Math. Proc. Camb. Phil. Soc. (2024), **177**, 185–218
doi:10.1017/S0305004124000197
First published online 19 September 2024

The Failure of Galois Descent for p-Selmer Groups of Elliptic Curves

BY ROSS PATERSON
School of Mathematics and Statistics, University of Glasgow, University Place, Glasgow, G12 8QQ.
e-mail: rosspatersonmath@gmail.com

(*Received* 07 *February* 2022*; accepted* 01 *May* 2024)

Abstract

We show that if F is $\mathbb{Q}$ or a multiquadratic number field, $p \in \{2, 3, 5\}$, and K/F is a Galois extension of degree a power of p, then for elliptic curves $E/\mathbb{Q}$ ordered by height, the average dimension of the p-Selmer groups of E/K is bounded. In particular, this provides a bound for the average K-rank of elliptic curves $E/\mathbb{Q}$ for such K. Additionally, we give bounds for certain representation–theoretic invariants of Mordell–Weil groups over Galois extensions of such F.

The central result is that: for each finite Galois extension K/F of number fields and prime number p, as $E/\mathbb{Q}$ varies, the difference in dimension between the Galois fixed space in the p-Selmer group of E/K and the p-Selmer group of E/F has bounded average.

2020 Mathematics Subject Classification: 11G05 (Primary); 11G07, 11N45, 14H52 (Secondary)

1. *Introduction*

As E varies amongst elliptic curves over the rational numbers (ordered by height), Bhargava and Shankar [**BS15a**] were the first to show that the average rank of the Mordell–Weil group $E(\mathbb{Q})$ is bounded. It is then natural to ask: for a fixed number field K, is the same true of $E(K)$? Moreover, what dependence does the average rank of $E(K)$ have on K? For multiquadratic extensions $K/\mathbb{Q}$, an upper bound for the average rank can be derived from the work of Bhargava–Shankar. With the exception of these bounds, we provide the first known results in this direction.

Let

$$\mathcal{E} = \left\{ (A, B) \in \mathbb{Z}^2 : \begin{array}{c} \gcd(A^3, B^2) \text{ is } 12^{th}-\text{power free}, \\ 4A^3+27B^2 \neq 0 \end{array} \right\},$$

which parametrises a set of elliptic curves via the identification $(A, B) \leftrightarrow E_{A,B} : y^2 = x^3 + Ax + B$. It is well known, see e.g. [**Sil09**, III·1], that every elliptic curve defined over the rational numbers is isomorphic to a unique curve in the set of curves parametrised by $\mathcal{E}$. The height of $(A, B) \in \mathcal{E}$, or equivalently of the curve $E_{A,B}$, is defined to be $H(A, B) = H(E_{A,B}) = \max\{4\,|A|^3\,, 27B^2\}$, and for every positive real number X, we write $\mathcal{E}(X)$ for the finite subset of $\mathcal{E}$ of pairs which have height at most X. Our main result is then:

THEOREM 1·1. *Let $p \in \{2,3,5\}$, F be either $\mathbb{Q}$ or a multiquadratic number field, and K/F be a Galois p–extension. Then*

$$\limsup_{X\to\infty} \frac{\sum_{(A,B)\in\mathcal{E}(X)} \operatorname{rk} E_{A,B}(K)}{\#\mathcal{E}(X)} \leq \begin{cases} [K:F]C_2(K/F) + [K:\mathbb{Q}]\left(C_2(F/\mathbb{Q}) + \frac{3}{2}\right) & \text{if } p=2 \text{ and } F\neq\mathbb{Q}, \\ [K:F]\left(C_p(K/F) + \frac{p+1}{p}[F:\mathbb{Q}]\right) & \text{else,} \end{cases}$$

where $C_p(K/F)$ and $C_p(F/\mathbb{Q})$ are explicit constants (see Section 1·5).

By a multiquadratic number field, we will always mean a number field F which is a finite Galois extension $F/\mathbb{Q}$ with $\mathrm{Gal}\,(F/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^r$ for some $r > 0$. For a prime number p we say that a Galois field extension K/F is a p-extension if $\mathrm{Gal}\,(K/F)$ is a finite p-group.

Remark 1·2. One can obtain stronger bounds in the case that $K/\mathbb{Q}$ is multiquadratic. These are obtained from the results of Bhargava and Shankar by computing the average size of the 5–Selmer group of the Weil restrictions of our $E/\mathbb{Q}$ from K (see Proposition 2·14).

Remark 1·3. Conditional on a conjecture of Poonen and Rains [**PR12**, conjecture 1·1(b)], the conclusion of Theorem 1·1 holds for every prime number p. In Section 1·4 we discuss the consequences of this conjecture to our results.

Remark 1·4. This average rank growth compares nicely with Iwasawa–theoretic considerations in $\mathbb{Z}_p$–towers above F, as we discuss in Section 1·6.

1·1. *Galois descent*

Theorem 1·1 arises, as is the fashion, from a detailed study of statistical properties of Selmer groups (see e.g. [**Sil09**, X·4]). For a finite Galois extension of number fields K/F and prime number p, we study the failure of Galois descent from K to F for p-Selmer groups of elliptic curves $E/\mathbb{Q}$. That is, we examine the difference

$$\dim_{\mathbb{F}_p} \mathrm{Sel}_p\,(E/K)^G - \dim_{\mathbb{F}_p} \mathrm{Sel}_p\,(E/F), \tag{1}$$

where $G = \mathrm{Gal}\,(K/F)$.

In the case that $p \nmid \#G$ this difference is 0: the finite cohomology groups $H^i(K/F, E(K)[p])$ and their local analogues are trivial, so the inflation–restriction exact sequence yields an isomorphism $\mathrm{Sel}_p\,(E/F) \cong \mathrm{Sel}_p\,(E/K)^G$ (see also Section 2 for a more geometric explanation). In other words, Galois descent does not fail in the "good characteristic" case.

The interesting case, that of so-called "bad characteristic", is when $p \mid \#G$. In this case, Galois descent can fail to an arbitrary extent. Indeed, consider the congruent number curve, which has Weierstrass equation $y^2 = x^3 - x$, and let $K/\mathbb{Q}$ be an arbitrary quadratic field. On one hand, a recent result of Morgan and the author [**MP20**, theorems 1·1 and 1·3] implies that, for any fixed positive real number z, 100% of quadratic twists E_d of E have

$$\dim_{\mathbb{F}_2} \mathrm{Sel}_2\,(E_d/K)^G = \dim_{\mathbb{F}_2} \mathrm{Sel}_2\,(E_d/K) > z;$$

https://doi.org/10.1017/S0305004124000197 Published online by Cambridge University Press

on the other hand, early work of Heath-Brown [**HB93, HB94**] shows that more than 99.9% of quadratic twists E_d of E have

$$\dim_{\mathbb{F}_2} \mathrm{Sel}_2(E_d/\mathbb{Q}) \leq 6.$$

In particular, in this latter proportion of twists the difference (1) must be arbitrarily large.

Remark 1·5. There are many more examples of this phenomenon: if $E/\mathbb{Q}$ is any elliptic curve with full 2-torsion then the result of Morgan and the author implies the same behaviour for the groups $\mathrm{Sel}_2(E_d/K)$; if additionally E has no rational 4-isogeny then the same behaviour as above is known to holds for $\mathrm{Sel}_2(E_d/\mathbb{Q})$ by work of Kane [**Kan13**, theorem 3] and Swinnerton-Dyer [**SD08**].

The core statistical result in this paper shows that, despite this, the average size of the failure of Galois descent is bounded as we vary over all elliptic curves over the rational numbers (ordered by height).

THEOREM 1·6 (Theorem 5·8). *Let p be a prime number, F be a number field and K/F be a finite Galois extension. Writing $G = \mathrm{Gal}(K/F)$, we have that*

$$\limsup_{X\to\infty} \frac{\sum_{(A,B)\in\mathcal{E}(X)} \left|\dim_{\mathbb{F}_p} \mathrm{Sel}_p(E_{A,B}/K)^G - \dim_{\mathbb{F}_p} \mathrm{Sel}_p(E_{A,B}/F)\right|}{\#\mathcal{E}(X)} \leq C_p(K/F),$$

where $C_p(K/F)$ is an explicit constant (see Section 1·5).

1·2. *Selmer ranks*

In the case of a Galois p-extension, the p-Selmer group is a modular representation of the Galois group. Appealing to the theory of such, we use Theorem 1·6 to bound the average dimension of the full Selmer group.

THEOREM 1·7 (Corollary 6·3). *Let $p \in \{2, 3, 5\}$, F be either $\mathbb{Q}$ or a multiquadratic number field, and K/F be a Galois p–extension. Then*

$$\limsup_{X\to\infty} \frac{\sum_{(A,B)\in\mathcal{E}(X)} \dim_{\mathbb{F}_p} \mathrm{Sel}_p(E_{A,B}/K)}{\#\mathcal{E}(X)}$$

$$\leq \begin{cases} [K:F]C_2(K/F) + [K:\mathbb{Q}]\left(C_2(F/\mathbb{Q}) + \frac{3}{2}\right) & \text{if } p = 2 \text{ and } F \neq \mathbb{Q}, \\ [K:F]\left(C_p(K/F) + \frac{p+1}{p}[F:\mathbb{Q}]\right) & \text{else,} \end{cases}$$

where $C_p(K/F)$ and $C_p(F/\mathbb{Q})$ are explicit constants (see Section 1·5).

It is from this result, and the usual inclusion $E(K)/pE(K) \subseteq \mathrm{Sel}_p(E/K)$, that we obtain Theorem 1·1.

Example 1·8. The bounds obtained in Theorem 1·7 are typically rather large. Let $K/\mathbb{Q}$ be the splitting field of $x^{10} - 35x^6 + 130x^4 + 160$, so that the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ is isomorphic to D_{10} the dihedral group of order 10. In this case, $F = \mathbb{Q}(\sqrt{-10})$ is a multiquadratic field contained in K, and K/F is a degree 5 extension, so we can apply Theorem

https://doi.org/10.1017/S0305004124000197 Published online by Cambridge University Press

1·7 with $p = 5$. We can compute that $C_5(K/F) \leq 8.36$. Thus we have that the average dimension of 5-Selmer groups over K of elliptic curves over $\mathbb{Q}$ is less than 54, and in particular the same bound is true of the average rank of the Mordell–Weil groups E(K).

1·3. *Mordell–Weil Lattices*

We deduce some representation–theoretic information about the "free part" of Mordell–Weil groups from Theorem 1·6. Specifically, for an elliptic curve $E/\mathbb{Q}$ and number field K write $\Lambda(E/K)$ for the so–called Mordell–Weil lattice, that is, the quotient of the group $E(K)$ by its torsion subgroup

$$\Lambda(E/K) = E(K)/E(K)_{\text{tors}}.$$

For a finite Galois extension K/F, writing $G = \text{Gal}\,(K/F)$, $\Lambda(E/K)$ is a $\mathbb{Z}$-free $\mathbb{Z}[G]$-module, i.e. a $\mathbb{Z}[G]$-module which is free as an abelian group; we refer to such modules as $\mathbb{Z}[G]$-lattices.

The integral representation theory of finite groups is more delicate than representation theory over fields. For example if for some prime number p there is a p–Sylow subgroup of G which is not cyclic of order at most p^2 then there are infinitely many isomorphism classes of indecomposable $\mathbb{Z}[G]$-lattices [**CR81**, theorem 33·6]. Moreover, the unique decomposition of representations, which holds over fields as a result of the Krull–Schmidt–Azumaya theorem [**CR81**, theorem 6·12], does not generally hold for $\mathbb{Z}[G]$–lattices, so the naïve notion of multiplicity of indecomposable sublattices need not be well defined.

We begin by providing a suitable notion of "multiplicity" for a $\mathbb{Z}[G]$–lattice Λ (see Definition 7·2) inside of $\Lambda(E/K)$, which we denote by $e_\Lambda(K/F; E)$. We then provide a bound for the average of $e_\Lambda(K/F; E)$, so long as Λ satisfies a local condition somewhere and F is a contained in a multiquadratic field.

THEOREM 1·9 (Corollary 7·8). *Let $p \in \{2, 3, 5\}$, F be either $\mathbb{Q}$ or a multiquadratic number field, and K/F be a finite Galois extension. Writing $G = \text{Gal}\,(K/F)$, we have that for every $\mathbb{Z}[G]$-lattice Λ such that $\dim_{\mathbb{F}_p} (\Lambda/p\Lambda)^G \geq 1$,*

$$\limsup_{X\to\infty} \frac{\sum_{(A,B)\in\mathcal{E}(X)} e_\Lambda(K/F; E_{A,B})}{\#\mathcal{E}(X)} \leq \frac{1}{\dim_{\mathbb{F}_p} (\Lambda/p\Lambda)^G} \cdot \begin{cases} C_2(K/F) + [F:\mathbb{Q}]\left(C_2(F/\mathbb{Q}) + \frac{3}{2}\right) & \text{if } p = 2 \text{ and } F \neq \mathbb{Q}, \\ C_p(K/F) + \frac{p+1}{p}[F:\mathbb{Q}] & \text{else,} \end{cases}$$

where $C_p(K/F)$ and $C_p(F/\mathbb{Q})$ are explicit constants (see Section 1·5).

For example, if G is a p-group then, by the orbit stabiliser theorem, for every $\mathbb{Z}[G]$-lattice Λ we have $\dim_{\mathbb{F}_p} (\Lambda/p\Lambda)^G \geq 1$. Of course, in this case these multiplicities can already be shown to be bounded by applying Theorem 1·1.

Remark 1·10. Many lattice multiplicities can already be bounded using Theorem 1·1, even when $K/\mathbb{Q}$ is not of the correct form for direct application. If $K/\mathbb{Q}$ is Galois with group G, then if one can choose a normal subgroup $N \leq G$ for which $\Lambda^N \neq 0$ then we can track the

https://doi.org/10.1017/S0305004124000197 Published online by Cambridge University Press

multiplicity by passing to the associated subfield. More precisely, in this setting if $L = K^N$ then for each $E/\mathbb{Q}$,

$$e_\Lambda(K/\mathbb{Q}; E) \leq \frac{\operatorname{rk} E(L)}{\operatorname{rk} \Lambda^N}.$$

If the subextension $L/\mathbb{Q}$ is of the correct form for Theorem 1·1, i.e. G/N is an extension of a (possibly trivial) elementary abelian 2-group by a p-group, then we can still bound the multiplicity with Theorem 1·1.

In light of the above, one may ask whether Theorem 1·9 is a formal consequence of Theorem 1·1. The following example demonstrates that this is not the case.

