[p] \cong \mathbb{F}_p \times \mathbb{F}_p$, G is identified with a subgroup of $GL_2(\mathbb{F}_p)$. 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 $\mathrm{Gal}(K/\mathbb{Q})$. However, they are unique if the extension is Abelian, which turns out to be the most interesting case.)

Recall that q splits into $[G_0 \colon D_q]$ 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).

Proposition 5.1 (Serre, [19, Section 1.11]). *I_p is either*

(a) *conjugate to a subgroup of the form $\left(\begin{smallmatrix} 1 & 0 \\ 0 & \mathbb{F}_p^\times \end{smallmatrix}\right)$ 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)*

Case (b) means $4 \mid p^2-1 \mid |G|$ so we can exclude it.

Remark. Case (b) would also contradict Assumption (II) since it implies supersingular reduction at p.

5.2. Image in GL_2 and PGL_2

Serre gives a classification for $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$, based on the following definitions. Borel and split Cartan subgroups are defined as conjugate to respectively

$$\begin{pmatrix} \mathbb{F}_p^\times & \mathbb{F}_p \\ 0 & \mathbb{F}_p^\times \end{pmatrix} \qquad \text{and} \qquad \begin{pmatrix} \mathbb{F}_p^\times & 0 \\ 0 & \mathbb{F}_p^\times \end{pmatrix}.$$

Non-split Cartan subgroups are as defined in Proposition 5.1.

Proposition 5.2 (Serre). *G satisfies at least one of these:*

(a) $G = \mathrm{GL}_2(\mathbb{F}_p)$
(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 (a), (c) and (d), p does not divide $|G|$. Therefore

Proposition 5.3. *If $p \mid |G|$ but $4 \nmid |G|$ then G is contained in a Borel subgroup.*

Proposition 5.4 (Serre [19, Section 2.6]). *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, containing a cyclic subgroup C of index 2. C is contained in a unique Cartan subgroup of $PGL_2(\mathbb{F}_p)$ normalised by H. Then G is in the normaliser of a Cartan subgroup.*
(iii) *H is isomorphic to A_4, S_4 or A_5.*

Proposition 5.5. *Suppose that $4 \nmid |G|$. Then G lies in a Borel subgroup.*

Proof. Using Proposition 5.3 we can assume that $p \nmid |G|$. Then we look at the cases in Proposition 5.4.

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. Otherwise I_p must have been a nonsplit Cartan subgroup, which leads to $4 \mid |G|$.

In case (ii), by [19, Proposition 14] the Cartan subgroup normalised by G contains the semi-Cartan subgroup I_p (see Proposition 5.1). We use the basis where I_p is $\left(\begin{smallmatrix} 1 & 0 \\ 0 & \mathbb{F}_p^\times \end{smallmatrix}\right)$. Then the projection of $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ is in the Cartan subgroup normalised by H, thus in the index 2 cyclic subgroup of H. Since it has order 2, the index 2 cyclic subgroup of H has even order hence $4 \mid |H| \mid |G|$.

In case (iii), it is enough to note that $|A_4|$, $|S_4|$ and $|A_5|$ are all multiples of 4. ∎

5.3. 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'.

Mazur's results [16] show that a non-CM curve $E/\mathbb{Q}$ can only have isogenies with prime degree for

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

We exclude further primes with the following simple observation.

Proposition 5.6. *Assume in addition to (I)-(III) that $p \equiv 1 \pmod 4$. Then*

$$[K\colon \mathbb{Q}]/2 \equiv 0 \pmod 2$$

Proof. From the Weil pairing, $K \geqslant \mathbb{Q}(\mu_p)$ so $4 \mid [\mathbb{Q}(\mu_p)\colon \mathbb{Q}] \mid [K\colon \mathbb{Q}]$. ∎

With this and Assumption (I), we can exclude all primes but 7 and 11.

5.4. Inertia in the Borel case

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 as

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

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.