Example 1·11. Let $K/\mathbb{Q}$ be a finite Galois extension with Galois group $G \cong \mathbb{F}_5 \rtimes \mathbb{F}_5^\times$. Let $\mathfrak{p} \lhd \mathbb{Z}[\zeta_5]$ be the prime ideal lying over 5 in the ring of integers of the 5th cyclotomic field, upon which $\mathbb{F}_5$ acts by multiplication by ζ_5 and $\mathbb{F}_5^\times$ acts as $\operatorname{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$. It is elementary to check that the actions above induce the structure of a $\mathbb{Z}[G]$–lattice on $\mathfrak{p}$. Since $\dim_{\mathbb{F}_5}(\mathfrak{p}/5\mathfrak{p})^G = 1$, we can bound the multiplicity using Theorem 1·9.

However, Theorem 1·1 does not bound this multiplicity, even via the sophisticated application in Remark 1·10 since the action of every non-trivial normal subgroup $N \leq G$ on $\mathfrak{p}$ is without fixed points.

Our method does not allow us to bound the multiplicity of the lattice $\mathbb{Z}[\zeta_5]$ with the analogous action of G: this lattice has no G-fixed space, so for every prime number p we have that

$$(\Lambda/p\Lambda)^G \cong H^1(G, \mathbb{Z}[\zeta_5])[p],$$

and one can easily compute that $H^1(G, \mathbb{Z}[\zeta_5]) = 0$. In particular, Theorem 1·9 does not allow us to bound the average multiplicity of $\mathbb{Q}(\zeta_5)$ as an irreducible subrepresentation inside of $E(K) \otimes \mathbb{Q}$.

1·4. *Interaction with the Poonen–Rains heuristics*

Theorems 1·1, 1·7 and 1·9 all depend on p being a small prime. However this is an artefact of our current state–of–the–art, rather than an indication of special behaviour. The following is a well known conjecture in the literature.

Conjecture 1 ([**PR12**, conjecture 1·1(b)]). For each prime number p, the average of $\#\operatorname{Sel}_p(E/\mathbb{Q})$ over all $E/\mathbb{Q}$ is $p + 1$.

Conjecture 1 is known to be true already if $p \in \{2, 3, 5\}$, via the works of Bhargava and Shankar [**BS15a, BS15b, BS13**], and indeed we use this to obtain our unconditional bounds. More specifically, Conjecture 1 predicts that for every prime number p the average of $\dim_{\mathbb{F}_p} \operatorname{Sel}_p(E/\mathbb{Q})$ is at most $(p + 1)/p$.

In fact, for $p \in \{2, 3, 5\}$, Bhargava and Shankar proved that the conjectural average in Conjecture 1 is also true in the family of all elliptic curves $E/\mathbb{Q}$ satisfying finitely many congruence conditions (and indeed infinitely many, assuming some technical conditions). In light of this, we do not think it unreasonable to expect the average in Conjecture 1 to hold

https://doi.org/10.1017/S0305004124000197 Published online by Cambridge University Press

true for the family of all $E/\mathbb{Q}$ which satisfy a fixed finite number of congruence conditions. We mark this as a hypothesis for using later below:

Hypothesis 1. Let $\tilde{\mathcal{E}} \subseteq \mathcal{E}$ be a subset defined by finitely many congruence conditions, and for every positive real number X write $\tilde{\mathcal{E}}(X) = \mathcal{E}(X) \cap \tilde{\mathcal{E}}$. For each prime number p, the average of $\#\,\mathrm{Sel}_p\,(E/\mathbb{Q})$ for $E \in \tilde{\mathcal{E}}(X)$ goes to $p+1$ as $X \to \infty$.

THEOREM 1·12 (Corollary 6·3, Corollary 7·8). *Assuming Hypothesis 1, the conclusions of Theorems 1·1, 1·7 and 1·9 hold for every prime number p.*

Remark 1·13 In fact, the work in [**PR12**] predicts an exact summation for the average value of $\dim_{\mathbb{F}_p} \mathrm{Sel}_p\,(E/F)$. We have opted to work with the average size and then bound the average rank by elementary estimates so as to match up with what is currently known. This does not affect the growth in p of the bounds.

1·5. *Bound shape*

The bounds in Theorems 1·1, 1·6, 1·7 and 1·9 all depend on the constants $C_p(K/F)$ and $C_p(F/\mathbb{Q})$. We now comment on their behaviour. Explicitly, for a prime number p and finite Galois extension of number fields K/F,

$$C_p(K/F) = 2\omega_F(6p\Delta_K) + [F:\mathbb{Q}] + \delta_2(p)r_1(F) + 2\sum_{\substack{\ell prime \\ \ell \nmid 6p\Delta_K}} \omega_F(\ell)\frac{2\ell^8 - \ell^7 - 1}{\ell^{10} - 1},$$

where: $\delta_2(p) = 1$ if $p = 2$ and $\delta_2(p) = 0$ otherwise; for an integer n, $\omega_F(n)$ is the number of prime ideals of F which divide the ideal generated by n over the integers of F; $r_1(F)$ is the number of real embeddings of F; and Δ_K is the discriminant of K.

This implies some asymptotic bounds for the growth in average ranks of elliptic curves over extension fields. To ease notation somewhat, for each number field K write

$$\mathrm{Avrk}\,(K) := \limsup_{X\to\infty} \frac{1}{\#\mathcal{E}(X)} \sum_{(A,B)\in\mathcal{E}(X)} \mathrm{rk}\,E_{A,B}(K),$$

for the average rank of the K–points on elliptic curves $E/\mathbb{Q}$. Then for K/F and p as in Theorem 1·1,

$$\mathrm{Avrk}\,(K) \ll [K:\mathbb{Q}]\omega_{\mathbb{Q}}(\Delta_K), \tag{2}$$

where the implied constant is absolute. Moreover, as in Theorem 1·12, under the Poonen–Rains heuristics the same holds if we allow p to be chosen from the set of all prime numbers.

One example application is the growth of ranks in towers of number fields with restricted ramification.

Example 1·14. (Fixed base field F). Let F be $\mathbb{Q}$ or a fixed multiquadratic number field, and let $F^{(p)}$ be a pro–p extension of F that ramifies only above rational primes in a fixed

https://doi.org/10.1017/S0305004124000197 Published online by Cambridge University Press

finite set S. For each finite Galois extension K/F such that $K \subseteq F^{(p)}$, write

$$\text{Avrk}\,(K) = \limsup_{X\to\infty} \frac{1}{\mathcal{E}(X)} \sum_{(A,B)\in\mathcal{E}(X)} \text{rk}\, E(K).$$

Then the asymptotic in (2) shows that

$$\text{Avrk}\,(K) \ll [K : F],$$

that is, the average K-rank grows at most linearly in the degree of the extension. In particular this holds if $F^{(p)}$ is the limit of a ray class field tower, or if $F^{(p)}$ is a $\mathbb{Z}_p$–extension.

We can also provide a uniform bound for average ranks over infinitely many extensions.

Example 1·15. Theorem 1·1 implies that there are infinitely many S_3 number fields K for which

$$\text{Avrk}\,(K) < 65. \tag{3}$$

Indeed, for each prime number ℓ take K_ℓ to be the splitting field of $X^3 - \ell$. These are cubic extensions of their shared quadratic subfield $F = \mathbb{Q}(\zeta_3)$, so we compute that if $\ell \equiv 2 \mod 3$ then $C_3(K_\ell/F) \leq 8.44$; thus (3) holds with $K = K_\ell$.

Remark 1·16. Although we can often obtain uniform bounds for average ranks over infinitely many extensions with Galois group isomorphic to some fixed G, we cannot use these methods to obtain a bound which works for a positive proportion of such extensions. Indeed, any sensible ordering of such extensions would see the number of ramified primes grow, which in turn causes our bound to grow.

1·6. *Comparison to Iwasawa theory*

Strict rank growth control has been observed and predicted for fixed elliptic curves in a few cases; we now show some examples of this and discuss the relationship with our results. For the duration of this section, we fix a prime number p. If $p \geq 7$ then we also assume Hypothesis 1. Recasting Theorem 1·1, as in Example 1·14, we obtain a bound for rank growth in $\mathbb{Z}_p$–extensions.

COROLLARY 1·17. *Let F be $\mathbb{Q}$ or a multiquadratic number field, and let F_∞/F be a $\mathbb{Z}_p$–extension. For each integer $n \geq 1$, let F_n be the intermediate field $F \subseteq F_n \subseteq F_\infty$ such that* $\text{Gal}\,(F_n/F) \cong \mathbb{Z}/p^n\mathbb{Z}$. *Then for every integer $n \geq 1$*

$$\text{Avrk}\,(F_n) \ll p^n,$$

where the implied constant is computable and depends only on the choice of base field F.

We now compare this result with some conjectures and results in the literature for fixed elliptic curves.

Recall that the cyclotomic $\mathbb{Z}_p$–extension of a number field F is the unique subfield $F_{p-\text{cyc}} \subseteq \bigcup_{n\geq 1} F(\zeta_{p^n})$ such that $\text{Gal}\,(F_{p-\text{cyc}}/F) \cong \mathbb{Z}_p$. Work of Kato [**Kat04**] and Rohrlich [**Roh84**] (see also [**Gre01**, theorem 1·4]) shows the following: for each elliptic curve $E/\mathbb{Q}$, there is an integer C_E such that for all subfields $K \subseteq \mathbb{Q}_{p-\text{cyc}}$ we have $\text{rk}\,(E(K)) \leq C_E$

https://doi.org/10.1017/S0305004124000197 Published online by Cambridge University Press

The author is not aware of any reason to expect these C_E to be uniformly bounded across all $E/\mathbb{Q}$, in fact there is substantial debate in the area on whether even the ranks of the rational points $E(\mathbb{Q})$ are even uniformly bounded (see [**PPVW19**, section 3] for a historical survey). Moreover, prior to this work it appeared unclear whether, for example, the curves of height at most X could have C_E of order $\exp\exp(X)$ and typically attain said maximum at low levels of the tower $\mathbb{Q}_{p-\mathrm{cyc}}/\mathbb{Q}$. Corollary 1·17 shows that the hypothetical behaviour of C_E above cannot possibly occur.

Fix an imaginary quadratic field $F/\mathbb{Q}$, then for a general $\mathbb{Z}_p$–extension F_∞/F, there is the growth conjecture of Mazur [**Maz84**, section 18], as extended by Lei and Sprung [**LS20**, conjecture 1·2], which claims: if $E/\mathbb{Q}$ has good reduction at p, and F_∞ is not the anticyclotomic extension, then there is an integer $C_{E,F}$ such that for all intermediate fields F_n (as in Corollary 1·17), we ought to have $\mathrm{rk}\,(E(F_n)) \leq C_{E,F}$. As in the $\mathbb{Q}_{p-\mathrm{cyc}}$ case above, Corollary 1·17 shows that statistically this $C_{E,F}$ cannot behave wildly as $E/\mathbb{Q}$ varies. Moreover, this conjecture only accounts for the $E/\mathbb{Q}$ with *good reduction* at p, which excludes a positive proportion of elliptic curves. Corollary 1·17 suggests that, at least on average, there should not be overly fast growth of ranks for the elliptic curves with bad reduction at p.

We now consider the case that F_∞/F is the anticyclotomic extension, which is characterised by its being dihedral over $\mathbb{Q}$. The growth number proposition [**Maz84**, section 18] shows that if $E/\mathbb{Q}$ has good ordinary reduction at p, and the Néron fibre of E is geometrically connected at every place $v \mid p$ at which the extension F_∞/F splits infinitely, then for each layer F_n (as in Corollary 1·17), we must have

$$\mathrm{rk}\,(E(F_n)) = a(E, F_\infty/F)p^n + e_n(E),$$

where $\{e_n(E)\}_{n\geq 1}$ is a bounded sequence of integers associated to E, and $a(E, F_\infty/F)$ is a fixed growth constant (independent of n).

The growth number conjecture of Mazur ([**Maz84**, section 18 growth number conjecture]) predicts that (for $E/\mathbb{Q}$ as in the growth number proposition):

$$a(E, F_\infty/F) = \begin{cases} 0 & \text{if } w_E = 1, \\ 1 & \text{if } w_E = -1 \text{ and } E \text{ does not have CM by } F, \\ 2 & \text{if } w_E = -1 \text{ and } E \text{ has CM by } F. \end{cases}$$

Note that the condition $w_E = -1$ is conjectured to hold for 50% of $E/\mathbb{Q}$, and is known to hold for at least 27.5% of $E/\mathbb{Q}$ by [**BS13**, theorem 6]. The additional stipulations on E and its Néron model should again be positive proportion (and for large p this proportion tends towards 100%). In particular $a(E, F_\infty/F) > 0$ is expected to hold for a positive proportion of $E/\mathbb{Q}$, and so we should expect from this conjecture that there is *at least* linear growth of average ranks in the degree of the extension. That is, if F_∞/F is the anticyclotomic extension and for each $n \geq 1$, F_n is the nth layer of F_∞/F as in Corollary 1·17, we should expect

$$\mathrm{Avrk}\,(F_n) \gg p^n.$$

Corollary 1·17 shows that, in fact, this is not just a lower bound but is the best possible asymptotic behaviour.

https://doi.org/10.1017/S0305004124000197 Published online by Cambridge University Press

1·7. *Outline*

In Section 2 we review some well known properties of the Weil restriction of scalars. We then use these properties to obtain bounds for average dimensions of Selmer groups in "good characteristic" over multiquadratic fields.

In Section 3 we compute local norm indices for elliptic curves over unramified extensions, extending work of Kramer [**Kra81**], which may be of independent interest.

In Section 4 we recall and extend certain results and definitions from [**MP20**] to the setting of interest, and define the genus theory invariant of an elliptic curve with respect to a Galois extension and prime number p, which will represent an upper bound for the size of the obstruction to Galois descent. We then use this in Section 5 to obtain Theorem 1·6.

Following this, in Section 6 and Section 7 respectively, we use Theorem 1·6 to prove Theorem 1·7 and Theorem 1·9 At the end of Section 7 we also provide a family of examples which generalise Example 1·11.

1·8. *Limitations and extensions*

Whilst our family of curves is that of all elliptic curves over $\mathbb{Q}$, one should be able to use these methods to obtain similar results for similar sets of elliptic curves over a fixed number field ordered by height. We have opted not to do this here, since to do so requires choosing a way to extend the definition of the set $\mathcal{E}$ from $\mathbb{Q}$ to a number field. If the ideal class group of this number field is non-trivial then there can be more than one such parametrisation, so the question of how to parametrise "all elliptic curves" is nuanced.