Recall that we chose K to be the minimal field over which K_∞ is a pro-p extension. Therefore K is contained in the fixed field of the unipotent subgroup of K. Then elements of G_0 (understood as cosets in G) will be written as

$$\begin{pmatrix} a & \mathbb{F}_p \\ 0 & b \end{pmatrix}$$

for $a, b \in \mathbb{F}_p^\times$. Note that by some abuse of terminology these have well-defined trace and determinant.

G_0 is isomorphic to a subgroup of $\mathbb{F}_p^\times \times \mathbb{F}_p^\times$ and is therefore Abelian. For a rational prime q, let I_q be the inertia subgroup of $\mathrm{Gal}(K/\mathbb{Q})$ at q.

The isomorphism

$$\bigwedge^2 E[p] \cong \mu_p$$

implies that the action of $\mathrm{Gal}(K/\mathbb{Q})$ on μ_p is given by the determinant on G_0. The kernel of det is $\mathrm{Gal}(K/\mathbb{Q}(\mu_p))$.

Since $\mathbb{Q}(\mu_p) \subset \mathbb{Q}(K)$, det is surjective to $\mathbb{F}_p^\times$. Moreover, $\det\colon I_p \to \mathbb{F}_p^\times$ is a bijection since both have $p-1$ elements (Prop. 5.1).

Therefore $\det\colon G_0 \to \mathbb{F}_p^\times$ belongs to split exact sequence i.e.

$$G_0 \cong \mathrm{Gal}(K/\mathbb{Q}(\mu_p)) \times I_p.$$

Proposition 5.7. *$2 \nmid [K\colon \mathbb{Q}]/2$ is equivalent to $p \equiv 3 \pmod 4$ and $2 \nmid |I_q|$ for all rational primes $q \neq p$.*

Proof. $[K\colon \mathbb{Q}] = |G_0| = |I_p| \times |\mathrm{Gal}(K/\mathbb{Q}(\mu_p))|$.

$|I_p| = p - 1$ so if $p \equiv 1 \pmod 4$ we are done, and otherwise $[K\colon \mathbb{Q}]/2 \equiv |\mathrm{Gal}(K/\mathbb{Q}(\mu_p))| \pmod 2$.

If for any $q \neq p$, I_q is contained in $\mathrm{Gal}(K/\mathbb{Q}(\mu_p))$ since $\mathbb{Q}(\mu_p)$ is unramified at q. Hence $|I_q| \mid |\mathrm{Gal}(K/\mathbb{Q}(\mu_p))|$.

In the other direction, I_q together generate all of $\mathrm{Gal}(K/\mathbb{Q}(\mu_p))$ (otherwise $\mathbb{Q}$ would have an unramified extension), so if each is odd then $\mathrm{Gal}(K/\mathbb{Q}(\mu_p))$ has odd exponent, therefore also odd order. ■

Note that our I_q for a prime $q \neq p$ is the same as Serre's ϕ_q (This follows from $p \geqslant 5$ and [19, Proposition 23 (b)]).

Proposition 5.8 (Serre [19, Section 5.6 part a)]). *Let $\mathbb{Q}_q^{\mathrm{unr}}$ be a maximal unramified extension of $\mathbb{Q}_q$ and suppose E has potentially good reduction at q. Then $|I_q|$ is the degree of the minimal extension over $\mathbb{Q}_q^{\mathrm{unr}}$ where E obtains good reduction.*

Proposition 5.9. *If $E/\mathbb{Q}$ has additive, potentially multiplicative reduction at q, $|I_q| = 2$.*

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 coefficients of E (see [21]). ■

Therefore, in particular, $|I_q| = 1$ is equivalent to E being semistable at q. Serre states that since E obtains good reduction at q (its discrimant Δ has q-valuation 0 (mod 12)) at a field extension with Galois group I_q, $|I_q| v_q(\Delta) \equiv 0 \pmod{12}$, and if $\gcd(q, 12) = 1$ then $\mid I_q \mid = \frac{12}{\gcd(12, v_q(\Delta))}$.