1·9. *Notation and conventions*

For a field F of characteristic 0, we write $\bar{F}$ for a (fixed once and for all) algebraic closure of F, and denote its absolute Galois group by $G_F = \mathrm{Gal}\,(\bar{F}/F)$. By a G_F-module M we mean a discrete abelian group M on which G_F acts continuously, and for each $i \geq 0$ we write $H^i(F, M)$ as a shorthand for the continuous cohomology groups $H^i(G_F, M)$. If moreover M is p-torsion for some prime number p then we say that M is an $\mathbb{F}_p[G_F]$-module, and for $V \subseteq H^i(F, M)$ we write $\dim V$ for the $\mathbb{F}_p$-dimension of V. For such M, we define the *dual* of M to be

$$M^* := \mathrm{Hom}\,(M, \boldsymbol{\mu}_p),$$

where $\boldsymbol{\mu}_p$ is the G_F-module of pth roots of unity in $\bar{F}$. This is an $\mathbb{F}_p[G_F]$-module with action given as follows: for $\sigma \in G_F$, $\phi \in M^*$ and $m \in M$,

$$^{\sigma}\phi(m) = \sigma\phi(\sigma^{-1}m).$$

For $i \geq 0$, if L/F is a finite extension we denote the corresponding restriction and corestriction maps by

$$\mathrm{res}_{L/F} : H^i(F, M) \to H^i(L, M)$$

and

$$\mathrm{cor}_{L/F} : H^i(L, M) \to H^i(F, M),$$

respectively.

For a number field F, we write Ω_F for the set of places of F and for each $v \in \Omega_F$ we write F_v for the completion of F at v. For each $v \in \Omega_F$ we fix (once and for all) an embedding

https://doi.org/10.1017/S0305004124000197 Published online by Cambridge University Press

$\bar{F} \hookrightarrow \bar{F}_v$, and so an inclusion $G_{F_v} \subseteq G_F$. Thus each G_F-module M is naturally a G_{F_v}-module and moreover when v is non-archimedean (finite), we denote by F_v^{nr} the maximal unramified extension of F_v, and write

$$H^1_{\mathrm{nr}}(F_v, M) = \ker\left(H^1(F_v, M) \xrightarrow{\mathrm{res}} H^1(F_v^{\mathrm{nr}}, M)\right)$$

for the subgroup of unramified classes.

For a number field F, an elliptic curve E/F and a finite place $v \in \Omega_F$, when we describe the reduction type of E at v we are implicitly referring to the type of E in the Kodaira–Néron classification (see e.g. [**Sil94**, IV theorem 8·2]).

By an arithmetic function, we mean a function $f : \mathbb{Z} \to \mathbb{C}$ such that for each $n \in \mathbb{Z}$ we have $f(-n) = f(n)$. We denote by μ the Möbius function and by gcd the greatest common divisor function, each extended from $\mathbb{N}$ to $\mathbb{Z}$ by composition with the archimedean absolute value. For arithmetic functions f and g, we denote by $f * g$ the Dirichlet convolution of the two, i.e. for each $n \in \mathbb{Z}$

$$(f * g)(n) := \sum_{d|n} f(d)g(n/d),$$

where the sum is over positive divisors of n. We say that an arithmetic function f is multiplicative if for coprime integers $m, n \in \mathbb{Z}$ we have that $f(mn) = f(m)f(n)$.

For each prime number ℓ we write v_ℓ for the normalised valuation on $\mathbb{Q}_\ell$, i.e. the unique valuation such that $v_\ell(\ell) = 1$.

2. *Good characteristic: Weil restriction*

For the duration of this section, fix a finite Galois extension of number fields K/F and an elliptic curve $E/\mathbb{Q}$, and write $G = \mathrm{Gal}(K/F)$. We begin in Section 2·1 with expository material on twists of elliptic curves and the Weil restriction. In Section 2·2 we then go on to survey some results on p-Selmer groups in extensions of degree coprime to p. This material is closely related to, and inspired by, that appearing in [**MR07**, section 3]. Finally, in Section 2·3, we explain how this material allows us to extend the results of Bhargava and Shankar bhargava3Sel,bhargava5Sel on the average dimension of 3- and 5-Selmer groups over $\mathbb{Q}$ to a bound for the average dimension of 3- and 5-Selmer groups over any multiquadratic number field.

2·1. *Twists of elliptic curves*

As in Milne [**Mil72**, section 2] (see also [**MRS07**]), there is a general construction of twists of powers of an elliptic curve, which we now recall.

Definition 2·1. Let $n \geq 1$. To each matrix $M = (m_{i,j})$ in $\mathrm{Mat}_n(\mathbb{Z})$ we can associate an endomorphism of E^n given by

$$(P_1, ..., P_n) \longmapsto \left(\sum_{j=1}^{n} m_{1,j}P_j, ..., \sum_{j=1}^{n} m_{n,j}P_j\right).$$

In this way we view $\mathrm{GL}_n(\mathbb{Z})$ as a subgroup of $\mathrm{Aut}_F(E^n)$. Now suppose that Λ is a free rank-n $\mathbb{Z}$-module equipped with a continuous G_F-action. Choosing a basis for Λ gives rise

https://doi.org/10.1017/S0305004124000197 Published online by Cambridge University Press

to a homomorphism

$$\rho_\Lambda : G_F \longrightarrow \mathrm{GL}_n(\mathbb{Z}),$$

which we view as a 1-cocycle valued in $\mathrm{Aut}_{\bar{F}}(E^n)$. The class of ρ_Λ in $H^1(F, \mathrm{Aut}_{\bar{F}}(E^n))$ does not depend on the choice of basis. Associated to this cocycle class is a twist of E^n, which we denote $\Lambda \otimes E$. This is an abelian variety over F of dimension n, equipped with a $\bar{F}$-isomorphism $\varphi_\Lambda : E^n \to \Lambda \otimes E$ satisfying $\varphi_\Lambda^{-1}\varphi_\Lambda^\sigma = \rho_\Lambda(\sigma)$ for all $\sigma \in G_F$.

The Weil restriction of E can now be defined as a specific example of such a twist.

Definition 2·2. The Weil restriction of E from K to F is the abelian variety

$$\mathrm{Res}_{K/F} E = \mathbb{Z}[G] \otimes E.$$

Remark 2·3. The Weil restriction $\mathrm{Res}_{K/F}E$ is classically defined as the unique scheme over F representing the functor on F-schemes

$$T \longmapsto E(T \times_F K).$$

As in [**MRS07**, theorem 4·1], this is equivalent to the construction given above.

2·2. *Selmer groups in good characteristic*

Here we remark on the structure of n-Selmer groups in the case that n is coprime to $\#G$, the case of so–called "good characteristic". In this case, the n-Selmer group splits as a sum over twists of E. This can be viewed as a finite-level explication of the results in [**MR07**, section 3], where similar results are shown for Pontrjagin dual p^∞–Selmer vector spaces without our restriction on p.

LEMMA 2·4. *For every positive integer n, not necessarily coprime to #G,*

(i) *there is a natural isomorphism of $\mathbb{Z}[G_F]$–modules*

$$\mathrm{Res}_{K/F} E[n] \cong \mathbb{Z}[G] \otimes_{\mathbb{Z}} E[n],$$

where $\sigma \in G_F$ acts on the right-hand side diagonally;

(ii) *the above isomorphism induces an isomorphism of $\mathbb{Z}[G]$–modules*

$$\mathrm{Sel}_n\,(\,\mathrm{Res}_{K/F}\, E/F) \cong \mathrm{Sel}_n\,(E/K),$$

where the action of G on the left-hand side is induced by the action of G on $\mathbb{Z}[G]$ by left multiplication.

Proof. (i) is found in [**MRS07**, theorem 2·2(ii)], see also [**Mil72**, section 1(a)]. For (ii), we give an analogous argument to that in [**MR07**, proof of proposition 3·1(iii)], see also [**Mil72**, proof of theorem 1] for a similar result for Shafarevich–Tate groups. Indeed, by (i), Shapiro's lemma (see, e.g. [**Neu13**, theorem 4·9]) provides a $\mathbb{Z}[G]$ isomorphism

$$H^1(F, (\,\mathrm{Res}_{K/F}\, E)[n]) \cong H^1(K, E[n]),$$

https://doi.org/10.1017/S0305004124000197 Published online by Cambridge University Press

where the action of G on the left-hand side is induced by left multiplication on $\mathbb{Z}[G]$ in the isomorphism of (i). It is then elementary to check that this isomorphism commutes with the corresponding isomorphisms at the local extensions, and thus restricts to one of Selmer groups.

Definition 2·5. Let ρ be an irreducible finite dimensional $\mathbb{Q}[G]$–module. As in [**MRS07**, definition 4·3] we define the twist of E by ρ to be

$$E_\rho = (\mathbb{Q}[G]_\rho \cap \mathbb{Z}[G]) \otimes E,$$

where $\mathbb{Q}[G]_\rho$ is the ρ-isotypic component of $\mathbb{Q}[G]$, that is, the sum of all left ideals of $\mathbb{Q}[G]$ isomorphic to ρ.

Example 2·6. If K/F is multiquadratic then these twists are extremely concrete. Since G is an elementary abelian 2 group, its irreducible representations are order 2 characters induced by the quadratic subextensions. Let $\Delta \in F$ be an element such that $F(\sqrt{\Delta}) \subseteq K$, and let χ_Δ be the corresponding at–most–quadratic character of G_F. Identifying χ_Δ with its corresponding one dimensional $\mathbb{Q}[G]$-module, this construction gives rise to all irreducible finite-dimensional $\mathbb{Q}[G]$-modules. Moreover, it is clear that $\mathbb{Q}[G]_{\chi_\Delta} \cap \mathbb{Z}[G]$ is a rank one free abelian group with action of $\sigma \in G$ given by multiplication by $\chi_\Delta(\sigma)$. In particular, by [**MRS07**, theorem 2·2(i)] we obtain that $E_{\chi_\Delta} = E^{(\Delta)}$ is just the usual quadratic twist of E by Δ.

We can then split the n-Selmer group of the Weil restriction into those of these twists. This result is analogous to [**MR07**, corollary 3·7], where they study the Pontrjagin dual Selmer vector spaces.

PROPOSITION 2·7. *If n is an integer which is coprime to $\#G$, then we have an isomorphism of $\mathbb{Z}[G]$-modules*

$$\mathrm{Sel}_n(E/K) \cong \bigoplus_\rho \mathrm{Sel}_n(E_\rho/F),$$

where the sum is over isomorphism classes of irreducible finite dimensional $\mathbb{Q}[G]$-modules and the action of G on the summands on the right hand side is induced by the action of G on $\mathbb{Q}[G]_\rho \cap \mathbb{Z}[G]$ via the isomorphism in Lemma 2·4(i).

Proof. By Lemma 2·4 we need only show that $\mathrm{Sel}_n(\mathrm{Res}_{K/F} E/F)$ splits in this way. The natural map

$$f : \bigoplus_\rho \left(\mathbb{Z}[G] \cap \mathbb{Q}[G]_\rho\right) \to \mathbb{Z}[G],$$

is injective with finite cokernel, so by [**MRS07**, theorem 4·5, see also lemma 2·4] induces an F–isogeny

$$f_E : \bigoplus_\rho E_\rho \to \mathrm{Res}_{K/F} E.$$

Moreover, since the cokernel of f is $\#G$–torsion, the degree of the isogeny f_E must be a divisor of some power of $\#G$ [**MRS07**, proof of lemma 2·4] and so coprime to n. In particular,

https://doi.org/10.1017/S0305004124000197 Published online by Cambridge University Press

f_E induces an isomorphism of n–Selmer groups, and moreover since f_E is an F–isogeny the isomorphism is one of $\mathbb{Z}[G]$–modules.

Remark 2·8. In [**MR07**, corollary 3·7] the authors do not need to make assumptions about coprimality, since the error that occurs when $p \mid \#G$ contributes an additional torsion module to the p^∞-Selmer groups. This in turn vanishes when taking the tensor product with $\mathbb{Q}_p$ to form the Pontrjagin dual Selmer vector space $\mathrm{Hom}(\mathrm{Sel}_{p^\infty}(E/K), \mathbb{Q}_p/\mathbb{Z}_p) \otimes \mathbb{Q}_p$.

2·3. *Average selmer ranks in good characteristic over multiquadratic fields*

In this subsection, we will restrict our interest to multiquadratic number fields. We use the Weil restriction as in Section 2 to give a bound for Selmer ranks in good characteristic using results of Bhargava and Shankar [**BS15b, BS13**]. First, we adapt the results of Bhargava–Shankar for quadratic twists.

PROPOSITION 2·9. *For each squarefree integer D and $p \in \{2, 3, 5\}$, we have*

$$\lim_{X\to\infty} \frac{\sum_{(A,B)\in\mathcal{E}(X)} \#\,\mathrm{Sel}_p\,(E^{(D)}_{A,B}/\mathbb{Q})}{\#\mathcal{E}(X)} = (p+1).$$

Moreover, assuming Hypothesis 1 the conclusion holds for every prime number p.

Remark 2·10. For $p \in \{2, 3, 5\}$ this can be seen directly from the methods of Bhargava–Shankar [**BS15a**], since the quadratic twist $E^{(D)}_{A,B}$ has a (possibly not minimal)Weierstrass equation given by $E_{AD^2,BD^3} : y^2 = x^3 + AD^2x + BD^3$, and their proofs never make use of the minimality condition and work with finitely many congruence conditions. However, for completeness (and when $p > 5$) we provide a proof below.

Proof. Fix a squarefree integer D. Since the quadratic twist $E^{(D)}_{A,B}$ has a (possibly not minimal) Weierstrass equation given by $E_{AD^2,BD^3} : y^2 = x^3 + AD^2x + BD^3$. Thus there is a bijection between $\left\{E^{(D)}_{A,B} : (A, B) \in \mathcal{E}(X)\right\}$ and the set

$$\mathcal{E}_D(X) = \left\{ (A,B) \in \mathbb{Z}^2 : \begin{array}{c} 4|A|^3, 27B^2 \le D^6X; \\ D^2|A,\ D^3|B; \\ 4A^3+27B^2 \neq 0; \\ \forall \ell \nmid D \text{ prime, if } \ell^4|A \text{ then } \ell^6 \nmid B; \\ \forall \ell | D \text{ prime, if } \ell^6|A \text{ then } \ell^9 \nmid B \end{array} \right\},$$

given by identifying $(A, B) \in \mathcal{E}_D(X)$ with the curve $E_{A,B}$. We now partition $\mathcal{E}_D(X)$ into parts, so as to identify with minimal Weierstrass models. For each pair (d_1, d_2) of positive squarefree integers such that $D = \pm d_1 d_2$, we define

$$\mathcal{E}_{d_1,d_2}(X) = \left\{ (A,B) \in \mathcal{E}(D^6X) : \begin{array}{c} 4|A|^3, 27B^2 \le \left(\frac{d_1}{d_2}\right)^6 X; \\ 4A^3+27B^2 \neq 0; \\ \forall \ell \nmid d_1 d_2 \text{ prime, if } \ell^4|A \text{ then } \ell^6 \nmid B; \\ \forall \ell | d_1 \text{ prime: } \ell^2|A,\ \ell^3|B, \text{ and if } \ell^4|A \text{ then } \ell^6 \nmid B; \\ \forall \ell | d_2 \text{ prime: if } \ell^2|A \text{ then } \ell^3 \nmid B. \end{array} \right\}.$$

https://doi.org/10.1017/S0305004124000197 Published online by Cambridge University Press

Note that $\mathcal{E}_{d_1,d_2}(X) \subseteq \mathcal{E}\left(((d_1)/d_2)^6 X\right)$, and moreover $\mathcal{E}_{d_1,d_2}(X)$ parametrises a large family of elliptic curves ordered by naïve height in the sense of Bhargava–Shankar [**BS15a**, **BS15b**, **BS13**]. Further, we have that

$$\mathcal{E}_D(X) = \bigsqcup_{D=\pm d_1 d_2} \left\{(d_2^4 A, d_2^6 B) : (A,B) \in \mathcal{E}_{d_1,d_2}(X)\right\},$$

where the disjoint union is over pairs of squarefree positive integers d_1, d_2 satisfying $D = \pm d_1 d_2$.

Note that for any fixed pair of squarefree positive integers d_1, d_2 we have by [**BS15a**, theorem 3·17] that

$$\begin{aligned}\lim_{X\to\infty} \frac{\#\mathcal{E}_{d_1,d_2}(X)}{\#\mathcal{E}(X)} &= \left(\prod_{\substack{\ell \mid d_1 \\ \text{prime}}} \frac{(\ell^2-1)\ell^3 + (\ell^3-1)}{\ell^{10}-1}\right)\left(\prod_{\substack{\ell \mid d_2 \\ \text{prime}}} \frac{\ell^2(\ell^2-1)\ell^6 + \ell^2(\ell^3-1)\ell^3}{\ell^{10}-1}\right) \\ &= d_2^5 \left(\prod_{\substack{\ell \mid D \\ \text{prime}}} \frac{\ell^5-1}{\ell^{10}-1}\right).\end{aligned}$$

Thus,

$$\begin{aligned}&\lim_{X\to\infty} \frac{1}{\#\mathcal{E}(X)} \sum_{(A,B)\in\mathcal{E}(X)} \#\operatorname{Sel}_p\left(E_{A,B}^{(D)}/\mathbb{Q}\right) \\ &= \lim_{X\to\infty} \frac{1}{\#\mathcal{E}(X)} \sum_{(A,B)\in\mathcal{E}_D(X)} \#\operatorname{Sel}_p\left(E_{A,B}/\mathbb{Q}\right) \\ &= \lim_{X\to\infty} \frac{1}{\#\mathcal{E}(X)} \sum_{D=\pm d_1 d_2} \sum_{(A,B)\in\mathcal{E}_{d_1,d_2}(X)} \#\operatorname{Sel}_p\left(E_{A,B}/\mathbb{Q}\right) \\ &= (p+1)\left(\prod_{\substack{\ell \mid D \\ \text{prime}}} \frac{\ell^5-1}{\ell^{10}-1}\right)\sum_{d\mid D} d^5 \\ &= (p+1),\end{aligned}$$

where the penultimate equality follows from the large family average Selmer group sizes in [**BS15a**, **BS15b**, **BS13**] and the computation above, and the final follows from an elementary identity for power-of-divisor sums.

Assuming Hypothesis 1, since the families $\mathcal{E}_{d_1,d_2}(X)$ are defined by finitely many congruence conditions, the argument above holds for all prime numbers p.

https://doi.org/10.1017/S0305004124000197 Published online by Cambridge University Press

We can then relate this to our ordering via elementary estimates, and similarly obtain a bound for the average Selmer rank.

PROPOSITION 2·11. *For each squarefree integer D and $p \in \{2, 3, 5\}$, we have*

$$\limsup_{X\to\infty} \frac{\sum_{(A,B)\in\mathcal{E}(X)} \dim \mathrm{Sel}_p\,(E^{(D)}_{A,B}/\mathbb{Q})}{\#\mathcal{E}(X)} \leq \frac{(p+1)}{p}.$$

Moreover, assuming Hypothesis 1 the same is true for every prime number p.

Proof. For each $r \geq 0$ we use the inequality $p^r \geq pr$, so for each $E/\mathbb{Q}$ we have $\dim \mathrm{Sel}_p\,(E/\mathbb{Q}) \leq \#\,\mathrm{Sel}_p\,(E/\mathbb{Q})/p$. Thus it follows from Proposition 2·9.

Definition 2·12. For a squarefree integer D, we write χ_D for the quadratic character of $G_\mathbb{Q}$ cutting out $\mathbb{Q}(\sqrt{D})$, and for an abelian group M we write M^{χ_D} for the discrete $G_\mathbb{Q}$-module M with action by $\sigma \in G_\mathbb{Q}$ given by multiplication by $\chi_D(\sigma) \in \{\pm 1\}$.

LEMMA 2·13. *Let F be a field contained in a multiquadratic number field, write $G = \mathrm{Gal}\,(F/\mathbb{Q})$, and let $E/\mathbb{Q}$ be an elliptic curve. Then for every odd prime number p there is an isomorphism of $\mathbb{Z}[G]$-modules*

$$\mathrm{Sel}_p\,(E/F) \cong \bigoplus_{D\in\mathcal{Q}(F)} \mathrm{Sel}_p\,(E^{(D)}/\mathbb{Q})^{\chi_D},$$

where $\mathcal{Q}(F)$ is the set of squarefree integers D such that $\mathbb{Q}(\sqrt{D}) \subseteq F$ and $E^{(D)}$ is the quadratic twist of E by D.

Proof. This follows by applying Proposition 2·7 to multiquadratic extensions as in Example 2·6.

Now we can state an easy statistical consequence of the decomposition in Lemma 2·13.

PROPOSITION 2·14. *Let F be either $\mathbb{Q}$ or a multiquadratic number field. Then for $p \in \{3, 5\}$,*

$$\limsup_{X\to\infty} \frac{\sum_{(A,B)\in\mathcal{E}(X)} \dim \mathrm{Sel}_p\,(E_{A,B}/F)}{\#\mathcal{E}(X)} \leq \frac{p+1}{p}[F:\mathbb{Q}],$$

Moreover, assuming Hypothesis 1 the same holds for all odd prime numbers p.

Proof. Let p be an odd prime number. Using the decomposition in Lemma 2·13,

$$\dim \mathrm{Sel}_p\,(E/F) = \sum_{D\in\mathcal{Q}(F)} \dim \mathrm{Sel}_p\,(E^{(D)}/\mathbb{Q}),$$

where $E^{(D)}$ is the quadratic twist of E by D and $\mathcal{Q}(F)$ is the set of squarefree integers D such that $\mathbb{Q}(\sqrt{D}) \subseteq F$. The result now follows from Proposition 2·11, noting that the size of $\mathcal{Q}(F)$ is precisely $[F:\mathbb{Q}]$.

https://doi.org/10.1017/S0305004124000197 Published online by Cambridge University Press

3. *Local computations*

In this section, let $F, \mathcal{O}_F, v$ be a finite extension of $\mathbb{Q}_\ell$ for some prime number ℓ, its ring of integers and normalised valuation, respectively and let E/F be an elliptic curve with multiplicative reduction. Moreover, let K/F be an unramified extension, let n be its degree and write $N_{K/F} = \sum_{g \in \mathrm{Gal}\,(K/F)} g \in \mathbb{Z}[\,\mathrm{Gal}\,(K/F)]$ for the usual norm element. We perform some local computations, extending results of Kramer [**Kra81**] in the case $n = 2$. Specifically, we determine the norm index for such E using the Tate parametrisation (see e.g. [**Sil94**, V sections 3-5]), the properties of which we recall below.

Recall from [**Sil94**, V Thms 3·1 and 5·3] that there is a unique element $q \in \mathcal{O}_F$ with $v(q) > 0$ such that E is isomorphic over $\bar{F}$ to $\mathbb{G}_m/q^{\mathbb{Z}}$. We call q the Tate parameter associated to E, and fix such an isomorphism and call it the Tate parametrisation. Moreover, if E has split multiplicative reduction, then we may assume that the Tate parametrisation is defined over F.

Let L/F be the unramified quadratic extension, and for each extension M/F define

$$I(M) := \left\{x \in (M \cdot L)^\times : N_{(M\cdot L)/M}(x) \in q^{\mathbb{Z}}\right\},$$

$$I_0(M) := \left\{x \in (M \cdot L)^\times : N_{(M\cdot L)/M}(x) = 1\right\}.$$

If E has non-split multiplicative reduction, then the quadratic twist of E by L has split multiplicative reduction, so we may assume that the Tate parametrisation is defined over any field containing L. However, for a finite extension M/F which does not contain L, by [**Sil94**, V corollary 5·4] the Tate parametrisation over the compositum $M \cdot L$ yields an isomorphism between $E(M)$ and $I(M)/q^{\mathbb{Z}}$. This isomorphism identifies $E_0(M)$, the points of the connected component of the identity in the Néron model of E, with $I_0(M)/q^{\mathbb{Z}}$.

LEMMA 3·1. *If E/F has split multiplicative reduction, then the corresponding Tate parameter q satisfies*

$$v(q) = v(\Delta_E),$$

where Δ_E is a minimal discriminant for E/F.

Proof. By [**Sil94**, V theorem 3·1(b)] we have $\Delta_E = q\prod_{n\geq 1}(1-q^n)^{24}$, so the result is immediate.

PROPOSITION 3·2. *If E/F has split multiplicative reduction, then*

$$E(F)/N_{K/F}E(K) \cong \mathbb{Z}/\gcd(v(\Delta_E), n)\mathbb{Z},$$

where Δ_E is a minimal discriminant for E/F.

Proof. If E has Tate parameter $q \in \mathcal{O}_F$ then, since the Tate parametrisation is defined over F, we have a commutative square

$$\begin{array}{ccc} E(K) & \xrightarrow{\sim} & K^\times/q^{\mathbb{Z}} \\ \downarrow{\scriptstyle N_{K/F}} & & \downarrow{\scriptstyle N_{K/F}} \\ E(F) & \xrightarrow{\sim} & F^\times/q^{\mathbb{Z}}, \end{array}$$

https://doi.org/10.1017/S0305004124000197 Published online by Cambridge University Press

and so

$$E(F)/N_{K/F}(E(K)) \cong F^\times / \left(N_{K/F}(K^\times) \cdot q^{\mathbb{Z}}\right).$$

Since the extension K/F is unramified, local class field theory identifies the exact sequence

$$0 \longrightarrow \frac{q^{\mathbb{Z}}}{q^{\mathbb{Z}} \cap N(K^\times)} \longrightarrow \frac{F^\times}{N_{K/F}(K^\times)} \longrightarrow \frac{F^\times}{\left(N_{K/F}(K^\times) \cdot q^{\mathbb{Z}}\right)} \longrightarrow 0,$$

with

$$0 \longrightarrow \langle v(q) \rangle \longrightarrow \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/\gcd(v(q), n)\mathbb{Z} \longrightarrow 0\ .$$

The result now follows from Lemma 3·1.

PROPOSITION 3·3. *If E/F has non-split multiplicative reduction and $n \in 2\mathbb{Z}$, then*

$$\#\left(E(F)/N_{K/F}E(K)\right) = \begin{cases} 2 & \text{if } v(\Delta_E) \in 2\mathbb{Z}, \\ 1 & \text{else.} \end{cases}$$

Proof. By assumption E has split multiplicative reduction over the unramified quadratic extension L/F, which is contained in K. Write $\tau \in \mathrm{Gal}(K/F)$ for the Frobenius element, so that $N_{K/F} = \sum_{k=0}^{n-1} \tau^k$, and L/F is the fixed field of the group generated by τ^2. The Tate parametrisation of E/K gives a commutative diagram

$$\begin{array}{ccc} E(K) & \xrightarrow{\sim} & K^\times/q^{\mathbb{Z}} \\ \downarrow{\scriptstyle N_{K/F}} & & \vdots{\scriptstyle \alpha} \\ E(F) & \xrightarrow{\sim} & I(F)/q^{\mathbb{Z}}, \end{array}$$

where since the norm map $N_{K/F}$ factors through the field L over which the Tate parametrisation is defined, the rightmost vertical map α is induced by the action of the element $\sum_{k=0}^{n-1} \chi_L(\tau^k)\tau^k$, where χ_L is the quadratic character cutting out the extension L/F. Note that for $x \in K^\times/q^{\mathbb{Z}}$

$$\alpha(x) = \prod_{k=1}^{n/2} \frac{\tau^{2k}(x)}{\tau^{2k+1}(x)} = \prod_{k=1}^{n/2} \tau^{2k}\left(\frac{x}{\tau(x)}\right) = N_{K/L}\left(\frac{x}{\tau(x)}\right).$$

Thus, since by Hilbert's theorem 90 we have

$$\left\{\frac{x}{\tau(x)} : x \in K^\times\right\} = \ker\left(N_{K/F} : K^\times \to F^\times\right),$$

we obtain that

$$\begin{aligned} E(F)/N_{K/F}(E(K)) &\cong \frac{I(F)}{N_{K/L}(\ker(N_{K/F})) \cdot q^{\mathbb{Z}}} \\ &\cong \frac{N_{L/F}(L^\times) \cap q^{\mathbb{Z}}}{q^{2\mathbb{Z}}}, \end{aligned}$$

where since the norm map is surjective on units in unramified extensions, in particular $\ker(N_{L/F}) \cap I(F) \subseteq N_{K/L}(\ker(N_{K/F}))$, the final isomorphism is just obtained by pushing through the map $N_{L/F}$. It is then clear that the size of this norm index is at most 2, and is 2

https://doi.org/10.1017/S0305004124000197 Published online by Cambridge University Press

precisely when q is a norm from L, which by local class field theory occurs precisely when $v(q)$ is even. The result then follows from Lemma 3·1.