Note that by inspecting Serre's list of possibilites in points a_1), a_2) and a_3) of section 5.6. in [19], the only odd possibilities for $|I_q|$ are 1 and 3.

Summarizing the above, we have the following.

Theorem 5.10. *Suppose that* $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$ *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* $q \neq p$ *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.*

Note that these properties can be checked quickly by a computer as long as it can factorise the discriminant.

Proposition 5.11. *Suppose that* E *is an elliptic curve with a* p*-isogeny and* $|I_q| = 1$ *for all primes* $q \neq p$*. Let* E' *be the* p*-isogeny pair of* E*. Then either* E *or* E' *have rational* p*-torsion.*

Proof. By [19, Proposition 21 ii)], one of

$$0 \to \mathbb{Z}/p\mathbb{Z} \to E[p] \to \mu_p \to 0$$

$$0 \to \mu_p \to E[p] \to \mathbb{Z}/p\mathbb{Z} \to 0$$

is an exact sequence of Galois modules. These imply that respectively one of

$$0 \to \mu_p \to E'[p] \to \mathbb{Z}/p\mathbb{Z} \to 0$$

$$0 \to \mathbb{Z}/p\mathbb{Z} \to E'[p] \to \mu_p \to 0$$

is an exact sequence as well. ∎

Now we can rule out $p = 11$. The theorem above means that for all $q \neq 11$, $|I_q|$ is 1 or 3. The latter is impossible since I_q is a subgroup of $\mathbb{F}_{11}^{\times} \times \mathbb{F}_{11}^{\times}$ but $3 \nmid 100$. Then $I_q = 1$ for all $q \neq p$ and the proposition above implies the existence of an elliptic curve with rational 11-torsion. But there is no such curve by the work of Mazur [16].

We set $p = 7$. A result of Greenberg, Rubin, Silverberg and Stoll (Theorem 3.6 in [10]) gives a parametrisation of all E that have odd $[\mathbb{Q}(E[p]) : \mathbb{Q}]/2$, up to isogeny. G_0 is given by

$$\begin{pmatrix} \chi' & \mathbb{F}_p \\ 0 & \chi'' \end{pmatrix}$$

for characters χ', χ'', giving the action on $\ker\varphi$ and $E[p]/\ker\varphi$ respectively, where φ is a p-isogeny.

Let ω denote the character $\mathrm{Gal}(K/\mathbb{Q}) \to \mathbb{F}_p^\times$ given by action on μ_p.

Then the characters χ',χ'' restricted to I_p are $\omega^{a'}$ and $\omega^{a''}$ respectively for some a', a''. From the determinant, $\omega^{a'+a''} = \omega$ so one of a' and a'' must be even, hence the p-inertia part of a character has odd order. Since $|I_q|$ is odd for all primes $q \neq p$, one of χ' and χ'' has odd order. Changing E to its 7-isogeny pair E' interchanges χ' and χ'' so up to isogeny, we can assume that the order of χ' divides 3. Then we can adapt the theorem almost word by word, setting $k = \mathbb{Q}$.

Theorem 5.12. *Let $E/\mathbb{Q}$ be an elliptic curve and p a prime. Under Assumptions* (I)-(III), $[K\colon \mathbb{Q}]/2$, *equivalently* $[\mathbb{Q}\,(E\,[p]) : \mathbb{Q}]/2$, *is odd if and only if E has a rational 7-isogeny and there is a $v \in \mathbb{Q}$ such that E is 7-isogenous over $\mathbb{Q}$ to the elliptic curve*

$$A_{v,t}\colon y^2 + a_1(v,t)xy + a_3(v,t)y = x^3 + a_2(v,t)x^2 + a_4(v,t)x + a_6(v,t)$$

defined as in [10, Theorem 3.6], with an appropriate rational parameter t.

Remark. Here t determines the character χ'.

6. A lower bound for τ

In this section we establish $\tau \geqslant 2$ under Assumptions (I)-(IV) and the extra condition $j(E) \notin \mathbb{Z}$. Recall that K is the minimal field satisfying Assumption (III). See Proposition 3.4 for other fields in the tower.

Note that $j(E) \notin \mathbb{Z}$ guarantees $\tau \geqslant s_{E/K} \geqslant 1$ as the denominator of $j(E)$ will be divisible by some prime.

Now suppose $\tau = 1$, which is odd, therefore $p = 7$ and E has a 7-isogeny by the previous section.

6.1. 7-torsion

Suppose $|I_q| = 1$ for all primes $q \neq 7$, then by Proposition 5.11 E or its isogeny pair E' has rational 7-torsion.

Let $A \in \{E, E'\}$ be the curve with rational 7-torsion. Suppose for contradiction that E has good reduction at 2. Then its rational 7-torsion points map injectively to its reduction $\tilde{A}$ over $\mathbb{F}_2$ [21]. 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. A variant of the above argument is given in [19].

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 4.3 the reductions at these primes are all split multiplicative, which gives $2 \leqslant s_{E/K} \leqslant \tau$. Note that from parity, we have in fact $3 \leqslant \tau$. This is attained by the example given in [3].

6.2. Additive reduction at q

If the above does not hold, there is some prime $q \neq p$ with $|I_q| \neq 1$.

Let $\ell \in \mathbb{Q}$ be a rational prime dividing the denominator of the j-invariant of E i.e. a prime where E has potentially multiplicative reduction. By Theorem 5.10 this is semistable multiplicative reduction and $|I_\ell| = 1$.

We show that ℓ must decompose in K. Suppose for contradiction that ℓ does not decompose i.e. its decomposition subgroup is all of G_0. G_0 is then the quotient of the decomposition subgroup by I_ℓ, and as such it should be cyclic. Recall that $|I_q|$ must be a nontrivial factor of $|\mathbb{F}_p^\times|$. G_0 contains $I_q \times I_p$ which cannot be cyclic since $\gcd(|I_q|, |I_p|) = |I_q| > 1$.

Therefore there will be at least 3 primes in K lying over ℓ. These will all have split multiplicative reduction by Proposition 4.3, hence $3 \leqslant s_{E/K}$ and our claim follows.

7. Integral j-invariant

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 curve $X_0(p)$.*

Using Theorem 5.12, we can restrict to $p = 7$. Therefore we are looking for integral points on $X_0(7)$.

7.1. Integral points on $X_0(7)$

$X_0(7)$ has genus 0, therefore it has a rational parametrisation (see, e.g. [12])

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

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

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

Modulo a, the numerator is $7^{14}b^8$. Using $(a,b) = 1$, this is divisible by a if and only if $a \mid 7^{14}$. 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).

Moreover $t = 1$ 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 are $j \in \{3^2 \cdot 7 \cdot 2647^3, 3^2 \cdot 7^4, -3^3 \cdot 37 \cdot 719^3, 3^3 \cdot 37\}$.

7.2. Twisting

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

$$E\colon y^2 = x^3 + a_2x^2 + a_4x + a_6,$$
$$E_d\colon dy^2 = x^3 + a_2x^2 + a_4x + a_6.$$

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. [21]) 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.*

Lemma 7.3. *Let $E/\mathbb{Q}$ be an elliptic curve with a p-isogeny, having good reduction at a prime $q \neq p$. Let $\left(\frac{d}{\cdot}\right)$ be a quadratic character with conductor divisible by q. Then the order of the inertia subgroup of q in $\mathrm{Gal}(\mathbb{Q}(E_d[p])/\mathbb{Q})$ 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 Proposition 5.8. ∎

Proposition 7.4. *For any given j-invariant j_0, there are only finitely many curves $E/\mathbb{Q}$ having $j(E) = j_0$ and also satisfying Assumptions (I)-(IV) and $4 \nmid [\mathbb{Q}(E[p])\colon \mathbb{Q}]$. These curves have the same conductor apart from a possible factor of 7^2.*

Proof. Let $E/\mathbb{Q}$ be a curve with minimal conductor N_E among elliptic curves with j-invariant j_0 and satisfying the conditions. Then by our previous results, E has a rational 7-isogeny.