PROPOSITION 3·4. *If E/F has non-split multiplicative reduction, and n is odd then*

$$\#\left(E(F)/N_{K/F}E(K)\right) = 1.$$

Proof. Let χ_L be the character associated to the unramified quadratic extension L/F and write $\mathrm{Gal}\,(K\cdot L/F) = \langle \tau : \tau^{2n} = 1\rangle$. Letting U denote units, we consider the map f given by the composition

$$U_{K\cdot L} \xrightarrow{\tilde{f}} I_0(K) \xrightarrow{Q} E_0(K),$$

where for $u \in U_{K\cdot L}$ we set $\tilde{f}(u) := u/\tau^n(u)$ and Q is the Tate parametrisation map. By Hilbert's theorem 90 and the fact that the extension $K\cdot L/K$ is unramified, the map $\tilde{f}$ is surjective and so since Q is also surjective we must have that f is a surjection. Moreover for each $u \in U_{K\cdot L}$,

$$\begin{aligned} f(u) &= Q\left(\frac{u}{\tau^n(u)}\right) \\ &= Q(u) - Q\left(\tau^n(u)\right) \\ &= Q(u) - \chi_L(\tau^n)\tau^n\left(Q(u)\right) \\ &= Q(u) + \tau^n\left(Q(u)\right) \\ &= N_{K\cdot L/K}(Q(u)). \end{aligned}$$

Identifying $N_{K/F} = \sum_{k=0}^{n} \tau^{2k}$, we obtain a commutative square

$$\begin{array}{ccc} U_{K\cdot L} & \xrightarrow{f} & E_0(K) \\ \downarrow{\scriptstyle N_{K/F}} & & \downarrow{\scriptstyle N_{K/F}} \\ U_L & \xrightarrow{f} & E_0(F). \end{array}$$

In particular, the right-hand vertical map is now a surjection since the left is by local class field theory. This then means that $E_0(F) = N_{K/F}E_0(K) \subseteq N_{K/F}E(F)$, so in particular we have a natural surjection

$$E(F)/E_0(F) \twoheadrightarrow E(F)/N_{K/F}E(K).$$

Since E has non-split multiplicative reduction, so has Tamagawa number 1 or 2, we must have that $E(F)/N_{K/F}E(K)$, which has odd order as it is a quotient of $E(F)/nE(F)$, is trivial.

Our main application of the above results will be when E/F has reduction type I_1.

LEMMA 3·5. *If E/F has reduction type I_1, then the norm is a surjection*

$$N_{K/F} : E(K) \twoheadrightarrow E(F).$$

Proof. By Tate's algorithm (see Lemma 5·1), if E/F has reduction type I_1 then $v(\Delta_E) = 1$. Thus the claim follows from Propositions 3·2, 3·3, and 3·4.

https://doi.org/10.1017/S0305004124000197 Published online by Cambridge University Press

4. *The (co)-restriction Selmer groups*

We will now review the properties of Selmer structures and their associated Selmer groups, before going on to extend some definitions and basic results from [**MP20**, section 4]. More details on Selmer structures can be found in [**Was97, MR04**] and the references therein.

For the duration of this section let F be a number field, K/F be a finite Galois extension and G be its Galois group. Moreover, let E/F be an elliptic curve and p be a prime number.

Definition 4·1. A *Selmer structure* $\mathcal{L} = \{\mathcal{L}_v\}_v$ for a finite $\mathbb{F}_p[G_F]$-module M is a collection of subgroups

$$\mathcal{L}_v \subseteq H^1(F_v, M),$$

one for each $v \in \Omega_F$, such that $\mathcal{L}_v = H^1_{\mathrm{nr}}(F_v, M)$ for all but finitely many v. The associated *Selmer group* $\mathrm{Sel}_{\mathcal{L}}(F, M)$ is defined by the exactness of the sequence

$$0 \to \mathrm{Sel}_{\mathcal{L}}(F, M) \to H^1(F, M) \to \prod_{v \in \Omega_F} H^1(F_v, M)/\mathcal{L}_v.$$

For each $v \in \Omega_F$ we write $\mathcal{L}_v^*$ for the orthogonal complement of $\mathcal{L}_v$ with respect to the local Tate pairing, so that $\mathcal{L}_v^* \subseteq H^1(F_v, M^*)$. We then define the *dual Selmer structure* $\mathcal{L}^*$ for M^* by taking $\mathcal{L}^* = \{\mathcal{L}_v^*\}$, and refer to $\{\mathrm{Sel}_{\mathcal{L}^*}\}(F, M^*)$ as the *dual Selmer group*.

The following theorem describes the difference in dimension between a Selmer group and its dual.

THEOREM 4·2 (Greenberg–Wiles). *Let $\mathcal{L} = \{\mathcal{L}_v\}_v$ be a Selmer structure for a finite $\mathbb{F}_p[G_F]$-module M. Then we have*

$$\dim \mathrm{Sel}_{\mathcal{L}}(F, M) - \dim \mathrm{Sel}_{\mathcal{L}^*}(F, M^*) = \dim M^{G_F} - \dim (M^*)^{G_F} + \sum_{v \in \Omega_F} (\dim \mathcal{L}_v - \dim M^{G_{F_v}}).$$

Proof. This follows from [**Wil95**, proposition 5·1(b)]. See also [**Was97**, theorem 2].

Remark 4·3. Note that $E[p]$ is naturally an $\mathbb{F}_p[G_F]$-module and the Weil pairing induces an $\mathbb{F}_p[G_F]$-isomorphism $E[p] \cong E[p]^*$. Making this identification, the local Tate pairing at a place $v \in \Omega_F$ becomes an alternating bilinear pairing on $H^1(F_v, E[p])$, and the two global terms on the right-hand side of Theorem 4·2 cancel.

We firstly define notation for the Selmer structure associated to the usual p-Selmer group.

Definition 4·4. For each finite extension L/F and every place $v \in \Omega_L$, we denote by $\mathscr{S}_v(L; E)$ the image of the coboundary map

$$\delta_v : E(L_v)/pE(L_v) \hookrightarrow H^1(L_v, E[p]),$$

arising from the short exact sequence of G_{L_v}-modules

https://doi.org/10.1017/S0305004124000197 Published online by Cambridge University Press

$$0 \longrightarrow E[p] \longrightarrow E \xrightarrow{p} E \longrightarrow 0.$$

These local groups form a Selmer structure $\mathscr{S}(L) = \mathscr{S}(L;E) = \left\{\mathscr{S}_v(L;E)\right\}_v$. Note that the associated Selmer group is $\mathrm{Sel}_{\mathscr{S}(L)}(L, E[p]) = \mathrm{Sel}_p(E/L)$, the classical p-Selmer group.

Remark 4·5. The local groups $\mathscr{S}_v(L;E)$ above are in fact known to be maximal isotropic subgroups of $H^1(L_v, E[p])$ with respect to the local Tate pairing (see e.g. [**PR12**, proposition 4·10]). In particular, $\mathscr{S}(L)$ is self-dual.

Definition 4·6. For each $v \in \Omega_F$ and any $w \in \Omega_K$ extending v, let

$$\mathscr{F}_v(K/F;E) := \mathrm{res}^{-1}_{K_w/F_v}\left(\mathscr{S}_w(K;E)\right) \leq H^1(F_v, E[p]).$$

Note that the definition does not depend on the choice of w as our extension is Galois. We then have a Selmer structure $\mathscr{F}(K) = \mathscr{F}(K/F;E) = \left\{\mathscr{F}_v(K/F;E)\right\}_v$ for $E[p]$ over F. We further define the Selmer structure $\mathscr{C}(K) = \mathscr{C}(K/F;E)$ for $E[p]$ to be the dual of $\mathscr{F}(K)$, and denote the corresponding local groups by $\mathscr{C}_v(K/F;E)$.

LEMMA 4·7. *We have*

$$\mathrm{Sel}_{\mathscr{F}(K)}(F, E[p]) = \mathrm{res}^{-1}_{K/F}\left(\mathrm{Sel}_p(E/K)\right).$$

Proof. This follows from the compatibility of local and global restriction maps.

LEMMA 4·8. *For every $v \in \Omega_F$ and every place $w \in \Omega_K$ extending v, we have*

$$\mathscr{C}_v(K/F;E) = \mathrm{cor}_{K_w/F_v}\left(\mathscr{S}_w(K;E)\right) \leq H^1(F_v, E[p]).$$

Proof. In the case $p = 2$ this is already noted by Kramer in the paragraph following equation 10 in [**Kra81**], and the proof in this case is explicated in [**MP20**, proof of lemma 4·3(i)]. The result for general p follows *mutatis mutandis*. We replicate it here for the reader's convenience.

For $v \in \Omega_F$ and $w \in \Omega_K$ extending v, it follows from [**Neu13**, I·5·4] and [**Neu13**, II proposition 1·4(c) and theorem 5·6] that res_{K_w/F_v} and cor_{K_w/F_v} are adjoints with respect to the local Tate pairings. By [**PR12**, proposition 4·10], $\mathscr{S}_v(F;E)$ and $\mathscr{S}_w(K;E)$ are maximal isotropic subspaces of the corresponding cohomology groups with respect to the Tate pairings. Thus we have inclusions

$$\mathrm{cor}_{K_w/F_v}\left(\mathscr{S}_w(K;E)\right) \subseteq \mathscr{F}_v(K/F;E)^*$$

and

$$\mathrm{res}_{K_w/F_v}\left(\mathrm{cor}_{K_w/F_v}\left(\mathscr{S}_w(K;E)\right)^*\right) \subseteq \mathscr{S}_w(K;E)^* = \mathscr{S}_w(K;E).$$

The result then follows.

We now relate the Selmer structures $\mathrm{Sel}_{\mathscr{F}(K)}(F, E[p])$ and $\mathrm{Sel}_{\mathscr{C}(K)}(F, E[p])$ to specific representation theoretic invariants of the $\mathbb{F}_p[G]$-module $\mathrm{Sel}_p(E/F)$.

https://doi.org/10.1017/S0305004124000197 Published online by Cambridge University Press

LEMMA 4·9. *Let* $N_{K/F} := \sum_{g\in G} g \in \mathbb{Z}[G]$ *be the norm element. We have that:*

(i) $\dim\left(N_{K/F}\cdot \mathrm{Sel}_p(E/K)\right) \le \dim \mathrm{Sel}_{\mathscr{C}(K)}(F, E[p])$;

(ii) $\dim\left(\mathrm{Sel}_p(E/K)^G\right) = \dim \mathrm{Sel}_{\mathscr{F}(K)}(F, E[p]) - \dim H^1(K/F, E(K)[p]) + \dim(\mathrm{im}(\tau))$,

where $\tau : H^1(K, E[p]) \to H^2(K/F, E(K)[p])$ *is the transgression map.*

Proof. (i) is given by naturality of the corestriction map, which is induced by action of $N_{K/F}$. By Lemma 4·7, the inflation-restriction sequence yields an exact sequence

$$0 \longrightarrow H^1(K/F, E(K)[p]) \xrightarrow{\inf} \mathrm{Sel}_{\mathscr{F}(K)}(F, E[p])$$
$$\mathrm{Sel}_p(E/K)^G \xrightarrow{\tau} H^2(K/F, E(K)[p]).$$
(res)

Thus (ii) holds.

We now introduce the function that will bound the failure Galois descent in our statistical results.

Definition 4·10. We define the genus theory invariant of the p-Selmer group of E arising from the extension K/F to be

$$g_p(K/F; E) := \sum_{v\in\Omega_F} \dim E(F_v)/\left(N_{K_w/F_v}E(K_w) + pE(F_v)\right),$$

where, in each summand, $w \in \Omega_K$ is any place of K lying over v.

LEMMA 4·11. *We have*

$$\dim \mathrm{Sel}_{\mathscr{F}(K)}(F, E[p]) - \dim \mathrm{Sel}_{\mathscr{C}(K)}(F, E[p]) = g_p(K/F; E),$$

and moreover,

$$0 \le \dim \mathrm{Sel}_{\mathscr{F}(K)}(F, E[p]) - \dim \mathrm{Sel}_p(E/F) \le g_p(K/F; E).$$

Proof. For each $v \in \Omega_F$, the groups $\mathscr{C}_v = \mathscr{C}_v(K/F; E)$ and $\mathscr{F}_v = \mathscr{F}_v(K/F; E)$ are orthogonal complements under the local Tate pairing, so we have $\dim \mathscr{F}_v = \dim H^1(F_v, E[p]) - \dim \mathscr{C}_v$. Moreover, since $\mathscr{S}_v(F; E)$ is maximal isotropic, we have $\dim H^1(F_v, E[p]) = 2\dim E(F_v)/pE(F_v)$. Combining this with Lemma 4·8, we obtain

$$\begin{aligned}\dim \mathscr{F}_v &= 2\dim E(F_v)/pE(F_v) - \dim \mathscr{C}_v \\ &= 2\dim E(F_v)/pE(F_v) - \dim\left(N_{K_w/F_v}E(K_w)/\left(pE(F_v)\cap N_{K_w/F_v}E(K_w)\right)\right) \\ &= \dim E(F_v)/pE(F_v) + \dim E(F_v)/\left(N_{K_w/F_v}E(K_w) + pE(F_v)\right).\end{aligned}$$

It then follows from Theorem 4·2 that

$$\begin{aligned}&\dim \mathrm{Sel}_{\mathscr{F}(K)}(F, E[p]) - \dim \mathrm{Sel}_{\mathscr{C}(K)}(F, E[p]) \\ &= \sum_{v\in\Omega_F} \dim E(F_v)/\left(N_{K_w/F_v}E(K_w) + pE(F_v)\right)\end{aligned}$$

https://doi.org/10.1017/S0305004124000197 Published online by Cambridge University Press

$$+ \sum_{v \in \Omega_F} (\dim E(F_v)/pE(F_v) - \dim E(F_v)[p])$$

$$= g_p(K/F; E),$$

where the last equality is obtained by applying Theorem 4·2 to the self-dual Selmer structure $\mathscr{S}(E/F)$, so the first equation in the lemma statement holds.