Let Δ be the minimal discriminant of $E/\mathbb{Q}$. If d is a square-free integer not dividing 7Δ, then there is prime $q \neq 7$ dividing d where E has good reduction. Then by the above lemma, $2 \mid |I_q|$ so by Proposition 5.7, $4 \mid [\mathbb{Q}(E_d[7])\colon \mathbb{Q}]$.

Therefore all exceptional curves with j-invariant j_0 are twists of E by some square-free divisor of 7Δ, 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 $7^2 N_E$ (since additive bad reduction appeared at p) or has a prime divisor $q \neq 7$ 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 $p \geqslant 5$ the exponent of p in the conductor of any elliptic curve with integral j-invariant is 0 or 2. ■

7.3. Calculations

Together with the list of possible j-invariants, Proposition 7.4 provides a list of all curves that could have $\tau = 1$. Using the SAGE [22] function `EllipticCurve_from_j`, we obtain a minimal conductor elliptic curve for each j-invariant involved. We take all curves with these conductors and also their -7-twists. Using Cremona's tables [7], these are

Label	j-invariant	Discriminant
$1369b1$	$3^3 \cdot 37$	-37^8
$1369b2$	$-3^3 \cdot 37 \cdot 719^3$	-37^8
$1369c1$	$3^3 \cdot 37$	-37^2
$1369c2$	$-3^3 \cdot 37 \cdot 719^3$	-37^2
$67081b1$	$3^3 \cdot 37$	$-7^6 \cdot 37^8$
$67081b2$	$-3^3 \cdot 37 \cdot 719^3$	$-7^6 \cdot 37^8$
$67081d1$	$3^3 \cdot 37$	$-7^6 \cdot 37^2$
$67081d2$	$-3^3 \cdot 37 \cdot 719^3$	$-7^6 \cdot 37^2$
$3969a1$	$3^2 \cdot 7^4$	$3^4 \cdot 7^8$
$3969a2$	$3^2 \cdot 7 \cdot 2647^3$	$3^4 \cdot 7^8$
$3969c1$	$3^2 \cdot 7^4$	$3^4 \cdot 7^2$
$3969c2$	$3^2 \cdot 7 \cdot 2647^3$	$3^4 \cdot 7^2$
$3969e1$	$3^2 \cdot 7^4$	$3^{10} \cdot 7^2$
$3969e2$	$3^2 \cdot 7 \cdot 2647^3$	$3^{10} \cdot 7^2$
$3969f1$	$3^2 \cdot 7^4$	$3^{10} \cdot 7^2$
$3969f2$	$3^2 \cdot 7 \cdot 2647^3$	$3^{10} \cdot 7^2$

Next, we use Theorem 5.10 to rule out rows with 37^2 and 3^{10} in the discriminant.

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

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

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

p	E *(label)*	*j-invariant*	*Discriminant*	*rank over* $\mathbb{Q}$
7	$1369b1$	$3^3 \cdot 37$	-37^8	1
7	$1369b2$	$-3^3 \cdot 37 \cdot 719^3$	-37^8	1
7	$67081b1$	$3^3 \cdot 37$	$-7^6 \cdot 37^8$	0
7	$67081b2$	$-3^3 \cdot 37 \cdot 719^3$	$-7^6 \cdot 37^8$	0
7	$3969a1$	$3^2 \cdot 7^4$	$3^4 \cdot 7^8$	1
7	$3969a2$	$3^2 \cdot 7 \cdot 2647^3$	$3^4 \cdot 7^8$	1
7	$3969c1$	$3^2 \cdot 7^4$	$3^4 \cdot 7^2$	0
7	$3969c2$	$3^2 \cdot 7 \cdot 2647^3$	$3^4 \cdot 7^2$	0

Note that the first and second four curves in this table form two equivalence classes: these are isomorphic or 7-isogenous over $\mathbb{Q}(\sqrt{-7}) \leqslant \mathbb{Q}(\mu_7) \leqslant K$ (for any possible K) and since λ and $s_{E/K^{\mathrm{cyc}}}$ are isogeny invariants, these have the same τ given assumptions (I)-(IV).