The second equation follows from the inclusions

$$\mathrm{Sel}_{\mathscr{C}(K)}(F, E[p]) \subseteq \mathrm{Sel}_p(E/F) \subseteq \mathrm{Sel}_{\mathscr{F}(K)}(F, E[p]).$$

5. *Galois Descent for p-Selmer groups*

We will now use the algebraic results of Sections 3 and 4 to obtain our statistical results. This will culminate in a proof of Theorem 1·6 which tells us that, for a finite Galois extension of number fields K/F and a prime number p, as we vary over the E parametrised by $\mathcal{E}(X)$, the average value of

$$\left| \dim \mathrm{Sel}_p(E/K)^{\mathrm{Gal}(K/F)} - \dim \mathrm{Sel}_p(E/F) \right|,$$

which we refer to as the failure of Galois descent, is bounded as $X \to \infty$. We use Lemma 4·9(ii) to relate the Selmer group $\mathrm{Sel}_{\mathscr{F}(K)}(F, E[p])$ to the Galois fixed space, which allows us to use Lemma 4·11 to bound this failure of Galois descent by the genus theory invariant $g_p(K/F; E)$. The remainder of the proof is then showing that the function $g_p(K/F; E)$ has bounded average as E varies in $\mathcal{E}$.

5·1. *Preliminary counting lemmas*

We begin by recalling the description, afforded by Tate's algorithm, of the reduction type of the curves $E_{A,B}$ in terms of the pair $(A, B) \in \mathcal{E}$ at almost all places.

LEMMA 5·1. *For a prime number $\ell \geq 5$ and $(A, B) \in \mathcal{E}$, the reduction type of $E_{A,B}/\mathbb{Q}_\ell$ is:*

(i) I_n for $n > 0$ if and only if $v_\ell(4A^3 + 27B^2) = n$ and $v_\ell(AB) = 0$;
(ii) additive if and only if $v_\ell(\gcd(A, B)) > 0$,

where v_ℓ is the normalised valuation on $\mathbb{Q}_\ell$.

Proof. This is a consequence of Tate's algorithm [**Sil09**, IV·9·4].

PROPOSITION 5·2. *There exists a constant $C > 0$ such that for all real numbers $X \in \mathbb{R}_{>0}$,*

$$\sum_{(A,B) \in \mathcal{E}(X)} \# \left\{ \ell \geq \log(X) : \begin{array}{c} \ell \text{ is prime;} \\ E_{A,B}/\mathbb{Q}_\ell \text{ has bad reduction of type different from } I_1. \end{array} \right\} \leq C \left(\frac{X^{5/6}}{\log(X)} \right).$$

Proof. We split the summand into counts of additive and multiplicative primes.

By Lemma 5·1, primes of additive reduction for $E_{A,B}$ divide $\gcd(A, B)$, so are bounded by the absolute values of A and B. Therefore, we have

https://doi.org/10.1017/S0305004124000197 Published online by Cambridge University Press

$$\begin{aligned}
&\sum_{(A,B)\in\mathcal{E}(X)} \#\left\{\ell \geq \log(X) : \begin{array}{l}\ell \text{ is prime;}\\ E_{A,B}/\mathbb{Q}_\ell \text{ has additive reduction.}\end{array}\right\}\\
&\leq \sum_{\substack{\log(X)\leq \ell\leq X^{1/3}\\ \text{prime}}} \sum_{\substack{|A|\leq (X/4)^{1/3}\\ \ell\mid A}} \sum_{\substack{|B|\leq (X/27)^{1/2}\\ \ell\mid B}} 1\\
&\ll \sum_{\substack{\log(X)\leq \ell\leq X^{1/3}\\ \text{prime}}} \left(\frac{4X^{5/6}}{\ell^2} + O\left(\frac{X^{1/2}}{\ell}\right)\right)\\
&\ll \left(X^{5/6}\int_{\log(X)}^{X^{1/3}} \frac{1}{y^2}dy\right) + X^{1/2}\log\log(X)\\
&\ll \frac{X^{5/6}}{\log(X)},
\end{aligned}$$

where the penultimate inequality uses an integral estimate for the main term, that the sum of reciprocals of prime numbers has order $\log\log(X)$ and the prime number theorem for the error term.

For the multiplicative primes: Lemma 5·1 shows that if ℓ is multiplicative of type different from I_1 for $E_{A,B}$ then $\ell^2 \mid (4A^3 + 27B^2)$ but $\ell \nmid AB$. Hence we have

$$\begin{aligned}
&\sum_{(A,B)\in\mathcal{E}(X)} \#\left\{\ell \geq \log(X) : \begin{array}{l}\ell \text{ is prime;}\\ E_{A,B}/\mathbb{Q}_\ell \text{ has multiplicative reduction of type different from } I_1.\end{array}\right\}\\
&\leq \sum_{\substack{\log(X)\leq \ell\leq \sqrt{31X}\\ \text{prime}}} \sum_{\substack{|A|\leq (X/4)^{1/3}\\ \ell\nmid A}} \sum_{\substack{|B|\leq (X/27)^{1/2}\\ \ell^2\mid 4A^3+27B^2}} 1\\
&\ll \sum_{\substack{\log(X)\leq \ell\leq \sqrt{31X}\\ \text{prime}}} \left(\frac{X^{5/6}}{\ell^2} + O\left(X^{1/3}\right)\right)\\
&\ll \frac{X^{5/6}}{\log(X)}.
\end{aligned}$$

The result follows.

5·2. *Bounding the genus theory invariant*

We begin by noting some elementary bounds on the norm indices which occur as summands in the genus theory invariant (as in Definition 4·10).

LEMMA 5·3. *Let F be a number field, K/F be a finite extension, p be a prime number and E/F be an elliptic curve.*

https://doi.org/10.1017/S0305004124000197 Published online by Cambridge University Press

$$\dim E(F_v)/pE(F_v) \leq \begin{cases} 2+[F_v:\mathbb{Q}_p] & \text{if } v \mid p, \\ 2 & \text{if } v \text{ is a finite place and } v \nmid p, \\ 1 & \text{if } v \text{ is a real place and } p=2, \\ 0 & \text{otherwise.} \end{cases} \tag{4}$$

In particular, for every $v \in \Omega_F$ and each $w \in \Omega_K$ extending v, the same bound holds for $\dim E(F_v)/\left(N_{K_w/F_v}E(K_w)+pE(F_v)\right)$.

Proof. For each finite place $\mathfrak{p} \in \Omega_F$ and each $E/\mathbb{Q}$, there is a finite index subgroup, arising from the filtration by formal groups, of $E(F_\mathfrak{p})$ which is isomorphic to the additive group of integers $\mathcal{O}_\mathfrak{p}$ of $F_\mathfrak{p}$ (see e.g. [**Sil09**, VII proposition 6·3]). Thus these norm indices are bounded by

$$\#E(F_\mathfrak{p})/pE(F_\mathfrak{p}) = (\#E(F_\mathfrak{p})[p])(\#\mathcal{O}_\mathfrak{p}/p\mathcal{O}_\mathfrak{p}) \leq \begin{cases} p^{2+[F_\mathfrak{p}:\mathbb{Q}_p]} & \mathfrak{p} \mid p, \\ p^2 & \text{else.} \end{cases} \tag{5}$$

Moreover, for archimedean places $v \in \Omega_F$, if p is odd or v is complex then we have $\dim E(F_v)/pE(F_v) \leq \dim H^1(F_v, E[p]) = 0$. If, on the other hand, $p=2$ and v is real then elementary computations show that the dimension of the quotient at v is at most 1.

We are now mathematically ready to bound the average of the genus theory invariant, but first we require a small amount of notation.

Notation 5·4. For a number field F, we define the function ω_F on the set of ideals of the integers of F to send the ideal I to

$$\omega_F(I) := \#\left\{\mathfrak{p} \in \Omega_F : \mathfrak{p} \mid I\right\}.$$

We also define $r_1(F)$ to be the number of real embeddings of F. Moreover, δ_2 is the function which takes each prime number p to 1 if $p=2$ and 0 otherwise.

We now bound the average of the genus theory invariant.

PROPOSITION 5·5. *For every number field F, finite Galois extension K/F, prime number p and real number $X \in \mathbb{R}_{>0}$ we have*

$$\frac{\sum_{(A,B)\in\mathcal{E}(X)} g_p(K/F; E_{A,B})}{\#\mathcal{E}(X)} \leq C_p(K/F) + O\left(\frac{[F:\mathbb{Q}]}{\log(X)}\right),$$

where

$$C_p(K/F) = 2\omega_F(6p\Delta_K) + [F:\mathbb{Q}] + \delta_2(p)r_1(F) + 2\sum_{\substack{\ell \text{prime} \\ \ell \nmid 6p\Delta_K}} \omega_F(\ell)\frac{2\ell^8-\ell^7-1}{\ell^{10}-1}.$$

https://doi.org/10.1017/S0305004124000197 Published online by Cambridge University Press

Proof. For each elliptic curve $E/\mathbb{Q}$, number field F, and finite Galois extension K/F, define

$$g_p^{(0)}(K/F;E) = \sum_{\substack{v\in\Omega_F \\ v\mid 6p\infty\Delta_K}} \dim E(F_v)/\left(N_{K_w/F_v}E(K_w)+pE(F_v)\right),$$

$$g_p^{(1)}(K/F;E) = \sum_{\substack{\mathfrak{p}\in\Omega_F \\ \mathfrak{p}\nmid 6p\infty\Delta_K \\ \mathfrak{p}\mid N(E/F)}} \dim E(F_\mathfrak{p})/\left(N_{K_\mathfrak{P}/F_\mathfrak{p}}E(K_\mathfrak{P})+pE(F_\mathfrak{p})\right),$$

where in each summand, w (resp. $\mathfrak{P}$) is a place of K above v (resp. $\mathfrak{p}$), and $N(E/F)$ is the conductor of E/F. By [**Maz72**, corollary 4·4], the norm map is surjective at primes of good reduction which are unramified in K/F, so the norm indices at such primes are trivial. Thus

$$g_p(K/F;E) = g_p^{(0)}(K/F;E) + g_p^{(1)}(K/F;E),$$

so we bound the average of $g_p^{(i)}(K/F;E)$ for $i\in\{0,1\}$.

If $i=0$ then by Lemma 5·3,

$$\sum_{(A,B)\in\mathcal{E}(X)} g_p^{(0)}(K/F;E_{A,B}) \le (2\#\{\mathfrak{p}\in\Omega_F : \mathfrak{p}\mid 6p\Delta_K\} + [F:\mathbb{Q}] + \delta_2(p)r_1(F))\,\#\mathcal{E}(X).$$

We now deal with the case that $i=1$. By Lemma 3·5, the norm index at primes of reduction type I_1 is trivial. Thus, for each elliptic curve $E/\mathbb{Q}$, the sum $g_p^{(1)}(K/F;E)$ is the sum of norm indices at unramified primes of bad reduction of type different from I_1 over F. By the methods of [**CJ20**, theorem 1·4], which work identically for our height as for theirs, for each prime number $\ell\in[5,X^{1/6}]$ one has

$$\#\left\{(A,B)\in\mathcal{E}(X) : \begin{smallmatrix} E_{A,B}/\mathbb{Q}_\ell \text{ has bad reduction} \\ \text{of type different from } I_1\end{smallmatrix}\right\} = \#\mathcal{E}(X)\frac{2\ell^8-\ell^7-1}{\ell^{10}-1} + O\left(\ell X^{1/2}\right). \tag{6}$$

Since we are looking at unramified local extensions $F_\mathfrak{p}/\mathbb{Q}_\ell$, curves with bad reduction of type different from I_1 over $F_\mathfrak{p}$ must satisfy the same condition over $\mathbb{Q}_\ell$. We then have

$$\begin{aligned}
&\sum_{(A,B)\in\mathcal{E}(X)} g_p^{(1)}(K/F;E_{A,B}) \\
&\le 2\sum_{\substack{5\le\ell\le 31X \\ \text{prime} \\ \ell\nmid p\Delta_K}} \sum_{\substack{\mathfrak{p}\in\Omega_F \\ \mathfrak{p}\mid\ell}} \#\left\{(A,B)\in\mathcal{E}(X) : \begin{smallmatrix} E_{A,B} \text{ has bad reduction} \\ \text{of type different from } I_1 \text{ at } \ell\end{smallmatrix}\right\} \\
&\le 2\sum_{\substack{5\le\ell\le\log(X) \\ \text{prime} \\ \ell\nmid p\Delta_K}} \sum_{\substack{\mathfrak{p}\in\Omega_F \\ \mathfrak{p}\mid\ell}} \left(\#\mathcal{E}(X)\frac{2\ell^8-\ell^7-1}{\ell^{10}-1} + O\left(\ell X^{1/2}\right)\right) + O\left(\frac{X^{5/6}[F:\mathbb{Q}]}{\log(X)}\right)
\end{aligned}$$

https://doi.org/10.1017/S0305004124000197 Published online by Cambridge University Press

$$\leq 2\#\mathcal{E}(X) \sum_{\substack{\ell \text{ prime} \\ \ell \nmid 6p\Delta_K}} \#\{\mathfrak{p} \in \Omega_F : \mathfrak{p} \mid \ell\} \frac{2\ell^8 - \ell^7 - 1}{\ell^{10} - 1} + O\left(\frac{X^{5/6}[F:\mathbb{Q}]}{\log(X)}\right),$$

where in the first inequality we bound the norm index by Lemma 5·3, and in the second we discount large primes using Proposition 5·2 and then apply (6). The bound then follows from the well known fact that $\#\mathcal{E}(X) \sim cX^{5/6}$ for some $c > 0$.

5·3. *Proof of Theorem 1·6*

We first use the Selmer structures of Section 4 to approximate the dimension of the corresponding fixed space. To begin, almost no elliptic curves defined over $\mathbb{Q}$ have nontrivial n-torsion over a fixed number field K. The proof of this is obtained verbatim from the argument of Duke [**Duk97**, lemma 5] in the case $K = \mathbb{Q}$, applying the relevant sieve conditions only at totally split primes as performed by Zywina [**Zyw10**, proposition 5·7].

LEMMA 5·6. *Let n be a positive integer and let $K/\mathbb{Q}$ be a finite extension. Then*

$$\frac{\#\left\{(A,B) \in \mathcal{E}(X) : E_{A,B}(K)[n] \text{is nontrivial}\right\}}{\#\mathcal{E}(X)} \ll_{n,K} \frac{\log(X)}{X^{1/6}}.$$

Using this result, we can prove the following.

LEMMA 5·7. *Let p be a prime number, F be a number field and K/F be a finite Galois extension. We have that*

$$\frac{\sum_{(A,B)\in\mathcal{E}(X)} \left|\dim \mathrm{Sel}_p(E_{A,B}/K)^G - \dim \mathrm{Sel}_{\mathscr{F}(K)}(F, E[p])\right|}{\#\mathcal{E}(X)} \ll_{K,p} \frac{\log(X)}{X^{1/6}},$$

where $G = \mathrm{Gal}(K/F)$ is the Galois group.

Proof. Let $D_p(G)$ be a positive integer such that, for every $\mathbb{F}_p[G]$-module M of dimension at most 2 and every $i \in \{1, 2\}$, we have

$$\dim H^i(G, M) \leq D_p(G).$$

Since there are only finitely many such M, $D_p(G)$ certainly exists. By Lemma 4·9, for every elliptic curve $E/\mathbb{Q}$ we have

$$\left|\dim \mathrm{Sel}_p(E_{A,B}/K)^G - \dim \mathrm{Sel}_{\mathscr{F}(K)}(F, E[p])\right| \leq \begin{cases} 0 & \text{if } E(K)[p] \text{ is trivial,} \\ D_p(G) & \text{else.} \end{cases}$$

The result then follows from Lemma 5·6.

We now combine this with Proposition 5·5 to prove Theorem 1·6, namely that the average failure of Galois descent is bounded.

https://doi.org/10.1017/S0305004124000197 Published online by Cambridge University Press

THEOREM 5·8. *Let p be a prime number, F be a number field and K/F be a finite Galois extension. Writing $G = \mathrm{Gal}(K/F)$, we have that*

$$\limsup_{X\to\infty} \frac{\sum_{(A,B)\in\mathcal{E}(X)} \left|\dim \mathrm{Sel}_p(E_{A,B}/K)^G - \dim \mathrm{Sel}_p(E_{A,B}/F)\right|}{\#\mathcal{E}(X)} \leq C_p(K/F),$$

where $C_p(K/F)$ is as in Section 1·5.

Proof. By Lemma 5·7, we immediately have

$$\limsup_{X\to\infty} \frac{\sum_{(A,B)\in\mathcal{E}(X)} \left|\dim \mathrm{Sel}_p(E_{A,B}/K)^G - \dim \mathrm{Sel}_p(E_{A,B}/F)\right|}{\#\mathcal{E}(X)}$$
$$\leq \limsup_{X\to\infty} \frac{\sum_{(A,B)\in\mathcal{E}(X)} \left|\dim \mathrm{Sel}_{\mathscr{F}(K)}(F, E_{A,B}[p]) - \dim \mathrm{Sel}_p(E_{A,B}/F)\right|}{\#\mathcal{E}(X)}.$$

Since by Lemma 4·11 this average is bounded by that of the genus theory invariant, the result follows from Proposition 5·5.

From this we derive an immediate consequence.

COROLLARY 5·9. *Let $p \in \{2, 3, 5\}$ and let $K/\mathbb{Q}$ be a finite Galois extension. Then, writing $G = \mathrm{Gal}(K/\mathbb{Q})$, we have*

$$\limsup_{X\to\infty} \frac{\sum_{(A,B)\in\mathcal{E}(X)} \dim \mathrm{Sel}_p(E_{A,B}/K)^G}{\#\mathcal{E}(X)} \leq C_p(K/\mathbb{Q}) + \frac{p+1}{p},$$

where $C_p(K/\mathbb{Q})$ is as in Section 1·5. Assuming Hypothesis 1 the same is true if p is any prime number.

Proof. This follows from Theorem 5·8 and Proposition 2·11.

Example 5·10. Consider the splitting field $K/\mathbb{Q}$ of $x^3 - 2$, which is a degree 6 extension with Galois group $G \cong S_3$.

If $p = 2$, it follows from Corollary 5·9 that the average dimension of $\mathrm{Sel}_2(E/K)^G$ is at most $C_2(K/\mathbb{Q}) + \frac{3}{2}$. The primes dividing $6p\Delta_K$ are 2 and 3, so that

$$C_2(K/\mathbb{Q}) = 6 + 2\sum_{\substack{\ell\neq 2,3\\ \text{prime}}} \frac{2\ell^8 - \ell^7 - 1}{\ell^{10} - 1} \approx 6.339.$$

Thus, the average of $\dim \mathrm{Sel}_2(E/K)^G$ is less than 7.839.

Similarly, if $p = 3$, the average of $\dim \mathrm{Sel}_3(E/K)^G$ is less than 6.672.

For every prime number p different from 2 and 3, and every elliptic curve $E/\mathbb{Q}$, we have that $\mathrm{Sel}_p(E/K)^G \cong \mathrm{Sel}_p(E/\mathbb{Q})$ by Proposition 2·7 (one can also note this by the vanishing of the finite group cohomology in the inflation restriction sequence). In particular, for $p = 5$ the average of the dimension of this fixed space is at most 6/5 by [**BS13**], and for the remaining p is predicted by the Poonen–Rains heuristics.

https://doi.org/10.1017/S0305004124000197 Published online by Cambridge University Press

6. *Boundedness of Selmer ranks*

In this section we use the modular representation theory of p–groups to leverage the result of Theorem 5·8 to obtain a bound for the average dimension of the entire p–Selmer group, not just that of the fixed space. Combining this with estimates for p–Selmer groups over multiquadratic extensions from Proposition 2·14 we then prove explicit upper bounds for average p–Selmer ranks over Galois p–extensions of $\mathbb{Q}$ and of multiquadratic number fields.

6·1. *p-Selmer ranks for p-extensions*

The modular representation theory of groups of prime order is well known, we recall it below.

LEMMA 6·1. *Let p be a prime number, and G be a cyclic group of order p. The isomorphism classes of finitely generated indecomposable $\mathbb{F}_p[G]$-modules are represented precisely by $\{M_k\}_{k=1}^{p}$, where M_1 is the 1-dimensional vector space $\mathbb{F}_p$ with trivial G-action and M_k is a non-split extension of M_{k-1} by M_1. Moreover, every $\mathbb{F}_p[G]$-module is isomorphic to a unique direct sum of these indecomposable modules.*

Proof. By the orbit-stabiliser theorem we have that there is precisely one simple $\mathbb{F}_p[G]$-module, the trivial module M_1. The result then follows from the Krull–Schmidt theorem and the existence of Jordan normal form (see, for example, [**Alp86**, page 24]).

This will be sufficient to extend the boundedness result to the full p-Selmer group.

THEOREM 6·2. *Let p be a prime number, F be a number field and K/F be a Galois p–extension. Then*

$$\limsup_{X\to\infty} \frac{\sum_{(A,B)\in\mathcal{E}(X)} \dim \mathrm{Sel}_p\,(E_{A,B}/K)}{\#\mathcal{E}(X)} \leq [K:F]\left(C_p(K/F) + \limsup_{X\to\infty} \frac{\sum_{(A,B)\in\mathcal{E}(X)} \dim \mathrm{Sel}_p\,(E_{A,B}/F)}{\#\mathcal{E}(X)}\right),$$

where $C_p(K/F)$ is as in Section 1·5.

Proof. Write $[K:F]=p^k$ for some integer $k>0$. As G is soluble, we let $F=L_0\subseteq L_1\subseteq\cdots\subseteq L_k=K$ be intermediate subfields such that for each $i\in\{1,\dots,k\}$ we have $\mathrm{Gal}\,(L_i/L_{i-1})\cong\mathbb{Z}/p\mathbb{Z}$. We have for each such i that by Lemma 6·1 there are precisely p indecomposable $\mathbb{F}_p[\,\mathrm{Gal}\,(L_i/L_{i-1})]$-modules, each of which is given by mapping a generator to a Jordan block of length between 1 and p. Hence, for every elliptic curve $E/\mathbb{Q}$, we have an inequality

$$\dim \mathrm{Sel}_p\,(E/K) \leq p \dim \mathrm{Sel}_p\,(E/K)^{\mathrm{Gal}\,(K/L_{k-1})}.$$

Moreover, since $\mathrm{Sel}_p\,(E/K)^{\mathrm{Gal}\,(K/L_{k-1})}$ is an $\mathbb{F}_p[\mathrm{Gal}\,(L_{k-1}/L_{k-2})]$-module we again obtain

$$\dim \mathrm{Sel}_p\,(E/K)^{\mathrm{Gal}\,(K/L_{k-1})} \leq p \dim \left(\mathrm{Sel}_p\,(E/K)^{\mathrm{Gal}\,(K/L_{k-1})}\right)^{\mathrm{Gal}\,(L_{k-1}/L_{k-2})}$$

https://doi.org/10.1017/S0305004124000197 Published online by Cambridge University Press

$$= p \dim \mathrm{Sel}_p\,(E/K)^{\mathrm{Gal}\,(K/L_{k-2})}.$$

Continuing, we obtain

$$\dim \mathrm{Sel}_p\,(E/K) \leq p^k \dim \mathrm{Sel}_p\,(E/K)^{\mathrm{Gal}\,(K/F)},$$

so the result follows from Theorem 5·8.

We can then combine the bound in Theorem 6·2 with the bound already established in Proposition 2·14 to obtain the full statement of Theorem 1·7 and so Theorem 1·1 via the inclusion $E(K)/pE(K) \subseteq \mathrm{Sel}_p\,(E/K)$.

COROLLARY 6·3. *Let $p \in \{2, 3, 5\}$, F be either $\mathbb{Q}$ or a multiquadratic number field, and K/F be a Galois p–extension. Then*

$$\limsup_{X\to\infty} \frac{\sum_{(A,B)\in\mathcal{E}(X)} \dim \mathrm{Sel}_p\,(E_{A,B}/K)}{\#\mathcal{E}(X)}$$

$$\leq \begin{cases} [K:F]C_2(K/F) + [K:\mathbb{Q}]\left(C_2(F/\mathbb{Q}) + \frac{3}{2}\right) & \text{if } p = 2 \text{ and } F \neq \mathbb{Q}, \\ [K:F]\left(C_p(K/F) + \frac{p+1}{p}[F:\mathbb{Q}]\right) & \text{else,} \end{cases}$$

where $C_p(K/F)$ is the explicit constant in Section 1·5. Moreover, assuming Hypothesis 1 the same is true if p is any prime number.

Proof. If p is odd, then this is immediate from Theorem 6·2 and Proposition 2·14. If both $p = 2$ and $F = \mathbb{Q}$ then it is immediate from Theorem 6·2 and Proposition 2·11. If $p = 2$ and F is a multiquadratic extension, then we apply Theorem 6·2 twice: first to the extension K/F, then to $F/\mathbb{Q}$, since both are Galois 2–extensions. The result in this case then follows from Proposition 2·11.

7. *Mordell–Weil lattices over Galois extensions*

7·1. *Mordell–Weil lattices*

Our main object of study here will be the Mordell–Weil lattice, which is the "free part" of the Mordell–Weil group.

Definition 7·1. For a number field K and an elliptic curve E/K, the Mordell–Weil lattice is the quotient

$$\Lambda(E/K) := E(K)/E(K)_{\mathrm{tors}}.$$

When K/F is a Galois extension of number fields and E is defined over F, this is evidently a finitely generated $\mathbb{Z}[\mathrm{Gal}\,(K/F)]$-module which is free as a $\mathbb{Z}$-module. We refer to such modules as $\mathbb{Z}[\mathrm{Gal}\,(K/F)]$-lattices. We begin by giving a precise notion of "multiplicity" for indecomposable lattices in Mordell–Weil lattices.

Definition 7·2. Let p be a prime number, K/F be a finite Galois extension of number fields and E/F be an elliptic curve. For each finitely generated $\mathbb{Z}[\mathrm{Gal}\,(K/F)]$ -lattice Λ, define the

https://doi.org/10.1017/S0305004124000197 Published online by Cambridge University Press

multiplicity of Λ in $E(K)$ to be

$$e_\Lambda(K/F;E) := \max\left\{ e \in \mathbb{Z}_{\geq 0} : \begin{array}{l} \Lambda^{\oplus e} \text{ is a direct summand of } \Lambda(E/K) \\ \text{as } \mathbb{Z}[\mathrm{Gal}\,(K/F)]-\text{lattices} \end{array} \right\}.$$

Example 7·3. Let $K/\mathbb{Q}$ be the splitting field of the polynomial $x^3 - 3x - 1$. Note that $K/\mathbb{Q}$ is Galois and has degree 3, and write $G = \mathrm{Gal}\,(K/\mathbb{Q})$. There are two irreducible $\mathbb{Q}[G]$-modules: the line $\mathbb{Q}$, with trivial G-action, and the third cyclotomic field $\mathbb{Q}(\zeta_3)$, where a generator of G acts by multiplication by ζ_3. Moreover, Maschke's theorem tells us that finite dimensional $\mathbb{Q}[G]$-modules are semisimple, so are isomorphic to direct sums of these irreducible modules.

Let $E/\mathbb{Q}$ be the elliptic curve described by the Weierstrass equation

$$E : y^2 + xy = x^3 - x^2 - 42x - 19.$$

The computer algebra program MAGMA [**BCP97**] can compute that E(K) is torsion–free of rank 2 and $E(\mathbb{Q})$ is trivial. Since there are no points fixed by the Galois action, $e_{\mathbb{Z}} = 0$ where $\mathbb{Z}$ is the set of integers acted on trivially by G. Moreover, $E(K) \otimes \mathbb{Q} \cong \mathbb{Q}(\zeta_3)$, so the Mordell–Weil group is isomorphic to a $\mathbb{Z}[\zeta_3]$-stable lattice inside of $\mathbb{Q}(\zeta_3)$. Such lattices are precisely the fractional ideals, and since scaling such a lattice gives an isomorphic module and the class group of $\mathbb{Q}(\zeta_3)$ is trivial, $\Lambda(E/K) = E(K)$ is isomorphic to $\mathbb{Z}[\zeta_3]$ as $\mathbb{Z}[G]$-lattices. In particular, $e_{\mathbb{Z}[\zeta_3]}(E/K) = 1$.

We shall give upper bounds for the averages of some of these exponents by considering the lattice modulo p, and then estimating the various exponents in terms of the fixed space in the p-Selmer group.