Remark. From these data it follows that all these curves have rank 1 over $\mathbb{Q}(\sqrt{-7})$ which is a necessary condition for $\tau = 1$. Further Iwasawa theoretic calculations would be needed to compute their λ rank (which equals their τ rank).

References

[1] K. Ardakov, *Centres of skewfields and completely faithful Iwasawa modules*, J. Inst. Math. Jussieu **7** (2008) 457-468.

[2] J. Coates, *Fragments of the GL_2 Iwasawa theory of elliptic curves without complex multiplication*, Arithmetic theory of elliptic curves (Cetraro, 1997), 1–50, Lecture Notes in Math., 1716, Springer, Berlin, 1999.

[3] 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.

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

[5] J. Coates, P. Schneider, R. Sujatha, *Modules over Iwasawa algebras*, J. Inst. Math. Jussieu **2** (2003), 73–108,

[6] J. Coates, S. Howson, *Euler characteristics and elliptic curves II*, J. Math. Soc. Japan **53** (2001), no. 1, 175-235.

[7] J. 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, vol. 4076, pages 11–29, 2006.

[8] T. Dokchitser, V. Dokchitser, *Parity of ranks for elliptic curves with a cyclic isogeny*, J. Number Theory **128** (2008), 662-679.

[9] R. Greenberg, *Iwasawa Theory for Elliptic Curves*, Arithmetic of Elliptic Curves, LNM 1716, Springer, 1999.

[10] R. Greenberg, K. Rubin, A. Silverberg, M. Stoll, *On elliptic curves with an isogeny of degree 7.* to appear in the American Journal of Mathematics,http://arxiv.org/abs/1007.4617.

[11] Y. Hachimori, O. Venjakob, *Completely faithful Selmer groups over Kummer extensions*, Documenta Mathematica, Extra Volume: Kazuya Kato's Fiftieth Birthday (2003), 478.

[12] M. 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.

[13] S. Howson, *Euler Characteristics as Invariants of Iwasawa Modules*, Proc. London Math. Soc. **85**(3) (2002), 634-658.

[14] S. Howson, *Structure of central torsion Iwasawa modules*, Bull. Soc. Math. France **130** (2002), no. 4, 507–535.

[15] H.W. Lenstra, F. Oort, *Abelian varieties having purely additive reduction*, Journal of Pure and Applied Algebra **36** (1985), 281–298.

[16] B. Mazur, *Rational isogenies of prime degree*, Inventiones Math. **44**(2) (1978), 129–162.

[17] Y. Ochi, O. Venjakob, *On ranks of Iwasawa modules over p-adic Lie extensions.* Math. Proc. Camb. Philos. Soc. **135** (2003), 25–43.

[18] D. Rohrlich. *Galois theory, elliptic curves, and root numbers*, Compositio Mathematica **100** (1996), no. 3, 311–349.

[19] J.-P. Serre. *Propriétés Galoisiennes des points d'ordre fini des courbes elliptiques*, Inventiones mathematicae **15** (1971/72), 259–331.

[20] J.-P. Serre, J. Tate, *Good reduction of abelian varieties*, The Annals of Mathematics Second Series **88** (1968), no. 3, 492–517.

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

[22] W. Stein et al., *Sage Mathematics Software (Version 5.1)*, The Sage Development Team, 2012, http://www.sagemath.org.

[23] G. Zábrádi, *Pairings and functional equations over the* GL_2*-extension*, Proc. London Math. Soc. **101**(3) (2010), 893–930.

Address: Tibor Backhausz: Trinity College, Trinity Street, CB2 1TQ Cambridge, United Kingdom.

E-mail: taback@math.elte.hu

Received: 23 May 2014; **revised:** 6 June 2014