LEMMA 7·4. *Let p be a prime number, K/F be a finite Galois extension of number fields, and E/F be an elliptic curve. Writing $G = \mathrm{Gal}\,(K/F)$, we have that*

$$\dim\left(\Lambda(E/K)/p\Lambda(E/K)\right)^G \leq \dim \mathrm{Sel}_p\,(E/K)^G - \dim E(F)[p] + \dim H^1(G, E(K)[p]).$$

Proof. Since $E(K)[p^\infty]/pE(K)[p^\infty] \cong E(K)[p]$ as $\mathbb{Z}[G]$–modules, there is a short exact sequence of $\mathbb{F}_p[G]$-modules

$$0 \longrightarrow E(K)[p] \longrightarrow E(K)/pE(K) \longrightarrow \Lambda(E/K)/p\Lambda(E/K) \longrightarrow 0,$$

so that, taking cohomology over G, we obtain

$$\dim\left(\Lambda(E/K)/p\Lambda(E/K)\right)^G \leq \dim\left(E(K)/pE(K)\right)^G - \dim E(F)[p] + \dim H^1(G, E(K)[p]).$$

Moreover, the short exact sequence induced by multiplication by p gives an inclusion of $\mathbb{F}_p[G]$-modules

$$\delta : E(K)/pE(K) \hookrightarrow \mathrm{Sel}_p\,(E/K),$$

completing the result.

https://doi.org/10.1017/S0305004124000197 Published online by Cambridge University Press

PROPOSITION 7·5. *Let p be a prime number, K/F be a finite Galois extension of number fields, and E/F be an elliptic curve. Writing $G = \mathrm{Gal}(K/F)$, then for every $\mathbb{Z}[G]$-lattice Λ such that $\dim(\Lambda/p\Lambda)^G \geq 1$, we have that*

$$e_\Lambda(K/F;E) \leq \frac{1}{\dim(\Lambda/p\Lambda)^G}\left(\dim \mathrm{Sel}_p(E/K)^G - \dim E(F)[p] + \dim H^1(G,E(K)[p])\right).$$

Proof. If $\Lambda^{\oplus e}$ is a direct summand of $\Lambda(E/K)$, then

$$\left((\Lambda/p\Lambda)^G\right)^{\oplus e} \subseteq (\Lambda(E/K)/p\Lambda(E/K))^G,$$

so that, since $\dim \Lambda/p\Lambda^G \geq 1$, we have

$$e_\Lambda(K/F;E) \leq \frac{\dim(\Lambda(E/K)/p\Lambda(E/K))^G}{\dim(\Lambda/p\Lambda)^G}. \tag{7}$$

Thus the result follows from Lemma 7·4.

7·2. *Average Multiplicities*

We now use Theorem 5·8 to obtain the average multiplicity of certain lattices in Mordell–Weil lattices of elliptic curves.

THEOREM 7·6. *Let K/F be a finite Galois extension of number fields, write $G = \mathrm{Gal}(K/F)$ and let p be a prime number. For every $\mathbb{Z}[G]$-lattice Λ such that $\dim(\Lambda/p\Lambda)^G \geq 1$,*

$$\limsup_{X\to\infty} \frac{\sum_{(A,B)\in\mathcal{E}(X)} e_\Lambda(K/F;E_{A,B})}{\#\mathcal{E}(X)}$$
$$\leq \frac{1}{\dim(\Lambda/p\Lambda)^G}\left(C_p(K/F) + \limsup_{X\to\infty}\frac{\sum_{(A,B)\in\mathcal{E}(X)} \dim \mathrm{Sel}_p(E_{A,B}/F)}{\#\mathcal{E}(X)}\right),$$

where $C_p(K/F)$ is as in Section 1·5.

Proof. Let $D_p(G)$ be an integer such that for every elliptic curve $E/\mathbb{Q}$ we have that

$$\dim H^1(G,E(K)[p]) - \dim E(F)[p] \leq D_p(G).$$

Note that this exists, since there are only finitely many $\mathbb{F}_p[G]$-modules of dimension at most 2. Now, by Lemma 5·6

$$\frac{\sum_{(A,B)\in\mathcal{E}(X)}\left(\dim H^1(G,E(K)[p]) - \dim E(F)[p]\right)}{\#\mathcal{E}(X)} \ll_{K,p} D_p(G)\frac{\log(X)}{X^{1/6}},$$

and the result follows from Proposition 7·5 and Theorem 5·8.

Remark 7·7. The requirement that $(\Lambda/p\Lambda)^G$ is non-trivial for some prime number p is rather easy to check. If $\Lambda^G \neq 0$ then already this is non-trivial for every prime number, and if $\Lambda^G = 0$ then via the short exact sequence induced by multiplication by p, $(\Lambda/p\Lambda)^G$

https://doi.org/10.1017/S0305004124000197 Published online by Cambridge University Press

is isomorphic to the p-torsion of the finite cohomology group $H^1(G, \Lambda)$. Computing this cohomology group in any given instance is a purely mechanical task.

We then immediately obtain Theorem 1·9.

COROLLARY 7·8. *Let $p \in \{2, 3, 5\}$, F be either $\mathbb{Q}$ or a multiquadratic number field, and K/F be a finite Galois extension. Write $G = \mathrm{Gal}(K/F)$, then for every $\mathbb{Z}[G]$-lattice Λ such that $\dim(\Lambda/p\Lambda)^G \geq 1$,*

$$\limsup_{X\to\infty} \frac{\sum_{(A,B)\in\mathcal{E}(X)} e_\Lambda(K/F; E_{A,B})}{\#\mathcal{E}(X)} \leq \frac{1}{\dim(\Lambda/p\Lambda)^G} \cdot \begin{cases} C_2(K/F) + [F:\mathbb{Q}]\left(C_2(F/\mathbb{Q}) + \frac{3}{2}\right) & \text{if } p = 2 \text{ and } F \neq \mathbb{Q}, \\ C_p(K/F) + \frac{p+1}{p}[F:\mathbb{Q}] & \text{else,} \end{cases}$$

where $C_p(K/F)$ is the explicit constant in Section 1·5. Moreover, under Hypothesis 1 the same is true if p is any prime number.

Proof. Applying Theorem 7·6 and Lemma 5·6, it is sufficient to replace the numerator in the left hand side with $\dim \mathrm{Sel}_p(E_{A,B}/F)$ and bound the average appropriately in each case.

If $p \in \{3, 5\}$, then this follows from Proposition 2·14; if $p = 2$ and $F = \mathbb{Q}$ then it follows from Proposition 2·11; and finally, if $p = 2$ and F is a multiquadratic number field then it follows from Corollary 6·3.

7·3. *An example: semidirect products*

We conclude by providing a family of examples of lattices which satisfy the hypotheses of Theorem 7·6 and generalise Example 1·11 from the introduction. Let $K/\mathbb{Q}$ be a finite Galois extension such that $G = \mathrm{Gal}(K/\mathbb{Q})$ is an inner semidirect product $N \rtimes H$. Consider the augmentation ideal $\Lambda \subseteq \mathbb{Z}[N]$, which is defined by the short exact sequence of $\mathbb{Z}[N]$–modules:

$$0 \longrightarrow \Lambda \longrightarrow \mathbb{Z}[N] \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0, \tag{8}$$

where the augmentation map ε is given explicitly by $\sum_{n\in N} a_n \cdot n \mapsto \sum_{n\in N} a_n$.

Identifying each $n \in N$ with the coset $nH \in G/H$ provides an isomorphism of $\mathbb{Z}[N]$–modules $\mathbb{Z}[N] \cong \mathbb{Z}[G/H]$. This identification allows us to induce a G–action on $\Lambda \subseteq \mathbb{Z}[G/H]$, and to upgrade (8) to a short exact sequence of $\mathbb{Z}[G]$–modules. Taking cohomology over N we obtain an exact sequence of $\mathbb{Z}[G/N]$–modules

$$0 \longrightarrow \Lambda^N \longrightarrow \mathbb{Z}[G/H]^N \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow H^1(N, \Lambda) \longrightarrow 0. \tag{9}$$

In particular, as $\mathbb{Z}[G/H]^N = \mathbb{Z} \cdot (\sum_{n\in N} nH)$ so that ε is injective on the fixed points, we have that $\Lambda^N = 0$. By Remark 7·7, since $\Lambda^G \subseteq \Lambda^N = 0$, we have that for every prime number p

$$(\Lambda/p\Lambda)^G \cong H^1(G, \Lambda)[p].$$

https://doi.org/10.1017/S0305004124000197 Published online by Cambridge University Press

It follows from the inflation restriction short exact sequence that $H^1(G, \Lambda) \cong H^1(N, \Lambda)^{G/N}$. Again considering (9), we have that $H^1(N, \Lambda) \cong \mathbb{Z}/\#N\mathbb{Z}$ with trivial G/N–action. In particular, for all primes $p \mid \#N$ we have that

$$(\Lambda/p\Lambda)^G \cong \mathbb{Z}/p\mathbb{Z}.$$

Thus, if $\#N$ is divisible by 2,3 or 5 then by Corollary 7·8 we have that the average of $e_\Lambda(K/\mathbb{Q}; E)$ is bounded as $E/\mathbb{Q}$ runs through elliptic curves ordered by height. Moreover, assuming Hypothesis 1 the same is true for any nontrivial N.

Acknowledgements. The author would like to thank Alex Bartel for countless helpful comments and suggestions. We would also like to thank Efthymios Sofos for helpful comments on an earlier version of this paper. We are grateful to the anonymous referee for their thorough reading of the article, and their insight on the flexibility of the works of Bhargava–Shankar, which prompted the choice of height in the article and also Remark 2·10. Throughout this work, the author was supported by a PhD scholarship from the Carnegie Trust for the Universities of Scotland.

REFERENCES

[Alp86] J. L. ALPERIN. *Local Representation Theory*, Camb. Stud. Adv. Math. vol.11, (Cambridge University Press, Cambridge, 1986). Modular representations as an introduction to the local representation theory of finite groups.

[BCP97] W. BOSMA, J. CANNON and C. PLAYOUST. The Magma algebra system. I. The user language. *J. Symbolic Comput.* **24**(3-4) (1997), 235–265. Computational algebra and number theory (London, 1993).

[BS13] M. BHARGAVA and A. SHANKAR. The average size of the 5-Selmer group of elliptic curves is 6, and the average rank is less than 1. ArXiv:1312.7859v1 [math.NT] (2013).

[BS15a] M. BHARGAVA and A. SHANKAR. Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves. *Ann. of Math.* (2) **181**(1) (2015), 191–242.

[BS15b] M. BHARGAVA and A. SHANKAR. Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0. *Ann. of Math.* (2) **181**(2) (2015), 587–621.

[CJ20] P. J. CHO and K. JEONG. On the distribution of analytic ranks of elliptic curves. ArXiv:2003.09102v1 [math.NT] (2020).

[CR81] C. W. CURTIS and I. REINER. *Methods of Representation Theory, vol. I.* With applications to finite groups and orders, Pure and Applied Mathematics. (Wiley-Interscience, 1981), xxi+819.

[Duk97] W. DUKE. Elliptic curves with no exceptional primes. *C. R. Acad. Sci. Paris Sér. I Math.* **325**(8) (1997), 813–818.

[Gre01] R. GREENBERG. Introduction to Iwasawa theory for elliptic curves. *Arithmetic algebraic geometry* (Park City, UT, 1999), (2001), pp. 407–464.

[HB93] D. R. HEATH-BROWN. The size of Selmer groups for the congruent number problem. *Invent. Math.* **111**(1) (1993), 171–195.

[HB94] D. R. HEATH-BROWN. The size of Selmer groups for the congruent number problem.II. *Invent. Math.* **118**(2) (1994), 331–370. With an appendix by P. Monsky.

[Kan13] D. KANE. On the ranks of the 2-Selmer groups of twists of a given elliptic curve. *Algebra Number Theory* **7**(5) (2013), 1253–1279.

[Kat04] K. KATO. *p-adic Hodge theory and values of zeta functions of modular forms*, Cohomologies p-adiques et applications arithmétiques, III (2004), pp. ix, 117–290.

[Kra81] K. KRAMER. Arithmetic of elliptic curves upon quadratic extension. *Trans. Amer. Math. Soc.* **264**(1) (1981), 121–135.

[LS20] A. LEI and F. SPRUNG. Ranks of elliptic curves over $\mathbb{Z}^2$ -extensions. *Israel J. Math.* **236**(1) (2020), 183–206.

[Maz72] B. MAZUR. Rational points of abelian varieties with values in towers of number fields. *Invent. Math.* **18**(1972), 183–266.

[Maz84] B. MAZUR. Modular curves and arithmetic. *Proceedings of the International Congress of Mathematicians*, vol. 1, 2 (Warsaw, 1983), (1984), pp. 185–211.

[Mil72] J. S. MILNE. On the arithmetic of abelian varieties. *Invent. Math.* **17** (1972) 177–190.

[MP20] A. MORGAN and R. PATERSON. On 2-Selmer groups of twists after quadratic extension, *J. London Math. Soc.* (2). **105**(2) (2022), 1110–1166. ArXiv:2011.04374v1.

[MR04] B. MAZUR and K. RUBIN. Kolyvagin systems. *Mem. Amer. Math. Soc.* **168**(799) (2004), viii+96.

[MR07] B. MAZUR and K. RUBIN. Finding large Selmer rank via an arithmetic theory of local constants. *Ann. of Math.* (2) **166**(2) (2007), 579–612.

[MRS07] B. MAZUR, K. RUBIN and A. SILVERBERG. Twisting commutative algebraic groups. *J. Algebra* **314**(1) (2007), 419–438.

[Neu13] J. NEUKIRCH. *Class Field Theory* (Springer, Heidelberg, 2013). The Bonn lectures, edited and with a foreword by Alexander Schmidt, Translated from the 1967z German original by F. Lemmermeyer and W. Snyder, Language editor: A. Rosenschon.

[PPVW19] J. PARK, B. POONEN, J. VOIGHT and M. M. WOOD. A heuristic for boundedness of ranks of elliptic curves. *J. Eur. Math. Soc. (JEMS)* **21**(9) (2019), 2859–2903.

[PR12] B. POONEN and E. RAINS. Random maximal isotropic subspaces and Selmer groups *J. Amer. Math. Soc.* **25**(1) (2012), 245–269.

[Roh84] D. E. ROHRLICH. On L-functions of elliptic curves and cyclotomic towers, *Invent. Math.* **75**(3) (1984), 409–423.

[SD08] P. SWINNERTON-DYER. The effect of twisting on the 2-Selmer group. *Math. Proc. Camb. Phil. Soc.* **145**(3) (2008), 513–526.

[Sil09] J. H. SILVERMAN. *The arithmetic of elliptic curves*, 2nd ed. Graduate Texts in Math. vol.106 (Springer, Dordrecht, 2009).

[Sil94] J. H. SILVERMAN. Advanced topics in the arithmetic of elliptic curves. *Graduate Texts in Math.* vol.151 (Springer-Verlag, New York, 1994).

[Was97] L. C. WASHINGTON. *Galois cohomology*. Modular forms and Fermat's last theorem (Boston, MA, 1995), (1997), pp. 101–120.

[Wil95] A. WILES. Modular elliptic curves and Fermat's last theorem. *Ann. of Math.* (2) **141**(3) (1995), 443–551.

[Zyw10] D. ZYWINA. Elliptic curves with maximal Galois action on their torsion points. *Bull. London Math. Soc.* **42**(5) (2010), 811–826.